経済産業省

資料４

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

平成30年8月3日

経済産業省　商務情報政策局

サイバーセキュリティ課

米国における最近の動き

- サイバーセキュリティフレームワークの改訂
- 2017年5月大統領令に基づく各種報告書の公表
  - 連邦政府のサイバーセキュリティリスクに関する報告書
  - ボットネット対策等に関する報告書
- NIST SP800-171

サイバーセキュリティフレームワークの改訂

- 2度の意見募集を踏まえた修正を行った上で、**2018年4月**、米国国立標準技術研究所（NIST）が**「Cybersecurity Framework Version1.1」を決定。**
- 国際標準化に向けた活動も開始。

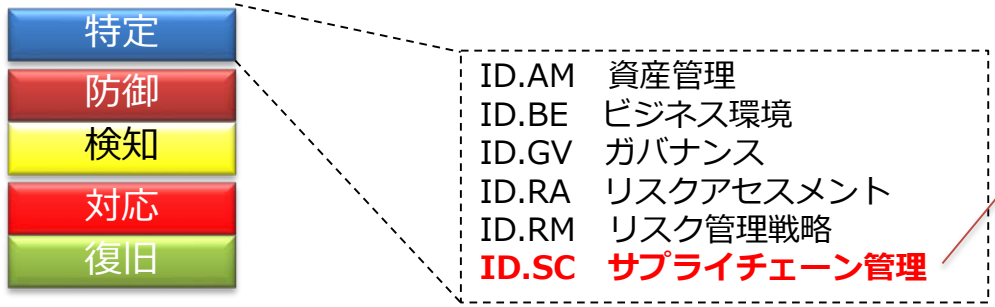
NIST「Cybersecurity Framework」の経緯

- 2014年2月、サイバーセキュリティ対策の全体像を示し、「特定」、「防御」、「検知」、「対応」、「復旧」に分類して対策を記載した「Cybersecurity Framework Vesion1.0」を策定。
- 2017年1月、「Cybersecurity Framework Version1.1 draft1」を公表。
- 2017年12月、「Cybersecurity Framework Version1.1 draft2」を公表。
- 2018年4月、「Cybersecurity Framework Version1.1」を決定。

NIST「Cybersecurity Framework Version1.1」の特徴

- Version1.1は、Version1.0より特に以下の点が追記され、その重要性が説かれている。
  - サプライチェーンのリスク管理（Supply Chain Risk Management）
  - サイバーセキュリティリスクの自己評価（Self-Assessing Cybersecurity Risk）

Cybersecurity Frameworkにおける5つの分類



Version1.1でID.SCが新規に追加され、**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を要求

2017年5月大統領令に基づく各種報告書の公表

- 2017年5月、トランプ大統領が「サイバーセキュリティ強化のための大統領令」に署名。関係省庁に対して複数の報告書の策定を命令。
- **2018年５月29-31日、関係省庁は国内での議論を喚起するため、可能な範囲で各種報告書を公表。**

1．連邦政府のサイバーセキュリティリスクに関する報告書 (5/29 国土安全保障省・行政管理予算局):
- 96の政府機関のサイバーセキュリティ管理能力のアセスメント結果と改善策を報告。

2．ボットネット対策等に関する報告書 (5/30 国土安全保障省・商務省):
- ボットネット対策等のために官民が取るべき対策を報告。120日以内にロードマップを策定予定。

3．電力網への攻撃に対するインシデント・レスポンスに関する報告書 (5/31 エネルギー省):
- 電力事業者がインシデントに対応するための７つの能力ギャップと提言について報告。

4．人材育成に関する報告書 (5/31 国土安全保障省・商務省):
- 299,000人分のオンライン上のセキュリティ関連空きポストに対応するための取組について報告。

5．米国のサイバー利益保護のための国際活動に関する報告書（5/31 国務省）:
- 開放的で相互運用可能で安全で信頼の高いサイバー空間のために必要な外交活動等について報告。

6．敵対勢力に対する抑止等に関する報告書 (5/31 国務省):
- 武力等により抑止を行うべき悪意あるサイバー活動の基準・閾値等について報告。

7．重要インフラ防御に関する報告書 (5/31 国土安全保障省):
- 各政府機関が各重要インフラ事業者に対して有する権限や能力について特定し、改善策を報告。

8．市場の透明性に関する報告書 (5/31 国土安全保障省):
- 事業者のセキュリティリスクの透明化のために必要な調査・政策検討について報告。

連邦政府のサイバーセキュリティリスクに関する報告書

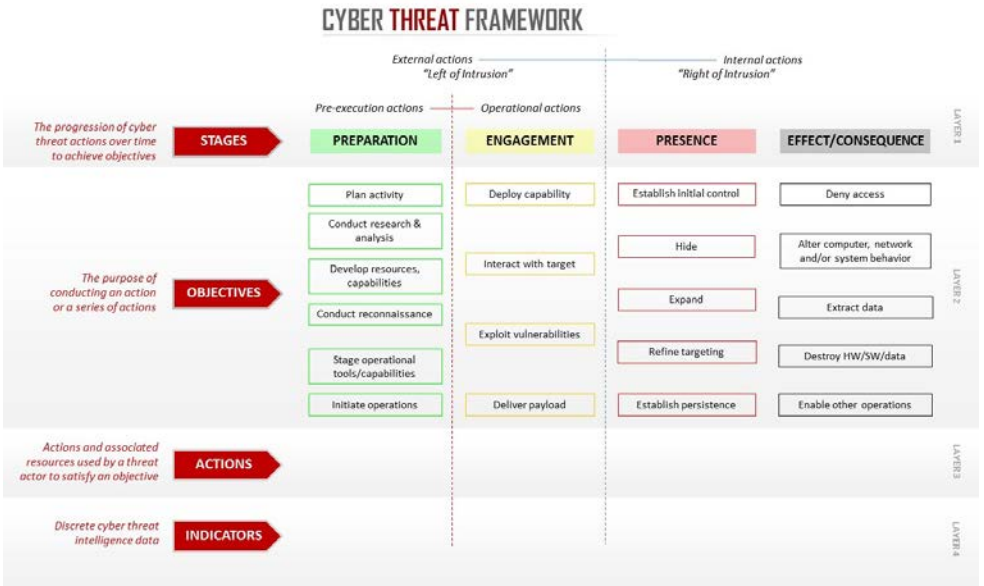
- 行政管理予算局（OMB）と国土安全保障省（DHS）が**政府機関のサイバーセキュリティ管理能力のアセスメント**を行い、**96機関中71機関（74%）の機関が高リスク又はリスクがあると報告。**

改善に必要とされる４つのコア活動

（１）サイバー脅威フレームワークの活用により、リスクの優先順位をつけて対策に取組む。
（２）ＩＴとサイバーセキュリティに係るコスト管理と資産マネジメント能力の標準化。
（３）ＳＯＣの統合により検知・対応能力を向上。
（４）プロセス改善や繰り返しのリスクアセスメントにより、説明責任能力を向上。

◆ **サイバー脅威フレームワーク（右図）**

- **国家情報長官官房（ODNI）が開発。**
- **サイバー攻撃における一連の活動を、４つの段階（Preparation → Engagement → Presence → Effect/Consequence）に分けて整理。**
- **サイバー攻撃に関する共通的な語彙と枠組みを提供し、脅威の傾向や必要な対策等を検討する際に使用されることを目指している。**



出典：国家情報長官官房（ODNI）

ボットネット対策等に関する報告書

- **ボットネット及びその他の自動化・分散化した脅威に対するインターネット・通信のエコシステムの強靭性の強化**に関する**報告書。**
- **5つの目標を設定。**
  - 適応可能、持続可能かつ安全な技術市場環境の実現に向けた明確な道筋の特定
  - 進化する脅威に動的に対応するためのインフラのイノベーションの促進
  - ネットワークのエッジにおけるイノベーションの促進による、自動化・分散化した脅威の防止、検出、影響の緩和
  - 国内外のセキュリティ、インフラ、運用技術の各コミュニティ間の連携の促進と支援
  - エコシステム全体にわたる啓発・教育の強化
- **商務省及び国土安全保障省に対して、本報告書承認後120日以内に、産業界・社会・国際パートナーと協議し、初期ロードマップ策定を要請。**

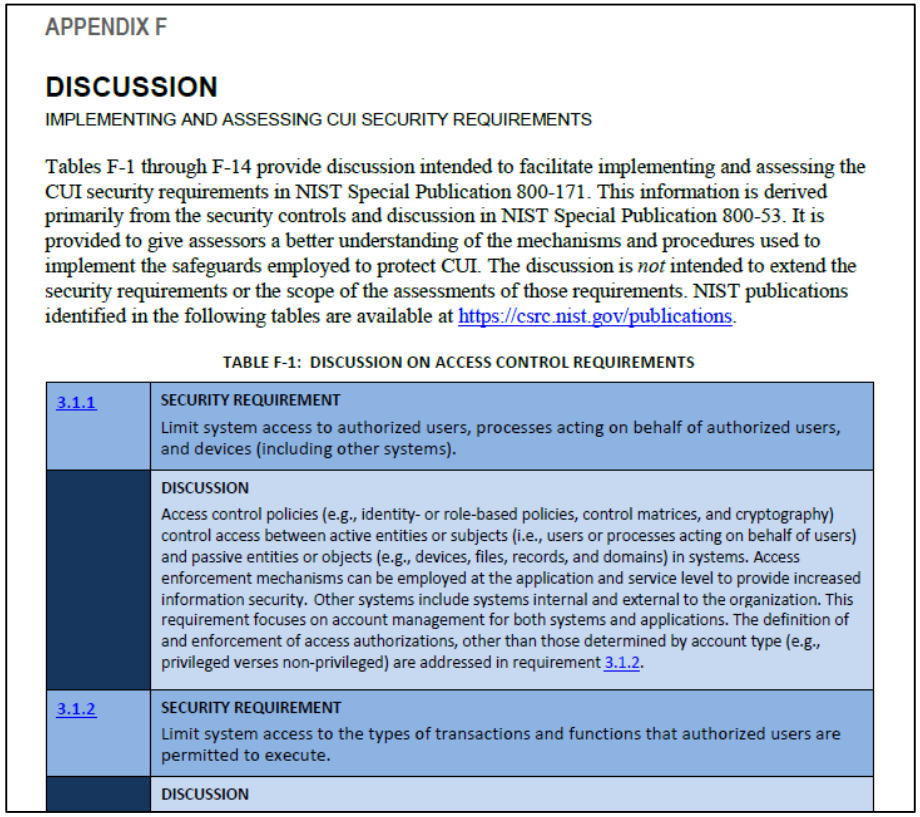
2018年5月最終報告書

A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats（ボットネット及びその他の自動化・分散化した脅威に対するインターネット・通信のエコシステムの強靭性の強化に関する報告書）　2018年5月22日
本報告書の公表をもって取組が終わる訳ではないとした上で、連邦政府が取り組むべき事項に力点を置き、関係者による様々な取組の調整・協働をサポートするための道筋を提示

NIST SP800-171

- NIST SP800-171は、CUI (*1)の保護を目的に14個のカテゴリと109の項目から構成。
- NISTは、SP800-171の定期的なメンテナンスを実施し、2018/06/07にも、アップデート版を公表。

(*1) Controlled Unclassified Information；管理対象となるが秘密指定されていない情報



APPENDIX F

DISCUSSION

IMPLEMENTING AND ASSESSING CUI SECURITY REQUIREMENTS

Tables F-1 through F-14 provide discussion intended to facilitate implementing and assessing the CUI security requirements in NIST Special Publication 800-171. This information is derived primarily from the security controls and discussion in NIST Special Publication 800-53. It is provided to give assessors a better understanding of the mechanisms and procedures used to implement the safeguards employed to protect CUI. The discussion is *not* intended to extend the security requirements or the scope of the assessments of those requirements. NIST publications identified in the following tables are available at https://csrc.nist.gov/publications.

TABLE F-1: DISCUSSION ON ACCESS CONTROL REQUIREMENTS

3.1.1	SECURITY REQUIREMENT Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
	DISCUSSION Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. This requirement focuses on account management for both systems and applications. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged verses non-privileged) are addressed in requirement 3.1.2.
3.1.2	SECURITY REQUIREMENT Limit system access to the types of transactions and functions that authorized users are permitted to execute.
	DISCUSSION

2018/06/07アップデート版では、セキュリティ要件を満たすために必要な具体的な事項を記載した「APPENDIX F：DISCUSSION」が追加された。

例

3.1.13	**SECURITY REQUIREMENT** リモートアクセスセッションの機密性を保護するために暗号メカニズムを採用する。
	DISCUSSION 一般に適用される暗号標準には、FIPSで検証された暗号とNSAで承認された暗号が含まれる。

欧州における最近の動き

- Cybersecurity Certification Framework
- eプライベート規則
- NIS指令

欧州における最近の動き

- 欧州では、**「Cybersecurity Certification Framework」の導入に向けた議論を継続。**
- **2018年5月25日、EU一般データ保護規則（GDPR）施行。**
- **eプライバシー規則**も審議中。

「Cybersecurity Certification Framework」の経緯

- 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、そこには新たにサイバーセキュリティ認証フレームワーク（Cybersecurity Certification Framework）の導入について言及。
- 2018年2月、EU標準化団体とENISAにより、「Cybersecurity Act」に関する会議開催。
- 2018年3月、欧州委員会とENISAにより、「Cybersecurity Certification Framework」に関する会議開催。
- 2019年5月、Cybersecurity Actの施行予定。

eプライバシー規則

- eプライバシー規則（ePrivacy Regulation：Regulation on Privacy and Electronic Communications）、別名「クッキー（Cookie）法」は、プライバシー保護を目的としたEUの新規制。
- クッキーを利用してWebサービスの利用者を追跡する場合、利用者に対して明確な同意を得ることを要求。また、もし利用者が追跡行為を拒否しても、平等にWebサービスの提供を義務付け。
- Google、Facebook等の大手デジタル企業は、eプライバシー規則が施行されると、広告収入に基づく現行のビジネスモデルが崩壊することを危惧し、反対キャンペーンを実施。

NIS指令

- 2016年8月、EUにおいて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**）が発効。
- NIS指令は、サイバーセキュリティに関するEU最初の指令であり、EU全体のセイバーセキュリティレベルを高める法的措置を提供。
- **2018年5月9日までに**、EU各国に対して、NIS指令に基づく**国内法の整備を要求**。
- **2018年11月9日までに、重要インフラ事業者やデジタルサービス提供者等に対して、リスクマネジメントやインシデント報告の義務を要求**。

NIS指令の目的

（1）国家レベルでのサイバーセキュリティ能力向上。

（2）EUレベルの協力強化。

（3）重要インフラ事業者やデジタルサービス提供者等に対するリスクマネジメントやインシデント報告義務化。

対象事業者の義務

・適切なセキュリティ対策。

・各国当局へのインシデントの通報。

以下のセキュリティ対策を含む。

① リスクの予防

② ネットワークと情報システムのセキュリティ確保

③ インシデントハンドリング