2022 年度調査報告書

戦略的イノベーション創造プログラム（ＳＩＰ）第２期

／ＩｏＴ社会に対応したサイバー・フィジカル・セキュリティ

／ＩｏＴ社会に対応したサイバー・フィジカル・セキュリティに係る海外動向調査及び分析

2022 年 12 月

国立研究開発法人新エネルギー・産業技術総合開発機構

委託先　　株式会社サイバー創研

内容

まえがき

IoT は、Society 5.0　の基盤技術であり、社会インフラ、産業システム、生活環境、自然環境等のフィジカル空間に埋め込まれた IoT 機器が、多様なネットワークを介してクラウド等のサイバー空間と連結され、AI に代表される高度な知識処理やビッグデータとしての分析・解析処理と連携することにより、様々な付加価値やサービスを創出し、フィジカル空間である経済社会に多大な恩恵をもたらすと期待されている。一方、サイバー攻撃の対象は急激に拡大し、攻撃の手法も著しく高度化している。特に、産業社会や家庭生活に新たな価値創造をもたらす IoT の普及・拡大に伴い、サイバー攻撃の脅威は、サイバー空間だけでなくフィジカル空間を合わせた、あらゆる産業活動に潜むようになっている。また、製品やサービスを製造し流通する過程で不正なプログラムの組込みや改造が行われるサプライチェーンリスクの問題も顕在化しつつあり、グローバルなサプライチェーンにおいてサイバーセキュリティ対策の強化が求められている。セキュアな Society 5.0 の実現に向け、様々な IoT 機器を守り、社会全体の安全・安心を確立するため、IoT システム・サービス及び中小企業を含む大規模サプライチェーン全体を守ることに活用できる『サイバー・フィジカル・セキュリティ対策基盤』の開発と実証が「戦略的イノベーション創造プログラム（SIP）第 2 期 /IoT 社会に対応したサイバー・フィジカル・セキュリティ」（以下「 本プロジェクト 」という。）において行われている。

今後は一定の水準のセキュリティ要件を満たさない事業者、製品、サービスがグローバルな調達要件からはじき出される恐れがあり、輸出の大部分を占める製造業の参入機会を確保することが重要な課題となる。このため、米国・欧州等において公的機関等が進める IoT セキュリティとサプライチェーンセキュリティ技術の標準化や制度に関する最新の動向調査を、対象関連機関の有識者へのヒアリング及び文献調査等により調査・分析した。

本報告書では、これらの調査結果を基に、研究開発成果の海外展開を達成するための米国と欧州のステークホルダーとの連携に関する活動案について検討した。また、本プロジェクトで策定した目標項目と国際的な目標水準に新たに盛り込むべき事項について調査・分析を行った。

1　動向調査の成果と達成状況

和文要約

セキュアな Society 5.0 の実現に向け、様々な IoT 機器を守り、社会全体の安全・安心を確立するため、国内では、IoT システム・サービス及び中小企業を含む大規模サプライチェーン全体を守ることに活用できる『サイバー・フィジカル・セキュリティ対策基盤』の開発と実証が「戦略的イノベーション創造プログラム（SIP）第 2 期 /IoT 社会に対応したサイバー・フィジカル・セキュリティ」において行われている。今後は一定の水準のセキュリティ要件を満たさない事業者、製品、サービスがグローバルな調達からはじき出される恐れもあり、これらの開発を促進し社会への普及を進めるには、研究開発のグローバルな国際連携が重要である。

本調査事業では、米国・欧州等における IoT セキュリティ、サプライチェーンセキュリティに関する制度やガイドライン等の標準化動向、技術政策の在り方や業界の最新技術動向を調査した。

米国では、2020 年 12 月の重要インフラへのサイバー攻撃などを契機として、大統領令によるサイバーセキュリティ対策基盤やソフトウェアサプライチェーンの強化に向けた取り組みが加速しており、NIST、CISA 等の政府機関、標準化機関を中心に、多くのサイバー・フィジカル・セキュリティ関連ガイドラインに関するドラフト公開、審議会・セミナー活動が活発に行われ、消費者向け IoT セキュリティと SBOM に関する活動が顕著になってきている。

また、EU においても、2019 年 6 月に制定されたサイバーセキュリティ法や情報セキュリティ指令等に示された要件を具現化すべく、情報セキュリティ機関である ENISA の強化が行われ、サイバーセキュリティ強化の活動が展開されている。さらに、Horizon 2020 を契機として設立された、Cybersecurity Competence Centre/Network (ECCC) を中心に、欧州各国の Network of National Coordination Centre (NCC)と連携して欧州のサイバーセキュリティにおけるイノベーションと産業政策を支援する活動が行われている。また、サイバーレジエンス法案が発表され、サイバーセキュリティのための措置に関する指令が欧州議会で承認されるなど、欧州での制度面での整備が進展している。

本報告書では、これらの調査結果を基に、本プロジェクトの国際連携に関する現状の課題を整理し、研究開発を加速し国際連携を推進するためのステークホルダーとして、米国の NIST と、欧州の ENISA、および ETSI を対象として連携の方法を提言した。

例えば、2022 年 12 月に公開されている NIST SP 1800-36 (Draft)に関するパブリックコメントの機会を活用して、SIP-CPS の研究成果を基に提案コメントを寄せることにより相互の連携・交流を行う契機とすることが考えられる。一方、NIST の活動で検討されてきた多くのガイドライン文書は最終版として確定されてきており、本プロジェクトの活動成果をガイドライン文書に盛り込むことが難しくなっているものもある。これらのガイドライン文書については、その具体運用や今後の改定において本プロジェクトの活動成果を反映する活動が可能である。今後の連携・協力関係の構築を図る上で NIST へのこのような活動を継続することが重要である。

また、米国においては、政府機関のセキュリティ強化をホワイトハウスが主導し、政府機関は連携してその強化のための活動を行っている。日本国内の活動を集約し政府の活動として米国政府の活動と戦略的な連携を働きかけることも、米国のステークホルダーとの連携には重要と考えられる。

欧州との連携に関しては、日本と EU の既存の ICT 国際連携の枠組みを活用して本プロジェクトの活動成果を伝える活動と、本プロジェクトの参加企業が欧州の現地法人を通じて欧州の標準化機関等の CPS 関連活動へ参加する活動を平行して進めることが重要である。

国際的な目標水準に盛り込むべき事項に関しては、世界の最新技術動向を調査し、本研究開発の目標と比較することにより、新たに追加が必要と考えられる 5 つの評価項目を選定し、その目標水準の設定の参考となる技術を提示した。NIST IoT Program の発行文書と SIP-CPS の成果の対応関係が本プロジェクトの研究開発担当メンバーにより示されている。これに加え、SIP-CPS に追加が必要と考えられる評価項目と SIP-CPS の成果との対応関係を、提示した技術の実現レベル

を現在のトップレベルと位置付けて分析することにより新たな国際的な目標水準を設定する活動とすることを提案する。

英文要約

In order to establish the safety and security of society as a whole for the realization of a secure Society 5.0, the development and demonstration of a "Cyber Physical Security Infrastructure" which can be utilized to protect IoT system/services and large-scale supply chains including SMEs is being conducted under the "Strategic Innovation Program Phase 2: Cyber Physical Security for IoT Society" (SIP-CPS) project in Japan. In the future, businesses, products, and services that do not meet a certain level of security requirements may be excluded from global procurement, and global international collaboration in research and development is important to promote the development and diffusion of these products and services to society.

In this research project, we investigated the latest trends in systems and guidelines related to IoT security and supply chain security in the United States, Europe, and other countries.

In the U.S., several cyber-attacks on critical infrastructure in December 2020 and other incidents have accelerated efforts to strengthen cyber security countermeasure infrastructure and software supply chains through executive orders issued by J. Biden, and many government agencies and standardization organizations, such as NIST and CISA, have been working on a number of Drafts on cyber physical security related guidelines are being released, and council and seminar activities are being actively conducted. In addition, activities related to consumer IoT security and SBOM are becoming more prominent. In the EU, activities to strengthen cyber security are also underway, with the strengthening of European Network and Information Security Agency (ENISA) to embody the requirements set forth in the Cyber Security Law and Information Security Directive enacted in June 2019. In addition, the Cybersecurity Competence Centre/Network (ECCC), which was established in the wake of Horizon 2020, and the Network of National Coordination Centers (NCC) in European countries are working together to support innovation and industrial policy in cybersecurity in Europe. Furthermore, institutional developments in Europe are progressing with the publication of proposal for Cyber Resilience Act and the approval by the European Parliament of Directive on measures for a high common level of cybersecurity across the Union.

Based on the results of these surveys, this report summarizes the current issues related to international collaboration on SIP-CPS project and recommends future collaboration methods targeting NIST in the US, ENISA in Europe, and ETSI as stakeholders to accelerate R&D and promote international collaboration.

For example, taking the opportunity for public comments on NIST SP 1800-36 (Draft), which is available in December 2022, will provide an opportunity for mutual collaboration by providing proposal comments based on SIP-CPS research results. On the other hand, many guideline documents that have been published in NIST activities have been finalized as final versions, and it has become difficult to incorporate the results of this project's activities into the guideline documents. However, it is possible to reflect the results of this

project's activities in the operation and future revision of these guideline documents. It is important to continue such activities to NIST in order to establish future collaboration and cooperative relationships.

In the United States, the White House is leading the effort to strengthen security at government agencies. Several government agencies are working together to strengthen them. It is important for cooperation with U.S. stakeholders to consolidate activities in Japan and encourage strategic coordination with U.S. as a government activity.

In Europe, it is important to communicate the results of this project's activities using the existing framework for international ICT collaboration between Japan and the EU, and at the same time to encourage companies in this project to participate in CPS-related activities of European standardization organizations through their local subsidiaries in Europe.

Regarding additions to the international target level, we surveyed the latest global technological trends and selected five evaluation items that need to be added in comparison with the goals of this R&D, and presented the technologies that will serve as a reference for setting the target level. The correspondence between the NIST IoT Program's published documents and the SIP-CPS results has been presented by the members in this project. In addition to this, we propose to analyze the correspondence between the SIP-CPS results and the evaluation items that need to be added to the SIP-CPS, and to make this an activity to set a new international target level.

2　動向調査の目的

本調査事業では、米国・欧州等における IoT セキュリティ、サプライチェーンセキュリティに関する制度やガイドライン等の標準化動向、技術政策の在り方や業界の最新技術動向を調査・分析することによって、本プロジェクトの国際連携を推進すること、海外のステークホルダーとの連携に関する活動案をまとめることを目的とする。また、本プロジェクトで開発する技術の国際的な目標水準の妥当性について調査・分析することを目的とする。

3　事業の概要

本調査事業では、以下の調査・分析活動を行った。

① 海外における制度、標準、規制、技術などの動向に関する調査

米国・欧州等において公的機関公的機関が進める IoT セキュリティとサプライチェーンセキュリティ技術の標準化や制度に関する最新の動向調査を、対象関連機関の活動に精通した有識者へのヒアリング及び文献調査等により実施した。本報告の 4.1 節にて報告する。

② 海外における制度や標準のとりまとめプロセスに関する調査

上記①の動向調査と並行し、IoT セキュリティとサプライチェーンセキュリティに関する公的機関などが関連する産業や他の公的機関（他国含む）と、どのように連携標準を取りまとめようとしているかについて動向調査を行なった。本報告の 4.2 節で報告する。

③　海外における技術開発プロジェクト等における技術目標に関する調査

海外の IoT セキュリティ技術とサプライチェーンセキュリティ技術に関連する技術開発プロジェクトについてヒアリングにより候補を抽出し、先端のセキュリティ製品等とあわせて、それらのプロジェクトの達成目標レベルについて文献調査等を行った。本報告の 5.1 節で報告する。

④　調査結果の分析と取りまとめ

上記①②の調査を通して、本プロジェクトに係る制度や標準等の検討の進め方に関する課題を抽出し、①②の調査結果と併せて取りまとめ、結果の分析から海外のステークホルダーとの連携に関する活動案をまとめた。本報告の 4.3 節で報告する。

また、上記③において調査・分析した結果から、実証評価 WG で策定した国際的な目標水準に新たに盛り込むべき事項をとりまとめ、提言を行う。本報告の 5.2 節で報告する。

⑤　WG 運営業務

海外動向調査 WG の開催、日程調整、議事録の作成など、WG の事務局及び運営全般を行い、運営に係る費用全般の支払いを行った。

また、WG に関連する資料の立案・作成を、本プロジェクトのプログラムディレクター・NEDO 及び本プロジェクト関係者と協議の上行ない、資料作成にあたっては、本プロジェクトについての知見の有無にかかわらず多くの方に理解できるよう努めた。本報告の 6 章で報告する。

4　海外における制度、標準、規則、技術などの動向に関する調査

4.1　海外における制度、標準、規則、技術などの動向

4.1.1 調査方法

本プロジェクトの国際連携の推進のために、IoT セキュリティとサプライチェーンセキュリティ技術の標準化や制度に関する最新の動向を調査する。

米国の NIST（米国立標準技術研究所）と ENISA （欧州サイバーセキュリティ庁）などに加え、標準化組織と世界の主要企業が参加する業界組織、これらの関連情報を入手することができた組織を調査対象として、調査対象組織による報道発表や公開情報などを基本とする文献情報を調査した。調査対象とした組織を表 1 に示す。

また、海外における NIST や ENISA 等の公的機関が進める標準化や制度に関する調査を強化するために、米国在住の調査協力者から入手した対象組織等の活動と、IoT セキュリティとサプライチェーンセキュリティに関する情報についても調査対象とした。調査から得られた情報を一覧表（付表）に集約し、分析を行った。分析結果は 4.2 にて制度や取りまとめのプロセスの具体事例として記述する。

表 1　調査対象組織

	組織略称	組織名	説明
米国	CISA ‡	CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY／サイバーセキュリティ・インフラストラクチャセキュリティ庁	独立した米国連邦機関。国土安全保障省（DHS）の監視下にある運用部門。2018 年発足。サイバーセキュリティの問題に対処し今日直面している電子的、物理的、人為的、技術的、自然的などのあらゆる脅威から身を守り、将来に向けてより安全で回復力のあるインフラストラクチャを構築するために政府機関と民間機関の両方を支援する。
	DHS ‡	United States Department of Homeland Security／米国国土安全保障省	テロリズムの防止、国境の警備・管理、出入国管理と税関業務、サイバーセキュリティ、防災・災害対策を使命とする 2004 年発足の米国連邦政府の行政機関。
	NIST †	The National Institute of Standards and Technology／米国立標準技術研究所	商務省の傘下組織。経済的安全保障を高め、生活の質を向上させるような方法で測定科学、標準、及び技術を進歩させることによって、米国の技術革新及び産業競争力を促進することを使命とする。1901 年設立。Information Technology Laboratory にて IoT を取り巻くいわゆるサイバーセキュリティに関わる活動を行っている。
欧州	ENISA ‡	The European Union Agency for Cybersecurity／欧州サイバーセキュリティ庁	欧州連合の専門機関の一つ。EU 加盟国をはじめとする関係者と連携し、アドバイスやソリューションを提供しサイバーセキュリティ能力の向上を図る。国境を越えたサイバーセキュリティのインシデントや危機への対応を支援し、サイバーセキュリティの認証スキームを策定している。2004 年発足。
	ETSI †	European Telecommunications Standards Institute／欧州電気通信標準化機構	EU が後援し情報通信技術に世界的に適用可能な標準を作成している欧州の電気通信の全般にかかわる標準化組織。
	CyberSec 4Eupope	Cyber Security for Europe／（欧州サイバーセック）	欧州連合が資金提供を行っている研究開発プロジェクト。将来の欧州サイバーセキュリティ・コンピタンスネットワークのためのガバナンス構造の可能性を設計、テスト、実証している。
業界	GSMA*	GSM Association／GSM アソシエーション	GSM 方式の携帯電話システムを採用している移動体通信事業者や関連企業からなる業界団体。当該システムでの標準化や技術開発、宣伝活動の支援を目的に 1995 年に設立された。
その他	CYBER SEC	European Cybersecurity Forum／欧州サイバーセキュリティフォーラム	欧州最大級のサイバーセキュリティイベントの 1 つ。テクノロジーがもたらす現在の課題、新たなサイバー脅威、敵対的なインターネットに対処する方法について意見を共有し、共有された価値観に基づいてグローバルなサイバーセキュリティシステムの創造と実施のための安全なロードマップを提供する。
	EIAS	European Institure for Asian Studies／欧州アジア研究所	ブリュッセルに拠点を置くシンクタンク。EU とアジアの関係に焦点を当て、政策研究センターとして欧州連合とアジアの理解を促進することを目的としている。
	MDPI	Multidisciplinary Digital Publishing Institute／（多元的デジタル出版研究所）	スイスのバーゼルにある学術関連の出版社。あらゆる分野のオープンな科学交流を促進することを使命とし、319 誌の多様な査読付きオープンアクセスジャーナルを出版。1996 年設立。
	RUSI ‡	Royal United Services Institute for Defence and Security Studies／英国王立防衛安全保障研究所	1831 年に創設された防衛・安全保障分野における世界で最も古いイギリスのシンクタンク。

† 標準化組織／ ‡ 政府機関等／* 業界組織／

4.1.2 調査結果

調査対象期間中に調査を行った米国、欧州における IoT セキュリティとサプライチェーンセキュリティに関連する動向情報の一覧を巻末の付表に示す。これらの情報を基に、米国、欧州における主要な動向情報を整理して、以下に示す。

4.1.3 米国の動向

本節では、対象期間中、アメリカ合衆国でのいわゆる Internet of Things (以下 IoT と略記)を中心とした動静を、The National Institute of Standards and Technology (以下 NIST と略記)を中心に記す。対象期間中 6 月 22 日に NIST Cybersecurity for IoT Program が online で実施した Workshop を中心に NIST の IoT security に関連する主な動向を観測することができ、8 月 25 日に MITRE が McLean, Virginia 所在の MITRE Campus にて会場開催で実施した Workshop からも主要な Supply Chain Security に関連する主な動向を観測することができる。本節では、まず対象期間中に NIST が発行した関係文書類を時系列順に報告し、続いて IoT に関する米国連邦政府諸機関の動静、Supply Chain に関する米国連邦政府諸機関の動静を報告し、最後に IoT 並びに Software Supply Chain について連邦政府外で観察された諸動向を報告する。

4.1.3.1 NIST 発行の文書類

本稿対象期間中を中心に、今年 NIST より発行された IoT 並びに Supply Chain Security に関連する文書類を以下に時系列順に示す。

(1) Report for the Assistant to the President for National Security Affairs (APNSA) on Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software（以下、Summary Report と略記）[1]

2022 年 5 月 10 日発行。昨年発行の Executive Order 14028: Improving the Nation's Cybersecurity（以下 EO 14028 と略記）により NIST に課せられた指示への回答と位置付けられる。文書正式名称に見られる通り、内容は IoT 並びに Software の消費者向けのわかりやすい Labeling

[1] 報告本文
<https://www.nist.gov/system/files/documents/2022/05/24/Cybersecurity%20Labeling%20for%20Consumers%20under%20Executive%20Order%2014028%20on%20Improving%20the%20Nation's%20Cybersecurity%20Report%20(FINAL).pdf>
EO14028 に対する NIST 活動のポータル Improving the Nation's Cybersecurity: NIST's Responsibilities Under the May 2021 Executive Order: <https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity>
Cybersecurity Labeling for Consumers: <https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/cybersecurity-labeling-consumers-0>
NIST IoT Product Criteria: <https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/iot-product-criteria>
News and updates <https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/news-updates>

策定に関する要旨報告である。 報告は下記のように構成されている。

1. 当該活動の履歴
2. IoT 並びに Software Labeling 文書に寄せられたコメント類の統計
3. IoT Labeling Criteria について（3. Arriving at the Recommended Criteria に記載）
4. 結論

とされている。

(2) NIST SP 800-161 Rev.1 (Final): Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations[2]

2022 年 5 月 5 日発行。Cybersecurity Supply Chain Risk Management Program (以下 C-SCRM と略記) [3]による NIST SP 800-161 の改版であるが、同時に昨年発令の EO 14028 Section 4 (c), (d)により NIST に課せられた課題への回答が Appendix F に記載されている[4]。

(3) NIST Cybersecurity SCRM Fact Sheet[5]

2022 年 5 月 12 日発行[6]。上述の SP 800-161 Rev.1 を発行した C-SCRM の概況報告書。NIST が検討している Risk Management は組織全体の Risk Management の一環として位置づけられるべきとし、組織全体の Risk Management として、

1. Managing Information Security Risk (NIST SP 800-39)
2. NIST Cybersecurity Framework
3. Integrating Cybersecurity and Enterprise Rick Management (NISTIR 8286)

の 3 文書がこの典拠、依存文書として例示されている。また報告書の 2 頁には、C-SCRM のこれまでの成果文書が一覧されており[7]、当分野の目録として役立ちうる。

(4) NISTIR 8425 Profile of the IoT Core Baseline for Consumer IoT Products[8]

2022 年 6 月 17 日に Draft が発行され、同 7 月 31 日までコメントが受け付けられた後、同 9 月 20 日に最終版が公開された。NIST Cybersecurity for IoT Program が従前発行してきた

---

[2] <https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final>
関連報道として、<https://www.nextgov.com/cybersecurity/2022/05/nists-supply-chain-security-guidance-tells-agencies-look-fedramp-first/366564/>

[3] <https://csrc.nist.gov/projects/cyber-supply-chain-risk-management>

[4] <https://www.nist.gov/news-events/news/2022/05/new-eo-guidance-cybersecurity-supply-chain-risk-management>, <https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains>

[5] <https://csrc.nist.gov/csrc/media/Projects/cyber-supply-chain-risk-management/documents/C-SCRM_Fact_Sheet.pdf>
関連報道として、<https://www.nextgov.com/cybersecurity/2022/05/nists-supply-chain-security-guidance-tells-agencies-look-fedramp-first/366564/>

[6] <https://csrc.nist.gov/projects/cyber-supply-chain-risk-management>

[7] 筆頭に、NIST SP 800-161 Revision 1 が掲載されている。

[8] <https://csrc.nist.gov/publications/detail/nistir/8425/final>

NISTIR8259 シリーズ[9] （NISTIR 8259 [10], 8259A[11] , 8259B[12] ,8259C[13]）は IoT 全般を対象とし、特定分野向けの IoT を対象としてきたものではなかったが、今回の NISTIR 8425 は Consumer IoT という特定分野を対象と位置付けられている[14]。あわせて 2021 年 5 月 12 日発行の Executive Order 14028 で NIST に具体的に課された Criteria Cybersecurity Labeling for Consumer Internet of Things (IoT)を強く意識しており、例えば従来の NISTIR 8259 では前提として想定されていたが、語彙としては定義されていなかった IoT Product について定義、規定するなど[15] Consumer IoT という特定の分野を対象とした各論という位置付けと考えられる。

本文の内容は、Consumer IoT に必要とされる要件である設定変更機能、データ保護、Interface access control など技術的な要件に加え、Documentation, 製造業者の外部から連絡できるセキュリティ受付の設置、セキュリティ情報の一般への連絡、Education and Awareness など、非技術的な要件で構成されている。

(5) Discussion Paper: Ideas for the Future of IoT Cybersecurity at NIST[16]

2022 年 6 月 21 日発行。NIST Cybersecurity for IoT Program の次の課題について、初期的な検討資料と考えられる。従来の NISTIR 8259 シリーズを始めとする文書類や従来の活動一般は、IoT の製造業者が想定する、あるいは想定できるユーザーとユースケースを前提としてきた。ところが、現在製造業者が想定していなかったユーザーによる利用、想定外のユースケースでの利用が見られ、また IoT そのものも機能も制約も多種多様なため、特にこのような例外的な状況において、リスクの把握が困難な状況でどのようにリスクの把握、特定を行うか、という問題提起がなされている。

---

[9] NISTIR 8259 Series <https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series>

[10] Foundational Cybersecurity Activities for IoT Device Manufacturers <https://csrc.nist.gov/publications/detail/nistir/8259/final>

[11] IoT Device Cybersecurity Capability Core Baseline <https://csrc.nist.gov/publications/detail/nistir/8259a/final>

[12] IoT Non-Technical Supporting Capability Core Baseline <https://csrc.nist.gov/publications/detail/nistir/8259b/final>

[13] Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline < https://csrc.nist.gov/publications/detail/nistir/8259c/draft>

[14] 同 1. Introduction

[15] NIST Cybersecurity for IoT Program では、従来 IoT “device”を対象とし、IoT “Product”は昨年発行の EO 14028 に呼応して作成された Labeling 文書 ”Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products” <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf>で示された。

[16] .<https://www.nist.gov/system/files/documents/2022/06/21/IoTRiskIdentificationDiscussionPaper.pdf>, <https://csrc.nist.gov/News/2022/nist-iot-cybersecurity-program-releases-new-docume>

(6) SP 1800-36 (Draft): Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management: Enhancing Internet Protocol-Based IoT Device and Network Security (Preliminary Draft)

2022 年 12 月 5 日公開され、2023 年 2 月 3 日締め切りでコメントの受付が行われている。公開された Draft を見る限り、SP 1800-36 (Draft)の A パートの全部あるいは一部となる Executive Summary 部分のみだが、ここから SP 1800-36 が目指す目的や内容が理解できる。公開されたドラフトから、SP1800-36 は IoT 端末と接続されるネットワークの相互認証、すなわち端末は接続されるべき正しいネットワークであり、不正なネットワークでないことを認証し、ネットワークは接続が正当とされる IoT であることを認証するための具体的なガイドを目指すものと考えられる。構成として、SP 1800-36A: Executive Summary、SP 1800-36B: Approach, Architecture, and Security Characteristics, そして SP 1800-36C: How to Guides の 3 部構成を予定している。文中で扱われる予定の解決策 (Solutions) は、NIST Cybersecurity Framework security standards and guidelines, NISTIR 8259A12, NISTIR 8228 に加え、ETSI EN 303 645 に規定される要件との対応関係が結び付けられる予定 (will map to) とされている。

IoT Onboarding は、SIP-CPS の研究開発で培われた「信頼の創出、証明」と一致し役立ちうる点が多いと考えられる。この分野で実装可能な具体的な知見を持つのは、SIP-CPS と FIDO FDO[17] と推察されることから、可能であればコメント締め切りまでに NIST にコメントをよせることができると考えられる。

4.1.3.2 IoT に関する米国政府および関連機関の動静

(1) NIST Online Workshop: ”Building on the NIST Foundations: Next Steps in IoT Cybersecurity”

2022 年 6 月 22 日、NIST Cybersecurity for IoT Program は Online 形式で、”Building on the NIST Foundations: Next Steps in IoT Cybersecurity” と題した Workshop を実施した[18]。会議後、数時間分の録画が掲出され、同 7 月 15 日には Katerina Megas, Program Manager 執筆の blog により会合の概要が示された[19]。更に同 9 月 20 日、NISTIR8431 Workshop Summary Report for “Building on the NIST Foundations: Next Steps in IoT Cybersecurity” が、会議報告として公開されている[20]。これらの文献を総合すると、IoT セキュリティについて何らかの Standards（標準）は必要であること、他方サプライチェーンは世界規模で展開されており、セキュリティ要件の強制は困難であること、IoT 機器がネットワークに接続され、当初想像されていなかった利用をされるとリスク評価が極めて困難なことなどが指摘、議論された模様。基調講演では、Chief Product Security Officer（CPSO）が講演を行い、NISTIR8431 でもその重要性が

[17] <https://fidoalliance.org/iot-specifications-overview-2/>

[18] <https://www.nist.gov/news-events/events/2022/06/building-nist-foundations-next-steps-iot-cybersecurity>, Agenda: <https://www.nist.gov/agenda/building-nist-foundations-next-steps-iot-cybersecurity>

[19] <https://www.nist.gov/blogs/standards-cpsos-best-friend>

[20] <https://csrc.nist.gov/publications/detail/nistir/8431/final>

Takeaway 1 として本文 5 頁に記述されている。この CPSO とはインシデント対応の世界でいう PSIRT の責任者に相当すると考えられ、製品製造業者において PSIRT に見られるような機能の確立、充実が求められているように思われる。実際、過去にご報告した通り、EO14028 への回答として作成された NIST Cybersecurity Whitepaper[21] でも、個別 Criteria 群の後半には明らかに PSIRT の諸機能が期待されていることがうかがえる。

(2) The Whitehouse の動向

昨年の EO 14028 に対する回答、報告の様々な締め切りが 2022 年前半に集中していたが、2022 年後半になり、IoT 関連分野の動向に動きが出てきている。そのうち象徴的なものとして、FACT SHEET: Biden-Harris Administration Delivers on Strengthening America's Cybersecurity[22] が挙げられる。当文献は 2022 年 10 月 11 日に The Whitehouse より発行。いわゆるサイバーセキュリティに関するこれからの政策につき 11 項目が示されている、そのうち、"Developing a new label to help Americans know their devices are secure" という項目で IoT Labeling について以下の 2 点が言及されている。

- 今月 2022 年 10 月に企業、関係団体、政府などを招き、IoT devices についてラベルの開発について議論すること
- セキュリティリスクと影響が最も大きいと考えられるルータ[23]とホームカメラから始めること

このうち、最初のラベル開発の議論は 2022 年 10 月 19 日に The Whitehouse にて開催された Workshop で実施され、2023 年春開始を目標として消費者向け IoT 製品の Labeling Program の検討を進めることが確認された。詳細は会議後の発表[24] に示されているが、政府、民間とも主要な関係者が集結し、特に政府側参加者の真剣度が伝わってくる。会合には欧州委員会も参加しており、欧州の合意を基に事実上の世界標準を目指していることも考えられる。民間事業者の多くが米国企業であるが、韓国から Samsung, LG、日本から SONY が参加している。

(3) U.S. Department of Commerce Appoints Members for New Internet of Things Advisory Board

NIST も所属している U.S. Department of Commerce（米国商務省）は新たに設立された Internet of Things Advisory Board (IoTAB) の専門家 16 人を指名し、2022 年 10 月 24 日に発表

---

[21] NIST Cybersecurity Whitepaper Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf>

[22] <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/11/fact-sheet-biden-harris-administration-delivers-on-strengthening-americas-cybersecurity/>

[23] ここにおける「ルータ」とは、企業向け、あるいは Internet Backbone 向けのルータではなく、IoT の文脈で言われる Home/SOHO routers を指すと考えるのが妥当と考えられる。

[24] <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/20/statement-by-nsc-spokesperson-adrienne-watson-on-the-biden-harris-administrations-effort-to-secure-household-internet-enabled-devices/>

した[25]。この IoTAB は、2021 連邦政府会計年度版 National Defense Authorization Act の求める要件として、the Federal Advisory Committee Act に基づき設立とされ、NIST が運営支援を実施とされる。

(4) FBI Private Industry Notification

2022 年 9 月 12 日、FBI より Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities と題する民間への警戒を喚起する文書が公開された。（FBI PIN Number 20220912-001）[26]

内容は、IoT に見られる共通した脆弱性などが説明されているが、医療機器が対象とされ人命に関わりうるためか、危機感の高い記述が諸所に見られるのが特色である。CISA のトップ、Jen Easterly 氏は Mandiant Worldwide Information Security Exchange (mWISE™) Conference にて、水道、病院、小中高学校を来年の優先領域とする旨発言したと報じられており[27]、また米国、欧州とも医療分野の IoT への関心は総じて高いこと、医療分野への攻撃も残念ながら高止まりしていることも背景かと思われる。

4.1.3.3 Supply Chain Security に関する米国政府および関連機関の動静

本調査期間中に見られた Supply Chain Security, 特に、Software Supply Chain Security を中心に以下に示す。

(1) MITRE Hot topics in Supply Chain Security

MITRE の Robert Martin 氏を中心に開発が進められてきた Supply Chain Security 強化を目的とした Software of Trusts Framework が 2022 年 6 月にサンフランシスコで開催の RSA Conference 2022 で発表され[28]、同時に MITRE に専用のサイト[29]が公開された。その後、HITCON でも基調講演の一つとして発表が行われた[30]。更に 8 月 25 日には、アメリカ・ヴァージニア州の MITRE McLean Campus にて、Hot Topics in Supply Chain Security Summit[31]が開

---

[25] <https://www.nist.gov/news-events/news/2022/10/us-department-commerce-appoints-members-new-internet-things-advisory-board>、Internet of Things Advisory Board: <https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/internet-things-advisory-board>

[26] <https://www.ic3.gov/Media/News/2022/220912.pdf>

[27] <https://www.cybersecuritydive.com/news/CISA-water-schools-healthcare/634657/>

[28] <https://www.rsaconference.com/usa/agenda/session/Addressing%20Supply%20Chain%20Security%20Risks%20MITREs%20System%20of%20Trust>, <https://www.rsaconference.com/library/Video/2022-quick-look-addressing-supply-chain>

[29] <https://sot.mitre.org>

[30] <https://hitcon.org/2022/en/agenda/635efb14-6be6-4f43-bb15-3596e1d169f4/>

[31] 開催元 MITRE からの通知<https://groups.google.com/a/list.nist.gov/g/sw.assurance/c/EPL2JrdboS4>, <https://groups.google.com/a/list.nist.gov/g/sw.assurance/c/4M9DwcZmaEU>
会合総合案内 <https://na.eventscloud.com/website/43098/>
Agenda: <https://na.eventscloud.com/website/43098/home/#Agenda>
Robert Martin 氏も関わっているとされる IETF SCITT WG の IETF115 での最新の議論は以下より入手可能。<https://datatracker.ietf.org/group/scitt/documents/>
<https://datatracker.ietf.org/meeting/115/materials/slides-115-scitt-combined-scitt-presentations-00>

催された。

(2) Software Supply Chain Guidance from NSA, CISA, and ODNI

National Security Agency (NSA)[32] , CISA[33], 並びに Office of the Director of National Intelligence (ODNI)[34]の 3 者連名による、Software Supply Chain Guidance3 部作が、9 月 1 日以降順次発行され始めている。

まず、9 月 1 日付報道発表[35]によると 、Securing the Software Supply Chain- Recommended practices guide for developers[36] が一般公開された。CISA の当該報道発表によると 3 部作の最初の第 1 部とされる[37]。内容は既存の基本的な文献である NIST SSDF[38] あるいは SBOM などが随時参照されたソフトウェア開発者向けの Software Supply Chain の指南書と言える。

続いて 10 月 31 日付報道発表[39]により、Securing the Software Supply Chain- Recommended practices guide for suppliers[40] が一般公開された。内容は、Developers と Customers の間と位置付けられた Supplier が Software Supply Chain Security の確保になすべきこと、心得を記した文献だが、ソフトウェア作成、商品開発、管理者など、Developers 以外のソフトウェア会社の 様々な役割に期待される役割が示されていると考えてよい。

なお、次回最終作は、for Consumers、すなわち消費者、利用者向けの文献の発行が予定される。

このような文献の発行がこれら 3 組織から一般に公開されたという事実が、連邦政府の Software Supply Chain に対する関心の強さと危機感の現れとも考えられる。

(3) OMB M-22-18 MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

2022 年 9 月 14 日、Office of Management and Budget (以下 OMB と略記)[41]より、標題 M-22-18 MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES が連邦各省庁トップに対し発行された[42]。本 Memorandum は昨年の EO 14028 を根拠とし、連

---

32 <https://www.nsa.gov/about/>
33 <https://www.cisa.gov/about-cisa>
34 <https://www.odni.gov/index.php/who-we-are>
35 <https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3146465/nsa-cisa-odni-release-software-supply-chain-guidance-for-developers/>
36 <https://media.defense.gov/2022/Sep/01/2003068942/-1/-1/0/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF>
37 <https://www.cisa.gov/uscert/ncas/current-activity/2022/09/02/cisa-nsa-and-odni-release-part-one-guidance-securing-software>
38 <https://csrc.nist.gov/Projects/ssdf>
39 <https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3204427/esf-partners-nsa-and-cisa-release-software-supply-chain-guidance-for-suppliers/>
40 <https://media.defense.gov/2022/Oct/31/2003105368/-1/-1/0/SECURING_THE_SOFTWARE_SUPPLY_CHAIN_SUPPLIERS.PDF>
41 <https://www.whitehouse.gov/omb/>
42 <https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf>

邦各省庁において第三者(Third Party) ソフトウェアの利用に際し、Software Supply Chain 確保のために実施されるべき要領と実施期限が具体的に示される。個別実施要領と各要領の実施期限は、Appendix A で一覧表として示されている。

(4) Securing Open-Source Software Act

米国議会上院において、Securing Open Source Software Act[43] が 2022 年 9 月 22 日に委員会で法案として審議が開始され、いくつかの報道が観察された[44]。中間選挙を 1 月半後に控えた時期に審議が開始された意図は不明だが、共和民主超党派の提案であり、選挙の影響が少ないかも知れない。

選挙後の 12 月 15 日、米国議会上院　国土安全保障委員会議長を務める Gary Peters 上院議員への Washington Post の取材記事によると、Open Source Software のセキュリティは優先課題の一つとして挙げられている[45]。

4.1.3.4 その他の IoT あるいは Software Supply Chain Security に関連する動向

本報告期間中、IoT あるいは Software Supply Chain Security に関連する、民間を中心とした動静について以下に記す。

(1) Open-Source Software Security Summit II

2022 年 5 月 12 日、EO14028 発行一周年に開催された。1 月に The Whitehouse National Security Council で開催された初回会合に続き、2 回目の会合である。The Linux Foundation[46] 並びに Open Source Software Security Foundation (OpenSSF)[47] が共催、37 社より 90 人以上の幹部、並びに連邦政府より、NSC[48], ONCD[49], CISA, NIST, DOE[50]、並びに OMB[51]からの参加があったとされる。

会合の結果として、3 つの目標と 10 箇条の計画(Three Goals of the 10-point plan)が以下の通り採択された。

---

[43] <https://www.hsgac.senate.gov/media/majority-media/peters-and-portman-introduce-bipartisan-legislation-to-help-secure-open-source-software >

[44] 報道類 <https://www.zdnet.com/article/whats-what-in-the-united-states-securing-open-source-software-act/> <https://www.washingtonpost.com/politics/2022/09/22/senators-introduce-bill-protect-open-source-software/>

[45] <https://www.washingtonpost.com/politics/2022/12/15/here-what-next-senate-cybersecurity/>

[46] Linux Foundation 報道発表 <https://www.linuxfoundation.org/press-release/linux-foundation-openssf-gather-industry-government-leaders-open-source-software-security-summit/>
本文 <https://www.cio.gov/assets/files/Federal-IT-Operating-Plan-June-2022.pdf>

[47] OpenSSF 報道発表 <https://openssf.org/press-release/2022/05/12/the-linux-foundation-and-open-source-software-security-foundation-openssf-gather-industry-and-government-leaders-for-open-source-software-security-summit-ii/>

[48] National Security Council: <https://www.whitehouse.gov/nsc/>

[49] Office of the National Cyber Director: <https://www.whitehouse.gov/oncd/>

[50] Department of Energy: <https://www.energy.gov/national-security-safety/cybersecurity>

[51] <https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3204427/esf-partners-nsa-and-cisa-release-software-supply-chain-guidance-for-suppliers/>

- Three Goals:
  1. Securing Open-Source Security Production
  2. Improving Vulnerability Discovery and Remediation
  3. Shorten Ecosystem Patching Response Time
- 10-point Plan:
  1. Security Education (and Certification for software development)
  2. Risk Assessment: public, vendor neutral, objective-metrics-based risk assessment dashboard for the top 10,000 or more OSS components
  3. Digital Signatures (for software releases)
  4. Memory Safety (replacing non-memory-safe languages)
  5. Incident Response (establish the Open SSF Open Source Security Incident Response Team)
  6. Better scanning (Accelerate discovery of new vulnerabilities by maintainers and experts)
  7. Code Audits (third-party code reviews of up to 200 most critical OSS components once a year)
  8. Data sharing (Coordinate industry-wide data sharing)
  9. SBOMs everywhere (improve SBOM tooling and training to drive adoption)
  10. Improved supply chains (Enhance the 10 most critical OSS build systems, package managers, and distribution systems with better supply chain security tools and best practices.)

計画 10 箇条は全て重要だが、SBOM のツールとトレーニングの拡大は、今後の SBOM 導入に向けての追い風として注目される。

(1) CIS Software Supply Chain Security Guide Version 1.0[52]

Center for Internet Security (CIS）が 6 月 22 日に発行[53]。当該文献は Aqua Security との共作である。当該文献発行と同時に、Aqua Security は当該文献に沿った検証、監査を実施できる、Chain-Bench というツールを一般公開した[54]。先述の SBOM tool 同様、具体的な tools 類が公開されると現場の実務者にとっては大きなメリットがあり、文献発行者にとっても、紙の上の議論だけでなく実践してもらえる機会や関心の高まりが期待できる。

(2) Cloud Security Technical Reference Architecture[55]

2022 年 6 月 23 日、CISA が発行。連邦政府文民省庁でのクラウド利用時のセキュリティ

---

[52] <https://github.com/aquasecurity/chain-bench/blob/main/docs/CIS-Software-Supply-Chain-Security-Guide-v1.0.pdf>

[53] CIS 報道発表 <https://www.cisecurity.org/about-us/media/press-release/aqua-security-collaborates-with-center-for-internet-security-to-create-guide-for-software-supply-chain-security>, Aqua Security 報道発表 <https://www.aquasec.com/news/software-supply-chain-security-guide-cis-aqua-security/>

[54] <https://github.com/aquasecurity/chain-bench>

[55] 発表 <https://www.cisa.gov/uscert/ncas/current-activity/2022/06/23/cisa-releases-cloud-security-technical-reference-architecture>
文書本文
<https://www.cisa.gov/sites/default/files/publications/Cloud%20Security%20Technical%20Reference%20Architecture.pdf>

ガイダンスという位置付けの文書である。IoT に特化した文書ではないが、SIP-CPS では、その研究開発計画 において各構成要素の一つとしてクラウドが例示されている点で、特に IoT 類がクラウドに依拠するユースケースへの影響が考えられうる。

(3) Microsoft SBOM tool を一般公開[56]

同社が従来社内で利用してきた SBOM tool を GitHub で 2022 年 7 月 12 日に一般公開[57]。一般で広く使える有効なツールが公開され利用が始まると、SBOM の展開、普及への貢献が期待できる。

(4) GUAC- Graph for Understanding Artifact Composition

2022 年 10 月 20 日、GitHub 上で展開されている Open Source Project, GUAC[58] が発表された[59]。この発表は、GUAC について概略が説明されており、Software Security Metadata を収集し、entity 属性を踏まえてこれを図示することにより、Supply Chain をわかりやすく把握できることが期待される。具体的に、SBOM に加え、Signed Attestation として SLSA, SLSA3, GitHub Actions Builder, Google Cloud Build、脆弱性データベースとして OSV.dev, GSD が例示されている。

(5) Microsoft は S2C2F を OpenSSF に寄贈

2022 年 11 月 16 日、Microsoft 並びに OpenSSF は、Microsoft が開発し社内で利用している Secure Supply Chain Consumption Framework (以下 S2C2F と略記)を OpenSSF に寄贈と発表した[60]。今後、Microsoft が議長を務める OpenSSF Secure Supply Chain Consumption Framework (S2C2F) SIG[61] が S2C2SF のメンテナンスを行うとのことである。

4.1.3.5 IoT 等に今後も影響しうる事例

調査期間中に観測された、IoT 並びに Supply Chain Security に影響しうる事例について以下に主要なものを例示する。

---

56 <https://github.com/microsoft/sbom-tool>

57 <https://devblogs.microsoft.com/engineering-at-microsoft/microsoft-open-sources-software-bill-of-materials-sbom-generation-tool/>

58 <https://github.com/guacsec/guac>

59 <https://security.googleblog.com/2022/10/announcing-guac-great-pairing-with-slsa.html>

60 Microsoft: <https://www.microsoft.com/en-us/security/blog/2022/11/16/microsoft-contributes-s2c2f-to-openssf-to-improve-supply-chain-security/>
OpenSSF: <https://openssf.org/blog/2022/11/16/openssf-expands-supply-chain-integrity-efforts-with-s2c2f/>

61 <https://github.com/ossf/s2c2f>

(1) 米国司法省、RSOCS Botnet takedown を発表[62]

2022 年 6 月 16 日、米国司法省は、同省並びに独、蘭、英の捜査当局と合同で、ロシアが運用とされ IoT も含め世界中で 325,000 以上の感染機器類で構成される botnet として知られる RSOCKSbotnet の takedown を実施と発表。ロイター並びに Ars Technica は、RSOCKS は元来 IoT 端末類を対象と報道している。

(2) OT: ICEFALL report[63]

2022 年 6 月 20 日、Forescout は、多岐にわたる ICS/OT 製品の計 56 件の脆弱性の報告書を公開。同 6 月 22 日には CISA より本件に関する alert が発行され[64]、警戒と対策が呼びかけられている。これら脆弱性に共通する、そして従来から知られている 4 つの要因が挙げられており、基本的なセキュリティ対策の遅れが懸念される。

- Insecure engineering protocols
- Weak cryptography or broken authentication schemes
- Insecure firmware updates
- Remote code execution via native functionality

2022 年 12 月 14 日には、Washington Post 紙が、Microsoft が 12 月に発行した報告書[65] を引用しつつ、75%の ICS 装置類が脆弱で、パッチも当てられていない旨報じている。更に翌同 15 日、CISA は 41 件にわたる ICS 脆弱性のアドバイザリを一斉に公開した[66] 。

(3) GitHub Commit に検知された脆弱性[67]

2022 年 7 月 15 日、GitHub の各 Branch で、ファイルに対する変更を記録する Commit に、よりによって timestamp 並びに creator identity に関するメタデータが改竄可能という脆弱性が Checkmarx より報告され、諸処で大きく報じられた。 GitHub は、Commit Signature Verification（署名検証機能）を対策として導入したが、そもそも Commit が署名されていない場合何の効果も期待できないという問題が指摘されている。

---

62 司法省報道発表 <https://www.justice.gov/usao-sdca/pr/russian-botnet-disrupted-international-cyber-operation>
ロイター報道 <https://www.reuters.com/world/us-partners-dismantle-russian-hacking-botnet-justice-dept-says-2022-06-16/>
Ars Technica: <https://www.theregister.com/2022/06/17/rsocks_russia_botnet/>

63 Blog: <https://www.forescout.com/blog/ot-icefall-56-vulnerabilities-caused-by-insecure-by-design-practices-in-ot/>
報告本文 <https://www.forescout.com/resources/ot-icefall-report/>

64 <https://www.cisa.gov/uscert/ncas/current-activity/2022/06/22/cisa-releases-security-advisories-related-oticefall-insecure>

65 The Convergence of IT and Operational Technology: Cyber Risks to Critical Infrastructure on the Rise <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5daTD>

66 <https://www.cisa.gov/uscert/ncas/current-activity/2022/12/15/cisa-releases-forty-one-industrial-control-systems-advisories>

67 <https://checkmarx.com/blog/unverified-commits-are-you-unknowingly-trusting-attackers-code/>

(4) GitHub 大規模不正（偽）プロジェクト複製事件[68]

2022 年 8 月 3 日、35,000 件以上の不正な複製プロジェクトが GitHub 上で検知された旨報告された[69]。これらは単なる偽プロジェクトではなく、遠隔からのコードの実行、API keys, tokens, AWS 認証情報、暗号化に利用される鍵の詐取などの攻撃に利用可能な不正なコードが含まれており、純正プロジェクトと錯誤した善意の利用者を騙し、不正なコードを導入、拡散させる、いわゆる Software Supply Chain attack を企図したものと考えられる。

(5) PyPI

2022 年 8 月 8 日、Checkpoint は、Python で開発された software repository 最大手、Python Package Index (PyPI)にて十件の不正な package を検知し、PyPI に連絡して削除されたインシデントの詳細を公開した[70]。これら不正な package は著名な別パッケージそっくりの体裁とよく似た名称を有し、不正な package が download されやすくなっており、いわゆる Software Supply Chain 攻撃を目的とされる。

また同 9 月 1 日、SentinelOne[71] と Checkmarx[72] は、彼らが JuiceLedger と呼称する Phishing campaigner が PyPI contributors に対し Phishing 攻撃を同 8 月に実施したことを公開、発表した。この攻撃について PyPI は 8 月 24 日に警告を公開し[73] 、対策としてスポンサーの Google から提供された Hardware based 2-factorauthentification に必要な Hardware Token を 4,000 個限定で配布を実施した[74]。SentinelOne によると、この攻撃により２つの PyPI Package が不正化され、あわせてほぼ 7 万件の不正パッケージのダウンロードが報告されている。本件との関係は不明だが、9 月 5 日、Rsecurity が公開した Evil Proxy- Phishing as a Service には、PyPI の認証情報詐取機能が具備とされる[75]。

11 月 1 日には、Phylum が PyPI 内で Python Developers に W4SP Stealer を送付、感染させることを目的としたと考えられる python packages を複数確認と発表している[76]。同 9 日には、Checkpoint より Steganography を利用、悪用し不正コードを難読化させた不正な Python

---

68 <https://checkmarx.com/blog/unverified-commits-are-you-unknowingly-trusting-attackers-code/>

69 発見者の方の報告 <https://twitter.com/stephenlacy/status/1554697077430505473>,<https://twitter.com/stephenlacy/status/1554733783198314496>、関連報道: <https://nakedsecurity.sophos.com/2022/08/04/github-blighted-by-researcher-who-created-thousands-of-malicious-projects/>

70 <https://research.checkpoint.com/2022/cloudguard-spectral-detects-several-malicious-packages-on-pypi-the-official-software-repository-for-python-developers/>

71 <https://www.sentinelone.com/labs/pypi-phishing-campaign-juiceledger-threat-actor-pivots-from-fake-apps-to-supply-chain-attacks/>

72 <https://checkmarx.com/blog/first-known-phishing-attack-against-pypi-users/>

73 <https://twitter.com/pypi/status/1562442188285308929>

74 <https://pypi.org/security-key-giveaway/>, <https://twitter.com/pypi/status/1545455297388584960> しかしこの配布予定の Hardware Token は、Google が導入時に議論を呼んだ中国製の Titan Security Key であることに要注意。

75 <https://resecurity.com/blog/article/evilproxy-phishing-as-a-service-with-mfa-bypass-emerged-in-dark-web>

76 <https://blog.phylum.io/phylum-discovers-dozens-more-pypi-packages-attempting-to-deliver-w4sp-stealer-in-ongoing-supply-chain-attack>

Package が PyPI 上で検知された旨発表している[77]。更に同 17 日、Checkmarx Security は、Phylum 並びに Checkpoint が検知した攻撃が同一の攻撃主体によるものであり、不正な package の upload に、polymorphic malware を利用し、被害者のパソコンから、Discord のアカウント、パスワード、暗号通貨の Wallets、Credit Cards、その他めぼしいファイル類を詐取しているとの見解を発表した[78]。

これらの事件以外に、Software Supply Chain に関係し Python 特有の課題も指摘されている。Checkmarx は、Python Package の download, install 両方で起動される setup.py script に不正な記述を簡単に挿入可能という見解を示している[79]。この見解が正しい場合、例えば PyPI などのような package repository から単純に download (“Pip download <package name>”)した場合でも不正な setup.py が起動され、不正な package が拡散しやすい可能性が懸念される。

(6) Shikigeta malware

2022 年 9 月 6 日、AT&T Alien Labs は、Shikigeta という Linux 系の OS を対象とした malware の詳細を発表した[80]。同発表によると Linux 系 malware は今年 2022 年前半で対前年比 650%の伸びが見られること[81]、並びに当 Shikigeta は、code size 300 bytes, file size 370 bytes と小さく、Linux で動作している endpoints に加え、Linux で動作する IoT 類を攻撃対象としていることが示されている。BusyBox など Linux 系の OS で動作する IoT 類は多くの利用が考えられ、Linux 向けの malware の増加に伴い、これら IoT 類への悪影響が懸念される。

(7) Zerobot

2022 年 12 月 6 日、Fortinet 社の FortiGuard Labs は、Zerobot という Go で記述され、IoT に感染し拡散する多機能な bot について発表した[82]。 同発表によると Go で記述され、IoT にて拡大、対象 OS は Linux とされる。 Go で書かれた他の malware 同様、多種の CPU に対応するが、同発表によると Zerobot の場合、i386, amd64, arm, arm64, mips, mips64, mips64le, mipsle, ppc64, ppc64le, riscv64, 及び s390x と、Go で書かれた他の malware と比べても対応 architecture が多く、多種多様な IoT 類を標的としている可能性が懸念される。 また、自己複製、複数プロトコルを利用した攻撃、自己拡散など多機能で、最悪 worm 化も懸念される。同報告の Figure 1 では、アメリカの Thanksgiving holidays 前後に活動が活発化しているように観察できる。 すなわち、Zerobot は、malware の危険な特徴、最近数年観測された危険な

---

77 <https://research.checkpoint.com/2022/check-point-cloudguard-spectral-exposes-new-obfuscation-techniques-for-malicious-packages-on-pypi/>

78 <https://medium.com/checkmarx-security/wasp-attack-on-python-polymorphic-malware-shipping-wasp-stealer-infecting-hundreds-of-victims-10e92439d192>

79 <https://checkmarx.com/blog/automatic-execution-of-code-upon-package-download-on-python-package-manager/>

80 <https://cybersecurity.att.com/blogs/labs-research/shikitega-new-stealthy-malware-targeting-linux>

81 AT&T Alien Labs は、atlas VPN 発 2022 年 7 月 27 日の発表を引用している。
<https://atlasvpn.com/blog/linux-malware-on-a-rise-reaching-all-time-high-in-h1-2022>

82. <https://www.fortinet.com/blog/threat-research/zerobot-new-go-based-botnet-campaign-targets-multiple-vulnerabilities>

動向の多くを具備した極めて危険な bot であり、その潜在的な力によって今後将来にわたりその活動が懸念される。

4.1.4 欧州の動向

4.1.4.1 英国 NCSC

(1) Organizational use of Enterprise Connected Devices[83]

2022 年 5 月 10 日、NCSC-UK より発行。当文書は、Laptop computer からプリンタ、センサまで、企業情報ネットワークに接続される多様な端末類を対象としたセキュリティ解説文書だが、あくまで「企業情報ネットワークに接続」を前提としており、一般の消費者よりも知識、責任、ネットワーク並びにサイバーセキュリティに対する責任を有することが想定されている点で、NIST が過去に取り組んできた Labeling の文書と前提が異なることにご注意いただきたい。ただし、企業情報システム環境での利用上の注意として役立つこと、並びに下記の記述に見られるように、SIP-CPS の前提、対象と親和性が高いと考えられる。

” Enterprise IoT is the advancement in technology that enables physical 'things' with embedded computing devices to participate in business processes for reducing manual work and increasing overall business efficiency. Taking advantage of a combination of technologies ranging from embedded devices with sensors and actuators to internet-based communication and cloud platforms, enterprise IoT applications can now automate business processes that depend on contextual information provided by programmed devices such as machines, vehicles, and other equipment.”

(2) Device Security Guidance Version 2.0[84]

2022 年 5 月 10 日、NCSC-UK より発行[85]。当文書は、さる 2021 年 6 月 29 日に発行の初版の改版となる。これは各種 OS 類の具体的な設定などが示される点で Configuration Guide としての性格が観察できる[86]一方で、Device security principles for manufactures (beta release)[87] に示される 11 箇条は、むしろ NIST IoT Program がここ数年策定してきた NISTIR 類と同様、製造業者への期待（あるいは事実上の要件）と類似の性質、位置付けと考えられる。

[83] <https://www.ncsc.gov.uk/report/organisational-use-of-enterprise-connected-devices>
[84] <https://www.ncsc.gov.uk/collection/device-security-guidance>
[85] 同 6 月 10 日に改定されている模様だが、内容の変化が確認できない。
[86] <https://www.ncsc.gov.uk/collection/device-security-guidance/platform-guides>
[87] <https://www.ncsc.gov.uk/collection/device-security-guidance/security-principles>

(3) Supply chain cyber security: Accessing and gaining confidence in your suppliers[88]

2022 年 10 月 12 日、NCSC-UK より発行[89]。当文書は、昨今増加傾向とされる Supply Chain cyber attacks に備え、各組織で準備、点検しておくべき指針と考えられる。文書は次の 5 つの柱で構成され、それぞれに対策が示されている。

1. Before you start
2. Develop an approach to assess supply chain cyber security
3. Apply the approach to new supplier relationships
4. Integrate the approach into existing supplier contracts
5. Continuously improve

最後に、”Continuously improve” で締め括られている通り、「これをやったら終わり、万全。」という安直なものではなく、継続し続けなければならないという当たり前のことを示し、求める文書である。本文中では、上記それぞれの柱で期待される実施要領、並びに期待される成果 （outputs）が示されている。

4.1.4.2 NIS2、欧州議会で承認、欧州委員会で採択、発行へ

NIS2 Directive, あるいは単に NIS2 として知られる、Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)[90] について、2022 年 5 月 13 日、欧州議会と欧州委員会(European Council)が原則合意に達し[91]、同 11 月 10 日、欧州議会での評決で承認[92]、同 28 日には欧州委員会が報道発表[93]により、公式採択手続き (formal adoption)を実施し EU’s Official Journal

---

[88] <https://www.ncsc.gov.uk/files/Assess-supply-chain-cyber-security.pdf>
NCSC 報道発表 <https://www.ncsc.gov.uk/news/ncsc-issues-fresh-guidance-following-recent-rise-in-supply-chain-cyber-attacks>
How to assess and gain confidence in your supply chain cyber security
<https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security>

[89] 同 6 月 10 日に改定されている模様だが、内容の変化が確認できない。

[90] <https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union>
現在の NIS 含め背景は、<https://digital-strategy.ec.europa.eu/en/policies/nis-directive>
Revision of the Network and Information Security Directive: Questions and Answers: <https://digital-strategy.ec.europa.eu/en/faqs/revision-network-and-information-security-directive-questions-and-answers>

[91] European Commission の反応 < https://digital-strategy.ec.europa.eu/en/news/commission-welcomes-political-agreement-new-rules-cybersecurity-network-and-information-systems>
European Commission Press Release on May 13, 2022:
<https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2985>
報道例: < https://www.infosecurity-magazine.com/news/eu-cybersecurity-legislation/>
NIS2 提案の概要 <https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2> or
<https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333>

[92] <https://www.europarl.europa.eu/news/en/press-room/20221107IPR49608/cybersecurity-parliament-adopts-new-law-to-strengthen-eu-wide-resilience>

[93] <https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/>

に近日発表が予定され、同発表後 20 日後に発効と発表された。各 EU 加盟国は 21 ヶ月以内に NIS2 に対応した国内法の整備を実施する。これにより、欧州域内のネットワーク、システムに IoT を含み、かつ IoT にとどまらないより広範に、より厳格化された法制度が少なからぬ影響をもたらすことは間違いない。

4.1.4.3 DSA 及び DMA

欧州委員会発表によると、2022 年 3 月 25 日に Digital Markets Act（以下 DMA と略記）、同 4 月 23 日に Digital Services Act（以下 DSA と略記）が政治的合意に達し[94]、この 2 つの法の成立、施行が確実となり、DMA は 2022 年 11 月 1 日に発効した[95]。これを反映するかのように、ダボス会議で著名な世界経済フォーラムは DMA, DSA 施行の一環として、シリコンバレーが所在するサンフランシスコベイエリアに EU が拠点を開設中の旨報じている[96]。欧州委員会の発表に見られる通り、DSA, DMA はパッケージとして 2 つを一体として扱われることが多いが、両者が共通する目標として、デジタルサービスの全ての利用者の基本的人権が保護される、より安全なデジタル空間の創造、並びに欧州単一市場並びに世界的なイノベーション、成長、競争力の涵養を目的としている。本件は最低でも欧州域内のネットワーク、システムの IoT を含み、IoT にとどまらない広範な影響をもたらすことは間違いない。

4.1.4.4 Proposal for Cyber Resilience Act

2022 年 9 月 8 日、欧州委員会が、IoT 類を含むネットワークに接続される機器類への規制強化を含む、Proposal for Cyber Resilience Act を 2022 年 9 月 13 日に発表との数々の記事が欧州を中心に観察された[97]。実際には同 9 月 15 日現在、欧州委員会は Proposal for a Cyber Resilience Act につ

---

[94] 欧州委員会発表 <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>
DSA <https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/digital-services-act/timeline>,
DMA <https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/digital-markets-act/timeline>

[95] <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6423>, <https://eur-lex.europa.eu/eli/reg/2022/1925/oj>

[96] <https://www.weforum.org/agenda/2022/08/why-the-european-union-is-opening-a-silicon-valley-embassy>

[97] 例えば、Reuters: Draft EU rules target smart devices with cybersecurity risks: <https://www.reuters.com/technology/draft-eu-rules-target-smart-devices-with-cybersecurity-risks-2022-09-08/>
Euractiv: LEAK: Commission to introduce cyber requirements for Internet of Things products: <https://www.euractiv.com/section/cybersecurity/news/leak-commission-to-introduce-cyber-requirements-for-internet-of-things-products/>
Techmonitor: EU's Cyber Resilience Act to toughen cybersecurity rules for smart IoT devices: <https://techmonitor.ai/policy/privacy-and-data-protection/eu-cyber-resilience-act-iot-connected-devices>

いて発表した[98]。以下に欧州委員会が発表した当該 Proposal の内容を示す[99]。

- 2 つの主要目標
  1. 市場に流通するハードウェア、ソフトウェアのより少ない脆弱性の担保と、製造業者による製品ライフサイクルの最初から最後まで真剣な取り組みの担保により、セキュアな製品開発の条件を創造。
  2. Digital Elements をもつ製品を選択あるいは使用にあたり、ユーザーがサイバーセキュリティを考慮できる条件を創造。
- 4 つの具体的な目標
  1. Digital Elements の設計、開発段階から全てのライフサイクルで製造業者が製品セキュリティの改善を保障。
  2. ハードウェア、ソフトウェア製造業者の法規制遵守を促す首尾一貫したサイバーセキュリティフレームワークの保障。
  3. Digital Elements を持つ製品のセキュリティの透明性の保障。
  4. 事業者、一般消費者を含むユーザーが Digital Elements を持つ製品のセキュアな利用を可能とすること。

今後、同 Proposal は欧州議会と欧州委員会で精査、審議され、採択された場合、欧州連合加盟国は 2 年以内に新しい要件を実施とされる[100]。

4.1.4.5 ETSI

ETSI Technical Committee on Cybersecurity (TC CYBER)[101] が作成し、2020 年 6 月 30 日に一般に公開された ETSI EN 303 645, CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements に準拠あるいは由来する関連付属文書類について、外部から確認できる状況を以下に示す。

(1) TS 103 701: Cybersecurity assessment for consumer IoT products[102]

2021 年 8 月 16 日付で確定、公表された、消費者向け IoT の基本要件の Conformance Assessment（適否認定評価）に関する Technical Specification。

(2) TS 103 848 V1.1.1 (2022-03): Technical Specification: Cyber Security for Home Gateways; Security Requirements as vertical from Consumer Internet of Things

2022 年 4 月 7 日発表の ETSI 報道発表によると、宅内ネットワークと公衆網の間の物理的

98 報道発表 <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5374>, <https://digital-strategy.ec.europa.eu/en/news/new-eu-cybersecurity-rules-ensure-more-secure-hardware-and-software-products>
Q&A: <https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_5375>
99 <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>
Factsheet: <https://ec.europa.eu/newsroom/dae/redirection/document/89528>
100 Next Steps: <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5374>
101 <https://www.etsi.org/committee/cyber>
102 <https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58434>

なネットワークとトラフィックをセキュア化し、Home Gateway を対象にした世界初の標準とされている[103]。

(3) TR 103 621 V1.2.1(2022-09): Guide to Cyber Security for Consumer Internet of Things[104]

2022 年 9 月 6 日付公式発行。消費者向け IoT のサイバーセキュリティガイド。

TR= Technical Report と位置付けられる。

(4) DTS/CYBER-0014 (TS 103 486) Identity Management and Discovery for IoT[105]

2022 年 9 月 22 日に最新の Draft V 0.0.26 が Stable Draft として提示され、議論されている模様である。他方、2022 年 4 月 20 日、ETSI は、"Annual Report 2021[106]" 及び "Work Programme 2022-2023[107]" を発行している[108]。このうち、Work Programme 2022-2023 Page 12 において、IoT にかかる活動として以下の記載がある。

1. Smart Door Locks、及び Sensor Hub への脅威に関する Technical Standards の発行。
2. Consumer IoT Cybersecurity に関する Vendors を対象とした新しい Guide を Technical Report として発行。
3. Security of Home Gateways 並びに Network Routers の 2 件の Technical Report の発行。

このうち、上記 2. については、NIST IoT Program が作成してきた NISTIR 類と類似の性質が考えられる。3. に関しては、ここで示される 2 つの Technical Report と、上述の 4 月 7 日発行の TS 103 848 V1.1.1 (2022-03): Technical Specification: Cyber Security for Home Gateways; Security Requirements as vertical from Consumer Internet of Things との関連が不明である。新たに 2 件の Technical Reports が発行される可能性も捨てきれないが、TS 103 848 との差異は不明である。

また、2022 年 10 月 11 日から 14 日まで、ETSI IoT Week 2022 という催事が開催され[109]、その中で、ETSI IoT Conference 2022 が開催されている[110] 。

4.1.4.6 ENISA

2022 年 6 月 2 日より 3 日の 2 日間、ENISA 主催、ENISA Cybersecurity Certification Conference

---

103 ETSI Press Release: <https://www.etsi.org/newsroom/press-releases/2051-2022-04-etsi-world-first-standard-to-secure-consumer-iot-devices-is-extended-to-home-gateways>

104 <https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=66181>

105 <https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=47653>

106 <https://www.etsi.org/e-brochure/Annual-Reports/AR-202204/mobile/index.html#p=1>

107 <https://www.etsi.org/e-brochure/Work-Programme/2022-2023/mobile/index.html#p=1>

108 <https://www.etsi.org/newsroom/news/2057-2022-04-etsi-releases-its-annual-report-and-work-programme-2022-2023>

109 <https://www.etsi.org/events/upcoming-events/2060-etsi-iot-week-2022>

110 <https://www.etsi.org/events/upcoming-events/2088-etsi-iot-conf-2022>

2022[111]が開催された。Agenda[112]、並びに会議後公開された情報[113]を見る限り、彼らの従来の取り組み分野、すなわち、Common Criteria (EUCC), Cloud Services (EUCS), EU 5G, 並びに Cybersecurity Market について議論された模様で、IoT を集中審議、あるいは独立した項目、取り組み課題として扱ったようには見られない。しかし、この Cybersecurity Market を引用する ”EU Cybersecurity Market Analysis - IoT in Distribution Grid” という文書が去る 2022 年 4 月 8 日に発行され、その中で送電網 electric distribution grid で利用される IoT について検討がなされている点にご注意いただきたい[114]。例えば先述の通り 9 月に欧州委員会が公開した Cybersecurity Resilience Act 提案と関連して、IoT に対する EU Certification が議論される可能性はある。

111 <https://www.enisa.europa.eu/events/enisa-cybersecurity-certification-conference-2022>
112 <https://www.enisa.europa.eu/events/enisa-cybersecurity-certification-conference-2022/agenda>
113 <https://www.enisa.europa.eu/news/enisa-news/cybersecurity-certification-breaking-new-ground>
114 <https://www.enisa.europa.eu/news/enisa-news/cybersecurity-market-analysis-in-support-of-informed-cybersecurity-business-decisions>

4.2　海外における制度や標準のとりまとめプロセス

4.2.1 調査方法

IoT セキュリティとサプライチェーンセキュリティに関する公的機関などが、関連する産業や他国を含む他の公的機関とどのように連携・協議して制度や標準を取りまとめようとしているかについての動向調査を行うために、公的機関や標準化組織などの制度やそれらの標準のとりまとめプロセスを調べる。

調査対象組織については、上記 4.1 節の組織を候補として、今回の動向調査で取りまとめの活動が進展し、そのプロセスが確認できるものを中心に分析の対象とし、次の手順で調査を行った。

ステップ 1： 調査対象組織のホームページ上の公開情報を調査し、各種ガイドライン文書の制定プロセス関連情報を調査する。

ステップ 2： 4.1 の調査で得られた対象組織の一連の動向情報を分析・整理し、制定プロセスに沿った制定プロセス活動として取りまとめる。

取りまとめの具体的な活動が把握できない組織については、その組織が定めている取りまとめの方法を調査し報告する。

4.2.2 米国における制度や標準のとりまとめプロセス

4.2.2.1 NIST のガイドライン・標準策定プロセス

(1) NIST の役割

米国立標準技術研究所（NIST : The National Institute of Standards and Technology）は、幅広い範囲で、民間部門の運営や政策に関する規制上の議題や期待に影響を与える可能性のあるガイダンス文書を作成することにより、技術問題に関するリーダーシップの役割を果たしている。

NIST は非規制機関であり、その制定プロセスに関しては、国家技術移転推進法（P.L.104-113[115]）に従い、連邦政府が使用する基準の優先ソースとして、自発的なコンセンサス基準の開発と使用をサポートすると定められている[116]。NICT が策定・発表するガイダンス及び標準の策定プロセスは、連邦官報（Federal Register）に掲載される FIPS（Federal Information Processing Standards）の規格のように、米規制当局に適用される行政手続法（Administrative Procedure Act：APA[117]）に則り、案の告示と意見聴聞を行ってパブリックコメントを募集する告示及びコメント（notice and comment）プロセスに類似した経緯を経る場合があるが[118]、SP（Special Publications）やフレームワーク等のガイドラインについては、他の政府機関、業界、学術機関などのステークホルダーが参加するワークショップや会合を開催し、関係機関と密接に連携しながら任意のコンセンサスに

115 <https://www.govinfo.gov/content/pkg/PLAW-104publ113/pdf/PLAW-104publ113.pdf>
116 <https://www.nist.gov/itl/standards-activities>
117 <https://www.epa.gov/laws-regulations/summary-administrative-procedure-act>
118 <https://www.nist.gov/itl/procedures-developing-fips-federal-information-processing-standards-publications>

基づく標準を策定する傾向にある[119]。ITL が発行する草案を含む多数の出版物にはパブリックコメントが求められており、そのガイドライン・標準は、オープンかつ透明性の高い方法で、世界中の業界及び学術機関の専門家による幅広い知見を得て策定されていることが特徴である。

NIST は商務省の傘下組織として、首都ワシントンに程近い Gaithersburg, Maryland、並びに Boulder, Colorado に大規模なキャンパスを有し[120]、発足時の物理科学に加え多様な分野を所掌する 6 研究所を有す[121]。このうち、情報技術研究並びに標準化を行う Information Technology Laboratory[122]（以下 ITL と略記）が、Cybersecurity for IoT Program[123]（以下 NIST IoT Program と略記）を運営、IoT を取り巻くいわゆるサイバーセキュリティに関わる活動を行っている。NIST IoT Program はアメリカ商務省長官が承認している文書 FIPS 200[124]（連邦情報及び情報システムのための最低セキュリティ要件）に準拠するための具体的な指針を示す文書 NIST SP 800-53（情報システムと組織のためのセキュリティとプライバシーの管理）に基づいている。NIST IoT Program はその課題（The Challenge）として、「IoT エコシステム中の装置並びにデータに対するサイバーセキュリティを産業界横断的に大規模に推進」を掲げ、「IoT への信頼を高め、標準、指針、並びに関連するツール類を通じて世界規模での技術革新を可能とする環境の促進」を行ない、そのミッションとして、標準や公式文書制定とその確定前の過程で行われるドラフト類の公開と一般からのコメント募集を行う。

NICT 発行の文書種類と、FIPS の発行のプロセスを図 1 と図 2 示す。

119 <https://www.wiley.law/alert-3496#_ftn23>
120 <https://www.nist.gov/about-nist/visit>
121 <https://www.nist.gov/about-nist/our-organization>
122 <https://www.nist.gov/itl>
123 <https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program>
124 <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf>

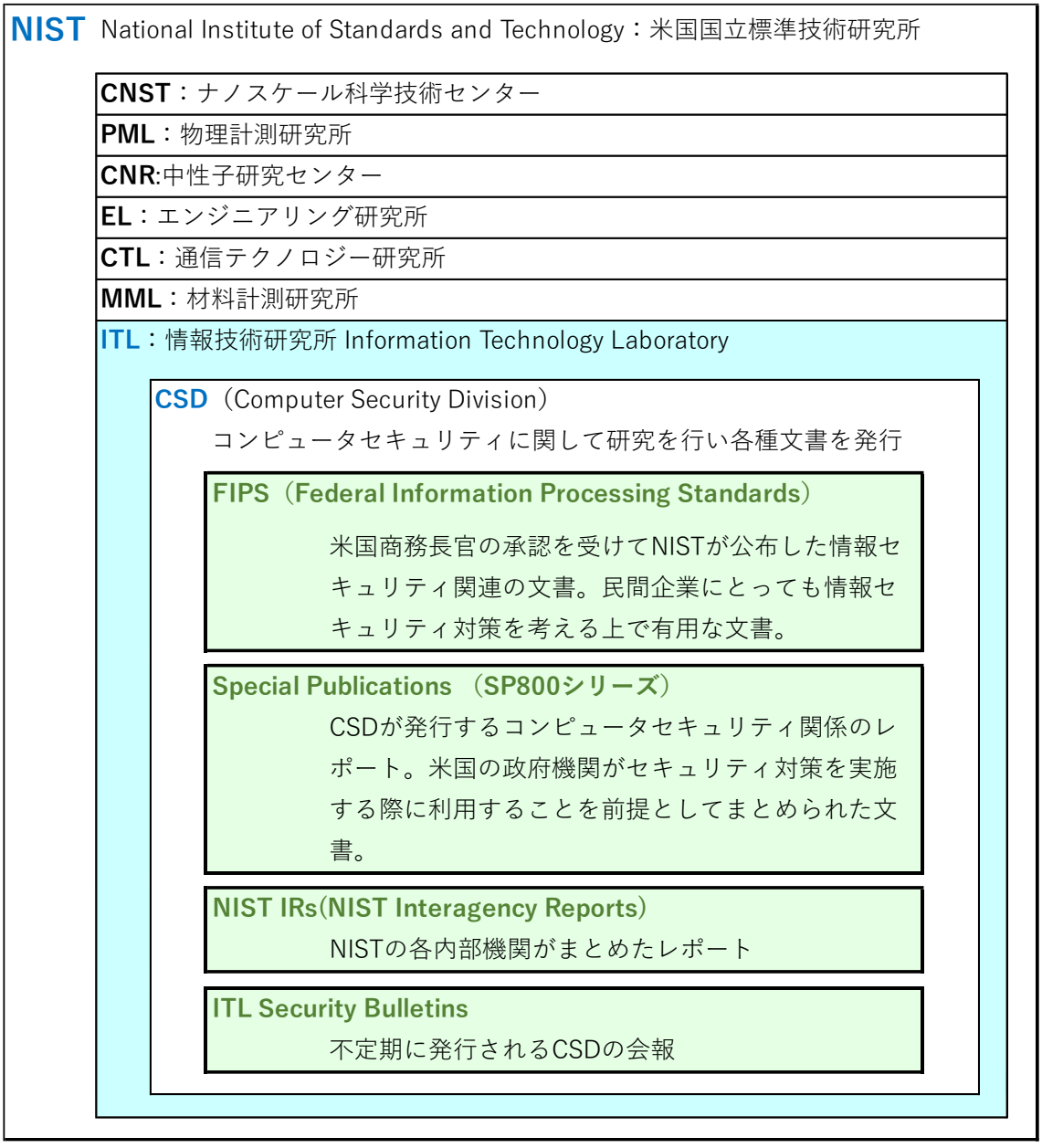


図 1 NIST 発行の文書種類

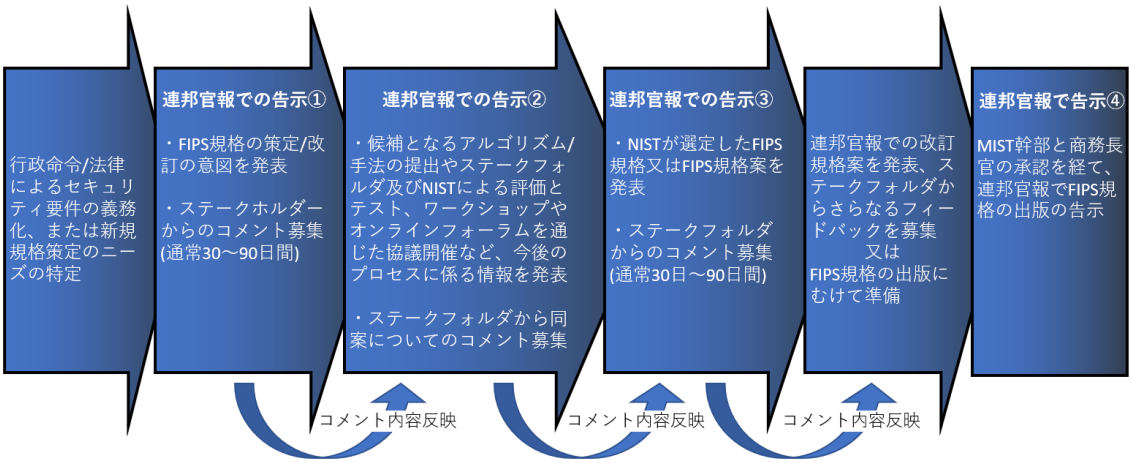


図 2 NIST IoT Program におけるガイドライン・標準策定プロセス

(2) NIST の制定文書類とプロセス

NIST IoT Program が制定を進めている NISTIR 8259 の文書類の制定手続きとこれまでのプロセスを以下に報告する。

IoT Program を含む NIST ITL が作成する連邦政府情報システムを対象とした指針、標準の多くは、根拠法としての Federal Information Security Management Act of 2002（FISMA：連邦情報セキュリティマネジメント法)と 2014 年に改定された Federal Information Security Modernization Act of 2014[125]（以下 FISMA と略記）がある。Office of Management and Budget[126]（OMB：行政管理予算局）に対してセキュリティ報告書を送るように求めており、FISMA と OMB Circular A-130[127] Management Federal Information as a Strategic Resource（行政管理予算庁通達 A-130、以下 OMB A-130 と略記）をよりどころとして、連邦政府機関が情報セキュリティを強化することを義務付け、NIST に対しては、そのための規格やガイドラインの開発を義務付けている[128]。また、2006 年発行し商務省長官が承認している文書の FIPS 200：Minimum Security Requirements for Federal Information and Information Systems[129]（連邦情報及び情報システムのための最低セキュリティ要件）において連邦の最低限のセキュリティ要求事項について、17 のセキュリティ関連分野にわたり規定している。これに対し NIST SP 800-53 はアメリカ政府内の情報システムをより安全なものにし、効果的にリスク管理するためのガイドラインを具体的に定めるものであり、2020 年 9 月 23 日 7 年ぶりの改訂が公開された後、2020 年 10 月 20 日にワークショップの議論を経て一部改訂が行われた。

この FIPS 800-53 に準拠するための指針を示す文書が NISTIR 8259: Security and Privacy Controls for Information Systems and Organizations（情報システムと組織のためのセキュリティとプライバシ

125 <https://www.cisa.gov/federal-information-security-modernization-act>
126 <https://www.whitehouse.gov/omb/>
127 <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf>
128 <https://www.ipa.go.jp/security/publications/nist/fisma.html>
129 <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf>

ーの管理）である。NISTIR 8259 は、2019 年 7 月の 1st Draft、2020 年 1 月 7 日の 2nd Draft 公開を経て、その過程で集めたパブリックコメントへの対応や議論の結果をフィードバックして 2020 年 5 月 29 日に NISTIR 8259 及び NISTIR 8259A として最終版が公開された。

また、連邦政府機関が取得する予定の IoT デバイスを連邦情報システムに統合する方法を検討する際に役立つ背景と推奨事項が含まれており、デバイスの観点からシステムセキュリティを考慮する方法を示す IST SP 800-213 (Draft) : IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements[130]が 2020 年 12 月 15 日に公開された。

NISTIR 8259 の指針を基に IoT デバイスの連邦機関での採用を行うための追加指針である NISTIR 8259B/C/D 等の制定についても、2020 年 12 月 20 日に Draft が公開された。パブリックコメント募集及びこれらの Draft の説明や議論を行うための The National Cybersecurity Center of Excellence[131] （NCCoE）主催のワークショップや、Consumer Technology Association[132]（CTA：消費者技術協会）主催の Roundtabe を開催し、幅広い分野の知見を集めるオープンで透明な策定プロセスに基づいた活動を進めている。NCCoE は NIST の一部であり業界団体、政府機関、及び学術機関が協力して、企業の最も差し迫ったサイバーセキュリティの問題に対処する。これらの文書は、制定後に、商務省を通じて各連邦機関に伝達され、各機関における IoT 機器調達指針として活用されることが期待されている。

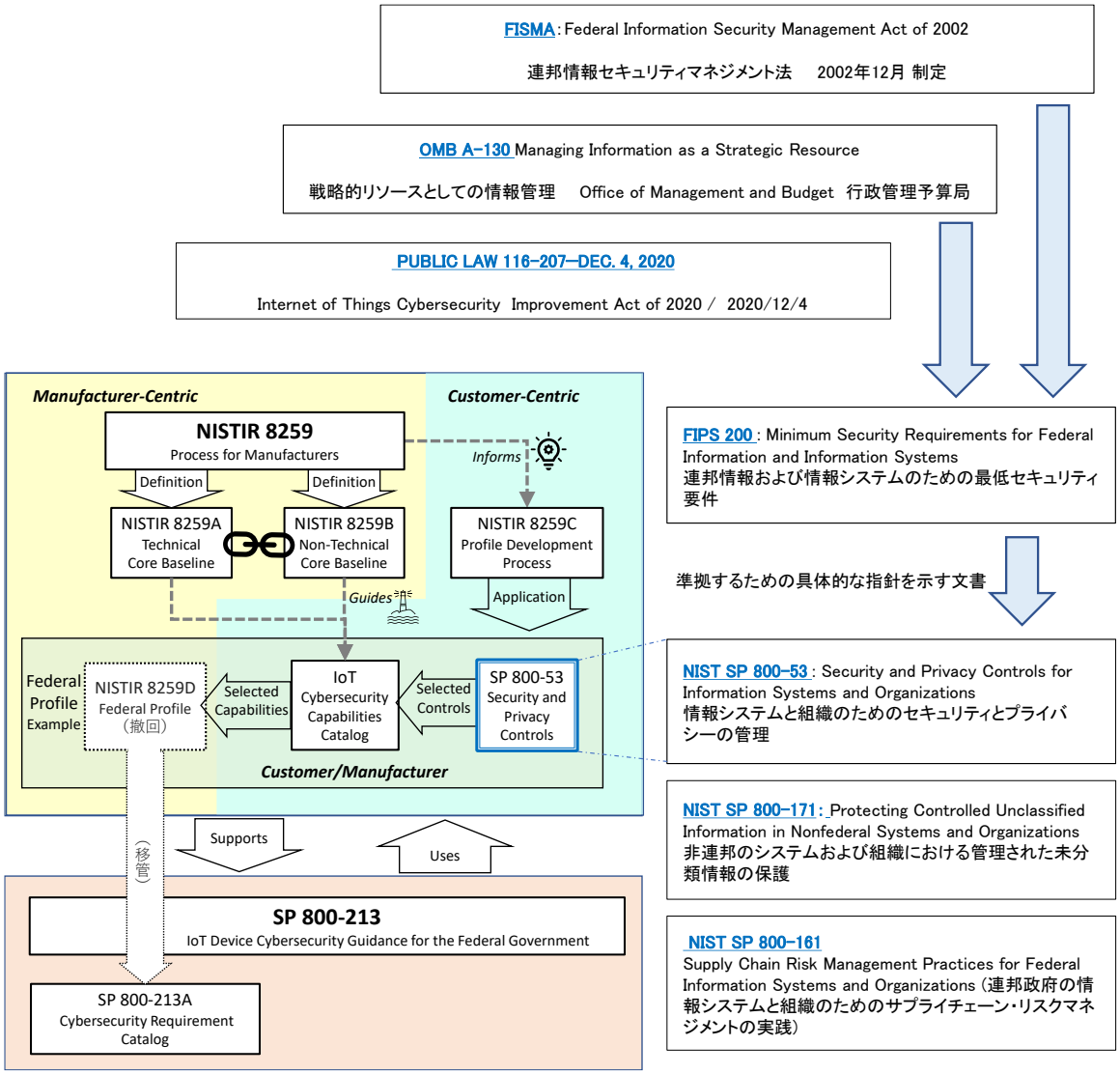
その後、NISTIR 8259B は 2021 年 8 月 25 日に最終版発行された。本文書では IoT 端末に求められるセキュリティについて、メーカーや関連する第三者の通常必要とされる技術的ではないサポート活動を示している。

さらに、NIST SP 800-213 は 2021 年 11 月 29 日に最終版発行が発行され、その分冊として SP 800-213A も同日に発行された。SP 800-213A の Appendex には、NIST IoT Program が作成を行ってきた NISTIR 8259D (Draft)の内容が移管されて、NISTIR 8259D は撤回された。

2022 年 3 月において、NIST IoT Program の担当文書で確定していない Draft 文書は NISTIR 8259C となっている。

以上の諸指針及び FIPS-200、NIST SP800-53、NISTIR 8259 関連文書の相関マップを図 3 に、NISTIR8259 文書ファミリーの概要を図 4 に示す。

130 <https://csrc.nist.gov/publications/detail/sp/800-213/draft>
131 <https://www.nccoe.nist.gov/about-the-center>
132 <https://www.cta.tech/>



出展：NISTの公開情報を基に作成

図 3 米国内の文書制定の役割と NIST の関係、 NSIR 8259 の位置づけ

NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers
製造業者が IoT デバイスを顧客に販売する前に実施することを検討すべきサイバーセキュリティ関連の推奨活動について説明

NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline
IoT デバイスのサイバーセキュリティ能力のコア・ベースラインを定義。組織が製造、統合、または取得する新しい IoT デバイスのデバイス・サイバースセキュリティ能力を特定するための出発点を提供

NISTIR 8259B IoT Non-Technical Supporting Capability Core Baseline
8259Aおよび8259Bは補完的なペアであり、技術的および非技術的な要件の取り扱いにバランスを取り、NISTIR 8259で呼び出された6つの活動を実行するメーカーに対してより包括的なガイダンスを提供。メーカーや関連する第三者から通常必要とされる、技術的でないサポート活動を詳述

NISTIR 8259C (Draft) Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline
特定の IoT デバイスの顧客やアプリケーションに適した IoT サイバーセキュリティ・プロファイルを開発するために、組織やアプリケーション固有の要件と統合する方法を説明する利用可能なプロセスを記述

SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirement
IoT デバイスをシステムやインフラストラクチャに統合しようとする連邦政府機関向けの全体的なガイダンス

SP 800-213A IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog
IoTデバイスのサイバーセキュリティ能力、及び非技術的サポート能力のカタログを提供

図 4 NISTIR 8259 文書ファミリー

(3) 標準化に向けた NIST の活動

NIST は、2015 年 12 月に国際サイバーセキュリティ標準化ワーキンググループ（IICS WG）を設立し、2018 年 11 月 29 日に NISTIR 8200：Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT)[133]（IoT に関する国際サイバーセキュリティ標準化の状況に関する機関間レポート）を作成・公開し、IoT サイバーセキュリティの標準環境の分析と IoT システム関連項目と IoT 関連のサイバーセキュリティ標準とのマッピングを行っている。

また、2020 年 5 月 19 日に発行された NISTIR 8259A では IoT device cybersecurity capability core baseline（IoT デバイスのサイバーセキュリティ能力のコアベースライン）の定義とあわせて、それらと同様または関連のある他の標準化組織や業界団体などの既存の IoT サイバーセキュリティガイダンスへの参照が示されており、各能力をより詳細に理解し、合理的な方法で各能力を実装する方法を学ぶ上で非常に貴重なものとなると述べられている。15 組織の資料が参照され、NIST IoT Program の活動は、これらのサイバーセキュリティの標準やガイドラインとの連携を視野に進められていると考えられる。

4.2.2.2 大統領令に基づく活動

米国の大統領令（executive order）は行政命令であり、具体的な法律を明記して行政組織に法執行を命じるものである。バイデン大統領は SIP-CPS に関連するものとして、2021 年 2 月 24 日に重要品目の米国サプライチェーンにおける潜在的な脆弱性についての大統領令を発行した。また、2021 年 5 月 12 日には、邦政府の情報資産におけるサイバーセキュリティの向上を目的とする大統領令を発行した。米国における制度や標準のとりまとめプロセスとして、この２件の大統領令に伴う動きを報告する。

(1) Executive Order on America’s Supply Chains (EO 14017)[134]

2021 年 2 月 11 日、ホワイトハウスの報道官は、政権は現在サプライチェーンにおける潜在的な問題点を特定し、産業界の主要な利害関係者や取引先と協力して積極的に活動しており、政権は将来を見据えて半導体の供給不足という長年の問題は大統領が署名する行政命令に署名と発表し[135]、2 月 24 日にバイデン大統領はコンピュータチップ、医療機器、電気自動車用バッテリー、レアメタルなどの重要品目の米国サプライチェーンにおける潜在的な脆弱性について、100 日間の政府のレビューを命じる大統領令に署名した。また、１年間のレビューの対象分野は、国防、公衆衛生、ICT、ネルギー、運輸、農業並びに食糧生産のサプライチェーンとされ、具体的に国防総省、厚生省、商務省、エネルギー省、運輸省、農業省に報告義務が明示されている。

133 <https://csrc.nist.gov/publications/detail/nistir/8200/final>
134 <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/>
135 <https://thehill.com/policy/technology/538474-biden-to-sign-executive-order-addressing-chip-supply-chain-shortage>

EO 14017 の 1 年後に当たる 2022 年 2 月 23 日 Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry[136] が商務省と国土安全保障省の連名で発表されている。ICT ハードウェア及びソフトウェア製品の現在のサプライチェーン状況を評価し、これらを混乱させる恐れのある主要なリスクを特定し、これを軽減しサプライチェーンの回復力を強化する戦略を提案している。

(2) Executive Order on Improving the Nation's Cybersecurity (EO 14028)[137]

2021 年 5 月 12 日、バイデン大統領が発行した EO 14028 は連邦政府の情報資産におけるいわゆるサイバーセキュリティの向上を目的とした、政策執行からクラウド利用対策、ソフトウエアセキュリティへの対策、インシデント検知、対応の向上、CISA, FBI による連邦政府ネットワークのモニタリングに至るまで、非常に広範な内容を含む。また連邦政府情報システムへの一連の攻撃を踏まえた行動であるとされ、アメリカにおけるサイバーセキュリティへの影響はかなり大きい。なお、EO 14028 の主な対象は既存のいわゆる IT あるいは OT での情報システムであり、IoT については極めて限定的である。

EO 14028 の Section. 4.は、Enhancing Software Supply Chain Security と題された章でその大部分はソフトウェアサプライチェーンに関する内容で、2020 年 12 月に検知された Solarwinds Orion の不正な更新プログラム、その他の脆弱性を悪用した連邦政府情報システムへの攻撃が背景としてあると考えられる。また、この中で IoT の一般消費者向け Labeling Program のための IoT cybersecurity criteria の特定が、商務長官と NIST 所長に命じられ、検討にあたり FTC（公正取引委員会）の議長と連携して実施するように指示された。これに基づき、消費者向け IoT 製品と消費者向けソフトウェアの セキュリティ能力の labeling に関する検討が開始された。

NIST は、2021 年 7 月 28 日に Workshop and Call for Papers on Cybersecurity Labeling Programs for Consumers: Internet of Things (IoT) Devices and Software[138]を発行して、一般消費者向けソフトウェア Labeling に関する Call for Papers を行った結果を 9 月 2 日に公開した後、2021 年 9 月 14 日にワークショップを開催している。

また、この間の 2021 年 8 月 31 日には IoT 機器のサイバーセキュリティ能力に関する Labeling Program の基準案をまとめたホワイトペーパーである DRAFT Baseline Security Criteria for Consumer IoT Devices を発表[139]し、パブリックコメントを受け付けている。

その後、2022 年 2 月 4 日に NIST Cybersecurity Whitepaper: Recommended Criteria for

136 <https://www.dhs.gov/news/2022/02/23/joint-statement-secretaries-raimondo-and-mayorkas-assessment-critical-supply-chains>, <https://www.dhs.gov/publication/assessment-critical-supply-chains-supporting-us-ict-industry>

137 <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

138 <https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/workshop-and-call-papers-cybersecurity-labeling>

139. <https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/iot-device-criteria>, <https://www.nist.gov/system/files/documents/2021/08/31/IoT%20White%20Paper%20-%20Final%20202021-08-31.pdf>

Cybersecurity Labeling for Consumer Internet of Things (IoT) Products[140] として消費者向け IoT 製品、NIST Cybersecurity Whitepaper: Recommended Criteria for Cybersecurity Labeling of Consumer Software[141]として消費者向けソフトウェアのサイバーセキュリティ Labeling 推奨基準の最終版を発行した。

大統領令の 1 年後に当たる 2022 年 5 月 10 日に、NIST はそれまでに寄せられたコメントに加え、パイロットや関連する問題について一般から寄せられた追加の意見を考慮し、これらの消費者向け IoT 製品および消費者向けソフトウェア製品のサイバーセキュリティ Labeling に関する総括報告書 Report for the Assistant to the President for National Security Affairs (APNSA) on Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software[142]を発行している。

NIST は上記 2 月の Whitepaper に対応して、2002 年 9 月に NISTIR 8425: Profile of the IoT Core Baseline for Consumer IoT Products にて消費者向け IoT 製品の IoT コアベースラインプロファイルの規格文書を発行し、2023 年春開始を目標とする消費者向け IoT 製品の Labeling Program 実施に向けて活動を進めている。

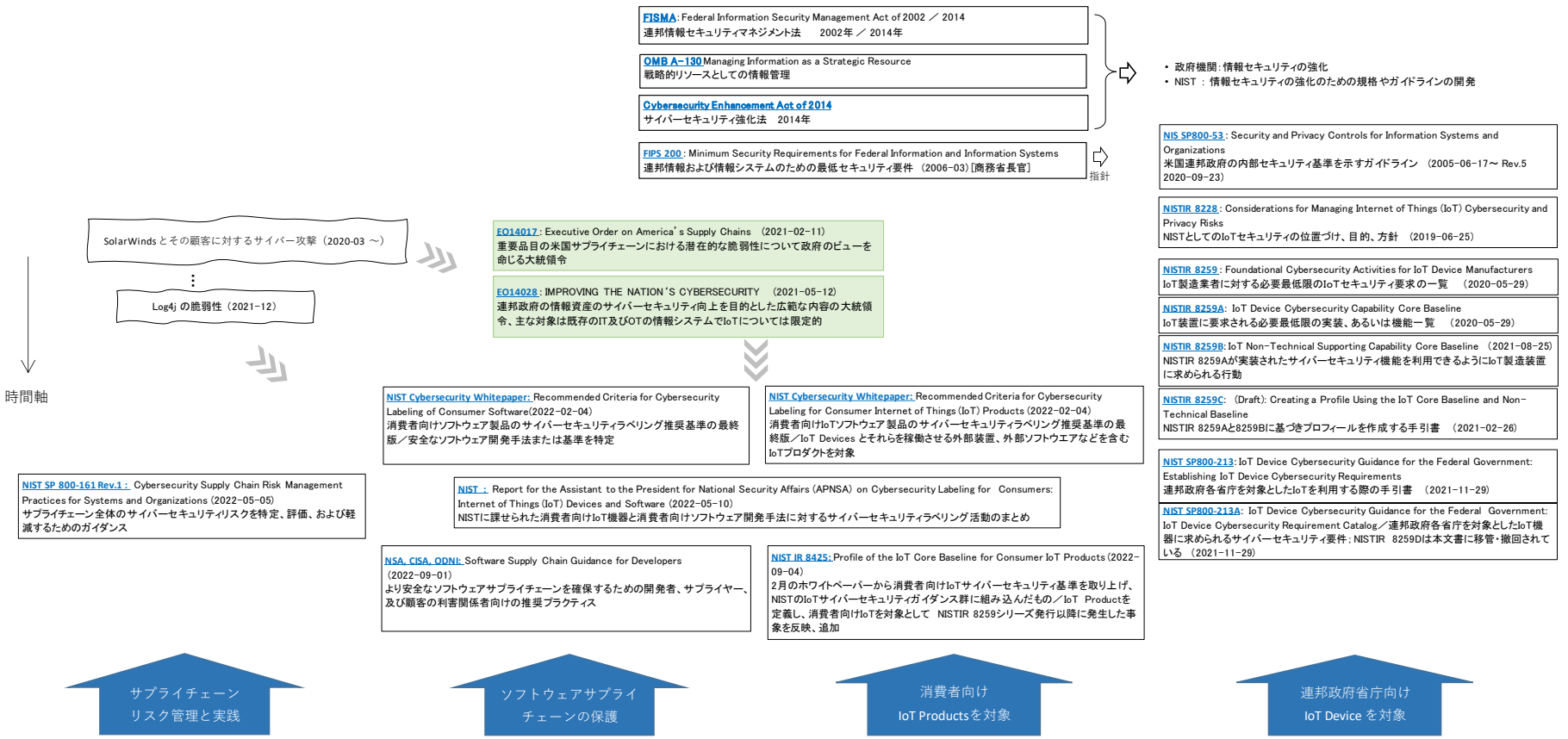
また、EO14028 に対応したソフトウェアサプライチェーンセキュリティの向上に向けた動きとして、2022 年 9 月 1 日に NSA、CISA、ODNI 共同で Securing the Software Supply Chain for Developers を発表し、連邦政府のソフトウェアを取得する顧客に加えて、ソフトウェア サプライヤと開発者の両方に対する体系的なレビュー、プロセスの改善、およびセキュリティ基準などを定めている。

これらの大統領令 EO14017,EO14028 が出されて以降の米国における IoT 関連対象分野に関するガイドライン文書の概要を図 5 に示す。

[140] <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf>

[141] < https://csrc.nist.gov/publications/detail/white-paper/2022/02/04/recommended-criteria-cybersecurity-labeling-of-consumer-software/final >

[142] <https://www.nist.gov/system/files/documents/2022/05/24/Cybersecurity%20Labeling%20for%20Consumers%20under%20Executive%20Order%2014028%20on%20Improving%20the%20Nation's%20Cybersecurity%20Report%20(FINAL).pdf >



CISA　Cybersecurity and Infrastructure Security Agency ：サイバーセキュリティ・社会基盤安全保障庁
EO　Executive Order ：大統領令（行政命令）
FTC　Federal Trade Commission ：連邦取引委員会
NIST　National Institute of Standards and Technology ：米国国立標準技術研究所
NSA　National Security Agency ：アメリカ国家安全保障局（アメリカ国防総省の情報機関）
ODNI　Director of National Intelligence ：国家情報長官
OMB　Office of Management and Budget （行政予算管理局）

図 5　大統領令を契機とした IoT 関連の米国ガイドラインと対象分野

4.2.3 欧州における制度や取りまとめのプロセス

4.2.3.1 標準化機関（ETSI）

欧州委員会公認の標準化機関として約 30 年前に設立された ETSI がある。欧州委員会の規制に適合した技術仕様を標準化する。仕様の実装が正しいかどうかは市場が判断することであり、ETSI が何らかの認証を発行することはない。但し、仕様に準拠しているかどうかを判断するためのツールキットを提供している。ETSI は監督機関、認証機関、インターオペラビリティの監督当局ではない。

ETSI 規格及び技術仕様の実施に技術的に不可欠な知的財産権（IPR）は、適時に宣言され、金銭的補償なしで公平、妥当かつ差別のないライセンス条件（FRAND : Fair, Reasonable And Non-Discriminatory）でライセンスされる必要がある。

メンバーシップは国の代表団単位ではなく、直接加入制であり、ネットワーク事業者、メーカー、政府機関、研究機関などが、独立したメンバーとして加入している。世界各国のいかなる団体の加入を歓迎する。ただし、欧州に拠点を持たない団体の場合、「準メンバー（Associate member）」となる。日本企業も準メンバーとして参加している。準メンバーにも正メンバー同様の議決権が与えられている。ETSI での投票構造は、各企業の売上高に相関して決まる分担金ユニットの数によって議決権の重み付けが決まる。ただし、欧州委員会の政策に関係する EN 規格の策定には参加出来ない。

ETSI は ISO（国際標準化機構）及び IEC（国際電気標準会議）と一部リエゾン関係を持っている。国際レベルでのパートナーは ITU（国際電気通信連合）であり、セクターメンバーである。ITU の下には ITU への標準提出の下準備を行う機構として GSC（Global Standards Collaboration）があり、地域別に定期的な会合を設けている。

ETSI の規格のタイプによって規格化の作業が異なり、3 種類の規格化プロセスがある。**表 2** に規格のタイプと規格化のプロセスを示す。

表 2 ETSI の規格のタイプと規格化プロセス

規格のタイプ（略記号）	投票と承認	注釈	規格化プロセス
技術仕様 (TS)	起草した技術委員会によって承認	技術的な要件が含まれ、迅速に使用できることが重要な場合	I
技術レポート (TR)	起草した技術委員会によって承認	説明資料が含まれる	
グループ仕様 (GS)	業界仕様グループ(ISG)内で作成及び承認	技術的な要件、説明資料、またはその両方を提供	
グループレポート (GR)	業界仕様グループによって公表を承認	情報提供要素のみ	

特別レポート (SR)	作成した技術委員会によって承認	情報を参照のために一般に公開	
ガイド (EG)	メンバーシップ全体	特定の技術標準化活動の取り扱いに関する一般的なガイダンス	Ⅱ
ETSI 規格 (ES)	メンバーシップ全体	技術要件が含まれる	
欧州規格 (EN)	技術委員会によって起草され、欧州標準機関によって承認		Ⅲ

(1) 規格化プロセス Ⅰ

技術仕様（TS）、技術レポート（TR）、グループ仕様（GS）、グループレポート（GR）及び特別レポート（SR）の規格化プロセスであり、技術委員会または業界仕様グループが草案を承認した後、標準を公表する ETSI 事務局に提出する。これらの文書の手順プロセスを図 に示す。

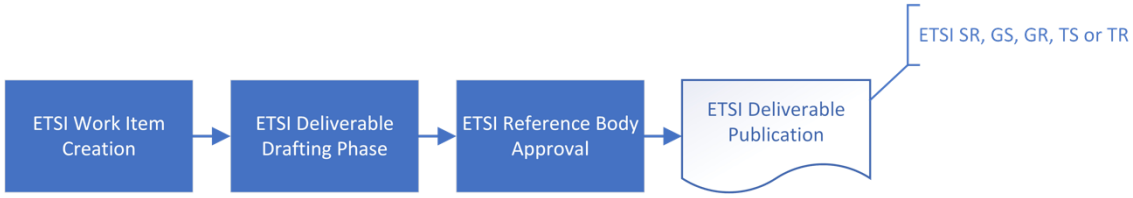


図 6 技術仕様(TS)、技術レポート(TR)、グループ仕様(GS)、グループレポート(GR) 及び特別レポートの承認手順

(2) 規格化プロセス Ⅱ

ETSI ガイド（EG）及び ETSI 規格（ES）の規格化プロセスであり、これらの文書は、「メンバーシップ承認手続き」を使用して、ETSI メンバーシップによって承認される。

技術委員会が草案を承認した後、ETSI 事務局は、その文書を会員に公開する。各 ETSI フル及びアソシエイトメンバーは、基準を採用すべきかどうかについて投票することができる。60 日間以内の投票により採用された場合、ETSI 事務局は標準を公表する。そうでなければ委員会に照会される。規格化プロセスを図 に示す。

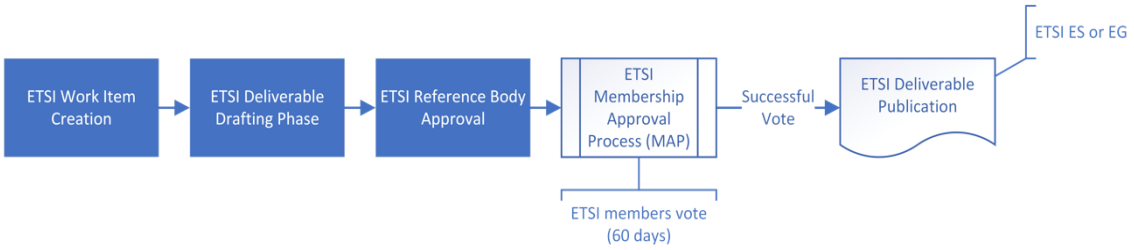


図 7　ETSI ガイド(EG) 及び ETSI 規格(ES)の承認手順

(3) 規格化プロセス Ⅲ

欧州規格（EN）の規格化プロセスであり、ほとんどの EN はパブリック問い合わせと加重投票を 1 つのプロセスで行う。

技術委員会が草案を承認した後、ETSI 事務局は、文書を欧州各国の規格制定団体の NSOs（National Standards Organizations[143]）に公開する。NSOs はパブリック問合せを実施する。これには、標準に関する国家的地位（重み付け投票）の協議と提出が含まれる。この 90 日間以内の投票により採用され、この協議の結果として実質的なコメントが得られなかった場合、ETSI 事務局は草案を最終決定し、基準を公表する。

パブリック問合せの間に受け取った技術的なコメントは、技術委員会によって検討され、草案を改訂して事務局に再提出する可能性がある。変更が重要な場合、事務局は別のパブリック問合せを開始することができる。それ以外の場合、草案は 2 回目の投票に直接提示され、投票が成功した後、事務局は標準を公表する。このプロセスを図 に示す。

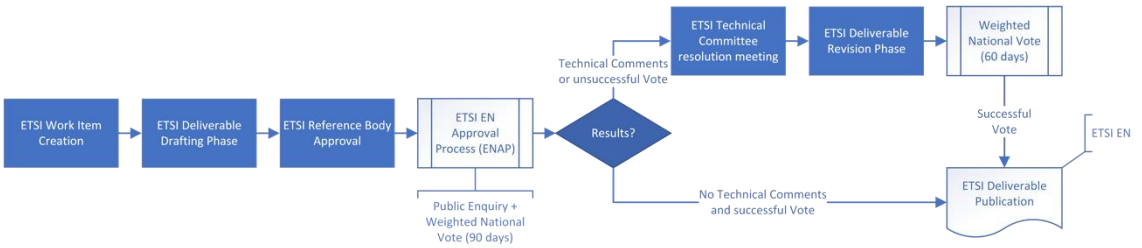


図 8　欧州規格(EN)の承認手順

ETSI の重み付け投票において、少なくとも 71%が草案に賛成している場合、投票は承認される。これは、一部のグループ仕様を除くすべてのタイプの文書に適用される。欧州基準（EN）では、各国の投票は ETSI 総会で合意された重み付けが行われる。他のタイプの文書については、各 ETSI メンバーの投票はメンバー間で合意された重み付けが行われる。

143 <https://portal.etsi.org/TB-SiteMap/NSO/Home>

ETSI では 2019 年から 2021 年にかけてコンシューマ向け IoT セキュリティの文書が制定されている[144]。文書はサイバーセキュリティ技術委員会（TC CYBER：TECHNICAL COMMITTEE CYBER[145]）にて開発されたものである。

TC CYBER では、ユーザー、メーカー、ネットワーク、インフラ、サービス事業者、規制当局に対して、市場主導型のサイバーセキュリティ標準化ソリューション、アドバイス、ガイダンスを提供する信頼できる専門センターであり、利害関係者と密接に協力し、ヨーロッパおよび世界中の組織や市民のプライバシーとセキュリティを向上させる標準を開発している。

(4) ETSI EN 303 645：CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements[146]コンシューマ向け IoT のためのサイバーセキュリティ：ベースライン要件

サイバーセキュリティの専門家が毎日目にしているスマートデバイスに対する大規模で広範な攻撃を防ぐために、接続された消費者製品のセキュリティ基準値を確立し、将来の IoT 認証スキームの基礎となるよう設計された欧州規格であり、IoT 製品にセキュリティ対策を後付けするのではなく、製品の設計段階からセキュリティを組み込むことを要求している。

文書では 13 の推奨事項を規定しており、上位の 3 項は、デフォルトパスワードの廃止、脆弱性開示ポリシーの実装、ソフトウェアの更新の継続となっている。

文書は 2019 年 2 月に ETSI TS 103 645（技術企画）として公開され、2019 年 11 月に 欧州規格の承認手順が開始された。その後 2020 年 6 月に ETSI EN 303 645（欧州規格）として公開されている。

(5) ETSI TS 103 701：CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements[147] コンシューマ向け IoT のためのサイバーセキュリティ：ベースライン要件に対する適合性評価

2021 年 8 月に発行された技術仕様（TS）である。2020 年 6 月に発行された欧州規格 ETSI EN 303 645 の規定に対して、民生用 IoT 製品を評価するためのベースライン要件の評価を規定したものであり、必須および推奨の評価を定めている。EN 303 645 の規定に対するテストであり、EN 303 645 を拡張するものではない。

(6) ETSI TR 103 621： Guide to Cyber Security for Consumer Internet of Things[148] コンシューマ向け IoT のためのサイバーセキュリティの手引き

2022 年 9 月に公開されている手引きの技術レポート（TR）では、製造業者やその他の関係者が

144 <https://www.etsi.org/technologies/consumer-iot-security>
145 <https://www.etsi.org/committee/cyber>
146 <https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf>
147 <https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf>
148 <https://www.etsi.org/deliver/etsi_tr/103600_103699/103621/01.02.01_60/tr_103621v010201p.pdf>

ETSI EN 303 645 に定義された規定を満たすために役立つ使いやすい手引き示されている。EN 302 645 の規定を満たす実装例のセットが含まれているが、すべての可能な実装が示されているわけではない。

4.2.3.2 EU の政策と ECCC の設立

EU のサイバーセキュリティ法、情報セキュリティ指令等に示された要件を具現化すべく、ENISA の強化が行われてサイバーセキュリティ強化の活動が展開された。さらに、Horizon 2020 の 4 つのパイロットプロジェクトにおいて、組織のガバナンス、機能、技術について議論が行われた。これらの進捗から、2021 年 6 月 8 日に Cybersecurity Competence Centre/Network（ECCC) [149] が設立されている。

(1) EU のサイバーセキュリティ関連政策

2019 年 6 月に The EU Cybersecurity Act[150]（欧州サイバーセキュリティ法）が発行され、ENISA の恒久機関化と次の役割が定められ、サイバーセキュリティ認証制度の要件を示が示された。

- EU サイバーポリシーへの貢献
- 欧州サイバーセキュリティ認証制度による ICT 製品、サービス、およびプロセスの信頼性確保
- 加盟国および EU 機関との協力

また 2020 年 12 月には Proposal for directive on measures for high common level of cybersecurity across the Union [151]（ネットワーク・情報セキュリティ指令改定案）が示され、セキュリティ事故報告対象の OTT 等への拡大、加盟国の報告方法の統一、報告機関の指定、報告様式の統一、などが定められている。

同じく 2020 年 12 月 16 日に New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient[152] （EU のサイバーセキュリティ新戦略と、フィジカルとデジタルの重要事業体の耐障害性を高める新ルール）が策定され、欧州の人々の安全と基本的権利および自由に対するリスクに対処するための強力なガードレールを備えたグローバルでオープンなインターネットの構築要件として次が示された。

- レジリエンス、技術的主権、リーダーシップ
- 防止、抑止、対応するための運用能力の構築
- グローバルでオープンなサイバースペースの推進

これらの政策に対して ENISA は次の活動を行っている。

149 <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre>
150 <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>
151 <https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union>
152 <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391>

- GUIDELINES FOR SECURING THE INTERNET OF THINGS Secure supply chain for IoT[153]（モノのインターネットを安全にするためのガイドライン）を発表 (2020/11)
  IoT の専門家の意見を取り入れ、要件や設計から最終用途の配送や保守、廃棄に至るまで、全ライフスパンに対する IoT のサプライチェーンを保護するためのセキュリティガイドラインを作成。
- Cybersecurity Certification: Candidate EUCC Scheme V1.1.1 [154]（サイバーセキュリティの認証：EUCC スキーム V1.1.1 候補）を発表 (2021/5/25)
  欧州の共通標準ベースのサイバーセキュリティ認証スキーム。 IEC15408:Common Criteria、および ISO / IEC18045:Common Methodology for Information Technology Security Evaluation に基づいて構成され ICT 製品のサイバーセキュリティの認証スキームを示す。
- ENISA Threat Landscape for Supply Chain Attack [155]（サプライチェーンへの攻撃に関する脅威の状況）を発表 (2021/7/29)
  2020 年 1 月から 2021 年 7 月にかけての 24 件のサプライチェーンへのサイバー攻撃を分析。攻撃の 66%がサプライヤのコードに焦点を合わせていることを発見している。

(2) Horizon 2020 project[156]におけるパイロットプロジェクト

Horizen 2020 は複数のパートナーによる研究・イノベーションプロジェクトを助成する EU の枠組みである。欧州サイバーセキュリティ法と連携し、欧州サイバーセキュリティコンピテンスネットワークのパイロットの確立と運用、および共通の欧州サイバーセキュリティ研究とイノベーションロードマップの開発の Call for proposals 2017 - H2020 - Cybersecurity[157]（Horizon 2020 サイバーセキュリティコール）が行われている。(2018/8-2019/11)

次の４つのプロジェクトが採択されており、欧州のサイバーセキュリティエコシステムと協力して活動を幅広く調整し、欧州でのサイバーセキュリティの研究、革新、展開の方法を推進する。

- CONCORDIA　2019-01-01～2022-12-31　https://www.concordia-h2020.eu/
- ECHO　2019-02-01～2023-01-31　https://echonetwork.eu/
- SPARTA　2019-02-01～2022-01-31　https://www.sparta.eu/
- CyberSec4Europe　2019-02-01～2022-07-31　https://cybersec4europe.eu/

(3) ECCC の設立

デジタル単一市場を保護するために必要な EU のサイバーセキュリティ技術および産業能力を維持および開発するとして、欧州のサイバーセキュリティ能力を強化および維持し、欧州をサイバーセキュリティ市場で主導的な地位に置く機関として Cybersecurity Competence Centre/Network

153 <https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things>
154 <https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1>
155 <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>
156 <https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-2020_en>
157 <https://euroalert.net/call/3643/call-for-proposals-2017-h2020-cybersecurity>

（ECCC)[158]が 2021 年 6 月 8 日に設立され業務を開始した。

EU は、EU 全体に断片化して広がるサイバーセキュリティに対応する技術を集約し、サイバーセキュリティに関連する投資を適切に行うために ECCC を設立する必要があった。ECCC の目的は、デジタル単一市場を保護するために必要な EU のサイバーセキュリティ技術および産業能力を維持および開発して、欧州のサイバーセキュリティ能力を強化および維持し、欧州をサイバーセキュリティ市場で主導的な地位に置くこととしている。ECCC は、欧州連合の機能に関する条約（TFEU）に基づいて 2021 月 6 月 8 日に設立された新しい EU 機関である

ECCC は、戦略的な投資決定を行い、EU、加盟国、業界からの間接的なリソースをプールして、技術と産業のサイバーセキュリティ能力を改善および強化し、EU のオープンな戦略的自律性を強化する。 センターは、デジタルヨーロッパプログラムとホライズンヨーロッパプログラムのサイバーセキュリティ目標を達成する上で重要な役割を果たす。

また、ECCC は EU 各国の国内調整センター（NCC : the Network of National Coordination Centres）と連携して、サイバーセキュリティ技術共同体の能力を強化し、経済と社会をサイバー攻撃から守り、優れた研究を維持してこの分野における EU 産業の競争力を強化するための、サイバーセキュリティにおけるイノベーションと産業政策を支援する欧州の新しい枠組みである[159]。

2022 年 10 月に欧州委員会は EU 資金を管理する各国調整センターの能力を評価するためのガイドラインを採用している。NCC には次の条件が課せられている。

- 公共部門の組織であるか、大部分が国によって所有されているか、または行政機能を実行し、コンピテンス センターとネットワークがその使命を果たすのをサポートする能力を持っていること
- サイバーセキュリティの研究および技術的専門知識を所有するか、これらにアクセスできること
- 産業界、公共部門、学界および研究界、市民と効果的に関わり調整する能力を有すること

その後、2022 年 2 月には EU 加盟各国に配置された NCC が承認され、表 3 の NCC のリストが公開されている[160]。

158 <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre>
159 < https://cybersecurity-centre.europa.eu/about-us_en>
160 < https://cybersecurity-centre.europa.eu/nccs_en>

表 3　National Coordination Centres の一覧

COUB4:C20	NATIONAL COORDINATION CENTRE
Austria ／ オーストリア	Federal Chancellery of Austria in cooperation with the Austrian Research Promotion Agency ／ オーストリア連邦首相府とオーストリア研究促進庁の協力
Belgium ／ ベルギー	Centre for Cybersecurity Belgium (CCB) ／ サイバーセキュリティ ベルギー センター
Bulgaria ／ ブルガリア	Ministry of Electronic Governance ／ 電子政府省
Cyprus ／ キプロス	Digital Security Authority (DSA) ／ デジタル セキュリティ オーソリティ
Czech Republic ／ チェコ共和国	National Cyber and Information Security Agency ／ 国家サイバー情報セキュリティ局
Germany ／ ドイツ	National Coordination Centre for Cybersecurity - Federal Office for Information Security (BSI) ／ サイバーセキュリティのためのナショナルコーディネーションセンター - 連邦情報セキュリティ局
Denmark ／ デンマーク	The Danish Business Authority ／ デンマーク事業局
Estonia ／ エストニア	Estonian Information System Authority ／ エストニア情報システム局
Greece ／ ギリシャ	National Cybersecurity Authority of Greece ／ ギリシャ国家サイバーセキュリティ局
Ireland ／ アイルランド	National Cyber Security Centre of Ireland ／ アイルランド国立サイバーセキュリティセンター
Spain ／ スペイン	National Cybersecurity Institute (INCIBE) ／ 国立サイバーセキュリティ研究所
Finland ／ フィンランド	Finnish Transport and Communications Agency Traficom's National Cyber Security Centre (NCSC-FI) ／ フィンランド運輸通信庁 トラフィコムのナショナル・サイバー・セキュリティ・センター(NCSC-FI)
France ／ フランス	Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) ／ 独立行政法人情報システム安全保障機構
Italy ／ イタリア	Agenzia per la Cybersicurezza Nazionale (ACN) ／ 国家サイバーセキュリティ機構
Lithuania ／ リトアニア	National Coordination Centre, Ministry of National DefenceSearch for available translations of the preceding linkEN••• ／ 国防省ナショナル・コーディネーション・センター
Luxembourg ／ ルクセンブルク	NATIONAL CYBERSECURITY COORDINATION CENTRE LUXEMBOURG ／ ルクセンブルグ国立サイバーセキュリティ調整センター
Latvia ／ ラトビア	Ministry of Defence ／ 防衛省
Malta ／ マルタ	Malta Information Technology Agency ／ マルタ情報技術庁
Netherlands ／ オランダ	The Netherlands Enterprise Agency (RVO) ／ オランダ企業庁
Poland ／ ポーランド	National Cybersecurity Coordination Centre Unit in the Chancellery of the Prime Minister ／ 首相官邸内ナショナル・サイバーセキュリティ・コーディネーション・センターユニット
Portugal ／ ポルトガル	Portuguese National Coordination Centre ／ ポルトガル国内調整センター
Romania ／ ルーマニア	Centrul Național de Coordonare ／ ナショナル・コーディネーション・センター
Sweden ／ スウェーデン	Swedish Civil Contingencies Agency ／ スウェーデン民間非常事態庁
Slovenia ／ スロベニア	Office of the Government of the Republic of Slovenia for Information Security ／ スロベニア共和国情報セキュリティ局
Slovakia ／ スロバキア	Cyber Security Competence and Certification Centre (KCCKB) ／ サイバーセキュリティ・コンピテンス＆サーティフィケーションセンター

4.3　海外のステークホルダーとの連携

4.3.1 制度や標準の進め方に関する課題

制度や標準に関する本プロジェクトの海外の連携パートナーとしては、IoT セキュリティとサプライチェーンセキュリティに関するガイドラインや標準文書などを発行して大きな影響力を持ち、その制定プロセスの会合などに海外からの参加が可能である組織が候補となる。

米国における IoT セキュリティとサプライチェーンセキュリティの制度や標準については、政府の情報システムに対する取り組みが顕著である。特に米国内のサプライチューンや IoT 機器のセキュリティ強化に関してホワイトハウスは 2021 年に EO14017 と EO14028 の 2 件の大統領令を発行し、連邦政府機関に対して調査と対策を指示してきた。制度や運用については NSA、CISA、NIST の活動が注目される。NSA（National Security Agency：アメリカ国家安全保障局）はアメリカ国防総省の情報機関であり、その活動に参加することは困難である。また、NSA の外局である CISA（Cybersecurity & Infrastructure Security Agency: アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁）の ICT Supply Chain Risk Management Task Force においてサプライチェーンのセキュリティとレジリエンスを検討しているが、メンバーは政府及び業界メンバーであることから、本プロジェクトからの直接の働きかけは難しいと考えられる。

一方、米国の国立標準技術研究所である NIST (National Institute of Standards and Technology) の活動は、その制定プロセスに海外からも参加が可能で、パブリックコメントに対して海外組織からも提案活動を行うことができることから、NIST と NIST においてサイバーセキュリティに関する活動を行っている Cybersecurity for IoT Program（IoT Program と略記）を、連携を進めるべき重要なステークホルダーとして位置付けることができる

しかし、現状では NIST および IoT Program の実担当者には本プロジェクトの活動が認識されているとはいえず、連携を進めるためには IoT Program において本プロジェクト活動の認知度を高めることが必要である。

また、欧州における標準化活動は、基本的に域内企業が参画する ENISA、ETSI 等の標準化機関で進められているが、本プロジェクトや国内企業がこれらの活動に対して直接的に関与することはできないことが課題として挙げられる。

4.3.2 米国とのステークホルダーとの連携

日本では研究開発成果の報道発表や学会等での発表により認知度を高めることができるが、米国では学会活動への参加者と制度や標準を取り纏める担当者は異なり、学会活動などが認知度を高めることには直接は結びつかない。NIST、および IoT Program の実担当者は文書類の制定に直接関わっていることから、本プロジェクトの認知度を高めるためには、文書類のドラフトに対して迅速にコメントを発出する活動を通じて本プロジェクトを紹介して行くことが効果的な方法となる。海外からのコメントであっても米国の立場から有用な内容であれば検討の対象とされる。

IoT Program の文書制定やパブリックコメント、カンファレンスの開催などの情報は一般への公開が義務付けられており、ホームページや RSS（Rich Site Summary）で確認することができるた

め、日本からこれらの情報を入手することに問題はなく、コメントの送付やカンファレンスへの参加も行うことができる。近年はインターネットを経由して参加が可能なバーチャルイベントが開催されており参加への障壁は大きくはない。質疑応答などの機会を捉えて、IoT Program の関係者と意見交換を行うことにより、本プロジェクトの認知度を高めると同時に連携の方法を探ることができる。

一方で、IoT Program の活動は、多くの検討中のガイドライン文書が最終版として確定されてきており、ガイドライン文書に本プロジェクトの活動成果を盛り込むことは難しくなっている。しかしながら、本プロジェクトの活動成果をガイドライン文書の具体運用や今後の改定フェーズにおいて展開することは可能と考えられ、NIST へのアプローチを継続することは今後の連携・協力関係の構築を図る上で重要である。

このためには、これまで公開されてきた IoT Program 関連文書と本プロジェクトの活動成果との対応関係を本プロジェクトの研究開発担当メンバーが整理し取りまとめた成果普及・実証評価 WG の活動成果をベースに SIP-CPS 活動の有効性を関係機関に伝えていくことが有効である。具体例として、4.1.3.1 節で示したような SP 1800-36 (Draft)に関するパブリックコメントの機会を活用して、SIP-CPS の研究成果を基に新たな提案コメントを寄せることにより相互の連携・交流を行う契機とすることが考えられる。SIP CPS で培われた「信頼の創出、証明」の分野で実装可能な具体的な知見を持つのは、SIP-CPS と FIDO FDO[161] と考えられることから、締め切りまでに NIST にコメントを寄せ、SIP-CPS の成果とすることは一つの活動と考えられる。

また、米国連邦政府が資金提供している非営利組織である MITRE[162] は米国の安全性、安定性、福祉に関する活動を展開している。2022 年 6 月にサプライチェーンセキュリティの強化を目的にとした Software of Trust Framework を発表し、8 月に Hot Topics in Supply Chain Security Summit を開催した。2023 年 1 月には SOFTWARE & SUPPLY CHAIN ASSURANCE MEETINGS（SSCA） の開催が予定されている。SSCA は世界中の政府、産業界、学術界の参加者が、ソフトウェアとサプライチェーンのリスク、効果的な実践と緩和戦略、ツールや技術、関係者、プロセス、技術に関するあらゆるギャップに関する知識と専門知識を共有する場とされている。SSCA は無料ですべての関係者に公開され、毎年 2 回から 3 回の開催が計画されていることから、これに参加することによって海外のステークホルダーとの連携を図る機会とすることができる。

米国においては、政府機関のセキュリティ強化をホワイトハウスが主導し、政府機関は連携してその強化のための活動を行っている。日本国内の活動を集約し政府の活動として米国政府の活動と戦略的な連携を働きかけることも、米国のステークホルダーとの連携には重要と考えられる。

4.3.3 欧州のステークホルダーとの連携

欧州における標準化活動は、基本的に域内企業が参画する ENISA、ETSI 等の標準化機関で進められているが、日本と欧州の相互連携の動きとしては、総務省と欧州委員会（通信ネットワーク・コンテンツ・技術総局）との間で、ICT 政策に関する情報交換・意見交換の場として定期的に開催

161 <https://fidoalliance.org/iot-specifications-overview-2/>
162 <https://attack.mitre.org>

している「日 EU・ICT 政策対話」や、欧州委員会の国際標準化に関する国際連携プロジェクトである InDiCo (International Digital Cooperation project on ICT standardization) プロジェクトと連携した活動がある。「日 EU・ICT 政策対話」が 2022 年 2 月に開催され、4 月にはデジタル分野における政策について日 EU の官民で相互理解を深め連携・協力を推進することを目的として定期的に開催している「日 EU・ICT 戦略ワークショップ」が開催されて「サイバーセキュリティ」に関して引き続き日 EU 間の協力を進めていくことを確認がされている。

本プロジェクトの参加企業においては、欧州の現地法人を通じた上記標準化機関への CPS 関連活動への参加をより積極的に進めるとともに、上記に挙げた既存の ICT 国際連携の枠組みを活用して、本プロジェクトの活動成果を伝える活動が有効であると考えられる。

4.3.4 今後の方向性と政府の活動

米国では、2021 年の大統領令から重要品目のサプライチェーン脆弱性対策や、消費者用 IoT 製品のセキュリティ強化が、既存の IoT Program の活動と並行して行われている。

大統領令 EO14017 では、コンピュータチップ、医療機器、電気自動車用バッテリー、レアメタルなどの重要品目の米国サプライチェーンにおける潜在的な脆弱性についての政府のレビューを命じ、さらに国防、公衆衛生、ICT、ネルギー、運輸、農業並びに食糧生産のサプライチェーンを対象に 1 年間のレビューを実施して報告することを国防総省、厚生省、商務省、エネルギー省、運輸省、農業省に義務付けた。1 年後の 2022 年 2 月 24 日には商務省と国土安全保障省の連名で ICT 製造分野を対象とした評価結果が報告され、多くの課題事項とこれらのサプライチェーン・レジリエンス強化のための 8 項目の提言が示されている。

また、連邦政府のサイバーセキュリティ向上を目的とした大統領令 EO14028 では、CPS 分野における具体策として IoT とソフトウェアに関連する Labeling Program が示されている。

これに対し、NIST は 2022 年 2 月に 2 件の NIST Cybersecurity Whitepaper を発行し消費者向け IoT 製品とソフトウェア製品のサイバーセキュリティ Labeling の推奨基準の最終版を公開した。

9 月には IoT 機器のサイバーセキュリティ要件や製造業者の組織の行動要件に対し、消費者向け IoT 製品に必要とされる詳細化を行った規格文書 NISTIR 8424 を発行し、10 月にはホワイトハウスがサイバーセキュリティを強化するための行動指針を発表し、消費者向けの IoT 機器の Labeling Program 関連のワークショップを開催して、2023 年春を目標として製品ラベルの標準化を推進する方針を示している。

また、ソフトウェアに関しては 9 月に NSA、CISA、ODNI が連名でより安全なサプライチェーンを確保するためのソフトウェア開発者向けのガイダンスを発表し、続けて 10 月にはソフトウェアサプライヤ向けのガイダンスを発表している。さらに、今後消費者向けのガイダンスの発行が予定されており、米国政府のサプライチェーンに対する取り組みが際立っている。

10 月のホワイトハウスのワークショップには、米国政府系機関のほかに、欧州委員会と企業団体 17 組織が参加しており、韓国企業 2 社に対して日本企業は 1 社のみの参加となっている。米国政府のこのような活動については動向を把握し、日本政府と国内団体や企業が連携した活動が今

後必要になっていく。

欧州においては、 欧州のサイバーセキュリティ能力を強化・維持し、サイバーセキュリティ市場で主導的な立場を確保する組織として 2021 年 6 月に ECCC (European Cybersecurity Competence Network and Centre)が設立された。2022 年 2 月には ECCC と連携する EU 各国の国内調整センタ（NCC : the Network of National Coordination Centres）が承認されてサイバーセキュリティ技術共同体の能力を強化する活動が行われている。

また 9 月には欧州で販売されるデジタル要素を有するさまざまな製品を対象とするサイバーレジリエンス法案が発表され、11 月には大手企業のプラットフォームをオープンで相互運用可能なものにするデジタルマーケット法（DMA）が発効し、さらに EU 全域での共通した高いレベルのサイバーセキュリティのための措置に関する指令（NIS2）が欧州議会で承認され、今後欧州各国において法整備が行われる。

以上のように、IoT セキュリティ強化とサプライチェーンのセキュリティに関する取り組みが欧米各国で急速に強化されており、SBOM や Labeling などが米国の調達条件へ反映され、また欧州においては各国の法律に展開されることが想定されることから、今後の動向を引き続き注意深く注視していく必要がある。

日本では、政府調達の情報システムのセキュリティ要件の策定方法が定めてられているが、これを米国の連邦システムの調達条件や欧州の法制度に対応できるサプライチェーンセキュリティとレジリエンスの要件にまで拡張して国内企業に展開することが、本プロジェクトの成果を海外へ展開し国内企業がグローバルに活動するために有効な方法と考えられる。

また、これと併せて本プロジェクトの成果を用いて構築されるサプライチェーンのプラットフォームが世界のサプライチェーンと相互に運用されることを期待する。

5　海外における技術開発プロジェクト等における技術目標に関する調査

5.1　海外における技術開発プロジェクト等における技術目標

5.1.1 調査方法

調査方法の内、調査対象については、本調査の比較対象となる「戦略的イノベーション創造プログラム（SIP）第 2 期／IoT 社会に対応したサイバー・フィジカル・セキュリティ（以下、SIP-CPS)」の技術課題領域に対応する技術の研究開発を進めていると考えられる活動の調査に加え、セキュリティの専門家が評価している「RSA Conference Announces Finalists for RSAC Innovation Sandbox Contest 2022」の入賞製品を対象に調査を行った。

SIP-CPS の 2022 年度の研究開発は次の研究開発項目で構成されている。

（A）「信頼の創出・証明」技術の研究開発

A1： IoT サプライチェーンの信頼の創出技術基盤の研究開発

A2： IoT 機器等向け真贋判定による信頼の証明技術の研究開発

（B）「信頼チェーンの構築・流通」技術の研究開発

B2： 信頼チェーンに関わる情報の安全な流通技術の研究開発

B3： サプライチェーン全体の信頼性確保に向けた信頼データ交換・共有技術」

（C）「信頼チェーンの検証・維持」技術の研究開発

C2： 信頼チェーンの維持技術の研究開発

SIP-CPS の課題領域を意識した調査として、研究開発項目の A1 に対しては、米国 NIST 公募・評価の IoT 用軽量暗号技術を、B2 に対しては、主要な BlockChain コンソーシアムの製品・技術を、技術を特定していない A2、B3、C2 に対しては、欧州の商取引環境整備を目指す IDSA/GAIA-X の活動（本体、提案ユースケースなど）を調査対象とした。

また、調査内容としては、SIP-CPS との比較を行う観点から、セキュリティ強度、監視対象、監視項目、協調している機能、などを対象に調査を行った。

調査対象の一覧を以下に示す。

1. RSA Conference Announces Finalists for RSAC Innovation Sandbox Contest 2022 の入賞 10 製品・企業（以下、RSA2022[163]製品・企業）
2. 米国 NIST IR 8425 [164]として公開された、IoT 製品の IoT core に対するセキュリティのベースラインプロファイル（初版）
3. 欧州の Gaia-X[165] が提供している、データ主権の信頼の場の構築を支援する推奨規定
4. 欧州の IDSA（International Data Space ）[166]が提供している IDS コンポーネント[167]

5.1.2 調査結果

5.1.2.1 RSA2022 コンテスト入賞製品・企業[168]

「RSA Conference Announces Finalists for RSAC Innovation Sandbox Contest 2022」は、セキュリティの専門家集団が主催する著名な会議で審査された製品・組織であり、2022 年のファイナリストは、現時点で技術的に最も到達レベルが高く競争力の高い製品・組織と判断できる。

以下、ファイナリスト 10 件について調査した概要を示すと共に、考察として、SIP-CPS 技術・製品との類似性、SIP-CPS 技術・製品が参考とすべきと思われる点などを示す。

(1) Araali Network[169]

Araali は、クラウドネイティブ環境向けの脅威管理ソリューションである。脅威を検出するだけでなく、ブロックすることもできる。 eBPF（Extended Berkeley Packet Filter ）を利用すること

163 <https://www.rsaconference.com/library/press-release/rsa-conference-announces-finalists-for-rsac-innovation-sandbox-contest-2022>
164 <https://csrc.nist.gov/publications/detail/nistir/8425/archive/2022-06-17>
165 <https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html>
166 <https://internationaldataspaces.org/we/>
167 <https://internationaldataspaces.org/make/use-cases-overview/>
168 <https://www.rsaconference.com/library/press-release/rsa-conference-announces-finalists-for-rsac-innovation-sandbox-contest-2022>
169 <https://www.araalinetworks.com/>

で、仮想プライベートクラウドで「誰が何をできるか」に関する明示的なポリシーを適用し、悪意のあるコードによるバックドアの確立やサービスへのアクセスをブロックできる。

Araali はランタイムを継続的に監視して、コンテキストに応じた実用的なアラートとクラウドネイティブ IDS（Intrusion Detection System）を提供する。具体的には、資産に対する完全かつ包括的な可視性については、クラスター、名前空間、ポッド、コンテナにズームインしてランタイムを理解することができ、完全で包括的なビューが得られる。

アプリ同士の対話方法、サードパーティ サービス、クラウド サービス、SaaS を継続的に可視化できる。

キーとなる技術は、カーネル内でパケットをフィルタリングする技術で、有用なネットワークパケットをカーネルから直接キャプチャし、それらをユーザー空間にはコピーしない。 これにより、不要なパケットは、カーネル内で早期に破棄することができる。1992 年に発明されている。[170]

［考察］

Araali Network は、サーバーレベルで、他のシステムの送受信を監視し、異常パケットをブロックできる技術である。カーネル内にフィルターを設定することが可能のため、SIP-CP の C2 機能の性能向上に資する技術として、連携候補の技術と判断する。目標とする評価項目ではなく、必要により、連携を図る対象と考えられる。

(2) BastionZero, Inc.[171]

BastionZero は、開発チームに、インフラストラクチャ（サーバー、クラスター、データベースなど）へのゼロトラストアクセスを提供するクラウド サービスである。新しい暗号化プロトコル設計を使用して、サービスへの侵害がインフラストラクチャへの侵害につながらないよう機能する。

［考察］

BastionZero は、システム開発時のセキュア環境の維持と、もしもの場合の影響範囲を抑える機能を有している。サイバー・フィジカルシステムでは、常に、システム自体が機能拡張等が行われることから、ソフトウェアや構成などの変化時のセキュリティ安全性も重要な評価指標となると考える。

SIP-CPS の研究開発項目 A2 においても、他ベンダーによるアプリケーション開発時のセキュリティの観点で、A2 の特徴的な技術の真贋判定機能と比較を行う対象候補と考えられる。

(3) Cado Security[172]

Cado Security は、クラウド検査プラットフォームを提供する。クラウド環境全体のインシデン

---

170 <https://f.hubspotusercontent00.net/hubfs/6860301/Technology%20Page%20-%20Website/BPF%20to%20eBPF.pdf>

171 <https://www.bastionzero.com/>

172 <https://www.cadosecurity.com/>

ト対応を可能とする本システムは、フォレンジック レベルのデータキャプチャと処理を自動化し、クラウド、コンテナ、およびサーバレス環境で簡単にフォレンジックデータを取得できる。これにより、これまでアナリストが数日かかっていたデータ収集を数分で自動収集する。

技術的な特徴は、end-to-end でのインシデント対応プロセスの高速化、クラウドを活用したデータ処理の迅速化、である。

［考察］

Cado Security は、インシデントレベルのセキュリティ脅威を検知・分析する技術である。SIP-CPS C2 と同様の監視系の技術であるが、クラウド（サイバー系）を対象としており、比較候補ではないと判断する。

クラウド環境全体のデータキャプチャの自動化を得意としている可能性があり、必要により、連携を図る対象と考えられる。

(4) Cycode[173]

Cycode は、SDLC[174] 全体の可視性、セキュリティ、および整合性を提供するソフトウェア・サプライチェーン・セキュリティ・ソリューションである。 本ソリューション は、DevOps ツールおよびインフラストラクチャと統合して、セキュリティ体制を強化し、一貫したガバナンスを実装し、脅威を検出し、侵害のリスクを軽減する。

技術的な特徴には、①ハードコードされたシークレット検出し、プル要求でシークレットをブロック、②疑わしい動作を特定し、独自のコード漏えいを検出するソースコードのリーク検出、③パイプライン構成分析を使用して SDLC 全体のすべての依存関係の脆弱性を検出する次世代の SCA（Software Composition Analysis：ソフトウェアコンポジション解析）- パイプライン構成分析、④すべての DevOps ツールにわたる CI / CD（Continuous Integration：継続的インテグレーション/Continuous Delivery：継続的デリバリ）セキュリティポリシーとソース管理のガバナンスを管理する CI/CD セキュリティとソース管理、⑤開発の早い段階でカスタムコードの脆弱性を迅速に排除する SAST （静的アプリケーションセキュリティテスト）、⑥整合性検証、異常検出、重要なコード監視、ガバナンスを組み合わせた包括的なコード改ざん防止ソリューション、⑦クラウドの設定ミスを防ぎ、Kubernetes、Terraform、CloudFormation などにセキュリティ標準を適用するコードセキュリティとしてのインフラストラクチャ、がある。

［考察］

Cycode は、ソフトウェア開発のライフサイクルでのセキュリティリスクを回避するプラットフォームである。

ソフトウェア開発プロセスが対象であり、SIP-CP 第 2 期が対象とする IoT を含むソフトウェアに言及していないが、SIP-CPS 第 2 期 A2 の真贋判定技術と同様、ソフトウェアの改ざん検知の仕組みをいくつか有しており、優劣を判定する比較対象の候補の 1 つと考える。

---

173 <https://www.cadosecurity.com/>

174 Systems/Software Development Life Cycle

(5) Dasera[175]

Dasera は 、利用者により多くのデータを提供しながら、更新されていく大規模なデータを保護するという課題を解決するデータガバナンスプラットフォームである。コンテキストを継続的に監視し、データ ライフサイクル全体でセキュリティとコンプライアンスを自動的に統合することで、データ ガバナンスを運用可能にしている。

［考察］

Dasera は、データガバナンスプラットフォーム技術である。SIP-CPS 第 2 期が目指す技術領域とは異なると考える。このため比較候補ではないと判断する。

(6) Lightspin[176]

Lightspin のグラフベースのプラットフォームは、DevOps とセキュリティ チームがクラウドスタックを安全に保つために必要な時間、コスト、およびリソースを削減する。重要な攻撃パスを特定することで、Lightspin はさまざまなセキュリティ問題の間の点を結び付け、ビルド時間からランタイム、運用に至るまで、最も重要な重要な問題に優先順位を付けて修正する。

主な機能には、①インフラストラクチャをコードとしてスキャンし、展開前に構築のリスクがないことを確認する IaC（Infrastructure as Code）セキュリティ、②完全なコンプライアンスを達成し、クラウドセキュリティのベストプラクティスを確保する CSPM（Cloud Security Posture Management : クラウドセキュリティ体制管理）+ KSPM（Kubernetes[177] Security Posture Management : Kubernetes セキュリティ体制管理）、③関連する CVE（Common Vulnerabilities and Exposures：共通脆弱性識別子）を特定し、セキュリティの調査結果とその重要な攻撃パスに結び付けるワークロードスキャン、④クラウド環境全体に存在する重大な構成ミスと脆弱性を迅速に特定する攻撃パス分析、⑤実行時に生成されたコードを使用して、サーバー上の既存のマルウェア侵入を検出するランタイム保護、⑥AWS、Azure、GCP のパブリッククラウドのフットプリントを即座に発見できる攻撃対象領域の検出、がある。

［考察］

Lightspin は、クラウドを対象としたセキュリティ監視システムである。クラウドを対象としているが、SIP-CPS 第 2 期の A2（生成コード活用ランタイム保護）、C2（共通脆弱性識別子の特定と攻撃パスとの結びつき分析、クラウド環境の構成ミスと攻撃パス分析、攻撃対象領域検出）が開発を進めている機能に近いものもある。IoT を対象とはしていないが、機能ベースでは優劣を判定する比較対象の候補の 1 つと考える。

---

175 <https://www.dasera.com/>

176 <https://www.lightspin.io/>

177 Kubernetes は、コンテナ化したアプリケーションのデプロイ、スケーリング、および管理を行うための、オープンソースのコンテナオーケストレーションシステム。元は Google が設計したシステムであるが、現在は Cloud Native Computing Foundation がメンテナンスを行っている。

(7) Neosec[178]

Neosec は、XDR[179]（Extended Detection and Response）技術を API の保護に導入することで、アプリケーション セキュリティを提供する。この SaaS プラットフォームは、すべての API を検出し、その動作を分析して、内部に潜む脅威を阻止する。これにより、セキュリティプロフェッショナルは API 資産全体の動作を可視化できる。

主な特徴は下記である。

① データの重要性に基づく行動分析

このデータ分析プラットフォームはデータドリブンでる。単一の要求で動作する他のソリューションとは異なり、30 日間にわたって API データセット全体を分析し、動作をベースライン化し、時間の経過に伴う使用状況を把握する。このデータ豊富なアプローチにより、セキュリティチームは無意味なアラートではなく、実際の脅威に集中できる。

② すべてを調べることで API の悪用を理解するコンテキスト認識型セキュリティ

行動分析は、時間の経過とともにデータを調べることによってのみ可能である。このため、この PF は、API 資産内のすべてのエンティティの動作の動的プロファイルを作成する。セキュリティチームと開発者は、コンテキストを理解することでより良い決定を下すことができ、悪用やデータ侵害を防ぐことができる。

③ XDR 手法によるアプリケーション・セキュリティ

XDR(拡張検出と応答)カテゴリを設けることで、従来のアプリケーション・セキュリティを再構築し、API セキュリティを実現し、XDR と同じ精度の動作分析を可能とした。

［考察］

Neosec は、長期に渡る API データセット全体を分析してセキュリティを検知するプラットフォームである。

SIP-CPS 第 2 期の C2 の信頼チェーンの検証・維持と同じ目標を持つプラットフォームであるが、SaaS プラットフォームであり、クラウドを対象としている可能性がる。

対象としているシステムの範囲が異なる可能性はあるが、API データセット全体を分析するという特徴については、比較評価の候補の 1 つである。

(8) Sevco Security[180]

Sevco Security はクラウドネイティブの資産インテリジェンス プラットフォームである。オンプレミスとクラウドの両方ですべての資産、ユーザー、およびアプリケーションに可視性を提供し、より良い意思決定のための包括的で信頼できる信頼できる情報源を作成する。

特許取得済みのテレメトリエンジンは、セキュリティと IT のリスクの検出を軽減できる。

---

178 <https://www.neosec.com/>

179 エンドポイントだけでなく、ネットワーク、アプリケーションスイート、ユーザーペルソナ、オンプレミスのデータセンター、クラウドでホスティングされているワークロード全体を通じて、サイバー攻撃の検知と防止を実現できるようにするセキュリティアプローチ

180 <https://www.sevcosecurity.com/>

主な特徴は下記である。

① リアルタイム資産インベントリ

このデータパイプラインは、異なるデータソースを継続的に集約して、数時間～数週間前などの古いスナップショットではなく、リアルタイムの資産インベントリを提供する。

② マルチソースの相関と調整

環境内のすべての既存のツールを集約および重複排除することにより、包括的なインベントリを提供する。

③ 資産テレメトリ

継続的なデータパイプラインを通じて、ツールによって観察されたすべての変更に対して資産テレメトリを生成する。すべてのイベント（デバイスが IP アドレスを変更した瞬間、やデバイスが別の物理的な場所に表示された瞬間、など）がキャプチャされる。Sevco の資産テレメトリは、調査をサポートするために簡単に照会することも、SIEM (Security Information and Event Management) および SOAR (Security Orchestration, Automation and Response) プラットフォームに直接プッシュすることもできる。

④ API ベースの統合による数分での構成完了

デプロイエージェントではなく、このシステムのネイティブ API を介して既存のツールに接続し、保有データを自動的に取り込み、正規化し、調整してすぐに結果を提供する。

［考察］

Sevco Security は、クラウドを対象としたリアルタイムセキュリティ監視システムである。

他のツールなどの情報も集約し分析を行っている。デバイスも監視対象であり、IoT 対応も可能と思われる。

SIP-CPS 第 2 期の C2 の信頼チェーンの検証・維持と同じ目標を持つプラットフォームと考えられる。デプロイ方法に特徴を有していると思われるが、他の特徴は一般的な内容であり、比較候補ではないと判断する。目標とする評価項目ではなく、必要により、連携を図る対象と考えられる。

(9) Talon Cyber Security[181]

Talon は、企業向けに特別に構築された安全なブラウザを提供することで、セキュリティ プログラムを最新化し、ハイブリッド ワークのユーザーエクスペリエンスを向上させる。 本ブラウザは、セキュリティを簡素化するために必要な、SaaS アプリケーションに対する詳細なセキュリティの可視性と制御を提供する。

主な特徴は下記である。

① 安全で分離された Chromium ベースのワークスペース

Talon の安全なエンタープライズ ブラウザである TalonWork は、強化された Chromium ベースのブラウザであり、Web トラフィックをエンドポイントでローカルに分離し、レスポンシブでネイティブなユーザー エクスペリエンスを提供する。TalonWork は、一般的な

[181] <https://talon-sec.com/>

ID ブラウザと統合して、ユーザーのオンボーディングとポリシーの適用を合理化する。

② データ損失防止

TalonWork は、サイバー リスクを軽減するための包括的な DLP を提供する。 これには、機密ファイルが外部で共有されたり、エンドポイントに保存されたりするのを防ぐためのファイル暗号化が含まれる。 TalonWork は、クリップボード、印刷、スクリーンショットの細かな制限も提供する。

③ 脅威からの保護

TalonWork は、強化された安全なブラウジング機能により、悪意のあるドメイン、URL、およびフィッシング Web サイトへのアクセスを防ぐ。TalonWork は、アップロード/ダウンロードされたファイルをスキャンし、CrowdStrike の Falcon X QuickScan エンジンと統合して高度なマルウェア保護を提供できる。

④ ゼロトラスト

TalonWork は、基盤となる OS、パッチ バージョン、インストールされているセキュリティソフトウェアなど、エンドポイントのセキュリティ体制を包括的に検証することで、ゼロトラスト アプローチと連携する。 また、TalonWork は、エンタープライズ リソースにアクセスするユーザーとエンドポイントを継続的に認証および承認する。

⑤ SaaS の可視性と保護

TalonWork は、従業員や第三者のプライバシーに影響を与えることなく、仕事に関連するすべての Web ブラウジングを包括的に監視する。 TalonWork は、SaaS および Web アプリケーション内のユーザーアクティビティを監査して、セキュリティとコンプライアンスの要件に対処する。

［考察］

Talon Cyber Securit は、ブラウザを中核に据えたセキュリティシステムである。特徴的なセキュリティ機能に、従業員や第三書の Web ブラウジングの包括的監視がある。

SIP-CPS 第 2 期では、人間を対象とした B の信頼チェーンの構築・流通が目標とするセキュリティの領域に対応すると考える。

人間のミスや悪意に対するリスクの観点で、評価対象、連携対象の候補の１つと考えられる。

(10) Torq[182]

Torq は、セキュリティ チーム向けのノーコードのセキュリティ構築の自動化プラットフォームである。無限の接続性、ドラッグ・アンド・ドロップ編集、数百のテンプレートにより、あらゆるプロセスを簡単に自動化できる。大規模な組織から最先端の新興企業まで、セキュリティ チームは Torq を信頼して複雑さを最小限に抑え、保護を最大化している。

主な特徴は下記である。

① セキュリティ体制の強化

[182] <https://torq.io/>

自動的にトリガーされるフローで脅威に迅速に対応でき、環境内でリスクが検出されるとすぐに修復する、また、誤検知や事後対応型作業を排除したプロアクティブな姿勢への転換ができる。

② セキュリティ運用の迅速化と自動化

コード不要のドラッグ&ドロップ デザイナーでフローを構築できるため、開発者やプロフェッショナル サービスは不要で、環境内の任意のツールに簡単に接続して、完全な保護を確保でき、何百ものすぐに使えるテンプレートにより、数分で作業を開始できる。

③ 自分のやり方でより速く作業

1 つのステップを自動化することから始め、フローを複雑なブランチに拡張できる。また、ベスト・プラクティス・テンプレートを使用すると、迅速に作業を開始でき、REST API は必要に応じてカスタマイズも可能である。また、どこからでもフローをトリガー (Web、Slack、コマンドライン) 、または自動化できる。

④ 準拠した安全なプラットフォーム

このプラットフォームのインフラストラクチャと運用は、Torq プラットフォームが業界最高級のセキュリティおよびコンプライアンス基準を満たすように、厳格な外部監査を受けている。

- SOC 2[183]タイプ 2 認定
- HIPAA[184]準拠
- ISO 27001 認証取得
- GDPR[185]準拠

［考察］

Torq は、ドロップ・アンド・ドロップで簡便にセキュリティ設計が可能なツールである。

SIP-CPS 第 2 期の目標と異なっているが、セキュリティ設計人材の層を厚くしていく観点から、連携候補の 1 つと考えられる。

5.1.2.2 NIST IR 8425[186] ：IoT 製品の IoT core に対するセキュリティのベースラインプロファイル

米国 NIST が IoT Core に対するセキュリティの ベースラインの消費者プロファイルを 2022 年 6 月に初版を公開し、2022 年 9 月に最終版を公開した。

IoT 製品の機能に対する要件と、非機能的なサポート要件から構成されている。

概要を以下紹介する。

---

183 SOC 2（Service Organization Control Type 2）：米国公認会計士協会（AICPA）が開発したサイバーセキュリティ・コンプライアンス・フレームワーク

184 HIPAA（Health Insurance Portability and Accountability Act ）：米国において保護された健康情報の合法的な使用と開示の概要を示す一連の連邦規制基準

185 GDPR（General Data Protection Regulation：一般データ保護規則）：欧州議会・欧州理事会および欧州委員会が欧州連合 内の全ての個人のためにデータ保護を強化し統合することを意図している規則

186 <https://csrc.nist.gov/publications/detail/nistir/8425/final>

(1) IoT 製品の機能

- Asset Identification

IoT 製品は一意に識別可能であり、IoT 製品のすべてのコンポーネントのインベントリを作成する。

1. IoT 製品は、顧客およびその他の許可されたエンティティ (IoT 製品開発者など) によって一意に識別できる。
2. IoT 製品は、各 IoT 製品コンポーネントを一意に識別し、接続された製品コンポーネントの最新のインベントリを維持する。

サイバーセキュリティ ユーティリティ:

IoT 製品とそのコンポーネントの識別機能は、更新のための資産管理、データ保護、およびインシデント対応のためのデジタル フォレンジック機能をサポートするために必要。

［考察］

IoT 製品に Asset Identification 機能（IoT 製品の一意識別可能性）を要求しており、SIP-CPS 第 2 期の課題 A1、A2、B1、B2、B3、特に、A1 の機能に対応していると考えられる。

- Product Configuration

IoT 製品の構成は変更可能で、デフォルト設定を復元する機能を有し、すべての変更は許可された個人、サービス、その他 IoT 製品コンポーネントによってのみ実行できる。

1. 顧客は、IoT 製品コンポーネントを介して IoT 製品の構成設定を変更できる。
2. IoT 製品は、該当する IoT コンポーネントに構成設定を適用する。

サイバーセキュリティ ユーティリティ:

IoT 製品の機能側面を変更する機能は、顧客がニーズと目標に合わせて IoT 製品の機能を調整するのに役立つ。ユーザーは、リスク選好度（risk appetite）に基づいて特定の脅威やリスクを回避するように IoT 製品を構成できる。

［考察］

IoT 製品に Product Configuration 機能（IoT 製品の構成変更可能性）を要求しており、SIP-CPS 第 2 期の課題 A2 の機能に対応していると思われる。

- Data Protection

IoT 製品とそのコンポーネントは、(すべての IoT 製品コンポーネントにわたって) 保存され、(IoT 製品コンポーネント間/ IoT 製品の外部の両方で）送信されるデータを、不正なアクセス、開示、および変更から保護する。

1. 各 IoT 製品コンポーネントは、保存データを安全な手段で保護する。顧客、自宅、家族などから収集、または収集・保存されたアクセスできないデータを削除または

レンダリングする機能を含む。

2. IoT 製品のコンポーネント間または製品の外部でデータが送信される場合、データ送信の保護を使用する。

サイバーセキュリティ ユーティリティ:

データの機密性、整合性、および可用性を維持することは、IoT 製品のサイバーセキュリティの基盤。 ユーザーは、データが保護され、データの保護が IoT 製品の安全で意図された機能を保証するのに役立つことを期待する。

［考察］

IoT 製品に Data Protection 機能（データへの不正なアクセス、開示、および変更から保護）を要求しており、SIP-CPS 第 2 期の課題 C2 の機能に対応していると思われる。

- Interface Access Control

IoT 製品とそのコンポーネントは、ローカル インターフェイス（IF）とネットワーク IF、およびそれらの IF で使用されるプロトコルとサービスへの論理アクセスを、許可された個人、サービス、および IoT 製品コンポーネントのみに制限する。

1. 各 IoT 製品コンポーネントは、許可されたエンティティのみへのアクセスを制限するために、すべての IF（ローカル IF、ネットワーク IF、プロトコル、およびサービスなど）へのアクセス（との間）を制御する。少なくとも、IoT 製品とそのコンポーネントは次のことを行う必要がある。
   a. IoT 製品の操作に必要な IF のみを使用し、アクセスできるようにする。他のすべてのチャネルとチャネルへのアクセスは削除されるか、保護される。
   b. IoT 製品の使用に必要なすべての IF に対して、アクセス制御手段が用意されている（例：固有のパスワードベースの多要素認証）。
   c. すべての IF について、アクセスおよび変更権限は制限されている。
2. IoT 製品は、一部のコンポーネントを介して手段を実行し、IF アクセス コントロールを保護および維持する。少なくとも、IoT 製品は次のことを行う必要がある。
   a. IoT 製品コンポーネント間で共有されるデータが、フォーマットとコンテンツの指定された定義と一致することを検証する。
   b. 不正な送信や他の製品コンポーネントへのアクセスを防止する。
   c. 初期接続中（オンボーディング中）および切断または停止後に接続を再確立するときは、適切なアクセス制御を維持する。

サイバーセキュリティ ユーティリティ:

IoT 製品へのすべての内部/外部 IF へのアクセスをインベントリし、制御することは、不正なアクセスと変更を防止することにより、IoT 製品、そのコンポーネント、およびデータの機密性、整合性、および可用性を維持するのに役立つ。

［考察］

IoT 製品に Interface Access Control 機能（アクセスを、許可された個人、サービス、およ

び IoT 製品コンポーネントのみに制限）を要求しており、SIP-CPS 第 2 期の課題との対応関係は明確ではない。

- Software Update

すべての IoT 製品コンポーネントのソフトウェアは、許可された個人、サービス、およびその他の IoT 製品コンポーネントが、IoT 製品コンポーネントごとに適切な安全で構成可能なメカニズムを使用することによってのみ更新できる。

1. IoT 製品の各コンポーネントは、検証済みのソフトウェア更新を受け取り、検証し、適用できる。
2. IoT 製品は、IoT 製品コンポーネントのソフトウェアを最新の状態に保つための手段を実装する（例：更新の自動適用または IoT 製品を介した利用可能な更新の一貫した顧客通知）。

サイバーセキュリティ ユーティリティ:

IoT 製品の展開後にソフトウェアの脆弱性が発見される場合がある。 ソフトウェア更新機能により、セキュリティ パッチを安全に配信できる。

［考察］

IoT 製品に Software Update 機能（ IoT 製品コンポーネントのソフトウェアが、IoT 製品コンポーネントごとに適切な安全で構成可能なメカニズムを使用することによってのみ更新）を要求しており、SIP-CPS 第 2 期の課題 A2 の機能に対応していると思われる

- Cybersecurity State Awareness

IoT 製品は、IoT 製品のコンポーネントとそれらが保存および送信するデータに影響を与える、または影響を受けるサイバーセキュリティ インシデントの検出をサポートする。

1. IoT 製品は、IoT 製品コンポーネントに影響を与えたり影響を受けたりするサイバーセキュリティ インシデントと、それらが保存および送信するデータを検出するために使用できる IoT コンポーネントの状態に関する情報をキャプチャおよび記録する。

サイバーセキュリティ ユーティリティ:

データの保護と適切な機能の確保は、デバイスが予期しない方法で動作を開始したときに顧客に警告する機能によってサポートできる。

具体的には

・不正アクセスが試みられている
・マルウェアがロードされている
・ボットネットが作成されている
・デバイスのソフトウェア エラーの発生
・IoT 製品ユーザーまたは開発者が意図したものではない種類のアクションの発生

［考察］

IoT 製品に Cybersecurity State Awareness 機能（IoT 製品のコンポーネントとそれらが保存および送信するデータに影響を与える/受けるサイバーセキュリティ インシデントの検出をサポート）を要求しており、SIP-CPS 第 2 期の課題 C2 の機能に対応していると考えられる。

(2) IoT 製品の非技術的サポート機能

- Documentation（ライフサイクル記録）

IoT 製品の開発者は、IoT 製品とその製品コンポーネントのサイバーセキュリティに関連する情報を、顧客の購入前、および製品の開発とその後のライフサイクル全体で作成、収集、保存する。

・ 開発ライフサイクル全体を通じて、IoT 製品の開発者は、IoT 製品とその製品コンポーネントのサイバーセキュリティに関連する情報を作成または収集し、保存する。これには、以下が含まれる。

a. 開発プロセス中に行われた仮定、および IoT 製品に関連するその他の期待。
   i. 想定される顧客とユースケース。
   ii. IoT 製品とその製品コンポーネントの場所のセキュリティを含む物理的な使用（例: デバイスにオフ スイッチがある家の中で使用するカメラと、オフのスイッチがない家の外で使用するセキュリティ カメラ デバイスのスイッチを入れる）、および特性。
   iii. ネットワーク アクセスと要件（帯域幅要件など）。
   iv. IoT 製品によって作成および処理されるデータ。
   v. 予想されるデータの入力と出力（エラー コード、頻度、タイプ/形式、許容値の範囲などを含む）。
   vi. IoT 製品の開発者が想定する IoT 製品のサイバーセキュリティ要件。
   vii. IoT 製品および関連するサポート活動が準拠するすべての法規制。
   viii. IoT 製品に関連する予想される寿命と予想されるサイバーセキュリティ コスト（メンテナンスの価格など）、およびサポート期間と期間。
b. IoT 製品の一部である IoT デバイスを含むがこれに限定されない全 IoT コンポーネント。
c. どのベースライン製品基準が IoT 製品コンポーネントによって満たされていないか、およびその理由（例: リスク評価に基づいてその機能が必要ないなど）を含め、製品コンポーネント全体で IoT 製品によってベースライン製品基準がどのように満たされているか。
d. IoT 製品に関連する製品設計およびサポートに関する考慮事項。下記に例:
   i. IoT 製品を作成するために使用される（つまり、各製品コンポーネントを作成するために使用される）すべてのソース（オープン ソース、適切なサードパー

ティ、社内で開発されたものなど）からのすべてのハードウェアおよびソフトウェア コンポーネント。

ii. IoT 製品の開発と運用に使用される IoT プラットフォーム、および関連ドキュメントを含むその製品コンポーネント。

iii. IoT 製品とその製品コンポーネントを作成するために実装されたソフトウェアおよびハードウェア要素の保護（例: セキュア ブート、ハードウェア ルート オブ トラスト、セキュア エンクレーブ)。

iv. IoT 製品に関連する既知のリスクと、既知の潜在的な誤用に対する考慮。

v. 安全なソフトウェア開発とサプライ チェーン プラクティスの使用。

vi. サイバーセキュリティの認定、認定、評価結果 - 関連する慣行。

vii. 顧客による IoT 製品のインストールと保守の容易さ（つまり、製品の使いやすさ [ISO9241] ）。

e. IoT 製品の保守要件。以下に例。

i. サイバーセキュリティ メンテナンスの期待事項と関連する指示または手順（脆弱性/パッチ管理計画など)。

ii. IoT 製品の開発者が、保守活動を実行できる承認されたサポート パーティ (承認された修理センターなど) を特定する方法。

iii. メンテナンス プロセスのサイバーセキュリティに関する考慮事項 (例: メンテナンス プロセスに関係のない顧客データが、メンテナーからも機密として扱われる方法)。

f. 以下を含む、IoT 製品に関連する安全なシステム ライフサイクル ポリシーとプロセス。

i. IoT 製品とその製品コンポーネントに既知の悪用可能な脆弱性がないことを確認するために、開発中に実行される手順。

ii. IoT 製品とその製品コンポーネントのセキュリティが、サポートされているライフサイクルの間維持されることを保証するために、コンポーネント サプライヤおよびサードパーティ ベンダーと協力するプロセス。

iii. IoT 製品とその製品コンポーネントを引き続き使用する顧客のセキュリティ、プライバシー、または安全性に重大な影響を与える脆弱性の発見など、サポート終了後の考慮事項。

g. IoT 製品に関連する脆弱性管理のポリシーとプロセス。以下を含む。

i. 脆弱性のレポートを受信する方法。

ii. 報告された脆弱性を記録するプロセス。

iii. コンポーネントサプライヤーとサードパーティベンダー間の脆弱性対応活動を調整するプロセスを含む、報告された脆弱性に対応するためのポリシー。

iv. 報告された脆弱性を開示するためのポリシー。

v. 生産終了、サポート終了、非推奨ステータス（製品の使用が推奨されなくなっ

たなど）など、提供されたコンポーネントのステータスの変更について、コンポーネント サプライヤおよびサード パーティ ベンダーから通知を受け取るためのプロセス。または既知の不安。

サイバーセキュリティ ユーティリティ:

IoT 製品とその開発に関する重要な情報（IoT 製品の評価、作成と維持に使用される開発手法など）を生成、キャプチャ、および保存することで、製品の実際のサイバーセキュリティ体制について IoT 製品開発者に知らせることができる。

［考察］

IoT 製品の非技術的サポート機能として、Documentation（ライフサイクル記録：IoT 製品のセキュリティに関するライフサイクル記録）機能を要求しており、SIP-CPS 第 2 期でも技術成果を社会実装し、継続的なセキュリティレベルの向上を図っていく、社会・組織としての運用の仕組みとして重要な視点であり、国レベルでのガイドラインとしての導入などが必要と思われる。

- Information and Query Reception（最新情報収集と質問受付対応の環境）

IoT 製品開発者が、サイバーセキュリティに関連する情報を受け取り、サイバーセキュリティに関連する情報について顧客等からの質問に答える能力。

・ IoT 製品の開発者は、IoT 製品とその製品コンポーネントのサイバーセキュリティに関連する情報を受け取ることができ、IoT 製品とその製品コンポーネントのサイバーセキュリティに関連する顧客やその他からの問い合わせに応答できる。

a. IoT 製品開発者が、IoT 製品エコシステム（例：修理技術者が顧客の代行）内の顧客や他の人からメンテナンスや脆弱性に関する情報（例: バグ報告機能とバグ報奨金プログラム）を受け取る連絡先を特定する能力。

b. IoT 製品開発者が、IoT 製品とそのコンポーネントのサイバーセキュリティについて、顧客や IoT 製品エコシステム内の他のユーザーから質問を受け回答するる能力。

サイバーセキュリティ ユーティリティ:

IoT 製品が顧客によって使用されると、それらの顧客は、時間の経過とともに IoT 製品のサイバーセキュリティを改善するのに役立つ質問や問題の報告を受け取ることがある。

［考察］

IoT 製品の非技術的サポート機能として、Information and Query Reception（最新情報収集と質問受付対応の環境：IoT 製品開発者が、サイバーセキュリティに関連する情報を受け取り、サイバーセキュリティに関連する情報について顧客等からの質問に答える能力）機能を要求しており、SIP-CPS 第 2 期でも技術成果を社会実装し、継続的なセキュリティレベルの向上を図っていく、社会・組織としての運用の仕組みとして重要な視点であり、国レベルでのガイドラインとしての導入などが必要と思われる。

- Information Dissemination（情報発信）

IoT 製品の開発者は、サイバーセキュリティに関連する情報をブロードキャスト (例: 一般に) /配布（例: 顧客や IoT 製品エコシステム内の他のユーザー）する。

・ IoT 製品の開発者は、チャネル（例：パブリック チャネルへの投稿など）を介して多く/すべてのエンティティにブロードキャストし、IoT 製品の一般および顧客に、サポートライフサイクル全体のサイバーセキュリティ関連の情報とイベントについて警告することができる。少なくとも、この情報には以下が含まれるものとする。

a. 更新されたサポート条件（例: 更新の頻度と適用のメカニズム)、およびソフトウェア更新の入手可能性/適用の通知。
b. IoT 製品のサポート期間または機能の終了。
c. メンテナンス作業の必要性。
d. 新しい IoT デバイスの脆弱性、関連する詳細、顧客の緩和アクションの必要性。
e. 侵害の発見通知：顧客が使用する IoT 製品とその製品コンポーネント、関連する詳細、および顧客から必要な緩和措置（ある場合）に関連する侵害。

・ IoT 製品の開発者は、IoT 製品とその製品コンポーネントのサイバーセキュリティに関連する情報を配布して、適切なエコシステム エンティティ（例：一般的な脆弱性追跡機関、認定者と認証機関、サードパーティのサポートと保守組織）にサイバーセキュリティ関連情報の警告。下記に例

a. IoT 製品およびその製品コンポーネントの設計および開発中に取得された該当するドキュメント。
b. サイバーセキュリティと脆弱性のアラート、および脆弱性の解決に関する情報。
c. IoT 製品開発者が使用する情報セキュリティの実践と保護手段の概要。
d. IoT 製品開発者のサイバーセキュリティ関連の実践に対する認定、認定、および/または評価の結果。
e. IoT 製品開発者のビジネス環境のリスク体制に関するリスク評価レポートまたは概要。

サイバーセキュリティ ユーティリティ:

IoT 製品、そのコンポーネント、脅威、緩和策が変化するにつれて、IoT 製品を安全に使用する方法を顧客に知らせる必要がある。

［考察］

IoT 製品の非技術的サポート機能として、Information Dissemination（情報発信：IoT 製品の開発者は、サイバーセキュリティに関連する情報を顧客やユーザーにブロードキャストする。）機能を要求しており、SIP-CPS 第 2 期でも技術成果の社会実装において、IoT 製品のセキュリティに関する情報発信は、継続的なセキュリティレベルの向上を図っていく、社会・組織としての運用の仕組みとして重要な視点であり、国レベルでのガイドラインとしての導入などが必要と思われる。

- Product and Education Awareness（製品のセキュリティに関する顧客教育）

IoT 製品の開発者は、IoT 製品とその製品コンポーネントに関連するサイバーセキュリティ関連の情報（考慮事項、機能など）について、IoT 製品のエコシステム内の顧客やその他の人々の意識を高め、教育する。

・ IoT 製品開発者は、IoT 製品とその製品コンポーネントのサイバーセキュリティに関連する情報について、顧客を対象とした意識を高め、教育を提供する。以下が含まれる。

a. 少なくとも以下を含む、IoT 製品のサイバーセキュリティ機能の存在と使用:

i. 構成設定を変更する方法と、設定の変更によるサイバーセキュリティへの影響（ある場合）。

ii. アクセス制御機能を構成および使用する方法（パスワードの設定と変更など）。

iii. ソフトウェア アップデートの適用方法と、ソフトウェア アップデート機能の使用方法についてお客様に必要な指示。

iv. IoT 製品のデータの作成、更新、削除など、デバイスデータの管理方法。

b. IoT 製品の開発者からのセキュリティ サポート（ソフトウェアの更新やパッチの配信など）の期間後も含め、IoT 製品とその製品コンポーネントをその有効期間中に維持する方法。

c. IoT 製品とその製品コンポーネントを安全に再プロビジョニングまたは廃棄する方法。

d. 顧客が使用できる IoT 製品またはその製品コンポーネントで利用できる脆弱性管理オプション （構成およびパッチ管理、マルウェア対策など）。

e. 顧客が IoT 製品のセキュリティに関する情報に基づいた購入決定を行うために使用できる追加情報（たとえば、ソフトウェアのアップグレードやパッチによる製品サポートの期間と範囲）。

サイバーセキュリティ ユーティリティ:

デバイスを安全に使用して、顧客と消費者向け IoT 製品市場にとって最高のサイバーセキュリティの結果をもたらす方法について、顧客に通知する必要がある。

［考察］

IoT 製品の非技術的サポート機能として、Product and Education Awareness（製品のセキュリティに関する顧客教育：IoT 製品の開発者は、IoT 製品とその製品コンポーネントに関連するサイバーセキュリティ関連の考慮事項、機能など について、IoT 製品のエコシステム内の顧客やその他の人々の意識を高め、教育する。）機能を要求しており、IoT 製品のセキュリティに関する顧客教育は、SIP-CPS 第 2 期でも技術成果を社会実装し、継続的なセキュリティレベルの向上を図っていく、社会・組織としての運用の仕組みとして重要な視点であり、国レベルでのガイドラインとしての導入などが必要と思われる。

5.1.2.3 Gaia-X[187]：データ主権の信頼の場の構築を支援する推奨規定

Gaia-X は、IDS を取り巻く環境との連携を規定している。特に、持続性（エコ）、開放性などを規定している。

主な成果には、人間系とデジタル系の連携の枠組みとして、・Trust-Framework-22.04、・Labelling Framework_0、・labelling-criteria-v22.04_Final、・Policy-Rules_Document_v22.04_Final がある。

特に、Labelling Framework_0 では、1 つのラベルで複数のコンプライアンス基準を収集（複数のコンプライアンスを 1 つのラベルに集約）の枠組み、及び、これにより、短時間で、煩雑で困難な検査を行うことなうなど必要なレベルの信頼度を達成できる点が注目される。

Gaia-X を支える価値観には、下記の 7 つが挙げられている。

1. 欧州のデータ保護
2. 開放性、可逆性、透明性
3. 信憑性と信頼
4. デジタル主権と自己決定
5. 自由市場へのアクセスとヨーロッパの価値創
6. モジュール性と相互運用性
7. インフラのフェデレーション（連合）

上記価値観の元、GAIA-X ビジョンへの準拠を保証する技術ガイドラインには、下記が謳われている。

セキュリティ by デザイン
プライバシーby デザイン
フェデレーション/配布/分散化の実現
使いやすさとシンプルさ
機械加工性
セマンティック表現
⇒ エコシステムアーキテクチャ
GAIA-X データエコシステム
GAIA-X インフラエコシステム
GAIA-X フェデレーションエコシステム

主な成果の・Trust-Framework-22.04、・Labelling Framework_0、 ・labelling-criteria-v22.04_Final、・Policy-Rules_Document_v22.04_Final について概要を以下に示す。

(1) Gaia-X-Trust-Framework-22.04[188]

Gaia-X がデジタル プラットフォームで高いレベルの信頼を確保するためには、信頼を理解し

187 <https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html>
188 <https://gaia-x.eu/wp-content/uploads/2022/05/Gaia-X-Trust-Framework-22.04.pdf>

やすく、採用された原則にする必要がある。

このため、Gaia-X は Trust Framework (以前は Gaia-X コンプライアンス) と、エコシステムのデータ保護、透明性、セキュリティ、移植性、柔軟性、主権とヨーロッパの管理を保護する Labeling Framework を開発した。

Trust Framework は、Gaia-X エコシステムの一部となる最低限のベースラインを定義する一連のルールで、ユーザーが選択を完全に制御できるようにしながら、個々のエコシステム全体で共通のガバナンスと基本レベルの相互運用性を保証する。

具体的な、ルールの概要は以下である。

1. Gaia-X Trust Framework

1.1 Trust Framework scope

これらのルールは全 Gaia-X 自己記述ファイルに適用され、全エンティティの自己記述ファイルがある。Gaia-X アーキテクチャ ドキュメントで説明されている Gaia-X 概念モデルの一部として定義されている。このリストは主に次のもので構成されている。

・コンシューマ、フェデレータ、プロバイダの参加者

・サービスの提供

・リソース

1.2 Gaia-X Self-Description

Gaia-X 自己記述ファイル： 形式は W3C Verifiable Credentials Data Model に準拠機械可読テキストファイル、コンテンツの改ざんを防止する暗号署名付きファイル、リンクデータを使用した属性記述

1.3 Gaia-X Trust Framework

4 種のルール： シリアル化の形式と構文、暗号署名の検証、鍵ペアに関連付けられた ID の検証、属性値の一貫性、属性の信憑性検証

2. Trust anchors

コンプライアンスのために、 Trust anchors は、要求に署名するための証明書を管理する責任を負う Gaia-X 承認エンティティである。

Gaia-X Trust Framework に準拠するには、クレームの署名に使用されるすべてのキーペアが、証明書チェーンに少なくとも 1 つのトラスト アンカーを持っている必要がある。

有効なトラスト アンカーのリストはいつでも Gaia-X レジスタに保存されている。

2.1 List of defined trust anchors

State: トラスト サービス プロバイダ (TSP) は、州によって検証された ID 発行者である必要がある。参加者は、legalAddress.country が EEA 内にある場合、TSP は eiDAS に準拠している必要がある。 2022 年第 1 四半期末までは、オンボーディングと採用を容易にするために、DV SSL も使用できる。 Gaia-X アソシエーションは、Gaia-X アソシエーション メンバーの有効な TSP でもある。

eiDAS:　eIDAS 規則 (EU) No910/2014 で定義されている電子署名の認定証明書の発行者

DV SSL:　Domain Validated (DV) Secure Sockets Layer (SSL) ：証明書発行者。一時的に有効なトラスト サービス プロバイダと見なされる。

Gaia-X 2022Q1 以降に定義予定。

EDPB CoC:　EDBP によって承認された行動規範に認定された監視機関のリスト

gleif:　登録された LEI 発行者のリスト。

3. Participant

Participant は、識別され、オンボーディングされ、Gaia-X の自己記述を持つ法人または自然人。 それ以外は禁止している。

アーキテクチャ ドキュメントは、参加者が Gaia-X エコシステム内で持つことができる 3 つの役割 (プロバイダ、コンシューマ、およびフェデレータ) を定義している。

これらはまだ Trust Framework の一部ではなく、将来のリリースで定義される予定となっている。

［考察］

Gaia-X-Trust-Framework が目指しているように、サプライチェーンでは、新たな取引相手を公開情報から選ぶ機能が必要と思われる。その際、公開情報に対するセキュリティの確保に加え、信頼性、公平性なども重要な要件となってくる

SIP-CPS 第 2 期でも、課題 B においては信用できる新たな取引相手をセキュアに見つられる機構について、目指すべき機能の 1 つの候補として、検討が必要と思われる。

(2) Gaia-X Labelling Framework_0[189]

Gaia-X は、デジタル プラットフォームで高いレベルの信頼を提供するため、信頼を理解しやすい原則にする必要がある。このため、Gaia-X は、サービスに特定のラベルを付与するために必要なすべてのテストと検証を自動化する、コンプライアンスとラベル付けの技術フレームワークを開発した。

ラベルは、短時間で、困難な検査を行うことなく、必要なレベルの信頼を達成するための手段で、1 つのラベルで複数のコンプライアンス基準を収集する。

これにより、複数の検証可能な資格情報を暗示する。

ラベルを使用すると、すべての基準を簡単にグループ化し、コンプライアンスとラベル付けのフレームワークの背後にある検証の複雑さを隠すことができる。

例えば、市場は、特定のエンティティによって定義された Gaia-X ラベルを検索して、特定の規制市場で「安全」、「安全」、または「信頼できる」が何を意味するのかを技術的に特定する。

これにより、信頼の根拠が内であるかの意味を気にすることなく、信頼できる構成要素（ラベルを持つ）を選ぶことができる。

これにより、生成されるラベル所有者と発行者の Gaia-X ラベルエコシステムは、規範、規制、

189 <https://gaia-x.eu/wp-content/uploads/files/2021-11/Gaia-X%20Labelling%20Framework_0.pdf>

および複雑なコンプライアンス規則を詳細に検討する必要なく、特定のニーズに暗黙的に準拠するサービスを探し、見つけ、使用するための簡単で革新的な方法になりる。

1.The key principles

Transparency: 透明性: サービスの特性を検査して信頼を得る

Sovereignty:主権: サービスの制御能力、その振る舞いの所有権を獲得する

Interoperability: 相互運用性: プロバイダやサービスを自由に選択できるようにする

Compliance and Labels

・Gaia-X ラベル：「ビジネスや規制上の決定をサポートするには、個別に不十分な自己記述型の属性」

・Gaia-X Compliance ： 「ファイル形式と構文、暗号化署名の検証、属性値の一貫性、および属性値の検証に関して、自己記述型の互換性の最小レベルを達成するために、一連の自動的に適用可能なルールを調べて検証するプロセス」

2.The value of labels

EXPRESS VALUE TO THE BUSINESS ：ラベルは Gaia-X サービスによって提供される価値を表現

BRING EXPLANATION AND TRANSPARENCY ：ラベルは本質的な機能を透明にする

ENABLE TRUSTED DECISIONS ：ラベルは、顧客とプロバイダ間の契約条件を強化し、採用を促進に役立

COMPETITIVENESS：ラベルは可視性と独自性を促進し、市場競争を促進

BUILD MOMENTUM：ラベルは意識を高め、プレイヤーの Gaia-X への参加を促進する

3.Labelling principles

NO PROVIDER-WIDE SCOPE

-Gaia-X ラベルは、サービス プロバイダや他のエンティティ、資産ではなく、特定のサービス提供に対して発行

NO PROVIDER CONTROL

- Gaia-X サービス プロバイダは、ラベル自体を変更または管理できない

FEDERATION OF VERIFICATION

-Gaia-X ラベルは、分散型コンセンサスによって発行・検証される。Gaia-X は基礎となるサービス属性の既存認証を再利用するため、既存の認証済みサービスの Gaia-X ラベル付けを採用するコストと複雑さを軽減する。

ONE SHARED COMPLIANCE FRAMEWORK

- Gaia-X アソシエーションは、コンプライアンスおよびラベル付けフレームワーク定義の単一の機関

COMPOSABILITY

- Gaia-X ラベルは、構成可能なサービス属性の論理グループ

SCALABILITY

- 新しい Gaia-X ラベルは、国やドメイン固有の要件に対応する拡張プロファイルを

使用して、新しいニーズに合わせて作成できる。 Gaia-X アソシエーションの理事会は、一貫性とラベルの影響を保護するために、Gaia-X が保持するラベルを承認する唯一の機関

4.Label Owners & Issuers

Label Owners

- ビジネスのために特定のラベルを定義することを決定するエンティティ。例えば、サービス プロバイダ、サービス ユーザー、政府機関、標準化機関、業界団体、業界団体など。Gaia-X ラベル定義は、その潜在的な使用と利益に基づいて行われる。例えば、銀行協会は、銀行に固有のラベルを定義し、銀行の関連会社が採用するすべてのクラウドが特定の要件を満たすことができるようにすることができる

Label Issuers

-ラベルを実装および発行するために Gaia-X アソシエーションによって定義されたエンティティ。ラベルの実装は、すべてのラベル要件を検証可能なクレデンシャルに分解することで構成される。検証可能なクレデンシャルは、コンプライアンスとラベリングのフレームワークでエンコードされるため、自動的に検証可能。ラベルの発行者は、Gaia-X または AISBL によって検証および承認された別の発行者。

5.Gaia-X Basic Labels

Label Level 1

- ビジネスのために特定のラベルを定義することを決定するエンティティ。例えば、サービス プロバイダ、サービス ユーザー、政府機関、標準化機関、業界団体、業界団体など。Gaia-X ラベル定義は、その潜在的な使用と利益に基づいて行われる。例えば、銀行協会は、銀行に固有のラベルを定義し、銀行の関連会社が採用するすべてのクラウドが特定の要件を満たすことができるようにすることができる

Label Level 2

- ラベル レベル 2 は、レベル 1 の基本要件を拡張し、より高いレベルのセキュリティを反映。適用される法的規則と潜在的な依存関係の透明性。ヨーロッパのサービス拠点のオプションを消費者に提供する必要がある。サイバーセキュリティに関しては、ENISA European Cybersecurity Scheme - Substantial Level を満たすことが最低限の要件。

Label Level 3

- データ保護、セキュリティ、透明性、移植性、柔軟性、およびヨーロッパの管理に関する最高水準。レベル 1/2 を拡張し、ヨーロッパ以外のアクセスに対する耐性と、ベンダー ロックインに対する強力な制御を保証する基準を備える。ヨーロッパのサービス拠点は必須。サイバーセキュリティの最小要件は、ENISA の European Cybersecurity Scheme - High Level を満たすこと。

［考察］

Gaia-X Labelling Framework では、新たな取引相手を公開情報から選ぶため、サービスに、セキュアで信頼性高く、公平性を保ってラベルを付与し、要件補償のテストと検証を自動化

できるラベル付け技術のフレームワークを開発している。サプライチェーンでは、新たな取引相手を公開情報から選ぶ機能が必要と思われる。その際、公開情報に対するセキュリティの確保に加え、信頼性、公平性なども重要な要件となってくる。

SIP-CPS 第 2 期でも、課題 B においては信用できる新たな取引相手をセキュアに見つられる機構について、目指すべき機能の 1 つの候補として、検討が必要と思われる。

(3) Gaia-X-labelling-criteria[190]

Gaia-X アソシエーションがデジタルプラットフォームで高いレベルの信頼を確保するために、信頼を理解しやすく、採用された原則にする必要がある。 このため、Gaia-X は Trust Framework (以前は Gaia-X コンプライアンス) と、エコシステムのデータ保護、透明性、セキュリティ、移植性、柔軟性、主権とヨーロッパの管理を保護する Labeling Framework を開発した。

Trust Framework は、Gaia-X エコシステムの一部となる最低限のベースラインを定義する一連のルール。主要なルールは、ユーザーが選択を完全に制御しながら、個々のエコシステム全体で共通のガバナンスと基本レベルの相互運用性を保証する。

1.Design Principles（設計思想）

Gaia-X エコシステム間の一貫性

スケーラビリティと拡張性

構成可能性とモジュール性

規格、自己評価、および適合性評価機関 (CAB)

検証の連合（ederation of Verification）

2.Contractual governance

基準 1: プロバイダは、法的拘束力のある行為を確立する能力を提供するものとする。この法的拘束力のある行為は文書化されなければならない

基準 2: プロバイダは、法的拘束力のある各行為が EU/EEA/加盟国の法律に準拠するオプションを有するものとする

基準 3~4:（省略）

3.Transparency

基準 5: プロバイダは、サービスの中断と事業継続 (サービス レベル アグリーメントなどによる)、プロバイダの倒産、またはプロバイダが法律上存続しなくなる可能性があるその他の理由に関する特定の条項があることを確認するものとする。

基準 6: プロバイダは、当事者がサービスおよびその中のデータを使用する権利を管理する条項があることを確認するものとする

基準 7～18:（省略）

4.Data Protection

基準 19: プロバイダは、EU または EU/EEA/加盟国の法律に基づいて、特に GDPR 要件に対処する契約を確立する機能を提供するものとする。

---

190 <https://gaia-x.eu/wp-content/uploads/2022/05/Gaia-X-labelling-criteria-v22.04_Final.pdfi/>

基準 20: プロバイダは、各当事者の役割と責任を定義するものとする

基準 21～31

5.Security

基準 32: 情報セキュリティの組織: 組織内の情報セキュリティ フレームワークを計画、実装、維持、および継続的に改善する

基準 33: 情報セキュリティ ポリシー: グローバルな情報セキュリティ ポリシーを提供し、セキュリティ要件に関するポリシーと手順に導き、ビジネス要件をサポートする

基準 34～51

6.Portability

基準 52: プロバイダは、データを受信するプロバイダによって要求または要求された場合に、プロバイダの切り替えと、一般的に使用される構造化された機械可読形式 (オープン スタンダード形式を含む) でのデータの移植を容易にするための慣行を実装するものとする。

基準 53: プロバイダは、ユーザーが別のプロバイダへの切り替えを希望する場合に適用されるデータ ポータビリティ、技術的要件、時間枠、および料金のプロセスに関する十分に詳細で明確かつ透明な情報を含む、契約前の情報が存在することを保証するものとする。データを独自の IT システムに戻す

7.European Control

基準 54: ラベル レベル 2 の場合、プロバイダは、すべてのデータが EU/EEA のみで処理および保存されるというオプションを提供するものとする。

基準 55: ラベル レベル 3 の場合、プロバイダはすべてのデータを EU/EEA 内でのみ処理および保存する必要がある。

基準 56～61

［考察］

Gaia-X-labelling-criteria では、Gaia-X アソシエーション（集団）がデジタルプラットフォームで高いレベルの信頼を確保するために、信頼を理解し易い原則を Labeling Framework として示している。

SIP-CPS 第 2 期でも、課題 B においては相手の信頼の度合いをサイバー空間でも容易に理解し易い機構について、目指すべき機能の 1 つの候補として、検討が必要と思われる。

(4) Gaia-X_Policy-Rules_Document[191]

Gaia-X のポリシー ルールは、Gaia-X エコシステムの付加価値と原則を保護する高レベルの目標を定義する。

検証を可能にするために、高レベルの目的は、適切な基準カタログの具体的な要件によって支えられている。

これは、Gaia-X ラベルおよび Trust Framework Document でさらに指定されている。

[191] <https://gaia-x.eu/wp-content/uploads/2022/05/Gaia-X_Policy-Rules_Document_v22.04_Final.pdf>

ポリシールールの意図は、オープン性、透明性、データ保護、セキュリティ、および移植性などの価値など、Gaia-X のヨーロッパの値を示すための明確な制御を特定することである。

Gaia-XFrameworkを介して提供される各サービスは､次のすべての目的に準拠するものとする。

一般に、適用される EU/EEA 法 (データ保護やセキュリティなどの分野など) を完全に順守することが前提条件であるため、以下のポリシーや規則を放棄したり、影響を受けたりすることはない。

次の構成で Cloud Service Provider に対するルールが具体的に示されている。

1. Contractual Framework
2. Contractual governance
3. Transparency
4. Data Protection
5. Security

［考察］

Gaia-X_Policy-Rules では、ポリシールールの意図として、オープン性、透明性、データ保護、セキュリティ、および移植性などの価値など、Gaia-X のヨーロッパの値を示すための明確な制御ルールを示すことである。

汎用的なルールと国・地域の思想に基づくルールが含まれてれいる、

SIP-CPS 第 2 期においては、政治的なルールは対象外と思われるため本機能は対象外と考える。

5.1.2.4 IDS コンポーネント[192]

IDSA（International Data Space Association）[193] は、主に産業間のデータを安全に流通、利用する仕組みを検討している。そこでは、IDS のデータ主権を守り、セキュアで公平な、データ流通環境を支える ISD コンポーネントの開発が進んでいる。

One2One でのデータ主権でセキュアな情報流通の機能の仕組みの IDS trust Connector に加え、分散型システムの公開データ ソースとサービスを検索できる中央ディレクトリが必要不可欠である。概念図を、図 5 に示す。

現在、IDS の枠組みで開発が進んでいるセンター側のコンポーネントを紹介する。

① IDS Metadata Broker[194]

IDS Metadata Broker は、 データ マーケットプレイス （技術的な用語ではメタデータ ディレクトリ）であり、データ ソースとその使用条件を公開および表示する。デバイスが自律的に発見できるようにするには、メタデータを機械可読形式での提供が必要となる。

192 <https://internationaldataspaces.org/make/use-cases-overview/>
193 <https://internationaldataspaces.org/we/>
194 <https://international-data-spaces-association.github.io/DataspaceConnector/CommunicationGuide/v6/IdsEcosystem/Broker>

② IDS Vocabulary Provider[195]

IDS Vocabulary Provider は、語彙プロバイダであり、ドメイン知識を語彙とオントロジーの形で提供する。トラフィックやモビリティ データ形式 (DATEX II、NeTEx など) 、 API (SIRI、TRIAS など) に関する必要データの相互運用性が必要となる。

③ IDS Identity Provider [196]

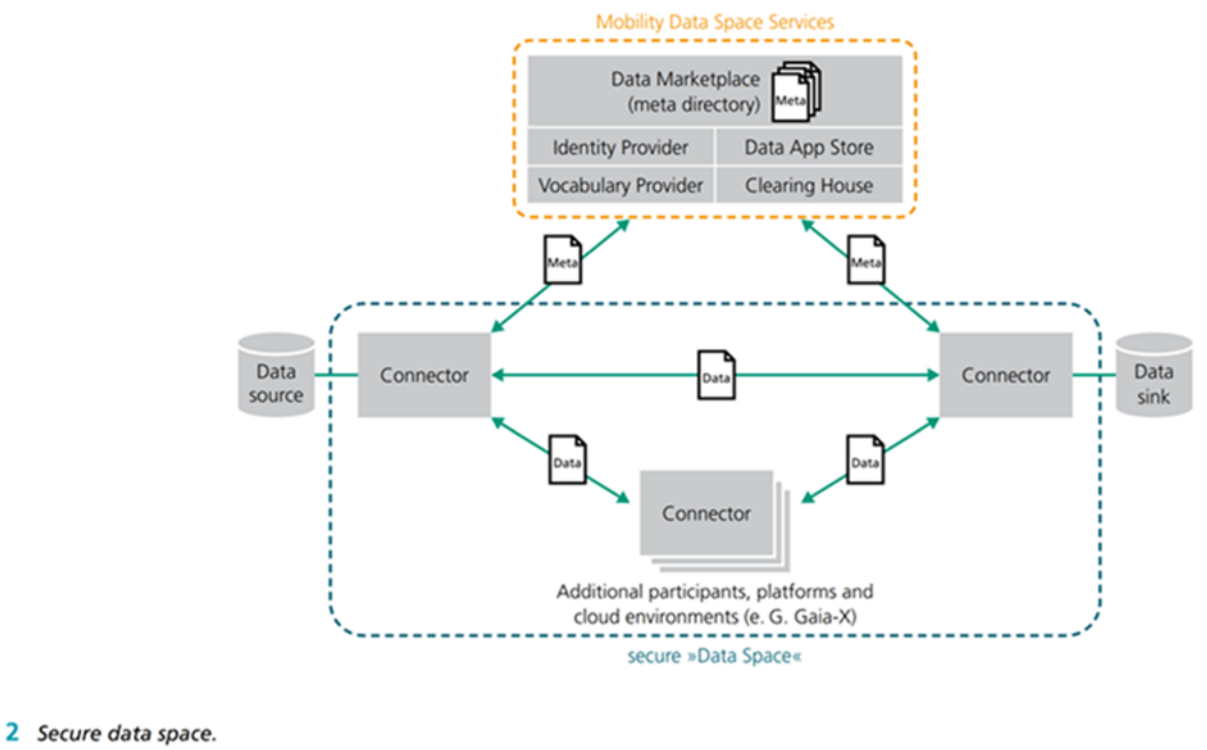
IDS Identity Provider は、ID プロバイダであり、データプロバイダ、ユーザー、データ/データアプリの信頼性を基準に基づき安全な通信を可能にする。

④ IDS App Store[197]

IDS App Store は、 データアプリストアであり、モビリティに関連するデータの処理用に、データアプリの簡単な登録とマーケティングを支援する。

⑤ IDS Clearing House[198]

IDS Clearing House は、クリアリング ハウスであり、システムの中央ロギングコンポーネント、分散システム内トランザクションを記録し、請求や品質分析に利用される。



2 *Secure data space.*

図 5 Secure data Space を支えるコンポーネント[199]

[195] <https://github.com/International-Data-Spaces-Association/IDS-VocabularyProviderr>
[196] <https://international-data-spaces-association.github.io/DataspaceConnector/CommunicationGuide/v6/IdsEcosystem/IdentityProvider>
[197] <https://github.com/International-Data-Spaces-Association/IDS-G/blob/main/Glossary/README.md#app-store>
[198] <https://github.com/Fraunhofer-AISEC/ids-clearing-house-service>
[199] <https://www.fraunhofer.de/en/research/lighthouse-projects-fraunhofer-initiatives/international-data-spaces.html>

(1) IDS Metadata Broker

IDS Metadata Broker は、サプライチェーンの取引相手を選定し、取引相手との IDS のデータマーケットプレイスとして運用される。IDS のオプションコンポーネントであり、Connector で送信のメタデータ公開用システムであるインデックス サービスを提供する。データ ソースのリンクベースの検出を許可し、メタ データを除くデータの実際の転送には、常に関与しない。

IDS には、複数のブローカが存在する場合があり、IDS の種々のプロバイダからの種々の Meta Data Broker 実装が存在する場合がある。Connector オペレータは、どの （メタ） データ パーティションを IDS メタ データ ブローカに送信するかを個別に定義でき、IDS Participant は、IDS エンティティのメタデータをホストするために、サーバーを使用できる。

Connector と IDS Meta Data Broker 間の通信は、メッセージ指向で、メッセージの発行 (インデックス サービスへのメタデータの配信)と、 クエリメッセージ （インデックス サービスからのメタデータのクエリ）を用いる。

永続的なストレージは、適切なストレージバックエンドを使用して実現できるが、インデックスサービスの永続性は事前定義されていない。

［考察］

IDS Metadata Broker が目指しているように、サプライチェーンでは、新たな取引相手を公開情報から選ぶ機能が必要と思われる。その際、公開情報に対するセキュリティの確保に加え、信頼性、公平性なども重要な要件となってくる。

SIP-CPS 第 2 期でも、課題 B において信用できる新たな取引相手をセキュアに見つられる機構について、目指すべき機能の１つの候補として、検討が必要と思われる。

(2) IDS Vocabulary Provider

IDS Vocabulary Provider は、サプライチェーンの間で流通する概念・用語の語彙プロバイダとして運用される。

IDS Vocabulary Provider は、ボキャブラリの文書化と管理を行う。軽量の外部語彙とカタログを使用して、データ パッケージとリソースのコンテンツを指定する。

このシステムは、対応する概念を保存、維持、文書化、再利用するだけでなく、Git ベースのバージョン管理システムを介してクラウドベースの作成、保守、開発も行う。

［考察］

IDS Vocabulary Provider は、比較的公開情報を扱う機能であることから、セキュリティ観点での SIP-CPS 第 2 期への要求条件は少ないと思われる。

(3) IDS Identity Provider [200]

IDS Identity Provider は、Certification Authority (CA) 、Dynamic Attribute Provisioning Service (DAPS) 、 Participant Information System (ParIS) などの ID ごとの ID プロバイダとして運用される。

IDS コネクタは、自身を認証するために、DAPS と呼ばれる中央の IDS コンポーネントからデジタル署名された JSON Web トークン (JWT) を要求する。これらの DAPS トークン (DAT) がなければ、コネクタは IDS に参加できない。

Dataspace Connector は、デフォルトで Fraunhofer AISEC が提供する DAPS と通信する。

なお、リポジトリはオープンソースであり、GitHub で公開されている。

DAT の内容はリスト化され、説明されている。

［考察］

IDS Identity Provider は、サプライチェーンにおいて、識別が必要な各種 ID の信頼性と公開性を保証し、長期にわたって維持管理が必要な機構である。

SIP-CPS2 期においても、課題 B においてサプライチェーンで用いる可能性がある ID についてセキュアに周知させる機構として、目指すべき機能の 1 つの候補として、検討が必要と思われる。

(4) IDS App Store

IDS App Store は、データアプリを配布するための安全なプラットフォームであり、 さまざまな検索オプションを備えている

（例：機能的または非機能的なプロパティ、価格モデル、認定ステータス、コミュニティ評価などによる）。

［考察］

IDS App Store は、比較的公開情報を扱う機能であることから、セキュリティ観点での SIP-CPS 第 2 期への要求条件は少ないと思われる。

(5) IDS Clearing House

IDS Clearing House のサービスは、産業用データスペースのクリアリングハウスであり、クリアリング ハウスのデータは暗号化されて保存され、実質的に不変性を保証する機構である。クリアリング ハウスがデータの不変性を強制する方法は複数ある。

例えば、Logging Service を使用すれば、データベース内の既存のログエントリを更新する方法はない。データベース内のログエントリには、以前のログエントリのハッシュ値が含まれており、すべてのログエントリが連鎖する。以前のログエントリを変更すると、後続のすべてのログエントリを再ハッシュする必要がある。

また、クリアリングハウスのコネクタログ情報は、タイムスタンプと現在のチェーンハッシュ

[200] <https://international-data-spaces-association.github.io/DataspaceConnector/CommunicationGuide/v6/IdsEcosystem/IdentityProvider>

を含む署名付きの領収書をクリアリングハウスから受け取る。任意のコネクタを所有する単一の有効なレシートは、レシートに示されている時間までのデータへの変更を検出するのに十分である。

［考察］

IDS Clearing House の機構は、サプライチェーンの運用中などに不測の事態が発生した場合などに、事実の検証用の情報として必要不可欠な機構である。

SIP-CPS 第 2 期でも、サプライチェーンでの活動を、中立的な立場で分析可能とする機構について、目指すべき機能の 1 つの候補として、検討が必要と思われる。

5.2　国際的な目標水準に盛り込むべき事項

以上のように、前項に示した調査対象の技術、製品、活動の評価項目を、SIP-CPS 第 2 期の研究開発項目の評価項目は、ほぼカバーしていると考えられるが、一部に連携候補としての検討と、技術目標としての必要性も含めた検討が必要と考えられる以下の評価項目がある。

5.2.1 RSA2022 コンテスト入賞製品・企業関連

RSA2022 コンテスト入賞製品・企業の評価項目関連では、下記の 10 種がある。

(1) Araali Network：他のシステムの送受信監視・異常パケットブロック技術
(2) BastionZero ：システム開発時のセキュア環境維持と影響範囲を抑える技術
(3) Cado Security：インシデントレベルのセキュリティ脅威検知・分析技術
(4) Cycode：ソフトウェア開発のライフサイクルでのセキュリティリスク回避技術
(5) Dasera：データガバナンスプラットフォーム技術
(6) Lightspin：ランタイム侵入保護、攻撃因子・攻撃パス・攻撃対象領域分析技術
(7) Neosec：API データセット分析によるセキュリティ検知技術
(8) Sevco Security：他のツールなどの情報も集約して分析を行う技術
(9) Talon Cyber Securit：人間のミスや悪意も対象に分析をする技術
(10) Torq：ドロップ・アンド・ドロップセキュリティ設計技術

この中で、追加候補となりそうな評価項目として、

ⅰ）悪意・ミス検知（(9)Talon Cyber Securit）、
ⅱ）セキュア設計スキルの一般化（(10)Torq）、
ⅲ）ライフサイクルセキュア環境（(4)Cycode、Satori、(5)Dasera）

を抽出した。

［考察］

ⅰ）悪意・ミス検知については、SIP-CPS 第 2 期の研究開発項目 A2 の中に含まれていると考えられるが、内部からの攻撃も明示的な目標とすることが必要かもしれない。
ⅱ）セキュア設計スキルの一般化については、セキュリティ技術者層を厚くする 1 つの手法であり、SIP-CPS 第 2 期の目標ではないが、重要な項目と考える。
ⅲ）ライフサイクルセキュア環境については、サプライチェーンが日々変化していく社会環

境の中、サプライチェーン群のライフサイクルセキュア環境として、SIP-CPS 第 2 期の最終目標に設定されていると考える。

［提案］

目標水準候補として、ⅰ）悪意・ミスの検知、ⅱ）セキュア設計スキルの一般化を提案する。

5.2.2 NIST IR 8425 関連

米国NISTが公開した IoT Coreに対するセキュリティのベースラインの消費者プロファイルは、下記の IoT 製品の機能要件と、非技術的サポート要件を規定している。

(1) IoT 製品の機能要件

- Asset Identification 機能（IoT 製品の一意識別可能性）
- Product Configuration 機能（IoT 製品の構成変更可能性）
- Data Protection 機能（データへの不正なアクセス、開示、および変更から保護）
- Interface Access Control 機能（アクセスを、許可された個人、サービス、および IoT 製品コンポーネントのみに制限）
- Software Update 機能（ IoT 製品コンポーネントのソフトウェアが、IoT 製品コンポーネントごとに適切な安全で構成可能なメカニズムを使用することによってのみ更新）
- Cybersecurity State Awareness 機能（IoT 製品のコンポーネントとそれらが保存および送信するデータに影響を与える/受けるサイバーセキュリティ インシデントの検出をサポート）

(2) IoT 製品の非技術的サポート要件

- Documentation（ライフサイクル記録: IoT 製品のセキュリティに関するライフサイクル記録）
- Information and Query Reception（最新情報収集と質問受付対応の環境：IoT 製品開発者が、サイバーセキュリティに関連する情報を受け取り、サイバーセキュリティに関連する情報について顧客等からの質問に答える能力）
- Information Dissemination（情報発信：IoT 製品の開発者は、サイバーセキュリティに関連する情報を顧客やユーザーにブロードキャストする。）
- Product and Education Awareness（製品のセキュリティに関する顧客教育：IoT 製品の開発者は、IoT 製品とその製品コンポーネントに関連するサイバーセキュリティ関連の考慮事項、機能など について、IoT 製品のエコシステム内の顧客やその他の人々の意識を高め、教育する。）

［考察］

6 つの機能要件は、SIP-CPS 第 2 期の目標とほぼ同じと考える。

これに対し、非技術的サポート要件である、セキュリティに関連するライフサイクル記録、最新情報収集と質問受付対応の環境、情報発信、製品のセキュリティに関する顧客教育は、いずれも、社会実装としてライフサイクルなセキュリティ運用を可能とする大変重要なサポート機能であり、残されたプロジェクト期間の中で、プロジェクト終了後の進め方の枠組みなどの具体化が必要と考える。

［提案］

社会実装に向けては、IoT 製品の非技術的サポート要件への対応については、現 SIP-CPS 第 2 期のプロジェクト内で、プロジェクト終了後の進め方の枠組みなどの具体化を提案する。

5.2.3 Gaia-X ：データ主権の信頼の場の構築を支援する推奨規定関連

Gaia-X では、データ主権の信頼の場の構築を支援する下記の 4 種の規定を推奨している

Gaia-X-Trust-Framework

新たな取引相手を公開情報から選ぶ機能として、公開情報のセキュリティ確保、信頼性、公平性などの要件を規定

Gaia-X Labelling Framework：

新たな取引相手を公開情報から選ぶため、サービスに、セキュアで信頼性高く、公平性を保ってラベルを付与し、要件補償のテストと検証を自動化できるラベル付け技術のフレームワーク

Gaia-X-labelling-criteria

Gaia-X アソシエーション（集団）がデジタルプラットフォームで高いレベルの信頼を確保するために、信頼を理解し易い原則を Labeling Framework

Gaia-X_Policy-Rules

ポリシールールの意図として、オープン性、透明性、データ保護、セキュリティ、および移植性などの価値など、Gaia-X のヨーロッパの価値観を示すための明確な制御ルール

［考察］

いずれの推奨規定も、アソシエーション（集団）として、信頼できる相手を公平でセキュアに選定できる枠組みを構築するためのフレームワークであり、クライテリアであり、ルールとなっている。価値観（ヨーロッパとして合意）まで含めて規定しており、SIP-CPS 第 2 期の枠を超えている内容も含まれている。

全体を通して、システムとしての部分と、人間、集団としての部分を意味のある形で規定しており、重要な示唆を与えていると考える。課題 B に対応する内容が多く含まれていると考える。

［提案］

目標水準候補として、サプライチェーンに関連する集団が人として、SIP-CPS の成果を信じて利用できる観点を提案する。

5.2.4 IDS コンポーネント関連

IDSA が提供している ISD コンポーネントには、データ所有者の主権を担保する IDS Trust Connector（ピアツーピアのセキュア接続を提供）に加え、活動の場を運用するために、下記の 5 種がある。

IDS Metadata Broker

サプライチェーンでは、新たな取引相手を公開情報からセキュリティの確保に加え、信頼性、

公平性など担保して選ぶ機能

IDS Vocabulary Provider

用語を統一し、同様の解釈を提供する機能。比較的公開情報を扱うこととなる

IDS Identity Provider

サプライチェーンにおいて、識別が必要な各種 ID の信頼性と公開性を保証し、長期にわたって維持管理を行う機構

IDS App Store

セキュアで信頼できるアプリケーションを紹介・提供する機能。比較的公開情報を扱う

IDS Clearing House

サプライチェーンの運用中などに不測の事態が発生した場合などに、事実の検証用の情報として必要不可欠な機構。中立的な立場でのクリアリングが必要

［考察］

SIP-CPS でも、システムに依存する部分を増やしていくためには、サプライチェーンの場をセキュアに保ちつつ、信頼性高く公平に運用する共通のシステムが必要となってくる。

そのため、基準を満たす利用者には、信頼性を担保し、しかも偏っていない（公平な）情報をセキュアに提供する公共的なシステムの構築・運用が重要な要件になると考える。

［提案］

目標水準候補としては、サプライチェーンの場を信頼性高く、公平でセキュアに運営する観点を提案する。

5.2.5 まとめ

SIP-CSP の目標に関係し、世界で先端と考えられる研究開発内容と製品の調査から、SIP-CPS 第 2 期との比較対象となる技術を抽出し分析を行った。これらを SIP-CPS 第 2 期が展開する研究開発目標と対比することにより、SIP-CPS 第 2 期への追加が必要と考えられる評価項目と、目標水準設定の参考となる技術を選択した。

追加が必要と考えられる評価項目として、下記を提案する。

① 悪意・ミスの検知（サプライチェーン内の内部犯行に対する対応）
② セキュア設計スキルの一般化（どのセキュリティレベルの技術者がセキュア設計が可能か）
③ 社会への普及のための体制（セキュリティ環境普及体制の自律性、持続可能性評価）
④ 利用者が感じる信頼度（システムが提供する信頼性と人間が感じる信頼性のギャップ軽減）
⑤ 公共性のシステム化度（参加者（集団）が公平と感じるシステム化のカバー範囲）

目標水準については、選定した各技術の実現レベルを現在のトップレベルと位置付け、個々の研究開発項目と比較して設定を行う必要があると考える。NIST IoT Program の発行文書と SIP-CPS の成果の対応関係が本プロジェクトの研究開発担当メンバーにより成果普及・実証評価 WG の活動として示されている。これに加えて、SIP-CPS に追加が必要と考えられる評価項目と SIP-CPS の成果との対応関係を、提示した技術の実現レベルを参照して分析することにより新たな国際的な目標水準を設定する活動とすることを提案する。

6　WG の運営業務

6.1　海外動向調査 WG 活動状況

本調査業務開始にあたり、PD、NEDO と調整の上、海外動向調査 WG の調査方針、活動内容、報告形態等を定めた調査活動計画を策定した。計画実施に当たっては、特に以下の事項に留意した。

- 関係者への速やかな情報配信

海外の最新情報を速やかに SIP-CPS 関係者に配信することを最優先事項とした。配信先として、SIP-CPS 参加企業、団体メンバー、本プロジェクトの他の WG のメンバー、内閣府、NEDO、省庁関連機関の関係者を選定し、メーリングリストを作成して、配信を行った。

- WG 開催方法

本プロジェクトの複数の WG の活動を考慮して、メーリングリストによる最新情報の随時配信に加えて 2022 年 9 月の中間報告と 2022 年 12 月の最終報告の 2 回の報告書の配信を行った。

6.2　中間報告

前半活動（6 月～9 月）までの海外動向情報を取りまとめ、9 月 16 日に中間報告書を配信した。

6.3　最終報告会

12 月 14 日にリモート会議による最終報告会を実施した。最新の IoT セキュリティとサプライチェーンセキュリティ関連の海外動向について、米国や欧州の動向の調査協力者が米国よりリモート会議に出席して説明を行い、その後活発な Q&A、意見交換が行われた。

最終報告会の参加者は計 43 名であった。

なお、会議で報告した報告書の最終版は 12 月 19 日に配信を行った。

6.4　海外動向情報配信実績

本プロジェクトに関係する海外動向情報として、メーリングリストを用いて本プロジェクトの関係者へ随時情報として配信した結果を**表 4** に示す。

表 4 海外動向情報配信実績

情報共有件数		政府機関関連情報	セキュリティ関連情報／その他	セミナー／シンポジウムレポート
米国	欧州			
80	21	52	40	8

結び

SIP-CSP の研究開発成果の海外展開を達成するために、海外における IoT セキュリティ、サプライチェーンセキュリティに関する制度やガイドライン等の標準化動向、技術政策の在り方や業界の最新技術動向を米国と欧州を中心に調査・分析した。また、これに加え海外の IoT セキュリティ技術とサプライチェーンセキュリティ技術に関連する技術開発プロジェクト等と最新の製品を対象に、それらの技術内容を調査した。

ほぼ 6 か月にわたる本調査期間に、今後に影響を与えうる重要な事象が数々発生したことに気付かされる。Labeling を含む IoT 類の提供、販売、保守に直接関係しうる法規制の厳格化、ソフトウェアをはじめとする Supply Chain 分野、あるいは欧州での今後の情報セキュリティ分野に大きな影響が見込まれる IoT、Supply Chain を含む IT 全般に影響する法制度の進捗、並びに継続して検知され続ける脆弱性や実際に発生したインシデント類は、さまざまな方向から SIP-CPS の諸課題に様々な影響が考えられ、SIP-CPS が満了した後も、IoT に関わるインシデント対応、脆弱性対応への今後の影響が考えられる。一方で、NIST SP1800-63 に見られるように、SIP-CPS が今まで取り組んだ研究開発内容が活かされうる動きが米国で観察されることは、SIP-CPS の考え、計画がこれから世界的に評価されうる心強い可能性を示している。

本プロジェクトの研究開発の国際連携を行ない、研究開発成果の海外展開を達成するための活動として、米国の NIST、および IoT Program に対するアプローチの方法を提案した。この実現のためには NIST IoT Program を含め海外から発信される情報を継続して把握する体制が求められる。また、欧州について、欧州の現地法人を通じた ENISA、ETSI の CPS 関連活動への参加と、政府が行っている欧州委員会との ICT 国際連携の枠組みを活用して、本プロジェクトの活動成果を伝える活動を行うことを提案した。

さらに、海外における技術開発プロジェクトと製品の調査から、本プロジェクトに対し追加が必要と考えられる評価項目 5 点を提案し、目標水準の設定のための参考となる技術を選定した。

付表 IoT セキュリティとサプライチェーンセキュリティに関連する情報一覧

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源									要旨	参照先	その他特記事項
			政府・行政機関	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他組織化	その他標準	報道機関	その他			
2022/3/16	Standardisation conference explores EU cybersecurity legislation	標準化会議でEUのサイバーセキュリティ法を調査	1	1								1					2022年3月にENISAは、リスク管理に関して一貫性のある概要を提供し、標準に準拠した実装を実現するために使用できる方法論とツールについて説明することを目的とする「リスク管理標準」を公開しました。 本書は、各EU機関（institutions, bodies, agencies）に対して、リスク管理に関する標準化の手順を導くものです。これらのドメインで起こりうるギャップの概要を示し、関連するEU機関が法律に由来するサイバーセキュリティポリシーをさらに実装するため、これらのギャップを埋めるための活動を開始できることを目指すものです。 さらに、本書は、組織内またはサイバーセキュリティ認証スキームの開発においてリスク管理を実装するためのリスク管理基準および方法論のライブラリとして組織が使用することもできます。 標準準拠には、利害関係者によって指定された技術専門家間の知識の共有、コンセンサスの構築、プロセスを通じた開発および定義が含まれます。 標準の開発と確立に関しては、多種多様なプレーヤーが存在することから、当然、これらのプレーヤーの間には競争がありますが、特に共通の関心がある場合は、多くの実例で協力することもあります。 当該標準の準拠は任意であり、それを適用するための自動的な法的義務は伴いません。ただし、法令は標準に言及している場合があり、標準への準拠を義務付ける場合もあります。 本書では、リスク管理の分野の標準に関して、主要なプレーヤー向けに平易に紹介し、これらのプレーヤーによって公開されたさまざまな資料の主な特徴を紹介しています。	https://www.enisa.europa.eu/news/enisa-news/standardisation-conference-explores-eu-cybersecurity-legislation https://www.enisa.europa.eu/publications/risk-management-standards	
2022/3/16	Risk Management Standards	ENISAが“Risk Management Standards”を出版	1							1							この資料は、リスク管理の側面に対処する公開された標準の一貫した概要を提供し、その後、これらの標準に準拠または実装するために使用できる方法論とツールについて説明することを目的としている。 この資料は、サイバーセキュリティリスクの管理に関連する標準と方法論の利用可能性に関する各EU機関（institutions, bodies, agencies）へのガイダンスを提供し、これらのドメインで起こりうるギャップの概要を示し、関連するEU機関が法律に由来するサイバーセキュリティポリシーをさらに実装するため、これらのギャップを埋めるための活動を開始できるようにする。さらに、この資料は、組織内またはサイバーセキュリティ認証スキームの開発においてリスク管理を実装するためのリスク管理基準および方法論のライブラリとして組織が使用することもできる。 この資料は対象読者がリスク管理プロセスとそれに関連する基準を理解できるように関連分野をカバーする章で構成されている。５章で提供された分析に基づいて、リスク管理標準とリスク管理方法論を区別し、6章で、さまざまな利害関係者グループに対するリスク管理標準の使用に関する一連の推奨事項を提案する。	https://www.enisa.europa.eu/publications/risk-management-standards	サプライチェーンのリスク管理に関連する標準、ツール（MEDUSA、MITIGATE）が記載されている。 本資料は以下の標準化会合（2022/3/15開催）のニュースリリースのリンク先にある。 https://www.enisa.europa.eu/news/enisa-news/standardisation-conference-explores-eu-cybersecurity-legislation
2022/4/7	New SME Guide based on ISO/IEC 27002 standard: Essential controls for SMEs to protect user's privacy and data and ensure GDPR compliance	ISO/IEC 27002規格に基づく新しいSMEガイド：ユーザーのプライバシーとデータを保護し、GDPRに準拠するための中小企業向けの必須管理項目		1								1					サイバー攻撃は増え続けており、データ侵害が増え、サイバーセキュリティの障害が深刻化している。中小企業がデジタル資産を保護するための対策は、より複雑で費用がかかる。この状況に対処するために、DIGITAL SMEは、情報セキュリティ管理に関するSBS SMEガイドを作成し、サイバーセキュリティ標準の実装を通じてSMEが本質的なレベルの保護に到達できるように支援する。 このガイドでは、ISO/IEC 27002標準に示されている114のコントロールのうち、SMEがデジタル資産を適切に保護するために実装する必要のある16の重要なコントロールを示している。 この実装ガイドは、サイバーセキュリティの認識を高めることに加えて、中小企業のデジタル強度を向上させるための継続的な取り組みに貢献することを目的としている。サイバーセキュリティSMEは、このガイドを使用して、ICT以外のSME向けのソリューションを調整し、セキュリティ要件を強化すると同時に、デジタル機能のレベルをアップグレードできる。 SBSは、ISO/IEC 27001標準に基づいた情報セキュリティ管理のSMEガイドも公開している。 2つのガイドを組み合わせることで、SMEが包括的なサイバーセキュリティ要件を実装するのに役立つ。	https://www.digitalsme.eu/new-sme-guide-on-information-security-controls/	79ページからなるガイドライン、サプライヤーに関係したコントロールが示されている。 EU DIGITAL SME alliance:ヨーロッパで最大のICT中小企業ネットワークであり、合計で45,000を超える企業を代表している。 アライアンスは、デジタルSMEをEUの議題の中心に置くために、EU加盟国および近隣諸国からの30の国内および地域SME協会の共同の取り組み。
2022/4/7	ETSI'S WORLD-FIRST STANDARD TO SECURE CONSUMER IOT DEVICES IS EXTENDED TO HOME GATEWAYS	消費者向けIOTデバイスを保護するためのETSIの世界初の標準がホームゲートウェイに拡張		1	1						1						ETSIのCYBER技術委員会は、ETSI TS 103 848と呼ばれるホームゲートウェイ(HG)の新しいサイバーセキュリティ仕様を発表した。この技術仕様は、消費者向けIoTデバイスを保護するための世界初の規格ETSI EN 303 645の規定から適合するホームネットワークとパブリックネットワーク間の物理デバイス、およびこれらのネットワーク間のトラフィックを保護するために作成された。 本仕様は、ETSI EN 303 645規格を適応させ、ユーザーの役割と管理者の役割の区別など、HG製品にとって重要なセキュリティ概念が含まれる。また、ユニバーサルパスワードの使用、ソフトウェアアップデート、機密データの保存、安全な通信、公開された攻撃対象領域、ソフトウェアの整合性、ログデータの収集、HGのインストールとメンテナンスに関する追加の要件もある。 製造業者やその他の利害関係者を支援するために、ETSI CYBER技術委員会は、ETSI EN 303 645の規定を実施するためのガイダンスを提供する技術報告書ETSI TR 103 621も発表した。開発から廃止およびその後の保守終了までのライフサイクル全体にわたって、HGの標準的でテスト可能なセキュリティ対策を規定している。	https://www.etsi.org/newsroom/press-releases/2051-2022-04-etsi-world-first-standard-to-secure-consumer-iot-devices-is-extended-to-home-gateways	ETSI TS 103 848は、欧州規格であるETSI EN 303 645は、さまざまな民生機器、スマート 家電などに世界規模で実装されている。ENの13のサイバーセキュリティ要件とデータ保 護要件は、すべての消費者向けIoTデバイスのベースラインセキュリティ要件を提供する。 新しい仕様は、欧州無線機器指令(RED: Radio equipment directive)第3条(3)の基準のサイバーセキュリティ要件の明確な適合性パスを作成するのに役立つ。

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源								要旨	参照先	その他特記事項
			政府機関・行政	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他組織化	その他標準	報道機関	その他			
2022/4/11	NCSC CAF guidance	NCSC CAF ガイダンス	1	1								1					NCSCは、非常に重要なサービスである防御活動を担当する組織が使用することを目的としたサイバー評価フレームワークCAFのコレクションを開発しました。National Cyber Strategyで述べられているように、CAFは、政府のサイバーセキュリティの向上を目的とした新しいプログラムの一部として導入されています。政府以外では、CAFコレクションが最も有用であると思われる組織を、大きく3つのカテゴリに分類しています。 ・UK Critical National Infrastructure（CNI）内の組織　・ネットワークおよび情報システム（NIS）規制の対象となる組織 ・公安に対するサイバー関連のリスクを管理する組織 CAFコレクション作成の背景 　2015年のウクライナの電力網への攻撃や2017年のWannacryランサムウェア攻撃などの歴史的な出来事、米国のコロニアルパイプラインやイスラエルの水インフラ攻撃などから、国家インフラに対して重要な影響があることが明らかになっています。そこで、英国全体のネットワークおよび情報システムのセキュリティを改善する必要があるとしています。特に、侵害された場合、経済、社会、環境、および個人の生活、福祉に重大な損害を与える可能性のある重要な機能に焦点を当てています。	https://www.ncsc.gov.uk/collection/caf https://www.ncsc.gov.uk/information/cyber-assessment-framework--caf--changelog	この改訂では、原則のフレームワーク、その貢献する成果、およびグッドプラクティスの指標（IGP）の明確さと一貫性を向上させるための言語の改訂に焦点が当てられています。
2022/4/22	MITRE SoT Framework.	MITRE 信頼のシステムフレームワーク			1							1					MITRE Corpは、Supply Chainのリスク問題に関して国と国土安全保障のコミュニティを支援し、国内および国際的な標準化団体と協力して、グローバルなSupply Chain Securityにおけるリスクを軽減してきました。また、国家安全保障システム、サイバーフィジカルシステム、IoTシステムにおけるICTの活用など、情報通信技術(ICT)のサプライチェーンセキュリティに特化したプロジェクトにも深く取り組んできました。 今日、堅牢で回復力のあるサプライチェーン、信頼できるパートナー、グローバルに製造された信頼できるコンポーネントとシステムの必要性にますます焦点が当てられているため、信頼性に影響を与える可能性のあるリスクを理解するための信頼できる道が不可欠です。このパスは、広く理解され、共有され、大規模に使用可能でなければなりません。 これらのサプライチェーンのセキュリティ課題に対処する方法として、MITREは信頼システム(SoT™)フレームワークを開発し、導入しました。このフレームワークは、組織の信頼できるサプライヤー、消耗品、およびサービスプロバイダーの妨げとなる特定の懸念とリスクを定義し、調整し、対処することを目的としています。最も重要なのは、このフレームワークは、サプライヤー、消耗品、サービスプロバイダーを評価するための包括的で一貫性のある反復可能な方法論を提供し、数十年にわたるサプライチェーンセキュリティの経験、関心のある調達コミュニティが直面する複雑な課題に対する深い洞察、および文献や標準におけるこのトピックに関する関連する共有思考の幅広い知識に基づいています。	https://sot.mitre.org/overview/about.html https://sot.mitre.org/framework/system_of_trust.html	
2022/4/22	It'll take a few years for Medtronic to receive U.S.-made chips from the CHIPS	メドトロニックがCHIPS法から米国製チップを受け取るには数年かかるだろう、とCEOは言う													1		メドトロニックの会長兼CEOであるジェフ・マーサが「クロージング・ベル」に加わり、CHIPS法でメドトロニックにとって何が危機に瀕しているのか、メドトロニックが使用するチップはどこから来たのか、そしてCHIPS法の成立によって同社がどれくらい早く影響を受けるのかについて議論します。	https://www.cnbc.com/video/2022/07/26/itll-take-a-few-years-for-medtronic-to-receive-u-s-made-chips-from-the-chips-act-says-ceo.html	
2022/4/25	The Application of Cybersecurity for IoT Capabilities to Real-World Scenarios	IoT機能のためのサイバーセキュリティの現実世界のシナリオへの適用						1									NISTのNational Cybersecurity Center of Excellence(NCCoE)とCybersecurity for the Internet of Things(IoT)プログラムに関するNCCoEからの最近のプロジェクトレポート。関連するIoTデバイスのサイバーセキュリティ機能と非技術的支援機能のマッピングが含まれておりNIST IoT Programが今までに作成した成果類に基づき、具体的なユースケースで実際に適用しうる具体的な三つの事例について下記の通り文書化、公開された ①遠隔医療リモート患者監視エコシステムの保護：医療用機器類(IoT)を対象。 •NIST SP 1800-30A/B/C ②分散型エネルギー資源の確保：IIoT-産業用IoTを対象に、gridを主なユースケースに •NIST SP 1800-32A/B/C ③産業用制御システム環境における情報とシステムの整合性の保護：ICS, IT 及びOTを対象。 •NIST SP 1800-10A/B/C	https://www.nist.gov/blogs/cybersecurity-insights/application-cybersecurity-iot-capabilities-real-world-scenarios	
2022/4/25	Securing Telehealth Remote Patient Monitoring Ecosystem	遠隔医療リモート患者監視エコシステムの保護		1				1									①遠隔医療リモート患者監視エコシステムの保護 従来、患者監視システムは、医療施設や制御された環境に導入されてきました。しかし、遠隔患者モニタリング(RPM)は、モニタリング装置が患者の自宅に配備されているという点で異なる。これらの新機能には、ビデオ会議機能を利用するサードパーティのプラットフォームプロバイダーが関与し、RPMデバイスと組み合わせたクラウドおよびインターネットテクノロジを活用する可能性があります。これらの機能の使用が拡大し続けるにつれて、それらをサポートするインフラストラクチャが患者データの機密性、整合性、および可用性を維持できるようにすることが重要です。	https://www.nccoe.nist.gov/healthcare/securing-telehealth-remote-patient-monitoring-ecosystem	
2022/4/25	Securing Distributed Energy Resources	分散型エネルギー資源の確保	1	1				1									②分散型エネルギー資源の確保 グリッドエッジの産業用モノのインターネット(IIoT)デバイスは急速に増加しており、電力網を変革しています。彼らの接続性、つまり彼らが脆弱になる可能性のある導管は、配電網に対する新たなサイバー脅威です。 配電網事業者は、サイバーフィジカルグリッドエッジデバイスのデジタル通信、データ、および制御を保護する必要があります。NCCoEは、電力部門、メリーランド大学、サイバーセキュリティ技術ベンダーの利害関係者と協力して、キャンパス分散型エネルギー資源(DER)マイクログリッドと相互接続された配電ユーティリティを表す実験室環境を構築しました。この環境を使用して、商業規模および公益事業規模のDERと配電網との間の情報交換を、どのように監視、信頼、および保護できるかを探りました。	https://www.nccoe.nist.gov/energy/securing-distributed-energy-resources	

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源									要旨	参照先	その他特記事項
			政府・行政機関	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他標準化組織	報道機関	その他			
2022/4/25	Protecting Information and System Integrity in Industrial Control System Environments	産業用制御システム環境における情報とシステムの整合性の保護	1	1				1								③産業用制御システム環境における情報とシステムの整合性の保護 競争力を維持するために、メーカーはますます運用技術(OT)システムを情報技術(IT)システムに接続しています。メーカーはテクノロジーを活用して企業全体の接続性を拡大し、リモートアクセスを可能にし、強化された革新的なビジネスプロセスと機能を実現しています。 競争力を維持するために、メーカーは運用技術(OT)システムを情報技術(IT)システムに接続しています。ITネットワークとOTネットワークの統合は、メーカーの生産性の向上と効率の向上に役立っていますが、悪意のあるアクターによってもたらされるサイバーセキュリティの脅威に対してより脆弱になっています。	https://www.nccoe.nist.gov/manufacturing/protecting-information-and-system-integrity-industrial-control-system-environments	
2022/5/5	SP 800-161 Rev. 1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations	SP 800-161 Rev. 1 システムおよび組織のためのサイバーセキュリティ・サプライチェーン・リスク管理の実践	1	1				1								組織は、悪意のある機能を含む可能性のある製品やサービス、偽造品、またはサプライチェーン内の製造および開発慣行が不十分なために脆弱な製品やサービスに関連するリスクを懸念しています。これらのリスクは、企業が取得したテクノロジの開発、統合、展開方法、または製品やサービスのセキュリティ、回復力、信頼性、安全性、完全性、品質を保証するために使用されるプロセス、手順、標準、およびプラクティスに対する可視性の低下と理解に関連しています。 この出版物は、組織のあらゆるレベルでサプライチェーン全体のサイバーセキュリティリスクを特定、評価、および軽減するためのガイダンスを組織に提供します。この出版物は、C-SCRM戦略実施計画、C-SCRMポリシー、C-SCRM計画、および製品およびサービスのリスク評価の開発に関するガイダンスを含む、マルチレベルのC-SCRM固有のアプローチを適用することにより、サイバーセキュリティサプライチェーンリスク管理(C-SCRM)をリスク管理活動に統合しています。	https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final	
2022/5/10	Report for the Assistant to the President for National Security Affairs (APNSA) on Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software	国家安全保障問題担当大統領補佐官（APNSA）向け報告書 消費者向けのサイバーセキュリティの表示。モノのインターネット（IoT）機器とソフトウェアに関する報告書	1	1				1								大統領令（EO）14028：国家のサイバーセキュリティの改善（2021年5月12日）は、様々な連邦機関に行動を割り当てた。連邦政府機関に行動を割り当てました。EOの第4項では、NISTに対して、サイバーセキュリティの開始を含む様々な措置を講じるよう指示しました。ラベリングパイロットプログラムを2つの分野（消費者向けIoT機器、消費者向けソフトウェア開発手法）で開始することを含む、さまざまな措置をとるようNISTに指示しました。 NIST は、民間および公共部門の強力なステークホルダーの参加に基づき、以下を特定しました。IoT 製品および消費者向けソフトウェア開発手法に対するサイバーセキュリティ消費者向けラベリングの推奨基準を特定しました。推奨基準の発表後、NIST は、以下のような試験的な取り組みを開始し、潜在的なラベリングプログラムへの参加に関する寄付を募りました。 2021年5月12日のEOから1年以内に、NISTは、民間セクターおよび関連機関と協議の上、どのような改善が可能かを判断するよう指示された。本書はそのレビューのまとめである。	https://www.nist.gov/system/files/documents/2022/05/24/Cybersecurity%20Labeling%20for%20Consumers%20under%20Executive%20Order%2014028%20on%20Improving%20the%20Nation's%20Cybersecurity%20Report%20(FINAL).pdf	昨年発行のExecutive Order 14028: Improving the Nation's Cybersecurity (以下EO 14028と略記)によりNISTに課せられた指示への回答と位置付けられる。　文書正式名称に見られる通り、内容はIoT並びにSoftwareの消費者向けにわかりやすいLabeling策定に関する要旨報告である。　報告の構成は以下の通り。 ・当該活動の履歴　- IoT並びにSoftware Labeling文書に寄せられたコメント類の統計　- ・IoT Labeling Criteriaについて
2022/5/10	Organisational use of Enterprise Connected Devices	エンタープライズコネクテッドデバイスの組織的使用	1	1								1				エンタープライズコネクテッドデバイスを使用する英国の組織に対するサイバーセキュリティの脅威を評価 このホワイトペーパーは、エンタープライズコネクテッドデバイスに対する現在のサイバーセキュリティの脅威の評価を提供することを目的としています。この情報は、業界および接続されたデバイスを使用するすべての人にとって興味深いものになります。近年、組織によって使用および展開されるデバイスは劇的に変化しています。リモートで柔軟な作業を可能にすることから、効率と生産性の向上まで、これらのデバイスは範囲が広く、多くの場合、接続能力に依存しています。これにより、リスクが高まります。 NCSCはDCMSと協力して、これらのエンタープライズコネクテッドデバイスのランドスケープを評価するプロセスを開始し、この分野のセキュリティを推進するためのフレームワークとしてデバイスセキュリティ原則(ベータ)を開始しました。	https://www.ncsc.gov.uk/report/organisational-use-of-enterprise-connected-devices	当文書は、Laptop computerからプリンタ、センサまで、企業情報ネットワークに接続される多様な端末類を対象としたセキュリティ解説文書だが、あくまで「企業情報ネットワークに接続」を前提としており、一般の消費者よりも知識、責任、ネットワーク並びにサイバーセキュリティに対する責任を有することが想定されている点で、NISTが過去に取り組んできたLabelingの文書と前提が異なることにご注意いただきたい。
2022/5/10	Device Security Guidance	デバイスセキュリティガイダンス	1	1								1				デバイスを安全に選択、構成、および使用する方法に関する組織向けのガイダンス デバイスをセキュリティで保護することは、主にインターネットから発生するさまざまな脅威から組織を保護する上で不可欠な部分です。携帯電話、タブレット、ラップトップ、デスクトップ、さらには他の接続されたデバイスを含むこれらのデバイスをどのように正確に保護する必要がありますか?この問題について考え始めると、いくつかの質問が頭に浮かびます。 ・どのデバイスを購入する必要がありますか? ・これらのデバイスをどのように構成する必要がありますか? ・どのセキュリティソフトウェアをロードする必要がありますか? デバイスをセキュリティで保護するために、NCSC はこれらの質問などに回答しています。当社のデバイスガイドは、デバイスの選択と購入からエンドユーザーに与えるべきアドバイスまで、あらゆる懸念事項をカバーしています。	https://www.ncsc.gov.uk/collection/device-security-guidance	当文書は、各種OS類の具体的な設定などが示される点でConfiguration Guideとしての性格が観察できるが 、Device security principles for manufactures (beta release) に示される11箇条は、むしろNIST IoT Programがここ数年策定してきたNISTIR類と同様、製造業者への期待（あるいは事実上の要件）と考えると、SIP CPS検討の技術目標の一つの事例とも考えられる。

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源									要旨	参照先	その他特記事項
			政府・行政機関	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他標準化組織	報道機関	その他			
2022/5/11	Cybersecurity of 5G networks: EU publishes report on the security of Open RAN	5Gネットワークのサイバーセキュリティ：EUはOpenRANのセキュリティに関するレポートを出版										1				EU加盟国は、OpenRANのサイバーセキュリティに関するレポートを公開した。 この新しいタイプの5Gネットワークアーキテクチャは、今後数年間で、オープンインターフェイスに基づいて5Gネットワークの無線アクセス部分を展開する代替方法となる。 このレポートは、5Gネットワークのサイバーセキュリティに関するEUレベルでの協調作業における主要なステップであり、5Gネットワークのセキュリティの課題に共同で対応し続け、5Gテクノロジーとアーキテクチャの開発に遅れないという強い決意を示している。 5Gおよび次世代のモバイル通信ネットワークによって実現される高度で革新的なアプリケーションを使用するEU市民および企業は、最高のセキュリティ標準の恩恵を受ける必要がある。 5Gサイバーセキュリティに関するEUツールボックスを使用して5Gネットワークのセキュリティを強化するためにEUレベルですでに行われている調整作業のフォローアップとして、EU加盟国はOpenRANのセキュリティへの影響を分析した。 レポートでは以下のOpenRANの新しいリスクと既存のリスクへの影響を示している。 ●OpenRANの機能とインターフェースにおける脅威と脆弱性の拡大 ●オープンRANネットワークの障害管理の複雑さ ●RAN技術仕様開発プロセスの欠陥 ●クラウドサービス/インフラストラクチャプロバイダーへの新規または増加した依存 ●EU 5Gサプライチェーンの持続可能性の低下と非EUプレーヤーへの潜在的な依存： ●Open RANミックスアンドマッチアプローチがネットワークセキュリティとパフォーマンスに与える影響： ●ソース共有による新たなリス	https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2881 https://digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks	
2022/5/12	Research and Innovation Brief - Annual Report on Cybersecurity Research and Innovation Needs and Priorities	研究とイノベーションの概要-サイバーセキュリティの研究とイノベーションのニーズと優先事項に関する年次報告書														デジタル時代における欧州連合(EU)の未来は、個人、企業、組織が課題に対処し、欧州と世界が公衆衛生危機から回復する一方で、将来の課題の解決と機会を得ることを重視して います。このドキュメントは、これらの課題と機会のいくつかについて、将来を見据えた視点を提供します。ENISAが特定した４つのテーマの主な概要は、以下です。 ・セキュアで人間が中心となるHyperconnected Worldでは、将来を目指した学術的な研究　が必要だとされており、全ての物がデータ化されることを強調しています。 ・Intelligent Systemsの時代では、AIがサイバー防御の方法を改良すると同時にサイバー攻撃を指揮するとしています。 ・Computational Securityでは量子技術も視野に入れた次世代への持続可能な暗号、ブロックチェーン技術によるプライバシーの確保、ユーザー制御暗号化によるプライバシーの拡張、ハードウェアによるセキュリティおよびプライバシーを確保する　ためのAIのテーマが示されています。 ・Cyberbiosecurityでは、その緊急性、既知のCyberbiosecurityの課題、ギャップと　それらのマッピング、広く認識されていないバイオ技術への脅威の展望が示されています。 各テーマについて「注目すべき課題とギャップ」と「関連する将来の研究の必要性とプライオリティ」がレポートのTable1に示されています。これらのテーマ間で連携して取り組むことが重要であるとしています。特にIoTによりデジタルエコシステムの構築が進む中、全てのテーマにAIが関わることが強調されています。	https://www.enisa.europa.eu/publications/research-and-innovation-brief	ENISAは、このレポートで概説した課題と研究ニーズに関するより技術的な情報を 今後も、提供する予定です。並行して、 ENISAは利害関係者や研究コミュニティと 引き続き関与し、サイバーセキュリティに関連するこれらのテーマについて議論して いく予定です。
2022/5/12	Notice on the Continuation of the National Emergency with Respect to Securing the Information and Communications Technology and Services Supply Chain	情報通信技術・サービスのサプライチェーンの安全確保に関する国家緊急事態の継続に関するお知らせ	1	1								1				2019年5月15日、大統領は大統領令13873により、国際緊急経済力法（50 U.S.C. 170l et seq）に基づき、特定の情報通信技術およびサービス取引の無制限の取得および使用によって構成される米国の国家安全保障、外交政策および経済に対する異常で並外れた脅威に対処するための国家緊急事態を宣言しました。 外国の敵対者が所有し、支配し、またはその管轄や指示に従う者が設計、開発、製造、または供給する情報通信技術やサービスを米国内で無制限に取得または使用すると、これらの外国の敵対者が情報通信技術やサービスの脆弱性を作り出し利用する能力が増大し、壊滅的な影響を与える可能性があります。 この脅威は、米国の国家安全保障、外交政策、経済に対し、異常で並外れた脅威を与え続けている。 このため、2019年5月15日に宣言された国家非常事態は、2022年5月15日以降も効力を維持しなければならない。 したがって、国家非常事態法（50 U.S.C. 1622(d)）第202(d)項に従い、私は情報通信技術およびサービスのサプライチェーンの確保に関して大統領令13873で宣言された国家非常事態を1年間継続します。 この通知は、連邦官報に掲載され、議会に伝達されるものとする。	https://www.whitehouse.gov/briefing-room/presidential-actions/2022/05/12/notice-on-the-continuation-of-the-national-emergency-with-respect-to-securing-the-information-and-communications-technology-and-services-supply-chain-2/	去る2019年5月15日に前トランプ政権で発行された、Huawei, ZTEなど米国に害をもたらしうる企業製品の情報通信設備への利用を国家緊急事態として禁じたEO13873を当初期限より更に一年延長され、議会に通知された。

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源									要旨	参照先	その他特記事項
			政府・行政機関	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他標準化組織	その他	報道機関	その他			
2022/5/13	Commission welcomes political agreement on new rules on cybersecurity of network and information systems	欧州委員会、ネットワークと情報システムのサイバーセキュリティに関する新ルールに関する政治的合意を歓迎	1	1								1					欧州委員会は、2020年12月に欧州委員会が提案した、EU全域で共通レベルの高いサイバーセキュリティのための措置に関する指令（NIS 2指令）について、本日、欧州議会とEU加盟国の間で政治的合意が成立したことを歓迎する。 ネットワークおよび情報システムのセキュリティに関する既存の規則（NIS指令）は、サイバーセキュリティに関するEU全体の最初の法律であり、多くの加盟国におけるサイバーセキュリティに対する考え方、制度、規制のアプローチに大きな変化をもたらす道筋をつけました。しかし、社会のデジタル化と相互接続が進み、世界レベルでサイバー犯罪が増加しているため、この法律は更新される必要がありました。 このように欧州がサイバー脅威にさらされる機会が増えたことに対応するため、NIS 2指令は、公共電子通信サービス、デジタルサービス、廃棄物処理、重要製品の製造、郵便・宅配サービス、中央・地方行政など、経済・社会にとって重要なより多くの分野の中・大規模企業を対象とするようになりました。また、COVID-19の大流行で生じたセキュリティ上の脅威の高まりを受け、医療機器メーカーを含めるなど、ヘルスケア部門をより広くカバーすることになりました。新規則の対象範囲の拡大は、より多くの事業体や部門にサイバーセキュリティのリスク管理対策を効果的に義務付けることで、中長期的には欧州のサイバーセキュリティのレベルアップに寄与するものと思われます。 NIS 2指令はまた、企業に課されるサイバーセキュリティの要件を強化し、サプライチェーンとサプライヤー関係のセキュリティに対応し、サイバーセキュリティ義務の不履行に対する経営トップの説明責任を導入しています。報告義務を合理化し、国家当局に対するより厳しい監督措置と、より厳格な執行要件を導入し、加盟国間の制裁制度の調和を図るものである。これは、国およびEUレベルでのサイバー危機管理に関する情報共有と協力の強化に役立つだろう。	https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2985	NIS2 Directive, あるいは単にNIS2として知られる、Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) について、2022年5月13日、欧州議会が原則合意に達した。 欧州議会での最終的な立法化の時期、欧州連合加盟国内での国内法制整備など今後の事態の推移や予定は不明だが、少なくとも欧州域内のネットワーク、システムにIoTを含み、かつIoTにとどまらない広範な影響をもたらすことは間違いない。
2022/5/16	Cybersecurity for IoT: The Road We've Traveled, The Road Ahead	IoTのためのサイバーセキュリティ:私たちが歩んできた道、今後の道	1	1				1									NIST Cybersecurity for IoTプログラムは、約3年前の2019年6月にConsiderations for Management of Things(IoT)サイバーセキュリティとプライバシーリスク(NISTIR 8228)を発表しました。それ以来、IoT技術は発展を続け、セクターや市場全体で採用されています。NIST自身の研究は、IoTの内外で、NISTIR 8228の出版以来、進歩しています。これらの開発は、NISTIR 8228の内容とNISTの将来のIoTサイバーセキュリティの優先事項について、新たな見方をする必要があります。 私たちの研究は、さまざまなデバイスタイプ、アーキテクチャ、および構成を考慮し、可能な限り技術に依存しないアプローチを取ろうとしています。同時に、特定の種類のIoTデバイスやシステム、特にハードウェアに制約があるデバイスやシステム(メモリや処理能力の制限、エネルギー供給の制限、接続性の制限など)について、メーカーと顧客の両方にとってサイバーセキュリティの課題について一貫して聞いてきました。これらの制約により、サイバーセキュリティの目標の達成が困難または不可能になる可能性があります。制約のあるデバイスは、多くの場合、常にではありませんが、他の機器とは異なる、おそらく低いリスクに直面する可能性があります。 サイバーセキュリティ for IoT Program は 2022 年 6 月 22 日にイベントを開催し、IoT の展望とチームの次のステップについて他のユーザーと話し合う予定です。	https://www.nist.gov/blogs/cybersecurity-insights/cybersecurity-iot-road-weve-traveled-road-ahead	内容の大部分は、NIST IoT Programの今までの経緯と成果で占められているが、注目すべき点として文末に、来たる2022年6月22日にNIST IoT program主催のオンライン催事の予定が述べられている 。
2022/6/3	NIST analysis on RFI for CSF and SCRM	CSFとSCRMのRFIに関するNISTの分析	1	1				1									2022年2月22日、NISTは「a public Request for Information (RFI),"Evaluating and Improving NIST Cybersecurity Resources:The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management.」という公開情報要求(RFI)を発行しました。 RFIは、NIST Cybersecurity Frameworkの使用に関する情報と、Frameworkの有効性と他のCybersecurity Resourcesとの整合性を改善するための推奨事項を求めました。RFIはまた、NISTの他のサイバーセキュリティの取り組み、特にサプライチェーンのサイバーセキュリティリスクに関連する情報を提供するための提案を求めました。 RFIが発行されたとき、商務副長官のDon Gravesは、次のように述べています。「すべての組織は、産業界、政府、学界のいずれであっても、ビジネスの一環としてサイバーセキュリティリスクを管理する必要があります。それは彼らの回復力と我が国の経済安全保障にとって極めて重要です。支援できるツールは数多くあり、CSFは民間部門のサイバーセキュリティ維持のための主要なフレームワークの1つです。私たちは、民間部門と公共部門の組織が、中小企業を含め、それをさらに有用で広く使用できるようにする手助けをしたいと考えています。」 このドキュメントは、RFI 応答の初期の概要を示しています。NISTは、複数の組織または多数の組織を代表する協会によって共同で提出された多くのコメントを含む、130以上のRFI回答を受け取りその内容を取りまとめました。	https://www.nist.gov/system/files/documents/2022/06/03/NIST-Cybersecurity-RFI-Summary-Analysis-Final.pdf	ドキュメント本文は32ページの文書ですが、通読したところ、SIP-CPSに関連しうる部分は、Theme 6、Theme 7に関する2つのパートと考えられる。特に7.2ではSBOM関連として、部品表（ソフトウェア部品表、SBOMなど）を含む資産管理情報のガイダンスとリソースを改善する必要性について言及している。 また、クラウドサービス用のSaaSBOMを確立する必要があるとの提案も寄せられている。、7.3にてopen-source software security issuesへの取組みが記載されている。
2022/6/14		2022-3月以降の海外動向情報														1	米国・足立氏による2022-3月以降の海外動向情報		
2022/6/16	Russian Botnet Disrupted in International Cyber Operation	国際的なサイバー作戦でロシアのボットネットを破壊										1			1		米国司法省は、ドイツ、オランダ、英国の法執行機関パートナーとともに、世界中の何百万ものコンピュータやその他の電子機器をハッキングしたRSOCKSとして知られるロシアのボットネットのインフラストラクチャを解体しました。 ボットネットは、ハッキングされたインターネットに接続されたデバイスのグループで、所有者の知らないうちにグループとして制御され、通常は悪意のある目的に使用されます。ロシアのサイバー犯罪者によって運営されているRSOCKSボットネットは、世界中で何百万ものハッキングされたデバイスで構成されていました。RSOCKSボットネットは当初、モノのインターネット(IoT)デバイスをターゲットにしていました。IoTデバイスには、産業用制御システム、タイムクロック、ルーター、オーディオ/ビデオストリーミングデバイス、スマートガレージドアオープナーなど、インターネットを介して通信できるため、IPアドレスが割り当てられる幅広いデバイスが含まれます。米国検事のランディ・グロスマンは、検察チーム、FBI、司法省刑事局のコンピュータ犯罪および知的財産セクションが、この事件に関する優れた仕事をしてくれたことに感謝した。「この作戦は、米国および海外でサイバー侵入を行ったロシアを拠点とする非常に洗練されたサイバー犯罪組織を混乱させました」とFBI特別捜査官のステイシー・モイは述べた。「サイバー犯罪プラットフォームとの闘いは、米国におけるサイバーセキュリティと安全性を確保する上で重要な要素です。本日発表する行動は、国際および民間セクターのパートナーと協力して外国の脅威アクターを追求するというFBIの継続的なコミットメントの証です。	司法省関連報道発表： https://www.justice.gov/usao-sdca/pr/russian-botnet-disrupted-international-cyber-operation Reuters報道： https://www.reuters.com/world/us-partners-dismantle-russian-hacking-botnet-justice-dept-says-2022-06-16/	対象がIoT限定ではなく、NIST CSF, Supply Chain, IoTと広範で、SIP_CPSのscope とかなり近い、今後のSIP-CPSと海外機関との国際連携を考える上で、今回のRFI を通じて日本の活動と米国での活動の整合性を検討することも有効と考える。

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源									要旨	参照先	その他特記事項
			政府機関・行政	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他組織	その他標準	報道機関	その他			
2022/6/17	NISTIR 8425 (Draft) Profile of the IoT Core Baseline for Consumer IoT Products	コンシューマIoT製品のIoTコアベースラインのプロファイル	1	1				1									この出版物は、NISTのIoTコアベースラインの消費者プロファイルを文書化し、消費者IoTセクターに一般的に必要とされるサイバーセキュリティ機能(すなわち、家庭用または個人用のIoT製品)を特定する。また、中小企業がIoT製品の購入を検討するための出発点にもなります。消費者プロファイルは、大統領令14028に対するNISTの対応の一環として開発され、当初は消費者向けモノのインターネット(IoT)製品のサイバーセキュリティラベリングの推奨基準に掲載されました。コンシューマー プロファイル機能は、IoT 製品全体に適用されることを意図したサイバーセキュリティの結果として表現されます。このドキュメントでは、推奨されるコンシューマー プロファイルを作成するための基礎と、関連する考慮事項についても説明します。	https://csrc.nist.gov/publications/detail/nistir/8425/draft	2022年初めに発行のCriteriaをNISTIRとして発行する最初のドラフトであり、7月末締め切りでPublic Commentに付されている。
2022/6/17	NISTIR 8425 (Draft)：Profile of the IoT Core Baseline for Consumer IoT Products	NISTIR 8425 (Draft)：消費者向けIoT製品のIoTコアベースラインのプロファイル	1	1				1									NISTは、以下の2つの草案文書をリリースしました。 1）ディスカッションエッセイ「「NISTにおけるIoTサイバーセキュリティの未来のためのアイデア:IoTリスク識別の複雑さ」：この文書では、IoT向けサイバーセキュリティに関するNISTの以前の研究(NISTIR8259など)に基づいて、IoTにおけるリスク識別の基礎を提示し、IoTデバイスのリスクを特定して対処する方法に関する将来を見据えた議論の道筋を示す。 2）NISTIR 8425 (Draft)：消費者向けIoT製品のIoTコアベースラインのプロファイル この出版物は、NISTのIoTコアベースラインの消費者プロファイルを文書化し、消費者IoTセクターに一般的に必要とされるサイバーセキュリティ機能(すなわち、家庭用または個人用のIoT製品)を特定します。また、中小企業がIoT製品の購入を検討するための出発点にもなります。 消費者プロファイルは、大統領令14028に対するNISTの対応の一環として開発され、当初は消費者向けIoT 製品のサイバーセキュリティラベリングの推奨基準に掲載されました。コンシューマー プロファイル機能は、IoT 製品全体に適用されることを意図したサイバーセキュリティの結果として表現されます。 このドキュメントでは、推奨されるコンシューマー プロファイルを作成するための基礎と、関連する考慮事項についても説明します。現在Public Comment受付中であり、締め切りは7月31日となっています。	https://csrc.nist.gov/publications/detail/nistir/8425/draft https://www.nist.gov/system/files/documents/2022/06/21/IoTRiskIdentificationDiscussionPaper.pdf https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8425.ipd.pdf	
2022/6/21	Ideas for the Future of IoT Cybersecurity at NIST: IoT Risk Identification Complexity	ディスカッション・ペーパー：NISTにおけるIoTサイバーセキュリティの将来像に 関するアイデア：IoTリスク識別の複雑さ	1	1				1									IoT のサイバーセキュリティに関する NIST の取り組みは多くの経路を 辿ってきました。NISTIR 8228では、IoT が企業組織の共通のサイバーセキュリティ目標にどのように影響し得るかを探りました。NISTIR 8259は、顧客のサイバーセキュリティのニーズと目標を念頭に置いてIoTデバイスを開発する領域でIoTデバイスの製造業者を指導しています。SP 800-213は、連邦政府機関に対して、IoTデバイスがその情報システムに与える影響を適切に考慮し、緩和するためのプロセスを提供しています。これらの作業を通じて、一貫してフィードバックされたポイントは、IoTの特性がリスク特定にもたらす多くの課題でした。IoTデバイスメーカーからは、IoTの使用と顧客の異質性により、想定されるすべての顧客に対してすべてのリスクを特定し、対処することは本質的に不可能であるとの声が聞かれました。顧客にとって、IoT技術とリスクの複雑さ、およびIoTデバイスと製品のブラックボックス化により、あらゆる種類の顧客（家庭の消費者、企業組織など）が、自社のネットワーク上でこれらの製品を保護するという責任に直面したとき、暗闇の中にいるような状態になります。 このディスカッションペーパーでは、IoTのサイバーセキュリティに関するNISTの先行研究（例：NISTIR 8259）に基づき、IoTにおけるリスク識別の根拠を示し、IoTデバイスのリスクを識別し対処する方法に関する前向きな議論の道筋を示します。	https://www.nist.gov/document/iot-paper-ideas-future-iot-cybersecurity-nist-iot-risk-identification-complexity	ざっと見る限り、リスク予想をこれから検討するようであるが、この文書にも書いてある通り、IoT vendorにも予想できない利用をされたときに対処する方法が本当にあるのか、リスクを予想できるのか、できなかった場合のliabilityをどうするのか、など、多くの質問疑問を呼ぶと思われる。
2022/6/22	CISA Releases Security Advisories Related to OT:ICEFALL (Insecure by Design) Report	CISAがOT:ICEFALL(設計による安全性の低い)レポートに関連するセキュリティ勧告を発表	1	1					1							1	（OTにおける安全でない設計プラクティスによって引き起こされる 56 の脆弱性） Digital Bond社が実施した研究プロジェクトであるProject Basecampが、運用技術(OT)デバイスとプロトコルがどれほど重要であるかを調査してから10年が経ちました。それ以来、Industroyer、TRITON、Industroyer2、INCONTROLLERなどの非常に影響力のある現実世界のOTマルウェアが、安全でない設計上の機能を悪用しているのを見てきました。 CISAの脆弱性開示プロセスと協力して、Forescout社のVedere Labsは、10のOTベンダーのデバイスに影響を与える56の脆弱性のセットであるOT:ICEFALLを開示しています。 OT:ICEFALL の脆弱性は、主に次の4つのカテゴリに分かれています。 ・安全でないエンジニアリングプロトコル ・脆弱な暗号化または壊れた認証スキーム ・安全でないファームウェアアップデート ・ネイティブ機能によるリモートコード実行	https://www.cisa.gov/uscert/ncas/current-activity/2022/06/22/cisa-releases-security-advisories-related-oticefall-insecure https://www.forescout.com/blog/ot-icefall-56-vulnerabilities-caused-by-insecure-by-design-practices-in-ot/ https://www.forescout.com/resources/ot-icefall-report/	
2022/6/22	CIS Software supply chain security Guide	CIS ソフトウェアサプライチェーンセキュリティガイド	1	1										1			クラウドネイティブセキュリティのリーディングカンパニーであるアクアセキュリティと、コネクテッドワールドの信頼性向上をミッションとする独立非営利団体インターネットセキュリティセンター（CIS）は、本日、ソフトウェアサプライチェーンセキュリティに関する業界初の正式ガイドラインを発表しました。 両組織の協力により作成されたCISソフトウェアサプライチェーンセキュリティガイドは、一般的に使用されている様々な技術やプラットフォームに適用できる100以上の基礎的な推奨事項を提供しています。さらに、アクアセキュリティは、新しいオープンソースツール「Chain-Bench」を発表しました。これは、CISの新しいガイドラインへの準拠を保証するために、ソフトウェアサプライチェーンを監査するための最初で唯一のツールです。 ソフトウェアサプライチェーンに対する脅威は増加し続けていますが、調査によると、開発環境全体のセキュリティは依然として低いままです。新しいガイドラインは、ソフトウェア成果物のサプライチェーンレベル（SLSA）やアップデートフレームワーク（TUF）などの主要な新しい標準をサポートする一般的なベストプラクティスを確立し、Benchmarkがサポートするプラットフォームにおける設定と監査に関する基礎的な推奨事項を追加しています。 このガイドでは、ソースコード、ビルドパイプライン、依存関係、アーティファクト、デプロイメントなど、ソフトウェアのサプライチェーンに関する5つのカテゴリについて推奨しています。	ガイドライン本文： https://github.com/aquasecurity/chain-bench/blob/main/docs/CIS-Software-Supply-Chain-Security-Guide-v1.0.pdf CIS発表： https://www.cisecurity.org/about-us/media/press-release/aqua-security-collaborates-with-center-for-internet-security-to-create-guide-for-software-supply-chain-security	

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源								要旨	参照先	その他特記事項
			政府機関・行政	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他組織化	その他標準	報道機関	その他			
2022/6/23	CISA Releases Cloud Security Technical Reference Architecture	CISAがクラウドセキュリティのテクニカルリファレンスアーキテクチャーを公開	1	1					1								CISAは、6月23日付でCloud Security Technical Reference Architecture（CS TRA）をリリースし、連邦民間部門および機関がクラウドに安全に移行するための指針としました。 CISA、米国デジタルサービス、および連邦リスクおよび承認管理プログラムによって共同執筆されたCS TRAは、大統領令14028「国家のサイバーセキュリティの向上」の履行における重要な任務を果たすため、共有サービス、クラウド移行、およびクラウドセキュリティ態勢管理に関する考慮事項を定義し、明確にします。 本Architectureでは、Cloud Security Posture Management（CSPM）を活用した政府機関のデータ収集と報告のためのクラウド移行とデータ保護の推奨アプローチを説明し、各機関がゼロエミッションを実施する際に、クラウドベースのサービスを採用する利点と固有のリスクについても説明しています。	CIS発表： https://www.cisa.gov/uscert/ncas/current-activity/2022/06/23/cisa-releases-cloud-security-technical-reference-architecture 本文： https://www.cisa.gov/sites/default/files/publications/Cloud%20Security%20Technical%20Reference%20Architecture.pdf	
2022/7/5	NIST Announces First Four Quantum-Resistant Cryptographic Algorithms	NISTが最初の4つの耐量子暗号アルゴリズムを発表	1	1				1									米国国立標準技術研究所 (NIST) は、オンラインバンキングや電子メールソフトウェアなど、私たちが日常的に頼りにしているデジタルシステムのプライバシー保護に使用されるセキュリティを解読する可能性のある、将来の量子コンピューターの攻撃に耐えるように設計された暗号化ツールの最初のグループを選択しました。選択された4つの暗号化アルゴリズムは、NISTのポスト量子暗号標準の一部となり、約2年以内に完成する予定です。 この規格に含めるために4つの追加アルゴリズムが検討されており、NISTは将来、そのラウンドのファイナリストを発表する予定です。NISTは、堅牢なさまざまな防衛ツールの必要性から、2段階でその選択を発表しています。NISTの取り組みの初めから暗号学者が認識していたように、暗号化を使用するさまざまなシステムとタスクがあり、有用な標準は、さまざまな状況向けに設計されたソリューションを提供し、暗号化にさまざまなアプローチを使用し、脆弱性が証明された場合にユースケースごとに複数のアルゴリズムを提供します。 安全なWebサイトにアクセスするときに使用される一般的な暗号化のために、NISTはCRYSTALS-Kyberアルゴリズムを選択しました。その利点の中には、2つの当事者が簡単に交換できる比較的小さな暗号化キーと、その操作速度があります。 デジタル取引中に身元を確認する必要がある場合や、リモートで文書に署名する必要がある場合によく使用されるデジタル署名の場合、NISTはCRYSTALS-Dilithiumの3つのアルゴリズムを選択しました。レビュアーは最初の2つの高効率を指摘し、NISTはCRYSTALS-Dilithiumを主要なアルゴリズムとして推奨し、FALCONはDilithiumが提供できるよりも小さなシグネチャを必要とするアプリケーション向けに推奨しています。3番目のSPHINCS+は、他の2つよりもやや大きくて遅いですが、NISTの他の3つの選択すべてとは異なる数学的アプローチに基づいているという1つの主な理由から、バックアップとして価値があります。	https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms https://www.nextgov.com/cybersecurity/2022/07/nist-identifies-four-quantum-resistant-encryption-algorithms/368954/	
2022/7/6	How to map the Cybersecurity Threat Landscape? Follow the ENISA 6-step Methodology	サイバーセキュリティの脅威の状況をどのようにマッピングするか?ENISAの6ステップの方法論に従う	1	1						1							ENSAは、サイバーセキュリティ脅威ランドスケープの６つのステップ方法論 を発表しました。ENISAによって開発されたサイバーセキュリティ脅威ランドスケープ（CTL: Cybersecurity Threat Landscape）方法論は、EU全体で一貫性のある透過的な脅威インテリジェンスの共有を促進することを目的としています。ENISA脅威ランドスケープレポート2021の改訂版に続いて、ENISAはこのフラッグシップイニシアチブをさらに改善し続けています。 この方法論の構成は、脅威ランドスケープを把握するオープンで透過的なフレームワークを利用します。 この方法論では、データ収集と分析のための体系的かつ透過的なプロセスのおかげで、水平的、テーマ別、およびセクター別のCTLの透過的かつ体系的な配信のベースラインを提供することを目的としています。 この方法論は、ENISAの利害関係者、および独自のサイバー脅威ランドスケープを生成したい利害関係者が利用できます。 このCTLフレームワークを採用し適応させることで、状況認識を構築し、既存および潜在的な脅威を監視して対処する能力が強化されます。また、この方法論を使用して、強化されたENISA脅威ランドスケープ（ETL: ENISA Threat Landscape）が提供されます。	https://www.enisa.europa.eu/news/enisa-news/how-to-map-the-cybersecurity-threat-landscape-follow-the-enisa-6-step-methodology	
2022/7/8	Hackers Say They Can Unlock and Start Honda Cars Remotely	ハッカーは、ホンダカーのロックを解除してリモートで起動できると言う													1		セキュリティ研究者によると、ハッカーはホンダ車のほぼすべてのモデルのロックを解除し、リモートで起動することができると主張する脆弱性に関する技術レポートとビデオを公開しました。 ビデオでは、Kevin2600と彼の同僚は、ラップトップに接続されたデバイスでホンダ車のさまざまなモデルのロックを解除することによって、攻撃がどのように機能するかを示しています。攻撃をテストしたホンダのモデルは、いわゆるローリングコードメカニズムを使用しており、理論的には、車の所有者がキーフォブを使用するたびに、別のコードを送信して開きます。これにより、コードをキャプチャして再度使用することが不可能になります。しかし、研究者らは、コードをロールバックし、古いコードを再利用して車を開くことを可能にする欠陥があることを発見しましたとKevin2600は言いました。 Kevin2600は、攻撃は痕跡を残さないので、誰かがあなたの車を開くために欠陥を悪用したかどうかを知る方法はないと書いています。この問題を解決するために、理想は所有者が地元のディーラーに車を持ち帰ることができるようにリコールすることですが、keyfobの脆弱なファームウェアにパッチを当てる可能性もあります。	https://www.vice.com/en/article/z34xnw/hackers-say-they-can-unlock-and-start-honda-cars-remotely	
2022/7/12	Predatory Sparrow: Who are the hackers who say they started a fire in Iran?	略奪すずめ：イランで火事を起こしたハッカーは誰か?													1		Predatory Sparrowと呼ばれるハッキンググループは、彼らが攻撃の背後にいて深刻な火災を引き起こしたと言い、それを裏付けるビデオをリリースしました。このビデオは、機械が溶鋼と火を噴き出す前に工場労働者が工場の一部を離れる様子 を映し出す事件のCCTV映像であり、ビデオは、人々がホースで火に水を注ぐところで終わっています。 Predatory Sparrowは、これはイスラム共和国が行った不特定の「侵略」行為に対応して、6月27日にイランの鉄鋼メーカーに対して行った3つの攻撃の1つだったとしており、このグループはまた、機密の電子メールを含む、企業から盗まれたと主張するギガバイトのデータを共有し始めました。「彼らは自分たちをハクティビストのグループだと主張しているが、その洗練さと高い影響力を考えると、このグループは国民国家によって運営されているか、後援されていると考えています」と、Check Point Softwareのサイバー調査責任者であるItay Cohenは述べています。英国を拠点とする反体制派イランの活動家で、独立したサイバースパイ調査官のナリマン・ガリブ氏は、この動画が本物だと確信しており、次のように話しています。「もしイスラエルがこれらの攻撃の背後にいるのなら、彼らは単にサービスを混乱させるのではなく、本当の損害を与えることができることを示していると思います。」	https://www.bbc.com/news/technology-62072480	

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源								要旨	参照先	その他特記事項
			政府機関・行政	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他標準化組織	報道機関	その他			
2022/7/12	Healthcare Orgs Struggle With IIoT, OT Security Project Implementation	IIoT、OTセキュリティプロジェクトの実施に悩む医療機関												1	1	ヘルスケア部門は、産業用モノのインターネット（IIoT）と運用技術（OT）のセキュリティプロジェクトの実施に苦労していることが、Barracudaの委託を受けた調査会社Vanson Bourne が実施したレポートにより明らかになりました。 研究者は、組織内のIIoTとOTを担当する800人の上級ITマネージャ、ITセキュリティマネージャ、およびプロジェクトマネージャを調査し、セキュリティプロジェクト、実装の問題、および現在のサイバー脅威の状況に関する意見を得ました。 多くの企業において、セキュリティ侵害は金銭的損失以外にも影響を与えることが示されており、その結果、重大なダウンタイムが発生し、侵害の影響が長期に亘っています。 調査結果によると、産業用プロトコルの検出と適用、Webアプリケーションファイアウォール (WAF)、異常検出、高度な脅威保護などのテクノロジを実装した組織は、セキュリティの有害事象の影響を軽減することに成功しており、効果的な IIoT セキュリティプロジェクトを完了している組織では、75% が大きなインシデントの影響をまったく受けていません。 産業分野での導入状況では、重要なインフラストラクチャ組織は導入をリードしており、石油とガスの 50% がプロジェクトを完了していますが、製造業では24%、医療分野ではわずか17%しかプロジェクトを完了していません。 調査対象となった全業界の組織全体の93%が、主にテクノロジー、タイミング、コストの問題が原因で、実装プロジェクトに失敗しています。IIoT と OT セキュリティは引き続き攻撃者の主要な標的ですが、プロアクティブなアプローチをとる企業には期待が寄せられています。企業は、効果的なネットワークセグメンテーションと高度な脅威保護を可能にし、多要素認証を提供し、さらにはゼロトラストアクセスを実装することができる安全なクラウドサービスを介して、安全なエンドポイント接続機器や堅牢なネットワークファイアウォールの使用など、これらの課題に対処するためのツールを実装する必要があります。	https://healthitsecurity.com/news/healthcare-orgs-struggle-with-iiot-ot-security-project-implementation https://www.barracuda.com/news/article/853# https://assets.barracuda.com/assets/docs/dms/NetSec_Report_The_State_of_IIoT_final.pdf	
2022/7/14	Cyber Safety Review Board Releases Unprecedented Report of its Review into Log4j Vulnerabilities and Response	サイバー安全審査委員会、Log4jの脆弱性と対応に関する前例のないレビュー報告書を発表	1	1								1				米国国土安全保障省(DHS)は、政府と業界に対する19の実用的な勧告を含むサイバー安全審査委員会(CSRB)の最初の報告書を発表しました。 CSRBは、最初のレビューで、約80の組織や個人と協力して、Log4jイベントに関する洞察を収集し、調査結果を通知し、将来のインシデントをより効果的に防止して対応するための実用的な推奨事項を作成しました。 CSRBからの勧告は、政府と業界のリーダーが一堂に会し、重要なサイバーセキュリティイベントをレビューおよび評価し、国のネットワークとインフラストラクチャをよりよく保護する前例のない官民イニシアチブであり、広く使用されているLog4jオープンソースソフトウェアライブラリで2021年後半に発見された脆弱性によってもたらされる継続的なリスクに対処しています。これらは、近年発見された最も深刻な脆弱性の1つです。 CSRBの勧告は、ソフトウェア製品のセキュリティの向上と、深刻な脆弱性に対応する公的および民間部門の組織の能力の向上に焦点を当てています。 CSRBは、大統領令14028「国家のサイバーセキュリティの改善」を通じてバイデン大統領の指示の下でマヨーカス長官が2022年2月に設立し、連邦政府と民間部門のサイバーセキュリティのリーダーで構成されています。 CSRBには規制権限はなく、執行機関でもありません。代わりに、その目的は、国家サイバーセキュリティの進歩を可能にするために学んだ教訓を特定し、共有します。DHSの政策担当次官であるRobert Silversが議長を務め、Googleのセキュリティエンジニアリング担当バイスプレジデントであるHeather Adkinsが副議長を務めています。	https://www.dhs.gov/news/2022/07/14/cyber-safety-review-board-releases-report-its-review-log4j-vulnerabilities-and 報告書本文： https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf	報告書　Section 3 (Page 18)以降に、Recommendationsがいろいろ書かれていますが、Software built in security, SBOM、その他PSIRT含むインシデントレスポンスや脆弱性ハンドリングで昔から言われていたことも多く含まれています。例えば（Page 25 12項）：「ソフトウェアの構成要素をカタログ化できるSBOMのようなトレーサビリティ機能は、有望な可能性ではあるが、現時点では限界がある。理事会は、将来的にSBOMの実装と採用が改善され、組織がSBOMを脆弱性管理に活用できるようになることを期待している。」（利用するためのツールがないと利用が進まない）
2022/7/15	Amazon Ring gave police data without user consent 11 times so far in 2022	Amazon Ringは、2022年にこれまでに11回、ユーザーの同意なしに警察のデータを提供しました												1		Amazonは、米国上院議員のEd Markey(民主党、マサチューセッツ州)からの問い合わせに回答し、2022年にRingが警察の「緊急」要請に応じた11件のケースがあったことを確認した。いずれの場合も、Ringはビデオやオーディオを含むプライベート録画データを引き渡したが、警察が彼らのデータにアクセスし、潜在的にダウンロードされたことをユーザーに知らせていなかった。これは、警察の民間監視への依存度が高まっていることに対する多くの懸念を提起し、この慣行は長い間規制されていない。Ringは、「差し迫った死亡の危険や重大な身体の傷害を伴う場合、緊急の法執行機関からの情報要求に直ちに対応する」と説明している。その方針は、警察からの援助要請を検討し、「その要請が連邦法に基づく周知の基準を満たしているかどうか、遅滞なく情報の開示を必要とする人物に死亡または重大な身体的傷害の差し迫った危険があるかどうかを誠実に判断する」としている。オンラインで市民の自由を保護することに専念する非営利団体、電子フロンティア財団の政策アナリスト、 Matthew Guariglia氏は、規制当局が警察が民間監視にどれだけ頼ることができるかを制限するより多くの基本ルールを敷くことを望んでおり、Ringのような企業が、ドアベルのデフォルト設定を変更して音声録音をオフにし、警察やRingなどの第三者がアクセスするのを防ぐためにデータを自動的に保存することで、潜在的に違法な監視からユーザーを保護するためにより多くの措置を講じることを望んでいる。 Ed Markey上院議員はRingの最大の批判者の一人に数えられており、連邦機関による生体認証技術の使用を禁止し、州および地方団体に連邦補助金の資金提供を条件付け、生体認証技術の使用を一時停止する顔認識・生体認証技術モラトリアム法を議会に提出し、活動している。	https://arstechnica.com/tech-policy/2022/07/amazon-finally-admits-giving-cops-ring-doorbell-data-without-user-consent/ Ed Markey議員の声明： ttps://www.markey.senate.gov/news/press-releases/senator-markeys-probe-into-amazon-ring-reveals-new-privacy-problems	SIP CPS様に限らず、日本のIoTの議論でprivacyの話題や議論をあまり聞かないが、特に欧州ではIoTの話にはprivacyは絶対欠かされない論点である。
2022/7/15	UNVERIFIED COMMITS: ARE YOU UNKNOWINGLY TRUSTING ATTACKERS' CODE?	未確認のコミット: 攻撃者のコードを無意識のうちに信頼していますか?													1	憂慮すべきソフトウェアサプライチェーン攻撃手法により、脅威アクターは開発者をだまして潜在的に悪意のあるコードを使用させることができます。GitHub 上でコミットのメタデータをスプーフィングして偽造する機能を利用することで、攻撃者はユーザーを欺き、有害なリポジトリを使用するように誘導することができます。オープンソースプロジェクトを探している開発者は、アクティブでメンテナンスされているものを選択する可能性が高く、過去数年間の活動実績を持つ長年の開発者を信頼する可能性が高くなります。GitHub では、このメタデータの多くを提供することで、これを簡単に評価できます。残念ながら、これらのデータポイントの一部は簡単に偽造される可能性があります。GitHub でのユーザアクティビティの顕著な尺度は、ユーザのプロファイルページに表示される「アクティビティグラフ」です。このグラフは、基本的にユーザーのアクティビティを時系列で示すヒートマップです。したがって、必要なタイムスタンプでコミットを捏造することができれば、このグラフを改ざんされたアクティビティで埋めることができます。このブログでは、Checkmarx SCS チームが、脅威アクターが GitHub の機能を利用して開発者をだまして、潜在的に悪意のあるコードでリポジトリを使用させる 2 つの方法について詳しく説明しています。	https://checkmarx.com/blog/unverified-commits-are-you-unknowingly-trusting-attackers-code/	

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源									要旨	参照先	その他特記事項
			政府機関・行政	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他の組織化	その他標準	報道機関	その他			
2022/7/20	DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators	DHSが重要なパイプラインの所有者とオペレーターのための新しいサイバーセキュリティ要件を発表	1	1					1								米国国土安全保障省（DHS）の運輸保安局（TSA）部門が、石油および天然ガスパイプラインの所有者と運営者に対するサイバーセキュリティに関して、Operational Technology(以下、OT)を含んだセキュリティ指令を改訂および再発行したと発表しました。この指令は、米国国土安全保障省（DHS: U.S. Department of Homeland Security）の運輸保安局（TSA: Transportation Security Administration）部門から発行された、サイバーセキュリティ要件をさらに1年間延長し、重要なサイバーセキュリティの成果を達成するための規範的な対策ではなく、パフォーマンスベースの対策に焦点を当てています。 天然ガスパイプラインなどの施設の所有者/運用者に対して以下の内容を求めています。 ・サイバーセキュリティ対策と成果達成のスケジュールに関する記述に関して、TSA承認のサイバーセキュリティ実施計画を作成し、実施すること。 ・ガスまたは液体パイプラインの情報システムおよび/またはOTシステムに対して、　サイバーセキュリティインシデントへの対応計画、リスク対応範囲拡散の低減、重大な影響に対応する能力を開発し最新化すること。 ・所有者/オペレーターがサイバーセキュリティ対策の有効性を積極的かつ定期的に　評価し、デバイス、ネットワーク、および/またはシステムの脆弱性を特定して解決する方法として、サイバーセキュリティ評価の年間計画を確立すること。 OTに関しては、運用を中断されることを防御できるような設計として、接続される関連システム等のゾーン境界の設定と運用することの重要性を述べています。	https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators#_blank	
2022/7/21	NIST Updates Guidance for Health Care Cybersecurity	NISTが医療サイバーセキュリティに関するガイダンスを更新		1				1									NISTはSP 800-66 Rev.2：「健康保険の相互運用性と説明責任法（HIPAA）セキュリティルール：サイバーセキュリティリソースガイド」のドラフトを公表しました。草案では、業界が電子保護医療情報(ePHI)の機密性、完全性、可用性を維持できるように設計されています。この用語は、処方箋、検査結果、病院訪問およびワクチン接種の記録など、幅広い患者データを対象としています。 1996年の医療保険の携行性と説明責任に関する法律(HIPAA)は、患者の同意や知識なしに患者の健康情報が開示されないようにするための国家基準の作成を要求する連邦法です。HIPAA の一部はセキュリティ ルールで、特に医療機関が作成、受信、維持、または送信する ePHI の保護に焦点を当てています。NISTはHIPAAを施行するための規制を作成していませんが、改訂された草案はサイバーセキュリティガイダンスを提供するというNISTの使命に沿っています。NISTの更新されたガイダンスは、米国保健福祉省が医療に影響を与えるサイバー攻撃の増加を指摘しているため、特にタイムリーです。 NISTが改訂版を開発した主な理由の1つは、2008年に改訂版1が公開されたときには存在しなかった他のNISTサイバーセキュリティガイダンスと統合することです。それ以来、NISTはよく知られているサイバーセキュリティフレームワークを開発し、組織が独自のリスク管理アプローチを調整するために使用できるセキュリティとプライバシーコントロール(NIST SP 800-53)のコレクションを繰り返し更新しました。新しいHIPAAセキュリティルールガイダンス草案は、これらおよび他のNISTサイバーセキュリティリソースに明示的に接続しています。NISTは、2022年9月21日まで、草案の公表に関するコメントを求めています。	https://www.nist.gov/news-events/news/2022/07/nist-updates-guidance-health-care-cybersecurity SP 800-66 Rev.2 https://csrc.nist.gov/publications/detail/sp/800-66/rev-2/draft	文書の題名Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide からご推察いただ けるように、HIPAA関連ガイドです。 内容、特に本文見ても、あちこちにIoTが 出てきますが、IoTに特化した話ではなく、あくまで情報システム全体をHIPAAに 最適化するためのガイドでaru.
2022/7/21	Top CVEs to Patch: Insights from 2022 Unit 42 Network Threat Trends Research Report	パッチ適用する上位CVE: 2022 Unit 42 ネットワーク脅威の傾向に関する調査レポートからの洞察			1											1	2022 Unit 42 Network Threat Trends Research Reportでは、Palo Alto Networks Advanced Threat Preventionセキュリティサービスによって次世代ファイアウォールとPrisma SASEで米国、シンガポール、日本、オーストラリア、カナダ、ヨーロッパなどの地域からキャプチャされたデータを使用して、野生のエクスプロイトを観察および分析しました。 同社のデータには、大学、病院、電子商取引ベンダー、金融機関、ハイテク企業などの組織に対する攻撃が含まれます。これには、2021 年からの 2 億 6,200 万件の攻撃トラフィック セッションが含まれます (内部トラフィックを除く)。 この情報を使用して、攻撃者が 2021年に最も一般的に悪用した脆弱性を特定し、2022年と 2023年にどの脆弱性に注目するかを予測しました。組織では、リストの上位に挙げられた脆弱性にパッチを適用することをお勧めします。 Apache Log4j の脆弱性は、その深刻さと悪用の容易さを考えると当然のことながら、2021 年で最も悪用された CVE であり、1か月足らずで 1,100万件以上の攻撃セッションが観察されました。この脆弱性は 2021 年 12 月に公開されましたが、脆弱性に対する攻撃セッションは、観察された攻撃セッション全体の4.2%を占めており、これらの脆弱性がセキュリティに及ぼした深刻な影響を強調しています。	https://unit42.paloaltonetworks.com/network-threat-trends-research-report/	
2022/7/28	House Passes Chips Act to Boost U.S. Semiconductor Production	議会は米国の半導体生産を後押しするチップ法を可決	1	1											1		下院は、米国の半導体製造と中国との競争力を高めることを目的とした2800億ドルの法案を可決しました。 この法案は、半導体製造に390億ドルを割り当てていますが、半導体製造の研究と労働力トレーニングを進めるための110億ドルと、実験室の進歩を軍事やその他のアプリケーションに迅速に変換するための20億ドルの資金も含まれています。 Intel、TSMC、GlobalFoundriesなどのいくつかのチップ製造業者は、法案の可決を条件として、米国に工場を建設する計画をすでに発表しています。	https://www.wsj.com/articles/house-passes-chips-act-to-boost-u-s-semiconductor-production-11659035676?mod=hp_lead_pos3	

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源									要旨	参照先	その他特記事項
			政府・行政機関	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他組織	その他標準	報道機関	その他			
2022/7/29	Joint Statement of the U.S.-Japan Economic Policy Consultative Committee: Strengthening Economic Security and the Rules-Based Order	日米経済政策諮問委員会共同声明:経済安全保障の強化とルールに基づく秩序	1									1					ブリンケン国務長官とライモンド商務長官は、林外務大臣及び萩生田経産大臣とともに日米経済政策諮問委員会(EPCC)の初回閣僚会議を開催した。閣僚は、ルールに基づく国際経済秩序の利益を強調する前向きな経済ビジョンを提示するとの共通の決意を確認し、我々の経済をより競争力と強靭なものにする必要性を強調した。 ●ルールに基づく経済秩序による平和と繁栄の実現　●経済的強制と不公正で不透明な融資慣行への対抗 ●重要かつ新興のテクノロジーと重要インフラの促進と保護 ・日米両国は、日米グローバル・デジタル・コネクティビティ・パートナーシップを支持し、2030年までに世界の5G市場におけるOpen RANの市場シェアを大幅に拡大するという野心に鑑み、安全でオープンな5Gネットワークをグローバルに展開する努力を引き続き支援する意図を有する。 ワイヤレスネットワーク技術に対するオープンRANベースのアプローチを含む、高度な通信ネットワークのための安全な技術オプションを促進する。 ・日米両国は,デジタル政策問題に関する国際的及び多国間の場における調整を強化し,安全で信頼される海底ケーブルシステムの戦略的に重要かつ互恵的なプロジェクトを促進し,支援するため,パートナーとの協力を促進する意図を有する。 ・日米両国は,重要インフラに対する脅威に関する情報を共有することの重要性を確認する。 ●サプライチェーンのレジリエンスの強化 日米両国は、日米の下での商業・産業パートナーシップ及び特に半導体、電池及び重要鉱物を含む戦略的セクターにおけるサプライチェーンの強靭性を促進するためのその他の枠組みの取組を前進させようと努める。この目的に向けて、両国は、 a.バイデン大統領と岸田総理が次世代半導体の開発を探求するために発表した合同タスクフォースの進展を歓迎し、このメカニズムを通じた継続的な協力にコミットする。 b.日本企業が米国における電池製造への投資を増やし、サプライチェーンの強靭性に貢献していること、両国が志を同じくする国々間の協力を主導するために強固なバッテリーサプライチェーンを構築することが重要であることを認識した。 c.レアアースを含む重要鉱物の多様で強固なサプライチェーンを構築するため、特にエネルギー安全保障を強化し、クリーンエネルギーの移行を支援する処理のボトルネックに対処するために、資金支援の提供を含む協力の重要性を強調する。	https://www.state.gov/joint-statement-of-the-u-s-japan-economic-policy-consultative-committee-strengthening-economic-security-and-the-rules-based-order/ https://www.commerce.gov/news/press-releases/2022/07/joint-statement-us-japan-economic-policy-consultative-committee	日本の報道を見ると、半導体の研究センターの話しか見かけないが、米国の文書を見る限り、半導体には言及されているが、むしろ、食料、5G, 海底ケーブル、電池、希土類と、戦略資源が並び、あくまで戦略資源のサプライチェーンの強化と確保が目的とされている。
2022/7/29	ENISA Threat Landscape for Ransomware Attacks	ランサムウェア攻撃のENISA脅威ランドスケープ	1	1						1							この脅威ランドスケープレポートでは、2021年5月から2022年6月までの報告期間中に、EU、英国、米国で合計623件のランサムウェアインシデントが分析された。この期間のランサムウェアの脅威アクターによって毎月約10テラバイトのデータが盗まれ、盗まれたデータの58.2%には従業員の個人データが含まれていた。これらのデータを分析し、少なくとも47のユニークなランサムウェア脅威アクターが見つかりました。インシデントの94.2%について、会社が身代金を支払ったかどうかは不明だが、ネゴシエーションが失敗すると、攻撃者は通常、自分の Web ページでデータを公開して利用できるようにします。これは事件の37,88%の現実です。したがって、残りの62,12%の企業は攻撃者と合意に達したか、別の解決策を見つけたと結論付けることができます。上記の数字は全体像の一部であり、この調査ではランサムウェア攻撃の総数がはるかに多いことが明らかとなった。この調査から5つの異なるランサムウェアビジネスモデルが浮上した。 1. 個々の攻撃者に焦点を当てたモデル。　2. グループの脅威アクターに焦点を当てたモデル。　3. サービスとしてのランサムウェアモデル。　4. データ仲介モデル。　5. ランサムウェアビジネスを成功させるための鍵として悪名高いことを達成することを主な目的としたモデル。 ランサムウェアに対する回復力を強化するには、次のようなアクションを実行します。 ・ビジネスファイルと個人データの最新のバックアップを保持する;　・このバックアップをネットワークから隔離する。 ・バックアップの3-2-1ルールを適用します:　3コピー、2つの異なるストレージメディア、1コピーオフサイト。 ・エンドポイントデバイスのほとんどのランサムウェアを検出するように設計されたセキュリティソフトを実行する。 ・管理者権限を制限する。等。 ランサムウェア攻撃の被害に遭った場合:・国家のサイバーセキュリティ当局または法執行機関に連絡してガイダンスを求める。 ・身代金を支払わず、脅威アクターと交渉しないでください。　・影響を受けるシステムを隔離する。　・ユーロポールのイニシアチブであるNo More Ransom Projectをご覧ください、等。	https://www.enisa.europa.eu/news/ransomware-publicly-reported-incidents-are-only-the-tip-of-the-iceberg	
2022/8/2	Deception at Scale: How Malware Abuses Trust	大規模な欺瞞:マルウェアが信頼を悪用する方法			1										1	1	セキュリティプラットホーム企業のVirusTotalがマルウェアに関する調査レポートを公表した。同社のプラットフォームは、毎日200万件のファイルの提出に基づいて、2021年1月から2022年7月までの統計を示すレポートを作成し、マルウェアの配布方法の傾向を示しています。このレポートでは、攻撃者がマルウェアの拡散、防御の回避、またはソーシャル エンジニアリング攻撃の成功の最大化に使用するさまざまな信頼の悪用アプローチについて説明している。 ●正当なドメインの悪用：合法的で人気のある上位のWebサイトを通じてマルウェアを配布することで、脅威アクターはIPベースのブロックリストを回避し、高可用性を享受し、より高いレベルの信頼を提供できる。 ●盗まれたコード署名証明書の使用：企業から盗まれた有効な証明書を使用してマルウェアサンプルに署名することは、ホスト上のAV検出とセキュリティ警告を回避する信頼性の高い方法である。 ●人気のあるソフトウェアに変装：マルウェアの実行可能ファイルを合法的で人気のあるアプリケーションとして装うことは、2022年に上昇傾向にある。 ●正当なインストーラのレース：最後に、正規のアプリケーションインストーラ内にマルウェアを隠し、実際のアプリケーションがフォアグラウンドで実行されている間に感染プロセスをバックグラウンドで実行するというトリックがある。 ●安全を保つ方法：ソフトウェアをダウンロードする場合は、OSの組み込みアプリストアを使用するか、アプリケーションの公式ダウンロードページにアクセスしてください。また、検索結果の宣伝広告は、正当なサイトのように見えるように簡単に偽装される可能性があるため、上位にランク付けされる可能性がある。	https://blog.virustotal.com/2022/08/deception-at-scale.html https://assets.virustotal.com/reports/2022-deception-at-scale https://www.bleepingcomputer.com/news/security/wolf-in-sheep-s-clothing-how-malware-tricks-users-and-antivirus/	

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源									要旨	参照先	その他特記事項
			政府・行政機関	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他標準化組織	報道機関	その他			
2022/8/2	Senators Introduce Bill to Ensure Resiliency of Federal Data Centers	上院議員が連邦データセンターの回復力を確保するための法案を提出	1											1		超党派の上院議員のグループは、全国の連邦データセンターのベースラインサイバーセキュリティ要件と壊滅的な気象関連の災害に対する新しい保護を確立するための法律を提出しました。上院国土安全保障・政府問題委員会委員長のGary Peters上院議員(民主党)は、Jacky Rosen上院議員(民主党)とJohn Cornyn上院議員(共和党)と共に法案を提出しました。 入手した法案のコピーによると、この法案は、連邦データセンターの閉鎖と統合のための最近の取り組みを基盤としています:2010年以来、6,000以上の施設が統合されており、その傾向は推定58億ドルのコスト削減とコスト削減をもたらしました。エージェンシーのリーダーは、データセンターの使用状況を定期的に評価して、データセンターの運用を継続するかどうかを判断し、レガシーシステムが更新され、最新のテクノロジーが採用され、施設が全体的に最適化され、潜在的な脆弱性に対して安全であることを確認する任務を負います。 「連邦システムに保存されている機密情報は、サイバー攻撃や自然災害などの脆弱性にさらされているままにしておくことはできません」とCornyn氏は声明で述べています。「この法律は、連邦政府のデータを保護し、最適化を促進するのに役立ち、納税者のドルを節約し、連邦政府に情報を委ねるアメリカ人を保護するでしょう。」Jacky Rosen氏はまた、声明で「サイバー攻撃と自然災害の脅威が高まっている」と指摘し、法案はデータを保護するために「新しい一連のセキュリティと回復力の基準を制定する」と述べています。	https://www.nextgov.com/cxo-briefing/2022/08/senators-introduce-bill-ensure-resiliency-federal-data-centers/375245/	
2022/8/4	Internet of Things (IoT) Security	IoTセキュリティ	1	1								1				モノのインターネット (IoT) は、センサー、ソフトウェア、およびインターネットを介して他のデバイスと接続してデータを交換するその他のテクノロジがインストールされた物理オブジェクトのネットワークを表します。これらのデバイスは、日常の家庭用品から産業用ツールまでさまざまです。今日、約 70 億のデバイスが IoT を通じて接続されており、このテクノロジーを使用するデバイスは 2025 年までにさらに 200 億増加すると推定されています。 医療、金融、製造、物流、小売など、このテクノロジを運用する多くの組織とともに、このテクノロジに伴うセキュリティの懸念が高まっています。そのアーキテクチャは通常、ワイヤレス ネットワークと、データを交換するためのいくつかのコンポーネントで構成されます。 IoT プロジェクトは異なる場合がありますが、主要なアーキテクチャ レイヤーは一貫しています。このテクノロジーの使用が増えると、それに対するサイバー攻撃の増加も懸念されます。分散型サービス妨害 (DDoS) または中間者攻撃 (MITM) は、IoT に対して使用される一般的なエクスプロイトの一部です。さらに、組織に IoT を追加すると、ネットワークが安全なゾーンに分割されていない場合、企業が脆弱になる可能性のある攻撃面が増える可能性があります。インターネットに接続されているすべてのオブジェクトと同様に、それらは、優れた物理的セキュリティから、ファームウェアの定期的な更新の確保まで、これらのデバイスを保護するのに役立つ方法です. IoT は、インターネットに接続できる物理的なオブジェクトです。 これらのさまざまなオブジェクトをすべて接続し、それらにセンサーを追加することで、リアルタイムでの通信を可能にする新しいレベルのインテリジェンスが追加されます。 モノのインターネットは、デジタル ユニバースと物理ユニバースを融合させることで、私たちの周りの世界をより応答性の高いものにしています。	https://www.hhs.gov/sites/default/files/internet-of-things-security-analyst-note.pdf	
2022/8/8	CloudGuard Spectral detects several malicious packages on PyPI – the official software repository for Python developers	CloudGuard Spectralは、 Python開発者のための公式ソフトウェアリポジトリとして利用されているPyPI上のいくつかの悪意のあるパッケージを検出			1									1		PyPI は主要な Python リポジトリであり、Python ユーザーによって最も一般的に使用されています。すべての Python 開発者は、必要な Python ソフトウェアを導入するための「pip install」を行うことを日常的に行っています。 Pypi は、開発者がこのコミュニティの他の開発者によって開発および共有されているソフトウェアを見つけてインストールするのに役立ちます。 Pypi 自身の Web サイトによると、Pypi には 612,240 人を超えるアクティブ ユーザーがおり、391,325 のプロジェクトに取り組んでおり、3,664,724 のリリースがあります。多くのユーザーが気付いていないのは、このワンライナーの単純なコマンドがユーザーを危険にさらす可能性があるという事実です。 pip install コマンドは、setup.py スクリプトを含めることができるパッケージのインストールをトリガーします。このスクリプトには、ターゲット インストーラマシンで必要なインストール プロセスを実行するための Python スニペットを含めることができます。ハッカーはこの機能を利用して、悪意のあるコードをインストール スクリプトの一部として配置します。このコードは、気付かれることなくユーザーのマシン上でシームレスに実行されます。この場合、無知は至福ではありません。このような攻撃は、一般的に、パスワードや Apiトークンなどの非常に重要なデータ ポイントを収集するためです。さらに、そのような攻撃は増加しています。 (1) CloudGuard Spectral は、Python プログラミング言語の開発者が使用する主要な Python パッケージ インデックスである PyPIで10 個の悪意のあるパッケージを検出した。 (2) 悪意のあるパッケージは、攻撃者が開発者の個人データと個人の資格情報を盗むことを可能にするinfo-stealersをインストールします。 (3) 検出されるとCPR は情報を公開しこれらのパッケージに関するPyPIに警告を発した。後で PyPI によって削除される。 本ブログでは、PyPI以外にも、以下のサービスで同様の事例があることを示しています。 Ascii2text　Pyg-utils, Pymocks and PyProto2　Test-async　Free-net-vpn and Free-net-vpn　2Zlibsrc Browserdiv　WINRPCexploit なお、PyPIに関しては、同様の脆弱性情報がSonatype社より公表されています	https://research.checkpoint.com/2022/cloudguard-spectral-detects-several-malicious-packages-on-pypi-the-official-software-repository-for-python-developers/ https://blog.sonatype.com/python-packages-upload-your-aws-keys-env-vars-secrets-to-web	

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源									要旨	参照先	その他特記事項
			政府機関・行政	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他標準化組織	報道機関	その他			
2022/8/8	China Extends Military Exercises as Taiwan Battles Cyberattacks	中国は台湾がサイバー攻撃と戦うにつれて軍事演習を延長												1		中国は先週のナンシー・ペロシ下院議長の訪問を受けて台湾周辺での軍事演習を拡大していると述べたが、台湾軍は月曜日、北京が島に対して持続的なサイバー攻撃を続けており、主要な政府運営のウェブサイトにアクセスできなくなったと非難した。中国軍、人民解放軍は月曜日、島を効果的に封鎖する能力を実証した木曜日と日曜日の間の4日間の演習を終えた後、不特定の期間演習を継続すると述べた。これらの期間における中国のサイバー攻撃では、大学のウェブサイトやセブン-イレブンの店舗が影響を受けており、場合によってはナンシー・ペロシ下院議長に侮辱を投げかけている。 いくつかのセブン-イレブン コンビニエンス ストアのディスプレイ画面は、歯をむき出しにしてしかめっ面のペロシ夫人を表示するようにプログラムされ、「戦争屋ペロシは台湾から出て行け」というフレーズが表示され、駅の画面にはメッセージが表示されました。ソーシャルメディアで広く流布された画像によるとペロシ夫人を「古い魔女」と呼んでいます。 台湾でセブンイレブンチェーンを運営するプレジデント・チェーン・ストア・コーポレーションは、騒ぎは「未知の出所」から来たと述べ、詳しく説明することなく、直ちに修正を指示したと述べた。店舗は通常通り営業しているという。台湾の鉄道事業者は、問題の鉄道駅のスクリーンは広告会社が所有しており、鉄道事業者は影響を受けていないと述べ、すぐに画面の電源を切り、広告会社に明らかな侵害を通知した、と述べた。 台湾の国家通信委員会は、中国製ソフトウェアの使用の危険性について企業に警告しながら、予備調査が事件が中国製ソフトウェアの使用に関連していることを示唆したと述べた、と政府機関の責任者、Chen Yaw-shyang は先週の記者会見で述べた。ハッカーに悪用される可能性があります。	https://www.wsj.com/articles/china-extends-military-exercises-as-taiwan-battles-cyberattacks-11659969484	
2022/8/10	10 malicious Python packages exposed in latest repository attack	最新のリポジトリ攻撃で公開された10の悪意のあるPythonパッケージ			1									1		研究者は、Pythonプログラムとコードライブラリの公式で最も人気のあるリポジトリであるPyPiで、さらに別の悪意のあるパッケージのセットを発見しました。一見馴染みのあるパッケージにだまされた人は、マルウェアのダウンロードやユーザーの資格情報とパスワードの盗難の対象となる可能性があります。月曜日に調査結果を報告したCheck Point Researchは、10個のパッケージをダウンロードした人の数はわからないと書いているが、PyPiには613,000人のアクティブユーザーがおり、そのコードは390,000以上のプロジェクトで使用されていると指摘した。このコマンドを使用して PyPi からインストールすることは、多くの Python プロジェクトを開始またはセットアップするための基本的な手順です。Pythonプロジェクトのダウンロードを推定するサイトPePyは、悪意のあるパッケージのほとんどが何百ものダウンロードを見たことを示唆しています。このようなサプライチェーン攻撃は、特に世界のソフトウェアの広い範囲をサポートするオープンソースソフトウェアリポジトリの間で、ますます一般的になっています。Pythonのリポジトリは頻繁に標的にされており、研究者は2017年9月に悪意のあるパッケージを発見しました。2021年6月、7月、11月。そして今年の6月。しかし、トリックパッケージは、2020年のRubyGems、2021年12月のNPM、そしてさらに多くのオープンソースリポジトリでも見つかっています。最も顕著なのは、SolarWindsビジネスソフトウェアを介したロシアのハッカーによる民間ソースのサプライチェーン攻撃が顕著な大混乱を引き起こし、100以上の企業と、国家核安全保障局、内国歳入庁、国務省、国土安全保障省を含む少なくとも9つの米国連邦政府機関が感染したことです。偽の悪意のあるパッケージの発見がますます一般的になり、リポジトリが動作するように移動しています。ちょうど昨日、JavaScript パッケージの NPM リポジトリの所有者である GitHub は、パッケージ開発者がパッケージに署名して検証するためのオプトインシステムの提供に関するコメントのリクエストを開きました。NPM 開発者は、多数のオープン ソースと業界団体のコラボレーションである Sigstoreを使用してパッケージをサインオフし、パッケージ内のコードが元のリポジトリと一致することを通知できます。	https://arstechnica.com/information-technology/2022/08/10-malicious-python-packages-exposed-in-latest-repository-attack/	
2022/8/10	China could be reviewing security bugs before tech companies issue patches, DHS official says	中国はハイテク企業がパッチを発行する前にセキュリティバグをレビューする可能性がある、とDHS当局者は言う	1		1									1		北京の厳格な脆弱性報告規則は、政府当局者が最も深刻な脆弱性にも「早期アクセス」できることを意味すると、DHSのRobert Silvers政策次官はラスベガスでのBlackhutサイバーセキュリティ会議で述べました。 中国政府が、影響を受ける企業が修正を展開する前に、ゼロデイ、または以前は知られていなかったソフトウェアの欠陥を分析している場合、北京は米国やその他のデジタル敵対者に対してサイバー攻撃を実行する際に優位に立つ可能性があるということです。Silvers 氏によると、中国の技術大手 Alibaba によって最初に発見された最近の Log4j ソフトウェアの脆弱性を調査するために集められた DHS の審査委員会は、中国の開示規則に関する「非常に厄介な」質問で調査を終了しました。Silvers氏によると、Log4jの脆弱性の場合、中国の開示規則にもかかわらず、Alibabaは中国政府に通知する前に欠陥を明らかにしたということです。「Alibabaは正しいことをした」とSilvers 氏は述べましたが、氏によると、審査委員会の調査結果は、アリババが中国政府によって処罰された可能性が高いことを示唆しており、中国当局がセキュリティ開示情報を使用するかどうか、またどのように使用しているかについて疑問を投げかけています。中国企業は、脆弱性を発見してから2日以内に政府に報告する必要があります。彼らはまた、「主要な国家イベント」中に脆弱性を公に開示することも禁じられています。Silvers氏は、先月Log4jの脆弱性に関する最初の調査が終了した15人の公共および民間部門のサイバーセキュリティ専門家のトップグループであるDHSサイバーセーフティレビュー委員会の調査結果について話しました。彼は、委員会のメンバーは、Alibabaが中国政府に警告する前に脆弱性を公に開示したことで罰せられたという中国のニュース報道を懸念していると述べました。Silvers氏は、Log4jに関するレビュー委員会の作業を「史上最大の大規模なサイバー対応」と言い、彼は、委員会の作業が完了している間、Log4jの脆弱性によるリスクはすぐには消えないと述べました。この脆弱性は非常に簡単に悪用でき、非常に遍在しているため、組織は脅威が「今後数年間、おそらく10年以上」続くことを覚悟する必要があります。	https://www.cyberscoop.com/dhs-official-chinese-rules-exploit/	
2022/8/11	Defaultinator from Rapid 7	Rapid 7による Defaultinator			1										1	Defaultinator は、一般的なデバイスやアプリケーションのデフォルトパスワードを格納および照会するためのデータリポジトリです。このツールは、CWE-798 (https://cwe.mitre.org/data/definitions/798.html) に対する脆弱性を最小限に抑え、消費者保護法およびベスト プラクティスへの準拠を評価する際に役立つように、攻撃対象領域を強化しようとしている防御側をサポートするように設計されています。	https://defaultinator.com/	

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源									要旨	参照先	その他特記事項
			政府・行政機関	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他標準化組織	報道機関	その他			
2022/8/19	The Pentagon may require vendors certify their software is free of known flaws. Experts are split.	ペンタゴンは、ベンダーに、自社のソフトウェアに既知の欠陥がないことを証明するよう 要求するかもしれない。専門家は分かれている	1											1		ペンタゴンは、ベンダーに、セキュリティ上の問題を引き起こす可能性のある既知の脆弱性や欠陥のない軍事ソフトウェアのみを販売するよう要求する必要があるか？　表面的には、それは合理的な要求のように思えます。しかし、セキュリティ研究者のJerry Gamblinが、7月14日に可決された大規模な2023年の国防権限法案の中から、下院のソフトウェア脆弱性条項のスクリーンショットをツイートしたとき、サイバーセキュリティコミュニティを分裂させました。この議論は、2つの重要な議論に要約されます: 要件は不必要で達成不可能であるか、ソフトウェアベンダーに欠陥のある技術を販売した責任を負わせ始めるゲームを変える動きです。バイデン政権は、ソフトウェアベンダーに、自社の商品に既知の一般的な脆弱性やエクスポージャー、つまりCVE が含まれていないことを確認する責任を負わせる側にいます。 ソフトウェア業界は、自動車の寿命を通じて「メーカーが所有権と責任を保持する」自動車業界をエミュレートすべきであると、サイバーおよび新興技術担当国家安全保障副顧問のAnne Neuberger氏は述べています。しかし、サイバーセキュリティのエグゼクティブであるDan Lorenc氏は、脆弱性のないソフトウェアなどというものは存在しないと主張しています。Lorenc氏の側には提案された法律に声高に反対する多くの者が含まれており、著名なサイバーセキュリティ ポリシーの専門家である Harley Geiger は「すべての脆弱性が重大であるとは限らないこと、または軽減できる/軽減されるべきではないことを理解してください。」と主張している。Lorenc氏はまた、脆弱性管理データに基づく政府の標準リポジトリであるNISTのNational Vulnerability Database(NVD)は、大規模には実行不可能であると述べ、「業界として、私たちはスケーラブルな方法で、重大度を正確にスコアリングし、影響を測定し、既知の脆弱性を追跡する方法を理解していない。」と主張している。	https://www.cyberscoop.com/pentagon-vendors-vulnerability-testing/	法案への反対を述べるDan Lorenc氏の意見は、産業界の大方の反応となっている。 現役のvendorsは誰も公式には何も言わないので、元vendorだった方から取材したと思われるが、「ここだけの話」として足立氏が業界関係者から聞いている話と一致している。 これで、誰もソフトウエアがらみの政府入札に応じなくなったらどうなるのか、 との懸念の声も聞かれている。
2022/8/22	Third-party attacks spike as attackers target software connections	攻撃者がソフトウェア接続を標的にしているため、サードパーティの攻撃が急増			1									1		最近のTwilioや Mailchimpのようなサードパーティの侵入は、サプライチェーン攻撃がいかに迅速かつ広範囲に広がる可能性があるかを改めて思い出させてくれます。1つの組織への攻撃が多くの組織への潜在的な攻撃の窓口になると、脅威アクターは注意を払い、さらに攻撃を仕掛けます。不正アクセスは、フィッシングやソーシャルエンジニアリング攻撃によって行われることがよくあります。この増幅効果により、サードパーティベンダーへの攻撃が増加しています。サプライチェーン全体でのアクセスまたはデータの潜在的な露出のレベルは、脅威アクターにより多くのターゲットをより一貫して成功させる手段を提供します。 サードパーティのツールとサービスは、サイバー犯罪者に広範な経路を開く可能性のある攻撃面を提供します。大企業またはその他の意図されたターゲットの正面または側面のドアがより適切に防御されている場合、通気口に弱点がある可能性があります。これらの妥協点を見つけることは、多くの場合、下流での攻撃の機会を引き起こします。サプライチェーン攻撃の中には、特定の組織を高度に標的とする攻撃もあれば、ランダムで、サプライチェーン内のリンクが侵害された後、攻撃者を潜在的なセカンダリターゲットに導くものもあります。	https://www.cybersecuritydive.com/news/supply-chain-cyberattacks/630179/	
2022/8/24	Biden is asking critical infrastructure owners to hit cybersecurity goals, and they're not happy about it	バイデン氏は、重要なインフラ所有者にサイバーセキュリティの目標達成を求めており、彼らはそれについて満足していない	1	1										1		連邦政府機関は来月、バイデン政権が最も重要なデジタルインフラストラクチャの所有者に達成してほしいサイバーセキュリティの目標のリストを提供する予定です。このリストは業界の批判を引き起こしました。 サイバーセキュリティ・インフラセキュリティ庁(CISA)は、このリストに関するフィードバックを数カ月間求めており、先週まで業界団体などが解説をするための延長を認めています。目標は自発的なものですが、一部の業界関係者は、「パフォーマンス目標」が規制の前奏曲であるかどうかについて不快感を抱いています。リストの目標の例を紹介すると。 ・「所有者/オペレーターは、運用を維持するために不可欠なユーティリティ(水道、電力、HVACなど)を定義し、フェールオーバーシステムを展開して定期的にテストして、これらのリソースの中断のない供給を確保する必要がある。 ・「所有者/運営者は、悪意のある脅威活動と不注意な脅威活動の両方のリスクを軽減するために、すべての組織の従業員と請負業者に基本的なサイバーセキュリティトレーニングを提供する必要がある。査読者は、すべての職員が少なくとも年に1回はトレーニングを受けていることを確認する必要がある。 ・目標には、各目標が対処する主要なリスクと、進捗状況を測定する方法も含まれている。 国土安全保障省の一部であるCISAは、パフォーマンス目標に関するワークショップで1,000件以上のコメントを受け取りました。 パフォーマンス目標が、NISTの広く受け入れられているサイバーセキュリティフレームワーク、それ自体が独自の更新の真っ只中にある一連の自発的なサイバーガイドラインと完全に一致していないことに不満を抱いていると述べた。 彼らの苦情にもかかわらず、業界関係者は、CISAが彼らのフィードバックを受け入れていることを賞賛し、CISAはすでに以前の一連の目標から改善を加えていると述べた。CISAは草案をもう一度更新する予定です。広報担当者は、CISAがそのタスクを完了する具体的な日付を提供できませんでした。	https://www.washingtonpost.com/politics/2022/08/24/industry-groups-arent-thrilled-about-new-cyber-performance-goals/	
2022/8/31	MITRE Hot Topics in Supply Chain Security Report	MITRE Hot Topics in Supply Chain Security 会合報告													1	米国・足立氏によるMITRE Hot Topics in Supply Chain Security 会合報告（詳細は報告書本文参照）		
2022/9/1	NSA, CISA, ODNI Release Software Supply Chain Guidance for Developers	NSA、CISA、ODNI が開発者向けのソフトウェアサプライ チェーンガイダンスをリリース	1	1					1			1				SolarWinds とその顧客に対して実行された最近のサイバー攻撃や、Log4j などの脆弱性を悪用するエクスプロイトは、ソフトウェア サプライ チェーンの弱点を浮き彫りにしています。これに対応して、ホワイトハウスは国家のサイバーセキュリティの改善に関する大統領令 (EO 14028) を発表し、連邦政府のソフトウェア サプライ チェーンを保護するための新しい要件を確立し、連邦政府のソフトウェアを取得する顧客に加えて、ソフトウェア サプライヤーと開発者の両方に対する体系的なレビュー、プロセスの改善、およびセキュリティ基準などを定めています。 　同様に、ESFのSoftware Supply Chain Working Panel は、開発者、サプライヤー、及び顧客の利害関係者向けの推奨プラクティスの要約であり、より安全なソフトウェアサプライチェーンを確保するためのガイダンスを確立しました。 このドキュメントは、ソフトウェア開発者が参照することを強く推奨する業界のベストプラクティスと原則に沿ったガイダンスを提供します。これらの原則には、セキュリティ要件の計画、セキュリティの観点からのソフトウェア アーキテクチャの設計、セキュリティ機能の追加、およびソフトウェアと基盤となるインフラストラクチャ (環境、ソースコードのレビュー、テストなど) のセキュリティの維持が含まれます。	https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3146465/nsa-cisa-odni-release-software-supply-chain-guidance-for-developers/ 文書本文： https://media.defense.gov/2022/Sep/01/2003068942/-1/-1/0/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF	文書そのものは8月に作成されていたように見えますので、課報機関、治安維持機関としては相当迅速に一般公開したと思われる。ざっと見たところ、内容はNIST SSDFやSBOMなどよく知られた関連文献が多く引用された実践ガイドのように見える。見方を変えると、「ベンダーにはどういうことを要求せよ。」という指南書のようなものとも受け取れる。

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源									要旨	参照先	その他特記事項
			政府機関・行政	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他組織化	その他標準	報道機関	その他			
2022/9/1	Privacy invasion via smart-home hub in personal area networks	パーソナル エリア ネットワークのスマート ホーム ハブを介したプライバシーの侵害			1											1	スマートホーム デバイスは、私たちの日常生活でますます使用されています。これらのデバイスは、ユーザーに便利な機能を提供する反面、ユーザーの個人情報が漏洩するなど、便利な機能の代償が大きくなる可能性があります。 このホワイト ペーパーでは、スマートホームデバイスのプライバシーリスクに対処するためのシステム ChatterHub について説明します。具体的には、この作業は、Zigbee または Z-wave を使用し、インターネットに接続するためのパーソナル エリア ネットワーク(PAN)内の集中型スマートホーム ハブによって制御されるデバイスに焦点を当てています。 ChatterHub は、暗号化されたネットワーク トラフィックをハブから受動的に傍受し、機械学習技術を活用します。スマートホーム デバイスのイベントと状態を分類します。ChatterHub を 3 つの実世界のスマートホーム設定に展開して、その精度と効率を評価しました。評価結果は、攻撃者がスマートホーム デバイスの動作を 89% 以上の再現率で開示することに成功したことを示しています。また、攻撃者がスマートホーム ハブの通信を妨害し、パケットを選択的にドロップして、セキュリティ センサーやスマート ロックなどのデバイスのステータスをユーザーに通知できないようにすることも示しています。さらに、緩和アプローチとして、1日あたりわずか 9.2 MB の余分なネットワーク トラフィックを生成することで、ChatterHubからの脅威を効果的に防止するパケットインジェクション アプローチを開発しました。	https://www.sciencedirect.com/science/article/abs/pii/S1574119222000955	
2022/9/6	Shikitega - New stealthy malware targeting Linux	Shikitega - Linux を標的とする新しいステルス マルウェア														1	AT&T Alien Labs は、Linux オペレーティング システムを実行しているエンドポイントと IoT デバイスを標的とする新しいマルウェアを発見しました。Shikitega は、各モジュールがペイロードの一部に応答し、次のモジュールをダウンロードして実行する、多段階の感染チェーンで配信されます。攻撃者は、実行され持続するように設定される暗号通貨マイナーに加えて、システムを完全に制御することができます。 ・このマルウェアは、Metasploit の「Mettle」Meterpreterをダウンロードして実行し、感染したマシンを制御します。 ・Shikitega は、システムの脆弱性を悪用して高い権限を取得し、暗号マイナーを永続化して実行します。 ・このマルウェアはポリモーフィック エンコーダーを使用して、ウイルス対策エンジンによる検出を困難にしています。 ・Shikitega は、正規のクラウド サービスを悪用して、一部のコマンドアンドコントロール サーバーを格納しています。	https://cybersecurity.att.com/blogs/labs-research/shikitega-new-stealthy-malware-targeting-linux	報告URL情報の最後部にIoCsが掲載されているので、点検等にご利用できる。
2022/9/6	Mirai Variant MooBot Targeting D-Link Devices	D-Linkの機器を狙うMirai亜種MooBot													1		8月上旬、Unit 42のリサーチャーは、ネットワークおよび接続製品を専門とするD-Link製のデバイスに存在する複数の脆弱性を利用した攻撃を発見しました。 侵害を受けた場合、これらの機器は完全に攻撃者のコントロール下に置かれます。攻撃者はこれらの機器を利用し、分散型サービス拒否(DDoS)攻撃などのさらなる攻撃を行えます。Unit 42のリサーチャーが捉えたエクスプロイト試行は、Linux を稼働する公開ネットワーク機器を標的とし、前述の脆弱性を悪用して、MooBotというMiraiの亜種を拡散させるものでした。D-Linkは本稿に記載した全脆弱性についてセキュリティ情報を公開していますが、パッチが適用されていないか古いバージョンのデバイスを使っているユーザーはまだ存在する可能性があります。Unit 42は可能な限りアップグレードやパッチを適用することを強く推奨します。	https://unit42.paloaltonetworks.jp/moobot-d-link-devices/	
2022/9/7	A Recent Chinese Hack Is a Wake-up Call for the Security of the World's Software Supply Chain	最近の中国のハッキングは、世界のソフトウェア サプライ チェーンのセキュリティに対する警鐘です													1		最近の報告によると、中国政府が支援するハッキング グループが悪意のあるコードを中国のメッセージング アプリ MiMi に挿入し、悪名高いSolarWinds のハッキングに相当するものを実質的に実行しました。 MiMi のユーザーには、悪意のあるコードが追加されたバージョンのアプリが提供されました。これは、攻撃者がアプリを配信したサーバーを制御したためです。つまり、これはソフトウェア サプライ チェーンへの攻撃であり、ソフトウェア デリバリー パイプラインが侵害されました。そして、何ヶ月も誰も知りませんでした。このハッキングは、西側のメディアではあまり報道されていませんが、西側の企業と政府は注意を払い、防御の準備を開始する必要があります。 これはソフトウェアサプライチェーン攻撃であり、攻撃者は世界のデジタル経済の機能に不可欠になっているソース コード、ソフトウェ ビルドシステム、またはソフトウェア公開パイプラインのいずれかを改ざんします。中国政府が支援するハッキング グループがソフトウェア サプライ チェーンへの攻撃を行っているということは、賢明な指導者は、この傾向を単なるサイバー犯罪ではなく、国家戦略の一部と見なす必要があることを意味します。この傾向は、国境を越えたデジタル取引の自由な流れを脅かし、購入者が「信頼できない」販売者からの購入をますます精査するにつれて、ソフトウェア取得のコストが増加することを意味します。	https://thediplomat.com/2022/09/a-recent-chinese-hack-is-a-wake-up-call-for-the-security-of-the-worlds-software-supply-chain/	中国発アプリに対する最近の日米政府のスタンスの差が気になります。 日本： https://prtimes.jp/main/html/rd/p/000000750.000030435.html TikTok、デジタル庁と連携のもと、マイナンバー制度の普及啓発を目的としたショートムービーを9月8日から公開 米国：https://dot.la/tiktok-key-logging-2657890141.html キーロギングの論争により、TikTok が米国政府の監視下に戻る
2022/9/7	A Recommendation To Support Research In Password-less Authentication	パスワードレス認証の研究を支援するための推奨事項	1	1								1					CyberSec4Europeは、数ヶ月の検討の結果として、パスワードレス認証の研究をサポートするための推奨事項を公開しました。強力なパスワードであっても、セキュリティを保証するのに十分ではありません。安全に(ハッシュ値などとして)保存できる場合でも、ユーザー(ソーシャルエンジニアリングなど)またはシステム(パスワードの漏えいなど)を標的とする さまざまな攻撃を受ける可能性があります。EU市民は何百ものパスワードを処理する必要があるため、簡単に推測できるパスワードを選択したり、セキュリティに深刻な影響を与えるパスワードを再利用したりする可能性があります。脆弱で時代遅れの認証方法は、個々のアカウントの侵害につながる可能性があり、権限のエスカレーションを介して、ヨーロッパの組織全体と重要なインフラストラクチャを危険にさらす可能性があります。 したがって、EUは加盟国と利害関係者に、パスワード攻撃に対抗するように設計および実装されているFIDO（Fast Identity Online）などの安全で真のパスワードレス認証ソリューションを開発および実装するよう要求する必要があります。 このアプローチでは、ユーザーは秘密を知っていることをサーバーに納得させることで、それが何であるかを明らかにすることなく、身元を証明します。そのようなアプローチの1つがFIDO2です。これは、パスワードを使用しない認証メカニズムであり、Web標準です。ここ数年で、認証への新しい実用化へのアプローチが登場しました。それは、パスワードを使用しない認証です。このアプローチでは、ユーザーは秘密を知っていることをサーバーに納得させることで、それが何であるかを明らかにすることなく、身元を証明します。	https://cybersec4europe.eu/a-recommendation-to-support-research-in-password-less-authentication/	CyberSec4Europeは、ベストプラクティスの例とパートナーの専門知識と経験を使用 して、将来の欧州サイバーセキュリティコンピテンスネットワークの潜在的なガバナンス構造を設計、テスト、実証している Horizon2020のプロジェクトです。

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源									要旨	参照先	その他特記事項
			政府・行政機関	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他標準化組織	報道機関	その他			
2022/9/12	Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities	パッチが適用されていない旧式の医療機器はサイバー攻撃の機会を提供する	1	1								1				FBIは、旧式のソフトウェアで動作するパッチ未適用の医療機器や、十分なセキュリティ機能を持たない機器がもたらす脆弱性が増加していることを確認しています。医療機器の脆弱性を悪用するサイバー脅威者は、医療施設の運営機能、患者の安全、データの機密性、およびデータの完全性に悪影響を及ぼします。医療機器の脆弱性は主に機器のハードウェア設計と機器ソフトウェアの管理に起因しています。日常的な課題としては、標準化された構成の使用、ネットワーク上の相当数の管理対象機器を含む特殊な構成、機器に組み込まれたセキュリティ機能の欠如、これらの機能のアップグレードができないことなどが挙げられます。	https://www.ic3.gov/Media/News/2022/220912.pdf	
2022/9/14	OMB: New Acquisition Rule Coming for Vendors to Vouch for Their Software Security	OMB: ベンダーがソフトウェアのセキュリティを保証するための新しい取得規則	1	1								1				連邦調達規制評議会はまもなく、米国国立標準技術研究所（NIST)のガイダンスを使用して製品が開発されたというソフトウェアベンダーからの保証を求める際に、連邦機関に統一された標準的な自己構成証明フォームを使用することを要求する規則を提案します。管理予算局が水曜日に発表したメモによると、新しい規則に沿って、「各機関は、利用可能になる予定の標準的な自己証明書を使用することが推奨される」といいます。 このメモは、少なくとも9つの連邦機関を危険にさらす侵入キャンペーンで悪用された連邦IT管理請負業者にちなんで、SolarWindsと呼ばれるハッキングに対応して2021年5月にジョー・バイデン大統領が署名した大統領令14028に基づいて発行されました。OMBのメモには、各機関がベンダーの証明書を収集し、最終的にはサイバーセキュリティおよびインフラセキュリティ庁がホワイトハウスと連携して証明書のための安全な機関間リポジトリを確立するための具体的なスケジュールが明示されています	https://www.nextgov.com/cybersecurity/2022/09/omb-new-acquisition-rule-coming-vendors-vouch-their-software-security/377140/ Memorandum本文: https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf	本Memorandumは昨年のEO 14028を根拠とし、連邦各省庁において第三者(Third Party)ソフトウエアの利用に際し、Software Supply Chain確保のために実施されるべき要領と実施期限が具体的に示されている。 個別実施要領と各要領の実施期限は、Appendix Aで一覧表として示されている。
2022/9/15	Biden Orders Deeper Scrutiny of Foreign Investment in Tech and Supply Chains	バイデン氏は、テクノロジーとサプライチェーンへの外国投資のより深い精査を命じる	1	1								1				バイデン政権は、中国や他の敵に重要な技術へのアクセスを与えたり、サプライチェーンや個人データを危険にさらす可能性のある取引の精査を強化するために、国家安全保障上のリスクについて外国投資をスクリーニングするパネルを命じています。 木曜日にバイデン大統領が署名した大統領令は、対米外国投資委員会の範囲を拡大するものではなく、むしろ、省庁間パネルの行政の優先事項への焦点を鋭くし、追加のスクリーニングに値する可能性のある取引の種類を企業に知らせることを意図している、と政権当局者は述べました。	https://www.wsj.com/articles/biden-orders-deeper-scrutiny-of-foreign-investment-in-tech-and-supply-chains-11663246802?mod=e2twp	SIP CPS関係ありませんが、最後の"personal data"は、つい最近の上院法務委員会でのTiktokのありえない証言拒否との関連あるいは影響が考えられます。
2022/9/16	Cyber security experts team up to protect UK construction projects	サイバーセキュリティの専門家が協力して英国の建設プロジェクトを保護する	1	1								1				英国の建設プロジェクトを支援するための新しいベストプラクティスガイダンスが、国家サイバーセキュリティセンター(NCSC)、ビジネス、エネルギー、産業戦略省(BEIS)、および国家インフラ保護センター(CPNI)と業界の専門家との間で共同発行されました。本ガイダンスの特徴は、以下の３点があげられています。 ・英国政府は産業界と英国のHS2（高速鉄道２）およびCrossrailなどの主要なインフラストラクチャプロジェクトでデータセキュリティを向上させるためのベストプラクティスガイダンスについて協力している。 ・GCHQ(Government Communications Headquarters)のNational Cyber Security Centreが発行した新しいアドバイスは、情報セキュリティリスクを管理するための最善の　アプローチを示している。 ・建設部門は、悪意のあるアクターによる継続的な標的にさらされることから、本ガイダンスに従うよう促されている。 　HS2などの主要な建築プロジェクトに協力している建設会社は、業界と政府から、これまでにないセキュリティに関するアドバイスを提供されます。 このガイドは、ジョイントベンチャー（JV）プロジェクトで作成、保存、共有するデータを安全に処理する方法について個別のアドバイスを提供することにより、これらの企業が機密データを攻撃者から安全に保つのを支援することを目的としています。HS2やCrossrailなどの主要なインフラストラクチャ契約を含む合弁事業の経験を持つ企業からの情報が含まれており、これらの契約は、通常、規模が大きく、価値があり、複雑であるため、情報セキュリティリスクが特に関連しています。推奨される手順に従うことで、企業は物理的、人的、およびサイバーセキュリティを改善し、ランサムウェアを含む脅威が世界的に重大な問題を引き起こし続けているため、悪意のある攻撃者にとって魅力的な標的とならないようにすることができます。	https://www.ncsc.gov.uk/news/joint-ventures-construction-guidance	
2022/9/16		中間報告													1	米国足立氏による海外動向調査中間報告		
2022/9/19	European Cybersecurity Skills Framework (ECSF) - User Manual	欧州サイバーセキュリティスキルフレームワーク(ECSF)-ユーザーマニュアル	1	1						1						ENISAではサイバーセキュリティの労働力不足とスキルギャップを調査し、サイバーセキュリティの役割とスキルを定義するための包括的なアプローチがヨーロッパにおいて必要であることを確認しました。そこで、ENISAは、フレームワークの開発に取り組み、ヨーロッパのサイバーセキュリティスキルフレームワーク(ECSF: European Cybersecurity Skills Framework)を発表しました。ECSFは、ヨーロッパのサイバーセキュリティ専門家の役割に関連するタスク、能力、スキル、および知識の特定と明確化をサポートする実用的なツールを提供します。このフレームワークの主な目的は、EU加盟国の個人、雇用主、学習プログラムの提供者の間で共通の理解を作り、サイバーセキュリティの専門職の職場と学習環境の間のギャップを埋める貴重なツールとすることです。 このフレームワークでは、12の典型的なサイバーセキュリティ専門家のロールプロファイルのセットを定義し、専門的なサイバーセキュリティ部門の最も重要な要件を説明しています。これらのロールプロファイルは、専門的なサイバーセキュリティのコンテキストで必要な主要なサイバーセキュリティの使命、タスク、およびスキルの共通の理解を提供し、サイバーセキュリティの専門家が必要とするスキルと知識をプロファイリングするためのリファレンスとなります。 さらにこのフレームワークは、詳細なサイバーセキュリティの考察を提供するのに十分なほど理解しやすく包括的であると同時に、各ユーザーのニーズに基づいてカスタマイズできるように柔軟に設計されています。すべての利害関係者の視点を組み込むことにより、フレームワークはあらゆるタイプの組織に適用でき、すべてのサイバーセキュリティ専門家の育成をサポートします。	https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf	

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源									要旨	参照先	その他特記事項
			政府機関・行政	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他組織化	その他標準	報道機関	その他			
2022/9/20	Open IIOT Podcast COMING SOON! 'Industry 4.0 and Beyond'	Open IIOT Podcast 「インダストリー4.0とその先」														1	Open IIOTのチームが、インダストリー4.0を実現できるよう、専門用語に切り込みます。 この唯一無二のポッドキャストは、製造業のスケールアップに必要な「SMARTS」を手に入れるのに役立ちます。 インダストリー4.0について多くのことが語られていますが、おそらく十分なアクションはありません。 私たちの全く新しいポッドキャストでは、製造業の足かせとなっているものと、それを克服するための実践的なアドバイスについて、内部事情を紹介します。15分間のポッドキャストで、実際のインダストリー4アプリケーションや導入のヒントに関する情報を得ることができます。 Open IIOTは、ビジネスを製造業の未来へと導き、企業がノイズを切り抜けて実際の実装に取り掛かるのを支援します。インダストリー4.0とその先へ」のポッドキャストをお聞きください。 初回の放送は日本時間で明日21日（水）10:00AMに開始予定です。	https://openiiot.com.au/open-iiot-podcast/	
2022/9/20	2022 State of Public Cloud Security Report	2022年版パブリッククラウドセキュリティの現状報告														1	Cloud SecurityPlatformを提供するOrca Security社からPubric Cloud Securityに関するレポート。 本レポートでは、パブリッククラウドのセキュリティに関するさまざまな分野を評価し、現在のセキュリティ状況を明らかにすることで、企業が最も重要なセキュリティギャップがどこにあるのかをよりよく理解できるようにします。さらに、クラウドのセキュリティ体制を大幅に改善するために、どのような対応が必要であるかについても提言しています。 今年の調査では、多くの企業がクラウドセキュリティをITの最優先事項の1つに挙げている一方で、基本的なセキュリティ対策が遵守されていないケースが多いことが明らかになりました。クラウドへのリソース移行を急ぐあまり、企業は、拡大し続けるクラウドの攻撃表面や複雑化するマルチクラウドへの対応に苦慮しています。サイバーセキュリティのスキルを持つ人材が不足している現状は、さらに状況を悪化させています。	https://orca.security/wp-content/uploads/2022/09/2022-State-of-Public-Cloud-Security-Report.pdf	
2022/9/20	NISTIR 8425 Profile of the IoT Core Baseline for Consumer IoT Products	NISTIR 8425 コンシューマ IoT 製品の IoT コア ベースラインのプロファイル		1				1									本報告書は、NIST の IoT コア ベースラインの消費者プロファイルを文書化し、消費者向け IoT セクター (つまり、家庭用または個人用の IoT 製品) に一般的に必要とされるサイバーセキュリティ機能を特定します。また、中小企業が IoT 製品の購入を検討する際の出発点にもなります。消費者プロファイルは、行政命令 14028 に対する NIST の対応の一環として開発され、最初は消費者向けモノのインターネット (IoT) 製品のサイバーセキュリティラベル付けの推奨基準で公開されました。消費者プロファイル機能は、IoT 製品全体に適用されることを意図したサイバーセキュリティの成果として表現されています。このドキュメントでは、推奨される消費者プロファイルと関連する考慮事項を作成するための基礎についても説明します。	https://csrc.nist.gov/publications/detail/nistir/8425/final	
2022/9/20	NISTIR 8431 Workshop Summary Report for “Building on the NIST Foundations: Next Steps in IoT Cybersecurity”	「NIST 基盤の構築: IoT サイバーセキュリティの次のステップ」のワークショップ概要レポート		1				1									本報告書は、2022年6月に開催された仮想ワークショップにおいて、IoT製品のサイバーセキュリティ基準に関するNIST Cybersecurity for the Internet of Things（IoT）プログラムの作業について寄せられたフィードバックをまとめたものです。このワークショップの目的は、IoT製品のサイバーセキュリティに関する具体的な検討事項とその検討事項に対処するための技術についてフィードバックを得ることでした。これらの考慮事項は、民生用IoT製品分野や産業用IoT分野を含むIoT製品分野に広く適用可能です。消費者向けIoTについては、Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products に示された基準を、NIST IR 8425：Profile of the IoT Core Baseline for Consumer IoT Products に移行するにあたってこれらの検討事項が生まれ、さらにワークショップ前に発表したIoTにおけるリスク識別の複雑性に関する討議文書も併せて発表されました。	https://csrc.nist.gov/publications/detail/nistir/8431/final	
2022/9/20	Jumping NAT to Shut Down Electric Devices	電気機器をシャットダウンするためのNATのジャンプ		1											1		Team82は、同社のインテリジェント配電ユニット製品であるDataprobeのiBoot-PDUの複数の脆弱性を発見し、開示しました。iBoot-PDUは、Webベースのインタフェースを介して任意の場所から管理できます。インターネットに直接接続されていないデバイスは、Dataprobeのクラウドベースのプラットフォームを介して管理することもできます。 Team82によって発見された脆弱性の一部は、iBoot-PDU上で認証されていないリモートコードの実行につながる可能性があります。Team82 は、クラウドに接続された iBoot-PDU デバイスを列挙できる手段も開発し、利用可能な攻撃対象領域を接続されているすべてのデバイスに拡大しました。攻撃者は、デバイスへの直接 Web 接続またはクラウドを介して、これらの脆弱性をリモートから悪用する可能性があります。Dataprobeは、新しいバージョンのアップデートでこれらの脆弱性に対処しました。ユーザーは、バージョン1.42.06162022 に更新することをお勧めします。Dataprobe では、これらの脆弱性の一部に対する軽減策として、SNMP、telnet、および HTTP が使用されていない場合は無効にすることも推奨します。	https://claroty.com/team82/research/jumping-nat-to-shut-down-electric-devices https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	概要の最後の項目に示されているように、これらの機器には（ラック搭載用のかなり高度な仕様が期待される機体にもかかわらず）telnetやhttpを利用という、consumer IoT並みの仕様も散見されるようですので、その点を含めた点検が必要かと思われます。
2022/9/21	Tarfile: Exploiting the World With a 15-Year-Old Vulnerability	Tarfile: 15 年前の脆弱性で世界を悪用する		1											1		Pythonオープンソースプログラミング言語の15年前の欠陥は、多くの場所でパッチが当てられていないままであり、世界中の何十万ものオープンソースプロジェクトとクローズドソースプロジェクトの両方にその道を進んでいます。これは、ほとんどの影響を受ける組織が気づいていない、広く脆弱なソフトウェアサプライチェーンを誤って作成している、と研究者は警告した。 Trellix Advanced Research Centerによると、CVE-2007-4559として追跡されたパストラバーサル関連の脆弱性は、現在350,000以上のユニークなオープンソースリポジトリでパッチが適用されていないため、ソフトウェアアプリケーションが悪用に対して脆弱であることがわかりました。 9月21日に公開されたブログ記事で、主任エンジニアで脆弱性研究ディレクターのDouglas McKee氏は、問題のコードベースは、主にソフトウェア開発、人工知能/機械学習、コード開発など、セキュリティ、IT管理、メディアなどの多様な分野を含む膨大な数の業界にまたがるソフトウェアに存在すると述べました。	https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/tarfile-exploiting-the-world.html https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/open-source-intelligence.html https://www.darkreading.com/application-security/15-year-old-python-flaw-software-worldwide	

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源								要旨	参照先	その他特記事項
			政府・行政機関	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他標準化組織	報道機関	その他			
2022/9/21	Senators introduce a bill to protect open-source software	上院議員がオープンソース ソフトウェアを保護するための法案を提出	1											1		研究者が昨年、ユビキタスなオープンソースの log4j システムに数億台のデバイスに影響を与える可能性のある脆弱性を発見したとき、行政機関はすぐに行動に移し、主要なテクノロジー企業はホワイトハウスに集まりました。 現在、上院国土安全保障および政府問題委員会の指導者たちはサイバーセキュリティ202 によって最初に報告された、オープンソース ソフトウェアを保護するのに役立つ法律を導入しています。議長のGary Peters (民主党、ミシガン州) と最高位の共和党の Rob Portman (オハイオ州) は、次のことを計画しています。彼らが共催している法案について、来週投票を行います。 Peters/Portman の法律は、サイバーセキュリティおよびインフラストラクチャ セキュリティ エージェンシーに、オープンソース ソフトウェアに依存するシステムのリスクを評価して軽減する方法を開発するよう指示するものです。その後、CISA は、そのフレームワークを重要なインフラストラクチャに適用する方法を研究することになります。Log4Shellがまだリスクをもたらさないというわけではありません。7月、連邦政府のサイバー安全審査委員会は、log4jのバグを「風土病」と呼び、何十年にもわたって危険をもたらすと述べた。また、下院エネルギー・商業委員会の委員は、8月に各機関がこの脆弱性にどのように対処しているか、最新情報の提供を求めた。国土安全保障省のロバート・シルヴァーズ政策担当次官はこの夏、「Log4jは史上最も深刻なソフトウェアの脆弱性の一つである」と述べた。	https://www.washingtonpost.com/politics/2022/09/22/senators-introduce-bill-protect-open-source-software/	Log4Shellは今のところ既知の広範な被害をもたらしていない"との記述があるが油断できないと認識する必要がある。
2022/9/24	How Europe Is Using Regulations to Harden Medical Devices Against Attack	ヨーロッパが規制を利用して医療機器を攻撃に対して強化する方法	1	1										1		医療機器のサイバーセキュリティ リスクに対する懸念が高まっているため、欧州連合の規制当局は、サイバー インシデントの結果として患者が被害を受けるリスクを軽減し国民の医療制度を守るために、医療機器および体外診断用医療機器に対する一連の新しい市場参入要件を提案しました。EU 規制当局は、2021年5月26日に施行された欧州連合医療機器規則(MDR) および欧州連合体外診断規則(IVDR) により、サイバーセキュリティ要件の基準を引き上げています。透明性があり、予測可能で持続可能な規制の枠組み、イノベーションをサポートしながら高いレベルの安全と健康を保証します。 組織は、2024年5月26日まで、または現在の市場認定の有効期限が切れるまでに、新しい要件に準拠するために品質管理システムと技術文書に必要な変更を加える必要があります。多数の評価プロセス、基準、およびガイダンスドキュメントが提供されているにもかかわらず、医療機器メーカー、プロバイダー、および認証サービスの準備が間に合わない場合があります。現在有効な AIMDD/MDD 証明書の 90% 以上が 2024 年までに期限切れになるため、市場に参入する新しいデバイスに加えて、かなりの数の既存のデバイスを再承認する必要があります。現在市場に出回っている製品の 85% は、依然として MDR.IVDR に基づいた新しい認証を必要としていると推定されています。このプロセスには13～18か月かかることを考慮すると、企業は 2024 年の期限に間に合わせるために、今すぐプロセスを開始する必要があります。	https://www.darkreading.com/edge-articles/how-europe-is-using-regulations-to-harden-medical-devices-against-attack	
2022/9/26	ICS Cybersecurity Conference														1	SecurityWeekが毎年開催していたICS Cybersecurity Conferenceが、今年は会場開催で復活する。（Atlantaにて開催） 開催は2022/10/26-28を予定している。	https://www.icscybersecurityconference.com Agenda: https://ics2021.sched.com	
2022/9/27	What the Securing Open Source Software Act does and what it misses	Securing Open Source Software Act が何を行い、何を見逃しているか	1											1		米国上院で共和党と民主党の超党派がオープンソース ソフトウェアの安全性を高めるための法案を提出しました。この法案は、米国政府がオープンソースソフトウェアのセキュリティ脆弱性を予測して軽減し、最も機密性の高いデータを保護することを保証するものです。 2021 年のLog4j セキュリティの大規模な爆発とその継続的な余震により、オープンソース コード攻撃に対して私たちがいかに脆弱であるかが示されました。Securing Open Source Software Act は、オープン ソースを政策と規制の決定の領域から連邦法に移行させます。この法案は、オープンソース コードが連邦政府によってどのように使用されているかを評価するためのリスク フレームワークを開発するよう CISA に指示します。CISA は、重要なインフラストラクチャの所有者と運用者が同じフレームワークをどのように使用できるかについても決定します。Open Source Security Foundation (OpenSSF) による法律の分析によると、「CISA は、オープンソース コードのリスクを処理するための初期評価フレームワークを作成し、政府、業界、およびオープンソース コミュニティのフレームワークとソフトウェアのベスト プラクティスを取り入れます。要するに、CISA は車輪の再発明を試みるのではなく、既存のオープンソース セキュリティ技術の最良のものを使用します。これは、開発者が「アプリケーションごとに SBOM [ソフトウェア部品表] を購入者に提供する必要がある」と述べた、ジョセフ・バイデン大統領の国のサイバーセキュリティの改善に関する大統領令の足跡をたどってい ます。	https://www.zdnet.com/article/whats-what-in-the-united-states-securing-open-source-software-act/	審議が始まったところなので、これからどうなるかはわからないが、超党派の議員提案なので、内容が固まったら採決の可能性は高いと思われる。
2022/9/30	Supply Chain Attack via a Trojanized Comm100 Chat Installer	トロイの木馬化したComm100 チャットインストーラーを介したサプライチェーンへの攻撃													1	CrowdStrike社の解析チームは、同社の顧客エンゲージメントプラットフォームのインストール中に新しいサプライチェーン攻撃を特定し、展開中のComm100ライブチャットアプリケーションのトロイの木馬化されたインストーラが関与していることを確認しました。 このサプライチェーン攻撃で配信されるペイロードは、アジアのオンラインギャンブル事業体を標的とした、同じアクターに関連する以前のインシデントで特定されたペイロードとは異なります。さらに、最近の活動は、Comm100のウェブサイトを介してトロイの木馬化されたアプリを提供するターゲットスコープとサプライチェーン攻撃メカニズムの両方で、オンラインギャンブルを標的とした活動とは異なります。さらに、CrowdStrike Intelligenceは、このアクターが中国のつながりを持っている可能性が高いと適度な自信を持って評価しています。この評価は、マルウェアにおける中国語のコメントの存在、前述の戦術、技術、手順 (TTP)、および東アジアおよび東南アジアのオンラインギャンブルエンティティのターゲットとの関連性に基づいています。	https://www.crowdstrike.com/blog/new-supply-chain-attack-leverages-comm100-chat-installer/	Crowdstrike社は中国に由来する攻撃と予測していますが、これが事実であれば、 ロシアGRU（軍事情報機関）由来の攻撃とされるSolarwindsに続き、中国も同様の攻撃を行っている現実的な可能性が増します。

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源								要旨	参照先	その他特記事項
			政府・行政機関	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他の組織化	その他標準	報道機関	その他			
2022/10/4	Securing Developer Tools: A New Supply Chain Attack on PHP	開発者ツールのセキュリティ保護:PHPに対する新しいサプライチェーン攻撃														1	サプライチェーン攻撃は、今日の開発組織にとってホットなトピックです。昨年、過去最大のソフトウェアサプライチェーン攻撃で、バックドアが18,000人のSolarWinds顧客に感染しました。 今年初め、Sonar社は、PHPサプライチェーンの中心的なコンポーネントであるPackagistの重大な脆弱性を発見しました。この脆弱性により、Packagistの制御が可能になります。これは、PHP パッケージマネージャ Composer が、開発者がプロジェクトに含めたソフトウェアの依存関係を判別してダウンロードするために使用されます。セキュリティ研究者は、この新しいサプライチェーン攻撃技術を使用して、Apple、Microsoft、PayPal、およびその他の技術大手を侵害することができました。これらの攻撃によって悪用される根本的な設計は、現代のすべてのソフトウェアが他のサードパーティ製ソフトウェアコンポーネントの上に構築されており、多くの場合、ダウンロードされたすべてのパッケージの明確な可視性がないことです。また、多くのコンポーネントを再利用することで開発プロセスをスピードアップできますが、サプライチェーンに感染することは、一度に多くの組織を危険にさらす非常に効果的で微妙な攻撃ベクトルです。 PHPコードを実行している事実上すべての組織は、毎月20億のソフトウェアパッケージを提供するComposerを使用しています。これらの要求のうち 1 億件以上がハイジャックされ、悪意のある依存関係を配布し、何百万ものサーバーを侵害している可能性があります。	https://blog.sonarsource.com/securing-developer-tools-a-new-supply-chain-attack-on-php/	当該脆弱性を悪用した攻撃は現在まで検知されていませんが、脆弱性の性質は、 大規模なSoftware Supply Chain security上の懸案に加え、log4shell以降連邦政府の優先度が高いOpen Source Security上の懸念という、二つの優先度の高い懸念への警戒を裏付ける事例となります。
2022/10/6	NSA, CISA, FBI Joint Alert：Top CVEs Actively Exploited By People's Republic of China State-Sponsored Cyber Actors	警告 (AA22-279A)：中華人民共和国政府が支援するサイバー攻撃者によって積極的に悪用された上位の CVE	1	1					1								この合同サイバーセキュリティ勧告（CSA）は、NSA、CISA、FBIが評価した、中華人民共和国（PRC）の国家支援型サイバー行為者が2020年から使用している上位の共通脆弱性情報（CVE）を提供するものである。 中国政府が支援するサイバー攻撃者は、既知の脆弱性を引き続き悪用して、米国および同盟国のネットワーク、ならびにソフトウェアおよびハードウェア企業を積極的に標的にし、知的財産を盗み、機密ネットワークへのアクセスを進めています。この共同 CSA は、これまでの NSA、CISA、FBI の報告を基に、連邦政府および州、地方、部族、領土 (SLTT) 政府、防衛産業基盤セクターを含む重要インフラ、民間組織に、注目すべき傾向や持続的な戦術、技術、手順 (TTPs) についての情報を提供するものです。NSA、CISA、FBI は、米国および同盟国の政府、重要インフラ、民間組織が、防御態勢を強化し、PRC が支援する悪質なサイバーアクターからの侵害の脅威を軽減するため、緩和策のセクションおよび付録 A に記載された推奨事項を適用するよう促します。中国がスポンサーとなっている悪質なサイバー行為に関する詳細については、CISAのChina Cyber Threat Overview and Advisories webpage、FBIのIndustry Alerts、NSAのCybersecurity Advisories & Guidanceを参照してください。	https://www.cisa.gov/uscert/ncas/alerts/aa22-279a	Apache Log4j 脆弱性 CVE-2021-44228 (aka Log4Shell)が最上位に示されており、少なくとも本Alert発行三機関が最初に載せたかったもの、最も警戒を呼びかけているものと推測できます。
2022/10/7	ETSI flagship event Security Conference attracts nearly 200 attendees onsite	ETSIフラッグシップイベントセキュリティカンファレンスには、オンサイトで約200人の参加者が集まります	1	1							1						ETSIのセキュリティカンファレンス2022に27か国より約200名が参加しました。 3日間のプログラムでは、欧州委員会、政府代表者、その他の標準化団体、さまざまな業界セクターから講演者が集まり、世界的な規制と認証の展望、セキュリティの垂直方向、技術の水平方向、およびツールボックスについて議論されました。 専門家は、技術がサイバー脅威と同じ速さで進化する必要があるサイバーセキュリティに固有の課題を概観し、標準はこの絶え間なく変化する環境を予測して適応します。 デモンストレーションとポスターにおいては、AI、消費者向けIoTデバイス、クラウドエコシステムでのアクセス制御のための暗号化、インテリジェントトランスポートシステムのセキュリティ保護など、さまざまな分野向けのETSI標準の商用実装を強調しました。 研究プロジェクトと概念実証においては、ゼロタッチ管理システム※、5Gネットワークスライス、スマートシティ、または医療機器に関する標準化前の作業が紹介されました。	https://www.etsi.org/newsroom/news/2126-2022-10-etsi-flagship-event-security-conference-attracts-nearly-200-attendees-onsite	
2022/10/11	FACT SHEET: Biden-Harris Administration Delivers on Strengthening America's Cybersecurity	バイデン-ハリス政権、米国のサイバーセキュリティ強化で成果を挙げる	1	1								1					バイデン-ハリス政権は、米国のサイバー防御の改善に絶え間ない焦点を当て、「デジタルドアをロックする」ための包括的なアプローチを構築し、米国のサイバーセキュリティを強化し保護するために積極的な行動を起こしています。 以下に、サイバーセキュリティ強化の成果として挙げられた項目を示します。 ●重要インフラのサイバーセキュリティを向上させる。 ●新しいインフラはスマートで安全であることを保証する。 ●連邦政府のサイバーセキュリティ要件を強化し、政府の購買力によりハードルを上げる。 ●ランサムウェア攻撃への対策で、米国人のオンラインを守る。 ●より安全なサイバースペースを実現するための同盟国やパートナーとの協働。 ●悪意のある行為者にコストを課し、我々の安全保障を強化する。 ●国際的に認められたサイバー規範を実施すること。 ●デバイスが安全であることを米国人が認識できるようにするための新しいラベルを開発する。 ●国のサイバー人材育成とサイバー教育の強化。 ●量子抵抗性暗号の開発により、オンライン商取引から国家機密まで、未来を守る。 ●国家量子イニシアティブと、脆弱な暗号システムに対するリスクを軽減しつつ量子コンピューティングに おける米国のリーダーシップを促進するための国家安全保障メモランダム 10（NSM-10）を通じて、技術的な優位性を開発している。	https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/11/fact-sheet-biden-harris-administration-delivers-on-strengthening-americas-cybersecurity/	中間選挙に向けた政権の成果のアピールの一環と思われる。

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源								要旨	参照先	その他特記事項
			政府・行政機関	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他標準化組織	報道機関	その他			
2022/10/11	White House to unveil ambitious cybersecurity labeling effort modeled after Energy Star	ホワイトハウスは、Energy Starをモデルにした野心的なサイバーセキュリティラベル付けの取り組みを発表	1	1								1		1		ホワイトハウスの国家安全保障会議は、インターネットに接続されたデバイスのデジタル保護を改善することを目的とした消費者製品のサイバーセキュリティラベルプログラムの計画を火曜日に発表すると、ホワイトハウスの高官は語った。 消費者製品協会、製造会社、技術系シンクタンクから約 50 名の代表者が10月19日にホワイトハウスに集まり、2023 年春に予定されている発売に先立ち、自発的な取り組みに関するワークショップを開催します。 ホワイトハウスは、さまざまなサイバーセキュリティイニシアチブを概説する火曜にリリースした文書で、この取り組みについて簡単に説明しました。行政は、いわゆるモノのインターネットデバイスの使用に関連するリスクを伝えるラベルの基礎として製造業者が使用できる、3 つまたは 4 つのサイバーセキュリティ標準を推奨することから始める予定です。 検討中の基準は、メーカーがソフトウェアの脆弱性に対するパッチを展開する頻度や、デバイスがパスワードなしでインターネットに接続するかどうかに基づいて、製品を評価する可能性があると当局者は述べています。企業の主張を誰が検証するのかはまだ明らかではない。ホワイトハウスは、このプログラムがサイバーセキュリティに投資する企業に報いると同時に、消費者がより安全な製品を見つけるのを助けることを望んでいます.米国サイバーセキュリティ・ソラリウム委員会（CSC)は、最終報告書で、ソフトウェア、デバイス、産業用制御システムを含む「情報通信技術の自主的なサイバーセキュリティ認証およびラベル付けプログラムの確立と管理」を任務とする非営利の国家サイバーセキュリティ認証およびラベル付け機関を議会に創設するよう勧告しました.	https://www.cyberscoop.com/white-house-to-unveil-internet-of-things-labeling/ https://www.cybersecuritydive.com/news/white-house-energy-star-rating-iot/633933/	
2022/10/12	NCSC issues fresh guidance following recent rise in supply chain cyber attacks	サプライチェーンのサイバー攻撃が最近増加したことを受けて、NCSC が新たなガイダンスを発行	1	1								1				GCHQ の一部である National Cyber Security Center (NCSC) は、組織がサプライ チェーンのサイバー セキュリティを効果的に評価し、信頼を得るのに役立つ新しいガイダンスを本日 発行しました。これは、SolarWinds 攻撃などの注目を集めるインシデントを含む、近年のサプライ チェーン内の脆弱性に起因するサイバー攻撃の大幅な増加に続くものです。新しいガイダンスは、中規模および大規模の組織がサプライヤーと協力することのサイバーリスクを効果的に評価し、軽減策が実施されているという保証を得るのに役立つように設計されています.サプライチェーンへの攻撃は、広範囲に及ぶ費用のかかる混乱を引き起こす可能性がありますが、最新の政府データによると、10分の1以上の企業が直接のサプライヤーがもたらすリスクを見直しており (13%)、サプライチェーン全体の割合はわずか7% です。このガイダンスは、金融セクターの運用回復力の向上を支援する Cross Market Operational Resilience Group (CMORG) と連携して発行されていますが、アドバイスはあらゆるセクターの組織を対象としています。これは、サイバー セキュリティの専門家、リスク管理者、調達の専門家が NCSCの12 のサプライ チェーン セキュリティ原則を実践するのを支援することを目的としており、さらなるアドバイスの必要性を強調した昨年の意見募集に対する政府の対応に従います。典型的なサプライヤーとの関係と、サプライ チェーンを攻撃にさらす可能性のある潜在的な弱点について説明し、予想される結果を定義し、組織がサプライ チェーンのセキュリティを評価するのに役立つ重要な手順を示します。	https://www.ncsc.gov.uk/news/ncsc-issues-fresh-guidance-following-recent-rise-in-supply-chain-cyber-attacks https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security https://www.ncsc.gov.uk/files/Assess-supply-chain-cyber-security.pdf	各組織において対処すべき点と、期待される成果（outcome)は体系的に示されているが、「何をしたらいいか」という答えが書かれた文書ではない。例えば、最初の頁の1. Before You start, 2. Devvelop an approach to assesss…などの各項は、 それぞれの組織でできている部分とできていないところ、など、かなり差があると思われるが、そのようなgap analysisや点検、 抜本的な対策を行うのには役立つと考えられる。
2022/10/17	Export controls aim to deprive China of equipment and software it needs to manufacture high-end chips with military applications	輸出規制は、軍事用途のハイエンドチップを製造するために必要な機器とソフトウェアを中国から奪うことを目的としている	1	1								1				西側のサプライヤーは、米国の新たな輸出規制に対応して、一部の中国の半導体メーカーとの関係を断ち始めている。これは、バイデン政権が中国の軍事開発を妨害するよう命じている部分的な技術分離の別の兆候である.チップ製造装置の大手サプライヤーである ASML は、米国の従業員に対し、新しい規則を整理している間は、中国のチップ工場での装置の設置や修理を中止するように言いました。別の機器プロバイダーであるアプライド マテリアルズは、輸出制限により、第4四半期に約 4 億ドルの売上が達成できないと述べています。欧米企業は、米国による新たな規制の直後に輸出を全面的に停止し、ルールを解読してから再開するのが一般的だと弁護士は言う。しかし、国家安全保障の専門家によると、中国が高度なチップを生産するのを阻止することを目的とした新しい規制は、米国が制定した中で最も厳しいものの 1 つです。 米国人は中国の半導体産業で重要な役職に就いており、メーカーが外国のライバルに追いつくための半導体開発に貢献している。ところが、中国の最先端の半導体開発を米国人が支援することを禁じる新たな輸出規制を米国が打ち出したため、こうした米国人幹部の立場が中ぶらりんになっている。上場している中国半導体企業の上級幹部のうち、少なくとも43人が米国人である。各社の当局への提出書類や公式ウェブサイトでウォール・ストリート・ジャーナルが確認した。その多くは最高経営責任者（CEO）や副社長、会長といった経営幹部に就いている。米国人幹部のほぼ全員が、シリコンバレーで米国の半導体メーカーや半導体製造装置メーカーに勤めた後、中国の同業界に移っていることが、各社の提出書類で分かった。こうした経歴は、かつて人材が国境を越えて企業間で自由に行き来していた事実を反映している。中国政府が2008年に始めた人材招致プロジェクト「千人計画」などを通じて、中国に渡った米国人もいる。	https://www.washingtonpost.com/technology/2022/10/17/export-controls-us-china-chips/ https://jp.wsj.com/articles/american-executives-in-limbo-at-chinese-chip-companies-after-u-s-ban-11666064496?mod=djem_Japandaily_t	
2022/10/17	ETSI IoT week highlights how ICT standards can help sustainability	ETSI IoTウィークは、ICT標準が持続可能性にどのように役立つかを強調しています	1	1							1					ETSIは「デジタルおよびグリーントランスフォーメーションの追求」に焦点を当てた2022 ETSI IoT Weekイベントを主催しました。　IoTセキュリティに関して、2つのセッションで7件の発表がありました。産業界、研究、大学、都市、その他の標準化団体(SDO)から52人の講演者が、具体的な例を挙げて、ICT標準が国連の持続可能な開発目標(SDG)と欧州のグリーンディールを達成するのにどのように役立つかを、世界22か国の聴衆に向けて実演しました。 セッションでは、セマンティクスとオントロジー、デジタルツイン、IoTとエッジ、IoTとAI、より良い生活のためのIoT(デジタルおよびグリーントランスフォーメーションとeHealthを含む)、および垂直ビジネスセクター向けの水平ETSI IoT標準が取り上げられました。初日には、IoTアプリケーション開発者を対象としたチュートリアルセッションが行われ、オントロジーとは何か、およびオントロジーがどのように構築および拡張されるかを学ぶ機会となりました。 　この会議は、聴衆と意見を交換し、特にeHealthにおけるAIの倫理などの課題を指摘するためのいくつかのパネルセッションで構成されました。エンジニアはAIのアルゴリズムの作業を開始する際に倫理について考えるべきであることが強調されました。この問題に対処するために、Securing AI ETSIグループが作成されました。	https://www.etsi.org/newsroom/news/2132-2022-10-etsi-iot-week-highlights-how-ict-standards-can-help-sustainability?jjj=1666240072133	

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源									要旨	参照先	その他特記事項
			政府機関・行政	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他組織化	その他標準	報道機関	その他			
2022/10/17	Review And Reflections On Maritime Transport	海上輸送に関するレビューと考察			1							1					CyberSecurity for EuropeのプロジェクトのWP5内およびWP3が連携して、海事セクターを対象としたさまざまなサイバーセキュリティサービスを統合、拡張、展開しました。公開されたドキュメントには基盤となるセキュリティサービスの統合の結果が示されています。 海上輸送は国際貿易の主要な促進要因の1つであるため、海上インフラとサービスは欧州の重要インフラの一部と見なされています。海上インフラとサービスには、自動識別システム(AIS)、VHFデータ交換システム(VDES)、監視制御およびデータ取得(SCADA)システム、ポートコミュニティシステム(PCS)、ターミナルオペレーティングシステム(TOS)、船舶交通サービス、船舶情報システム(SIS)、電子海図表示情報システム(ECDIS)などがあります。 海上輸送で利用される主な資産には、港湾インフラと船舶が含まれます。船舶は、海上輸送業務を行うための海上輸送手段です。現在、自律型船舶は、人間の介入が制限されているか、まったくなくても、航行可能な水域では貨物を輸送できます。海上輸送のデジタル化により、基礎となるプロセスの複雑さと必要なコラボレーションが増加するため、関連する資産間の（相互）依存関係とサイバー物理的相互作用が増加しています。	https://cybersec4europe.eu/review-and-reflections-on-maritime-transport/	
2022/10/20	National cybersecurity strategy to debut within months, White House official says	ホワイトハウス当局者によると、国家サイバーセキュリティ戦略は数か月以内に登場する													1		・ナショナル サイバー ディレクターの Chris Inglis 氏は、バイデン政権が長年待ち望んでいた国家サイバーセキュリティ戦略は、早ければ 11 月下旬には準備が整う可能性があるが、最終的な完成までにはさらに数か月かかる可能性がある。 ・Inglis 氏は水曜日にワシントンDCで開催された mWISE カンファレンスで講演し、この戦略は国際的なサイバーセキュリティの問題と、情報セキュリティ業界の主要な問題である労働力開発の懸念に重点を置いていると述べました。 ・当局は、戦略の策定に関して民間部門にかなりの働きかけを行っており、約300件の関与の3分の2が民間業界の当局者と行われています。 Inglis氏は、Mandiantの CEO である Kevin Mandia との基調講演で、情報セキュリティ分野におけるセキュリティ戦略とその他の差し迫った問題について概説しました。 国家のサイバーセキュリティ戦略を正しく遂行するためには、サイバーセキュリティを社会の適切な場所に配置する必要がある、とInglis氏は述べた。また、サイバーや IT を肩書に持つ人々をはるかに超えて、はるかに幅広い人々のニーズと懸念に対処します。 Inglis 氏は、サイバーセキュリティ戦略を機能させるには、協力して防御可能な企業を構築することが重要になると述べました。 Inglis氏は特に、Colonial Pipeline 攻撃に言及しました。この攻撃は、燃料供給の技術または重要な機能を攻撃することを目的としていた可能性があります。しかし、Inglis 氏は、Colonialの攻撃や、それを好む他の人々を、国民の信頼に対する攻撃と見なしています。	https://www.cybersecuritydive.com/news/us-cyber-strategy-chris-inglis/634585/	
2022/10/20	Statement by NSC Spokesperson Adrienne Watson on the Biden-Harris Administration's Effort to Secure Household Internet-Enabled Devices	家庭用インターネット接続機器の安全性に関するバイデン-ハリス政権の取り組みに関するNSC報道官Adrienne Watsonの声明	1	1								1					昨日、ホワイトハウスは、民間企業、学術機関、米国政府のリーダーを招集し、IoTデバイスに対する国家レベルのサイバーセキュリティ・ラベリングプログラムを推進することを発表しました。バイデン＝ハリス政権は、米国のサイバーセキュリティを強化することを優先事項としており、その取り組みの重要な部分は、ベビーモニターやスマート家電など、米国の一般家庭で当たり前に使われるようになった機器をサイバー脅威から確実に保護することです。このような機器を保護するためのラベル付けプログラムは、米国の消費者に、家庭に持ち込まれる技術が安全であるという安心感を与え、メーカーがより高いサイバーセキュリティ基準を満たし、小売業者が安全な機器を販売する動機付けとなります。 昨日の対話では、国家的なサイバーセキュリティ標識プログラムを実施し、インターネット対応機器のセキュリティ基準を向上させ、世界的に認知されるラベルを作成する最善の方法について話し合われました。政府と業界のリーダーは、消費者がより多くの情報を得た上でサイバーセキュリティを選択できるよう、機器に簡単に認識できるラベルを付けることによって、インターネットに接続する消費者向け機器全体のセキュリティを向上させる信頼できるプログラムの重要性について議論しました。これらの対話は、より安全なインターネット接続機器の構築を支援するために、民間部門と米国標準技術局（NIST）が先駆けて行ってきた基礎的な作業の上に築かれるものです。また、バイデン大統領による「国家のサイバーセキュリティの改善に関する大統領令」を受け、IoTセキュリティの改善の必要性を強調し、NISTが連邦取引委員会と連携して、これらの機器のサイバーセキュリティ基準の改善と製品ラベルの標準化を推進することを命じたものでもあります。 昨日の議論を踏まえ、ホワイトハウスは、2023年春の目標展開に向け、国家サイバーセキュリティラベルプログラムの開発を進めていきます。	https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/20/statement-by-nsc-spokesperson-adrienne-watson-on-the-biden-harris-administrations-effort-to-secure-household-internet-enabled-devices/ https://www.cyberscoop.com/white-house-iot-labeling-program/	
2022/10/24	Uncovering Security Blind Spots in CNC Machines	CNCマシンのセキュリティ盲点の発見		1												1	Industry 4.0 は、機械加工プロセスを大幅に改善したスマート ファクトリーを生み出しましたが、CNC マシンなどのネットワーク化された産業機器を悪用しようとするサイバー犯罪者の扉も開いています。 Industry 4.0では、CNC マシンなどの様々な製造装置に、ネットワーク統合とスマート接続を可能にする機能が搭載され、ダウンタイムが短縮され、製造業者のターンアラウンド タイムが短縮されます。しかし、コネクテッド ファクトリが標準になるにつれ、スマート マニュファクチャリング環境の運用を妨害したり、そこから貴重なデータを盗んだり、スパイしたりしようとするサイバー攻撃者にとって、コネクテッドファクトリは魅力的な標的になってしまいます。したがって、メーカーは、産業用機械の相互接続から生じる可能性のある危険を認識しておくことが不可欠です。 Celadaと共同で実施した研究では、、シミュレーションと実際のマシンのインストールの両方を使用して、CNC コントローラーに対してさまざまな攻撃シナリオを実行しました。私たちは、世界的なリーチと広範な市場経験、または製造業界で広く使用されている技術の開発のために選択した 4 つのベンダーの CNC コントローラーでテストを実行した結果さまざまな攻撃クラスを特定しました。生産ラインのデジタル化に伴う脅威を阻止するために、これらの企業はCNCコントローラについての対策が求められます。	https://www.trendmicro.com/en_us/research/22/j/uncovering-security-blind-spots-in-cnc-machines.html	

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源								要旨	参照先	その他特記事項
			政府・行政機関	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他組織化	その他標準	報道機関	その他			
2022/10/27	DHS Announces New Cybersecurity Performance Goals for Critical Infrastructure	DHSが重要なインフラストラクチャの新しいサイバーセキュリティパフォーマンス目標を発表	1	1					1								国土安全保障省(DHS)は、あらゆる規模の企業や重要なインフラストラクチャの所有者がサイバー脅威から身を守るために実行できる最も優先度の高いベースライン対策を概説する自主的な慣行であるサイバーセキュリティパフォーマンス目標(CPG)を発表しました。CPGは、WhiteHouseの指示により、CISAを通じてDHSによって開発されました。 CPGは、コスト、複雑さ、影響などのわかりやすい基準に基づいて測定可能な目標を明確に概説することにより、あらゆる規模の組織に適用できるように設計されています。この取り組みは、重要なインフラストラクチャのセキュリティを確保し、エスカレートする国家サイバーリスクを軽減するためのバイデンハリス政権の継続的な取り組みの一部です。 CISAは、米国国立標準技術研究所(NIST)と緊密に連携してCPGを開発しました。結果として得られるCPGは、NIST Cybersecurity Frameworkと連携して実装することを目的としています。すべての組織は、NISTサイバーセキュリティフレームワークを使用して、厳格で包括的なサイバーセキュリティプログラムを開発する必要があります。 今後数か月のうちに、CISAは、重要インフラストラクチャ・コミュニティ全体のパートナーからCPGに関するフィードバックを積極的に求め、この意見を受け取るためのディスカッションWebページを開設しました。CISAはまた、今後数か月以内にセクター固有のCPGを構築する際に、個々の重要インフラストラクチャセクターとの直接作業を開始します。	https://www.dhs.gov/news/2022/10/27/dhs-announces-new-cybersecurity-performance-goals-critical-infrastructure https://www.cisa.gov/cpg	
2022/10/31	White House Kicks Off Second International Counter Ransomware Initiative Summit	ホワイトハウスが第2回国際カウンターランサムウェアイニシアチブサミットを開始	1	1								1			1		ホワイトハウスは、本日から2日間にわたり、第2回国際カウンターランサムウェア イニシアチブでメキシコ、オランダ、ニュージーランド、ノルウェー、ポーランド、フランス、ドイツ、ウクライナ、英国などの国々と、国の重要なインフラストラクチャを混乱させる壊滅的なランサムウェア攻撃を防ぐ方法に関する協議に参加する。サミットのイニシアチブは、世界中のデジタル ネットワークを保護するというジョーバイデン大統領の計画の一環として、昨年開始されました。いくつかの同盟国は、ランサムウェアの脅威の監視と防止に特化しており、政権当局者は、リトアニアとインドのデジタル インフラストラクチャの回復力、オーストラリアのサイバーディスラプション研究、シンガポールと英国の仮想通貨イニシアチブ、スペインの公衆育成におけるリーダーシップなど、世界中で行われた専門的な取り組みを強調しています。民間企業もサミットに参加し、バイデン政権が技術政策の多くに導入するために取り組んできた重要な措置を実行します。出席している企業は、Crowdstrike、Cyber Threat Alliance、Microsoft、Cybersecurity Coalition、Palo Alto Networks、SAP、Siemens等、サイバーセキュリティ ソフトウェア技術のリーダーです。 これらの企業は、ランサムウェアの脅威の影響を受けるさまざまな地域および重点分野を網羅する強力な代表プールとして選ばれました。サミットでは、企業の専門家と経営陣が、政府が民間部門の組織とどのように協力するのが最も効果的か、公共部門の組織がサイバー攻撃を最も効果的に防止できる方法を尋ねられます。	https://www.nextgov.com/emerging-tech/2022/10/white-house-kicks-second-international-counter-ransomware-initiative-summit/379113/	
2022/10/31	ESF Partners, NSA, and CISA Release Software Supply Chain Guidance for Suppliers	ESF パートナー、NSA、および CISA がサプライヤー向けのソフトウェア サプライ チェーン ガイダンスをリリース	1	1					1			1					国家安全保障局 (NSA)、CISA、国家情報長官室 (ODNI) は本日、ソフトウェア サプライ チェーンの保護: サプライヤー向けの推奨プラクティス ガイドをリリースしました。この製品は、NSAとCISAが主導する官民横断の作業グループである永続的セキュリティフレームワーク (ESF)を通じて提供され、国の重要なインフラストラクチャに対する優先度の高い脅威に対処するためのサイバーセキュリティ ガイダンスを提供します。サプライヤーにガイダンスを提供するために、ESF は SolarWinds 攻撃につながったイベントを調査しました。これにより、ソフトウェア サプライヤーのニーズに焦点を当てた一連の業界および政府評価のベストプラクティスを作成するための投資が必要であることが明らかになりました。 ソフトウェア開発者は、コードを安全に開発して配布し、サードパーティ コンポーネントを検証し、ビルド環境を強化する必要があるため、防止はソフトウェア開発者の責任と見なされることがよくあります。しかし、サプライヤは、当社のソフトウェアのセキュリティと完全性を保証する重要な責任も負っています。結局のところ、ソフトウェア ベンダーは、顧客とソフトウェア開発者の間の連絡を取る責任があります。この関係を通じて、契約上の合意、ソフトウェアのリリースと更新、脆弱性の通知と緩和を通じて、追加のセキュリティ機能を適用できます。ソフトウェア サプライヤーは、NSAとそのパートナーから、ソフトウェア セキュリティチェックの定義、ソフトウェアの保護、安全性の高いソフトウェアの作成、継続的な脆弱性への対応による組織の準備に関するガイダンスを見つけることができます。すべての利害関係者がそれぞれの責任範囲に固有の懸念を緩和しようとするまで、ソフトウェア サプライチェーン サイクルは脆弱であり、潜在的な侵害のリスクにさらされます。	https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3204427/esf-partners-nsa-and-cisa-release-software-supply-chain-guidance-for-suppliers/ https://media.defense.gov/2022/Oct/31/2003105368/-1/-1/0/SECURING_THE_SOFTWARE_SUPPLY_CHAIN_SUPPLIERS.PDF	前回のdeveloper向けに続き、今回のsupplier向けでは、supplierをdeveloperとcustomerの間の役割と位置付けられ、developerにcode書かせる前に、Security Requirementsを含めたソフトウエア設計、あるいはThird party software supplierのsecurity確認など、管理者あるいは製品 product managerなどがやらなければならない様々なことが含まれています。 特に、Appendix C: Supply Chain Levels for Software Artifacts (SLSA)では、信頼の作成、検証などでソフトウエアご担当の方もご興味を持たれるかも知れません。
2022/11/3	Volatile Geopolitics Shake the Trends of the 2022 Cybersecurity Threat Landscape	不安定な地政学が2022年のサイバーセキュリティ脅威の状況の傾向を揺るがす	1	1						1							サイバー戦争とHacktivismを引き起こす地政学的な状況により、警戒すべきサイバー作戦と悪意のあるサイバー攻撃が、欧州連合サイバーセキュリティ機関(ENISA)によって発表された脅威ランドスケープレポートの第10版の傾向を変えた。 ENISAThreatLandscape2022(ETL)レポートは、サイバーセキュリティ脅威ランドスケープの状態に関するEUサイバーセキュリティ庁の年次レポートです。第10版は、2021年7月から2022年7月までの報告期間をカバーしている。 毎月10テラバイトを超えるデータが盗まれるランサムウェアは、依然として新しいレポートで主要な脅威の1つとして扱われており、フィッシングはそのような攻撃の最も一般的な最初のベクトルとして特定されている。ランサムウェアと並んで上位にランクされるその他の脅威は、分散型サービス拒否(DDoS)攻撃とも呼ばれる可用性に対する攻撃である。しかし、地政学的な状況、特にロシアのウクライナ侵攻は、グローバルサイバードメインの報告期間中にゲームチェンジャーとして機能した。脅威の数は依然として増加しているが、ゼロデイエクスプロイトやAIを利用した偽情報やディープフェイクなど、より幅広いベクトルが出現していることも確認している。その結果、より悪意のある広範な攻撃が出現し、より大きな被害をもたらす。 脅威の影響評価では、5種類の影響が明らかになる。評判、デジタル、経済的、物理的または社会的性質の損害。ただし、ほとんどのインシデントでは、被害者が情報を開示しないか、情報が不完全なままであるため、実際の影響は不明のままである。 主な脅威は、動機の観点から分析された。この調査では、ランサムウェアが純粋に金銭的利益によって動機付けられていることが明らかになった。ただし、国が後援するグループの動機は、スパイ活動や混乱などの脅威を伴う地政学から引き出される可能性がある。イデオロギーは、ハクティビストによるサイバー攻撃の原動力となっている可能性もある。	https://www.enisa.europa.eu/news/volatile-geopolitics-shake-the-trends-of-the-2022-cybersecurity-threat-landscape レポート本文： https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022	

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源									要旨	参照先	その他特記事項
			政府・行政機関	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他組織	その他標準	報道機関	その他			
2022/11/4	Microsoft Digital Defense Report 2022	マイクロソフトデジタル防御レポート2022													1	1	去 1 年間で、重要なインフラストラクチャを標的としたサイバー攻撃は、Microsoft が検出したすべての国家への攻撃の 20% から 40% に急増しました。この急増は主に、ウクライナのインフラに損害を与えるというロシアの目標と、米国を含むウクライナの同盟国を標的とする積極的なスパイ活動によるものです。ロシアはまた、NATO 加盟国の政府機関の顧客を妨害したり、IT 企業の顧客から情報を取得したりする方法として、IT 企業を侵害する試みを加速させました。過去 1 年間に検出されたロシアの攻撃の 90% は NATO 加盟国を標的としており、これらの攻撃の 48% は NATO 加盟国に拠点を置く IT 企業を標的としていました。中国からの攻撃の多くは、「ゼロデイ脆弱性」を見つけてコンパイルする中国の能力によって強化されています。これは、セキュリティ コミュニティがこれまで知らなかった、パッチが適用されていないソフトウェア固有の脆弱性です。中国のこれらの脆弱性の収集は、中国の事業体が発見した脆弱性を他者と共有する前に政府に報告することを義務付ける新しい法律の直後に増加したようです. 今年のレポートには、人々や組織が攻撃から身を守る方法について、さらに多くの推奨事項が含まれています。人々ができる最大のことは、多要素認証の有効化、セキュリティ パッチの適用、システムへの特権アクセスを意図的に行うこと、主要なプロバイダーの最新のセキュリティ ソリューションの展開など、基本に注意を払うことです。平均的な企業には、基本的なエンドポイント保護によって保護されていない 3,500 台の接続されたデバイスがあり、攻撃者はこれを悪用しています。攻撃を早期に検出することも重要です。多くの場合、サイバー攻撃の結果は、攻撃が始まるずっと前に決定されます。攻撃者は脆弱な環境を利用して初期アクセスを取得し、監視を行い、ラテラル ムーブメントと暗号化または流出によって大混乱を引き起こします。	https://blogs.microsoft.com/on-the-issues/2022/11/04/microsoft-digital-defense-report-2022-ukraine/ https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us https://therecord.media/microsoft-accuses-china-of-abusing-vulnerability-disclosure-requirements/	
2022/11/8	SolarWinds Faces Potential SEC Enforcement Act Over Orion Breach	ソーラーウインズ、Orionの情報漏えいでSECの強制捜査の可能性に直面													1		米国証券取引委員会 (SEC) は、同社での 2019 年のデータ侵害に関する声明と開示を行った際に、エンタープライズ ソフトウェア企業が連邦証券法に違反した疑いがあるとして、SolarWinds に対して執行措置を取る態勢を整えている。 SECが前進した場合、SolarWindsは民事上の罰金に直面する可能性があり、申し立てられた違反に対して「その他の衡平法上の救済」を提供する必要があります。この訴訟はまた、SolarWinds が関連する連邦証券法に今後違反することを禁止するものです。 SolarWinds は、最近 SEC に提出したフォーム 8-K で、SEC の潜在的な執行措置を明らかにしました。提出書類の中で、SolarWinds は、規制当局の執行スタッフが執行措置を推奨する予備決定を行ったことを指摘する、いわゆる「ウェルズ通知」を SEC から受け取ったと述べました。Wells Notice は、基本的に、証券規制当局が回答者に対して提起しようとしている告発について回答者に通知するため、回答者は回答を準備する機会を得ることができます。SolarWinds は、「開示、公式声明、管理、および手順は適切であった」と主張しました。 これとは別に、しかし同じ提出書類の中で、SolarWinds は、同社とその一部の幹部に対して提起された集団訴訟の請求を解決するために 2,600 万ドルを支払うことに同意したと述べた。訴訟は、同社がサイバーセキュリティの慣行と管理について、公式声明で投資家を誤解させたと主張していた. 和解は、事件に対する過失、責任、または不正行為の承認を構成するものではありません。和解は、承認された場合、会社の該当する賠償責任保険によって支払われます。	https://www.darkreading.com/application-security/solarwinds-faces-potential-sec-enforcement-act-over-orion-breach	本報道のポイントは、（1）SolarWindsのOrion製品への攻撃に関連して、SECの法執行部門が動き出したこと、（2）SolarWindsの対策手法、にあります。 特に（2）については、①開発環境を分離する措置を取ったこと。②エフェメラル オペレーションにより、攻撃者が侵害する長期的な環境がないこと。③すべての IT および開発スタッフにハードウェア トークン ベースの多要素認証を実装し、ソフトウェア開発中に発生するすべてのことを記録、ログ、および監査するためのメカニズムを展開したこと。④「侵入を想定する」考え方を採用し、レッドチームによる演習と侵入テストを取り入れたこと。同社がやっていることはインシデント対応の視点からかなりポイントを押さえていると思われます。
2022/11/15	FDA Updates Medical Device Cyber Response Playbook	FDAが医療機器サイバー対応プレイブックを更新	1	1								1					FDA は、MITRE と協力して、「Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook」を更新しました。このプレイブックは、医療機器の機能に影響を与える医療機器のサイバーセキュリティの問題に対する準備と対応に焦点を当てています。プレイブックの更新内容は次のとおりです。 ・臨床医、医療技術管理の専門家、IT、緊急対応、リスク管理および施設のスタッフを含む、サイバーセキュリティの準備と対応の演習に参加する多様なチームを持つ必要性を強調します。 ・地域の対応モデルとパートナーの使用から恩恵を受ける、サイバーセキュリティインシデント中の広範囲にわたる影響とダウンタイムの延長に関する考慮事項を強調します。 ・リソースの付録を追加して、医療機関が医療機器のサイバーセキュリティ インシデント （ランサムウェアを含む）に備えて対応するのに役立つツール、リファレンス、および その他のリソースを見つけやすくします。 laybook クイック スタート コンパニオン ガイドも利用できます。このガイドは、医療機関が医療機器のインシデント対応プログラムを開発する際に開始する必要がある準備と対応活動について説明するプレイブックの短縮版です。 また、FDA は、臨床医が接続された医療機器のサイバーセキュリティについて患者と話し合うのに役立つ新しいビデオ「臨床医向けのヒント - 患者の接続された医療機器を安全に保つ」をリリースしました。これらのヒントは、患者とのコミュニケーションに焦点を当てており、このトピックに取り組む際の臨床医の快適さを高めることを目的としています.	https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity	標題は"Medical Device Cybersecurity"ですが、書かれている内容は、ほとんどCSIRTの構築、運用の教科書のような内容です。 ただ、このガイドの特徴として、Regional Responsesにかなり重きを置かれていること、これは通常のCSIRTの教科書ではあまり触れられないですが、さすがに人の命を預かる病院、医療機関の矜持が感じられるものとなっています。Critical Infrastrucutureでも医療のほか銀行など人の命や生活に関わることでは必要な考え方と思われます。
2022/11/15	Sandia studies vulnerabilities of electric vehicle charging infrastructure	サンディアが電気自動車充電インフラの脆弱性を研究	1	1								1					電気自動車の普及に伴い、電気自動車の充電設備やシステムに対するサイバー攻撃のリスクと危険性も増大しています。サンディア国立研究所の電気技師であるジェイ・ジョンソンは、過去 4 年間、電気自動車の充電インフラのさまざまな脆弱性を研究し、最近、電気自動車充電器の既知の脆弱性の概要を科学雑誌Energiesに掲載しました。 「電気自動車充電器の脆弱性に関するこの調査を実施することで、政策立案者への推奨事項に優先順位を付け、業界が必要とするセキュリティの改善を通知することができます」と Johnson 氏は述べています。「超党派インフラ法は、電気自動車の充電インフラに75億ドルを割り当てています。この資金調達の一環として、連邦政府は州に物理的およびサイバーセキュリティ戦略を実施するよう求めています。私たちのレビューが、州によって確立された強化要件の優先順位付けに役立つことを願っています。私たちの取り組みは、連邦政府がベスト プラクティスを標準化し、将来的に電気自動車充電器の最低限のセキュリティ レベルを義務付けるのにも役立ちます。」	https://newsreleases.sandia.gov/ev_security/	

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源									要旨	参照先	その他特記事項
			政府機関・行政	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他標準化組織	報道機関	その他			
2022/11/16	Microsoft contributes S2C2F to OpenSSF to improve supply chain security	Microsoftは、S2C2FをOpenSSFに提供して、サプライチェーンセキュリティを向上させます		1											1	2022年8月4日、Microsoftは、2019 年以来、独自の開発プラクティスを保護するために使用しているフレームワーク、 Secure Supply Chain Consumption Framework (S2C2F)、を公開しました。 オープン ソースの大規模な消費者および貢献者として、Microsoft は、開発者がソフトウェアを構築する際にオープン ソース ソフトウェア (OSS) の依存関係をどのように使用および管理するかを保護するための堅牢な戦略の重要性を理解しています。 このたび、S2C2F が OpenSSF に採用されたことをお知らせします。Supply Chain Integrity Working Group の下で、独自の Special Initiative Group (SIG) を形成しました。OpenSSF および世界中の仲間は、この作業がすべての人のサプライ チェーン セキュリティを改善する上でいかに基本的であるかという点に関して、Microsoft に同意しています。	https://www.microsoft.com/en-us/security/blog/2022/11/16/microsoft-contributes-s2c2f-to-openssf-to-improve-supply-chain-security/	
2022/11/17	OpenSSL Usage In UEFI Firmware Exposes Weakness In SBOMs	UEFI ファームウェアで OpenSSL を使用すると、SBOM の弱点が露呈する	1	1											1	Binarly REsearchチームは、最近 OpenSSLセキュリティ更新がUEFIファームウェアサプライチェーン エコシステムにどのように反映されているか、および OpenSSLバージョンの広範な使用がファームウェアコンテキストでどのように多様化されているかを詳しく調べています。 テクノロジー業界では、サプライ チェーンのセキュリティ リスクに対処するための「ソフトウェア部品表」（ SBOM ）の使用について活発な議論が行われています。サプライチェーンのセキュリティプラクティスを実装するには、ソフトウェアの依存関係の透明性を高める必要があります。以前は、ソフトウェアの依存関係やサード パーティのコンポーネントに関する情報を提供せずに、ブラックボックスとして出荷されたソフトウェアがありました。ファームウェアは、おおむね同じように見られてきました。以前のブログ投稿で、Binarly チームは、UEFIファームウェア エコシステムとサプライ チェーンの分類における複数レベルの複雑さについて説明しました。 SBOM は依存関係をよりよく理解するのに役立ちますが、多くの場合、ベンダーはSBOM 情報をファームウェア パッケージまたはイメージとは別に配布しています。これは、SBOMが関連性がないか、誤解を招く情報を含む可能性がある場合に、サプライチェーンの問題に関する以前の議論と同じ問題を引き起こします。現在、SBOMに結び付けられたサプライ チェーンがあり、多くの場合、SBOMはベンダーから提供された情報の静的なスナップショットです。 マイクロソフトは最近、「デジタル・ディフェンス・レポート2022」の中で強調した。分析したファームウェアイメージの32%に、少なくとも10の既知の重要な脆弱性が含まれている。Binarly Platformのデータ（エンタープライズグレードのベンダーの調査に基づく）によると、ファームウェアアップデートの約20%が、少なくとも2〜3の既知の脆弱性（以前に公開されたもの）を含んでいます。	https://www.binarly.io/posts/OpenSSL_Usage_in_UEFI_Firmware_Exposes_Weakness_in_SBOMs	
2022/11/22	Vulnerabilities in BMC Firmware Affect OT/IoT Device Security	BMC ファームウェアの脆弱性が OT/IoT デバイスのセキュリティに影響を与える		1	1									1		IT サーバーのマザーボードに利用されているベースボード管理コントローラー (BMC)は、コンピューターのリモート監視および管理用に設計された補助的なシステムオンチップであり、ブートストラップからの直接のキーボードとマウスの対話、システム電源制御、BIOS ファームウェアの再フラッシュなど、リモートで低レベルのシステム操作を実行できることから、最近はITサーバ以外に運用技術 (OT) およびモノのインターネット (IoT) セクターに利用が広がっているデバイスです。このBMCデバイスの脆弱性として、13の脆弱性が報告されています。これらの脆弱性を悪用することで、認証されていない攻撃者が BMC のルート権限でリモートコード実行 (RCE) を達成し、BMC を完全に侵害して、管理対象ホストの制御を取得する可能性があります。	https://www.nozominetworks.com/blog/vulnerabilities-in-bmc-firmware-affect-ot-iot-device-security-part-1/	
2022/11/22	Vulnerable SDK components lead to supply chain risks in IoT and OT environments	脆弱な SDK 評価は、IoT および OT 環境でサプライチェーンのリスクにつながる			1										1	Boaウェブサーバーは、IoTデバイスの開発において依然として広く普及していますが、その理由の一つとして、マイクロチップに実装されたSOC（System On Chip）を動作させるための必須機能が一般的なSDKに含まれていることが考えられます。BoaやSDKのような脆弱な部品は、機器内に組み込まれて顧客に配布されることが多く、サプライチェーンの脆弱性の一因となっています。RealTek社がリリースしているような一般的なSDKは、ルーター、アクセスポイント、リピーターなどのゲートウェイ機器を製造する企業に提供されるSOCに使用されています。RealTekのSDKを使用したデバイスのデジタル管理に影響を与えるCVE-2021-35395や、ゼロクリックオーバーフローの脆弱性であるCVE-2022-27255など重大な脆弱性は、世界中で数百万台のデバイスに影響を与え、攻撃者によるコードの起動やデバイスの侵害、ボットネットの展開、ネットワーク上の横移動が可能になると報告されています。主な論点として、 - Recorded Futureが4月に発行したインドを中心とした送電網への攻撃に、2005年に提供停止されていたBoa web serverの脆弱性が悪用されていた。ただし、一番最近のTata PowerへのHive Ransomware攻撃との関連は文面から不明。 - Microsoftによると、2005年に提供停止されたはずのBoaが、RouterからカメラまでIoT devicesで現在も多用され、あろうことか端末設定、管理用画面、挙句にSign in screenに利用。 - Figure 2は、IoTデバイスのサプライチェーンは、脆弱性が下流の組織とその資産にどのように配布されるかを示しており、BoaとReal Tek SDKの脆弱性を両方とも攻撃に悪用できるとされている。 - Figure 1は、デバイス上のインターネットに公開された Boa Web サーバーのグローバル マッピングを示しており、インドが圧倒的に多いが、アメリカ、ブラジル、南アフリカ、ベトナム、韓国が「微妙」。日本はそんなに濃くないが、欧州よりは　濃いように見える。日本になくとも、アメリカ、インドを踏み台にした日本への攻撃などが懸念される。	https://www.microsoft.com/en-us/security/blog/2022/11/22/vulnerable-sdk-components-lead-to-supply-chain-risks-in-iot-and-ot-environments/	

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源									要旨	参照先	その他特記事項
			政府・行政機関	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他組織	その他標準	報道機関	その他			
2022/11/24	UK Parliament Statement:Security Update on Surveillance Equipment	英国議会の声明：監視機器に関するセキュリティの最新情報	1	1								1			1		英国議会、セキュリティ上の懸念から、政府建物での中国製カメラを制限 政府セキュリティグループは、政府の敷地に視覚的監視システムを設置することに関連して、現在および将来起こりうるセキュリティリスクの見直しを行いました。レビューは、英国に対する脅威と、これらのシステムの能力と接続性の向上に照らして、追加の管理が必要であると結論付けました。したがって、省庁は、中華人民共和国の国家情報法の対象となる企業によって製造された機密サイトへのそのような機器の配備を中止するように指示されています。これらのサイトでは常にセキュリティの考慮事項が最優先事項であるため、セキュリティ リスクの発生を防ぐための措置を講じています。 さらに、部門は、そのような機器を部門のコアネットワークに接続するべきではなく、スケジュールされたアップグレードを待つのではなく、重要なサイトに展開されているそのような機器を取り外して交換する必要があるかどうかを検討する必要があるとアドバイスされています。部門はまた、同じリスク軽減を拡張したい機密サイトの定義外のサイトがあるかどうかを検討するようにアドバイスされています。政府は引き続きこのリスクを調査し、必要に応じてさらなる措置を講じます。	https://questions-statements.parliament.uk/written-statements/detail/2022-11-24/hcws386 https://www.reuters.com/world/uk/uk-restricts-chinese-cameras-government-buildings-over-security-fears-2022-11-24/	
2022/11/29	SP 1800-22 Bring Your Own Device (BYOD) Second Draft	SP 1800-22 Bring Your Own Device (BYOD)第二次草案	1	1				1									SP 1800-22 Bring Your Own Device (BYOD) Second Draftの公開：認定されたテクノロジーを使用して強力なデータ機密性が実装される明確で再現性のあるリファレンスモバイルアーキテクチャのためのサイバーセキュリティガイダンス BYODとは、個人所有のデバイスで仕事関連のアクティビティを実行する慣行を指します。このプラクティス ガイドでは、Android および Apple モバイル デバイスの BYOD 展開でセキュリティとプライバシーを強化する方法を示すソリューション例を提供します。 BYOD 機能を組織に組み込むことで、従業員の作業方法の柔軟性を高め、組織のリソースにアクセスする機会と方法を増やすことができます。一部の組織では、従来のオフィス内プロセスとモバイルデバイステクノロジーを組み合わせることで、ポータブルなコミュニケーションアプローチと適応型ワークフローが可能になります。他の人にとっては、従業員が主にモバイルデバイスを使用してコミュニケーションとコラボレーションを行うモバイルファーストのアプローチを促進します。 組織がBYODの柔軟性の恩恵を受けながら、セキュリティとプライバシーに関する重要な課題の多くから身を守るために、このプラクティスガイドでは、標準ベースの市販製品とステップバイステップの実装ガイダンスを使用したソリューション例を提供します。	https://www.nccoe.nist.gov/mobile-device-security/bring-your-own-device	
2022/12/7	Securely Onboarding All the Things: The FIDO Fit in IoT	Securely Onboarding All the Things: The FIDO Fit in IoT参加レポート	1	1												1	Securely Onboarding All the Things: The FIDO Fit in IoT参加レポート（足立氏） 会合の主旨：・FIDOの組織としての広報　・IoTを対象としたFIDO Device Onboard (以下FDO)の概説　・FDO対応製品向けのConformance Programの紹介　　以下に会議から得られた、あるいは気づいた所見を以下に示す。 ・FDOの土台は、Intelが自社で開発していたSecure Device Onboard (SDO)である。　IntelはSDOをFIDOに寄贈し、これにより、FIDO IoT Technical Working Group　(IoT TWG)が構成されFDOの本格的な検討が始まった由。ただしFDOに関する本日の講師は全てIntelの方々であり、Intel主導で「標準化」された感が強い。 ・FDO（あるいは原型のSDO)の目的は、proprietaryな技術に依存することなく、いわゆるzero touch onboardingの実現である。具体的には、untrusted installermodelに基づき、IoT端末のinstallerは単に電源を入れるだけでonboardingを完結できることを目指した。どこかで何か不具合が起こり、電源入れてもonboardingできなかったら製造元などへ返品と想定し、問題端末がonboardされないように対策する。 ・FDOの主な構成要素として、TO (Transfer Ownership)と呼ばれるプロトコル群 (TO0, TO1, and TO2), broker並びに認証を担うRendezvous Server, Deviceに格納されるOwnership Voucherなどで構成される。 ・Rendezvous Serverにより実施されるOnboardingに先立つ認証は、端末並びにOwner/Rendezvous Server相互の相互認証が実施され、Ownership voucherなどの端末が格納する基本情報は鍵署名され正当性を検証可能とされる。 ・上述から、FDOのSpecの中で言われる"Owner"とは、Rendezvous Server(s)のことであり、自然人、法人ではない。 ・実際に品物を製造している製造元では、製品にRendezvous serversの情報と、認証に必要なパッケージを誰が投入するか、という二つの情報しか投入しない。（installerだけではなく、製造元もuntrustedと扱われていると思われる。） ・オプション記述、あるいは拡張記述と思われるFIDO Service Information Module　を現在策定中。現段階でdownload, upload, command, csr, wgetの策定と標準化が進んでおり興味がある組織のFIDOへの加盟並びに参加が呼びかけられた。	https://fidoalliance.org/specifications/download-iot-specifications/ https://fidoalliance.org/specs/FDO/FIDO-Device-Onboard-PS-v1.1-20220419/FIDO-Device-Onboard-PS-v1.1-20220419.html	
2022/12/14	Severe vulnerabilities found in most industrial controllers	ほとんどの産業用コントローラーで発見された深刻な脆弱性	1	1											1	1	The Cybersecurity 202 で最初に共有された調査によると、電力や水処理プラントなどの施設の安全と運用を維持するデバイスの4分の3には、深刻な、パッチが適用されていないサイバーセキュリティの脆弱性があります。 Microsoft は、顧客の運用テクノロジ ネットワークの調査に基づいて、産業用制御デバイスの深刻度の高い脆弱性についてこの数値を導き出しました。これは、ハッカーがそれをつかむと、多くの混乱を引き起こす可能性がある脅威に関する最新のデータ ポイントです。 ・Stuxnetワームは、10年以上前にイランの核遠心分離機の推定5分の1を、そのような産業用コントローラーを標的にして全滅させました 。 ・Industroyerマルウェアは、2016年に産業用制御システムに影響を与え、ウクライナのキエフの一部への電力を1時間遮断しました。 ・昨年、ハッカーがフロリダ州オールズマーの水処理プラントで、人間にとって危険なレベルまでアルカリ液のレベルを上げることに成功しました。幸いなことに、工場のオペレーターがハッカーに気づき、迅速に阻止することができました。 ルーターやカメラなどの「モノのインターネット」 (IoT) デバイスにおける運用技術 (OT) と情報技術 (データの収集と送信により重点を置いている) の融合は、脅威が高まっていることを意味していると Microsoft は恐れています。これは、最も重要な米国のインフラストラクチャに特に当てはまります。	https://www.washingtonpost.com/politics/2022/12/14/severe-vulnerabilities-found-most-industrial-controllers/ https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5daTD	

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源									要旨	参照先	その他特記事項
			政府・行政機関	民間	一般	特定組織	不明	NIST	DHS CISA	ENISA	ETSI	その他の政府・行政機関	その他組織化	その他標準	報道機関	その他			
2022/12/15	Where the Senate's cyber agenda-setters want to go in 2023	2023年、上院のサイバーアジェンダ設定者はどこへ行こうとしているのか	1												1		国土安全保障・政府問題委員会の委員長であるGary Peters上院議員(民主党、ミシガン州)は、来年の主要なサイバーセキュリティの優先事項は、中小企業、オープンソースソフトウェア、連邦政府機関、および産業施設で使用される重要なテクノロジーのサイバー防御を強化することだと語った。 ［Peters委員長］今後の立法の狙い: 急速に変化するサイバーセキュリティの世界では、Peters氏は1か月以内に別の答えが得られる可能性があると述べた。しかし今のところは以下の4つを検討している。 ●log4jのようなオープンソースソフトウェアを保護するために設計された法律：一般的なソフトウェアツールで発見された脆弱性は、何億ものデバイスを脅かしたとCISAは述べています。 ●連邦政府機関に情報セキュリティの枠組みを提供する法律の更新：そうするための法案は、今年下院で「いくつかの難問に遭遇した」とPeters氏は言った。彼はマスコミの前で交渉したくなかったので、その問題点については触れないという。 ●産業機器の稼働と安全を維持する運用技術を守る方法を見つける：「多くの場合、悪意のある人物がこれらの物理システムの一部を攻撃することに成功した場合、オンラインに戻るには、ソフトウェアの修正を行うよりもはるかに長い時間が　かかる可能性がある」とPeters氏は述べています。 ●中小企業をサイバー攻撃から保護する：	https://www.washingtonpost.com/politics/2022/12/15/here-what-next-senate-cybersecurity/	
2022/12/15	Announcement of Proposal to Revise FIPS 180-4, Secure Hash Standard (SHS)	FIPS 180-4、セキュアハッシュ標準 (SHS) を改訂する提案の発表	1	1				1									NIST の暗号規格とガイドラインの定期的な見直しの一環として、NIST の暗号出版審査委員会は、 2022 年 6 月に連邦情報処理規格の発行 FIPS 180-4、セキュア ハッシュ規格 (SHS)の見直しを発表しました。 NIST は、FIPS 180-4 の改訂を提案しています。この改訂により、標準から SHA-1 が削除されます。SHA-1 仕様は、FIPS 180-5 が発行された後も、 FIPS 180-4のアーカイブされたコピーで引き続き利用できます。NIST は、すべての アプリケーションを SHA-1 から移行する計画を立てています。詳細については、ハッシュ関数に関する NIST ポリシーを参照してください。NIST は、NIST SP800-131A を改訂して、移行に関する詳細を追加する予定です。SHA-1 を参照する他の NIST 出版物は、定期的なレビュー サイクル中に改訂されます。 Cryptographic Module Validation Program (CMVP) は、FIPS 140-3 実装ガイダンス (IG) の開発を計画しており、ハッシュ関数のソフトウェア実装で通常使用される Init、Update、Final インターフェイスについて説明しています。 2023年1月31日までに FIPS 180-4 を改訂するという決定についてのコメントを募集しています。	https://csrc.nist.gov/News/2022/proposal-to-revise-fips-180-4-secure-hash-standard https://csrc.nist.gov/news/2022/nist-transitioning-away-from-sha-1-for-all-apps	
2022/12/15	Tracking Malicious Glupteba Activity Through the Blockchain	ブロックチェーンを介した悪意のあるGluptebaアクティビティの追跡															脅威アクターは、サイバー攻撃を開始するためにブロックチェーンテクノロジーをますます活用しています。ブロックチェーンの分散型および分散型の性質を利用することにより、悪意のある攻撃者は、マルウェアの伝播からランサムウェアの配布に至るまで、さまざまな攻撃に対してその匿名性を悪用できます。 Gluptebaトロイの木馬は、ブロックチェーンベースのテクノロジーを利用して悪意のある活動を実行する脅威アクターの例です。このブログでは、Nozomi Networks LabがGluptebaに関する最新の調査結果と、セキュリティチームがブロックチェーン内の悪意のあるアクティビティを検索する方法を紹介します。	https://www.nozominetworks.com/blog/tracking-malicious-glupteba-activity-through-the-blockchain/	1. IoT:IoTを対象とするbackdoor trojanであり、bot化されている。ベンダー提供の様々なIoT（Internet of Things）アプライアンスの脆弱性を突くことを目的としたGrupteba モジュールが複数存在する。 2. Blockchainの本来利用：本来のblockchainの利用のされ方ですが、犯罪者がC&Cの構築に利用できるのなら、SIP CPSの信頼の構築・検証、あるいは昨今のSupply Chainで同じユースケースを利用することも可能だと考えられる。
2022/12/19	Announcement of Proposal to Update FIPS 197, The Advanced Encryption Standard	高度暗号化標準であるFIPS 197の更新提案の発表	1	1				1									NISTの暗号標準とガイドラインの定期的なレビューの一環として、NISTの暗号公開審査委員会(「審査委員会」)は、2021年5月に連邦情報処理標準公開(FIPS)197、高度暗号化標準(AES)のレビューを発表しました。 NIST は FIPS 197 の更新を提案しています。 パブリケーションの更新は、エラーを修正したり解釈を明確にしたりするための変更のみが必要であり、技術的な内容に変更が加えられない場合に適しています。 ［FIPS 197 の更新ドラフトの概要］ バージョン履歴は、FIPS 197 のドラフト更新の付録 D にまとめられています。更新草案には、2001 年 11 月に公開されたバージョンに対する次のような広範な編集上の改善が含まれています。 ・フロントマターは近代化され、例えば、序文と要約が追加されます。 ・用語と記号は、より包括的かつ一貫して定義されます。 ・書式設定/組版はさまざまな方法で改善されています。 ・不要な形式は削除されます。 ・3つの主要なスケジュールの図が含まれています。 ・いくつかの参考文献が更新され、追加の参考文献が提供されました。	https://csrc.nist.gov/news/2022/aes-draft-fips-197-update-available-for-comment	

研究発表・講演、文献、特許等の状況

（1）研究発表・講演

なし

（2）論文

なし

（3）特許等（知財）

なし

（4）受賞実績

なし

（5）成果普及の努力（プレス発表等）

なし

契約管理番号：	22100196-0