２０１９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

標準化動向調査

調査報告書

２０２０年２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　株式会社情報通信総合研究所

目次

表目次

図目次

要約（和文）

サイバー空間とフィジカル空間を高度に融合したSociety5.0の実現が目前に迫ってきている。Society5.0の実現は、我々の社会や生活を豊かにし、新たなビジネスチャンスを創発するが、その一方で、IoT機器やシステム等の脆弱性を狙ったサイバー攻撃が世界各地で拡大してきていることから、IoTセキュリティの確保は国内外で喫緊の課題である。

その他にも、海外の公的機関等が定める政府調達の要件は当該国企業のみならず、サプライチェーンに関連する他国の企業にも影響が波及することが予想されており、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する制度等に関する情報収集を行い、その現状を把握することはグローバルなビジネスを円滑に行う上でも必要不可欠である。

上記のような背景のもと、本調査においては、『サイバー・フィジカル・セキュリティ対策基盤』の開発成果の普及促進に資する情報である、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調査・分析した。

具体的には、北米、欧州のIoTセキュリティ、サプライチェーンセキュリティなどを担う標準化団体（NIST、FIRST、ENISA、ETSI等）に関するここ2～3年程度の動向について情報収集とその整理を行った。また、標準化団体のみならず、IoTセキュリティに関する法律を公表した米国カルフォルニア州、イギリスに関する情報収集も合わせて行った。

情報収集の結果、IoTデバイスに関するトレンドとIoTサプライチェーンに関するトレンドについて分けて整理を行った。IoTデバイスに関するトレンドとしてはIoTデバイスを製造するにあたりセキュリティを事前に確保する取り組みである「プリマーケット」とセキュリティインシデントが発生した際に対応する「ポストマーケット」の動向があることが明らかになった。また、IoTサプライチェーンに関しては、北米、欧州ともに具体的なサプライチェーンのベストプラクティスに関する調査報告書が公表されており、より具体的な議論が進んでいることが明らかになった。その他には、NIST、ENISAといった機関が中心となりタスクフォースやワーキンググループを形成し、多様なステークホルダーが議論に参加して連携を図ろうとしていることが明らかになった。

今回の調査内容より、今後のSIP研究開発に資する調査、情報収集については、今回実施したIoTセキュリティやサプライチェーン・マネジメントに関して影響力を有する北米、欧州の標準化団体の動きに加えて、米国カルフォルニア州やイギリスといった国、自治体レベルでの動き、またグローバルなサプライチェーンの一角を担うアジアにおける

IoT セキュリティの制度や個人情報の取り扱いについてどのような対応が行われているかという点について調査が必要との結論に至った。

また、米国、欧州の IoT セキュリティやサプライチェーンに関するステークホルダーとの連携については、オープンな会合への参加の他に、標準化団体等が公表するドラフト文章にコメントすることを通じて、SIP と海外のステークホルダーの関係性の確保、SIP が取り組む内容の海外発信の可能性について検討を行った。

要約（英文）

The realization of Society5.0, which achieves a high degree of convergence between cyberspace (virtual space) and physical space (real space), is imminent. The realization of Society 5.0 will enrich our society and life and create new business opportunities, but on the other hand, cyber attacks targeting vulnerabilities in IoT devices while IoT systems are expanding around the world. Therefore, IoT security is an urgent issue for our society.

In addition, the requirements for government procurement stipulated by overseas public organizations are expected to affect not only companies in that country but also companies in other foreign countries. It is indispensable that collecting information and grasping the current situation on IoT security systems and supply chain management for global business.

For this reason, this study collect information which is related to IoT security and supply chain management in foreign countries. We surveyed and analyzed trends, technology policies, and the latest technology trends in the industry.

Specifically, over the past few years, information was collected from the standardization organizations (NIST, FIRST, ENISA, ETSI, etc.) responsible for IoT security and supply chain security in North America and Europe. In addition to this, we also collect information of the state of California and the United Kingdom, which published IoT security laws in 2020.

As a result, we find that there are some trends in IoT devices and IoT supply chain. It has become clear that there are two trends regarding IoT devices: "Pre-Market", which is an initiative to secure security when manufacturing IoT devices, and "Post-Market", which responds when a security incident occurs. Regarding the IoT supply chain, NIST and ENISA have been publishing research reports on specific supply chain best practices in North America and Europe, and it is clear that more specific discussions on supply chain management are underway. In addition, NIST and ENISA form a task force and working group, which various stakeholders are participating in discussions and trying to cooperate.

Based on this study, we conclude that surveys that will contribute to future SIP R & D will be collecting activities of North American and European standards organizations that have an influence on IoT security and supply chain management, and in addition to this, surveys are also needed on the movements at the national and local government levels such as the United Kingdom and the United Kingdom. And as another perspective, current status of cybersecurity and personal information management in Asia is needed. Because Asia is indispensable to global supply chain.

Regarding cooperation with stakeholders related to IoT security and the supply chain in the U.S. and Europe, in addition to participating in open meetings, comment on draft texts published by standardization organizations, etc. And the possibility of disseminating the contents of SIP's efforts overseas.

1. はじめに

サイバー空間とフィジカル空間を高度に融合したSociety5.0の実現が目前に迫ってきている。その一方で、IoT機器やシステム等の脆弱性を狙ったサイバー攻撃が世界各地で拡大してきていることから、IoTセキュリティの確保は喫緊の課題である。

また、海外の公的機関等が定める政府調達の要件は、サプライチェーンに関連する他国の企業にも影響が波及することが予想されており、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する制度等に関する情報収集及び現状把握はグローバル化するビジネスを円滑に行う上でも必要不可欠である。

上記のような背景のもと、本調査においては、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調査・分析した。

2. 事業概要

サイバー空間とフィジカル空間を高度に融合したSociety5.0の実現が目前に迫ってきている。Society5.0の実現は、我々の社会や生活を豊かにし、新たなビジネスチャンスを創発するが、その一方で、IoT機器やシステム等の脆弱性を狙ったサイバー攻撃が世界各地で拡大してきていることから、IoTセキュリティの確保は国内外で喫緊の課題である。その他にも、海外の公的機関等が定める政府調達の要件は当該国企業のみならず、サプライチェーンに関連する他国の企業にも影響が波及することが予想されており、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する制度等に関する情報収集を行い、その現状を把握することはグローバルなビジネスを円滑に行う上でも必要不可欠である。

上記のような背景のもと、本調査においては、『サイバー・フィジカル・セキュリティ対策基盤』の開発成果の普及促進に資する情報である、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調査・分析することによって、当プロジェクトの国際連携を推進するため、米国、欧州などのステークホルダーとの連携に関する活動案をまとめることを目的とする。

3. 調査手法

本事業の目的を達成するために、以下の調査項目を検討した。

調査対象の検討

【主要な情報源に関する検討】

- IoT サプライチェーンやセキュリティに関する主要な標準化団体を選定するとともに、主要な情報源を検討する。

上記の事業目的を達成するための手段として、本調査で採用した手法は以下の通りである。

海外における制度、標準、規制、技術等に関する情報収集を行うために、文献、またはNIST、ENISA といった関連団体が公表するニュースリリースまたは関連するホワイトペーパー、サイバーセキュリティ等の情報を取り扱うニュースメディアが公表する情報を収集し、IoT に関連するトレンドに関して情報を把握する。

上記の情報収集に加えて、より深い情報の収集や、また日本からの情報発信を目的として、本調査で海外での調査を担当する担当者との情報交換の場を設けて、情報収集を行った。

4. 調査対象の選定

本事業の目的を達成するために、IoT セキュリティやサプラチェーンに関する制度、標準、規制、技術等に関する海外動向を把握するために、以下の団体を調査対象候補として選定した。

4.1 調査対象

調査対象としては、主に北米、欧州の IoT のセキュリティ及び関連する標準化等に対象を絞ることとした。北米、欧州以外でも IoT セキュリティに関する動向は見られるが、先進的な動きや他国への影響を勘案すると、北米、欧州の動向を注視することが重要であるからである。

調査対象は以下の通りである。

表 4-1 調査対象となる機関/団体名と概要

機関/団体名	概要
NIST （National Institute of Standards and Technology）	NIST（米国国立標準技術研究所）は、技術革新や産業の競争力を強化する技術の標準化の研究を実施している。 IoT セキュリティやサプライチェーン関連では政府調達要件である「SP800-171」やサイバーセキュリティ対策の全体像である「Cybersecurity Framework」を公表する等、IoT セキュリティやサプライチェーンに関して重要なプレイヤである。
FIRST （Forum on Incident Response and Security Teams）	世界各国の CSIRT（Computer Security Incident Response Team）が情報交換、インシデントに関する協力を構築する目的で設立されたフォーラムである。
ENISA （European Network and Information Security Agency）	ENISA（欧州ネットワーク情報セキュリティ庁）は、情報セキュリティに関する専門の機関である。 欧州全域におけるネットワークデバイスの認証フレームワーク導入に向け、EU（欧州連合）や加盟国との間でアドバイス等を行っている。
ETSI （European Telecommunications Standards	欧州の電気通信の標準化仕様を策定する非営利の団体である また、ICT 関連技術に関する標準化も取り扱うことからサイバーセキュリティも活動領域の一つとなっている。

Institute)	

また、後に続く具体的な調査内容において取り扱うことはなかったが、上記以外にもIoTセキュリティ等に関連する機関/団体等として、ISO（International Organization for Standardization)、GSMA（GSMA Association)、Charter of Trust等についても参照し、適宜情報収集を行った。

4.2　主要な情報収集源について

情報収集については、4.1で記載した機関/団体が公表するニュースリリース、ホワイトペーパー、ドラフト文章等を参照し、また、セキュリティに関する専門的な情報を提供しているウェブサイトからも、IoTセキュリティやサプライチェーンに関連した情報収集を行った。以下に記すウェブサイト以外からも、検索等を通じて情報収集を行い、複数の情報源から情報収集や分析を行うことに努めた。

表4-2 主要な情報収集源のURL等

機関/団体名	カテゴリ、URL等
NIST	News https://www.nist.gov/news-events/news Events https://www.nist.gov/news-events/events Publication https://www.nist.gov/publications Publication - Cybersecurity https://www.nist.gov/publications/search?ta%5B0%5D=248731
FIRST	Newsroom https://www.first.org/newsroom/ Standards https://www.first.org/standards/ Publications https://www.first.org/resources/papers/
ENISA	Newsroom

	https://www.enisa.europa.eu/news Publications https://www.enisa.europa.eu/publications#c5=2010&c5=2020&c5=false&c2=publicationDate&reversed=on&b_start=0
ETSI	Newsroom https://www.etsi.org/newsroom Press Releases https://www.etsi.org/newsroom/press-releases

また、参考までに上記以外に参照した機関/団体の情報源については以下の通りとなる。

表 4-3 その他参照した機関/団体の情報源の URL

機関/団体名	カテゴリ、URL 等
ISO	News and Events https://www.iso.org/events.html セキュリティ関連の標準に関する情報 https://www.iso.org/isoiec-27001-information-security.html
GSMA	Press Release https://www.gsma.com/newsroom/press-releases/ IoT Security Assessment https://www.gsma.com/security/ IoT Security Guidelines and Assessment https://www.gsma.com/iot/iot-security/iot-security-guidelines/
Charter of Trust	Latest https://www.charteroftrust.com/latest/

その他にも、IoT セキュリティやサプライチェーンに関する諸課題について、ニュース記事を掲載しているメディアも参照した。調査にあたっては複数のニュースサイトを参照したが、以下では基本的な情報源となった情報源について記載する。

表 4-4　ニュースサイトに関する URL

ウェブサイト	カテゴリ、URL 等
ZDNet	Security https://www.zdnet.com/topic/security/
CNET	Security https://www.cnet.com/topics/security/
Forbes	Cybersecurity https://www.forbes.com/cybersecurity/#7ecb75b026cc
SECURITY WEEK	IoT Security https://www.securityweek.com/iot-security
CS Magazine	Security News https://www.scmagazine.com/home/security-news/
Info security	The Internet of Things https://www.infosecurity-magazine.com/the-internet-of-things/

以上の情報源を基本として、本事業の主要な目的である海外における 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について情報収集を実施した。

5. IoT サイバーセキュリティ及びサプライチェーンの動向調査

5.1 IoT サイバーセキュリティ及びサプライチェーンの動向に関する調査項目

上記 4. で示した調査対象が公表するプレスリース、公開文章などを調査し、本事業の調査に資するものについて、「公開された時期」、「報告書名/プレスリリースタイトル等」、「要旨」を北米分については表 5-1、欧州分については表 5-2 にまとめた。

本調査の調査期間は 2019 年 8 月からとなるが、調査期間以前の動向についても全体像や流れを把握するためには必要であるので、関連する内容については期間を 2 年程度遡り情報としてまとめている。

表 5-1、表 5-2 で取り上げている動向は一覧としてまとめているため、続く 5.2 でより詳細な概要を紹介する。なお、米国、欧州の IoT サイバーセキュリティ及びサプライチェーンの動向を作成するにあたっては経済産業省 商務情報政策局 サイバーセキュリティ課が公開する資料「サプライチェーン・サイバーセキュリティ等に関する海外の動き[1]」及び NIST、ENISA が公表する参照した。脚注に示される URL は 2020 年 2 月末現在のものである。

まず、北米の動向については以下の通りである。

表 5-1 北米における IoT サイバーセキュリティ及びサプライチェーンの主要な動向

時期	報告書名/プレスリリースタイトル等・要旨
2018 年 4 月	NIST Cybersecurity Framework version 1.1
	前バージョンより「サプライチェーンのリスク管理」「サイバーセキュリティリスクの自己評価」を追記
2018 年 5 月	ボットネット対策等に関する報告書
	ボットネット等の脅威に対するネットワークのエコシステムの強靭性強化に関して 5 つの目標を設定
2018 年 6 月	SP800-171 Rev.1 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizationsの更新
	セキュリティ要件を満たすために必要な具体的事項の記載を追加。
2018 年 9 月	Draft NISTIR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks
	IoT 機器により生じる、サイバーセキュリティとプライバシーリスクを軽減するための対策例を整理
2018 年 9 月	カリフォルニア州の IoT セキュリティ法

[1] https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/004_03_04.pdf

	インターネットに接続する機器に合理的なセキュリティ機能を備えることを製造者に求める法律
2018 年 10 月	NIST Cybersecurity Whitepaper
	IoT 製品・サービスの信頼に影響を及ぼす 17 の技術的な懸念事項を整理
2018 年 10 月	ICT Supply Chain Risk Management Task Force
	ICT サプライチェーンのリスクを特定、管理するために形成された官民パートナーシップを形成
2018 年 11 月	対ボットネット強靭化ロードマップ
	5 月の報告書で示した個々のボットネット対策のステークホルダー、実施スケジュールを整理
2018 年 11 月	NISTIR 8200 Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT)
	IoT の 5 つのユースケースに対するリスク、脅威分析及び国際標準化状況を整理
2019 年 2 月	Considerations for a Core IoT Cybersecurity Capabilities Baseline
	IoT 機器のコアになるサイバーセキュリティ機能のベースラインとなる 12 の候補を公表
2019 年 4 月	NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1
	ロードマップに関する資料が公開。新たなトピックスが追加された。
2019 年 6 月	NISTIR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks
	IoT デバイスの機能 (capabiliy)、サイバーセキュリティとプライバシーで考慮すべき事項、またこれらのリスクの低減に伴う課題、提言を公表
2019 年 7 月	NISTIR 8259(Draft) Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers
	IoT デバイスを製造する企業が IoT デバイスを製造する際に自主的に採用すべきセキュリティの基本項目の諮問文章を公表
2019 年 10 月	NISTIR 8267(Draft) Security Review of Consumer Home Internet of Things (IoT) Products
	「スマートライト」といったコンシューマ向けのホーム IoT デバイス

	のセキュリティに関する技術を検証したドラフト文章を公表
2020 年 1 月	カルフォルニア州の IoT セキュリティ法（Senate Bill No. 327）が施行
	カルフォルニア州で IoT セキュリティ法が施行された。
2020 年 1 月	California Consumer Privacy Act (CCPA)が施行
	カルフォルニア州でプライバシー法が施行された。
2020 年 2 月	Improving the IoT Cybersecurity Baseline with Stakeholder Input: Draft (v2) NISTIR 8259 Available for Public Comment February 4, 2020
	2019 年 7 月に公表された文章のドラフト第 2 版が公表された。
2020 年 2 月	Key Practices in Cyber Supply Chain Risk Management: Observations from Industry
	サプライチェーンマネジメントについて、効率的な企業のリスクマネジメントを支援する目的のガイダンス文書を公表
2020 年 2 月	Case Studies in Cyber Supply Chain Risk Management: Anonymous Consumer Goods Company
	米国の消費財、また食品製造業者に関するサプライチェーンマネジメントに関するケーススタディを記載
2020 年 2 月	Case Studies in Cyber Supply Chain Risk Management: Mayo Clinic
	米国の医療機関である「Mayo Clinic」のサプライチェーンマネジメントに関するケーススタディを記載
2020 年 2 月	Case Studies in Cyber Supply Chain Risk Management: Seagate Technology
	米国のハードディスク製造業者である「Seagate Technology」のサプライチェーンマネジメントに関するケーススタディを記載
2020 年 2 月	Case Studies in Cyber Supply Chain Risk Management: Palo Alto Networks, Inc.
	米国のサイバーセキュリティ企業である「Palo Alto Networks, Inc.」のサプライチェーンマネジメントに関するケーススタディを記載
2020 年 2 月	Case Studies in Cyber Supply Chain Risk Management: Anonymous Renewable Energy Company
	米国の再生エネルギー企業に関するサプライチェーンマネジメントに関するケーススタディを記載
2020 年 2 月	Case Studies in Cyber Supply Chain Risk Management: Anonymous

	Consumer Electronics Company
	米国の家電製造業者に関するサプライチェーンマネジメントに関するケーススタディを記載
2020 年 2 月	SP800-171 Rev.2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizationsの更新
	諮問を経て Rev.2 が公表されてる。

次に欧州の動向については、以下のようにまとめることができる。

表 5-2　欧州における IoT サイバーセキュリティ及びサプライチェーンの主要な動向

時期	報告書名/プレスリリースタイトル等・要旨
2017 年 9 月	The EU Cybersecurity Act: a new Era dawns on ENISA
	ネットワークにつながる機器を対象と認証フレームワークの導入に向けた議論
2017 年 11 月	Baseline Security Recommendations for IoT
	IoT セキュリティに関する課題を抽出し、解決に有用な考え方を念頭にベストプラクティスを整理
2018 年 9 月	European Cybersecurity Centres of Expertise Map ~Definition and Taxonomy~
	サイバーセキュリティに関する活動を、①研究領域、②セクター、③適用・技術、の 3 次元で分類
2018 年 9 月	Towards secure convergence of Cloud and IoT
	IoT とクラウドのセキュリティを「接続性」「分析」「統合」の 3 カテゴリに分類、セキュリティ課題を特定
2018 年 10 月	消費者向け IoT 製品のセキュリティに関する行動規範（英国）
	IoT 製品の製造メーカー等が実践すべき対策を 13 項目のガイドラインにまとめたもの
2018 年 11 月	Good Practice for Security of IoT in the context of Smart Manufacturing
	産業 IoT のセキュリティ確保に求められる対策指針をポリシー・組織・技術という 3 つの側面で整理
2018 年 11 月	セキュアルータの技術ガイドライン（ドイツ）
	“Mirai”の事例を受けて作成された、ルータのセキュリティ要件を定めた技術ガイドライン
2019 年 6 月	The European Union Agency for Cybersecurity - A new chapter for

	ENISA
	EU の Cybersecurity Act が正式に施行
2019 年 7 月	CONSULTATION PAPER - EU ICT INDUSTRIAL POLICY: BREAKING THE CYCLE OF FAILURE
	IoT セキュリティに関するコンサルテーションペーパーを公表
2019 年 7 月	Bolstering ENISA in the EU Cybersecurity Certification Framework
	「サイバーセキュリティ認証フレームワーク」の具体的なスキームに関する文章を公表
2019 年 10 月	1st Inter-EU ISACs meeting at ENISA
	ENISA がホストとなり、第 1 回目の EU ISACs(Information Sharing and Analysis Centres)会合を開催
2019 年 11 月	Advisory Group discusses Work Program 2021
	ENISA のアドバイザリーグループが会合を実施。Work Program 2021 について検討
2019 年 11 月	Good Practices for Security of IoT - Secure Software Development Lifecycle
	ENISA は IoT に関するセキュリティバイ・デザインを推進することを目的とした報告書を公表
2019 年 11 月	Good practices under the National Cyber Security Strategies
	EU におけるサイバーセキュリティのグッドプラクティスに関する文章を公表
2019 年 11 月	ENISA good practices for security of Smart Cars
	コネクテッドカーの導入により登場する新たなサイバー脅威の分類、コネクテッドカーや自動運転車におけるサイバーセキュリティ改善の具体的な方法、既存の法律、標準化等に関して掲載
2019 年 11 月	Good practices for Cybersecurity in the Maritime Sector - Port Security
	港湾に関するサイバーセキュリティの報告書。デジタルトランスフォーメーションが進む中で、港湾関係者もサイバーセキュリティの課題に直面しているとし、港湾関係者が検討すべき課題をリストアップ
2019 年 11 月	ENISA cybersecurity certification preparation underway
	サイバーセキュリティ認証フレームワークに関するスキーム検討状況について初めての会合を実施。会合には産業を代表する 20 名と EU 加盟国の認定団体から 12 名が参加

2019 年 12 月	Cybersecurity certification: lifting the EU into the cloud
	ENISA はクラウドサービスに関するサイバーセキュリティ認証スキームの準備を開始
2019 年 12 月	Call for expression of interest for an ad hoc Working Group
	ENISA はクラウドサービスに関するサイバーセキュリティ認証を検討するアドホックグループへの参加を求めるリリースを発表
2019 年 12 月	Supporting the deployment of the EU Cybersecurity Certification Framework
	ENISA は同機関が進めるサイバーセキュリティ認証フレームワークの検証に関するワークショップを開催。ワークショップでは、脆弱性の取り扱い、スキームの維持方法、認証の内容などについて議論。
2020 年 1 月	Supporting the deployment of the EU Cybersecurity Certification Framework
	ベルギーにおいて EU のサイバーセキュリティ認証フレームワークに関するワークショップを開催
2020 年 1 月	Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation
	イギリス政府が消費者向け IoT デバイスをサイバー攻撃から守る具体的な法律を公開
2020 年 2 月	Standardisation and the EU Cybersecurity Act
	サイバーセキュリティ政策を支える標準化に関する研究及び新たなサイバーセキュリティ認証フレームワークに関する文章を公表

5.2 北米の機関/団体における IoT セキュリティ及びサプライチェーンの動向に関する動きの概要

5.2.1 北米に関する動向

表 5-1 ではここ 2～3 年の間に北米で生じた、IoT セキュリティ及びサプライチェーンの主要な動向について、主に NIST が公表した文章等の概要を紹介している。

5.2.2 Cybersecurity Framework について

NIST は 2014 年 2 月にサイバーセキュリティ対策の全体像として、「特定」、「防御」、「検知」、「対応」、「復旧」対策を示した「Cybersecurity Framework Version 1.0[2]」を公表し

[2] https://www.nist.gov/cyberframework/framework-version-10

た。

その後、2017年1月、2017年2月に上述のVersion1.0の内容を修正するドラフトが公表された。その2度のドラフト文章の公表を経て2018年4月には「Cybersecurity Framwork Version 1.1[3]」が公表された。Version1.1で公表された内容では、「サプライチェーンのリスク管理（Supply Chain Risk Management)」、また「サイバーセキュリティの自己評価（Self-Assessing Cybersecurity Risk)」が追記されたことが特徴である。また、サプライチェーン全体で対策を実施することや、必要に応じて監査を行うことが求められている。また、2019年4月にはロードマップが公表され、追記されている。

サプライチェーン関連の動きとしては、2016年12月に公表されたSP800-171がセキュリティ要件を満たすための具体的事項の記載が追記され、2018年6月にRev1として公表された。また2020年2月には、「SP800-171 Rev.2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations[4]」が公表されている。

5.2.3　NISTIR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks[5]について

2018年9月にIoT機器によって起こりうる、サイバーセキュリティをプライバシーに関するリスクを軽減することを目的とした対策例の整理を行った「Draft NISTIR 8228」が公表された。このドラフト文章は諮問を経たのち、2019年6月に「NISTIR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks」として公開されている。

本文章では、IoTデバイスがサイバーセキュリティのリスクやプライバシーに影響を与える可能性があるポイントとして、以下3点に整理している。

- 多くのIoTデバイスは一般的なITデバイスが行うようなものとは異なる方法で物理的な世界とやり取りを行っている点
- 多くのIoTデバイスは一般的なITデバイスで可能なアクセス、管理、モニタリング（監視）を行うことができない点
- IoTデバイスに対するサイバーセキュリティとプライバシーの利用可能性、効率、有効性は一般のITデバイスとは異なる点

以上のような可能性を指摘した上で、IoTデバイスにおけるサイバーセキュリティのリスク、プライバシー問題を軽減するためのゴール（目標）として、以下の点を記載してい

[3] https://www.nist.gov/cyberframework/new-framework
[4] https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
[5] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

る。

【ゴール 1：デバイスのセキュリティを守る】

- アセット、IoT デバイスの脆弱性、アクセスの管理を行うとともに、デバイスのセキュリティインシデントの管理を行う。

【ゴール 2：データのセキュリティを守る】

- データの保護、データ・セキュリティのインシデント検知を行うようにする。

【ゴール 3：個人のプライバシーを守る】

- 情報フローの管理の実施、特定個人情報の処理権限管理、特定個人情報の提供に際する意思決定、データ管理との分離、プライバシー違反の検知を行うようにする。

また、IoT デバイスのサイバーセキュリティリスクやプライバシー問題を軽減するための勧告として、以下の点を記載している。

- IoT デバイスのリスク懸念について理解し、リスク軽減にチャレンジする。
- サイバーセキュリティやプライバシーのリスク軽減について、組織のポリシーやプロセスを調整する
- 最新のサイバーセキュリティやプライバシーのリスク軽減方法に取り組む。

5.2.4　NIST Cybersecurity Whitepaper[6]について

2018 年 10 月には、IoT デバイス・サービスの信頼性に影響を及ぼす 17 の技術的な懸念事項を整理した「NIST Cybersecurity Whitepaper」が公表されている。

本文章では、IoT 製品やサービスが所望の動作を提供できるかどうかを判断する際に利用者が使用する IoT、サービス、データを信頼できるかという観点が重要とされており、IoT 製品やサービスの信頼に悪影響を及ぼす可能性のある 17 の技術的な懸念事項について、一般的な IT 技術者に広く理解を促すためのホワイトペーパーとなっている。

上述の 17 の技術的な懸念事項については以下の通りである。

1. 「圧倒的なスケーラビリティ」
2. 「異種性」
3. 「所有者と管理の喪失」
4. 「合成性、相互運用性、統合性、互換性」
5. 「豊富な機能」

[6] https://csrc.nist.gov/publications/detail/white-paper/2018/10/17/iot-trust-concerns/draft

6. 「同期」
7. 「測定の欠如」
8. 「予測可能性」
9. 「テストと保証」
10. 「IoT 認証基準の欠如」
11. 「セキュリティ」
12. 「信頼性」
13. 「データの整合性」
14. 「過剰なデータ」
15. 「スピードとパフォーマンス」
16. 「ユーザビリティ」
17. 「可視性と発見可能性」

5.2.5　NISTIR 8200 Status of International Cybersecurity Standardization for the IoT[7]について

2018 年 11 月には「NISTIR 8200 Status of International Cybersecurity Standardization for the IoT」が公開された（2018 年 2 月にドラフト版を公開している）。

本文章においては、数ある IoT のカテゴリの中から 5 つをユースケースとして選択し、IoT サイバーセキュリティの目的、リスク、脅威の分析及び国際標準化状況を整理を行っている。5 つのユースケースとしては以下の通りである。

1. コネクティッドカー（CV:Connected Vehicle）：車両、道路、交通インフラが交通データを共有するサービス
2. 消費者向け IoT：屋内の IoT アプリケーションと、ウェアラブル端末によるサービス
3. ヘルスケア・メディカルデバイス：電子化された診察記録や患者から取得されたヘルスケアデータを共有するサービス
4. スマートビルディング：エネルギー使用量監視システム、制御セキュリティシステム、照明制御システム等のサービス
5. スマート製造：データ、テクノロジー、高度な生産能力、クラウド、その他のサービスを統合するサービス

5.2.6　Considerations for a Core IoT Cybersecurity Capabilities Baseline[8]につい

[7] https://csrc.nist.gov/News/2018/NIST-Publishes-Interagency-Report-(NISTIR)-8200
[8]https://www.nist.gov/system/files/documents/2019/02/01/final_core_iot_cybersecurity_capabilities_baseline_considerations.pdf

て

2019年2月には、「Considerations for a Core IoT Cybersecurity Capabilities Baseline」が公表された。これは、IoT機器のサイバーセキュリティ機能のコアとなる、12のベースライン候補が含まれており、具体的には以下のものが候補として掲載されている。

【全て又はほとんどのIoT機器に適用されるベースライン候補】

1. 論理的かつ物理的に識別できる。
2. ソフトウェア及びファームウェアは、安全で制御された設定可能な機構を用いてアップデートできる。
3. 許可されたユーザーは、安全な「デフォルト」状態への復元を含めて、機器の設定を安全に変更できる。機器設定に対する許可されていない変更を防ぐことができる。
4. 機器及び機器インターフェースへのローカル及びリモートのアクセスを制御できる。
5. 保存及び送受信されたデータを保護するための暗号を使用できる。
6. 機器通信のすべての層に、業界が承認した標準化されたプロトコルを使用できる。
7. サイバーセキュリティイベントの詳細をログに記録し、許可されたユーザー及びシステムがそれらにアクセスできる。
8. 機器上の全ての保存データは、許可されたユーザーによってリセットでき、全ての内部データストレージから安全に削除される。

【全てのIoT機器に要求するには適さない可能性があるベースライン候補】

9. ソフトウェア、ファームウェア、ハードウェア及びサービスの全ての取得元を確認するための情報が開示され、アクセスできる。
10. バージョンやパッチの状態を含む、現在の機器内部のソフトウェア及びファームウェアの一覧が開示され、アクセスできる。
11. 機器の設計や設定を通じて、機能を最小限とする指針を実施できる。
12. 物理的なアクセスを制御できるように設計される。

5.2.7　NISTIR 8259(Draft) Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers[9]について

2019年7月には、IoTデバイスを製造する企業がIoTデバイスを製造する際に自主的に

[9] https://csrc.nist.gov/publications/detail/nistir/8259/draft

採用すべきセキュリティの基本項目を整理したドラフト文章「NISTIR 8259(Draft) Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers」が公表された。2020年1月にはドラフト文章の第2版が公表されており、2020年2月までパブリックコメントが求められている。

本文章に記載されたIoTデバイスのセキュリティ機能に関する推奨機能は以下の通りである。

【デバイスの識別】

- IoTデバイスは論理的かつ物理的にユニークに識別することが可能にするべき。
- ネットワークに接続する際にシリアルナンバーやユニークアドレスが利用されるべき。

【デバイスの設定】

- 認証されたユーザがデバイスのソフトウエアやファームウェア設定の変更を行えるようにすべき。多くのIoTデバイスは機能やセキュリティ機能の管理を変更する方法を有する。

【データ保護】

- IoTデバイスに格納され、またネットワークを通じて送信されるデータについて、不正なアクセスや改変からどうやって保護するかを明らかにするべき。あるデバイスではデバイスの内部ストレージに保持するデータを暗号化している。

【インターフェースへの論理的なアクセス】

- デバイス自身のローカル及びネットワークインタフェースへのアクセスを制限されるべき。

【ソフトウエアとファームウェアのアップデート】

- デバイスのソフトウエアとファームウェアはセキュアかつ設定可能なメカニズムでアップデート可能にするべき。いくつかのIoTデバイスでは自動アップデートが製造業者から配信され、利用者の負担は少ない。

【サイバーセキュリティの状況検知（サイバーセキュリティイベントログ)】

- IoTデバイスはサイバーセキュリティに関するイベントのログを保存可能とするべき。また、そのログについてはIoTデバイスの保有者または製造者のみがアクセスできるようにするべき。
- これらのログはユーザや開発者がデバイスの脆弱性をセキュアにしたり改善する助けになる。

5.2.8 NISTIR 8267(Draft) Security Review of Consumer Home Internet of Things

(IoT) Products[10]について

2019年10月、NISTは「NISTIR 8267(Draft) Security Review of Consumer Home Internet of Things (IoT) Products」を公表している。このドラフト文章は「スマートライト」といったコンシューマ向けのホームIoTデバイスのセキュリティに関する技術を検証した文章である。

検証対象となったIoTデバイスは、スマートライト（電球)、スマートセキュリティ・ライト、スマートセキュリティ・カメラ、スマートドアベル、スマートプラグ、スマートサーモスタット、スマートテレビの7種類となっている。

上記した7種類のデバイスに対して、セキュリティに関する検証を行うために、具体的に以下のような調査を実施している。

- 公開情報によるデバイスの情報収集
- ネットワーク対応状況（Wi-Fiなどへの対応)、デバイス操作とデバイス機能、セキュリティ対応状況
- ハンズオンによるデバイス機能のレビュー
- ネットワーク機能
- セキュリティ機能の分析
- デバイス認証、ソフトウエア/ファームウェアのアップデート、デバイス設定、デバイスのリセット、データ保護、セキュリティイベント発生時のログ方法、インターフェースへのアクセス

以上の検証から発見された内容、またセキュリティの改善点を以下のように記載している。

- IoTデバイスがモバイルデバイスやウェブアプリと接続する際のログインに脆弱性がある。
- 「 man-in-the-middle proxy」への未対応（今回の調査の半数で未対応）のデバイスがある。
- 通信やソフトウエアのアップデートにかかる通信に古いTLS暗号が利用されている、または暗号化されていないデバイスがある。
- 攻撃者が操作可能なポートがオープンになっている。
- IoTデバイスに攻撃者が利用可能な物理的リセットボタンが搭載されている。
- IoTデバイスの製造業者がソフトウエアやファームウェアのアップデートを公開しているにも限らず、適用されていないデバイスがある。

[10] https://csrc.nist.gov/publications/detail/nistir/8267/draft

- UPnP（ユニバーサルプラグアンドプレイ）がデフォルトの状態で認証がないまま利用されている。
- IoTデバイスに搭載するサイバーセキュリティの機能を誰でも利用できるユーザーフレンドリーなものにする。

5.2.9 Key Practices in Cyber Supply Chain Risk Management: Observations from Industry[11]について

2020年2月、NISTは「Key Practices in Cyber Supply Chain Risk Management: Observations from Industry」を公表した。NISTは2008年より、サプライチェーンリスクマネジメント（C-SCRM）プログラムを実施している。

C-SCRMプログラムでは、継続的にサプライチェーンに関するセキュリティのベストプラクティスに関する調査・研究を行ってきた。今回発表した「Key Practices in Cyber Supply Chain Risk Management: Observations from Industry」では2015～2019年に行われた調査の結果から得られた内容を踏まえて、勧告を記載するものとなっている。

また、本ドラフト文章は2020年3月4日までパブリックコメントが募集されている。24のケーススタディから得られた勧告を抜粋すると、以下のようにまとめることができる。

- 組織にサプライチェーンリスク協議会（council）を設立する。
- サプライチェーン、セキュリティ、製品セキュリティ、物理セキュリティ機能のための明示的な役割、構造、プロセスを構築する。
- C-SCRMに役員の関与を増やし、定期的にリスクに関するディスカッションやパフォーマンスに関する測定の情報を共有する。
- サプライヤーリレーションシップのセキュリティについて明確な役割と責任を定義する。
- サブサプライヤーまでセキュリティ要件を浸透させる。
- サプライヤー決定にCritically Analysis Process ModelまたはBIAを利用する。
- サプライヤーの生産プロセスを可視化する。
- 自社のデータやインフラはサブサプライヤーまでアクセス可能であることを認識する。
- アクワイアラとサプライヤーの双方で同一基準（標準）を利用することを求める。

[11] https://csrc.nist.gov/publications/detail/nistir/8276/draft

- インシデント対応、ビジネス継続性、災害復旧の計画や試験に主要なサプライヤーを参加させる。
- 脆弱性の公表、インシデント通知のプロトコルを確立する。
- インシデント発生した際の外部ステークホルダーとのコミュニケーションのプロトコルを確立する。

5.2.10　NISTによるサプライチェーンマネジメントの調査

また、2020年2月、NISTはこれらの一部のケーススタディの結果を公開している。具体的な文章、対応する産業等は以下で紹介するが、それぞれのケーススタディにおける評価方法は共通しており、

- 企業概要（リスクプロファイルを含む）
- 組織としてのサプライチェーンリスクとサイバーセキュリティへの取り組みの概要
- サプライヤーマネジメント

が評価のポイントになっている。

以下は、具体的な文章名と調査対象となった産業の事例である。

「Case Studies in Cyber Supply Chain Risk Management: Anonymous Consumer Goods Company[12]」

- 米国の消費財、また食品製造業者に関するサプライチェーンマネジメントに関するケーススタディを記載している。

「Case Studies in Cyber Supply Chain Risk Management: Mayo Clinic[13]」

- 米国の医療機関である「Mayo Clinic」のサプライチェーンマネジメントに関するケーススタディを記載している。

「Case Studies in Cyber Supply Chain Risk Management: Seagate Technology[14]」

- 米国のハードディスク製造業者である「Seagate Technology」のサプライチェーンマネジメントに関するケーススタディを記載している。

「Case Studies in Cyber Supply Chain Risk Management: Palo Alto Networks, Inc.[15]」

[12] https://www.nist.gov/publications/case-studies-cyber-supply-chain-risk-management-anonymous-consumer-goods-company
[13] https://www.nist.gov/publications/case-studies-cyber-supply-chain-risk-management-mayo-clinic
[14] https://www.nist.gov/publications/case-studies-cyber-supply-chain-risk-management-seagate-technology
[15] https://www.nist.gov/publications/case-studies-cyber-supply-chain-risk-management-palo-alto-networks-inc

・ 米国のサイバーセキュリティ企業である「Palo Alto Networks, Inc.」のサプライチェーンマネジメントに関するケーススタディを記載している。

「Case Studies in Cyber Supply Chain Risk Management: Anonymous Renewable Energy Company[16]」

・ 米国の再生エネルギー企業に関するサプライチェーンマネジメントに関するケーススタディを記載している。

「Case Studies in Cyber Supply Chain Risk Management: Anonymous Consumer Electronics Company[17]」

・ 米国の家電製造業者に関するサプライチェーンマネジメントに関するケーススタディを記載している。

5.2.11 その他米国での動き（米国カルフォルニア州）

その他、IoT に関する米国での動向としてカルフォルニア州の動向をあげる。カルフォルニア州で採用された法律は米国の他の州でも同様の内容が採用される可能性があり、また、カルフォルニア州で活動する日本企業にも影響を及ぼすからである。

2018 年 9 月、米国カルフォルニア州は IoT デバイスに対するセキュリティ向上を目的とした新法（Senate Bill No. 327[18]）を設立し、2020 年 1 月 1 日からこの新法が発効することとなった。

IoT セキュリティ法の概要をまとめる[19]と以下の通りである。

・ インターネットに接続するデバイスの製造業者は、当該デバイスに合理的なセキュリティ機能または以下のすべてを備えたものとする。
・ デバイスの性質及び機能に適するもの
・ 収集、保持、送信することが可能な情報に適するもの
・ デバイス及びデバイスに含まれるすべての情報を不正アクセス、破壊、使用、変更または開示から保護されるように設定されているもの
・ 接続されるデバイスが LAN 外からのアクセスに対して認証機能を備えている場合には、以下のいずれかの要件が満たされる場合、当該認証機能は、合理的なセキュリティ機能であるとみなす。

---

[16] https://www.nist.gov/publications/case-studies-cyber-supply-chain-risk-management-anonymous-renewable-energy-company

[17] https://www.nist.gov/publications/case-studies-cyber-supply-chain-risk-management-anonymous-consumer-electronics-company

[18] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327 s

[19] 内容については、湯淺墾道「カルフォルニア州 IoT セキュリティ法に関する若干の考察」情報法制研究第 5 号（2019.5）や西村あさひ法律事務所「カルフォルニア州の IoT セキュリティ法について（日本語仮訳）」を参照した。

・　あらかじめ設定されてるパスワードが、デバイスごとで固有のものであること
・　初回アクセス時にユーザが新たな認証手段を生成しなければならないセキュリティ機能を備えていること。

また、IoT セキュリティそのものではないがセキュリティに関連するものとして、同日カルフォルニア州消費者プライバシー法（CCPA：California Consumer Privacy Act[20]）が施行された。CCPA が対象とする事業者を以下にまとめる。

1. 年間の総収入（annual gross revenues）が 2,500 万ドル以上であること
2. 5 万人以上のカリフォルニア州民の個人情報を処理している
3. カリフォルニア州民の情報を売却することで年間の収入の 50%を得ている

次に、CCPA が対象とする個人情報の範囲であるが、以下のように規定されている。カリフォルニア州民または世帯について識別し、関連し、記載し、結び付け、直接または間接的に合理的にたどることができるあらゆる情報を指すと広く定義されており、本件に関して JETRO（出典記載）では、その例として、「実名、仮名、電話番号、IP アドレス、メールアドレス、口座、社会保障番号、運転免許証、パスポート、商品・サービスの購入履歴、虹彩・網膜・指紋・掌紋・顔・声・DNA などの身体的・生体的特徴を含む生体情報、ウェブサイトの閲覧・検索履歴、位置情報データ、職歴・学歴などが列挙されているが、これらに限定されない」としている。

また、CCPA で認められている、消費者の権利としては（以下出典等注意）以下ものが挙げられる。

・　企業が収集した個人情報のカテゴリー、情報源、情報の用途および収集した情報の開示先など、企業のデータ収集の運用について開示請求する権利
・　消費者による請求から過去 12 カ月の間にその消費者について収集した具体的な個人情報のコピーを受け取る権利
・　本人の個人情報を削除してもらう権利
・　企業のデータ売却の運用について知り、その消費者の個人情報を第三者に売却しないよう求める権利（オプトアウト）
・　消費者らが CCPA により付与された新たな権利を行使したことに基づいて差別されない

最後に CCPA に違反した場合だが、以下のような処罰が定められている。

・　消費者から情報の開示請求があった場合、事業者は 45 日以内に開示することが求め

[20] https://oag.ca.gov/privacy/ccpa

られるが、これに対応できない場合、事業者は州司法長官から 30 日以内に違反を是正するよう通知を受ける可能性がある。

・ さらに、この通知後も違反が是正できない場合、消費者からの請求 1 件当たりの違反ごとに最大 2,500 ドル（故意だと認定される場合には最大 7,500 ドル）の罰金（民事罰）を科せられる可能性がある。

5.3 欧州における機関/団体における IoT セキュリティ及びサプライチェーンの動向に関する動きの概要

5.3.1 欧州の動向について

欧州で ENISA 等が公表してきたサイバーセキュリティ関連のここ数年の動向織り交ぜながらまとめた上、2019 年度の動きについてまとめる。

5.3.2 Cybersecurity Act 関連について

Cybersecurity Act[21]に関連する動向について、年を追って以下の通りにまとめた。

2019 年 6 月に、EU におけるサイバーセキュリティ政策である「Cybersecurity Act」が正式に発効された。この政策に欧州における統一的なサイバーセキュリティの認証フレームワークの設立も含まれている。この発効までの主要な項目を遡ると以下のようなプロセスを経て、決定されて来たことになる。

2017 年 9 月、ユンカー欧州委員会委員長の施政方針演説で、EU におけるサイバーセキュリティ政策（Cybersecurity Act）が発表され、新たなサイバーセキュリティ認証フレームワーク（Cybersecurity Certification Framework[22]）の導入について言及が行われた。

2017 年 11 月、ENISA が「Baseline Security Recommendations for IoT[23]」（IoT のベースラインセキュリティの推奨事項）を発表した。

2018 年 2 月、EU 標準化団体と ENISA により「Cybersecurity Act」に関する会議が開催された。

2018 年 3 月、欧州委員会と ENISA により「Cybersecurity Certification Framework」

[21] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act
[22] https://www.enisa.europa.eu/topics/standards/certification
[23] https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

に関する会議が開催された（2018 年 11 月にも開催）。

2018 年 9 月、ENISA が「Towards secure convergence of Cloud and IoT[24]」を発表。

2018 年 9 月、欧州委員会が「European Cybersecurity Centre of Expertise ～ Taxonomy and Definitions～[25]」を発表。

2018 年 11 月、ENISA が「Good Practices for Security of Internet of Things in the context of SmartManufacturing[26]」を公表。

2018 年 12 月、欧州議会、欧州連合理事会、欧州委員会が Cybersecurity Act について政治合意に至った。

5.3.3　Baseline Security Recommendations for IoT[27]について

2017 年 11 月に公表された「Baseline Security Recommendations for IoT」においては、IoT のセキュリティに関する一般的な課題を抽出し、関係者が解決するために有用となる考え方やツール（既存の規格、ガイドライン、研究資料等）、具体的な産業分野（スマートホーム、スマートカー等）を念頭においたベストプラクティスが紹介されている。

5.3.4　European Cybersecurity Centre of Expertise ～Taxonomy and Definitions～について

2018 年 9 月に欧州委員会が公表した「European Cybersecurity Centre of Expertise ～Taxonomy and Definitions～[28]」では、欧州共同研究センター（JRC）が DG-CONNECT の協力を得て、国際標準規格等を参照しつつ、様々なサイバーセキュリティに関する活動を、①研究領域、②セクター、③適用・技術、3 つの次元で分類する方式を策定している。

具体的な研究領域、セクター、適用・技術は以下の通りである。

項目	内容
研究領域	・保証・監査・認証 ・暗号 ・データセキュリティ・プライバシー

[24] https://www.enisa.europa.eu/news/enisa-news/towards-secure-convergence-of-cloud-and-iot
[25] https://publications.jrc.ec.europa.eu/repository/bitstream/JRC111441/taxonomy_final.pdf
[26] https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot
[27] https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
[28] https://publications.jrc.ec.europa.eu/repository/bitstream/JRC111441/taxonomy_final.pdf

	・教育・訓練 ・インシデントハンドリング・デジタルフォレンジック ・ヒューマンファクター ・ID・アクセス管理 ・セキュリティ管理・統治 ・ネットワーク・分散システム ・セキュリティエンジニアリング ・セキュリティ測量 ・法的観点 ・基礎的理論 ・信用の管理・保証・説明責任
セクター	・防衛 ・デジタルインフラ ・エネルギー ・金融 ・政府・公共機関 ・ヘルスケア ・海洋 ・メディア ・原子力 ・観光 ・運輸 ・スマートエコシステム ・宇宙 ・サプライチェーン ・公衆安全
適用・技術	・AI ・ビッグデータ ・ブロックチェーン ・クラウド・仮想化 ・組込みシステム ・ハードウェア技術 ・高性能計算（HPC） ・HMI ・制御システム ・情報システム

	・IoT ・モバイル端末 ・OS ・分散システム ・量子技術 ・衛星システム ・サプライチェーン ・車両システム

5.3.5　Towards Secure Convergence of Cloud and IoT について

2018 年 9 月には、ENISA が IoT とクラウドを 3 つのカテゴリ（接続性、分析、統合）に分類し、セキュリティ課題を特定するとともに、IoT とクラウドの組み合わせに関する懸念に基づく攻撃シナリオを例示し、安全なソリューションを実現する方法を提示した「Towards Secure Convergence of Cloud and IoT[29]」を公表した。

5.3.6　Good Practices for Security of Internet of Things in the context of Smart Manufacturing について

2018 年 11 月には、ENISA が「Good Practices for Security of Internet of Things in the context of Smart Manufacturing[30]」を公表している。同文章ではスマートマニュファクチャリングの観点から、産業 IoT のセキュリティ確保に求められる対策指針をポリシー・組織・技術という三つの側面で整理している。

また、サイバーセキュリティの共通理解を促進するための用語定義、スマートマニュファクチャリングにおいて守るべき機器・サービス等の分類、産業 IoT における脅威の分類を実施している。その他、セキュリティ対策ごとに既存のセキュリティ関連文書との対応関係も整理している。

5.3.7　CONSULTATION PAPER - EU ICT INDUSTRIAL POLICY: BREAKING THE CYCLE OF FAILURE について

2019 年 7 月には、IoT セキュリティに関するコンサルテーションペーパーである「CONSULTATION PAPER - EU ICT INDUSTRIAL POLICY: BREAKING THE CYCLE OF FAILURE[31]」を公表した。

[29] https://www.enisa.europa.eu/news/enisa-news/towards-secure-convergence-of-cloud-and-iot
[30] https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot
[31] https://www.enisa.europa.eu/news/enisa-news/enisa-puts-out-eu-ict-industrial-policy-paper-for-consultation

これは、ENISA が政策の改善とサイバーセキュリティ産業の発展を見据えて、サイバーセキュリティの観点から EU の ICT 産業政策の長所と不足点を検討したものである。デジタル分野での主権性や欧州におけるサイバーセキュリティ関連製品のサプライチェーンの問題について掘り下げるとともに、ICT 市場とサイバーセキュリティ市場の関係をグローバルに概観している。

今回のパブリックコンサルテーションでは、市民や民間・公的部門の利害関係者に対し、欧州の ICT・サイバーセキュリティ市場をいかに理解し、改善し得るかの意見を公募している。パブリックコンサルテーションの結果は、欧州委員会の新体制（2019 年 11 月に発足予定）と欧州議会に議論の材料として提供する模様である。

パブリックコンサルテーションでは、市民および民間・公的部門の利害関係者に向け「ICT・サイバーセキュリティ市場について、競争政策や法制度、法解釈を見直す必要があるか」「サイバーセキュリティ関連企業の財務状況と成長力の改善のために何をし得るか」など全 8 項目がかけられた。

ENISA は、グローバルな ICT 市場で EU は米国勢とアジア勢に挟み込まれているとの見解を示しており、アナログ通信や GSM など移動体通信技術では優位を保っていたが、近年、第 5 世代移動通信システム（5G）でアジアなどの域外サプライヤーとの競合にさらされていると指摘しており、また、EU の移動通信端末メーカーがアジアや米国との競争にさらされているのに加えて、ICT 分野の成功企業の多くが域外の大企業に買収されていると懸念している点がこの諮問の背景にある。

5.3.8　Bolstering ENISA in the EU Cybersecurity Certification Framework について

2019 年 7 月には、ENISA は「サイバーセキュリティ認証フレームワーク」の具体的なスキームを作りにあたってどのようなことが ENISA 等に求められているのかという点を明らかにした「Bolstering ENISA in the EU Cybersecurity Certification Framework[32]」を公表した。

この文章では、サイバーセキュリティ政策（Cybersecurity Act）のもとで ENISA に与えられている役割として、サイバーセキュリティ認証フレームワーク候補の作成を支援すること、また EC がサイバーセキュリティの課題に取り組むことを支援することが使命であるとしている。

[32] https://www.enisa.europa.eu/publications/bolstering-enisa-in-the-eu-cybersecurity-certification-framework

スキーム制定に向けた具体的な取り組みは以下のように記載されている。

- 候補となる認証スキームの準備を行うか、既存の認証スキームに関して検証を実施する
- サイバーセキュリティ認証フレームワーク、EU 加盟国における認証スキーム等に関する専用のウェブサイトの維持管理を行う
- EU のサイバーセキュリティ認証スキームのセキュリティ対象、保証レベルなどに関する必要条件について検討する
- European Cybersecurity Certification Group（ECGC）の事務局運営を担うことで欧州委員会を支援する
- 欧州委員会と協働で Stakeholder Cybersecurity Certification Group（SCCG）の議長を務める
- Stakeholder Cybersecurity Certification Group（SCCG）の事務局運営を行う
- サイバーセキュリティ認証フレームワークのドラフトを作成する間にアドホックなワーキンググループを設立し、アドバイスを行う

5.3.9 Good Practices for Security of IoT - Secure Software Development Lifecycle について

2019 年 11 月には、IoT に関するセキュリティバイ・デザインを推進することを目標とした報告書である「Good Practices for Security of IoT - Secure Software Development Lifecycle[33]」を公表している。

報告書の主要な目的は、IoT のソフトウエア開発ライフサイクルにおけるサイバーセキュリティを促進することを目的とした、グッドプラクティスの情報収集を行うことであり、また、脅威、リスク、攻撃のシナリオなどについても同じく情報収集を行っている。

本報告書のターゲットは「IoT のソフトウエア開発者」、「IoT プラットフォーム、SDK 及び API の開発者と消費者」、「IoT インテグレータ」であり、IoT システムにおけるソフトウエア開発ライフサイクルのセキュリティに特化したグッドプラクティスを掲載している。グッドプラクティスを検証するにあたっては、次の 5 つのステップを踏むことにより、調査を実施している。

1. 専門家の情報提供による調査範囲と検討すべき項目の設定
2. デスクトップによる情報収集
3. 専門家、ステークホルダへのアンケートとインタビューの実施

[33] https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

4. 分析（2及び3から攻撃のシナリオ等を作成、分析）
5. 報告書の作成と検証

5.3.10 コネクテッドカー、港湾に関するサイバーセキュリティについて

2019年11月、ENISAはコネクテッドカーに関するサイバーセキュリティの報告書「ENISA good practices for security of Smart Cars[34]」を公表した。この報告書では、コネクテッドカーの導入により登場する新たなサイバー脅威の分類、コネクテッドカーや自動運転車におけるサイバーセキュリティ改善の具体的な方法、既存の法律、標準化等に関して掲載されている。

また、同年11月には、港湾に関するサイバーセキュリティの報告書「Good practices for Cybersecurity in the Maritime Sector - Port Security[35]」を公表した。
デジタルトランスフォーメーションが進む中で、港湾関係者もサイバーセキュリティの課題に直面しているとし、港湾関係者が検討すべき課題をリストアップしている。

5.3.11 Cybersecurity certification: lifting the EU into the cloudについて

2019年12月、ENISAは「Cybersecurity certification: lifting the EU into the cloud[36]」と題したプレスリリースを公表した。プレスリリースには、ECがCybersecurity Actの48(2)条に基づき、ENISAがクラウドサービスに関するサイバーセキュリティ認証スキームの準備を行うように求めたとある。

プレスリリースの中でENISAは、クラウドサービスは公共部門、企業にとって重要なビジネス機会をもたらすものであり、欧州における単一の認証スキームはEU内で国境を超えて情報を動かすためには重要なものであり、クラウドサービスのサイバーセキュリティ認証システムは国境を超えたデータ処理のセキュリティにおける信頼性の向上と法的な確実性をもたらすことになると指摘している。

ECは民間と公的部門のステークホルダーからなる「CSPCERT（the Cloud Service Provider Certification）Working Group」の設立を行いクラウドサービスの認証におけるアドバイスをENISAに提供するように求めており、このCSPCERTへ関心があるステークホルダーは今後ENISAのウェブサイトを通じて募集されることがプレスリリースの中で明らかになった。

[34] https://www.enisa.europa.eu/publications/enisa-good-practices-for-security-of-smart-cars
[35] https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector
[36] https://www.enisa.europa.eu/news/enisa-news/cybersecurity-certification-lifting-the-eu-into-the-cloud

2019年12月9日には、ENISAは12月2日に公表したプレスリリースで触れられていたCSPCERT Working Groupへの参加を求める内容が記載された、プレスリリースである「Call for expression of interest for an ad hoc Working Group[37]」を公表した。
ENISAはステークホルダーが自身の関心について議論できるように、幅広い分野からの参加を呼びかけている。ステークホルダーの候補としてはクラウドサービスのブロバイダ、クラウドサービスのユーザ、消費者団体等を想定している。
アドホックグループへの参加申し込みは2020年の1月20日で締め切られた。

5.3.12 STANDARDISATION IN SUPPORT OF THE CYBERSECURITY CERTIFICATION Recommendations for European standardisation in relation to the Cybersecurity Actについて

2020年2月、ENISAは「STANDARDISATION IN SUPPORT OF THE CYBERSECURITY CERTIFICATION Recommendations for European standardisation in relation to the Cybersecurity Act[38]」を公表した。

本文章では、ENISAがサイバーセキュリティ認証に関する具体的なスキームを検討する際に標準化が重要な役割を担うことが記述されており、サイバーセキュリティの標準化の範囲と意義（価値）が示された後、標準化を担う機関（Standardization Bodies）の概要及び事例、サイバーセキュリティ認証スキームの内容、サイバーセキュリティ認証スキームにおける標準化の役割について述べられている。

また、主要な結論としては、標準化を担う機関の間での競争を避け、ECのサポートのもと、他の機関を共同で標準化に向けたアプローチを取るべきといった内容となっている。

5.3.13 ENISAが主催する会合やセミナーについて

ENISAは2019年6月にCybersecurity Actが正式に施行された後、欧州域内の専門家やステークホルダーを招いて、積極的に会合やセミナーを開催していることがプレスリリースを通じて理解することができる。本調査期間内に実施された会合等の実施時期や内容については以下の通りである。

2019年10月
1st Inter-EU ISACs meeting at ENISA[39]

- ENISAがホストとなり、第1回目のEU ISACs(Information Sharing and

[37] https://www.enisa.europa.eu/news/enisa-news/call-for-expression-of-interest-for-an-ad-hoc-working-group
[38] https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa-i
[39] https://www.enisa.europa.eu/news/enisa-news/enisa-hosts-the-first-inter-eu-isac-meeting

Analysis Centres)会合を開催

2019年11月

Advisory Group discusses Work Program 2021[40]

- ENISAのアドバイザリーグループが会合を実施。Work Program 2021について検討

2019年11月

ENISA cybersecurity certification preparation underway[41]

- サイバーセキュリティ認証フレームワークに関するスキーム検討状況について初めての会合を実施。会合には産業を代表する20名とEU加盟国の認定団体から12名が参加

2019年12月

Supporting the deployment of the EU Cybersecurity Certification Framework[42]

- ENISAは同機関が進めるサイバーセキュリティ認証フレームワークの検証に関するワークショップを開催。ワークショップでは、脆弱性の取り扱い、スキームの維持方法、認証の内容などについて議論
-

2020年1月

Supporting the deployment of the EU Cybersecurity Certification Framework[43]

- ベルギーにおいてEUのサイバーセキュリティ認証フレームワークに関するワークショップを開催

5.3.14　その他欧州での動き（イギリス）

その他、今回の調査対象ではないものの、IoTセキュリティに関する大きな動きとしては2020年1月にイギリス政府が消費者向けIoTデバイスをサイバー攻撃から守ることを義務付けられたことがある（Consultation outcome Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation[44]）。

---

[40] https://www.enisa.europa.eu/news/enisa-news/advisory-group-discusses-work-programme-2021
[41] https://www.enisa.europa.eu/news/enisa-news/enisa-cybersecurity-certification-preparation-underway
[42] https://www.enisa.europa.eu/news/enisa-news/supporting-the-deployment-of-the-eu-cybersecurity-certification
[43] https://www.enisa.europa.eu/news/enisa-news/supporting-the-deployment-of-the-eu-cybersecurity-certification
[44] https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation

法律化に向けた動きとしては、2018 年 10 月から始まっており、イギリスのデジタル・文化・メディア・スポーツ省（DCMS）は消費者向け IoT デバイスを利用するユーザーのセキュリティに関する負担を軽減することを目的として、IoT デバイスの開発、製造及び販売の段階でセキュリティが確保されるように、製造メーカー等が実践すべき対策をガイドラインにまとめて公表した。

このガイドラインでは、以下の内容が勧告されている。

- デフォルトのパスワードを使用しない、
- 脆弱性に関する情報公開のポリシーを公開する
- ソフトウエアを定期的に更新する
- 認証情報とセキュリティ上重要な情報を安全に保存する
- 安全に通信する
- 攻撃対象になる場所を最小限に抑える
- ソフトウエアの整合性を確認する
- 個人データの保護を徹底する
- 機能停止時の復旧性を確保する
- システムの遠隔データを監視する
- 消費者が個人データを容易に削除できるように配慮する
- デバイスの設置とメンテナンスを容易にできるように配慮する
- 入力データを検証する

2019 年 5 月には、イギリス政府は消費者向けの IoT デバイスをサイバー攻撃から守る法案の検討を開始することを公表され、諮問が開始された。その後、2020 年 1 月 27 日、法律により消費者向けの IoT デバイスをサイバー攻撃から守ることが義務付けられた。

次に、具体的に消費者向け IoT デバイスの製造メーカーに義務付けられた内容について紹介する。具体的には以下 3 つの義務付けが行われる事になった。

1. 「消費者向け IoT デバイスにおいては、ユニークなものであり、工場出荷時点のパスワードにリセット不可であるとすること」
2. 「消費者向け IoT デバイスの製造者は誰もが脆弱性を報告することができる連絡先をもうけ、タイムリーに対応できるようにすること」
3. 「消費者向け IoT デバイスの製造者は販売店、またはオンラインにおいて、デバイスがセキュリティアップデートを受けられる最少期間を明示しなくてはならない」

6. IoT セキュリティ及びサプライチェーンの動向調査の分析

6.1 事例調査から抽出されるトレンド

5.では北米及び欧州の IoT セキュリティ及びサプライチェーンに関する標準化団体等の動向について関連する事例を抽出した。以下では、そこから読み取れるトレンドについての分析・考察を行う。

IoT サイバーセキュリティ及びサプライチェーンに関するトレンドとしては、大きく分けて以下 2 点の議論が進んでいるといえる。

① IoT デバイスに関する動向
② IoT サプライチェーンに関する動向

以下では、上記 2 つの議論について解説を行う。

6.2 IoT デバイスに関する動向

まず、①IoT デバイスに関する動向としては、標準化団体において IoT デバイスを利用する際のセキュリティリスクを以下に減らすかということが議論されている。そのような議論を行う際の一つの観点として以下の 2 つに分類することが可能である。

観点 1：プリマーケット
観点 2：ポストマーケット

観点 1 の「プリマーケット」だが、今回の調査対象である NIST や ENISA からは、製造メーカーが IoT デバイスを製造するにあたってセキュリティを確保するために自主的に採用すべき基本項目に関する提言やあらかじめ IoT デバイス等の製品設計の際にセキュリティを組み込んでおくという「セキュリティバイ・デザイン」に関する調査報告書が公表されている。

このようなプリマーケットの動きについては、NIST や ENISA 以外にも米国のカルフォルニア州が 2020 年 1 月 1 日から施行した IoT セキュリティ法（Senate Bill No.327）やイギリス政府が 2020 年 1 月 27 日に公表した「Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation」においても同様の動きがみられる。

以上のことより、北米、欧州ともに IoT デバイスの製造メーカーに対して、セキュリティリスクを事前に減少させるような対策を求めるようになってきていることが理解することができる。一見すると日本には影響がないように思われるかもしれないが、IoT デバイスを製造し海外へ輸出する日本の製造メーカーにとって大きな影響を与えることが予想さ

れる。特に米国カルフォルニア州やイギリス政府が発効したばかりの法律であるため、この法律がどのように運用・適用されるかには不明な点が多い（違反した場合、どのような罰則が適用されるか等）。また IoT デバイスの製造業者が具体的にどのような動きを見せるかという点についても注目が必要である。

次に、観点 2 の「ポストマーケット」については、販売されている IoT デバイスがセキュリティインシデントを発生させた際にどのように取り締まるのかという議論である。例えば、今回事例として取り上げた中では、IoT セキュリティそのものではないが、米国カルフォルニア州が IoT セキュリティ法と同時に発効したカルフォルニア州消費者プライバシー法が想定できる。この法律は、4.の事例で紹介したように、カルフォルニア州の消費者のプライバシーを保護するものである。もし、違反が認められた場合には、最終的には罰金が課される場合がある。こちらに関しても、まだ法律が施工されたばかりであり、適用事例がないため、法律がどのように運用、また適用されるかは今後の動向を見守る必要がある。

6.3　IoT サプライチェーンに関する動向

IoT のサプライチェーンに関してはリスクマネジメントに関する文章が NIST、ENISA より公表されている。

北米に関しては、2018 年の「Cybersecurity Framework Version1.1」の決定以降、前述した IoT デバイスを製造する企業に自主的にサイバーセキュリティに考慮すべき事項の発表の他に、サプライチェーン・マネジメントに関するガイダンス文章が発表されている。また 2020 年 2 月には、米国の産業におけるサプライチェーン・マネジメントに関するベストプラクティスの調査報告書が複数公表されており、より具体的な議論が進んでいることがうかがえる。

また、欧州に関しては、2019 年 6 月にサイバーセキュリティ政策（Cybersecurity Act）が施行され、サイバーセキュリティ認証フレームワークのスキームに関しても、NIST から関連する文章が公表されるとともに、ENISA が主催する会合やワークショップに欧州行域内のサイバーセキュリティの専門家、またステークホルダーが集まり、情報共有と具体的なサイバーセキュリティ認証フレームワークの実現に向けた議論が進んでいることがうかがえる。

サイバーセキュリティ認証のフレームワークに関しては、ENISA は標準化が必要であると検討している模様であるが、その一方でサイバーセキュリティ認証の乱立化を懸念しており、他の標準化団体との強調が必要と述べている。

6.4　IoT セキュリティ及びサプライチェーンに関するステークホルダーとの連携

今回の調査対象である NIST、ENISA の IoT セキュリティに関する共通点及びトレンドと

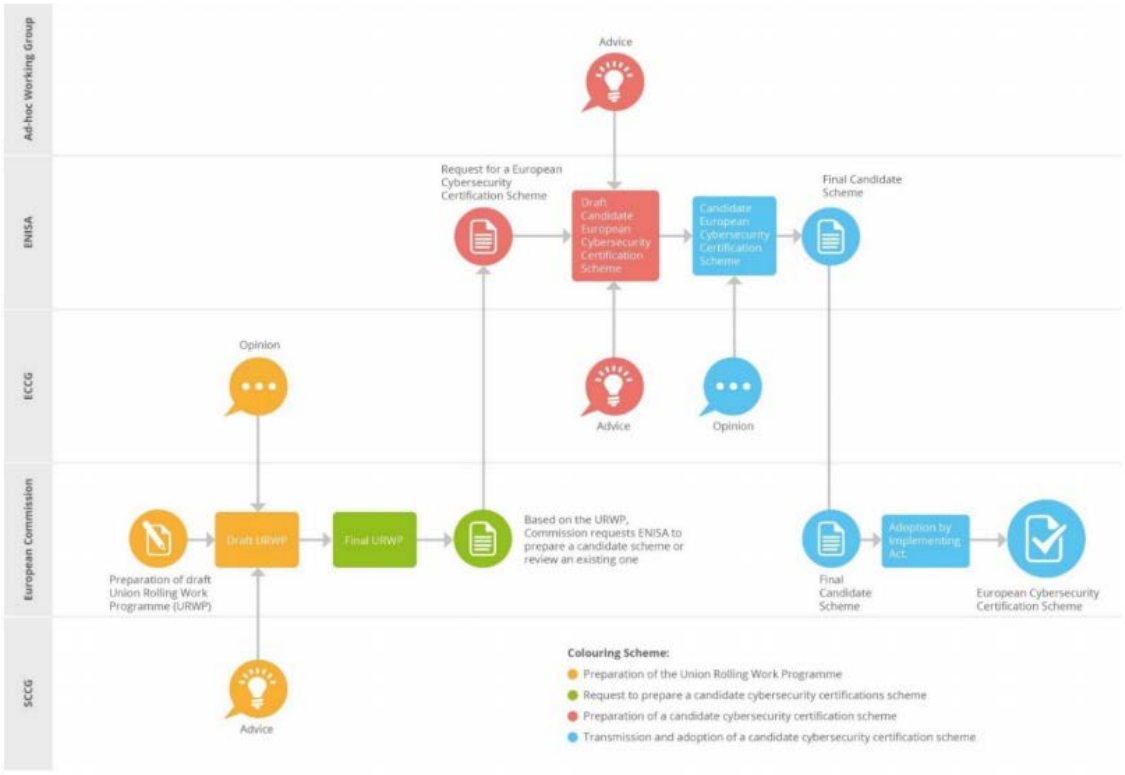
して挙げられるものは、ステークホルダーとの連携の仕方である。

例えば、米国においては、DHS（国土安全保障省）が 2018 年 10 月末にグローバル ICT サプライチェーンのリスクを把握し、管理するための官民パートナーシップである「ICT Supply Chain Risk Management Task Force」が設置された。民間企業からは AT&T、Verizon といったような通信キャリア、Cisco 等のネットワーク機器、その他 Intel、Microsoft といったステークホルダーが議論に参加しており、IoT サプライチェーンのリスクマネジメントに関して、産業界との連携をタスクフォースを通じて実現しようとしていることが理解できる。

一方、欧州においては、2019 年 6 月に Cybersecurity Act が正式に施行されたのち、プレスリリースに掲載されているものだけでも、5 件（2019 年 10 月に 1 件、2019 年 11 月に 2 件、2019 年 12 月に 1 件、2020 年 1 月に 1 件）ENISA や EU 加盟国の担当者、専門家、そのほか関連産業からのステークホルダーが参加する会合が開催されており、米国と同様に産業界との連携を図ろうとしていることがうかがえる。

2019 年 7 月に ENISA によって公表された文章である「Bolstering ENISA in the EU Cybersecurity Certification Framework」においては、サイバーセキュリティ認証フレームワーク作成に向けた動きの中で ENISA が EU 加盟国とステークホルダー等の間をつなぐことがうかがえる（図 6-1）

図 6－1 ENISA のサイバーセキュリティ認証フレームワーク作成に関する考え方



その他、2019年12月にENISAがクラウドサービスに関するサイバーセキュリティ認証スキームの準備を開始することをプレスリリース「Cybersecurity certification: lifting the EU into the cloud」で公表した際に、民間部門と公的部門のステークホルダーからなる「CSPCERT（the Cloud Service Provider Certification）Working Group」の設立を行うことが公表され、関心があるステークホルダー（クラウドサービスのプロバイダ、クラウドサービスのユーザ、消費者団体等を想定）はENISAを通じてこのワーキンググループに参加することが可能であることが合わせて公表された。

以上のように、欧州においてはIoTセキュリティについて民間部門と公的部門のステークホルダーが連携を図る上で、ENISAがその要となっていることが理解できる。

7. SIP 研究開発への反映に向けた今後の調査の方向性

本調査を踏まえて、今後 SIP 研究開発に資する調査、情報収集について検討し、以下の通りに整理を行った。

7.1 調査対象について

今回の調査対象は北米、欧州の IoT セキュリティやサプライチェーンに関して大きな影響力を持つ「NIST」、「First」、「ENISA」、「ETSI」を主な調査対象とした。また調査を続けて行く中で、IoT セキュリティに関する法律を公表、発効した米国のカルフォルニア州、イギリスを追加的に取り上げた。

今後の調査対象として基本となるのは、引き続き今回の調査対象である 4 団体である。今回の調査から明らかになったように、北米、欧州では、IoT セキュリティやサプライチェーンに関する制度の準備が完了し、それぞれのエリア内でのベストプラクティスに関する調査・研究の報告書が積極的に報告される等、進展を見せている。そのため、引き続き北米及び欧州を調査対象とすることが重要である。

また、それに加えて IoT セキュリティを法律化する海外政府の動向も調査対象として加えるべきである。「NIST」や「ENISA」が対象エリアとなる北米や欧州を超えて IoT セキュリティやサプライチェーンの標準化に影響を与えることはいうまでもないが、今回の米国カルフォルニア州やイギリスについても、日本企業が進出している地域であるため、今後の調査対象として加えるべきである。

今回の調査においては、対象外であったが、上記の調査対象にアジアについても対象のエリアとして加えるべきである。アジアはサプライチェーンの一角を担う重要な地域であり、グローバルに活動を行う企業にとっては外すことのできない存在である。その一方で、アジアは IoT セキュリティに先進的なエリアと比較すると、IoT セキュリティに関する制度や個人情報の取り扱いについては、今後の整理が見込まれるエリアである。前述のようにグローバルに展開する企業にとって、アジアは欠かすことのできない存在であるが、IoT セキュリティやサプライチェーンにおいて、グローバルな協調が困難になってしまう可能性がある。

そのため、例えばモノの製造の現場であるアジアにおいて、IoT セキュリティやサプライチェーン・マネジメント、さらには個人情報の取り扱いについてどのような対応が行われているのかについて調査を行うことが重要である。

7.2　調査内容について

7.2.1　IoT セキュリティ及びサプライチェーンの標準化動向

今回と同様に日本企業への影響力が大きいと北米、欧州に関する標準化動向について、引き続き情報収集を行い、そのトレンドについて整理すべきである。前述のように、北米、欧州においては、IoT セキュリティやサプライチェーンの制度についてデバイスあるいは産業単位でのベストプラクティスに関する報告書が公表されており、これらの動向について引き続き情報収集することは重要である。

7.2.2　米国、欧州のステークホルダーとの連携

6. で示したように、NIST、ENISA の双方ともに IoT セキュリティやサプライチェーンに関するステークホルダーとタスクフォースやワーキンググループの形成を通じて産業界との対話や連携を行うことを意図していることが理解できる。

ENISA は今後策定されるサイバーセキュリティ認証のフレームワークについて、EU 加盟国やセキュリティの専門家、その他関連する産業界のステークホルダーを招いて議論を重ねることで、産業界と連携を図ろうとしていることがみてとれる。

7.2.1 にも記載したように、IoT セキュリティやサプライチェーンの制度について、具体的な産業についての調査が NIST や ENISA で行われている中、今後も引き続き、NIST や ENISA 等がどのように産業界と連携を図ろうとしているかという点について、オープンになっている会合に参加して情報収集を行うことが重要である。

また、本調査におけるワーキンググループを実施した際に、参加者より NIST や ENISA が公表している IoT セキュリティやサプライチェーンに関するドラフト文章に関してコメントを行う方法もあるのではないかとの意見があった。これまでの SIP の活動の中で得られた知見を他の標準化に関連する団体にフィードバックすることで、新たな関係性を築くとともに、SIP の考え方等に関して海外へ発信することが可能になる。

7.2.3　アジアのサプライチェーンに関する現地調査

前述のように、グローバルなサプライチェーンの一角を担うアジアの調査は重要である。

その際には国として、IoT セキュリティやサプライチェーンに対してどのように対応しているか、また個人情報保護の水準などについて情報収集を行い、IoT セキュリティやサプライチェーンの制度で先を進む国やエリアとどの程度差があるか（あるいはないのか）

ということを比較する調査が重要である。

また、それに加えて、工場などサプライチェーンが絡む現場において、セキュリティ等に関してどのような取り組みが行われているのか、という点については公表資料では明らかにならない点があるので、実際の現場に赴いて、ヒアリング調査を通じて情報収集を行うことが重要である。

アジアに関する情報収集が完了すると、北米、欧州、アジアといったエリアの中で、日本の IoT セキュリティやサプライチェーンの制度がどのようなポジションにあるのかということも明らかにすることが可能となる。

8. 参考資料

以下では、本調査では触れなかったが、調査対象となる団体/機関の動向について IoT セキュリティに関連する動きを示している内容を参考資料として掲載する。

表 8-1 FIRST に関する動向

時期	報告書名/プレスリリースタイトル等・要旨
2019 年 6 月	Computer Security Incident Response Team (CSIRT) Services Framework Version 2.0 (Review Release)
	2019 年 6 月、FIRST は CSIRT のサービスフレームワークのバージョン 2.0 を公表した。 2019 年 4 月末に、1.1.1 にマイナーバージョンアップされたが、そこから大きく変更されている。 大きな変更点の一つとしては、バージョン 1.1.1 で 7 つに分けられていた「Service Area」がバージョン 2.0 では 5 つにまとめられている点である。
2018 年 7 月	FIRST publishes updated Common Vulnerability Scoring System for worldwide security teams
	2019 年 7 月 12 日、FIRST は共通脆弱性評価システム（Common Vulnerability Scoring System）のアップデートを行ったことを公表した。 バージョンが 3.0 から 3.1 にアップデートされたことにより、シンプルかつセキュリティコミュニティに受け入れられやすい形に変更された。 詳細については、FIRST のウェブサイトで公開されている。

表 8-2 ETSI に関する動向

時期	報告書名/プレスリリースタイトル等・要旨
2019 年 2 月	ETSI releases first globally applicable standard for consumer IoT security
	2019 年 2 月 19 日、ETSI は ioT におけるサイバーセキュリティの標準に関する文章を公表した。消費者向け IoT デバイスのセキュリティのベースラインの確立や IoT デバイスに関する将来的な認証の基礎を提供することを目的としている。 この文章においては、多くのセキュリティに関する問題の源になっているデフォルト・パスワードを使用しないこと、また脆弱性に関する公表のポリシーが求められている。
2019 年 8 月	How to secure consumer IoT devices: and why it matters
	2019 年 8 月、ETSI は自身の Blog サイトにて、コンシューマ向け IoT デバイスのセキュリティを守る方法やなぜそれが重要であるかについて、解説を行っている。 記事では、IoT デバイスのセキュリティ問題について多くの人が理解しているが、どうやって解決していいかが不明なままであることが課題として指摘しており、そのために ETSI がコンシューマ向け IoT の標準化に世界初で取り組んでいることを紹介している。
2019 年 11 月	CYBER;Cyber Security for Consumer Internet of Things （Draft ETSI EN 303 645 V2.0.0 ）
	2019 年 11 月、ETSI はコンシューマー向け IoT デバイスのサイバーセキュリティに関するドラフト文章を公表した。 4 章では、IoT デバイスのセキュリティに対するベースラインが記載されており、「デフォルトパスワードを設定しない」、「ソフトウエアのアップデートを常に行えるようにする」、「利用者がパーソナルデータを容易に削除できるようにする」といったことが記されている。
2019 年 12 月	CYBER;Increasing smart meter security （ETSI TR 103 644 V1.1.1）
	2019 年 12 月、ETSI は重要インフラの一つである、電気、ガス、水道で利用されるスマートメーターに関するセキュリティ監視機能について文章を公表した。 第 4 章において、セキュリティ監視機能のフレームワークについて詳細が記載されている。

表 8-3 Charter of Trust（SIEMENS）に関する動向

時期	報告書名/プレスリリースタイトル等・要旨
2019 年 2 月	February 15, 2019 - The first steps have been taken, and things are now moving quickly.
	2019 年 2 月 15 日、Charter of Trust 設立 1 周年を迎える。 Munich Security Conference2019 において、参加 16 社で設立からの振り返りと 2019 年の展望を議論。
2019 年 4 月	April 1, 2019 - Raising awareness at Hannover Messe 2019
	2019 年 4 月 1 日、Hannover Messe 2019 に出展した SIEMENS ブースにおいて、SIEMENS の Chief Cybersecurity Officer である Natalia Oropeza 氏とパートナー企業の代表が、振り返りと今後の展望について議論を行った。
2019 年 4 月	April 2, 2019 - Charter of Trust talks to Europe
	2019 年 4 月 2 日、ブリュッセルにおいて、Charter of Trust のパートナー企業と EU の Cybersecurity Act の責任者である Despina Spanou 氏が将来のアクションに関する議論を行った。4 章では、IoT デバイスのセキュリティに対するベースラインが記載されており、「デフォルトパスワードを設定しない」、「ソフトウエアのアップデートを常に行えるようにする」、「利用者がパーソナルデータを容易に削除できるようにする」といったことが記されている。
2019 年 4 月	April 23, 2019 - Seeking support in Asia
	2019 年 4 月 23 日は、Charter of Trust として初のロードショーをアジアで行い、パートナーを日本のメディアに紹介した。
2019 年 5 月	May 6, 2019 - Promoting the charter in the German capital.
	2019 年 5 月 6 日、ドイツ・テレコムのオフィスにおいて、Charter of Trust のプロモーションを実施した。
2019 年 5 月	May 17, 2019 - On the way to G7
	2019 年 5 月、パリで開催された AtoS Tech Days の期間中に OECD との協力に関して議論を行った。
2019 年 6 月	June 12, 2019 - To Silicon Valley
	2019 年 6 月 12 日、NXP が開催した会合にて Charter of Trust の議論を実施
2019 年 9 月	September 19, 2019 - The Charter of Trust train stops in Graz and creates trust
	2019 年 9 月 19 日、Austrarian university city で EC の代表者等とともに今後 6 ヶ月間の課題について議論を行った。

また、ISO でもサイバーセキュリティに関する国際標準化が進められている。特にサイバーセキュリティに関連するものとしては、ISO/IEC 27000 ファミリーが重要であると考えられる。ISO/IEC 27000 ファミリーは情報セキュリティマネジメントシステム（ISMS：Information Security Management System）における国際規格であり、ISO や IEC（国際電気標準会議）の設置する合同専門委員会の分科会委員会 SC27 において標準化作業が進められているものである。

以下では、本調査に関連する国際標準について、表にまとめる。

表 8-4　ISO/IEC 27000 ファミリー

国際標準	内容
ISO/IEC TS 27100	サイバーセキュリティの概要、概念、用語定義
ISO/IEC TS 27101	サイバーセキュリティフレームワーク策定のための指針
ISO/IEC 27102	サイバー保険の指針
ISO/IEC TR 27103:2018	サイバーセキュリティフレームワークと ISO/IEC 文書等の対応
ISO/IEC 27030	IoT におけるセキュリティ及びプライバシーの指針
ISO/IEC 27032	サイバーセキュリティにおけるインターネットセキュリティ
ISO/IEC 27019:2017	エネルギー産業における制御システムセキュリティの指針

表 8-5 本調査に関連する報告書及びプレスリリース等の URL

団体名など	タイトル	URL
NIST	Framework Version 1.0	https://www.nist.gov/cyberframework/framework-version-10
NIST	SP 800-171 Rev. 2 (Draft) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/draft
NIST	Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks	https://www.nist.gov/publications/considerations-managing-internet-things-iot-cybersecurity-and-privacy-risks
NIST	White Paper (Draft) Internet of Things (IoT) Trust Concerns	https://csrc.nist.gov/publications/detail/white-paper/2018/10/17/iot-trust-concerns/draft
NIST	Status of International Cybersecurity Standardization for the Internet of Things (IoT): NISTIR 8200	https://csrc.nist.gov/News/2018/NIST-Publishes-Interagency-Report-(NISTIR)-8200
NIST	NISTIR 8259 (Draft) Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline (2nd Draft)	https://csrc.nist.gov/publications/detail/nistir/8259/archive/2020-01-07
NIST	NISTIR 8267 (Draft)	https://csrc.nist.gov/publications

	Security Review of Consumer Home Internet of Things (IoT) Products	/detail/nistir/8267/draft
NIST	NISTIR 8276 (Draft) Key Practices in Cyber Supply Chain Risk Management: Observations from Industry	https://csrc.nist.gov/publications/detail/nistir/8276/draft
NIST	Case Studies in Cyber Supply Chain Risk Management: Anonymous Consumer Goods Company	https://www.nist.gov/publications/case-studies-cyber-supply-chain-risk-management-anonymous-consumer-goods-company
NIST	White Paper Case Studies in Cyber Supply Chain Risk Management: Mayo Clinic	https://csrc.nist.gov/publications/detail/white-paper/2020/02/04/case-studies-in-cyber-scrm-mayo-clinic/final
NIST	Case Studies in Cyber Supply Chain Risk Management: Seagate Technology	https://www.nist.gov/publications/case-studies-cyber-supply-chain-risk-management-seagate-technology
NIST	Case Studies in Cyber Supply Chain Risk Management: Palo Alto Networks, Inc.	https://www.nist.gov/publications/case-studies-cyber-supply-chain-risk-management-palo-alto-networks-inc
NIST	Case Studies in Cyber Supply Chain Risk Management: Anonymous Renewable Energy Company	https://www.nist.gov/publications/case-studies-cyber-supply-chain-risk-management-anonymous-renewable-energy-company
NIST	Case Studies in Cyber Supply Chain Risk Management: Anonymous Consumer Electronics	https://www.nist.gov/publications/case-studies-cyber-supply-chain-risk-management-anonymous-consumer-electronics-company

	Company	
California Legislative Information	Senate Bill No. 327 CHAPTER 886	https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327
State of California Department of Justice	California Consumer Privacy Act (CCPA)	https://oag.ca.gov/privacy/ccpa
EU	The EU Cybersecurity Act	https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act
ENISA	Standards and Certification	https://www.enisa.europa.eu/topics/standards/certificatio
ENISA	Baseline Security Recommendations for IoT	https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
ENISA	NEWS ITEM Towards secure convergence of Cloud and IoT	https://www.enisa.europa.eu/news/enisa-news/towards-secure-convergence-of-cloud-and-iot
ENISA	Good Practices for Security of Internet of Things in the context of Smart Manufacturing	https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot
ENISA	Baseline Security Recommendations for IoT	https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
ENISA	NEWS ITEM ENISA puts out EU ICT Industrial Policy paper for consultation	https://www.enisa.europa.eu/news/enisa-news/enisa-puts-out-eu-ict-industrial-policy-paper-for-consultation
ENISA	Bolstering ENISA in the EU Cybersecurity Certification Framework	https://www.enisa.europa.eu/publications/bolstering-enisa-in-the-eu-cybersecurity-certification-framework

ENISA	Good Practices for Security of IoT - Secure Software Development Lifecycle	https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1
ENISA	ENISA good practices for security of Smart Cars	https://www.enisa.europa.eu/publications/smart-cars
ENISA	Port Cybersecurity - Good practices for cybersecurity in the maritime sector	https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector
ENISA	NEWS ITEM Cybersecurity certification: lifting the EU into the cloud	https://www.enisa.europa.eu/news/enisa-news/cybersecurity-certification-lifting-the-eu-into-the-cloud
ENISA	NEWS ITEM Call for expression of interest for an ad hoc Working Group	https://www.enisa.europa.eu/news/enisa-news/call-for-expression-of-interest-for-an-ad-hoc-working-group
ENISA	Standardisation in support of the Cybersecurity Certification	https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa-i
ENISA	NEWS ITEM 1st Inter-EU ISACs meeting at ENISA	https://www.enisa.europa.eu/news/enisa-news/enisa-hosts-the-first-inter-eu-isac-meeting
ENISA	NEWS ITEM Advisory Group discusses Work Programme 2021	https://www.enisa.europa.eu/news/enisa-news/advisory-group-discusses-work-programme-2021
ENISA	NEWS ITEM ENISA cybersecurity certification preparation underway	https://www.enisa.europa.eu/news/enisa-news/enisa-cybersecurity-certification-preparation-underway
ENISA	NEWS ITEM Supporting the	https://www.enisa.europa.eu/news/enisa-news/supporting-the-

	deployment of the EU Cybersecurity Certification Framework	deployment-of-the-eu-cybersecurity-certification
Department for Digital, Culture, Media & Sport (イギリス)	Consultation outcome Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation	https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation
FIRTS	Computer Security Incident Response Team (CSIRT) Services Framework	https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1
FIRST	FIRST publishes updated Common Vulnerability Scoring System for worldwide security teams	https://www.first.org/newsroom/releases/20190712
ETSI	ETSI RELEASES FIRST GLOBALLY APPLICABLE STANDARD FOR CONSUMER IOT SECURITY	https://www.etsi.org/newsroom/press-releases/1549-2019-02-etsi-releases-first-globally-applicable-standard-for-consumer-iot-security?jjj=1582869014039
ETSI	How to secure consumer IoT devices: and why it matters	https://www.etsi.org/newsroom/blogs/entry/etsi-consumer-iot-security

契約管理番号：１９１０１１３２―0