【産業競争力懇談会　2017年度　プロジェクト　最終報告】

【Society5.0 を支えるセキュアトラスト基盤】

２０１８年２月２１日

産業競争力懇談会 COCN

【エグゼクティブサマリ】

1. 本プロジェクトの基本的な考え方

ネットワークの普及や高速化、IoT の進展、デジタル化などを背景に、産業におけるサイバー空間の重要度がますます高まっており、それにともなってサイバー空間におけるセキュリティ脅威が拡大しつづけている。

欧米では、サイバー脅威の高まりに備え、ICT 活用が急速に進む国防産業や重要インフラ産業を対象とし、セキュリティ要件の具体化・制度化が進んでいる。これにより、欧米のサイバーセキュリティ施策がより強制力を持ち、今後、日本企業に影響する可能性がある。また、日本は Society 5.0 として、現実世界とサイバー空間が高度に融合し、様々なシステムやサービスが連携・結合し、新たな価値を創造する社会の実現を目指している。このような社会では、従来の単独企業体による対策ではカバーしきれないほどサイバー脅威が増加・拡大することが予想される。

上記背景から、欧米のサイバーセキュリティ施策への対応は今後日本企業がグローバルビジネスを行う上でのコスト、施策自体が非関税障壁となる可能性があり、欧米施策の明確化、具体的な対応策が必要となる。また、Society 5.0 時代については、一企業に対するサイバー攻撃の被害が複数の企業に伝播すると想定されるため、企業活動の連鎖として業界内外及び国内外で広がるサプライチェーン全体を守ることが重要となり、各企業のリテラシーの向上が課題となる。本プロジェクトでは、これらの課題を解決し、グローバル市場における日本企業のさらなる競争力強化に有効な仕掛けについて提言することを目的とした。

2. 検討の視点と範囲

１章で挙げた課題の解決に向けて、本プロジェクトでは欧米のサイバーセキュリティ施策に対する日本企業の状況を把握した上で、業界内外及び国内外で広がるサプライチェーン全体のサイバーセキュリティを確保する仕掛けを検討した。

① 欧米のサイバーセキュリティ施策に対する日本企業の状況

欧米日のサイバーセキュリティ施策(米国：NIST SP800-171、欧州：NIS 指令、日本：ISMS など)を分析し、欧米施策に関して一部業界の企業・組織(8 団体程度)で事業推進に携わっている現場担当者等を対象にヒアリング調査を実施した。調査結果から、欧米のサイバーセキュリティ施策に対する企業・組織の認識は、以下の三点に集約され、欧米施策周知の必要性、欧米施策への対応コストを抑える仕掛けづくりの必要性を理解した。

(1) 顧客要望など必要に迫られれば対応するが、現状は必要性を感じない
(2) 欧米施策への対応はコスト面などでの負担が大きい
(3) 欧米施策の拡張はビジネスチャンスになり得る

② サプライチェーン全体のサイバーセキュリティを確保する社会的仕掛けの検討

業界内外及び国内外に広がるサプライチェーン全体のサイバーセキュリティを確保する具体的な社会的仕掛けについて検討した。

現状のサプライチェーンにおけるサイバーセキュリティへの対応として、事業者双方による ISMS(ISO/IEC 27001) 等の取得状況の確認や契約書における遵守条項の規定、定期的な監査などが行われている。これらを踏まえ、事業者間で異なっていたサイバーセキュリティ対策の充足度に対して、事業者が適切なレベルのサイバーセキュリティを確保していることの可視化を中心に据えた。また、サイバーセキュリティを確保すべき観点として、サプライチェーンを形成する事業者の組織、プロセス、ヒト・モノ等に対する要求事項を設定し、サプライチェーン全体のより強固なサイバーセキュリティを確保する方向性を導出した。

上記に基づき検討した社会的仕掛け案(セキュアトラスト基盤フレームワーク) を図 i に示す。本案では、サプライチェーンを形成する事業者の組織、プロセス、ヒト・モノ等の観点でサイバーセキュリティの確保状況を客観的に認証・監査を行う機関を設置することとした。また、サプライチェーンの各事業者で認証・監査機関による適合性判定結果を容易、かつ、効率的に確認できるよう、適合性判定結果を流通する仕掛けを設けることとした。

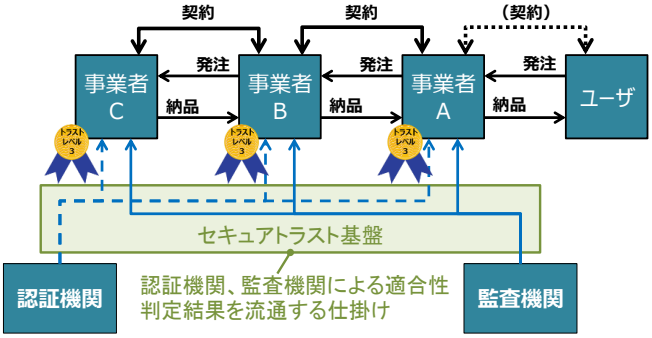


図 i ：セキュアトラスト基盤フレームワーク

3. 産業競争力強化のための提言施策及び官民の役割分担

本プロジェクトの検討により導出した日本企業の産業競争力強化に向けた提言、及び官民の役割分担を以下に示す。

提言	官への期待	民の役割
【提言 1】 グローバルに対応したサイバーセキュリティに関するリテラシー向上	● 欧米等でのサイバーセキュリティ施策動向の把握・産業界へ情報発信を行う仕掛けづくり ● 産業サイバーセキュリティ研究会（経済産業省、2017 年 12 月設置）等内におけるサプライチェーン全体のサイバーセキュリティに関する検討結果の周知	● 欧米等でのサイバーセキュリティ施策動向に基づく業界内・企業内でのリテラシー向上策の実践（例：本プロジェクトの活動結果に関する COCN からの情報発信等）
【提言 2】 セキュアトラスト基盤フレームワーク実現に向けた検討推進	● セキュアトラスト基盤フレームワークに関する制度設計 ● 中小企業へのセキュアトラスト基盤フレームワーク適用への施策推進 ● 欧米等でのサイバーセキュリティに関する施策の相互認証実現への施策推進 ● アジア圏等の欧米以外のグローバルな事業者へのセキュアトラスト基盤フレームワーク適用への施策推進	● セキュアトラスト基盤フレームワークに必要となる技術の研究開発の推進 ● セキュアトラスト基盤フレームワークの検証・運用 ● 既存のサプライチェーンで用いられているシステムとの連携に向けた推進

【目次】

【はじめに】

ICT の進展によりサイバー空間の利用が経済・社会活動の基盤として定着するに伴い、パソコンのみならず、家電、自動車、ロボット、スマートメーター等のあらゆる「モノ」がインターネット等のネットワークに接続され、現実世界（フィジカル空間）とサイバー空間との融合が高度に深化した社会を迎えつつある。このため、サイバー空間の安全の確保はこれまで以上に重要となっているが、サイバー空間を脅かす悪意ある攻撃がとどまることはなく、ウェブサイト改ざんのような個人の愉快犯から、詐欺、機密情報の窃取、重要インフラを狙ったサイバー攻撃、国家の関与が疑われるようなサイバー攻撃に発展し、国民生活及び経済・社会活動に影響を及ぼしており、我が国の安全保障に対する脅威も年々高まってきている。また、セキュリティに対する意識や知識が国民全体に十分に浸透しているとは言い難く、かつ国民の ICT に対するリテラシーの度合いにかかわらず、様々な場面において危険性が顕在化している状況にある。

ICT を最大限に活用し、複数の異なるシステムを連携協調させ、現実世界とサイバー空間とを融合させた取組みにより、人々に豊かさをもたらす超スマート社会(Society 5.0)では、サイバー空間に対する脅威、サイバー攻撃の影響範囲はさらに拡大し、サイバー空間における安全の確保がさらに重要になる。

Society 5.0 時代におけるサイバー空間の安全を確保するためには、これまでの企業体等単体でのサイバーセキュリティ対策のみでは不十分であり、業界内外及び国内外で広がるサプライチェーン全体を守っていくことが極めて重要である。

本プロジェクトでは、サプライチェーン全体をサイバー攻撃から守り、Society 5.0 時代の安全を確保することを目的としており、これらを実現するため、「セキュアトラスト基盤」の構築を推進する。また、セキュアトラスト基盤の構築を進めていく中で、サプライチェーン上の事業者のリテラシーを向上することも目的としている。

本プロジェクトの活動を通じたセキュアトラスト基盤の構築により、Society 5.0 によって広がるサイバー脅威を抑制し、我が国における産業発展を下支えできると考える。

産業競争力懇談会
理事長
小林　喜光

【プロジェクトメンバー】

No.		会社名	氏名
1	リーダー	株式会社日立製作所	石原 修
2	サブリーダー	株式会社日立製作所	鍛 忠司
3	メンバー	三菱電機株式会社	中澤 宣彦
4	メンバー	三菱電機株式会社	島田 克幸
5	メンバー	三菱電機株式会社	宮崎 一哉
6	メンバー	富士電機株式会社	小倉 英之
7	メンバー	富士電機株式会社	梅崎 一也
8	メンバー	日本電気株式会社	谷 幹也
9	メンバー	日本電気株式会社	岡田 勲
10	メンバー	日本電気株式会社	増田 幸一郎
11	メンバー	株式会社東芝	白井 保隆
12	メンバー	株式会社東芝デジタルソリューションズ	岡田 光司
13	メンバー	株式会社東芝デジタルソリューションズ	斯波 万恵
14	メンバー	株式会社東芝デジタルソリューションズ	野崎 華恵
15	メンバー	早稲田大学	戸川 望
16	メンバー	早稲田大学	橋本 和夫
17	メンバー	トヨタ自動車株式会社	小渕 真巳
18	メンバー	損害保険ジャパン日本興亜株式会社	浜野 裕介
19	メンバー	損害保険ジャパン日本興亜株式会社	佐藤 裕一
20	メンバー	SOMPO リスケアマネジメント株式会社	永塚 純一
21	メンバー	SOMPO ホールディングス株式会社	高橋 浩人
22	メンバー	慶應義塾大学	手塚 悟
23	メンバー	株式会社日立製作所	斎藤 浩
24	メンバー	株式会社日立製作所	九野 伸
25	メンバー	株式会社日立製作所	瀬野尾 修二
26	メンバー	株式会社日立製作所	甲斐 隆嗣
27	メンバー	株式会社日立製作所	池田 尚司
28	メンバー	株式会社日立製作所	大倉 隆史
29	メンバー	株式会社日立製作所	古内 克周
30	メンバー	株式会社日立製作所	甲斐 賢
31	メンバー	株式会社日立製作所	江丸 裕教
32	メンバー	株式会社日立製作所	重本 倫宏
33	メンバー	株式会社日立製作所	下条 智貴
34	メンバー	株式会社日立総合計画研究所	松本 洋人
35	メンバー	株式会社日立総合計画研究所	福角 浩昭
36	メンバー	株式会社日立総合計画研究所	櫻井 祥樹
37	メンバー	株式会社日立コンサルティング	川西 康則
38	メンバー	株式会社日立コンサルティング	並木 雅

No.		会社名	氏名
39	オブザーバー	一般財団法人日本情報経済社会推進協会	伊藤 滋行
40	オブザーバー	一般財団法人日本情報経済社会推進協会	風間 正行
41	COCN 担当実行委員	日本電気株式会社	江村 克己
42	COCN 事務局長	一般社団法人産業競争力懇談会	中塚 隆雄
43	COCN 副事務局長	株式会社東芝	五日市 敦
44	COCN 担当企画小委員	トヨタ自動車株式会社	佐藤 桂樹
45	COCN 企画小委員	富士通株式会社	寺田 透
46	COCN 企画小委員	三菱電機株式会社	金枝上 敦史
47	COCN 企画小委員	三菱ケミカル株式会社	田中 克二
48	COCN 企画小委員	日本電気株式会社	武田 安司
49	プロジェクト事務局	株式会社日立製作所	勝田 正彦
50	プロジェクト事務局	株式会社日立製作所	廣田 倫子
51	プロジェクト事務局	株式会社日立コンサルティング	若山 哲郎
52	プロジェクト事務局	株式会社日立コンサルティング	木下 翔太郎

【用語定義】

用語	定義
Society 5.0	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） （内閣府ホームページより）
サイバー セキュリティ	電子的方式、磁気的方式その他人の知覚によっては認識することができない方式により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていること。 （「サイバーセキュリティ基本法案」より）
サプライチェーン	IT システムや提供する製品・サービスにおいて、設計・開発・製造・運用・保守・廃棄に至るまでの一連のプロセスにわたり、業務の一部を系列企業やビジネスパートナー等へ外部委託することは一般的となっている。このような外部委託者が関与する供給の連鎖 （独立行政法人 情報処理推進機構「情報セキュリティに関するサプライチェーンリスクマネジメント調査 - 調査報告書 -」より）
セキュアトラスト	サプライチェーン上で取引を行う事業者が適切なサイバーセキュリティを具備していることを確認できること。確認対象としては、組織、プロセス、ヒト・モノ等を想定する。

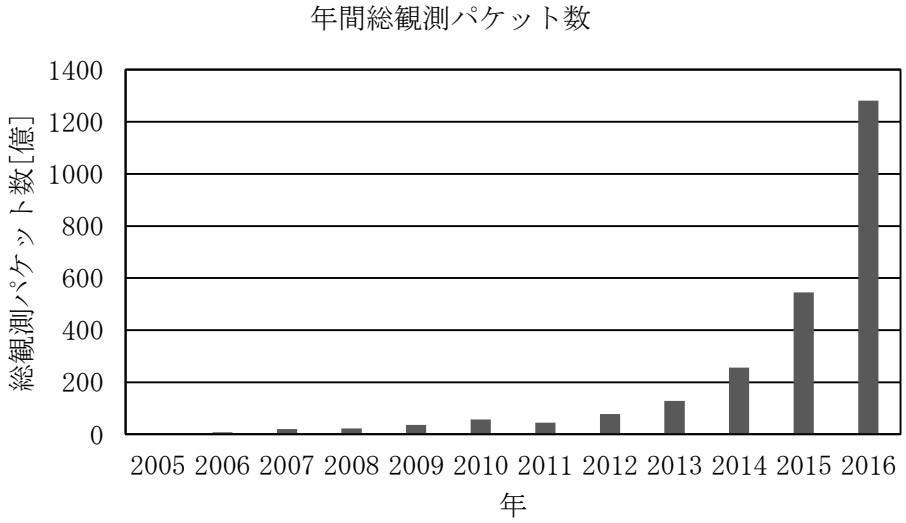
【本文】

1. 本プロジェクトの背景・目的

1.1. 本プロジェクトの背景

1.1.1. Society 5.0 時代を取り巻くサイバーセキュリティに関する動向

近年、我が国では、ネットワークの普及や高速化、IoT の進展、デジタル化などを背景に、サイバー空間が産業においてますます重要度を高めているが、それと並行してサイバー空間における脅威が拡大しつづけている。国立研究開発法人 情報通信研究機構（NICT: National Institute of Information and Communications Technology）によれば、世界中から我が国に向けられたサイバー攻撃関連の通信（ダークネットから受信している通信）は増加の一途をたどっており、2016 年は前年比 2.4 倍の約 1,281 億件と過去最高であり、今後もサイバー空間における脅威は拡大すると考えられる（図 1-1）。



(出所)NICT「NICTER 観測レポート 2016」より作成

図 1-1：ダークネット観測パケット数の年間統計

① 欧米におけるサイバーセキュリティに関する動向

米国や欧州では、サイバー攻撃による脅威の高まりに備え、ICT 活用が急速に進む国防産業や重要インフラ産業を対象として、セキュリティ要件を規格化・具体化し、環境を整備するための制度を整えることで、セキュリティ対策を強化・徹底させる動きが進んでいる。

例えば、米国・国防省（DoD）は、サプライチェーン全体を守る仕掛けとして、調達応札事業者及びその下請事業者に対し、国の定めるセキュリティ要件（NIST SP800-171）への準拠を 2017 年末以降、“義務化”した。このような動きは、これまでガイドラインとして遵守が推奨されてきたセキュリティ規格が、より強制力を持つようになることを意味しており、これらの動きが日本の企業に影響する可能性がある。

欧州においても、GDPR（General Data Protection Regulation、「EU 一般データ保護規則」）

があり、既に日本国内で影響が出ている。

② 日本におけるサイバーセキュリティに関する動向

内閣府は、平成 28 年 1 月 22 日、今後 10 年先を見通した 5 年間の科学技術の振興に関する総合的な計画である「第 5 期科学技術基本計画」を閣議決定した。当該計画の中で肝として示されているのは『世界に先駆けた「超スマート社会」の実現（Society 5.0)』である。「超スマート社会」とは、「必要なもの・サービスを、必要な人に、必要な時に、必要なだけ提供し、社会の様々なニーズにきめ細かに対応でき、あらゆる人が質の高いサービスを受けられ、年齢、性別、地域、言語といった様々な違いを乗り越え、活き活きと快適に暮らすことのできる社会」と定義されている。このような社会では、「生活の質の向上をもたらす人とロボット・AI との共生」、「ユーザーの多様なニーズにきめ細かに応えるカスタマイズされたサービスの提供」、「潜在的ニーズを先取りして人の活動を支援するサービスの提供」、「地域や年齢等によるサービス格差の解消」、「誰もがサービス提供者となれる環境の整備」等の実現が期待される。

超スマート社会を実現する社会基盤（以降、Society 5.0 基盤）においては、デジタル化により、現実世界とサイバー空間が高度に融合し、様々なシステムやサービスが連携・結合し、ビジネスが創出されることで新たな価値を創造する。Society 5.0 基盤では様々なシステムやサービスが結合するため、業種に関わらず、従来の個々の企業体のみの対策ではカバーしきれないほどサイバー脅威が増加・拡大すると予想される。

1.1.2. Society 5.0 時代に向けて取り組むべき課題

1.1.1 の①で述べたような欧米におけるサイバーセキュリティ施策は、今後日本企業がグローバルビジネスを行う上でのコスト負担、あるいは非関税障壁となる可能性がある。欧米におけるサイバーセキュリティ施策の分析を行い、日本のサイバーセキュリティ施策との差分や各業界における影響を正しく認識し、またサイバーセキュリティに関する組織リテラシーを向上した上で、日本企業がグローバルに活躍するための仕掛けづくりが課題となる。

また、従来組織が個別にサイバーセキュリティ対策を施していたが、1.1.1 の②で述べたようにサイバー空間の連携・影響範囲が拡大する Society 5.0 時代においては、一企業に対するサイバー攻撃の被害が複数の企業に伝播するため、企業活動の連鎖として業界内外及び国内外で広がるサプライチェーン全体を守ることが重要な課題の一つとなる。

1.2.　本プロジェクトの目的

1.1.2 で述べた課題を踏まえ、業界内外及び国内外に広がるサプライチェーン全体のサイバーセキュリティを確保するための仕掛けを構築し、企業群(事業主体のみならず、委託先や取引先など)が対策レベルを向上させ、グローバル市場における国際競争力を高めることが非常に重要である。結果として、日本の強みである高い品質に、さらに高い水準のセキュリティを備える製品やサービスを提供できる環境が整うことになる。

本プロジェクトでは、現状を把握した上で業界内外及び国内外で広がるサプライチェーン全体のサイバーセキュリティを確保するための社会的仕掛けについて検討し、その実現に向けた政策提言を行うことを目的とする。

2. 本プロジェクトの実施方針と進め方

2.1. 本プロジェクトの実施方針

本プロジェクトでは、業界内外及び国内外で広がるサプライチェーン全体のサイバーセキュリティを確保するための仕掛けについて、現状を把握した上であるべき姿について検討を進めた。

2.2. 本プロジェクトの進め方

実施方針に従って、以下について調査・検討を進めた。

① 欧米のサイバーセキュリティ施策に対する日本企業の状況（3 章）

- 日本及び欧米でのサイバーセキュリティに関する施策の整理
- 日本産業界における欧米でのサイバーセキュリティに関する施策への認識整理

② サプライチェーン全体のサイバーセキュリティを確保する社会的仕掛けの検討（4 章）

- 社会的仕掛けを検討する上での着目点
- サイバーセキュリティを確保するために確認すべき観点
- 社会的仕掛け案の検討

3. 欧米のサイバーセキュリティに対する日本企業の状況

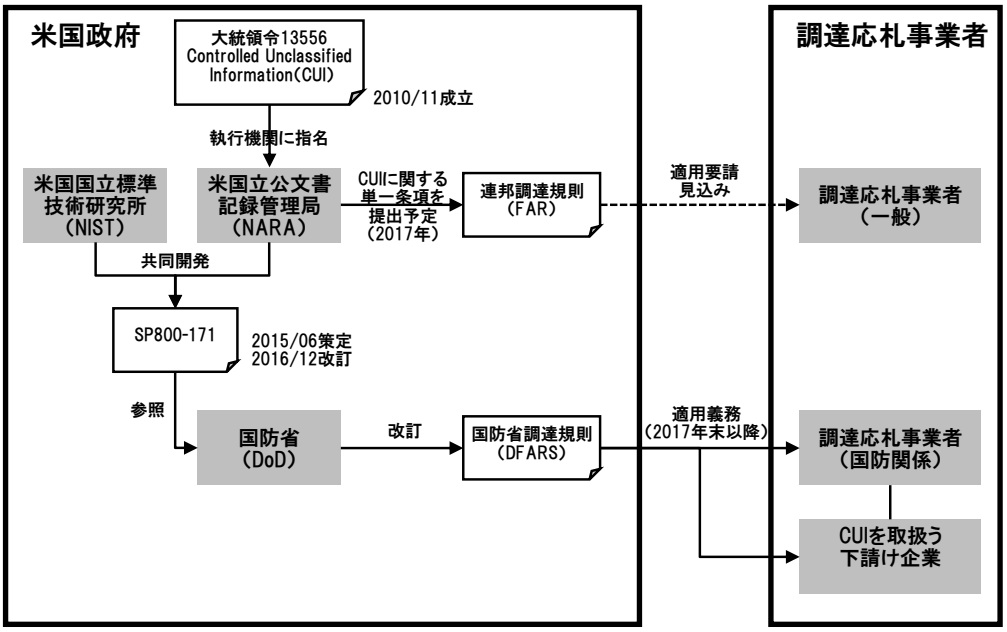
3.1. 日本及び欧米でのサイバーセキュリティに関する施策の整理

3.1.1. 米国

2014年2月12日、米国のホワイトハウスは、重要インフラのサイバーセキュリティ対策の強化を目的としたガイドラインである「Framework for Improving Critical Infrastructure Cybersecurity Version 1.0（以降、CSF)」を公開した。2013年2月12日に大統領令 13636 号が発布され、この行政命令を受けた米国国立標準技術研究所（NIST: National Institute of Standards and Technology）が中心となって、官民の意見を纏めて策定したものがCSFである。CSFは、組織のサイバーセキュリティのリスクに対して、現状とあるべき姿として掲げた目標とのギャップ分析を実施し、必要となる対策の検討、組織としての対策レベルの底上げを図ることを目的としたガイドラインである。重要インフラに係わる企業向けに実施すべきセキュリティ対策を「特定」、「防御」、「検知」、「対応」、「復旧」の5つの機能に分類し、さらにそれらの機能を22のカテゴリーで提示している。上記に加え、2017 年 12 月 5 日に CSF の改訂草案である「Framework for Improving Critical Infrastructure Cybersecurity Version 1.1（以降、CSF Version 1.1） Draft 2」が公開され、その中には新たにサプライチェーンにおけるサイバーセキュリティもスコープに追加されている状況である。

また、米国連邦政府組織がセキュリティ対策を実施する際に参考文書として利用することを前提として、NIST傘下のコンピュータ部門（CSD: Computer Security Division）によりNIST SP800シリーズ(Special Publications 800 Series)が公開されている。当該NIST SP800シリーズは、セキュリティマネジメント、リスクマネジメント、セキュリティ技術、セキュリティの対策状況を評価する指標、セキュリティ教育、インシデント対応等、セキュリティに関する幅広い分野を網羅していることから、政府機関、民間企業を問わず、セキュリティ担当者において活用されている。このような、政府機関、民間企業を問わず活用されている文書群の中で、現在特に注目を集めているのが NIST SP800-171「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」である。その理由は、米国連邦政府組織のCUI（Controlled Unclassified Information の略。秘・極秘等として指定される情報（国防・軍事関連情報）以外の一般情報のうち、「管理された非格付け情報」に相当する情報を指す。）を取扱う調達応札事業者及びサプライヤに対して当該文書で示されるセキュリティ要件に準拠を求める方向にあるからである。NIST SP800-171はNIST SP800-53「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」をベースとして策定されており、NIST SP800-53は米国連邦政府組織に対する要件として規定されているが、NIST SP800-171 は米国連邦政府組織以外への CUI の取り扱いに関する要件も含まれていることから、政府機関向けに適用されていたSP800シリーズが民間向けに適用され始めている。具体的には、国防省（DoD）の調達応札事業者及びそのサプライヤは国防省調達規則（DFARS）により、2017年末からNIST SP800-171への準拠が義務付けられた。また、2017

年に連邦調達規則（FAR）において、NIST SP800-171 のセキュリティ要件を契約者に適用する条項が提出され、一般の調達応札事業者及びそのサプライヤにおいても準拠が求められており、日本の企業も例外ではない。



(出所)各種公開資料より作成

図 3-1：NIST SP800-171 を取り巻く環境

以下に、NIST SP800-53、171 の要点(表 3-1)を示すとともに、CSF、NIST SP800-171、ISO/IEC 27001,27002(ISMS)の比較表(表 3-2)を示す。

表 3-1：NIST SP800-53、171 の要点

NIST SP800-53	名称	Recommended Security Controls for Federal Information Systems（訳：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）
	目的	米国連邦政府組織及び連邦政府の情報システムに対するセキュリティ管理策とプライバシー管理策の提供
	対象	米国連邦政府組織及び連邦政府の情報システム
	概要	米国連邦政府組織及び連邦政府の情報システムに対するセキュリティ管理策のカタログを、連邦政府組織及び連邦政府の情報システムに対するプライバシー管理策のカタログと合わせて提示する文書であるとともに、さまざまな脅威（自然災害・人的ミス・悪質なサイバー攻撃・構造上の欠陥等）から組織のミッション・組織が有する機能・組織のイメージ・組織に対する評判・組織の業務・組織の資産・個人・他組織・国家を保護するために管理策を選択するプロセスを提示する文書
NIST SP800-171	名称	Protecting Controlled Unclassified Information in Nonfederal Systems and Organization（訳：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）
	目的	米国連邦政府外のシステムと組織に存在する管理された非格付け情報（CUI)の保護
	対象	米国連邦政府組織の CUI を取扱う調達応札事業者/サプライヤ
	概要	米国連邦政府外のシステムと組織に存在する管理された CUI(*1)の保護は、米国連邦政府組織にとって最も重要なものであり、米国連邦政府の指定されたミッションとビジネス運用をうまく行うための能力に直接影響を及ぼす可能性があることから、CUI の機密性保護についての推奨されるセキュリティ要件を提供する文書 (*1) CUI について、大統領令 13556 号で以下のような記載がある。 “ such as information that involves privacy, security, proprietary business interests, and law enforcement investigations” 上記から、個人情報や製造仕様書や設計図などもその対象とみなせ、米国政府調達に関わるすべての企業が手にするほとんどの重要情報が対象となると考えられる。

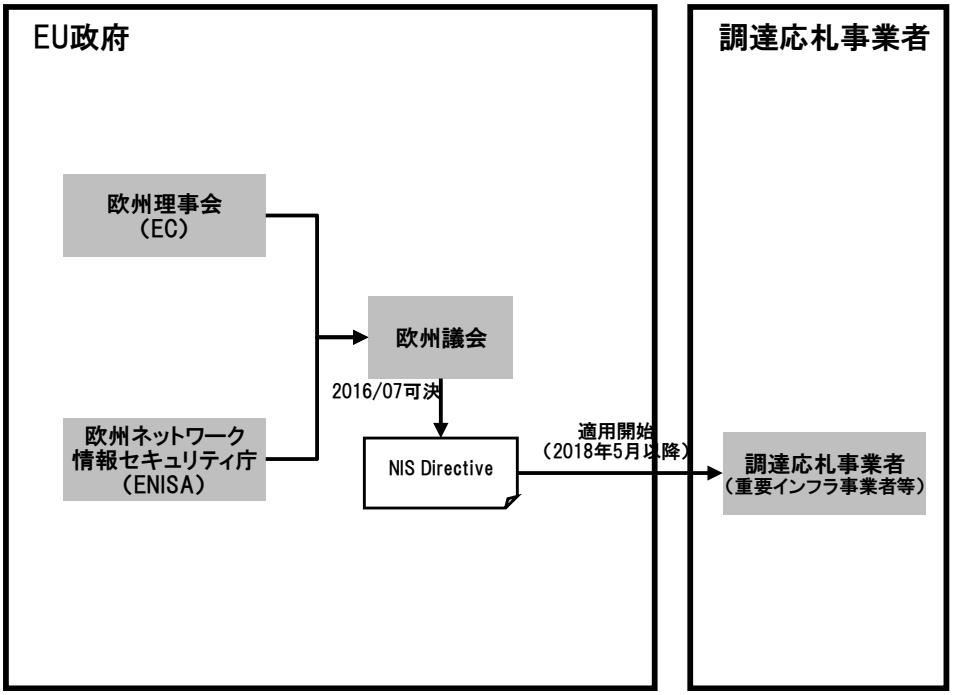
(出所)各種公開資料より作成

表 3-2：CSF、NIST SP800-171、ISO/IEC 27001,27002(ISMS)の比較表

名称	適用対象	目的	特徴
CSF	重要インフラサービスの提供に直接関わるプロセス、情報、システム	左記に対するサイバーセキュリティリスクの管理を可能にする、「優先順位付けができ、柔軟性があり、繰り返し適用することが可能で、成果ベースの、費用対効果の高いアプローチ」を実現すること。	・対策を「特定」、「防御」、「検知」、「対応」、「復旧」に整理している ・ISO/IEC27001 と比較し、特に復旧で独自項目有り
NIST SP800-171	CUI を処理し、保存し、または送信するような米国連邦政府組織外のシステムのコンポーネント	左記に対して、CUI の機密性を保護するための米国連邦政府組織に推奨されるセキュリティ要件を提供すること。	・CUI の保護に目的を限定し、細かな項目を整理している ・DFARS により 2018 年 1 月より調達先に対応を義務化している
ISO/IEC27001, 27002(ISMS)	情報資産(電子データのみならず紙や人の知識などすべてを対象とする)	リスクマネジメントプロセスを適用することによって情報の機密性、完全性及び可用性を保護し、かつ、リスクを適切に管理しているという信頼を利害関係者に与えること。	・適用範囲が広い ・必要な組織的対策、人的対策、物理的対策、技術的対策を網羅的に記載している

3.1.2. 欧州

欧州では、EU 初の包括的なサイバーセキュリティに関する指令である「NIS 指令」(The Directive on security of Network and Information Systems) が 2016 年 7 月 6 日に欧州議会で可決され、同 8 月に法制化された。各加盟国は 2018 年 5 月 9 日までに NIS 指令を国内法に組み込むことが要求されており、当該指令においては、欧州または国際的に取り入れられている標準に関して、重要インフラ事業者等に準拠するように求めている。対象とされた業種範囲は、①エネルギー（電力、石油、ガス)、②交通（空輸、鉄道、海運、陸運)、③銀行、④金融、⑤ヘルスケア、⑥水道、⑦デジタル（インターネットサービス等）とされている。



(出所)各種公開資料より作成

図 3-2：NIS 指令を取り巻く環境

3.1.3. 日本

欧米に対して、日本におけるサイバーセキュリティに関する制度の動向としては、以下に挙げる規格やガイドラインについて重要インフラ事業者等の自主的な実施が推奨されている状況である。

① サイバーセキュリティ経営ガイドライン（経済産業省、独立行政法人 情報処理推進機構）

日本における全ての経営者が実施すべきサイバーセキュリティの原理原則を示し、事業者が当該ガイドラインを参考に主体的に対策を実施している。

② 情報セキュリティマネジメントシステム（ISMS: Information Security Management System）

情報セキュリティを管理するための認証制度として、情報セキュリティマネジメントシステムがあり、認証取得要件として JIS Q 27001：2014(ISO/IEC 27001)を適用している。しかしながら、情報セキュリティマネジメントシステムの取得は任意とされている。2017 年 7 月 5 日現在では、取得組織数は 5,258 件である。

③ 重要インフラ分野別に定めた情報セキュリティ確保に係るガイドライン

内閣サイバーセキュリティセンター(NISC: National center of Incident readiness and Strategy for Cybersecurity)が定めた「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」をベースに、重要インフラ所管省庁にてガイドラインを策定し、重要インフラ事業者が当該ガイドラインを参考に主体的に対策を実施している(表 3-3)。

表 3-3：重要インフラ分野別に定めた情報セキュリティ確保に係るガイドライン一覧

分野		安全基準等名称
情報通信	電気通信	✓情報通信ネットワーク安全・信頼性基準 ✓電気通信分野における情報セキュリティ確保に係る安全基準（第 3 版） ✓電気通信事業法／電気通信事業法施行規則／事業用電気通信設備規則
	放送	✓放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン
	ケーブル	✓ケーブルテレビの情報セキュリティ確保に係る「安全基準等」策定ガイドライン
金融	銀行等 生命保険 損害保険 証券	✓金融機関等におけるセキュリティポリシー策定のための手引書 ✓金融機関等コンピュータシステムの安全対策基準・解説書 ✓金融機関等におけるコンティンジェンシープラン策定のための手引書
航空	航空運送	✓航空運送事業者における情報セキュリティ確保に係る安全ガイドライン（第 4 版）
	航空管制	✓航空管制システムにおける情報セキュリティ確保に係る安全ガイドライン（第 4 版）
鉄道	－	✓鉄道分野における情報セキュリティ確保に係る安全ガイドライン（第 3 版）
電力	－	✓電力制御システム等における技術的水準・運用技術に関するガイドライン ✓電気設備の技術基準の解釈 ✓電気事業法施行規則第 50 条第 2 項の解釈適用に当たっての考え方 ✓スマートメータシステムセキュリティガイドライン ✓電力制御システムセキュリティガイドライン
ガス	－	✓製造・供給に係る制御系システムのセキュリティ対策ガイドライン
政府・行政サービス	－	✓地方公共団体における情報セキュリティポリシーに関するガイドライン
医療	－	✓医療情報システムの安全管理に関するガイドライン（第 4.2 版）
水道	－	✓水道分野における情報セキュリティガイドライン
物流	－	✓物流分野における情報セキュリティ確保に係る安全ガイドライン（第 3 版）
化学	－	✓石油化学分野における情報セキュリティ確保に係る安全基準
クレジット	－	✓クレジット CEPTOAR における情報セキュリティガイドライン
石油	－	✓石油分野における情報セキュリティ確保に係る安全ガイドライン

(出所)NISC「2016 年度重要ｲﾝﾌﾗにおける安全基準等の継続的改善状況等の調査」より作成

3.1.4. 日本及び欧米における施策の比較

3.1.3 に示した通り、日本ではサイバーセキュリティに関する規格やガイドラインはあるものの、重要インフラ事業者等の自主的な実施に任されている状況である。一方で、欧米では､国において重要インフラ事業者等に対して求めるサプライチェーンを視野に入れたセキュリティ要件を制度化し、当該事業者へ準拠を求める動きが活発化しつつある(表 3-4)。

このような状況を受け、日本においても ISMS（ISO/IEC 27001）のように従来の組織が個別にサイバーセキュリティ対策を実施することに加え、企業活動の連鎖であるサプライチェーン全体を守る取組みが重要であると理解できる。

表 3-4：日本及び欧米でのサイバーセキュリティに関する施策の比較

区分	対象	実施事項	規格
米国	重要インフラ事業者	組織のサイバーセキュリティリスクに対する対策(※**サプライチェーン**もスコープに含まれる）の実施	CSF Version 1.1 ※2017/12/5 時点 Draft2
	米国連邦政府組織及び連邦政府の情報システム	情報システムに対する管理策の遵守	NIST SP800-53
	CUI を扱う米国連邦政府組織外の事業者（※DFARS により国防省(DoD)に関しては**サプライチェーン**に含まれる全ての事業者）	CUI を守るための管理策の遵守	NIST SP800-171
欧州	重要インフラ事業者等	国際標準を遵守したセキュリティ要件への準拠やインシデント情報を共有	NIS 指令
日本	情報資産を有する事業者	ISMS（ISO/IEC 27001）の管理策の適用	ISMS（ISO/IEC 27001）等

※ISMS(ISO/IEC 27001)と CSF Verision 1.1 で求められる管理策の比較については、NIST で公開している「Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 Draft 2」内の「Appendix A: Framework Core」をご参照ください。
(URL:https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf)

※ISMS(ISO/IEC 27001)と NIST SP800-171 で求められる管理策の比較については、独立行政法人情報処理推進機構(IPA)で公開されている「SP 800-171 rev.1」の翻訳版「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」内の「附属書 D」をご参照ください。
(URL: https://www.ipa.go.jp/files/000057365.pdf)

3.2.　日本産業界における欧米でのサイバーセキュリティに関する施策への認識整理

欧米のサイバーセキュリティ施策(NIST SP800、NIS 指令)に関して、業界ごとの認知度や施策、対応に関する課題や施策が拡大した際に生じる影響についてヒアリングにより調査を実施した(表 3-5)。

なお、当ヒアリングでは表 3-5 に示す団体で事業推進に携わっている現場担当者等を対象に調査した結果である。

表 3-5：ヒアリング先一覧

No.	調査対象	ヒアリングの観点
1	建設機械メーカ	欧米セキュリティ施策に関する各社の認識や取り組みなど
2	自動車関連メーカ	
3	電機メーカ①	
4	電機メーカ②	
5	電機メーカ③	
6	保険会社	
7	IT 関連業界団体	米国のセキュリティ施策に対する取り組みや見識など
8	自動車関連業界団体	

※No.5,6 はアンケートにより調査を実施

3.2.1. 欧米でのサイバーセキュリティに関する施策に対する取り組みの状況

欧米施策への取り組み状況について各業界のステークホルダーへのヒアリングにより調査を実施した(表 3-6)。現状は欧米企業からの調達業務に関わりのある企業・担当者が認識している状況であった。

海外のセキュリティ施策を認識している企業では、現時点では直接的な影響がなくとも今後の制度拡張などに備え情報収集を行っている。しかしながら、具体的な対策を施しているケースはまだ少ない。

施策を認識していない企業でも、従来から海外における企業活動で必要な制度に対しては個別に対応している。現時点では新たな欧米施策の影響が想定されなければ、対応の必要性を感じていない。

表 3-6：欧米施策認知度に関するヒアリング結果

調査対象	調査結果
建設機器メーカ	✓ 欧米施策について認識はない ✓ 米国については、販売代理店を立てているが、現地からの要求はない
自動車関連メーカ	✓ ISO と比較して欧米にて強固なサイバーセキュリティに関する施策の動向があるということは認識している。防衛や重要インフラからの適用であり自動車関連はこれから適用する/しないを議論するという認識である ✓ 対応の方向性としては、ISO とそれら欧米の施策を比較して何が異なっているのかを整理し、事実把握をすることが第一歩である ✓ 自動車業界では、製品のサイバーセキュリティに関しては、ISO を基準としてその対応を推進している。業界で自動車向けに関しての ISO 化を推進中である
電機メーカ①	✓ 欧米施策について認識はない
電機メーカ②	✓ NIST SP800 について、感度の高い者は認識しているが、現状対策は行っていない
電機メーカ③	✓ 米国政府系の調達関連での情報の授受に関連して NIST SP800-171 への対応の必要性が生じており、認証取得や運用体制について検討中である
保険会社	✓ 再保険業界で影響が考えられ、認識している ✓ 保険引受などにおいても、商材やサービスの提供先の最終的な使途を把握できない場合、高リスク企業となり保険料が高くなる可能性がある

※欧米施策に関する認識について質問をした調査対象のみを記載

一方、本プロジェクトの遂行する上で、欧米等で事業展開をする企業の企画系部門/情報システム部門の担当者に伺うことができた意見では､欧米施策を非常に注視しているとのことであった。

3.2.2. 欧米でのサイバーセキュリティに関する施策の拡張がもたらす影響

欧米施策が拡張された場合の影響について､各業界のステークホルダーおよび関連機関への調査を実施した。事業領域・立場の違いによって意見が分かれる結果となった(表 3-7、表 3-8)。

欧米のセキュリティ施策が将来的に民間の取引に拡張された場合には､影響が懸念されると捉える企業が多い。また、現状国内では業界ごとにガイドラインが制定されているが、それらを統一した見本となるべきガイドライン･基準を国で整備できると望ましいとの希望は多い。

表 3-7：欧米施策への危機感に関する立場別ヒアリング結果

意見	ヒアリング先(立場)	コメント
現状影響なし	完成品メーカ	✓ 欧米施策が事業に与える影響は現状少ない
顧客次第	部品メーカ	✓ 必要に応じて顧客、国ごとに対応している ✓ 要望により対応が必要となるため、準備が必要である
事業機会増加	システムベンダ	✓ 対応によるコスト増加や認証遅れによる機会損失が懸念される ✓ 施策が拡張されれば各社対応が必要となり､新たなビジネス機会となる
	保険会社	✓ 欧米施策対応のリスクに供えるための「サイバー保険」の需要が高まる
負担増加	全般	✓ 施策が拡大された場合はコスト面など影響力が大きい ✓ 特に中小企業にとっては深刻である

表 3-8：欧米施策への危機感に関するヒアリング結果

ヒアリング先	コメント	
建設機器メーカ	要点	✓ **現状は欧米施策対応が必要な取引はなく、影響なし** ✓ **施策が民間企業に拡大されれば大きな影響がある**
	内容	✓ 欧米施策は現時点では影響はないと考える ✓ アメリカが国外企業を排除しようとして、それを狙うようなレギュレーションを確立しようとしても、建設機械業界はサプライヤがグローバルに及んでおり、日本だけが困るような状況は起こらないと考える ✓ NIST SP800 などについて、米国販売代理店とのやり取りは当該企業とのルールが決められれば、そのルールに従うことになると考える。その他に関しては、米国のルールに合わせなくてはいけないと考える。ただし、実現方法については検討が必要である ✓ 欧米施策が民間企業間の取引に拡張された場合には、大きな影響が発生すると考える。現地の企業に影響が発生し、当社にもその影響が及ぶと考える
自動車関連メーカ	要点	✓ **欧米施策については顧客の要望など必要に応じて対応予定である** ✓ **必要な対策の明確化が必要である**
	内容	✓ 米国の NIST SP800-171 ではどのような脅威を想定して、どのような対応が必要なのか明確にすることから始める必要ありと考えている ✓ 顧客や顧客企業からの要望があれば、従う必要ありと考えている。業界の動向は把握しておく必要がある ✓ 欧米のサイバーセキュリティ施策のように、米国、欧州等の各国ルールが異なる中では、効率的に対応していく必要があると考えている ✓ 現時点では国や上位団体による指示や、事業を展開する国で必要となる対応は必要に応じて検討する
電機メーカ①	要点	✓ **欧米施策が民間企業に拡張された場合は、各社セキュリティ強化施策を実施すると考えられるため、ビジネスチャンスとなる**
	内容	✓ 欧米施策について、日本も同様のルールになると事業機会が増加する。サイバーを守るためにフィジカルも守る必要がある。日本でも重要インフラではガイドラインが出ているが、あまり徹底していないという認識である ✓ 欧米のセキュリティ施策が民間企業の取引などに拡張された場合、事業者内部でセキュリティを強化することとなり、良い影響がある
電機メーカ②	要点	✓ **欧米施策は導入されれば対応するという考え方である** ✓ **施策対応はかなりのコストアップに繋がると懸念される**
	内容	✓ 自動車は他に ISO 26262 など厳しい規定が多くある。NIST SP800 についても、導入されたら準拠するという姿勢だろう ✓ 製造業における情報系では、意識がそれほど高くないことが課題と考える ✓ NIST SP800 の対象範囲が産業界に波及した場合はかなりのコストアップになる。顧客はコストアップを認めないため、内部コストになってしまう
電機メーカ③	要点	✓ **適用が重要インフラ他に拡大すれば影響を受ける業界・業種は拡大すると考えられる** ✓ **対応によるコスト増加や認証遅れによる機会損失が懸念される**
	内容	✓ 欧米施策を関連会社まで適用する場合に導入コスト/IT 専門家の配置などのコストがかさむ恐れがある ✓ 認証プロセスが各国/業界毎に異なっていたり明確化されていない場合に、必要以上にコストがかかったり、各国の規制の変更による認証遅れに起因してビジネス喪失のリスクがある ✓ グローバルにて事業を行う場合に、その国のルールに従うのはやむを得ない。各国の施策に対して早期に対応し実績を積むことが必要 ✓ 各国それぞれの規制に対応するのは効率的でなく、コスト的に大変なので、ISO などの標準が活用できるようになればよい
保険会社	要点	✓ **施策が拡大すれば、リスク対策として「サイバー保険」が求められる** ✓ **保険会社としては、サイバーリスクの算定に関する説明責任が求められる**
	内容	✓ 適合企業の事業リスクにあった「サイバー保険」が求められると共に、適

ヒアリング先	コメント	
		合不明の企業が高リスクの評価となり保険料が高額になることも想定される ✓ どれだけ欧米の施策や規定・規格等に対応しても、残存するリスクがあるために、それに対応するリスクファイナンスの手段として、「サイバー保険」の加入を求められる可能性があると想定する ✓ 罰則及び賠償額予測、賠償命令判例なども考慮した影響の検討とその発生確率に基づくリスク算定による説明責任が求められてくる
IT 関連業界団体	要点	**✓ サプライチェーンのセキュリティ対応には数年前まで反発があったが、変わりつつある** **✓ 中小企業はコスト増などのため対応が難しい。これは日米共通である**
	内容	✓ NIST が 2013 年当時サイバーセキュリティフレームワークにサプライチェーンのセキュリティを盛り込もうとした際、企業の反発が大きかったが、数年かけて合意形成でき、フレームワーク改訂版に記載した。ただし、中小企業では対応が難しく、実装は簡単ではない(コストや実装の監査、実証など)
自動車関連業界団体	要点	**✓ 自動車関連各社から欧米のセキュリティ対策について自動車関連メーカから問い合わせを受けている状況**
	内容	✓ 欧米のセキュリティ対応について組織としてどのように考えているか、といった問い合わせを自動車関連メーカから受けることはある

また、本プロジェクトの遂行する上で、欧米等で事業展開をする企業の企画系部門/情報システム部門の担当者に伺うことができた意見では､欧米のセキュリティ施策が将来的に民間の取引に拡張された場合には、影響を非常に懸念しているとのことであった。

3.3. まとめ

欧米のサイバーセキュリティに関する施策として NIST SP800 シリーズ(米国)、NIS 指令が存在しており､日本でもサイバーセキュリティ経営ガイドラインや ISMS(ISO/IEC 27001)、重要インフラ分野別に定めた情報セキュリティ確保に係るガイドラインなどを実施しているが、日本企業が海外事業を推進する上では欧米施策への対応が必要となる。

各業界ステークホルダーへの調査について、主な意見は以下 3 つに集約できると考える。

(1)顧客要望など必要に迫られれば対応するが、現状は必要性を感じない

(2)欧米施策への対応はコスト面などでの負担が大きい

(3)欧米施策の拡張はビジネスチャンスになり得る

現状､欧米施策対策は必要がなければ取り組まれていない状況であった。自動車業界などグローバルな取引のある企業ではリスクとして感度が高い傾向が見られたが､実施している企業も取引先との契約ベースでの取組みが中心であり､取組みの内容にバラツキがある。一方で対応が必要になった際の影響力は大きいという意見は多く､必要となった場合に備えてグローバルに活動していく上で注視しておくべきものとして､欧米施策の周知活動が必要である。さらに、対応に必要なコストを抑えるための仕掛けづくりも、中小企業を含めたサプライチェーン全体への普及に向けては重要な課題である。

欧米への展開に向けて欧米施策への対応は今後重要性を増すと考えられるが、取組みの具体策が不明確という意見もある。欧米施策対応に関する明確なルールを定めてサプライチェーン全体で取り組んでいくことが日本の競争力強化につながり、結果として対策コストの低減にも繋がることとなる。

4. サプライチェーン全体のサイバーセキュリティを確保する社会的仕掛けの検討

4.1. 社会的仕掛けを検討する上での着目点

本プロジェクトで検討する、業界内外及び国内外に広がるサプライチェーン全体のサイバーセキュリティを確保する社会的仕掛け（以降、社会的仕掛け）は、1.2 で述べた通り、日本の事業者が従来の強みであった高い品質に、さらに高い水準のセキュリティを備える製品やサービスの提供を可能とすることで、グローバル市場における国際競争力向上の実現を目指すものである。ここでは、そのような社会的仕掛けを検討するにあたっての着目点に関して検討した結果を示す。

なお、産業界で提供される製品やサービスは全て何らかのサプライチェーンに基づき供給されており、そのサプライチェーンの在り方は業界・業種等で異なることを踏まえ、本プロジェクトでは、まずそれらの業界・業種等における特異点は考慮せず、全ての業界・業種等に共通する単純化したモデルを用いて検討することとした。例えば、サプライチェーンのモデルとしては以下に示すようなモデルを用いることとした。当然のことながら、現在のグローバル社会におけるサプライチェーンは国内外の事業者の連鎖により形成されることから、下図に登場する事業者には日本の事業者のみならず、海外の事業者を含むケースも想定している。

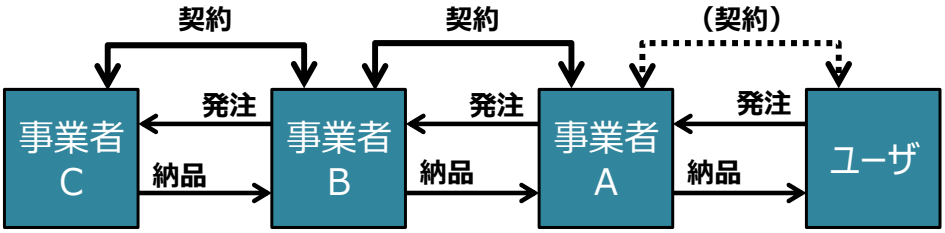


図 4-1：単純化したサプライチェーン・モデル

社会的仕掛けの着目点を整理するにあたり、従来のサプライチェーンの事業者間（例えば、図 4-1 における事業者Ａと事業者Ｂ間の取引）でやり取りされる情報やモノ等の流れを、単純化したモデルにて整理すると図 4-2 の通りとなる。

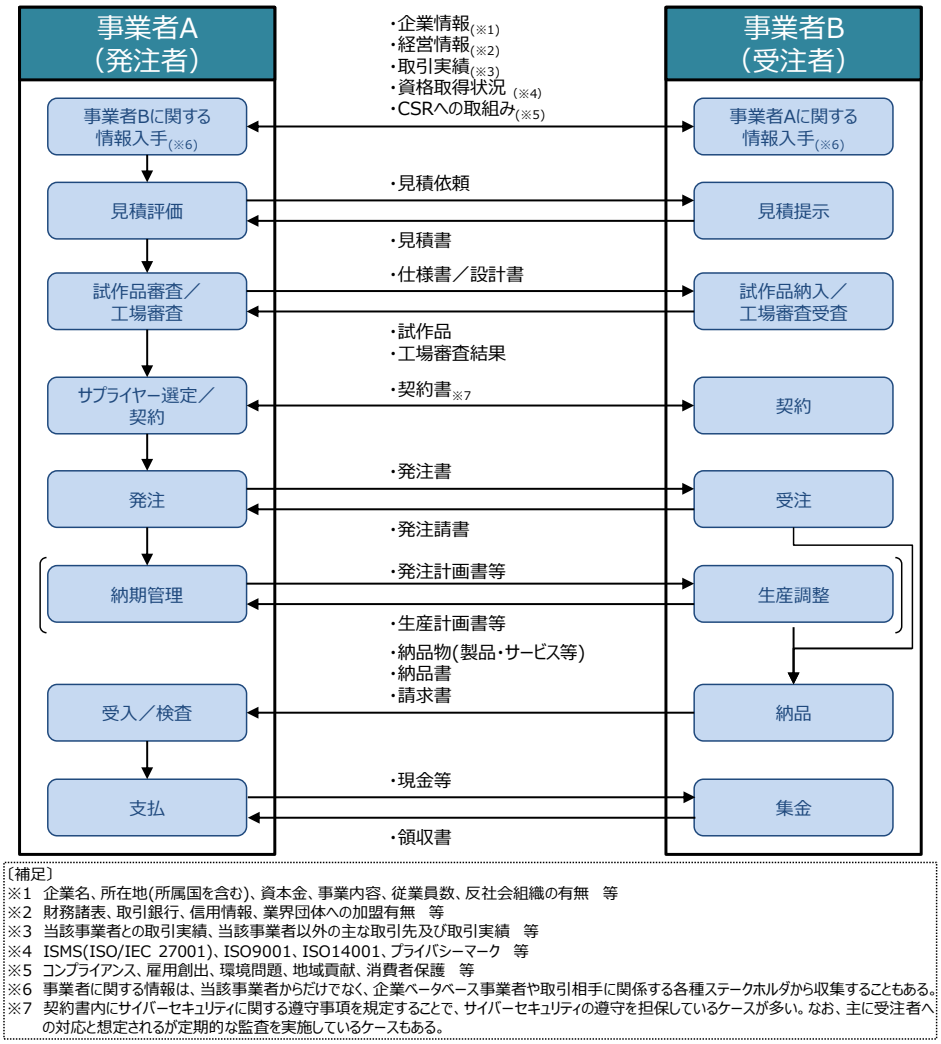


図 4-2：従来のサプライチェーンの事業者間でやり取りされる情報やモノ等の流れ

図 4-2 より、従来のサプライチェーンでは、事業者間におけるサイバーセキュリティへの対応を、事業者双方で ISMS（ISO/IEC 27001）等の取得状況の確認や契約書における遵守条項の規定、主に受注者への対応と想定されるが定期的な監査等で確認が行われていることが分かる。

しかし、現状のような状況では、事業者や取引ごとに契約書における遵守条項の粒度や内容が異なることや、サイバーセキュリティに関する監査の実施有無、当該監査の厳格度等により、サプライチェーン全体においてはサイバーセキュリティ対策の充足度にバラツキが生じていることが想定され、最悪な場合には十分な対策が施されていないケースも含まれることが予想される。

このような状況を踏まえ、本プロジェクトで検討する社会的仕掛けでは、サプライチェーンにおける各事業者でのサイバーセキュリティについて適切なレベルを確保する確認内容及びそれを確認する仕掛けに着目することとした。このような点に着目することにより、今

後サイバー脅威の増加・拡大が想定される状況の中で、これまでそれぞれのサプライチェーンの事業者間でバラバラであったサイバーセキュリティ対策の充足度やバラツキへの対策として、取引を行う事業者が適切なレベルのサイバーセキュリティを具備していることを可視化することができ、セキュアトラストを実現した環境を整備できると考えた。

また、上記に加えて社会的仕掛けを検討する上では、3.3 で欧米でのサイバーセキュリティに関する施策への対応として挙げた、欧米施策に明確なルールを定めて取り組んでいくこと、制度活用にあたって必要となるコストを抑えることも考慮事項とした。

4.2. サイバーセキュリティを確保するために確認すべき観点

4.2.1. 確認すべき観点案

ここでは、サプライチェーンにおける事業者において、適切なレベルのサイバーセキュリティを確保するために確認すべき観点とその内容について検討した結果を示す。

サプライチェーン全体のサイバーセキュリティを確保し、更にはそれらとの相互認証を確立するために確認すべき観点については、サプライチェーンを形成する事業者自体及びその事業者のサプライチェーン内における活動に注目し、以下に示す 3 つの視点に基づき整理した。

〔サイバーセキュリティを確保するために確認すべき観点の整理に用いた視点〕

①事業者自体が信頼できること

②事業者の製品・サービスの提供過程が信頼できること

③②の提供過程で用いる事物（リソース）等が信頼できること

上記の 3 つの視点に基づき、サイバーセキュリティを確保するために確認すべき具体的な観点を整理すると、①についてはサプライチェーンに属する組織の観点、②については当該組織で製品・サービスを提供するために実施されるプロセスの観点、③についてはそれらのプロセスを遂行するために用いるヒトやモノ等の観点であると考えた。

上記したサプライチェーン全体のサイバーセキュリティを確保するために確認すべき観点の定義案を図 4-3 に示す。

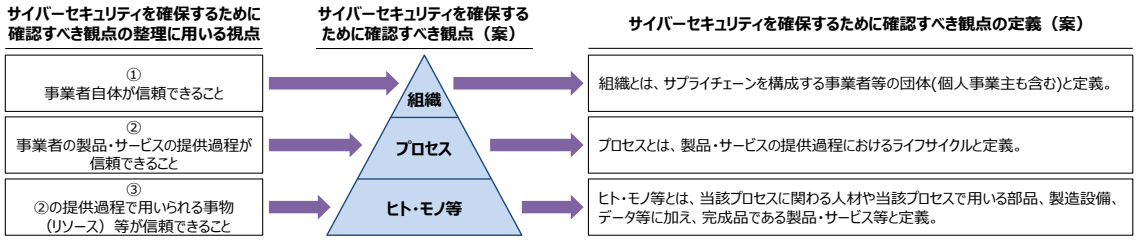


図 4-3：サプライチェーン全体のサイバーセキュリティに関して確認すべき観点（案）

4.2.2. 確認すべき観点案により期待される効果

3.1.1 で述べた通り、米国・国防省による調達においてサプライチェーン全体での準拠が求められている NIST SP800-171 は、米国連邦政府組織へ製品やサービスを提供する、調達応札事業者及びサプライヤの情報システム等で利用、管理、提供等される CUI の機密性を保護することに特化したセキュリティ要件を規定したものである。これと比較して、前述したサイバーセキュリティを確保するために確認すべき観点は、CUI のみならず、サプライチェーンを形成する事業者の組織、プロセス、ヒト・モノ等の観点を含めたサプライチェーン全体を対象とする。このようにすることで、真にサプライチェーン全体のサイバーセキュリティを確保し、欧米と比較して一段も二段も高いセキュリティ水準を実現でき、グローバル市場において日本の事業者の差異化を図ることができると考える。

また、上記のように整理した確認すべき観点において、具体的にどのような要求事項とするかについては、欧米におけるサイバーセキュリティに関する施策や国内外のサイバーセキュリティに関する規格・ガイドライン等との整合(相互認証)を確保することが重要である。このようにすることで、日本の事業者は当該社会的仕掛けに適合することで、国内外の様々な規格やガイドライン等に自動的に適合できることになる。この効率性は、グローバル市場における日本の事業者の更なる優位性の確保に繋がると考える。

4.3. 社会的仕掛け案の検討

4.3.1. 社会的仕掛け案

4.2 で示したサプライチェーン全体のサイバーセキュリティを確保するために確認すべき観点を想定した上で、社会的仕掛け案について検討した結果を示す。

社会的仕掛け案では、「認証機関」及び「監査機関」を設置することを検討した。「認証機関」は、事業者において、4.2 で述べたサプライチェーン全体のサイバーセキュリティで確保すべき組織、プロセス、ヒト・モノ等の観点における要求事項への適合性を評価し、認証を行う役割を担うことを想定する。また、「監査機関」は、上記の認証を受けた事業者が認証を受けた要求事項に対する適合性を維持しているか、定期的に監査を行う役割を担うことを想定する。

また、サプライチェーンを形成する上で、各事業者におけるサイバーセキュリティの確保状況、言い換えれば、上記の認証機関及び監査機関による組織、プロセス、ヒト・モノ等の観点から判定された適合性判定結果を流通できるようにすることを検討した。このようにすることで、サプライチェーン全体における高水準のサイバーセキュリティを実現できるとともに、事業者間においてはセキュアトラストを容易、かつ、効率的に確認することが可能になると考える。

以上に述べたような、サプライチェーン全体のサイバーセキュリティを確保する社会的仕掛けを、本プロジェクトでは「セキュアトラスト基盤フレームワーク」と定義した。

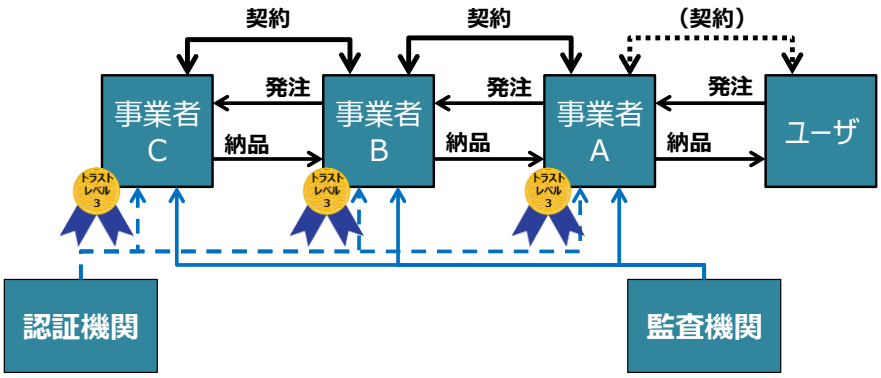


図 4-4：社会的仕掛け案（セキュアトラスト基盤フレームワーク）

① 認証機関/監査機関

セキュアトラスト基盤フレームワークにて、第三者の「認証機関」「監査機関」を設置する形態とした理由は、適合性の評価に関する客観性を確保することを目指したものであるのに加え、業界・業種等によりサイバーセキュリティを確保するための要求事項やその対策のレベルが異なると考えられることから、専門的に認証や監査を実施する機関を設けることが有効と考えたためである。

一方で、認証の取得を目指す事業者は、国内外かつ大企業から中小企業までと非常に広範囲に及ぶことから、当該サプライチェーンで取引関係にある事業者間で認証を行う（例えば、発注者が取引する受注者の認証を行う）案も考えられたが、当該案ではサプライチェーンにおける発注者が受注者ごとに認証や監査を担うことになり、発注者側、受注者側ともに膨大な負荷が生じてしまうデメリットが想定された。このことから、前述した「認証機関」「監査機関」を設置する形態の方が優れていると考えた。

このように、本プロジェクトでは第三者の「認証機関」「監査機関」を設置する形態を検討結果としたが、認証機関/監査機関の設置有無、業界・業種等によりサイバーセキュリティを確保するための要求事項及びその対策のレベルの定義等の制度面や運用面について、より詳細な検討が重要となる。

② セキュアトラスト基盤

上記したセキュアトラスト基盤フレームワークを運用する上では、事業者におけるサイバーセキュリティの確保状況（認証機関及び監査機関による適合性判定結果）を流通できる仕掛けが必要になると考える。その仕掛けを本プロジェクトでは「セキュアトラスト基盤」と定義した。

セキュアトラスト基盤フレームワークにおけるセキュアトラスト基盤の位置付けイメージを図 4-5 に示す。

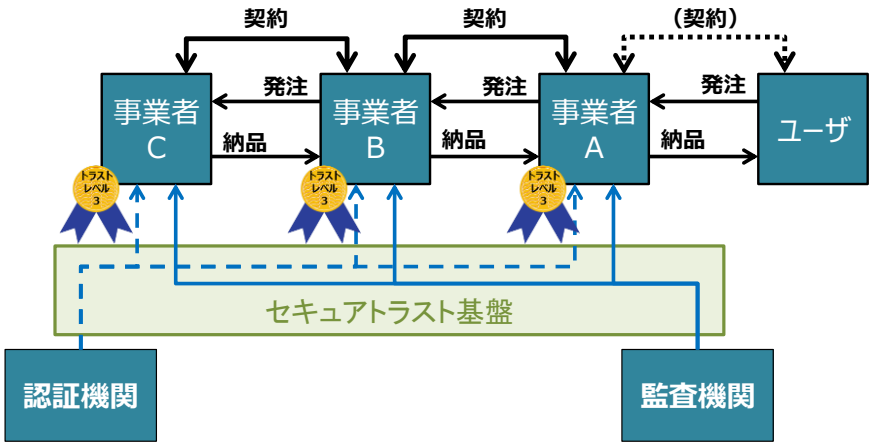


図 4-5：セキュアトラスト基盤の位置付けイメージ

4.3.2. 社会的仕掛け案の実現に向けた課題

4.3.1 では社会的仕掛け案であるセキュアトラスト基盤フレームワークに関して述べた。しかし、当該フレームワークを実現していく上ではまだ多くの課題について検討が必要な状況である。ここでは、本プロジェクト内で挙げられた主だった課題の概要を示す。これらの課題について、引き続き解決の方向性、解決策の検討への取組みが重要となると考える。

① サプライチェーン全体のサイバーセキュリティを確保するための観点に関する課題

セキュアトラスト基盤フレームワークでは、現在のサプライチェーンにおける ISMS（ISO/IEC 27001）等の取得状況の確認、契約書における遵守条項の規定、定期的な監査等より詳細な観点（組織、プロセス、ヒト・モノ等）に対応した要求事項の確認を実施していくことになる。このことにより、サプライチェーンを形成する事業者に新たな負荷等が生ずることが想定されるため、それらの負荷等も十分に考慮した上で、組織、プロセス、ヒト・モノ等のどのような観点で、どのような要求事項とするか整理していくことが重要と考える。

② 適合性判定結果の流通により生ずるリスクに関する課題

セキュアトラスト基盤では、事業者に関するサイバーセキュリティへの取組状況を、従来の ISMS（ISO/IEC 27001）等の取得状況の確認、契約書における遵守条項の規定、定期的な監査等より詳細な観点に基づく適合性判定結果を流通することになる。このことから、当該事業者がどのレベルまでサイバーセキュリティ対策を実施しているか第三者が把握することができる可能性があり、ひいては当該事業者に関する脆弱性に関する情報が拡散するリスクが考えられる。このような側面についても適切に配慮した仕掛けとすることが重要となる。

③ 中小企業を取込むべくフレームワークの運用に関する課題

現在のサプライチェーンは大企業から中小企業まで非常に広範囲の事業者により形成さ

れており、特に中小企業においてはセキュアトラスト基盤フレームワークに対応できる体力を有しない企業があることも想定される。このような、中小企業等をどのように取込んでいくかの解決策を見出していくことが重要となる。

④　グローバルを見据えたフレームワークの運用に関する課題

現在のサプライチェーンは、国内の事業者にとどまらず国外の事業者も含めたグローバルで形成されており、国外の事業者においては欧米企業だけなく、アジア圏等の欧米以外のグローバルな事業者も含まれる。当該圏内の現地事業者には国等で運用されたサイバーセキュリティに関する制度等がないことも想定されることから、制度間の相互認証は望むべくもないため、当該圏内の現地事業者をどのように取込んでいくかの解決策を見出していくことが重要となる。

⑤　既存のサプライチェーンで用いられているシステムとの共存に関する課題

業界によっては業界共通の電子商取引のネットワークや、大企業では独自のサプライチェーン管理システムを構築・活用しているケースがある。セキュアトラスト基盤フレームワークを構築・運用していく上では、それら既存のシステムとの関係や連携等のあり方について方向性を定め、各ステークホルダーと協調して推進していくことが重要となる。

4.4.　まとめ

4.3.1 で述べたような、セキュアトラスト基盤フレームワークを実現することで、事業者が個別にサイバーセキュリティ対策を施してきた従来に対して、サプライチェーンの上流から下流までの全体を対象とした、高い水準のセキュリティ環境を適切なコストで整備することが可能となる。これは、従来の日本の強みである高い品質に加え、更に高いセキュリティを備える製品やサービスの提供が可能となり、グローバル市場における日本の事業者の差異化、ひいては国際競争力の向上に繋がると考える。

また、セキュアトラスト基盤フレームワークは、4.2 で述べた通り、欧米におけるサイバーセキュリティに関する施策や国内外のサイバーセキュリティに関する規格・ガイドライン等との整合を確保及び相互認証を確立することにより、セキュアトラスト基盤フレームワークの認証を取得した日本の事業者は、自動的に国内外の様々な規格やガイドラインへ適合することが可能となり、グローバル市場における優位性の確保に繋がると考える。

なお、セキュアトラスト基盤フレームワークの実現に向けては、4.3.2 に述べた通り、多くの検討課題が残されている状況である。これらの検討課題については、引き続き解決の方向性、解決策への取組みが重要となる。

以上が本プロジェクトで取りまとめた、Society5.0 時代における様々なシステムやサービスが連携・結合する観点を基点とした、業界内外及び国内外に広がるサプライチェーンに

関してサイバーセキュリティを確保する社会的仕掛けの検討結果である。今後は、前述したこれらの実現に向けた検討課題への取組みに並行して、これまでの検討を活用し、現実世界とサイバー空間がより高度に融合するSociety5.0に適合したセキュアトラスト基盤フレームワークの実現につなげられていくことが望まれる。

5. 本プロジェクトからの提言

本プロジェクトでは､欧米で活発化するサイバーセキュリティに関する施策の動向に基づき､サプライチェーン全体におけるサイバーセキュリティに関する取組みの重要性を示すとともに、セキュアトラスト基盤フレームワークの社会実装の方向性を示した。

これらの検討を通じ、セキュアトラスト基盤フレームワークに関して、今後官民一体となった取組みの推進に係る提言を以下に示す。

【提言 1】グローバルに対応したサイバーセキュリティに関するリテラシー向上

現時点では直接的な影響が発生していない業界・業種等では、欧米等で活発化するサイバーセキュリティに関する施策に関する関心が低い傾向にある。しかし、サイバーセキュリティはどの業界・業種等にも共通する要素であることから、これまで影響のなかった業界・業種等に対して新たな施策が欧米等で適用される可能性も十分考えられる。このことからも、官民が連携して欧米等でのサイバーセキュリティに関する施策の動向を把握・周知・共有する仕掛けをつくり、グローバルに対応したサイバーセキュリティに関するリテラシー向上を図ることが必要である。

〔官への期待〕

- 欧米等でのサイバーセキュリティ施策動向の把握・産業界へ情報発信を行う仕掛けづくり
- 産業サイバーセキュリティ研究会（経済産業省、2017 年 12 月設置）等内におけるサプライチェーン全体のサイバーセキュリティに関する検討結果の周知

〔民の役割〕

- 欧米等でのサイバーセキュリティ施策動向に基づく業界内・企業内でのリテラシー向上策の実践(例:本プロジェクトの活動結果に関する COCN からの情報発信等)

【提言 2】セキュアトラスト基盤フレームワーク実現に向けた検討推進

グローバル市場における日本の事業者の差異化を図り、より高い信頼に繋げるセキュアトラスト基盤フレームワークについて、官民が連携して実現に向けた取組みを推進していくことが必要である。なお、取組みに当たってはまず業界共通での検討を進め、その後に業界ごとの特異点を踏まえた検討を進めることを想定する。

〔官への期待〕

- セキュアトラスト基盤フレームワークに関する制度設計
- 中小企業へのセキュアトラスト基盤フレームワーク適用への施策推進
- 欧米等でのサイバーセキュリティに関する施策の相互認証実現への施策推進
- アジア圏等の欧米以外のグローバルな事業者へのセキュアトラスト基盤フレームワーク適用への施策推進

〔民の役割〕

・セキュアトラスト基盤フレームワークに必要となる技術の研究開発の推進
・セキュアトラスト基盤フレームワークの検証・運用
・既存のサプライチェーンで用いられているシステムとの連携に向けた推進

また、4.4で述べた通り、本プロジェクトでは、Society5.0時代における様々なシステムやサービスが連携・結合する観点を基点として、業界内外及び国内外で広がるサプライチェーンを対象に、サイバーセキュリティを確保する社会的仕掛けについて検討した。今後はSociety5.0時代における現実世界とサイバー空間がより高度に融合するSociety5.0に適合したセキュアトラスト基盤フレームワークの実現につなげていくことが重要となる。

一般社団法人 産業競争力懇談会（ＣＯＣＮ）

〒100-0011　東京都千代田区内幸町２－２－１
日本プレスセンタービル　４階
Tel：03-5510-6931　Fax：03-5510-6932
E-mail：jimukyoku@cocn.jp
URL：http://www.cocn.jp/
事務局長　中塚隆雄