2021 年度成果報告書

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

2022 年 3 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の妥当性について調査・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 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、Cybersecurity Competence Centre/Network (ECCC) が設立されている。

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。また、世界の最新技術動向を調査し、本研究開発の目標水準と比較することにより妥当性を評価した。この調査により追加が必要と考えられる評価項目を提案し、目標水準設定の参考となる技術を提示した。

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 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, organizational governance, functions,

and technology were discussed in the Horizon 2020 pilot project and the Cybersecurity Competence Centre/Network (ECCC) has been established.

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. We also surveyed the latest global technological trends and evaluated appropriateness of the target level of this R&D by comparing with them. The survey suggested evaluation items that may need to be added, and suggested technologies that can be used as a reference for setting the 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 国際的な目標水準の妥当性評価

本プロジェクト内で推進する実証評価ワーキンググループにおいて、本プロジェクトで策定した国際的な目標水準の妥当性について、上記③で得た調査結果に照らし、海外のプロジェクトの特徴と、本プロジェクトで開発する技術の特徴の、類似性や対応関係を調査し、対応関係の分析を行った。本報告の 5.2 節で報告する。

⑤　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③④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 5.3 節で報告する。

⑥　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。

昨年度の調査の米国の 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

4.1.2.1 米国の主要動向情報

米国における動向の発生状況を示すために、調査期間に発生した主要な動向情報を時系列で以下に示す。発生日時は動向発生地の現地時間である。下記に示した主要な動向については、それぞれ発生後に電子メールにて本プロジェクト（以後 SIP-CPS と記す）の関連者に報告を行った。本項においては主要な動向の項目と概要を示し、動向の個々の情報は付表に記載する。

- 2021 年 7 月 28 日 National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems[1]発表
  - Whitehouse 発行。
  - 対象は米国内重要インフラストラクチャ事業者並びにこれらに関連する業界。

- 2021 年 7 月 28 日 Workshop and Call for Papers on Cybersecurity Labeling Programs for Consumers: Internet of Things (IoT) Devices and Software[2]発表
  - NIST 発行、2021 年 5 月 12 日発行の Executive Order 14028[3]（以下 EO14028 と略記）で NIST 担当とされた業務を行うもの。
  - 2021 年 9 月 14,15 両日にオンラインでワークショップの実施、及び一般消費者向けソフトウェアラベリングに関する Call for Papers の二件を発表。Call for Papers の締め切りは同 8 月 17 日。
  - Call for Papers へ応募と提出された文書類は、Consumer Software Labeling Position Papers[4]に示される。

- 2021 年 8 月 25 日 NISTIR 8259B Non-Technical Supporting Capability Core Baseline 最終版発行 [5]
  - NIST 発行。
  - 2020 年 5 月 29 日に最終確定版が発行された NISTIR 8259[6]並びに NISTIR 8259A[7]に続き、NISTIR 8259B の最終確定版。製造業者が IoT デバイスを顧客に販売する前にセキュリティ強化のため実施が推奨される 6 つの活動を示した NISTIR 8259 と、セキュリティ確保のため IoT デバイスに求められる機能類 (features and

1. <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/>
2. <https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/workshop-and-call-papers-cybersecurity-labeling>
3. <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>, <https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity>
4. <https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/consumer-software-labeling-position-papers>
5. <https://csrc.nist.gov/publications/detail/nistir/8259b/final>
6. NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers: <https://csrc.nist.gov/publications/detail/nistir/8259/final>
7. NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline <https://csrc.nist.gov/publications/detail/nistir/8259a/final>

functions)を示した NIST 8259A に対し、NISTIR 8259B 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非技術的なサポート活動を示している。NISTIR 8296 の 6 つの活動のうち、Activities 1~4 は Primarily Pre-Market Impact、Activities 5~6 は Primarily Post-Market Impact と分類される。

- NIST IoT Program の担当文書類のうち、この時点で残る Drafts 類は、NISTIR 8259C[8], NISTIR 8259D[9], 並びに NIST SP 800-213[10]の三つとなった。その後のこれらの動向については、2021 年 11 月 29 日の項で示す。

- 2021 年 8 月 25 日 FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity を発表 [11]
  - 同日開催のバイデン大統領とアメリカ主要企業トップとの会談の直後に Whitehouse より発表。

- 2021 年 8 月 31 日 DRAFT Baseline Security Criteria for Consumer IoT Devices 発表 [12]
  - NIST よりパブリックコメントを 10 月 17 日締め切りでの募集が発表された。
  - EO 14028 の Section 4.は、Enhancing Software Supply Chain Security と題された節で他の Section と比べても記述量が多い。Section 4 の(s)項と(t)項では 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 所長に命じられており、この業務に呼応するものである。
  - 既に最終版が確定された、NISTIR 8259: Foundational Cybersecurity Activities for IoT Device Manufacturers、 NISTIR 8259A: IoT Device Cybersecurity Capability Core Baseline 並びに NISTIR 8259B: IoT Non-Technical Supporting Capability Core Baseline に基づいた Profiles を業界別、Use case 別に作成することを勧奨。
  - ドラフトの Table 1~3 は NISTIR 8259, 8259A, 8259B からの引用、再編であり、これが Consumer IoT devices に対する米国内での事実上の技術目標となりうる可能性が高いと考えられる。

- 2021 年 8 月 31 日[Project Description] Mitigating Cybersecurity Risk in Telehealth Smart Home Integration: Cybersecurity for the Healthcare Sector 発表 [13]
  - NIST 発表。パブリックコメントを 10 月 4 日締め切りで募集。

---

[8]. NISTIR 8259C(Draft): Creating a profile using the IoT Core Baseline and Non-Technical Baseline <https://csrc.nist.gov/publications/detail/nistir/8259c/draft>
[9]. NISTIR 8259D (Draft): Profile using the IoT Core Baseline and Non-Technical Baseline for the Federal Government <https://csrc.nist.gov/publications/detail/nistir/8259d/draft>
[10]. NIST SP 800-213 (Draft): IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements: <https://csrc.nist.gov/publications/detail/sp/800-213/draft>
[11]. <https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/>
[12]. <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%20202 1-08-31.pdf>
[13]. <https://csrc.nist.gov/publications/detail/white-paper/2021/08/31/mitigating-cyber-risk-in-telehealth-smart-home-integration/draft>

- NIST と MITRE[14]との共同で、NCCoE[15]の一環で実施と類推される、医療用 IoT 機器のサイバーセキュリティリスクの低減を目指すプロジェクトが発足。 MITRE は米国の連邦政府が資金を提供する研究 (FFRDCs[16]) を複数運営する非営利組織であり、活動領域は量子、宇宙からいわゆるサイバーセキュリティまで幅広い。NCCoE は NIST Information Technology Laboratory(ITL)の一部門として、最先端のサイバーセキュリティ技術導入の加速を目的として 2012 年に設立されている。
- 標題は Mitigating Cybersecurity Risk は、文献に示されているいわゆるサイバーセキュリティ、リスク管理に加え、Identity and Access Management など本人認証並びに認可(authorization)、プライバシーリスク、HIPAA を通じた法規制への対応など、DHS 指定重要インフラストラクチャの一つでもある医療分野での検討課題を含み、対象範囲は幅広い。

- 2021 年 9 月 21, 22 日 ICSJWG 2021 Fall Virtual Meeting[17]
  - DHS CISA 主催、年二回開催。 ICS, OT が中心の会合。
  - A (Not So) Boring Talk About Upcoming Changes Through Regulation：ドイツ BSI 講師よりいくつかの最近の法制度について説明。
  - How Much Cyber Security is Enough? ：いくつかの前提を設定し、FAIR (Factor Analysis of Information Risk)や NIST SP 800-30 に基づき Risk 評価のシミュレーションを実施。

- 2021 年 9 月 22 日 Software and Supply Chain Assurance Forum[18]
  - NIST 主催、MITRE が関与して参画。

- 2021 年 10 月 14 日 Improving the Nation’s Cybersecurity: Progress and Next Steps in Carrying Out Executive Order[19]
  - NIST 主催。EO 14028 で NIST に割り当てられた業務の遂行並びに進捗状況について、NIST から発表。

- 2021 年 10 月 20 日 ICSJWG Webinar THE END IS NEAR… Now What? Best Practices for End of Service and End of Life[20]
  - DHS Industrial Control Systems Joint Working Group (ICSJWG)主催。
  - 年二度開催され、次回 ICSJWG Spring Meeting は、2022 年 4 月 26, 27 の両日、オンライン実施予定。

- 2021 年 10 月 28 日 SP 800-161 Rev. 1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (2nd Draft) 公開 [21]

---

14. <https://www.mitre.org/about/corporate-overview>
15. National Cybersecurity Center of Excellence <https://www.nccoe.nist.gov/our-approach/about-center>, <https://www.nist.gov/programs-projects/national-cybersecurity-center-excellence>
16. Federally Funded Research and Development Centers
17. <https://gateway.on24.com/wcc/eh/3049745/icsjwg-2021-fall-virtual-meeting>
18. <https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/ssca>
19. <https://www.nist.gov/news-events/events/2021/10/improving-nations-cybersecurity-progress-and-next-steps-carrying-out>
20. <https://us-cert.cisa.gov/sites/default/files/ICSJWG-Archive/Web_Oct_21/INV_ICSJWG_Oct21_Webinar16_Flyer_FIN_20210923_508C.pdf>
21. <https://us-cert.cisa.gov/sites/default/files/ICSJWG-Archive/Web_Oct_21/INV_ICSJWG_Oct21_Webinar16_Flyer_FIN_20210923_508C.pdf>

- NIST より同 12 月 3 日までコメント受付として公開。他の NIST SP 同様連邦政府文民省庁を対象とする、連邦政府情報システムに利用されるソフトウェア、ハードウェア製品類のサプライチェーンリスク管理に求められる標準。対象とされる連邦政府各省庁はこの標準を遵守して調達、購入を行うため、他の NIST SP 文書と同様連邦政府への納入事業者にも大きく影響する。
- 大きくな拡大されている Appendix A はコントロール(controls)類であり、納入事業者への遵守が求められ、技術標準との関連あるいは影響が認められるものも含まれる。

- 2021 年 11 月 8 日 Executive Order 14028: Guidelines for Enhancing Software Supply Chain Security[22]
  - NIST 主催。オンライン実施。
  - 20221 年 10 月 14 日に引き続き、EO 14028 で NIST に割り当てられた業務の遂行並びに進捗状況を中心に NIST から発表。

- 2021 年 11 月 22 日 NIST Cybersecurity for IoT Program の website 刷新 [23]
  - twitter にて NIST より 11 月 22 日に広報されたが、刷新の背景や意図は触れられておらず、体裁は異なるものの掲載されている情報に差異、変化などは見られない。

- 2021 年 11 月 22 日 Preliminary Draft NIST SP 1800-34 A, B, and C, Validating the Integrity of Computing Devices 発行 [24]
  - NIST より公開され、2022 年 1 月 17 日期限でコメントを受付け。
  - コンピュータ端末装置類の真正性(integrity)の検証(validation)についての標準である。対象は IoT に限られないものの、SIP-CPS で実施される信頼の証明、信頼チェーンの検証と維持に関連性が認められるため、参考文献、参考動向として留意する必要がある。

- 2021 年 11 月 29 日 SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements[25]及び SP 800-213A IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog [26]の２文献最終版の発行
  - NIST IoT Program が作成を続けてきた、NIST SP 800-213 最終版の公開、加えて、新たに NIST SP 800-213A が発行された。

---

22. <https://www.nist.gov/news-events/events/2021/11/executive-order-14028-guidelines-%03enhancing-software-supply-chain>
23. <https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program>, <https://twitter.com/NISTcyber/status/1462781231372795908>
24. NIST SP 1800-34A: Executive Summary: <https://www.nccoe.nist.gov/sites/default/files/legacy-files/nist-sp1800-34a-tpm-sca-preliminary-draft.pdf>
NIST SP 1800-34B: Approach, Architecture, and Security Characteristics <https://www.nccoe.nist.gov/sites/default/files/legacy-files/tpm-sca-nist-sp1800-34b-preliminary-draft.pdf>
NIST SP 1800-34C: How-To Guides <https://www.nccoe.nist.gov/sites/default/files/2021-11/sca-nist-sp-1800-34c-preliminary-draft.pdf>
25. SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements: <https://csrc.nist.gov/publications/detail/sp/800-213/final>
26. SP 800-213A IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog: <https://csrc.nist.gov/publications/detail/sp/800-213a/final>

- NIST IoT Program が作成してきた、NISTIR 8259D (Draft)の内容の中核は新 NIST SP 800-213A の Appendix へ移管された上、NISTIR 8259D (Draft)の撤回 (withdrawn)[27]が併せて発表された。

- 2021 年 12 月 3 日　Consumer Cybersecurity Labeling for IoT Products: Discussion Draft on the Path Forward[28]
  - NIST より発行。5 月 12 日に発令の EO 14028 で NIST に割り当てられた業務のうち、IoT Products への Labeling を規定する文書の 12 月時点での草稿 (Draft)。

- 2021 年 12 月 9 日 Cybersecurity Labeling for Consumer IoT and Software: Executive Order Update and Discussion[29]
  - NIST 主催。オンラインで実施。
  - 20221 年 10 月 14 日、同 11 月 8 日の二回に引き続き、EO 14028 で NIST に割り当てられた業務のうち、会合直前に発行された Draft Cybersecurity Labeling for Consumer IoT and Software の進捗状況並びに今後の予定を中心に NIST からの発表。

- 2022 年 1 月 11 日　NISTIR 8349 (Draft) Methodology for Characterizing Network Behavior of Internet of Things Devices[30]
  - NIST 並びに NCCoE により作成、公開され、同 2 月 11 日までパブリックコメントに付されたドラフト。
  - システム管理並びに安全の確保のため、接続された IoT の挙動を MUD-Manufacture Usage Description を利用して把握する際、端末管理責任者並びにシステム管理者が心得るべき留意点について述べ、NCCoE が開発したツール MUD-PD[31]の利用方法について説明されている。

- 2022 年 1 月 13 日　Internet of Things Advisory Board (IoTAB) の新設並びに候補者の nomination 公告 [32]
  - NIST の所属する商務省 (Department of Commerce)より発表。2021 米国会計年度国防権限法及び連邦諮問委員会法 (in accordance with the requirements of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, and in accordance with the Federal Advisory Committee Act, as amended)に依拠とされる。

---

[27]. NISTIR 8259D (Draft) Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government:
"Planning Note (11/29/2021):　This document has been withdrawn, and based on public comments the content is now available in an appendix of SP 800-213A."
<https://csrc.nist.gov/publications/detail/nistir/8259d/archive/2020-12-15>
[28].<https://www.nist.gov/system/files/documents/2021/12/03/FINAL_Consumer_IoT_Label_Discussion_Paper_20211202.pdf>
[29]. <https://www.nist.gov/news-events/events/2021/12/cybersecurity-labeling-consumer-iot-and-software-executive-order-update>
[30]. <https://csrc.nist.gov/publications/detail/nistir/8349/draft>
Project Page: <https://www.nccoe.nist.gov/projects/iot-device-characterization>
[31]. <https://github.com/usnistgov/MUD-PD>
[32]. NIST 発表 <https://www.nist.gov/news-events/news/2022/01/department-commerce-seeks-internet-things-experts-new-advisory-board>
Federal Register <https://www.federalregister.gov/documents/2022/01/13/2022-00419/establishment-and-call-for-nominations-to-serve-on-the-internet-of-things-advisory-board>

- 2022 年 1 月 13 日　Whitehouse 主催 Software Security 会合 [33]
  - 報道によれば、2021 年末から話題となった、Apache log4j の脆弱性問題に端を発し、Whitehouse National Security Council Jake Sullivan 氏が招集、Anne Neuberger 氏が主導した模様。
  - Apache Log4j 脆弱性の影響範囲は確定できていないが、現状、Appliances を含むいわゆる IT 向け Hardware が利用するソフトウェアとアプリケーション並びにサービスが中心となっており、SIP-CPS の対象領域との明確な関連性は認められない。
  - IT 機器類に加え、複数の ICS 機器類への Log4j 脆弱性の影響は 1 月現在既に確認、報道 [34]されている。
  - Log4j に類似した IoT 類に広範に影響しうる脆弱性として、Kcode の NetUSB に存する RCE 脆弱性 (CVE-2021-45608)[35]が会合前の同 11 日に公開されており、Log4j 脆弱性と同様の影響や対策が近い将来必要となりうる。

- 2022 年 2 月 3 日 NIST SP 800-218 Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities 確定最終版の発行、公開 [36]
  - EO14028 に示されるソフトウェアの脆弱性対策を反映したソフトウェア開発ライフサイクル（SDLC）実施フレームワークとしての NIST SP である。

- 2022 年 2 月 4 日　NIST Cybersecurity White Paper: Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products 発行 [37]
  - 2021 年 5 月 12 日発令の EO 14028 で NIST に割り当てられた業務のうち、IoT Products への Labeling を規定する文書の最終版が NIST より発行された。

- 2022 年 2 月 7 日　List of Critical and Emerging Technologies が更新され、米国政府より発行。
  - Whitehouse 並びに国務省より報道発表 [38]。

---

[33]. Whitehouse: <https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/>
Apache Position Paper: <https://cwiki.apache.org/confluence/display/COMDEV/Position+Paper>
Washington Post: <https://www.washingtonpost.com/politics/2022/01/14/open-source-bugs-present-an-extermination-problem-government/>
[34] ICS Vendors Respond to Log4j Vulnerabilities <https://www.securityweek.com/ics-vendors-respond-log4j-vulnerabilities>
[35]. CVE-2021-45608 | NetUSB RCE Flaw in Millions of End User Routers (SentinelOne on January 11, 2021): <https://www.sentinelone.com/labs/cve-2021-45608-netusb-rce-flaw-in-millions-of-end-user-routers/>, NetUSB (USB Over IP), KCodes <https://www.kcodes.com/product/1/36>
[36]. <https://csrc.nist.gov/publications/detail/sp/800-218/final>
[37]. NIST: <https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/cybersecurity-labeling-consumers-internet-things>,
本文 <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf>
[38]. Whitehouse: <https://www.whitehouse.gov/ostp/news-updates/2022/02/07/technologies-for-american-innovation-and-national-security/>
国務省発表:<https://www.state.gov/united-states-releases-updated-list-of-critical-and-emerging-technologies/>
本文: <https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf>

- アメリカの国家安全保障に重要な影響を持つ技術並びに技術分野を指定したリストが更新されて一般公開された。
- 国務省の報道発表によると、「米国政府、民間、同盟国、パートナーが、民主主義の価値を守るために理解しなければならない(must)」とされている。

- 2022 年 2 月 16 日　Our Quest: Advancing Product Labels to Help Consumers Consider Cybersecurity の公開 [39]。
  - NIST blog, CYBERSECURITY INSIGHTS[40]に掲載される。
  - 共著者の一人である NIST IoT Program の責任者、Katarina Megas 氏が IoT に関する部分を記述。主に IoT Program の過去の経緯、実績が述べられている。

- 2022 年 2 月 22 日　NIST より Cybersecurity Framework 並びに Supply Chain Guidance 更新に対する RFI の公告。
  - Federal Register に掲載され公告された [41]。
  - 対象が IoT に加え、NIST Cybersecurity Framework, Cybersecurity Supply Chain などが対象とされ、将来の NIST Cybersecurity Framework と Cybersecurity Supply Chain Management Guidance[42]との統合の可能性が示唆されている。

- 2022 年 2 月 23 日　Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry 発行 [43]
  - 昨年 2021 年 2 月 24 日発行 Executive Order on America's Supply Chains 発令 (以下 EO 14017 と略記)[44]に対する商務省並びに国土安全保障省の連名での発表。

- 2022 年 3 月 7 日　Workshop to inform Implementation Guidance for Federal Procurement of Secure Software 実施案内の発行 [45]
  - 標題会合を同 3 月 22 日に、NIST と OMB 共催でオンラインにて実施の案内と参加申し込みの受付を開始。

---

[39] <https://www.nist.gov/blogs/cybersecurity-insights/our-quest-advancing-product-labels-help-consumers-consider>

[40] <https://www.nist.gov/blogs/cybersecurity-insights>

[41] "Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management", Federal Register Dated on 2/22/2022, Document Type: Notice, Document Citation: 87 FR 9579, Docket Number: 220210-0045, Document Number: 2022-03642 <https://www.federalregister.gov/documents/2022/02/22/2022-03642/evaluating-and-improving-nist-cybersecurity-resources-the-cybersecurity-framework-and-cybersecurity>

[42] Federal Register 公告標題にも含まれる Cybersecurity Supply Chain Management Guidance とは何か具体的には不明である。現在 NIST Cybersecurity Supply Chain Risk Management program (C-SCRM)が発行の関連文献は、2021 年発行分だけで Final, Drafts 含めて三件存在する。<https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/publications>

[43] <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>

[44] <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/>, <https://www.federalregister.gov/documents/2021/03/01/2021-04280/americas-supply-chains> EO14017 は、IoT に限らず、ハードウェア、ソフトウェアなど全てを対象にした Supply Chain の米国の現状の問題、対策を求める大統領命令である。

[45] <https://www.nist.gov/news-events/events/2022/03/workshop-inform-implementation-guidance-federal-procurement-secure>

- NIST SP 800-218 Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities36 の説明を含む四時間のオンライン会合が予定される。

- 2022 年 3 月 7 日　Workshop Celebrating 50 Years of Cybersecurity at NIST!が、NIST Cyber Security Insights, a NIST blog に掲載 [46]
  - 1972 年、NIST の前身 National Bureau of Standards (NBS)で Computer Security Program が開始されてから今年で 50 年を迎える。その経緯と主要な事象を示す年表を含め NIST blog に掲載された。

- 2022 年 3 月 9 日 TLStorm 脆弱性につき速報 [47]
  - APC 製 UPS に関わる三つの脆弱性の詳細が ARMIS より公開。
  - 遠隔地の攻撃者が APC Smart-UPS デバイスを乗っ取り、物理デバイスと IT 資産の両方を標的とした過激な攻撃を行うことができる。
  - SIP CPS が対象とするユースケースに類似の構成であり、またこれら三つの脆弱性は UPS に限らずどのような IoT でも発生しうる脆弱性である。

4.1.2.2　欧州の主要動向情報

- 2021 年 5 月 25 日 Cybersecurity Certification: Candidate EUCC Scheme V1.1.1[48] 発表
  - ENISA 発表
  - 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、および ISO 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。

- 2021 年 6 月 8 日 Cybersecurity Copetence Centre/Network（ECCC) 設立 [49]。
  - EU 発表
  - 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。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。

- 2021 年 7 月 29 日 Threat Landscape for Supply Chain Attacks 発表 [50]
  - ENISA 発行
  - 当該文献は報告者が属する ENISA 専門家部会 (Ad-Hoc Working Group on Cyber Threat Landscapes) 宛に draft 段階で内容照会があり、コメント類を提出したもの。

- 2021 年 7 月 29 日 Threat Landscape for Supply Chain Attacks、“Methodology for Sectoral Cybersecurity Assessments, EU Cybersecurity Certification Framework” 発行 [51]。

---

[46] <https://www.nist.gov/blogs/cybersecurity-insights/celebrating-50-years-cybersecurity-nist>
[47] <https://www.armis.com/research/tlstorm/>
[48] <https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1>
[49] <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre>
[50] <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>
[51]. <https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment>

- ENISA 発行
- 産業別、業界別(Sectoral)に、EU Cybersecurity Act（CSA）で定められる EU Certification Scheme に準拠しつつ、それぞれの業界に適した Certification Scheme を作成する参考書

- 2021 年 8 月 ETSI TS 103 701 Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements[52]が最終版として確定した模様。
  - ETSI EN 303 645[53]の定める Consumer IoT Baseline requirements への適合試験(Conformance testing)実施の手順、要領について具体的に規定

- 2021 年 11 月 24 日 “The Product Security and Telecommunications Infrastructure (PSTI) Bill” 法案が英国で公開 [54]
  - 製造者、輸入者、流通者に対し、一般消費者向け接続可能な機器類のセキュリティ機能実装を義務付け、柔軟に技術の進歩に応じることができる枠組みを提供し、取締りを含むとされる [55]。

- 2021 年 12 月 2~3 日 ENISA Cybersecurity Certification Conference 2021[56]
  - ENISA 主催
  - 欧州連合で導入が予定される製品、サービスの認証 (Certification)に関する年次会合。今回の会場はギリシャ・アテネで、オンラインとの並行開催で実施された。対象はあくまで欧州連合での認証であり IoT に限定されてはいない。

- 2022 年 1 月 27 日 Pan European Systemic Cyber Incident Coordination Framework (EU-SCISF)の発足を European Systemic Review Board (ESRB)が欧州金融機関向けに勧告 [57]
  - EU-SCISF は欧州連合内の金融当局、関係政府並びに国際金融組織等との Incident Coordination を強化し、EU Cyber Incident Response Frameworks を補完するものと位置付けられる。

4.1.3 米国の動向

4.1.3.1 NIST IoT Program の動向

調査対象期間中に NIST IoT Program が従来から取り組んできた文書類が成熟し、いくつかは内

---

[52].<https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf>, <https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58434>

[53] <https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf>

[54]. <https://www.gov.uk/guidance/the-product-security-and-telecommunications-infrastructure-psti-bill-product-security-factsheet#how-we-are-going-to-do-it>

[55]. <https://www.gov.uk/government/collections/the-product-security-and-telecommunications-infrastructure-psti-bill-factsheets>

[56]. <https://www.enisa.europa.eu/events/enisa-cybersecurity-certification-conference-2021>

[57]. 報道発表<https://www.esrb.europa.eu/news/pr/date/2022/html/esrb.pr.220127~f1548f677e.en.html>
勧告本文
<https://www.esrb.europa.eu/pub/pdf/recommendations/esrb.recommendation220127_on_cyber_incident_coordination~0ebcbf5f69.en.pdf/>
報道例 <https://www.bleepingcomputer.com/news/security/eu-to-create-pan-european-cyber-incident-coordination-framework/>

容確定の上最終版として発行や、統合が行われた。IoT Program が作成した文書類を示し、それぞれの文書の状態を示す。

(1) 本事業開始前に確定していた前提となる基本文書類

- NISTIR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks: 2019 年 6 月 25 日確定、最終版発行 [58]。
- NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers: 2020 年 5 月 29 日確定、最終版発行。 製造業者が IoT デバイスを顧客に販売する前にセキュリティ強化のため実施が推奨される 6 つの活動を示す [59]。
- NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline: 2020 年 5 月 29 日確定、最終版発行。 セキュリティ確保のため IoT デバイスに求められる機能類 (features and functions)を示す。

(2) 本事業実施期間中に確定した文書類

- NISTIR 8259B Non-Technical Supporting Capability Core Baseline: 2021 年 8 月 25 日確定、最終版発行 [60]。NISTIR 8259B 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。
- NIST SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements: 2021 年 11 月 29 日確定され最終版発行
- SP 800-213A IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog: : NISTIR 8259D (Draft)[27] の主旨を Appendix A に収容し、SP800-213 の分冊として 2021 年 11 月 29 日確定、 発行 [61]
- NISTIR 8259D (Draft) Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government: 上述の SP 800-213A Appendix A に収容の上 2021 年 11 月 29 日撤回 (withdrawn)

(3) 現在公開中の Draft

- NISTIR 8259C (Draft) Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline[62]

4.1.3.2 IoT Program 以外の NIST 内の動向

NIST の IoT Program は NIST において IoT を取り巻くいわゆるサイバーセキュリティに関する活動を行っている。IoT Program 以外で SIP-CPS に関連する NIST の動向として次の動きがみられた。

- NIST SP 800-218 Secure Software Development Framework (SSDF) Version 1.1 が 2021 年 9 月 30 日に Draft 公開、同 11 月 5 日を締め切りとしてパブリックコメントが受け付けられ [63]、翌 2022 年 2 月 3 日に最終版が確定、公開された [64]。

---

58. NISTIR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks: <https://csrc.nist.gov/publications/detail/nistir/8228/final>

59 「6 つの活動」のうち、Activities 1~4 は Primarily Pre-Market Impact, Activities 5~6 は" Primarily Post-Market Impact"と分類される。

60. NISTIR 8259B IoT Non-Technical Supporting Capability Core Baseline <https://csrc.nist.gov/publications/detail/nistir/8259b/final>

61. SP 800-213A IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog <https://csrc.nist.gov/publications/detail/sp/800-213a/final>

62. <https://csrc.nist.gov/publications/detail/nistir/8259c/draft>

63. <https://csrc.nist.gov/publications/detail/sp/800-218/draft>

64. <https://csrc.nist.gov/publications/detail/sp/800-218/final>

- NIST SP 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations Rev.1(2nd Draft)が進行中。2021 年 10 月 28 日に Draft が公開され、同 12 月 10 日までコメントが受け付けられた。
- Federal Register にて、”Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management”が RFI として NIST より 2022 年 2 月 22 日に公告。　応募締め切りは 2022 年 4 月 25 日とされる[41]。

4.1.3.3 Executive Order 14028 の影響[3]

2021 年 5 月 12 日発行の Executive Order 14028（EO 14028 と表記）に対応、呼応して、報告対象期間中 NIST の活発な活動が観察された[65]。調査期間の前半は Delta Variant が、後半は Omicron Variant がアメリカ各地で感染猛威を振るったにもかかわらず、かなり迅速な動があった。EO 14028 との関連あるいは影響が認められる動向を以下に記す。

(1) EO 14028 に呼応して発行された Consumer IoT Labeling に関わる文書類

- Critical Software Definition （2021 年 6 月 25 日）[66]
- Security Measures for “EO- Critical Software” use （2021 年 7 月 9 日)[67,68]
- Guidelines on Minimum Standards for Developer Verification of Software （2021 年 7 月 9 日）[69,68]
- DRAFT Baseline Security Criteria for Consumer IoT Devices (2021 年 8 月 31 日)[70]：最初のドラフト
- Consumer Cybersecurity Labeling for IoT Products: Discussion Draft on the Path Forward (2021 年 12 月 3 日)[28]：更新されたドラフト
- NIST Cybersecurity White Paper: Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products :最終版[37]

(2) EO 14028 に呼応して NIST が実施[71]した活動

- Workshop on Cybersecurity Labeling Programs for Consumers: Internet of Things (IoT) Devices and Software (2021 年 9 月 14~15 日)[72]
- Improving the Nation’s Cybersecurity: Progress and Next Steps in Carrying Out Executive Order (2021 年 10 月 14 日)[19]
- Executive Order 14028: Guidelines for Enhancing Software Supply Chain Security (2021 年 11 月 8 日)[22]
- Cybersecurity Labeling for Consumer IoT and Software: Executive Order Update and Discussion (2021 年 12 月 9 日)[29]

---

65. <https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity>
66. <https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition>
67. <https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eo-critical-software-use-2>
68. <https://www.nist.gov/news-events/news/2021/07/nist-delivers-two-key-publications-enhance-software-supply-chain-security>
69. <https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/recommended-minimum-standards-vendor-or>
70<https://www.nist.gov/system/files/documents/2021/08/31/IoT%20White%20Paper%20-%20Final%2020210-08-31.pdf>
71. EO 14028 に関する NIST ITL portal site <https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity>
72. <https://www.nist.gov/news-events/events/2021/09/workshop-cybersecurity-labeling-programs-consumers-internet-things-iot>

4.1.3.4 Whitehouse の動向

前述の EO 14028、あるいは Supply Chain に関する EO14017 以外の目立った Whitehouse の動向を以下に示す。

(1) バイデン大統領と IT 企業等民間幹部との会合

- 2021 年 8 月 25 日、Whitehouse にて実施。
- バイデン大統領とアメリカ主要 IT 企業並びにサイバー保険を提供する保険会社など、アメリカのいわゆるサイバーセキュリティに深く関係する企業トップとの会談。
- 会議後公開された Factsheet によると 11、民間企業各社がこれから実施することが列挙されているが、サプライチェーン、Zero Trust, 並びにユーザーへの教育、啓発が主要な傾向としてみられる。

(2) White House Meeting on Software Security[73]

- 2022 年 1 月 13 日、Whitehouse にて実施。
- 2021 年末から話題となった、Apache Log4j の脆弱性問題に端を発し、National Security Advisor Jake Sullivan 氏が招集、Deputy National Security Advisor Anne Neuberger 氏が主導したと報道されている。
- Apache Log4j 脆弱性の影響範囲は確定できていないが、Appliances を含むいわゆる IT 向け Hardware が利用するソフトウェア、並びにアプリケーション並びにサービスが対象で、SIP-CPS の対象領域との直接的あるいは密接な関連性は認められない。

Log4 脆弱性の影響範囲はサーバ類､IT 機器類を中心としているが､複数の ICS への Log4j 脆弱性の影響が会合前 1 月初めには既に知られていた [74]。また、Log4j に類似した IoT 類に広範に影響しうる脆弱性として Kcode の NetUSB に存する RCE 脆弱性 (CVE-2021-45608)[75] が会合前の同 11 日に公開されており、Log4j 脆弱性と同様の影響が発生した場合には、同様の対策が必要となることが想定された。

(3) National Security Memorandums

下記の 2 件の National Security Memorandum が発行された。国家安全保障に関する Memorandums であり、IoT に限定されるものではなく、連邦情報システム全体に関わるものである。

- National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems[1] (2021 年 7 月 28 日発行)
  - 対象は Critical Infrastructure の ICS だが、冒頭に"the systems that control and operate the critical infrastructure on which we all depend"とあり、既存の ICS の概念以上に拡大される可能性がある。
  - この Goals は、Critical Infrastructure Owners and Operators が守るべき(should) Baseline

---

[73]. 会議後 Whitehouse からの発表 <https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/>

[74] 例えば、ICS Vendors Respond to Log4j Vulnerabilities <https://www.securityweek.com/ics-vendors-respond-log4j-vulnerabilities>

[75]. CVE-2021-45608 | NetUSB RCE Flaw in Millions of End User Routers (SentinelOne on January 11, 2021): <https://www.sentinelone.com/labs/cve-2021-45608-netusb-rce-flaw-in-millions-of-end-user-routers/>, NetUSB (USB Over IP), KCodes <https://www.kcodes.com/product/1/36>

Security Practices であり、ICS とは明示されていない。

- 主な内容として、Industrial Control Systems Cybersecurity Initiative の設立 (Section 2 and 3)、及び Critical Infrastructure Cybersecurity Performance Goals の策定を国土安全保障長官並びに商務長官に命令(Section 4 (a))し、執行宛として NIST 所長を明示。

- Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems[76]
  - EO 14028 に関連し、国家安全システム(NSS)に対する NSA 長官の権限と責任の明確化、強化を確認。
  - NSS で実装されるべき NIST 標準、実装技術が指定され、実装計画提出期限、その他関連する行動並びにその期限が示される。
  - NSS に指定されない連邦システム、民間は適用対象外だが、NSS で利用されるハードウェア、ソフトウェア、サービスを提供する事業者には直接間接の影響が見込まれる。

(4) CRITICAL AND EMERGING TECHNOLOGIES LIST UPDATE

- 2022 年 2 月 7 日、米国の安全保障に直結する重要技術分野の指定が更新された。

4.1.4 欧州の動向

4.1.4.1 英国

2021 年 11 月、英国政府は議会に対し、IoT の統制並びに取締(enforcement)を含む法案を提出した。これにより、IoT に適切なセキュリティ、保護の実装が法制化される可能性、遵守なき場合取り締まりの対象とされる可能性が高まった。英国議会で承認、法制化された場合、EU、米国、他英連邦諸国をはじめ世界各国に影響を与え、各国で法制化、取締強化の動向が加速する可能性がある。法案提出に至る英国政府の動向と内容、政府の懸念などを以下に示す。

(1) 法案提出直前の動向

- 2021 年 11 月 12 日、NCSC Weekly Threat Report 12th November 2021[77]冒頭に、“Majority of IoT device manufacturers fail to provide route to report security flaws”と題する記述が発せられる。この攻撃的とも取れる見出しの報告は、IoT Security Foundation が 11 月 4 日に発行した、“The Contemporary use of vulnerability Disclosure in IoT Report 4”[78]に基づくが、NCSC からの IoT セキュリティを取り巻く現状への強い警鐘でもある。

- 2021 年 11 月 15 日、英国政府 DCMS は、“Cyber resilience captains of industry survey 2021”を発行。Inforsecurity 誌では次のように報道されている。
  - 調査対象英国企業 CEO の三分の一近く(31%)が、彼らの supply chain 中でのサイバ

[76]. <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/>
[77]. <https://www.ncsc.gov.uk/report/weekly-threat-report-12th-november-2021>
[78]. <https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/The-Contemporary-Use-of-Vulnerability-Disclosure-in-IoT-IoTSF-Report-4-November-2021.pdf>

ーリスク管理を実施していない。
- 同程度(35%)の企業で、これらのサイバーリスクが取締役会に伝えられていない。
- サプライチェーンセキュリティの向上を強制する手段として法制化の可能性

(2) 法案公開

- 2021 年 11 月 24 日、“The Product Security and Telecommunications Infrastructure (PSTI) Bill” 法案が公開される。当該法案は製造者、輸入者、流通者に対し、一般消費者向け接続可能な機器類のセキュリティ機能実装を義務付け、柔軟に技術の進歩に応じることができる枠組みを提供し、取締を含むとされる。当法案は、英国が 2018 年に IoT 利用の心得、留意点として導入し、ETSI での標準化の原典ともなった Code of Practice for Consumer IoT Security[79]の趣旨に基づく。
- 必要な手続きの後、女王陛下の承認後 12 ヶ月の猶予が IoT 製造者、輸入事業者、流通事業者などに与えられる。

これにより、Code of Practice for Consumer IoT Security の趣旨と原則は ETSI により欧州標準となり、英国においては法案提出に至ったこととなる [80]。

4.1.4.2 ENISA

Cybersecurity に関わる様々な分野で活動が見られ、SIP-CPS に関連するものとして、ENISA より Threat Landscape for Supply Chain Attacks が 2021 年 7 月 29 日に発行された。Solarwinds インシデントの余波が冷めやらぬ中、毎年 ENISA より発行されている Threat Landscape Report の別冊として先行して発行された。

同じ 7 月 29 日に Threat Landscape for Supply Chain Attacks、”Methodology for Sectoral Cybersecurity Assessments, EU Cybersecurity Certification Framework”が発行されている。産業別、業界別（Sectoral）に、EU Cybersecurity Act（CSA）で定められる EU Certification Scheme に準拠しつつ、それぞれの業界に適した Certification Scheme を作成する参考書という位置付けで強制力はない。しかし、本格的な EU Certification Schemes 導入の具体的な導入の契機となると予想され、継続的は動向の確認が必要と考えられる。

2021 年 12 月 2~3 日には、例年同様に ENISA Cybersecurity Certification Conference 2021 が開催された。

4.1.4.3 ETSI

2020 年 6 月 30 日に ETSI Technical Committee on Cybersecurity (TC CYBER) が作成し公開された

---

[79].<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf>
[80]. 議会での審議状況 <https://bills.parliament.uk/bills/3069>

ETSI EN 303 645: CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements[81]の関連付属文書類のうち、ETSI TS 103 701 Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements が 2021 年 8 月に最終版として確定した模様。 これは、ETSI EN 303 645 の定める Consumer IoT Baseline requirements への適合試験 (Conformance testing) 実施の手順、要領について具体的に規定する。 関連 ETSI 標準との関連は Figure 1 に示されている。

作業は進捗しているものの未だ草稿段階にある文書類として次がある。

- DTR/CYBER-0057 (TR 103 621) Guide to Cyber Security for Consumer Internet of Things[82]
  初期草稿 (Early Draft)とされ、6 月に contribution が提出されて以降更新が見られない。

更に会員外に内容は公開されていないが、関連する文書としては以下がある。

- DTS/CYBER-0014 (TS 103 486) Identity Management and Discovery for IoT[83]
  Stable Draft で、2021 年 9 月には２件の contributions の提出が記録され、まだ議論が継続中と類推される。

4.1.4.4 その他

IoT に限定されてはいないが、European Systemic Review Board (ESRB)が欧州金融機関向けとして、Pan European Systemic Cyber Incident Coordination Framework (EU-SCISF)の発足を 2022 年 1 月 27 日に勧告 [84]。EU-SCISF は欧州連合内の金融当局、関係政府並びに国際金融組織等との Incident Coordination を強化し、EU Cyber Incident Response Frameworks を補完するものと位置付けられる。金融機関、ECB を中心とする金融規制当局などに接続されている IoT 機器類に由来し大規模インシデントが発生した場合は当該勧告の対象となる。本勧告の作成と同じ時期にウクライナをめぐる危機で、サイバー攻撃や金融制裁が議論されており、金融機関以外の重要インフラストラクチャ分野でも同様の動きがなされるかどうか、動向を注視することが必要と考えられる。

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

---

81. <https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf>
82. <https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=59473>
83. <https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=47653>
84 報道発表<https://www.esrb.europa.eu/news/pr/date/2022/html/esrb.pr.220127~f1548f677e.en.html>
勧告本文
<https://www.esrb.europa.eu/pub/pdf/recommendations/esrb.recommendation220127_on_cyber_incident_coordination~0ebcbf5f69.en.pdf/>
報道例 <https://www.bleepingcomputer.com/news/security/eu-to-create-pan-european-cyber-incident-coordination-framework/>

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[85]）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 [86]。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[87]）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 [88]、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基づく標準を策定する傾向にある [89]。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。

---

85 <https://www.govinfo.gov/content/pkg/PLAW-104publ113/pdf/PLAW-104publ113.pdf>
86 <https://www.nist.gov/itl/standards-activities>
87 <https://www.epa.gov/laws-regulations/summary-administrative-procedure-act>
88 <https://www.nist.gov/itl/procedures-developing-fips-federal-information-processing-standards-publications>
89 <https://www.wiley.law/alert-3496#_ftn23>

NIST は商務省の傘下組織として、首都ワシントンに程近い Gaithersberg, Maryland、並びに Boulder, Colorado に大規模なキャンパスを有し[90]、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[91]。このうち、情報技術研究並びに標準化を行う Information Technology Laboratory[92]（以下 ITL と略記）が、Cybersecurity for IoT Program[93]（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[94]（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。

[90] <https://www.nist.gov/about-nist/visit>
[91] <https://www.nist.gov/about-nist/our-organization>
[92] <https://www.nist.gov/itl>
[93] <https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program>
[94] <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf>

NIST National Institute of Standards and Technology：米国国立標準技術研究所

CNST：ナノスケール科学技術センター

PML：物理計測研究所

CNR:中性子研究センター

EL：エンジニアリング研究所

CTL：通信テクノロジー研究所

MML：材料計測研究所

ITL：情報技術研究所 Information Technology Laboratory

CSD（Computer Security Division）

コンピュータセキュリティに関して研究を行い各種文書を発行

FIPS（Federal Information Processing Standards）

米国商務長官の承認を受けてNISTが公布した情報セキュリティ関連の文書。民間企業にとっても情報セキュリティ対策を考える上で有用な文書。

Special Publications （SP800シリーズ）

CSDが発行するコンピュータセキュリティ関係のレポート。米国の政府機関がセキュリティ対策を実施する際に利用することを前提としてまとめられた文書。

NIST IRs(NIST Interagency Reports)

NISTの各内部機関がまとめたレポート

ITL Security Bulletins

不定期に発行されるCSDの会報

図 1 NIST 発行の文書種類

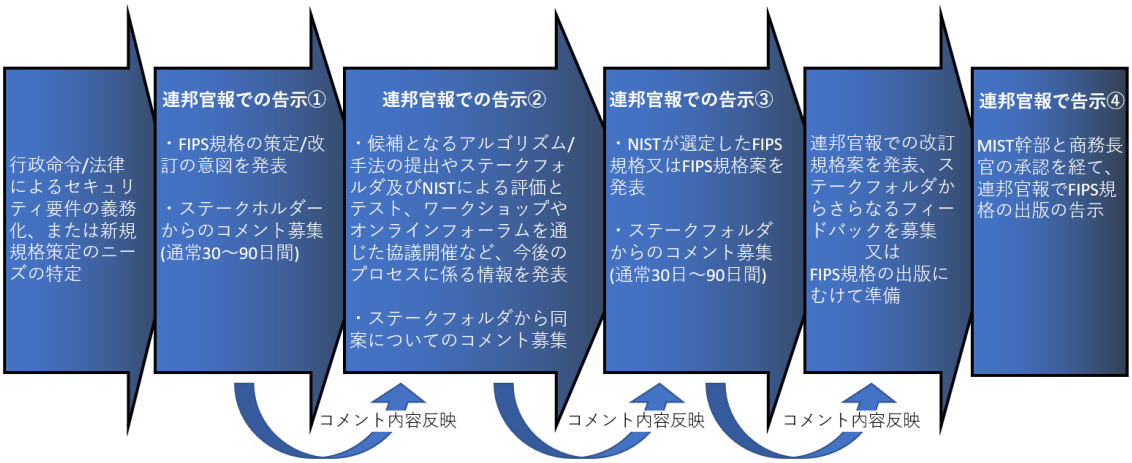


図 2 NIST IoT Program におけるガイドライン・標準策定プロセス

(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[95]（以下 FISMA と略記）がある。Office of Management and Budget[96]（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[97] 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[98]。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[99]（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

---

95 <https://www.cisa.gov/federal-information-security-modernization-act>
96 <https://www.whitehouse.gov/omb/>
97 <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf>
98 <https://www.ipa.go.jp/security/publications/nist/fisma.html>
99 <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf>

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[100]が 2020 年 12 月 15 日の公開された

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[101]（NCCoE）主催のワークショップや、Consumer Technology Association[102]（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。

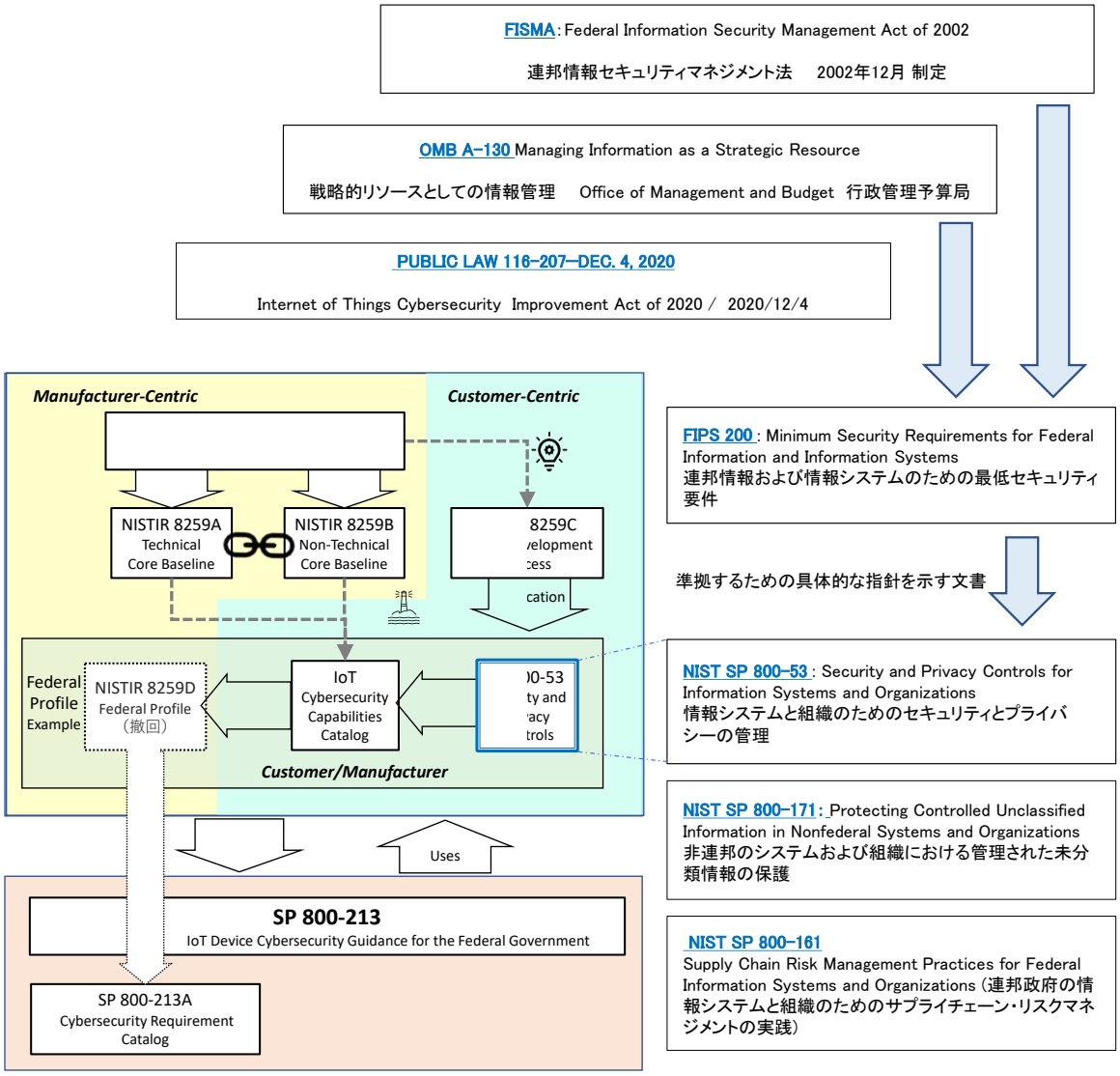
さらに、NIST SP 800-213 は 2021 年 11 月 29 日に最終版発行が発行され、その分冊として SP 800-213A も同日に発行された。SP 800-213A の Appendex には、NIST IoT Program が作成を行ってきた NISTIR 8259D (Draft)の内容が移管されて、NISTIR 8259D は撤回された。

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。

---

100 <https://csrc.nist.gov/publications/detail/sp/800-213/draft>
101 <https://www.nccoe.nist.gov/about-the-center>
102 <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)[103]（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。

さらに、2021 年 2 月 21 日に NIST blog で公開された“2021: What’s Ahead from NIST in Cybersecurity and Privacy?”[104]と題された NIST の 2021 年の活動計画では横断的な標準化活動に取り組むことが示されている。

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)[105]

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[106] し、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、

---

[103] <https://csrc.nist.gov/publications/detail/nistir/8200/final>
[104] <https://www.nist.gov/blogs/cybersecurity-insights/2021-whats-ahead-nist-cybersecurity-and-privacy>
[105] <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/>
[106] <https://thehill.com/policy/technology/538474-biden-to-sign-executive-order-addressing-chip-supply-chain-shortage>

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。

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[107] 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)108

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 所長に命じられている。この検討にあたり FTC（公正取引委員会）の議長と連携して実施するようにとも命令されており、IoT 製品の security 能力の labeling が連邦政府内で検討されている可能性がうかがえる。

NIST はこれに対し、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[109]を発行して、一般消費者向けソフトウェアラベリングに関する 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ラベリングプログラム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

---

[107] <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>

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

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

Consumer IoT Devices を発表[110]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 Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products[111] として消費者向け IoT ソフトウェア製品のサイバーセキュリティラベリング推奨基準の最終版を発行し、大統領令の 1 年後に当たる 2022 年 5 月 12 日までに、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、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ラベリングに関する総括報告書を発行するとしている。これらの大統領令に対する NIST の活動は Improving the Nation's Cybersecurity: NIST's Responsibilities under the May 2021 Executive Order[112]として公開されている。

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

---

110. <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>

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

112 <https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity>

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

- 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 5 に示す。

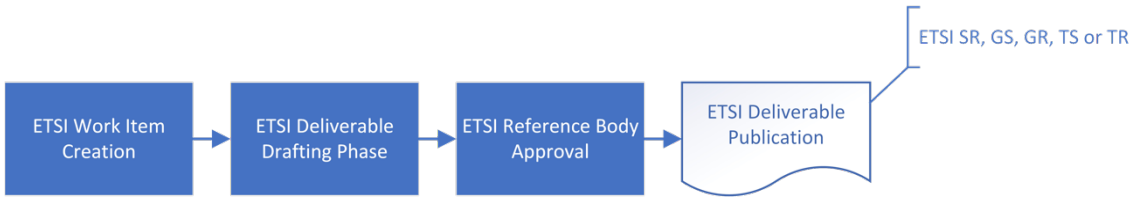


図 5 技術仕様(TS)、技術レポート(TR)、グループ仕様(GS)、グループレポート(GR) 及び特別レポートの承認手順

● 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 6 に示す。

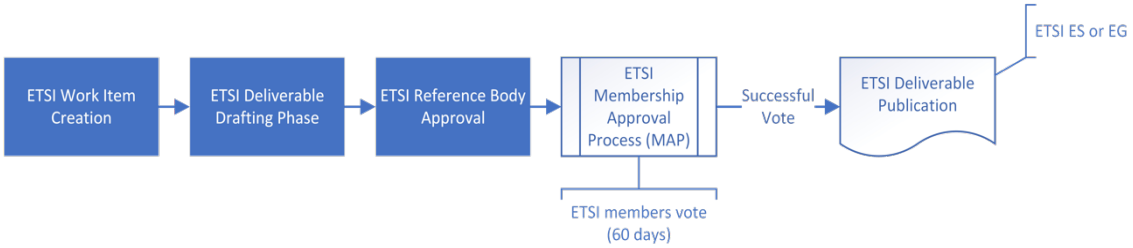


図 6 ETSI ガイド(EG) 及び ETSI 規格(ES)の承認手順

● 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[113]）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 7 に示す。

[113] <https://portal.etsi.org/TB-SiteMap/NSO/Home>

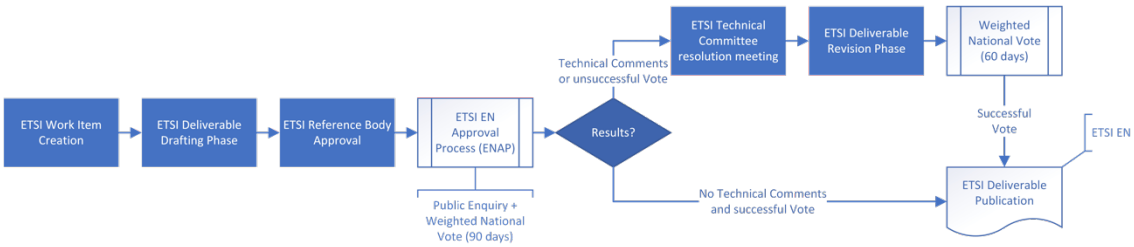


図 7　欧州規格(EN)の承認手順

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。

4.2.3.2　業界団体（GSM Association）

IoT セキュリティ及びサプライチェーンセキュリティに関連する活動を行っている業界団体で、IoT セキュリティガイドラインを公開している組織として GSM Association（GSMA と略記）があり、その標準に関わる活動を調査した。

GSMA は、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である。GSMA は世界の 220 ヶ国で展開しており、800 社近くの移動体通信事業者や端末製造ベンダー、ソフトウェア企業、装置プロバイダー、インターネット企業、メディアやエンタテインメント企業といった関連産業に属する企業 200 社以上が加盟している。

図 8 にモバイル関連の標準化に関わる標準化関連団体の一つである 3GPP を中心とした関連を示す。詳細なベンダー仕様を含めた新しいサービスなどは、あらかじめ 3GPP と GSMA が連携して議論し、その中で標準化、勧告化すべき欧州共通の仕様を ETSI 標準とする。さらに国際的に共通化すべき事項を ITU 勧告として定める（アップストリーム活動）。この動きは図 8 の GSMA →3GPP→ETSI→ITU の流れとなる。

また、この動きとは逆に、国際協調すべき概念を定め、それに応じ勧告、標準を策定する場合 ITU、ISO/IEC などで先行的に議論し、地域、ベンダー仕様と詳細仕様を定めるアプローチ（ダウンストリーム活動）もある。

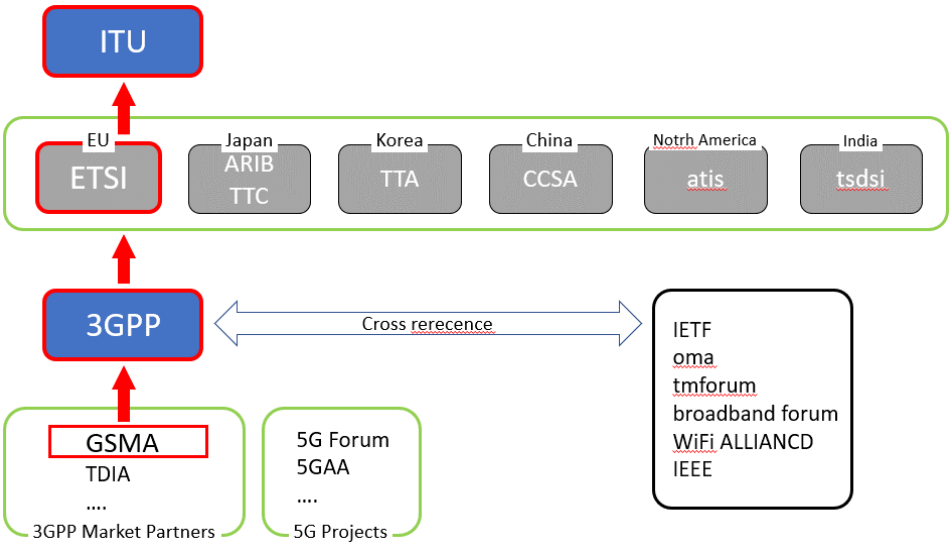


図 8 モバイル関連の標準化団体の 3GPP を中心とした関連

3GPP の図[114]を参考にアップストリーム活動（GSMA→3GPP→ETSI→ITU）を朱書きで示す

GSMA と 3GGP の関係を NESAS（Network Equipment Security Assurance Scheme）を例に図 9 に示す。NESAS は産業界全体としてセキュリティレベルの向上を促進するためのセキュリティ保証のフレームワークである。下位層の仕様として、GSMA で主にベンダーが共通に有するべき要件や仕様を定め、仕様の適用方法の確立と監査人の指名とテストラボのリスト化を行っている。3GPP では上位層として、機器のセキュリティ要件とテストケース、セキュリティ保障仕様を定めている。このように、GSMA では 3GPP と連携、協調した仕様化していることが多くみられる。

[114] <https://www.3gpp.org/ftp/Information/presentations/presentations_2018/2018_10_17_tokyo/presentations/2018_1017_3GPP%20Summit_02_Key%20Note_SCRASE.pdf>

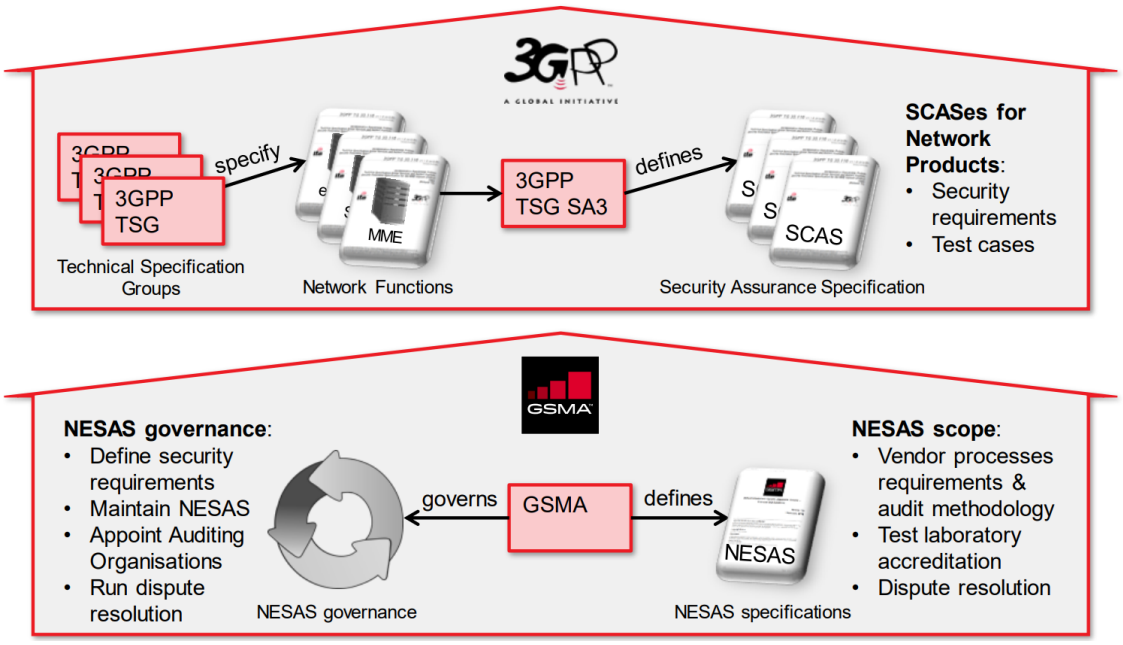


図 9 仕様に関する 3GPP-GSMA の役割

GSMA Network Equipment Security Assurance Scheme (NESAS)[115]

4.2.3.3 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）[116] 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[117]（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

115 <https://www.gsma.com/security/wp-content/uploads/2021/02/FS.13-NESAS-Overview-v2.0.pdf>
116 <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre>
117 <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>

across the Union [118]（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[119]（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。

- GUIDELINES FOR SECURING THE INTERNET OF THINGS Secure supply chain for IoT[120]（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 [121]（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 [122]（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[123]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

---

[118] <https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union>
[119] <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391>
[120] <https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things>
[121] <https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1>
[122] <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>
[123] <https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-2020_en>

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[124]（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 Copetence Centre/Network（ECCC)[125]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。

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おける取り組みが顕著であり、その中核に NIST IoT Program（以後 IoT Program と略記）がある。NIST は米国の国立標準技術研究所であるが、その制定プロセスに海外

[124] <https://euroalert.net/call/3643/call-for-proposals-2017-h2020-cybersecurity>
[125] <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre>

からの参加が可能で、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、連携を進めるべき重要なステークホルダーとして NIST および IoT Program を位置付けることができる。

しかし、IoT Program の責任者の Katerina Megas 氏とその一部の関係者を除き、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はいない。連携を進めるためには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。

なお、米国の CISA（Cybersecurity & Infrastructure Security Agency）の ICT Supply Chain Risk Management Task Force（ICT SCRM タスクフォースと略記）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。

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つつあり、これらの初期草案に本プロジェクトの活動成果を盛り込むことは難しい段階にきていると思われる。しかしながら、それらの具体運用や今後の改定フェーズにおける連携を考える上でも、現時点からでもこれらの制定プロセスにて NIST へのアプローチを行うことは今後の連携・協力関係の構築を図る上で重要であると考えられる。

このためにも、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整理し取りまとめることで、SIP-CPS 活動の有効性を確認し関係機関に伝えていく必要がある。また、これらの技術成果のとりまとめは、本プロジェクトの研究開発担当メンバーを中心に進める必要があると考えられる。

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 standardisation) プロジェクトと連携した活動が行われている。例えば、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」では、昨年 6 月に「IoT セキュリティ」をテーマとして日欧相互の関連技術者の技術交流が行われる等の動きがみられている。

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、既存の IoT Program と並行して、2021 年の大統領令に伴う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に関する新たな動きが現れてきている。

バイデン大統領は、2021 年 2 月 24 日に大統領令 EO14017 として、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、2021 年 5 月 12 日には、ソフトウェアサプライチェーンのセキュリティと完全性に関連する様々なイニシアチブを通じて米国のサイバーセキュリティを強化する大統領令 EO14028 が発表され、その具体施策として、CPS 分野においては、IoT とソフトウェアに関連するラベリングプログラムの開始を行う動きとなっている。

これらは 2022 年度以降に具体運用が進められることになるが、政府調達案件が対象とは言え、民間製品への波及することは避けられないことから、今後の SIP-CPS 活動にも大きな影響を与えることが予想され、具体運用の方法などについてその動向に注意していく必要がある。

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)が設立されている。

また、IoT 関連の動きとして、ENISA はハードウェア、ソフトウェア、サービスを含む IoT のサプライチェーン全体を対象とした Guidelines for Securing the IoT - Secure Supply Chain for IoT を

2020 年 11 月 9 日に発行している。

また、一般消費者向け IoT に求められるセキュリティ要件を規定した ETSI EN 303 645 が 2020 年 6 月に改訂されている。これらの規定をベースにフィンランドでは IoT 向けのラベリング基準を策定し、既に一部の運用が開始されている状況にある。

以上のような状況から、IoT セキュリティ強化に加え、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今後急速に強化され、特に米国においては連邦システムの調達条件やガイドライン等に反映される可能性が高いと考えられる。これらは SBOM やラベリングなど当初の SIP-CPS のスコープにはないものも含まれており、今後の動向に引き続き注目していく必要がある。

日本においては、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を定めているが、これを調達におけるサプライチェーンのセキュリティとレジリエンスの要件にまで拡張し、米国の連邦システムの調達条件等に対応できるものとすることが、本プロジェクトの成果を海外へ展開しセキュリティを強化する上で重要となる。このためには、米国で実施中のサプライチェーンの潜在的脆弱性レビューの活動が複数の政府機関を対象としていることから、合衆国政府に対して内閣府などからのアプローチも必要と考えられる。また、これと並行して本プロジェクトの成果によりセキュリティを保証する機能を有するサプライチェーンのプラットフォームが、その構築と評価を通じて示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の達成レベル

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／Ｉｏ Ｔ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と、「RSA Conference Announces Finalists for RSAC Innovation Sandbox Contest 2021」の入賞製品を対象に調査を行った。

SIP-CPS の 2021 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

RSA Confarence はセキュリティに関して世界有数の会議であり、そこで注目製品としてセキュ

リティ専門家から高く評価されて入賞した製品を分析することにより先端製品の技術開発レベルを調査することができる。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、IoT デバイスの信頼の創出・証明のための基本機能として必要になり、かつ世界各国からの提案が行われ候補として残っている米国 NIST 公募・評価の IoT 用軽量暗号技術を、B2 の信頼チェーンに係る安全な流通技術に関しては、サプライチェーンの開発がビジネス先行で展開されステークホルダーが参加してユースケースが示されている主要な BlockChain コンソーシアムの製品・技術を、技術を特定することなく信頼の起点をベースに開発している A2、B3、C2 に対しては、同じく信頼の起点をベースする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、調査内容については、SIP-CPS に必須と位置付けられている項目に関して優位性を確認する観点から、セキュリティ強度や、監視対象、監視項目、協調している機能などの調査を行った。

調査対象の一覧を以下に示す。

1. RSA Conference Announces Finalists for RSAC Innovation Sandbox Contest 2021 の入賞 10 製品・企業（以下、RSA2021 製品・企業）
2. 米国 NIST 公募・評価の IoT 用軽量暗号（以下、NIST 公募 IoT 用軽量暗号技術）
3. 主要な BlockChain コンソーシアム（以下、BlockChain コンソーシアム）
4. 欧州の IDSA/GAIA-X の基本コンセプトとユースケース（以下、GAIA-X ユースケース）

5.1.2 調査結果

5.1.2.1 RSA2021 製品・企業 [126]

「RSA Conference Announces Finalists for RSAC Innovation Sandbox Contest 2021」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、2021 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) Abnormal Security[127]

行動データサイエンスを使用して、従来の電子メールゲートウェイでは検出することができない斬新で洗練された電子メール攻撃から企業を保護するクラウドネイティブの電子メールセキュリティプラットフォームである。

ワンクリックで Microsoft365 と GoogleWorkspace に展開し、すぐに結果を提供する。

［考察］

Abnormal Security は、電子メール攻撃に特化した技術である。SIP-CPS との比較候補ではないと

126 <https://www.rsaconference.com/library/press-release/rsa-conference-announces-finalists-for-rsac-innovation-sandbox-contest-2021>

127 <https://abnormalsecurity.com/>

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) Apiiro[128]

Apiiro（米国）は、RSA2021 製品・企業の最優秀製品の提供企業である。

製品名は、CodeRiskPlatform™であり、設計からコード、クラウドに至るまで、あらゆる変更にリスクの可視性を提供する。

本製品の売りは、完全なリスクの可視性と重要なリスクに抽出であり、アプリケーション、インフラストラクチャ、オープンソースコード全体のセキュリティとコンプライアンスのリスク、開発者の経験、およびビジネスへの影響を 360 度見渡せる。

Apiiro が提供する完全なリスクの可視性については、データ駆動型の意思決定により、より良い意思決定を行う。アプリとインフラコードの動作のリアルタイムインベントリ、開発者の知識、サードパーティのセキュリティアラートとビジネスへの影響を使用して、デザインからコード、クラウドまでの、セキュリティとコンプライアンスのリスクを明らかにする。

Apiiro の重要なリスクの抽出については、すべての変更を確認し、すべてのアラートを調査して、開発者、コード、クラウド全体のコンテキストを分析してリスクのある重要な変更を特定し、実用的な作業計画を自動的に作成する。これにより、専門知識を最大限に活用できる。

重要なリスク抽出の実現手法では、①セキュリティ、コンプライアンス、ビジネスリスクによってアプリに優先順位を付ける、②リスクベースの修復決定を行う、③アプリとクラウドセキュリティプログラムの効率を測定する、の３つの特徴を有している。

自動ガバナンスとリスク修復では次の６つの特徴を有する。

①Prioritize changes for sec reviews：秒単位での変更に優先順位付け

②Narrow pen-testing scope：絞ったテスト観点

③Reduce noise of SAST tools：静的アプリケーションセキュリティ解析ツールのノイズ削減

④Remediate risky material changes：危険な重要な変更の修正

⑤Identify cloud misconfiguration：クラウドの構成ミスの特定

⑥Assure regulatory compliance：規制コンプライアンスを保証

［考察］

Apiiro は、設計からコード(開発時)、クラウド（運用時）に至るまで、あらゆる変更に対するリスクの可視化という特徴を有している。SIP-CPS の研究開発項目 A2 では、特徴的な技術として真贋判定機能を提供しており、比較対象候補と考えられる。

(3) Axis Security[129]

Axis Security は、アプリへのアクセスに新しくシンプルなアプローチを提供する。

ゼロトラストアプローチに基づいて構築された AppAccess Cloud は、VPN、VDI、ネットワークの変更、またはすべてのデバイス上のエージェントを必要とせずにユースケースを可能にする。

---

128 <https://apiiro.com/>

129 <https://www.axissecurity.com/>

［考察］

Axis Security は、アプリへのアクセスに特化した技術である。SIP-CPS との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。

(4) Cape Privacy[130]

Cape Privacy は、グローバルな暗号化学習プラットフォームである。

これにより、企業は、専有データや機密データを危険にさらすことなく、機械学習モデルで共同作業を行うことができる。企業はデータモデルを充実させ、ビジネス価値を高めるために外部の関係者とデータを共有するため、Cape のプラットフォームではプライバシーがデフォルトで保護されている。

［考察］

Cape Privacy は、グローバルな暗号化学習プラットフォームであり、AI を組み込んだすべてのアプリの学習時のセキュリティリスクに対応できる技術である。SIP-CPS との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。

(5) Deduce[131]

Deduce は、アカウントの乗っ取り、データ漏洩、および ID 詐欺を防御する。

5 万を超える Web サイトと 10 億を超える毎日の認証済みユーザーイベントの包括的な消費者データネットワークを利用して、企業が ID ベースの脅威インテリジェンスの総合力を活用できるようにする。

［考察］

Deduce は、ID ベースの脅威を抑えることに特化した技術である。SIP-CPS との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。

(6) Open Raven[132]

Open Raven は、データレイクとウェアハウスの可視性と制御を復元することを目的としたクラウドネイティブデータプラットフォームである。

Open Raven は、セキュリティチームとクラウドチーム向けに構築されており、データ漏洩の防止やコンプライアンス目標の達成などのセキュリティタスクを自動化しながら、インベントリや分類などのデータガバナンスアクティビティを簡単にする。

［考察］

Open Raven は、データ漏洩の防止やコンプライアンス目標の達成などに焦点を縛った技術である。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。

---

130 <https://capeprivacy.com/>
131 <https://www.deduce.com/>
132 <https://www.openraven.com/>

(7) Satori[133]

Satori は、最新のデータインフラストラクチャにデータアクセス、セキュリティ、プライバシーを提供する。

Satori のユニバーサルデータアクセスサービスにより、企業は DataOps を採用し、データへのアクセスを合理化すると同時に、資格、分類、およびセキュリティを自動化できる。

［考察］

Satori は、データアクセスサービスのセキュリティ達成に焦点を縛った技術である。SIP-CPS との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。

(8) Strata[134]

Strata の Maverics Identity Orchestration Platform は、分散型マルチクラウド ID の ID オーケストレーションである。

Maverics Identity Orchestration Platform を使用すると、企業はオンプレミスとクラウドベースの認証およびアクセスシステムを統合して、マルチクラウド環境で一貫した ID 管理を行うことができる。

［考察］

Maverics Identity Orchestration Platformi は、一貫した ID 管理に焦点を縛った技術である。SIP-CPS との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) Wabbi[135]

Wabbi は、DevOps チームにスケーラブルなアプリケーションセキュリティインフラストラクチャを提供する。

具体的には、分析機能として、既存の SecOps および DevOps ツールからの結果とデータを分析して、プロジェクトの属性、およびダウンストリームの意思決定を促進するセキュリティリスクプロファイルを理解する。 確認機能として、既存の DevOps ワークフローで、ポリシーや手順から制御に至るまで、すべてに関する関連情報を表示することで、セキュリティ基準が満たされていることを確信できる。出荷においては、自動化された知識に基づいた意思決定を開発パイプラインに戻し、コードが最新の基準を満たしていることを完全に確認して出荷し続けることができる。

Wabbi の上記の提供機能により、セキュリティとソフトウェアの両方が継続的に進化しているため、CI / CD の一部としてセキュリティ要件を継続的かつ動的に管理し、どのような変更があっ

---

133 <https://satoricyber.com/>
134 <https://www.strata.io/>
135 <https://wabbisoft.com/>

たとしても、コードを常に最新のセキュリティ標準に沿って出荷できるようになる。これにより、企業は俊敏性とセキュリティのどちらかを決定する必要がなくなる。

［考察］

Wabbi は、セキュリティとソフトウェアの両方の継続的な進化に焦点を縛った技術である。SIP-CPS との比較候補ではないが、ソフトウェアのサプライチェーン観点で、連携候補の１つと考えられる。

(10) Wiz[136]

Wiz は、組織、企業のクラウドインフラストラクチャを大規模に保護する。

Wiz の特徴の１つは、リソースやワークロードのパフォーマンスに影響を与えることなく、あらゆるクラウド環境に対応でき、数分で接続し（エージェントやサイドカーは不要)、ビジネスオペレーションを遅くすることなく、クラウドスタックのすべてのレイヤーから情報を収集する。これにより、数分で完全なカバレッジを実装することができる。

次の特徴は、ワークロード、アカウント、および環境全体で、クラウドインフラストラクチャのインベントリを構築し、仮想マシンやコンテナからサーバーレス機能まで、クラウドとコンピューティングアーキテクチャ全体で統一されたカバレッジを提供する。Wiz Security Graph は、クラウドリソースとそのフィールド、および相互接続を表示して、攻撃者が侵害を認識していることを明らかにできる。これにより、Wiz は、クラウド環境全体の攻撃者の侵入を見ることができる。

もう一つの特徴は、セキュリティスタック全体を継続的に分析して、実際のリスクを表す問題のある組み合わせを発見する。クラウドコントロールは、サイロ化されたポリシーを手動で分析する作業を取り除き、実際に重要なアラートの優先リストを提供する。きめ細かいアクセス制御により、チームは複雑な環境をセグメント化し、プロセスとアラートルーティングを合理化できる。これにより、Wiz は、重要なリスクに焦点を当てることができる。

最後の特徴は、エンドツーエンドの可視性により、問題が本番環境に到達するのを防ぐ。組み込みの修復ガイダンスは当て推量を取り除くのに役立ち、オプションの自動修復はシングルクリックで設定ミスの修正をサポートする。また、完全に公開された API、多数の統合、およびカスタム SOAR プレイブックのサポートにより、ワークフローの柔軟性が無制限になり、修復までの時間が短縮できる。これにより、Wiz は、次の脅威を防ぐことができる。

［考察］

Wiz は、IT(クラウドインフラストラクチャ)運用トータルのセキュリティリスクを抑えることに焦点を当てた技術である。対象システムは異なるが、IoT、OT のセキュリティを対象とする SIP-CPS の C2 との連携候補の１つと考えられる。

136 <https://www.wiz.io/>

5.1.2.2 NIST 公募 IoT 用軽量暗号技術

米国 NIST が IoT 用の軽量暗号の公募・評価、標準化を推進している。

米国推奨候補として、優劣の比較評価を行っており、調査時点で評価中の候補は、到達レベルの高い技術・製品と考えられることから調査対象とした。

現時点で候補となっており、確認できたのは、Elefant、Liliput、TGIF の 3 技術である。

NIST の公募・評価については、数年前に、この問題に対処するために軽量暗号というプロジェクトとグループを立ち上げている。このプロジェクトの目標は、現在の NIST 暗号標準に対応できない、制限された環境に適した軽量暗号アルゴリズムを公募、評価、標準化することである。

軽量暗号アルゴリズムの 1 次候補として 56 候補が残っており、調査時点で評価中となっている。名前が分かっている候補の Elephant、Liliput、Thank Goodness It's Friday (TGIF) の概要を以下紹介する。

(1) Elephant[137]

Elephant は、認証付き暗号化スキームである。

暗号化機構/性能については、①LFSR を使用してマスクされた暗号順列を使用し、②スポンジベースの軽量ハッシュに使用される順列の広範な文献に依存して構築されている。

セキュリティ強度については、NIST 軽量呼び出しで推奨されているセキュリティ目標に一致しながら、160 ビットの順列まで小さくすることができる。

具体的には、Elephant のモードは、ナンスベースの encrypt-then-MAC 構造であり、暗号化はカウンターモードを使用して実行され、メッセージ認証は Wegman-Carter-Shoup MAC 機能のバリアントを使用して実行される。どちらのモードも、内部的には LFSR を使用してマスクされた暗号順列を使用する。これは、Granger etal のマスクされた EvenMansour 構造に似ていえる。

このモードは順列ベースであり、この順列を順方向でのみ評価する。そのため、OCB ベースの認証付き暗号化スキームとは異なり、複数のプリミティブまたはプリミティブの逆を実装する必要はない。さらに、これにより、スポンジベースの軽量ハッシュに使用される順列の広範な文献に依存して構築することができる。

しかし、Elephant 自体はスポンジベースではなく、シリアル順列ベースの認証付き暗号化の従来のアプローチとは異なる。 Elephant は設計により並列化可能であり、マスキングに LFSR を使用するため実装が容易であり（有限体の乗算は不要)、最後に、マスキングを正確に実行する方法を洗練された方法で決定できるため効率的である。

理想的な順列モデルのセキュリティ分析は、Elephant のモードが構造的に健全であることを示している。

Elephant は並列化可能であるため、インスタンス化する必要はない。

Elephant with a large permutation：

NIST 軽量呼び出しで推奨されているセキュリティ目標に一致しながら、160 ビットの順列まで

---

[137] <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/elephant-spec.pdf>

小さくすることができる。

Elephant スキームは次の 3 つのインスタンスで構成されている。

1.Dumbo: Elephant-Spongent-π.

このインスタンスは、セキュリティ分析で指定された最小順列サイズを満たしている。オンラインの複雑さが最大で約 246 ブロックであれば、112 ビットのセキュリティを実現する。Spongent と同じく、このインスタンスはハードウェアに特に適している。

2.Jumbo: Elephant-Spongent-π

これは Elephant のもう少し保守的なインスタンスである。同じ順列ファミリーに基づいているが、オンラインの複雑さに関する同じ条件下で 127 ビットのセキュリティを実現している。なお、Spongent-πは ISO / IEC 標準化されている。

3.Delirium: Elephant-Keccak-f

この変異体は、ハードウェアで十分に機能するが、ソフトウェアの使用に向けて開発されている。 Keccak-f でインスタンス化された Elephant も、127 ビットのセキュリティを実現し、オンラインの複雑さの上限は約 270 ブロックである。順列は、NIST SHA-3 標準の最小のインスタンスであり、今回のニーズに適合している。

Dumbo は主要な提出物である。各順列は比較的小さいため、並列処理をサポートしているにもかかわらず、Elephant のすべてのバージョンの状態サイズは小さくなっている。マスキングに使用される LFSR は、特定のインスタンスに合わせて調整される。

また、特定の暗号順列で適切に動作するように開発されている。たとえば、Spongent インスタンスとペアになっている LFSR は、状態更新のために実行する必要のある XOR 操作の数を最小限に抑えるように選択されているが、Keccak ベースのインスタンスはソフトウェアプラットフォームで適切に実行されるように選択されている。

Elephant の 3 つの暗号化順列は、暗号化ハッシュにも使用できる。Spongent と Keccak はスポンジだが、小さな順列を求めているため、これらの暗号化ハッシュ関数は、認証済み暗号化スキームによって保証された 112、127 ビットのセキュリティレベルを満たすことができない。 または。少なくとも 112 ビットのセキュリティでスポンジベースのハッシュを実行するには、少なくとも 225 ビットのサイズの暗号順列を使用する必要がある。

(2) Liliput[138]

調整可能なブロック暗号 Lilliput-TBC に基づく新しい AEAD(Authenticated Encryption with Associated Data) スキームである。その特徴は、①実装配備された暗号化コンポーネントをより簡単に管理、②暗号化コミュニティによって大幅に研究された構築スキーム（認証暗号化モード、暗号化プロセス）に基づく、③誤用防止モードを有する、の 3 つが挙げられる。

暗号化機構/性能については、①8 ビット（Atmel AVR ATmega128 など）/16 ビット（Texas Instruments MSP430F1611 など）プラットフォームでのソフトウェア実装、②実行時間（消費電力

[138] <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/LILLIPUT-AE-spec.pdf>

に関連）:ACORN および Ascon に匹敵、③実装：認証モードのないプレーン AES のシリアル実装と同等、としている。

その他の特徴として、①サイドチャネル保護が容易、②フォールトインジェクション：最後の 7 ラウンドを保護（実行時間オーバーヘッドは 22%)、としている。

(3) Thank Goodness It's Friday (TGIF) [139]

調整可能なブロック暗号（TBC）TGIF-TBC に基づく関連データ（AEAD）スキームを使用した認証済み暗号化である。

暗号化機構/性能については、TGIF-TBC に適用される ICE と呼ばれるモードがあり（ブロック暗号)、これにより理想的暗号モデルに依存するセキュリティ証明を犠牲にし、スキーム全体のサイズを縮小できる（完全な n ビットセキュリティを提供)、としている。

セキュリティ強度については、Liliput と同等と思われる。

［考察］

米国 NIST が IoT 用の軽量暗号の公募・評価の候補として残っている、Elephant、Liliput、Thank Goodness It's Friday (TGIF) については、SIP-CPS の実施項目 A1 が採用している楕円暗号とは異なるが、セキュリティ強度や実装規模など、比較対象の候補と考えられる。

5.1.2.3 BlockChain コンソーシアム

BlockChain 技術は、複数の利害者間で、データ主権を維持してセキュアに交換・開示する技術として注目され、業界を連携させるセキュアなサプライチェーンを目指したコンソーシアムが多数確認できている。

その中で、現時点でも成長を維持している BlockChain コンソーシアムは、セキュアな技術、運用や、業界への親和性や使　い勝手の良さなどが評価されていると考えられる。この観点から、運営が活発な BlockChain コンソーシアムを、技術の到達レベル評価のための調査対象とした。

以下、運営が活発な 5 件の BlockChain コンソーシアム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) Hyperledger[140]

Hyperledger は、界間のブロックチェーン(BC)技術を推進するために作成されたオープンソースの共同の取り組みであり、Linux が 2016 年に設立した。金融、銀行、IoT、サプライチェーン、製造、テクノロジーを含む、Linux 財団が主催するグローバルなコラボレーションである。

---

[139] <https://csrc.nist.gov/CSRC/media/Events/lightweight-cryptography-workshop-2019/documents/papers/updates-on-romulus-remus-tgif-lwc2019.pdf>

[140] <https://www.hyperledger.org/>

アクティビティとしては、誰でもプロセスに参加 OK で、インキュベーションフェーズがあり、段階的な成長に向け、6 種のライフサイクルプロセス（建議、潜伏、卒業、休眠、廃止、終末期）を規定している。卒業プロジェクトについては紹介サイトがある。

代表的な例として、①ドバイのデジタルシルクロードは、Hyperledger Fabric との貿易 vv 近代化を進めており、②Kiva は、Hyperledger Indy とアフリカ初の国家分散 ID システムを起動している。また、③DLT ラボ™&ウォルマート カナダは、Hyperledger Fabric で貨物請求書管理の変革を目指し、④openIDL は、Hyperledger Fabric を使用して米国の保険業界向けの規制報告を合理化し、⑤医薬品サプライチェーンに最適な台帳ドメインの Hyperledger Fabric ソリューション、⑥ハネウェル航空宇宙は、Hyperledger Fabric でオンライン部品市場を作成している。

Hyperledger の工夫点・注視点としては下記がある。

① Hyperledger Besu には、PoW、PoA (IBFT、IBFT 2.0、エサハッシュ、クリーク) を含むいくつかのコンセンサス アルゴリズムを有する。
② Hyperledger Burrow は、シンプルさ、スピード、開発者のアーゴノミクスに焦点を当てた完全な単一バイナリブロックチェーンディストリビューションを有する。
③ Hyperledger Fabric では、コンセンサスやメンバーシップサービスなどのコンポーネントをプラグ アンド プレイにできる。そのモジュール式で多目的な設計は、幅広い業界ユースケースに対応可能である。
④ Hyperledger Indy は、管理ドメイン、アプリケーション、およびその他のサイロ間で相互運用可能なように、ブロックチェーンやその他の分散型台帳に基づいてデジタル ID を提供するためのツール、ライブラリ、再利用可能なコンポーネントを提供する。
⑤ HyperLedger Iroha は、独自のコンセンサスと注文サービス アルゴリズム、豊富なロールベースのアクセス許可モデル、およびマルチシグネチャ サポートを備えた、使いやすいモジュラー分散型ブロックチェーン プラットフォームを提供する。
⑥ Hyperledger Sawtooth は、柔軟でモジュール式のアーキテクチャを提供し、アプリケーションドメインからコア システムを分離するため、スマート コントラクトは、コア システムの基になる設計を知らなくてもアプリケーションのビジネス ルールを指定できる。

Hyperledger の活動メンバーは 97 社（2021 年調査時点）あり、プレミアムメンバーは、IBM、アクセンチュア、富士通、日立、DTCC、consensys、JPM の 7 社となっている。

［考察］

Hyperledger では、コンセンサスの形成、豊富なロールベースのアクセス許可モデル、など利害関係があるプレーヤ間でのインタラクションのセキュアな解決を実現する機能を多数提供している。SIP-CPS においてもその観点での機能の必要性など、検討が必要と思われる。

(2) Enterprise Ethereum Alliance[141]

Enterprise Ethereum Alliance は、エンタープライズグレードのブロックチェーンである。トラン

[141] <https://entethalliance.org/>

ザクションと多くの追加機能でプライバシーを確保する。250 人以上の会員で構成されている。日々の業務に Ethereum technology(分散型アプリケーション (DApps) やスマートコントラクトを構築するためのプラットフォーム)を採用している。

Enterprise Ethereum Alliance のアクティビティとしては、メンバーによる技術開発を行っており、①Enterprise Ethereum Alliance Client Specification v6、②Enterprise Ethereum Alliance Permissioned Blockchains Specification v2（EEA Permissioned Blockchains S)、③EEA Architecture Stack 12/2020、④Enterprise Ethereum Alliance Off-Chain Trusted Compute Specification v1.1 を公開している。

図 10 に、Enterprise Ethereum Architecture Stack と、そのアーキテクチャの上で公開しているツールなど示す。

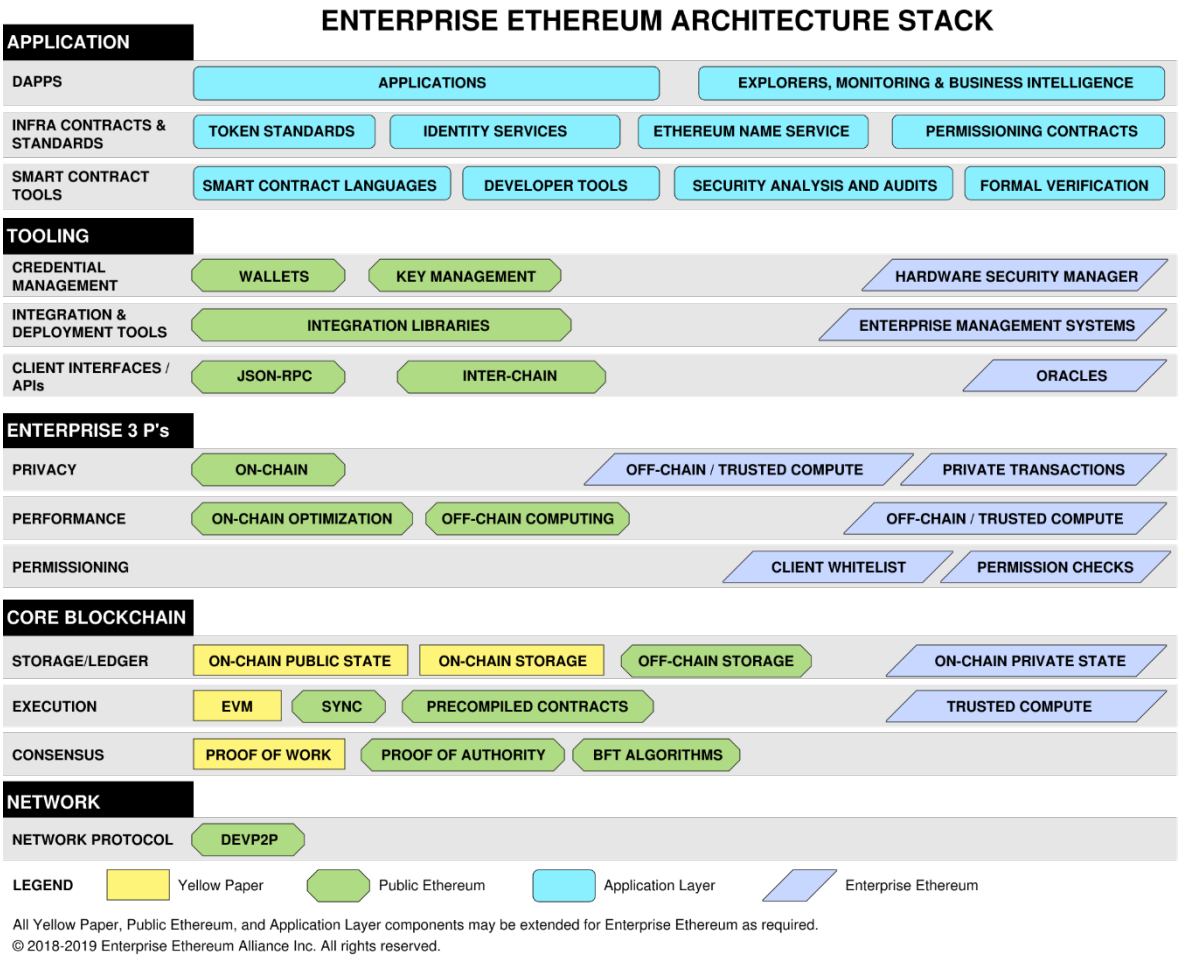


図 10 Enterprise Ethereum Architecture Stack[142]

公開内容の例には、EEA Permissioned Blockchains Sd では、アプリケーション層として、ĐApps サブレイヤー、インフラストラクチャ契約と標準サブレイヤー、スマートコントラクトツールサ

142 <https://coinrivet.com/ja/what-is-the-enterprise-ethereum-alliance/>

ブレイヤーを開発し、リリースしている。

ツールとして、クレデンシャル管理サブレイヤー（組織アカウントのレジストリ（さまざまなタイプのプルーフをサポートするためのプラグ可能性、組織アカウントのスマートコントラクトベースのレジストリ））、統合および展開ツールサブレイヤー、クライアントインターフェイスとAPI サブレイヤー（スマートコントラクトの許可（ノードの許可（ノード許可機能、クライアントの実装、チェーンの初期化））、アカウントの許可（アカウント許可スマートコントラクトインターフェース機能、クライアントの実装、契約の実施、チェーンの初期化）、など）をリリースしている。

ツールとして、クレデンシャル管理サブレイヤー（組織アカウントのレジストリ）、統合および展開ツールサブレイヤー、クライアントインターフェイスと API サブレイヤー（スマートコントラクトの許可、アカウントの許可など）をリリースしている。

Enterprise Ethereum Alliance の工夫点・注視点として、④Enterprise Ethereum Alliance Off-Chain Trusted Compute Specification v1.1 仕様には次の 4 つの目的がある。

- BC にアクセスできる他のパーティにトランザクションの詳細を開示することなく、相互に信頼できないパーティ間のブロックチェーンでのプライベートトランザクションをサポートできる
- 同じ選択された当事者からの他の情報の機密性を維持しながら、BC 上の選択当事者への選択情報の開示をサポート「選択的プライバシー」を実現できる。
- 集中的な処理をメイン BC からオフチェーンのトラステッドコンピューティング機能に移行し、スループットとスケーラビリティを向上できる。
- 証明済みのオラクルをサポートできる。

これらの目的は、オフチェーンの信頼できるコンピューティングでメインチェーンから BC トランザクションの一部を実行することによって達成される。現在、この仕様でサポートされているトラステッドコンピューティングには次の 3 つのタイプがある。

- 信頼できる実行環境（ハードウェアベース）
- ゼロ知識証明（ソフトウェアベース）
- 信頼できるマルチパーティ計算（MPC）（ソフトウェア/ハードウェアベース）。

［考察］

Enterprise Ethereum Alliance では、詳細情報を開示することなく「相互に信頼できないパーティ間のプライベートトランザクション」や、「選択的プライバシー」など、プレーヤの対立や非対象性を全体として機能の提供を行っている。SIP-CPS についても同様のスキームに対する対応の必要性について、検討が必要と思われる。

(3) MOBI[143]

MOBI は、非営利でテクノロジーに依存しないグローバルコンソーシアムである。オープンで包括的なコアサービスインフラストラクチャを構築によるデジタルトランスフォーメーションを目指す。対象は、スマートモビリティとスマートシティにおけるブロックチェーンのイノベーションで、活動内容は、専門知識の共有、業界標準の定義、世界中のモビリティサービスの持続可能性、効率性、アクセシビリティの向上実現を目指している。

会員には、自動車メーカー8 社を含め 100 社程度が加入している。

MOBI のアクティビティとしては、下記のプロジェクト単位の活動がある。

① 車両のアイデンティティ、履歴、データ追跡
② サプライチェーンの追跡、透明性、および効率
③ 自律的な機械と車両の支払い
④ 安全なモビリティエコシステムコマース
⑤ 自律運転と人間運転のデータ市場
⑥ カーシェアリングとライドヘイリング
⑦ 車両、保険、エネルギー、混雑、汚染、インフラストラクチャなどの使用量ベースのモビリティの価格設定と支払い

MOBI の工夫点・注視点としては、デジテルツイン（DT）のための VID 機能関連の ID の規格化をベースにしている点が挙げられる。また、①Verifiable 関連（認証可能)、特に、検証可能なプレゼンテーション（VP)、②車両に関する少なくとも３つの ID、がある。

［考察］

MOBI では、Verifiable 関連（認証可能)、特に、検証可能なプレゼンテーション（VP)に注視している。SIP-CPS でも、プレーヤがどのような可視情報で、信頼・安全と認識するか、制度設計も含め、検討が必要と思われる。

(4) Industrial Internet Consortium（IIC）[144]

IIC は、ベストプラクティスを特定し、組み立て、テスト、および普及促進することにより、Industrial Internet の成長を加速するために必要な組織とテクノロジーを結集するために、2014 年 3 月に設立している。メンバーは、大小のテクノロジーイノベーター、垂直市場のリーダー、研究者、大学、政府機関からなる。セキュリティＷＧの Blockchain アクティビティとしては、①信頼できる IIoT システムの開発と実装促進、②技術的な IIoT セキュリティフレームワークとベストプラクティスの開発、③安全な IIoT の採用の加速、などがある。

IIC の最近のアクティビティとしては、BLOCKCHAIN AND THE CITY(2019.5)、Implementation Aspect: IIoT and Blockchain （White Paper 2020.7)、The Trusted IoT Alliance IoT Challenge Program:Blockchain and the City Challenge(2018)などがある。

IIC の工夫点・注視点には、IIOT ソリューションでブロックチェーンを使用する場合、欠点と

---

143 <https://dlt.mobi/>
144 <https://www.iiconsortium.org/>

して、スケーラビリティやパフォーマンスなど、対処が必要な未解決の問題が多数存在する。また、ブロックチェーンベースの IIoT ソリューションを設計する際には、特別な注意を払う必要があることである。

一方、利点としては、プロビジョニング、使用状況の追跡、資産の廃止など、IIoT 対応資産のライフサイクルの多く問題を解決可能であり、更に、不正開封防止の CoC を可能にし、異種 IIoT エコシステムの重要なイベントや構造変化を追跡することができる。これにより、ブロックチェーンの関連性を正当化するために必要なエコシステムの複雑さと信頼レベルの評価が可能となる。

更に、利点として、データの配布と所有権（IIOT の所有者、管理者：公開鍵と秘密鍵のペア管理）に関しては、①プラットフォーム制御のウォレット（欠点：プラットフォームの信用度依存、リンク信頼度依存)、②IIOT 側制御のウォレット（欠点：特殊専用ハード、開発コスト高)、③スマートコントラクトの強化（ブロックチェーンに直接埋め込まれたビジネスロジックを実装、ログとロジックの改ざん防止)、が挙げられている。

［考察］

Industrial Internet Consortium（IIC）では、IoT の資産管理の観点でのセキュリティリスクの解消を目指している。これは IoT を中心としたサプライチェーンのセキュリティ課題を解決する枠組みと捉えることができる。SIP-CPS でも、どのようなサプライチェーンのタイプに対応可能かなど、検討が必要と思われる。

(5) Energy Web Foundation (EWF)[145]

Energy Web Foundation は、エネルギー部門で主導権を取っている。参加メンバーは、市場、運用、規制ニーズに関連するメンバーも含め 100 以上の会員から構成されている。活動開始は、2019 年半である。

Energy Web Foundation のアクティビティとしては、グーグル、欧州全域の低炭素電力市場の調和を実現する EW を支持（2021.4)、(EWF とフォルクスワーゲンが共同でエネルギー市場統合のためのブロックチェーンの可能性を調査(2021.3)、EW トークン(EWT)がクラーケン（暗号通貨取引所）に上場（2021.3)、ウォルマートやファイザーなどの企業に供給するドイツのオートメーションメーカーASA オートメーションは、EW ゼロを活用して国際的なサプライチェーンを脱炭素化（2021.1)、EW スイッチボードを発表（2020.12)、などがある。

EWF の工夫点・注視点には、SWICHBORD と Energy Web Token (EWT)がある。

SWICHBORD は､アイデンティティ/アクセス管理(IAM)ツール(自己主権アプローチ:ユーザー、資産、アプリケーション開発者向け）である。あらゆる分野で、ブロックチェーンベースまたは非ブロックチェーンデジタルソリューションで使用可能である。完全な IAM ソリューションとして、スイッチボードは、認証、承認 (アプリケーションでのロールベースのアクセス管理など) とアカウンティング (ユーザーアクティビティ履歴のログ記録) にセルフソブリン ID (SSI)、分散識別子 (DD)、検証可能な要求 (VC) を活用している。また、ユーザー向けには、スイッチボード

[145] <https://www.energyweb.org/>

を使用すると、コアアイデンティティと関連する VC、資産(ソーラーパネル、サーモスタット、電気自動車、バッテリーなど)、さまざまなアプリケーションやデジタルサービス(メッセージングやストレージなど)への登録を管理できる。アプリケーション開発者向けには、ユーザー ロールと関連するアクセス許可の定義、ユーザーとアセットの承認、ユーザー操作のログ記録を行うことができる。

Energy Web Token (EWT)は、不正行為からネットワークを保護し、取引手数料とブロック料を通じて検証者を補償し、dApps を合理化し強化するサービスの支払いに使用できる。

［考察］

Energy Web Foundation では、Energy Web Token (EWT)による不正行為からネットワークを保護し、これによる取引手数料とブロック料を通じて検証者を補償することで、エコシステムを構築している。SIP-CPS でも、不正行為からのネットワーク、システムの保護に対し対価をえる仕組みなど、検討が必要と思われる。

5.1.2.4 IDSA[146]ユースケース [147]

IDSA（International Data Space ）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、IDSA ユースケースとして、データ流通に伴い直面する種々の課題について、IDSA ユースケースとして提案型で検討が進められている。

それぞれのユースケースは、SIP-CPS が目指す IoT 社会に対応するサイバー・フィジカル・セキュリティとサプライチェーンと関連性が高いこと、また、公開型で現在検討が進められていることから、最も進んだ活動として、調査対象とした。

以下、注目される 9 件の IDSA ユースケース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) Collaborative Warranty and Quality Management[148]

主催は、SAP と Fraunhofer で、Fraunhofer からは、Fraunhofer AISEC / Fraunhofer FIT / Fraunhofer IESE / Fraunhofer ISST が参画している。

重要な課題認識としては、多層サプライチェーンでは、品質管理データの共有が遅れている。この遅延は、情報が次の層に渡される前にデータの蓄積が繰り返し発生することによって発生する。その結果、体系的な品質欠陥の発見が遅れ、欠陥製品の生産が継続する。 また、メリットがないため、必要なデータが共有されるとは限らない。 たとえば、自動車関連では、修理工場で発見された品質問題は、 保証請求のコンテキストで問題が発生した場合にのみメーカーに連絡される。

この課題に対する目標として、「共同保証および品質管理」アプリを目指している。SAP は、IDS データ共有の概念を利用して、会社間のコラボレーションを促進するスマートデータアプリを提

146 <https://internationaldataspaces.org/we/>
147 <https://internationaldataspaces.org/make/use-cases-overview/>
148 <https://internationaldataspaces.org/usecases/sap-fraunhofer/>

供し、ビジネスプロセスを改善する。例えば、保証請求との関連性に関係なく、修理工場が製造サプライチェーン全体で車両品質データの共有を奨励する。 どの層のサプライヤも、さまざまな下流の支店から品質問題の透明に獲得できる。 サプライヤがそのような品質問題の根本原因分析を行う場合、ダウンストリームまたはアップストリームの品質と使用状況データを統合できる。これらのデータは、使用ポリシーに従って共有される。

この機能による効用としては、①サプライチェーンに沿った品質データの交換の増加 、②進化する品質問題のタイムリーな発見、③ビジネスプロセスの並列化、が期待されている。

活用する技術コンポーネントとして、IDS Trusted Connector 、SAP IDS App Store 、SAP S/4 HANA、Usage Control (MYDATA)、が対象となっている。

［考察］

Collaborative Warranty and Quality Management が目指しているように、サプライチェーンは多層化運用が必然と考えられる。

SIP-CPS でも、多層化サプライチェーンのセキュリティの安全性について、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) Integration Test Camp for IDS Components – Step by Step to a Trusted Infrastructure[149]

主催は、Software Quality Systems (SQS)で、参画企業は、ATOS Innovalia nicos Orbiter となっている。

重要な課題認識としては、国際データスペース（IDS)用テストシナリオの提供で、コネクタ、DAPS、アプリなどの多くのコンポーネントの相互作用の検証には、開発者用テスト環境が必要となることである。本番環境のようなシナリオで作成した商用前の IDSA コンポーネントの相互運用性テストのテストシナリオの提供が課題である。

この課題に対する目標として、「Integration Test Camp」の提供を目指す。リモートアクセス可能なテストインフラストラクチャとして、IDSA コンポーネントの機能と相互運用性を検証する機会を企業に提供する。統合テストキャンプは、毎月のイベントの一環として誰でも参加できる。IDSA コンポーネントとサービス商業化のスピードアップのため、インフラストラクチャ全体が利用可能で、2 時間の時間枠（予約）が与えられる。この間、参加者は SQS チームと連絡を取り合っている。ビデオ通話で、両者は何が起こっているかを確認し共有できる。セッションガイドラインでは、テストステップを指定している。

この機能による効用としては、①IDS コンポーネントとサービスの商業化をスピードアップ、②データ共有サービスの開発と提供におけるコスト削減と IDS コンプライアンスの保証、③データ駆動型サービスを提供する際のリスクの軽減と投資収益率の向上、が期待されている。

活用する技術コンポーネントとしては、オープンソースとして提供されている IDS Connector、及び、DAPS、Data Broker and Data Consumer、が対象となっている。

［考察］

---

[149] <https://internationaldataspaces.org/usecases/sqs/>

Integration Test Camp for IDS Components では、他のシステムと連携させて統合システムの研究開発機能の有効性、安全性等を評価するテストシナリオ、テスト機能、テスト環境・仕組みの提供を目指している。SIP-CPS でも、研究開発機能・システムだけでなく、他のシステムと連携させて統合システムのテスト環境について必要性も含め検討が必要と思われる。

(3) Horizontal Supply Chain Collaboration[150]

主催は、SICK Sensor Intelligence となっている。

重要な課題認識としては、サプライチェーンステークホルダーに、マテリアルフローに関するステータス情報を提供し、コスト削減を図る。また、デジタル化でサプライチェーンにおけるマテリアルフローを最適化するための基礎を提供する。加えて、透明性を確立し、プロセスのコスト削減の新しい可能性を提示し、サードパーティのサプライヤにアウトソーシングできるロジスティックタスクを実現する、となっている。

この課題に対する目標として、「追跡および追跡システム」を目指している。具体的には、①デジタルサービスと組み合わせることで、サプライチェーン全体を良くする。②バーコード、2D コード、RFID などで材料を識別する。③ロジスティックプロセスをデジタル化する。例えば、荷役単位での資材の再梱包や検証など 。④これらのシステムは、IDS データ構造を介して、すべての利害関係者に必要で信頼できる情報を提供する。⑤安全なデータ交換に基づいて、請求プロセスなどのデータ駆動型プロセスの自動化を推進する、としている。

この機能による効用としては、①サプライチェーン全体におけるマテリアルフローのデジタル化された信頼できる透明性、②プロセスコストを削減するためのサプライチェーンでの新しいビジネスモデルの生成における柔軟性、③株式の固定資本コストの削減、が期待されている。

活用する技術コンポーネントとしては、IDA のコンポーネントである IDS Connector、Data Broker、Identity Provider、に加え、Corda (Blockchain / distributed ledger)、SICK track and trace system with digital service が対象となっている。

［考察］

Horizontal Supply Chain Collaboration では、サプライチェーンは利害関係者向けに追跡可能な情報提供が重要であるとしている。SIP-CPS においても、利害関係者間のセキュリティを維持しつつ、情報を提供する枠組みも検討が必要と思われる。

(4) Telekom Data Intelligence Hub – Creating Value from Data[151]

主催は、Deutsche Telekom となっている。

重要な課題認識としては、「企業が重要な情報を取引先に渡さない」を保証できる課題である。これを実現しようとすると、データの透明性、セキュリティ、信頼を欠く例が多い。例えば、生産、販売、流通(サプライチェーン)企業は、データや制御を失うことを恐れて、重要な情報を取引先に渡さない。

---

150 <https://internationaldataspaces.org/usecases/SICK/>
151 <https://internationaldataspaces.org/usecases/deutsche-telekom-2/>

この課題を解決する目標として、企業が国際データスペース（IDS)の原則に沿った安全なビジネスエコシステムを介してデータを交換できる「テレコムデータインテリジェンスハブ(TelekomDataIntelligence Hub)」によるデータアクセスを促進する。

具体的には、①企業間のデジタル接続として機能し、②商用データ取得とオープンデータの両ソースを用いる。③この PF は、データの取得、交換、処理に加えて、分析ツールをユーザーに提供し、④これを用いて、プログラマー、データエンジニア、データジャーナリスト、データサイエンティストなどの業界の専門家は、新しいビジネスモデル、データ駆動型の製品またはサービスを開発する。また、大学の研究者が、新しい洞察を得るためにデータとアルゴリズムの組み合わせのモデルを開発にも用いる、としている。

この機能による効用としては、①ユーザー権利の管理を含む、セキュリティ保護された制御可能なデータ交換、②データ駆動型の製品とサービスを開発するための分析ツールのための安全な作業環境、③会社の枠を越えたデータの簡易検索と使用、が期待されている。

［考察］

Telekom Data Intelligence Hub でも、サプライチェーンは、利害関係者向けの情報提供が重要であるとしている。SIP-CPS でも、利害関係者間のセキュリティを維持しつつ、情報を提供する枠組みも検討が必要と思われる。特に、セキュリティを維持したまま、提供する情報の信頼性をどう担保するかがポイントと考えられる。

(5) ONCITE – Sharing Data in the Supply Chain[152]

主催は、German Edge Cloud となっている。

重要な課題認識としては、「データ主権を失うことなく、サプライ チェーン全体でパートナーとデータを簡単、迅速、安全に交換する方法」を保証する課題である。

この課題の背景には、①データ価値の最大限活用には、データを効率的かつインテリジェントにキャプチャ、保存、処理、評価できる必要がある。 ②企業はサプライチェーン全体のパートナーとデータ交換が必要なため重要。③意思決定者は、産業環境のこのような変化への対応問題に直面している、などがある。

この課題を解決する目標として、「ONCITE」センターの運用を提唱している。

これにより、①企業はパブリッククラウドを介してデータ交換前に、サイトでデータ処理/保存できる。②プロセス全体でデータ主権が保証される。 なお、ONCITE は、エッジクラウドテクノロジーに基づくコンパクトなコンピューティングセンターとしている。

ONCITE の心臓部は、IDS 認定のサプライヤコネクタで、 ユーザーインターフェイスは、パートナー間のデータ交換を監視/制御する。 コネクタ使用で、パートナーはデータを評価し、自社または OEM のシステムで使用できるようにできる、としている。

この機能による効用としては、①データをデジタルプロセスで使用可（サプライヤとメーカ)、②パブリッククラウドでデータ交換前に、現場でデータを処理/保存できる（企業)、③リアルタイ

---

152 <https://internationaldataspaces.org/usecases/german-edge-cloud/>

ムで最高レベルのセキュリティでデータ交換トランザクションが可能、が期待されている。
［考察］
ONCITE では、企業はサプライチェーン全体のパートナーとのデータ交換が必要となるため、中立的な立場でセンター的な役割を担うシステムの提供を進めている。SIP-CPS でも、中立的な立場でサプライチェーン全体のパートナーとのデータ交換を行うセンター的な役割を担うシステム、組織の必要性について検討が必要と思われる。

(6) Smart Factory Web – Connecting the Industrie 4.0 Asset Administration Shell[153]

主催は、Fraunhofer IOSB となっている。参画企業/エコシステムには、Fraunhofer Data Spaces、IDS-Industrial Community、Platform Industrie 4.0、Industrial Internet Consortium (IIC)、KETI、Microsoft、SAP が名を連ねている。
重要な課題認識としては、「パートナー間のデータ交換は、工場など重要な生産データが関係し、困難」との課題である。
この課題の背景には、顧客はできるだけ多くの情報を求めるが、プロデューサーは不明なパートナーとのデータ共有をためらうことがある。
これに対し、IDSA は、データ所有者が特定のドメイン (製造、エネルギー、ヘルスケア、ロジスティクスなど) 内でデータの使用/配布方法を選択できる安全なグローバルデータスペース（IDS)の作成に努めている。
具体的には、IDS OPC UA ファクトリコネクタは、スマートファクトリを OPC UA 経由で IDS に接続するコネクタとして提供し、ユース ケースには、工場の所有者が世界中の顧客に生産能力を提供するスマートファクトリ Web（産業生産用 Web）としている。 産業生産用 Web でサプライ チェーンをモデル化することで、工場所有者は、どのパートナーと、どのような条件と制約の下で工場データを使用できるかを決定できる。例えば、工場所有者は、検証済みの SFW の顧客と製品に関する情報を共有できるが、生産データはアクティブなサプライチェーンのパートナーにのみ表示される。
IDS OPC UA ファクトリコネクタ（IDS-OPC コネクタ）は、IIC、IDSA、プラットフォームインダストリー 4.0 などの標準の接続を目的としている。IDS-OPC コネクタは、IDS へのゲートウェイであり、ファクトリを他の顧客や Smart Factory Web などの IDS 参加者に接続する。このコネクタは、IDS コネクタ (安全標準化通信、データ使用制御) の利点と、Industrie 4.0 の相互運用性テクノロジーとアプリケーションを組み合わせている。 その結果、工場内の資産管理シェル (AAS) を IDS を介して公開/保護できる。このソリューションを実現するために、バルクソーターの AAS モデルとインスタンスを OPC UA 形式で作成している。
Smart Factory Web では、サプライチェーン（SC)をモデル化している。 IDS-OPC コネクタは、AAS からデータを取得し、SC のどのパートナーがどのデータ要素の使用を許可されているかを確認できる。

---

153 <https://internationaldataspaces.org/usecases/smart-factory-web/>

この機能による効用としては、①資産管理シェルとの統合と相互運用性、②データユーセージ Control 経由での国際データスペース（IDS）、③Smart Factory Web などの工業生産向けの市場で Factory の機能と資産を公開することによる新しいビジネスチャンス 、が期待されている。

活用する技術コンポーネントとしては、OPC UA Factory Connector (Extended IDS Base Connector)、IDS “MYDATA Usage Control” 、Smart Factory Web, platform / marketplace for industrial production as source for supply chain information、Asset Administration Shell in different technology mappings (e.g. OPC UA, AutomationML) が対象となっている。

［考察］

Smart Factory Web では、サプライチェーンにおけるデータ共有と非対象性の安全性を高める仕組みとして、ドメインなどの閉域を構成し、運用する仕組みを目指している。SIP-CPS でも、サプライチェーンにおけるデータ共有と非対象性の安全性を高める仕組みの必要性も含めて、検討が必要と思われる。

(7) GAIAboX – Secure Resource Management, File Storage and Data Exchange in IDS[154]

主催は、Nicos となっている。

重要な課題認識としては、「安全で主権を持つリソース管理とファイルストレージ」の提供である。

この課題の背景には、データの提供後もデータの利用について制御可能（主権）とし、安全なデータ運用の保証が、多くのプレーヤが参加するサプライチェーンではより重要となるとの認識がある。

GAIAboX では、従来からのデータアクセスのスキームとして、FTP、SSH、HTTP を介してアクセスでき、「Linked Data Platform」（LDP、W3C を参照）の概念に従う。データ共有に限定されず、オープンインベントリプラットフォームとして、任意のリソースを表すことができるとこを目標としている。

GAIAboX は、「パブリッシュ/サブスクライブ」を利用可能にするために、mqtt、gRPC、WebSocket などのアプリケーションプロトコルも提供する。資産管理シェル（AAS）の概念に従って、標準の意味的記述方法でデータと情報の提供を目的としているため、相互運用性と簡単な対話が可能である。

GAIAboX の目標は、IDS アーキテクチャ技術を使用しデータ主権を保証することである。IDS コネクタプロバイダーとして機能し、格納リソースへのきめ細かなアクセス制御と IDS 使用管理の概念も確立する。リソースの GAIAboX への保存は、リソースをどこに残し、どのように使用するかを決定するコントラクトとポリシーによって強化できる。 GAIAboX は、他の GAIAboX にもアクセスできるように Web クライアントアプリケーションを実装している。

この機能による効用としては、①プラットフォームの独立性、②IDS 適合性、③AWS、Azure、エッジサーバーなどのクラウドへのデプロイ、が期待されている。

---

[154] <https://internationaldataspaces.org/usecases/nicos-gaiabox-secure-resource-management-file-storage-data-exchange-in-ids/>

活用する技術コンポーネントとしては、Linked Data Platform (LDP)、IDS Connector technology、Publish/ subscribe mechanisms が対象となっている。

［考察］

GAIAboX では、サプライチェーンにおけるデータ主権（制御可能）の確保を目指している。サプライチェーンにおけるデータ主権（制御可能）の確保は重要と思われ、SIP-CPS でも、データ主権者が保有する能力、機能について検討の必要性も含め、検討が必要と思われる。

(8) Supply Chain Manager – Achieving Transparency in Automotive Supply Chains[155]

主催は、Volkswagen AG、thyssenkrupp、Fraunhofer ISST となっている。

重要な課題認識としては、「サプライチェーンの回復力を堅固なものにすること」である。

この課題の背景には、在庫、生産量、生産プログラムなどの機密データを双方向相関関係とすることで、長期的な目標が現実的になりる。 つまりチェーンの双方向で機密データの関係を維持することが、長期的に回復力を堅固にできるとの認識がある。

IDS は、そのタイプのデータ交換の技術的基盤を表し、高レベルの安全要件を遵守しながら、組織間のデータ主権をサポートするとこを目指してる。

信頼は、自動車生産など材料プロバイダーや生産的な消費者などの産業環境でのコラボレーションの最も高い評価要件の 1 つである。しかし、特に機密データの交換が必要な場合、IT システムへのアクセスは人間の制御が及ばないため、純粋に信頼だけでは不十分である。

この技術的な解決策としては、技術を使用して信頼を確立し、両端でデータ主権を確保するために必要とし、これを目標としている。

この機能による効用としては、①データ交換と使用でプロセス改善、②自動車サプライチェーンにおける透明性の向上、③相互信頼を確立しポリシーの実施が可能、が期待されている。

活用する技術コンポーネントとしては、IDS Connector、IDS Connector Framework が対象となっている。

［考察］

Supply Chain Manager では、サプライチェーンの回復力を堅固にすることを目指している。SIP-CPS でも、重要な技術開発の目標と考えられ、特に機密データの観点でもセキュリティを確保しつつ長期的な堅牢性確保の枠組みの検討が必要と思われる。

(9) Personal Data Banking - Reinventing the Internet With Trust and Data Sovereignty[156]

主催は、Orbiter、idento.one となっている。参画企業は、Scope、Polar Mohr となっている。

重要な課題認識としては、「企業と個人間のデータ使用方法（データ主権）の制御の重要性」である。

この課題の背景には、①サプライチェーンは企業間でのチェーンを中心としているが、個々人

---

155 <https://internationaldataspaces.org/usecases/supply-chain-manager-achieving-transparency-in-automotive-supply-chains/>

156 <https://internationaldataspaces.org/usecases/orbiter-idento-one/>

への配送もサプライチェーンの一部と考える必要があり、その際、大量の個人データを扱うことが必要不可欠であること、②一方、消費者は日々、その価値を考えずに大量の個人データを開示している。このデータは、消費者に報酬を与えたり、情報を提供したりすることなく、大規模に商業的に取引されている、との認識がある。

これは、個人データ保護の認識レベルが高くない個人を含めた、データ使用方法（データ主権）の制御の必要性を示している。

この技術的な解決策としては、データの使用方法（データ主権）を制御できるようにする企業と個人間の「データブローカー」を目標としている。

具体的には、「Idento.one」として、検証済みのデジタル ID を提供し、デジタル経済で自分自身を容易に識別可能とする。また、個人を特定できる情報の取り扱いに関する GDPR 要件を解決する。データを管理/保護し、データプライバシーを保証する。Idento.one を使用すると、個人データの使用について第三者に同意を与える（同意を取り消す）ことができる。これにより個人のデータを使用したい企業と個人間の「データブローカー」として機能する。

この機能による効用としては、①検証済みのデジタル ID、②安全な分散型データストレージ、③データの使用方法はカスタマイズ可、が期待されている。

活用する技術コンポーネントとしては、IDS Broker、DS Connecto、IDS Clearing House が対象となっている。

［考察］

Personal Data Banking では、企業と個人間のデータ使用方法（データ主権）の制御の実現を目指している。SIP-CPS でも、サプライチェーンにおける個人情報保護のための、データ使用方法（データ主権）の枠組みについて検討が必要と思われる。

5.2 国際的な目標水準の妥当性

5.2.1 調査方法

調査期間中に提供いただいた SIP-CPS の国際的な目標水準の妥当性を確認するため、SIP-CPS が設定している評価軸を調査した。調査結果を 5.2.2 項に示す。

次に、SIP-CPS の目標水準の妥当性の判断を可能とするため、5.1 節で調査した技術・製品（以下、調査技術・製品）について、個別の実施項目に対応する調査技術・製品を抽出し、SIP-CPS の実施項目との比較のための尺度とする。5.1 節の調査技術・製品は、現時点で最先端のものを対象としており、それらと比較することで、到達水準の確認が可能と考えられる。

また、対応する技術・製品があることは、SIP-CPS が設定している評価軸は妥当であることを示している。SP-CPS の実施項目に対応している調査技術・製品については、5.2.3 項に示す。

最後に、SIP-CPS の実施項目の評価軸に対応するものがない課題解決を行っている技術や製品については、新たな評価軸、又は、サブ評価軸としての必要性を検討し、評価軸やサブ評価軸としての不足の有無を検証する。

検証結果を含め、国際的な目標水準に盛り込むべき事項を 5.3 節で紹介する。

5.2.2 SIP-CPS の目標水準

SIP-CPS のグローバルベンチマークの評価軸としては、社会への普及までを視野にいれて大きく捉え、セキュリティ強度、性能、社会実装性の 3 点を評価軸としている。

また、セキュリティ強化対象としては、研究開発項目 A、B、C 共通で、「サプライチェーンセキュリティ」、「IoT セキュリティを含む」としている。

個々の実施項目別では、研究開発項目 A では、「信頼の創出・証明」、研究開発項目 B では、「信頼チェーンの構築・流通」、研究開発項目 C では、「信頼チェーンの検証・維持」を目標としている。

更に、各研究開発項目のサブ項目ごとに、個別の目標設定を行っており、個別項目は、上記観点の評価軸の組合せで評価を行っている。

個別研究開発項目ごとに評価が必要なグローバルベンチマークの評価軸として、セキュリティ強度関連と適用領域関連、性能関連に加え、市場性、価格が挙げられている。なお、市場性と価格は社会実装性の評価に対応していると考えられる。

5.2.3 SIP-CPS 実施項目に対応する調査技術・製品

5.2.3.1 研究開発項目 A1

A1 は、「信頼の創出・証明」の実現に向け、「IoT 端末機能向けセキュリティチップへの搭載」を目指しており、同様の目標で選定が進んでいる米国 NIST が IoT 用の軽量暗号の公募・評価、標準化への応募技術に着目した。その軽量暗号の技術の中で、調査時点で評価対象として残っている技術が現時点での最先端の技術と考えられる。

具体的には、Elefant、Liliput、TGIF の 3 技術で、概要等は、5.1 節の 5.1.2.2 項に記載している。これらの３技術では暗号性能、チップサイスなどが評価対象であり、評価にあたり提供いただいた研究開発項目 A1 のベンチマーク情報の評価軸と同じであり、項目は妥当と考える。

NIST では、承認済み暗号ブロック（AES (Advanced Encryption Standard) 、TDEA (Triple Data Encryption Algorithm; トリプル DES：3DES) を用いた実行を推奨しており、楕円暗号を用いている A1 技術のセキュリティ性能は、最先端の目標水準をクリアしていると考えられる。なお、性能については、実測値等の比較が必要と考える。

5.2.3.2 研究開発項目 A2

A2 は、「信頼の創出・証明」の実現に向け、「IoT/OT 機器の真贋判定」の判定性能・判定対象が目標水準の判定の中核となる項目である。

これとほぼ類似する目標を掲げている 5.1.2.1 項の RSA2021 製品・企業での最優秀製品の Apiiro の対象は IT とは異なるがシステム全体のライフライクルでの真贋判定を対象としており、提供いただいた研究開発項目 A2 の目標項目の設定が妥当であることを示している。

また SIP-CPS での到達レベルは、SIP-CPS 一期での IT に加え、IoT/OT を含めると共に、システムがつながるサプライチェーンを対象にしており、高い水準となっている。

5.2.3.3　研究開発項目 B2、B3

B2、B3 は、「信頼チェーンの構築・流通」の実現に向けたものであり、このうち B2 は「安全な情報共有」、B3 は「信頼の創出、信頼の証明、信頼のチェーンの構築と維持」を目指している。

これらに対応する技術開発は、前者は主に Blockchain コンソーシアムにおいて、また後者は主に IDSA（International Data Space）の企業連合体において、多数の技術、製品の開発がコンソーシアムとして開発が進められている。

このような外部の動きは、研究開発項目 B2、B3 の目標項目の設定の妥当性を示していると考える。

到達レベルについては、5.1.2.3 項で述べた BlockChain では、下記となっている。

- Hyperledger：コンセンサスの形成、豊富なロールベースのアクセス許可モデル、など利害関係があるプレーヤ間でのインタラクションのセキュアな解決を実現する機能
- Enterprise Ethereum Alliance：詳細情報を開示することなく「相互に信頼できないパーティ間のプライベートトランザクション」や、「選択的プライバシー」など、プレーヤの対立や非対象性を全体として機能
- MOBI：Verifiable 関連（認証可能）、特に、検証可能なプレゼンテーション（VP)
- Industrial Internet Consortium（IIC）: IoT の資産管理の観点でのセキュリティリスクの解消（IoT を中心としたサプライチェーンのセキュリティ課題を解決する枠組み）
- Energy Web Foundation：Energy Web Token (EWT)による不正行為からネットワークを保護し、これによる取引手数料とブロック料を通じて検証者を補償するエコシステム

提供いただいた SIP-CPS の B2、B3 の目標水準への到達レベルの評価の観点では、これらの観点も目標項目、目標水準のサブ項目として検討が必要と考えられる。

また、5.1.2.4 項 IDSA ユースケースでは、到達レベルは下記となっている。

- Collaborative Warranty and Quality Management：サプライチェーンの多層化運用
- Integration Test Camp for IDS Components ：他のシステムと連携させて統合システムの研究開発機能の有効性、安全性等を評価するテストシナリオ、テスト機能、テスト環境・仕組み
- Horizontal Supply Chain Collaboration：サプライチェーンの利害関係者に追跡可能な情報提供
- Telekom Data Intelligence Hub ：サプライチェーンの利害関係者の情報提供
- ONCITE ：サプライチェーン全体のパートナーとのデータ交換を行う中立的なシステム
- Smart Factory Web ：サプライチェーンのデータ共有と非対象性の安全性を高める仕組み（ドメインなどの閉域の構成と運用）
- GAIAboX：サプライチェーンにおけるデータ主権（制御可能）の確保
- Supply Chain Manager：サプライチェーンの回復力
- Personal Data Banking：企業と個人間のデータ使用方法（データ主権）の制御

SIP-CPS の技術開発項目 B2、B3 の目標水準への到達レベルの評価の観点では、これらの観点についても必要性も含め、検討が必要と考えられる。

5.2.3.4 技術開発項目 C2

C2 では、「信頼チェーンの検証・維持」の実現に向け、「IoT システムの可用性向上」、「セキュリティ対策の早期適用」、「サプライチェーンの信頼性維持」を目指している。

目標とする観点も多岐に渡り、複雑な防御対象、攻撃の進化、マルチドメイン、即時監視・即時検知・即時支援、IoT データの多様化（データ改ざん検知困難）、また、迅速な一時対処や事前検証のための「攻撃シミュレーション」によるサイバー攻撃の影響の可視化、リスクアセスメントの自動化、サイバー攻撃に対する対象策案の提示、などを目指している。

提供いただいた C2 の目標水準の妥当性検証の候補として、IoT セキュリティ製品として評価軸を明示している、「IOT SECURITY[157]（paloaito）」を選定した。

IOT SECURITY は、アラートのみを提供するのではなく、組み込み予防としてシームレスに統合されたクラウド配信のセキュリティサービスを使用して、IoT、IoMT や OT のデバイスを脅威からの保護を提供する。そのセキュリティ検知能力として、DEVICES DETECTED IN 48 HOURS：90%、EVASIONS BLOCKED：100%、AVERAGE TIME SAVED：15-20h を謳っている。

製品の特長は下記となっている。

- 「IoT 資産管理」として、定期的な署名の更新や人間のサポートなしで、新しい非表示のデバイスを識別し、重要なデバイス属性を表示
- 「IoT リスク評価」として、脆弱性分析を実行し、デバイスの異常な動作の異常を検出し、リスクを計算して評価し、アクションに優先順位を付与
- 「リスク削減ポリシー適用」として、デバイスの詳細を分析して、信頼できる動作のみを許可するコンテキストアウェアマイクロセグメンテーションとデバイスベースのポリシーを適用
- 「既知脅威対応」として、IoT を標的とする既知のマルウェア、スパイウェア、エクスプロイト、および Web ベースの脅威を防ぎ、注意が必要な大量のアラートからセキュリティチームを保護
- 「未知脅威検出」として、集合的な脅威インテリジェンスを使用して、未知の脅威に対するリアルタイムの保護を提供し、IoT 環境に固有の動作異常やその他のこれまでにない脅威を調査

監視項目としては、「リアルタイムで監視」として、デバイスのリスクレベルを継続的に分析し、クラウドソーシングで機械学習を使用して、すべてのデバイスを迅速かつ正確に検出し、リスクを評価し、異常を検出し、自動ポリシー推奨を提供する唯一のソリューションであるとしている。

SIP-CPS の研究開発項目 C2 と、この IOT SECURITY との対応関係は次となっており、ほぼ同じ課題設定となっている。

また、IOT SECURITY は、次のセキュリティ検知能力を示しており、提供いただいた C2 の技術目標水準判断のための比較候補となる。

- 「IoT 資産管理」に対して、マルチドメイン、IoT データの多様化（データ改ざん検知困難）、

[157] <https://www.paloaltonetworks.com/network-security/iot-security>

複雑な防御対象

- 「IoT リスク評価」に対して、リスクアセスメントの自動化
- 「リスク削減ポリシー適用」に対して、サイバー攻撃の影響の可視化、サイバー攻撃に対する対象策案の提示
- 「既知脅威対応」、「未知脅威検出」、「リアルタイムで監視」に対して、即時監視・即時検知・即時支援、迅速な一時対処困難、攻撃の進化

5.3 国際的な目標水準に盛り込むべき事項

以上のように、海外における先端の技術開発プロジェクトとして 5.1.2 項に示した調査対象の技術、製品、活動の評価項目に対して、提供いただいた SIP-CPS の研究開発の評価項目は、ほぼカバーしていると考えることができるが、一部については SIP-CPS との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評価項目がある。これらを調査対象ごとに以下に示す。

5.3.1 RSA2021 製品・企業関連

RSA2021 製品・企業の評価項目関連では、下記の 9 種がある。

・Abnormal Security：電子メール攻撃に特化した技術。
・Axis Security：アプリへのアクセスに特化した技術
・Cape Privacy：グローバルな暗号化学習に特化したプラットフォーム技術
・Deduce：ID ベースの脅威を抑える技術
・Open Raven：データ漏洩の防止やコンプライアンス目標の達成などに焦点を縛った技術
・Satori：データアクセスサービスのセキュリティ達成に焦点を縛った技術
・Maverics Identity Orchestration Platformi：一貫した ID 管理に焦点を縛った技術
・Wabbi：セキュリティとソフトウェアの両方の継続的な進化に焦点を縛った技術
・Wiz：IT 運用トータルのセキュリティリスクを抑えることに焦点を当てた技術

この中で、追加候補となる評価項目として、ⅰ）ID 管理（Deduce、Maverics Identity Orchestration Platformi）、ⅱ）進化（Cape Privacy、Wabbi）、ⅲ）データ（Open Raven、Satori、Wiz）を抽出した。

［考察］

ⅰ）ID 管理と、ⅲ）データについては、SIP-CPS の研究開発項目 B3 の中に含まれるが、ⅱ）進化については、SIP-CPS の実施項目の中では、明確な目標となっていないと考えられる。

［提案］

目標水準候補としては、ⅱ）進化、を提案する。

5.3.2 BlockChain コンソーシアム関連

Blockchain コンソーシアムの評価項目関連では、下記の 5 種がある。

・Hyperledger：コンセンサスの形成、豊富なロールベースのアクセス許可モデル、など利害関係があるプレーヤ間でのインタラクションのセキュアな解決を実現する機能

・Enterprise Ethereum Alliance：詳細情報を開示することなく「相互に信頼できないパーティ間のプライベートトランザクション」や、「選択的プライバシー」など、プレーヤの対立や非対象性を全体として機能

・MOBI：Verifiable 関連（認証可能）、特に、検証可能なプレゼンテーション（VP)

・Industrial Internet Consortium（IIC）: IoT の資産管理の観点でのセキュリティリスクの解消（IoT を中心としたサプライチェーンのセキュリティ課題を解決する枠組み）

・Energy Web Foundation：Energy Web Token (EWT)による不正行為からネットワークを保護し、これによる取引手数料とブロック料を通じて検証者を補償するエコシステム

［考察］

上記の中で、追加候補となる評価項目として、ⅰ）利害、非対称関係者のセキュリティ（Hyperledger、Enterprise Ethereum Alliance）、ⅱ）検証可能 HMI（MOBI）、ⅲ）IoT 資産管理（Industrial Internet Consortium（IIC））、ⅳ）セキュリティ監視と料金回収（Energy Web Foundation）を抽出した。

ⅰ）利害、非対称関係者のセキュリティは、SIP-CPS 実施項目 B2 で意識されているが、目標の明示が必要と考える。

ⅱ）検証可能 HMI についても、SIP-CPS 実施項目 C2 やその他の実施項目でも検討されている内容であるが、目標の明示が必要と考える。

ⅲ）IoT 資産管理については、SIP-CPS 研究開発項目 B3 の中に含まれていると考えられる。

ⅳ）セキュリティ監視と料金回収は、SIP-CPS 研究開発項目 A2,C2 で目標となっている。

［提案］

目標水準候補として、ⅰ）利害、非対称関係者のセキュリティ、ⅱ）検証可能 HMI、を提案する。

5.3.3 IDSA ユースケース関連

IDSA ユースケースの評価項目関連では、下記の 9 種がある。

- Collaborative Warranty and Quality Management：サプライチェーンの多層化運用
- Integration Test Camp for IDS Components ：他のシステムと連携させて統合システムの研究開発機能の有効性、安全性等を評価するテストシナリオ、テスト機能、テスト環境・仕組み
- Horizontal Supply Chain Collaboration：サプライチェーンの利害関係者に追跡可能な情報提供
- Telekom Data Intelligence Hub ：サプライチェーンの利害関係者の情報提供
- ONCITE ：サプライチェーン全体のパートナーとのデータ交換を行う中立的なシステム
- Smart Factory Web ：サプライチェーンのデータ共有と非対象性の安全性を高める仕組み（ドメインなどの閉域の構成と運用）
- GAIAboX：サプライチェーンにおけるデータ主権（制御可能）の確保
- Supply Chain Manager：サプライチェーンの回復力

・ Personal Data Banking：企業と個人間のデータ使用方法（データ主権）の制御

［考察］

上記の中で、追加候補となる評価項目として、サプライチェーン関連の、ⅰ）多層化運用（Collaborative Warranty and Quality Management）、ⅱ）連携テスト環境（Integration Test Camp for IDS Components）、ⅲ）利害関係者追跡可能情報（Horizontal Supply Chain Collaboration、Telekom Data Intelligence Hub、ONCITE、Smart Factory Web）、ⅳ）データ主権（制御可能）（GAIAboX、Personal Data Banking）、ⅴ）回復力（Supply Chain Manager）を抽出した。

i) 多層化運用については、SIP-CPS 実施項目 B2 の中に含まれていると考えられる。
ii) 連携テスト環境は、SIP-CPS 実施項目 A2,C2 で既に実施中であり、引き続きの運用継続が求められる。
iii) 利害関係者追跡可能情報は、SIP-CPS 実施項目 B2 で意識されているが、目標の明示が必要と考える。
iv) データ主権（制御可能）については、SIP-CPS 実施項目 B3 で意識されているが、目標の明示が必要と考える。
v) 回復力については、SIP-CPS の実施項目ごとに意識されているが、サプライチェーン全体としての回復力は、目標の明示が必要と考える。

［提案］

目標水準候補としては、サプライチェーンのⅲ）利害関係者追跡可能情報、**ⅳ）**データ主権（制御可能）、**ⅴ）**回復力を提案する。

5.3.4 まとめ

調査期間中に提供いただいた 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 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 が展開する研究開発目標と対比することにより、SIP-CPS 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進化（セキュリティとソフトウェアの両方の継続的な進化や、暗号学習への対応）
②利害関係者間のセキュリティと追跡可能性
③検証可能な HMI
④データ主権（データの制御可能）
⑤サプライチェーンの回復力

目標水準については、選定した各技術の実現レベルを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。

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 事務局と調整の上、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、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配信に加えて 2021 年 11 月の中間報告と 2022 年 3 月の最終報告の 2 回の報告を行った。

6.2　中間報告

前半活動（7 月～10 月）までの海外動向情報を取りまとめ、11 月 2 日の SIP-CPS シンポジウム開催後に中間報告書を提出した。また、ピュアレビューに用いる海外動向調査の活動概要を作成した。

6.3　最終報告会

3 月 8 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 30 分にわたり、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 31 名であった。

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の送付状況を**表 3** に示す。

表 3 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			
68	23	44	35	10

結び

サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する人間中心の社会である Society 5.0 をセキュアに実現するための研究開発プロジェクト「IoT 社会に対応したサイバー・フィジカル・セキュリティ」を実施して、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』の開発と実証が行なわれている。

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。

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、欧州については、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指標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	その他標準化組織	報道機関	その他			
2021/4/22	Workshop Addressing Public Comment on NIST Cybersecurity for IoT Guidance	IoTガイダンスのためのNISTサイバーセキュリティに関するパブリックコメントに関するワークショップ	1					1								NISTは、202/12/15に公開された4つのIoT公開ドラフト文書（SP 800-213、NISTIR8259B/C/D）のサイバーセキュリティに対するコメントのテーマについて議論するワークショップを4/22に開催した。このワークショップでは、SP800-213、NISTIR8259Bで提起されたコメントのテーマについての議論に焦点を当てている。 ワークショップの目的は、コメントからテーマを取り、パネルを通じて利害関係者から追加の意見を得ることであり、聴衆の参加と質問を含む主要なトピックに関する異なる視点を結集させる。また、ワークショップでは、ドキュメントの進め方に役立つ重要な質問に関して、すべてのワークショップ参加者に対して簡単にディスカッションを行った。	https://www.nist.gov/news-events/events/2021/04/workshop-addressing-public-comment-nist-cybersecurity-iot-guidance	
2021/4/22	SP1800-32(Draft) Securing the Industrial Internet of Things: Cybersecurity for Distriibuted Energy Resources (Preliminary Draft)	SP 1800-32 (ドラフト) 産業用モノのインターネットの保護:分散型エネルギー資源のサイバーセキュリティ(予備案)	1					1								NISTのNational Cybersecurity Center of Excellence（NCCCoE)よりEnergy Sector Use Casesの一つとして一般公開された初期草案。（5/24までPubric Commentsが公募） 産業用モノのインターネット（IoT)は、輸送、エネルギー、その他の重要なインフラ分野の機械や車両に計測器や接続されたセンサーやその他のデバイスを適用することを指す。エネルギー分野では、太陽光発電や風力タービンなどの分散エネルギー資源(DER)には、センサ、データ転送および通信システム、機器、およびネットワーク接続されているその他の市販デバイスが含まれ、DER は、電力の分散制御システムと DER との間で情報交換を行い、分配グリッド内のエネルギーの流れを管理する。この実習ガイドでは、商用およびユーティリティ規模のDERと配電グリッドの運用間の情報交換を監視し、特定のサイバーセキュリティの脅威や脆弱性から保護する方法について説明する。 NCCoE は、市販製品を使用して参照アーキテクチャを構築し、通信とデータの整合性、マルウェア検出、ネットワーク監視、認証とアクセス制御、クラウドベースの分析と視覚化など、いくつかのサイバーセキュリティ機能を適用して分散したエンド ポイントを保護し、DER の IIoT 攻撃対象を削減する方法を組織に示した。	https://csrc.nist.gov/publications/detail/sp/1800-32/draft	本文献は、彼らがDistributed Energy Resources (DER、分散発電源的なもの）と呼ぶ、風力や太陽光による発電装置(Photovoltaics)を対象とした産業向けIoT(IIoT)が接続された情報システム並びにPower Gridという極めて具体的なユースケースを想定、対象とし、具体的な実践を扱っているとされる、対象、具体性、内容から、連邦政府機関が利用するIoTのFISMAあるいはNIST SP 800-53 への適用を目指していると考えられるNIST IoT Program とは対象や目標が異なる。
2021/4/23	SP 800-82 Rev. 3 (Draft) PRE-DRAFT Call for Comments: Guide to Industrial Control Systems (ICS) Security	SP 800-82 Rev. 3 (ドラフト) 事前ドラフトコメントの呼びかけ:産業用制御システム(ICS)セキュリティガイド	1					1								NISTは、2015年以来改定されていないSP-800-82Rev.2の更新を開始した。関連する NIST ガイダンス (例: NIST SP 800-37 Rev.2、NIST SP 800-53 Rev.5、NIST SP 800-53B、およびサイバーセキュリティフレームワーク v1.1)に合致し、その他の関連する制御システムのサイバーセキュリティ基準と推奨される慣行に合致し、脅威の状況の変化に対処する。 具体的には、NIST は次の情報に対する入力を要求している。 1.産業制御システムから制御システム全般へのSP 800-82の範囲の拡大 2.制御システム環境における新たなサイバーセキュリティ機能の適用 3.中小規模制御システムの所有者およびオペレータに特有のガイダンスの開発 4.システムの脅威、脆弱性、標準、推奨されるプラクティスを制御するための更新プログラム 5.制御システムオーバーレイの更新 6.現在のドキュメントから不要な材料を削除	https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/draft	Rev.3草稿前の意見照会が2021/5/28迄行われた。SP 800-82 はICSを対象とし、SCADA、DCS並びにPLCが具体的な対象とされ、必ずしもIoTのみを対象としているわけではないが、SIP-CPSで研究成果の利用用途としてICS/SCADAも想定されている場合は、今後観察が必要と思われる。
2021/4/29	SP 800-161 Rev. 1 (Draft) Cyber Supply Chain Risk Management Practices for Systems and Organizations	SP 800-161 Rev. 1 (ドラフト) システムおよび組織におけるサイバーサプライチェーンリスク管理の実践	1					1								企業は、潜在的に悪意のある機能を含む、偽造された、またはサイバーサプライチェーン内の製造および開発慣行が悪いために脆弱である可能性のある製品やサービスに関連するリスクを懸念している。これらのリスクは、企業が取得する技術がどのように開発、統合、展開されているか、および製品と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、および実践に対する可視性の低下と理解に関連している。 この文書は、組織のすべてのレベルにおけるサイバーサプライチェーンのリスクの特定、評価、軽減に関するガイダンスを提供する。この出版物は、C-SCRM戦略実施計画の開発、C-SCRMポリシー、C-SCRM計画、およびC-SCRMリスク評価の製品およびサービス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る。 2021年6月14日までに受け取ったコメントに基づき、NISTは2021年9月に2回目のドラフトをリリースし、2022年4月までに最終版をリリースする予定。	https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-draft.pdf	NIST SP 800-161 Rev.1(Draft）へのPublic Commen t sの受付が2021/4/29より開始、当初予定された6/14の締め切りが6/25まで延長された。Public Comments受付期間中の5/12にはオンラインで本件に関するWorkshoPが開催されている。Workshopで利用されたスライドの今後のスケジュールから、本年9月に第二版草稿が一般公開され10月までPubllc Comments の受付、翌2022年４月に最終催宝版が発行の予定とされる。

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			
2021/5/5	How to Secure the Connected & Automated Mobility (CAM) Ecosystem	コネクテッド&自動モビリティ（CAM）エコシステムを保護する方法	1							1						欧州連合サイバーセキュリティ機関は、コネクテッドモビリティ/自動モビリティ(CAM)セクターが直面するサイバーセキュリティの課題に関する詳細な分析を開示し、それらを軽減するための実行可能な推奨事項を提供する。CAMセクターは、さまざまなアクターと利害関係者によって形成されたサービス、オペレーション、インフラストラクチャのエコシステム全体である。ENISAが提案した勧告は、サイバーセキュリティの脅威と懸念の増大に関する今日の文脈において、すべてのCAM関係者を導くことを目的としています。 発行された勧告は、欧州連合(EU)のCAMエコシステムにおけるサイバーセキュリティの改善と調和に寄与するものである。	https://www.enisa.europa.eu/news/enisa-news/how-to-secure-the-connected-automated-mobility-cam-ecosystem https://www.enisa.europa.eu/publications/recommendations-for-the-security-of-cam/	
2021/5/12	Executive Order on Improving the Nation's Cybersecurity	国のサイバーセキュリティの改善に関する大統領命令	1									1				バイデン大統領は、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Executive order(以下EOと略記)を発行（EO 14028）。EOは、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、非常に広範な内容が含まれ、ソフトウェアサプライチェーンのセキュリティと完全性に関連する様々なイニシャチブを通じてサイバーセキュリティを強化することを、NIST,CISAなど連保政府傘下の複数の機関に要求している。EOは以下のセクションで構成されている。 Sec.1. Policy ポリシー、Sec.2. Removing Barriers to Sharing Threat Information 脅威情報共有の障壁の除去、Sec.3. Modernizing Federal Government Cybersecurity連邦政府のサイバーセキュリティの近代化、Sec.4. Enhancing Software Supply Chain Security ソフトウェアサプライチェーンセキュリティの強化、Sec.5. Establishing a Cyber Safety Review Board サイバー安全審査委員会の設置、Sec.6. Standardizing the Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents サイバーセキュリティの脆弱性とインシデントへの対応に関する連邦政府のプレイブックの標準化、Sec.7 Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks 連邦政府ネットワークシステムにおけるサイバーセキュリティの脆弱性とインシデントの検出の改善、Sec.8. Improving the Federal Government's Investigative and Remediation Capabilities 連邦政府の調査及び修復能力の向上、Sec.9. National Security Systems 国家安全保障システム、Sec.10. Definitions	https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/	Section 4の大部分は「ソフトウェアJ Supply Chain に関する内容で、2020年12月に検知されたSolarwmdsorion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考えられている。
2021/5/14	White Paper (Draft) Establishing Confidence in IoT Device Security: How do we get there?	ホワイトペーパー（ドラフト） IoTデバイスセキュリティに対する信頼を確立する:どうやってそこにたどり着くのか?	1					1								NISTは、2020年11月から2021年1月にかけて、モノのインターネット(IoT)デバイスのサイバーセキュリティに対する信頼を提供するための代替アプローチの見直しを行い、これらのアプローチの専門家である政府および民間機関にインタビューを行った。このホワイトペーパーでは、アプローチの利用可能な風景を説明し、インタビュー中に一般的に聞くテーマを引き出しており、市場で IoT デバイスのセキュリティを確立するために現在利用できる信頼メカニズムの状況について説明する。 当文献は、IoTはネットワーク接続を介して情報やデータを収集、蓄積、伝送する点で他のITシステムと同様にセキュリティが必要であること、IoTの購入者、利用者の製品セキュリティの信頼を得るための方法(Confidence Mechalusm)として、大きく分けて業界による規制など政府の規制を伴わない方法と政府の規制を伴う方法が述べられている。ラベリング(labeling､label)の言及が随所に見られる。	https://csrc.nist.gov/publications/detail/white-paper/2021/05/14/establishing-confidence-in-iot-device-security/draft https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.05142021-draft.pdf	NISTより標題のWhite paper(Draft)が5/14に公開され、6/14までPulbic Commentsが受け付けられた。 本文献の著者の一人は、NIST IoT Programを率いるKaterilla Megas氏である。
2021/5/20	Trusted Internet of Things (IoT) Device Network Layer onboarding and lifecyde Management	信頼できるモノのインターネット（ioT）デバイスネットワーク層のオンボーディングとライフサイクル管理	1					1								モノのインターネット (IoT) デバイスのネットワーク層オンボーディングは、そのデバイスへのネットワーク資格情報のプロビジョニングである。現在、信頼できる IoT デバイスのオンボーディング プロセスが存在しない場合、多くのネットワークは、承認されていないデバイスがデバイスに接続される可能性がある。また、デバイスのオンボードが許可されていないネットワークによって引き継がれやすいデバイスも残る。 このナショナルサイバーセキュリティセンターオブエクセレンス(NCCoE)プロジェクトは、IoTデバイスの信頼できるネットワーク層オンボーディングへのアプローチとデバイスのライフサイクル管理に焦点を当てる。NCCoEは、NISTサイバーセキュリティフレームワークに沿った一連のサイバーセキュリティの課題に対処する市販の技術を使用して、信頼できるネットワークレイヤーオンボーディングソリューションの例を構築する。このプロジェクトは、自由に利用できるNISTサイバーセキュリティ実践ガイドになる。	https://www.nist.gov/news-events/news/2021/05/trusted-iot-device-network-layer-onboarding-and-lifecycle-management https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/trusted-iot-network-device-project-description-final.pdf	NISTがNationa1 Cybersecurity Center of Excellence (NCCCOE)のプロジェクトとして2021年５月20日に発足した同名プロジェクト発行の最初の文献。信頼性が必要とされるネットワークへの接続に先立ち、IoT製品のAuthentication and Authorization (AuthN and AuthZ、認証認可)に関わる分野に焦点。

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			
2021/5/21	ICT SUPPLY CHAIN RISK MANAGEMENT TOOLKIT	ICTサプライチェーンリスクマネジメントツールキット	1						1								ICT SUPPLY CHAIN RISK MANAGEMENT (SCRM) TASK FORCEの活動 戦略的メッセージ１：サプライチェーンのレジリエンスを強化する新しいツールキット このツールキットは、戦略的なメッセージ、ソーシャルメディア、ビデオ、リソースを含み、情報通信技術(ICT)サプライチェーンのセキュリティ保護において当社が果たす役割を強調するように設計されている。以下に詳述するすべての製品は、サプライチェーンの回復力を高めるために非常に効果的なツールを作るために業界標準を組み込んでいる。 戦略的メッセージ2：ベンダーとサプライヤーの信頼性を評価するためのリソース 文書として|、"Mitigating ICT Supply Chain Risks with Qualined Bidder and Manufacturer Lists"を発行。購入、調達に際し、サプライチェーンの真正性維持に適したベンダーの資格要件を定めている。 戦略的メッセージ３：適格な入札者リストとメーカーリストによるICTサプライチェーンリスクの緩和 文書として、"Building A More Resilient ICT Supply Chain: Lessons Leamed During The COVID-19 Pandemic"を発行。　今次感染症の世界的流行に伴うサプライチェーン上の教訓について分析。	https://www.cisa.gov/ict-scrm-task-force https://www.cisa.gov/ict-supply-chain-toolkit https://www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Qualified-Bidders-Lists_508.pdf https://www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Qualified-Bidders-Lists_508.pdf	戦略的メッセージ３の文書では、IoT、ITに限らずひろく物品調達一般を対象とするが、半導体不足、米国外一部地域でのワクチン不足に直面する現在にも教訓となるし、2011年の東日本大震災時のサプライチェーン問題から分析を開始している点も興味深い。
2021/5/25	Cybersecurity Certification: Candidate EUCC Scheme V1.1.1	サイバーセキュリティの認証：EUCCスキームV1.1.1候補			1					1							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	https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme	
2021/5/26	SP 1800-15 Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD	SP 1800-15 スモール ビジネスおよびホーム モノのインターネット (IoT) デバイスのセキュリティ保護: メーカーの使用状況の説明 (MUD) を使用したネットワーク ベースの攻撃の軽減	1					1									インターネット技術標準化委員会のメーカー使用法記述 (MUD) 仕様の目標は、モノのインターネット (IoT) デバイスがデバイスの製造元が意図したとおりに動作することである。MUD は、デバイスが意図した機能を実行するために必要なネットワーク通信を製造元が示す標準的な方法を提供する。MUD を使用すると、ネットワークは IoT デバイスが意図したとおりに実行する必要があるトラフィックのみを送受信することを自動的に許可し、ネットワークはデバイスとの他のすべての通信を禁止し、それによってネットワーク ベースの攻撃に対するデバイスの回復性を高める。このプロジェクトでは、NCCoE は、IoT デバイスが家庭または小規模ビジネス ネットワークに接続したときに、MUD がデバイスが意図した機能を実行するために必要なトラフィックのみを送受信することを自動的に許可できることを確認する機能を実証した。このNISTサイバーセキュリティプラクティスガイドでは、MUDプロトコルとツールがボットネットやその他のネットワークベースの脅威に対するIoTデバイスの脆弱性を軽減し、悪用されたIoTデバイスによる被害を減らす方法について説明する。また、IoT デバイスの開発者やメーカー、ネットワーク機器の開発者やメーカー、MUD 対応コンポーネントを使用するサービス プロバイダが、Mud を統合して使用して IoT ユーザーのセキュリティ要件を満たす方法を示す。	https://csrc.nist.gov/publications/detail/sp/1800-15/final https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-15.pdf	NISTNCCCOEが2019年から取り組んでいた、Manufacturer usage DescriPtion (MUD) (IETF RFC 8520) の利用に関する文書の最終版が公開された。　本文書は、IoT一般というより、ＭＵＤの具体的な実装指針と考えるのがよい。
2021/5/26	☒YBER; Identity Management and Discovery for IoT	サイバー;IoT ID 管理と IoT	1								1						このドキュメントでは、以下について、説明している。 ・IoT デバイスに適用可能な ID 管理のモデルについて ・デバイスの識別子とプロパティを管理するための、権限属性ツリーとして記述されたデータ構造を定義する。 ・既存のオントロジー SAREF にこれらの権限属性ツリーを適用する方法について ・権限属性ツリーの信頼を確立するための暗号化方式の要件を概説し、それらの要件を既存の暗号モデルにマッピングする。 （例えば、機能的暗号化、対称システムおよび非対称システムなど)。 ・ID 情報の公開、またはこの情報に基づく検出の受け入れまたは拒否に関して、ユーザーまたはデバイスのポリシーに関するポリシーの定義や推奨事項は定義または推奨されない。 ・いくつかの情報提供用の別館を使用して、ID 管理モデルを適用する方法を示す。 ・附属書 B は、他のデバイスによる権限属性ツリーの検出を可能にする「信頼義務」プロトコルで ID 管理モデルを適用]する方法を示す。 ・Annex C は、ID 管理モデルが既存のプロトコルにどのように適用され、検出を制御する能力を示している。	https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=47653	

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			
2021/6/2	Workshop and Call for Position Papers on Standards and Guidelines to Enhance Software Supply Chain Security	ソフトウェアサプライチェーンセキュリティを強化するための標準とガイドラインに関するワークショップと求人	1					1								NISTは、2021年6月2日と3日に、ソフトウェアサプライチェーンのセキュリティを強化し、2021年5月12日に発行された連邦政府のサイバーセキュリティ改善に関する大統領の執行命令(14028)を履行するためのバーチャルワークショップを開催した。 EOのセクション4は、NISTを通じて、ソフトウェアサプライチェーンのセキュリティを強化するための基準、ツール、ベストプラクティス、およびその他のガイドラインを特定する際に、連邦機関、民間セクター、学界、およびその他の利害関係者と協議するよう、商務長官に指示し、これらの基準とガイドラインは、連邦政府のソフトウェア調達を管理するために他の機関によって使用される。 このワークショップでは、EOのセクション4の課題に焦点を当てている。 ワークショップの目的は次のとおり。 行政命令によって求めるソフトウェア関連の標準とガイドラインを策定するNISTの計画を共有し、NISTがこれらの標準とガイドラインを開発する際に考慮すべきアプローチとコンテンツに関する情報やアイデアを受け取り、議論する。	https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/news-updates	
2021/6/2	CYBER Guide to Cyber Security for Consumer Internet of Things（Early Draft）	消費者向けモノのインターネットのためのサイバーセキュリティに関するサイバーガイド（初期草稿）	1								1					この技術報告書は、EN 303 645 および TS 103 645 のコンシューマー IoT デバイスに関して定義されている規定を満たすために製造業者および他の利害関係者を支援するためのガイダンスドキュメントとして役立つ。 この作業はEN 303 645およびTS 103 701と補完的である。これらの仕様と、それらの仕様の関係と、それらがどのように一緒に使用できるかについて説明され、規定を満たす完全な実装例のセットが提供される。可能な実装がすべて含まれるわけではなく、関連する場合は、サポート仕様へのポインタが含まれる。業界のプレーヤーによる使用と、将来の標準の開発が考慮される(例えば、特定のユースケースの専門分野、認定の側面)。	https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=59473	同上
2021/6/8	FACT SHEET: Biden-Harris Administration Announces Supply Chain Disruptions Task Force to Address Short-Term Supply Chain Discontinuities	バイデン-ハリス政権は、短期的なサプライチェーンの不連続性に対処するためのサプライチェーンの混乱タスクフォースを発表	1									1				広く戦略物資一般を対象に、2021/2/24、White House　より、米国のSupply Chain の課題、問題点のReview等を命じる大統領令（EO)14017 America's Supply Chains で示された、APIと呼ばれる薬品成分、Cntica1 Minera1 と言われるいわゆるレアメタル類、半導体、並びに大容量電池の特定四分野に対する100日Reviewの報告が6/8 White Houseより発表され。この報告はあくまで特定四分野を対象とし、IoTに限定されたものではないが、IoTだけでなく広くIT、OT製品、今や消費財一般にも利用される半導体が含まれている。	https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/08/fact-sheet-biden-harris-administration-announces-supply-chain-disruptions-task-force-to-address-short-term-supply-chain-discontinuities/	

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			
2021/6/8	European Cybersecurity Competence Centre and Network	欧州サイバーセキュリティ・コンピテンス・センター・ネットワーク			1							1				欧州サイバーセキュリティ・コンピテンス・センター（ECCC）は、ナショナル・コーディネーション・センター（NCC）のネットワークとともに、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フレームワークである。このエコシステムは、サイバーセキュリティ技術コミュニティの能力を強化し、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、この分野におけるEU産業の競争力を強化する。 ブカレストに設置されるECCCは、加盟国、産業界、サイバーセキュリティ技術コミュニティとともに、技術開発と、公共の関心分野や企業、特に中小企業への幅広い展開のための共通のアジェンダを策定し実施する。 センターとネットワークは、戦略的なサイバーセキュリティ・プロジェクトへの共同投資を通じて、技術的主権を強化する。 U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また、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Cybersecurity Copetence Centre/Network（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するとして、ヨーロッパのサイバーセキュリティ能力を強化および維持し、ヨーロッパ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）の第173条（3）および第188条（1）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。 センターとネットワークは、戦略的な投資決定を行い、EU、加盟国、間接的に業界からの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。 さらに、革新的なサイバーセキュリティソリューションの展開をサポートし、コミュニティ内のすべての関連する利害関係者、特に研究および産業コミュニティ、ならびに公的機関の間でのコラボレーションと専門知識および能力の共有を促進する。	https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre	EUにできた新組織であるが、以下のホライゾンのパイロットプロジェクトを最新動向の情報源として参照している。 CONCORDIA: https://www.concordia-h2020.eu/cybersecurityevents/ ECHO: https://echonetwork.eu/events/ SPARTA: https://www.sparta.eu/events/ CyberSec4Europe: https://cybersec4europe.eu/events/ Events are also available on their join
2021/6/8	The European Cybersecurity Network and Cybersecurity Competence Centre help the EU retain and develop cybersecurity technological and industrial capacities.	ECCC「欧州サイバーセキュリティコンピテンシーセンター／ネットワーク」がブカレストで業務開始	1									1				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また、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Cybersecurity Copetence Centre/Network（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するとして、ヨーロッパのサイバーセキュリティ能力を強化および維持し、ヨーロッパ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）の第173条（3）および第188条（1）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。 センターとネットワークは、戦略的な投資決定を行い、EU、加盟国、間接的に業界からの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。 さらに、革新的なサイバーセキュリティソリューションの展開をサポートし、コミュニティ内のすべての関連する利害関係者、特に研究および産業コミュニティ、ならびに公的機関の間でのコラボレーションと専門知識および能力の共有を促進する。	https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre	EUにできた新組織であるが、以下のホライゾンのパイロットプロジェクトを最新動向の情報源として参照している CONCORDIA: https://www.concordia-h2020.eu/cybersecurityevents/ ECHO: https://echonetwork.eu/events/ SPARTA: https://www.sparta.eu/events/ CyberSec4Europe: https://cybersec4europe.eu/events/
2021/6/8	NISTIR 8259B Roundtable Series	NISTIR 8259B オンライン会合	1					1								NISTIR 8259B (DRAFT)、IoT Non-Technical Supporting Capability CoreBaselineに関するRoundtableを、オンラインで4回に渡り実施。 当該文書の構成分野要素毎に実施された模様。　会合の後、blogで模様が公開されており、製造業者だけでなく、ユーザの意識向上の必要性、対象毎のセキュリティ文書作成の必要と、それが負担な場合、中間者の介在の可能性など、いくつか興味深い提起が見られる。	https://www.nist.gov/blogs/cybersecurity-insights/iot-non-technical-supporting-capabilities-you-talked-we-listened	
2021/6/14	ETSI Security Week 2021	ETSI セキュリティ・ウィーク 2021														ETSIのサイバーセキュリティに関する主要な年次イベントが、2021年6月14日から18日にかけてバーチャルで開催され、世界各国からさらに多様な参加者が集まり、サイバーセキュリティの5つの重要な側面について議論した。 ・人工知能（AI）の保護 ・モノのインターネット（IoT） ・ネットワーク機能仮想化(NFV) ・マルチアクセス・エッジコンピューティング(MEC) ・サイバーセキュリティ政策	https://www.etsi.org/events/1923-etsi-security-week-2021	

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			
2021/6/16	Software and Supply Chain Assurance Forum	ソフトウェアとサプライチェーン保証フォーラム	1					1								Cyber Supply Chain Risk Management （C-SCRM）によるSoftware and Supply Chain Assurance Forumを開催。 2つのセッションは、保健セクターとエネルギーセクターのスピーカーを備えている。各部門には独自の特性と課題があるが、サイバーサプライチェーンのリスク管理とソフトウェアおよびハードウェアアシュアランスの実践、ツール、セキュリティコントロールの多くは、本質的に横断的であり、あらゆる組織が適用することができる。 このイベントは、エグゼクティブ・オーダー14028に関するNISTの取り組みに関する簡単なアップデートを提供する。	https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/ssca	
2021/6/23	EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents	EUサイバーセキュリティ：欧州委員会は、大規模なセキュリティインシデントへの対応を強化するための共同サイバーユニットを提案	1									1				欧州委員会は本日、欧州連合全体の企業や市民の生活だけでなく、公共サービスに影響を与える深刻なサイバーインシデントの増加に対処するための新しい共同サイバーユニットを構築するビジョンを提示した。サイバー攻撃の数、規模、結果が増大し、セキュリティに大きな影響を与えるにつれて、サイバーセキュリティの分野における高度で協調的な対応がますます必要になっている。 EU内のすべての関連する関係者は、「知る必要がある」だけでなく、「共有する必要がある」という原則に基づき、集合的に対応し、関連する情報を交換する準備をする必要がある。 ウルズラフォンデアライエン大統領が政治ガイドラインで最初に発表した共同サイバーユニットは、本日提案された、EUとその加盟国が利用できるリソースと専門知識を結集して、大量のサイバー事件や危機を効果的に防止、抑止、対応することを目的としている。共同サイバーユニットにより、彼らは仮想的および物理的な協力のプラットフォームを持つことになる。関連するEUの機関、団体、機関は、加盟国とともに、大規模なサイバー攻撃に対抗するための連帯と支援のためのヨーロッパのプラットフォームを段階的に構築していく。	https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3088	
2021/6/23	EU Boost against cyberattacks: EU Agency for Cybersecurity welcomes proposal for the Joint Cyber Unit	サイバー攻撃に対するEUのブースト：EUサイバーセキュリティ機関は、共同サイバーユニットの提案を歓迎	1							1		1				欧州委員会のフォン・デア・ライエン委員長が2年前に提案した共同サイバーユニット(JCU)の概念は、欧州のサイバーセキュリティ危機管理フレームワークを完成するための重要なステップである。EUサイバーセキュリティ機関(ENISA)は、共同サイバーユニットを構築するための委員会勧告の提案とそれが果たす役割を歓迎する。 サイバーセキュリティ法は、機関が運用レベルで協力し、連合の機関、団体、オフィス、機関との相乗効果を確立することを義務付けている。JCUは、機関が構造的な方法でこれを達成するのに貢献する。 EUサイバーセキュリティ機関が共同サイバーユニットの構築に提供する支援は、サイバーセキュリティ法に定められた規定の強化として行われ、機関の活動の範囲が広がっている。この新しいイニシアチブは、欧州連合(EU)内のより高い共通レベルのサイバーセキュリティを達成するために、機関がどのように貢献できるかについての重要なステップである。	https://www.enisa.europa.eu/news/enisa-news/eu-boost-against-cyberattacks-eu-agency-for-cybersecurity-welcomes-proposal-for-the-joint-cyber-unit	共同サイバーユニットの提案により、ENISAの拠点がBrusse1にCERT-EUに隣接して開設され、これら二拠点を中核として、EU加回国各国のNationa1 CSIRTs、Europo1など法執行機関、軍を含めたインシデント対応とコーディネーションの実現が期待される。
2021/6/25	Definition of Critical Software Under Executive Order (EO) 14028	大統領命令（EO）14028に基づく重要なソフトウェアの定義	1					1								大統領令（E0 14028）に基づくCritical Software（重要ソフトウェア）の定義を示す文書がNISTより公開された。	https://www.nist.gov/system/files/documents/2021/06/25/EO%20Critical%20FINAL_1.pdf	
2021/6/25	ETSI virtual Security Week 2021: recorded presentations now available	ETSI virtual Security Week 2021: 録画されたプレゼンテーションを公開			1						1					6月14日から6月18日まで開催されたETSIセキュリティウィーク2021は、70か国以上から1000人以上の視聴者が参加して成功裏に終了した。このイベントでは、さまざまな利害関係者が集まり、プレゼンテーション、パネルディスカッション、ライブQ＆Aセッションでサイバーセキュリティの5つの側面が議論された。 「人工知能の保護」セッションでは、AIを保護するための問題と解決策、およびAIのテスト方法が紹介された。目標は、さまざまなアルゴリズムを考慮したAIおよびAIベースのシステムのテストのガイドラインを作成することにある。 「モノのインターネット（IoT）」セッションでは、IoTと次のサイバーセキュリティ認証制度が発表され、業界、政府機関、研究所からIoT認証に関するフィードバックと経験が提供された。 「ネットワーク機能仮想化（NFV）」では、そのリスク、脅威、および将来に向けて取り組む必要のある脆弱性を取り上げた。他セッションでは、NFV標準、特にETSI標準と、重要な問題を軽減および対処する方法が紹介された。 「マルチアクセスエッジコンピューティング（MEC）」では、MECセキュリティの標準化の概要が示され、MECテクノロジーが5Gの多くの重要なユースケースにどのように役立つかが強調された。MECデバイスの5Gエッジコンピューティング、自動車、およびソフトウェアのセキュリティとメンテナンスが説明された。 最終日には、サイバーセキュリティ法に基づく標準の将来計画とともにサイバーセキュリティポリシーに焦点が当てられた。CSAに基づく5G認定、現在のスキームからCSAスキームへの移行、新しい手順とラボの認定に関する経験の復活、およびSMEへの影響とSMEからの貢献が含まれた。（CSA:サイバーセキュリティ法、SME:中小事業者）	https://www.etsi.org/newsroom/news/1942-etsi-virtual-security-week-2021-recorded-presentations-now-available	サイバーセキュリティ認証制度に関するセッションにおける発表において、Huaweiは既に存在する各地域の認証制度との相互関係を示す必要性が業界意見として示されている。各発表は登録により視聴可能となっている。

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			
2021/7/9	Security Measures for “EO-Critical Software” Use	「EOクリティカルソフトウェア」使用のセキュリティ対策	1					1								特権の最少、ネットワークのセグメンテーション、適切な構成の適用を含む、重要なソフトウェア使用のセキュリティ対策を概説する公開ガイダンスは、2021年5月12日の国家のサイバーセキュリティ改善に関する大統領執行命令(14028)が求めるソフトウェアサプライチェーンのセキュリティを強化するためのNISTの課題の1つである。NISTは、ポジションペーパーやワークショップの呼びかけを通じて一般からの広範な意見を検討し、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(CISA)および管理予算局(OMB)と緊密に協力してこのガイダンスを作成した。	https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eo-critical-software-use-2 https://www.nist.gov/system/files/documents/2021/07/09/Critical%20Software%20Use%20Security%20Measures%20Guidance.pdf	
2021/7/13	Recommended Minimum Standards for Vendor or Developer Verification (Testing) of Software Under Executive Order	ソフトウェアのベンダーまたは開発者の検証(テスト)に推奨される最低基準(EO)14028	1					1								NISTは、コミュニティからポジションペーパーを募り、インプットを収集するための仮想ワークショップを主催し、国家安全保障局(NSA)と協議して、堅牢なテストプログラムの文脈で基準を置くために推奨される最低基準と補足資料を開発した。	https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/recommended-minimum-standards-vendor-or https://www.nist.gov/system/files/documents/2021/07/13/Developer%20Verification%20of%20Software.pdf	
2021/7/15	The corrdinated framework for cyber resilience provisioning guaranteeing tusted supply chains of ICT systems	ICTシステムの信頼できるサプライチェーンを保証するサイバーレジリエンスプロビジョニングのための調整されたフレームワーク			1							1				革新的なテクノロジーとビジネスモデルを備えたICTシステムの止められない進化は、大規模なデジタル変革とインダストリー4.0革命を推進している。 同時に、ICTシステムへの信頼性が高い社会ほど、ICTインフラストラクチャのわずかな混乱の影響がより重大になる。 今日、ICTシステムの回復力は非常に高く、すべてのICTシステムは、あらゆるタイプの混乱をタイムリーに防止、抵抗、および回復するための少なくとも一連の基本的なメカニズムを実装し、サービス品質とユーザー体験への影響を最小限に抑えることが期待されている。 この期待に対してFishy プロジェクトは5つの課題を挙げ、それらのソリューションの提案を進めるとしている。 課題1：脆弱性とリスク管理のためのエンドツーエンドのソリューションの必要性。 課題2：セキュリティ保証と信頼保証のための証拠に基づく測定基準の欠如。 課題3：ICTシステムのマルチアクターおよびマルチベンダーサプライチェーンにおける面倒な調整。 課題4：静的なサイバーセキュリティネットワーク構成と動的なシステム監査。 課題5：構成されたICTシステムに統合サイバーセキュリティソリューションが広く採用される可能性は低い。	https://fishy-project.eu/promotional-material/white-paper https://fishy-project.eu/sites/fishy-project.eu/files/public/content-files/2021/FISHY_White_paper_last.pdf	Fishy Projectは'A coordinated framework for cyber resilient supply chain systems over complex ICT infrastructures'のタイトルで2020年9月1日に開始され、2023年8月31日に終了予定であり、いくつかのユースケースに取り組んでいる。
2021/7/19	NIST blog: IoT Non-Technical Supporting Capabilities: You Talked, We Listened	NIST ブログ: IoTの非技術的なサポート機能に関する意見聴取						1								2020年12月に4つのIoTサイバーセキュリティドラフト文書が発表された後の継続的なコミュニティ活動の一環として、NISTは2021年6月に、NISTIR 8259B、IoT非技術サポート機能コアベースラインの草案に焦点を当てた円卓会議のカルテットを開催した。ラウンドテーブルは4週間に及び、NISTIR 8259Bで定義された4つのコア機能とベースラインの適用に関する一般的な議論に取り組んだ。 ・6月8日:ドキュメント　6月15日:情報の受信と普及　6月22日:教育と意識　6 月 29 日: 非技術力ベースラインの適用 ・円卓会議参加者は、NISTIR 8259Bベースラインに記載されている4つの機能すべてを支持。 ・IoTデバイスのセキュリティにおける消費者の役割に対する意識を高める努力は重要であり価値がある。 ・顧客がIoTデバイスの問題を簡単で技術的スキルを伴わない方法で報告できる単一の場所への要望。	https://www.nist.gov/blogs/cybersecurity-insights/iot-non-technical-supporting-capabilities-you-talked-we-listened	
2021/7/26	2021年 3月下旬以降の SIP CPSへ影響しうる諸動静	2021年 3月下旬以降の SIP CPSへ影響しうる諸動静													1	米国・足立氏による米国・EUにおける2021年 3月下旬以降7月26日時点までの SIP CPSへ影響しうる諸動静の報告書。 米国： 5/12大統領令EO14028におけるSec. 4.：Enhancing Software Supply Chain Securityにて2020/12の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を背景としたSoftware Supply Chainへのセキュリティ強化に向けた活動が進められている。 EU： ENISA含む欧州連合ではIoT分野についてはあまり大きな動向は少なくとも外部からは確認できない。ただし、報告期間中、一般的なサイバーセキュリティの様々な分野、例えばEU Cybersecurity Certification, Incident Response and CSIRT, 5G, Pandemic, Telecom Securityなどで活発な活動が観察される。		足立氏レポートを参照

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			
2021/7/26	From ports to rail yards, global supply lines struggle amid virus outbreaks in the developing world	途上国でのウイルス発生で、港から鉄道まで、グローバルなサプライラインが苦境に立たされる												1		コロナウイルスが新たに発生し、ベトナムやバングラデシュなどで工場の操業停止を余儀なくされている。サプライチェーンの混乱に拍車がかかり、消費者が学校に戻る買い物を始めるにつれて、米国の一部の小売店では棚が空になる可能性がある。 今回の海外での労働停止は、パンデミックに関連した製造業や輸送業の苦境の中で、約1年半ぶりの出来事である。アメリカの大手鉄道会社2社は先週、西海岸の港からシカゴまでの輸送を制限した。 アジアの工場地帯からアメリカ中西部まで、感染力の強いデルタウイルスを追い越そうとする景気回復の流れの中で、供給面での問題が深刻化している。コビド19の感染が相次いだ中国の主要港の制限による余震は、今月末には米国西海岸の 工場の滞留状況を悪化させることが予想される。	https://www.washingtonpost.com/business/2021/07/27/supply-chains-freight-rail-ports/	
2021/7/26	☒VBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements	サイバー; 消費者のモノのインターネットのためのサイバーセキュリティ：ベースライン要件の適合性評価	1								1					提案されたドキュメントは、EN 303 645 / TS 103 645の規定に照らして消費者向けIoT製品を評価するためのテストシナリオを指定することである。必須および推奨される評価、およびそれらの実装をサポートするためのガイダンスと例を示す。 このドキュメントは、関連製品のセキュリティを保証するテストラボや認証機関、および自己評価の実施を希望するメーカーが使用することを目的としている。 このドキュメントが使用されている保証スキームとその結果は、範囲外です。 提案された文書はまた、詳細なテストプロトコルを設定していない。 ただし、提案されたドキュメントは、サイバーセキュリティ法で提案されている将来のEU共通サイバーセキュリティ認証スキームへの入力として意図されている。 Version 1.1.1とされる版が一般からダウンロード可能となっており、文書名などから 2021年 8月に確定したものと推測できる。	https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58434	ETSI TS 103 645並びにETSI EN 303 645の定める Consumer IoT Baseline requirementsへの適合試験 (Conformance testing)実施の手順、要領について具体的に規定。 関連 ETSI標準との関連は Figure 1 (Page 15)に示される。 関連付属文書類の進捗は認められるもののまだ草稿段階にある模様。
2021/7/27	Workshop and Call for Papers on Cybersecurity Labeling Programs for Consumers: Internet of Things (IoT) Devices and Software	消費者のためのサイバーセキュリティラベリングプログラムに関するワークショップと論文の呼びかけ: モノのインターネット(IoT)デバイスとソフトウェア	1					1								NISTより、EXECUTIVE ORDER 14028, IMPROVING THE NATION'S CYBERSECURITYに対して、次の 2 点について発表された。 1. Workshop on Cybersecurity Labeling Programs for Consumers: Internet of Things (IoT) Devices and Softwareを9月14,15の両日、11am~4pm EDTでオンラインで実施 2. Consumer Software LabelingについてCall for Paper発出、8月17日締め切り	https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/workshop-and-call-papers-cybersecurity-labeling 応募・提出Paper情報 https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/consumer-software-labeling-position-papers	NISTは、IoT機器や消費者向けソフトウェアの cybersecurity labelingの取組みを開始するための課題や実践的なアプローチに関する提案やフィードバックを求めている。 この情報は、国家のサイバーセキュリティの向上に関する大統領令（EO）の任務をNISTが遂行するのに役立てられる。 利害関係者は論文募集への対応、近日公開予定のホワイトペーパーのドラフトへのコメント、2021年9月14日～15日に開催されるワークショップへの参加が求められている
2021/7/28	National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems	重要なインフラストラクチャ制御システムのサイバーセキュリティの改善に関する国家安全保障覚書	1									1				National Security Memorandum Sec.1 方針 国家の重要なインフラストラクチャの保護は政権の方針であり、特に国家の重要な機能をサポートするシステムのサイバーセキュリティと回復力に焦点を当てている。 Sec.2 産業用制御システムサイバーセキュリティイニシアチブ 重要なシステムのサイバーセキュリティの改善のために、産業用制御システムサイバーセキュリティイニシアチブ（イニシアチブ）を設立する。 イニシアチブの主な目的は、脅威の可視性、兆候、検出、警告を提供し、重要な制御システムと運用技術におけるサイバーセキュリティの対応機能を促進する技術とシステムの展開を促進し、米国の重要なインフラストラクチャを守ることである。 Sec.3 イニシアチブの促進 (a)イニシアチブは、電力サブセクターとのパイロット作業から始まり、現在は天然ガスパイプラインについても同様の作業が続いている。 上下水道セクターシステムと化学セクターへの取り組みは、今年後半に続く予定。 (b)セクターリスク管理機関、およびその他の執行部門および機関は、適切かつ適用法と一致して、重要なインフラストラクチャの利害関係者と協力する。 Sec.4 サイバーセキュリティパフォーマンスの目標 この取り組みは、国土安全保障長官が2021年9月22日までに重要なインフラストラクチャセクター全体の制御システムの予備目標を発行することから始まり、その後1年以内にセクター間の最終制御システム目標が発行される。	https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/	主な命令内容として - Industrial Control Systems Cybersecurity Initiativeの設立 (Section 2 and 3) - Critical Infrastructure Cybersecurity Performance Goalsの策定を国土安全保障長官並びに商務長官（執行宛としてNIST所長を明示）に命令 (Section 4(a)) - このGoalsの対象は、Critical Infrastructure Owners and Operatorsが守るべき(should) Baseline Security Practicesであり、ICSとは明示されていない点に注意。 - 初期目標 Preliminary Goalsを9月22日までに、業界ごと Sector specificの目標を当memorandom発行日より起算して一年以内に作成

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			
2021/7/29	Iran's Secret Cyber Files	イランのサイバー攻撃研究ファイル												1		スカイニュースはイランからのサイバー攻撃やインフラをどのように攻撃するかの研究レポートを入手した。入手した内部ファイルには、世界の海運業界で使用されている衛星通信デバイスに関する情報や、世界中のスマートビルの照明、暖房、換気などを制御するコンピュータベースのシステムも含まれている。 攻撃の対象例として、大型貨物船（バラスト水について）、ガソリンスタンド（給油システム）、会場通信（衛星通信）、スマートビル（建物管理システム）等が示されている。	https://news.sky.com/story/irans-secret-cyber-files-on-how-cargo-ships-and-petrol-stations-could-be-attacked-12364871	
2021/7/29	2021 SONICWALL CYBER THREAT REPORT Cyber threat intelligence for navigating today's business reality	2021 SONICWALL CYBER THREATREPORT今日のビジネスの現実をナビゲートするためのサイバー脅威インテリジェンス		1												ソニックウォール：わずか6か月で3億470万ランサムウェアの攻撃を記録するECLIPSE2020グローバル合計 ・ランサムウェアは、米国（185%）、英国（144%）で年初来の大規模な急増を示した ・Ryuk、Cerber、SamSamが今年のトップファミリーであり、ランサムウェアの全量の64%を占める。 ・政府、教育、ヘルスケア、小売業界がランサムウェアの標的になりつつある ・世界全体で年初来で59%増加し、IoTマルウェアは2018年以降も成長を続けている ・クリプトジャッキングマルウェアは主要な脅威であり、世界全体で年初来23%増加し、米国で22%増加している。 ・SonicWallの特許取得済みのRTDMI™は、これまでにないマルウェアを発見し、2020年上半期に年々54%の増加を記録。	https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2021-cyber-threat-report.pdf	
2021/7/29	Threat Landscape for Supply Chain Attacks	サプライチェーン攻撃の脅威の状況			1					1						サプライチェーン攻撃は、単一のサプライヤに対する1回の攻撃によって引き起こされる連鎖反応がプロバイダーのネットワークを危険にさらす可能性があるため、サイバーセキュリティの専門家にとって長年懸念されてきた。 マルウェアは、攻撃者が攻撃の62%で利用する攻撃手法となっている。 2020年1月から2021年7月にかけての24件の攻撃を分析したこのENISAレポートによると、攻撃者がすでにサプライヤに注意を向けている場合、組織にとって強力なセキュリティ保護でも十分ではない。これは、システムのダウンタイム、金銭的損失、評判の低下など、これらの攻撃の影響が増大していることからも明らかである。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たと報告している。 サプライチェーン攻撃は、2021年には昨年と比較して4倍になると予想されている。 この新しい傾向は、政策立案者とサイバーセキュリティコミュニティが今行動する必要性を強調してる。 そのため、将来の潜在的なサプライチェーン攻撃を防止して対応し、その影響を軽減するための新しい保護対策を早急に導入する必要がある。	https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks	
2021/7/29	Methodology for a Sectoral Cybersecurity Assessment	セクター別サイバーセキュリティ評価の方法論	1	1						1						ENISAより 7月 29日に、”Methodology for Sectoral Cybersecurity 211 Assessments, EU Cybersecurity Certification Framework”が発行された。これは産業別、業界別(Sectoral)に、EU Cybersecurity Act（以下 CSAと略記）で定められる EU Certification Schemeに準拠しつつ、それぞれの業界に適した Certification Schemeを作成する参考書という位置付けである。この文書で説明するセクター型サイバーセキュリティ評価(SCSA方法論)の方法論は、セクター間のマルチステークホルダーシステムおよびセクターによるサイバーセキュリティ認証スキームの作成に関するICTセキュリティのコンテキストにおける目的に対応している。SCSA手法を適用することで、セクターICTシステムと関係するステークホルダー間の関係に関する健全な情報を生成し、ICT関連リスクに関する透明性を提供し、セクターICTシステムのICTセキュリティの実施を最適化する可能性を提供している。また、リスクベースのセキュリティ要件と保証要件の識別に関する欧州サイバーセキュリティ法の要件を完全にサポートすることもできる。	https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment	本ガイドラインの強制力はないが、本格的な EU Certification Schemes導入の具体的な入り口となり、予想される IoT Certification Schemeへの警戒と監視の継続が必要と考える。
2021/7/29	Understanding the increase in Supply Chain Security Attacks	サプライチェーンセキュリティ攻撃の増加を理解する			1					1						サプライチェーン攻撃は、単一のサプライヤに対する1回の攻撃によって引き起こされる連鎖反応がプロバイダーのネットワークを危険にさらす可能性があるため、サイバーセキュリティの専門家にとって長年懸念されてきた。 マルウェアは、攻撃者が攻撃の62%で利用する攻撃手法となっている。 2020年1月から2021年7月にかけての24件の攻撃を分析したこのENISAレポートによると、攻撃者がすでにサプライヤに注意を向けている場合、組織にとって強力なセキュリティ保護でも十分ではない。これは、システムのダウンタイム、金銭的損失、評判の低下など、これらの攻撃の影響が増大していることからも明らかである。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たと報告している。 サプライチェーン攻撃は、2021年には昨年と比較して4倍になると予想されている。 この新しい傾向は、政策立案者とサイバーセキュリティコミュニティが今行動する必要性を強調してる。 そのため、将来の潜在的なサプライチェーン攻撃を防止して対応し、その影響を軽減するための新しい保護対策を早急に導入する必要がある。		参考文献 https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks/view/++widget++form.widgets.fullReport/@@download/ENISA+Threat+Landscape+for+Supply+Chain+Attacks.pdf

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			
2021/7/29	ENISA Threat Landscape for Supply Chain Attack	サプライチェーンへの攻撃に関する脅威の状況			1					1						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％がサプライヤーのコードに焦点を合わせていることを発見している。	https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks	
2021/8/1	Draft NIST SP 800-160 Vol. 2 Rev. 1, Developing Cyber-Resilient Systems; A Systems Security Engineering Approach	Draft NIST SP 800-160 Vol. 2 Rev. 1, サイバーレジリエント・システムの開発：システム・セキュリティ・エンジニアリング・アプローチ	1					1								NISTのシステム・セキュリティ・エンジニアリング・イニシアチブの目的は、ステークホルダーの要求や保護ニーズの観点から、セキュリティ、安全性、回復力の問題に、確立されたエンジニアリング・プロセスを用いて取り組み、システムのライフサイクル全体にわたって要求やニーズに確実に対応し、より信頼性の高いシステムを開発することにある。この目的のために、NIST Special Publication (SP) 800-160 Volume 2では、サイバーレジリエンスエンジニアリングに焦点を当てている。これは、レジリエンスエンジニアリングやシステムセキュリティエンジニアリングと組み合わせて適用することで、より生存性の高い、信頼できるシステムを開発するための、新たな専門システムエンジニアリング分野である。サイバーレジリエンスエンジニアリングとは、サイバーリソースを利用する、あるいは利用可能な不利な状況、ストレス、攻撃、侵害を予測し、それに耐え、回復し、適応する能力を備えたシステムの信頼性を構築、設計、開発、維持することを目的としている。リスク管理の観点から、サイバーレジリエンスは、サイバーリソースに依存することによるミッション、ビジネス、組織、またはセクターのリスクを軽減することを目的としてる 本書は、ISO/IEC/IEEE 15288:2015、NIST Special Publication (SP) 800-160, Volume 1、NIST SP 800-37と併せて使用する。これは、リスク管理プロセスと連動したシステムライフサイクルプロセスに関するシステムエンジニアリングの視点に基づいて、特定されたサイバーレジリエンスの成果を達成するためのハンドブックとみなすことができ、組織の経験と専門知識が、その目的のために何が正しいかを判断するのに役立つと考えられる。組織は、本書に記載されているサイバーレジリエンスの構成要素（目的、技術、アプローチ、設計原則など）の一部またはすべてを選択、適応、使用し、システムを設計する必要のある技術、運用、脅威の環境に構成要素を適用することができる。	https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/draft	
2021/8/4	INFRA:HALT	RESEARCH REPORT													1	Forescoutリサーチラボと JFrogセキュリティリサーチは、INFRA:HALTと総称して呼び出しているNICHEStack TCP/IPスタックに影響を与える14の新しい脆弱性のセットを発見した。この新しい脆弱性により、リモートでコードが実行され、サービス拒否、情報漏洩、TCP スプーフィング、または DNS キャッシュ ポイズニングが可能になる。 NicheStackは、いくつかの重要なインフラストラクチャ分野で一般的に見られる運用技術(OT)デバイスで使用され、主要なOTデバイスベンダーがこれらの脆弱性の影響を受けていると推定している。 Forescout Research LabsおよびJFrog Security Researchは、影響を受ける製品(オープンソースのTCP/IPスタック検出器がこの点で役立つ可能性がある)を特定し、その結果をサイバーセキュリティコミュニティと共有するベンダーを支援することに取り組んでいる。これらの脆弱性の性質は、リスクの高まりにつながり、業界が世界的な公益事業、石油・ガスパイプライン事業者、ヘルスケアおよびサプライチェーンに対するOT攻撃の増加を見ている時期に、国家の重要なインフラを暴露する可能性がある。	https://www.forescout.com/resources/infrahalt-discovering-mitigating-large-scale-ot-vulnerabilities/ https://www.forescout.com/blog/new-critical-operational-technology-vulnerabilities-found-on-nichestack/	
2021/8/5	IoT Random Number Generator vulnerability presented at DefCon just a few days ago	数日前にDefConで提示されたIoT乱数ジェネレータの脆弱性													1	DefConでの 8/5の発表に関する情報。 IoTセキュリティの基盤には、世界中の350億台ものデバイスに影響を与える欠陥がある。基本的に、ハードウェアの乱数生成器（RNG）を搭載したすべてのIoTデバイスに乱数を適切に生成できないという深刻な脆弱性があり、上流で使用する際のセキュリティが損なわれる。	https://labs.bishopfox.com/tech-blog/youre-doing-iot-rng https://thehackernews.com/2021/08/a-critical-random-number-generator-flaw.html	・古典的なRNGに起因の脆弱性。講師の言う 通りだと「既存の」IoTへの影響は大きくA. 信頼の創出、証明で、 HAL function(関数）で生成されたHardware RNGを利用しておられる場合、 検討が必要。
2021/8/10	MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES （Protecting Critical Software Through Enhanced Security Measures）	行政部および行政機関の長のための覚書（強化されたセキュリティ対策による重要なソフトウェアの保護）	1									1				5月にホワイトハウスから出された大統領令（Executive Order14028）に関連して、大統領行政府のOffice of Management and Budget（OMB）からCritical Softwareに関する覚書（memorundam）が出た。 連邦各省庁でcritical softwareの特定とNISTが先日公開の関連指針による対策の実施が求められる。 NISTのガイダンスを実装するには、政府機関は重要なソフトウェアを特定し、そのソフトウェアの使用に 必要なセキュリティ対策を採用する必要があります。それにより、本件の基本的な目的の達成が可能になる。 全ての政府機関はシステムの重要なソフトウェアを60日以内に特定し、位年以内にセキュリティ対策を実施する ことが求められる。	https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-30.pdf https://www.nextgov.com/cybersecurity/2021/08/white-house-memo-orders-agencies-identify-critical-software/184495/	

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			
2021/8/16	Advisory: Multiple Issues in Realtek SDK Affects Hundreds of Thousands of Devices Down the Supply Chain	Realtek SDKの複数の問題が、サプライチェーンの下にある数十万のデバイスに影響を与える													1	IoT 空間の多くの組み込みデバイスに見られるRealtek チップセットRTL819xDは、SDKの機能によりRealtekから提供される別のバイナリコードを実行できることが判明した。IoT Inspector社ではこれらの機能に対する脆弱性調査を行い、コマンドインジェクションからUPnP、HTTP(管理Webインターフェイス)、Realtekのカスタムネットワークサービスに影響を与えるメモリ破損に至るまで、12以上の脆弱性を特定し、少なくとも65の影響を受けるベンダーを特定した。 影響を受けるデバイスは、ワイヤレス機能を実装し、使用事例の広い範囲をカバーしている。	https://www.iot-inspector.com/blog/advisory-multiple-issues-realtek-sdk-iot-supply-chain/ https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2021-35392_35395.pdf	IoT Inspectorが実施したと思われるCVSS(おそらくversion V.3.x)評価によると、CVE-2021-35395, 35394がともに9.8, 35393, 35392が8.1とされる。 これらの評価が妥当な場合、かなり深刻な脆弱性と考えられる。
2021/8/17	CVE-2021-28372：ThroughTek Kalay P2P SDK vulnerability	CVE-2021-28372：ThroughTek Kalay P2P SDK 脆弱性情報							1							監視映像IoTソリューション企業であるThroughTekのSDKに関する脆弱性情報： 影響を受ける ThroughTek P2P 製品は、不適切なアクセス制御に対して脆弱である可能性がある。この脆弱性により、攻撃者は機密情報 (カメラ フィードなど) にアクセスしたり、リモートでコードを実行したりする可能性がある。 ThroughTekは、クラウドプラットフォームの一部としてP2P接続を備えたIPカメラの複数の相手先ブランドを供給している。	https://us-cert.cisa.gov/ics/advisories/icsa-21-229-01 https://www.fireeye.com/blog/threat-research/2021/08/mandiant-discloses-critical-vulnerability-affecting-iot-devices.html	CVE-2021-28372のCVSS v3 base score は 9.8 (AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). すなわち、極めて危険性の高い脆弱性と考えられる。
2021/8/23	Botnet targets hundreds of thousands of devices using Realtek SDK	ボットネットは、RealtekSDKを使用して数十万のデバイスをターゲットにしています												1		8月16日、IoT Inspector Research Labによって、Realtek製チップセットの一部として配布されているソフトウェアSDKに複数の脆弱性があることが公表された。この脆弱性により、攻撃者は影響を受けたデバイスを完全に侵害し、制御することができる。 公開からわずか2日後、SAM Seamless Network社のホームセキュリティソリューション「Secure Home」は、これらの脆弱性を悪用してマルウェア「Mirai」の亜種を拡散しようとする試みを検知した。	https://www.bleepingcomputer.com/news/security/botnet-targets-hundreds-of-thousands-of-devices-using-realtek-sdk/	
2021/8/25	SP 800-140C Rev. 1 (Draft) CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759	SP 800-140C Rev. 1（ドラフト）CMVP承認済みセキュリティ機能：CMVP検証機関によるISO / IEC24759の更新							1							NIST特別刊文書(SP)800-140xシリーズは、連邦情報処理標準(FIPS)出版140-3、暗号モジュールのセキュリティ要件、および関連する検証テストプログラムである暗号モジュール検証プログラム(CMVP)をサポートしています。 シリーズは、FIPS 140-3 の派生テスト要件(DTR)の変更を指定し、ISO/IEC 24759 と共に使用されます。 今回公表されたのは、NIST SP 800-140xシリーズのうち、下記に示す三点のDraft (案)であり、コメント受付締め切りは9月20日である。 ・Draft NIST SP 800-140C, Revision 1, CMVP Approved Security Functions:CMVP Validation Authority Updates to ISO/IEC 24759 ・Draft NIST SP 800-140D, Revision 1, CMVP Approved Sensitive Security Parameter Generation and Establishment Methods: CMVP Validation Authority Updates to ISO/IEC 24759 ・Draft NIST SP 800-140F, Revision 1, CMVP Approved Non-Invasive Attack Mitigation Test Metrics: CMVP Validation Authority Updates to ISO/IEC 24759	https://csrc.nist.gov/publications/detail/sp/800-140c/rev-1/draft https://csrc.nist.gov/publications/detail/sp/800-140d/rev-1/draft https://csrc.nist.gov/publications/detail/sp/800-140f/rev-1/draft	米国連邦政府で利用可能な暗号アルゴリズム等の適合審査 Cryptographic Module Validation Programで認められる具体的な技術の更新。　これらが利用されConformantでないと少なくともアメリカ連邦政府並びに関連する政府調達業者、実体上はアメリカほぼ全土、並びにアメリカのIT企業製品での利用に強い影響が考えられる。
2021/8/25	Multiple attempts to exploit Realtek vulnerabilities discovered by our researchers	私たちの研究者によって発見されたRealtekの脆弱性を悪用する複数の試み												1		3日前の8月16日、Realtekチップセットの一部として配布されたソフトウェアSDKの複数の脆弱性がIoTインスペクターリサーチラボ[1]によって開示された。この脆弱性により、攻撃者は影響を受けるデバイスを完全に侵害し、制御することができる。ちょうど昨日、出版からわずか2日後、私たちのホームセキュリティソリューション、Secure Homeは、Miraiマルウェアの変種を広めるためにこれらの脆弱性を悪用する試みを検出した。公開された脆弱性の 1 つである CVE-2021-35395 は、SDK の一部である Web インターフェイスに影響を及ぼし、6 つの異なる脆弱性の集合である。8月18日現在、CVE-2021-35395を悪用する試みを特定した。	https://securingsam.com/realtek-vulnerabilities-weaponized/	

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			
2021/8/25	NISTIR 8259B IoT Non-Technical Supporting Capability Core Baseline	NISTIR 8259B IoT非技術的サポート機能コアベースライン		1				1								NISTIR 8259B：IoT非技術的サポート機能コアベースライン（最終版） 非技術的なサポート機能とは、IoT デバイスのサイバーセキュリティをサポートするために、メーカーやサードパーティの組織が実行するアクションである。この資料では、IoT (IoT) デバイスメーカーの非技術的サポート機能コアベースラインを定義している。この資料の目的は、組織が製造、統合、または取得する IoT デバイスに関連して必要な非技術的なサポート機能を特定する際に使用する出発点を提供することである。本書は、NISTIR 8259、IoTデバイスメーカー向けの基礎的なサイバーセキュリティ活動、およびNISTIR 8259AIoTデバイスサイバーセキュリティ機能コアベースラインと組み合わせて使用することを目的としている。	https://csrc.nist.gov/publications/detail/nistir/8259b/final	既に最終確定版が発行された、NISTIR 8259並びに NIST IR 8259A に続き、NISTIR 8259Bの最終確定版。
2021/8/25	FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity	ファクトシート：バイデン政権と民間部門 91人のリーダーが国のサイバーセキュリティを強化するための野心的なイニシアチブを発表	1	1								1				バイデン大統領は民間部門や教育リーダーと会い、サイバーセキュリティの脅威に対処するために必要な全国的な取り組みについて話し合った。 会議は、パートナーシップと個別に国のサイバーセキュリティを強化する機会について話し合うことが目的であり、参加者は、以下を含むコミットメントとイニシアチブを発表した。 ・バイデン政権は、米国国立標準技術研究所（NIST）が業界や他のパートナーと協力して、テクノロジーサプライチェーンのセキュリティと整合性を向上させるための新しいフレームワークを開発すると発表した。 このアプローチは、安全なテクノロジーを構築し、オープンソースソフトウェアを含むテクノロジーのセキュリティを評価する方法に関する公的および民間のエンティティへのガイドラインとして機能する。 Microsoft、Google、IBM、Travellers、およびCoalitionは、このNIST主導のイニシアチブへの参加を約束した。 ・バイデン政権はまた、産業用制御システムサイバーセキュリティイニシアチブを2番目の主要セクターである天然ガスパイプラインに正式に拡張することを発表した。 ・Apple、Google、IBM、Microsoft、Amazonを含む民間企業はこの政府方針に沿った今後のセキュリティ強化に向けた活動・投資プランを発表した。	https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/	・Whitehouseより、同日開催のバイデン大統領とアメリカ主要 IT企業並びにサイバー保険を提供する保険会社など、いわゆるアメリカのサイバーセキュリティに深く関係する企業トップとの会談の直後に発表。 ・民間企業各社がこれから実施することが列挙されているが、サプライチェーン、Zero Trust, 並びにユーザへの教育、啓発が重視の傾向がみられる。 ・米国著名 IT企業を含む大企業トップと大統領、ホワイトハウスの会談の成果ゆえ、明日すぐ何かが劇的に変わるとは思えないが、政府と民間のいわば約束のようなものであり、後から重要な意味を持つ可能性もある。
2021/8/31	DRAFT Baseline Security Criteria for Consumer IoT Devices	コンシューマーIoTデバイスのベースラインセキュリティ基準	1	1				1								NISTは、2021年5月12日に発行された「国家のサイバーセキュリティの向上に関する大統領令（14028）」に基づく任務の一環として、IoT（Internet-of-Things）機器のサイバーセキュリティ能力に関するラベリングプログラムの基準案をまとめたホワイトペーパーを発表した。これは、消費者向けのサイバーセキュリティのラベリングに関連する大統領令の下での多面的な取り組みの一つである。ドラフトに対するパブリックコメントを、2021年10月17日が締め切りで募集する。 大統領令に基づき、NISTは2022年2月6日までにIoTラベリングの取り組みに関する詳細を発表する。 NISTは、独自のプログラムを構築するのではなく、最低限の要求事項と望ましい属性という観点から、ラベリングプログラムの主要な要素を特定し、望ましい結果を規定することで、プロバイダーや顧客がそれぞれの機器や環境に最適なソリューションを選択できるようにする。1つのサイズがすべてに適合するわけではなく、ラベルプロバイダーによって複数のソリューションが提供される可能性もある。	https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/iot-device-criteria	・EO 14028 Sections 4(s)及び 4(t)にて示された業務に呼応。 ・既に最終版が確定された、NISTIR 8259, NISTIR 8259A: IoT Device Cybersecurity Capability Core Baseline並びに NISTIR 8259B: IoT Non-Technical Supporting Capability Core Baselineに基づいた Profilesを業界別、Use case別に作成することを勧奨。 ・文中の Table 1~3は NISTIR 8259, 8259A, 8259Bからの引用、再編であるが、これがConsumer IoT devicesに対する米国内での事実上の技術目標となりうる可能性が高いのではと考えられる。
2021/8/31	[Project Description] Mitigating Cybersecurity Risk in Telehealth Smart Home Integration: Cybersecurity for the Healthcare Sector	[プロジェクトの説明]テレヘルス・スマートホーム統合におけるサイバーセキュリティリスクの緩和:ヘルスケア分野のサイバーセキュリティ		1				1								NISTはMITREと共同で、NCCoEの一環で実施と類推されるテレヘルススマートホームインテグレーションにおけるサイバーセキュリティリスクの軽減に関する新しいプロジェクト記述案を発表した。このドラフトに関するフィードバックを参考にして、プロジェクトの改良に役立てるため、2021年10月4日を締め切りとするパブリックコメントを募集する。 ヘルスケアソリューションは、患者が消費者向けIoTデバイスを使用して健康情報を確認し、医療提供機関(HDO)が運営するシステムと対話することを可能にする可能性があり、ラボの結果の取得、ケアチームとの訪問をスケジュール、予約のリマインダーを設定、処方箋の補充を要求等のために IoT デバイスを使用できる。これらの機能により、IoTはテクノロジーの導入者に対して、家庭環境と家庭が相互接続するネットワークをどのように保護する必要があるか再考する必要がある。 このプロジェクトは、遠隔医療プログラムの一環として、スマートホームとヘルスケアシステムとの統合のための参照アーキテクチャを説明する実践ガイドとなるものである。	https://csrc.nist.gov/publications/detail/white-paper/2021/08/31/mitigating-cyber-risk-in-telehealth-smart-home-integration/draft	標題は Mitigating Cybersecurity Riskだが、文献にも示されるように、いわゆるサイバーセキュリティ、リスク管理に加え、Identity and Access Managementなど本人認証並びに認可(authorization)、プライバシーリスク、HIP AAに示されるように法規制への対応など、DHS指定重要インフラストラクチャの一つでもある医療分野での検討課題ゆえ、対象範囲は幅広い。

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			
2021/9/6	NTIA Releases Minimum Elements for a Software Bill of Materials	NTIAがソフトウェア部品表の最小要素をリリース												1		バイデン大統領は、国家のサイバーセキュリティの改善に関する行政命令(EO)の中で、サイバーインシデントの防止、検出、評価、改善を政権の最優先事項と考えた。商務省とNTIAは、より透明性と安全性の高いソフトウェアサプライチェーンを作り出す重要なツールであるソフトウェア部品表(SBOM)の最小限の要素を公開するようEOによって指示された。 SBOM は、ソフトウェアを製造、購入、運用する人々に、サプライチェーンに対する理解を深める情報を提供する。 SBOM は、すべてのソフトウェア セキュリティ問題を解決するわけではないが、新たに出現した既知の脆弱性やリスクを追跡する可能性を提供し、さらにセキュリティ ツール、プラクティス、保証を構築できる基盤となるデータ層を形成できる。 SBOMは決して単独のコンセプトではない。SBOMの価値は、現在進行中の他の取り組みを支援し、サイバーセキュリティとデータ管理のアプローチのためのさらなるインテリジェンスの取り組みを可能にすることである。長い目で見れば、SBOMは独自のスイートと考えるべきではなく、私たちが推進・育成すべき多面的なサイバーセキュリティのアジェンダの一部であるべきである。	https://www.ntia.gov/blog/2021/ntia-releases-minimum-elements-software-bill-materials https://www.nextgov.com/cybersecurity/2021/09/governments-software-transparency-journey-moves-blueprint-practice/185116/	2019年の SIPシンポジウムで招待講演に登壇されたAllan Friedman氏による説明
2021/9/7	Tripwire: IoT Devices Built to Meet Cybersecurity Needs	Tripwire: サイバーセキュリティのニーズを満たすように構築されたIoTデバイス													1	改ざん検知ソフトウェア開発企業のTripwireが発行しているThe State of Security情報：NIST IoT ProgramのNISTIR 8259を中心とした円卓会議の成果について以下の観点で解説している。 ・IoT デバイスの非技術サポート機能の概略 ・IoTデバイスのセキュリティ保護におけるメーカーの役割 IoT デバイスに対して非技術的な機能を顧客と消費者に提供することで、デバイスのサイバーセキュリティ機能を補完し、IoT デバイスの継続的なセキュリティを維持する能力が強化される。	https://www.tripwire.com/state-of-security/security-data-protection/iot/iot-devices-built-to-meet-cybersecurity-needs/	
2021/9/7	Moving the U.S. Government Towards Zero Trust Cybersecurity Principles	ゼロトラストサイバーセキュリティ原則に向けた米国政府の動き	1						1			1				連邦政府より、行政予算管理局（OMB）並びにDHS CISAによる以下の三文献draftsが公開され、政府機関がゼロトラストのサイバーセキュリティアーキテクチャを採用することを強く求めている。OMBからの包括的な連邦政策に関するフィードバックとCISAからの技術参照アーキテクチャと成熟モデルの草案であり、このガイダンスは、連邦政府全体のサイバーセキュリティ強化に関する5月の行政命令に続き、多要素認証、暗号化、ゼロトラストなどの特定のセキュリティ方法とツールを挙げている。 ・OMB: Federal Zero Trust Strategy（Public Comments期限：9月21日） ・CISA: Zero Trust Maturity Model（Public Comments期限：10月1日） ・CISA: Cloud Security Technical Reference Architecture（Public Comments期限：10月1日）	OMB: Federal Zero Trust Strategy ： https://zerotrust.cyber.gov/federal-zero-trust-strategy/ CISA: Zero Trust Maturity Model ： https://zerotrust.cyber.gov/zero-trust-maturity-model/ CISA: Cloud Security Technical Reference Architecture ： https://zerotrust.cyber.gov/cloud-security-technical-reference-architecture/	OMB, CISAともDHSで進行中のCDM（Continuous Diagnostics and Mitigation）プログラムの重視は共通しており、例えば、信頼データ交換、共有技術あるいは信頼チェーンの検証技術、維持技術をEDR（Endpoint Detection and Response）に転用できると、これらの目指している基準、技術目標に合致できる可能性がある。
2021/9/8	New study finds gaps in Commission's approach to IoT cybersecurity	IoTサイバーセキュリティに対する欧州委員会のアプローチにギャップがあることが新たな調査で判明			1									1		DIGITALEUROPEの調査によると、欧州委員会の製品サイバーセキュリティに対する現在の断片化されたアプローチは、セキュリティリスクと法的不確実性につながることが分かったとしている。 この調査は、18人の標準専門家へのインタビューに基づいており、接続されたデバイスのサイバーセキュリティに関する新しい水平方向に展開される法律と、サイバーセキュリティの調和した標準の開発を可能にする時間枠が必要であると結論付けている。 主な調査結果と推奨事項 ・ベースラインのサイバーセキュリティ要件の70%は、接続されているすべての 製品に共通していおり、これに取り組むには、新しい水平方向の法律が最も適 切である。 ・専門家の94%は、パスワードなどの物理的な製品要件に加えて、サイバーセキ ュリティ管理ルールなどの組織要件が不可欠であると考えている。物理的な製 品機能は、接続された製品に必要なすべてのサイバーセキュリティ要件の44% しか占めていない。 残りの要件（56%）は、より広範な管理、手順、または 組織の側面に焦点を当てる必要がある。対照的に、既存の製品法は主に製品要 件のみに焦点を合わせているため、サイバーセキュリティに対処するために既 存の製品法を使用するべきではない。または、必要に応じて、製品関連の要件 に厳密に焦点を当てる必要がある。 ・専門家は、接続されているすべての製品のベースラインサイバーセキュリティ 要件を定義することが、現在の低レベルのサイバーセキュリティを改善するた めに重要であるとしている。ただし、適切な調和標準の開発には少なくとも5 年かかり、政策立案者は十分な時間を確保し、法律と標準の間のリンクを最大 化する必要がある。"	https://www.digitaleurope.org/news/new-study-finds-gaps-in-commissions-approach-to-iot-cybersecurity/ https://www.digitaleurope.org/wp/wp-content/uploads/2021/09/DIGITALEUROPE_Setting-the-standard_How-to-secure-the-Internet-of-Things.pdf	

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			
2021/9/9	Identity Management and Discovery for IoT	IoTの ID 管理と検出		1							1					この文書では、IoT デバイスに適用可能な ID 管理のモデルについて説明している。具体的には、デバイスの識別子とプロパティを管理するための権限属性ツリーとして記述されたデータ構造を定義し、既存のオントロジーSAREFに対するこれらの権限属性ツリーの適用について説明している。また、権限属性ツリーの信頼を確立するための暗号化方式の要件を概説し、それらの要件を既存の暗号モデルにマッピングしている (例えば、機能的暗号化、対称システム、非対称システムなど)。 この文書では、ID 情報の公開、またはこの情報に基づく検出の受け入れまたは拒否に関して、ユーザーまたはデバイスのポリシーに関するポリシーを定義または推奨していない。 Annex B は他のデバイスによる権限属性ツリーの検出を可能にする「信頼義務」プロトコルで ID 管理モデルを適用する方法を示す。Annex C は、ID 管理モデルが既存のプロトコルに適用されるしくみ、および検出を制御する機能を示す。	https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=47653	
2021/9/16	EU chief announces cybersecurity law for connected devices	EU長官、コネクテッドデバイス向けのサイバーセキュリティ法を発表			1										1	欧州委員会のウルスラ・フォン・デア・ライエン委員長は水曜日（9月15日）に、接続されたデバイスに共通のサイバーセキュリティ基準を設定することを目的としたサイバーレジリエンス法を年次一般教書演説で発表した。接続されたデバイスの数が増えると、サイバー攻撃に対する脆弱性も高まると述べた。その中で「デジタルテクノロジーの急速な普及は、行政や病院などの重要なインフラストラクチャを混乱させるために、ならず者国家または非国家グループが電力を使用できる方法における大きなイコライザーだった」と述べている。 欧州議会のNIS2ファイルを主導するBartGroothuis氏は、NIS2は重要なサプライチェーンのセキュリティに取り組んでいますが、接続されたデバイスはEUのサイバーセキュリティ兵器の盲点であり、2つのEU法の補完性を強調している。 「モノのインターネットは、セキュリティが生産者の頭にないことが多いため、多くのセキュリティで保護されていない製品をもたらしている。そして、まだヨーロッパの規格はなく、IoT機器がハッカーが自宅のITシステムに侵入する手段となっている」とGroothuis氏はEURACTIVに話した。これはEuroconsumersと呼ばれるキャンペーングループが主導するプロジェクトであるHackable Homeで示されたものであり、倫理的なハッキングを通じて、ほとんどのスマートホームデバイスには基本的なサイバーセキュリティ標準すら欠けていることを示している。 Euroconsumersのポリシーおよび施行の責任者であるBruggeman氏は「EU全体で消費者の安全を確保するために、これを長い間提唱してきた。委員会がサイバーセキュリティのリーダーになりたいのであれば、消費者がIoTを信頼できるようにするサイバー脅威に対する一般的なEUのアプローチに取り組む必要がある。」と述べている。 サイバーセキュリティ要件を定義する必要性に関する同様の懸念は、DigitalEuropeによっても提起された。 最近の報告では、業界団体は既存の製品安全規制が接続されたデバイスにサイバーセキュリティ義務を設定できなかったと警告している。	https://www.euractiv.com/section/cybersecurity/news/eu-chief-announces-cybersecurity-law-for-connected-devices/	EUの新しい法律。まだ、一般公開されていない。
2021/9/16	NXP certified to support supply chain standard for automotive security	NXP社、自動車用セキュリティのサプライチェーン規格をサポートする認証を取得				1									1	NXPセミコンダクターは、最近コネクテッドカーシステムのハッキングに対する懸念が高まっている中、OEMとそのサプライチェーンがコンポーネント、サーバー、およびプロセスに対してより堅牢なセキュリティを設計できるようにすることを目的とした自動車サイバーセキュリティエンジニアリング標準であるISO / SAE21434に準拠していることがサードパーティラボによって認定されたと述べた。 NXPによると、このエンジニアリング標準は、2022年7月に標準のコンプライアンス義務が発効したときにヨーロッパ、日本、韓国での車両の発売に影響を与える国際的な自動車サイバーセキュリティ規制であるR155の実装をサポートする。R155は世界の車両の3分の1以上に影響を与え、 ISO/SAE 21434は、この生産量を支えるサプライチェーンの準備が整っていることを保証する。	https://www.fierceelectronics.com/electronics/nxp-certified-to-support-supply-chain-standard-for-automotive-security	対象：コネクテッドカーシステムのOEMとそのサプライチェーン
2021/9/20	SP 1800-32 (Draft), Securing IIoT- Distributed Energy Resources - CSRC	SP 1800-32 (Draft), 産業用IoTnoインターネットの保護：分散型エネルギー資源のサイバーセキュリティ	1					1								小規模な分散型エネルギー資源(DER)の利用は急速に拡大し、電力網の変革を遂げつつある。実際、ディストリビューション ユーティリティでは、何千もの DER やその他のグリッド エッジ デバイスとリモートで通信する必要があります。DER 通信を拒否、中断、改ざんする攻撃を行うと、ユーティリティが必要な制御操作を実行できなくなる 可能性があり、グリッドの復元力が低下する可能性があります。 このガイドでは、モノの接続された産業用インターネットデバイスの異常な動作を監視および検出し、信頼できる IIoT データ フローの包括的な監査証跡を構築するためのサンプル ソリューションを示します。 パブリックコメント期限：10月20日	https://csrc.nist.gov/publications/detail/sp/1800-32/draft	内容は、DER, それもsmall-scale distributed DERの利用を前提としたPower Grid use caseというシナリオであり、日本の送電網でDERを利用する場合は電力業界に影響しうると思われる。

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			
2021/9/20	Software and Supply Chain Assurance Forum	ソフトウェアとサプライチェーン保証フォーラム						1								ソフトウェアとサプライチェーン保証フォーラム： SSCAフォーラムバーチャルイベントが、9月22日(水)午前10時30分から東部時間午後1時まで開催されます。 最初の2つのセッションでは、それぞれイスラエル政府とイギリス政府の当局者からの講演が行われ、その後、通信分野に焦点を当てた2つのセッションが行われます。 Session1: Steps Taken by Israel to Address Cyber Attacks in the Supply Chain Session2: How Many Petals on the Supply Chain Security Flower? Session3: ATIS 5G Supply Chain Standard: Creating the Foundation for Assured 5G Networks Session4: TIA's 9000 Supply Chain Security Standard		
2021/9/21	ICT SCRM TASK FORCE: PRELIMINARY CONSIDERATIONS OF PATHS TO ENABLE IMPROVED MULTI-DIRECTIONAL SHARING OF SUPPLY CHAIN RISK INFORMATION	ICT SCRMタスクフォース：サプライチェーンのリスク情報の改善された多方向共有を可能にするためのパスの予備的考察	1	1					1							ICTサプライチェーンリスク管理(SCRM)タスクフォース情報共有ワーキンググループ(WG1)は、国のICTサプライチェーンへの脅威を軽減するために、連邦政府と民間産業間のサプライチェーンリスク情報(SCRI)の共有を改善するための考慮事項を提供することを目的として作られた。このレポート「サプライチェーンリスク情報(SCRI)の多方向共有を改善するためのパスの予備的な考慮事項」は、責任制限に対処する上で、民間企業または政府の利用に関する法的および政策上の考慮事項に関する主題専門家の調査を提供する。 この報告書では、WG1は、SCRIを共有するための重大な責任を課す可能性のある7つの潜在的な行動原因(すなわち、名誉毀損、ビジネスまたは商業格差、詐欺的な虚偽表示、契約違反)を考慮した。 このレポートには、SCRI共有フレームワークに参加し、最終的には民間および公共部門間で共有されるSCRIの量と品質を改善しようとする民間企業の保護を最大化する方法として、検討のため提案された更新された定義と追加の責任保護が含まれている。	https://www.cisa.gov/publication/ict-scrm-task-force-improve-multi-directional-scri	Supply Chain Risk Informationを民間企業が他の民間企業や連邦政府機関を含む他者と共有する場合に直面する契約上、法務上の課題を 7つの潜在的な課題として提示。米国の事情、文脈によるため、必ずしも日本含む他国で全てを参考にできるとは思えないが、日本と米国含む外国の事業体との国際契約などで役に立ちうる、あるいは応用できる知見が存在する場合が考えられる。
2021/9/21	ICT SCRM TASK FORCE: OPERATIONALIZING THE VENDOR SCRM TEMPLATE FOR SMALL AND MEDIUM-SIZED BUSINESSES	ICT SCRMタスクフォース：中小企業向けのベンダーSCRMテンプレートの運用		1					1							このガイド「SMB の仕入先 SCRM テンプレートの運用」では、今年初めにリリースされたエンタープライズ仕入先 SCRM テンプレートを SMB に対してよりアクセスしやすく、使用しやすくすることに重点を置いて説明している。SMBバージョンでは、WGは、買収者、インテグレーター、サプライヤーの観点からICTサプライチェーンリスク態勢を評価し、SMBの実装と業界標準の適用とベスト プラクティスに関する一連の質問を提供し、サプライチェーンリスク計画を導くのに役立つ。 また、この製品を利用するための代替ツールとしてスプレッドシートバージョンをダウンロードし、各質問に対する「はい、いいえ」、または「部分的な回答」に対応するためのオプションを提供することを目的としています。	https://www.cisa.gov/publication/ict-scrm-task-force-operationalizing-vendor-scrm-template-smbs	中小規模事業者を対象に、Acquirer, Integrator, 並びに Supplierの三つの役割を想定し、三つのユースケースにより、彼ら中小規模事業者のVendor Supply Chain Riskへの可能な対処を分析、提示。
2021/9/22	ICSJWG 2021 Fall Meeting Report	ICSJWG 2021 Fall Meeting レポート	1	1					1						1	ICSJWG 2021 Fall Meeting 参加報告 報告対象講演： (1)挨拶： Jen Easterly, CISA Director (2)基調講演： Alexis Wales, Acting Associate Director, Threat Hunting, CISA, DHS (3)TTP's to Totally Owned: Identify your Weaknesses before they become an issue： 講師: Kevin Tambascio and David Charbel, Cleveland Clinic (4)How much Security is enough?： 講師: Mike Radigan, Business of Security (5)A (Not So) boring talk about upcoming changes through regulation (EO 14028,RED, NIS2, IT SIG 2.0)： 講師: Jens Wiesner, BSI (Federal Office for Information Security of Germany) (6)CSET Ransomware and you： 講師: Barry Hansen, Idaho National Laboratory (7)Living off the Land in an ICS/OT Penetration Test： 講師: Aaron Boyd and Francesca Brogden, Dragos (8)Creating Resiliency to Cyber Incidents through Exercises： 講師: Jason Wells, Gary Benedict, CISA	https://gateway.on24.com/wcc/eh/3049745/icsjwg-2021-fall-virtual-meeting https://www.isa.org/news-press-releases/2021/july/isagca-and-ics4ics-announce-cybersecurity-first-re https://www.youtube.com/watch?v=DCLvdwbHOVo https://us-cert.cisa.gov/ncas/current-activity/2021/06/30/cisas-cset-tool-sets-sights-ransomware-threat	足立氏参加報告レポート参照

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			
2021/9/22	ICSJWG 2021 Fall Meeting Report [How Much Cyber Security is Enough?]	ICSJWG 2021 Fall Meeting 報告 ： [サイバーセキュリティはどれくらいで十分か？]	1	1					1						1	ICSJWG 2021 Fall Meeting出席の足立氏報告 (1)：How Much Cyber Security is Enough? ・電力提供を停止させる要因として掘削、オペレーションミス、材料、設備等の故障、自然災害などが上位を占め、「サイバー」はまだ停止の主要因とはなっていない。従って現状から予想可能なパラメータとモデルを利用し、Riskを推算している。講師想定のシミュレーションでは、- Power Station A のサイバーリスクの分析、- Cyber incidentによりLoss of availabilityが発生し、forced outageが発生というシナリオ、- AssetsとしてControl Systemを想定、とした前提で試算したRisk評価によると、サイバーインシデント類は、Primary Revenue Loss（直接的な収入への損失）の最悪の場合の値が他の要因（Leak, heaterbypass, pump故障など）と比べ段違いに大きいことが示される。 ・講師より、サイバーの場合直接的に会社が痛むだけですむPrimary Lossに加え、Secondary Lossが大きくなる傾向がある旨指摘される。これは、数ヶ月前のColonial Pipelineの事件で明らかになった。このsecondary lossにはreputational loss（会社の評判への悪影響）なども考慮される必要がある。 ・講師が実施されたような分析は、業態ごと、組織ごと、ネットワーク構成、シミュレーションに利用するモデル、設定されるパラメータ(probablityとimpactの設定値）などに大きく依存するが、それでも、できるだけCyber並びにoperational riskを一般的なrisk metricにより可能な限り算出し、〇最適の(optimal) リスク管理上の意思決定を可能たらしめること、〇その際にOperational Riskの比較を行い、優先順位をつけること、を勧められ、これにより、安全で安定し、利益の上がるoperationの実現に寄与すべきとしている。 ・OTとITの間の意思疎通の深化に加え、実際に動作しているプラント側とOTの意思決定者間の信頼関係が重要である。		
2021/9/22	ICSJWG 2021 Fall Meeting Report [A (Not So) Boring Talk About Upcoming Changes Through Regulation]	ICSJWG 2021 Fall Meeting 報告 ： [規制による今後の変更についての退屈な話]	1	1					1						1	ICSJWG 2021 Fall Meeting出席の足立氏報告 (2)：A (Not So) Boring Talk About Upcoming Changes Through Regulation BSI（ドイツ内務省傘下で標準化とインシデント対応を行う機関）の技術者である講師が、最近の法制度についての感想や印象を説明。法制度として、EO 14028 、RED or Radio Equipment Directive 、CSA Cybersecurity Act EU 2019/881 、NIS 2、IT SIG 2.0 等について説明。BSIで現役の技術者の方が語る法制度感という、あまりない機会で興味深く聴講できたが、EUの法制度について懐疑的、scanとhoneypot運用が可能になったことについて語られたことが印象的な内容であった。		
2021/9/22	Software and Supply Chain Assurance Forum	ソフトウェアおよびサプライチェーン保証フォーラム	1	1					1							Software and Supply Chain Assurance Forum 参加報告。 ・主催：　NIST Cyber Supply Chain Risk Management (aka C-SCRM) - ATIS 5G Supply Chain Standard: Creating the Foundation for Assured 5G Networks ATISがさる 9月 16日に報道発表4した標題文書5に基づき、現状並びに今後についてATISの講師による発表。 ・2019年 12月、ATISで 5G Supply Chain Working Groupが発足、産業界、政府、学界から五十以上の参加組織、T-Mobile USA, Verizon, 並びに NTIAが WG leadershipを担う。 ・従来のいわゆる「サイバーセキュリティ」とは外部からの攻撃に焦点が当てられてきたが、Supply Chainはより internalで、system そのものに影響と講師の見解。 - TIA's 9000 Supply Chain Security Standard TIAが作成中の Supply Chain Security 9001 (SCS 9001) Standardについて、TIAの講師による発表。 ・TIAでの標準策定の理由は、ICTに特有、必要な要件を定め、これを監査可能、計測可能とすること。 実際に ISO 27000シリーズ、Cloud Security Alliance発行の文献類、 CMMC, あるいは ENISAの関連文献を調査し、それぞれの定める要件を比較し、どれにも規定されていない要件を抽出とのこと。 ・2021年中に公開予定。 それ以前にコメント受付などを予定されているようだが、一般からのコメント受付か、TIA会員限定かなどは不明。標準はまだ完成していないが、ANABが当該標準の Accreditation Bodyとなることは内定している模様、すなわちアメリカでの展開では事実上の認証要件となりうる可能性が高い。	https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/ssca	今回の会合に関していえば"Software" Supply Chainに限定されず、ICTあるいは通信事業分野限定とはいえ、ある分野、業界を想定した広範な Supply Chain全体の要件化、標準策定の様子をかなり具体的に聞くことができる機会となった。 ATIS, TIAの事例とも、最終的に SIP_CPS様の「技術目標」への参考資料になりうるし、米国で達成しなければならない要件として今後の動向に SIP_CPSにおいても今後の観測などが必要かも知れない動向である。

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			
2021/9/23	SP 1800-10 (Draft) Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector	SP 1800-10 (ドラフト) 産業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:製造業におけるサイバーセキュリティ						1								NIST SP 1800-10 の草案は、製造メーカーが産業制御システム(ICS)をデータ整合性攻撃から保護するための実用的なサンプルソリューションである。. このガイドで紹介するアーキテクチャとソリューションは、標準ベースの市販製品を基に構築されており、いくつかの可能なソリューションを表す。このソリューションは、動作異常検出(BAD)、アプリケーション許可リスト、ファイル整合性チェック、変更制御管理、ユーザー認証と承認などの標準的なサイバーセキュリティ機能を実装している。このソリューションは、組立ライン生産を表す個別の製造作業セルと、化学製造産業を代表する連続プロセス制御システムの2つの異なるラボ設定でテストされている。 パブリックコメント期限：11月7日	https://csrc.nist.gov/publications/detail/sp/1800-10/draft	SIP_CPSの研究開発課題では工場が信頼の起点とされており、工場での製造に直接関わるICSのintegrityはいわば基点の基点と考えられること、A. 信頼の創出、証明において、製造業から確認等を行う機関に提出されるように思われる真贋判定とプロシージャ保証の基礎データは、製造業ICSのintegrityが前提とされると考えて関連情報としている。
2021/9/24	Quad Principles on Technology Design, Development, Governance, and Use	テクノロジーの設計、開発、ガバナンス、および使用に関するQUADの原則	1									1		1		第二回QUAD Leader’s Summit声明 [Quad Principles on Technology Design, Development, Governance, and Use] ・技術のサプライヤー、ベンダー、ディストリビューターには、安全なシステムを作成および維持し、信頼性が高く、透明性があり、その実践に責任があることを期待している。技術開発者はまた、安全性と設計によるセキュリティのアプローチを組み込み、堅牢な安全性とセキュリティの実践が技術開発プロセスの一部となるようにする必要がある。技術の不法な譲渡または盗難は、グローバルな技術開発の基盤そのものを損なう一般的な課題であり、対処する必要がある。 ・ハードウェア、ソフトウェア、およびサービスのための、回復力があり、多様で、安全なテクノロジーサプライチェーンは、私たちの共通の国益にとって不可欠である。私たちの価値観を共有する同盟国やパートナーとのサプライチェーンに関する緊密な協力は、私たちの安全と繁栄を強化し、国際的な災害や緊急事態に対応する能力を強化するものである。 [Fact Sheet: Quad Leaders’ Summit] Critical and Emerging Technologies: ・技術標準、5Gの多様化と展開、地平線スキャン、テクノロジーサプライチェーンの4つの取り組みを中心に作業を整理した。 Cybersecurity: ・クワッドシニアサイバーグループの立ち上げ：リーダーレベルの専門家が定期的に会合し、共有サイバー標準の採用と実装を含む分野で継続的な改善を推進するための政府と業界間の作業を進め、安全なソフトウェアの開発、労働力と才能の構築、安全で信頼できるデジタルインフラストラクチャのスケーラビリティとサイバーセキュリティを促進する。	https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/quad-principles-on-technology-design-development-governance-and-use/ https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/fact-sheet-quad-leaders-summit/ 関連報道記事： https://www.theregister.com/2021/09/27/quad_communqiue_technology_announcements/ 外務省発表： https://www.mofa.go.jp/fp/nsp/page4e_001178.html	
2021/9/30	7 new TMF awards	7つの新しいTMF賞	1											1		バイデン政権は、今年初めに可決されたアメリカ救済計画の一環として10億ドルの大規模な注入を受けた技術近代化基金を通じて資金を授与される7つの連邦技術プロジェクトのうち6つについて公に発表した。 TMFは、2017年に機関がITアップグレードのための融資を申請できる中央基金として設立され、以前は11の賞を受賞し、議会が1億7500万ドルを寄付した。しかし、第2のパンデミック刺激策の一環として、ファンドは10億ドルのブーストと、重要なサイバーセキュリティとパンデミック関連プロジェクトの返済要件を緩和する義務を負った。 今回の発表では、10億ドルの約3分の1が、3つのゼロトラストサイバーセキュリティプロジェクト、一般サービス管理局が運営する2つの政府間プログラム、そして南西部国境の移民問題に対処するための技術の展開に充てられる。 3つのゼロトラストサイバーセキュリティプロジェクトは、ゼロトラスト・アーキテクチャの実装に関するものであり、以下の部門でゼロトラストプロジェクトが推進される。 ・ゼロトラストネットワーキング:人事管理局:990万ドル ・ゼロトラストアーキテクチャー:教育省:2,000万ドル ・ゼロトラストの推進:一般サービス管理局:2,980万ドル	https://www.nextgov.com/cybersecurity/2021/09/white-house-announces-7-tmf-awards-big-focus-zero-trust/185762/ https://fcw.com/articles/2021/09/30/tmf-awards-login-classified-zero-trust.aspx https://washingtontechnology.com/articles/2021/09/28/tmf-awards-hsgac-hearing.aspx	

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			
2021/10/14	Improving the Nation’s Cybersecurity: Progress and Next Steps in Carrying Out Executive Order 14028	国家のサイバーセキュリティの改善：大統領命令の実行における進捗状況と次のステップ 14028	1					1								Executive Order 14028の中で、4条(Enhancing Software Supply Chain Security) を中心にNISTに割り当てられた項目類につき、NISTのoutputあるいは進捗状況が説明された。 (1)Critical software definition, security measures, and software verification ・Critical functionsを担うsoftwareはcommercial,opensourceなどを問わずcritical softwareとして扱われ,OS, Hypervisors, container environmentsについては、昨今の当該分野の脆弱性の検知並びに対策の頻出という事象から、重要。 (2) (4c)Enhance the software supply chain ・EO 4条(c)項で定められる件について、NIST SP 800-161の更改、更新により対処中。 ・NISTIR 8259 and 8259A, CISA Internet of things Acquisition Guidanceには反映途上。 (3)(4e) Secure Software Development Framework update ・NIST Security Software Development Frameworkについて、現在19のpracticeで構成され、現状既にEO 4(e)が求める内容のほぼ全てを網羅している。現在、DRAFT NIST SP 800-218[3]として公開しコメント募集中。 (4)Labeling for Consumers: Internet of Things (IoT) Devices and Software ・labelingの件について、今までの活動が簡潔に説明される。 NISTがlabeling programを作るのでは「なく」、鍵となる諸要素を特定identifyするという点が強調された。 (5)New technology supply chain security initiative ・さる8月25日にバイデン大統領と米国IT大手を中心とした大企業とのSummitで、NISTが大手企業と実施するように決められたTechnology Supply Chain security Initiativeについて説明。拙速にやるのではなく、実現可能な方法をNISTで検討中。 ・バイデンサミットで示された官民連携の実現にあたり、Supply Chain Securityの実現に必要な情報の交換、開示には、知的財産、あるいはセキュリティに関わる情報の開示には民間で躊躇、困難、あるいは契約等で不可能な場合が見られるとの見解が示された。ホワイトハウスが発した"Technology Supply Chain" Securityという語彙については、NIST側は「softwareの製造過程におけるintegrityの担保を中心としたsecurity」という理解で進めている模様。	https://www.nist.gov/news-events/events/2021/10/improving-nations-cybersecurity-progress-and-next-steps-carrying-out https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition https://www.nist.gov/news-events/news/2021/05/nist-releases-draft-nist-sp-800-161-revision-1-comment-cyber-supply-chain https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/	
2021/10/20	ICSJWG Webinar: THE END IS NEAR … Now What? Best Practices for End of Service and End of Life	ICSJWGウェビナー：サービス終了およびサポート終了のベストプラクティス	1	1					1							DHS ICSJWG Webinar 2021年10月20日開催 内容は耐用年数の長い重要インフラと産業用制御システム（Critical ICS）におけるサポート終了（EOC)時のセキュリティリスクの課題にどのように対処すべきかというものである。扱われた論点を以下に列記する。 - Physical Access Protection　- Network Separation　- Data Diodes　- Logical Separation (by Firewall) - Application Level Gateway　- Jump Server/ Jumphost　- Hardening Systems　- Logging and monitoring - Deployment of Virtual Machines　- Backup and recovery　- Spare parts ・ Slide 16で示されるConsiderationsにおいて、ICSの構成機器には長期に利用される機体が多く含まれることから、新しい製品、ソフトウエア、技術の導入に際しbackward compatibilityの担保が非常に重要な課題と認識されていることが発表者たちの説明から紙で書かれている以上に重要と認識される。 ・従来の物理防御はドローンなどの新しい技術には役に立たない。これはいわゆるITでも最近最新の攻撃動向に対応できない情報システムに対し、必ずしも高度に技術がなくとも攻撃が成功する昨今の事情に対する教訓とも考えられる。 ・Deployment of Virtual Machinesにおいて、ICS一筋20年(?)の発表者の方は、ICSでVMは使わないと明言。 ・Spare Parts:　ICSを構成する機器類で長期に亘り利用されるものには、将来ベンダーから修理部品が入手できない場合に備え、予備のパーツをきちんと調達保管しておくことがICS業界ではかなり常態化している模様。 ・バックアップについて、ICS関係の方より、Offline backupの重要性と、バックアップデータの内容の点検（malwareなどが入っていないかなど）の重要性が指摘されたことは重要。 ・ICS業界のこのような文化、技術、ノウハウなどの若手への継承が課題とも指摘された。	https://us-cert.gov/sites/default/files/ICSJWG-Archive/Web_Oct_21/INV_ICSJWG_Oct21_Webinar16_Flyer_FIN_20210923_508C.pdf	米国・足立氏によるウェビナー参加レポート

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			
2021/10/20	Digitally-Signed Rootkits are Back – A Look at FiveSys and Companions	デジタル署名されたルートキットが復活–FiveSysとコンパニオン		1	1										1	過去数か月間、Bitdefenderの研究者は、WHQL署名プロセスを通じてMicrosoftによって発行された有効なデジタル署名を持つ悪意のあるドライバーの急増を見てきた。 この調査では、ドライバー認定プロセスを通過したデジタル署名されたルートキットであるFiveSysについて説明している。 主な調査結果 ・Bitdefender の研究者は、マイクロソフトが発行したデジタル署名を持つルートキットを特定した。 ・ルートキットは、攻撃者が関心を持つインターネット アドレスにトラフィックをプロキシするために使用される。 ・ルートキットは、資格情報の盗難とゲーム内購入ハイジャックの主な目標を持つオンラインゲームをターゲットと仮定する。 ・ルートキットは1年以上前からコンピュータユーザーをターゲットにしている。 ・ルートキットの普及は中国に限られており、市場に大きな関心を持つ脅威アクターによって運営されていると推測される。	https://www.bitdefender.com/blog/labs/digitally-signed-rootkitsare-back-a-look-atfivesys-and-companions/ https://www.bitdefender.com/files/News/CaseStudies/study/405/Bitdefender-DT-Whitepaper-Fivesys-creat5699-en-EN.pdf	BitdefenderはMicrosoftに連絡し、MSFTは当該certificateをrevokeしたとされ、現状対処済みと思われる。同様の手法はStuxnetで利用され、ICS, Critical infrastructure向けの攻撃にすでに利用実績があることであり、SIP CPSの信頼の創出、検証に影響しうると思われる。
2021/10/21	欧州 Horizon2020 pilot project SPARTAがSAFAIRを発表	欧州 Horizon2020 pilot project SPARTAがSAFAIRを発表										1				人工知能（AI）の拡大は、人間の生活のほぼすべての領域における進歩と改善への扉を開いた。この方法は無敵ではなく、2つの主要な問題を含む多くの問題によって妨げられる可能性がある。一つは、新しいサイバー攻撃がいくつも出現し続けているかという事実に関連しており、適切な対策を講じる必要がある。 AIの普及を成功させるためのもう一つの問題は、信頼、公平性、その他の社会的課題などに関連している。その中には、説明可能性の問題もある。つまり、アルゴリズムの結果を透過的に説明して、人間のオペレーターが決定の出所を理解できるようにすることである。 SAFAIR（Secure And FAIR AI systems for citizens）プログラムでは、これらの問題を解決することが求められている。 SAFAIRプログラムの第一の目標は、信頼できるAIソリューションを提供することである。AIベースのソリューションを、脅威となる改ざんに対してより強固なものにすると同時に、AIによる意思決定が公正で説明可能なものであることを保証することを目標としている。その結果、信頼できるレジリエントなシステムを作ることができる。 作業は5つのステップに分けられた。 最初に、AIベースのアーキテクチャのサポートを提供することを目的とした一連の体系的な脅威分析ツールが開発された。 その上に、SAFAIR脅威知識ベースが構築され、公開された。 これにより、ユーザーと開発者の両方が脅威の状況をよりよく理解し、脆弱性、およびデータの整合性に対するさまざまなサイバー攻撃やその他の脅威の考えられる結果を認識する機会が得られる。 説明可能性と公平性を強化する多くのメカニズムが設計された。その中には、Hybrid Oracle-Explainer xAIシステムがある。これは、高品質の予測を提供し、代理タイプの説明を使用して、それらをわかりやすく表示できる最先端のソリューションである。フェイクニュースの検出に使用されるBERTベースのAIモデルに説明可能性を適用する方法が開発され、Shapley Valuesを使用した機械学習モデルが調査された。 AIベースのシステムによる決定の偏りを減らし、システムを可能な限り公平で差別のないものにするたのメカニズムにもかなりの努力が払われた。	https://www.sparta.eu/news/2021-10-21-secure-and-fair-ai-systems-for-citizens-program-results.html	進行中のプログラムの中間報告的位置づけの発表である。

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			
2021/10/24	Microsoft：New activity from Russian actor Nobelium	ロシアNobeliumの最新の活動状況	1	1												今日、我々はロシアの国家活動であるNobeliumから観察した最新の活動を共有している。これは、2020年にSolarWindsの顧客を標的としたサイバー攻撃の背後にある同じアクターであり、米国政府などがSVRとして知られるロシアの外国情報機関の一部であると特定した。 Nobeliumは、グローバルITサプライチェーンに不可欠な組織をターゲットにすることで、過去の攻撃で使用したアプローチを再現しようと試みてきた。今回は、サプライチェーンの別の部分、つまりカスタマイズ、展開する再販業者やその他のテクノロジーサービスプロバイダーを攻撃しており、 顧客に代わってクラウドサービスやその他のテクノロジーを管理する。Nobeliumは最終的には再販業者が顧客のITシステムに直接アクセスし、組織の信頼できるテクノロジーパートナーになりすまして、下流の顧客にアクセスしやすくなる。 Microsoftは2021年5月にこの最新のキャンペーンの監視を開始し、影響を受けたパートナーと顧客に通知すると同時に、再販業者コミュニティ向けの新しい技術支援とガイダンスを開発した。5月以降、対象となった140を超える再販業者 とNobeliumによりターゲットとされたテクノロジーサービスプロバイダーに通知した。引き続き調査を続けているが、現在までに、これらの再販業者とサービスプロバイダーのうち14社が侵害されたと考えている。	https://blogs.microsoft.com/on-the-issues/2021/10/24/new-activity-from-russian-actor-nobelium/ SolarWindsの侵害に関する関連情報（Whitehouse）： https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/ SolarWindsの侵害に関する関連情報（NCSC）： https://www.ncsc.gov.uk/news/joint-advisory-further-ttps-associated-with-svr-cyber-actors	SolarWindsの侵害に関しては、上記の関連情報に示すように、4月にWhitehouseより正式に米国の見解としてSolarwindsへの攻撃をRussia SVRとし、更に5月に、米国(NSA,CISA)と英国(NCSC, GCHQの傘下組織）は共同声明で、同内容に詳細を加えた発表をしている。
2021/10/25	State Department to Form New Cyber Office to Face Proliferating Global Challenges	国務省:増大するグローバルな課題に直面するために新しいサイバーオフィスを設立	1	1										1		国務省は、ランサムウェアや世界的なデジタルの自由の衰退などの国際的なサイバーセキュリティの課題に立ち向かうための組織変更を計画している、と米国当局は述べた。 再編には、上院で確認された大使が率いるサイバースペースとデジタル政策の新しい局の創設と、重要で新興技術のための新しい別個の特使が含まれると当局者は述べた。 新しいサイバー局は、抑止、政策立案、同盟国や敵対者との交渉など、国際的なサイバーセキュリティ問題に焦点を当てた部門で構成される。 2番目の部門は、信頼できる通信システムを海外に宣伝するなど、デジタルポリシーに専念する。 3番目の部門は、オンラインでの人権の保護や市民社会との協力など、デジタルの自由に焦点を当てる。	https://www.wsj.com/articles/state-department-to-form-new-cyber-office-to-face-proliferating-global-challenges-11635176700 https://www.washingtonpost.com/national-security/us-officials-caution-companies-about-risks-of-working-with-chinese-entities-in-ai-and-biotech/2021/10/21/d8e8e300-32c1-11ec-9241-aad8e48f01ff_story.html	10/27付け日経朝刊記事： 米国務省のプライス報道官は25日の記者会見で、サイバー対策やデジタル政策を横断的に扱う組織を省内に新設すると発表した。統括する担当大使のポストも置く。安全保障や経済の脅威となっている中国やロシアによるサイバー攻撃に対処する体制を整える。プライス氏は新設する「サイバー空間・デジタル政策局」について「国際的なサイバー空間の安全保障、国際的なデジタル政策、デジタルの自由という3分野を重点的に扱う」と述べた。新組織はサイバー問題を巡る抑止力向上などを手がける。
2021/10/26	FCC Revokes China Telecom America's Telecom Services Authority	FCCがChinaTelecom AmericaのTelecomServicesAuthorityを取り消す				1							1			連邦通信委員会は、China Telecom（Americas）Corporationが米国内で国内の州間および国際通信サービスを提供する能力を終了する命令を採択した。 失効および終了に関する命令は、China Telecom Americasに対し、命令のリリース後60日以内に、第214条の権限に従って提供する国内または国際的なサービスを中止するように指示している。 国家安全保障を促進することは、公共の利益を促進する委員会の責任の不可欠な部分であり、今日の行動は、潜在的なセキュリティの脅威から国の通信インフラストラクチャを保護する使命を実行する。 FCC　Carr委員長は次の声明を出した。 「本日、これを終了できることをうれしく思う。我々はチャイナテレコムアメリカの国内および国際的なセクション214の権限を取り消すことに投票している。今日の我々の決定は、国家安全保障のレビューに責任を持つ行政機関により提出された見解によって通知される。彼らは、チャイナテレコムアメリカズの米国の電気通信インフラストラクチャへの継続的なアクセスに関連する実質的で容認できない国家安全保障と法執行のリスクがあるとアドバイスした。 また、China Telecom Americasの事業は、中国の国営の関係者がスパイ活動に従事し、企業秘密やその他の機密ビジネス情報を盗む機会を提供すると述べている。」	https://www.fcc.gov/document/fcc-revokes-china-telecom-americas-telecom-services-authority FCC　Carr委員長の声明: https://docs.fcc.gov/public/attachments/DOC-376902A3.pdf	FCC委員長の声明に、China Telecomの通信免許剥奪と直接関係なさそうな、深圳所在のDJI製DroneのFCC Covered Listへの追加が述べられている。　追加理由はHuawei同様国家安全保障への懸念であり、このDroneと同様の施策は、他のIoT機器、あるいはFTC以外の規制機関 (DoC Entity List, DHS CBP等）でも実施可能な点で注意する必要があると思われる。

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			
2021/10/26	Kaspersky Report：North Korea's Lazarus Group Turns to Supply Chain Attacks	Kasperskyレポート：北朝鮮のラザルスグループがサプライチェーン攻撃に転向													1	北朝鮮の悪名高いラザログループの最近の活動は、信頼できるITサプライチェーンベンダーを企業ネットワークへのエントリポイントとして使用することに対する脅威アクターの関心の高まりを示す新たな証拠を提供する。 カスペルスキーのセキュリティ研究者は最近、Lazarusグループが IT企業のネットワークに侵入した2つの別々のキャンペーンを発見した。 事件の1つで、Lazarus Groupは韓国のセキュリティソフトウェアベンダーのネットワークにアクセスし、同社のソフトウェアを悪用して、韓国のシンクタンクのネットワークにブラインドカンとコッパーヘッジと呼ばれる2つのリモートアクセストロイの木馬(RAP)を展開した。昨年、米国サイバーセキュリティ・インフラセキュリティ庁(CISA)は、8月と5月に別々のアラートを発令し、Lazarusグループが2つのRAを使用して侵害されたネットワーク上でのプレゼンスを維持することを警告した。 カスペルスキーの研究者が最近観察した2回目のラザロサプライチェーン攻撃には、ラトビアに拠点を置くIT資産監視製品ベンダーが関与した。この攻撃では、ラザログループは再び技術プロバイダーのネットワークにCopperhedgeバックドアを配備した。 「これは、複数の[コマンドとコントロール]サーバーの2つの層を使用して慎重な多段階プロセスで行われた」と、カスペルスキーのシニアセキュリティ研究者、アリエル・ユングハイトは言っている。	https://securelist.com/apt-trends-report-q3-2021/104708/ Lazarusグループの攻撃に関する報道1：https://www.darkreading.com/threat-intelligence/north-korea-s-lazarus-group-turns-to-supply-chain-attacks Lazarusグループの攻撃に関する報道2：https://threatpost.com/lazarus-apt-it-supply-chain/175772/	Solarwinds/Kaseya同様、純正ソフトウエア開発配送システムへの不正ソフトウエアの注入、配布攻撃であり、留意すべきと思われる。
2021/10/27	Warehouse belonging to Chinese payment terminal manufacturer raided by FBI	FBIに襲撃された中国の決済端末メーカーの倉庫												1		米国のFRBは火曜日、フロリダ州ジャクソンビルにある中国の決済端末メーカーPAXテクノロジーに属する倉庫を創作しているところを目撃された。マシンにはプリインストールされたマルウェアが含まれているとの憶測が高まっていた。 PAXテクノロジーは中国の深圳に本社を置く世界最大の電子決済プロバイダーの1つであり、120カ国以上で約6,000万ポイント・オブ・セール(PoS)決済端末を運営している。	https://www.theregister.com/2021/10/27/pax_technology_warehouse_raid/	Pre installed malwareの嫌疑については、SIP CPSにおける解決したい課題に関連するものと思われる。また、PAX TechnologyのPoS端末は、報道によると120カ国6千万台出荷実績とされ、PAX全製品に同様の嫌疑の可能性がある場合は日本を含む世界的な影響が懸念される。
2021/10/27	2021 CWE Most Important Hardware Weaknesses	2021CWEの最も重要なハードウェアの弱点		1									1			2021 CWE Most Important Hardware WeaknessesがMITREより以下の通り発行された。MITREは連邦政府、州政府、地方自治体、産学官の間で公共の利益のために活動する非営利団体であり、CWEは米国国土安全保障省のCISA（Cybersecurity and Infrastructure Security Agency）の支援を受けてMITREにより運営されているWebサイトである。 「2021年CWE™最も重要なハードウェアの弱点」は、ハードウェア設計、製造、研究、セキュリティ分野、学界、政府内の組織を代表する個人のためのコミュニティフォーラムであるハードウェアCWE特別利益グループ(SIG)内でのコラボレーションの最初のものであり、その結果である。 2021 ハードウェアリストの目標は、CWE を通じて一般的なハードウェアの弱点を認識し、製品開発ライフサイクルの初期段階で重要なミスを排除する方法について設計者やプログラマーを教育することによって、ソースでのハードウェアセキュリティの問題を防ぐことである。セキュリティ アナリストとテスト エンジニアは、セキュリティテストと評価の計画を準備する場合に、このリストを使用できる。ハードウェアの消費者は、リストを使用して、サプライヤーからより安全なハードウェア製品を求めることができる。最後に、マネージャと CIO は、ハードウェアを保護する努力の進捗状況の測定棒としてリストを使用し、根本原因を排除することで、広範囲の脆弱性を軽減するセキュリティ ツールや自動化プロセスを開発するリソースをどこに向けるかを確認できる。	https://cwe.mitre.org/scoring/lists/2021_CWE_MIHW.html	SIP CPSでどのような実装まで作成されるかわからないが、SIP-CPS研究開発計画におけるIoTシステム・サービス提供サプライチェーンやシステムの運用に関連する内容が含まれると思われる。

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			
2021/10/28	SP 800-161 Rev. 1 (Draft) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (2nd Draft)	SP 800-161 Rev.1（ドラフト）システムと組織のためのサイバーセキュリティサプライチェーンのリスク管理慣行（第2ドラフト）	1	1				1								NISTは、第2回公開版 SP 800-161 rev.1,Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations（システムおよび組織向けサイバーセキュリティサプライチェーンリスク管理プラクティス）を公開した。 12月3日を期限としてパブリックコメントを募集する。 今回の改訂にあたり、最初の公開草案は2021年4月に公表され、2021年5月12日に発行された国家のサイバーセキュリティの改善に関する大統領の執行命令(EO)14028のリリースに先立って公表された。このEOは、NISTを含む複数の機関に対し、さまざまな取り組みを通じてサイバーセキュリティを強化するとともに、ソフトウェアサプライチェーンのセキュリティと完全性に重点を置いていた。 今回のドラフトでは、ドキュメントの構造を変更し、オーディエンスプロファイルを追加することで、実装ガイダンスをさまざまな対象者によってより消耗品にすることに取り組んだ。また、連邦部門と機関に焦点を当てた2つの新たなAppendixを追加した。 Appendix E：A Federal Acquisition Supply Chain Security Act of 2018 (FASCSA)サプライチェーンリスク評価要因、評価ドキュメント、リスクの重大度レベル、およびリスク対応に関連する連邦行政機関に合わせた追加ガイダンスを提供する。 Appendix F：SP 800-161リビジョン1の文脈における既存の業界標準、ツール、推奨慣行を概説することにより、EOのセクション4(c)に概説された指令に対応することを目指す、予備ガイドラインの公表またはソフトウェアサプライチェーンセキュリティの強化に関するEO14028の呼びかけに対する回答 と最近の規律の発展に起因する推奨プラクティスを提供する。	https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft SP 800-161 rev.1(Draft)： https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-draft2.pdf	Appendix Aがかなりの分量と内容がある。技術標準ではないが、Controls標準として包括的なものであり、納品ベンダーには影響が大きいと思われる。
2021/10/28	Cybersecurity Roadmap for Europe by CONCORDIA	CONCORDIAによる欧州のサイバーセキュリティ・ロードマップ			1										1	研究とイノベーション、教育とスキル、経済と投資、法と政策、認証と標準、コミュニティ構築の6つの側面から総合的に見て、ヨーロッパのデジタル主権に関わる課題を特定し、対処、軽減し、同時にデジタル主権の構築、維持による利益を増幅することを目的としている。 「研究とイノベーション」は、技術的主権の側面に取り組んでいる。 「教育とスキル」は、ITとサイバーセキュリティの能力を構築する必要性を指している。 「経済学と投資」では、新しいデジタル価値モデル、ビジネスモデルの開発、および投資の誘致について説明されている。 「法と政策」は、規制と法的な側面と戦略に焦点を当てている。 「認証と標準」は、ICT製品、サービス、およびプロセスに関するヨーロッパのサイバーセキュリティ認証フレームワークで重要な役割を果たしており、この側面で対処されている。 「コミュニティ構築」の側面は、ヨーロッパの断片化を克服し、さまざまな利害関係者を相互接続する必要性に対処する。デジタルエコシステムを構築し、さまざまな利害関係者を相互接続し、この確立された信頼と協力により、ヨーロッパのデジタル主権を構築するヨーロッパの方法であり、米国と中国の間に挟まれることはない。 6つの側面は、互いに独立していない。それぞれが互いに絡み合っている。たとえば、技術的主権に取り組む研究とイノベーションは、能力（教育とスキルの側面）にも取り組む場合にのみ成功することができる。	https://www.concordia-h2020.eu/blog-post/cybersecurity-roadmap-for-europe-by-concordia/	文書はpreliminary versionとなっており、最終版はプロジェクトの終了時点で公開するとしている。6つの側面を別pdfファイルとしてWeb上で全て公開している。 Cybersecurity Roadmap for Europe Preliminary Version https://www.concordia-h2020.eu/roadmap/
2021/11/1	DRAFT Baseline Criteria for Consumer Software Cybersecurity Labeling	消費者向けソフトウェアのサイバーセキュリティラベリングのベースライン基準 （ドラフト）	1	1				1								5月12日に発行された国家のサイバーセキュリティ改善に関する大統領執行命令(EO 14028)に基づく任命の一環として、NISTは消費者ソフトウェアサイバーセキュリティラベルの基準案を含むホワイトペーパーを発表した。これは、消費者のサイバーセキュリティラベル付けに関連する行政命令の下で多面的なイニシアチブの一部である。 NISTは、消費者向けソフトウェアの潜在的なベースラインセキュリティ基準のセットを示唆するドラフト基準に関するパブリックコメントを求めている。（提出期限：12月16日） これは、IoT製品のサイバーセキュリティ関連の消費者ラベリングに対処する同様のドキュメントを補完する。このドキュメントの基準は、2021年9月のワークショップでNISTに提供された広範な情報と、NISTに提出されたポジションペーパー、および公的機関と民間部門の組織や専門家との機関の調査と議論に基づいている。 EOに従って、NISTは2022年2月6日までにこれらの基準の最終バージョンを作成する予定である。	https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/consumer-software-criteria ホワイトペーパー： https://www.nist.gov/document/draft-baseline-criteria-consumer-software-cybersecurity-labeling	特に2.3.2以降の内容は、ケースバイケースで、SIP CPSで開発されているソフトウエアの技術目標に関する参考文献として活用できる可能性がある。

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			
2021/11/1	KYPO Cyber Range Platform is the European Commission's Innovation Radar Prize Winner	KYPO Cyber Range Platformが欧州委員会のイノベーションレーダー賞を受賞				1						1				マサリク大学の実践的なサイバーセキュリティ教育のための仮想環境であるKYPO Cyber Range Platformは、欧州委員会の第7回イノベーションレーダーコンテストで受賞した。 専門家の審査員は、10月21日に破壊的技術部門の優勝者として発表した。 このカテゴリは、その分野に大きな影響を与える可能性のあるハイテクイノベーションを対象としている。	https://www.concordia-h2020.eu/news/press-release-kypo-cyber-range-platform-is-the-european-commissions-innovation-radar-prize-winner/	
2021/11/8	2021年中間報告	2021年中間報告			1										1	米国・足立氏による2021年海外動向調査の中間報告（詳細は資料参照）		
2021/11/8	2021年中間報告（EU）	2021年中間報告（EU）			1										1	サイバー創研調査によるCPSに関係するEU動向の中間報告（詳細は資料参照）		EUの近年の政策動向から、Cybersecurityにおける動向を把握するために、ECCCとその機能を支える４つのHorizonパイロットプロジェクトの動きに注目することが重要である
2021/11/9	Executive Order 14028: Guidelines for Enhancing Software Supply Chain Security	大統領命令14028：ソフトウェアサプライチェーンのセキュリティを強化するためのガイドライン	1	1				1								NIST主催　EO14028に基づくGuidelines for Enhancing Software Supply Chain Security ワークショップ報告 5月12日に発行のExecutive Order 14028について、第4条を中心にNISTに割り当てられた業務の進捗、成果についての報告。 NISTから主に現在までの関係分野の進捗の発表、米国民間企業からは関連分野に関する各社からの発表がなされた。 (1)Draft NIST SP800-218 Secure Software Development Framework (SSDF) Version 1.1: ・SSDFは、業種環境を問わず、柔軟に、カスタム化可能、選択可能で利用できるよう考慮された基本的なframework。 ・Draft NIST 800-218の特色として、EO 14028に対応として、Appendix Aを追加。 (2)Security Compassからの発表 ・CVE-2021-26084について、ソフトウエア開発に過去の脆弱性の経験が全く反映されていないことへの警鐘事例の説明。 (3)Chainguard ・Attestationとして、TPMに加え、In-Totoの紹介。 (https://github.com/in-toto/attestation) ・codeの検証には、当該コードが書かれたkeyboard、Codeがbuilt onされた機体まで遡らないと意味がない。 少しでもそれに近づくためには、強固な認証が不可欠。 (4)Cisco https://www.cisco.com/c/en/us/about/trust-center.html (5)Microsoft https://devblogs.microsoft.com/engineering-at-microsoft/generating-software-bills-of-materials-sboms-with-spdx-at-microsoft/ (6)Vulnerability Disclosure Programs ・NIST SP 800-216 (draft)を中心に説明。当該SPのきっかけとなった法的根拠として、IoT Cybersecurity Improvement Act of 2020 (Public Law 116-207 Section 5)があったこと、更にその背景として、Homeland Security Actがあったことが言及 ・民間vendorには評判のよくないSBOMについて、当会合であからさまな批判は見られなかったが、ギリギリまで踏み込んだ発言を連発した印象。	https://www.nist.gov/news-events/events/2021/11/executive-order-14028-guidelines-%03enhancing-software-supply-chain https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity	米国・足立氏によるワークショップ参加レポート
2021/11/11	On the Watch for Incident Response Capabilities in the Health Sector	ヘルスケアセクターにおけるインシデント対応能力の監視について					1				1					ENISAは、NIS指令の実施以降、ヘルスケアセクターにおけるセクター別CSIRT機能の開発の現状の分析を発行している。最近リュブリャナとオンラインで開催されているCSIRTネットワークとCyCLONeの会議は、特定のセクターのインシデント対応ツールとプロセスの効率を高めるためのCSIRT機能に関する新しいレポートを公開するための準備を整えた。今回は「ヘルスケアセクターにおけるCSIRT機能」が発表された。 病院などの医療機関は、今日、運営のために複雑で重要なインフラストラクチャに依存している。 2020年、ENISAは、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指令（NIS指令）に基づく重要なセクターから重大な影響を与えるサイバーセキュリティインシデントに関する合計742件のレポートを受け取った。 ヘルスケアセクターでは、2020年にインシデントが前年と比較して47％増加した。	https://www.enisa.europa.eu/news/enisa-news/on-the-watch-for-incident-response-capabilities-in-the-health-sector	

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			
2021/11/12	2021 Gloval PKI and IoT, Trends Study.	2021 Gloval PKIおよびIoT、トレンド調査。			1										1	Ponemon Instituteは、Entrustが後援する2021年のグローバルPKIおよびIoTトレンド調査の結果を発表した。 調査結果によると、デジタル証明書の使用はクラウドアプリケーションとユーザー認証のために急速に成長している。 さらに、IoTデバイスの使用の急速な成長は、PKIテクノロジーの使用に影響を与えており、PKIがIoTに重要なコア認証テクノロジーを提供しているという認識がある。 PKI調査は、2021年4月に発表された、17か国の6,610人の回答者を対象とした大規模な調査の一部である。 このレポートでは、Ponemon Instituteが、次の17の国と地域で組織のエンタープライズPKIに関与している2,513人のITおよびITセキュリティ専門家の調査に基づいた調査結果を示している。：オーストラリア、ブラジル、フランス、ドイツ、香港、日本、韓国、メキシコ、中東、オランダ、ロシア連邦、東南アジア、スペイン、スウェーデン、台湾、英国、米国。	https://info.entrust.com/rs/104-QOX-775/images/2021-pki-iot-trends-study-re.pdf	
2021/11/13	Cloudflare blocks an almost 2 Tbps multi-vector DDoS attack	Cloudflareは、ほぼ2Tbpsのマルチベクトル DDoS攻撃をブロック													1	今週の初め、Cloudflareは、これまでで最も大きな2 Tbpsを下回るDDoS攻撃を自動的に検出し、これを軽減した。これは、DNS増幅攻撃とUDPフラッディングを組み合わせたマルチベクトル攻撃であった。攻撃全体は1分間続いた。この攻撃は、IoT デバイス上の元の Mirai コードのバリアントを実行している約 15,000 のボットと、パッチが適用されていない GitLab インスタンスから開始された。	https://blog.cloudflare.com/cloudflare-blocks-an-almost-2-tbps-multi-vector-ddos-attack/	少なくとも15,000台規模のIoT devicesで構成されたbotでほぼ2Tbpsの規模の攻撃実績ができてしまったという実績は無視できず、近い将来SIP CPS準拠製品が攻撃利用される可能性もある。
2021/11/15	Cyber resilience captains of industry survey 2021	2021年の業界調査のサイバーレジリエンスキャプテン										1				英国のデジタル文化メディア＆スポーツ省（DCMS）の産業界のキャプテンのサイバーレジリエンスに関する調査報告 ・「業界のキャプテン」の大多数は、組織の取締役会は、企業が直面するすべてのリスクと比較してサイバー脅威が高リスクであると考えており、サイバーレジリエンスに関する意思決定を行う十分な情報を得ていると述べている。しかし、取締役会メンバーは、サイバーレジリエンスに関する意思決定能力を向上させるために、さらなる意識向上とターゲットトレーニングを必要とする等、さらに多くのことが必要と考えている。 ・キャプテンの10人に7人(69%)は、彼らの組織がサプライチェーンリスクを積極的に管理していることを示唆している。 同様の割合(68%)で、サプライチェーンにおけるサイバーリスクは、サイバーセキュリティリスクの管理に役立つ書面の一部であると述べている。	https://www.gov.uk/government/publications/captains-of-industry-cyber-resilience-research-2021/cyber-resilience-captains-of-industry-survey-2021 Infosecurity Magazine記事： https://www.infosecurity-magazine.com/news/government-regulation-supply-chain/	Infosecurity Magazine記事の結論はタイトルの、「政府はサプライチェーンのセキュリティを強化するための規制を計画」となるが、どの程度の規制となるかはまだ不明。立て続けにこのような動きが報じられるということから、少なくとも英国において政府レベルでSupply Chain Securityについて動きがある可能性も考えられる。
2021/11/16	New Report on Industry Adoption of Vulnerability Disclosure Practice Published	脆弱性開示慣行の業界採用に関する新しいレポートが公開されました			1										1	モノのインターネット (IoT) セキュリティ財団 (IoTSF) の調査によると、インターネットに接続されたデバイスの製造元の 80% が、自社製品のセキュリティ上の欠陥を報告する方法を提供していない可能性がある。このギャップは、ユーザーがサイバー攻撃に対して脆弱になる可能性がある。 IoTセキュリティ財団報告書： 2021年11月4日：脆弱性開示実務の業界導入に関する新たな報告書を発表 消費者向けIoTセクター - 基本的なサイバーセキュリティ衛生の実践はまだ起こっていない IoTセキュリティ財団は、企業やB2Bモデルへの拡張を含む、コンシューマーIoTにおける脆弱性の開示の実践を調査する第4回報告書を発表した。 容認できないほど低い「…5社のうちほぼ4社は、セキュリティの脆弱性をベンダーに報告して修正できるようにするための非常に基本的なセキュリティ衛生メカニズムを提供できていません。」	https://www.ncsc.gov.uk/report/weekly-threat-report-12th-november-2021 https://www.iotsecurityfoundation.org/consumer-iot-sector-basic-hygiene-practice-still-not-happening/	
2021/11/17	Cybersecurity Spending: An analysis of Investment Dynamics within the EU	サイバーセキュリティ支出：EU内の投資ダイナミクスの分析					1				1					ENISAは、NIS指令の規定に基づいてサイバーセキュリティへの投資がどのように発展したかについての新しいレポートを発行した。NIS指令は、27の加盟国で調査されたエッセンシャルサービス（OES）またはデジタルサービスプロバイダー（DSP）のオペレーターとして特定された947の組織の82％によって実装されており、67％はその実装に追加の予算が必要となっている。 EU全体のサイバーセキュリティに関する最初の法律として、NIS指令の目的は、すべての加盟国で高い共通レベルのサイバーセキュリティを達成することにある。 NIS指令の3つの柱の1つは、OESとDSPのリスク管理と報告義務の実施である。 このレポートは、オペレーターがサイバーセキュリティにどのように投資し、NIS指令の目的に準拠しているかを調査している。また、ITセキュリティスタッフ、サイバー保険、OESおよびDSPにおける情報セキュリティの組織化などの側面に関連する状況の概要についても説明している。 レポートの調査結果は、欧州議会および欧州連合理事会で現在議論されているEU全体のサイバーセキュリティの高い共通レベルの対策に関する指令の提案（NIS2）にさらに反映するために使用できる。	https://www.enisa.europa.eu/news/enisa-news/cybersecurity-spending-an-analysis-of-investment-dynamics-within-the-eu	レポート本体（pdf 86ページ） https://www.enisa.europa.eu/publications/nis-investments-2021

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			
2021/11/18	Executive Order 14028: Guidelines for Enhancing Software Supply Chain Security	大統領命令14028：ソフトウェアサプライチェーンのセキュリティを強化するためのガイドライン	1	1				1								11月8日開催のEO14028 Guidelines for Enhancing Software Supply Chain Securityに関するNISTワークショップの講演ビデオが公開された。	https://www.nist.gov/news-events/events/2021/11/executive-order-14028-guidelines-%03enhancing-software-supply-chain	
2021/11/20	New plans to boost cyber security of UK's digital supply chains	英国のデジタルサプライチェーンのサイバーセキュリティを強化する新しい計画										1				英国のデジタル文化メディア＆スポーツ省（DCMS）情報： 英国のデジタルサプライチェーンのサイバーセキュリティを強化する新しい計画 －企業のITサービスのセキュリティ強化に向け新たな施策を公表 ・調査によると、サイバーセキュリティはビジネス上の優先事項であるが、アクションは遅れている ・デジタル管理会社が厳しい新しいセキュリティ基準に従うための提案 情報の元となっている政策論文：サプライチェーンサイバーセキュリティに関する見解の要請に対する政府の対応 サプライチェーンサイバーセキュリティに関する政府の理解を知らせるために、組織が現在サプライチェーンのサイバーセキュリティリスクをどのように管理しているのか、またどのような追加の政府支援によって組織がこれをより効果的に行うことができるのかについて業界からの洞察を求めた。	https://www.gov.uk/government/news/new-plans-to-boost-cyber-security-of-uks-digital-supply-chains 資料2： https://www.gov.uk/government/publications/government-response-on-supply-chain-cyber-security/government-response-to-the-call-for-views-on-supply-chain-cyber-security	対象としているIT Service Providersとは、CloudやMSPなどが想定されていると文脈から想像できる。
2021/11/22	Preliminary Draft NIST SP 1800-34 Validating the Integrity of Computing Devices	暫定ドラフトNISTSP1800-34コンピューティングデバイスの完全性の検証	1	1				1								NCCoEは、予備草案NISTサイバーセキュリティ実践ガイド1800-34、コンピューティングデバイスの完全性を検証する第C巻をリリースした。ボリュームC(ハウツーガイド)予備草案のパブリックコメント期間は2022年1月17日迄。 草案は、NISTと、Dell Technologies,Eclypsium,HP,Hewlett Packard Enterprise,Intel,RSA,Seagateの共同作成である。 ●NIST SP 1800-34A: ハードウェア・ルーツ・オブ・トラストは、コンピュータ・システムの信頼モデルを構築するための基盤であり、システムに1つ以上のセキュリティ固有の機能を提供するためのハードウェアの基礎を形成する。ハードウェア・ルーツ・オブ・トラストを取得およびライフサイクル管理プロセスに組み込むことで、組織はサプライチェーン攻撃の可視化を達成し、高度な永続的脅威やその他の高度な攻撃を検知することができる。コンピューティングデバイスがサプライチェーンを通過する際にハードウェア・ルーツ・オブ・トラストを活用することで、コンピューティングデバイスの運用ライフサイクルを通じて信頼性を維持することができる。 このプロジェクトでは、部品やプラットフォームの検証可能な記述をどのように作成するか（OEM、プラットフォーム・インテグレータ、さらにはIT部門が行う場合もある）、OEMと顧客との間の1回の取引で機器や部品をどのように検証するか、システム・ライフサイクルの後続段階で機器や部品を運用環境でどのように検証するかなど、いくつかのプロセスを取り上げる。このプロジェクトでは、検証プロセス自体を検査する方法も示す。 ●NIST SP 1800-34B: 1.2 Solution 課題に対処するため、NCCoEはテクノロジーベンダーと協力してプロトタイプの実装を開発している。このプロジェクトが完了すると、組織が入手したコンピュータ・デバイスの内部コンポーネントが本物であり、改ざんされていないことを確認する方法が示される。このソリューションは、デバイス・ベンダーが各デバイス内に情報を保存し、組織が市販のツールとオープンソースのツールを組み合わせて、保存された情報を検証する。	https://www.nccoe.nist.gov/supply-chain-assurance 公開文書： NIST SP 1800-34A: Executive Summary： https://www.nccoe.nist.gov/sites/default/files/legacy-files/nist-sp1800-34a-tpm-sca-preliminary-draft.pdf NIST SP 1800-34B: Approach, Architecture, and Security Characteristics： https://www.nccoe.nist.gov/sites/default/files/legacy-files/tpm-sca-nist-sp1800-34b-preliminary-draft.pdf NIST SP 1800-34C: How-To Guides： https://www.nccoe.nist.gov/sites/default/files/2021-11/sca-nist-sp-1800-34c-preliminary-draft.pdf	

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			
2021/11/24	The Product Security and Telecommunications ,Infrastructure (PSTI) Bill - factsheets	製品セキュリティおよび通信インフラストラクチャ (PSTI) の法案－製品セキュリティファクトシート		1								1				［製品セキュリティおよび通信インフラストラクチャ (PSTI) の法案－製品セキュリティファクトシート ］ 現在、スマートテレビ、スマートフォン、インターネット接続スピーカーなどの接続可能な消費者向け製品は、プライバシーや個人データの喪失などのサイバー危害から消費者を保護するための規制はありません。この規制のギャップを埋めるために、法案は次の事項を行います。 ・製造業者、輸入業者、販売業者に対し、消費者が利用できる消費者用の接続可能製品に関して最低限のセキュリティ要件が満たされていることを確認する必要がある。そして ・急速な技術進歩、悪意のあるアクターが採用する進化する技術、およびより広範な国際的な規制環境に直面して、適応し、有効であり続けることができる堅牢な規制フレームワークを提供します。 ●実施方法 規制に定めるセキュリティ要件は、次の要件になります。 ・既定のパスワードを禁止する　・製品に脆弱性開示ポリシーを要求する　・製品が重要なセキュリティ更新プログラムを受け取る期間について、透明性を要求します。 製品セキュリティ対策(法案の第1部)は、以下の措置を講じます。 ・消費者の接続可能な製品に関連して、最低限のセキュリティ要件を指定し、修正する権限を閣僚に提供する。 ・これらの製品に関連して遵守しなければならない製造業者、輸入業者および流通業者に義務を課す。そして ・これらの義務の違反に対して強制されることを可能にする権限を提供する。 ●法案に含まれる製品 法案は、すべての消費者の接続可能な製品に関連してセキュリティ要件を遵守することを義務付けています。 ●製造業者、輸入業者、流通業者がこの新しい法律に準拠しなければならない期間 政府は、コンプライアンス違反の事例が積極的に施行される前に、企業がビジネス慣行を調整するのに適切な時間を与えられることを保証することにコミットしています。法案のロイヤル・アセンドに続いて、政府は、立法枠組みが完全に発効する前に、製造業者、輸入業者、流通業者がビジネス慣行を調整できるように、少なくとも12ヶ月の通知を提供する。	https://www.gov.uk/guidance/the-product-security-and-telecommunications-infrastructure-psti-bill-product-security-factsheet#how-this-approach-to-legislation-has-developed https://www.gov.uk/government/collections/the-product-security-and-telecommunications-infrastructure-psti-bill-factsheets	
2021/11/29	NIST SP 800-213, 213A and withdrawn NISTIR 8259D (Draft)	NIST SP 800-213、213Aおよび撤回されたNISTIR 8259D（草案）		1				1								● NIST SP 800-213／連邦政府のIoTデバイスサイバーセキュリティガイダンス:IoTデバイスサイバーセキュリティ要件の確立（最終確定版） 組織は、提供できるミッションのメリットのためにモノのインターネット(IoT)デバイスをますます使用しますが、IoTデバイスの取得と実装には注意が必要である。この資料には、取得する予定の IoT デバイスをシステムに統合する方法を検討するのに役立つ背景と推奨事項が記載されている。IoT デバイスとセキュリティ制御のサポートは、組織およびシステムのリスク管理のコンテキストで示される。この資料では、デバイスの観点からシステム セキュリティを検討する方法について説明します。これにより、デバイスのサイバーセキュリティ要件(組織が IoT デバイスとその製造元やサードパーティに求める 能力とアクション)を識別できる。 ● NIST SP 800-213A／連邦政府向けIoTデバイスサイバーセキュリティガイダンス:IoTデバイスサイバーセキュリティ要件カタログ この出版物は、モノのインターネット(IoT)デバイスサイバーセキュリティ機能(セキュリティ制御をサポートするためにデバイスから必要な機能)と非技術的支援機能(デバイスメーカーやその他のサポートエンティティから必要なセキュリティ制御をサポートするために必要なアクションとサポート)のカタログを提供し、組織が特別出版物(SP)800-213を使用してサイバーセキュリティ要件を決定および確立するのに役立つ。 ● NISTIR 8259D (Draft)の新NIST SP 800-213A Appendixへの移管並びに撤回(withdrawn) パブリックコメントに基づき、NISTIR 8259D（連邦政府の IoT コア ベースラインと非技術的ベースラインを使用したプロファイル）のコンテンツはSP 800-213Aの付録に移管され、NISTIR 8259Dは撤回された。	SP 800-213： https://csrc.nist.gov/publications/detail/sp/800-213/final SP 800-213A： https://csrc.nist.gov/publications/detail/sp/800-213a/final NISTIR 8259D (Draft)： https://csrc.nist.gov/publications/detail/nistir/8259d/archive/2020-12-15	

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			
2021/12/1	5G rollouts offer Internet of things a ,more sophisticated outlook	5Gの展開により、IoTのより洗練された展望が提供される												1		「モノのインターネット」(IoT)は、ドライバーレス車から「接続された冷蔵庫」からロボット工場まで、センサーを使用してデータを収集するさまざまな項目を説明するキャッチオールフレーズとしてよく使用されます。 しかし、リモートモニタリング、診断、ヘルスケアなどのデータ集約型タスクにIoT技術が広く採用される中、5Gネットワークの需要も同様に増加しています。古いネットワークよりも速度、制御、セキュリティを提供する5Gの普及率が高まっており、IoT技術のより高度な世界が出現しました。 パンデミックの間に加速した自動化の使用の成長は、IoTを潜在的に大きなビジネスに変えました。 長い間IoTを潜在的な成長ドライバーとしてターゲットにしてきた通信グループのVodafoneは、今月、IoT SIMカードの数を過去1年間で1億1,200万から1億3,600万に増やし、最大のグローバル接続プロバイダーになっていると述べました。 IoTは、英国の上場企業に年間約10億ユーロの収益をもたらし、その数字は2桁の速度で成長しています。 テクノロジーコンサルタントであるOmdiaのIoTエンタープライズ調査によると、IoTを受け入れる企業が増えており、インタビューを受けた企業の70%近くが、IoT技術が今後18ヶ月間にビジネスにとってより重要な要因になると予想しています。 およそ半数はパンデミックがIoT計画を加速させたと述べ、ほぼ3分の2はIoT戦略に最大500万ドルを費やすと述べました。 OmdiaのIoTリサーチディレクター、ジョシュア・ピルダ氏は「Covid-19が生み出した大規模な混乱により、IoTソリューションに対する企業の需要が大幅に増加し、多くの場合、これらの企業は事業を維持し、従業員の安全を確保することができました」と述べています。 一方で、Omdiaの予測によると、スマートフォン市場の動きは少ない可能性が高い。成長機会は、5G携帯電話の需要の増加とは対照的に、ファーウェイの市場シェアの崩壊とLGの出口によって引き起こされます。 中国、米国、ドイツは、自動車やヘルスケアなどの分野で産業オートメーションが進歩したため、今後数年間でIoTの最高レベルの成長を記録すると予測されています。Omdiaは、中国が2025年までに、米国の2.5億台に対して、18億台のIoTデバイスの設置ベースを持っていると見ています。（記事中のDigital markets　Country size forecast, index (2024)を参照）	https://www.ft.com/content/1a274206-59df-4d97-9228-c1cfd50c040f	記事の最下部に2024年のDigital marcketの各国の市場規模が載せられているが、 この数字では日本におけるIoT marcketの比率は他の国に比べてそれほど大きくないように示されている。
2021/12/2	ENISA Cybersecurity Certification Conference 2021	ENISAサイバーセキュリティ認証会議2021								1						［ENISA Cybersecurity Certification Conference 2021］参加報告（米国・足立氏） ●Thomas Skordas, Acting Deputy Director General, Digital Connect, European Unionの録画による基調講演より、EUが進める認証 (Cybersecurity Certification)は、EU Cyber Resilience Act[1]の趣旨にも沿い、Market enablerとしての位置付け、ユーザが性能を理解でき、製造者にSecure by designを同期づけるとの意見。この講演、あるいは後のパネルでたびたび言及されたのは、Resilience, Sustainability, Trustであり、少なくとも大西洋の両側で、今年の流行り言葉はこの三つの単語であることが感じられる。 ●Juhan Lepassaar – ENISA, Executive Director 　ENISAトップによる講演。 彼はResilienceという言葉は用いなかった代わりにSustainabilityという語で、EU Certificationがいかに素晴らしいかを主唱。Certificationが実現できる課題として - Trusted Solutions　- Capacity Building　- Operational Cooperation　- Cybersecurity Policy の四分野を挙げられる。どのようなCertificationにおいても、Applicationが鍵となる旨述べられた。 ●European Cybersecurity Competence Center or ECCCについて複数の講師から言及があった。　どうやらEU内部でも、Certificationについて、ENISAとECCCの果たす役割の違いがきちんと理解されていない可能性が考えられる。 ●BSIより、NESASのドイツ版実装について紹介。　聞いている限りでは電気通信設備（明言はなかったが明らかに新規の5G設備）でのドイツでの認証certificationの基準として、NESASに基づきドイツ版の認証基準を策定し認証を進めているとのこと。これはNESAS Cybersecurity Certification Scheme German Implementation (NESAS CCS-GI)として紹介された。 ●IoTパネルでは、NCSC-FI（昔のCERT-FI), Eurosmart, ANECなどからパネリストが参加。主にLabelingの話題が中心。　彼ら非EU系の組織であるからかも知れないが、IoTについては、最近のRED (Radio Equipment Directive)などの法規制、ETSIの関係標準など既存の規制で十分おなかいっぱいな雰囲気が漂っていたように感じられる。	https://www.enisa.europa.eu/events/enisa-cybersecurity-certification-conference-2021/agenda https://ec.europa.eu/commission/commissioners/2019-2024/breton/blog/how-european-cyber-resilience-act-will-help-protect-europe_en https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre https://www.gsma.com/security/network-equipment-security-assurance-scheme/ https://www.kyberturvallisuuskeskus.fi/en/news/finland-becomes-first-european-country-certify-safe-smart-devices-new-cybersecurity-label	

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			
2021/12/2	ENISA Cybersecurity Certification Conference 2021	ENISAサイバーセキュリティ認証会議2021								1						12月2～3日、欧州ネットワーク情報セキュリティ機関（ENISA）は、第4回サイバーセキュリティ認証会議を開催した。 ・この会議には1800以上がオンラインで参加し、サイバーセキュリティの専門家、サービスプロバイダー、適合性評価、監督機関、各国当局が一堂に会し、EUサイバーセキュリティ認証に関連する市場機会と新技術のイノベーションの課題に取り組む方法について話し合った。 ・認証会議に先立ち、週の最初の部分ではアドホックワーキンググループ（AHWG）が会議を行い、プレナリーが開催された。共通規範、クラウドサービス、5G、サイバーセキュリティ市場に関する専門家グループは、アテネで物理的に組織され、オンラインで参加した。 ・ENISAは、5Gネットワークのサイバーセキュリティ認証スキームの候補を準備する目的で、11月29日にEU5Gに関するアドホックワーキンググループを立ち上げている。これは、EUが調整したリスク評価、5G脅威の状況、および5Gツールボックスに関するNIS協力グループのガイダンスに対応するものである。 ・また、サイバーセキュリティ市場に関するアドホックワーキンググループは、2021年11月17日に発足し、2021年11月29日に、相互接続されたデバイス、IoT、5G、市場の評価と分析の方法、最後にサイバーセキュリティ市場セグメントの定義などの新興セクターに影響を与える市場動向をテーマに第2回会議を開催している。 ・サイバーセキュリティ認証会議の際に、サイバーセキュリティ認証に関する意識向上に関する最初の専用キャンペーンが開始された。 今年のキャンペーンは、適合性評価機関（CAB）に関係する「認証できるもの」に焦点を当てた。 CABが何であるかについての洞察を提供する専用のビデオ（認証スキームとCAB-Q＆A-ENISA）が作成された。 ・「サイバーセキュリティ認証会議」において記録されたパネルと討論は2022年初頭に公開を予定している。次回の「サイバーセキュリティ認証会議」は、2022年6月2日から3日に開催される。	https://www.enisa.europa.eu/news/enisa-news/going-full-throttle-on-cybersecurity-certification-and-market	
2021/12/2	Consumer Cybersecurity Labeling for IoT ,Products：Discussion Draft on the Path	IoT、製品の消費者サイバーセキュリティラベリング：今後の方向性に関するディ	1	1				1								NISTは、大統領令EO14028に基づき、一般からのフィードバックを考慮に入れ、さらなるディスカッションペーパー「Consumer Cybersecurity Labeling for IoT Products: Discussion Draft on the Path Forward（IoT製品の消費者サイバーセキュリティラベリング:パスフォワードに関する議論の草案」を発表しました。 このホワイトペーパーは、12月9日に行われる4時間のワークショップ「Cybersecurity Labeling for Consumer IoT and Software: Executive OrderUpdate and Discussion」で説明されるとのことです。	https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/iot-product-criteria	
2021/12/9	NIST Workshop：NIST Cybersecurity Labeling for Consumer IoT and Software Executive Order Update and Discussion	NISTワークショップ：NISTサイバーセキュリティラベリング消費者向けIoTとソフトウェアの大統領命令の更新とディスカッション	1	1				1								さる5月にWhitehouseより発行のExecutive Order 14028でNISTに課された命令のうち、Consumer Software [1]並びにConsumer IoTに対するCybersecurity Labeling[2]の原案作成に関連しNISTが主催したオンラインでの会合である。 1.　会議全体から窺われるNISTの姿勢 ・現状の最優先課題は、EO 14028に定められた2022年2月6日までに二つのlabeling criteriaを含む成果物を完成させること。 ・本件の由来がEOであることからか、アメリカの市場で販売入手される製品を対象とし、EOに示された内容を具体化するのが主目的であり、既存の標準との整合性、調整や外国との連携などはどちらかというと二の次。 ・EOに由来するこれらの活動の適用先もよくわからないところがある。例えば、NISTの標準類は連邦政府文民省庁を適用対象としているが、今回のEOに由来する成果物については、「NISTがAudienceを決める立場にない。」との見解が示された。特にIoT labeling programについては、EOではNISTに加えFTCの関与も含まれており、米国内で販売される全てのConsumer IoTあるいはConsumer Softwareにこれらのlabelingが適用される可能性も否定できない。 ・既存のrequirements, criteriaは、実現目標を示しているが個別実装を求めているわけではないし、NISTのlabeling draftは、運用者 Scheme Ownerが決めることと割り切っているようにも解釈できる。	https://www.nist.gov/news-events/events/2021/12/cybersecurity-labeling-consumer-iot-and-software-executive-order-update https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/consumer-software-criteria https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/iot-product-criteria	

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			
2021/12/9	SP800-160Vol.2 Rev.1（Final）	SP800-160Vol.2 Rev.1（最終）	1	1				1								NISTは12月9日付でSP800-160Vol.2 Rev.1（最終版）：「サイバー弾力のあるシステムの開発:システムセキュリティエンジニアリングアプローチ」を公開した。 これは、システムセキュリティエンジニアリングおよびレジリエンスエンジニアリングと組み合わせて適用される存続可能で信頼できる安全なシステムを開発するための新しい特殊システムエンジニアリング分野である。 サイバーレジリエンシーエンジニアリングは、サイバーリソースに対するストレス、攻撃、または侵害を予測し、それに適応し回復する能力を備えたシステム信頼性を設計、開発、実装、維持継続することを目的としている。 本文書は、以下の文書と組み合わせて使用される。 ・ISO/IEC/IEEE 15288:2015：Systems and software engineering—Systems life cycle processes ・NIST SP800-160, Volume 1：　Systems Security Engineering—Considerations for a Multidisciplinary Approach　in the Engineering of Trustworthy Secure Systems、 ・NIST SP800-37：Risk Management Framework for Information Systems and　Organizations　—A System Life Cycle Approach for Security and Privacy ・NIST SP 800-53：Security and Privacy Controls for Information Systems and Organizations	https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf	
2021/12/14	Artificial Intelligence: How to make Machine Learning Cyber Secure?	人工知能：機械学習をサイバーセキュアにする方法について								1						機械学習（ML）によるサイバー攻撃を防ぐ方法は。 パフォーマンスを妨げることなくコントロールを展開するにはどうすればよいか。 ENISAは、新しいレポートで、MLのサイバーセキュリティに関する質問に回答している。	https://www.enisa.europa.eu/news/artificial-intelligence-how-to-make-machine-learning-cyber-secure	Securing Machine Learning Algorithms https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms
2021/12/15	Consumer_Cybersecurity_Labeling_for_IoT_Products並びに周辺関連文献の比較と考察							1		1		1			1	米国・足立氏による「Consumer_Cybersecurity_Labeling_for_IoT_Products並びに周辺関連文献の比較と考察」資料 12/2に発行されたNIST Consumer_Cybersecurity_Labeling_for_IoT_Productsに関連して、同9日に実施されたNIST Workshopの発表・質疑を踏まえた留意点、及び、標題文書がめざすIoT Labellingの先行事例としてEU標準のETSI EN 303 645、並びにLabellingを実施している国々の事例について取りまとめ海外動向調査WGメンバーに送付された。（詳細は文書参照）		
2021/12/20	KNXlock – an attack campaign against KNX-based building automation systems	KNXlock –KNXベースのビルディングオートメーションシステムに対する攻撃キャンペーン												1		Limes Security社による、欧州におけるBuilding Automation Systemsへの攻撃事例の紹介報道 あるビルオートメーションエンジニアリング会社が、オフィスビルの顧客のために構築したビルオートメーションシステム（BAS）から、まれに見るサイバー攻撃によってロックアウトされ、照明スイッチ、モーションセンサー、シャッターコントローラーなど、数百のビルオートメーションシステム（BAS）機器と突然連絡が取れなくなる事態に見舞われた。ドイツにある同社は、オフィスビルのシステムネットワーク内にあるBAS機器の4分の3が、意図せず「スマート」になっていて、システムのデジタルセキュリティキーでロックされ、それが攻撃者の支配下にあることを発見した。ビルの照明を点灯させるためには、中央のサーキットブレーカーを手動でオン・オフするしかなかった。 Limes Security社では、ヨーロッパで広く普及しているビルディングオートメーションシステム技術であるKNXを使用したBASシステムに対して、同様の攻撃を受けたという報告を受けている。具体的には、セキュリティ機能であるはずのプログラミングパスワード（BCUキー）を悪用して、敵対者がコンポーネントを操作できないようにしていたということであった。	https://limessecurity.com/en/knxlock/ https://www.darkreading.com/attacks-breaches/lights-out-cyberattacks-shut-down-building-automation-systems	

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			
2021/12/24	Honeypot experiment reveals what hackers want from IoT devices	ハニーポットの実験により、ハッカーがIoTデバイスに何を求めているかが明らかになる												1		IoTが攻撃される場合、何が狙われ、何をされるのか、ハニーポットを三年動かし観測されたデータに基づき解析したNISTとフロリダ大学の研究者による論文が発表された。 相互作用の少ないハニーポットエコシステムでの実際の攻撃者の行動を観察することにより、 （1）ハニーポットの相互作用の高度化を徐々に高める、敵対者に対峙する多段階で多面的なハニーポットエコシステムを作成する新しいアプローチを提示し、（2）攻撃者が何を標的にしているのかを研究者がより深く理解できるようにする、カメラ用の相互作用の少ないハニーポットを設計・開発し、（3）敵対者の目標を特定する革新的なデータ分析方法を、考案した。 3年間のハニーポット実験により、アクターがなぜ特定のデバイスを狙うのかが明確になった。 デバイスを保護する方法： ハッカーによるIoTデバイスの乗っ取りを防ぐために、以下の基本的な対策を行っていただきたい。 ・デフォルトのアカウントをユニークで強力な（長い）ものに変更する。 ・IoTデバイス用に別のネットワークを設定し、重要な資産から隔離しておく。 ・利用可能なファームウェアやその他のセキュリティアップデートがあれば、できるだけ早く適用する。 ・IoTデバイスを積極的に監視し、悪用の兆候を探す。 最も重要なことは、インターネットに接続する必要のないデバイスは、ファイアウォールやVPNの内側に設置し、不正なリモートアクセスを防止することである。	https://www.bleepingcomputer.com/news/security/honeypot-experiment-reveals-what-hackers-want-from-iot-devices/ https://arxiv.org/pdf/2112.10974.pdf	
2022/1/6	Log4j	Log4j関連情報	1	1								1		1		・SecurityWeekは、最近のLog4jの脆弱性を受けて、産業用制御システム（ICS）やその他の産業関連ベンダーが発表したアドバイザリをまとめた。 12月初旬以降、Log4jロギングユーティリティーにいくつかの脆弱性が発見されていますが、その中でも最も重要なのは、「Log4Shell」と呼ばれるCVE-2021-44228である。Log4Shellは、サイバー犯罪者や国家が支援する脅威アクターによる多くの攻撃に悪用されており、その中には産業組織に対するものも含まれている。 当該記事にはICS機器類での脆弱性はまだあまり具体的に触れられていないが、各種のツール類、例えばRemote access platform(ABB), Voice Applications (Honeywell),Cloud Services (Phoenix Contact, Schneider Electric, Sierra Wireless)、その他Software (WAGO)などに脆弱性が確認されている。 ・FTCはLog4jの脆弱性修正を促す企業への警告を行った。FTCは、Log4jや同様の既知の脆弱性の結果として、消費者データの漏洩を防ぐための合理的な措置を講じなかった企業を、法的権限をフルに活用して追及していく意向である。	https://www.securityweek.com/ics-vendors-respond-log4j-vulnerabilities https://www.ftc.gov/news-events/blogs/techftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability https://twitter.com/FTC/status/1478452070684504068?s=20	
2022/1/10	Apache Position Paper	Apache 状況説明													1	米国でのlog4j問題に関して、Apacheがこの問題についてのPosition Paperを公開した。 ・完全なリリースでさえ、ダウンストリームプロバイダーによって採用および展開されるまでに数年かかる場合があり上流の生産者だけに焦点を当てることによって、オープンソースのサプライチェーンの問題を解決することはできない。 ・コミュニティは、自発的に参加し仕事をする人々によって定義されており、政府からのセキュリティ指令は、すでに作業を行っている少数のメンテナに追加の資金のない負担をかけないようにする必要がある。 ・最近のApacheLog4jの脆弱性は、Javaプラットフォーム内で独立して設計された機能の不幸な組み合わせであった。少なくともデフォルト構成内で、時代遅れで不要な機能を無効にすると、この脆弱性を防ぐことができる。 ・安全でない操作の間接的なアクティブ化を防ぐためにプラットフォームのセキュリティを改善することは、非常に大きなメリットになる可能性がある。	https://cwiki.apache.org/confluence/display/COMDEV/Position+Paper	
2022/1/11	CVE-2021-45608	NetUSB RCE Flaw in Millions of End User Routers	CVE-2021-45608	何百万ものエンドユーザールーターのNetUSBRCEの欠陥										1	1	KCode作成NetUSBの脆弱性情報 ・SentinelLabsは、多数のネットワークデバイスベンダーが使用し、何百万ものエンドユーザールーターデバイスに影響を与えるKCodes NetUSBカーネルモジュールで重大度の高い欠陥を発見した。攻撃者は、この脆弱性をリモートで悪用して、カーネル内のコードを実行する可能性がある。 ・マイクロソフトは、この脆弱性を直接 KCodes に報告し、コンテストで TP-Link または Netgear デバイスのみを対象とするのではなく、ライセンシー間で配布した。これにより、コンテスト中にすべてのベンダーがパッチを受け取る。 潜在的なリスクを軽減するために、すべてのユーザーが上記の修復情報に従うことを推奨する。	https://www.sentinelone.com/labs/cve-2021-45608-netusb-rce-flaw-in-millions-of-end-user-routers/ https://www.kcodes.com/product/1/36 https://www.zdnet.com/article/kcodes-netusb-kernel-remote-code-execution-flaw-impacts-millions-of-devices/	脆弱性発見者とされるSentinelOneの本日付発表ではSOHO Routersが主に言及されているが、KCodeによるNetUSBの説明では、ほぼありとあらゆるConsumer/business IoTが対象と考えられる。

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			
2022/1/11	Draft NIST Special Publication 800-160, Volume1	NIST Special Publication 800-160, Volume1 ドラフト	1	1				1								NISTは1月11日付でSP800-160Vol.1 Rev.1（ドラフト）：「信頼できるセキュアシステムのエンジニアリング」を発表した。2月25日を期限として本ドラフトに対するパブリックコメントを募集している。 この出版物は信頼できる安全なシステムとシステムコンポーネントの開発に携わるエンジニアやエンジニアリング専門分野、建築家、設計者、および人員のための参考資料として機能することを目的としている。このガイダンスは、組織、個人、またはエンジニアリング チームによって選択的に適用され、システムおよびシステム コンポーネントのセキュリティと信頼性を向上させることができる。 SP 800-160Vol.1 Rev.1は、特に、以下の戦略的目標に焦点を当てている。 ・システムセキュリティエンジニアリング(SSE)をシステムエンジニアリング(SE)のサブ分野としてより強く位置づけ、 ・信頼できる安全なシステムのエンジニアリングに対する責任はセキュリティの専門分野に限定されず、セキュリティの成果はSE の成果と適切に一致する必要があることを強調する ・SSEの慣行を、資産の損失および資産の損失の結果に対処する安全慣行およびその他の分野と整合させる ・システムのセキュリティ機能の正確性と有効性の保証に焦点を当てて、承認された意図された行動および結果を達成し、悪影響と損失を制御する ・システムセキュリティエンジニアリング業務を国際規格に密接に連携させる	https://csrc.nist.gov/publications/detail/sp/800-160/vol-1-rev-1/draft https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1-draft.pdf https://www.nextgov.com/cybersecurity/2022/01/nist-updates-cybersecurity-engineering-guidelines/360587/	
2022/1/11	NISTIR8349（Draft）Methodology for Characterizing Network Behavior of Internet of Things Devices	NISTIR8349（Draft）：IoTデバイスのネットワーク挙動を特徴付けるための方法論	1	1				1								NISTは、NISTIR 8349 (Draft):(IoTデバイスのネットワーク挙動を特徴付けるための方法論)を公表した。 ネットワークのセキュリティ保護は、IoTデバイスが接続されている場合に、より困難で複雑な作業となる。このレポートでは、IoT)デバイスのネットワーク通信動作をキャプチャして文書化する方法について説明している。この情報から、製造元、ネットワーク管理者、およびその他のユーザーは、製造元の使用法の説明 (MUD) 仕様に基づいてファイルを作成および使用し、これらの IoT デバイスとの間のアクセスを管理できる。 また、このレポートでは、アプローチの実施の現状と将来の開発に向けた提案についても説明している。	https://csrc.nist.gov/publications/detail/nistir/8349/draft https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8349-draft.pdf	
2022/1/12	Hot Topics in Consumer Cybersecurity Labeling	消費者サイバーセキュリティラベリングのホットトピック	1	1				1								NIST責任者のKaterina Megasさんが昨年5月の大統領令（EO14028）以降のCybersecurity Labelingに関するNISTの取り組み状況とワークショップの状況説明をブログにて公表した。 ●ワークショップの状況（寄せられた質問、懸念点） ・ラベリングスキームの所有者の役割と責任範囲、彼らの経済学、および複数のスキーム所有者間の競合の可能性等。 ・説明責任の変動や基準の施行、構成証明の信頼性に関する疑問が提起： ・長期的なプログラムコストに関する質問：適合性を実証するためのコスト?消費者教育のための資金?メーカーの参加は、製品のコストにどのような影響を与えるか? ・スキーム所有者がその責任を負う適切な当事者か、消費者が階層化されたラベルの情報を利用するか、消費者教育の様々な側面が提起。 ・NISTの勧告と他の国や国際基準機関が策定している基準とガイドラインとの関係への懸念。参加者は、ソフトウェアとIoTサイバーセキュリティは世界的な問題であり、複数の体制下での認証はメーカーにとって負担と指摘。 ●今後について ・NISTはソフトウェアとIoTサイバーセキュリティ基準を最終決定しており、最終基準を公開する期限は2月6日である。 ・NISTは、EOに対応する際に行われた作業と、基準に具現化された決定の背後にある背景と推論を要約する。 ・基準が利用可能になると、パイロットフェーズで使用され、基準がラベル付けの取り組みをサポートし、消費者向けIoT製品およびソフトウェアに関連するサイバーセキュリティを改善する方法に関する情報を提供する。 ・EOは、2022年5月12日までに最終報告書を提出することを義務付けている。	https://www.nist.gov/blogs/cybersecurity-insights/hot-topics-consumer-cybersecurity-labeling-our-december-2021-workshop	

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			
2022/1/12	European Union to Launch Supply Chain Attack Simulation	欧州連合がサプライチェーン攻撃シミュレーションを開始			1									1		欧州連合（EU）は、主要なサプライチェーンのサイバー攻撃シミュレーションを計画していると報じられている。 ブルームバーグによると、訓練は数日中に開始され、6週間続く。この訓練は、欧州の流通ネットワークに影響を与える攻撃に対する加盟国の準備状況をテストするように設計されている。ブルームバーグは、「問題に精通している」内部文書と情報源を引用して、シミュレートされた攻撃は主にヨーロッパ全体のサプライチェーンを標的にするだろうと述べた。協調的な攻撃は、過去のサプライチェーンのハッキング、または将来可能な限り現実的である可能性が高いと考えられるハッキングに基づいて行われる。 「ストレステスト」に参加する人々は、攻撃に対する外交的および公的対応を調整し、他の加盟国における社会経済的影響の波及に対処する。 訓練は、2022年1月1日に欧州連合理事会の議長国を引き継いだフランスによって提案されたと考えられている。訓練後、EUは、現在欠如している主要な事件への共同対応の枠組みを開発することを目指してる。	https://www.infosecurity-magazine.com/news/eu-supply-chain-attack-simulation/	
2022/1/13	Cybersecurity Label for consumer products could be on the way	消費者向け製品のサイバーセキュリティラベルが進行中												1		NISTのCybersecurity Labelingに関するWashington Post記事 エルサルバドルの少なくとも35人がNSOGroupのPegasusスパイウェアの標的にされた件に関連して、ホワイトハウスは、log4jやその他のオープンソースソフトウェアの脆弱性について業界のリーダーを招き、議論する予定である。 商務省のある部門は、サイバーセキュリティで最も困難な問題の1つである、インターネットに接続されたデバイスがハッキング可能かどうかを消費者に気にさせることに取り組んでいる。 ほとんどの消費者は、どの製品がハッキングに対して最も安全であるかについて、漠然とした理解しか持っていないため、これは大きな課題となっている。 彼らがよりよく理解したとしても、専門家は、価格や機能などの要因よりも、購入決定においてセキュリティがはるかに低くランク付けされることを恐れている。 米国国立標準技術研究所（NIST）の大きな計画は、インターネットに接続されたデバイスがソフトウェアパッチの受け入れや、デバイスが収集して共有する情報をユーザーが制御できるようにするなど、一連の基本的なサイバー標準を満たしていることを確認する証明書プログラムである。 NISTはラベル自体を作成しているのではなく、ラベルがどのように表示されるかについての長い一連の推奨事項をまとめており、業界団体または標準設定機関が課題に取り組むことを望んでいる 5月のバイデン大統領の大規模なサイバーセキュリティ大統領命令から生まれたこの取り組みは、政府が重要な業界でのサイバー防御の強化を超えて、より広い国のサイバーセキュリティに対する考え方を実際に変えようとしているまれな例の1つとなっている。	https://www.washingtonpost.com/politics/2022/01/13/cybersecurity-labels-consumer-products-could-be-way/	
2022/1/13	Department of Commerce Seeks Internet of Things Experts for New Advisory Board	商務省は新しい諮問委員会のための物事のインターネットの専門家を求めている		1				1				1				NISTが新規に発足させるInternet of Things Advisory Board (IoTAB)のnominationが公告された。 商務長官は、2021年度のウィリアム・M(Mac)ソーンベリー国防承認法の要件に従い、改正された連邦諮問委員会法に従って、IoT諮問委員会(IoTAB)を設立した。商務省は、最近設立されたIoT連邦ワーキンググループに助言するために、新しいIoT諮問委員会の適格な指名を求めている。 諮問委員会は、モノのインターネット(IoT)に関する専門知識を持つ16人の連邦政府外の幅広い利害関係者で構成される。 推薦は、2022年2月28日までに行われ、NISTは諮問委員会に管理支援を提供し、ボード活動に関する情報はNISTのウェブサイトで見つけることができる。	https://www.nist.gov/news-events/news/2022/01/department-commerce-seeks-internet-things-experts-new-advisory-board https://www.federalregister.gov/documents/2022/01/13/2022-00419/establishment-and-call-for-nominations-to-serve-on-the-internet-of-things-advisory-board	

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			
2022/1/13	White House Hosts Open-Source Security Summit	ホワイトハウスがオープンソースセキュリティサミットを主催										1		1		爆発的なApache Log4jの脆弱性を受けて、ホワイトハウスはサミットで技術指導者と連邦政府機関を主催し、オープンソースソフトウェアセキュリティを改善する方法について話し合った。 当局者はイベント前の声明の中でISMGに対し、「この会議の目的は広く使用され、開発者によって検査、変更、強化が可能なオープンソースソフトウェアに関する重要な議論を促進することだ」と述べた。 出席組織には、Akamai, Amazon, Apache Software Foundation, Apple, Cloudflare, Facebook/Meta, GitHub, Google, IBM, Linux Open Source Foundation, Microsoft, Oracle, RedHat and VMWare.及び、 商務省国土安全保障エネルギー防衛部門、CISA、NCD、NIST、科学技術政策局、国立科学財団（NSF）などの米国機関である。 今日の会議の重要なテイクアウトは、「進化し続ける脅威の中で、オープンソースコミュニティが繁栄するために、より多くのことを行う必要がある。」という集団的認識である。 政権当局者は、この会議は2021年5月に発行されたサイバーセキュリティに関するバイデン大統領の執行命令によりソフトウェアセキュリティに焦点を当てた取り組みを推進してきた。この命令では、安全なソフトウェア開発ライフサイクルプラクティスを使用し、特定の連邦セキュリティガイダンスを満たす企業のみが連邦政府に販売できることを義務付けている。 行政命令はまた、連邦ベンダーのためのソフトウェア手形、またはSBOMの使用を制定した。SBOM は特定のソフトウェア コンポーネントの包括的なリストであり、脆弱性の漏えいを引き起こす可能性を受けて手動で識別するプロセスを削減できる。 Googleは、ハイテク大手は、重要なオープンソースプロジェクトの特定を含むトピックに関するいくつかの提案を共有したと話した。セキュリティ、メンテナンス、テストのベースライン確立そして、公的および私的支援には、オープンソースのメンテナンスとして機能する新しい組織の形成が含まれ、ボランティアと重要なプロジェクトをマッチングすると発言した。 「Log4jの脆弱性に対する反動にもかかわらず、ホワイトハウス会議は、主要な重要なインフラストラクチャシステム上で実行されているソフトウェアの可視性と、最小限の安全な開発基準の遵守を義務付ける、より多くの原動力となるべきである」とGeyer氏は付け加えた。	https://www.govinfosecurity.com/white-house-hosts-open-source-security-summit-big-tech-a-18304 https://www.commerce.gov/news/speeches/2022/01/remarks-us-commerce-secretary-gina-m-raimondo-white-house-open-source	
2022/1/13	How do we keep the supply chain cyber-secure? WHEN THE CHAIN ITSELF IS THE WEAKEST LINK Cybersecurity in the Supply Chain	サプライチェーンをサイバーセキュリティで保護するにはどうすればよいか			1							1				ランサムウェア、フィッシング、脆弱なソフトウェア、およびサーバーやネットワークへのその他の不正アクセスを通じて、すべての企業がサイバー犯罪者の潜在的な餌食になっている。また、チェーン内の相互接続性のために、独自のサイバーセキュリティを整えるだけではもはや十分ではない。サイバー犯罪者は、サプライヤーやビジネスパートナーを通じて最終目標をますますハッキングしている。 サプライチェーンにおけるサイバーセキュリティ サプライチェーンにおけるサイバーセキュリティは、頭の痛い怪物である。問題を構造的かつ的を絞って防ぐための「特効薬」がないことは明らかだ。しかし、それは、すべての組織が最初のインシデントが発生するまで待ってから行動を起こす必要があるという意味ではない。TNOは、サプライチェーンにおけるデジタルセキュリティの向上に向けた3つの具体的なステップを特定した。	https://ecs-org.eu/newsroom/how-do-we-keep-the-supply-chain-cyber-secure	ECSOメンバーのTNO社（オランダの独立研究組織）が2021/12に発表したレポートの紹介 https://publications.tno.nl/publication/34638899/zNP6Av/buningh-2021-als.pdf TNO社レポートの本体（オランダ語および英語）
2022/1/25	Policy paper Government Cyber Security Strategy: 2022 to 2030	政策文書 政府のサイバーセキュリティ戦略：2022年から2030年まで	1									1				英国政府のサイトに掲載された 2022年から2030年のサイバーセキュリティ政府戦略 【ビジョンと目的】 戦略のビジョンは、公共サービスの提供から国家安全保障装置の運用まで、中的な政府機能がサイバー攻撃に対して回復力を持ち、主権国家としての英国を強化し、民主的で責任あるサイバー大国としての権限を強化することを保証することである。 コアとなる政府機能は政府機関、地方自治体など、さまざまな公共部門の組織によって提供されている。この戦略では、そのようなすべての公共部門の組織が考慮されている。 ビジョンを達成するために、戦略は中心的な目標を追求する。政府の重要な機能が2025年までにサイバー攻撃に対して大幅に強化され、公共部門全体のすべての政府組織が2030年までに既知の脆弱性と攻撃方法に耐性を持つようにすることである。 政府全体でサイバーセキュリティリスクの組織的かつ客観的な可視性のレベルを達成するには、広範なプロセス、メカニズム、およびパートナーシップを確立する必要があり、さまざまなレベルのサイバー成熟度、機能、および容量によってタスクは複雑になる。これの鍵となるのは、主要な政府部門が、独立企業間組織およびその他の公的機関の範囲内でのマクロサイバーセキュリティの姿勢を評価および明確化できるようにすることである。 この目的の達成は、政府に非常に厳しい目標を課する。政府がデータを保護し、過度の混乱を招くことなく運用できるようにするだけでなく、政府組織は未知のより高度な脅威が発生した場合に管理できるように構造化および組織化される。	https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030/government-cyber-security-strategy-2022-to-2030-html	英国政府のホームページで提供されている84ページからなる政策文書がある。 https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030

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			
2022/1/26	An 'ingredients list' for software could help prevent the next	ソフトウェアの「成分表」は、次のlog4jを防ぐのに役立tu												1		政府のサイバー担当者が推進している大きなアイデアの1つが、技術システムの成分表を示すSoftware Bill of Materials (SBOM)である。この概念は以前から存在したが、政府関係者や産業界の幹部が技術的なエコシステム全体に広がっているソフトウェアに潜む非常に危険なバグに取り組む中、log4jの問題でさらに焦点が当てられている。SBOMは、log4jを防ぐことはできないが、後始末をはるかに早くすることができると考えられる。 CISAの上級顧問で、この取り組みに携わっているアラン・フリードマン氏は、「Log4jは、もし今日SBOMがあれば、もっと管理しやすくなるだろうと人々に気づかせてくれた。このプロジェクトは、ドルとセントの単位で実際に目に見える価値があるということを、人々に理解させることができた」と述べた。政府が自らSBOMを設計するのではなく、重要な産業がSBOMを利用しやすくなるようにしているのだ。 ［進捗状況］ 重要な産業分野でSBOM化の動きが出てきたが、まだ道のりは長い。電力会社は電力部門でのSBOMの使用を試験的に行っており、米国食品医薬品局（Food and Drug Administration）は、医療技術企業が新しい機器の承認を求める際に、SBOMを要求することを検討している。しかし、ほとんどの業界では、このアイデアはまだ初期段階にあり、リーダーたちは技術的な重荷がすべて経済的に意味をなすかどうか確信が持てていない。CISAの目標は、基本的にはSBOMの採用をできるだけ簡単にして、業界の計算を変えることにある。その狙いは、SBOMが業界内または業界間で同じように見えるように標準フォーマットを開発し、ソフトウェアサプライヤーが顧客と成分表を自動的に共有できるようなツールを開発することにあり、自由度を最小限として、できるだけ低コストで導入できるようにすることである。 連邦政府は、SBOM以外の取り組みとして、以下が検討されている。 ・連邦政府が使用するソフトウェアの設計強化を要求 ・ソフトウェアのバグをスキャンする自動化ツールの構築 ・製品にバグが発生した際に、技術企業がより良い対応ができるように支援する。	https://www.washingtonpost.com/politics/2022/01/26/an-ingredients-list-software-could-help-prevent-next-log4j/	
2022/1/27	Cyber Threat Modelling for Telco	通信事業者のためのサイバー脅威モデリング				1									1	サイバー脅威モデリング（CTM）と呼ばれる別のCTIの側面に焦点を当てている。CTIでは脅威の特定に使用できる可能性のあるデータオブジェクトの1つとして侵入の痕跡（IoC）が言及されることがある。 IoCは、マルウェアハッシュ、攻撃者のIPアドレス、悪意のあるURLなど、おおよそ脅威のシグネチャである。 IoCは把握、管理するための簡単な概念だが、CTIプラットフォームを使用して、実際の攻撃イベントの完全なチェーンを記述することもできる。つまり、CTIは、敵対的な行動のモデル化と共有の側面もカバーしている。 敵対行動のモデル化に最も広く使用されているフレームワークとして、マトリックスを使用して戦術（列）を実行し、目標を達成するために使用される一連の技法（行）を記述するMITRE ATT＆CK（敵対戦術、技法、および一般的な知識）がある。 MITRE ATT＆CKは、エンタープライズデバイスやモバイルデバイスなどのさまざまなテクノロジードメインに適用されており、そのドメイン内の既知の敵対行為の把握に対応するマトリックスが作成されている。 エンタープライズドメインとモバイルデバイスドメインにはATT＆CKマトリックスがあるが、テレコムネットワークにはない。Telcoドメインの場合、ATT＆CKマトリックスは役立つと考えている。	https://www.concordia-h2020.eu/blog-post/cyber-threat-modelling-for-telco/	HorizonプロジェクトCONCORDIAのブログに記載されている。MITER ATT＆CKの例が図示されいる。 MITRE　ATT＆CKl https://attack.mitre.org/
2022/1/28	The IoTAC Software Security Static Analysis Alerts Assessor	IoTAC ソフトウェアセキュリティ静的分析アラート評価器			1										1	セキュリティ関連の静的分析アラートの重要度を評価するための新しいメカニズムを提案した。 特に、（i）アラート自体、（ii）脆弱性の予測、（iii）ユーザーのフィードバックから取得した情報を考慮して、セキュリティ関連の静的分析アラートを重要度に基づいて分類および優先順位付けするための自己適応型手法であるセキュリティアラート重要度評価（SACA）を開発した。提案した手法は、実際のソフトウェアアプリケーションの静的分析レポートから取得したデータを使用して構築された機械学習モデル、特にニューラルネットワークに基づいている。 IoTACプロジェクトは下記によりIoTリファレンス・アーキテクチャに高レベルの保護を保証するとされている。 ・新しいアクセス制御メカニズム ・新しいセキュリティモジュールと手順を統合 ・セキュリティ要件、セキュリティ・フレームワーク、およびその評価プラットフォームを定義	https://iotac.eu/the-iotac-software-security-static-analysis-alerts-assessor/	EUが資金提供するH2020の研究およびイノベーションプロジェクト IoTACのホームページに掲載されたソフトウェアの静的分析に関する情報。 IoTACは産業界、学界、研究フォーラムの7か国からの13のパートナーで構成されている。 IoTAC : Security By Design IoT Development and Certificate Framework with Front-end Access Control https://isolate.norton.com/?url=https%3A%2F%2Fiotac.eu%2Fabout-us%2F

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			
2022/2/2	An In-Depth Look At The 23 High-Impact Vulnerabilities	影響力の大きい23の脆弱性を徹底解説												1		主要なIBV（Independent BIOS Developers）ソフトウェアの1つに、23の影響力の大きい脆弱性が発見された。これらの脆弱性は、単一のベンダーだけでなく、UEFIファームウェアソフトウェアにIBVのコードを採用したすべてのベンダーに影響を与える。Binarly社は、これらの脆弱性がすべて、主要な企業ベンダーのエコシステムのいくつかで発見されたことを確認した。影響を受けるベンダーの検証済みリストは、富士通、シーメンス、デル、HP、HPE、レノボ、マイクロソフト、インテル、Bull Atos。 中堅企業向けの試験的な取り組みにおいて、BinarlyチームはBinarly Platform Anomaly Checkerを使用して20台の異なる企業向けマシンでいくつかの繰り返し発生する異常を発見した。これらのアラートはすべて、富士通のLIFEBOOKラップトップシリーズに関連する類似のハードウェア構成によって引き起こされていた。これらの異常の性質を理解するために、分解コードを深く掘り下げると、これらの異常の大部分は、システム管理モード（SMM）において悪用可能な脆弱性であることが分かった。 この問題はCERT/CCに連絡され、CERT/CC チームは影響を受けたすべてのベンダー (DHS CISA が調整した複数の ICS ベンダを含む) に通知し、情報開示を行っている。脆弱性の漏えいのために(CERT/CCチームが開発した)VINCEプラットフォームは、実際の環境でテストされ、最初の開示から5ヶ月のスケジュールでのセキュリティ修正までの時間を大幅に短縮した(通常の単一ベンダー開示プロセスは6ヶ月以上かかる)。	https://www.binarly.io/posts/An_In_Depth_Look_at_the_23_High_Impact_Vulnerabilities/index.html	
2022/2/4	Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products	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	1	1				1								NISTは、標記ソフトウェア製品ラベリング推奨基準（最終版）をリリースした。 昨年5月12日に発表された大統領令EO14028の第4項では、NISTに対し、IoT機器のサイバーセキュリティ能力とソフトウェア開発手法について、一般消費者を教育するための取り組みを検討する際に既存の消費者向け製品のラベリングプログラムを考慮するよう指示しており、NISTはFTCやその他の機関と連携して以下の基準を定めるよう求められている。 ・消費者向けラベリングプログラムのためのIoTサイバーセキュリティの基準 ・消費者向けソフトウェアラベリングプログラムのための安全なソフトウェア開発の実践または基準。 NISTは、独自のプログラムを構築するのではなく、最低限の要求事項と望ましい属性の観点から、ラベリングプログラムの主要な要素を特定している。望ましい結果を特定することで、プロバイダーや顧客がそれぞれの機器や環境に最適なソリューションを選択できるようにしている。一つのサイズがすべてに適合するわけではなく、ラベルプロバイダーによって複数のソリューションが提供されるかもしれない。 これらの考え方に基づき、NISTは、昨年8月、IoT機器の潜在的なベースラインセキュリティ基準に関するホワイトペーパーを発表し、数度にわたるワークショップ開催とパブリックコメントに寄せられた意見を反映して、今回の最終版に至った。 大統領令の1年後に当たる2022年5月12日までに、NISTは、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ラベリングに関する総括報告書を発行する。この報告書では、こ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する。	https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/cybersecurity-labeling-consumers-internet-things https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf	
2022/2/8	Updated List of Critical and Emerging Technologie	重要・新興技術リストの更新	1									1				Whitehouse及び国務省は、重要なおよび新興技術の更新されたリストをリリースした。 米国政府、民間企業、そして同盟国やパートナーは、国家の安全保障、経済の繁栄、民主主義の価値を実現し守るために最も重要な技術を理解し、その開発と展開に注力し続けなければなりません。改定された最新リストでは、これらの重要・新興技術と幾つかの具体的なサブフィールドが示された。 重要技術・新興技術として以下が挙げられている。 - アドバンスト・コンピューティング　- 先端工学材料　- 先進のガスタービンエンジン技術　- 先進製造業 - 高度でネットワーク化されたセンシングとシグネチャ管理　- 先進原子力技術　- 人工知能 - 自律システム・ロボティクス　- バイオテクノロジー　- 通信・ネットワーク技術　- 指向性エネルギー - 金融技術　- ヒューマンマシンインタフェース　- ハイパーソニック　- ネットワーク化されたセンサーとセンシング - 量子情報技術　- 再生可能エネルギー発電・貯蔵　- 半導体・マイクロエレクトロニクス　- 宇宙技術・システム	https://www.whitehouse.gov/ostp/news-updates/2022/02/07/technologies-for-american-innovation-and-national-security/ https://www.state.gov/united-states-releases-updated-list-of-critical-and-emerging-technologies/ https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf	これらの技術リストにはIoTが具体的に示されていないが、対象分野のほとんどには、sensorsや部品にIoT含まれている可能性が高い分野となっている。

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			
2022/2/22	NIST Seeks Input to Update Cybersecurity Framework & Supply Chain Guidance	NIST、サイバーセキュリティの更新に向けた意見を募集中 フレームワークとサプライチェーンガイドライン	1	1				1								国立標準技術研究所(NIST)は、重要インフラサイバーセキュリティの改善のためのフレームワーク、サプライチェーンにおけるサイバーセキュリティの改善に関する情報を含む、様々な既存および潜在的な基準、ガイドライン、その他の情報を含むサイバーセキュリティリソースの評価と改善に役立つ情報を求めている。 NISTは、サイバーセキュリティのリスク、技術、リソースの変化する状況を説明するために、NISTサイバーセキュリティフレームワークの更新を検討しています。さらに、NISTは最近、サプライチェーンにおけるサイバーセキュリティリスクに対処するため、サプライチェーンにおけるサイバーセキュリティ改善のための国家イニシアチブ(NIICS)を立ち上げることを発表した。この幅広い官民パートナーシップは、テクノロジー開発者やプロバイダー向けのツールとガイダンスの特定と、そのような技術を取得する人のためのパフォーマンス指向のガイダンスに焦点を当てている。 NISTは、NIICSがどのように連携してサイバーセキュリティフレームワークと統合されるかなど、NIICSの方向性を知らせるために、セクター間のサプライチェーン関連のサイバーセキュリティニーズの特定と優先順位付けをサポートする情報を求めている。このRFIへの回答は、サイバーセキュリティフレームワークの改訂の可能性やNIICSイニシアチブに反映されることになる。	https://www.federalregister.gov/documents/2022/02/22/2022-03642/evaluating-and-improving-nist-cybersecurity-resources-the-cybersecurity-framework-and-cybersecurity https://www.nist.gov/news-events/news/2022/02/nist-seeks-input-update-cybersecurity-framework-supply-chain-guidance https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management	
2022/2/24	Joint Statement by Secretaries Raimondo and Mayorkas on Assessment of the Critical Supply Chains Supporting the Information and Communications Technology Industry	情報通信技術産業を支える重要なサプライチェーンの評価に関するライモンド長官とマヨルカス長官の共同声明	1									1				バイデン大統領の（E.O）14017による重要な6産業を支えるサプライチェーンのリスク耐性を強化するための政府全体のアプローチの一環として、商務省および国土安全保障省は、米国の情報通信技術（ICT）産業基盤の重要部門およびサブ部門のサプライチェーンについて、それぞれの省庁が定めた1年間の評価を実施した。 ●ICT製造の現状と課題：多くの製品の生産は、電子機器組立品とともに中国への集中が進んでいる。 ●ICTソフトウェア分野の現状とリスク：オープンソースソフトウェアのユビキタスな使用は、悪用されやすく、サプライチェーンのセキュリティを脅かす可能性がある。多くのOEMがファームウェア開発をサードパーティに委託し、プログラミングやサイバーセキュリティ基準の透明性の欠如に関連したリスクが発生している。 ●ICT人材の現状と関連リスク：ICT製造のアウトソーシングにより、国内のICT生産・製造の労働力は大幅に減少しているが、国内のソフトウェア開発者及びエンジニアリングの労働力は、今後も大幅に増加すると予想。しかし、両セグメントにおいて、有能な人材確保に苦労している。 ●米国ICT産業基盤に影響を与える横断的なサプライチェーンの脆弱性：ICTサプライチェーン全体の構造的脆弱性が、COVID-19パンデミックによる混乱の結果、より明白になった。ICT生産の多くのセグメントにおける国内エコシステムの欠如、単一ソースや単一地域のサプライヤーへの過度の依存、複雑なサプライチェーンによる製品の完全性維持の困難さなどが含まれる。 ●ICT産業基盤のサプライチェーンに対する外部リスク：ICT産業基盤のサプライチェーンの現状は、知的財産の盗難、経済的依存、脆弱な労働基準、気候への懸念に起因する様々な外部からのリスクに米国が過度にさらされていることを意味する。 レポートでは、これらの課題に対応するICTサプライチェーン・レジリエンス強化のため、以下を提言している。 ① 米国のICT製造基盤を活性化　②安全で透明性の高いサプライチェーンを通じた強靭性の構築　③サプライチェーンのセキュリティと回復力を向上させるための国際的なパートナーとの協働　④将来の ICT 技術に投資　⑤ICT人材のパイプラインを強化 ⑥6持続可能性が情報通信技術開発の要であることを確認　⑦業界のステークホルダーと連携した弾力的な取り組み ⑧ICT 産業基盤研究の継続	https://www.commerce.gov/news/press-releases/2022/02/joint-statement-secretaries-raimondo-and-mayorkas-assessment-critical https://www.dhs.gov/sites/default/files/2022-02/ICT%20Supply%20Chain%20Report_0.pdf	

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			
2022/2/24	Tackling Security Challenges in 5G Networks	5Gネットワークにおけるセキュリティの課題への取り組み								1						ENISAのレポートに関するニュース記事 ネットワーク機能の仮想化(NFV)は、5Gネットワークの新しい技術であり、柔軟性、スケーラビリティ、コスト、およびネットワーク管理の点で通信事業者にメリットをもたらす。ただし、この技術は新しいセキュリティの課題ももたらす。 発表されたレポートは、5Gツールボックスの実装、特にモバイルネットワークオペレーターがNFVのセキュリティグッドプラクティスに従うことを保証するためのEU加盟国への勧告で各国当局をサポートしている。 5Gネットワーク内のNFVに関連する課題、脆弱性、および攻撃を調査している。関連するセキュリティ制御を分析し、この非常に複雑で不均一で不安定な環境の特殊性を考慮に入れて、これらの課題とソリューションに対処するためのベストプラクティスを推奨している。 特定された60のセキュリティ上の課題から分類された課題の7つのカテゴリ 1. 仮想化またはコンテナ化 2. オーケストレーションと管理 3. 管理とアクセス制御 4. 新しいレガシーテクノロジー 5. オープンソースまたはCOTSの採用 6. サプライチェーン 　悪意のあるソフトウェアやハードウェア、偽造コンポーネント、不適切な 設計、製造プロセス、保守手順などのリスクをもたらすことにより、データや知的財産の盗難、5Gネットワークの整合性に対する信頼の喪失、システムやネットワークの障害を引き起こす悪用などの悪影響が生じる可能性がある。 7. 合法的傍受 レポートでは、技術、ポリシー、および組織のカテゴリに分類された合計55のベストプラクティスによる脆弱性、攻撃シナリオ、およびそれらが5G NFV資産に与える影響を説明している。	https://www.enisa.europa.eu/news/enisa-news/tackling-security-challenges-in-5g-networks	
2022/3/8	TLStorm	TLStorm			1										1	TLStorm : APC Smart-UPSデバイスに3つの重大な脆弱性が発見され、攻撃者は数百万台のエンタープライズデバイスの電源をリモートで操作することが可能になる。 Armisは、APC Smart-UPSデバイスに、遠隔地の攻撃者がSmart-UPSデバイスを乗っ取り、物理デバイスとIT資産の両方を標的とした過激な攻撃を行うことができる3つの重大な脆弱性のセットを発見した。 無停電電源装置（UPS）は、ミッションクリティカルな資産に緊急時のバックアップ電源を供給する装置で、データセンター、産業施設、病院などで見かけることができる。 APCはSchneider Electricの子会社であり、UPSデバイスの大手ベンダーの1社として、世界中で2,000万台以上のデバイスを販売しているま。TLStormと呼ばれるこの脆弱性が悪用されると、Smart-UPSデバイスを完全にリモートで乗っ取ることができ、極端なサイバーフィジカル攻撃を行うことが可能になる。Armisのデータによると、10社のうち約8社がTLStormの脆弱性にさらされている。 今回発見された脆弱性には、クラウド接続された Smart-UPS デバイスが使用する TLS 実装における 重大な脆弱性 2 件と、すべての Smart-UPS デバイスのファームウェアアップグレードが適切に署名および検証されていない設計上の欠陥の重大な脆弱性 1件が含まれている。	https://www.armis.com/research/tlstorm/	・CVE-2022-22806： TLS 認証バイパス。TLS ハンドシェイクにおける状態の混乱 が認証バイパスにつながり、ネットワークファームウェアのアップグレードを使用したリモート コード実行 (RCE) につながる可能性がある ・CVE-2022-22805： TLS バッファオーバーフロー。パケット再組み立てにおけるメモリ破壊のバグ (RCE) ・CVE-2022-0715： ネットワーク経由で更新可能な、署名されていないファームウェアのアップグ レード (RCE) ファームウェアのアップグレード機構の欠陥を悪用することは、APT攻撃の定番となりつつあり、組み込み機器のファームウェアへの不適切な署名は、様々な組み込みシステムで繰り返し見られる欠陥である。 Armisは 2021年10月31日にこれらの脆弱性をSchneider Electricに開示し、ArmisとSchneider Electricと協力してパッチの作成とテストを行い、現在、一般に公開している。

契約管理番号：	21500678-0