２０２０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

２０２１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

目次

まえがき

IoT は、Society 5.0[1]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、海外、特にアメリカ合衆国における 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・分析し、本プロジェクトの研究開発の国際連携を行い、研究開発成果の海外展開を達成するためのアメリカ合衆国のステークホルダーとの連携に関する活動案を提言した。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・分析を行い、新たに盛り込むべき目標水準の提言を行った。

---

[1] Society 5.0 とは、第 5 期科学技術基本計画（2016 年 1 月 22 日閣議決定）で提唱された概念であり、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（Society）のこと。

1　動向調査の成果と達成状況

和文要約

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。

このため、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。

本調査事業では、海外、特にアメリカ合衆国における 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・分析し、本プロジェクトの研究開発の国際連携を行い、研究開発成果の海外展開を達成するためのアメリカ合衆国のステークホルダーとの連携に関する活動案を提言することを目的とした。さらに、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・分析と新たに盛り込むべき目標水準の提言を行うことを目的とした。

英文要約

IoT is the fundamental technology of Society 5.0. Through the connection with cyberspace such as clouds via various networks and the collaboration with advanced knowledge processing and analysis processing as big data, IoT devices which are embedded in the physical spaces such as social

infrastructure, industrial system, living environment and natural environment, are expected to create various values added and services. They are also expected to bring great benefits to our economy society.

On the other hand, the scope of the targets of cyberattacks is rapidly expanding, and attack techniques are becoming more advanced. In addition, the risks of illegal programs being embedded, and programs being altered in an unauthorized manner during the processes of production and distribution of products and services, are becoming more prevalent within supply chains.

For this reason, for the purpose of protecting various IoT devices, and ensuring safety and security in society as a whole, we are engaging to develop and verify "Cyber Physical Security Infrastructure" which can be utilized to protect IoT system/services and large-scale supply chains including SMEs as a whole.

In the future, businesses, products, and services that do not meet a certain level of security requirements may be excluded from global procurement requirements, and it will be important to ensure that the manufacturing industry, which accounts for the majority of exports, has opportunities to enter the market.

The purpose of this research project is to investigate and analyze the standardization trends of systems and guidelines, the state of technology policy, and the latest technology trends in the industry regarding IoT security and supply chain security overseas, especially in the United States. We also propose activities for collaboration with U.S. stakeholders to achieve overseas deployment of R&D results. In addition, we will investigate and analyze the appropriateness of the international target level for the technologies to be developed in this project, and make recommendations for new target levels to be included.

2　動向調査の目的

「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、本プロジェクトと言う）においては、セキュアな Society5.0 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』の開発と実証に取り組んでいる。

本調査では、海外、特にアメリカ合衆国における 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、本プロジェクトの研究開発成果の国際連携を推進するにあたり、アメリカ合衆国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した。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・分析と新たに盛り込むべき目標水準の提言を目的とした。

3　事業概要

本調査事業では、本プロジェクトの研究開発成果の国際連携を推進するにあたり、アメリカ合衆国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ために、下記の①項の「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」と②項の「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」を実施した。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・分析と新たに盛り込むべき目標水準の提言のために、下記の③項の「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」と④項の「国際的な目標水準の妥当性評価」を実施した。以上の調査と評価の結果から、⑤項の「調査結果の分析と取りまとめ」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

海外、特にアメリカ合衆国において国立標準技術研究所（NIST[2]）等の公的機関が進める 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アメリカ合衆国に在住の有識者（以後、米国在住の有識者と略記）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章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章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と製品レベルについて文献調査等を行った。本報告の５章１節で報告する。

④国際的な目標水準の妥当性評価

本プロジェクト開発する技術の国際的な目標水準の妥当性を検証する方法として、上記③項で調査したプロジェクト・製品の特徴と、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章２節で報告する。

---

[2] https://www.nist.gov/about-nist
https://www.jetro.go.jp/ext_images/_Reports/02/2019/339d3d579a99af87/nyrp201901sp.pdf

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、特に合衆国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章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章３節で報告する。

4　海外における制度、標準、規制、技術などの動向

4.1　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

(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。

2019 年度調査のアメリカ合衆国の NIST（米国立標準技術研究所）と ENISA[3]（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、これらの関連情報が入手できる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、米国在住の有識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別表 A の一覧に集約し分析を行った。なお、調査対象機関の有識者へのヒアリングは COVID-19 への対処のため実施が困難となった。また調査対象の各種会合は参加者が会場に集まることなく Web 会議のみで開催される状況となった。このため有識者が集まる次の Web 会議に参加することによりその見解を調査した。

- ENISA Cybersecurity Certification of Cloud Services[4]（別表 A 2021/1/11）
- NIST Cybersecurity for IoT Draft Guidance: Rounding Up the Requirements[5]（別表 A 2021/1/26）

[3] https://www.enisa.europa.eu/about-enisa
[4] https://www.enisa.europa.eu/events/webinar-certification-of-cloud-services-in-europe
[5] https://www.nccoe.nist.gov/events/nist-cybersecurity-iot-draft-guidance-rounding-requirements

- Cybersecurity Standardization Conference 2021~European Standardization in support of the EU Cybersecurity Act [6]（別表 A 2021/2/3）
- U.S.-Japan Cooperation on High-Tech Supply Chain Security[7]（別表 A 2021/2/11）

[6] https://www.enisa.europa.eu/events/cybersecurity_standardisation_2021
[7] https://www.csis.org/events/us-japan-cooperation-high-tech-supply-chain-security

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／アメリカ合衆国国土安全保障省	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 年発足のアメリカ合衆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 が後援する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ヨーロッパ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	ヨーロッパ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 Institute 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。

(2) 調査結果

調査対象組織の 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主要な情報を調査し時系列順に整理し別表 A に示す一覧表を作成した。一覧表には、米国在住の有識者から提供された IoT セキュリティとサプライチェーンに関連する情報を含めている。この情報を分析して、以下に述べるアメリカ合衆国とヨーロッパの動向を調査した。

A) アメリカ合衆国の動向

A-1. NIST CYBERSECURITY FOR IOT PROGRAM

NIST （The National Institute of Standards and Technology：米国立標準技術研究所）の Cybersecurity for IoT Program[8] （以下 NIST IoT Program と略記）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」を行っている。

NIST は第一次世界大戦前夜、英国の覇権に対しドイツの台頭という情勢下、この二大国にアメリカの産業力を追いつかせるよう産業力強化を目的に、1901 年にアメリカで最も古い物理科学研究所として発足した。現在 NIST は商務省の傘下組織として、首都ワシントンに程近い Gaithersburg, Maryland、並びに Boulder, Colorado に大規模なキャンパスを有し[9]、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[10]。このうち、情報技術研究並びに標準化を行う Information Technology Laboratory[11]（以下 ITL と略記）が、NIST IoT Program 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[12]（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[13]（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。これらの文書と NIST IoT Program の関係、NIST 文書の制定のプロセス及び他

[8] https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program>
[9] https://www.nist.gov/about-nist/visit>
[10] https://www.nist.gov/about-nist/our-organization>
[11] https://www.nist.gov/itl
[12] https://csrc.nist.gov/publications/detail/fips/200/final
[13] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

の機関への働きかけなどについては次節 4.2 で述べる。

NIST IoT Program は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っている。感染症流行前の 2020 年 2 月までは一般を交えた会合が、San Francisco で開催の RSA Conference と同時期に現地で開催され、また夏季には NIST Gaithersburg 本部キャンパスで会合が開催されてきた。感染症拡大後の 2020 年 3 月以降はオンラインで一般も参加できる会合が開催されている。

A-2. NIST SP 800-53 Revision 5

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）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である。セキュリティ要求事項及びプライバシー要求事項を適用することにより、連邦政府のセキュリティ管理とプライバシー管理を行う。

本文書は 7 年ぶりに改訂され、2020 年 9 月 23 日に最終版が公開されて、2020 年 12 月 10 日に正誤表付きで関連付属文書と共に更新版の NIST SP 800-53 Revision 5（以下 NIST SP 800-53r5 と略記）が公開された。

NIST SP 800-53r5 における大きな更新は、FIPS 200 の定める 17 のセキュリティ要件の Control 群に加え、FIPS 200 以降に連邦政府の義務として”Program Management”、“PII Processing and Transparency”、”Supply Chain Risk Management”の三つの Control 群が追加された点である。IoT Program はこの最新版 NIST SP 800-53r5 に準拠している。

A-3. NISTIR 8259 シリーズ

NISTIR 8259[14]は、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を示す。これらの基礎的なサイバーセキュリティ活動は、顧客が必要とするサイバーセキュリティ関連の取り組みを製造業者が軽減するのに役立ち、IoT デバイスの侵害や、侵害されたデバイスを使って実行される攻撃の蔓延と深刻さを軽減することができる。

2020 年 5 月に発行された NISTIR 8259、並びに NISTIR 8259A[15]と併せて制定された関係文書及び現在意見集約中のドラフト文書の動向と最新の状況を NIST IoT Program の活動と

[14] https://csrc.nist.gov/publications/detail/nistir/8259/final
[15] https://csrc.nist.gov/publications/detail/nistir/8259a/final

合せて示す。

2020 年 12 月 15 日、NIST IoT Program 責任者 Katerina Megas 氏より、新規ドラフトのコメント募集に合わせ、かなり具体的な現状が blog で発表されている[16]。これを見ることにより、2020 年 3 月以降の経緯を把握することができる。基本的には、2020 年 2 月末に RSA Conference 2020 にあわせてサンフランシスコ市内で開催された NIST IoT Roundtable（以下 Roundtable と略記）での議論や発表の方向で制定の作業が進んでいる。

- Roundtable で触れられた NISTIR 8259:Foundational Cybersecurity Activities for IoT Device Manufacturers、並びに NISTIR 8259A: Technical Core Baseline は、Roundtable での説明にあった通り、2020 年 5 月 29 日に最終版として確定した[17]。この最終版確定の後、Katerina Megas 氏が 6 月 1 日付で両文書について blog で説明している[18]。
- 6 月 30 日に Foundational Cybersecurity Guidance for IoT Device Manufacturers: NISTIR 8259 Overview[19]としてオンラインのイベント[20]が開催され、解説と質疑応答を実施。IoT デバイスメーカーと産業用、及び家庭用 IoT デバイスの全てのユーザの参加を奨励している。
- 7 月 23 日と 24 日にはオンラインのワークショップ Building the Federal Profile For IoT Device Cybersecurity: Next Steps for Securing Federal Systems[21]が開催された。本ワークショップの報告は 2021 年 1 月 7 日発行 NISTIR 8322 : Workshop Summary Report for “Building the Federal Profile For IoT Device Cybersecurity” Virtual Workshop[22]として公開されている。
  - ワークショップは、会期中の各日 2 時間ずつオンラインで開催された。
  - 参加者は 500 名規模で、26 カ国とアメリカ国内 39 州からの参加があった。このうちアメリカ国外政府から 5 件、アメリカ国内の州政府から 8 件の参加が確認されている。
  - 基調講演を行った Grand Schneider, Federal Chief Information Security Officer (CISO)

---

16 https://www.nist.gov/blogs/cybersecurity-insights/rounding-your-iot-security-requirements-draft-nist-guidance-federal
17 https://csrc.nist.gov/publications/detail/nistir/8259/final
18 https://www.nist.gov/blogs/cybersecurity-insights/more-just-milestone-botnet-roadmap-towards-more-securable-iot-devices
19 https://www.nist.gov/news-events/events/2020/06/foundational-cybersecurity-guidance-iot-device-manufacturers-nistir-8259
20 https://www.nist.gov/news-events/events/2020/06/foundational-cybersecurity-guidance-iot-device-manufacturers-nistir-8259
21 https://www.nist.gov/news-events/events/2020/07/building-federal-profile-iot-device-cybersecurity-next-steps-securing
22 https://csrc.nist.gov/publications/detail/nistir/8322/final

は、消費者と組織の両方において、IoT セキュリティは十分に注意を払われていないとし、あらゆるタイプのシステムの相互接続が増加していることで、攻撃の対象が増加し、脅威が拡大していると指摘している。また、IoT デバイスは、サプライチェーンのセキュリティとリスク管理に関するより広範な懸念の構成要素であり、政府の行政府と立法府の両方の主要な焦点となっていると指摘している。

- パネルディスカッションで、連邦の IoT 機器のセキュリティ上の課題について論じられた。パネリストには国防総省サイバーセキュリティポリシー及び実装の責任者、ENISA の Apostolos Malatras 氏、英国から Peter Stephens, Head of Secure by Design, Cyber Security for the Internet of Things (UK) が含まれている。

- NISTIR 8322 には参加者の意見や観察など主観的ではあるが興味や関心事、当日の議論の雰囲気はある程度把握できる下記に示すような 13 件の Takeaway が記されている。Takeaway は参加者から聞いたアイデアで参加者やパネリストから大きな支持を得たものとされている。

  ［Takeaway 4］コミュニティは、IoT のための「国際的な信頼できる市場」の必要性を認識している。しかし、市場の力だけでは、それを実現するための十分なインセンティブは得られないだろう。
  ワークショップで問われた意見照会に対する回答では、71%の参加者が IoT Security 強化に対する政府による義務化に強い支持を示した。また、55%の参加者は IoT デバイスの開発者が製品を安全にするための適切なインセンティブの不足を指摘した。参加者は、IoT デバイス市場全体をサイバーセキュリティ強化の方向にシフトさせる経済的インセンティブを生み出すために、規制指導、顧客教育、サプライチェーンからの圧力などを組み合わせることを支持した。またインセンティブの目的は顧客が自信を持って IoT デバイスを調達できるような、信頼できる IoT デバイスの国際的な市場の発展を促すことである。

  ［Takeaway 12］IoT 機器のサプライチェーンは、セキュリティリスクの原因であると同時に改善のための機会である。
  現在の IoT サプライチェーンの複雑さと不透明さは、悪質な行為者がデバイスのサイバーセキュリティに悪影響を与えることと、購入者がそのサプライチェーンから出てきた特定の製品の特性に信頼を寄せることができないことへの懸念を引き起こしている。ENISA の Apostolos Malatras[23]氏は、他の製造業と比較して、「サプライチェーン内のピア間のサプライヤとプロバイダ間の

[23] Network and Information Security Expert, European Union Agency for Cybersecurity (ENISA)

関係は全く成熟していない。そして、それらは非常に頻繁に変化している」と ENISA は見ていると指摘。しかし、サプライチェーンについて収集した情報を共有する機会もあり、一部の組織では、サプライチェーンをサイバーセキュリティの取り組みをより効果的に集中させる場所として重視している。また、第三者による評価や認証、リコール手続きを必要とする規制など、他のメカニズムがサプライチェーンを通じた IoT デバイスのサイバーセキュリティに良い影響を与える可能性もある。

- 5 月の Roundtable で NIST が次の課題として言及していた Federal Profile は、NISTIR 8259D (Draft): Federal Profile[24]として文書化された。この結果、現在の NISTIR 8259 の構成は、NISTIR8259 本文を含む次の文書群から構成されている。

  - 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している。この基礎的なサイバーセキュリティ活動は、顧客が必要とするサイバーセキュリティ関連の製造業者の取り組みを軽減するのに役立ち IoT デバイスの侵害や侵害されたデバイスを使って実行される攻撃の蔓延と深刻さを軽減することができる。

  - NISTIR 8259A: Technical 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・サイバーセキュリティ能力を特定するための出発点を提供している。

  - NISTIR 8259B (Draft): Non-Technical Core Baseline[25]

    より安全なデバイスの構築の出発点として、6 つの基本的な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する。メーカーや関連する第三者からの通常必要とされる技術的ではないサポート活動を詳述している。NISTIR 8258A 及び NISTIR 8259B は補完的なペアであり、技術的及び非技術的な要件の取り扱いにバランスをとっている。

  - NISTIR 8259C (Draft): Profile Development Process[26]

    NISTIR 8259A および 8259B に用意されているコアベースラインから始まるあらゆ

[24] https://csrc.nist.gov/publications/detail/nistir/8259d/draft
[25] https://csrc.nist.gov/publications/detail/nistir/8259b/draft
[26] https://csrc.nist.gov/publications/detail/nistir/8259c/draft

る組織が使用できるプロセスを説明し、これらのベースラインを組織またはアプリケーション固有の要件（業界標準、規制ガイダンスなど)と統合して、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している。

・ NISTIR 8259D (Draft): Federal Profile[27]

連邦政府のユースケースのための最小限の安全性の基準の例として NIST SP800-53B に記述されている FISMA 低ベースラインに対して調整された NISTIR 8259A と NISTIR 8259B のコアベースラインのデバイス中心のサイバーセキュリティ指向のプロファイルを提供している。

- 上記 NISTIR 8259 B (Drafts)、NISTIR 8259 C (Drafts)、NISTIR 8259D (Drafts)は、2020 年 12 月 15 日に公開され、2021 年 2 月 12 日まで一般からコメントを受け付けると発表された。その後、2021 年 2 月 8 日にコメント期間が 2021 年 2 月 26 日まで延長されることになった。また、2021 年 2 月 24 日には NIST の blog にコメント送付のリマインダの通知と併せてコメントが紹介されている[28]。

- 同じく 2020 年 12 月 15 日に NIST SP 800-213 (Draft)：IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements[29]が公開された。本ドラフトには、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。これにより、連邦政府機関が IoT デバイスとその製造元、及び/または第三者に対してそれぞれ期待する能力とアクションである IoT デバイスのサイバーセキュリティ要件を特定することができる。本ドラフトのコメント期間はNISTIR 8259 B (Drafts)、NISTIR 8259 C (Drafts)、NISTIR 8259D (Drafts)と同じに設定されている。

A-4. ICT Supply Chain Risk Management Task Force

DHS（United States Department of Homeland Security[30]：アメリカ合衆国国土安全保障省）の管理下にある CISA（CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY[31]：サ

[27] https://csrc.nist.gov/publications/detail/nistir/8259d/draft
[28] https://www.nist.gov/blogs/cybersecurity-insights/theres-still-time-comment-iot-cybersecurity-guidance-send-us-your
[29] https://csrc.nist.gov/publications/detail/sp/800-213/draft>
[30] https://www.dhs.gov/
[31] https://www.cisa.gov/

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）と ICT Supply Chain Risk Management Task Force[32]の政府及び業界メンバーは 2020 年 12 月 17 日サプライチェーンのセキュリティと、発生したインシデントを沈静化して本来の状態回復への対応能力や手法（レジリエンス）に関する有意義なパートナーシップと分析を推進するための進捗状況についての年次報告書を発表した。本報告書は、ICT Supply Chain Risk Management（以下 SCRM と略記）の Task Force の 1 年目の作業を基に作成されており、情報共有、脅威分析、適格入札者リストと適格製造者リスト、ベンダー保証の課題に対処するために、タスクフォース内の進行中の取り組みをまとめて紹介している。

また、CISA が主催する ICT SCRM Task Force の会合が 2020 年 12 月 18 日にオンラインで開催された[33]。会議は ICT サプライチェーンに関する様々なトピックについて、情報技術・通信部門や連邦政府機関リーダー、専門家、様々な組織の代表者から話を聞き、実用的な ICT サプライチェーンリスク管理情報、ユースケース、ベストプラクティス、教訓などを学ぶことができる。

さらに、2021 年 2 月 4 日、同 Task Force の活動期間が 6 ヶ月延長され、2021 年 7 月まで活動が継続されることが発表された[34]。この延長により、ワーキンググループは、最新の脅威シナリオレポートやその他の次期製品のリリースを含め、2 年目の報告書で概説された作業を継続する。また、ICT サプライチェーンに更なるレジリエンスを構築するための推奨事項の運用を可能にし、政府と産業界のメンバーが、サプライチェーンに関する他の進行中の官民連携の取り組みに協力し続けるとされている。

A-5. アメリカ合衆国政府の動向

2020 年 12 月 20 日、DHS（国土安全保障省）は米国企業に対し、中華人民共和国に関連する企業からのデータサービスや機器の使用に関連するリスクを警告するビジネスアドバイザリー（勧告）を発行した。本勧告では、新たに制定された中国の法律により、学術機関、研究サービスプロバイダー、投資家を含む中国の企業や市民に、米国及び国際法や政策の原則に反するデータの収集、送信、保存に関連する行動を強制することができるため、中国政府が支援するデータ盗難のリスクが持続しかつ増大していることに注目と述べている。このような活動には、企業に中国の国境内でのデータ保管を要求したり、国家安全保障を装って日常的なデータを中国政府に引き渡したりすることが含まれる。中国関連企業からデータサービスや機器を調達したり、そのような企業が開発したソフトウェアや機器にデータ

[32] https://www.cisa.gov/ict-scrm-task-force
[33] https://www.cisa.gov/ict-scrm-task-force-events
[34] https://www.cisa.gov/ict-scrm-task-force

を保存したりすることを選択する個人や事業体は、これらの企業との取引に関連する経済的、評判、場合によっては法的なリスクを認識しておく必要がある。

2021 年 1 月 26 日にバイデン政権は、連邦政府の CISO 最高情報セキュリティ責任者にクリス・デルーシャ（Chris DeRusha）を選出したとの報道があった[35]。同氏はホワイトハウス、DHS、フォード・モーター・カンパニーでのサイバーセキュリティ・アドバイザーとしての経歴を有し、連邦、州、民間企業のサイバーセキュリティの経験を、連邦政府機関や国内最大級のハイテク企業に対する国家レベルのハッカーによるシステム侵害の疑いに対処する。

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に対処するための行政命令に大統領が署名すると発表[36]。2 月 24 日には、バイデン大統領はコンピュータチップ、医療機器、電気自動車用バッテリー、レアメタルなどの重要品目の米国サプライチェーンにおける潜在的な脆弱性について、100 日間の政府のレビューを命じる大統領令に署名した[37]。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。

さらに米国のパートナーや同盟国と協力して、強力で弾力性のあるサプライチェーンを確保するよう政権に指示している。当該大統領令の実施について総括責任者は国家安全保障補佐官、並びに経済政策担当補佐官とされ、経済政策であると同時に国家安全保障政策でとなっている。

なお、レビュー結果の扱いについては明らかになっていないが、公開される場合は 100 日レビューの報告は 2121 年夏季から秋季、１年レビューの報告は 2022 年前半に行われると期待される。

B)　ヨーロッパの動向

B-1. ENISA

EU（European Union：欧州連合）においては、その専門機関である European Union Agency

---

35 https://www.nextgov.com/cybersecurity/2021/01/bidens-federal-chief-information-security-officer-brings-public-and-private-sector-experience/171627/

36 https://thehill.com/policy/technology/538474-biden-to-sign-executive-order-addressing-chip-supply-chain-shortage

37 https://www.whitehouse.gov/briefing-room/statements-releases/2021/02/24/fact-sheet-securing-americas-critical-supply-chains/

for Cybersecurity（以後 ENISA と略記）がネットワークセキュリティと情報セキュリティに関する活動を一元的に担っている。2019 年の EU の The EU Cybersecurity Act[38]（EU サイバーセキュリティ法）によって、ENISA を刷新・強化し、デジタル製品、サービス、プロセスに対する EU 全体のサイバーセキュリティ認証フレームワークを確立するとされた。ENISA は、特定の認証スキームのための技術的基盤を準備し、専用のウェブサイトを通じて認証スキームや発行された証明書を一般に知らせることで、欧州のサイバーセキュリティ認証の枠組みを設定し、維持する上で重要な役割を果たしている。また、ENISA には、EU レベルでの運用協力を強化し、サイバーセキュリティインシデントへの対応を要請する EU 加盟国を支援し、国境を越えた大規模なサイバー攻撃や危機が発生した場合には EU の調整をサポートすることが義務付けられている。

- 4th IoT Security Conference[39]

ENISA は例年 Europol[40]と共催し、IoT Security Conference を開催している。

2020 年の IoT Security Conference は CERT-EU[41]も共催に加わり、感染症の影響で 10 月に 3 日間に渡りオンラインで実施された。この会議は、サイバー犯罪部門、CSIRT、国際機関、民間企業、規制機関、学界の専門家が一堂に会することで、幅広い議論を可能にすることを目的としており、次の３つのセッションが開催された。

- Operational IoT　（2020 年 10 月 7 日）
  現在の IoT セキュリティの課題とその原因、IoT インフラと関連プロジェクトのセキュリティ確保のための取り組み、そして規制の側面と認証スキームについて議論。このセッションでは、トピックの主要なポイントを紹介するとともに、参加者との交流を図り、IoT サイバーセキュリティの確保に役立つ運用やサービスについての議論を活発にすることを目的とした。

- Artificial Intelligence　（2020 年 10 月 14 日）
  AI は本質的に両用技術であり、社会に莫大な利益をもたらす一方で、デジタル、物理的、政治的な様々な脅威を引き起こす。犯罪者は AI を活用して攻撃を容易にし、それを改善することができる一方で、犯罪捜査の遂行において法執行機関が直面している課題の解決の一部にもなりうる。潜在的なリスクや新たな脅威と、犯罪捜査の効率化や有効性を高めるという法執行の観点からのメリットを振り返りながら、総合的な視点から AI について議論する。

---

[38] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act
https://eur-lex.europa.eu/eli/reg/2019/881/oj
[39] https://www.enisa.europa.eu/events/4th-iot-securiity-conference-online-series
[40] https://www.europol.europa.eu/
[41] https://cert.europa.eu/cert/plainedition/en/cert_about.html

・ Supply Chain for IoT （2020 年 10 月 21 日）
IoT 開発者がサードパーティ製のコンポーネントを利用することはよくあるが、これらのサードパーティ製コンポーネントはブラックボックスとして扱われることが多い。IoT エコシステム全体で安全なサプライチェーンを確立することは、IoT セキュリティの基本的な構成要素である。製品開発から製品消費に至るまでのさまざまなフェーズに焦点を当て、関連する脅威、リスク、緩和手法について、IoT サプライチェーンに関する幅広い議論を行うことを目的とする。

- Guidelines for Securing the IoT – Secure Supply Chain for IoT[42]
2020 年 11 月 9 日に、初期設計、半導体のファブリケーション、組み込みソフトを含む一連の製造工程上の注意並びにサプライチェーンへの脅威などを示すガイドラインとして Guidelines for Securing the IoT – Secure Supply Chain for IoT を発行。
この報告書は、ハードウェア、ソフトウェア、サービスを含むモノのインターネット（IoT）のサプライチェーン全体を対象としており、IoT 製品の開発に使用されるサプライチェーンの実際のプロセスを対象とした 2019 年版「Good Practices for Security of IoT - Secure Software Development Lifecycle」をベースにしている。報告書は、IoT セキュリティのリファレンス・ポイントとしての役割を果たすことを目的に数多く引用され、参照されている IoT のベースライン・セキュリティ勧告に関する ENISA の研究を補完するものとなっている。

- Cybersecurity Standardization Conference 2021~ European Standardization in support of the EU Cybersecurity Act [43]

例年開催されている Cybersecurity Standardization Conference が、2021 年 2 月 2 日から 4 日にかけて ENISA、CEN[44]、CENELEC[45]、ETSI[46]の共催で開催された。当初、会場並びに online 併設での開催が計画されていたが、全面オンラインで開催されることになった。

・ 会期 2 日目の 2 月 3 日に、Future Schemes Consumer IoT と題した会合が設定され、ETSI 含め登壇者による発表などが実施された。会期全体を通じて扱われた議題は下記の通り。

  - Panel 1: Cybersecurity and Radio Equipment Directive – setting up the scene and future

---

[42] https://www.enisa.europa.eu/news/enisa-news/iot-security-enisa-publishes-guidelines-on-securing-the-iot-supply-chain
https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

[43] https://www.enisa.europa.eu/events/cybersecurity_standardisation_2021
https://www.enisa.europa.eu/events/cybersecurity_standardisation_2021/std-2021-presentations

[44] https://www.cen.eu/about/Pages/default.aspx

[45] https://www.cenelec.eu/aboutcenelec/whoweare/index.html

[46] https://www.etsi.org/

work

- Panel 2: Cybersecurity and Radio Equipment Directive – implementing measures
- Panel 3: Standardization supporting the Cybersecurity Act
- Panel 4: Future schemes: Consumer IoT
- Panel 5: Future schemes: 5G
- Panel 6: Vision of the future

・ 会議では、EU IoT Certification Scheme が作られることが参加者、最低でも発表者では既に前提とされている雰囲気で、将来欧州が制定しうる関連新規法制への対応などにも関心が示された。

・ 議論の焦点は IoT の中でも消費者向け IoT が主体であり、appliance 並びに家の空調などの家電を含む。また Security と Privacy が中心となっているが、resilience と safety にも関心が寄せられている。

・ ETSI EN 303 645 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements[47]

Rapporteur を務める英国 DCMS（Department for Digital, Culture, Media and Sport[48]：デジタル・文化・メディア・スポーツ省)の Jasper Pandza 氏が ETSI EN 303 645 の概要を発表。文書自体は EN （European Standard）るが、世界中への適用、あるいは事実上の世界標準としたい意向が見えた。

ETSI EN 303 645 の目的は、現在のセキュリティ無法無為状態から、good な状態へ向上させることであり、better や best を目的とはしてない。ETSI EN 303 645 の作成中までに把握できた IoT に関わる攻撃や脅威ほぼ網羅できたと説明。実装として、ベンダーは内容を理解し、33 要件の全てを対象となる Consumer IoT に実装しなければならない。更にベンダーは推奨の 35 件の全ての実装に最大限の努力が求められる。35 件の推奨のうち、実装できなかったものにはその理由を記録文書化の必要がある。

更にガイダンスとして、2021 年第二四半期 ETSI TR 103 621 並びに TS 103 701 の承認、確定が予定されている。ETSI で 4 月の承認を予定している模様である。

- TR 103 621 : CYBER Guide to Cyber Security for Consumer Internet of

[47] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
[48] https://www.gov.uk/government/organisations/department-for-digital-culture-media-sport

Things[49]

Status: Stable draft (2020-12-13), Final draft for approval

- TS 103 701 : CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements[50]

  Status: Stable draft (2020-12-13), Final draft for approval

欧州域内ではドイツ BSI（Bundesamt für Sicherheit in der Informationstechnik：情報セキュリティ庁[51]）が SESIP という Consumer IoT へのラベリングを目的としたプログラムで ETSI EN 303 645 を適用。

・ 欧州家電産業界

一連の政府系機関の動向に対し、欧州家電産業界は、必要性を認めながらもビジネスの円滑な実施に政府側の配慮を期待しており、以下の要望があった。

- 将来計画される IoT Certification Scheme においては、欧州全体で一つとし、国毎の異なる規制を外す
- No reinventing the wheel（広く受け入れられ確立されている技術や解決法の作り直しをしない）
- 国際標準に準拠
- IoT Certification scheme は強制ではなく自発とする
- 近く制定が見込まれる新法制類との整合性
- 政府の一連のこれらの動きに対し、産業界を含めること、並びに透明性の確保

● EU Certification Scheme (EUCS)

EU サイバーセキュリティ法により ENISA に求められている EU 全体のサイバーセキュリティ認証フレームワークを確立するための認証スキームの最初のものとして、EUCS-Cloud Services Scheme Draft[52]が 2020 年 12 月 22 日に一般公開され、2021 年 2 月 7 日までの Public Consultation に付された。また、2021 年 2 月 3 日には EUCS for 5G の作成開始が発表[53]されている。

B-2. ETSI

ETSI(European Telecommunications Standards Institute：欧州電気通信標準化機構）はヨーロ

---

[49] https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=59473
[50] https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58434
[51] https://www.bsi.bund.de/DE/Home/home_node.html
[52] https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme
[53] https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification

ッパ圏の電気通信における標準仕様を策定するために設立された標準化団体であり、各国における、電気通信を管理する官公庁や電気通信事業者、メーカー、研究機関などから構成されている。

ETSI の Technical Committee on Cybersecurity (TC CYBER)が作成してきた、ETSI EN 303 645, CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements（消費者向け IoT のためのサイバーセキュリティ：ベースライン要件）の最終版が 2020 年 6 月 30 日に公開された[54]。発表によると、Test Specification、並びに Implementation guide が関連文書として公開される。後日開催された Cybersecurity Standardization Conference 2021 での英国 DCMS の Jasper Pandza の発表において、これらの文書が次の 2 件に該当することが示されている。

- TR 103 621：CYBER Guide to Cyber Security for Consumer Internet of Things
  Status: Stable draft (2020-12-13), Final draft for approval
- TS 103 701：CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements
  Status: Stable draft (2020-12-13), Final draft for approval

また、関係文書として次が存在している。

- DTS/CYBER-0014 (TS 103 486) Identity Management and Discovery for IoT55
  Status: Early draft (2020-10-27), Final draft for approval

B-3. 欧州業界の動向

IoT 産業界においては過去にセキュリティ上問題のある製品を欧州全体に販売し、事件や被害が発生している[56]。いくつかは明確に法に違反しているにも関わらず、積極的に対処対応ができず、政策当局の介入を招いていた。このため IoT 産業界は「運用、実践可能な」法規制や標準の導入を働きかけており、例えば ETSI EN 303 645 の策定の過程では、ETSI 会員企業からの議論の参加や貢献が行われてきていると考えられる。

上記 B-1 項で報告した Cybersecurity Standardization Conference 2021 における欧州家電業界からの発言は規制の必要性は議論の余地がないことを認めつつ、規制を行う場合には産業界が実施可能な規制、標準を期待することが語られている。また、政策や標準の立案過程の透明化あるいは産業界の参加の要望も示されているが、EU の標準化団体の ETSI、CEN（European Committee for Standardization：欧州標準化委員会）、CENELEC（European Committee

[54] https://www.etsi.org/newsroom/press-releases/1789-2020-06-etsi-releases-worldleading-consumer-iot-security-standard
[55] https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=47653
[56] https://www.nedo.go.jp/content/100904087.pdf

for Electrotechnical Standardization：欧州電気標準化委員会）は民間企業が参加可能であり、ENISA は主要な規則で Public Comments を招集するなどの対策が既にとられていることから、今までの方法が維持されることへの確認と捉えられる。

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が参加しているは業界団体である GSM Association[57]（以後、GSMA と略記）は 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い、3GPP を通じて ETSI への提案活動を行っている。ベンダーの開発工程、製品のライフサイクルプロセスに対するセキュリティ監査、テストラボの認証、ネットワーク機器のセキュリティ評価の手順を規定する文書 NESAS（Network Equipment Security Assurance Scheme[58]）の初版を 2019 年 10 月 7 日に公開している。2020 年 7 月 20 日と 2021 年 2 月 5 日に改訂が行われ、現在公開されている第 2 版[59]ではオープンソースソフトの扱い、サードパーティコンポーネントのセキュリティ要件を追加し、要求事項の再グループ化が行われた。

4.2 海外における制度や標準のとりまとめプロセス

(1) 調査方針

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

調査対象組織については、上記 4.1 節の組織を候補として、今回の動向調査で取りまとめの活動が進展し、そのプロセスが確認できるものを分析の対象とした。今回の動向調査で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。

---

[57] https://www.gsma.com/aboutus/
[58] https://www.gsma.com/security/network-equipment-security-assurance-scheme/
[59] https://www.gsma.com/security/wp-content/uploads/2021/02/FS.16-NESAS-Development-and-Lifecycle-Security-Requirements-v2.0.pdf

(2) 調査結果

A) アメリカ合衆国における制度や標準のとりまとめプロセス

A-1. NIST のガイドライン・標準策定プロセス

米国立標準技術研究所（NIST）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[60]）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[61]。NIST 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[62]）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[63]、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[64]。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。図 1 と図 2 に NIST 発行の文書種類と、FIPS の発行のプロセスを示す。

60 https://www.govinfo.gov/content/pkg/PLAW-104publ113/pdf/PLAW-104publ113.pdf
61 https://www.nist.gov/itl/standards-activities
62 https://www.epa.gov/laws-regulations/summary-administrative-procedure-act
63 https://www.nist.gov/itl/procedures-developing-fips-federal-information-processing-standards-publications
64 https://www.wiley.law/alert-3496#_ftn23

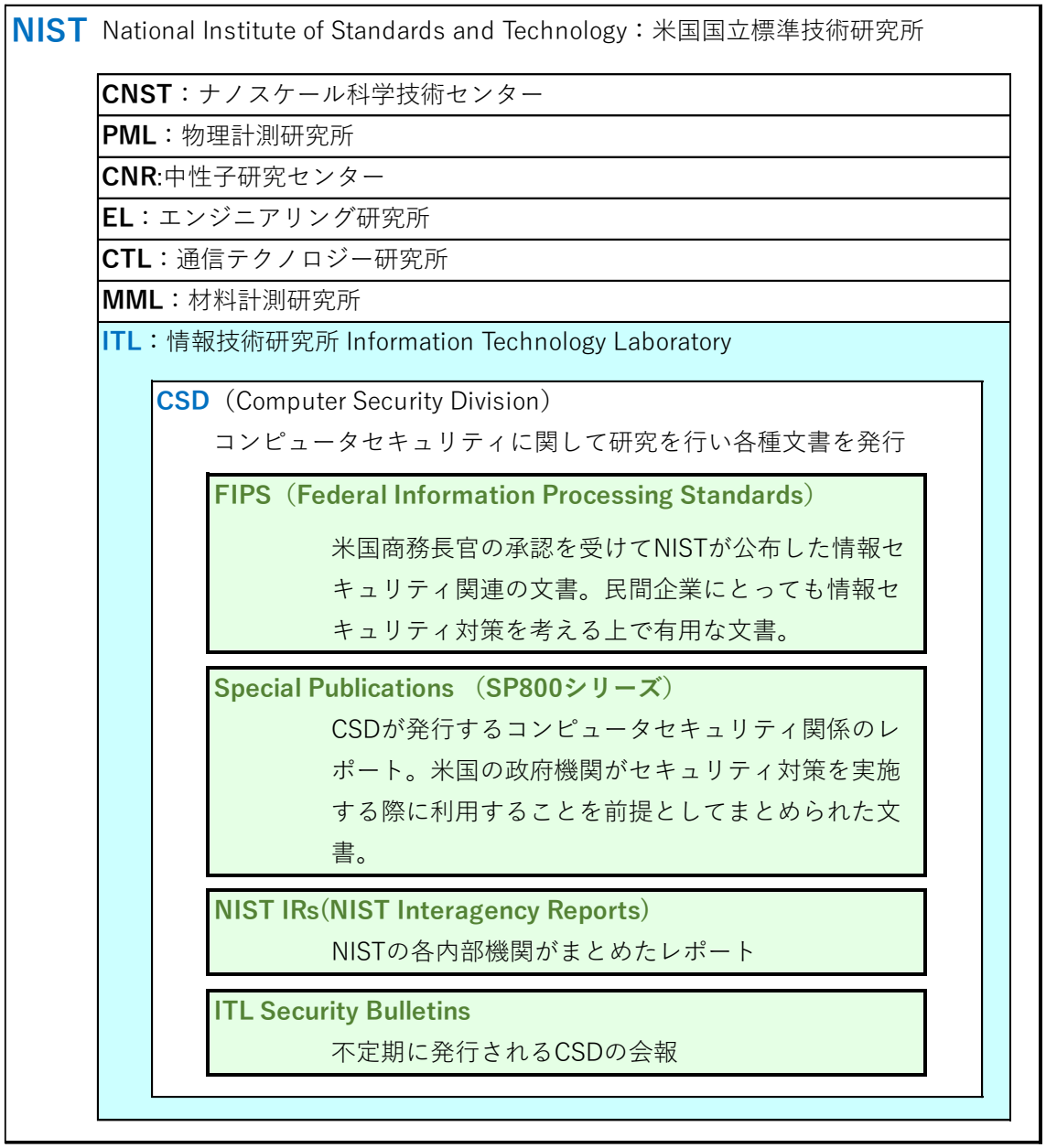

図 1 NIST 発行の文書種類

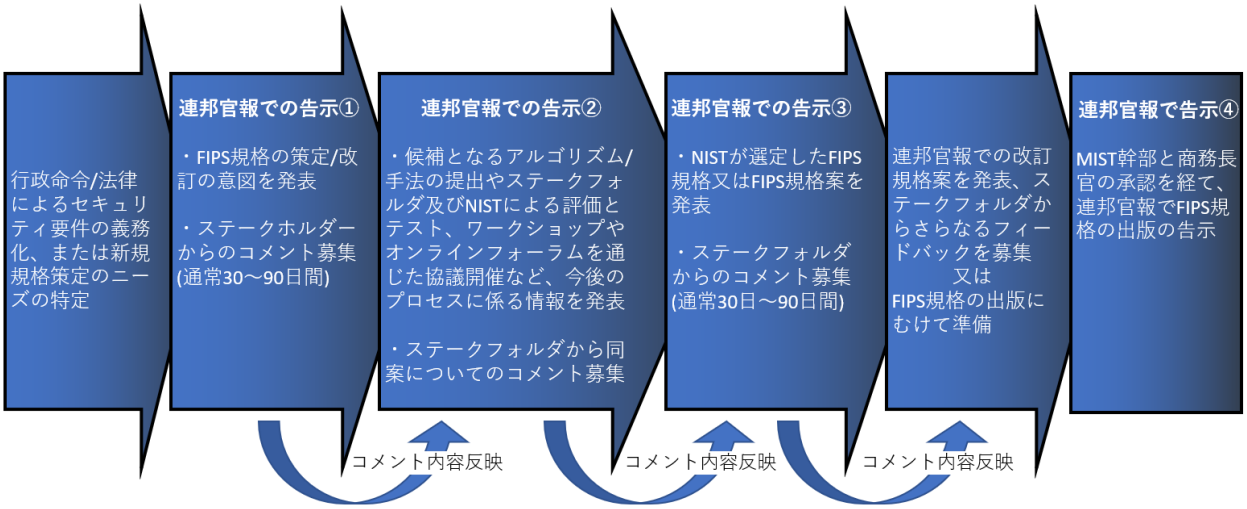

図 2 FIPS の発行プロセス NIST 資料[65]を基に作成

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

2020 年から 2021 年にかけて NIST IoT Program が制定を進めている NISTIR 8259 の文書類の制定手続きの進展が見られた。NISTIR 8259 の制定手続きと関連文書を具体的な制定のプロセスの例として、NIST の米国内のおける文書制定の役割と併せて以下に報告する。なお、文書の初案作成のプロセスについての活動は今回の調査から確認することはできなかった。

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諸指針、諸標準の多くは、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[66]（以下 FISMA と略記）がある。Office of Management and Budget[67]（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[68] 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

[65] https://www.nist.gov/itl/procedures-developing-fips-federal-information-processing-standards-publications
[66] https://www.cisa.gov/federal-information-security-modernization-act
[67] https://www.whitehouse.gov/omb/
[68] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

開発を義務付けている[69]。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[70]（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、7 年ぶりの改訂が行われ、2020 年 9 月 23 日に公開された後、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ている。

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

また、同様に、この指針を基に 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 日の Draft 公開、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[71]（NCCoE）主催のワークショップや、Consumer Technology Association[72]（CTA：消費者技術協会）主催の Roundtable 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。

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。

---

[69] https://www.ipa.go.jp/security/publications/nist/fisma.html
[70] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf
[71] https://www.nccoe.nist.gov/about-the-center
[72] https://www.cta.tech/

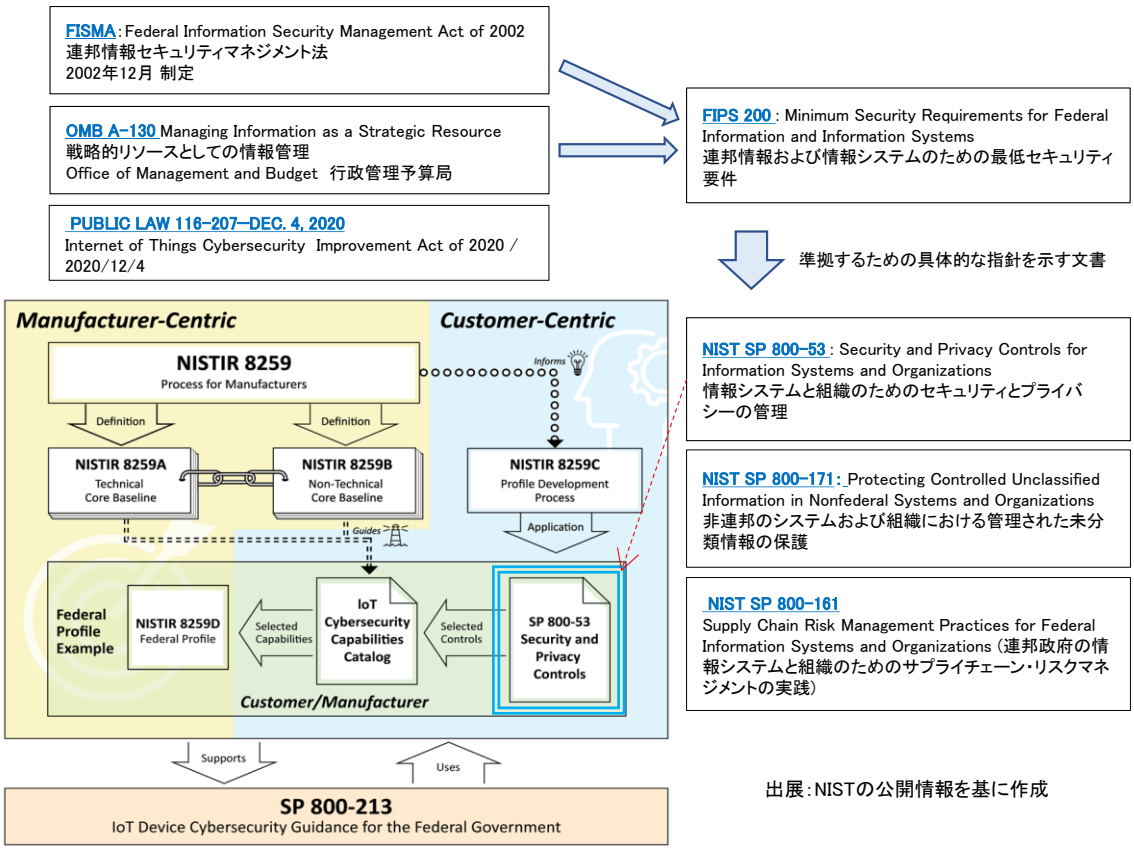

図 3 アメリカ合衆国内の文書制定の役割と NIST の関係、 NSIR 8259 の位置づけ

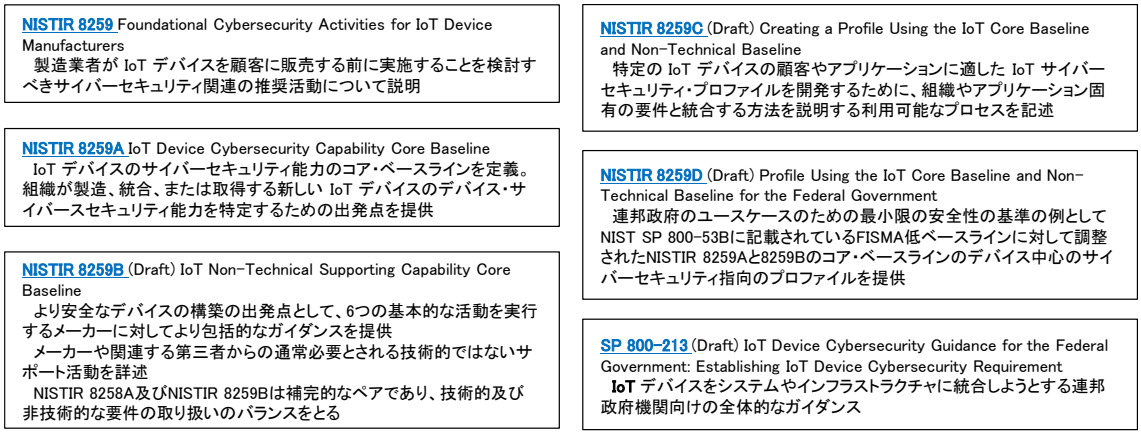

図 4 NISTIR 8259 文書ファミリー

前節 4.1 の A-3 項で報告した通り、NISTIR 8259 と NISTIR 8259A は 2020 年 5 月 29 日に発行されている。米国在住の有識者の見解によると、これらの文書の最終版の確定に対して州政府が直接的に対応することはないと考えられる。従来の州政府の活動状況からは、州政

府が独自調達することは少なく、今回も GSA（General Services Administration[73]：米国共通役務庁）の方針が決まるのを待って、それに合わせた対応や GSA の調達に参加する可能性が考えられる。また、調達先である業界は対応を開始しロビー活動を展開していると考えられるが、具体的な内容は不明である。

NIST8259 と 8259A の発行後の 2020 年 7 月 23 日と 24 日に開催されたオンラインワークショップ Building the Federal Profile For IoT Device Cybersecurity: Next Steps for Securing Federal Systems は、500 名規模の会合となり 26 カ国とアメリカ国内 39 州からの参加があった。アメリカ合衆国においては FOIA 法（Freedom Of Information Act[74]：情報自由法）により連邦政府に情報の公開が義務付けらえている。このため一般的にアクセス可能な Web や RSS により情報が公開されている。NIST においても、これに従って文書改訂やパブリックコメントによる意見募集、カンファレンスの開催の情報が公開されており、その情報に基づき制度や標準の制定作業が行われている。なお、公開情報の内容により、海外政府や標準化組織、州政府などに個別に情報が送付されるのが通例である。

NIST のドラフトに対する寄せられるコメントに関して、海外からのコメントが国内のコメントの扱いと異なることはなく、アメリカ合衆国からみて有用なものであれば取り上げられている。

A-3. NIST の標準化に向けた活動

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[75]（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。参照されているのは以下の 15 組織の資料であり、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ことが窺える。

- **AGELIGHT**: AgeLight Digital Trust Advisory Group, “IoT Safety Architecture & Risk Toolkit (IoTSA) v3.1”

---

[73] https://www.gsa.gov/
[74] Freedom Of Information Act
[75] https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8200.pdf

- **BITAG**: Broadband Internet Technical Advisory Group (BITAG), “Internet of Things (IoT) Security and Privacy Recommendations”
- **CSA**: Cloud Security Alliance (CSA) IoT Working Group, “Identity and Access Management for the Internet of Things”
- **CSDE**: Council to Secure the Digital Economy (CSDE), “The C2 Consensus on IoT Device Security Baseline Capabilities”
- **CTIA**: CTIA, “CTIA Cybersecurity Certification Test Plan for IoT Devices, Version 1.0.1”
- **ENISA**: European Union Agency for Network and Information Security (ENISA), “Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures”
- **ETSI**: European Telecommunications Standards Institute (ETSI), “Cyber Security for Consumer Internet of Things”
- **GSMA**: Groupe Spéciale Mobile Association (GSMA), “GSMA IoT Security Assessment”
- **IEC**: International Electrotechnical Commission (IEC), “IEC 62443-4-2, Edition 1.0, Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components”
- **IIC**: Industrial Internet Consortium (IIC), “Industrial Internet of Things Volume G4: Security Framework”
- **IoTSF**: IoT Security Foundation (IoTSF), “IoT Security Compliance Framework, Release 2
- **ISOC/OTA**: Internet Society/Online Trust Alliance (OTA), “IoT Security & Privacy Trust Framework v2.5”
- **NEMA**: National Electrical Manufacturers Association (NEMA), “Cyber Hygiene Best Practices”
- **OCF**: Open Connectivity Foundation (OCF) “OCF Security Specification Version 2.1.2”
- **PSA**: Platform Security Architecture (PSA) Joint Stakeholder Agreement (JSA) Members, “PSA Certified™ Level I Questionnaire, Version 2.0 Beta”

さらに 2021 年 2 月 21 に NIST blog で公開された“2021: What’s Ahead from NIST in Cybersecurity and Privacy?”[76]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おり、今後の NIST の取り組みに注目する必要がある。

[76] https://www.nist.gov/blogs/cybersecurity-insights/2021-whats-ahead-nist-cybersecurity-and-privacy

B) ヨーロッパにおける制度や取りまとめのプロセス

B-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（現在）の監督当局の管轄ではない。

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

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

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

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

表 2 ETSI の規格のタイプと規格化プロセス

規格のタイプ（略記号）	投票と承認	注釈	規格化プロセス
技術仕様 (TS)	起草した技術委員会によって承認	技術的な要件が含まれ、迅速に使用できることが重要な場合	I
技術レポート (TR)	起草した技術委員会によって承認	説明資料が含まれる	
グループ仕様 (GS)	業界仕様グループ(ISG)内で作成及び承認	技術的な要件、説明資料、またはその両方を提供	
グループレポート (GR)	業界仕様グループによって公表を承認	情報提供要素のみ	
特別レポート (SR)	作成した技術委員会によって承認	情報を参照のために一般に公開	
ガイド (EG)	メンバーシップ全体	特定の技術標準化活動の取り扱いに関する一般的なガイダンス	Ⅱ
ETSI 規格 (ES)	メンバーシップ全体	技術要件が含まれる	
欧州規格 (EN)	技術委員会によって起草され、欧州標準機関によって承認		Ⅲ

- 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。

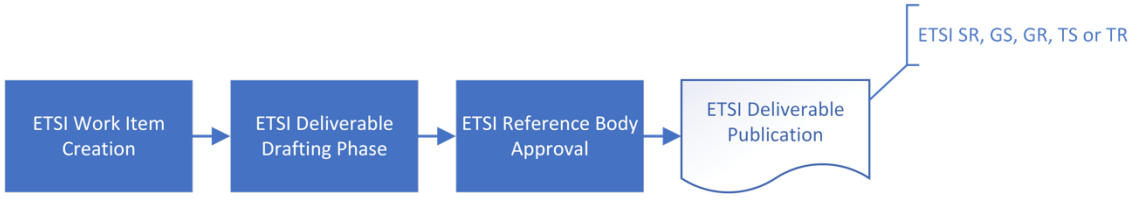

図 5 技術仕様(TS)、技術レポート(TR)、グループ仕様(GS)、グループレポート(GR) 及び特別レポートの承認手順

● 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。

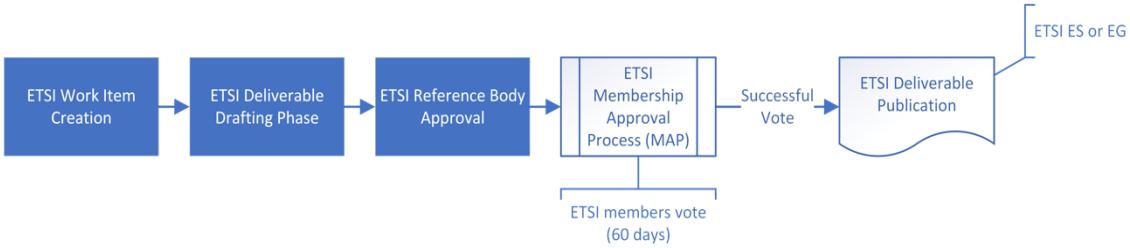

図 6 ETSI ガイド(EG) 及び ETSI 規格(ES)の承認手順

● 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[77]）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。

[77] https://portal.etsi.org/TB-SiteMap/NSO/Home

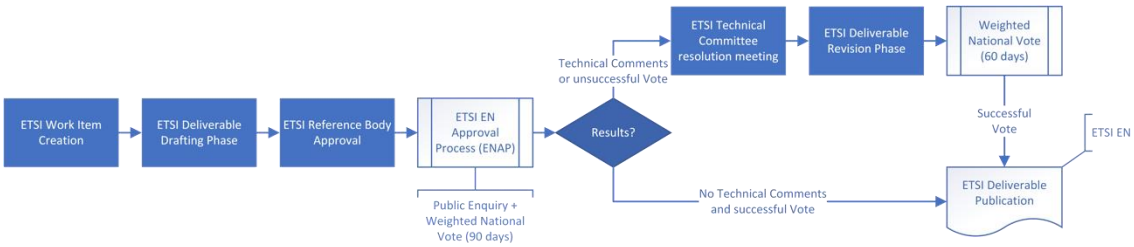

図 7　欧州規格(EN)の承認手順

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。

B-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、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。

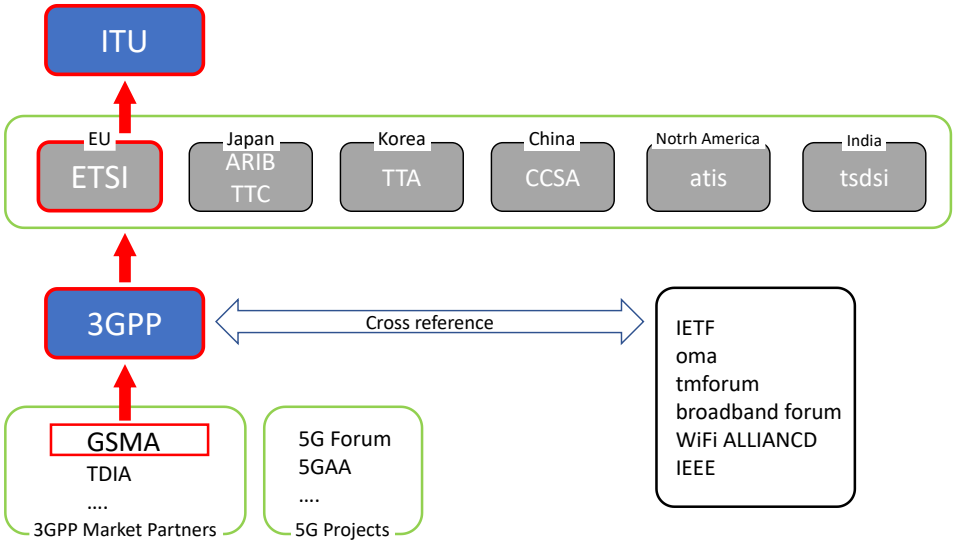

図 8 モバイル関連の標準化団体の 3GPP を中心とした関連

3GPP の図[78]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。

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

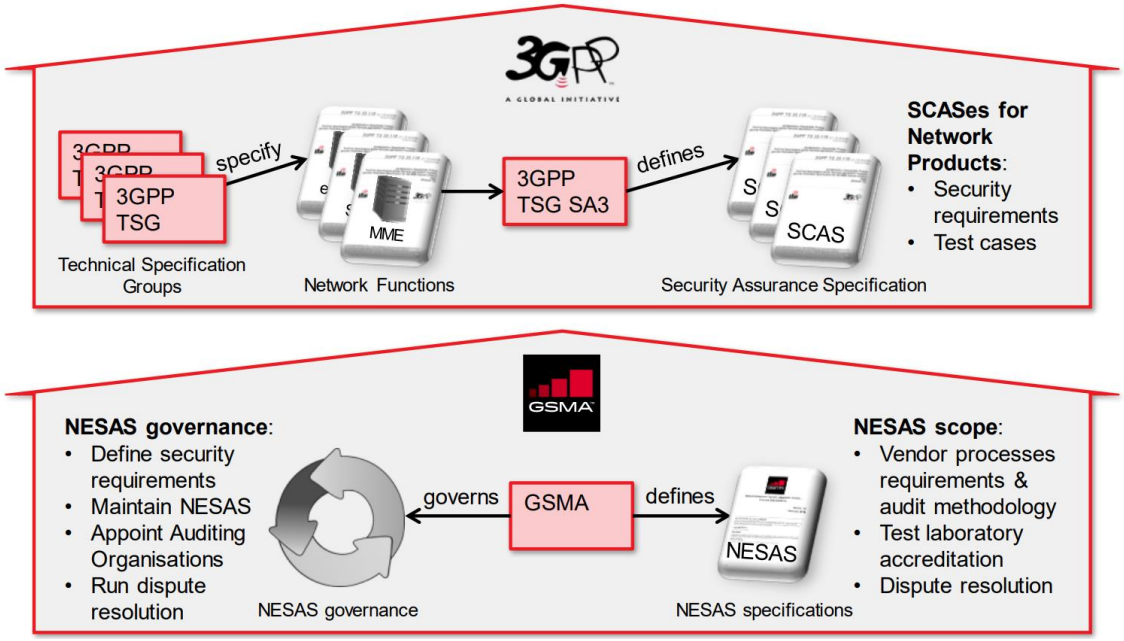

図 9 仕様に関する 3GPP-GSMA の役割

GSMA Network Equipment Security Assurance Scheme (NESAS)[79]

4.3 海外のステークホルダーとの連携

- 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。

アメリカ合衆国における 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 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 氏とその一部の関係者を除き、現状では 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。

[79] https://www.gsma.com/security/wp-content/uploads/2021/02/FS.13-NESAS-Overview-v2.0.pdf

なお、アメリカ合衆国の 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。

- 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。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。

次のイベントへの参加の機会としては、NISTIR 8259B、8259C、8259D のドラフトに対して 2021 年 2 月 26 日にまでに寄せられたコメントを反映したドラフトを IoT Program がまとめ、NIST が数か月後に開催すると想定される Online 説明会が考えられる。本プロジェクトからの有用なコメントや、IoT Program 関係者との意見交換を通じて本プロジェクトの活動の価値が認知され、本プロジェクトに対して直接カンファレンス開催の案内連絡や、意見照会が行われる状況を目指した活動を行うことが望ましい。

- 今後の方向性と政府の活動

アメリカ合衆国の商務長官の承認を受けて発行された文書 FIPS 200 で連邦情報および情報システムのセキュリティ要件を定められ、これに基づいて NISP SP 800-53 や NISTIR 文書類の発行活動が行われてきている。

2021 年 2 月 4 日に、DHS（アメリカ合衆国国土安全保障省）の管理下にある CISA ICT SCRM タスクフォースは過去 2 年間に渡り実施してきた活動を、7 月まで半年間延長することを発表した。ICT SCRM タスクフォースではサプライチェーンのセキュリティの確保と、発生したインシデントを沈静化して本来の状態回復を行うレ

ジリエンスに関する活動が行なわれる。

また、2 月 24 日にバイデン大統領はコンピュータチップ、医療機器、電気自動車用バッテリー、レアメタルなどの重要品目の米国サプライチェーンにおける潜在的な脆弱性についての 100 日間の政府のレビューを命じ、さらに国防、公衆衛生、ICT、エネルギー、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。この活動の総括責任者は国家安全保障補佐官、並びに経済政策担当補佐官とされており、国家安全保障政策と経済政策を同時に展開する形となっている。

ヨーロッパにおいて 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。

以上のような状況から、IoT セキュリティに加え、サプライチェーンのセキュリティに関する取り組みが今後急速に強化され、特にアメリカ合衆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。

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、アメリカ合衆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、アメリカ合衆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が必要と考えられる。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を構成できることが、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の技術目標

5.1 海外における技術開発プロジェクト等における技術目標の調査

(1) 調査方法

本調査対象の技術目標については、既に到達しているレベル、現時点で最も進んでいると評価されているレベル、これからの実現を目指しているレベルの調査を可能とすることを目標に、調査対象を選定した。

既に到達しているレベルについては、既に製品として認知されているものを対象とした。

現時点で最も進んでいると評価されているレベルについては、セキュリティ関連のカンファレンスでアワードを取っている製品とした。具体的には、RSA カンファレンスの Finalists for RSAC Innovation Sandbox Contest 2020 とした。

これからの実現を目指しているレベルについては、米国政府が選定しているプロジェクト（NISTIR 、NSF Award）や、公開している規定、欧州の HORIZON プロジェクト（HORIZON2020）に加え、都市 OS でセキュリティを担っている標準仕様（OAuth 2.0）を対象とした。

以下、(2) において既に到達している技術目標の調査結果を、(3) において現時点で最も進んでいる技術目標を、(4) (5) (6) でこれから実現を目指している技術目標を報告する。

(2) 既存製品

A) ZeroFOX[80]

（概要）

ZeroFOX プラットフォームは公開攻撃面保護のソリューションである。あらゆる公開される情報を常に監視し、組織を標的とした隠れた脅威やあらゆるタイプの悪意のあるサイバー攻撃を発見し、公開される前に脅威を排除することができる。

多様なデータソースと人工知能ベースの分析を用いて、ZeroFOX プラットフォームは、標的型フィッシング攻撃、証明書侵害、データ窃盗、なりすまし、ブランドハイジャック、位置情報などの公開プラットフォーム上の脅威を特定し対処することができる。

（技術の特徴）

ZeroFOX の技術的特徴は、一つのプラットフォームでの多様な情報の保護（ソーシャルメディア情報、ディープ・ダーク Web や Web 情報、E メールなどのデジタル情報、モバイルアプリストア、コード共有サイトなど）、AI や機械学習、ポリシーやルールベースでの解析である。

B) baffle[81]

（概要）

baffle は、データの非識別化やトークン化、フィールドレベルの暗号化、レコードレベルの暗号化、SaaS サービス向けの format preserving encryption（FPE）BYOK、動的データマスキング、ファイル暗号化、ファイルコンテンツ暗号化、暗号化 API サービスなどによるデータベース暗号化ソリューションと role-based access control（RBAC）、プライバシー保護のための分析、安全なデータ共有などを含むデータ保護サービスを

[80] https://www.zerofox.com/
[81] https://baffle.io/

提供している。

（技術の特徴）

Baffle Advanced Data Protection ソリューションは、Baffle Manager、管理コンソール、Baffle Shield、QL/NoSQL プロキシ、および暗号化されたデータの安全な計算を可能にするオプションのコンポーネントである Baffle SMPC Servlets で構成され、PKCS#11 または KMIP インターフェースを介して既存のキーストアと統合することができる。また、レコードレベルでのデータを保護し、必要なセキュリティレベルに応じて 4 つの保護モードをサポートすることができ、既存のアプリケーションの機能を中断することなく、暗号化の導入を簡単に行うことができる。

C) CATO Networks[82]

（概要）

CATO Networks は、SLA 保証付きの高速リンクから構成される Cato グローバルバックボーンによる SD-WAN 機能と、エンタープライズグレードのセキュリティ機能、更にセキュアなリモートアクセス環境をクラウドで提供する。SaaS、IaaS 導入の加速、モビリティの普及、自分のデバイス（BYOD）の持ち込み、IoT の導入により企業の複雑化するネットワークをシンプルにする事でオペレーションを簡略化し、アプライアンスの除去、回線コストの削減が可能となるゼロトラストネットワークサービスを提供している。

（技術の特徴）

CATO Networks は、ネットワークに以下のセキュリティ機能を有する。

- 専用ハードウェアの導入なしに、インターネットおよび内部通信のファイアウォール機能を提供する次世代型ファイアウォール
- フィッシングサイト等の悪質なサイトへのアクセスをブロックし、情報漏洩やマルウェア感染のリスクを軽減する Web セキュリティ
- HTTP/HTTPS トラフィックに対してマルウェア検出、検出時の通信ブロックが可能なマルウェア対策
- モバイル利用や Office365、Salesforce 等へのクラウドアプリケーションへのアクセス、および AWS、Azure への通信を安全に保護モバイル・クラウドセキュリティ

D) CLAROTY[83]

（概要）

CLAROTY は、既存の IT セキュリティインフラストラクチャに統合して OT 系のセ

[82] https://www.catonetworks.com/jp/
[83] https://claroty.com/

キュリティ管理（可視化、脅威検出、脆弱性管理、トリアージと緩和化）を行う Claroty プラットフォームである。これには、Continuous Threat Detection (CTD)と Enterprise Management Console (EMC)、Secure Remote Access (SRA) systems を含む。

（技術の特徴）

CLAROTY は、以下の技術的特徴を有する。

Continuous Threat Detection (CTD)

- 自動ですべての資産を発見し管理するとともに OT を可視化する
- リアルタイムで既知及び zero-day の脅威を検知する
- 継続的な脆弱性のモニタリング
- AI によるネットワークのゾーニングと分割化

Enterprise Management Console (EMC)

- ダウンタイムのゼロリスクのための迅速で安全な実装
- SOC 向けに設計された IT-OT の統一ビューの提供
- サイト横断での警告とリスク分析の統合化

Secure Remote Access (SRA) systems

- OT リモートアクセスの安全なコントロール
- リモートかつ第 3 者ユーザによるリスクの最小化
- IT-OT のセキュリティベストプラクティスの強化

E) Contrast Security[84]

（概要）

Contrast Security は、ソフトウェア開発ライフサイクルの全てのフェーズでネイティブに統合された継続的な DevSecOps 対応アプリケーション・セキュリティプラットフォームである。

（技術の特徴）

Contrast Security は、以下の技術的特徴を有する。

インタラクティブ・アプリケーション・セキュリティ・テスト(IAST)

- ソフトウェアにインストールされたエージェントによる脆弱性の調査と高い精度での自動的な特定
- エージェント型手法による WEB アプリケーションや API の開発やテスト中の自動的な脆弱性の調査
- 既存のソフトウェア開発ライフサイクル(SDLC)プロセスとのシームレスな連携

オープンソース・セキュリティ・ソフトウェアとコンプライアンスの自動化

- アプリケーション、サーバ、開発環境にマッピングされたオープンソースコンポ

[84] https://www.contrastsecurity.com/ja/

ーネント全体のインベントリの自動作成と管理

- OSS コンポーネントの既知と未知の脆弱性やライセンスリスクの継続的評価
- SDLC 全体でのカスタム・ポリシーの設定と自動実行
- 脆弱性のある OSS コンポーネントの使用状況の確認と脆弱性の修正作業に対する優先順位付け
- 本番環境で動作しているアプリケーションの継続的な監視と、脆弱性のある OSS に対する攻撃のブロック

ランタイムアプリケーション自己防衛（RASP)

- アプリケーション内でのエージェントによる攻撃の詳細情報の取得と可視化（エージェントにより監視と制御機能をアプリケーションへ付加）

F) ENVEIL[85]

（概要）

ENVEIL は、データを暗号化し（ホモモルフィック暗号化)、その状態のままでデータを利用することができるデータセキュリティソリューションである。

（技術の特徴）

ENVEIL は、以下の技術的特徴を有する。

- データ利用の全ライフサイクルで暗号化のままでの利用（ZeroReveal® Compute Fabric）
- セキュア検索機能の提供（ZeroReveal® Search）
- 低負荷 API ベースのアーキテクチャの実現
- 既存システムの変更を必要としない
- 安全な状態での機械学習でのデータの利用（ZeroReveal® Machine Learning）

G) RedLock / Prisma[86]

（概要）

RedLock / Prisma は、クラウドセキュリティソリューションで、クラウドへのアクセス時のセキュリティ保護やクラウド内に実装されたアプリケーションのセキュリティ保護を実現する。

（技術の特徴）

RedLock / Prisma は、以下の技術的特徴を有する。

- Prisma Access（セキュア アクセス サービス エッジ(SASE)機能）は、ネットワーク機能としては、SD-WAN、VPN、ゼロトラストネットワーク アクセス (ZTNA) 、Quality of service (QoS)、Clean Pipe 機能を実現する。ネットワークセキュリティ

[85] https://www.enveil.com/
[86] https://www.paloaltonetworks.jp/prisma

として、サービスとしてのファイアウォール(FWaaS)、高度な分析機能と機械学習による DNS トラフィック内の脅威の防御、脅威インテリジェンスを活用する脅威防御、静的分析と機械学習の活用による有害サイトのブロック、データ損失防止(DLP)（機密データの分類とポリシーの適用によるアクセス制御)、クラウドアクセス セキュリティ ブローカー(CASB) 機能を実現する。

- Prisma SaaS は、SaaS アプリケーションに対するデータ保護と一貫性によるリスク制御と利用者の cloud である。access security broker（クラウド アクセス セキュリティ ブローカー(CASB) ）に対応して、リスク検出、data loss prevention(データ損失防止： DLP)、コンプライアンス保証、データ ガバナンス、ユーザの振る舞いの監視、および脅威防御機能を提供する。
- Prisma Cloud（クラウドネイティブ セキュリティ プラットフォーム(CNSP) ）は、クラウド セキュリティ体制管理(CSPM)を有する。擬態的には、リソースに対する設定評価やコンプライアンスの監視とレポート、ユーザとエンティティの振る舞い分析や API ベースのネットワーク トラフィックの可視性や分析による脅威検出及びデータセキュリティ機能を実現する。加えて、クラウド ワークロード保護として、クラウドやオンプレミスの環境に対して、ライフサイクルを通して、脆弱性管理、ランタイムセキュリティ、コンプライアンス管理、アクセス制御、API 保護等のセキュリティ保護機能を実現する。

H) Unifyid

（概要）

Unifyid は、パスワードではなく、人の動きや環境などの要因に対して機械学習を利用して特徴づけ人を認証する認証プラットフォームである。

（技術の特徴）

Unifyid は、機械学習により、行動や環境要因に適用し、ユーザのデジタル指紋を作成し、個人を認証する。（歩き方の分析で、偽陽性率は５万分の１、99.999%の確率で個人を特定できる）

I) UpLevel[87]

（概要）

UpLevel は、グラフ理論による脅威分析ツールである。

（技術の特徴）

UpLevel は、以下の技術的特徴を有する。

- 攻撃状況の理解に関しては、通信アラートや事前のインシデント調査、および現

[87] https://www.uplevelsecurity.com/

在の脅威インテリジェンスに基づいてセキュリティグラフを作成する。

- 重要な関係の特定については、脅威インテリジェンス、過去のデータ、技術的な生成物の関係性を活用して、行動パターンを特定し、組織の脅威の全体像を生成する。
- 記録・情報システムの確立による脅威の予測については、セキュリティグラフに新たな優先度の高いアラートや調査の結果がグラフに組み込まれることで、時間の経過とともに成長し、将来の分析のための情報を提供する。

(3) Finalists for RSAC Innovation Sandbox Contest 2020[88]（以下 Finalists RSAC Sandbox 2020）

A) AppOmni[89]

（概要）

AppOmni は、RSA の審査において、パスワードではなく、人の動きや環境などの要因に対して機械学習を利用して特徴づけ人を認証する認証プラットフォームであるとされている。

（技術の特徴）

AppOmni の技術的な特徴を以下に示す。

- 発見：クロスクラウド セキュリティ ポスチャ管理（SaaS アプリケーションの構成ミス検出）
- 保護：データ アクセスの探索と露出防止（利便性とセキュリティのバランスの両立）
- モニター：簡単な監視と検出（別の監視ツール不要）
- 継続的なコンプライアンス（標準仕様準拠）

（自己アピールの概要）

AppOmni は、SaaS ソリューションのデータアクセスの可視性、管理、およびセキュリティを提供する。主要なサービスとしてのソフトウェア（SaaS）セキュリティおよび管理プラットフォームである。AppOmni の特許出願中のテクノロジーは、API、セキュリティコントロール、および構成設定を詳細にスキャンして、ミッションクリティカルで機密性の高いデータを保護する。

（自己アピールの特徴）

AppOmni の自己アピールの特徴として下記を上げている。

SaaS 環境において前例のないデータアクセスの可視性、管理、およびセキュリティを提供する唯一の SaaS 管理およびセキュリティプラットフォームで、AppOmni のリス

---

[88] https://www.rsaconference.com/about/press-releases/rsa-conference-announces-finalists-for-rsac-innovation-sandbox-contest-2020

[89] https://appomni.com/

ク評価は、これまで不可能だった洞察と可視性を提供する。
個々の項目の詳細は下記である。

- 発見：クロスクラウド・セキュリティ・ポスチャ管理（SaaS アプリケーションの構成ミス検出）
  導入が容易で、重要な SaaS 環境の可視性を迅速に把握できる。機密性の高い構成と管理アクションの使用を一元的に検出する。また、サードパーティアプリケーションと OAuth 認可を検出してインベントリする。推奨されるベストプラクティスの構成ポリシーと自動修復プラットフォーム機能を活用して、セキュリティイベントになる前に、問題を事前に修復する。
- 保護：データアクセスの探索と露出防止（利便性とセキュリティのバランスの両立）
  従業員、契約社員、外部第三者など、あらゆるタイプのユーザや統合によってアクセスできるデータをすぐに把握できる。会社ポリシーに基づいてアクセスを許可または禁止処理には、ホワイトリスト/ブラックリストセキュリティポリシーの詳細なセットを採用している。エキスパートが設計したデフォルトポリシーにより、SaaS アプリケーションチームは、継続的なセキュリティカバレッジを確保しながら、ビジネス機能をより迅速に提供できる。
- モニター：簡単な監視と検出（別の監視ツール不要）
  既存の SecOps チームに包括的な SaaS 検出機能を追加。SaaS 環境全体で発生している異常、不適切、または疑わしいアクティビティに関する警告を受ける。イベントの自動正規化と組み込みの検出により、既存のツールやチームに対して、信頼度の高いアラートが直接提供される。セキュリティに対する姿勢やデータアクセスの問題をプロアクティブに監視および検索し、インシデントの発生を抑える。
- 継続的なコンプライアンス（標準仕様準拠）
  SOC 2、ISO 27001、NIST CSF、NIST 800-53 などの標準マッピングを使用して、PCI、HIPAA、GDPR の要件を満たすため、重要な SaaS セキュリティ制御を自動的に適用する。構成エラーを自動修復し、複数のインスタンスに同時に一貫したセキュリティベースラインを展開する。合わせて、機密性の高い構成および管理アクションの使用を監査/監視する。詳細なコンプライアンスレポートとダッシュボードを使用して信頼度などを検証する。

B) BluBracket[90]
（概要）
BluBracket は、包括的なソフトウェアコードのエンタープライズセキュリティソリュ

[90] https://blubracket.com/

ーションである。
(技術の特徴)
BluBracket の技術的な特徴を以下に示す。

- コードを見つけて分類（アクセス権限）
- リスクを検出して監視（アクセス資格の誤用監視）
- 貴重なコードを保護（コードブックフィンガープリント）
- セキュリティポリシーを自動実施(CI/CD パイプライン：自動化)

(自己アピールの概要)
BluBracket は、ソフトウェア主導の世界におけるコードのエンタープライズセキュリティソリューションである。BluBracket を使用すると、開発者のワークフローや生産性を変更することなく、ソースコードがセキュリティリスクをもたらす場所を企業に可視化すると同時に、コードを完全に保護する。
(自己アピールの特徴)
BluBracket の自己アピールの特徴として下記を上げている。
包括的なエンタープライズセキュリティスイートとして、コードセキュリティの 4 つの重要なステップを実現している。
以下に概要を示す。

- コードを見つけて分類（アクセス権限）
  企業が把握できないコードの急増に対応する。BluBracket は、企業にコード環境の BluPrint を提供するため、組織の内外で、コードがどこにあり、誰がコードにアクセスできるかを知ることができる。更に、ワンクリックで最も重要なコードを分類できるため、監査やコンプライアンスのニーズに応じた詳細な管理過程を表示できる。
- リスクを検出して監視（アクセス資格の誤用監視）
  GitHub や StackOverflow などのコードサイトが企業のセキュリティに対するリスクを表している。実際、2019 年には、すべてのセキュリティ違反のほぼ半分が、コードで頻繁に見られる資格情報の誤用によるものである。
  BluBracket は、パスワードやトークンなどのコード内のシークレットを自動的に検出し、これらをすぐにローテーションして取り消すことができる。また、Git 構成の誤りを見つけて、経路をエンタープライズデータに直接公開し、サードパーティのアプリケーションと Webhook を監視してセキュリティコンプライアンスを確認できる。これにより、企業は、自社のコードによってもたらされるリスクと、是正への道筋について包括的な評価を行うことになる。
- 貴重なコードを保護（コードブックフィンガープリント）
  BluBracket は、アクションを実行してコードへの投資を保護するために必要な可視性、アラート、および修復法を提供する。高度な ML や AI 技術により、最も

重要なコードを正確に識別・分類できるため、状況に応じてアラートを受け取ることができる。例えば、許可されていない Webhook、まだアクセス権を持っている非アクティブや無効なユーザ、プライベートリポジトリの公開、などがある。BluBracket のコードフィンガープリントは、重要なコードや機密データがオープンソースに push されないようにすることもでき、コードが承認された信頼できるソースからのものであることを保証する。

- セキュリティポリシーを自動実施（CI/CD パイプライン：自動化）
  ソフトウェア開発ライフサイクルは高速で機敏であるため、セキュリティチームが重要なセキュリティポリシーに影響を与えて実施することは困難である。BluBracket は、CI/CD パイプラインでセキュリティポリシーを実行可能かつ実施可能にすることで、セキュリティ、開発、および DevOps チーム間のギャップを埋める。BluBracket は、開発者のワークフローを中断することなく、企業が必要とする Git アクセス制御も提供する。

C) ForAllSecure （Mayhem）[91]

（概要）

ForAllSecure は、セキュリティテストソリューションである。

（技術の特徴）

ForAllSecure の技術的な特徴を以下に示す。

- 高度なアプリケーション セキュリティテストの簡素化
- 継続的自律テストによる継続的開発
- 深い欠陥の発見（誤検知ゼロ、手動テスト排除、Shift-left DAST（動的アプリケーションセキュリティテスト）、リスク継承の軽減）

（自己アピールの概要）

ForAllSecure は、世界のソフトウェアを保護することを目的としている。ForAllSecure は、CMU の研究から得られた特許技術を使用して、テレコム、航空宇宙、自動車などの Fortune1000 企業に次世代の Fuzzing solution を提供する。DARPA は ForAllSecure をサイバーグランドチャレンジの勝者に指名し、MIT Technology Review はそれを 50 の最も賢い企業の 1 つに指名した。

（自己アピールの特徴）

ForAllSecure の自己アピールのポイントは、「前例のない速度、規模、精度で欠陥を継続的に発見できる」としている。

これを実現する技術的な特徴には下記がある。

- 自律的な欠陥の検出と検証により、手動テストの労力を大幅に削減する高度なア

[91] https://forallsecure.com/

プリケーション セキュリティテストの簡素化

- 継続的自律テストによる継続的開発
- 深い欠陥の発見（時間の経過とともにターゲットのインテリジェンスを取得、知識が増えるにつれて、分析が深まり、コードカバレッジが最大化されることにより、誤検知ゼロ、手動テスト排除、Shift-left DAST（動的アプリケーションセキュリティテスト）、リスク継承軽減を実現）

D) Obsidian Security [92]

（概要）

Obsidian Security は、SaaS にセキュリティを提供する。

（技術の特徴）

Obsidian Security の技術的な特徴を下記に示す。

- 統一された可視性と監視（参加者、特権、実施状況）
- クラウド侵害保護（継続的な監視と的を絞ったアラート）
- インサイダー脅威の監視（継続的な行動分析、強力アラート）
- データ保護（継続的な可視性、監視、分析）
- SaaS セキュリティ姿勢(POSTURE)管理

（自己アピールの概要）

Obsidian Cloud Detection and Response は、SaaS に摩擦のないセキュリティを提供する。独自の ID グラフと機械学習を使用して、クラウドで最も高度な攻撃を阻止する。アプリケーション、ユーザ、およびデータ全体の統一された可視性により、本番環境に影響を与えることなく、脅威の検出、違反の修正、およびセキュリティの強化が実現する。

（自己アピールの特徴）

Obsidian Security の自己アピールのポイントは下記としている。

- 統一された可視性と監視
  SaaS アプリケーションに誰が参加しているか、何に対して特権を持っているか、何をしているかについて、統一/正規化して可視性を取得する。
- クラウド侵害保護
  継続的な監視と的を絞ったアラートにより、新たな SaaS セキュリティの脅威を寄せ付けない。
- インサイダー脅威の監視
  継続的なセキュリティ監視、行動分析、強力なアラートにより、従業員、請負業者、特権ユーザによる内部脅威を特定し阻止する。

---

[92] https://www.obsidiansecurity.com/

- データ保護
  継続的な可視性、監視、分析により、SaaS 環境の貴重なデータを、漏えい、不適切なアクセス、意図しない露出から保護する。
- SaaS セキュリティ姿勢(POSTURE)管理
  継続的な可視性と監視、アクセス権のサイズ設定、構成管理により、SaaS アプリケーションを侵害や侵害からプロアクティブに保護する。

E) SECURITI.ai[93]

(概要)

SECURITI.ai は、マルチクラウド、SaaS、オンプレミスのデータのプライバシーとセキュリティ及びガバナンスのソリューションである。

(技術の特徴)

SECURITI.ai の技術的な特徴を下記に示す。

- データ・インテリジェント（機密データの自動特定）
- データの自動マッピング
- 非構造化データと構造化データのリアルタイムレコード
- Data Privacy（シンプルプラットフォーム）
- 個人の権利の自動履行
- Data Security（ハイリスクデータ特定）
- 隠れたデータリスクの発見・修復

(自己アピールの概要)

SECURITI.ai の自己アピールの概要を下記に示す。

AI を活用した PrivacyOps のリーダー。その PRIVACI.ai ソリューションは、特許出願中の PeopleDataGraphs™とロボット自動化によるプライバシーコンプライアンスを自動化する。これにより、企業はデータに関する権利を人々に与え、グローバルなプライバシー規制を遵守し、顧客との信頼を築くことができる。

(自己アピールの特徴)

SECURITI.ai の自己アピールのポイントを下記に示す。

マルチクラウド、SaaS、オンプレミスに対して AI を活用したデータのプライバシーとセキュリティを提供する。

具体的な内容を下記に示す。

- データ・インテリジェント（機密データの自動特定）
  構造化システムと非構造化システムで組織全体の機密データを特定する。データのプライバシー、セキュリティ、ガバナンスを自動化する。

---

[93] https://securiti.ai/

- データの自動マッピング
- 非構造化データと構造化データのリアルタイムレコード
- Data Privacy
  グローバルなプライバシーコンプライアンスを可能にするシンプルなPrivacyOps プラットフォームを提供する。
- 個人の権利の自動履行
  DSR、同意、インシデントを用い、手作業、コスト、およびリスクを削減する。これにより、ユーザの信頼を獲得する。
- Data Security（ハイリスクデータ特定）
  リスクの高いデータを特定し、保護を有効にする
- 隠れたデータリスクの発見
  データリスクを見つけて修復し、費用のかかる違反を回避する。

F) Sqreen

（概要）

Sqreen は、企業向けのアプリケーションセキュリティプラットフォームである。

（技術の特徴）

Sqreen の技術的な特徴は下記である。

- アプリケーション保護
- ランタイムアプリケーションの自己保護動作
- 邪魔にならない WAF（Web アプリケーションファイアウォール）
- 高視認性

（自己アピールの概要）

Sqreen の自己アピールを以下に示す。

現代の企業向けのアプリケーションセキュリティプラットフォームである。あらゆる規模の組織が、ソフトウェアの保護、監視、テストを Sqreen に任せている。パターンベースのアプローチとは対照的に、Sqreen はアプリ内実行をリアルタイムで分析し、パフォーマンスを低下させることなく、より堅牢なセキュリティを提供する。

（自己アピールの特徴）

Sqreen の特徴として、アプローチとプラットフォームの概要を上げている。

アプローチとしては、詳細なセキュリティ信号を活用してアプリケーションをより効果的に監視および保護するサンドボックス化されたマイクロエージェントを備えた分散アーキテクチャで、これまで知られていなかったものの可視化を可能としている。

また、プラットフォームの概要として、「Sqreen を使用すると、あらゆる規模の組織がアプリケーションのセキュリティを強化し、セキュリティインシデントの数を減らし、インシデントが発生したときにインシデントをより迅速に解決できる。」として

いる。具体的には、下記を上げている。

- アプリケーション保護
  データ侵害を防ぎ、アカウントの乗っ取りを停止し、ビジネスロジック攻撃をブロックすることにより、アプリケーションを保護する。
- ランタイムアプリケーションの自己保護動作
  Sqreen 独自の Runtime Application Self-Protection（RASP）アーキテクチャは、HTTP 層を超えた詳細な可視性と保護を提供する。
- Sqreen アプリ内 WAF（邪魔にならない WAF）
  Sqreen のアプリ内 Web アプリケーション WAF は、アプリケーションの完全なコンテキストを活用して、フェイルセーフで、誤検知が制限され、大幅な微調整を必要せず、すぐに使用できるクラウドネイティブの WAF を提供する。
- 高視認性
  インシデントをリアルタイムで監視し、インシデント対応管理を合理化し、アプリケーションインベントリを自動化することで、可視性を高める。

G) Tala Security[94]

（概要）

Tala Security は、Web のクライアント攻撃保護ソリューションである。

（技術の特徴）

Tala Security の技術的な特徴を下記に示す。

- Web データセキュリティとプライバシー
- クライアント攻撃の防御
- 標準ベースのセキュリティポリシーの自動化
- 機密データ保護
- プライバシーとユーザデータの整合性確保
- E コマース投資の保護
- クライアントセキュリティ展開の加速

（自己アピールの概要）

Tala Security の自己アピールを以下に示す。

クライアント側のリスクから Web を保護するため、Tala の AI 駆動型分析エンジンは、サイトアーキテクチャに継続的に問合せて、標準ベースのセキュリティをアクティブ化する高度な自動化エンジンと連携して、magecart、XSS（Cross-site scripting）、Session redirection、Client-side malware などの幅広いクライアント側攻撃を防ぐ。

（自己アピールの特徴）

---

[94] https://www.talasecurity.io/

Tala Security の自己アピールの特徴を下記に示す。

- Web データセキュリティとプライバシー
  機密データを保護し、可視性を高め、クライアント側の攻撃を排除する。
- クライアント攻撃の防御
  Magecart style、Form jack、XSS などのクライアント側の攻撃から機密データを保護する。
- 標準ベースのセキュリティポリシーの自動化
  Tala の高度な分析および自動化エンジンは、CSP[95]、SRI[96]、およびその他の重要な制御を継続的に適用して、広範囲なクライアント攻撃から保護する。
- 機密データ保護
  リスクエクスポージャーを特定し、ブラウザーを介して収集または送信されるすべてのデータを管理する。
- プライバシーとユーザデータの整合性確保
  GDPR[97]、CCPA[98]、および顧客データ保護を義務付けるその他の法律などのグローバルデータプライバシー規制へのコンプライアンスを推進する。
- E コマース投資の保護
  収益の充足を確保し、悪意のある広告の挿入を防ぎ、セッションのリダイレクトを排除する。
- クライアントセキュリティ展開の加速
  Cloudflare により、データの盗難を即座に防止し、クライアント側の攻撃を排除する。

H) Vulcan Cyber[99]

（概要）

Vulcan Cyber は、企業のサイバーリスク軽減、最新化する脆弱性修復およびオーケストレーションプラットフォームである。

（技術の特徴）

Vulcan Cyber の技術の特長を下記に示す。

- 脆弱性の検出と修正実施
- 脆弱性修復オーケストレーション（作業の優先付け）
- 修正順序優先付け（リスクの優先順位付け）
- 治療（修復）

---

95 Content Security Policy
96 Subresource Integrity
97 General Data Protection Regulation
98 California Consumer Privacy Act
99 https://vulcan.io/

- 修復プロセスの自動化

（自己アピールの概要）

Vulcan Cyber の自己アピールを以下に示す。

企業のサイバーリスク軽減、最新化する脆弱性修復およびオーケストレーションプラットフォームで、Vulcan は、修復主導のアプローチにより、脆弱性修復のライフサイクルを自動化、調整し、ビジネスの各チームがセキュリティ、運用、およびサイバーリスクを大規模に効果的に修復できるようにする。

（自己アピールの特徴）

Vulcan Cyber の自己アピールの特徴を以下に示す。

- 脆弱性の検出と修正実施
  Vulcan は脆弱性の修正を最初から最後まで調整するため、脆弱性を見つけるだけでなく、実際に脆弱性を修正する。
- 脆弱性修復オーケストレーション（作業の優先付け）
  脆弱性から確実に安全に移行する。Vulcan Cyber はツールと統合し、作業に優先順位を付け、厳選された救済策を提供し、修復結果を推進して修正実施に役立つ機能を提供する。
- 修正順序優先付け（リスクの優先順位付け）
  最も重要なものを修正する。Vulcan は、独自のリスク許容度を考慮し、リスクの重大度とビジネス資産への脅威に基づいて脆弱性に優先順位を付けする。
- 治療（修復）
  検索を減らし、修正を増やす。Vulcan 修復インテリジェンスを使用して、脆弱性に対する正確なパッチ、構成スクリプト、または回避策を取得する。見つかったものから修正されたものへ、すばやく移動する。
- 修復プロセスの自動化
  合理化、修正を繰返す。修正チケットのルーティングからパッチ適用までの修復プロセスを自動化することで、インフラストラクチャとアプリを大規模に自由に修正できる。

(4) 米国政府の動き

A) NISTIR[100]からの調査対象の抽出

NIST の今後の動きを分析する観点から、表 5- 1 と表 5- 2 に NIST Interagency Reports の IoT セキュリティ、サプライチェーンに関する報告書をリストアップした。

その内、技術基準要素を含むと思われるレポートは、IoT セキュリティ関連では、「IoT Device Cybersecurity Capability Core Baseline」、サプライチェーン関連では、

[100] https://csrc.nist.gov/publications/nistir

「Impact Analysis Tool for Interdependent Cyber Supply Chain Risks」を取り上げ、技術基準要素の観点で調査・分析した結果を示す。

表 5- 1　IoT セキュリティに関する NIST 内レポート

IoT関連

No	Series	Number	Title	Status	Release Date	概要	技術基準要素
1	NISTIR	8322	Workshop Summary Report for “Building the Federal Profile For IoT Device Cybersecurity” Virtual Workshop	Final	1/07/2021	IoTデバイスサイバーセキュリティの連邦政府プロファイルの構築	△
2	NISTIR	8267	Security Review of Consumer Home Internet of Things (IoT) Products	Draft	10/01/2019	消費者向けIoT製品のセキュリティレビュー	–
3	NISTIR	8259D	Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government	Draft	12/15/2020	IoTコアベースラインと非技術ベースラインの連邦政府プロファイル	–
4	NISTIR	8259C	Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline	Draft	12/15/2020	IoTコアベースラインと非技術ベースラインを使用したプロファイルの作成	–
5	NISTIR	8259B	IoT Non-Technical Supporting Capability Core Baseline	Draft	12/15/2020	IoT非技術的サポート機能コアベースライン	–
6	NISTIR	8259A	IoT Device Cybersecurity Capability Core Baseline	Final	5/29/2020	IoTデバイスのサイバーセキュリティ機能のコアベースライン	◎
7	NISTIR	8259	Foundational Cybersecurity Activities for IoT Device Manufacturers	Final	5/29/2020	IoTデバイスメーカー向けの基本的なサイバーセキュリティ活動	–
8	NISTIR	8228	Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks	Final	6/25/2019	IoTサイバーセキュリティとプライバシーリスクを管理するための考慮事項	○
9	NISTIR	8201	Internet of Things (IoT) Cybersecurity Colloquium: A NIST Workshop Proceedings	Final	12/22/2017	IoTサイバーセキュリティコロキウム：NISTワークショップ議事録	–
10	NISTIR	8200	Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT)	Final	11/29/2018	IoTの国際サイバーセキュリティ標準化の状況に関する省庁間レポート	△

表 5- 2　サプライチェーンに関する NIST 内レポート

Supply Chain関連

No	Series	Number	Title	Status	Release Date	概要	技術基準要素
1	NISTIR	8276	Key Practices in Cyber Supply Chain Risk Management: Observations from Industry	Final	2/11/2021	サイバーサプライチェーンのリスク管理における重要な実践：業界からの観察	○
2	NISTIR	8272	Impact Analysis Tool for Interdependent Cyber Supply Chain Risks	Final	8/25/2020	相互依存するサイバーサプライチェーンリスクの影響分析ツール	◎
3	NISTIR	8179	Criticality Analysis Process Model: Prioritizing Systems and Components	Final	4/09/2018	重要度分析プロセスモデル：システムとコンポーネントの優先順位付け	–
4	NISTIR	7622	Notional Supply Chain Risk Management Practices for Federal Information Systems	Final	10/16/2012	連邦情報システムの概念的なサプライチェーンリスク管理慣行	–

B)　IoT Device Cybersecurity Capability Core Baseline（NISTIR 8259A）[101]

本レポートは、IoT デバイスのサイバーセキュリティ機能のコアベースラインを規定している。具体的には、デバイス識別子、デバイス構成、データ保護、インターフ

[101] https://csrc.nist.gov/publications/detail/nistir/8259a/final

ェースへの論理アクセス、ソフトウェアの更新、サイバーセキュリティ状態の認識の6項目を規定している。

このレポートは、2020年5発29日に、「NISTIR8259のFoundational Cybersecurity Activities for IoT Device Manufacturers」と合わせて公開し、2020年12月5日には「NISTIR8259Bの IoT Non-Technical Supporting Capability Core Baseline」、「NISTIR8259Cの Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline」、「NISTIR8259Dの Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government」を公開している。

各項目の規定内容の詳細は、下記となっている。

- デバイス識別子：一意の論理識別子、一意の物理識別子の両方を有する
  - 一意の論理識別子：目的に応じて適切な識別子を選択できる。
  - 許可エンティティがアクセスできるデバイスの一意の物理識別子（内部/外部）：展開中や廃止昼夜、デバイス障害後など、論理識別子が使えない場合の識別用に必要。
- デバイス構成：ソフトウェア構成変更機能、構成変更承認エンティティのみが実行許可機能と承認エンティティの設定が可能
  - デバイスのソフトウェア構成設定を変更する機能：脆弱性管理、アクセス管理、データ保護、インシデント検出をサポートする。
  - 構成の変更を許可されたエンティティのみに制限する機能：ニーズに合わせたカスタマイズ。エンティティ環境に統合する。
  - 承認エンティティによって定義された安全な構成にデバイスを復元する機能：破損、破壊などからの安全な構成を復元する機能
- データ保護：保存データ/送信データの不正アクセス/変更からの保護
  - 標準化暗号化アルゴリズムと安全な暗号化モジュールを用いて、デバイスの保存と送信データの機密性と整合性を担保する機能：アクセス管理、データ保護、インシデント検出をサポートする。
  - デバイス上のすべてのデータにアクセスをブロックする機能（例：内部ストレージのワイプ、暗号化データの暗号化キーの破棄）：許可エンティティ（顧客、管理者、ユーザなど）は、データの機密性を保護する。
  - デバイス構成機能を使用するための構成設定（キーの長さの選択など）：許可エンティティは、データの整合性を保護する。
- インターフェースへの論理アクセス：プロトコルとサービスへの論理アクセスは、許可エンティティのみに制限可であること
  - デバイスのコア機能に必要のないローカル/NWインターフェースを論理的/物理的に無効にする機能

- NW インターフェースアクセスを許可エンティティのみに論理的に制限する機能（デバイス認証、ユーザ認証など）
- デバイス構成機能で使用する構成設定（アカウントをロック/無効、認証試行失敗しきい値、しきい値の有効化/無効化、など）

● ソフトウェアの更新：安全で構成可能なメカニズムを使用してのみ、承認されたエンティティによって更新できること

- リモート（NW ダウンロードなど）/ローカル手段（リムーバブルメディアなど）を介してデバイスのソフトウェア更新機能
- 更新をインストールする前に検証/認証する機能
- 承認エンティティが更新ソフトウェアを以前のバージョンにロールバックする機能
- 更新アクションを許可エンティティのみに制限する機能
- 更新を有効/無効にする機能
- デバイス構成機能で使用するための構成設定（下記を含む）
  a. 更新のダウンロードとインストールのために自動/手動で開始されるようにリモート更新メカニズムを構成する機能
  b. 更新が利用可能になったときに通知を有効/無効にし、通知する相手または内容を指定する機能

● サイバーセキュリティ状態の認識：サイバーセキュリティ状態のレポート。承認されたエンティティのみがその情報にアクセスできること

- デバイスのサイバーセキュリティ状態を報告する機能
- デバイスが期待どおりに動作する可能性が高い時期と、サイバーセキュリティが低下した状態にある可能性がある時期を区別する機能
- 状態インジケーターへのアクセスを制限して、許可エンティティのみが表示できるようにする機能
- デバイスの状態情報の維持を担当するエンティティを除き、エンティティ（許可/無許可）が状態を編集できないようにする機能
- イベント/状態ログサーバーなどの別のデバイス上のサービスで状態情報を利用できるようにする機能

C) Impact Analysis Tool for Interdependent Cyber Supply Chain Risks（NISTIR 8272)[102]

本レポートは、イベントの潜在的な影響を具体的に考慮したサプライチェーンのリスク分析をサポートするツールを規定している。このような規定はこれまでなかっ

[102] https://csrc.nist.gov/publications/detail/nistir/8272/archive/2020-03-13

た。

このレポートは、連邦政府機関が相互接続されたサプライチェーンにおけるサイバーセキュリティの影響を特定および評価するのに役立つように開発されたサイバーサプライチェーンリスク管理（C-SCRM）相互依存ツールの使用方法である。

サイバーリスクは通常、脅威、脆弱性、発生頻度と影響度の関数として定義されるが、現在のサイバーセキュリティリスクツールは主に脅威、脆弱性、発生確率に焦点を合わせている。このツールは、潜在的なサプライチェーンの混乱の相対的な影響を測定し、影響が大きく相互依存するノードに対してユーザが集中的なリスク軽減制御を適用する必要があるものを特定できるようにしている。

この目的のために、サプライヤ、製品、およびプロジェクトという用語を、サプライチェーンを特徴づける用語に選択した。プロジェクトは、組織内の個々の機能、ミッション、または事業部門を指す。各プロジェクトは、情報技術や運用技術（IT/OT）製品を利用し、製品は 1 つ以上のサプライヤによって提供される。

サプライチェーンの混乱の相対的な影響を測定するために、ツールは以下を分析する。

- 組織のサプライチェーン構造に関する基本情報
- 製品とサプライヤが組織の資産にアクセスできる程度
- 組織の特定サプライヤへの依存関係
- 製品とプロジェクトの重要度

各ノードには、影響スコア、相互依存スコア、および保証スコアが与えられ、影響の大きいノードの識別・視覚化する。

- 影響スコア

  影響スコアは、ノードが障害した場合に組織に与える最大の悪影響の可能性を表す。スコアは 0〜100 で、値が高いほど影響大。

  ノードの影響スコアを下げるには、組織は、ノードが接続されている製品やプロジェクトの重要度を下げる検討が必要。また、特定の製品への依存を減らし、サプライヤと製品へのアクセス（データ、物理、IT ネットワーク）を減らす方法もある。

- 相互依存スコア

  相互依存スコアは、組織のサプライチェーン全体でのノードの相対的な影響を表す。サプライヤの場合、スコアは、サプライヤが組織に提供する製品の数と、製品が組織全体で使用される範囲に変換される。製品の場合、スコアは、製品を提供するサプライヤの数と、製品が使用されるプロジェクトの数に依存する。このスコアには制限がなく、ノードの影響スコアと同様のノードの相互依存性スコアに関

連する。ノードの相互依存性スコアが高い場合、組織は、該製品の供給サプライヤの数を増やして、1 つのサプライヤへの依存度を減らす。製品の相互依存性スコアを下げるには、組織は影響スコアを下げる、又は、製品を供給するサプライヤ数を増やす方法がある。

- 保証スコア

保証スコアは、組織が特定のノードに対して C-SCRM 緩和策をどの程度完全に実装したかを表す。このスコアは、可能な緩和策に対する実装緩和策のパーセンテージであり、低い値は、組織が緩和策を実装するためにサプライヤと協力する必要があることを示す。

ノードの保証スコアを向上させるには、組織はサプライヤと協力してリスク軽減措置を実施する必要がある。これには、サプライヤのサードパーティの可視性を高め、サプライヤのレビューを実施することが含まれる。

D) NSF Award[103]

NSF(National Science Foundation:アメリカ国立科学財団）は、アメリカ合衆国の科学・技術を振興する目的で 1950 年に設立された連邦機関である。数学、コンピュータ科学、社会科学といった分野を含む、アメリカ国立衛生研究所（NIH）が管轄する医学分野を除く幅広い科学・工学分野に対する支援を行っている。

IoT セキュリティに関して、技術基準評価の観点で、表 5-3 の２つのプログラムを抽出し、調査を行った。

[103] https://www.nsf.gov/awardsearch/

表 5- 3　IoT セキュリティに関する NSF Award プログラム (1/2)

Award Number	1646130
	CPS: Breakthrough: Secure Interactions with Internet of Things
NSF Org	CNS Division Of Computer and Network Systems
Initial Amendment Date	2016年9月8日
Latest Amendment Date	2020年5月29日
Award Instrument	Continuing Grant
Program Manager	David Corman CNS Division Of Computer and Network Systems CSE Direct For Computer & Info Scie & Enginr
Start Date	2016年10月1日
End Date	2021年9月30日(推定)
Awarded Amount to Date	$538,800.00
Investigator(s)	Kang Shin kgshin@eecs.umich.edu (Principal Investigator)
Sponsor	Regents of the University of Michigan - Ann Arbor 3003 South State St. Room 1062 Ann Arbor, MI 48109-1274 (734)763-6438
NSF Program(s)	Special Projects - CNS, CPS-Cyber-Physical Systems
Program Reference Code(s)	042Z, 7354, 7918, 9251
Program Element Code(s)	033y, 1714, 7918
概要	研究の目的は、 (1)モノのインターネット(IoT)展開における相互作用の確保の課題に関する洞察を得ること、 (2)IoT相互作用に対するセキュリティとプライバシーの脅威を軽減する実用的な枠組みを開発すること、および (3)提案されたフレームワークを中規模のIoTテストベッドおよびユーザー研究で検証すること、である。 IoT コンピューティングの新しいパラダイムは、ユーザー、センサー、アクチュエータの間の対話を可能にすることで、ほぼすべての分野で新しいアプリケーションを約束する。これらの**相互作用は、デバイス間**(例：Bluetooth低エネルギー(BLE))や、**人間対デバイス(**例：音声制御)の形態をとることができる。これらの相互作用サーフェスの脆弱性を悪用することで、敵対者はIoTへの不正アクセスを取得し、追跡、プロファイリング、およびユーザーに害を与えることができる。何千もの多様なIoTメーカー、開発者、デバイスを使用して、すべてのデバイスが生産時に適切に保護され、生産後も最新の状態に保たれるようにすることは、不可能ではないにしても非常に困難。IoT ユーザーと管理者は、セキュリティ チェーンを破る最も安全性の低いデバイスを使用して、一連のデバイスに信頼を置く必要がある。
	信頼基盤をさまざまなメーカーや開発者から**ユーザーの管理下にある単一のフレームワークに移行する**ことで、IoTデバイスの導入がより実現可能になり、脆弱性が軽減される。 提案された枠組みは、国の健康、繁栄、福祉を促進し、国防を確保するのに役立つ。ケーススタディとして**IoTインターフェース面を保護**することは、**大学院レベルのコースに統合**され、**理論と実践のバランスの取れた組み合わせを必要とする学際的なトピック**で（特に過小評価されている女性の）学生を訓練するために使用され、全国的に必要な分野の**人材を育成する。** 提案された研究はまた、実際にIoT相互作用面を確保するための課題の理解を大幅に前進させ、科学の進歩を促進する。このプロジェクトは、現在および将来のIoT展開における相互作用を保護するための一般的な方向性を確立する。 セキュリティを適切に組み込み、維持できない場合に備えて、**追加の保護レイヤーを提供**する。

表 5- 3　IoT セキュリティに関する NSF Award プログラム (2/2)

Award Number	1704176
	SaTC: CORE: Medium: Collaborative: Energy-Harvested Security for the Internet of Things
NSF Org	CNS Division Of Computer and Network Systems
Initial Amendment Date	June 8, 2017
Latest Amendment Date	January 29, 2021
Award Instrument	Standard Grant
Program Manager	Sandip Kundu CNS Division Of Computer and Network Systems CSE Direct For Computer & Info Scie & Enginr
Start Date	September 1, 2017
End Date	August 31, 2021(推定)
Awarded Amount to Date	$881,992.00
Investigator(s)	Dong Ha ha@vt.edu (Principal Investigator) Patrick Schaumont (Former Principal Investigator) Dong Ha (Former Co-Principal Investigator)
Sponsor	Virginia Polytechnic Institute and State University Sponsored Programs 0170 BLACKSBURG, VA 24061-0001 (540)231-5281
NSF Program(s)	Special Projects - CNS, Secure &Trustworthy Cyberspace
Program Reference Code(s)	025Z, 7434, 7924, 9178, 9251
Program Element Code(s)	1714, 8060
概要	IoTは、コンピューターの仮想世界を実際のアプリケーションに統合し、効率、経済性、生活の質の向上につながる。 これには膨大な量の小型コンピューターが必要であり、このプロジェクトはそれらのコンピューターに持続可能な方法で電力を供給するという課題に取り組んでいる。 小型コンピューターは、太陽、振動、温度勾配などの収穫されたエネルギー源から逃げ出すことができる。 プロジェクトの目的は、このようなエネルギーに制約のあるデバイスが**安全で完全なインターネット接続をどのようにサポートできるか**を示すことである。 これは、安全なインターネット接続につながる計算をやり直し、時間をかけて分散させることで実現できる。 提案されたソリューションは、収集されたすべてのエネルギージュールを有用な計算に使用することを目的とする。
	このプロジェクトは、**暗号化エンジニアリング**、環境発電技術、フ**ォーマル検証**など、3つのドメインからの洞察に基づいている。**ハーベスタに適したバージョンの暗号化アルゴリズム**は、**クーポンを生成する事前に計算されたステップでパーティション化することによって作成される**。余剰エネルギーがある場合にクーポンが作成され、後のフェーズでオンライン計算を高速化するために使用できます。このプロジェクトは、**標準のインターネットスタックから暗号化を最適化**し、それをエネルギーハーベスターテクノロジーと統合する。検証技術は、インターネットプロトコルの事前に計算されたバージョンが主流の対応するものと機能的に同等であることを保証する。このプロジェクトは、**軽量暗号化**、形式手法、エネルギーハーベスティングシステムの実現などの重要な分野の研究課題に貢献している。このプロジェクトは、出版物、オープンソースハードウェア、およびソフトウェアを広め、モノのインターネットにおけるエネルギー制約の認識を高めるためのプログラミング競争を確立する。

E)　CPS: Breakthrough: Secure Interactions with Internet of Things（NSF Award 1646130）[104]

この研究の目的は、(1)IoT 展開における相互作用の確保の課題に関する洞察を得ること、(2)IoT 相互作用に対するセキュリティとプライバシーの脅威を軽減する実用的な枠組みを開発すること、および、(3)提案されたフレームワークを中規模の IoT テストベッドおよびユーザ研究で検証することである。

[104] https://www.nsf.gov/awardsearch/showAward?AWD_ID=1646130&HistoricalAwards=false

IoT コンピューティングの新しいパラダイムは、ユーザ、センサー、アクチュエータの間の対話を可能にすることで、ほぼすべての分野で新しいアプリケーションを約束する。これらの相互作用は、デバイス間（例：Bluetooth Low Energy(BLE) ）や、人間対デバイス間（例：音声制御）の形態をとることができる。これらの相互作用 Surface の脆弱性を悪用することで、攻撃者は IoT へ不正アクセスし、Tracking、Profiling、およびユーザに害を与えることができる。多種多様な IoT メーカー、開発者、デバイスを使用して、すべてのデバイスが生産時に適切に保護され、生産後も最新の状態に保たれるようにすることは、不可能ではないにしても非常に困難である。IoT ユーザと管理者は、セキュリティチェーンを破る最も安全性の低いデバイスを使用して、一連のデバイスに信頼を置く必要がある。

信頼基盤をメーカーや開発者からユーザの管理下にある単一のフレームワークに移行することで、IoT デバイスの導入がより実現可能になり、脆弱性が軽減される。

このプロジェクトは、現在および将来の IoT 展開における相互作用を保護するための、セキュリティを適切に組み込み、維持できない場合に備えて、追加の保護レイヤーを提供する。

研究成果には、下記の 3 件がある。

- フィジカルセキュリティ対策：ウェイクアップ機能の防御[105]

  車両を攻撃し、制御する様々な方法が実証されているが、これまで攻撃は、車両走行時のみ実現可能と考えられていたが、本稿では、遠隔車両攻撃は実現可能であり、車両が起動の場合にのみ防御が必要であることを示した。

  まず、電子制御ユニット(EUS)の動作（通常、休眠、聴き取り）モードが、車載ネットワーク標準でどのように定義されているか、また車両でどのように実装されているかを分析する。この分析から、攻撃者は、本来ユーザエクスペリエンス/利便性の向上（リモート診断、遠隔温度制御など）用に設計された車載ネットワークのウェイクアップ機能を攻撃に悪用できることを発見した。車載ネットワークのバッテリー節約機能により、攻撃者は ECO を容易に起こし、Battery Drain (BD) や Denial-of-Body-control (DoB)、Unmanned control (UC)を搭載することができる。特に、BD 攻撃は、最悪 1 時間以内に車両のバッテリーを完全に消耗させることができ、DoB 攻撃は、関連 ECU をシャットダウンして車両とキーフォブ間の通信を無効にして車両を動かすことをできなくし、UC 攻撃は、ドア/トランクロックを制御して車両に物理的にアクセスできることを示した。
- フィジカルセキュリティ対策：異種プロトコルへの対応[106]

[105] https://dl.acm.org/doi/10.1145/3319535.3363190
[106] https://dl.acm.org/doi/10.1145/3307334.3326085

接続型自動運転車（CAV）には、多様な電子制御ユニット（ECU）が搭載されており、その多くが大量のデータを生成する。データはCANバス（車両の事実上の標準）の車載ネットワークを介してECU間で交換されている。また、CAVは物理インターフェースだけでなく、テレマティックコントロールユニット（TCU）を介したインターネットへのデータ接続も強化されているため、モバイルデバイスを介したリモートアクセスが可能である。CANバスで送信されるデータは暗号化されていないため、CANバスを利用したり、CANバスとの間でデータを読み書きしたりすることもできる。これは自動車のサイバーセキュリティに関する懸念を引き起こす。これまでに報告された車両セキュリティ攻撃の共通点の1つは、最終的にCANバスへの書き込みアクセスが必要になることである。

車両の動作に的を絞った意図的な変更を加えるために、CANインジェクション攻撃にはCANメッセージ形式の知識が必要である。この形式はOEM独自のものであり、単一メーカーの車両の異なるモデル間でも異なる可能性があるため、対象となる各車両のCANメッセージ形式を手動でリバースエンジニアリングする必要がある。これは、時間のかかる面倒なプロセスで、この問題を軽減するために、最小限の労力でほとんどのCANメッセージを翻訳できるLibreCANを開発した。複数の車両に対するこの広範な評価は、精度、カバレッジ、必要な手作業、およびあらゆる車両への拡張性の点でLibreCANの有効性を示している。

- フィジカルセキュリティ対策：IoT設置場所の確実な確認[107]

スマート倉庫システムは、RFIDタグを活用することで在庫データをリアルタイムで視覚化できるため、在庫切れを最小限に抑え、倉庫保管と人件費を削減できる。スマート倉庫の問題は、タグを置き忘れても簡単にRFIDタグを見つけることである。固定棚アイテムのタグの置き忘れの検出は、位置のあいまいさ、位相のラッピング、デバイスの多様性、および位相のあいまいさのために非常に困難である。理論的分析、シミュレーションベースの予測、実験的検証の組み合わせを使用して、Particle Swarm Optimization（PSO）、Synthetic Minority Oversampling TEchnology（SMOTE）、および密度ベースを統合したFINDSと呼ばれる置き忘れたタグを検出する効果的な方法を提案する。ノイズのあるアプリケーションの空間クラスタリング（DBSCAN）アルゴリズムにより、理論上の位相と測定された位相を互いに一致させ、タグの配置ミスによって引き起こされる位相シフトを観察する。FINDSは、アンテナの動きも外乱も必要としない。20個のタグを使用してFINDSのプロトタイプを実装し、そのパフォーマンスを評価しました。これは、2つの固定アンテナの場合にFINDSの精度が0.92よりも高いことを示している。

[107] https://par.nsf.gov/biblio/10100930

F) SaTC: CORE: Medium: Collaborative: Energy-Harvested Security for the Internet of Things（NSF Award 1704176）

IoT は、コンピュータの仮想世界を実際のアプリケーションに統合し、効率、経済性、生活の質の向上につながる。これには膨大な量の小型コンピュータが必要であり、このプロジェクトはそれらのコンピュータに持続可能な方法で電力を供給するという課題に取り組んでいる。小型コンピュータは、太陽、振動、温度勾配などからを確保する。

本プロジェクトの目的は、このようなエネルギー制約のあるデバイスが安全で完全なインターネット接続をサポートできる方法を示すことである。

このプロジェクトは、暗号化エンジニアリング、環境発電技術、フォーマル検証など、3 つのドメインからの洞察に基づいている。ハーベスタに適したバージョンの暗号化アルゴリズムは、クーポンを生成する事前に計算されたステップでパーティション化することによって作成される。余剰エネルギーがある場合にクーポンが作成され、後のフェーズでオンライン計算を高速化するために使用できる。本プロジェクトでは、標準のインターネットスタックから暗号化を最適化し、それをエネルギーハーベスターテクノロジーと統合する。

セキュリティ観点での主な成果には、下記の 3 件がある。

- IoT セキュリティ階層モデル : IoT データセキュリティと保護メカニズムの軽量・高費用対効果[108]

  臨床環境以外でも継続的な健康の監視と治療を継続できるようにするため、小型ワイヤレス生物医学装置のメーカーは、注射剤、移植剤、摂取物、ウェアラブルなどの IoT 化を促進してきた。このようなデバイスは、物理的なサイズ、消費電力の予算、ストレージ容量、および計算能力に制約がある。しかしその制約下でも、IoT 機器は機密の個人情報を扱い、刺激/薬物送達によって患者の健康に直接影響を与えるため、信頼を必要とする。本稿では、IoT デバイスの基本コンポーネントとしてセキュリティの役割を考察し、起こりうる攻撃に対するデータセキュリティと保護メカニズムの軽量で費用対効果の高い実装をサポートするために、汎用階層化モデルを提案する。

- IoT SIA（Secure Intermittent Architecture：セキュア断続アーキテクチャ）: 中断容認 IoT のセキュリティ : 自己認証・リモート構成証明・セキュア通信 : 断続的なコンプアプリケーション[109]

  エネルギー確保技術の進歩は、資源に制約のある IoT デバイスの電池に代わるものとなり、断続コンピューティングモデルである新しいコンピューティングパラダイムにつながっている。このモデルでは、ソフトウェアモジュールは、エネルギー不足

[108] https://ieeexplore.ieee.org/document/9184564
[109] https://ieeexplore.ieee.org/document/8714997

が発生したときに中断した場所から実行を継続する。電源オン状態に加えて電源オフ状態は、攻撃者から保護が必要である一方で、セキュリティメカニズムは、デバイスのパフォーマンス、リソース消費、およびコストオーバーヘッドが低い必要があるため、断続的なソフトウェアモジュールのセキュリティを強制することは困難である。本稿では、リソース制約のある IoT デバイスのセキュリティアーキテクチャである SIA（Secure Intermittent Architecture：セキュア断続アーキテクチャ）を提案する。SIA は、市販マイクロコントローラで利用できる低コストのセキュリティ機能を活用して、断続的ソフトウェアモジュールの電源オン状態と電源オフ状態の両方を保護する。このため、SIA は、自己認証、リモート構成証明、およびセキュリティ保護通信など、多くのセキュア断続コンピューティング（secure intermittent computing）機能を実現する。このアーキテクチャは、従来方式と比較して、断続的コンピューティングモジュールに対して、機密保持と整合性を提供する。SIA の特徴は、ハードウェアの変更を必要としないため、既存の IoT に直接適用できる。

- SICP（Secure Intermittent Computing Protocol:セキュア断続コンピューティンプロトコル）：安全なチェックポイント技術

  断続コンピューティングシステムは、エネルギーハーベスト電源などの一時的な電源の下でタスクを実行する。電源断中、プログラム実行状態でのチェックポイントを不揮発性メモリに保存する。電源が復旧すると、システム状態がチェックポイントから再構築され、計算が続行される。攻撃が電力中断を使用する場合のセキュリティリスクを分析し、チェックポイントデータの完全性、信頼性、機密性、継続性、および最新性を保護する必要性を実証する。これにより SICP と呼ばれる安全なチェックポイント技術を提案する。提案されたプロトコルには、次のプロパティがある。

  まず、①チェックポイントの再生に対して、すべてのチェックポイントを電源オン状態に関連付ける。次に、②すべてのチェックポイントは暗号化によって前のチェックポイントに連結され、連続性が提供されるため、プログラマは、電源喪失イベントを越えて、認証されたプログラムイメージなどの実行時のセキュリティプロパティを実行できる。第三に、③SICP は電力損失に対して「atomic and resistant」がある。

(5) **欧州の動き**（HORIZON2020 IoT Security & Privacy Cluster Project[110]）

HORIZON2020 IoT Security & Privacy Cluster Project（以下、H2020）は、EC がファンドする８プロジェクトで、期間は 2018 年～2020 年、フォーカス分野は、Solutions for Federation, Interoperability, Security and Privacy、予算は 37M Eur である。

８つのプロジェクトの概要、特徴を以下に示す

[110] https://ec.europa.eu/digital-single-market/en/secure-solutions-internet-things

A) SecureIoT（Predictive Security for IoT Platforms and Networks of Smart Objects）[111]

SecureIoT は、複数の IoT プラットフォームとスマートオブジェクトのネットワークにまたがる次世代のダイナミックで分散型の IoT システムへ、さまざまな予測型 IoT セキュリティサービスを実装することで、システムの安全を保護するものであり、以下を実現する。

- End-to-End セキュリティモニタリング（AI ベースの予測型セキュリティ）
- IoT プラットフォーム間のセキュリティインターオペラビリティの実現
- クロスプラットフォームとクロスバーチカル

SecureIoT の技術的な特徴は、IoT アプリケーションのための最先端のリファレンスアーキテクチャ（RA）（Industrial Internet Consortium、OpenFog Consortium、Platform Industrie 4.0 の RA など）に沿って予測的なセキュリティサービスを構築し、IoT システムのエッジとコアの両方でセキュリティビルディングブロックを指定するための基礎となることである。SecureIoT は、セキュリティデータ収集、セキュリティ監視、予測セキュリティメカニズムの具体的な実装を提供し、リスク評価、規制や指令（GDPR、NIS、ePrivacy など）に対するコンプライアンス監査、プログラミングアノテーションに基づく IoT 開発者へのサポートなど、統合されたサービスを提供するための基礎となる。サービスはオープンで、SECaaS（Security-as-a-Service）パラダイムに基づいている。

B) SEMIoTICS（Smart End-to-end Massive IoT Interoperability, Connectivity and Security）[112]

SEMIoTICS は、既存の IoT プラットフォーム上に構築（ビルトオン）されたパターン駆動型のフレームワークで、IoT およびインダストリアル IoT（IIoT）アプリケーションにおける安全でディペンダブルな動作と半自動動作を可能とし、保証する。パターンには、個々のスマートオブジェクトのセキュリティ、プライバシー、依存性、相互運用性（SPDI）に関する特性と、それらを含むオーケストレーションに対応する特性との間の実証済みの依存関係がエンコードされている。

SEMIoTICS フレームワークには、以下の特徴がある。

- 異機種のスマートオブジェクト、ネットワーク、クラウドを含むクロスレイヤーのインテリジェントな動的適応のサポート
- 水平および垂直方向のドメイン内での複雑さやスケーラビリティのニーズに対応するためのスマートプログラマブルネットワーキングとセマンティック相互運用性メカニズムの実現

---

111 https://secureiot.eu/

112 https://www.semiotics-project.eu/

特に、セキュリティ機能については、ネットワークレイヤからアプリケーションレイヤまでの利用者の認証や、IoT 機器の同定、アプリケーションでのプライバシー・センシティブな情報の取扱い、エンドツーエンドでのセキュアなネットワーキング機能を提供する。

C) ENACT（Development, Operation, and Quality Assurance of Trustworthy Smart IoT Systems）[113]

ENACT は、以下を実現する新しい IoT プラットフォーム機能を実現する。

- 信頼できるスマート IoT システムで、信頼性を強化するエンドツーエンドのセキュリティとプライバシーや、回復力、ロバスト性、「協調的な」動作と動作間の競合に関連する課題を考慮した DevOps の提供
- 既存および新規の IoT プラットフォームなど（例：FIWARE、SOFIA、TelluCloud）の DevOps の円滑化

ENACT の技術的な特徴を下記に示す。

- 信頼性あるスマート IoT システムの継続的な提供では、センサーやアクチュエータ、ソフトウェアサービス、各構成のオーケストレーションの実現と IoT やエッジ、クラウド環境にまたがるこのオーケストレーションの自動テストや実装機能を提供
- アジャイルサポートの提供では、コンテキストの変化に応じてシステム自体にダイナミックな適応を可能とするメカニズムの提供
- 継続的な品質保証（quality assurance）のサポートでは、システムの継続的な評価や、システムの構造や振る舞い、インフラストラクチャのコントロールと適応、ロバスト性やレジリエンスの強化、エンドツーエンドセキュリティやプライバシーのためのメカニズムの提供、新たなリスク主導の意思決定支援機能の提供
- 既存 IoT プラットフォーム、レガシーやプロプライエタリな既存製品のソフトウェアやデバイスの活用では、ENACT DevOps フレームワークの個別の実装方法から独立した形での提供

D) IoTCrawler（a Search Engine for the Internet of Things Devices）[114]

IoTCrawler は、適応性と拡張性に優れたクローリング、インデックス作成、セマンティックデータ/サービスの検索と統合、プライバシーとセキュリティを実現し、オープンな IoT エコシステムを実現するためプラットフォームで、異なるプラットフォーム間の統合と相互運用性を有する。

---

[113] https://www.enact-project.eu/
[114] https://iotcrawler.eu/

IoTCrawler の技術的な特徴を以下に示す。

- 安全な IoT 情報アクセスとプライバシー保護のための分散型台帳技術と属性ベースの暗号化を統合した分散型アクセス制御の提供
- 一度認証された利用者によるデータアクセスの際のポリシーによる厳密な管理
- 異なるドメイン間での事前の信頼関係を持つことなく、IoTCrawler 検索エンジンによる IoT データへのアクセスの際に、分散型台帳技術（ブロックチェーンでインスタンス化された）による、共通のポリシーに合意するプロセスの提供

E) BRAIN-IoT （IoT: Model Based Framework for Dependable Sensing & Actuation in Intelligent Decentralized IoT Systems）[115]

BRAIN-IoT は、異なる IoT プラットフォームでの完全に分散化された、構成可能で動的な連合体において、スマートな協調動作をサポートするフレームワークと方法論を提供する。

オープンセマンティックモデルを使用して、相互運用可能なソリューションのプロトタイピングと統合を容易するモデルベースの開発ツールをサポートすることで、相互運用可能なオペレーションとデータと制御の交換機能を提供する。

全体として、高度に動的で分散した IoT シナリオにおいて AAA(Authentication, Authorization and Accounting)機能を提供する一貫したフレームワークにより、プライバシーと制御に関する機能を埋め込むソリューションあわせて、安全な運用を保証する。

BRAIN-IoT の技術的な特徴を以下に示す。

- 相互運用性と動的なプラットフォームの連合（IoT デバイスと動的にリンクしたシェアードセマンテックモデル）
- AI 機能に基づくスマート協働の振る舞い
- ダイナミック AAA 機能
- プライバシーの組込みとプライバシーコントロール
- ダイナミックコミッショニングと再構成（エッジ/クラウドの実装とバランシング）

F) SOFIE（Secure Open Federation for Internet Everywhere）[116]

SOFIE は、ブロックチェーンや台帳間技術を含む分散台帳技術（DLT）を使用して、アクチュエーションや監査可能性、スマートコントラクト、アイデンティティと暗号

[115] http://www.brain-iot.eu/
[116] https://www.sofie-iot.eu/

化キーの管理を可能にし、事実上無制限のスケーラビリティを持つ完全に分散化された安全でオープンなIoTフェデレーションのアーキテクチャとフレームワークを提供する。

SOFIEの技術的な特徴を以下に示す。

- 既存のIoTプラットフォーム間の相互運用性を可能とするセキュアなオープンでフェデレーション
- 複数の分散台帳技術（DLT）の同時利用
- オープンデータマーケットを可能とするIoTビジネスプラットフォームの提供

G) CHARIoT（Cognitive Heterogeneous Architecture for Industrial IoT）[117]

CHARIOTは、IoTシステムのプライバシー・セキュリティ・安全性（PSS）に向けての統一的なアプローチをサポートする設計手法とコグニティブコンピューティングプラットフォームを提供する。

CHARIOTの技術的な特徴を以下に示す。

- 安全なクリティカルシステム（safety as cross-cutting concern）の設計とオペレーションのための方法論フレームワーク
- 安全な方法での安全なクリティカルシステムとIoTシステムとの連携に対するオープンなコグニティブIoTアーキテクチャとプラットフォーム
- ランタイムIoTプライバシー、セキュリティ、セーフティ・スーパービジョンエンジン（IPSE）
  - PKIとブロックチェーン技術によるプライバシーエンジン
  - ファームウェアのセキュリティインテグリティチェック
  - IoTセーフティ・スーパービジョンエンジン
- 予測分析とダッシュボード

H) SerIoT（Secure and Safe Internet of Things）[118]

SerIoTでは、セキュアなIoTプラットフォームとネットワークを実装するためプラットフォームを提供し、単一のネットワークコンポーネント（IoTプラットフォーム＆デバイス、ハニーポット、SDN（Software Defined Networking）ルーター、オペレーターのコントローラーなど）による動的処理と分散処理の両方に基づいたクロスレイヤー的な方法で、IoTプラットフォームとネットワークにおける情報セキュリティを最適化することができる。

SerIoTの技術的な特徴を以下に示す。

---

[117] https://www.chariotproject.eu/
[118] https://seriot-project.eu/

- SDN 技術による分散 IoT サブシステム間を結ぶコグニティブパケットネットワークの構築
- サービス品質が良くエネルギー効率の高い安全なマルチホップルートを探索するスマートパケット(SP)の利用
- 全体的なネットワーク性能の向上と経路決定のためのランダムなニューラルネットワークの活用（セキュアアウェアルーティング）

(6) その他の動き

A) OAuth 2.0[119]（都市 OS のセキュリティ）

OAuth 2.0 では、ユーザが、サービス上にホストされている自分のデータへのアクセスを、自分のクレデンシャルズ（ID &パスワード）を渡すことなく、第三者のアプリケーションに許可するためのフレームワークである。RFC 6749（The OAuth 2.0 Authorization Framework）で定義される。

OAuth 2.0 の技術的な特徴としては、ユーザ、第三者(サービスなどアプリ側)、サービス提供者間においてユーザの同意の下、「アクセストークン」をやりとりする手順を標準化した API アクセス認可のための仕様となっており、以下の特徴がある。

- ユーザは第三者に ID/パスワードではなく、認証・同意の結果として、「アクセストークン」を渡すことによりアクセスの認可を与える。
- アクセストークンは、第三者がユーザの代理でサービスにアクセスするための許可証であり、これにより以下の制御が可能となる。
  - 第三者からの ID/パスワードの漏洩や不正利用が防止できる
  - 第三者がサービスへ代理アクセスする際、ユーザの許可した範囲・機能(scope)のみに限定できる
  - 第三者ごとに API のアクセス可否を制御できる

[119] https://openid-foundation-japan.github.io/rfc6749.ja.html

5.2 本プロジェクトの国際的な目標水準の妥当性

(1) 妥当性評価の進め方

SIP-CPS の技術の国際的な目標水準の妥当性を検証する方策として、5.1 項で調査したプロジェクト・製品（以下、調査技術）の特徴と、SIP-CPS 技術の特徴の類似性、対応関係を調査・分析する。

この調査・分析は、対応関係があるものは、方向性は同じで、比較対象が可能なもの、SIP-CPS 技術にはあるが調査技術にはないものは、先進的な取り組み、調査技術にはあるが SIP-CPS 技術にはないものは追加候補の目標と捉えることができると考え行った調査・分析である。

SIP-CPS 技術の特徴づけるものとして次の４つの軸を設けた。

１つ目は、研究開発テーマが目指している信頼形成のフェーズの軸である。具体的には、研究開発テーマが掲げている、創出・証明、構築・流通、検証・維持の３つのフェーズとした。

２つ目は、研究開発テーマが掲げている信頼形成の対象の軸である。具体的には、サイバー、フィジカルに加え、人・組織とサプライチェーンの 4 つを対象とした。

研究開発の観点の軸については、SIP-SIP が評価軸としている、機能性、効率性、信頼性、使用性の 4 つを設けた。

社会実装の観点の軸では、同じく、有効性、コスト、運用性、影響、波及効果、使用性の６つを設けた。

また、国際水準に盛り込むべき事項の候補を見つけるため、その他想定外と思われる事項もリストアップしている。次節で紹介する。

なお、調査したプロジェクトの特徴と SIP-CPS 技術の特徴は、以下のように対応付けている。

- 信頼形成のフェーズ（研究開発テーマ）

  信頼形成のフェーズについては、ソフトウェアやシステムの改ざん防止などを意識したセキュリティ対策を行っているシステムは「課題 A（信頼の創出・証明)」、外部システムとのつながりを意識したセキュリティ対策を行っているシステムは「課題 B（信頼チェーンの構築・流通)」、ログを用いてセキュリティ対策を行っているシステムは「課題 C（信頼チェーンの検証・維持)」の研究テーマに対応付けることとした。

- 信頼形成の対象

  信頼形成の対象については、外部システムとのつながりを意識したセキュリティシステムは「サプライチェーン」、運用や人的ミスを意識したセキュリティシステムは「人・組織」、IoT を意識したセキュリティシステムは「フィジカル」に対応付けることとした。

- 研究開発の観点

研究開発の観点では、前例のないセキュリティ対策機能を陽に謳っているシステム（他薦、自薦）は「機能性」、処理時間の短縮や性能向上、対象とする機器数の増加などを陽に謳っているシステムは「効率性」、セキュリティ異常に気付くまでの時間や復旧までの時間など、セキュリティ異常の状態の短縮を陽に謳っているシステムは「信頼性」、対象とする機器やプロトコル等バリエーションの拡大を陽に謳っているシステムは「使用性」に対応付けることとした。

- 社会実装の観点

社会実装の観点として、ユーザに取っての効用・価値の拡大を陽に意識したシステムは「有効性」、導入コストや運用コストなどの削減を陽に意識したシステムは「コスト」、自動設定や自立運用などを陽に意識したシステムは「運用性」、他のシステムへの波及や影響などを陽に意識したシステムは「影響」、該セキュリティシステムを構成要素として含み、メインのシステムを支えるなど、より上位概念のシステム、サービスなどを陽に意識システムは「波及効果」、該セキュリティシステムの使い勝手などを陽に意識したシステムは「使用性」に対応付けることとした。

(2) 信頼形成のフェーズ（研究開発テーマ）の観点から見た妥当性分析

A) 課題 A の研究開発テーマ

ソフトウェアやシステムの改ざん防止などを意識したセキュリティ対策を行っているシステムは、課題 A（信頼の創出・証明）の研究テーマに繋がっていくと捉えて分析を行った。

この観点では、Finalists RSAC Sandbox 2020 では、「AppOmni 」、「BluBracket 」、「ForAllSecure （Mayhem）」、「Sqreen 」、「Vulcan Cyber」の 5 システムが、既存製品では、「Contrast Security」の 1 システムが、H2020 では、「ENACT (Development, Operation, and Quality Assurance of Trustworthy Smart IoT Systems)」の 1 システムが類似機能を有している。

この内、Finalists RSAC Sandbox 2020 製品、既存製品は、サイバー（ソフトウェア）に限定しており、SIP-CPS の信頼形成の対象と比べ、範囲が狭いと思われる。

H2020 の「ENACT」は、フィジカルに加え、人・組織も信頼形成の対象としている。この調査結果から、H2020 の「ENACT」が、SIP-CPS の信頼形成と比較的近い研究領域と考えられる。

B) 課題 B の研究開発テーマ

外部システムとのつながりを意識したセキュリティ対策を行っているシステムは、課題 B（信頼チェーンの構築・流通）の研究テーマに繋がっていくと捉えて分析を行った。

この観点では、Finalists RSAC Sandbox 2020 では、「AppOmni」、「ForAllSecure（Mayhem）」、「Obsidian Security」、「SECURITI.ai」、「Tala Security」、「Vulcan Cyber」の 6 システム、既存製品では、「ZeroFOX」、「baffle」、「ENVEIL」、「GreatHorn」、「RedLock/Prisma（パロアルトネットワークスにより買収される）」の 5 システム、H2020 では、「SecureIoT（Predictive Security for IoT Platforms and Networks of Smart Objects）」、「SEMIoTICS （Smart End-to-end Massive IoT Interoperability, Connectivity and Security）」、「 ENACT(Development, Operation, and Quality Assurance of Trustworthy Smart IoT Systems)」、「IoTCrawler （Search Engine for the Internet of Things）」、「BRAIN-IoT（IoT: Model Based Framework for Dependable Sensing & Actuation in Intelligent Decentralized IoT Systems）」、「CHARIoT（Cognitive Heterogeneous Architecture for Industrial IoT）」の 6 システムが類似機能を有している。

上記と同様、H2020 の「SecureIoT」、「SEMIoTICS」、「ENACT」、「IoTCrawler」、「BRAIN-IoT」、「CHARIoT」が、SIP-CPS と比較的近い研究領域と考えられる。

C) **課題 C の研究開発テーマ**

ログを用いてセキュリティ対策を行っているシステムは、課題 C（信頼チェーンの検証・維持）の研究テーマに繋がっていくと捉えて分析を行った。

この観点では、Finalists RSAC Sandbox 2020 では、「ForAllSecure（Mayhem）」、「Tala Security」、「Vulcan Cyber」の 2 システムが、既存製品では、「Unifyid」、「UpLevel」の 2 システムが、H2020 では、「SecureIoT（Predictive Security for IoT Platforms and Networks of Smart Objects）」、「ENACT（Development, Operation, and Quality Assurance of Trustworthy Smart IoT Systems）」、「BRAIN-IoT（IoT: Model Based Framework for Dependable Sensing & Actuation in Intelligent Decentralized IoT Systems）」の 2 システムが類似機能を有している。

上記と同様、H2020 の「SecureIoT」、「ENACT」、「BRAIN-IoT」が、SIP-CPS と比較的近い研究領域と考えられる。

(3) **信頼形成の対象の観点から見た妥当性分析**

A) **外部システム（サプライチェーン）**

外部システムとのつながりを意識したセキュリティシステムは、サプライチェーンのセキュリティ対策に繋がっていくと捉えて分析を行った。

この観点では、Finalists RSAC Sandbox 2020 では、「ForAllSecure（Mayhem）」、「SECURITI.ai」の 2 システムが、既存製品では、「ENVEIL」の 1 システムが、H2020 では、「SEMIoTICS （Smart End-to-end Massive IoT Interoperability, Connectivity and Security）」、「IoTCrawler（Search Engine for the Internet of Things）」、「BRAIN-IoT（IoT: Model Based Framework for Dependable Sensing & Actuation in Intelligent Decentralized IoT

Systems)」、「SOFIE (Secure Open Federation for Internet Everywhere)」、「CHARIoT（Cognitive Heterogeneous Architecture for Industrial IoT）」の 4 システムが同様の信頼形成の対象を有している。

この結果から、Finalists RSAC Sandbox 2020 の「ForAllSecure （Mayhem）」、「SECURITI.ai 」及び、既存製品の「ENVEIL」は、フィジカルセキュリティについて明確に言及はしていないが、システム間のつながりを意識しており、サプライチェーン観点で、SIP-CPS と比較的近いシステムの可能性がある。

H2020 の「SEMIoTICS」、「IoTCrawler」、「BRAIN-IoT」、「CHARIoT」は、フィジカルも含め、サプライチェーン観点で、SIP-CPS と比較的近いシステムの可能性がある。

B) **人・組織（運用、人的ミス）**

運用や人的ミスを意識したセキュリティシステムは、人・組織に伴うセキュリティ対策に繋がっていくと捉えて分析を行った。

この観点では、Finalists RSAC Sandbox 2020 では、「AppOmni」、「BluBracket」、「Obsidian Security」、「SECURITI.ai」、「Tala Security」の 5 システムが、既存製品では、「GreatHorn」、「Unifyid」、「UpLevel」の 3 システムが、H2020 では、「SEMIoTICS（Smart End-to-end Massive IoT Interoperability, Connectivity and Security）」、「ENACT（Development, Operation, and Quality Assurance of Trustworthy Smart IoT Systems）」の 2 システムが同様の信頼形成の対象を有している。

この結果から、Finalists RSAC Sandbox 2020 の「AppOmni」、「BluBracket」、「Obsidian Security」、「SECURITI.ai」、「Tala Security」及び、既存製品の「GreatHorn」、「Unifyid」、「UpLevel」は、フィジカルセキュリティについて明確に言及はしていないが、運用や人的ミスを意識しており、信頼の流通の観点で、SIP-CPS と比較的近いシステムの可能性がある。

H2020 の「SEMIoTICS」、「ENACT」は、フィジカルも含め、信頼の流通の観点で、SIP-CPS と比較的近いシステムの可能性がある。

C) **フィジカル**（IoT）

IoT を意識したセキュリティシステムは、フィジカルを対象としたセキュリティ対策に繋がっていくと捉えて分析を行った。

この観点では、Finalists RSAC Sandbox 2020 製品には、陽にフィジカルを対象とした製品は見つからなかった。

既存製品では、「CATO Networks」が IoT を意識している。

H2020 の研究開発テーマは、全てフィジカルを対象としている。

(4) 研究開発の観点から見た妥当性分析

研究開発の観点では、Finalists RSAC Sandbox 2020 製品は、セキュリティの専門家により、複数のシステムの中から選ばれていることから、他薦により研究の優位点を有していると考えられる。

また、H2020 は、EU において、選ばれた研究開発システムであり、設定された目標が研究の優位点を有していると考えられる。

既存製品は、既に達成できている技術を用いていると考えられることから、研究開発の観点の比較対象としないこととした。同様に、米国政府の動きは、課題の整理と捉え比較対象のとしないこととした。

以上の整理の元、評価軸毎に分析した結果を以下に示す。

A) 機能性

前例のないセキュリティ対策機能を、他薦、自薦しているシステムは、研究開発の観点で機能性を意識したセキュリティ対策に繋がっていくと捉えて分析を行った。

この観点では、Finalists RSAC Sandbox 2020 製品では、「AppOmni」は SaaS 環境のデータアクセスの可視性と管理、「ForAllSecure（Mayhem）」は継続的自動セキュリティテスト、「Obsidian Security」は継続的な行動分析と強力アラート、「SECURITI.ai」はハイリスクデータの特定、「Sqreen」は高視認性（インシデントリアルタイム監視、合理化、など）、「Tala Security」はクライアントセキュリティ展開の加速、「Vulcan Cyber」は脆弱性修復ライフサイクルの自動化・調整、を自薦での研究観点の機能として謳っている。

H2020 では、「SecureIoT」は IoT プラットフォーム間のセキュリティの担保、「SEMIoTICS」は異種プラットフォーム間でのセキュリティ機能の実現、「ENACT」はスマート IoT システムのための DevOp 機能の提供、「IoTCrawler」はセキュリティやプライバシーを考慮した IoT 機器のクローリングや検索機能、「BRAIN-IoT」は異なるプラットフォーム間での IoT セキュリティ機能の実現、「SOFIE」は既存の IoT プラットフォーム間での相互運用性の実現、「CHARIoT」は PKI やブロックチェーン技術によるプライ橋保護やセキュリティの実現、「SerIoT」は IoT プラットフォームを結ぶ安全性を考慮したネットワーク技術の実現、を他薦（H2020 で採択）での研究観点の機能として謳っている。

上記のように、研究開発観点での機能性では、個々のシステムごとに、それぞれ他との差別化した機能を示している。SaaS 環境、自動修復、継続的な行動分析と強力アラート、ハイリスクデータの特定、高視認性（インシデントリアルタイム監視）など、SIP-CPS が目指している機能と類似しているものがある一方、IoT プラットフォームを対象とした各種機能など必ずしも SIP-CPS では陽に触れられていない機能も存在している。

B) **効率性**

処理時間の短縮や性能向上、対象とする機器数の増加などを他薦、自薦しているシステムは、研究開発の観点で効率性を意識したセキュリティ対策に繋がっていくと捉えて分析を行った。

この観点では、Finalists RSAC Sandbox 2020 製品では、「BluBracket」は把握できないコード急増対応、「ForAllSecure（Mayhem）」は前例のない速度、規模、精度で欠陥発見、を自薦での研究観点の能力として謳っている。

H2020 では、「SerIoT」が最適な経路選択技術、を他薦（H2020 で採択）での研究観点の能力として謳っている。

このように研究開発観点での効率性では、前例のない速度、規模、精度で欠陥発見は、SIP-CPS の研究目標と類似しているが、フィジカルセキュリティを陽には謳っていないため、目標が異なっている可能性もある。

C) **信頼性**

セキュリティ異常に気付くまでの時間や復旧までの時間など、セキュリティ異常の状態の短縮を意識したセキュリティシステムは、研究開発の観点で信頼性を意識したセキュリティ対策に繋がっていくと捉えて分析を行った。

この観点では、Finalists RSAC Sandbox 2020 製品には対象技術は見つからなかった。

H2020 では、「SOFIE」は分散台帳技術の利用、「CHARIoT」は PKI やブロックチェーン技術などの利用、「SerIoT」は最適な経路選択技術、を他薦（H2020 で採択）での研究観点の能力として謳っている。

このように研究開発観点での信頼性では、分散台帳技術の利用や、PKI やブロックチェーン技術などの利用は、SIP-CPS と類似の目標設定を行っている可能性がある。

D) **使用性**

対象とする機器やプロトコル等バリエーションの拡大を意識したセキュリティシステムは、研究開発の観点で使用性を意識したセキュリティ対策に繋がっていくと捉えて分析を行った。

この観点では、Finalists RSAC Sandbox 2020 製品、H2020 に対象技術は見つけられなかった。

(5) **社会実装の観点から見た妥当性分析**

A) **有効性**

ユーザに取っての効用・価値の拡大を陽に意識したセキュリティシステムは、社会実装の観点で有効性を意識したセキュリティ対策に繋がっていくと捉えて分析を行った。

この観点では、Finalists RSAC Sandbox 2020 製品では、「AppOmni」は利便性とセキュリティのバランスの両立、「BluBracket」は包括的なエンタープライズセキュリティ、「Obsidian Security」はインサイダー脅威監視、「SECURITI.ai」はグローバルなプライバシー規制を遵守、「Sqreen」はランタイムアプリケーションの自己保護、「Tala Security」は標準ベースのセキュリティをアクティブ化、「Vulcan Cyber」は治療（修復）、を自薦での社会実装観点の機能として謳っている。

既存製品では、「ZeroFOX」は一つのプラットフォームで多くのデジタル情報の保護か可能、「baffle」は既存アプリケーションでのデータ暗号化を容易に導入可能、「CATO Networks」はコストの削減や SLA 保証のネットワークの利用、「CLAROTY」は既存 IT 環境に加え OT 環境のセキュリティを管理することができる、「Contrast Security」はソフトウェアの開発におけるアプリケーションのセキュリティの担保、「ENVEIL」は暗号化された状態でのデータ利用が可能、「GreatHorn」は既存メールシステムへのセキュリティ機能をアドオンすることが可能、「RedLock/Prisma」は既存クラウド機能にセキュリティ機能を適用することができ、有効である、を自薦での社会実装観点の機能として謳っている。

H2020 では、「SecureIoT」は複数の IoT プラットフォームにまたがってセキュリティの対応が可能、「SEMIoTICS」は複数の IoT プラットフォームにまたがってセキュリティ機能の実現、「ENACT」はスマート IoT システムでの開発から運用までを対応でき有効性が高い、「IoTCrawler」は分散型台帳技術やポリシーベースによるセキュリティ機能の実現、「BRAIN-IoT」は複数の異種システムとの相互運用性の実現、「SOFIE」は分散台帳技術による安全性の高い相互運用性の実現、「CHARIoT」は PKI やブロックチェーン技術などの利用による安全性の確保、「SerIoT」は安全なマルチホップ技術やセキュアアウェアルーティンなどの技術の適用、を他薦（H2020 で採択）での社会実装観点の機能として謳っている。

このように、社会実装における有効性には、多様なアピールがなされている。

既存 IT 環境に加え OT 環境のセキュリティを管理や、ソフトウェアの開発におけるアプリケーションのセキュリティの担保、分散型台帳技術やポリシーベースによるセキュリティ機能の実現など、一部 SIP-CPS との対応関係が取れそうな有効性も存在している。

B) **コスト**

導入コストや運用コストなどの削減を陽に意識したセキュリティシステムは、社会実装の観点でコストを意識したセキュリティ対策に繋がっていくと捉えて分析を行った。

この観点では、Finalists RSAC Sandbox 2020 製品では、「BluBracket」は高速ソフトウェア開発ライフサイクル、「ForAllSecure（Mayhem）」は手動テストの労力を大幅に削減、

を自薦での社会実装観点の機能として謳っている。

既存製品では、「ZeroFOX」はクラウドサービス（SaaS)での提供のため比較的導入が容易、「CATO Networks」はネットワークプラットフォームの利用のため導入が容易、を自薦での社会実装観点の機能として謳っている。

H2020 では、コストについて言及している技術は見つからなかった。

このように、社会実装におけるコストでは、手動テストの労力を大幅に削減、クラウドサービス（SaaS)での提供のため比較的導入が容易、高速ソフトウェア開発ライフサイクルなど、SIP-CPS が目指す内容と類似していると思われる項目も存在している。

C) **運用性**

自動設定や自立運用などを陽に意識したセキュリティシステムは、社会実装の観点で運用性を意識したセキュリティ対策に繋がっていくと捉えて分析を行った。

この観点では、Finalists RSAC Sandbox 2020 製品では、「AppOmni」は継続的なコンプライアンス(標準仕様準拠)、「Sqreen」は可視性、「Vulcan Cybe」は修復プロセスの自動化、を自薦での社会実装観点の機能として謳っている。

既存製品では、「ZeroFOX」はクラウドサービス（SaaS)での提供のため比較的導入が容易、「baffle」は単独ソリューションとして提供可能(独立性が高い)、「CATO Networks」は SD（ソフトウェアデファイン）-WAN で利用時の独立性が高い、「CLAROTY」は単独のプラットフォームとして運用できる、「Contrast Security」はアプリケーション内に組み込まれたエージェントによる運用、「ENVEIL」は既存システムに導入可能、「GreatHorn」は既存メールシステムに導入可能、「RedLock/Prisma」は既存クラウドシステムへの適用が可能、「Unifyid」は単独のシステムとして利用可能、を自薦での社会実装観点の機能として謳っている。

H2020 では、「SecureIoT」は IoT プラットフォーム間のインターオペラビリティを実現、「SEMIoTICS」は IoT プラットフォーム間のインターオペラビリティを実現、「ENACT」はスマート IoT システムのための DE（開発） v Ops（運用）機能であり、運用性は高い、「IoTCrawler」は異なるドメイン（システム）への適用が可能、「BRAIN-IoT」は相互運用性と動的なプラットフォームの連合化、「SOFIE」は既存 IoT プラットフォーム間での相互運用性、「CHARIoT」はオープンな IoT プラットフォームの安全な運用、「SerIoT」は SDN をベースにした安全性を考慮したネットワーク技術の適用、を他薦（H2020 で採択）での社会実装観点の機能として謳っている。

このように、社会実装における運用性では、多様なアピールがなされている。この調査結果からはやはり運用性が重要であることが見て取れる。

特に、導入実績もある既存製品がアピールしている、既存との親和性には注目しておく必要がある。

D) **影響**

他のシステムへの波及や影響などを陽に意識したセキュリティシステムは、社会実装の観点で影響を意識したセキュリティ対策に繋がっていくと捉えて分析を行った。

この観点では、Finalists RSAC Sandbox 2020 製品、既存製品、H2020 とも本指標に関する技術は見つけられなかった。

E) **波及効果**

該セキュリティシステムを構成要素として含み、メインのシステムを支えるなど、より上位概念のシステム、サービスなどを陽に意識したセキュリティシステムは、社会実装の観点で波及効果を意識したセキュリティ対策に繋がっていくと捉えて分析を行った。

この観点では、Finalists RSAC Sandbox 2020 製品では、「SECURITI.ai」はグローバルなプライバシー規制を遵守し、顧客との信頼を築く、を自薦での社会実装観点の機能として謳っている。しかし、既存製品、H2020 とも本指標に関する技術は見つけられなかった。

このように、社会実装における波及効果を謳っているシステムは 1 システムのみであるが、世界標準への準拠による顧客との信頼構築は、SIP-CPS でも重要な観点と思われる。

F) **使用性**

該セキュリティシステムの使い勝手などを陽に意識したセキュリティシステムは、社会実装の観点で使用性を意識したセキュリティ対策に繋がっていくと捉えて分析を行った。

この観点では、Finalists RSAC Sandbox 2020 製品、H2020 とも本指標に関する技術は見つけられなかった。

既存製品では、「ZeroFOX」はクラウドサービスで提供する保護プラットフォームのため容易に利用可能、「CATO Networks」はアプリケーションの開発プロセスの中にセキュリティ機能が組み込まれるため使い勝手は良い、「ENVEIL」は既存システムを利用でき導入が容易、「Unifyid」はパスワード等を用いないため使用性は高い、を自薦での社会実装観点の機能として謳っている。

このように、社会実装における使用性ではセキュリティを意識しないでセキュアな環境を利用できることをアピールしており、この視点は SIP-CPS でも重要な観点と思われる。

5.3 国際的な目標水準に盛り込む事項

(1) 目標水準候補の抽出

5.2 節(1)でも示したように、国際水準に盛り込むべき事項の候補として、SIP-CPS の目標には陽に示されていない事項をリストアップした。その結果を以下に示す。

A) Finalists RSAC Sandbox 2020

Finalists RSAC Sandbox 2020 製品では、「AppOmni」では＜標準準拠性＞、「BluBracket」で＜セキュリティポリシーへの追従性・自動実施＞、「Obsidian Security」では＜継続的自律テスト＞、「SECURITI.ai」では＜可視性と監視の統一＞、「Sqreen」では＜プライバシー（個人権利）とのバランス＞、「Tala Security」では＜高視認性＞、「Vulcan Cyber」では＜プライバシーとユーザデータの整合性＞が抽出できる。

B) 既存製品

既存製品では、「CATO Networks」では＜ネットワークの意識＞、「Contrast Security」では＜未知の脆弱性＞、「ENVEIL」では＜既存システムの変更不要＞、「RedLock/Prisma」では＜アプリケーションに対するリスク制御等の一貫性＞が抽出できる。

C) H2020

H2020 では、「SEMIoTICS」では＜異機種＞、「ENACT」では＜既存の活用＞、「BRAIN-IoT」では＜異種システム＞、「SOFIE」では＜オープン性＞、「SerIoT」では＜ネットワークを意識＞が抽出できる。

D) NSF Program Award

NSF Program Award では、「CPS: Breakthrough: Secure Interactions with Internet of Things」では＜多様なプロトコル対応＞、「SaTC: CORE: Medium: Collaborative: Energy-Harvested Security for the Internet of Things」では＜新たな情報処理環境：断続的コンピューティング＞が抽出できる。

E) NISTIR

NISTIR では、「IoT Device Cybersecurity Capability Core Baseline（NISTIR 8259A）」では＜IoT のサイバーセキュリティ状態の認識＞、「Impact Analysis Tool for Interdependent Cyber Supply Chain Risks（NISTIR 8272）」では＜サプライチェーンに関する影響度等に関するスコア＞が抽出できる。

(2) 国際的な目標水準に盛り込む基準（案）

前項で示した前半 3 グループから抽出した基準候補は、＜標準準拠性＞、＜セキュリティポリシーへの追従性・自動実施＞、＜継続的自律テスト＞、＜可視性と監視の統一＞、＜プライバシー（個人権利）とのバランス＞、＜高視認性＞、＜プライバシーとユーザデータの整合性＞、＜ネットワークの意識＞、＜未知の脆弱性＞、＜既存システムの変更不要＞、＜アプリケーションに対するリスク制御等の一貫性＞、＜異機種＞、

＜既存の活用＞、＜異種システム＞、＜オープン性＞、＜ネットワークを意識＞となっている。

後半の米国政府の活動からは、＜多様なプロトコルの生成ツール＞、＜新たな情報処理環境：断続的コンピューティング＞、＜IoT サイバーセキュリティ状態の認識＞、＜サプライチェーンに関する影響度等に関するスコア＞となっている。

これらの特徴を整理すると、前半は、標準、ポリシー、ヒューマン対応（プライバシー、視認性)、未知、異種、既存、オープン、ネットワークなど、セキュリティシステムが意識し、連携、協調対象となるオープンなセキュリティ環境を連想させる用語が多く含まれている。

また、米国政府の活動内容からは、IoT やサプライチェーンが内在しているセキュリティリスクを評価指標やアーキテクチャとして具体化しており、オープンなセキュリティ環境に対する対応の手段を示しているとも捉えることができる。

一方、目標事項としては、ある程度の具体性も必要なことから、米国政府の活動から抽出できる項目に着目する選択肢も考えられる。

これらの結果から、以下の 4 点を、国際的な目標水準に盛り込む基準（案）として提案する。

- 制御プロトコルなどの既存システム、多種多様な機器などの多様性への対応力
- 未知、オープン、ポリシーの変化など想定外の事態に対する対応力
- サプライチェーンにおける影響スコア、相互依存スコア、保証スコアなどサプライチェーンの相互干渉への対応力
- IoT ならではの要件を考慮したセキュリティ環境（断続コンピューティング、設置場所、IoT の汚染度合い、など）への対応力

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アメリカ合衆国とヨーロッパを中心に調査・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製品を対象に、それらのプロジェクトの達成目標レベルを調査した。

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の第一歩として、アメリカ合衆国の NIST 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。

また海外における技術開発プロジェクトの目標の中から、本プロジェクトの目標には含まれていない目標を抽出して分析することにより、本プロジェクトの国際的な目標水準に盛り込む基準として４点を提案した。

付表・付図

別表 A　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			
2017/10/31	GSMA IoT Security Guidelines – Complete Document Set	GSMA IoTセキュリティガイドライン - 完全ドキュメントセット		1									1			GSMA IoT セキュリティ・ガイドライン文書群の公開 本文書は、黎明期の「モノのインターネット」業界における IoT のセキュリティ問題に対す る共通理解の確立を目的とした、GSMA による一連のセキュリテ ィ・ガイドライン文書であり、下記4編の文書から成り立つ。これら一連のガイドライン文書は、サービスのライフサイクル全体を通じてセキュリティのベストプラクティスが実装されることを保証するために、安全性の高い IoT サービスを開発するための方法論を示すもので、IoT サービ スにおける一般的なセキュリティへの脅威と脆弱性を軽減する方法についての推奨事項を提示している。 本文書の適用範囲は、IoT サービスの設計と実装に関する推奨事項に限定される。また、本文書は、新たな IoT 仕様や標準の作成を促すことを意図したものではなく、現時点で利用 可能なソリューション、ベストプラクティスを示す。 1. CLP.11 – IoT セキュリティ・ガイドライン概要説明書 2. CLP.12 - IoT サービスのエコシステムに関する IoT セキュリティ・ガイドライン 3. CLP.13 - IoT セキュリティ・ガイドライン・エンドポイント・エコシステム 4. CLP.14 - ネットワーク事業者向け IoT セキュリティ ガイドライン	https://www.gsma.com/iot/resources/gsma-iot-security-guidelines-complete-document-set/	日本語版あり https://www.gsma.com/iot/wp-content/uploads/2018/07/GSMA-IoT-Security-Guidelines_Japanese.zip
2019/2/1	Organising a Government for Cyber The Creation of the UK's National Cyber Security Centre	英国王立サイバーセキュリティセンターの創設	1									1				ロイヤル・ユナイテッド・サービス 防衛・安全保障研究所の沿革 サイバーセキュリティ解決のための設置経緯とGCHQとの関係を説明した資料。英国の背景理解用である。	https://www.rusi.org/ https://rusi.org/publication/occasional-papers/organising-government-cyber-creation-uks-national-cyber-security	
2019/2	NICTの標準策定プロセス		1	1											JETRO	JETROレポート「NISTの標準策定プロセス（組織構造、標準活動、人材確保）」 近年、セキュリティ標準など政府調達政策におけるNIST の策定した技術標準の影響力が高まる中、民間企業など他の組織もこうしたガイダンスを有効な技術標準として任意で採用するようになっており、NIST の組織構造、標準活動、人材確保を概観しつつ、その標準策定プロセスを確認する。 １．NISTの組織概要 (1)米国の標準活動におけるNIST のミッション及び役割　(2)NISTの組織構成　(3)NISTの予算概要 ２．NIST/ITLの標準化活動 (1)コンセンサスに基づくガイドライン・標準策定プロセス　(2)標準化機関におけるNIST／ITL の活動 ３．NISTを構成する人材 (1)NIST の雇用する職員の雇用形態と人員構成　(2)NIST 連邦職員のキャリアパス (3)人材の獲得・維持に向けた取組と課題	https://www.jetro.go.jp/ext_images/_Reports/02/2019/339d3d579a99af87/nyrp201901sp.pdf	
2019/4/17	The EU Cybersecurity Act	EUサイバーセキュリティ法			1							EU				EUサイバーセキュリティ法は、EUサイバーセキュリティ機関（ENISA）を刷新・強化し、デジタル製品、サービス、プロセスに対するEU全体のサイバーセキュリティ認証フレームワークを確立する。 EUのサイバーセキュリティ機関であるENISAは、より強力になりました。EUサイバーセキュリティ法は、同機関に恒久的な任務を与え、より多くのリソースと新たなタスクを提供。ENISAは、特定の認証スキームのための技術的基盤を準備し、専用のウェブサイトを通じて認証スキームや発行された証明書を一般に知らせることで、欧州のサイバーセキュリティ認証の枠組みを設定し、維持する上で重要な役割を果たす。また、ENISAには、EUレベルでの運用協力を強化し、サイバーセキュリティインシデントへの対応を要請するEU加盟国を支援し、国境を越えた大規模なサイバー攻撃や危機が発生した場合にはEUの調整をサポートすることが義務付けられている。この任務は、ネットワークと情報システムのセキュリティに関する指令（NIS指令）によって設立された国家コンピュータ・セキュリティ・インシデント・レスポンス・チーム（CSIRT）ネットワークの事務局としてのENISAの役割に基づいている。	https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act https://eur-lex.europa.eu/eli/reg/2019/881/oj	

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			
2019/7/31	NISTIR8259(Draft) Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers	セキュリティで保護可能なIoTデバイスのコアサイバーセキュリティ機能ベースライン：IoTデバイスメーカーの出発点	1	1												NISTIR8259(Draft)公開 本草案は、製造する IoT デバイスに対してメーカーが自発的に採用できるサイバーセキュリティ機能の基本計画を定義している。また、メーカーが顧客に最も適したコアベースラインを超えた機能を特定して実装する方法についても説明している。 NISTIR 8259の草案は、[NISTIR 8228:モノのインターネット(IoT)サイバーセキュリティとプライバシーリスクを管理するための考慮事項]に基づいている。 （パブリックコメント期間：～2019年9月30日）	https://csrc.nist.gov/publications/detail/nistir/8259/archive/2019-07-31	
2019/10/7	Network Equipment Security Assurance Scheme - Overview Version 1.0	ネットワーク機器のセキュリティ保証スキーム – 概要 1.0版		1									1			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。3GPPで作成されたSECAM関連の文書をベースに、セキュアな製品開発や製品ライフサイクルプロセスのためのセキュリティ要件や評価フレームワーク、ネットワーク機器のセキュリティ評価のためのセキュリティテストケースを定義しています。	https://www.gsma.com/security/wp-content/uploads/2019/11/FS.13-NESAS-Overview-v1.0.pdf	
2020年	Strategic presprectives on cybersecurity management and public policies European Cybersecurity Journal	サイバーセキュリティ管理と公共政策に関する戦略的予防策 ヨーロッパサイバーセキュリティジャーナル			1											サイバーセキュリティ管理と公共政策に関する戦略的予防策（European Cybersecurity Journal, 2020Volume 6, Issue 1） ・エネルギーインフラは現代社会にとって最も重要な資産の一つである。その有効な運営は、幅広い経済・社会活動へのエネルギー供給を確保するための前提条件であり、社会の福祉と安定を可能にする。 ・エネルギーインフラにおいて、進化するデジタル化は、エネルギーシステムをスマートにし、消費者がエネルギー市場に積極的に参加し、エネルギーサービスの恩恵を受けることを可能にする一方で、サイバー攻撃への露出が増え、エネルギー供給のセキュリティや消費者のデータプライバシーが危険にさらされる。 ・欧州のエネルギーセクターは、電力、ガス、石油における数多くの物理的な相互接続により、相互依存性が増大しており、サイバー攻撃の結果として生じる可能性のある連鎖的な影響は、多くの加盟国やEUの国境を越えて重要なインフラやエネルギーセクター全体でかなりの損害を与える可能性がある。 ・主に再生可能エネルギー源からの分散型発電の台頭により、このグリッドは「よりスマート」になった。しかし、電力を伝導するための運用技術は依然として重要である。したがって、グリッドをよりスマートにすることは、主に既存の運用技術を維持しながら、グリッドの制御レベルにデジタル技術を追加することを意味する。 ・EUの電力網の相互接続性が高いため、サイバーセキュリティの問題は、国家レベルだけで対策をとるよりも、EUレベルでの協力によって対処する方が良い。	https://cybersecforum.eu/media/ECJ_vol6_issue1.pdf	
2020/1/7	NISTIR8259(2nd Draft)Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline	IoTデバイスメーカーへの推奨事項：基本的な活動とコアデバイスのサイバーセキュリティ機能のベースライン（第2ドラフト）	1	1	1			1								NISTIR8259(2nd Draft)公開 本草案は、メーカーがIoTデバイスを顧客に販売する前に実行することを検討すべきサイバーセキュリティに関連する活動について説明している。この第2の公開草案には、最初の公開草案の概念を明確にし、寄せられたパブリックコメントに対処するために改訂されている。（パブリックコメント期間：～2020年2月7日） モノのインターネット（IoT）デバイスには、顧客がサイバーセキュリティリスクを軽減するために利用できるデバイスのサイバーセキュリティ機能が不足していることがよくある。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自主的な推奨活動について説明している。これらの活動は、製造業者が IoT デバイスの顧客が必要とするサイ バーセキュリティ関連の取り組みを軽減するのに役立ち、IoT デバイスの危殆化や危殆化した IoT デバイスを使用して実行される攻撃の有病率や妥当性を軽減することができる。	https://csrc.nist.gov/publications/detail/nistir/8259/archive/2020-01-07 https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259-draft2.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			
2020/1/31	Cyber Security for Europe Research and Development Roadmap	欧州のサイバーセキュリティ 研究と開発ロードマップ	1									1				欧州のサイバーセキュリティ　研究と開発ロードマップ（ CyberSec4Europe project） CyberSec4Europeプロジェクトは、欧州のデジタル単一市場の完全性を確保し維持するために必要なサイバーセキュリティ機能の統合と将来の予測を試験的に行うことを目的に活動しており、このロードマップの目標は、主要なサイバーセキュリティ分野の研究課題を特定し、その問題点と課題事項を説明することにある。 モノのインターネット（IoT）は、あらゆるエンティティの相互接続と、ほぼリアルタイムの情報の取得と処理を容易にするが、同時に、世界中のどこでも、インターネットに接続されたあらゆるエンティティ（商品から車両、インフラストラクチャまで）を標的としたサイバー攻撃の実行を容易にする。 本文書では、サイバーセキュリティ分野を（i）オープンバンキング、（ii）サプライチェーンセキュリティ保証、（iii）プライバシー保護ID管理、（iv）インシデント報告、（v）海上輸送、（vi）医療データ交換、および(vii) スマートシティの7つに分類し、分類毎に、全体像と概要、想定危機、想定攻撃者、研究課題、方法や解決手段を分析し、そのロードマップを示している。	https://cybersec4europe.eu/wp-content/uploads/2020/09/D4.3-Roadmap-v5-NEW.pdf	
2020/2/4	NIST Brog Improving the IoT Cybersecurity Baseline with Stakeholder Input: Draft (v2) NISTIR 8259 Available for Public Comment	利害関係者の意見によるIoTサイバーセキュリティベースラインの改善：パブリックコメントのためのNISTIR8259ドラフト（v2）	1	1				1								NISTIR 8259「IoTデバイス製造業者のための推奨事項」の第2草案（2nd Draft）を公開し、現在、パブリックコメントを受け付けている。2nd Draftは、1st Draftに対する450以上のパブリックコメントを反映し、タイトル、ドキュメント構造、内容を改定した。NISTIR 8259の目的として、常に基礎的な活動や製品の計画と開発プロセスのコンテキストにコアベースラインを置くことを明確化。 サンフランシスコで開催されるRSA Conference 2020の期間中に公開ラウンドテーブル・セッションを開催し、コメント期間から得られた初期の成果を共有し、IoTデバイス・サイバーセキュリティ・ベースラインの連邦政府の使用について利害関係者との対話を行う。	https://www.nist.gov/blogs/cybersecurity-insights/improving-iot-cybersecurity-baseline-stakeholder-input-draft-v2-nistir https://www.nist.gov/news-events/news/2020/02/nist-offers-strategies-help-businesses-secure-their-cyber-supply-chains	ステークフォルダとの対話のためのラウンドテーブルを開催
2020/2/4	NIST Offers Strategies to Help Businesses Secure Their Cyber Supply Chains	NISTは、企業がサイバーサプライチェーンを確保するのを支援する戦略を提供	1	1				1								NISTニュース：NISTは、企業がサイバーサプライチェーンを確保するのを支援する戦略を提供 最近の多くのサイバー侵害は、サプライチェーンのリスクに関連している。ドラフトNISTIR 8276は、サイバーサプライチェーンリスクマネジメントの主要な実践を示すものであり、サードパーティの組織が提供するコンポーネントやサービスを使用して一般的に構築されている最新の情報通信技術製品がもたらすサイバーセキュリティの問題に企業が対処するのに役立つ一連の戦略を提供するものである。（パブリックコメント期間：～2020年3月4日）	https://www.nist.gov/news-events/news/2020/02/nist-offers-strategies-help-businesses-secure-their-cyber-supply-chains	
2020/2/4	NISTIR 8276 (Draft) Key Practices in Cyber Supply Chain Risk Management: Observations from Industry	NISTIR 8276 (Draft) サイバーサプライチェーンのリスク管理における重要な実践：業界の観察から	1	1				1								2014年に「重要インフラストラクチャ・サイバーセキュリティ改善のためのフレームワーク（NIST Cybersecurity Framework）」とそ「重要インフラストラクチャ・サイバーセキュリティ改善のためのロードマップ」が発表されて以来、NISTは業界リーダーとの連携を通じて、サイバーサプライチェーン・リスク管理（C-SCRM）の業界慣行を調査してきた。本書は、2015年と2019年の企業へのインタビューを分析し、24のケーススタディ、サイバーサプライチェーンのリスク管理に関するNISTの先行研究、および多くの規格や業界のベストプラクティス文書に基づいている。NISTIR 8276は、効果的なサイバーサプライチェーンリスク管理プログラムの基礎となると主題専門家が判断したプラクティスを高レベルでまとめたものである。	https://csrc.nist.gov/publications/detail/nistir/8276/archive/2020-02-04	
2020/2/21	SP 800-171 Rev. 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	SP 800-171 Rev. 2 非連邦システムおよび組織における管理されていない機密情報の保護		1				1								SP 800-171 Rev. 2 :非連邦システムおよび組織における管理されていない機密情報の保護　を公開 本資料は、情報が非連邦系および組織に居住している場合に 未分類情報(CUI) の機密性を保護するための推奨セキュリティ要件を機関に提供する。要件は、CUIを処理、保管、および/または送信する非連邦システムおよび組織のすべてのコンポーネント、またはそのようなコンポーネントの保護を提供する組織に適用される。セキュリティ要件は、契約車両またはそれらの機関と非連邦組織との間で確立された他の契約上の契約機関での他の契約で使用することを目的としている。	https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.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			
2020/2/24～2/28	NIST IoT Roundtable Foundational Cybersecurity Guidance for IoT Device Manufacturers: NISTIR 8259 Overview	NIST IoTラウンドテーブル IoTデバイスメーカーのための基礎的なサイバーセキュリティガイダンス NISTIR 8259の概要	1	1	1			1									NISTIR 8259に関する公開ラウンドテーブル・セッションを開催 コメント期間から得られた初期の成果を共有し、IoTデバイス・サイバーセキュリティ・ベースラインの連邦政府の使用について利害関係者との議論を行った。 （概要） ・参加者は総勢12,3名程度。話の内容から数名は規制法方面の弁護士で、ほとんどがサンフランシスコベイエリア以外の参加者と推測。 ・NISTIR 8259は今回でコメント受付を終了し、NIST内で仕様凍結と確定手続きを行い確定版を公開する。NIST内部手続きから公開までおよそ2ヶ月を想定。NISTより、最終版公開後outreachを兼ねた公開の催事を実施する可能性があるが決定してはいない。 ・NISTIR 8259の確定の後、Federal IoT Device Cybersecurity Baselineの作成を開始する。連邦文民省庁がIoT製品を連邦政府内に導入、ネットワークに接続、利用する際のガイダンスという位置付けで、FISMA, FIPSを補完する機能が期待され、IoTの導入ガイドという位置付けなので、政府調達に直接影響する。 ・NISTあるいは商務省以外の省庁も、必要に応じIoTに関する規制やルールを策定しているが、これらがNISTの各種文献を不用意に参照、援用した場合、事実上の拘束力のある文書として捉えられる可能性がある。	開催案内： https://www.nist.gov/blogs/cybersecurity-insights/improving-iot-cybersecurity-baseline-stakeholder-input-draft-v2-nistir	
2020/5/27	CONVERGENCE OF BLOCKCHAIN, AI AND IOT	ブロックチェーン、AI, IoTとの融合			1										＊0		IoTでブロックチェーンを採用することで、単一のベンダーが提供する集中型ソリューションを、関心のある利害関係者のコンソーシアムによって開発され運営されている分散型IoTプラットフォームに置き換えるなど、これらの問題の一部を軽減できる可能性がある。 データは(ハッシュによって)封印され、一意に識別可能になり、(データレコードの公開キーを介して)見つけ出し可能になる。 システムと対話するデバイスの一意の識別子がデータと保存されると、ブロックチェーンを使用してプラットフォームに入る情報の証明を確保できる。さらには、エネルギー関連でのユースケースでは、AIとIoTとのブロックチェーンを融合させた試みが進んでおり、最初のブロックチェーンベースのハードウェアを開発も行っている。	https://www.eublockchainforum.eu/sites/default/files/reports/report_security_v1.0.pdf	＊0 : THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY & FORUM
2020/5/29	NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers	NISTIR 8259 IoTデバイスメーカー向けの基礎的サイバーセキュリティ活動	1	1				1									NISTIR8259最終版確定 この文書は、メーカーが IoT デバイスを顧客に販売する前に検討する必要があるサイバーセキュリティに関連する推奨アクティビティを提供する。	https://csrc.nist.gov/publications/detail/nistir/8259/final https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf	
2020/5/29	NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline	NISTIR 8259A IoTデバイスのサイバーセキュリティ機能のコアベースライン	1	1				1									NISTIR 8259A最終版確定 この文書は、IoTデバイスのサイバーセキュリティ機能コアベースラインを定義している。組織のデバイス、データ、システム、およびエコシステムを保護する一般的なサイバーセキュリティ制御をサポートするために一般的に必要なデバイス機能のセットである。	https://csrc.nist.gov/publications/detail/nistir/8259a/final https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.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			
2020/6/1	NIST Brog More than just a milestone in the Botnet Roadmap towards more securable IoT devices	NISTブログ より安全なIoTデバイスに向けたボットネット・ロードマップのマイルストーンの拡大	1	1				1									NIST ブログ：2017年の大統領令以降の米国におけるこれまでのサイバーセキュリティ強化に関する検討の経緯とNISTIR8259の内容を概説 ・IoTデバイスメーカーが製品機能を計画する際は、IoTデバイス自体、IoTデバイスに関連する他のデバイス、メーカーや顧客に代わって動作する他のシステムやサービス、およびそれらの堅牢性など、どのような技術的手段が提供されるか考慮する必要がある。NISTIR8259は、プレマーケットおよびポストマーケットの各製品フェーズで、メーカーがこの包括的なジレンマに対処するのに役立つ6つの特定の推奨アクティビティを提供する。 ・IoT のユース ケースは多くの業界や管轄区域にまたがり、多くの一般的な機能があることから、8259A は技術的なコア ベースラインを提供する。組織のデバイス、データ、システム、エコシステムの保護を目的として、一般的なサイバーセキュリティ管理をサポートするために必要なデバイス機能について概説している。 ・NISTは現在、NISRS 8259および8259Aを適応させ、より安全なIoTデバイスの連邦機関の採用を可能にするために必要なサイバーセキュリティデバイス機能を定義する連邦プロファイルを策定している。 ※ボットネット・ロードマップ：ボットネットおよびその他の自動化された分散型脅威に対するインターネットおよび通信エコシステムの回復力強化に関するロードマップ	https://www.nist.gov/blogs/cybersecurity-insights/more-just-milestone-botnet-roadmap-towards-more-securable-iot-devices	
2020/6/30	ETSI EN 303 645, CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements	ETSI EN 303 645, CYBER; コンシューマ・インターネット・オブ・シングスのためのサイバーセキュリティ：基本要件	1								1						ETSI、世界をリードするコンシューマIoTセキュリティ標準（ETSI EN 303 645）を発表 ETSIサイバーセキュリティ技術委員会(TC CYBER)は、インターネットに接続された消費者製品のセキュリティベースラインを確立し、将来のIoT認証スキームの基礎を提供するモノのインターネット（IoT)におけるサイバーセキュリティの標準：ETSI EN 303 645を発表した。 ENは、サイバーセキュリティの専門家が毎日目にするスマートデバイスに対する大規模で蔓延している攻撃を防ぐように設計されており、この標準に準拠すると、攻撃者が世界中のデバイス（ボットネットと呼ばれる）を制御してDDoS攻撃を開始し、暗号通貨をマイニングし、自宅のユーザーをスパイする能力が制限される。 これらの攻撃を防ぐことにより、ENはベースラインのセキュリティとプライバシーを大幅に向上させている。 ETSI EN 303 645は、インターネットに接続されたコンシューマデバイスおよび関連サービスのセキュリティに関する 13 の規格を規定している。IoT製品には、コネクテッド・チルドレンのおもちゃやベビーモニター、煙探知機やドアロックなどのコネクテッドセーフティ関連製品、スマートカメラ、テレビ、スピーカー、ウェアラブルヘルストラッカー、コネクテッドホームオートメーションとアラームシステム、コネクテッドアプライアンス(洗濯機、冷蔵庫など)、スマートホームアシスタントなどがある。 ENには、消費者向けIoTに対する5つの特定のデータ保護規定も含まれている。	https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf https://www.etsi.org/newsroom/press-releases/1789-2020-06-etsi-releases-world-leading-consumer-iot-security-standard	
2020/6/30	Foundational Cybersecurity Guidance for IoT Device Manufacturers: NISTIR 8259 Overview	IoTデバイスメーカー向け:NISTIR 8259ガイダンス		1				1									NIST がvirtual-only event,を開催し上記の解説と質疑応答を実施 ・本イベントでは、NISTのKat MegasとMichael Faganのプレゼンテーションが行われ、続いて聴衆のQ&A.IoTデバイスメーカーと産業用および/または家庭用IoTデバイスの全てのユーザーの参加を奨励。 ・NISTIR 8259 概説ビデオ視聴可能（45分）	https://www.nist.gov/news-events/events/2020/06/foundational-cybersecurity-guidance-iot-device-manufacturers-nistir-8259	

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			
2020/7	Perspectives on an EU Dialogue with China on Digitalization	デジタル化に関するEUの中国との対話に関する展望		1											EIAS:	デジタル化に関する中国とのEUの対話の展望：EIAS（European Institute for Asian Studies）Plicy Brief 06/2020 EUと中国の間にデジタル対話を確立することは、COVID-19危機からの世界的な回復と次の10年間の持続的な経済成長にとって不可欠である。 EUのデジタル戦略は、EU経済のデジタルでグリーンな回復を強調する最近承認されたEU回復計画を含め、2015年以降着実に進化してきた。 現在、EUと中国の両方が、中欧関係を改善し、進行中の緊張を緩和するために、二国間デジタル対話を維持する具体的な機会がある。 ・2020年1月、欧州委員会は、EU以外の技術プロバイダーによる5Gネットワークの設置に関連する安全保障リスクに対する共通のEUアプローチに関する勧告(ツールボックスの形で)を採択した。 ・中国は、5G技術、サイバーセキュリティ、データ共有、IoT、AI/自動化に関するヨーロッパとの効果的かつ具体的なデジタルダイヤログの重要性を認識しており、中国は米中政治貿易関係の悪化による悪影響を最小限に抑えるためにヨーロッパで代替パートナーを見つける必要がある。 中国は、欧州との協力に関する2018年の政策文書で、BRIイニシアチブの枠組みの中でEUとのデジタル接続性を開発するというコミットメントを強く再確認し、特に情報技術、通信、情報化を参照して、「Digital China」とEUデジタル単一市場との緊密な協力のメリットと利点を認識している。 ・EUと中国は、新しいEUと中国のデジタル対話と合意の条件を実現する上で相乗効果と強力な補完性を生み出すことを目指すべきである。これは、必要な信頼メカニズムを作成する上で建設的な協力につながる。 ・技術標準、認証、およびその他の国際的なサイバー規範の調和は、技術機器の法的確実性、透明性、および相互運用性を実現するために重要である。	https://www.eias.org/wp-content/uploads/2019/07/Policy-Brief-5G_Mogni_Goethals_EU-CN-Dialogue-Digitalization.pdf	
2020/7/20	Network Equipment Security Assurance Scheme – Development and Lifecycle Security Requirements Version 1.1	ネットワーク機器のセキュリティ保証スキーム ー 開発とライフサイクルのセキュリティ要件 1.1 版		1									1			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。3GPPで作成されたSECAM関連の文書をベースに、ベンダーの開発工程、製品のライフサイクルプロセスに対するセキュリティ要件を定義。 遠隔監査の追加、監査レポートのGSMAへの提出の必須化、アセスメント結果の判定方法の明確化、NESASのスコープの明確化、セキュリティテストラボ適正ガイドラインの追加（Annex）。 セキュリティ要件の再グループ化と並べ替えを実施。	https://www.gsma.com/security/wp-content/uploads/2020/09/FS.16-NESAS-Development-and-Lifecycle-Security-Requirements-v1.1.pdf	
2020/7/22～7/23	Building the Federal Profile for IoT Device Cybersecurity	IoT デバイスサイバーセキュリティ|の連邦プロファイルの構築ワークショップ	1	1				1							NIST IoT デバイスサイバーセキュリティ|の連邦プロファイルの構築ワークショップ開催 IoTデバイスのサイバーセキュリティのための連邦政府のプロファイルの構築。連邦システムのセキュリティを確保するための次のステップ ・イベント報告は NISTIR 8322として 2021/1/ 8 に発行されている ・参加者 500名規模、26か国から参加（外国政府 5 か国）、米国39州から参加（州政府8州） ・ワークショットの要約としてくり返し聞かれたテーマがTakeawayとして13件が記録されている。 ・ワークショップで意見照会結果 IoT Security 強化の政府による義務的な規制：71％が強い支持 IoT デバイスの開発者が製品を安全にするための適切なインセンティブが不足：55％	https://www.nist.gov/news-events/events/2020/07/building-federal-profile-iot-device-cybersecurity-next-steps-securing https://www.nist.gov/blogs/cybersecurity-insights/building-federal-profile-iot-device-cybersecurity-post-workshop-update	
2020/9/18	Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management	モノのインターネット(IoT)サイバーセキュリティ: 文献レビューとIoTサイバーリスク管理		1											MDPI	サイバー攻撃の脅威の増大に加え、サイバーセキュリティはIoTの最も重要な分野の1つとなっている。IoTサイバーセキュリティの目的は、IoT資産とプライバシーの保護を通じて、組織やユーザーのサイバーセキュリティリスクを軽減することである。 新しいサイバーセキュリティ技術とツールは、IoTセキュリティ管理の向上に潜在能力を提供する。しかし、経営者にとって効果的なIoTサイバーリスク管理フレームワークが不足している。IoTサイバーセキュリティ技術とサイバーリスク管理フレームワークについて説明し、4層のIoTサイバーリスク管理フレームワークを紹介する。また、複数のIoTサイバーセキュリティプロジェクトに対する金融資源の配分に対する線形プログラミング手法も取り上げる。	https://www.mdpi.com/1999-5903/12/9/157	

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			
2020/9/23	SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations	SP 800-53 Rev. 5 情報システムおよび組織のセキュリティとプライバシーの制御	1	1				1									SP 800-53 Rev. 5 公開 FISMA並びにFISMA対象連邦省庁に対するOMB回覧A-130の順守に必要なControlsを定める改定を実施。 NIST SP 800-53（連邦政府情報システム、および連邦組織のためのセキュリティ管理策とプライバシー管理策）は、米国連邦政府の内部セキュリティとプライバシー管理基準を示すガイドラインであり、これらのコントロールは柔軟でカスタマイズ可能で、リスクを管理する組織全体のプロセスの一部として実装されている。	https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final	
2021/10/720	4th IoT Security Conference	第４回 IoTセキュリティ会議			1					1							サイバー犯罪部門、CSIRT、国際機関、民間企業、規制機関、学界の専門家が一堂に会することで、幅広い議論を可能にすることを目的としてバーチャルイベントとして３つのセッションを開催。 ・Operational IoT　（2020年10月7日）：現在のIoTセキュリティの課題とその原因、IoTインフラと関連プロジェクトのセキュリティ確保のための取り組み、そして規制の側面と認証スキームについて議論。 ・Artificial Intelligence　（2020年10月14日）：AIの潜在的なリスクや新たな脅威と、犯罪捜査の効率化や有効性を高めるという法執行の観点からのメリットを振り返りながら、総合的な視点からAIについて議論。 ・Supply Chain for IoT　（2020年10月21日）：IoTエコシステム全体で安全なサプライチェーンを確立することは、IoTセキュリティの基本的な構成要素である。製品開発から製品消費に至るまでのさまざまなフェーズに焦点を当て、関連する脅威、リスク、緩和手法について、IoTサプライチェーンに関する幅広い議論。	https://www.enisa.europa.eu/events/4th-iot-securiity-conference-online-series	
2020/10/22	Workshop on Cybersecurity Risks in Consumer Home IoT Products	家庭用IoT製品におけるサイバーセキュリティリスクに関するワークショップ		1				1									Virtual Meeting開催 家庭用IoT製品におけるサイバーセキュリティの課題への対応と、消費者向けIoT製品にコアベースラインNISTIR 8259A IoT Device Cybersecurity Capability Core Baselineを実装する際の障壁について議論 ・ワークショップ説明／セッションビデオ公開	https://www.nist.gov/news-events/events/2020/10/workshop-cybersecurity-risks-consumer-home-iot-products	
2020/11	IoT Security: ENISA Publishes Guidelines on Securing the IoT Supply Chain	ENISA IoTサプライチェーンのセキュリティに関するガイドラインを公開	1							1							IoTセキュリティ:ENISAがIoTサプライチェーンの保護に関するガイドラインを公開 このENISA文書では、IoTのサプライチェーンを保護するためのガイドラインを定義。サプライチェーンは、IoTデバイスのセキュリティの基盤を築くものであり、ENISAは、IoT製品とサービスのサプライチェーン全体を調査し、IoTの専門家の意見を取り入れて、要件と設計から最終用途の配送と保守、廃棄まで、ライフスパン全体のセキュリティガイドラインを作成した。 IoTセキュリティは、初期の概念設計からエンドユーザーの運用と保守まで、サプライチェーンのすべての段階で検討する必要があり、関連するサプライチェーンのセキュリティ脅威を分析し、それに応じて、IoTサプライチェーンの信頼性に影響を与えるリスクを回避するのに役立つセキュリティ対策とガイドラインを設定することが重要である。 この文書は、IoTメーカー、開発者、インテグレーター、およびIoTのサプライチェーンに関与するすべての利害関係者が、IoTテクノロジーを構築、展開、または評価する際のセキュリティに関する意思決定を改善するのに役立つように開発。IoTサプライチェーンのさまざまな段階を分析し、各段階で考慮すべき重要なセキュリティ上の考慮事項をすべて調査している。	https://www.enisa.europa.eu/news/enisa-news/iot-security-enisa-publishes-guidelines-on-securing-the-iot-supply-chain	
2020/11/6	Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions	サプライチェーン4.0:サイバーセキュリティの課題、解決策、今後の方向性に関する調査			1										MDPI		サプライチェーン4.0：サイバーセキュリティの課題、解決策、今後の方向性に関する調査（ニューサウスウェールズ大学オーストラリア国防軍アカデミー工学・情報技術学部） サプライチェーン4.0は、サプライチェーン管理システムの第4次革命に位置付けられ、ICTとのマニュファクティング業務を統合する。サプライチェーン4.0の包括的な目的は、サプライチェーン内の生産システムの強化であり、グローバルリーチを利用し、敏捷性と新たな技術を高め、効率、適時性、収益性を高めるという究極の目標を持っている。また、サプライチェーン4.0では、新たな運用リスクとサイバーリスクが課題となる。 サプライチェーン4.0は、基準が不十分で、相互運用性が悪く、製造および情報技術プロセスの運用も十分ではない。サプライチェーン4.0を支える技術には、ブロックチェーン、スマートコントラクト、人工知能のアプリケーション、サイバー物理システム、IoT、 産業用インターネットなどがある。これらの技術はそれぞれ組み合わされ、対処すべきサイバーセキュリティの問題を生み出します。この論文では、軍事サプライチェーン4.0の性質と、それが商業用サプライチェーンとどのように異なるかを説明し、その長所、弱点、依存関係、およびそれらが構築される基礎技術を明らかにする。	https://www.mdpi.com/2079-9292/9/11/1864	

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			
2020/12/4	IoT Cybersecurity Improvement Act of 2020	2020年IoTサイバーセキュリティ向上法	1									1				米国標準技術研究所（NIST）と管理予算局（OMB）に、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を向上させるための特定の措置を講じることを求めている。IoTは、インターネット接続を物理的なデバイスや日常的な物体にまで拡張したもの。機関が所有または管理し、機関が所有または管理する情報システムに接続されたIoTデバイスの機関による適切な使用と管理について、デバイスに関連するサイバーセキュリティリスクを管理するための最低限の情報セキュリティ要件を含む基準とガイドラインを策定し、連邦政府向けに公表することをNISTに要求している。	https://www.congress.gov/116/plaws/publ207/PLAW-116publ207.pdf	NISTとOMBに対して、FISMA（Federal Information Security Management Act of 2002 連邦情報セキュリティマネジメント法）に基づいて規格やガイドラインの開発を義務付けている。DHS CISAの活動と関連して2020年12月に本法律が制定されていると思われる。
2020/12/10	SP 800-53 Rev. 5(DOI)	SP 800-53 Rev. 5 （更新版）	1	1				1								SP 800-53 Rev. 5 更新版を公開 SP 800-53 Rev. 5の主要な更新は以下の通り ・FIPS200（連邦情報システムの最小セキュリティ要件）の定める17のControl群に加え、FIPS200以降に連邦政府の義務として追加されたProgram Management、PII Processing and Transparency、Supply Chain Risk Managementの3つのControl群が追加	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	SP 800-53 Rev. 5の主要な更新の一つとして、FIPS200の定める17のControl群に加え、FIPS200以降に連邦政府の義務として追加されたProgram Management、PII Processing and Transparency、Supply Chain Risk Managementの3つのControl群が追加された。
2020/12/13	Emergency Directive 21-01 Mitigate SolarWinds Orion Code Compromise	緊急指令21-01 SolarWindsOrionコードの侵害の軽減			1				1							SolarWinds Orion製品が悪用されており、攻撃者はネットワークトラフィック管理システムへのアクセスが可能となる。これに対するアクションを指令。知識を持たない組織において、現在利用可能な唯一の既知の対処は、影響を受けるデバイスを切断することである。	https://cyber.dhs.gov/ed/21-01/	
2020/12/15	Rounding Up Your IoT Security Requirements: Draft NIST Guidance for Federal Agencies	NIST ブログ IoTセキュリティ要件のまとめ：連邦政府機関向けドラフトNISTガイダンス	1	1				1								NIST ブログ：連邦IoTサイバーセキュリティ要件の定義に関する4つの一般レビュードラフトガイダンスを公開 連邦IoTサイバーセキュリティに関する4つのドキュメントとNISTIR8259／NISTIR8259Aとの相互関係を説明	https://www.nist.gov/blogs/cybersecurity-insights/rounding-your-iot-security-requirements-draft-nist-guidance-federal	IoT Programの目的は、NIST SP800-53に適合順守してIoTを連邦情報システム内でどのように扱うか、そのために何が必要かという連邦政府官庁への指針を示すことでありIoT Programも最新のNIST SP800-53r5を前提としている。
2020/12/17	INFORMATION AND COMMUNICATIONS TECHNOLOGY SUPPLY CHAIN RISK MANAGEMENT TASK FORCE YEAR 2 REPORT	情報通信技術サプライチェーンリスクマネジメントタスクフォース2年目報告書			1				1							CISA (Cybersecurity and Infrastructure Security Agency) とICT SCRM (Supply Chain Risk Management) Task Force の政府および業界メンバーは、サプライチェーンのセキュリティとレジリエンスに関する有意義なパートナーシップと分析を推進するための進捗状況についての年次報告書を発表 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全体的なアプローチを提供するまとまりのある一連の製品と勧告を作成。情報共有に関連した作業は脅威分析に関する勧告の開発作業につながっており、この作業は認定入札者リストや認定製造者リストなどのベンダー保証と信頼メカニズムの構築に関連した作業に不可欠な基盤を提供。	https://www.cisa.gov/news/2020/12/17/cisa-releases-ict-supply-chain-risk-management-task-force-year-2-report https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force_year-two-report_508.pdf	CISAの他にUS Telecom と 米国情報技術工業協議会がICT SCRM タスクフォースの共同議長を務めている。 ・Bob Kolasky：CISA Assistant Director ・Robert Mayer：Senior Vice President of Cybersecurity and Innovation at USTelecom ・John Miller：Senior Vice President of Policy and Senior Counsel at Information Technology Industry Council (ITI)

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			
2020/12/17～2021/1/7	Alert (AA20-352A) Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations	警告（AA20-352A）政府機関、重要インフラストラクチャ、民間セクター組織への高度な持続的脅威			1				1							CISAは、少なくとも2020年3月から始まる高度な持続的脅威（APT）行為者による、米国の政府機関、重要インフラ事業体、および民間部門の組織への侵入を確認。侵入者を侵害された環境から排除することは、組織にとって非常に複雑で困難なことになると予想。 2021/1/6更新：初期の侵入先の1つは、SolarWinds Orion製品に含まれるダイナミックリンクライブラリ(DLL)を用いたサプライチェーン。	https://us-cert.cisa.gov/ncas/alerts/aa20-352a	2021年1月末でも、米国連邦政府官庁、民間企業とも、インシデントが発生した後の被害を最小限にするための事後対応対応を実施している状況。 また、各組織としては民間組織では侵害に気づいていないところが多い可能性がある。
2020/12/18	ICT SCRM Task Force Events PARTNERSHIP IN ACTION: DRIVING SUPPLY CHAIN SECURITY	ICT SCRMタスクフォースイベント、パートナーシップ活動：サプライチェーンのセキュリティを推進			1				1							ICTサプライチェーンに関する様々なトピックについて、情報技術・通信部門や連邦政府機関のリーダー、専門家、様々な組織の代表者から話を聞き、実用的なICTサプライチェーン・リスク管理情報、ユースケース、ベストプラクティス、教訓などを学ぶ。	https://www.cisa.gov/ict-scrm-task-force-events https://www.cisa.gov/publication/ict-scrm-event-agenda	
2020/12/20	NISTIR 8259B (Draft) 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				1								NISTIR8259B(Draft)を公開 本草案は、メーカーや関連するサードパーティから通常必要とされる追加の非技術的なサポート活動を詳述することにより、NISTIR8259Aデバイスのサイバーセキュリティコアベースラインを補完する。 この非技術的なベースラインは、ドキュメント、トレーニング、顧客フィードバックなどの明示的なサポート機能を収集して作成する。	https://csrc.nist.gov/publications/detail/nistir/8259b/draft https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259B-draft.pdf	
2020/12/20	NISTIR 8259C (Draft) Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline	NISTIR 8259C IoTコアベースラインと非技術ベースラインを使用したプロファイルの作成	1	1				1								NISTIR8259C(Draft)を公開 本草案は、NISTIRs 8259Aおよび8259Bに提供されるコアベースラインから始まるあらゆる組織が使用できるプロセスを説明し、これらのベースラインを組織またはアプリケーション固有の要件(例えば、業界標準、規制ガイダンス)と統合して、特定のIoTデバイスまたは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方法を説明している。NISTIR 8259Cのプロセスは、標準やその他のガイダンスなどの権威ある情報源に基づいて、特定のセクターの懸念に対応するより詳細な機能セットを定義する必要がある組織を導き、IoT技術の調達を求める組織や、自社の製品を顧客の要件に合わせようとするメーカーによって使用される。	https://csrc.nist.gov/publications/detail/nistir/8259c/draft https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259C-draft.pdf	
2020/12/20	NISTIR 8259D (Draft) Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government	NISTIR 8259D (Draft) 連邦政府のIoTコアベースラインと非技術ベースラインを使用したプロファイル						1								NISTIR8259D(Draft)を公開 本草案は、FISMAプロセスとSP 800-53のセキュリティおよびプライバシー管理カタログの要件が不可欠なガイダンスである連邦政府の顧客スペースに焦点を当てたNISTIR 8259Cプロセスを適用した場合の実際の例を提供する。 NISTIR 8259Dは、連邦ユースケースの最小のセキュリティ保護の基準の例としてNIST SP800-53Bで説明されているFISMA低ベースラインと整合を取るNISTIR 8259Aおよび8259Bコアベースラインのデバイス関連サイバーセキュリティ指向プロファイルを提供する。	https://csrc.nist.gov/publications/detail/nistir/8259d/draft	本年2月のroundtableで触れられたFederal ProfileをNISTIR8259Dとして文書化

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			
2020/12/20	SP 800-213 (Draft) IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements	SP 800-213 (Draft) 連邦政府向けの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	1	1				1								SP 800-213 (Draft)を公開 本草案には、連邦政府機関が取得を計画している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のに役立つ背景と推奨事項が含まれており、 IoTデバイスとそのセキュリティ制御のサポートが、組織およびシステムのリスク管理のコンテキストで提示されている。 SP 800-213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ためのガイダンスを提供する。 これにより、IoTデバイスのサイバーセキュリティ要件（連邦政府機関がIoTデバイスとその製造元および/またはサードパーティにそれぞれ期待する能力とアクション）を特定できる。	https://csrc.nist.gov/publications/detail/sp/800-213/draft https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-213-draft.pdf	
2020/12/22	DHS Warns American Businesses about Data Services and Equipment from Firms Linked to Chinese Government	DHS、中国政府とリンクした企業のデータサービスと機器について米国企業に警告			1				1							国土安全保障省は米国企業に対し、中華人民共和国（PRC）に関連する企業からのデータサービスや機器の使用に関連するリスクを警告するビジネスアドバイザリー（勧告）を発表。 本勧告では、新たに制定された中国の法律により、学術機関、研究サービスプロバイダー、投資家を含む中国の企業や市民に、米国および国際法や政策の原則に反するデータの収集、送信、保存に関連する行動を強制することができるため、中国政府が支援するデータ盗難のリスクが持続的かつ増大していることに注目。このような活動には、企業に中国の国境内でのデータ保管を要求したり、国家安全保障を装って日常的なデータを中国政府に引き渡したりすることが含まれる。また、この勧告は、中国のビジネスと経済の目的のためにデータを操作、誤用、搾取してきた中国の歴史を強調。PRC リンク企業からデータサービスや機器を調達したり、そのような企業が開発したソフトウェアや機器にデータを保存したりすることを選択する個人や事業体は、これらの企業との取引に関連する経済的、評判、場合によっては法的なリスクを認識しておく必要がある。	https://www.dhs.gov/news/2020/12/22/dhs-warns-american-businesses-about-data-services-and-equipment-firms-linked-chinese https://www.zdnet.com/article/dhs-warns-against-using-chinese-hardware-and-digital-services/ https://www.bleepingcomputer.com/news/security/dhs-warns-of-data-theft-risk-when-using-chinese-products/ https://www.theregister.com/2020/12/23/dhs_warns_us_businesses_dont_use_china_tech/	多くのメディアで報道されている。将来、米国での調達や品質管理の公式あるいは非公式の基準になると部品を提供する日本、あるいは国毎の端末製造認証規格に影響する可能性がある。 DHSがAmerican businessesへ出したとされる例示の中に、中国製品利用のData Centerや、wearable端末なども含まれている。 海外生産拠点が中国製品利用のData Centerを利用したクラウドなどを利用された場合、引っかかる可能性があり得る。wearableについてはPII（personally identifiable information）を詐取されうる点を懸念している模様。
2020/12/22	EUCS – Cloud Services Scheme	EUCS - クラウドサービススキーム			1					1						サイバーセキュリティ法1に従い、ENISAは、欧州サイバーセキュリティ認証フレームワークの一部として、クラウドサービスに関する候補スキームの作成に取り組むアドホック・ワーキング・グループ（AHWG）を設置しました。これは、クラウドサービスのサイバーセキュリティの認証を検討しているEUCS候補スキーム（European Cybersecurity Certification Scheme for Cloud Services）の外部レビューの基礎となるドラフト版である。レビューにより、提案されているスキームの原則と一般的な構成を検証し、セクションとアネックスの文言案に対するフィードバックを収集する。2020年12月22日から2021年2月7日まで、本文書に関する公開コンサルティングを開始した。	https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme	

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			
2021/1/5	JOINT STATEMENT BY THE FEDERAL BUREAU OF INVESTIGATION (FBI), THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA), THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI), AND THE NATIONAL SECURITY AGENCY (NSA)	連邦捜査局（FBI）、サイバーセキュリティおよびインフラストラクチャセキュリティエージェンシー（CISA）、国家情報局長官（ODNI）、および国家安全保障局（NSA）による共同声明			1				1			1					国家安全保障会議のスタッフは、連邦捜査局を含む重大なサイバー事件の調査と修復を調整するために、FBI、CISA、およびODNIで構成されるサイバー統一調整グループ（UCG）と呼ばれるタスクフォース構成を立ち上げた。 ロシア起源である可能性が高いAdvanced Persistent Threat（APT）アクターが、政府と非政府ネットワークの両方で最近発見された進行中のサイバー侵害のほとんどまたはすべてに関与していることを示している。 UCGは、Solar WindsのOrion製品の影響を受けた約18,000の公的および民間部門の顧客のうち、システムでの後続の活動によって侵害されたのははるかに少ないと考えている。これまでに、このカテゴリに分類される米国政府機関は10未満であり、影響を受ける可能性のある非政府機関を特定して通知するよう取り組んでいる。	https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure	
2021/1/8	NISTIR 8322 Workshop Summary Report for “Building the Federal Profile For IoT Device Cybersecurity” Virtual Workshop	NISTIR 8322 ワークショップ概要レポート「IoTデバイスサイバーセキュリティのための連邦プロファイルの構築」	1	1				1									NISTIR 8322：ワークショップ概要レポート「IoTデバイスサイバーセキュリティのための連邦プロファイルの構築」 2020年7月の仮想ワークショップでのデバイスサイバーセキュリティに関するNISTサイバーセキュリティIoTプログラムの作業に関するフィードバックをまとめたレポート。 NISTIR 8259、IoTデバイスメーカー向けの基本的なサイバーセキュリティ活動、NISTIR 8259AのIoTデバイスサイバーセキュリティ機能コアベースラインは、メーカーが顧客のサイバーセキュリティニーズと目標をサポートする役割を理解し、アプローチする方法に関する一般的なガイダンスを提供する。NISTは仮想ワークショップ「IoTデバイスサイバーセキュリティのための連邦プロファイルの構築」を実施し、連邦政府機関が使用するコアベースラインの連邦プロファイルの作成に関するコミュニティの意見を議論し、収集した。 ベースラインは、連邦政府のIoTコアベースラインのプロファイルであるNISTIR 8259Dで公開される。	https://csrc.nist.gov/publications/detail/nistir/8322/final https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8322.pdf	NISTIR8322からは、IoT Supply Chainが主要な関心事の一つと位置付けられている。 NISTIR8322には、13件のTakeawaysが記されている。参加者の意見や観察など主観的ではあるが、興味や関心事、当日の議論、当日の議論の雰囲気が把握できる。
2021/1/11	VIRTUAL EVENT：Webinar - Certification of Cloud Services	バーチャルイベント：Webinar - クラウドサービスの認定			1					1							ENISAは、EUCSA（サイバースセキュリティ法）に基づく欧州委員会の要請を受けて、2020年3月に設置したAHWG（Ad Hoc Working Group ）において、クラウドサービスに関するEUサイバーセキュリティ認証制度の候補案の作成支援を行なっている。AHWGは、20名の業界を代表するクラウドサービスプロバイダ、クラウドサービス顧客、適合性評価機関などのメンバーと、認定機関やEU加盟国からの約12名の参加者で構成されており、候補スキームEUCS (European Union Cybersecurity Certification Scheme on Cloud Services)をまとめた。 Webinarを開催して、候補スキームの草案を提示し参加者と質疑応答を行なった。 ・対象とするCloud Serviceは、ISO/IEC 17788による定義を採用し、広義のCloudを対象とする。　これにより、EUCSの対象は、Cloud on Cloud，VMやKubernetsなどcloudが利用しているcomponentsにも及び、Cloud Serviceのsupply chain全体が対象で、会議ではfull stackという言葉が何回か強調された。 ・用語はISO/IEC27000 とIAASB handbookから援用。ENISAから、用語集の定義の確認要望があった。 ・Assurance Levelsとして、Basic, Substantial, およびHighの三段階を設定。 ・Control Requirementsは、ISO/IEC 27000、並びにドイツC5に準拠、準用。 ・Assessment methodsはISOとISAEのaudit standardsに準拠	https://www.enisa.europa.eu/events/webinar-certification-of-cloud-services-in-europe https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/ComplianceControlsCatalogue-Cloud_Computing-C5.pdf	C5のRequirementは緩めに採用されていると思われる 参考 C5 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/ComplianceControlsCatalogue-Cloud_Computing-C5.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			
2021/1/11	Networking giant Ubiquiti alerts customers of potential data breach	ネットワーキング大手のユビキティ、顧客にデータ漏洩の可能性を警告			1									1	Ubiquiti	Ubiquitiが、顧客のデータが流出した可能性のあるとのセキュリティインシデントを発表。サードパーティのクラウドプロバイダーでホストされているシステムが攻撃者によってハッキングされたことを受け、顧客にパスワードの変更と2FA（Two Factor Authentication 二要素認証）を有効にするようにメールを送付。不正にアクセスされた顧客データベースは認識していないとしているが、攻撃によって顧客データが流出しなかったとは断言できない。データには、顧客の名前、電子メールアドレス、暗号化されたパスワード、顧客の住所、電話番号が含まれている場合がある。	https://www.bleepingcomputer.com/news/security/networking-giant-ubiquiti-alerts-customers-of-potential-data-breach/	Ubiquitiのオーナーは、UniFiがローカルデバイスを管理するためにクラウドアカウントを作成する必要があることに不満を感じており、多くはすべてをローカルで管理できることを希望している。 Ubiquitiのクラウド管理プラットフォームが広範囲に停止し、ユーザーがウェブやモバイルアプリを使用したり、デバイスを管理したりすることができなくなった。
2021/1/21	5G Cybersecurity (Preliminary Draft)	5G Cybersecurity (Preliminary Draft)	1	1				1								NISTの National Cybersecurity Center of Excellence (NCCoE) は5Gサイバーセキュリティに関する今後の実践ガイドの3巻の最初の予備草案をコメントに投稿した。 この実践ガイドは、5Gネットワークを運用または使用する組織やネットワーク事業者や機器ベンダーに利益をもたらす可能性があり、通信および公安コミュニティにとって特に興味深い。実践ガイドの各ボリュームを予備案としてリリースすることで、これまでの進捗状況を共有し、受け取ったフィードバックを使用して実践ガイドの将来のボリュームを形作り、組織が5Gに移行する際に使用できる最新の5G技術と実践を特集することができる。	https://csrc.nist.gov/publications/detail/sp/1800-33/draft	
2021/1/25	Executive Order on Ensuring the Future Is Made in All of America by All of America's Workers	全米の労働者によって全てアメリカで作られる未来を確実にする統領令	1									1				米国で生産され、米国で提供される物品、製品、材料、および サービスを最大限に利用するために、連邦財政援助賞および連邦調達を行う。米国政府は、可能な限り、米国企業が戦略的産業で競争し、米国の労働者が繁栄するのを助けるような財、製品、材料、サービスを調達する。 命令は、既存の抜け穴を塞ぐことを求め、GSAが主催するウェブサイトを含む新たな監視体制を構築して、一般公開された権利放棄書を掲載することを求めている。バイデン大統領の約束である「バイ・アメリカン」を実現し、企業が国内優遇措置を受けながらも生産や雇用を海外で行うことを可能にする抜け穴を塞ぐ。この命令により、バイデン大統領は、連邦政府が税金を使うときには、アメリカの労働者によるアメリカ製の製品とアメリカ製の部品に使われることを保証している。	https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/25/executive-order-on-ensuring-the-future-is-made-in-all-of-america-by-all-of-americas-workers/ https://www.nextgov.com/policy/2021/01/biden-orders-agencies-buy-more-american-made-products-and-publicly-post-exemptions/171613/	大統領令を厳密に運用あるいは要件化させられると、Supply Chainを原則全て米国内で完結させる必要が出てくる。 労働者層の支持獲得のための buy american を継承は、部品までアメリカ製するとアメリカの法規制を適用できるので、セキュリティ強化につながると前政権からアメリカの政策当事者考えている。しかし、アメリカ政府の裁量の範囲なので、今後どうなるのか、各企業様で定常的にモニタする必要がある。
2021/1/26	Biden's Federal Chief Information Security Officer Brings Public and Private-Sector Experience	バイデン氏の連邦最高情報セキュリティ責任者は官民の経験を提供	1									1				バイデン政権は、連邦政府のCISO最高情報セキュリティ責任者にクリス・デルーシャ（Chris DeRusha）を選出。クリス・デルーシャはホワイトハウス、DHS、フォード・モーター・カンパニーでのサイバーセキュリティ・アドバイザーとしての経歴を有し、連邦、州、民間企業のサイバーセキュリティの経験を連邦政府機関や国内最大級のハイテク企業が国家レベルのハッカーによるシステム侵害の疑いに対処する。 また、政権はサイバーセキュリティを優先し、1.9兆ドルの景気刺激策案には、技術の近代化とサイバーセキュリティとインフラセキュリティ機関のための90億ドルが含まれている。特に2億ドルを「数百人の専門家の迅速な雇用」のためにCISOと米国デジタルサービスが自由に使えるようにすることを求めています。連邦CISOとU.S.デジタルサービスの自由裁量に委ねるよう呼びかけている。	https://www.nextgov.com/cybersecurity/2021/01/bidens-federal-chief-information-security-officer-brings-public-and-private-sector-experience/171627/	

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			
2021/1/26	NIST Cybersecurity for IoT Draft Guidance: Rounding Up the Requirements	NISTの「IoTのためのサイバーセキュリティ」ドラフトガイダンス。要件の取りまとめ	1	1				1								NIST Cybersecurity for IoT Draft Guidance: Rounding Up the Requirements ：Webiner開催 NISTは、非技術的要件のサポートを含む連邦政府のIoTサイバーセキュリティ要件の定義に関するガイダンスの草案をレビューのために公開。4つの新しい文書は、IoTデバイスが連邦情報システムのセキュリティおよびプライバシー管理に統合されることを確実にすることを目標に、IoTサイバーセキュリティのためのガイダンスの範囲を拡大している。WebinarではNISTの執筆者が文書の重要なアイデアを発表し、質問を受け付ける。ベンダー・コミュニティと顧客コミュニティの双方がIoTデバイスがもたらすメリットを活用しながら、関連するリスクに思慮深く、積極的に対応できるようなIoTサイバーセキュリティのガイダンスを提供するためのフィードバックを期待している。 (1)IoT Program 紹介 ・NIST IoT ProgramはTrustを目標：Trustを実現する構成要素はSecurity、Privacy、Resilience, and Safety ・5つの基本原則：- Risk based understanding、- No one size fits all、- Ecosystem of Things、 - Outcome based approach、- Stakeholder engagement ・FISMAの遵守 (2)NISTIR8228の考え方が原点となっている ・リスクの軽減とSP800-53のControlsの実現（個々のIoT機器の能力に依存） ・連邦政府省庁がそれぞれのIoT機器にどの程度信頼性をおけるかの判断 (3)SP800-213、NISTIR8259B/C/Dのポイント説明 ・manufactures, vendorsに期待する連邦の要件 ・IoT装置に必要な能力capabilitiesの具体的なカタログをgithubで公開。	https://www.nccoe.nist.gov/events/nist-cybersecurity-iot-draft-guidance-rounding-requirements	Public Comments進行中の文献に関する説明会 https://github.com/usnistgov/FederalProfile-8259A
2021/2/1	SP 1800-33 (Draft) 5G Cybersecurity (Preliminary Draft)	SP 1800-33 (Draft) 5G サイバーセキュリティ（ドラフト）			1			1								NIST の National Cybersecurity Center of Excellence (NCCoE) は、近日公開予定の 5G サイバーセキュリティに関する実践ガイド 3 巻の第 1 弾である予備草案をコメント用に掲載。これまでの進捗状況を共有し、受け取ったフィードバックを使用して、今後の実践ガイドの形を整え、組織が 5G への移行時に利用できる最新の 5G 技術と実践とする。5Gネットワークを運用または使用している組織だけでなく、ネットワークオペレータや機器ベンダーにとっても有益なものであり、電気通信および公共安全のコミュニティにとっても特に関心の高いものとなる。	https://csrc.nist.gov/publications/detail/sp/1800-33/draft	
2021/2/1	Ford and Google sign six-year deal for in-car connectivity and cloud services	フォードとグーグル、車載コネクティビティとクラウドサービスで6年間の契約を締結				1								1		フォードとグーグルは6年契約に突入しており、自動車メーカーは数億ドルの価値があるとしている。 今回の提携により、グーグルは、自動車メーカーが拡大している車載コネクティビティやクラウドコンピューティングなどのテクノロジーサービスの多くを担うことになる。グーグルは、車載インフォテインメントシステムやリモート、あるいは上空からのアップデートなど、人工知能を使ってフォードを支援することが期待されている。このパートナーシップは、フォードの事業を合理化し、現在進行中の110億ドルの再編計画を加速させることを目的としています。これは、このようなシステムの開発と維持に近年毎年数億ドルを費やしてきた自動車メーカーにとって、大きな転換を意味する。	https://www.cnbc.com/2021/02/01/ford-and-google-sign-six-year-deal-for-android-in-car-apps-cloud.html	車に限らず、他の製造分野でもGoogleのサービスが使われる可能性がある。
2021/2/2	2021: What's Ahead from NIST in Cybersecurity and Privacy?	2021: サイバーセキュリティとプライバシーのNISTの計画	1	1				1								NIST ブログ：2021年のサイバーセキュリティやプライバシー関連の支援に関して、NISTが取り組む優先分野 2020年、NISTは人々の安全と経済の生産性を維持するために、個人や組織がネットワーク環境に移行するのを支援することを優先した。2021年はより大きな企業リスクの一部としてサイバーセキュリティリスクの管理に注意を向け、サイバーセキュリティとプライバシーにもっと注意を払い、、システムとコンポーネントのサイバーセキュリティを強調し、国際的な標準化作業に参加する。 ・春にはCybersecurity Framework (CSF) がどのように使われており、どのように改善されるのかパブリックコメントを募集 ・SP 800-161：「連邦情報システムおよび組織におけるサプライチェーンリスク管理の慣行」の改訂 ・昨年12月に発表されたこれら4つの文書INISTIR8279 B,C,Dと SP 800-213)は、IoTデバイスが連邦政府の情報システムのセキュリティおよびプライバシー管理に統合されることを確実にすることを目標とし、IoTサイバーセキュリティのためのガイダンスの範囲を拡大するもので、パブリックコメントを待っている。 ・暗号化規格と検証の強化：現在のNIST暗号規格の性能が許容されない制約された環境での使用に適した軽量暗号化アルゴリズムを募集、評価、標準化するコンペティションを予定。 ・サイバーセキュリティの指標と測定に関するプログラム：情報セキュリティのためのパフォーマンス測定ガイド(SP 800-55 リビジョン1)の更新版をリリースなど。	https://www.nist.gov/blogs/cybersecurity-insights/2021-whats-ahead-nist-cybersecurity-and-privacy	NICTSP800-161の改定はCPS supply chainに関連する動向として注目される。

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			
2021/2/3	Cybersecurity Standardization Conference 2021 European Standardization	サイバーセキュリティ標準化会議 2021 EU標準化														ENISA, CEN/CENELEC, ETSIが共催し onlineで開催 U IoT Certification Schemeが作られることが発表者では既に前提とされていると考えられ、将来欧州が制定しうる関連新規法制への対応などにも関心が示された。議論の焦点はIoTの中でも消費者向けIoTが主体で、appliance並びに家の空調などの家電を含む。議論の関心はsecurityとPrivacyが中心となっているが、resilienceとsafetyにも関心が寄せられている。	https://www.enisa.europa.eu/events/cybersecurity_standardisation_2021/std-2021-presentations	
2021/2/3	Securing EU's Vision on 5G: Cybersecurity Certification	5Gに関するEUのビジョンの確保：サイバーセキュリティ認証			1					1						ENISAは、5Gネットワークでのサイバーセキュリティ認証スキームの候補を求める欧州委員会の要請を歓迎する。 欧州委員会からの要請を受けて、ENISAは5Gでの新しい候補サイバーセキュリティ認証スキームの準備を進める。このステップは、5GセキュリティのEUツールボックスに続くものであり、より広範なリスク軽減戦略の一環として、特定のリスクへの対処に貢献するため、5Gネットワークのサイバーセキュリティをさらに強化することが期待される。 5Gのサイバーセキュリティ認証スキームは、既存のサイバーセキュリティ認証スキームによってすでに利用可能な規定と、サイバーセキュリティ認証に従事して獲得した経験に基づく。	https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification	
2021/2/4	ICT SCRM (SUPPLY CHAIN RISK MANAGEMENT) TASK FORCE ANNOUNCEMENTS	ICTサプライチェーン リスク管理タスクフォース発表			1				1							CISAは、ICT SCRMタスクフォースを2021年7月まで6ヶ月間延長することを発表。この延長により、ワーキンググループは、最新の脅威シナリオレポートやその他の次期製品のリリースを含め、第2年目の報告書で概説された作業を継続することができる。また、ICTサプライチェーンに更なるレジリエンスを構築するための推奨事項の運用を可能にし、政府と産業界のメンバーが、サプライチェーンに関する他の進行中の官民連携の取り組みに協力し続ける。	https://www.cisa.gov/ict-scrm-task-force	CISA：Cybersecurity & Infrastructure Security Agency ICT ： Infromation and Communications Technology SCRM ： Supply Chain Risk Management
2021/2/5	Network Equipment Security Assurance Scheme – Development and Lifecycle Security Requirements Version 2.0	ネットワーク機器のセキュリティ保証スキーム ー開発とライフサイクルのセキュリティ要件 2.0 版		1									1			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。3GPPで作成されたSECAM関連の文書をベースに、ベンダーの開発工程、製品のライフサイクルプロセスに対するセキュリティ要件を定義。 オープンソースソフトウェアの取り扱い、他社からのコンポーネントの取り扱い、セキュリティテストの拡張、製造段階・配達段階でのセキュリティ要件、ソースコードレビュー、サプライチェーン・セキュリティ。 すべての要求事項の再グループ化と番号の付け直しを実施。	https://www.gsma.com/security/wp-content/uploads/2021/02/FS.16-NESAS-Development-and-Lifecycle-Security-Requirements-v2.0.pdf	
2021/2/8	The comment period for all four drafts has been extended through February 26, 2021.	4案のすべてのコメント期間を2021年2月26日まで延長	1	1					1							NIST Cybersecurity for IoTチームは、連邦政府機関がIoTを安全に調達・統合し、FISMA義務を継続的に満たすことができるように、非技術的要件のサポートを含むIoTサイバーセキュリティ要件の定義に関するガイダンスを連邦政府機関およびIoTデバイス製造業者に提供する4つの文書の公開草案を公開している。 コミュニティからの意見は、NISTIR 8259Bの表1、NISTIR 9258Dの表1と表2の項目への特定の参照文書の内容のマッピングに関して特に求めており、4番目の列である「IoT参照例」の列を埋めるためのものである。NISTIR 8259Aの表1は、これらの有益な参照マッピングのモデルとして使用することができる。これらの文書に対するパブリックコメント期間は、2021年2月26日までとなっている。	https://csrc.nist.gov/news/2020/draft-guidance-for-defining-iot-cyber-requirements	期間延長はステークホルダの要望の可能性が考えられる。
2021/2/8	Hacker modified drinking water chemical levels in a US city	ハッカーが米都市の飲料水の化学物質レベルを改ざん	1									1		1		正体不明のハッカーがフロリダ州オールズマー市の水処理施設のコンピューターシステムにアクセスし、化学物質のレベルを危険なパラメータに変更した。ハッカーの侵入はすぐに発見され、ハッカーの改ざんはすぐに元に戻された。 攻撃のニュースは本日、市当局者の記者会見で明らかにされた。	https://www.zdnet.com/article/hacker-modified-drinking-water-chemical-levels-in-a-us-city/	米国では高い関心を集めた
2021/2/9	台湾TSMC、日本に子会社設立へ 3DIC材料を研究開発	同左			1									1		半導体の受託生産最大手、台湾積体電路製造（TSMC）は同社が100％出資する現地法人を日本の茨城県つくば市に設立することを決定。3次元集積回路（3DIC）材料の研究開発拠点となる見通し。拠出資本は186億円未満。	https://japan.cna.com.tw/news/aeco/202102090008.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			
2021/2/9	'Quad' nations sign up for meta think-tank to advance 'Techno-Democratic Statecraft'	「クアッド」参加国、「テクノ・民主主義的な国家体制」を推進するメタ・シンクタンクに参加			1									1		米国、日本、インド、オーストラリアが技術と地域の安全保障の交錯を探るフォーラムを開催 オーストラリア、アメリカ、日本、インドの大学やシンクタンクが、情報技術、地域の安全保障、インターネットの自由について議論を進めることを期待して、新たなグループを結成した。 メンバ：オーストラリア（オーストラリア国立大学国家安全保障大学） インド（オブザーバー研究財団） 日本（政策研究大学院大学） 米国（新米安全保障センター） 提案の中には、技術製品の継続的な流れを確保するためのサプライチェーンの改善方法についてのアイデアが含まれており、中でもレアアースは特に注目されている。目標の一つに技術政策が他の政策分野に影響を与えることを政府が理解できるようにすることがある。テクノロジー業界との連携も考慮されているが、ベンダーが売れると思うことを何でもやってしまうと、政府がAIのようなテクノロジーを規制するのは難しいと発表者は指摘している。	https://www.theregister.com/2021/02/09/quad_tech_network/	
2021/2/11	Biden to sign executive order addressing chip shortage	バイデン、チップ不足に対処する行政命令に署名	1									1				ホワイトハウスのジェン・プサキ報道官は、木曜日の毎日の記者ブリーフィングで、保留中の命令を発表し、命令は "今後数週間のうちに "署名されるだろうと述べた。 政権は現在、サプライチェーンにおける潜在的な難点を特定し、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いる。同時に、政権は将来を見据えており、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の動機の一つである。	https://thehill.com/policy/technology/538474-biden-to-sign-executive-order-addressing-chip-supply-chain-shortage	
2021/2/11	U.S.-Japan Cooperation on High-Tech Supply Chain Security	日米ハイテク・サプライチェーンの安全保障に関する協力			1										CSIS	CSIS経済学プログラムは、日本国際問題研究所（JIIA）と共同で、中国の第14次5カ年計画と二重循環戦略が中国の技術自給戦略とグローバル・サプライチェーンにおける役割に与える影響、そしてハイテク・サプライチェーンと新興技術の研究開発を確保するために日米がどのように協力していけるかについてパネルディスカッションを行う。イベントでは、JIIA理事長で元駐米日本大使の佐々江健一郎氏の挨拶も予定されている。	https://csis.zoom.us/webinar/register/WN_3c7k9gVWSgOKaup7pG970w	
2021/2/11	NISTIR 8276 Key Practices in Cyber Supply Chain Risk Management: Observations from Industry	NISTIR 8276 サイバーサプライチェーンのリスク管理における重要な実践：業界の観察から	1	1				1								NISTIR 8276 最終確定版を公開 サイバーサプライチェーンのリスクを管理するためのアプローチは、サイバーサプライチェーンリスク管理(C-SCRM)と呼ばれる。本資料で紹介する主要な実践は、増大し続けるデジタル・ビジネスのコミュニティに、あらゆる組織がサプライ・チェーンに関連するサイ バー・セキュリティ・リスクを管理するために利用できる一連の「重要事例」を提供する。提示されている「主要事例」は、あらゆる規模、範囲、複雑性の組織において、堅牢な C-SCRM 機能を実装するために利用できる。 これらの実践は、既存のC-SCRM政府および業界のリソースに含まれる情報と、2015年および2019年のNIST研究イニシアチブ中に収集された情報を組み合わせたものである。	https://csrc.nist.gov/publications/detail/nistir/8276/final https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf	
2021/2/12	Alert (AA21-042A) Compromise of U.S. Water Treatment Facility	注意喚起（AA212-042A）米国の水処理施設の侵害	1						1							2021年2月5日、米国の飲料水処理プラントの監視制御・データ収集（SCADA）システムに正体不明の犯罪者が不正アクセス。犯罪者は、SCADAシステムのソフトウェアを使用して、水処理プロセスの一部として水酸化ナトリウムの量を増加させた。SCADAシステムのソフトウェアが不正な変更を検知して警報を発する前に、水処理場の担当者は直ちに投与量の変更に気付き問題を修正。その結果、水処理プロセスは影響を受けず、通常通りに稼働し続けた。サイバー犯罪者は、パスワードのセキュリティが不十分であったことや、古いオペレーティング・システムを含むサイバーセキュリティの弱点を利用してシステムにアクセスした可能性が高いと考えられる。初期の情報では、TeamViewerなどのデスクトップ共有ソフトウェアがシステムへの不正アクセスに使用された可能性があることを示している。この事件の現場対応には、ピネラス郡保安官事務所（PCSO）、米国シークレットサービス（USSSS）、連邦捜査局（FBI）が参加した。	https://us-cert.cisa.gov/ncas/alerts/aa21-042a	侵入の原因はシステムの設定の不備をついた典型的な攻撃と考えらえる。

公開時期	タイトル（原文）	タイトル（邦訳）	組織(対象組織)					情報源								要旨	参照先	その他特記事項
			政府・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			
2021/2/12	The Long Hack: How China Exploited a U.S. Tech Supplier	ロングハック：中国がいかにして米国の技術サプライヤーを悪用したか			1									1		米国の捜査当局は何年も前から、スーパーマイクロコンピュータ社製の製品に改ざんが見つけていた。同社によると、そのことは知らされず、一般にも知らされていなかった。 2010年、米国国防総省は、数千台のコンピュータサーバーが軍事ネットワークデータを中国に送信していることを発見した。これはマシンの起動プロセスを処理するチップに隠されたコードによるものである。2014年、インテル社は、中国の精鋭ハッキンググループが、サプライヤーの更新サイトからマルウェアをダウンロードした1台のサーバーを介してネットワークに侵入したことを発見した。2015年、連邦捜査局は、中国の工作員がスーパー・マイクロ・コンピュータ社のサーバーにバックドアコードを搭載した余分なチップを隠していたことを複数の企業に警告した。米国のスパイマスターたちは、それぞれの攻撃に対抗し、中国の能力について詳しく知ろうとしていたため、操作を発見したものの、ほとんど秘密にしていた。 「Supermicroは、米国企業が中国で製造することを選択した製品の潜在的な不正な改ざんにどれほど影響を受けやすいかを示す完璧な例だ」と元FBI高官のJayTabbは述べた。	https://www.bloomberg.com/features/2021-supermicro/	
2021/2/24	米、同盟国と供給網整備　半導体・EV電池で中国に対抗	同左	1											1		バイデン米政権は半導体や電池など重要部材のサプライチェーン（供給網）づくりで同盟国や地域と連携する。関連の動きを加速させる大統領令に月内にも署名する。日本などアジア各国・地域との協力を念頭に、安定して調達できる体制を整備する。対立する中国に依存する供給網からの脱却を目指す。バイデン大統領は供給網の国家戦略をつくるよう命じる大統領令に署名する。	https://www.nikkei.com/article/DGXZQOGN192KP0Z10C21A2000000/	
2021/2/24	NIST blog There's Still Time to Comment on IoT Cybersecurity Guidance – Send Us Your Feedback Today!	IoTサイバーセキュリティガイダンスについてコメント募集（本日まで）														NISTブログ： NISTIR8259シリーズのドラフトに関するコメント募集の最終案内及びこれまで寄せられた一部コメント紹介、他のガイダンスと関連したNISTIR8259の位置付け、役割、活用方法等について説明。 特に、NISTIR8259と既存の国際規格、業界標準との関連性を明確にすることを求めるコメントとこれまでのNISTの全国オンライン情報参照(OLIR)プログラムを通じた活動（消費者技術協会(CTA)のCTA-2088の情報参照など）を紹介。	https://www.nist.gov/blogs/cybersecurity-insights/theres-still-time-comment-iot-cybersecurity-guidance-send-us-your	
2021/2/24	Today President Biden will sign an Executive Order to help create more resilient and secure supply chains for critical and essential goods.	本日バイデン大統領は、重要かつ不可欠な商品のために、より回復力があり、安全なサプライチェーンの構築を支援するために、行政命令に署名する	1									1		1		米国は、生産不足、貿易の途絶、自然災害、外国の競争相手や敵対者による潜在的な行動によって、米国が再び脆弱な状態に陥ることがないようにしなければならない。本日の行動は、サプライチェーンのリスクに包括的に対処するよう政権に指示するという大統領の選挙公約を実現するものである。私たちのサプライチェーンをより安全なものにするという課題は、有色人種のコミュニティを含む全国のコミュニティにとって、高給取りの仕事の源にもなりうるものであり、この仕事の利益がすべてのアメリカ人に行き渡ることを確実にするための措置がとられる。 この大統領令は、米国のサプライチェーンの包括的な見直しを開始し、連邦政府の各省庁に、広範なリスクと脆弱性に対して米国のサプライチェーンを安全にする方法を特定するよう指示するものである。弾力性のあるサプライチェーンを構築することは、重要な製品の不足に直面することから米国を守ることになる。 また、米国の競争力を維持し、米国の国家安全保障を強化するために必要な投資を促進する。 この命令は、4つの主要製品のサプライチェーンにおける脆弱性に対処するために、連邦政府機関全体で100日間の迅速な見直しを指示する。さらに米国のサプライチェーンのより広範なセットについて、より詳細な一年間の見直しを要求している。 E.O.は、この問題に関する超党派の議会の行動とリーダーシップを基盤としており、政権は引き続き議会と緊密に連絡を取り合い、レビュー期間中の提言を募る予定である。 バイデン大統領はまた、米国のパートナーや同盟国と協力して、強力で弾力性のあるサプライチェーンを確保するよう、政権に指示している。	https://www.whitehouse.gov/briefing-room/statements-releases/2021/02/24/fact-sheet-securing-americas-critical-supply-chains/ https://www.washingtonpost.com/business/2021/02/24/biden-supply-chain/	

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			
随時更新	NIST Cybersecurity for IoT Program	NIST IoTサイバーセキュリティプログラム	1		1			1								NISTIoTProgram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横断的に大規模に推進する。Program Missionとして、「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を促進する。」を掲げる。 NIST Cybersecurity for IoT Programに関連するNISTの最新情報が掲載されている。	https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program	NISTは商務省の傘下組織として、発足時の物理化学に加え多様な分野を所掌する6研究所を有する。このうち、情報技術研究並びに標準化を行うInformation Technology Laboratory（ITL）が、NIST Cybersecurity for IoT Programを運営し、活動を行っている。 https://www.nist.gov/about-nist/visit https://www.nist.gov/about-nist/our-organization https://www.nist.gov/itl

その他	NIST（米国標準技術研究所）とセキュリティ～概要編～		1												＊1	NISTにおけるセキュリティに関する活動についての解説。 NISTの概要と情報技術研究所の位置づけを説明し、情報技術研究所(ITL)の活動の解説の中でNISTの出版物を説明	http://www.intellilink.co.jp/article/column/sec-nist01.html	＊1 ：NTTデータ先端技術株式会社
	NIST SP 800-53の解説		1	1											＊2	米国国立標準技術研究所(NIST)が発行したNIST SP800-53の概要を解説 ・NIST SP 800-53（連邦政府情報システム、および連邦組織のためのセキュリティ管理策とプライバシー管理策）は、米国連邦政府の内部セキュリティ基準を示すガイドラインであり、FIPS Publication 200に準拠するための具体的な指針を示す文書として発行された。 ・NIST SP 800-53と関連の深い文書としてNIST SP 800-171がある。NIST SP 800-171は、NIST SP 800-53から民間企業・組織向けに要件を抽出したものである。	https://www.manageengine.jp/solutions/nist_publications/nist_SP800-53/lp/	＊2 ： ManageEngine
	NIST（米国標準技術研究所）とセキュリティ～NIST SP800-53の概要～		1												＊1	NISTは、各連邦政府機関に対して、情報および情報システムのセキュリティを強化するためのプログラムを開発、文書化、実践することを義務付けているFISMAの実施を支援し、情報および情報システムを保護を支援するための標準、ガイドライン、その他の出版物を開発および発行。 NIST SP800-53ｉは、米国の連邦情報システムのセキュリティおよびプライバシー管理の管理策を提供する。	http://www.intellilink.co.jp/article/column/sec-nist02.html	＊1 ：NTTデータ先端技術株式会社
	NIST（米国標準技術研究所）とセキュリティ～ NIST SP800-82/ NIST SP800-161/ NIST SP800-171の概要～		1												＊1	NISTが発行したNIST SP800-82、、NIST SP800-161、NIST SP800-171の概要について解説。 NIST SP800-82：Guide to Industrial Control Systems (ICS) Security （産業用制御システム（ICS）セキュリティガイド） NIST SP800-161：Supply Chain Risk Management Practices for Federal Information Systems and Organizations（連邦政府のための情報システムおよび組織のサプライチェーン・リスク・マネージメント・プラクティス） NIST SP800-171：Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations（連邦政府外のシステムと組織における管理された非格付け情報の保護）	http://www.intellilink.co.jp/article/column/sec-nist03.html	＊1 ：NTTデータ先端技術株式会社
	NIST Guidance	IoTサイバーセキュリティに関するNICTガイダンス	1	1				1								IoTサイバーセキュリティに関するこれまでのNICTガイダンス検討の経緯とガイダンスドキュメントの概要を説明 ・NISTIR 8228が示すIoTサイバーセキュリティの課題に対して、NIST IoT Cybersecurity Program の2年以上にわたるワークショップ等の活動を通じ、IoT デバイスが連邦システムや組織に導入する特定のリスクを連邦組織が理解するのを支援するため以下の追加ガイダンスを提供することとなった。 ・SP800-213、NISTIR8259、8259A、8259B、8259C、8259Dの各ガイダンスの概要を紹介	https://pages.nist.gov/IoT-Device-Cybersecurity-Requirement-Catalogs/nist-guidance/	

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			
	EU cybersecurity certification framework	EUのサイバーセキュリティ認証フレームワーク			1					1						欧州連合におけるネットワークおよび情報システムのセキュリティ確保は、EUのオンライン経済の機能性と安全性を維持するための重要な目的とみなされている。これに失敗すると、欧州市民に多大な影響を与え、市民、産業界、行政の信頼に影響を与える恐れがあることは明らかである。Regulation (EU) 2019/881（サイバーセキュリティ法）によってENISAの役割がさらに強化されたように、サイバーセキュリティ認証という重要な任務には、適切なステークホルダーの関与と支援が求められている。Regulation (EU) 2019/881に基づくEUサイバーセキュリティ認証枠組みの目的は、サイバーセキュリティ製品、サービス、プロセスに関する信頼とセキュリティを確立し、維持することである。EUレベルでサイバーセキュリティ認証制度を策定することは、特定の要件に対する製品、サービス、プロセスの遵守の度合いを確立するための適合性評価を実施する基準を提供する。EUのサイバーセキュリティ認証フレームワークにおけるENISAの使命は、製品やサービスのICT認証のための新たなEUフレームワークに積極的に貢献し、サイバーセキュリティ法に沿った認証スキームの候補の策定、および追加のサービスやタスクを実行することである。	https://www.enisa.europa.eu/topics/standards/certification	

契約管理番号：２０００２２７５－０