米国における重要インフラのサイバーセキュリティ確保に関する検討状況の調査

報告書

2013 年 12 月

北米連携センター

目次

1 背景

ITの普及とともにサイバー脅威もその数を増しており、米国は 21 世紀に入って、新たなセキュリティ問題に数多く直面している。サイバー攻撃に対する認識は国家レベルでも、個人レベルでも高まっているものの、他国同様、米国もその対応は遅い。「米国は、米国のサイバーセキュリティを脅かす、サイバーテロリスト、サイバースパイ、サイバー泥棒、サイバー戦士、及びサイバー・アクティビストと呼ばれるハッカー活動家等に対して、準備ができていない」[1]。サイバーセキュリティ分野の中でも、とりわけ重要インフラは、最も脆弱である。専門家は、サイバー攻撃に関して言えば、政府であれ企業であれ、もはや「いつ」起こるかが問題なのであり、「もし」起こったらという問題ではない[2]のが現状である。

このような世情を反映し、2013 年 2 月 12 日にオバマ大統領から「重要インフラのサイバーセキュリティの改善」と題された大統領令（大統領令 13636 号）が発布された。この大統領令では、重要インフラを「容量不足や破壊が生じれば、安全保障、経済的安全保障、公衆衛生、およびそれらが複合した問題により国家を衰弱させる、米国の生命維持に不可欠な、物理的なまたは仮想的な、システムおよび資産」[3]と定義している。

一方、経済協力開発機構（OECD）では、重要インフラを「崩壊すれば深刻に公共の安全や社会秩序、そして政府責任を妨げる可能性がある有形または無形資産」[4]と定義している。この定義のポイントは、政府の責任[5]について言及している点である。サイバーセキュリティは、政府の責任であるがゆえにその重要性が高い。サイバー法律論者の Paul Rosenweig（ポール・ローゼンウィーグ）氏は、「一般市民は、サイバースペースの拡大に対して、断固とした防衛策を政府に強く期待している」と説明している[6]。

米国の重要インフラの中には、民間企業が所有・運営している物もあるが、その安全の維持管理については、任意とするか規制とするかは米国では決定していない。これまで政府が規制してこなかったことが、今回のサイバーセキュリティに関する大統領令に発布に繋がった。

---

[1] "The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress," https://www.fas.org/sgp/crs/misc/R42984.pdf.
[2] Nels Olson, Aileen Alexander, and Jamey Cummings, "Cybersecurity Is the Board's Business," BusinessWeek.com (November 4, 2013), http://www.businessweek.com/articles/2013-11-04/cyber-security-is-board-business.
[3] President Barak Obama, "Executive Order 13636," The President of the United States, (Feb. 12, 2013), http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.
[4] Organization for Economic Co-operation and Development. "Protection of Critical Infrastructure and the Role of Investment Policies Relating to National Security." (2008) http://www.oecd.org/daf/inv/investment-policy/40700392.pdf.
[5] Ibid.
[6] Allan A. Friedman, "Cyber security and Trade: National Policies, Global and Local Consequences," *Brookings*, (Sept. 9, 2013), http://www.brookings.edu/~/media/research/files/papers/2013/09/19%20cybersecurity%20and%20trade%20global%20local%20friedman/brookingscybersecuritynew.pdf, 2.

一般に大統領令とは、「行政部門の中で求められる、あるいは、承認される大統領の命令」で、「内容、判断、及び大統領の関わりが最高レベルのもの」[7]だと定義されている。これは、大統領権限を与えられているが、議会で承認された法律とは異なる。

大統領令 13636 号を発布の背景には、議会でサイバーセキュリティ法案が 2 回先送りになったことと、増加するサイバー攻撃の対応に、政府、個人、民間企業が負担した費用が、昨年だけで 3,000 億ドルにまで上ったことがある[8]。

第 112 回連邦議会の失策は、膨大な法案が提案されたにもかかわらず、法律として制定されたものが全くなかったことにつきる。次に挙げる事例は、中でも最も大きな失策だったといえる[9]。

最初の法案は、Cybersecurity Act of 2012（サイバーセキュリティ法案）で、上院民主院内総務のHarry Reid（ハリー・リード）氏が超党派で包括的な法案を策定しようと試みたも[10]のだったが、上院共和党のJohn McCain（ジョン・マケイン）氏は、最低限の基準が企業にとってあまりにも負担が大きいとして、これに反対し、最終的には、基準を企業の任意とするよう内容を変更させた[11]。しかし、この妥協案にもかかわらず、上院の投票では共和党員の議事妨害にあったことで、この法案は致命的となり、2012 年中にサイバーセキュリティ法案通過を目指した民主党の望みは砕かれた[12]。

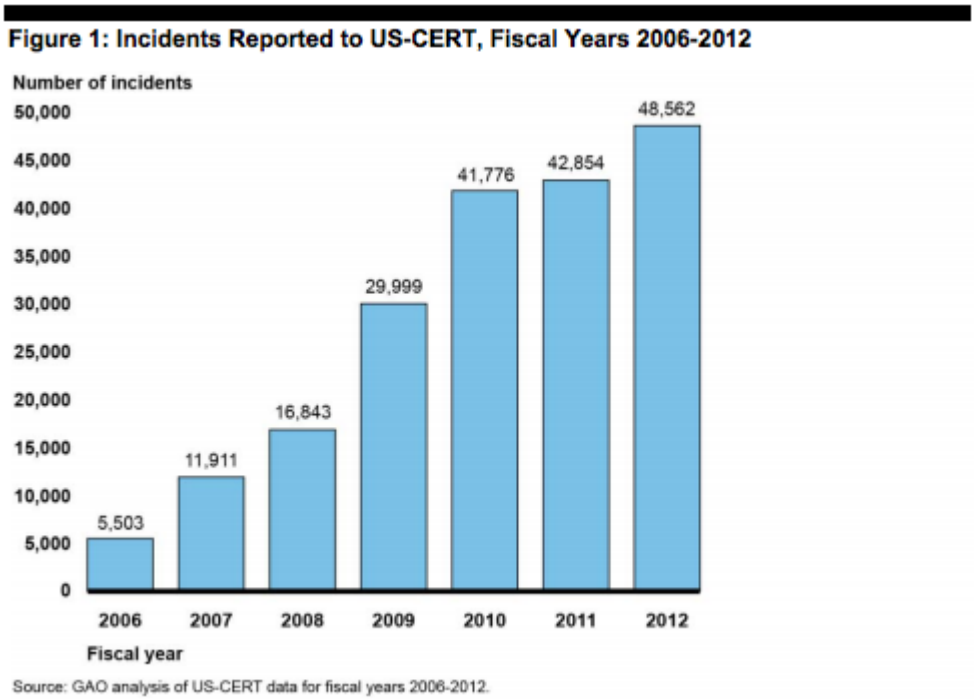
2 つ目のサイバーセキュリティ法案は、Ruppersberger（ルパース・バーガー）下院議員が提案したCISPA（Cyber Intellligence Sharing and Protection Act）法案（サイバー・インテリジェンスの共有および保護法案）で、下院は過したものの、民主優位の上院と、ホワイトハウスが拒否権行使を示唆たことで、制定には至らなかった。ホワイトハウスはこの法案に反対した理由として、消費者のプライバシー問題を挙げており、それから間もなく発布した大統領令では、プライバシー問題を取り上げている[13]。

今回の大統領令の重要な要素としては、米国の費用、件数、メディアの注目の点において、非常に大きくなっているサイバー攻撃の問題が挙げられる。過去 4 年で、米国に対するサイバー攻撃に対する費用は 78 パーセント増加し、昨年単独で見ても、26 パーセント増加した。プライバシー、データ保護、情報セキュリティを専門とする独立系調査

---

[7] Kenneth R Mayer, “Executive Orders and Presidential Power,” *University of Wisconsin-Madison,* http://users.polisci.wisc.edu/kmayer/Professional/Executive%20Orders%20and%20Presidential%20Power.pdf, 445.
[8] John Hamre, et al., “Protecting the American Economy from Cyber Attacks,” CSIS, (February 13, 2013), http://csis.org/files/attachments/131902_Cybersecurity_TS.pdf.
[9] Roger Runningen, “Obama Presses Cybersecurity Standards with Company Chiefs,” *Bloomberg.com,* (Oct. 29, 2013) http://www.bloomberg.com/news/2013-10-29/obama-presses-cybersecurity-standards-with-company-chiefs.html.
[10] Jeffrey Roman, “Piecemeal Approach to Cyber Legislation,” Bankinforsecurity.com, http://www.bankinfosecurity.com/piecemeal-approach-to-cyber-legislation-a- 6033.
[11] Michael S. Schimidt, “Obama Order Gives Firms Cyberthreat Information,” The New York Times, (Feb. 12, 2013), http://www.nytimes.com/2013/02/13/us/executive-order-on-cybersecurity-is-issued.html?_r=0.
[12] Ibid.
[13] Jason Koebler, “Obama Threatens to Veto CISPA, Citing Privacy Concerns,” *USNews.com,* (Apr. 16, 2013), http://www.usnews.com/news/articles/2013/04/16/obama-threatens-to-veto-cispa-citing-privacy-concerns.

会社である[14]Ponemon Institute（ポネモン・インスティチュート）による最新の調査によれば、2013 年、連邦機関を含めた 60 の組織においてサイバー犯罪にかかる平均費用は 1,160 万ドルだと見込まれている[15]。特に連邦機関に対するサイバー攻撃の数は、2006 年は 5,503 件だったが、2012 年には 48,462 件と、飛躍的に増加している[16]。



[17]

上図は、サイバー攻撃の増加傾向を示しているが、国防省曰く、1 日あたりのサイバー侵入は 1,000 万件に上る[18]。また、以下のように、メディアに掲載されたサイバー攻撃の記事も目立つようになっている。

- "Power-Grid Cyber Attack seen leaving Millions in Dark for Months," (Bloomberg, January 31, 2012)（電力系統へのサイバー攻撃の増加）
- "Major banks hit with biggest cyberattacks in history," (CNN, September 28, 2012)（大手銀行へのサイバー攻撃の増加）
- "Google Warns of New State-Sponsored Cyberattack Targets," (The New York Times, October 2, 2012)（国家が関与するサイバー攻撃の増加）

[14] Ponemon Institute, http://www.ponemon.org/
[15] Amber Corrin, "Frequency, cost of cyberattacks on the rise," *FCW.com*, (Oct. 08, 2013), http://fcw.com/articles/2013/10/08/cyberattacks-frequency-costs-rise.aspx.
[16] Gregory C. Wilshusen, "Testimony Before the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affars, U.S. Senate," United States Government Accountability Office, (March 7, 2013), http://www.gao.gov/assets/660/652817.pdf.
[17] Ibid.
[18] Dominic Basulto, "When will cybersecurity become a major campaign issue?" *The Washington Post*, (November 5, 2013), http://www.washingtonpost.com/blogs/innovations/wp/2013/11/05/when-will-cybersecurity-become-a-major-campaign-issue/.

- “Cyberattack on Saudi Oil Firm Disquiets US,” (The New York Times, October 24, 2012)（石油企業へのサイバー攻撃）

オバマ大統領と、前大統領候補Mitt Romney（ミット・ロムニー）氏も例外ではない。オバマ大統領の選挙キャンペーンはシリアから、ロムニー氏は中国からハッキングされていた[19]。サイバーセキュリティの警告は新しい試みではないものの、メディアで取り上げられる回数が増えるにつれて、政界でもその重要性が理解されている。重要インフラに対する攻撃の報道も増え、サイバー攻撃を受けやすい分野について、注意喚起している。重要インフラの重要性は、軽視されがちだが、国土安全保障省のIndustrial Control Systems Cyber Emergency Response Team (ICS-CERT)（産業制御システム・サイバー・緊急対応チーム）が出した 2012 年の報告書によると、政治家も一般市民も重要インフラについては注目している。同報告書では、以下のように述べている。「昨年の政府機関への攻撃は、198 件にのぼり、うち数件は侵入に成功した。エネルギーセクターは、最もターゲットになりやすい分野で、昨年は 82 回、また水産業も 29 回の攻撃を受けている。化学プラントは、7 回、原子力企業は 6 回のサイバー攻撃を受けた[20]。」

オバマ大統領の大統領令は、2014 年の大統領選挙年の混乱を前に、サイバーセキュリティ法案を通過させたいという希望だけでなく、現在の法律や規制が無い状態を補うメカニズムを設けることを目的に発令された。

[19] Ibid.
[20] David Goldman, “Hacker hits on U.S. power and nuclear targets spiked in 2012,” CNN.com, (January 9, 2013), http://money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks/.

2 大統領令

オバマ大統領が 2013 年 2 月 12 日付で下した大統領令は、以下の 12 のセクションから構成されている[21]。

No.	セクション名	概要
1	Policy（政策）	1. 情報共有の改善 2. リスクベースの基準の開発と導入
2	Critical Infrastructure（重要インフラ）	容量不足や破壊が生じれば、安全保障、経済的安全保障、公衆衛生、およびそれらが複合した問題により国家を衰弱させる、米国の生命維持に不可欠な、物理的なまたは仮想的な、システムおよび資産。
3	Policy Coordination（政策調整）	前述の政策が 2009 年 2 月 13 日の大統領令で確立した省庁間調整プロセスで実施する。
4	Cybersecurity Information Sharing（サイバーセキュリティ情報の共有）	Cybersecurity Act of 2012 の最後に記載されている「規制産業に関する異議」は今回の大統領令の最終目的ではない[22]が、Cybersecurity Act of 2012 の影響は随所に見られる。「情報共有及び、民間所有の重要インフラの保護」の条項は、今回の大統領令の根幹[23]であり、これまでの議会での失敗を生かして、第 113 回議会におけるサイバーセキュリティ法案の基礎を提供するというオバマ大統領の明確な意図を示している。 情報共有政策及び、司法長官、国土安全保障省長官、及び国家情報長官（DNI）のための期限について詳細に説明している。最初の期限は、大統領令が発布されてから 120 日目の 2013 年 7 月 12 日である。 その際、司法長官、国土安全保障省長官、及び国家情報長官（DNI）は、「特定の企業が標的になっているとわかっている場合に、米国に対するサイバー脅威に関して、機密扱いではない報告書を適時作成することを保証するため、共同の命令を発布する。 この報告書は、「諜報と法執行、及び情報源、方法、運営、捜査の妨げにはならない」というもので、司法長官、国土安全保障省長官、及び国家情報長官（DNI）は、「標的となっている企業へこの報告書を速やかに広めるプロセス」を取りまとめる。このプロセスは、国家のセキュリティ情報の保全を維持し、「この報告書の作成、頒布、配置の追跡システム」を考案する。 次の期限も、大統領令発布から 120 日後の 2013 年 7 月 12 日である。 国土安全保障省長官は、国防省長官と共同で、「全てのインフラセクタ

[21] NIST, “Improving Critical Infrastructure Cybersecurity Executive Order 13636: Preliminary Cybersecurity Framework,” NIST.gov, (Oct. 22, 2013), http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf.
[22] Eric Chabrow, “Cybersecurity Legislation: What’s Next?” (Sept. 13, 2013), http://www.bankinfosecurity.com/cybersecurity-legislation-whats-next-a-6063.
[23] Eric A Fischer et al., “The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress,” *Congressional Research Service*, (March 1, 2013), https://www.fas.org/sgp/crs/misc/R42984.pdf, 11.

		ーに対して、サイバーセキュリティ・サービスプログラムを拡大する手順を立ち上げる」と明言している。 このプログラムは、対象となる民間セクターである、重要インフラに、セキュリティサービスを提供するインフラ企業また商用サービスプロバイダーに対し、政府からの機密情報を提供するという、情報共有プログラムである。 加えて、国土安全保障省長官は、「重要インフラの所有者及び運営者に雇用された適切な人物に対するセキュリティクリアランス処理の迅速化」を推し進める。 同様に、「民間セクターの内容領域専門家を連邦機関に一時的に招聘するプログラムの利用拡大」も推し進める。この 2 つの条項も含めることで、民間セクターがサイバー脅威に関する情報を受け取ることが出来るようになるプロセスの迅速化が進むだけでなく、政府が民間セクターの優秀なアドバイザーと連携することができるようになる。
5	Privacy and Civil Liberties Protections（プライバシーおよび市民自由人権の保護）	大統領令によって実施される活動において、保証すべきプライバシー及び自由人権保護について記述している。 保証すべきプライバシー及び自由人権保護は、Fair Information Practice Principle（公正情報取扱原則）に基づいている。加えて、Chief Privacy Officer（プライバシー担当官）及び、国土安全保障省の Officer for Civil rights and Civil Liberties（市民権および市民自由人権局）は、プライバシー及び自由人権の侵害を軽減する方法を明記した違反報告書を作成し、この命令に沿って、類似の活動に従事するその他の機関もこの報告書にある評価を行う。 この違反報告書は、毎年レビューされ、必要に応じて修正される。この報告書を作成するに当たり、管理者は Privacy and Civil Liberties Oversight Board（プライバシーおよび市民自由人権監督ボード）に相談し、行政管理予算局（OMB）と調整する。
6	Consultative Process（助言プロセス）	国土安全保障省の長官に対し、インフラに対するサイバーセキュリティのリスクについて、以下の機関からの助言を考慮することを命じている。 • Critical Infrastructure Partnership Advisory Council（国土安全保障省が主導する重要インフラに関する官民パートナーシップ[24]） • Sector coordinating Councils（セクターごとの調整機関等） • 重要インフラ所有者及び運営者 • Sector-Specific Agencies（セクターごとの管轄連邦政府機関） • その他関連機関、独立規制機関、州、地方、準州及び部族政府、大学、外部専門家
7	Baseline Framework to Reduce Cyber	ここでは、サイバーリスク軽減のためのフレームワークについて述べている。

[24] Critical Infrastructure Partnership Advisory Council, http://www.dhs.gov/council-members-critical-infrastructure-partnership-advisory-council

	Risk to Critical Infrastructure（重要インフラへのサイバーリスクを軽減するベースラインフレームワーク）	米国国立標準技術研究所（NIST）長官が、重要インフラへのサイバーリスクを軽減するサイバーセキュリティフレームワークの作成を主導する。 このフレームワークには、基準、方法、手順及び、サイバーリスクに対応する為の政策と企業、技術的なアプローチが連携する手順が含まれている。さらにサイバーセキュリティを前進（進歩）させる任意の国際基準にも考慮しながら、ベストプラクティスと、コンセンサス基準が組み込まれている。このフレームワークは、サイバーリスクの識別や査定、管理において、重要インフラの所有者・運営者にパフォーマンスベースで、柔軟かつ繰り返し利用できる、費用対効果の高いアプローチを提供する。 このフレームワークでは、セクター間のセキュリティ基準とガイドラインを識別する、将来的な改善が必要な分野を特定する、技術的に中立なガイドラインを提供する、かつ、競争市場を考慮する、といったことを実施する。 また、このフレームワークを導入するに当たって、パフォーマンスを判断する機能も含まれている。このフレームワークには、導入の影響を最小限にとどめ、セキュリティとプライバシーを維持する方法が含まれている。 NIST 長官は、フレームワーク作成中に、パブリックレビュー及びパブリックコメントを求めると同時に、セクション 6 で挙げられているような関係者に相談をする。 また、国家情報長官（DNI）及び国土安全保障省長官は、このフレームワーク作成に役立てるため、脅威分析と技術的な専門知識を提供する。 このフレームワークのパフォーマンス目標は、セクション 9 にある。 期限： 大統領令発布後 240 日後の 10 月 12 日まで：初期フレームワークを発布 1 年以内の 2014 年 2 月 12 日まで：最終フレームワークを発行 ※レビューや更新情報を考慮するため、必要に応じてフレームワークに変更が加えられる。
8	Voluntary Critical Infrastructure Cybersecurity Program（任意の重要インフラサイバーセキュリティプログラム）	ここでは、フレームワークの採択を支持するために作成された任意のプログラムについて記載している。 セクターごとの管轄連邦政府機関は、このフレームワークをレビューし、導入ガイダンスまたは、具体的な補足資料を作成する。担当機関は、国土安全保障省長官にどの民間企業がプログラムに参加しているのかを報告する。長官は、このプログラムへの参加を促すために作られたインセンティブを確立する。 国防総省と米国連邦調達庁（GS）は、入手計画と契約管理の中に、セキュリティの利点とセキュリティ基準を組み込むメリットに関する提言を作成する。

		期限： 大統領令発布後 120 日以内：インセンティブの確立。
9	Identification of Critical Infrastructure at Greatest Risk（最も大きなリスクがある重要インフラの特定）	この大統領令発布から 150 日以内の 7 月 12 日までに、セクション 6 で特定した専門家とセクターごとの管轄連邦政府機関（Sector-specific agencies）が、アドバイザーとなって、国土安全保障省長官が重要インフラを特定するため、リスク分析を行う。 重要インフラの特定には、客観的な基準が使用され、商業商品やサービスは、その対象にはならない。また、特定された重要インフラも、毎年更新される。担当機関及び、民間企業は、国土安全保障省長官に必要な情報を提供する。重要インフラとして特定されたインフラには、特定の結果とその理由が通知される。インフラの所有者・運営者は、危険に瀕したインフラ企業、あるいはサービスプロバイダーとして、資料を提出し、再審を要求することでプロセスが決定する。 ※分析結果は公開されていない。
10	Adoption of Framework（フレームワークの採用）	重要インフラのセキュリティを担当する機関は、初期フレームワークをレビューし、現在のサイバー規制が充分であるかどうかを決定するための協議プロセスを行わなければならない。 初期フレームワーク発表から 90 日以内： 担当機関はこのフレームワークを確立し、現在のリスクに対応するための権限をもつか否かについて発表する。仮に、最終フレームワークが発表されてから 90 日以内に現在の規制要件が十分でないと判断される場合、担当機関は、サイバーリスクを軽減するための行動を提案する。 最終フレームワーク発表から 2 年以内： 担当機関及び民間インフラは、要件が効果的ではなく、特に難解だと判断した場合、その要件を軽減あるいは、削除するよう提言する。 国土安全保障省長官は、サイバーセキュリティに従事する人員とプログラムを開発するために、担当機関に対し技術支援を行う。独立規制機関は、サイバーリスクを軽減するため、作業に優先順位を付けることを検討する。
11	Definitions（定義）	大統領令で使用される用語を定義する。
12	General Provisions（権限の定義）	担当機関に対して、現行法で認められている権限以外には、何も追加されないことを明確にしている。この大統領令では、OMB の Director の権限を損なうものではなく、法執行と情報収集の方法及び情報源は、保護される。米国の国際的な責任は、この大統領令が実施されている間も維持する。

担当機関	権限
国土安全保障省長官[25]	• 重要インフラ全般に対する高度サイバーセキュリティを拡大する • 重要インフラ担当者のセキュリティクリアランス処理を迅速化する • 関連する民間セクターの専門家を連邦機関に一時的に招聘するプログラムを拡大する • 重要インフラのサイバーセキュリティを改善するための広範囲な協議プロセスを確立する • サイバー攻撃が、地域的あるいは国家的な被害になりうる重要インフラを毎年特定し、リストを更新する • 重要インフラと特定されたインフラの所有者及び運営者に、特定の結果とその理由を機密事項として知らせ、再審要求プロセスを作る • 重要インフラ規制機関のサイバーセキュリティについて、人員とプログラムを開発するための技術支援を行う • サイバー脅威事件の情報を収集し、標的となっている企業にその情報を広める • 大統領令による政府機関の活動に関して、プライバシーと自由人権を調整し、査定する
Sector Specific Agencies（セクターごとの管轄連邦政府機関）	• フレームワークのレビュー及びセクターごとの管轄ガイダンスを作成する • 重要インフラによるフレームワークの参加状況を毎年大統領に報告する • フレームワークの協議レビューを行う • 既存のサイバーセキュリティ要件が適切であるかを判断する • 担当機関が十分リスクに対応できるような要件を設けるための権限があるかどうかを、大統領に報告する • 必要性に応じて、追加承認を提案する • サイバーセキュリティの要件が効果的でない場合などに、解決策を特定し、提案する
National Institute of Standards and Technology（国立標準技術研究所）	• サイバーセキュリティのフレームワーク作成を主導する • フレームワークは技術的に中立である • フレームワークは、ベストプラクティス、ベストビジネスであることに焦点を当てている。基準は、セクター間共通で、任意のコンセンサスがあることが求められる • フレームワークは、改善する範囲を特定する • 必要に応じてフレームワークはレビュー及び更新される

[25] Eric A Fischer et al., “The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress,” 6-7.

2.1 議会の反応

民主党は、政党の方針に沿っているため、大統領令を支持している。特に上院多数党院内総務であるHarry Reid（ハリー・リード）上院議員は、サイバー攻撃から国民を守るため断固たる行動に出たと、大統領を称賛した[26]。Senate Commerce Committee（上院商務委員会）議長John D. Rockefeller IV（ジョン・ロックフェラー）上院議員、Senate Homeland Security Committee（上院国土安全保障委員会）議長Tom Carper（トム・カーパー）上院議員、及びSenate Intelligence Committee（上院諜報委員会）議長Dianne Feinstein（ダイアン・フェインシュタン）上院議員らも、今回の大統領令に対して強い賛同を表明している[27]。

サイバーセキュリティ法案は、大統領令発布以降、多く提出されているが、2013 年 12 月時点で、オバマ大統領に承認されたものはない。以下は、大統領令発布後に両院に提出されたサイバーセキュリティ関連法案の一覧である。

法案	状況	法案の内容
H.R. 3107 Homeland Security Boots-on-the-Ground Act	• 2013 年 9 月 17 日提出 • 2013 年 10 月 29 日下院投票	• サイバーセキュリティの職業分類作成 • サイバーセキュリティ業務従事者の評価 • サイバーセキュリティ業務従事者間の格差解消 • サイバーセキュリティ業務従事者に対する年次評価の発表
H.R. 756 Cybersecurity Enhancement Act of 2013	• 2013 年 2 月 15 日提出 • 下院通過 • 2013 年 4 月 17 日上院で上院通商科学交通委員会に提出	サイバーセキュリティに関するプログラムと調査を向上及び、サイバーセキュリティ業務従事者のニーズを政府に報告。
S. 1638 Cybersecurity Public Awareness Act of 2013	• 2013 年 10 月 31 日上院で国土安全保障・政府問題委員会に提出	国土安全保障省と国防総省の報告書及び、司法長官と FBI 長官の捜査・起訴に関する報告書によってサイバー事件へ注意喚起を促す。
H.R. 2556 Excellence in Cybersecurity Act	• 2013 年 6 月 27 日提出 • 2013 年 9 月 24 日研究技術小委員会に提出	サイバーセキュリティフレームワークに関する Vertical Centers of Excellence on Cybersecurity の作成を

[26] Privacy & Data Security Law Resource Center, “President Obama Signs Executive Order On Cybersecurity, Seeks Voluntary Standards.”
[27] Ibid.

		NIST に要求。
S. 1353 Cybersecurity Act of 2013	• 2013 年 7 月 24 日提出 • 2013 年 7 月 30 日通商科学交通委員会	サイバーセキュリティに対する反応に関し、サイバーセキュリティ研究、人材開発、教育、市民の認識、受け入れ準備を強化（旧 Cybersecurity Act of 2012）。
H.R. 1468 SECURE IT	• 2013 年 4 月 10 日提出 • 2013 年 6 月 24 日　研究技術小委員会に提出	研究、教育、情報、技術を通じたサイバーセキュリティの改善。
H.R. 624 Cyber Intelligence Sharing and Protection Act	• 2013 年 2 月 13 日提出 • 2013 年 4 月 22 日下院通過、上院で諜報活動特別委員会へ提出	諜報活動特別委員会とサイバーセキュリティ企業のサイバー脅威情報の共有。
Amendment for H.R. 624	2013 年 4 月 17 日投票により合意	共有・利用するサイバー攻撃等の脅威に関する機密情報の定義
H.R. 3032 Executive Cyberspace Coordination Act of 2013	• 2013 年 8 月 2 日提出 • 2013 年 9 月 16 日サイバーセキュリティ・インフラ保護・セキュリティ技術小委員会に提出	National Office for Cyberspace の創設及び、連邦情報セキュリティに関連する要件の修正。
H.R. 2952 CIRDA Act of 2013	• 2013 年 8 月 1 日提出 • 2013 年 10 月 29 日 Ordered to be Reported (Amended) by Voice Vote	重要インフラを保護するセキュリティ技術向上のための戦略作成。
Resolution H. 399 Supporting National Cyber Security Awareness Month	• 2013 年 10 月 30 日提出 • 2013 年 10 月 30 日下院科学宇宙技術委員会に提出	National Cyber Security Awareness Month（全米サイバーセキュリティ認識強化月間）への注目を集める。
H.R. 1640 Cyber Warrior Act of 2013	• 2013 年 4 月 18 日提出 • 2013 年 5 月 6 日 Subcommittee on Intelligence, Emerging Threats and Capabilities に提出	サイバー危機への対応力の向上。
S. 658 Cyber Warrior Act of 2013	• 2013 年 3 月 22 日軍事委員会に提出	サイバー危機への対応力の向上。
S. 1193	2013 年 6 月 20 日通商科学	個人情報を収集、管理する

Data Security and Breach Notification Act of 2013	交通委員会に提出	企業に対し、情報の保護と情報保護違反が発生した場合の告知を要求。

2.2 民間セクターの大統領令に対する反応

民間セクターが大統領令に応えて取った活動や行動は、様々である。以下は主要なものである。大統領令に応じて多くの報告書が発表されているのは、サイバーセキュリティのリスクへの答えを生み出すことにおいて、大統領令が一定の成功を収めているという例である。

組織	分類	反応の概要
US Telecom 社	通信会社	NIST長官であるPatrick Gallagher（パトリック・ギャラガー）氏を招いて、ワシントンD.C.で「National Cybersecurity Policy Forum（国家サイバーセキュリティ政策フォーラム）」を開催した[28]。
Center for Strategic and International Studies（CSIS）	シンクタンク	• 2013 年 7 月 22 日「Estimating the Cost of Cyber Crime and Cyber Espionage（サイバー犯罪とサイバースパイの被害額予測）」と銘打ったイベントを開催した[29]。 • 2013 年 10 月 23 日「Cybersecurity: 21st Century Threats, Challenges, and Opportunities（サイバーセキュリティ：21 世紀の脅威・チャレンジ・チャンス）」というイベントを開催した[30]。 • 「The Economic Impact of Cybercrime and Cyber Espionage（サイバー犯罪とサイバースパイの経済への影響）」と題した報告書をMcAfee社と共同で発表した[31]。
Booz/Allen/Hamilton（ブーズ・アレン・ハミルトン）社	コンサルティング	「The Cybersecurity Executive Order: Exploiting Emerging Cyber Technologies and Practices for Collaborative Success.（サイバーセキュリティ大統領令：協調による成功を実現するための先進サイバー技術と対策の追及）」という報告書を発表している[32]。

3 インセンティブ

大統領令のセクション 8 に応じて、2013 年 8 月 6 日、ホワイトハウスは、任意のサイバーセキュリティプログラムへの参加を促すための、インセンティブの候補のリストを

[28] “National Cybersecurity Policy,” *USTelecom.org*, (Accessed Oct. 28, 2013), http://www.ustelecom.org/events-education/executive-education/national-cybersecurity-policy-forum.
[29] “Estimating the Cost of Cyber Crime and Cyber Espionage,” *CSIS*, (Jul. 22, 2013), http://csis.org/event/estimating-cost-cyber-crime-and-cyber-espionage.
[30] “Cybersecurity:21st Century Threats, Challenges, and Opportunities,” *CSIS*, (Oct. 23, 2013), http://csis.org/event/cybersecurity-21st-century-threats-challenges-and-opportunities.
[31] CSIS, “The Economic Impact of Cybercrime and Cyber Espionage,” *CSIS*, (July 2013), http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf.
[32] Mike McConnell, et al., “The Cybersecurity Executive Order: Exploiting Emerging Cyber Technologies and Practices for Collaborative Success,” Boozallen.com, (2013), http://www.boozallen.com/media/file/BA13-051CybersecurityEOVP.pdf.

発表した[33]。これは、国土安全保障省、商務省、財務省が判断した、インセンティブの候補である。インセンティブの候補は、サイバーセキュリティ保険、補助金、プロセス選択、責任の範囲、規制の合理化、公的な認定、価格規制産業における価格転嫁、およびサイバーセキュリティ研究の 8 種類である[34]。

インセンティブ	概要
サイバーセキュリティの保険	サイバー保険の競争市場を作る目的で、保険産業と契約する。
補助金	サイバーセキュリティプログラムへの参加を連邦重要インフラ補助金の基準または条件とする。
プロセスの選択	既存の政府事業の実行を早めるか否かという政府の決定の検討に参加する。
責任の範囲	政府機関は、特定の分野（不法行為に基づく責任、賠償限度、高い立証責任等）における参加者の義務を軽減することで、重要インフラ企業のフレームワークの導入促進につながるかについて研究する。
規制の合理化	既存の法律と重複する点を削除することや、監査の負担を軽減することで、既存のサイバーセキュリティ規制を合理化し、コンプライアンス作成を簡便化する。
公的な認定	政府機関は、このプログラムの参加企業を公的に認定することがインセンティブとして効果があるかどうかを検討している。
価格規制産業における価格転嫁	サイバーセキュリティフレームワークに関連する投資の回収ができるよう公共料金を設定するかどうかについて、連邦、州、地方の各政府と協議する
サイバーセキュリティ研究	これまでにない商業的な解決策が可能である分野を決定するために研究と開発を行う。これによって政府が、最優先のサイバーセキュリティ問題に見合う研究と開発に焦点を当てることができる。

[35]

提案されたインセンティブに対して、様々なレビューが寄せられている。インセンティブは魅力的な選択肢であると考えられているので、このフレームワーク促進のための良いスタートだと考えている人もいる[36]。一方、インセンティブの中には、議会の規制を

[33] Michael Daniel, “Incentives to Support Adoption of the Cybersecurity Framework,” The White House Blog, (Aug. 6, 2013), http://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.
[34] Ibid.
[35] Jessica Goldenberg, “White House Posts preliminary cybersecurirty incentives,” Proskauer, (Aug. 22, 2013), http://privacylaw.proskauer.com/2013/08/articles/online-privacy/white-house-posts-preliminary-cybersecurity-incentives/.
[36] Brian E. Finch, “White House Incentives to Support Cybersecurity: A Good Start for an As-Of-Yet Defined Goal,” *The Huffington Post*, (Aug. 19, 2013), http://www.huffingtonpost.com/brian-e-finch/obama-administration-cybersecurity_b_3768034.html.

要するものや、政府に権限が与えられるものではないものもあると指摘する人もいる[37]。民間セクターは最終フレームワークが発表されるまで、このインセンティブに対してコメントする時間を与えられており、その時には、さらに他のインセンティブが提案される可能性もある。

4 NIST Preliminary Cybersecurity Framework（サイバーセキュリティフレームワーク案）

NIST が大統領令のセクション 7 に応じて作成したサイバーセキュリティフレームワークは、民間所有の重要インフラ企業／組織に対し、企業ごとのフレームワークを作成することで、サイバーセキュリティリスクの管理に関するガイドラインを提供するために作られたもので、今回の大統領令の中でも最も影響力があるものである。企業に既存のフレームワークがある場合は、既存のプロセスを補い、改善するためにサイバーセキュリティフレームワークを使用することができる。企業がフレームワークを持たない場合は、サイバーセキュリティフレームワークを、自社のフレームワークを作成するための基盤として使用できる。

4.1 フレームワーク案策定まで

フレームワークは、何度も推敲が重ねられ 2013 年 10 月 22 日に発表されたPreliminary Cybersecurity Framework（サイバーセキュリティフレームワーク案）が現時点で最新のものである[38]。フレームワーク草案は、3,000 人以上の業界の専門家及び学識経験者、政府役人、及び政府機関と重要インフラの所有者及び運営者からのデータをもとに作成されている[39]。作成に当たっては、米国内で 4 回のワークショップを開催し、また、オンラインで情報を求め、さらに、集めた情報で作成した草稿を最新版に更新した。

企業からの懸念事項や提案にNISTが回答したことは、好意的に受け取られており[40]、その情報収集と継続的な活動の両方が、民間セクターからの高い評価を受けている[41]。これは、単にNISTのこれまでの苦労が評価されただけでなく、フレームワーク全体として、サイバー攻撃等の脅威と戦うための、政府と産業の協力関係の始まりを表しているのである[42]。民間セクターは、最終フレームワークが発表される際にも同様に、NISTが引き続き民間からの情報を高く評価し、それに対応することを望んでいる。

---

[37] Tony Romm, “W.H. privacy meetings continue – Next steps after Obama admin floats cyber perks – The next FWD.us immigration push,” POLITICO, (Aug. 07, 2013), http://www.politico.com/morningtech/0813/morningtech11359.html.
[38] Alina Selyukh, “U.S. proposes minimal corporate cybersecurity standards,” *Reuters*, (Oct. 22, 2013), http://www.reuters.com/article/2013/10/22/net-us-usa-cybersecurity-standards-idUSBRE99L1LR20131022.
[39] Ibid.
[40] Cynthia Brumfield, “NIST’s latest cybersecurity framework reveals a lot of goodwill amidst continued criticism,” *CSO Online*, (Oct. 24, 2013), http://www.csoonline.com/article/741979/nist-s-latest-cybersecurity-framework-reveals-a-lot-of-goodwill-amidst-continued-criticism.
[41] “USA: NIST voluntary Cybersecurity Framework ‘hard to ignore,’” Data Guidance, (Oct. 30, 2013), http://www.dataguidance.com/news.asp?id=2139.
[42] Ibid.

第 4 回、第 5 回ワークショップが、11 月 14、15 日にノースカロライナ州で開催され、最後のパブリックコメントは、2013 年 12 月 13 日を期限となっている。フレームワーク作成日程の中でも、この最終コメントの期限が最終フレームワーク発表の 2014 年 2 月以前であることは、特に論争の的であった。

Core Security社のエンジニアリング部長であるKen Pickering（ケン・ピッカリング）氏のように、「市民がレビューを重要視しており、NISTがフィードバックを編集に反映させるのであれば、レビュー期間が 45 日であることは適当である」[43]とする専門家もいる。一方、Tripwire社の最高技術責任者Dwayne Melancon（ドワイニ・メランコン）氏のように、「フィードバックの時間が短いことを懸念している。このような種類のフレームワークは大変複雑であり、隔離された状態でフィードバックを収集することは問題である」[44]と指摘する声もあり、一部の人に好都合な状況を作り出す方法として、少数のフィードバック提供者がNISTに集まる可能性が懸念している。

NIST が民間セクターの懸念事項に目を向けるという点で、草稿の修正は重要であるといえる。最初の修正点は、プライバシーと自由人権に対して高まる関心と重要性についてである。大統領令では取り上げられているが、最初の草稿では、補足程度にしか記載されていなかった。

公正情報行動原則を受け入れるためのフレームワークが必要であれば、プライバシーは「明らかにフレームワーク開発プロセスの一部にならなかった」ということは、草稿の大きな欠点であった[45]。新たな草稿は、プライバシーのスタンダードとプラクティスに一致しながら、それぞれのベストスタンダード及びベストプラクティスに合っている。

次の大きな修正点は、ビジネスニーズに対する関心が高まった点であった。費用対効果やイノベーションのようなビジネスニーズを考慮することで、新たな草稿は、よりビジネスに対応したものとなった。NISTは、フレームワークのコア（後述）において柔軟性を発揮することで、これを実現したが、フレームワークがよりビジネスを意識したものになる一方で、フレームワークの効果も弱めてしまうのではないかという議論もある[46]。

第 3 の修正点は、このフレームワークの初期の草稿で、「重要インフラとその関連産業セクターの両方に対して、継続的な改善を行うことを強調していた」[47]点である。重要インフラセクターを対象とする代わりに、新たな草稿では、個々の組織とその責任に焦点を当てている。繰り返しになるが、この修正点は、フレームワークの果たすべき責任と義務に対する修正であるため、議論の的になると考えられている。この修正やフレームワークそのもの、さらに今回の大統領令に対する反応は、企業によって印象が違う理由を理解するためにも、詳細に渡って議論を必要とする。

---

[43] Richard Adhiari, “NIST Forges Ahead with Critical Infrastructure Security Plan,” *TechNewsWorld.com*, (Oct. 23, 2013), http://www.technewsworld.com/story/79263.html.
[44] Ibid.
[45] Jonathan Cain, “NIST Publishes Preliminary Federal Cybersecurity ‘Framework’ for Comment,” *Mintz-Levin*, (Oct. 24, 2013), http://www.mintz.com/newsletter/2013/Advisories/3486-1013-NAT-PRIV/index.html.
[46] Ibid.
[47] Ibid.

4.2 目的

フレームワークの目的は、サイバーセキュリティリスクの管理および改善を支援することと、それを達成する上での必要となる以下に関する組織内外でのコミュニケーションにおける共通言語・手順を提供し、また組織内外のコミュニケーションを促進することにある。

- 組織のサイバーセキュリティの現状把握
- 組織のサイバーセキュリティの目標設定
- 現状と目標のギャップの特定と改善事項の優先順位付け
- 目標達成状況のモニタリング

ただし、フレームワークはこの目的を達成する上で、既存のリスク管理プロセスを置き換えず、補完するのみであるとしており、そのため、フレームワークそのものも何も無い全く新しいところから作成したのではなく、既存の規格等に依存している。もちろん、まったくサイバーセキュリティ管理活動を実施していない場合は、参考にすることも可能であるとし、新たな規格、ガイドライン、プラクティスを発見したり、既存のものを修正するためのツールとして使用することも可能であるとしている。

また、大統領令に述べられているとおり、フレームワークは、リスクマネジメント手法を基本としている。これば、フレームワークがベースラインやチェックリスト方式により、重要インフラに関わる組織に一方的に負担を強いるのではなく、組織が、リスクの大きさに応じて、適切な経営判断をし、対策を講じることを促すためであり、官民で協力しなければ、サイバー攻撃等の脅威に対抗するための環境・文化を形成することは難しいことを認識しているからである。

また、NISTのパトリック・ギャラガー長官は、このフレームワークについて、「技術と脅威が変化するにつれて、そして、組織が成長していくにつれて継続的な改善が可能な生きた資料である」[48]とし、最終版発行以降も改善されつづけてくことを明言している。

4.3 構成

フレームワークは以下の 3 つの要素によって構成されている。

要素	概要
Framework Core （コア）	サイバーセキュリティ対策のための組織の管理活動集 また、「コア」には、Appendix B「Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program（サイバーセキュリティプログラムにおけるプライバシーおよび自由人権を保護する手法）」として、コアで特定した管理活動ごとに、実施する際に考慮すべき個人情報および自由人権を保護するための手法をまとめている。

[48] Dr. Patrick Gallagher, Opening Remarks: Press Briefing, Preliminary Cybersecurity Framework, *NIST*, (Oct. 22, 2013), http://www.nist.gov/director/speeches/cybersecurity-framework-remarks-102213.cfm.

要素	概要
Framework Profile （プロファイル）	サイバーセキュリティのレベルを把握し改善するためのツール
Framework Implementation Tiers （ティアー）	組織がどのようにサイバーセキュリティリスクを管理するかを表す区分

4.3.1 コア

フレームワークの「コア」とは、サイバーセキュリティ対策の主要な目標とその目標を達成する上で必要だと思われる管理活動（管理活動）をリストアップしたものである。ここで注意しなければならないのは、実施すべき管理活動を網羅したチェックリストではないということである。サイバーセキュリティ対策を実施する組織は、あくまでもこのリストをベースとして検討し、その組織にとって必要なサイバーセキュリティを見極めなければならない。

「コア」は、以下の 4 つの項目で構成されている。

1. Functions（ファンクション）
2. Categories（カテゴリー）
3. Subcategories（サブカテゴリー）
4. Informative References（参考リファレンス）

「ファンクション」とは、サイバーセキュリティに関するリスクマネジメントにおける PDCA サイクルを実施する上での全体の管理活動を以下の 5 つの活動に分類したものである。

1. IDENTIFY（特定）
2. PROTECT（保護）
3. DETECT（検知）
4. RESPOND（対応）
5. RECOVER（回復）

それぞれのファンクションにおいて、実施すべき管理活動を大きく分類したものが「カテゴリー」である。そして、そのカテゴリーにおおいて実施すべき管理活動をさらに細分類したものが「サブカテゴリー」である。サブカテゴリーのそれぞれには、「参考リファレンス」として、対応する従来からある IT 管理の標準規格がマッピングされている。また、ファンクション、カテゴリー、サブカテゴリーのそれぞれには、組織の内外でフレームワークに関するやりとりを円滑にするために、ID、AM、ID.AM-1 等の短縮形が定められている。

「特定」ファンクションでは、組織は、重要インフラ資産をたな卸し（AM）、組織が置かれるビジネス環境（BE）を理解したうえで、組織が定めているガバナンス要件や法令が定めるコンプライアンス要件に沿いながら（GV）、リスク評価を実施し（RA）、リスクへの対応を判断する（RS）。

「保護」ファンクションでは、組織は、「特定」ファンクションで特定した重要インフラ資産と関連するリスクを保護するための基盤を以下の 6 つ観点から構築する。

サブカテゴリー	活動内容
Access Control (AC)（アクセスコントロール）	情報と施設へのアクセスを承認されたユーザー、プロセス、デバイスと、承認された活動またはトランザクションに限定している。
Awareness and Training (AT)（アウェアネスとトレーニング）	組織の職員および提携してる企業に対して、定められた方針、手順、契約に合致した、情報セキュリティに関連する義務と責任を果たす上で十分なトレーニングを実施している。
Data Security (DS)（データセキュリティ）	情報と記録（データ）は、組織が、情報の機密性、信頼性、可用性を保護するために定めたリスク戦略に従って管理している。
Information Protection Processes and Procedures (IP)（インフォメーション・プロテクション・プロセスとプロシージャー）	セキュリティポリシー（目的、範囲、役割、責任、経営者のコミットメント、組織間の調整について定められていることが前提）、プロセス、プロシージャーを管理し、情報システムと資産の保護活動を管理するために活用している。
Maintenance (MA)（メンテナンス）	重要インフラと情報システムのコンポーネントの維持と補修を、方針やプロシージャーに従って実施している。
Protective Technology (PT)（プロテクティブ・テクノロジー）	方針、プロシージャー、契約と合致した、システムと資産のセキュリティと回復力を担保するために、技術的なセキュリティソリューションを管理している。

コアでは、「特定」ファンクションで特定した資産を、「保護」ファンクションで、サイバー攻撃等の脅威からの保護対策を実践する。「特定」ファンクションと「保護」ファンクションの管理活動の整理だけあれば、組織が、ISMS や Cobi 等（後述）の従来の標準規格をベースに情報セキュリティに関する管理活動を整理する場合と大差が無い。このフレームワークは、サイバーセキュリティに関する日々のオペレーションに関わる管理活動を切り出すことによって、フレームワークの目的である、サイバーセキュリティの管理を強調していることが独特である。

フレームワークでは、サイバー攻撃を「検知」する部分を一つのファンクションとして切り出し、検知したサイバーセキュリティ事象に「対応」と、サイバー攻撃により実際に被害・障害（インシデント）が発生した状態から「回復）」するための管理活動を、それぞれファンクションとして整理している。

例えば、日本の上場企業が内部統制監査制度（後述）に対応する場合、サイバーセキュリティの検知、対応、回復に関する管理活動を、監査対象として網羅しているケースは考えにくい。

ISMS や Cobit 等の標準規格であれば、「保護ファンクション」に該当する部分が、システム障害に対応する部分に組み込まれていると考えることができるが、これらの標準規格を運用する組織は、現状ではその障害の中にサイバーセキュリティ対策が含まれているとは理解しているものの、具体的な対策をマネジメントシステムの中に組み込んでいる組織は、まだごく一部であろう。例えば、フレームワークの「検知」ファンクションのサブカテゴリーに対応するためには、NICT が開発した対サイバー攻撃アラートシステ

ム「DAEDALUS（ダイダロス）」の様な、検知システム等によるサイバー攻撃のモニタリング活動を配置し、「対応」「回復」ファンクションにおいて、分析を実施しなければならない。

ただし、いずれのサブカテゴリーも必ず従来の標準規格を参照しており、全く新しく考えら得たものは無い。あくまでも、サイバーセキュリティの管理という観点で整理しなおしているということである。

4.3.1.1 ファンクション、カテゴリー、サブカテゴリー

ﾌｧﾝｸｼｮﾝ	カテゴリー	サブカテゴリー
IDENTIFY (ID)（特定）	**Asset Management (AM) （資産管理）** 組織が事業目的を達成することを可能にする、職員、デバイス、システム、施設を特定し、ビジネス目標と組織のリスク戦略に応じて管理している。	**ID.AM-1**: 物理的なデバイスとシステムのたな卸しを実施している。
		ID.AM-2: ソフトウェア・プラットフォームとアプリケーションのたな卸しを実施している。
		ID.AM-3: 通信の流れとデータの流れを可視化している。
		ID.AM-4: 外部の情報システムを可視化し、また一覧を作成している。
		ID.AM-5: ハードウェア、デバイス、データソフトウェアの分類、重要度、ビジネス上の価値によりリソースに優先順位をつけている。
		ID.AM-6: サイバーセキュリティを含むビジネスファンクションに関して、人員の役割と責任を定めている。
	Business Environment (BE) （ビジネス環境） 組織のミッション、目標、ステークホルダー、活動を理解し、優先順位をつけ、サイバーセキュリティ上の役割、責任、リスク判断を知らせる。	**ID.BE-1:** サプライチェーン上の組織の役割を特定し周知している。
		ID.BE-2: 重要インフラと所属する業界のエコシステム上の組織の位置づけを特定し周知している。
		ID.BE-3: 組織のミッション、目標、活動に関して、優先順位を特定している。
		ID.BE-4: 重要サービスを提供する上での依存関係と重要なファンクションを特定している。
		ID.BE-5: 重要サービスの提供を支援するために必要な回復力に関する要件を定めている。
	Governance (GV) （ガバナンス） 組織に対する規制、法律、リス	**ID.GV-1:** 組織の情報セキュリティポリシーを定めている。

ファンクション	カテゴリー	サブカテゴリー
	ク、環境、オペレーション上の要件を管理しモニタリングするための方針、プロシージャー、プロセスを理解し、サイバーセキュリティリスクを経営者に知らせている。	**ID.GV-2:** 情報セキュリティに関する役割と責任を調整し、整備している。
		ID.GV-3: プライバシーや自由人権に関する義務を含む、サイバーセキュリティに関する法律や規制上の要件を理解し、管理している。
		ID.GV-4: ガバナンスとリスクマネジメントプロセスがサイバーセキュリティリスクに対応している。
	Risk Assessment (RA) （リスク評価） 組織がオペレーション（ミッション、ファンクション、イメージ、レピュテーションを含む）、資産、所属する個人に対するサイバーセキュリティリスクを理解している。	**ID.RA-1:** 資産の脆弱性を特定し、文書化している。
		ID.RA-2: 情報共有フォーラム／ソースより、脅威と脆弱性に関する情報を入手している。
		ID.RA-3: 組織の資産に対する脅威を特定し、文書化している。
		ID.RA-4: 潜在的な影響を分析している。
		ID.RA-5: リスク対応を決定している。
	Risk Management Strategy (RM) （リスクマネジメント戦略）：組織の優先順位、制約、リスクトレランス、想定を確立し、オペレーション上のリスク判断の支援に利用している。	**ID.RM-1:** リスクマネジメントプロセスに関して合意し、そのプロセスを管理している。
		ID.RM-2: 組織のリスクトレランスを決定し、明確に伝えている。
		ID.RM-3: 重要インフラ上の役割と、その分野で要求されるリスク分析に応じて、組織が決定したリスクトレランスを周知している。
PROTECT (PR)（保護）	**Access Control (AC)（アクセスコントロール)** 情報と施設へのアクセスを承認されたユーザー、プロセス、デバイスと、承認された活動またはトランザクションに限定している。	**PR.AC-1:** 承認されたデバイスとユーザーのアイデンティティとクレデンシャルを管理している。
		PR.AC-2: リソースへの物理アクセスを管理し、セキュリティを確保している。
		PR.AC-3: リモートアクセスを管理している。
		PR.AC-4: アクセス権限を管理している。
		PR.AC-5: ネットワークの信頼性を保護している。
	Awareness and Training (AT)（アウェアネスとトレーニング) 組織の職員および提携しいてる企業に対して、定められた	**PR.AT-1:** 一般ユーザーに周知し、トレーニングを実施している。
		PR.AT-2: 特権ユーザーが役割と責任を理解している。

ファンクション	カテゴリー	サブカテゴリー
	方針、手順、契約に合致した、情報セキュリティに関連する義務と責任を果たす上で十分なトレーニングを実施している。	**PR.AT-3:** 外部関係者（サプライヤー、顧客、パートナー）が役割と責任を理解している。
		PR.AT-4: 経営幹部が役割と責任を理解している。
		PR.AT-5: 物理的セキュリティ担当者および情報セキュリティ担当者が役割と責任を理解している。
	Data Security (DS)（データセキュリティ） 情報と記録（データ）は、組織が、情報の機密性、信頼性、可用性を保護するために定めたリスク戦略に従って管理している。	**PR.DS-1:** Data-at-rest（保存データ）が保護されている。
		PR.DS-2: Data-in-motion（実行データ）の安全性を確保している。
		PR.DS-3: 資産を除去、移管、処分まで正式に管理している。
		PR.DS-4: 可用性を担保する上で十分な容量を維持している。
		PR.DS-5: データの漏洩対策を実施している。
		PR.DS-6: 知財を保護している。
		PR.DS-7: 不必要な資産は除去している。
		PR.DS-8: システム開発に用いるテスト環境は分離している。
		PR.DS-9: 個人のプライバシーと個人情報を保護している。
	Information Protection Processes and Procedures (IP)（情報保護プロセスとプロシージャー） セキュリティポリシー（目的、範囲、役割、責任、経営者のコミットメント、組織間の調整について定められていることが前提）、プロセス、プロシージャーを管理し、情報システムと資産の保護活動を管理するために活用している。	**PR.IP-1:** 情報技術とオペレーション技術に関してベースラインとなる設定を定めている。
		PR.IP-2: システムデベロップメントライフサイクルを導入している。
		PR.IP-3: 設定変更管理プロセスを導入している。
		PR.IP-4: 情報のバックアップの実施を管理している。
		PR.IP-5: 組織の資産の物理的なオペレーション環境に関するポリシーと規制が一致している。
		PR.IP-6: ポリシーと要件に従って、情報を破壊している。
		PR.IP-7: 保護プロセスを継続的に改善している。

ファンクション	カテゴリー	サブカテゴリー
		PR.IP-8: 適切な関係者と情報共有している。
		PR.IP-9: 対応計画（事業継続計画、災害復旧計画、インシデント対応計画）を施行し、管理している。
		PR.IP-10: 対策計画を実行している。
		PR.IP-11: 人事上の手順にサイバーセキュリティ（アカウントの解除、職員のスクリーニング、等）が含まれている。
	Maintenance (MA)（維持） 重要インフラと情報システムのコンポーネントの維持と補修を、方針やプロシージャーに従って実施している。	**PR.MA-1:** 承認され、管理されているツールを用いて維持・補修を実施し、適時に記録している。
		PR.MA-2: 不正アクセスを防ぎつつ、重要なオペレーションシステムや情報システムの可用性を支援するために、リモートメンテナンスを適時に承認、記録、実施している。
	Protective Technology (PT)（保護技術） 方針、プロシージャー、契約と合致した、システムと資産のセキュリティと回復力を担保するために、技術的なセキュリティソリューションを管理している。	**PR.PT-1:** 監査方針に基づいて、監査記録とログを保管している。
		PR.PT-2: 定めた方針に基づいて、リムーバルメディアを保護している。
		PR.PT-3: システムおよび資産へのアクセスを適切に管理している。
		PR.PT-4: 通信ネットワークの安全性を確保している。
		PR.PT-5: リスク分析に基づいて、機能が特化しているシステム（SCADA, ICS, DLS）を保護している。
DETECT (DE)（検知）	**Anomalies and Events (AE)（異常と事象）** 異常な活動を適時に検知し、事象の潜在的なインパクト（影響度）を理解している。	**DE.AE-1:** 通常のオペレーションとプロシージャーのベースラインを定め、管理している。
		DE.AE-2: 検知した事象は、攻撃の目標と手法を理解するために、分析している。
		DE.AE-3: サイバーセキュリティに関するデータ様々な異なる情報源の相関関係から導き出している。
		DE.AE-4: 潜在的なサイバーセキュリティ事象の影響度を判断している。

ファンクション	カテゴリー	サブカテゴリー
		DE.AE-05: 事象に対するアラートを立てる閾値を定めている。
	Security Continuous Monitoring (CM)（セキュリティの継続モニタリング） サイバーセキュリティ事象を特定し、保護対策の効果を検証するために、情報ステムと資産を監視している。	**DE.CM-1:** 潜在的なサイバーセキュリティ事象を検知するために、ネットワークを監視している。
		DE.CM-2: 潜在的なサイバーセキュリティ事象を検知するために、物理環境を監視している。
		DE.CM-3: 潜在的なサイバーセキュリティ事象を検知するために、職員の活動を監視している。
		DE.CM-4: 悪質なコードを検知している。
		DE.CM-5: 不正なモバイルコードを検知している。
		DE.CM-6: 外部サービスプロバイダーを監視している。
		DE.CM-7: 不正なリソースを監視している。
		DE.CM-8: 脆弱性評価を実施している。
	Detection Processes (DP)（検知プロセス） 異常な事象の適時かつ十分な認知を担保するために、検知プロセスとプロシージャーを維持し、テストしている。	**DE.DP-1:** アカウンタビリティを担保するために、検知に関する役割と責任を十分に定義している。
		DE.DP-2: 検知活動は、プライバシーと自由人権に関するものも含め、適用される要件を順守している。
		DE.DP-3: 備えを確固たるものとするのに十分な検知プロセスを実行している。
		DE.DP-4: 事象の検知情報を適切な関係者と共有している。
		DE.DP-5: 検知プロセスは、継続的に改善している。
RESPOND (RS)（対応）	**Response Planning (RP)（レスポンス・プランニング）** 異常な事象の適時かつ十分な認知を担保するために、検知プロセスとプロシージャーを維持し、テストしている。	**RS.PL-1:** 事象発生中または事後に対応計画を実行している。
	Communications (CO)（コミュニケーション） 対応活動を内外の関係者と調整している。これには、必要に応じて、連邦政府、州政府、警察から	**RS.CO-1:** 職員は、対応が必要とされる際の、責任とオペレーションの順番を認識している。
		RS.CO-2: 定めた基準に基づいて、事象を報告している。

ﾌｧﾝｸｼｮﾝ	カテゴリー	サブカテゴリー
	の支援を得る事も含む。	**RS.CO-3:** 対応計画に基づいて、プライバシーと自由人権に関する者も含め、検知と対応の情報（ブリーチ報告書、等）は共有している。
		RS.CO-4: 対応計画に基づいて、関係者と、プライバシーと自由人権に関する者も含め、調整している。
		RS.CO-5: 外部の関係者（ビジネスパートナー、情報共有分析センター、顧客、等）と、任意の調整をしている。
	Analysis (AN):（分析） 十分な対応を担保し、回復活動を支援するために、分析を実施している。	**RS.AN-1:** 検知システムから通知された内容を調査している。
		RS.AN-2: インシデントの影響度を理解している。
		RS.AN-3: フォレンジック（デジタルデータの保全・復元・解析[49]）を実施している。
		RS.AN-4: 対応計画に基づいて、インシデントを分類している。
	Mitigation (MI)（軽減） 事象の拡大を防ぐための活動を実施し、事象の影響を軽減し、インシデントを除去する。	**RS.MI-1:** インシデントを抑制している。
		RS.MI-2: インシデントを除去している。
	Improvements (IM)（改善） 現在および過去の検知および対応活動から得た教訓を生かすことによって、組織の対応活動を改善している。	**RS.IM-1:** 対応計画は教訓を生かしている。
		RS.IM-2: 対応戦略を更新している。
RECOVER (RC)（回復）	**Recovery Planning (RP)（回復計画）** サイバーセキュリティ事象から影響を受けたシステムまたは資産の適時回復を担保するために、回復プロセスとプロシージャーを維持し、テストしている。	**RC.RP-1:** 回復計画を施行している。
	Improvements (IM)（改善） 教訓を今後の活動に生かすことで、回復計画とプロセスを改善している。	**RC.IM-1:** 教訓を反映し、回復計画を更新している。
		RC.IM-2: 回復戦略を更新している。
	Communications (CO)（コミュニ	**RC.CO-1:** パブリックリレーションを管理している。

[49] KPMG FAS, http://fas-group.kpmg.or.jp/services/investigation-prevention-fraud/digital-forensic.html

ファンクション	カテゴリー	サブカテゴリー
	ケーション） 修復活動を、内部または、コーディネーションセンター、インターネットサービスプロバイダー、攻撃を受けているシステムのオーナー、被害者、他のCSIRT（シーサート[50]）組織、ベンダー等の外部と調整している。	**RC.CO-2:** 事象発生後の組織の評判を修復している。

4.3.1.2 参照リファレンス

「コア」の「参照リファレンス」で参照している標準規格は、以下の 5 つである。

- ISA 99.02.01
- COBIT
- NIST SP 800-53 Revision 4
- CCS CSC
- ISO/IEC 27001

ISA 99.02.01

国際計測制御学会（ISA: International Society of Automation）は、制御システムセキュリティに関して最も古くかつ活動的な組織であるが、その標準規格は、製造業に主に利用されている。IACS（Industrial Automation and Control Systems）、つまり制御システムのセキュリティ管理策の詳細として 99.02.01 - Establishing an IACS Security Program（IACS セキュリティプログラムの構築）を策定している[51]。

COBIT

COBITとは世界中の組織にITガバナンスのための明確な方針とより良い実務を提供するためにITカバナンスの枠組みと詳細なコントロール目標のガイドを示す一連の製品（資料やツール）[52]である。COBITはまた、米国における通称「企業改革法」（サーベンス・オクスリー法、SOX法、正式には、Public Company Accounting Reform and Investor Protection Act of 2002）のコンプライアンスのツールとして広く利用されている[53]他、日本でも 2006 年 6 月に成立した金融商品取引法で義務化された、財務報告に関する内部統制に関連し、経営者による評価・内部統制報告書の作成と監査人による監査証明[54]精度、内部統制報告制度（J-SOX）のツールとして多く利用されている。

---

[50] 「コンピュータセキュリティにかかるインシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動をする。」（独立行政法人情報処理推進機構）例：内閣官房情報セキュリティ推進室

[51] 「制御システムセキュリティガイドライン、標準及び認証への取組みに関する分析」、一般社団法人 JPCERT コーディネーションセンター、2009 年 11 月

[52] 日本ガバナンス協会、http://itgi.jp/cobit/faq.html

[53] ISACA

[54] あずさ監査法人、http://www.azsa.or.jp/knowledge/glossary/jsox.html

NIST SP 800-53 Revision 4

NISTが発行するSP800 シリーズは、コンピュータセキュリティ関係のレポートである。米国の政府機関がセキュリティ対策を実施する際に利用することを前提としてまとめられた文書で、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、インシデント対応など、セキュリティに関し、幅広く網羅しており、政府機関、民間企業を問わず、セキュリティ担当者にとって有益な文書である[55]。NIST SP 800-53 Revision 4 は、サイバー攻撃、自然災害、構造上の欠陥、作為または不作為のヒューマンエラー等、様々な脅威から、組織のオペレーション（ミッション、ファンクション、イメージ、レピュテーションを含む）、資産、個人、関連組織、および国家を保護するための、米国政府の情報システムと組織のセキュリティとプライバシーに関するコントロール（管理活動）と、管理活動を選択するプロセスのカタログ（可能な限り収集したもの）である[56]。

CCS CSC（Council on CyberSecurity (CCS) Top 20 Critical Security Controls (CSC)）

Council on CyberSecurity（サイバーセキュリティ評議会）は、開かれたインターネットの全世界レベルでのセキュリティにコミットする、専門家による独立した非営利団体（NPO）である[57]。サイバーセキュリティ評議会は、最も蔓延しているサイバー攻撃を阻止するために推奨される、20 の具体的かつ実践的な行動を集めた、最重要セキュリティコントロール集を定めている[58]。

ISO/IEC 27001

国際規格であるISO/IEC 27001 は、組織が情報セキュリティマネジメントシステム（ISMS）を構築するための要求事項をまとめた国際規格である[59]。また、ISMSの認証基準であり、ISMS適合性評価制度において、第三者である認証機関が本制度の認証を希望する組織の適合性を評価するための基準である。ISMSは、個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用することであり、組織が保護すべき情報資産について、機密性、完全性、可用性をバランス良く維持し改善することがを基本概念としている[60]。日本国内では、2013 年 11 月 29 日現在で 4,410 の組織が認証を受けている[61]。

サブカテゴリー	参考リファレンス

[55] 独立行政法人情報処理推進機構、
http://www.ipa.go.jp/security/publications/nist/nist_publications.html
[56] “ Security and Privacy Controls for Federal Information Systems and Organizations”, NIST SP 800-53 Rev.4, NIST, April 2013
[57] Council on CyberSecurity (CCS), http://www.counciloncybersecurity.org/about-us
[58] Council on CyberSecurity (CCS), http://www.counciloncybersecurity.org/practice-areas/technology
[59]一般財団法人日本情報社会推進協会（JIPDEC）、http://www.isms.jipdec.or.jp/about/index.html
[60] 一般財団法人日本情報社会推進協会（JIPDEC）、http://www.isms.jipdec.or.jp/isms/index.html
[61]一般財団法人日本情報社会推進協会（JIPDEC）、http://www.isms.jipdec.or.jp/lst/ind/suii.html

サブカテゴリー	参考リファレンス
ID.AM-1: 物理的なデバイスとシステムのたな卸しを実施している。	**• ISA 99.02.01 4.2.3.4** **• COBIT BAI03.04, BAI09.01, BAI09, BAI09.05** **• ISO/IEC 27001 A.7.1.1, A.7.1.2** **• NIST SP 800-53 Rev. 4 CM-8** **• CCS CSC1**
ID.AM-2: ソフトウェア・プラットフォームとアプリケーションのたな卸しを実施している。	**• ISA 99.02.01 4.2.3.4** **• COBIT BAI03.04, BAI09.01, BAI09, BAI09.05** **• ISO/IEC 27001 A.7.1.1, A.7.1.2** **• NIST SP 800-53 Rev. 4 CM-8** **• CCS CSC 2**
ID.AM-3: 通信の流れとデータの流れを可視化している。	**• ISA 99.02.01 4.2.3.4** **• COBIT DSS05.02** **• ISO/IEC 27001 A.7.1.1** **• NIST SP 800-53 Rev. 4 CA-3, CM-8, CA-9** **• CCS CSC 1**
ID.AM-4: 外部の情報システムを可視化し、また一覧を作成している。	**• NIST SP 500-291 3, 4** **• NIST SP 800-53 Rev. 4 AC-20, SA-9**
ID.AM-5: ハードウェア、デバイス、データソフトウェアの分類、重要度、ビジネス上の価値によりリソースに優先順位をつけている。	**• ISA 99.02.01 4.2.3.6** **• COBIT APO03.03, APO03.04, BAI09.02** **• NIST SP 800-53 Rev. 4 RA-2, CP-2** **• NIST SP 800-34 Rev 1** **• ISO/IEC 27001 A.7.2.1**
ID.AM-6: サイバーセキュリティを含むビジネスファンクションに関して、人員の役割と責任を定めている。	**• ISA 99.02.01 4.3.2.3.3** **• COBIT APO01.02, BAI01.12, DSS06.03** **• ISO/IEC 27001 A.8.1.1** **• NIST SP 800-53 Rev. 4 CP-2, PM-11** **• NIST SP 800-34 Rev 1**
ID.BE-1: サプライチェーン上の組織の役割を特定し周知している。	**• COBIT APO08.01, APO08.02, APO08.03, APO08.04, APO08.05, APO10.03, DSS01.02** **• ISO/IEC 27001 A.10.2** **• NIST SP 800-53 Rev. 4 CP-2**
ID.BE-2: 重要インフラと所属する業界のエコシステム上の組織の位置づけを特定し周知している。	**• COBIT APO02.06, APO03.01** **• NIST SP 800-53 Rev. 4 PM-8**
ID.BE-3: 組織のミッション、目標、活動に関して、優先順位を特定している。	**• ISA 99.02.01 4.2.2.1, 4.2.3.6** **• COBIT APO02.01, APO02.06, APO03.01** **• NIST SP 800-53 Rev. 4 PM-11**
ID.BE-4: 重要サービスを提供する上での依存関係と重要なファンクションを特定している。	**• COBIT DSS01.03** **• ISO/IEC 27001 9.2.2** **• NIST SP 800-53 Rev 4 CP-8, PE-9, PE-10, PE-11, PE-12, PE-14, PM-8**
ID.BE-5: 重要サービスの提供を支援するために必要な回復力に関する要件を定めている。	**• NIST SP 800-53 Rev. 4 CP-2, SA-14**

サブカテゴリー	参考リファレンス
ID.GV-1: 組織の情報セキュリティポリシーを定めている。	**• ISA 99.02.01 4.3.2.6** **• COBIT APO01.03, EA01.01** **• ISO/IEC 27001 A.6.1.1** **• NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)**
ID.GV-2: 情報セキュリティに関する役割と責任を調整し、整備している。	**• ISA 99.02.01 4.3.2.3.3** **• ISO/IEC 27001 A.6.1.3** **• NIST SP 800-53 Rev. 4 AC-21, PM-1, PS-7**
ID.GV-3: プライバシーや自由人権に関する義務を含む、サイバーセキュリティに関する法律や規制上の要件を理解し、管理している。	**• ISA 99.02.01 4.4.3.7** **• COBIT MEA03.01, MEA03.04** **• ISO/IEC 27001 A.15.1.1** **• NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)**
ID.GV-4: ガバナンスとリスクマネジメントプロセスがサイバーセキュリティリスクに対応している。	**• NIST SP 800-53 Rev. 4 PM-9, PM-11**
ID.RA-1: 資産の脆弱性を特定し、文書化している。	**• ISA 99.02.01 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12** **• COBIT APO12.01, APO12.02, APO12.03, APO12.04** **• ISO/IEC 27001 A.6.2.1, A.6.2.2, A.6.2.3** **• CCS CSC4** **• NIST SP 800-53 Rev. 4 CA-2, RA-3, RA-5, SI-5**
ID.RA-2: 情報共有フォーラム／ソースより、脅威と脆弱性に関する情報を入手している。	**• ISA 99.02.01 4.2.3, 4.2.3.9, 4.2.3.12** **• ISO/IEC 27001 A.13.1.2** **• NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5**
ID.RA-3: 組織の資産に対する脅威を特定し、文書化している。	**• ISA 99.02.01 4.2.3, 4.2.3.9, 4.2.3.12** **• COBIT APO12.01, APO12.02, APO12.03, APO12.04** **• NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-16**
ID.RA-4: 潜在的な影響を分析している。	**• ISA 99.02.01 4.2.3, 4.2.3.9, 4.2.3.12** **• NIST SP 800-53 Rev. 4 RA-3**
ID.RA-5: リスク対応を決定している。	**• NIST SP 800-53 Rev. 4 PM-9**
ID.RM-1: リスクマネジメントプロセスに関して合意し、そのプロセスを管理している。	**• ISA 99.02.01 4.3.4.2** **• COBIT APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02** **• NIST SP 800-53 Rev. 4 PM-9** **• NIST SP 800-39**
ID.RM-2: 組織のリスクトレランスを決定し、明確に伝えている。	**• ISA 99.02.01 4.3.2.6.5** **• COBIT APO10.04, APO10.05, APO12.06** **• NIST SP 800-53 Rev. 4 PM-9** **• NIST SP 800-39**
ID.RM-3: 重要インフラ上の役割と、その分野で要求されるリスク分析に応じて、組織が決定したリスクトレランスを周知している。	**• NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11**

サブカテゴリー	参考リファレンス
PR.AC-1: 承認されたデバイスとユーザーのアイデンティティとクレデンシャルを管理している。	**• ISA 99.02.01 4.3.3.5.1** **• COBIT DSS05.04, DSS06.03** **• ISO/IEC 27001 A.11** **• NIST SP 800-53 Rev. 4 AC-2, AC-5, AC-6, IA Family** **• CCS CSC 16**
PR.AC-2: リソースへの物理アクセスを管理し、セキュリティを確保している。	**• ISA 99.02.01 4.3.3.3.2, 4.3.3.3.8** **• COBIT DSS01.04, DSS05.05** **• ISO/IEC 27001 A.9.1, A.9.2, A.11.4, A.11.6** **• NIST SP 800-53 Rev 4 PE-2, PE-3, PE-4, PE-6, PE-9**
PR.AC-3: リモートアクセスを管理している。	**• ISA 99.02.01 4.3.3.6.6** **• COBIT APO13.01, DSS01.04, DSS05.03** **• ISO/IEC 27001 A.11.4, A.11.7** **• NIST SP 800-53 Rev. 4 AC 17, AC-19, AC-20**
PR.AC-4: アクセス権限を管理している。	**• ISA 99.02.01 4.3.3.7.3** **• ISO/IEC 27001 A.11.1.1** **• NIST SP 800-53 Rev. 4 AC-3, AC-4, AC-6, AC-16** **• CCS CSC 12, 15**
PR.AC-5: ネットワークの信頼性を保護している。	**• ISA 99.02.01 4.3.3.4** **• ISO/IEC 27001 A.10.1.4, A.11.4.5** **• NIST SP 800-53 Rev 4 AC-4**
PR.AT-1: 一般ユーザーに周知し、トレーニングを実施している。	**• ISA 99.02.01 4.3.2.4.2** **• COBIT APO07.03, BAI05.07** **• ISO/IEC 27001 A.8.2.2** **• NIST SP 800-53 Rev. 4 AT-2** **• CCS CSC 9**
PR.AT-2: 特権ユーザーが役割と責任を理解している。	**• ISA 99.02.01 4.3.2.4.2, 4.3.2.4.3** **• COBIT APO07.02** **• ISO/IEC 27001 A.8.2.2** **• NIST SP 800-53 Rev. 4 AT-3** **• CCS CSC 9**
PR.AT-3: 外部関係者（サプライヤー、顧客、パートナー）が役割と責任を理解している。	**• ISA 99.02.01 4.3.2.4.2** **• COBIT APO07.03, APO10.04, APO10.05** **• ISO/IEC 27001 A.8.2.2** **• NIST SP 800-53 Rev. 4 AT-3** **• CCS CSC 9**
PR.AT-4: 経営幹部が役割と責任を理解している。	**• ISA 99.02.01 4.3.2.4.2** **• COBIT APO07.03** **• ISO/IEC 27001 A.8.2.2** **• NIST SP 800-53 Rev. 4 AT-3** **• CCS CSC 9**
PR.AT-5: 物理的セキュリティ担当者および情報セキュリティ担当者が役割と責任を理解している。	**• ISA 99.02.01 4.3.2.4.2** **• COBIT APO07.03** **• ISO/IEC 27001 A.8.2.2** **• NIST SP 800-53 Rev. 4 AT-3** **• CCS CSC 9**

サブカテゴリー	参考リファレンス
PR.DS-1: Data-at-rest（保存データ）が保護されている。	**• COBIT APO01.06, BAI02.01, BAI06.01, DSS06.06** **• ISO/IEC 27001 A.15.1.3, A.15.1.4** **• CCS CSC 17** **• NIST SP 800-53 Rev 4 SC-28**
PR.DS-2: Data-in-motion（実行データ）の安全性を確保している。	**• COBIT APO01.06, BAI02.01, BAI06.01, DSS06.06** **• ISO/IEC 27001 A.10.8.3** **• NIST SP 800-53 Rev. 4 SC-8** **• CCS CSC 17**
PR.DS-3: 資産を除去、移管、処分まで正式に管理している。	**• COBIT BAI09.03** **• ISO/IEC 27001 A.9.2.7, A.10.7.2** **• NIST SP 800-53 Rev 4 PE-16, MP-6, DM-2**
PR.DS-4: 可用性を担保する上で十分な容量を維持している。	**• COBIT APO13.01** **• ISO/IEC 27001 A.10.3.1** **• NIST SP 800-53 Rev 4 CP-2, SC-5**
PR.DS-5: データの漏洩対策を実施している。	**• COBIT APO01.06** **• ISO/IEC 27001 A.12.5.4** **• CCS CSC 17** **• NIST SP 800-53 Rev 4 AC-4, PE-19, SC-13, SI-4, SC-7, SC-8, SC-31, AC-5, AC-6, PS-6**
PR.DS-6: 知財を保護している。	**• COBIT APO01.03, APO10.02, APO10.04, MEA03.01**
PR.DS-7: 不必要な資産は除去している。	**• COBIT BAI06.01, BAI01.10** **• ISO/IEC 27001 A.10.1.3** **• NIST SP 800-53 Rev. 4 AC-5, AC-6**
PR.DS-8: システム開発に用いるテスト環境は分離している。	**• COBIT BAI07.04** **• ISO/IEC 27001 A.10.1.4** **• NIST SP 800-53 Rev. 4 CM-2**
PR.DS-9: 個人のプライバシーと個人情報を保護している。	**• COBIT BAI07.04, DSS06.03, MEA03.01** **• ISO/IEC 27001 A.15.1.3** **• NIST SP 800-53 Rev 4, Appendix J**
PR.IP-1: 情報技術とオペレーション技術に関してベースラインとなる設定を定めている。	**• ISA 99.02.01 4.3.4.3.2, 4.3.4.3.3** **• COBIT BAI10.01, BAI10.02, BAI10.03, BAI10.05** **• NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-7, CM-9, SA-10** **• CCS CSC 3, 10**
PR.IP-2: システムデベロップメントライフサイクルを導入している。	**• ISA 99.02.01 4.3.4.3.3** **• COBIT APO13.01** **• ISO/IEC 27001 A.12.5.5** **• NIST SP 800-53 Rev 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-15, SA-17, PL-8** **• CCS CSC 6**
PR.IP-3: 設定変更管理プロセスを導入している。	**• ISA 99.02.01 4.3.4.3.2, 4.3.4.3.3** **• COBIT BAI06.01, BAI01.06** **• ISO/IEC 27001 A.10.1.2** **• NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10**
PR.IP-4: 情報のバックアップの実施を管理している。	**• ISA 99.02.01 4.3.4.3.9** **• COBIT APO13.01** **• ISO/IEC 27001 A.10.5.1** **• NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9**

サブカテゴリー	参考リファレンス
PR.IP-5: 組織の資産の物理的なオペレーション環境に関するポリシーと規制が一致している。	**• COBIT DSS01.04, DSS05.05** **• ISO/IEC 27001 9.1.4** **• NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18**
PR.IP-6: ポリシーと要件に従って、情報を破壊している。	**• COBIT BAI09.03** **• ISO/IEC 27001 9.2.6** **• NIST SP 800-53 Rev 4 MP-6**
PR.IP-7: 保護プロセスを継続的に改善している。	**• COBIT APO11.06, DSS04.05** **• NIST SP 800-53 Rev 4 PM-6, CA-2, CA-7, CP-2, IR-8, PL-2**
PR.IP-8: 適切な関係者と情報共有している。	**• ISO/IEC 27001 A.10** **• NIST SP 800-53 Rev. 4 AC-21**
PR.IP-9: 対応計画（事業継続計画、災害復旧計画、インシデント対応計画）を施行し、管理している。	**• COBIT DSS04.03** **• ISO/IEC 27001 A.14.1** **• NIST SP 800-53 Rev. 4 CP-2, IR-8**
PR.IP-10: 対策計画を実行している。	**• NIST SP 800-53 Rev.4 IR-3**
PR.IP-11: 人事上の手順にサイバーセキュリティ（アカウントの解除、職員のスクリーニング、等）が含まれている。	**• COBIT APO07.01, APO07.02, APO07.03, APO07.04, APO07.05** **• ISO/IEC 27001 8.2.3, 8.3.1** **• NIST SP 800-53 Rev 4 PS Family**
PR.MA-1: 承認され、管理されているツールを用いて維持・補修を実施し、適時に記録している。	**• ISO/IEC 27001 A.9.1.1, A.9.2.4, A.10.4.1** **• NIST SP 800-53 Rev 4 MA-2, MA-3, MA-5**
PR.MA-2: 不正アクセスを防ぎつつ、重要なオペレーションシステムや情報システムの可用性を支援するために、リモートメンテナンスを適時に承認、記録、実施している。	**• COBIT 5** **• ISO/IEC 27001 A.9.2.4, A.11.4.4** **• NIST SP 800-53 Rev 4 MA-4**
PR.PT-1: 監査方針に基づいて、監査記録とログを保管している。	**• ISA 99.02.01 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4** **• COBIT APO11.04** **• ISO/IEC 27001 A.10.10.1, A.10.10.3, A.10.10.4, A.10.10.5, A.15.3.1** **• NIST SP 800-53 Rev. 4 AU Family** **• CCS CSC 14**
PR.PT-2: 定めた方針に基づいて、リムーバルメディアを保護している。	**• COBIT DSS05.02, APO13.01** **• ISO/IEC 27001 A.10.7** **• NIST SP 800-53 Rev. 4 AC-19, MP-2, MP-4, MP-5, MP-7**
PR.PT-3: システムおよび資産へのアクセスを適切に管理している。	**• CCS CSC 6** **• COBIT DSS05.02** **• NIST SP 800-53 Rev 4 CM-7**
PR.PT-4: 通信ネットワークの安全性を確保している。	**• COBIT DSS05.02, APO13.01** **• ISO/IEC 27001 10.10.2** **• NIST SP 800-53 Rev 4 AC-18** **• CCS CSC 7**

サブカテゴリー	参考リファレンス
PR.PT-5: リスク分析に基づいて、機能が特化しているシステム（SCADA, ICS, DLS）を保護している。	**• COBIT APO13.01,** **• NIST SP 800-53 Rev 4**
DE.AE-1: 通常のオペレーションとプロシージャーのベースラインを定め、管理している。	**• ISA 99.02.01 4.4.3.3** **• COBIT DSS03.01** **• NIST SP 800-53 Rev. 4 AC-2, SI-3, SI-4, AT-3, CM-2**
DE.AE-2: 検知した事象は、攻撃の目標と手法を理解するために、分析している。	**• NIST SP 800-53 Rev. 4 SI-4, IR-4**
DE.AE-3: サイバーセキュリティに関するデータ様々な異なる情報源の相関関係から導き出している。	**• NIST SP 800-53 Rev. 4 SI-4**
DE.AE-4: 潜在的なサイバーセキュリティ事象の影響度を判断している。	**• NIST SP 800-53 Rev. 4 IR-4, SI -4**
DE.AE-05: 事象に対するアラートを立てる閾値を定めている。	**• ISA 99.02.01 4.2.3.10** **• NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-9** **• NIST SP 800-61 Rev 2**
DE.CM-1: 潜在的なサイバーセキュリティ事象を検知するために、ネットワークを監視している。	**• COBIT DSS05.07** **• ISO/IEC 27001 A.10.10.2, A.10.10.4, A.10.10.5** **• NIST SP 800-53 Rev. 4 CM-3, CA-7, AC-2, IR-5, SC-5, SI-4** **• CCS CSC 14, 16**
DE.CM-2: 潜在的なサイバーセキュリティ事象を検知するために、物理環境を監視している。	**• NIST SP 800-53 Rev. 4 CM-3, CA-7, IR-5, PE-3, PE-6, PE-20**
DE.CM-3: 潜在的なサイバーセキュリティ事象を検知するために、職員の活動を監視している。	**• NIST SP 800-53 Rev. 4 AC-2, CM-3, CA-7**
DE.CM-4: 悪質なコードを検知している。	**• COBIT DSS05.01** **• ISO/IEC 27001 A.10.4.1** **• NIST SP 800-53 Rev 4 SI-3** **• CCS CSC 5**
DE.CM-5: 不正なモバイルコードを検知している。	**• ISO/IEC 27001 A.10.4.2** **• NIST SP 800-53 Rev 4 SC-18**
DE.CM-6: 外部サービスプロバイダーを監視している。	**• ISO/IEC 27001 A.10.2.2** **• NIST SP 800-53 Rev 4 CA-7, PS-7, SI-4, SA-4, SA-9**
DE.CM-7: 不正なリソースを監視している。	**• NIST SP 800-53 Rev. 4 CM-3, CA-7, PE-3, PE-6, PE-20, SI-4**
DE.CM-8: 脆弱性評価を実施している。	**• NIST SP 800-53 Rev. 4 CM-3, CA-7, CA-8, RA-5, SA-11, SA-12**

サブカテゴリー	参考リファレンス
DE.DP-1: アカウンタビリティを担保するために、検知に関する役割と責任を十分に定義している。	**• ISA 99.02.01 4.4.3.1** **• COBIT DSS05.01** **• NIST SP 800-53 Rev 4 IR-2, IR-4, IR-8** **• CCS CSC 5**
DE.DP-2: 検知活動は、プライバシーと自由人権に関するものも含め、適用される要件を順守している。	**• ISA 99.02.01 4.4.3.2** **• NIST SP 800-53 Rev 4 CA-2, CA-7**
DE.DP-3: 備えを確固たるものとするのに十分な検知プロセスを実行している。	**• ISA 99.02.01 4.4.3.2** **• NIST SP 800-53 Rev 4 PM-14**
DE.DP-4: 事象の検知情報を適切な関係者と共有している。	**• NIST SP 800-53 Rev. 4 CP-2, IR-8**
DE.DP-5: 検知プロセスは、継続的に改善している。	**• COBIT APO11.06, DSS04.05** **• NIST SP 800-53 Rev 4 PM-6, CA-2, CA-7, CP-2, IR-8, PL-2**
RS.PL-1: 事象発生中または事後に対応計画を実行している。	**• ISA 99.02.01 4.3.4.5.1** **• NIST SP 800-53 Rev. 4 CP-10, IR-4** **• CCS CSC 18**
RS.CO-1: 職員は、対応が必要とされる際の、責任とオペレーションの順番を認識している。	**• ISO/IEC 27001 A.13.2.1** **• ISA 99.02.01 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4** **• NIST SP 800-53 Rev 4 CP-2, IR-8**
RS.CO-2: 定めた基準に基づいて、事象を報告している。	**• ISO/IEC 27001 A.13.1.1, A.13.1.2** **• ISA 99.02.01 4.3.4.5.5** **• NIST SP 800-53 Rev 4 IR-6, IR-8**
RS.CO-3: 対応計画に基づいて、プライバシーと自由人権に関する者も含め、検知と対応の情報（ブリーチ報告書、等）は共有している。	**• ISO/IEC 27001 A.10**
RS.CO-4: 対応計画に基づいて、関係者と、プライバシーと自由人権に関する者も含め、調整している。	**• ISO/IEC 27001 A.8.1.1, A.6.1.2, A.6.1.6, A.10.8.2** **• NIST SP 800-53 Rev. 4 CP-2, IR-8**
RS.CO-5: 外部の関係者（ビジネスパートナー、情報共有分析センター、顧客、等）と、任意の調整をしている。	**• NIST SP 800-53 Rev. 4 PM-15, SI-5**
RS.AN-1: 検知システムから通知された内容を調査している。	**• ISO/IEC 27001 A.6.2.1** **• NIST SP 800-53 Rev. 4 IR-4, IR-5, PE-6, SI-4, AU-13**
RS.AN-2: インシデントの影響度を理解している。	**• ISO/IEC 27001 A.6.2.1** **• NIST SP 800-53 Rev. 4 CP-10, IR-4**
RS.AN-3: フォレンジックを実施している。	**• ISO/IEC 27001 A.13.2.2, A.13.2.3** **• NIST SP 800-53 Rev. 4 IR-4**

サブカテゴリー	参考リファレンス
RS.AN-4: 対応計画に基づいて、インシデントを分類している。	**• ISO/IEC 27001 A.13.2.2** **• ISA 99.02.01 4.3.4.5.6** **• NIST SP 800-53 Rev. 4 IR-4**
RS.MI-1: インシデントを抑制している。	**• ISO/IEC 27001 A.3.6, A.13.2.3** **• ISA 99.02.01 4.3.4.5.6** **• NIST SP 800-53 Rev. 4 IR-4**
RS.MI-2: インシデントを除去している。	**• ISA 99.02.01 4.3.4.5.6, 4.3.4.5.10** **• NIST SP 800-53 Rev. 4 IR-4**
RS.IM-1: 対応計画は教訓を生かしている。	**• ISO/IEC 27001 A.13.2.2** **• ISA 99.02.01 4.3.4.5.10, 4.4.3.4** **• NIST SP 800-53 Rev. 4 CP-2, IR-8**
RS.IM-2: 対応戦略を更新している。	**• NIST SP 800-53 Rev. 4 CP-2, IR-8**
RC.RP-1: 回復計画を施行している。	**• COBIT DSS02.05, DSS03.04** **• ISO/IEC 27001 A.14.1.3, A.14.1.4, A.14.1.5** **• NIST SP 800-53 Rev. 4 CP-10, CP-2** **• CCS CSC 8**
RC.IM-1: 教訓を反映し、回復計画を更新している。	**• ISA 99.02.01 4.4.3.4** **• COBIT BAI05.07** **• ISO/IEC 27001 13.2.2** **• NIST SP 800-53 Rev. 4 CP-2**
RC.IM-2: 回復戦略を更新している。	**• COBIT APO05.04, BAI07.08** **• NIST SP 800-53 Rev. 4 CP-2**
RC.CO-1: パブリックリレーションを管理している。	**• COBIT MEA03.02** **• NIST SP 800-53 Rev. 4 IR-4, IR-8**
RC.CO-2: 事象発生後の組織の評判を修復している。	**• COBIT MEA03.02**

4.3.1.3 Appendix B「Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program（サイバーセキュリティプログラムにおけるプライバシーおよび自由人権を保護する手法）」

大統領令のセクション 5 に応じてフレームワークの Appendix B（付録 B）として提示されたプライバシー問題の解決策は、この大統領令の目玉である。付録 B は、サイバーセキュリティ対策活動の開発周辺や個人情報保護の観点から、プライバシーと自由人権に関する懸念に対処するための手法をまとめたものである。このプライバシー対策手法は、大統領令に定められているとおり、FIPP に基づいている。付録 B では、コアで特定した管理活動ごとに、実施する際に考慮すべき個人情報および自由人権を保護するための手法をまとめている。

また、「コア」と同様に、Appendix Bにも、「参照リファレンス」が記載されている。組織が個人情報に関連するプライバシー保護要件を定義することを助けることを意図して作成された国際標準規格であるISO/IEC 29100 も一部参照しているが、原則、NIST SP 800-53 Rev.4 Appendix J（付録J）をベースに作成されていることは、全てのカテゴリーに

おける個人情報および自由人権を保護するための手法が、同標準規格を参照していることからも明らかである。付録Jは、Revision 4（第 4 回改訂版）から新たに追加されたものであり、政府機関がプライバシーのニーズに対処するために、主に以下を実現することを目的としている[62]。

- 組織が、連邦法、大統領令、ディレクティブ、インストラクション、規制、政策、標準規格、ガイダンス、および組織特有の問題に対処するための取決めを遵守するための、系統立てた、ベストプラクティスに基づくプライバシーコントロール集の提供
- 遵守すべきプライバシーとセキュリティの要件を強制するための、プライバシーとセキュリティコントロールとの接続・連携の確立
- 政府内のプライバシーおよびセキュリティ担当者の協力の促進

ﾌｧﾝｸｼｮﾝ	カテゴリー	手法
IDENTIFY (ID)（特定）	**Asset Management (AM)（資産管理）**	組織が処理または分析に用いた個人情報、または、保持しないとしても組織のシステムを通過した個人情報を含め、従業員、顧客、その他、サイバーセキュリティプロシージャーの影響を受ける、またはプロシージャーに結びついている可能性のある個人情報のたな卸しを実施する。
	Business Environment (BE)（ビジネス環境）	なし
	Governance (GV)（ガバナンス）	憲法を含め、以下に対する、契約、規制、法律上の要件を特定する。 1. 「資産管理」カテゴリーで、特定された個人情報 2. Electric Communication Privacy Act（電子通信プライバシー法）やその他、考慮すべき自由人権等、電子通信の傍受、保護活動に関連するサイバーセキュリティ対策

[62] “ Security and Privacy Controls for Federal Information Systems and Organizations”, NIST SP 800-53 Rev.4, NIST, April 2013

ファンクション	カテゴリー	手法
		「資産管理」カテゴリーで、特定した個人情報に関してプライバシーまたは個人情報管理方法を定めているポリシーとプロシージャーを特定している。組織のサイバーセキュリティプロシージャーに関連し、そのポリシーとプロシージャーが、以下を提供しているかどうか、または、どの状況において提供しているかについて評価する。 1. 個人情報の収集、利用、配布、保持に関して、また、個人情報の利用における、適切なアクセス、収集、補償の仕組みに関して、影響を受ける個人に通知し、合意を得ている。 2. 個人情報を利用する目的を明確に伝えている。 3. 個人情報の収集が直接関連し、特定の目的の達成に必要であり、個人情報は、その目的の達成に必要かつ許可された期間のみ保持している。 4. 個人情報の利用は特定の目的にのみ使用され、個人情報は、個人情報の収集目的に合致した目的においてのみ共有されている。 5. 可能な限り、個人情報が、正確かつ関連性のあるもので、また適時かつ完全なものであることを担保している。
	Risk Assessment (RA) （リスク評価）	資産としての個人情報周辺の、脅威と脆弱性の有無を特定する。例えば、個人情報は、主要な商品価値のあるものとして、または、組織の他の資産にアクセスするために、狙われる。
	Risk Management Strategy (RM) （リスクマネジメント戦略）	「ガバナンス」カテゴリーで特定した、特定の目的にのみ個人情報を利用するプロセスを組織のリスクマネジメント戦略の一部となっているか判断する
PROTECT (PR)（保護）	**Access Control (AC)（アクセスコントロール）**	アプリケーション、サービス、施設へのアクセスする上で必要な、個人情報の利用と開示を、最低限にする。
	Awareness and Training (AT)（アウェアネスとトレーニング）	• 経営幹部をサポートすることは、プライバシーと市民お自由を尊重するサイバーセキュリティ文化を醸成する上で、非常に重要である。 • 特定の責任者に、プライバシーと自由人権に関するサイバーセキュリティ活動の影響を最小限にするための、プライバシーポリシーとプロシージャーを監督する責任を、持たせる。 • そのポリシーとプロシージャーに関して、職員および委託業者に対して定期的なトレーニングを実施する。 • ユーザーに、ユーザー自身の個人情報と通信内容を保護するステップを認識させ、プライバシーへの影響とセキュリティ対策周辺のトランペアレンシーを向上させる。
	Data Security (DS)（データセキュリティ）	組織の個人情報ライフサイクルの全ての段階に適切なセーフガードを導入し、喪失、盗難、不正アクセス、獲得、開示、コピー、使用、または改ざんを防止するため、個人情報のセンシティビティーに合わせる。

ファンクション	カテゴリー	手法
	Information Protection Processes and Procedures (IP)（情報保護プロセスとプロシージャー）。	不要になった個人情報は、安全に廃棄、ディ・アイデンティファイ（ID の末梢等）、匿名化する。 保持している個人情報は、保持する必要があるかどうかを、定期的に監査する。 インシデント発生中や、法律に基づいて警察や政府機関の捜査に協力する際に、適切にデータと通信を保護するための、ポリシーとプロシージャーを施行する。
	Maintenance (MA)（維持）	なし
	Protective Technology (PT)（保護技術）	• 個人情報を含むデータベースへのアクセスを監査する。 • 独立監査業務の一部として、個人情報のログを取得していないかどうか、また、サイバーセキュリティ活動を効果的に実施しながら、どの様にその個人情報を最小限にしているかを考慮する。
DETECT (DE)（検知）	**Anomalies and Events (AE)（異常と事象）**	• 異常または事象を検知している場合、サイバーセキュリティ事象の検知に不要な個人情報および通信内容の、収集または保持を最小限にするために、検知の範囲とフィルタリングの手法を、定期的に見直す。 • 収集、使用、開示、保持する個人情報が、正確かつ完全であるようにするための、ポリシーを定める。
	Security Continuous Monitoring (CM)（セキュリティの継続モニタリング）	• 個人または個人情報に関わるモニタリングを実施する場合、定期的にプロシージャーの効果を評価し、モニタリング範囲を最小限にし、侵害を最小限にする。 • 業務をトランスペアレントにする。
	Detection Processes (DP)（検知プロセス）	プライバシー担当者がコンプライアンスと検知活動の強制ポリシーのレビューに関与するように調整するためのプロセスを定める。
RESPOND (RS)（対応）	**Response Planning (RP)（レスポンス・プランニング）**	• 個人情報にリスクが生じていインシデントと、組織がインシデントを解決するために個人情報を使う場合とを、区別する。 • 組織は、その違いに応じて、対応計画に異なる手順を用いる必要がある。 • 例えば、個人情報にリスクが生じている場合、組織はどのセキュリティ活動を実施するか検討しなければならないが、個人情報を対応に利用する場合、個人のプライバシーまたは自由人権を保護するために、どの様に個人情報の利用を最小限にするかを考慮しなければならない。
	Communications (CO)（コミュニケーション）	• 個人情報の侵害を報告しなければならい法律上の義務を理解する。 • 任意でサイバーセキュリティ・インシデントの情報を共有する場合、個人情報または通信内容の開示を、インシデントの軽減または説明に必要な範囲に限定する。

ﾌｧﾝｸｼｮﾝ	カテゴリー	手法
	Analysis (AN):（分析）	• フォレンジックを実施する場合、調査に必要な個人情報または通信内容のみを保持する。 • 収集、使用、開示、保持する個人情報が、正確かつ完全であるようにするための、ポリシーを定める。
	Mitigation (MI)（軽減）	• インシデントを抑制する手法を検討する場合、中でも特に公共通信やデータ伝送システムの遮断を伴う手法を検討する場合、個人のプライバシーと自由人権への影響を評価する。 • その様な手法はトランスペアレントにする。
	Improvements (IM)（改善）	個人情報が関与するインシデントへの対応手順の改善を検討する場合、個人情報にリスクが生じていインシデントと、組織がインシデントを解決するために個人情報を使う場合、または、実行した対応計画がプライバシーまたは自由人権に影響する可能性がある場合とを、区別する。
RECOVER (RC)（回復）	**Recovery Planning (RP)（回復計画）**	• 個人情報にリスクが生じていインシデントと、組織がインシデントを解決するために個人情報を使う場合とを、区別する。 • 組織は、その違いに応じて、回復計画に異なる手順を用いる必要がある。 • 例えば、個人情報にリスクが生じている場合、組織はどのセキュリティ活動を実施するか検討しなければならないが、個人情報を回復に利用する場合、個人のプライバシーまたは自由人権を保護するために、どの様に個人情報の利用を最小限にするかを考慮しなければならない。
	Improvements (IM)（改善）	個人情報が関与するインシデントからの回復手順の改善を検討する場合、個人情報にリスクが生じていインシデントと、組織がインシデントを解決するために個人情報を使う場合、または、実行した対応計画がプライバシーまたは自由人権に影響する可能性がある場合とを、区別する。
	Communications (CO)（コミュニケーション）	影響を受けた個人、関係者、または一般大衆の信頼を、維持または再構築するために、インシデントとリスクの軽減戦略の一部として、個人情報の利用と開示についてのコミュニケーションを実施する。

4.3.2 プロファイル

フレームワークでは、「プロファイル」を「サイバーセキュリティのレベルを把握し改善するためのツール」と定義しているが、ツールと言うよりは、フレームワークを利用して、サイバーセキュリティ対策を実施する際の手順に関する用語であると捉えた方が理解しやすい。プロファイルは、組織のサイバーセキュリティ対策の状況を「コア」に照らし合わせて測ったものであり、組織の現状を組織の目標を示す以下の 2 つに分類される。

- Currnet Profile（現状プロファイル）：組織のサイバーセキュリティの現状
- Target Profile（目標プロファイル）：組織が目指すサイバーセキュリティの状態

また、フレームワークでは、プロファイルのテンプレートは提供しないため、フレームワークを実践する組織は、「コア」をベースとして、組織の現状を把握し、また目標を設定しなければならない。また、プロファイルは、重要インフラサービスを提供するパートナー間での共通言語として機能することを想定している。以下は、その例である。

- 目標プロファイルを、外部委託業者（例えばクラウドサービス）にデータを受け渡す際の要件として利用する。
- 現状プロファイルを、調達要件に対する報告・比較に利用する。
- 重要インフラ事業者が、依存する外部パートナーに対して、目標プロファイルを利用して、達成されるべきサイバーセキュリティ統制の大分類、小分類を周知する。
- 重要インフラセクターが、目標プロファイルを利用して、ベースラインを設定する。

4.3.3 ティアー

フレームワークでは、「ティアー」組織がどのようにサイバーセキュリティリスクを管理するか（しているか）を表す区分として定めている。組織は、望むティアーを決めなければならないが、選択するティアーは、組織のゴールを満たし、重要インフラのサイバーセキュリティのリスクを軽減し、また実施可能かつ費用対効果が見合っているものでなければならない。ティアーはまた、組織のサイバーセキュリティ対策の成熟度を表すことにもなる。

ティアー	リスク管理プロセス	統合プログラム	外部との連携
Partial（部分的に対応している）	• 正式ではない。 • サイバーセキュリティ対策が優先順位に組み込まれていない。	• リスクの全社的な認識度：Δ • 全社的なリスク管理プロセス：× • リスクインフォームド：× • サイバーセキュリティ情報の社内での共有：×	連携していない。

ティアー	リスク管理プロセス	統合プログラム	外部との連携
Risk-Informed（リスク情報を活用している）	経営層が承認しているが全社的なポリシーになっていない。	• リスクの全社的な認識度：o • 全社的なリスク管理プロセス：× • リスクインフォームド：o（リソースも十分） • サイバーセキュリティ情報の社内での共有：Δ	連携しているが正式ではない。
Risk-Informed and Repeatable（リスク情報を継続的に活用している）	• 正式に承認され、全社的なポリシーに組み込まれている。 • サイバーセキュリティ対策は、リスク管理プロセスにより定期的に更新されている。	• リスクの全社的な認識度：o • 全社的なリスク管理プロセス：o • リスクインフォームド：o（リスクの変化に対応できる） • サイバーセキュリティ情報の社内での共有：（記載なし）	連携している。外部から入手した情報を基に、リスクベースの経営判断をしている。
Adaptive（適応している）	• ベストプラクティスや知見からの予測に基づいたサイバーセキュリティ対策を実施。 • 継続的な改善活動により新たな脅威にも適時に適応している。	• リスクの全社的な認識度：o • 全社的なリスク管理プロセス：o • リスクインフォームド：o（リスクの変化に対応できる） • サイバーセキュリティ情報の社内での共有：o（サイバーセキュリティリスク管理が企業カルチャーに浸透している）	事象が発生する前にサイバーセキュリティを改善するために積極的に、正確に現時点の情報を共有している。

4.4 フレームワーク実施手順

フレームワークは、フレームワークを実施する手順として、以下の 6 つの手順のサイクルを推奨している。

順番	項目	概要
1	特定	ミッションの目的、関連システムおよび資産、規制要件、全体的なリスクアプローチの特定
2	現状プロファイルの作成	コアをベースの組織のサイバーセキュリティ対策の現状を把握する。コアに記載されている項目の全てを用いる必要は無く、また不足するものがあれば、追加しなければならない。
3	リスク評価の実施	把握した現状に対してリスク評価を実施する。
4	目標プロファイルの作成	リスク評価結果に基づいて、組織にとってあるべきサイバーセキュリティの状態を示す目標プロファイルを作成する。
5	ギャップ分析の実施	目標プロファイルと現状プロファイルのギャップ（差分）を特定し、改善するギャップの優先順位付けをする。（下図参照）
6	アクションプランの実施	ギャップ分析により特定した、必要な改善活動を実施する。目標プロファイルの達成度はモニタリングする。

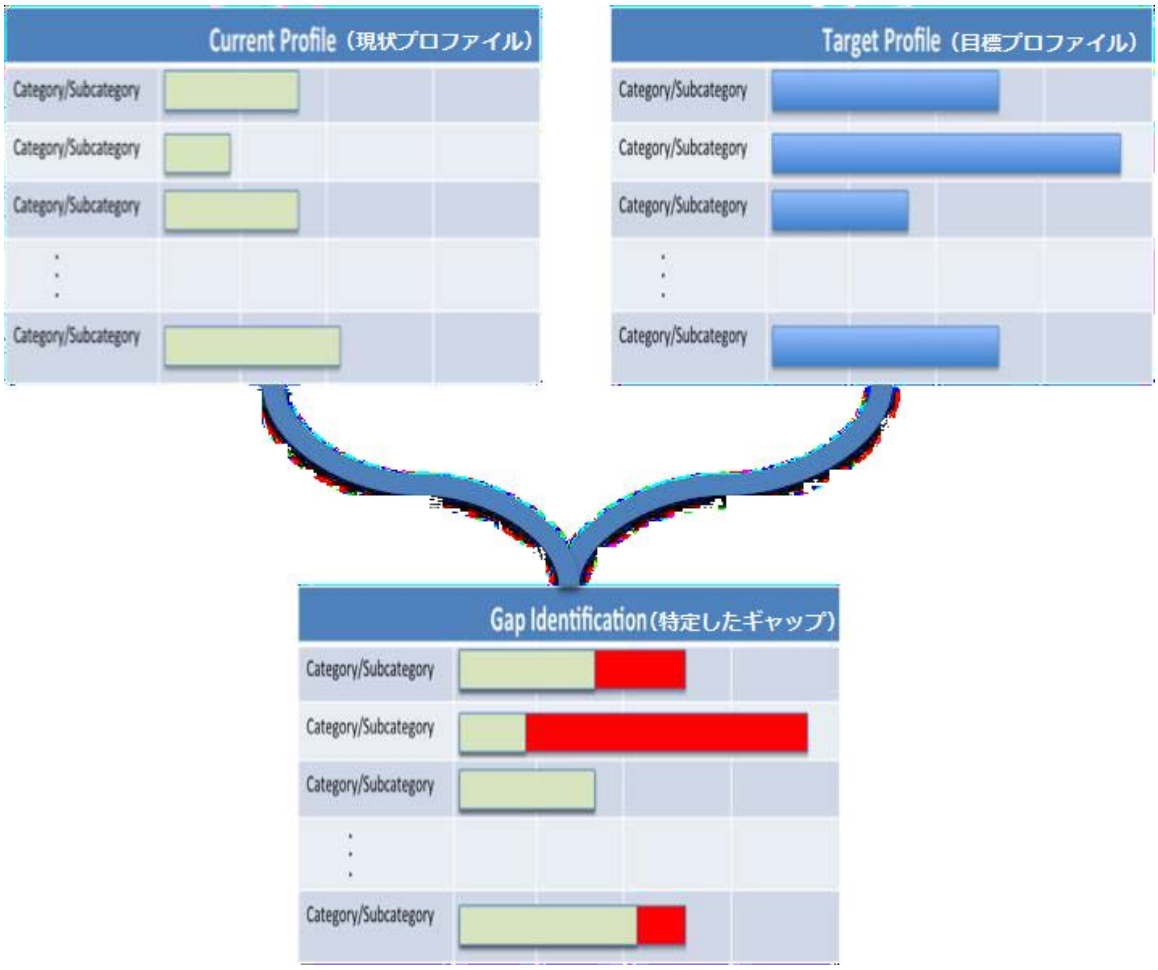


Figure 1：順番 5 のギャップ分析のイメージ（出典：NIST Preliminary Framework）

4.5　セキュリティフレームワークへの反応

フレームワークに対する反応を表すとすれば、躊躇している状態だと言える。民間セクターをはじめ、その他組織、及び個人が、大統領令、フレームワーク、その背後にある意図、及びサイバーセキュリティと産業が意味するものについてコメントを発表した。

フレームワークについての最初の苦情は、提言に重要性や緊急性を与えているにもかかわらず、提言を優先できていないという点である。NISTはその理由として、ガイドラインに含まれる大きな産業システムを持つ企業から、高速の取引プラットフォームを持つマーケットメーカーまで企業の範囲が広すぎて、優先事項全体が実現不可能になったことだとしている[63]。どこから始めるべきかわからない企業にとってこれは問題であり、そうでない企業は、自分たちのニーズに合わせたフレームワークを構築する選択の幅を広げることになっている。それでも、高い費用対効果を求める企業からすると、草稿の内容が的外れになってしまっている[64]。

「サイバー攻撃に関して言えば、知識こそが力だ」とする意見では、このフレームワークはサイバーセキュリティの主な目標を達成していると言える[65]。今回の大統領令が情報共有に焦点をあてていることを称賛する声があがる一方で、このフレームワークが何を達成しているのか疑問を呈する声もある。情報共有が重要インフラを守るカギだということに賛同する専門家はいるが、同時に「現在これらのシステムは完全に保護されていない状態にあり、このフレームワークが現実的な問題に対応する」[66]ということにさえ懐疑的な意見もあるが、いずれにせよ、2014 年 2 月に最終フレームワークが発表されれば結果が出ることで、企業はそれを採用することになる。

しかしこのフレームワークが採用されるかどうかについても議論は必要である。2 週間の政府閉等、ホワイトハウスとNISTが昨年から直面している様々な問題はあるものの、このフレームワークをあらゆる組織が採用することという最大の難問は、2 月になれば可能になる[67]。何故、重要インフラの所有者と運営者は、フレームワークを採用するのが難しいのか。まずその複雑さから検討する。

Internet Security Alliance社のLarry Clinton（ラリー・クリントン）社長が言うように、フレームワークの過去の草稿は、柔軟性に適応させるために変更され続けてきている[68]。

---

[63] Alan Wurtzel, "U.S. Gives Companies Cybersecurity Guidelines to Protect Critical Infrastructure," *The Wall Street Journal*, (Oct. 23, 2013), http://blogs.wsj.com/cfo/2013/10/23/u-s-gives-companies-cybersecurity-guidelines-to-protect-critical-infrastructure/.

[64] Cynthia Brumfield, "NIST's latest cybersecurity framework reveals a lot of goodwill amidst continued criticism."

[65] "Cyber Security, Critical Infrastructure, and Obama's Executive Order," *CIO Journal*, (Mar. 19, 2013), http://deloitte.wsj.com/cio/2013/03/19/cyber-security-critical-infrastructure-and-obamas-executive-order/.

[66] Michael S. Schmidt and Nicole Perlroth, "Obama Order Gives Firms Cyberthreat Information," The New York Times, (Feb. 12, 2013), http://www.nytimes.com/2013/02/13/us/executive-order-on-cybersecurity-is-issued.html?_r=0.

[67] Cynthia Brumfield, "Major changes ahead as NIST cybersecurity framework nears October publication," *CSOonline.com*, (Sept. 19, 2013), http://www.csoonline.com/article/740044/major-changes-ahead-as-nist-cybersecurity-framework-nears-october-publication.

[68] Ibid.

これは、小規模の企業にとってはまさにその通りで、「フレームワークの難解な性質」が（彼らを）躊躇させているということはわかっているだろう[69]。オバマ大統領自身は、採用を促す方法を見つけることを期待して、重要インフラの所有者及び運営者との会合を開くことで、この問題を解決しようとしていた。状況分析室（Situation Room）で開かれた 10 月 29 日の会議には、マスターカード社、ビザ社、シマンテック社、ノースロップグラマン社、ロッキードマーチン社、インテル社、バンクオブアメリカ社、ペペプコ社が出席した[70]。

ホワイトハウスが重要インフラの所有者・運営者を集めたのはこれが初めてではない。大統領令発布後の今年 3 月、オバマ大統領は、AT&T社のCEOとバンクオブアメリカ社とノースロップグラマン社幹部らを招き、サイバーセキュリティについて討論を行った[71]。このような大企業は、中小規模の重要インフラ所有者や運営者に及ぶことについて、必要な見識を多く与えることは出来ないが、少なくとも彼らが参加することで、フレームワークに対する情報が追加することができる。大企業が最も懸念しているのは、このフレームワークの支払いが困難であることである。

重要インフラの保護に、費用の話が出されるのは、自然だと思われるが、それがどれくらいかかるものなのかは、未だ不明である[72]。フレームワークの採択は各企業にとって意味あることであるが、重要インフラの所有者及び運営者は、フレームワークの導入は予算外であることを政府に訴え続けている。同時に、フレームワークの支持者は、「セキュリティチームがNISTの任意の基準に従うために大きな予算を受け取る」[73]という点を懸念しており、このことは、そもそもフレームワークがなぜ強制されないのかという疑問を支持者に残している。「結局のところ、リソースと法律によって企業が求められるセキュリティレベルがユーザーに与えられることになるだろう」[74]という意見も出ている。

フレームワークが規制となるか否かは、フレームワークの日程を決めるための大きな議論である。最初から、大統領、ホワイトハウス、議会及びNISTは、フレームワークは任意であり、そのままの方針でやっていくと述べている。大統領令発布以来、フレームワークが強制にベストプラクティスとベストスタンダードは、要件に代わる可能性があると懸念されている。米国商工会議所の国家セキュリティおよび緊急時に対する準備責任者は、フレームワークが強制になる可能性が高いことを理由に、大統領令の内容に反論した[75]。フレームワークの強制力については未知数だが、NISTのワークショップで行われた非公式の投票結果によれば、一部の参加者は少なくともフレームワークの一部が規

[69] Ibid.
[70] Tony Romm, “Obama holds cyber huddle with CEOs,” *POLITICO*, (Oct. 29, 2013), http://www.politico.com/story/2013/10/obama-ceos-tech-99037.html.
[71] Ibid.
[72] Alina Selyukh, “U.S. proposes minimal corporate cybersecurity standards.”
[73] Richard Adhiari, “NIST Forges Ahead with Critical Infrastructure Security Plan.”
[74] Ibid.
[75] Privacy & Data Security Law Resource Center, “President Obama Signs Executive Order On Cybersecurity, Seeks Voluntary Standards,” Bloomberg.com, (Feb. 18, 2013), http://www.bna.com/president-obama-signs-n17179872423/.

制要件になることを期待していることを示している[76]。2 月の期限が近付くにつれて、「任意のフレームワークが規制要件になるのでは」[77]ということに脅威を感じる民間セクターも多い。

一方、フレームワークの任意性が参加の決め手であると主張する人は多い。企業側は、仮にフレームワークが強制になるとしても、表向きその支持を取り下げるとは発表していないが、フレームワークの任意性を高く評価することで、その意思を表している。企業側は「規制を強制化すると、大統領令で望まれているような官民パートナーシップの実施難しい」[78]と考えている。ケン・ピッカリング氏のように、任意のフレームワークは殆ど意味がないとする少数派も、フレームワークの規制化に反対する多数派に流れる可能性がある[79]。

規制化に対する懸念がある一方、義務化の問題もある。フレームワークが強制となるか否かということは、契約査定基準に特に影響し、訴訟の対象となる案件における判断基準を作り出している。訴訟という結果にならなくても、金銭的な損失を引き起こしたとして企業イメージや評判には傷がつくことから、このフレームワークのサイバーセキュリティのリスク管理を実施しないことへのリスクは、各社の判断で決定することになる[80]。もっとも各社の選択ではあるが、義務化は、企業関係に直接影響するだけに、その反響は著しいだろう[81][82]。

今や企業は、全ての重要なサービスプロバイダーとの協定を見直さなくてはならない時期に差し掛かっている[83]。企業が重要インフラ企業からのアウトソーシングに頼るにせよ、あるいは、重要インフラ企業が他の会社にアウトソーシングを依頼するにせよ、フレームワーク採用と、義務化の可能性が、どの程度企業に影響するかを判断しなくてはならない。フレームワークを採用した企業と、そうでない企業間における責任の所在については、疑問が残る。

---

[76] Paul Molitor, "NIST moves forward on White House cybersecurity order," SmartGridNews.com, (Sept. 24, 2013), http://www.smartgridnews.com/artman/publish/Technologies_Security/NIST-moves-forward-on-White-House-cybersecurity-order-6051.html#.Uo_FgGTk9vk.
[77] Alina Selyukh, "U.S. proposes minimal corporate cybersecurity standards."
[78] Paul Rosenzweig and David Inserra, "Issue Brief: Obama's Cybersecurity Executive Order Falls Short," *The Heritage Foundation*, (Feb. 14, 2013), http://report.heritage.org/ib3852, 2.
[79] Richard Adhiari, "NIST Forges Ahead with Critical Infrastructure Security Plan."
[80] "USA: NIST voluntary Cybersecurity Framework 'hard to ignore.'"
[81] Hunton & Williams LLP, "NIST issues Preliminary Cybersecurity Framework," *Hunton & Williams*, (Nov. 6, 2013), http://www.hunton.com/files/News/45c578d7-b5e6-4a6f-b0af-2117b0558262/Presentation/NewsAttachment/2983b059-ec65-4e9c-a4e9-ed613e6359aa/NIST_Issues_Preliminary_Cybersecurity_Framework_revised%20.pdf.
[82] Rebecca Eisner, Howard W. Waltzman, and Lei Shen, "United States: The 2013 Cybersecurity Executive Order: Potential Impacts On the Private Sector," Mayer-Brown, (August 21, 2013), http://www.mayerbrown.com/The-2013-Cybersecurity-Executive-Order-Potential-Impacts-on-the-Private-Sector-08-13-2013/.
[83] Ibid.

情報共有の責任の問題も含め、義務化問題を解決できるのは、議会だけである[84]。このフレームワークの中にプライバシーガイドラインがあるにも関わらず、多くの企業は、情報共有には乗り気ではない[85]。

5 まとめ

サイバーセキュリティフレームワークはについて、専門家は、様々な既存の産業セキュリティ基準の寄せ集めだとしている[86]。しかしながら、これは、フレームワークをセクター特有のものにしない、あるいは、フレームワークが制限的な型に企業が従うことを求めないように意図的に行われたことである。

アナリストのJohn Pescatore（ジョン・ペスカトーレ）氏のように、「これは、もう一つのセキュリティフレームワークができただけである」[87]と考えている人は他にもいる。現在のサイバーセキュリティを維持したい企業にとっては、この複雑なフレームワークを遵守し、維持しなければならないことは、負担だが、サイバー脅威は、常に進化し、変化している[88]のも事実である。

他方、大統領令とフレームワークは、政府が重要インフラに対する脅威に真剣に対応している初めての兆候であるとする意見[89]もある。大統領令とフレームワークについて特筆すべきことは、脅威情報を共有のために準備しているステップであり、これは増加するサイバーセキュリティのカギだと考えられている[90]。

実際の重要インフラの所有者と管理者からの返答の大多数は、漠然としている。ケーブル事業者と通信事業者の業界団体であるNational Cable and Telecommunications Associationは、「我々は、16 件の重要インフラセクターの中から、多くの一般市民や民間ステークホルダーの重要な情報を得ようとしたNISTの協力に感謝している。」[91]と述べている。別の通信業界の業界団体は、が「2013 年 2 月に発布された大統領令は、サイバーセキュリティの弱点に対し、国家の対応力を高めるという内容であった。この中で大統領の掲げた目標を達成するという約束のために、NISTとギャラガー氏が尽力したことについて称賛している。」[92]と述べている。

フレームワークの採用を検討している意見の中には、フレームワークの採用が消費者物価指数の上昇を意味するとも言っている。電力事業者のペプコ社の幹部は、は、フレームワークの採用に賛成したものの、「企業は、フレームワークが薦めるベストプラクテ

---

[84] Paul Rosenzweig and David Inserra, “Issue Brief: Obama’s Cybersecurity Executive Order Falls Short,” 1.
[85] Ibid.
[86] Mauricio F. Paez, “Spotlight on the New US Cybersecurity Plan.”
[87] Alan Wurtzel, “U.S. Gives Companies Cybersecurity Guidelines to Protect Critical Infrastructure.”
[88] Paul Rosenzweig and David Inserra, “Issue Brief: Obama’s Cybersecurity Executive Order Falls Short,” 2.
[89] “Cyber Security, Critical Infrastructure, and Obama’s Executive Order.”
[90] Ibid.
[91] Cynthia Brumfield, “NIST’s latest cybersecurity framework reveals a lot of goodwill amidst continued criticism.”
[92] Ibid.

ィスを採用するのにかかった費用を顧客が負担するレートに組み入れるために、州議会の承認を求めるだろう」[93]と述べている。

このフレームワークの最大の欠点は、「実際にサイバーセキュリティのリスクを軽減することが対話の一部になっていないこと」[94]である。国際社会レベルでサイバーセキュリティリスクへの注意喚起を高めることを含めNISTが達成しようとしているにも関わらず、実際には、サイバーセキュリティリスクを軽減することには焦点が当てられていない。

このフレームワークが以前の試みより上に評価されているのは、官民協力の範囲を促進していることである。McAfee社の政府部門責任者は、「過去に、サイバーセキュリティにおいて、官民パートナーシップについて多くの協議がなされているが、このフレームワークは、現実的である。」[95]と述べている。今のところ、積極的に集められたフィードバックの取り込みが、このフレームワークの最大の功績だと言えるだろう。

[93] Eric Chabrow, “Obama, CEOs Meet on Cybersecurity Framework,” BankInfoSecurity.com, (Oct. 30, 2013), http://www.bankinfosecurity.com/obama-ceos-meet-on-cybersecurity-framework-a-6183/op-1.
[94] Cynthia Brumfield, “NIST’s latest cybersecurity framework reveals a lot of goodwill amidst continued criticism.”
[95] Ibid.