Framework for Improving Critical Infrastructure Cybersecurity

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フレームワーク

Version 1.1
1.1 版

National Institute of Standards and Technology
米国国立標準技術研究所

April 16, 2018
2018 年 4 月 16 日

この文書は以下の団体によって翻訳監修されています

IPA 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

Note to Readers on the Update

Version 1.1 of this Cybersecurity Framework refines, clarifies, and enhances Version 1.0, which was issued in February 2014. It incorporates comments received on the two drafts of Version 1.1.

Version 1.1 is intended to be implemented by first-time and current Framework users. Current users should be able to implement Version 1.1 with minimal or no disruption; compatibility with Version 1.0 has been an explicit objective.

The following table summarizes the changes made between Version 1.0 and Version 1.1.

Table NTR-1 - Summary of changes between Framework Version 1.0 and Version 1.1.

Update	Description of Update
Clarified that terms like "compliance" can be confusing and mean something very different to various Framework stakeholders	Added clarity that the Framework has utility as a structure and language for organizing and expressing compliance with an organization's own cybersecurity requirements. However, the variety of ways in which the Framework can be used by an organization means that phrases like "compliance with the Framework" can be confusing.
A new section on self-assessment	Added Section 4.0 *Self-Assessing Cybersecurity Risk with the Framework* to explain how the Framework can be used by organizations to understand and assess their cybersecurity risk, including the use of measurements.
Greatly expanded explanation of using Framework for Cyber Supply Chain Risk Management purposes	An expanded Section 3.3 *Communicating Cybersecurity Requirements with Stakeholders* helps users better understand Cyber Supply Chain Risk Management (SCRM), while a new Section 3.4 Buying Decisions highlights use of the Framework in understanding risk associated with commercial off-the-shelf products and services. Additional Cyber SCRM criteria were added to the Implementation Tiers. Finally, a Supply Chain Risk Management Category, including multiple Subcategories, has been added to the Framework Core.
Refinements to better account for authentication, authorization, and identity proofing	The language of the Access Control Category has been refined to better account for authentication, authorization, and identity proofing. This included adding one Subcategory each for Authentication and Identity Proofing. Also, the Category has been renamed to Identity Management and Access Control (PR.AC) to better represent the scope of the Category and corresponding Subcategories.
Better explanation of the relationship between Implementation Tiers and Profiles	Added language to Section 3.2 *Establishing or Improving a Cybersecurity Program* on using Framework Tiers in Framework implementation. Added language to Framework Tiers to reflect integration of Framework considerations within organizational risk management programs. The Framework Tier concepts were also refined. Updated Figure 2.0 to include actions from the Framework Tiers.

変更点について

この *サイバーセキュリティフレームワーク 1.1 版*は、2014 年 2 月に刊行された 1.0 版を、洗練、明確化、強化したものである。また、1.1 版の2つの草案に対するコメントも反映した。

1.1 版は、本 *フレームワーク*を初めて利用する組織にも、以前から継続して利用している組織にも、実施可能なものとなっている。1.0 版と 1.1 版の整合性を明確に意識して作成したため、継続利用者は、一切断絶を経験せずに（あるいは最低限の断絶のみで）実施を継続することができるようになっている。

1.0 版と 1.1 版の違いを、以下の表にまとめた。

表 NTR-1 フレームワーク 1.0 版と 1.1 版の違い

変更点	説明
「コンプライアンス」のように、不明確で、*フレームワーク*の各利害関係者にとって意味が大きく異なり得る用語を明確化した。	*フレームワーク*を、組織のサイバーセキュリティ上の要求事項を整理し、表現するための構造・言語として利用できるよう、明確化した。しかし、組織が *フレームワーク*を様々な方法で利用できるということは、「*フレームワーク*に関するコンプライアンス」というようなフレーズの意味が不明確になり得ることでもある。
新しく自己アセスメントに関するセクションを導入した。	セクション 4.0『フレームワークを利用したサイバーセキュリティリスクの自己アセスメント』を追加した。このセクションでは、*フレームワーク*を利用してサイバーセキュリティリスクを理解、評価する方法（リスク計測の活用も含む）を説明する。
*サイバーサプライチェーンリスクマネジメント*における *フレームワーク*の利用に関する説明を大幅に追加した。	『3.3 サイバーセキュリティ上の要求事項について利害関係者とコミュニケーションを行う』では、*サイバーサプライチェーンリスクマネジメント*（SCRM: Supply Chain Risk Management）に関する説明を追加した。また、新しいセクション『3.4 購入に関する決定』では、*フレームワーク*を活用して既成商品・サービスのリスクを理解する方法を説明した。インプリメンテーションティアに、*サイバーSCRM* に関する新しい基準を追加した。*フレームワークコア*に、*サプライチェーンリスクマネジメントカテゴリー*と、複数の *サブカテゴリー*を追加した。
認証、認可、アイデンティティの確認（本人確認）に関する説明を洗練した。	認証、認可、アイデンティティの確認に関する説明を洗練するため、*アクセス制御カテゴリー*の文言を変更した。その一環として、認証とアイデンティティの確認について、それぞれ1つずつ *サブカテゴリー*を追加した。また、当該 *カテゴリー*とその下の *サブカテゴリー*の内容をより正確に示した名称となるよう、*カテゴリー*の名称を *アイデンティティ管理とアクセス制御*（PR.AC）に変更した。
*インプリメンテーションティア*と *プロファイル*の関係に関する説明を拡充した。	『3.2 サイバーセキュリティプログラムの立ち上げまたは改善』では、*フレームワーク*の実施における *フレームワークティア*の利用についての説明を追加した。組織リスクマネジメントプログラムに *フレームワーク*上の検討事項を取り込むことを考慮して、*フレームワークティア*に関する説明を追加した。*フレームワークティア*の概念洗練した。図 2.0 に、*フレームワークティア*に基づくアクションを追加した。

Consideration of Coordinated Vulnerability Disclosure	A Subcategory related to the vulnerability disclosure lifecycle was added.

As with Version 1.0, Version 1.1 users are encouraged to customize the Framework to maximize individual organizational value.

脆弱性情報の開示を考慮した。	脆弱性情報の開示サイクルに関する*サブカテゴリー*を追加した。

各組織の価値が最大限に発揮されるよう、1.0 版同様、*フレームワーク*をカスタマイズして利用することを推奨する。

Acknowledgements

This publication is the result of an ongoing collaborative effort involving industry, academia, and government. The National Institute of Standards and Technology (NIST) launched the project by convening private- and public-sector organizations and individuals in 2013. Published in 2014 and revised during 2017 and 2018, this *Framework for Improving Critical Infrastructure Cybersecurity* has relied upon eight public workshops, multiple Requests for Comment or Information, and thousands of direct interactions with stakeholders from across all sectors of the United States along with many sectors from around the world.

The impetus to change Version 1.0 and the changes that appear in this Version 1.1 were based on:

- Feedback and frequently asked questions to NIST since release of Framework Version 1.0;
- 105 responses to the December 2015 request for information (RFI), *Views on the Framework for Improving Critical Infrastructure Cybersecurity*;
- Over 85 comments on a December 5, 2017 proposed second draft of Version 1.1;
- Over 120 comments on a January 10, 2017, proposed first draft Version 1.1; and
- Input from over 1,200 attendees at the 2016 and 2017 Framework workshops.

In addition, NIST previously released Version 1.0 of the Cybersecurity Framework with a companion document, *NIST Roadmap for Improving Critical Infrastructure Cybersecurity*. This Roadmap highlighted key "areas of improvement" for further development, alignment, and collaboration. Through private and public-sector efforts, some areas of improvement have advanced enough to be included in this Framework Version 1.1.

NIST acknowledges and thanks all of those who have contributed to this Framework.

謝辞

本書は、産学官におけるたゆまぬ協力の賜物である。米国国立標準技術研究所（NIST）は、2013 年に官民の組織と個人を招集し、本プロジェクトを立ち上げた。2014 年に発行され、2017 年と 2018 年に改定された『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フレームワーク（*Framework for Improving Critical Infrastructure Cybersecurity*）』は、8回に及ぶ公開ワークショップ、複数回に及ぶ「コメント、情報の募集（Requests for Comment or Information）」、米国の全業界、そして世界の様々な業界の利害関係者との数千回にわたる直接的な交流に基づいて作成されたものである。

1.0 版の改訂のきっかけと 1.1 版における変更は、以下に基づくものである。

- *フレームワーク 1.0 版*の公開以降に NIST に寄せられたフィードバックと、頻繁に問い合わせのあった質問。
- 2015 年 12 月の「情報の募集（RFI）」に対して寄せられた 105 の回答、『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フレームワーク』に対する意見。
- 2017 年 12 月 5 日に提案した 1.1 版 第 2 草案に対する 85 のコメント。
- 2017 年 1 月 10 日に提案した 1.1 版 第 1 草案に対する 120 のコメント。
- 2016 年、2017 年の *フレームワーク*ワークショップに参加した 1,200 人以上の参加者からのインプット。

また、NIST は *サイバーセキュリティフレームワーク 1.0 版*と合わせて、『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 NIST ロードマップ（NIST Roadmap for Improving Critical Infrastructure Cybersecurity）』を公開した。この *ロードマップ*は、さらなる進展、調整、協力が求められる主な「改善分野」を示したものだった。これらの改善分野の一部では、官民の努力により、*フレームワーク 1.1 版*に含めるのにふさわしい進展が見られた。

本 *フレームワーク*に貢献したすべての人々に感謝する。

Executive Summary

The United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. Similar to financial and reputational risks, cybersecurity risk affects a company's bottom line. It can drive up costs and affect revenue. It can harm an organization's ability to innovate and to gain and maintain customers. Cybersecurity can be an important and amplifying component of an organization's overall risk management.

To better address these risks, the Cybersecurity Enhancement Act of 2014[1] (CEA) updated the role of the National Institute of Standards and Technology (NIST) to include identifying and developing cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators. Through CEA, NIST must identify "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks." This formalized NIST's previous work developing Framework Version 1.0 under Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity" (February 2013), and provided guidance for future Framework evolution. The Framework that was developed under EO 13636, and continues to evolve according to CEA, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business and organizational needs without placing additional regulatory requirements on businesses.

The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The Framework consists of three parts: the Framework Core, the Implementation Tiers, and the Framework Profiles. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Core provide detailed guidance for developing individual organizational Profiles. Through use of Profiles, the Framework will help an organization to align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives.

While this document was developed to improve cybersecurity risk management in critical infrastructure, the Framework can be used by organizations in any sector or community. The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving security and resilience.

The Framework provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today. Moreover, because it references globally recognized standards for cybersecurity, the

[1] *See* 15 U.S.C. § 272(e)(1)(A)(i). The Cybersecurity Enhancement Act of 2014 (S.1353) became public law 113274 on December 18, 2014 and may be found at: https://www.congress.gov/bill/113th-congress/senatebill/1353/text.

エグゼクティブサマリー

米国は、重要インフラが確実に機能することに依存している。サイバーセキュリティに対する脅威は、重要インフラシステムの複雑化と接続性の向上を巧みに利用し、国家の安全保障、経済、そして市民の安全と健康を危険に晒している。財政的リスクや評判に関わるリスクと同様に、サイバーセキュリティを脅かすリスク（以下、サイバーセキュリティリスク）は企業の損益に影響を与える。例えば、コストを跳ね上がらせたり、収益を圧迫したりする。また、イノベーションを起こす能力や、顧客を獲得・維持する能力に悪影響を及ぼすこともある。サイバーセキュリティは、組織全体のリスクマネジメントを強化する、重要な要素である。

このようなリスクへの対処を強化するため、サイバーセキュリティ強化法（Cybersecurity Enhancement Act）（2014 年）[1] により、米国国立標準技術研究所（NIST）の新たな役割として、重要インフラ事業者・運営者が自主的に利用できるようなサイバーセキュリティリスクに関するフレームワークを識別、策定することが加えられた。サイバーセキュリティ強化法により、NIST は「重要インフラの事業者及び運営者が自主的に利用できる、サイバーリスクの識別、評価、管理に役立つ情報セキュリティ対策を含む、優先順位付けされた、柔軟な、繰り返し適用可能な、パフォーマンスベースの、費用効果の高いアプローチ」を識別することが義務付けられている。これにより、大統領令（Executive Order）第 13636 号「重要インフラのサイバーセキュリティの改善（Improving Critical Infrastructure Cybersecurity）」（2013 年 2 月）に基づく*フレームワーク 1.0 版*の策定が NIST の任務として正式に定められると同時に、その後の*フレームワーク*の進化の方向性が定められた。大統領令第 13636 号に基づき策定された*フレームワーク*は、サイバーセキュリティ強化法と共に進化していく。*フレームワーク*は、企業に対して新たな規制を追加するものではなく、ビジネス上のニーズと組織のニーズに基づいた、費用対効果の高いサイバーセキュリティリスク対策・管理の「共通言語」を記したものである。

*フレームワーク*は、サイバーセキュリティへの取組を自組織にとってのビジネス上のモチベーションにつながるものにすることと、サイバーセキュリティリスクを組織のリスクマネジメントプロセスの一環としてとらえることを重視している。*フレームワーク*は、*フレームワークコア*（Framework Core）、*インプリメンテーションティア*（Implementation Tier）、*フレームワークプロファイル*（Framework Profile）の 3 つの要素で構成されている。*フレームワークコア*は、すべてのセクター、重要インフラに共通となるサイバーセキュリティ対策、期待される成果、参考情報をまとめたものである。*フレームワークコア*の各要素は、組織が各々の*プロファイル*を作成するにあたっての詳細なガイダンスを提供している。*プロファイル*は、組織がビジネスやミッションに関する要件、リスク許容度、リソースに合わせて、サイバーセキュリティ対策を調整し、優先順位を決めるのに役立つ。*インプリメンテーションティア*は、組織のサイバーセキュリティリスクマネジメントに対するアプローチの特徴を把握し、理解するための仕組みを提供する。

本文書は、重要インフラのサイバーセキュリティリスクマネジメントを改善することを目的として作成されたものだが、*フレームワーク*は、どんな業界あるいはコミュニティの組織でも利用できる。*フレームワーク*は、組織の規模、サイバーセキュリティリスクの程度、サイバーセキュリティの複雑さに関わらず、組織がリスクマネジメントの原則とベストプラクティスを適用し、セキュリティとレジリエンスを改善することを可能にする。

*フレームワーク*は、現在効果が認められている基準、ガイドライン、プラクティスを集約することで、複数のアプローチを体系化する共通の構造を示している。また、*フレームワーク*は、世界的に認められているサイバーセキュリティ基準をベースにしているため、重要インフラ分野のみならず、他の業界や

[1] 15 U.S.C. § 272(e)(1)(A)(i)を参照。サイバーセキュリティ強化法（2014 年）（S.1353）は、2014 年 12 月 18 日に 公法第 113274 号として制定された。以下から閲覧できる。https://www.congress.gov/bill/113th-congress/senatebill/1353/text.

Framework can serve as a model for international cooperation on strengthening cybersecurity in critical infrastructure as well as other sectors and communities.

The Framework offers a flexible way to address cybersecurity, including cybersecurity's effect on physical, cyber, and people dimensions. It is applicable to organizations relying on technology, whether their cybersecurity focus is primarily on information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), or connected devices more generally, including the Internet of Things (IoT). The Framework can assist organizations in addressing cybersecurity as it affects the privacy of customers, employees, and other parties. Additionally, the Framework's outcomes serve as targets for workforce development and evolution activities.

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. They also will vary in how they customize practices described in the Framework. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.

To account for the unique cybersecurity needs of organizations, there are a wide variety of ways to use the Framework. The decision about how to apply it is left to the implementing organization. For example, one organization may choose to use the Framework Implementation Tiers to articulate envisioned risk management practices. Another organization may use the Framework's five Functions to analyze its entire risk management portfolio; that analysis may or may not rely on more detailed companion guidance, such as controls catalogs. There sometimes is discussion about "compliance" with the Framework, and the Framework has utility as a structure and language for organizing and expressing compliance with an organization's own cybersecurity requirements. Nevertheless, the variety of ways in which the Framework can be used by an organization means that phrases like "compliance with the Framework" can be confusing and mean something very different to various stakeholders.

The Framework is a living document and will continue to be updated and improved as industry provides feedback on implementation. NIST will continue coordinating with the private sector and government agencies at all levels. As the Framework is put into greater practice, additional lessons learned will be integrated into future versions. This will ensure the Framework is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions.

Expanded and more effective use and sharing of best practices of this voluntary Framework are the next steps to improve the cybersecurity of our Nation's critical infrastructure – providing evolving guidance for individual organizations while increasing the cybersecurity posture of the Nation's critical infrastructure and the broader economy and society.

コミュニティにおいても、サイバーセキュリティ強化のための国際協力のモデルとして活用できる。

*フレームワーク*は、サイバーセキュリティの物理的側面、サイバー的側面、人的側面に対する効果を含め、柔軟にサイバーセキュリティに取り組むための方法を示す。*フレームワーク*は、サイバーセキュリティの主な焦点が、情報技術（IT)であるか、産業用制御システム（ICS）であるか、サイバーフィジカルシステム（CPS）であるか、あるいはモノのインターネット（IoT）等の一般的な接続デバイスであるかに関わらず、技術に依存する組織に対して適用可能なものである。*フレームワーク*は、サイバーセキュリティが顧客、従業員、その他の関係者に対して影響を及ぼす中で、組織がサイバーセキュリティに取り組んでいくのを支援する。さらに、*フレームワーク*に示された成果は、労働力の開発・発展活動の目標としても活用できる。

*フレームワーク*は、重要インフラのサイバーセキュリティリスクマネジメントに対する万能なアプローチではない。各組織には、異なる脅威、異なる脆弱性、異なるリスク許容度に基づくそれぞれ特有のリスクがある。*フレームワーク*が示すプラクティスをどのように導入するかも多岐にわたる。重要サービスを提供する上で必要な対策を判断し、優先順位を決めて投資することで、組織はそれぞれの投資の効果を最大限に引き出すことができる。*フレームワーク*の最終的な目標は、サイバーセキュリティリスクの低減と、より適切な管理を実現することである。

組織特有のニーズに対処するために*フレームワーク*を活用する方法は様々である。*フレームワークをどのように利用するかは、それを実施する組織に委ねられている。例えば、目標のリスクマネジメントプラクティスを表現するのに*フレームワークインプリメンテーションティア*を利用するのも一つの方法である。また、リスクマネジメントポートフォリオ全体を分析するのに*フレームワーク*の 5 つの*機能*を利用することもできる。このような分析は、制御カタログ等のより詳細なガイダンスに基づいていても、そうでなくても良い。時として、*フレームワーク*の「コンプライアンス」が議論されることがある。また、*フレームワーク*は、組織のサイバーセキュリティ上の要求事項のコンプライアンスを整理し、表現するための構造と言語として利用できる。しかし、組織が*フレームワーク*を様々な方法で利用できるということは、「*フレームワーク*に関するコンプライアンス」というようなフレーズの意味が不明確になり得ること、様々な利害関係者にとって、異なる意味を持ち得ることを意味する。
*フレームワーク*は、現時点でのものであり、実施に関する産業界からのフィードバックに基づいて随時更新・改善されていく。NIST は、引き続き、民間部門及び政府機関とあらゆるレベルで協力していく。また、*フレームワーク*がより広く利用されることで得られる新たな教訓は、将来のバージョンに反映される。これにより、新たな脅威やリスク、解決策が次々に浮上するダイナミックで課題の多い環境に身を置く重要インフラ事業者・運営者のニーズを満たすことができる。

個々の組織に絶えず進化するガイダンスを提供し、米国の重要インフラ、そしてより広範囲な経済社会のサイバーセキュリティ意識を総じて向上させる、こうした自主参加型の*フレームワーク*の利用拡大、活用、ベストプラクティスの共有は、米国の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新たなステップとなる。

Table of Contents

List of Figures

List of Tables

目次

図

表

1.0 Framework Introduction

The United States depends on the reliable functioning of its critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. Similar to financial and reputational risks, cybersecurity risk affects a company's bottom line. It can drive up costs and affect revenue. It can harm an organization's ability to innovate and to gain and maintain customers. Cybersecurity can be an important and amplifying component of an organization's overall risk management.

To strengthen the resilience of this infrastructure, the Cybersecurity Enhancement Act of 2014[2] (CEA) updated the role of the National Institute of Standards and Technology (NIST) to "facilitate and support the development of" cybersecurity risk frameworks. Through CEA, NIST must identify "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks." This formalized NIST's previous work developing Framework Version 1.0 under Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," issued in February 2013[3], and provided guidance for future Framework evolution.

Critical infrastructure[4] is defined in the U.S. Patriot Act of 2001[5] as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Due to the increasing pressures from external and internal threats, organizations responsible for critical infrastructure need to have a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk. This approach is necessary regardless of an organization's size, threat exposure, or cybersecurity sophistication today.

The critical infrastructure community includes public and private owners and operators, and other entities with a role in securing the Nation's infrastructure. Members of each critical infrastructure sector perform functions that are supported by the broad category of technology, including information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), and connected devices more generally, including the Internet of Things (IoT). This reliance on technology, communication, and interconnectivity has changed and expanded the potential vulnerabilities and increased potential risk to operations. For example, as technology and the data it produces and processes are increasingly used to deliver critical services and support business/mission decisions, the potential impacts of a cybersecurity incident on an

[2] *See* 15 U.S.C. § 272(e)(1)(A)(i). The Cybersecurity Enhancement Act of 2014 (S.1353) became public law 113-274 on December 18, 2014 and may be found at: https://www.congress.gov/bill/113th-congress/senatebill/1353/text.

[3] Executive Order no. 13636, *Improving Critical Infrastructure Cybersecurity*, DCPD-201300091, February 12, 2013. https://www.gpo.gov/fdsys/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf

[4] The Department of Homeland Security (DHS) Critical Infrastructure program provides a listing of the sectors and their associated critical functions and value chains. http://www.dhs.gov/critical-infrastructure-sectors

[5] See 42 U.S.C. § 5195c(e)). The U.S. Patriot Act of 2001 (H.R.3162) became public law 107-56 on October 26, 2001 and may be found at: https://www.congress.gov/bill/107th-congress/house-bill/3162

1.0　フレームワークの紹介

米国は、重要インフラが確実に機能することに依存している。サイバーセキュリティに対する脅威は、重要インフラシステムの複雑化と接続性の向上を巧みに利用し、国家の安全保障、経済、そして市民の安全と健康を危険に晒している。財政的リスクや評判に関わるリスクと同様に、サイバーセキュリティを脅かすリスク（以下、サイバーセキュリティリスク）は企業の損益に影響を与える。例えば、コストを跳ね上がらせたり、収益を圧迫したりする。また、イノベーションを起こす能力や、顧客を獲得・維持する能力に悪影響を及ぼすこともある。サイバーセキュリティは、組織全体のリスクマネジメントを強化する、重要な要素である。

このようなインフラのレジリエンスを強化するため、サイバーセキュリティ強化法（2014 年）[2] により、米国国立標準技術研究所（NIST）の新たな役割として、サイバーセキュリティリスクに関するフレームワーク「の策定を推進、支援する」ことが加えられた。サイバーセキュリティ強化法により、NIST は「重要インフラの事業者及び運営者が自主的に利用できる、サイバーリスクの識別、評価、管理に役立つ情報セキュリティ対策を含む、優先順位付けされた、柔軟な、繰り返し適用可能な、パフォーマンスベースの、費用効果の高いアプローチ」を識別することが義務付けられている。これにより、大統領令第 13636 号「重要インフラのサイバーセキュリティの改善」（2013 年 2 月）[3] に基づく*フレームワーク 1.0 版*の策定が NIST の任務として正式に定められるとともに、その後の*フレームワーク*の進化の方向性が定められた。

米国愛国者法（U.S. Patriot Act）（2001 年）[4] では、重要インフラ [5] を「物理的存在か、仮想的存在かに関わらず、米国にとって必要不可欠なシステムや資産で、これらのシステムや資産が利用不能な状態になったり、破壊された場合、米国の国家安全保障、経済安全保障、国民の健康や安全またはこれらの問題のうち複数、あるいはすべてに悪影響を与える可能性があるもの」と定義している。外部からの脅威と内部からの脅威の両方が増大する中、重要インフラに責任を担う組織は、サイバーセキュリティリスクの識別、評価、管理に対し、一貫性のある繰り返し適用可能なアプローチを採る必要がある。こうしたアプローチは、組織の規模、晒されている脅威、今日のサイバーセキュリティの複雑さに関わらず必要である。

重要インフラコミュニティには、公共及び民間の事業者や運営者、その他国のインフラの安全性を守る役割を担う関係者が含まれる。各重要インフラ分野の事業者は、情報技術（IT）、産業用制御システム（ICS）、サイバーフィジカルシステム（CPS）、あるいはモノのインターネット（IoT）等の一般的な接続デバイスを含む、広範囲なテクノロジーに支えられ、各々の役割を果たしている。こうしたテクノロジー、通信機能、相互接続性への依存は、潜在的な脆弱性を変化・拡大させ、運用上の潜在的リスクを増大させた。例えば、テクノロジーやテクノロジーにより生成・処理されたデータが、重要サービスの提供やビジネス・ミッション上の意志決定に活用されるようになるにつれ、サイバーセキュリティインシデントが

---

[2] 15 U.S.C. § 272(e)(1)(A)(i)を参照。サイバーセキュリティ強化法(2014 年) (S.1353)は、2014 年 12 月 18 日に公法第 113274 号として制定された。以下から閲覧できる。https://www.congress.gov/bill/113th-congress/senatebill/1353/text.

[3] 大統領令第 13636 号, 重要インフラのサイバーセキュリティの改善(*Improving Critical Infrastructure Cybersecurity)*, DCPD-201300091, 2013 年 2 月 12 日. https://www.gpo.gov/fdsys/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf

[4] 42 U.S.C. § 5195c(e))を参照。米国愛国者法 (2001 年) (H.R.3162)は、2001 年 10 月 26 日に 公法第 107-56 号として制定された。以下から閲覧できる。https://www.congress.gov/bill/107th-congress/house-bill/3162
（訳注：語順の関係から脚注番号 4 と 5 が英語版と入れ替わっている）

[5] 国土安全保障省(DHS: Department of Homeland Security)重要インフラプログラムは、各セクターの重要機能、バリューチェーンの一覧を提供している。http://www.dhs.gov/critical-infrastructure-sectors

organization, the health and safety of individuals, the environment, communities, and the broader economy and society should be considered.

To manage cybersecurity risks, a clear understanding of the organization's business drivers and security considerations specific to its use of technology is required. Because each organization's risks, priorities, and systems are unique, the tools and methods used to achieve the outcomes described by the Framework will vary.

Recognizing the role that the protection of privacy and civil liberties plays in creating greater public trust, the Framework includes a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities. Many organizations already have processes for addressing privacy and civil liberties. The methodology is designed to complement such processes and provide guidance to facilitate privacy risk management consistent with an organization's approach to cybersecurity risk management. Integrating privacy and cybersecurity can benefit organizations by increasing customer confidence, enabling more standardized sharing of information, and simplifying operations across legal regimes.

The Framework remains effective and supports technical innovation because it is technology neutral, while also referencing a variety of existing standards, guidelines, and practices that evolve with technology. By relying on those global standards, guidelines, and practices developed, managed, and updated by industry, the tools and methods available to achieve the Framework outcomes will scale across borders, acknowledge the global nature of cybersecurity risks, and evolve with technological advances and business requirements. The use of existing and emerging standards will enable economies of scale and drive the development of effective products, services, and practices that meet identified market needs. Market competition also promotes faster diffusion of these technologies and practices and realization of many benefits by the stakeholders in these sectors.

Building from those standards, guidelines, and practices, the Framework provides a common taxonomy and mechanism for organizations to:

1) Describe their current cybersecurity posture;
2) Describe their target state for cybersecurity;
3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
4) Assess progress toward the target state;
5) Communicate among internal and external stakeholders about cybersecurity risk.

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. They also will vary in how they customize practices described in the Framework. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.

組織、個人の健康と安全、環境、コミュニティ、そしてより広範囲な経済社会に与える潜在的な影響を考慮することが必要になってくる。

サイバーセキュリティリスクを管理するためには、リスクマネジメントを行うビジネス上のモチベーション、自組織におけるテクノロジーの使い方に即したセキュリティ上の考慮事項を明確に理解することが必須となる。リスク、優先事項、システムは組織ごとに異なるため、*フレームワーク*が記述する成果の達成に使用されるツールや手法も変わってくる。

プライバシーと人権の保護が国民の信頼を得るのに果たす役割を認識した上で、*フレームワーク*は、重要インフラに携わる組織がサイバーセキュリティ対策を行うにあたって、個人のプライバシーと人権を保護するための方法論を示している。多くの組織には、既にプライバシーと人権の保護のためのプロセスが存在する。*フレームワーク*が示す方法論は、既存のプロセスを補完し、組織のサイバーセキュリティリスクマネジメントアプローチと整合性の取れたプライバシーリスクマネジメントを容易にするためのガイダンスを提供するものである。プライバシーとサイバーセキュリティの統合は、顧客の信頼を向上させ、より標準化された情報共有を可能にし、また、様々な法体制に跨る重要インフラの運用を容易にするという点で、組織にとって有益である。

*フレームワーク*は、技術的に中立なため、継続的に有効性が確保され、技術のイノベーションを支えるものとなっている。それと同時に、*フレームワーク*は、テクノロジーと共に進化する様々な既存の基準、ガイドライン、プラクティスも参考にしている。このような、産業界によって作成・運用・更新されてきたグローバルな基準、ガイドライン、プラクティスを拠り拠にすることにより、*フレームワーク*が示す成果の達成に使用されるツールや手法は、国境を超え、サイバーセキュリティリスクのグローバルな性質を反映し、技術の進歩やビジネス要件と共に発展していく。既存の基準や新たな基準の活用は、規模の経済（スケールメリット）を可能にし、識別した市場のニーズに合った効果的な製品、サービス、プラクティスの開発を推進する。また、市場競争は、そうして生まれた技術やプラクティスのより迅速な普及と、各業界の利害関係者による様々なメリットの実現を推進する。

こうした基準、ガイドライン、プラクティスを基に、*フレームワーク*は、組織が以下を実施するにあたっての一般的なタクソノミー（分類法）及び手法を示している。

1) 現行のサイバーセキュリティへの取組を説明する。
2) 目標とするサイバーセキュリティ対策の実施状態を説明する。
3) 継続的かつ繰り返し実施可能なプロセスにおける改善の機会を識別し、優先順位付けを行う。
4) 目標達成までの進捗を評価する。
5) 社内外の利害関係者とサイバーセキュリティリスクについてコミュニケーションを行う。

*フレームワーク*は、重要インフラのサイバーセキュリティリスクマネジメントに対する万能なアプローチではない。各組織には、異なる脅威、異なる脆弱性、異なるリスク許容度に基づくそれぞれ特有のリスクがある。*フレームワーク*が示すプラクティスをどのように導入するかも多岐にわたる。重要サービスを提供する上で必要な対策を判断し、優先順位を決めて投資することで、組織はそれぞれの投資の効果を最大限に引き出すことができる。*フレームワーク*の最終的な目標は、サイバーセキュリティリスクの低減と、より適切な管理を実現することである。

To account for the unique cybersecurity needs of organizations, there are a wide variety of ways to use the Framework. The decision about how to apply it is left to the implementing organization. For example, one organization may choose to use the Framework Implementation Tiers to articulate envisioned risk management practices. Another organization may use the Framework's five Functions to analyze its entire risk management portfolio; that analysis may or may not rely on more detailed companion guidance, such as controls catalogs. There sometimes is discussion about "compliance" with the Framework, and the Framework has utility as a structure and language for organizing and expressing compliance with an organization's own cybersecurity requirements. Nevertheless, the variety of ways in which the Framework can be used by an organization means that phrases like "compliance with the Framework" can be confusing and mean something very different to various stakeholders.

The Framework complements, and does not replace, an organization's risk management process and cybersecurity program. The organization can use its current processes and leverage the Framework to identify opportunities to strengthen and communicate its management of cybersecurity risk while aligning with industry practices. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one.

While the Framework has been developed to improve cybersecurity risk management as it relates to critical infrastructure, it can be used by organizations in any sector of the economy or society. It is intended to be useful to companies, government agencies, and not-for-profit organizations regardless of their focus or size. The common taxonomy of standards, guidelines, and practices that it provides also is not country-specific. Organizations outside the United States may also use the Framework to strengthen their own cybersecurity efforts, and the Framework can contribute to developing a common language for international cooperation on critical infrastructure cybersecurity.

1.1 Overview of the Framework

The Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business/mission drivers and cybersecurity activities. These components are explained below.

- The *Framework Core* is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories – which are discrete outcomes – for each Function, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.
- *Framework Implementation Tiers* ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the

組織特有のニーズに対処するために*フレームワーク*を活用する方法は様々である。*フレームワーク*をどのように利用するかは、それを実施する組織に委ねられている。例えば、目標のリスクマネジメントプラクティスを表現するのに*フレームワークインプリメンテーションティア*を利用するのも一つの方法である。また、リスクマネジメントポートフォリオ全体を分析するのに*フレームワーク*の 5 つの*機能*を利用することもできる。このような分析は、制御カタログ等のより詳細なガイダンスに基づいていても、そうでなくても良い。時として、*フレームワーク*の「コンプライアンス」が議論されることがある。また、*フレームワーク*は、組織のサイバーセキュリティ上の要求事項のコンプライアンスを整理し、表現するための構造と言語として利用できる。しかし、組織が*フレームワーク*を様々な方法で利用できるということは、「*フレームワーク*に関するコンプライアンス」というようなフレーズの意味が不明確になり得ること、様々な利害関係者にとって、異なる意味を持ち得ることを意味する。

*フレームワーク*は、組織のリスクマネジメントプロセス及びサイバーセキュリティプログラムを補完するものであり、これらに取って代わるものではない。自組織は現在のプロセスを利用しつつ、*フレームワーク*を活用し、業界のプラクティスを考慮しながらサイバーセキュリティリスクの管理の強化および関係者間のコミュニケーションを図るための機会を識別することができる。また、サイバーセキュリティプログラムを持たない組織は、*フレームワーク*を参考にしてプログラムを立ち上げることができる。

*フレームワーク*は、重要インフラに関するサイバーセキュリティリスクマネジメントを改善するために策定されたものではあるが、これに限らず、経済社会のどんな分野の組織でも利用することができるものである。フォーカスや規模に関係なく、企業、政府機関、非営利組織で利用することができる。*フレームワーク*が示す基準、ガイドライン、プラクティスの一般的なタクソノミーも各国固有のものではない。米国外に所在する組織でもサイバーセキュリティ対策の強化に*フレームワーク*を利用することが可能であるほか、*フレームワーク*は重要インフラのサイバーセキュリティに関する国際協力のための共通言語の確立にも役立つ。

1.1　フレームワークの概要

*フレームワーク*は、サイバーセキュリティリスクを管理するためのリスクベースアプローチであり、*フレームワークコア*、*フレームワークインプリメンテーションティア*、*フレームワークプロファイル*の 3 つの要素で構成されている。*フレームワーク*の各要素は、サイバーセキュリティへの取組とビジネス・ミッション上のモチベーションの結び付きを強くするものである。これらの要素の詳細を以下に記す。

- *フレームワークコア*（以下、*コア*）は、すべての重要インフラ分野に共通となるサイバーセキュリティ対策、期待される成果、適用可能な参考情報をまとめたものである。*コア*は、役員レベルから実施・運用レベルまで、自組織全体でサイバーセキュリティ対策と期待される成果を共有することができるような形で、業界標準、ガイドライン、プラクティスを示したものである。*フレームワークコア*は、「*識別（Identify）*」、「*防御（Protect）*」、「*検知（Detect）*」、「*対応（Respond）*」、「*復旧（Recover）*」という、並行して継続的に実行される 5 つの*機能*で構成される。これらの*機能*をまとめて考慮することによって、組織のサイバーセキュリティリスクマネジメントライフサイクルを、高度かつ戦略的にとらえることが可能になる。*コア*は次にこれらの各*機能*の内容を、鍵となる*カテゴリー*、*サブカテゴリー*（個別の成果）に細分化して、各*サブカテゴリー*について、参考となる既存の基準、ガイドライン、プラクティスを参考情報に例示し、識別する。

- *フレームワークインプリメンテーションティア*（以下、*ティア*）は、組織がサイバーセキュリティリスクをどのようにとらえているか、また、そうしたリスクを管理するためにどのようなプロセスが存在しているかを示す。*ティア*は組織のサイバーセキュリティリスクマネジメントプラクティスが、

characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.

- A *Framework Profile* ("Profile") represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business/mission drivers and a risk assessment, determine which are most important; it can add Categories and Subcategories as needed to address the organization's risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

1.2 Risk Management and the Cybersecurity Framework

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the potential resulting impacts. With this information, organizations can determine the acceptable level of risk for achieving their organizational objectives and can express this as their risk tolerance.

With an understanding of risk tolerance, organizations can prioritize cybersecurity activities, enabling organizations to make informed decisions about cybersecurity expenditures. Implementation of risk management programs offers organizations the ability to quantify and communicate adjustments to their cybersecurity programs. Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services. The Framework uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity. It supports recurring risk assessments and validation of business drivers to help organizations select target states for cybersecurity activities that reflect desired outcomes. Thus, the Framework gives organizations the ability to dynamically select and direct improvement in cybersecurity risk management for the IT and ICS environments.

The Framework is adaptive to provide a flexible and risk-based implementation that can be used with a broad array of cybersecurity risk management processes. Examples of cybersecurity risk management processes include International Organization for Standardization (ISO)

*フレームワーク*で定義されている特性（例:リスクおよび脅威に対する意識が高い、繰り返し適用可能である、適応している）をどの程度まで達成できているかも示す。*ティア*は組織のプラクティスが*ティア* 1（「*部分的である*」）から*ティア* 4（「*適応している*」）までのいずれの段階にあるかを示す。これらの*ティア*は、特に手順化されていない場当たりな事後的対処から、迅速でリスク情報を活用したアプローチまでの進展を反映している。*ティア*の選択プロセスにおいて、組織は現行のリスクマネジメントプラクティス、脅威環境、法規制上の要求事項、事業目的・ミッション、組織に課せられている制約を考慮する必要がある。

- *フレームワークプロファイル*（以下、*プロファイル*）は、*フレームワーク*の*カテゴリー*及び*サブカテゴリー*から組織が選択した、ビジネスニーズを基にした期待される成果を表している。*プロファイル*は、*コア*が示す基準、ガイドライン、プラクティスを、個別の実施シナリオに合わせて整理したものと言える。*プロファイル*はまた、「*現在の*」*プロファイル*（「今の」状態）」と「*目標の*」*プロファイル*（「目指す」状態）を比較することにより、サイバーセキュリティ対策を改善する機会を識別するために使用できる。*プロファイル*を策定するにあたって、組織は*コア*のすべての*カテゴリー*と*サブカテゴリー*を見直して、ビジネス・ミッション上のモチベーションとリスクアセスメント結果を基にして最も対策が必要なリスクを決定することができる。また、自組織のリスクに対処するために、必要に応じて*カテゴリー*と*サブカテゴリー*を追加することができる。これにより組織は*現在のプロファイル*を使用して、費用対効果やイノベーションを含むその他のビジネスニーズを考慮した上で、*目標のプロファイル*へ向けての対策の優先順位付けと進捗の測定を行うことができる。また、*プロファイル*を使用すれば、自己アセスメントを実施して、組織内または組織間でコミュニケーションを行うことが可能になる。

1.2　リスクマネジメントとサイバーセキュリティフレームワーク

リスクマネジメントはリスクの識別、アセスメント、対処を行う継続的なプロセスである。リスクを管理するためには、組織はセキュリティ上のイベントが発生する可能性と、その結果としてもたらされ得る影響を把握する必要がある。この情報により、組織の目的の達成において許容できるリスクレベルを決定し、これをリスク許容度として表すことができる。

リスク許容度を把握できれば、サイバーセキュリティ対策の優先順位付けが可能になり、サイバーセキュリティへの投資について十分な情報を得た上での決断が可能になる。リスクマネジメントプログラムを実施することにより、組織はサイバーセキュリティプログラムに対する調整を定量化し、そのような調整に関してコミュニケーションを行うことが可能になる。組織がリスクに対処する方法は様々である。重要サービスの提供に対してリスクが及ぼし得る潜在的影響に鑑みて、組織は、リスクの低減、移転、受容など、適切な対処法を選択する。*フレームワーク*はリスクマネジメントプロセスを通じて、組織がサイバーセキュリティに関する決定事項について伝え、優先順位付けを行えるようにする。*フレームワーク*は、繰り返し適用可能なリスクアセスメントと、ビジネス上のモチベーションの確立をサポートし、組織が期待される成果を得るためのサイバーセキュリティ対策を選択できるようにする。したがって、*フレームワーク*は IT/ICS 環境に対するサイバーセキュリティリスクマネジメントアプローチを動的に選択し、改善する能力を組織に与える。

*フレームワーク*は柔軟性のある、リスクに基づいた実施が可能なため、広範囲のサイバーセキュリティリスクマネジメントプロセスに使用できる。サイバーセキュリティリスクマネジメントプロセスには、

31000:2009[6], ISO/International Electrotechnical Commission (IEC) 27005:2011[7], NIST Special Publication (SP) 800-39[8], and the *Electricity Subsector Cybersecurity Risk Management Process* (RMP) guideline[9].

1.3 Document Overview

The remainder of this document contains the following sections and appendices:

- Section 2 describes the Framework components: the Framework Core, the Tiers, and the Profiles.
- Section 3 presents examples of how the Framework can be used.
- Section 4 describes how to use the Framework for self-assessing and demonstrating cybersecurity through measurements.
- Appendix A presents the Framework Core in a tabular format: the Functions, Categories, Subcategories, and Informative References.
- Appendix B contains a glossary of selected terms.
- Appendix C lists acronyms used in this document.

[6] International Organization for Standardization, *Risk management – Principles and guidelines*, ISO 31000:2009, 2009. http://www.iso.org/iso/home/standards/iso31000.htm

[7] International Organization for Standardization/International Electrotechnical Commission, *Information technology – Security techniques – Information security risk management*, ISO/IEC 27005:2011, 2011. https://www.iso.org/standard/56742.html

[8] Joint Task Force Transformation Initiative, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication 800-39, March 2011. https://doi.org/10.6028/NIST.SP.80039

[9] U.S. Department of Energy, *Electricity Subsector Cybersecurity Risk Management Process*, DOE/OE-0003, May 2012. https://energy.gov/sites/prod/files/Cybersecurity Risk Management Process Guideline - Final - May 2012.pdf

例えば、ISO 31000:2009[6]、ISO/IEC 27005:2011[7]、NIST Special Publication 800-39[8]、Electricity Subsector Cybersecurity Risk Management Process（RMP）ガイドライン[9]がある。

1.3　本文書の概要

本文書は以降、以下のセクションと付録で構成されている。

- セクション 2 は、*フレームワーク*の各要素（*コア*、*ティア*、*プロファイル*）について説明する。
- セクション 3 は、*フレームワーク*の使い方の例を示す。
- セクション 4 は、*フレームワーク*を利用した自己アセスメントの方法と、測定を通じてサイバーセキュリティの状態を示す方法を説明する。
- 付録 A は、*フレームワークコア*の *機能*、*カテゴリー*、*サブカテゴリー*、*参考情報*を表で示したものである。
- 付録 B は、一部の用語の定義を示す。
- 付録 C は、本文書で使用されている略語の一覧である。

[6] 国際標準化機構（ISO）, *Risk management – Principles and guidelines*, ISO 31000:2009, 2009. http://www.iso.org/iso/home/standards/iso31000.htm

[7] 国際標準化機構（ISO）/国際電気標準会議（IEC）, *Information technology – Security techniques – Information security risk management*, ISO/IEC 27005:2011, 2011. https://www.iso.org/standard/56742.html

[8] Joint Task Force Transformation Initiative, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication 800-39, 2011 年 3 月. https://doi.org/10.6028/NIST.SP.80039

[9] 米国エネルギー省, *Electricity Subsector Cybersecurity Risk Management Process*, DOE/OE-0003, 2012 年 5 月. https://energy.gov/sites/prod/files/Cybersecurity Risk Management Process Guideline - Final - May 2012.pdf

2.0 Framework Basics

The Framework provides a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage cybersecurity risk across entire organizations or it can be focused on the delivery of critical services within an organization. Different types of entities – including sector coordinating structures, associations, and organizations – can use the Framework for different purposes, including the creation of common Profiles.

2.1 Framework Core

The *Framework Core* provides a set of activities to achieve specific cybersecurity *outcomes*, and references examples of guidance to achieve those outcomes. The Core is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by stakeholders as helpful in managing cybersecurity risk. The Core comprises four elements: Functions, Categories, Subcategories, and Informative References, depicted in **Figure 1**:

Figure 1: Framework Core Structure

The Framework Core elements work together as follows:

- **Functions** organize basic cybersecurity activities at their highest level. These Functions are Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The Functions also align with existing methodologies for incident management and help show the impact of investments in cybersecurity. For example, investments in planning and exercises support timely response and recovery actions, resulting in reduced impact to the delivery of services.

2.0 フレームワークの基本的な考え方

*フレームワーク*は、サイバーセキュリティリスクを把握、管理し、内外の利害関係者に向けて表現するための共通言語を提供する。*フレームワーク*はサイバーセキュリティリスクを低減するためのアクションの識別と優先順位付けに使用できるものであり、また、そうしたリスクを管理できるようポリシー、ビジネスアプローチ、技術的アプローチを調整するためのツールでもある。*フレームワーク*は、関連する組織全体のサイバーセキュリティリスクマネジメントに利用することも、組織内の重要サービスの提供に焦点を絞って利用することもできる。*フレームワーク*は、様々な団体（業界をまとめる役割を担う業界団体、協会、組織等）が、様々な目的（共通*プロファイル*の作成等）で利用することが可能である。

2.1　フレームワークコア

*フレームワークコア*はサイバーセキュリティ上の成果を達成するための対策と、それらの成果の達成のための参考情報をまとめたものである。*コア*は実施すべき対策のチェックリストではない。*コア*はサイバーセキュリティリスクを管理する上で役に立つことが利害関係者によって識別された、サイバーセキュリティの主な成果を示したものである。*コア*は**図 1** で示されるように、*機能*、*カテゴリー*、*サブカテゴリー*、*参考情報*の 4 つの要素で構成されている。

図 1：フレームワークコアの構造

*フレームワークコア*の各要素は、以下のように連携する。

- ***機能***は、基本的なサイバーセキュリティ対策の最も上位を構成する要素である。ここでいう*機能*とは、*「識別」*、*「防御」*、*「検知」*、*「対応」*、*「復旧」*である。これらの*機能*は情報を整理し、リスクマネジメント上の意思決定を可能にし、脅威に対処し、過去の対策から学んだ教訓を基に改善を行うことにより、組織がサイバーセキュリティリスクをどう管理しているか表現するのに役立つ。また、これらの*機能*は既存のインシデント管理手法と紐付けて、サイバーセキュリティへの投資の効果を示すのに役立てることができる。例えば、計画・実施への投資はタイムリーな対応と復旧活動につながるため、結果としてサービスの提供に対する影響も軽減される。

- **Categories** are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management," "Identity Management and Access Control," and "Detection Processes."
- **Subcategories** further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category. Examples of Subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated."
- **Informative References** are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory. The Informative References presented in the Framework Core are illustrative and not exhaustive. They are based upon cross-sector guidance most frequently referenced during the Framework development process.

The five Framework Core Functions are defined below. These Functions are not intended to form a serial path or lead to a static desired end state. Rather, the Functions should be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk. See Appendix A for the complete Framework Core listing.

- **Identify** – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

  The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

- **Protect** – Develop and implement appropriate safeguards to ensure delivery of critical services.

  The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

- **Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

  The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

- ***カテゴリー***は、*機能*をサイバーセキュリティ成果グループ別に細分化したものであり、計画上のニーズや個別の対策と密接に結びついている。*カテゴリー*には、例えば*「資産管理」*、*「アイデンティティ管理とアクセス制御」*、*「検知プロセス」*などがある。
- ***サブカテゴリー***は、*カテゴリー*を技術的な対策や管理面での対策がもたらす成果別に詳細化したものである。*サブカテゴリー*は、包括的なものではないものの、各*カテゴリー*の成果の達成に役立つものである。*サブカテゴリー*には、例えば「外部情報システムが、カタログ作成されている」、「保存されているデータが、保護されている」、「検知システムからの通知は、調査されている」などがある。
- ***参考情報***は、すべての重要インフラ分野に共通となる基準、ガイドライン、プラクティスをまとめたセクションであり、各*サブカテゴリー*と関連する、期待される成果を達成するための方法を示す。*フレームワークコア*に記載された*参考情報*は、あくまでも例を示すためのものであり、包括的ではない。*参考情報*は*フレームワーク*を構築するプロセスにおいて最も頻繁に参照される分野横断的なガイダンスをベースにしている。

*フレームワークコア*を構成する 5 つの*機能*の定義を以下に示す。これらの*機能*は連続した工程を形成することや、静的な、期待される最終状態へと導くことを意図しているわけではない。むしろ、これらの*機能*は動的なサイバーセキュリティリスクに対処できる運用文化の形成を目的として、同時的・連続的に実行されるべきものである。*フレームワークコア*を網羅した一覧は、付録 A を参照のこと。

- ***識別*** – システム、人、資産、データ、機能に対するサイバーセキュリティリスクの管理に必要な理解を深める。

  *「識別」機能*における対策は、*フレームワーク*を効果的に使用する上で基本となる。組織はビジネスを取り巻く状況、重要な機能を支えるリソース、関連するサイバーセキュリティリスクを理解することで、組織のリスクマネジメント戦略とビジネスニーズに適合するように取り組みの対象を絞って、優先順位付けを行うことが可能になる。*「識別」機能*の成果*カテゴリー*には、例えば*「資産管理」*、*「ビジネス環境」*、*「ガバナンス」*、*「リスクアセスメント」*、*「リスクマネジメント戦略」*などがある。

- ***防御*** – 重要サービスの提供を確実にするための適切な保護対策を検討し、実施する。

  *「防御」機能*は、発生する可能性のあるサイバーセキュリティイベントがもたらす影響を抑制するのを支援する。*「防御」機能*の成果*カテゴリー*には、例えば*「アイデンティティ管理とアクセス制御」*、*「意識向上およびトレーニング」*、*「データセキュリティ」*、*「情報を保護するためのプロセス及び手順」*、*「保守」*、*「保護技術」*などがある。

- ***検知*** – サイバーセキュリティイベントの発生を識別するのに適した対策を検討し、実施する。

  *「検知」機能*はサイバーセキュリティイベントのタイムリーな発見を可能にする。*「検知」機能*の成果*カテゴリー*には、例えば*「異常とイベント」*、*「セキュリティの継続的なモニタリング」*、*「検知プロセス」*などがある。

- **Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

  The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

- **Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

  The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

2.2 Framework Implementation Tiers

The Framework Implementation Tiers ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Ranging from Partial (Tier 1) to Adaptive (Tier 4), Tiers describe an increasing degree of rigor and sophistication in cybersecurity risk management practices. They help determine the extent to which cybersecurity risk management is informed by business needs and is integrated into an organization's overall risk management practices. Risk management considerations include many aspects of cybersecurity, including the degree to which privacy and civil liberties considerations are integrated into an organization's management of cybersecurity risk and potential risk responses.

The Tier selection process considers an organization's current risk management practices, threat environment, legal and regulatory requirements, information sharing practices, business/mission objectives, supply chain cybersecurity requirements, and organizational constraints. Organizations should determine the desired Tier, ensuring that the selected level meets the organizational goals, is feasible to implement, and reduces cybersecurity risk to critical assets and resources to levels acceptable to the organization. Organizations should consider leveraging external guidance obtained from Federal government departments and agencies, Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs), existing maturity models, or other sources to assist in determining their desired tier.

While organizations identified as Tier 1 (Partial) are encouraged to consider moving toward Tier 2 or greater, Tiers do not represent maturity levels. Tiers are meant to support organizational decision making about how to manage cybersecurity risk, as well as which dimensions of the organization are higher priority and could receive additional resources. Progression to higher Tiers is encouraged when a cost-benefit analysis indicates a feasible and cost-effective reduction of cybersecurity risk.

- ***対応*** – 検知されたサイバーセキュリティインシデントに対処するための適切な対策を検討し、実施する。

  *「対応」機能*は、発生する可能性のあるサイバーセキュリティインシデントがもたらす影響を封じ込めるのを支援する。*「対応」機能*の成果*カテゴリー*には、例えば*「対応計画の作成」「コミュニケーション」「分析」「低減」「改善」*などがある。

- ***復旧*** – レジリエンスを実現するための計画を策定・維持し、サイバーセキュリティインシデントによって阻害されたあらゆる機能やサービスを元に戻すための適切な対策を検討し、実施する。

  *「復旧」機能*は、サイバーセキュリティインシデントがもたらす影響を軽減するために、通常の運用状態へタイムリーに復旧するのを支援する。*「復旧」機能*の成果*カテゴリー*には、例えば*「復旧計画の作成」「改善」「コミュニケーション」*などがある。

2.2　フレームワークインプリメンテーションティア

フレームワークインプリメンテーションティア(「*ティア*」)は、組織がサイバーセキュリティリスクをどのようにとらえているか、また、そうしたリスクを管理するためにどのようなプロセスが存在しているかを示す。*ティア*は、*ティア 1*(「部分的である」)から*ティア 4*(「適応している」)までの段階があり、サイバーセキュリティリスクマネジメントプラクティスがどの程度厳密で、高度なものかを表す。サイバーセキュリティリスクマネジメントがビジネスニーズにどの程度基づいていて、組織の全体的なリスクマネジメントプラクティスにどの程度組み入れられているかを判断するのにも役立つ。リスクマネジメントにおいて考慮すべき事項は、組織によるサイバーセキュリティリスクの管理やリスクの対処に、プライバシーと人権に関する考慮がどの程度組み入れられているかなどの、サイバーセキュリティの幅広い側面を含む。

*ティア*の選択プロセスでは、組織の現行のリスクマネジメントプラクティス、脅威環境、法規制上の要求事項、情報共有のプラクティス、事業目的・ミッション、サプライチェーンに関するサイバーセキュリティ上の要求事項、組織に課せられている制約を考慮する。組織は、適切な*ティア*を選択すべきである。選択した*ティア*のレベルは、自組織の目標に見合うものであり、実施可能で、かつ重要な資産とリソースに対するサイバーセキュリティのリスクを自組織にとって許容可能な程度まで低減できるようなものでなければならない。組織は、適切な*ティア*を判断するにあたって、連邦政府の各機関、情報共有分析センター(ISAC: Information Sharing and Analysis Centers)、既存の成熟度モデル等、外部から得られるガイダンスの活用を検討すべきである。

ティア 1(「部分的である」)にあたると識別された組織は、*ティア 2* 以上を目指すことが推奨されるが、だからといって*ティア*が成熟度を表しているわけではない。*ティア*は、サイバーセキュリティリスクをどのように管理するか、自組織のどの側面に優先的に取り組み、追加的なリソースを割り当てるかなどについて、組織が決定を行うのを支援するものである。より高位の*ティア*に進むことが推奨されるのは、費用対効果分析の結果、サイバーセキュリティリスクの低減が実現可能で、費用効率も高くなることが示された場合である。

Successful implementation of the Framework is based upon achieving the outcomes described in the organization's Target Profile(s) and not upon Tier determination. Still, Tier selection and designation naturally affect Framework Profiles. The Tier recommendation by Business/Process Level managers, as approved by the Senior Executive Level, will help set the overall tone for how cybersecurity risk will be managed within the organization, and should influence prioritization within a Target Profile and assessments of progress in addressing gaps.

The Tier definitions are as follows:

Tier 1: Partial

- *Risk Management Process* – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- *Integrated Risk Management Program* – There is limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.
- *External Participation* – The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. The organization does not collaborate with or receive information (e.g., threat intelligence, best practices, technologies) from other entities (e.g., buyers, suppliers, dependencies, dependents, ISAOs, researchers, governments), nor does it share information. The organization is generally unaware of the cyber supply chain risks of the products and services it provides and that it uses.

Tier 2: Risk Informed

- *Risk Management Process* – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- *Integrated Risk Management Program* – There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established. Cybersecurity information is shared within the organization on an informal basis. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs, but is not typically repeatable or reoccurring.
- *External Participation* – Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both. The organization collaborates with and receives some information from other entities and generates some of its own information, but may not share information with others. Additionally, the organization is aware of the cyber supply chain risks associated with the products and services it provides and uses, but does not act consistently or formally upon those risks.

*フレームワーク*の導入の成否は、*ティア*の選択に左右されるわけではなく、自組織が*目標のプロファイル*に定めた成果を達成できるかどうかによって決まる。ただし、*ティア*の選択・指定は、当然、*フレームワークプロファイル*に影響する。*上級役員レベル*が承認した*業務責任者*(*ビジネス／プロセスレベルマネージャー*)からの*ティア*に関する意見を聞くことで、サイバーセキュリティリスクを自組織内でどのように管理するか、全体の方針を決定するのに役立つ。また、これらの意見は、*目標のプロファイル*内での優先順位付けや、目標とのギャップに対する取り組みの進捗を評価する際にも影響してくるだろう。

以下に、ティアの定義を示す。

ティア 1: 部分的である（Partial）

- *リスクマネジメントプロセス* – 組織のサイバーセキュリティリスクマネジメントプラクティスが定められておらず、リスクは場当たり的に、場合によっては事後に対処される。サイバーセキュリティ対策の優先順位付けが、組織のリスク目標、脅威環境、またはビジネス・ミッション上の要求事項に基づいていない。
- *統合されたリスクマネジメントプログラム* – 自組織レベルでのサイバーセキュリティリスク意識が不足している。外部情報源から得たさまざまな経験や情報に基づいてサイバーセキュリティリスクを管理しているため、リスクマネジメントが不規則であり、ケースバイケースで実施されている。サイバーセキュリティ情報を自組織内で共有するためのプロセスがない場合もある。
- *外部からの参加* – より大きなエコシステムの中で、依存関係または依存者について、自組織がどのような役割を果たすのか、自組織が理解していない。他の関係者（例：バイヤー、サプライヤー、依存関係、依存者、ISAO、リサーチャー、政府機関）と協力したり、情報（例：脅威情報、ベストプラクティス、技術）を互いに共有しようとしていない。自組織が提供、利用する製品・サービスのサイバーサプライチェーンリスクを全体的に把握できていない。

ティア 2: リスク情報を活用している（Risk Informed）

- *リスクマネジメントプロセス* – リスクマネジメントプラクティスは経営層によって承認されているが、組織全体にわたるポリシーとして定められていない場合がある。サイバーセキュリティ対策と保護ニーズの優先順位付けは、組織のリスク目標、脅威環境、またはビジネス・ミッション上の要求事項に基づいて直接伝えている。
- *統合されたリスクマネジメントプログラム* – 自組織レベルでのサイバーセキュリティリスク意識はあるが、サイバーセキュリティリスクを管理するための組織全体にわたる取組は定められていない。サイバーセキュリティ情報は非公式的に自組織内で共有されている。組織の目標と計画におけるサイバーセキュリティ上の考慮事項は、自組織の一部の層には浸透しているが、すべての層には浸透していない。組織内外の資産のサイバーリスクアセスメントは実施されているものの、繰り返し適用可能なものや繰り返し実施されるものではない。
- *外部からの参加* – より大きなエコシステムの中で、依存関係または依存者について、自組織がどのような役割を果たすのか、どちらかは理解しているが、両方は理解していない。他の関係者と協力し、情報を受け取っており、組織自らも情報を創出しているが、その情報を他の関係者と共有していない。また、自組織が提供、利用する製品・サービスのサイバーサプライチェーンリスクを把握しているが、そのようなリスクに基づいて、継続的にまたは正式に対処することはできていない。

Tier 3: Repeatable

- *Risk Management Process* – The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
- *Integrated Risk Management Program* – There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. The organization consistently and accurately monitors cybersecurity risk of organizational assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risk. Senior executives ensure consideration of cybersecurity through all lines of operation in the organization.
- *External Participation* - The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks. It collaborates with and receives information from other entities regularly that complements internally generated information, and shares information with other entities. The organization is aware of the cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it usually acts formally upon those risks, including mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring.

Tier 4: Adaptive

- *Risk Management Process* – The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing threat and technology landscape and responds in a timely and effective manner to evolving, sophisticated threats.
- *Integrated Risk Management Program* – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risk and organizational objectives is clearly understood and considered when making decisions. Senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities and continuous awareness of activities on their systems and networks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated.

ティア 3: 繰り返し適用可能である（Repeatable）

- *リスクマネジメントプロセス* – 自組織のリスクマネジメントプラクティスは正式に承認され、ポリシーとして述べられている。組織のサイバーセキュリティプラクティスは、ビジネス・ミッション上の要求事項の変化と、脅威及びテクノロジー状況の変化へのリスクマネジメントプロセスの適用に基づいて、定期的に更新されている。
- *統合されたリスクマネジメントプログラム* – 組織全体のサイバーセキュリティリスクマネジメントへのアプローチが確立されている。リスク情報を活用したポリシー、プロセス、手順が定義され、意図した通りに実施され、レビューされている。リスクの変化に効果的に対応するための一貫した手法が存在している。従業員は割り当てられた役割と責任を果たすための知識とスキルを持っている。組織の資産のサイバーセキュリティリスクを、自組織が継続して正確にモニタリングしている。サイバーセキュリティ担当役員とその他の役員が、サイバーセキュリティリスクについて定期的にコミュニケーションを行っている。上級役員は、自組織のすべての運用部門で、サイバーセキュリティが考慮されるようにしている。
- *外部からの参加* – 自組織が、より大きなエコシステムの中における組織の役割、依存関係、依存者を理解しており、コミュニティにおけるリスクをより広範囲に捉えることに貢献している。他の関係者と協力し、情報を受け取り、それを組織が自ら創出する情報を補完するものとして利用している。また、創出した情報を他の関係者と共有している。自組織が提供、利用する製品やサービスのサイバーサプライチェーンリスクを把握している。さらに、そのようなリスクに基づいて、正式な対処を行っている。これには、基本要件、ガバナンス組織（例：リスク委員会）、ポリシーの実施とモニタリングについてコミュニケーションを行う合意書等の仕組みが含まれる。

ティア 4: 適応している（Adaptive）

- *リスクマネジメントプロセス* – 自組織は過去と現在のサイバーセキュリティプラクティス（そこから学んだ教訓と、それらの対策から得た兆候を含む）を基に、サイバーセキュリティ対策を調整する。自組織は最新のサイバーセキュリティ技術及びプラクティスを組み入れた継続的な改善のためのプロセスを介して、変化するサイバーセキュリティの技術と実践に進んで順応し、進化・高度化する脅威にタイムリーかつ効果的に対応している。
- *統合されたリスクマネジメントプログラム* – 発生する可能性のあるサイバーセキュリティイベントに対処するためのリスク情報を活用したポリシー、プロセス、手順を用いた、組織全体のサイバーセキュリティリスクマネジメントのアプローチが確立されている。意思決定の際には、サイバーセキュリティリスクと組織の目的の間の関係が明確に理解され、考慮されている。上級役員は、サイバーセキュリティリスクを、財政的リスクやその他の組織にとってのリスク同様にモニタリングしている。自組織の予算が、現在と今後予想されるリスク環境とリスク許容度の理解に基づいて決定されている。各部署は、自組織全体のリスク許容度に基づいて、役員が示したビジョンを実践し、システムレベルでのリスク分析を行っている。サイバーセキュリティリスクマネジメントは、自組織文化の一部となっており、また、過去の対策に対する理解、組織のシステムとネットワーク上の活動の継続的な把握に基づいて進化していく。リスクに関するアプローチとコミュニケーションについて、事業目的・ミッションの変更に迅速かつ効果的に対処することができる。

- *External Participation* - The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks. It receives, generates, and reviews prioritized information that informs continuous analysis of its risks as the threat and technology landscapes evolve. The organization shares that information internally and externally with other collaborators. The organization uses real-time or near real-time information to understand and consistently act upon cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it communicates proactively, using formal (e.g. agreements) and informal mechanisms to develop and maintain strong supply chain relationships.

2.3 Framework Profile

The Framework Profile ("Profile") is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. A Profile enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. Given the complexity of many organizations, they may choose to have multiple profiles, aligned with particular components and recognizing their individual needs.

Framework Profiles can be used to describe the current state or the desired target state of specific cybersecurity activities. The Current Profile indicates the cybersecurity outcomes that are currently being achieved. The Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals. Profiles support business/mission requirements and aid in communicating risk within and between organizations. This Framework does not prescribe Profile templates, allowing for flexibility in implementation.

Comparison of Profiles (e.g., the Current Profile and Target Profile) may reveal gaps to be addressed to meet cybersecurity risk management objectives. An action plan to address these gaps to fulfill a given Category or Subcategory can contribute to the roadmap described above. Prioritizing the mitigation of gaps is driven by the organization's business needs and risk management processes. This risk-based approach enables an organization to gauge the resources needed (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner. Furthermore, the Framework is a risk-based approach where the applicability and fulfillment of a given Subcategory is subject to the Profile's scope.

- *外部からの参加* – 自組織が、より大きなエコシステムの中における組織の役割、依存関係、依存者を理解しており、コミュニティにおけるリスクをより広範囲に捉えることに貢献している。優先順位付けされた情報を受け取り、創出し、レビューしている。このような情報は、脅威環境や技術環境が変化する中で、リスクを継続的に分析していくのに利用されている。自組織は、内外の協力者と情報を共有している。自組織が提供、利用する製品及びサービスに関連するサイバーサプライチェーンリスクを、リアルタイムな情報、あるいはリアルタイムに近い情報に基づいて把握し、継続的にそういったリスクに基づいて対処している。また、サプライチェーンにおいて強力な関係を築き、維持するために、正式な方法（例：契約）及び非公式な方法によって、積極的なコミュニケーションを行っている。

2.3 フレームワークプロファイル

フレームワークプロファイル（「*プロファイル*」）は、自組織のビジネス上の要求事項、リスク許容度、割当可能なリソースに基づいて調整された*機能*、*カテゴリー*、*サブカテゴリー*をまとめたものである。*プロファイル*は、法規制上の要求事項と業界のベストプラクティスを考慮して作成され、リスクマネジメント上の優先事項を反映することを可能にし、組織の目標のみならず、業界の目標も踏まえた、サイバーセキュリティリスクを低減するためのロードマップの確立を可能にする。最近は複雑な構造の組織が多いことから、個別の事業部門に合わせて調整された、個々のニーズを反映する複数のプロファイルを用意することを選択してもよい。

*フレームワークプロファイル*は、具体的なサイバーセキュリティ対策の現在の状態と目指す目標の状態を記述するのに使用できる。*現在のプロファイル*は、現時点で達成されているサイバーセキュリティ成果を示す。*目標のプロファイル*は、サイバーセキュリティリスクマネジメントの目標を達成するのに必要な成果を示す。*プロファイル*はビジネス・ミッション上の要求事項の達成を助け、組織内及び組織間でのリスクについてのコミュニケーションを支援する。*フレームワーク*では、実施に関して柔軟性を持たせることを意図して、*プロファイル*のひな形は規定しない。

*プロファイル*の比較（例:*現在のプロファイル*と*目標のプロファイル*の比較）は、サイバーセキュリティリスクマネジメント上の目標を果たす上で対処が必要なギャップを浮き彫りにする。*カテゴリー*または*サブカテゴリー*の達成に向けて、これらのギャップを埋めるための行動計画は、上述のロードマップの作成に役立つ。ギャップを埋める作業の優先順位付けは、自組織のビジネスニーズとリスクマネジメントプロセスから導出される。このリスクベースアプローチは、組織がサイバーセキュリティ目標をコスト効率よく、かつ優先順位けがなされる形で達成するために必要なリソース（例:人員、資金）の割出しを可能にする。また、*フレームワーク*は、リスクベースのアプローチであり、ある*サブカテゴリー*が適用されるか否か、達成されるか否かは、*プロファイル*の範囲による。

2.4 Coordination of Framework Implementation

Figure 2 describes a common flow of information and decisions at the following levels within an organization:

- Executive
- Business/Process
- Implementation/Operations

The executive level communicates the mission priorities, available resources, and overall risk tolerance to the business/process level. The business/process level uses the information as inputs into the risk management process, and then collaborates with the implementation/operations level to communicate business needs and create a Profile. The implementation/operations level communicates the Profile implementation progress to the business/process level. The business/process level uses this information to perform an impact assessment. Business/process level management reports the outcomes of that impact assessment to the executive level to inform the organization's overall risk management process and to the implementation/operations level for awareness of business impact.

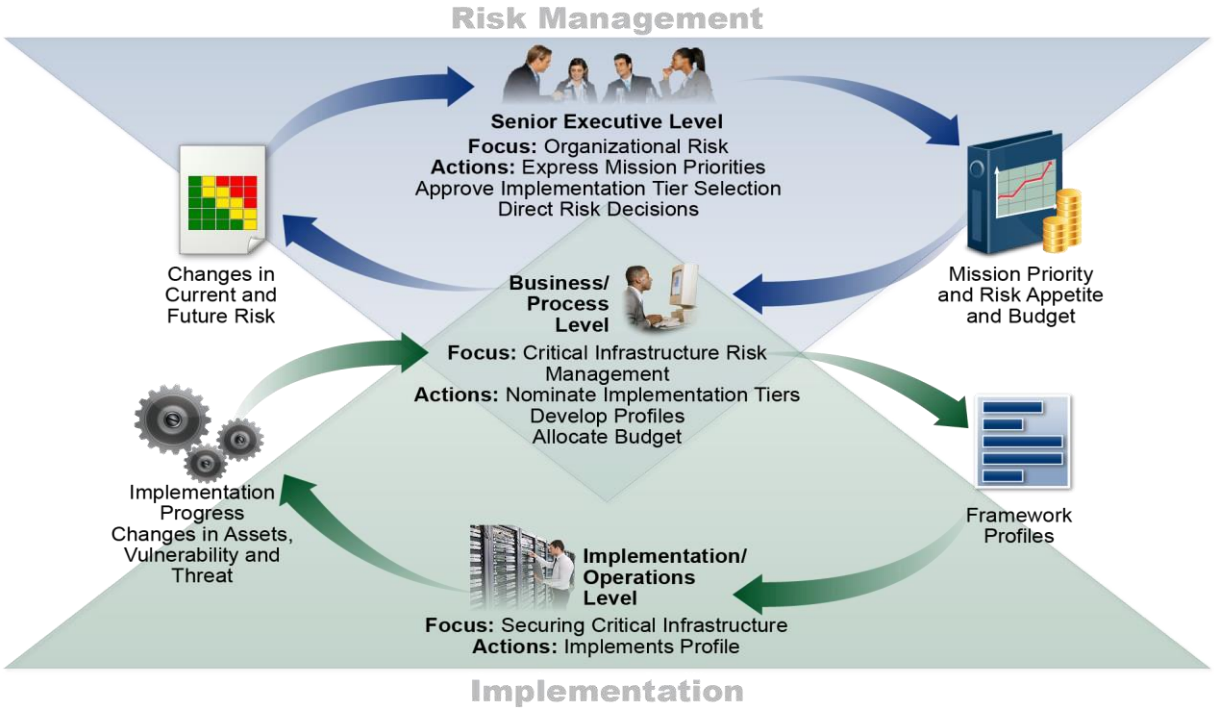

Figure 2: Notional Information and Decision Flows within an Organization

2.4 フレームワークインプリメンテーションの調整

図 2 は、組織内の以下の各レベルにおける情報と意思決定の一般的な流れを示したものである。

- 役員レベル
- ビジネス/プロセスレベル
- 実施/運用レベル

役員レベルはビジネス/プロセスレベルに対してミッションの優先順位、割当可能なリソース、全体的なリスク許容度について、コミュニケーションを行う。ビジネス/プロセスレベルはこの情報をリスクマネジメントプロセスへの入力情報として使用して、実施/運用レベルと連携してビジネスニーズについてコミュニケーションを行い、プロファイルを作成する。実施/運用レベルはビジネス/プロセスレベルに対して*プロファイル*の実施の進捗状況について、コミュニケーションを行う。ビジネス/プロセスレベルはこの情報を使用して影響のアセスメントを実施する。ビジネス/プロセスレベルの管理者は役員レベルに対して影響のアセスメント結果を報告し、自組織全体のリスクマネジメントプロセスに役立つ情報を提供する一方で、実施/運用レベルに対してビジネスに対する影響を伝える。

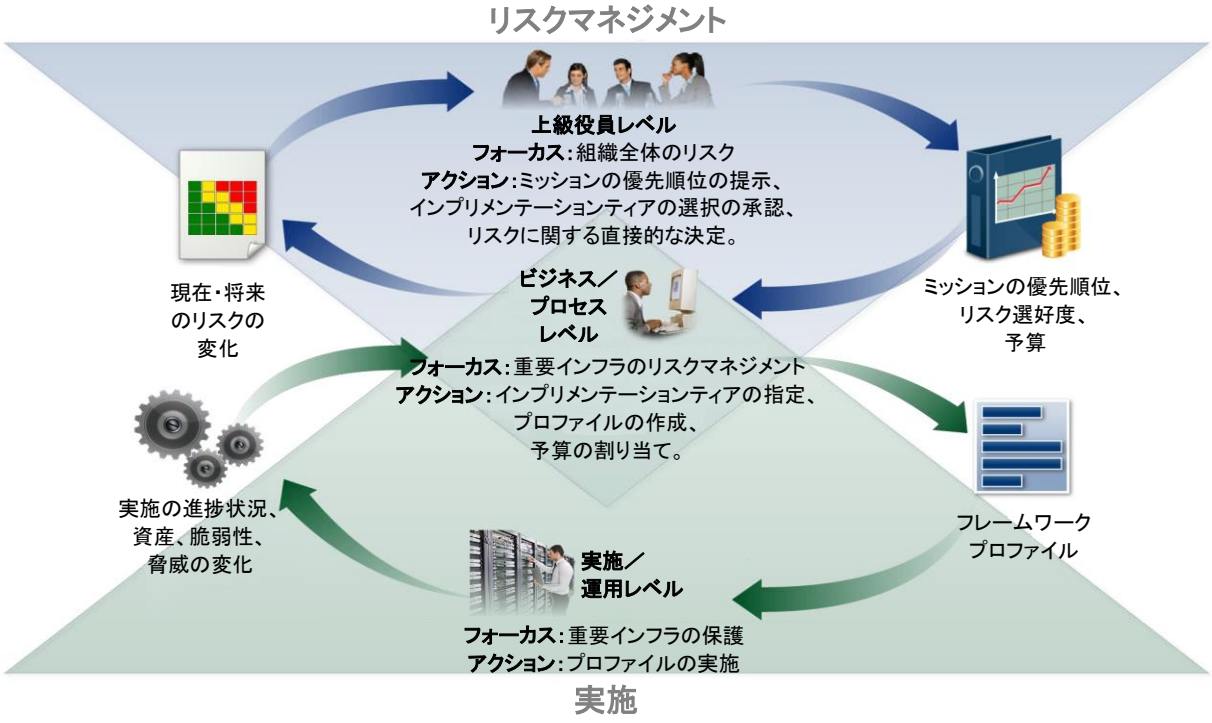

図 2: 組織内の情報と意思決定の流れ（概念図）

3.0 How to Use the Framework

An organization can use the Framework as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk. The Framework is not designed to replace existing processes; an organization can use its current process and overlay it onto the Framework to determine gaps in its current cybersecurity risk approach and develop a roadmap to improvement. Using the Framework as a cybersecurity risk management tool, an organization can determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment.

The Framework is designed to complement existing business and cybersecurity operations. It can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program. The Framework provides a means of expressing cybersecurity requirements to business partners and customers and can help identify gaps in an organization's cybersecurity practices. It also provides a general set of considerations and processes for considering privacy and civil liberties implications in the context of a cybersecurity program.

The Framework can be applied throughout the life cycle phases of plan, design, build/buy, deploy, operate, and decommission. The plan phase begins the cycle of any system and lays the groundwork for everything that follows. Overarching cybersecurity considerations should be declared and described as clearly as possible. The plan should recognize that those considerations and requirements are likely to evolve during the remainder of the life cycle. The design phase should account for cybersecurity requirements as a part of a larger multidisciplinary systems engineering process.[10] A key milestone of the design phase is validation that the system cybersecurity specifications match the needs and risk disposition of the organization as captured in a Framework Profile. The desired cybersecurity outcomes prioritized in a Target Profile should be incorporated when a) developing the system during the build phase and b) purchasing or outsourcing the system during the buy phase. That same Target Profile serves as a list of system cybersecurity features that should be assessed when deploying the system to verify all features are implemented. The cybersecurity outcomes determined by using the Framework then should serve as a basis for ongoing operation of the system. This includes occasional reassessment, capturing results in a Current Profile, to verify that cybersecurity requirements are still fulfilled. Typically, a complex web of dependencies (e.g., compensating and common controls) among systems means the outcomes documented in Target Profiles of related systems should be carefully considered as systems are decommissioned.

The following sections present different ways in which organizations can use the Framework.

3.1 Basic Review of Cybersecurity Practices

The Framework can be used to compare an organization's current cybersecurity activities with those outlined in the Framework Core. Through the creation of a Current Profile, organizations can examine the extent to which they are achieving the outcomes described in the Core Categories and Subcategories, aligned with the five high-level Functions: Identify, Protect, Detect, Respond, and Recover. An organization may find that it is already achieving the desired

[10] NIST Special Publication 800-160 Volume 1, *System Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, Ross et al, November 2016 (updated March 21, 2018), https://doi.org/10.6028/NIST.SP.800-160v1

3.0　フレームワークの使い方

組織はサイバーセキュリティリスクを識別、評価し、管理するための組織的なプロセスの重要な一部分として、*フレームワーク*を使用できる。*フレームワーク*は既存のプロセスに取って代わるものとして作成されたわけではない。組織は現行のプロセスをそのまま使用して、そのプロセスを*フレームワーク*に重ね、サイバーセキュリティリスクに対する現行の取組とのギャップを識別して、改善のためのロードマップを作成することができる。*フレームワーク*をサイバーセキュリティリスクを管理するためのツールとして使用することで、組織は重要サービスを提供する上で最も必要な対策を判断し、投資の優先順位を決定することが可能になり、結果として投資の効果を最大限に引き出せるようになる。

*フレームワーク*は既存のビジネス活動とサイバーセキュリティ活動を補完できるように意図されている。*フレームワーク*は新たなサイバーセキュリティプログラムの基盤として、あるいは既存のプログラムを改善する仕組みとして役割を果たす。*フレームワーク*はビジネスパートナーと顧客に対してサイバーセキュリティ上の要求事項を示す手段となり、組織のサイバーセキュリティプラクティスにおけるギャップの識別を支援する。また、*フレームワーク*は、サイバーセキュリティプログラムの実施に伴うプライバシーおよび人権に対する影響について、考慮すべき事項と、そうした考慮事項に対処するためのプロセス一式を提供する。

*フレームワーク*は、計画、設計、構築・調達、配備、運用、廃止のすべてのライフサイクルフェーズを通じて適用可能である。計画フェーズは、システムのライフサイクルの始まりで、その後に続くフェーズすべての基礎となる段階である。システム全体に関するサイバーセキュリティ上の考慮事項を、可能な限り明確に宣言、説明する。計画フェーズでは、これらの考慮事項と要求事項が、その後のライフサイクルの中で進化していく可能性が高いことを認識しておくべきである。設計フェーズでは、より大きな分野横断的システムエンジニアリングプロセスの一環として、サイバーセキュリティ上の要求事項に対処すべきである。[10] 設計フェーズの重要なマイルストーンは、システムのサイバーセキュリティの仕様が、*フレームワークプロファイル*で説明されている自組織のニーズとリスクの性質に見合ったものになっていることである。*目標のプロファイル*において優先順位付けされた、期待されるサイバーセキュリティ上の成果は、a）構築フェーズにおいてシステムを開発する際と、b）調達フェーズでシステムを購入またはアウトソーシングする際に、組み入れられるべきである。同一の目標のプロファイルが、システムのサイバーセキュリティ機能の評価項目一覧としての役割も果たす。システムを実際に配備し、この評価項目に基づいて、システムのサイバーセキュリティ機能がすべて実装されているか検証する。そのため、継続的なシステム運用は、*フレームワーク*を利用して判断されたサイバーセキュリティ上の成果を基にして行われるはずである。これには、随時再アセスメントを実施し、*現在のプロファイル*の状態を把握し、サイバーセキュリティ上の要求事項が満たされているかを検証することも含まれる。一般的に、システム間の依存関係が複雑な場合（例：補完制御や、共通制御）は、システムを廃止する際には、関連システムの*目標のプロファイル*に記された成果を慎重に考慮する必要がある。

以下のセクションでは、*フレームワーク*の様々な使い方を示す。

3.1　サイバーセキュリティプラクティスの基本的なレビュー

*フレームワーク*は、*コア*に記述されているサイバーセキュリティ対策と、現行のサイバーセキュリティ対策を比較するのに使用できる。*現在のプロファイル*を作成することで、組織は*「識別」*、*「防御」*、*「検知」*、*「対応」*、*「復旧」*の 5 つの高次の*機能*の観点から、*コア*の*カテゴリー*及び*サブカテゴリー*に記述されている成果が、どの程度達成されているかを検証できる。組織が既知のリスクに見合う

[10] NIST Special Publication 800-160 Volume 1, *System Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, Ross et al, 2016 年 11 月（2018 年 3 月 21 日改定）, https://doi.org/10.6028/NIST.SP.800-160v1

outcomes, thus managing cybersecurity commensurate with the known risk. Alternatively, an organization may determine that it has opportunities to (or needs to) improve. The organization can use that information to develop an action plan to strengthen existing cybersecurity practices and reduce cybersecurity risk. An organization may also find that it is overinvesting to achieve certain outcomes. The organization can use this information to reprioritize resources.

While they do not replace a risk management process, these five high-level Functions will provide a concise way for senior executives and others to distill the fundamental concepts of cybersecurity risk so that they can assess how identified risks are managed, and how their organization stacks up at a high level against existing cybersecurity standards, guidelines, and practices. The Framework can also help an organization answer fundamental questions, including "How are we doing?" Then they can move in a more informed way to strengthen their cybersecurity practices where and when deemed necessary.

3.2 Establishing or Improving a Cybersecurity Program

The following steps illustrate how an organization could use the Framework to create a new cybersecurity program or improve an existing program. These steps should be repeated as necessary to continuously improve cybersecurity.

Step 1: Prioritize and Scope. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance. Risk tolerances may be reflected in a target Implementation Tier.

Step 2: Orient. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then consults sources to identify threats and vulnerabilities applicable to those systems and assets.

Step 3: Create a Current Profile. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.

Step 4: Conduct a Risk Assessment. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

Step 5: Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and

サイバーセキュリティの管理を実施していて、期待される成果を既に達成している場合がある。また、改善の余地がある（または改善が必要である）と組織が判断する場合もある。自組織は既存のサイバーセキュリティプラクティスを強化し、サイバーセキュリティリスクを低減するための行動計画を作成する際に、そうした情報を活用できる。また、組織がとある成果を達成するために過剰な投資を行っていると判断する場合がある。この情報は、自組織がリソースの優先順位付けを見直す際に活用できる。

これらの 5 つの高次の*機能*は、リスクマネジメントプロセスに取って代わるものではないが、上級役員やその他の従業員がサイバーセキュリティリスクの基本概念を簡単につかめるようにするためのものであり、これにより従業員は、識別されたリスクがどのように管理されているかを評価し、既存のサイバーセキュリティ基準、ガイドライン、プラクティスと比較した際の組織の位置付けを評価できる。また*フレームワーク*は、組織が「我々の取組は十分であるか?」といった基本的な質問に対する答えを見つけるのに役立つ。それにより、サイバーセキュリティプラクティスの強化が必要な箇所に必要なタイミングで、十分な情報に基づいた強化対策を実施できるようになる。

3.2 サイバーセキュリティプログラムの立ち上げまたは改善

以下のステップは組織が*フレームワーク*をどのように使用して、新たなサイバーセキュリティプログラムを立ち上げたり、既存のプログラムを改善できるかを示している。これらのステップはサイバーセキュリティを継続的に改善できるよう、必要に応じて繰り返す必要がある。

ステップ 1: 優先順位付けを行い、範囲を決定する。自組織は事業目的・ミッションと、組織のハイレベルでの優先事項を識別する。この情報に基づいて、自組織はサイバーセキュリティの実施に関する戦略的な意思決定を行い、選択されたビジネスラインまたはプロセスを支援するシステムや資産の範囲を判断する。*フレームワーク*は、組織内のビジネスニーズと関連するリスク許容度が異なる、様々なビジネスラインまたはプロセスを支援するように調整できる。リスク許容度が、目標となる*インプリメンテーションティア*に反映される場合もある。

ステップ 2: 方向付けを行う。ステップ 1 で選択されたビジネスラインまたはプロセスに対するサイバーセキュリティプログラムの範囲が決定された後に、自組織は関連するシステムと資産、規制上の要求事項、全体的なリスクアプローチを識別する。その後、自組織はソース（情報源）と協力し、それらのシステムと資産に関する脅威と脆弱性を識別する。

ステップ 3: *現在のプロファイル*を作成する。自組織は*コア*の*カテゴリー*と*サブカテゴリー*の成果の内、現時点でどれが達成されているかを示す*現在のプロファイル*を作成する。一つの成果が部分的に達成されている場合は、その旨を記して、基本的な情報を提供すると後のステップで役立つ。

ステップ 4: リスクアセスメントを実施する。このアセスメントは、自組織の全体的なリスクマネジメントプロセスや過去のリスクアセスメント活動から導出される場合がある。自組織はサイバーセキュリティイベントが発生する可能性と、そのイベントが自組織にもたらす影響を把握するために、運用環境を分析する。浮上しつつあるリスクを識別し、内外のソースから得られるサイバー脅威情報を利用することで、サイバーセキュリティイベントの発生可能性や影響をより深く理解することが重要である。

ステップ 5: *目標のプロファイル*を作成する。自組織は期待されるサイバーセキュリティ成果について記述した*フレームワークカテゴリー*と*サブカテゴリー*のアセスメントに焦点を当てて*目標のプロファイル*を作成する。また、組織固有のリスクに対処するために、独自の*カテゴリー*や*サブカテゴリー*を

Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile. The Target Profile should appropriately reflect criteria within the target Implementation Tier.

Step 6: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address gaps – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile. The organization then determines resources, including funding and workforce, necessary to address the gaps. Using Profiles in this manner encourages the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan. The organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

An organization repeats the steps as needed to continuously assess and improve its cybersecurity. For instance, organizations may find that more frequent repetition of the orient step improves the quality of risk assessments. Furthermore, organizations may monitor progress through iterative updates to the Current Profile, subsequently comparing the Current Profile to the Target Profile. Organizations may also use this process to align their cybersecurity program with their desired Framework Implementation Tier.

3.3 Communicating Cybersecurity Requirements with Stakeholders

The Framework provides a common language to communicate requirements among interdependent stakeholders responsible for the delivery of essential critical infrastructure products and services. Examples include:

- An organization may use a Target Profile to express cybersecurity risk management requirements to an external service provider (e.g., a cloud provider to which it is exporting data).
- An organization may express its cybersecurity state through a Current Profile to report results or to compare with acquisition requirements.
- A critical infrastructure owner/operator, having identified an external partner on whom that infrastructure depends, may use a Target Profile to convey required Categories and Subcategories.
- A critical infrastructure sector may establish a Target Profile that can be used among its constituents as an initial baseline Profile to build their tailored Target Profiles.
- An organization can better manage cybersecurity risk among stakeholders by assessing their position in the critical infrastructure and the broader digital economy using Implementation Tiers.

Communication is especially important among stakeholders up and down supply chains. Supply chains are complex, globally distributed, and interconnected sets of resources and processes

作成・追加してもよい。また、*目標のプロファイル*を作成する際に、業界関係者、顧客、ビジネスパートナーなどの外部利害関係者がもたらす影響と、その要求事項を考慮する場合がある。*目標のプロファイル*には、目標の*インプリメンテーションティア*の基準を適切に反映させるべきである。

ステップ 6: ギャップを判断・分析し、優先順位付けを行う。自組織は*現在のプロファイル*と*目標のプロファイル*を比較してギャップを判断する。次に、組織はこれらのギャップの解消に取り組み、*目標のプロファイル*に記された成果を達成するための行動計画を作成する。この行動計画には、ミッションに基づく動機、費用対効果、リスクを反映する。続いて、ギャップに取り組むのに必要な資金、労働力等のリソースを判断する。*プロファイル*をこのように使用することで、サイバーセキュリティ対策に関して十分な情報に基づいた意思決定が可能になり、リスクマネジメントも容易になり、費用対効果の高い、目標とされる改善対策を実施しやすくなる。

ステップ 7: 行動計画を実施する。自組織はステップ 6 で識別されたギャップ（もしあれば）に対して取るべき行動を決定する。次に組織は、*目標のプロファイル*の達成に向けて、現行のサイバーセキュリティプラクティスを調整する。その他のガイダンスとして、*フレームワーク*では、*カテゴリー*と*サブカテゴリー*に関する*参考情報*の例を識別している。しかしながら、組織は業界固有のものを含め、どの基準、ガイドライン、プラクティスが組織のニーズに最適であるかを判断する必要がある。

組織は、上述のステップを必要なだけ繰り返し、サイバーセキュリティを継続的にアセスメントし、改善していく。例えば、ステップ 2「方向付けを行う」をより頻繁に実施することで、リスクアセスメントの質が改善する場合がある。さらに、*現在のプロファイル*が更新される度に、*現在のプロファイル*と*目標のプロファイル*を比較することによって、進捗状況のモニタリングが可能になる。組織はまた、この進捗状況を活用して、サイバーセキュリティプログラムを組織が選択した*フレームワークインプリメンテーションティア*に合わせて調整してもよい。

3.3　サイバーセキュリティ上の要求事項について利害関係者とコミュニケーションを行う

*フレームワーク*は、不可欠な重要インフラ製品・サービスの提供に責任を担う、互いに依存する利害関係者間で要求事項に関するコミュニケーションを可能にする共通言語を提供する。例としては以下が挙げられる。

- 組織は外部サービスプロバイダ（例:データをエクスポートしているクラウドプロバイダ）に対してサイバーセキュリティリスクマネジメント上の要求事項を伝えるために、*目標のプロファイル*を使用できる。
- 組織はサイバーセキュリティの状態を報告したり、調達要件と比較できるようにするために、*現在のプロファイル*を使用してサイバーセキュリティの状態を表すことができる。
- 重要インフラ事業者・運営者は、そのインフラが依存する外部パートナーを識別した上で、*カテゴリー*と*サブカテゴリー*を伝えるために*目標のプロファイル*を使用できる。
- 重要インフラ分野は、構成組織が活用できる初期プロファイルとして、業界独自の*目標のプロファイル*を作成することができる。
- 組織は、インプリメンテーションティアを用いて重要インフラやより広範囲なデジタル経済における自身の立場を評価することで、利害関係者間のサイバーセキュリティリスクをより適切に管理することができる。

サプライチェーンの上流・下流の利害関係者間でのコミュニケーションは、特に重要である。サプライチェーンとは、複数の階層の組織にまたがる、複雑かつグローバルに分散し、相互に連結された資源及び

between multiple levels of organizations. Supply chains begin with the sourcing of products and services and extend from the design, development, manufacturing, processing, handling, and delivery of products and services to the end user. Given these complex and interconnected relationships, supply chain risk management (SCRM) is a critical organizational function.[11]

Cyber SCRM is the set of activities necessary to manage cybersecurity risk associated with external parties. More specifically, cyber SCRM addresses both the cybersecurity effect an organization has on external parties and the cybersecurity effect external parties have on an organization.

A primary objective of cyber SCRM is to identify, assess, and mitigate "products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the cyber supply chain[12]." Cyber SCRM activities may include:

- Determining cybersecurity requirements for suppliers,
- Enacting cybersecurity requirements through formal agreement (e.g., contracts),
- Communicating to suppliers how those cybersecurity requirements will be verified and validated,
- Verifying that cybersecurity requirements are met through a variety of assessment methodologies, and
- Governing and managing the above activities.

As depicted in Figure 3, cyber SCRM encompasses technology suppliers and buyers, as well as non-technology suppliers and buyers, where technology is minimally composed of information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), and connected devices more generally, including the Internet of Things (IoT). Figure 3 depicts an organization at a single point in time. However, through the normal course of business operations, most organizations will be both an upstream supplier and downstream buyer in relation to other organizations or end users.

[11] Communicating Cybersecurity Requirements (Section 3.3) and Buying Decisions (Section 3.4) address only two uses of the Framework for cyber SCRM and are not intended to address cyber SCRM comprehensively.

[12] NIST Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, Boyens et al, April 2015, https://doi.org/10.6028/NIST.SP.800-161

プロセスである。サプライチェーンは、調達先の決定から始まり、設計、開発、製造、加工、取り扱い、エンドユーザへの製品・サービスの提供にまで及ぶ。これらの複雑な相互関係を考慮すると、サプライチェーンリスクマネジメント（SCRM）は、組織の重要な機能の一つである。[11]

サイバーSCRM は、外部関係者に関するサイバーセキュリティリスクマネジメントに必要な一連の活動である。より具体的には、サイバーSCRM は、組織が外部関係者に及ぼすサイバーセキュリティ上の影響と、外部関係者が組織に及ぼすサイバーセキュリティ上の影響の両方を扱う。

サイバーSCRM の主な目的は、「サイバーサプライチェーンにおける低品質な製造・開発プラクティスにより、潜在的に有害な機能を含む可能性のある、偽造されたまたは脆弱な製品及びサービス[12]」を識別し、評価し、抑制することである。サイバーSCRM の活動には、以下が含まれる：

- サプライヤーに対するサイバーセキュリティ上の要求事項を判断する。
- サイバーセキュリティ上の要求事項を、正式な合意（例：契約）として定める。
- それらのサイバーセキュリティ上の要求事項が、どのように検証、認証されるかについて、サプライヤーとコミュニケーションを行う。
- 様々な評価手法を用い、サイバーセキュリティ上の要求事項が満たされているか検証する。
- 上記の活動の統制、管理。

図 3 に示したとおり、サイバーSCRM には、技術系サプライヤー/バイヤーと、情報技術（IT）、産業用制御システム（ICS）、サイバーフィジカルシステム（CPS）、モノのインターネット（IOT）を含む接続機器一般といった最小限の技術のみを利用する、非技術系サプライヤー/バイヤーが含まれる。図 3 は、ある時点における組織の状態を示したものである。ただし、通常の営業活動を通じて、ほとんどの組織は、他組織またはエンドユーザとの関係において上流のサプライヤーにも、下流のバイヤーにもなる。

[11] 『3.3 サイバーセキュリティ上の要求事項について利害関係者とコミュニケーションを行う』及び『3.4 購入に関する決定』では、サイバーSCRM における本フレームワークの利用方法を2つ述べているのみで、サイバーSCRM について包括的に述べることは意図していない。

[12] NIST Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, Boyens et al, 2015 年 4 月, https://doi.org/10.6028/NIST.SP.800-161

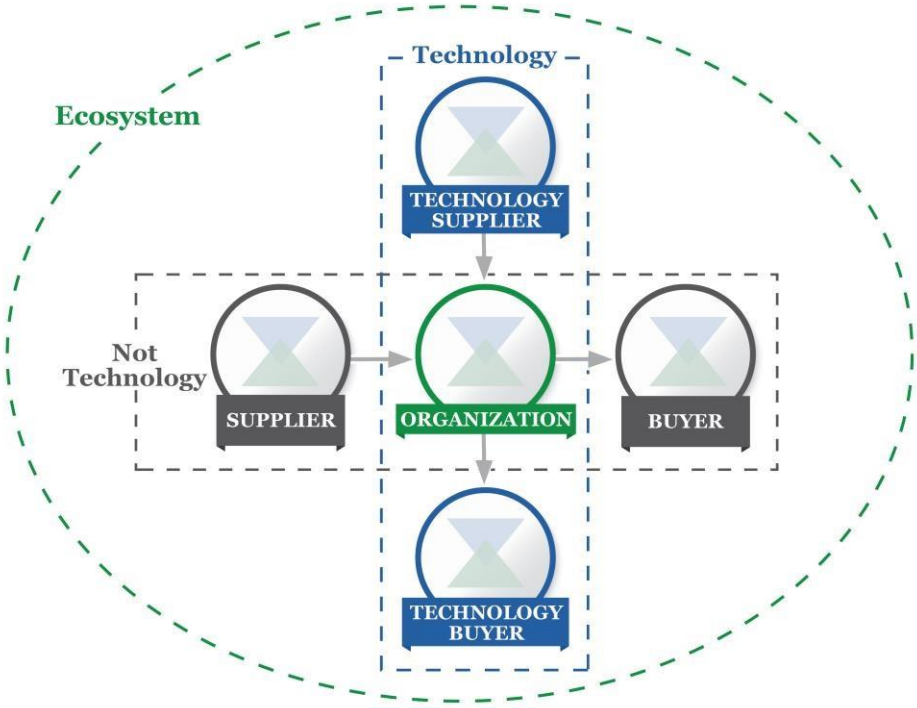

Figure 3: Cyber Supply Chain Relationships

The parties described in Figure 3 comprise an organization's cybersecurity ecosystem. These relationships highlight the crucial role of cyber SCRM in addressing cybersecurity risk in critical infrastructure and the broader digital economy. These relationships, the products and services they provide, and the risks they present should be identified and factored into the protective and detective capabilities of organizations, as well as their response and recovery protocols.

In the figure above, "Buyer" refers to the downstream people or organizations that consume a given product or service from an organization, including both for-profit and not-for-profit organizations. "Supplier" encompasses upstream product and service providers that are used for an organization's internal purposes (e.g., IT infrastructure) or integrated into the products or services provided to the Buyer. These terms are applicable for both technology-based and non-technology-based products and services.

Whether considering individual Subcategories of the Core or the comprehensive considerations of a Profile, the Framework offers organizations and their partners a method to help ensure the new product or service meets critical security outcomes. By first selecting outcomes that are relevant to the context (e.g., transmission of Personally Identifiable Information (PII), mission critical service delivery, data verification services, product or service integrity) the organization then can evaluate partners against those criteria. For example, if a system is being purchased that will monitor Operational Technology (OT) for anomalous network communication, availability may be a particularly important cybersecurity objective to achieve and should drive a Technology Supplier evaluation against applicable Subcategories (e.g., ID.BE-4, ID.SC-3, ID.SC-4, ID.SC-5, PR.DS-4, PR.DS-6, PR.DS-7, PR.DS-8, PR.IP-1, DE.AE-5).

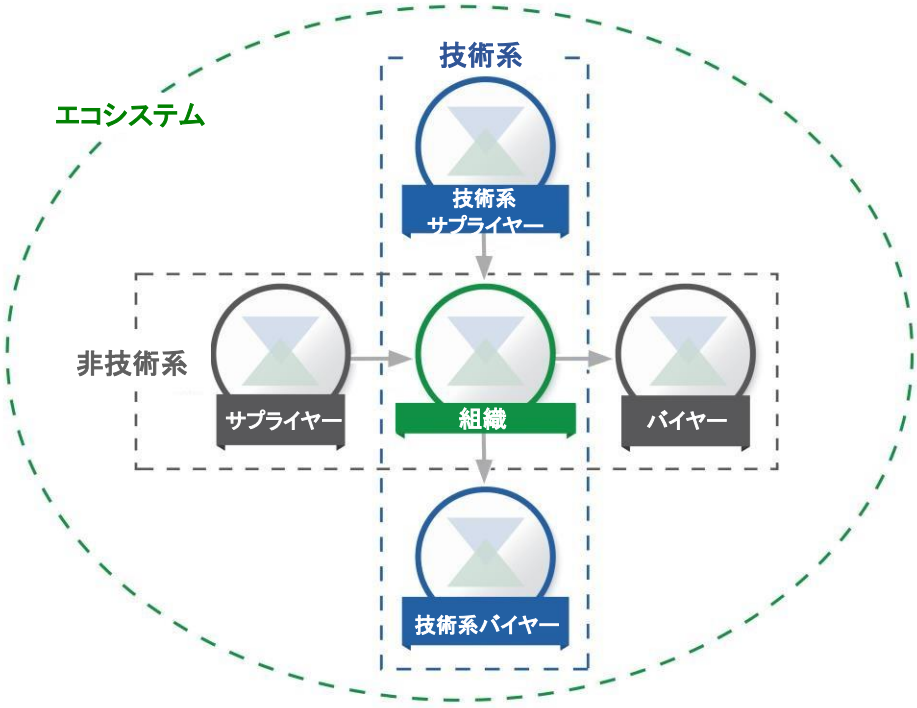

図 3:サイバーサプライチェーンにおける関係

組織のサイバーセキュリティ・エコシステムは、図 3 に示した当事者から成る。これらの関係は、重要インフラやより広範囲なデジタル経済におけるサイバーセキュリティリスクへの取り組みにおけるサイバーSCRM の役割の重要性を浮き彫りにする。これらの関係、各当事者が提供する製品及びサービス、各当事者がもたらすリスクは、識別され、組織の防御・検知機能と対応・復旧計画に反映されるべきである。

上図において、「*バイヤー*」とは、組織（営利組織・非営利組織の両方を含む）が提供する製品またはサービスを消費する、下流の人または組織を指す。「*サプライヤー*」には、組織内の目的のために利用される製品・サービス（例：IT インフラ）または*バイヤー*に提供された製品またはサービスに含まれる製品・サービスを上流で提供する者を指す。これらの用語は、技術製品・サービスと非技術製品・サービスの両方に適用される。

*フレームワークコア*の各 *サブカテゴリー*を検討するにせよ、*プロファイル*を包括的に検討するにせよ、*フレームワーク*は、組織とそのパートナーに、新規製品・サービスが重要なセキュリティ上の成果を達成することを確保するための方法を提供する。まず状況にとって適切な成果を選択すること（例：個人情報（PII）の送信、基幹サービスの提供、データ認証サービス、製品・サービス品質）により、自組織はそれらの基準をパートナーが満たすか評価することができる。例えば、オペレーショナル・テクノロジー（OT）のネットワーク通信異常を監視するシステムを購入する場合、利用可能性は、達成すべき重要なサイバーセキュリティ目標となることがあり、技術サプライヤーの評価は、これに該当するサブカテゴリーに基づいて行われるべきである（例：ID.BE-4、ID.SC-3、ID.SC-4、ID.SC-5、PR.DS-4、PR.DS-6、PR.DS-7、PR.DS-8、PR.IP-1、DE.AE-5）。

3.4 Buying Decisions

Since a Framework Target Profile is a prioritized list of organizational cybersecurity requirements, Target Profiles can be used to inform decisions about buying products and services. This transaction varies from Communicating Cybersecurity Requirements with Stakeholders (addressed in Section 3.3) in that it may not be possible to impose a set of cybersecurity requirements on the supplier. The objective should be to make the best buying decision among multiple suppliers, given a carefully determined list of cybersecurity requirements. Often, this means some degree of trade-off, comparing multiple products or services with known gaps to the Target Profile.

Once a product or service is purchased, the Profile also can be used to track and address residual cybersecurity risk. For example, if the service or product purchased did not meet all the objectives described in the Target Profile, the organization can address the residual risk through other management actions. The Profile also provides the organization a method for assessing if the product meets cybersecurity outcomes through periodic review and testing mechanisms.

3.5 Identifying Opportunities for New or Revised Informative References

The Framework can be used to identify opportunities for new or revised standards, guidelines, or practices where additional Informative References would help organizations address emerging needs. An organization implementing a given Subcategory, or developing a new Subcategory, might discover that there are few Informative References, if any, for a related activity. To address that need, the organization might collaborate with technology leaders and/or standards bodies to draft, develop, and coordinate standards, guidelines, or practices.

3.6 Methodology to Protect Privacy and Civil Liberties

This section describes a methodology to address individual privacy and civil liberties implications that may result from cybersecurity. This methodology is intended to be a general set of considerations and processes since privacy and civil liberties implications may differ by sector or over time and organizations may address these considerations and processes with a range of technical implementations. Nonetheless, not all activities in a cybersecurity program engender privacy and civil liberties considerations. Technical privacy standards, guidelines, and additional best practices may need to be developed to support improved technical implementations.

Privacy and cybersecurity have a strong connection. An organization's cybersecurity activities also can create risks to privacy and civil liberties when personal information is used, collected, processed, maintained, or disclosed. Some examples include: cybersecurity activities that result in the over-collection or over-retention of personal information; disclosure or use of personal information unrelated to cybersecurity activities; and cybersecurity mitigation activities that result in denial of service or other similar potentially adverse impacts, including some types of incident detection or monitoring that may inhibit freedom of expression or association.

The government and its agents have a responsibility to protect civil liberties arising from cybersecurity activities. As referenced in the methodology below, government or its agents that own or operate critical infrastructure should have a process in place to support compliance of cybersecurity activities with applicable privacy laws, regulations, and Constitutional requirements.

3.4 購入に関する決定

*目標のプロファイル*は、組織のサイバーセキュリティ上の要求事項を優先順位付けした一覧であるため、製品・サービスの購入に関する決定の参考情報としても利用できる。このような取引は、サプライヤーにサイバーセキュリティ上の要求事項を満たすよう求めることができないという点で、セクション 3.3『サイバーセキュリティ上の要求事項について利害関係者とコミュニケーションする』で説明したような取引とは異なる。ここでは、慎重に決定したサイバーセキュリティ上の要求事項の一覧を基に、複数のサプライヤーの中から最善のものを選んで購入することが目的である。そのため、*目標のプロファイル*とのギャップがある複数の製品またはサービスを比較して、ある程度の妥協を受け入れることもしばしば必要である。

製品またはサービスの購入後は、未解決のサイバーセキュリティリスクを追跡し、取り組むために*プロファイル*を利用することができる。例えば、購入したサービスまたは製品が、*目標のプロファイル*に記されたすべての目的を満たしていない場合、自組織は管理対策を通じて、未解決のリスクに取り組むことができる。また、*プロファイル*は、定期的なレビューとテストの仕組みを通じて、製品がサイバーセキュリティ上の成果を満たしているか評価するための方法を提供する。

3.5 新たな参考情報または改訂された参考情報の機会を識別する

*フレームワーク*は、組織による新たなニーズへの対処を支援する追加の*参考情報*が含まれる、新しい基準、ガイドライン、プラクティスの開発・改訂の機会を識別するのに使用できる。既存のサブカテゴリーを実施する組織または新規のサブカテゴリーを作成する組織が、役立つ*参考情報*をほとんど見つけられないといった状況に直面する可能性もある。こうしたニーズに対処するため、自組織には、その分野のリーダー的存在の技術ベンダや標準化団体と協力して基準、ガイドライン、プラクティスを起案、作成し、調整するといった選択肢がある。

3.6 プライバシーと人権を保護するための方法論

本セクションは、サイバーセキュリティが個人のプライバシーと人権にもたらす影響に対処するための方法を記述する。この方法はプライバシーと人権に対する影響について考慮すべき事項と、そうした考慮事項に対処するためのプロセスの一般的な例をまとめたものである。なぜ一般的な例であるかと言うと、プライバシーと人権に対する影響は業界ごとに異なったり、時間の経過とともに変わる可能性があり、組織によっては技術的実装の範囲内でそうした考慮事項やプロセスに対処することが考えられるからである。とはいえサイバーセキュリティプログラム内のすべての活動が、個人のプライバシーと人権を脅かすとは限らない。技術的プライバシー標準、ガイドライン、追加のベストプラクティスの作成が、技術的実装の改善を支援するためにも必要である。

プライバシーとサイバーセキュリティは、密接につながっている。個人情報を使用、収集、処理、維持、開示する際には、プライバシーと人権に対するリスクも生じる。例としては、個人情報の過剰収集または過剰保持につながるサイバーセキュリティ対策; サイバーセキュリティ対策とは無関係な個人情報の開示または使用; 表現の自由または結社の自由を阻害する可能性のある類のインシデント検知・モニタリングなど、サービス妨害または類似の悪影響を及ぼすサイバーセキュリティ対策といったものがある。

政府と政府機関はサイバーセキュリティ対策から人権を保護することに責任を負う。下記の方法が示すように、重要インフラを所有または運用する政府または政府機関には、サイバーセキュリティ対策がプライバシーに関して適用される法律、規制、憲法上の要求事項を遵守するのを支援するプロセスが存在するべきである。

To address privacy implications, organizations may consider how their cybersecurity program might incorporate privacy principles such as: data minimization in the collection, disclosure, and retention of personal information material related to the cybersecurity incident; use limitations outside of cybersecurity activities on any information collected specifically for cybersecurity activities; transparency for certain cybersecurity activities; individual consent and redress for adverse impacts arising from use of personal information in cybersecurity activities; data quality, integrity, and security; and accountability and auditing.

As organizations assess the Framework Core in Appendix A, the following processes and activities may be considered as a means to address the above-referenced privacy and civil liberties implications:

Governance of cybersecurity risk

- An organization's assessment of cybersecurity risk and potential risk responses considers the privacy implications of its cybersecurity program.
- Individuals with cybersecurity-related privacy responsibilities report to appropriate management and are appropriately trained.
- Process is in place to support compliance of cybersecurity activities with applicable privacy laws, regulations, and Constitutional requirements.
- Process is in place to assess implementation of the above organizational measures and controls.

Approaches to identifying, authenticating, and authorizing individuals to access organizational assets and systems

- Steps are taken to identify and address the privacy implications of identity management and access control measures to the extent that they involve collection, disclosure, or use of personal information.

Awareness and training measures

- Applicable information from organizational privacy policies is included in cybersecurity workforce training and awareness activities.
- Service providers that provide cybersecurity-related services for the organization are informed about the organization's applicable privacy policies.

Anomalous activity detection and system and assets monitoring

- Process is in place to conduct a privacy review of an organization's anomalous activity detection and cybersecurity monitoring.

Response activities, including information sharing or other mitigation efforts

- Process is in place to assess and address whether, when, how, and the extent to which personal information is shared outside the organization as part of cybersecurity information sharing activities.
- Process is in place to conduct a privacy review of an organization's cybersecurity mitigation efforts.

プライバシーへの影響に対処するために、組織は、以下のようなプライバシーの原則を組織のサイバーセキュリティプログラムに取り入れる方法を検討すべきである：サイバーセキュリティインシデントに関連する個人情報を含む資料を収集、開示、保持する際には、データを最小限に抑える; サイバーセキュリティ対策のために収集された情報の、サイバーセキュリティ対策以外の目的での使用を制限する; とあるサイバーセキュリティ対策の透明性を確保する; 個人情報をサイバーセキュリティ対策に使用することに関して、個人の同意を得て、悪影響が及んだ場合の救済措置を用意する; データの質、完全性、セキュリティを確保する; 説明責任と監査が行われるようにする。

組織が付録 A を参照して*フレームワークコア*を評価する際には、上述のプライバシーと人権に対する影響に対処する手段として、以下のプロセスと活動を検討する。

サイバーセキュリティリスクのガバナンス

- 組織によるサイバーセキュリティリスクのアセスメントと、潜在的リスクへの対応では、そのサイバーセキュリティプログラムがプライバシーにもたらす影響を考慮すること。
- サイバーセキュリティ関連のプライバシー問題に責任を負う個人は、十分な訓練を受けた者とし、適切な管理者層への報告を行うこと。
- サイバーセキュリティ対策がプライバシーに関して適用される法律、規制、憲法上の要求事項を遵守するのを支援するためのプロセスが存在すること。
- 前述の対策とコントロールの実施をアセスメントするためのプロセスが存在すること。

組織の資産とシステムにアクセスする個人を識別し、認証し、認可するためのアプローチ

- 個人情報の収集、開示、または使用を伴うアイデンティティ管理とアクセス制御における、プライバシーに対する影響を識別し、対処するための措置をとること。

意識向上とトレーニング対策

- 組織のプライバシーポリシーから抽出された必要関連情報が、サイバーセキュリティ労働力向けのトレーニング及び意識向上活動に含まれていること。
- その組織向けにサイバーセキュリティ関連サービスを提供するサービスプロバイダは、その組織の必要なプライバシーポリシーに関して知らされていること。

異常な活動の検知と、システム及び資産のモニタリング

- 組織による異常な活動の検知と、サイバーセキュリティモニタリングに対して、プライバシーの観点からのレビューを行うためのプロセスが存在すること。

情報共有またはその他の低減対策を含む対応活動

- サイバーセキュリティ情報の共有活動の一環として、いつ、どのように、どの程度の個人情報が自組織外で共有されているかを評価し、対処するためのプロセスが存在すること。
- 組織によるサイバーセキュリティ上のリスク低減対策に対して、プライバシーの観点からのレビューを行うためのプロセスが存在すること。

4.0 Self-Assessing Cybersecurity Risk with the Framework

The Cybersecurity Framework is designed to reduce risk by improving the management of cybersecurity risk to organizational objectives. Ideally, organizations using the Framework will be able to measure and assign values to their risk *along with* the cost and benefits of steps taken to reduce risk to acceptable levels. The better an organization is able to measure its risk, costs, and benefits of cybersecurity strategies and steps, the more rational, effective, and valuable its cybersecurity approach and investments will be.

Over time, self-assessment and measurement should improve decision making about investment priorities. For example, measuring – or at least robustly characterizing – aspects of an organization's cybersecurity state and trends over time can enable that organization to understand and convey meaningful risk information to dependents, suppliers, buyers, and other parties. An organization can accomplish this internally or by seeking a third-party assessment. If done properly and with an appreciation of limitations, these measurements can provide a basis for strong trusted relationships, both inside and outside of an organization.

To examine the effectiveness of investments, an organization must first have a clear understanding of its organizational objectives, the relationship between those objectives and supportive cybersecurity outcomes, and how those discrete cybersecurity outcomes are implemented and managed. While measurements of all those items is beyond the scope of the Framework, the cybersecurity outcomes of the Framework Core support self-assessment of investment effectiveness and cybersecurity activities in the following ways:

- Making choices about how different portions of the cybersecurity operation should influence the selection of Target Implementation Tiers,
- Evaluating the organization's approach to cybersecurity risk management by determining Current Implementation Tiers,
- Prioritizing cybersecurity outcomes by developing Target Profiles,
- Determining the degree to which specific cybersecurity steps achieve desired cybersecurity outcomes by assessing Current Profiles, and
- Measuring the degree of implementation for controls catalogs or technical guidance listed as Informative References.

The development of cybersecurity performance metrics is evolving. Organizations should be thoughtful, creative, and careful about the ways in which they employ measurements to optimize use, while avoiding reliance on artificial indicators of current state and progress in improving cybersecurity risk management. Judging cyber risk requires discipline and should be revisited periodically. Any time measurements are employed as part of the Framework process, organizations are encouraged to clearly identify and know why these measurements are important and how they will contribute to the overall management of cybersecurity risk. They also should be clear about the limitations of measurements that are used.

For example, tracking security measures and business outcomes may provide meaningful insight as to how changes in granular security controls affect the completion of organizational objectives. Verifying achievement of some organizational objectives requires analyzing the data only *after* that objective was to have been achieved. This type of lagging measure is more

4.0 フレームワークを利用したサイバーセキュリティリスクの自己アセスメント

*サイバーセキュリティフレームワーク*は、組織の目的に対するサイバーセキュリティリスクのマネジメントを改善することで、リスクを低減するように設計されている。*フレームワーク*を利用する組織が、リスクを許容可能なレベルまで低減するための手順の費用対効果と合わせて、リスクの値を計測し、割り当てることができると、理想的である。サイバーセキュリティ戦略・手順のリスク、費用、効果を計測する能力が高いほど、合理性、効果、価値の高いサイバーセキュリティ対策と投資が可能となる。

自己アセスメントと測定によって、投資の優先事項に関する意思決定を長期的に改善していくことが可能である。例えば、組織のサイバーセキュリティの状況と傾向を長期的に計測すること（もしくは、少なくともしっかりと特徴を把握すること）によって、有意義な情報を把握し、そのような情報を依存者、サプライヤー、バイヤー、その他の関係者に対して伝えることが可能になる。これは、組織内で行っても、第三者のアセスメント機関に依頼してもよい。このような測定は、制限を理解した上で適切に実施できれば、組織内外における強固な信頼関係の礎となる。

投資の効果を検証するには、組織はまず、組織の目的、組織の目的とそれを支えるサイバーセキュリティ上の成果の関係、そして個別のサイバーセキュリティ上の成果の実施・管理方法を明確に理解しておく必要がある。これらの項目の計測は、*フレームワーク*の範囲外であるものの、*フレームワークコア*に記されたサイバーセキュリティ上の成果は、以下のような形で、投資効果とサイバーセキュリティ対策の自己アセスメントに活用することができる。

- 様々なサイバーセキュリティ対策が*目標のインプリメンテーションティア*の選択にどのように影響するかを選択する。
- *現在のインプリメンテーションティア*を判断し、自組織のサイバーセキュリティリスクマネジメントに対するアプローチを評価する。
- *目標のプロファイル*を作成することで、サイバーセキュリティ上の成果を優先順位付けする。
- *現在のプロファイル*を評価することで、個別のサイバーセキュリティ対策の手順が、期待されるサイバーセキュリティ上の成果をどの程度達成しているか把握する。
- *参考情報*に記載された制御カタログまたは技術ガイダンスの実施の度合いを計測する。

サイバーセキュリティのパフォーマンス評価基準の開発は、絶えず進化を続けるプロセスである。組織は、測定結果を最適に利用できるよう、測定の利用方法については、深く配慮し、創造性を発揮するとともに、注意深く検討する必要がある。また、サイバーセキュリティリスクマネジメントを改善する上で、現在の状態と進捗を示す人工的な指標に依存するのは避けるべきである。サイバーリスクの判断には、規律が求められる。また、定期的な見直しも行うべきである。*フレームワーク*のプロセスの一環として計測を利用する場合は、それらの計測結果がなぜ重要なのか、あるいは、サイバーセキュリティリスク全体の管理にどのように貢献するのかといった点を、明確に識別し、理解しておくべきである。また、使用された計測の制限についても、明確にしておく必要がある。

例えば、セキュリティ対策とビジネス上の成果を追跡することで、高次のセキュリティ制御が組織の目的の達成に及ぼす影響について、有意義な見識を得ることができる。組織の目標には、一部、達成後にデータを分析することでしか、達成を検証できないものもある。このような事後的な計測の結果は、より絶対的なものではある。しかし、事前の計測によって、サイバーセキュリティリスクが生じる可能性が

absolute. However, it is often more valuable to predict whether a cybersecurity risk *may* occur, and the impact it *might* have, using a leading measure.

Organizations are encouraged to innovate and customize how they incorporate measurements into their application of the Framework with a full appreciation of their usefulness and limitations.

あるか否か、影響があり得るか否かを予測する方が、しばしば有益である。

組織には、測定の有用性と限界を十分に理解した上で、*フレームワーク*の利用に測定を取り込む方法を開発、カスタマイズしていくことが推奨される。

Appendix A: Framework Core

This appendix presents the Framework Core: a listing of Functions, Categories, Subcategories, and Informative References that describe specific cybersecurity activities that are common across all critical infrastructure sectors. The chosen presentation format for the Framework Core does not suggest a specific implementation order or imply a degree of importance of the Categories, Subcategories, and Informative References. The Framework Core presented in this appendix represents a common set of activities for managing cybersecurity risk. While the Framework is not exhaustive, it is extensible, allowing organizations, sectors, and other entities to use Subcategories and Informative References that are cost-effective and efficient and that enable them to manage their cybersecurity risk. Activities can be selected from the Framework Core during the Profile creation process and additional Categories, Subcategories, and Informative References may be added to the Profile. An organization's risk management processes, legal/regulatory requirements, business/mission objectives, and organizational constraints guide the selection of these activities during Profile creation. Personal information is considered a component of data or assets referenced in the Categories when assessing security risks and protections.

While the intended outcomes identified in the Functions, Categories, and Subcategories are the same for IT and ICS, the operational environments and considerations for IT and ICS differ. ICS have a direct effect on the physical world, including potential risks to the health and safety of individuals, and impact on the environment. Additionally, ICS have unique performance and reliability requirements compared with IT, and the goals of safety and efficiency must be considered when implementing cybersecurity measures.

For ease of use, each component of the Framework Core is given a unique identifier. Functions and Categories each have a unique alphabetic identifier, as shown in Table 1. Subcategories within each Category are referenced numerically; the unique identifier for each Subcategory is included in Table 2.

Additional supporting material, including Informative References, relating to the Framework can be found on the NIST website at http://www.nist.gov/cyberframework/.

付録 A: フレームワークコア

本付録は*フレームワークコア*、すなわち、すべての重要インフラ分野に共通となる、具体的なサイバーセキュリティ対策となる*機能*、*カテゴリー*、*サブカテゴリー*、*参考情報*の一覧を示す。本付録の*フレームワークコア*の記載は、実施に関して具体的な順番を示しているわけではなく、記載されている*カテゴリー*、*サブカテゴリー*、*参考情報*が重要度順に記載されているわけでもない。本付録に示されている*フレームワークコア*は、サイバーセキュリティリスクを管理するための対策の一般的な例である。*フレームワーク*は包括的なものではないが、拡張可能であり、組織、業界、その他の関係者が、費用対効果が高く効率的で、自身のサイバーセキュリティリスクを管理できるようになる*サブカテゴリー*と*参考情報*を活用することができる。対策は*プロファイル*作成時に*フレームワークコア*から選択でき、追加の*カテゴリー*、*サブカテゴリー*、*参考情報*を*プロファイル*に追加することもできる。組織のリスクマネジメントプロセス、法規制上の要求事項、事業目的・ミッション、組織に課せられている制約は、*プロファイル*作成時の上述の活動の選択に影響を与える。個人情報は、セキュリティリスクと保護対策をアセスメントする際に、*カテゴリー*で参照されるデータまたは資産の 1 つの要素である。

機能、*カテゴリー*、*サブカテゴリー*に識別されている目標とされる成果は IT であれ、ICS であれ同じであるが、運用環境や考慮すべき事項はそれぞれに異なる。ICS は個人の健康と安全に対する潜在的リスクと環境に対する影響など、物理的世界に直接的な影響を及ぼす。さらに、ICS には IT と比べると性能と信頼性に関するユニークな要求事項があり、サイバーセキュリティ対策を実施する際には、安全性と効率性について目標を立てる必要がある。

使いやすさを考慮して、*フレームワークコア*の各要素には個別の識別子が割り当てられている。表 1 に示されているように、*機能*と*カテゴリー*にはそれぞれアルファベットで記された個別の識別子が割り当てられている。表 2 の各*カテゴリー*内の*サブカテゴリー*には数字の、個別の識別子が割り当てられている。

*参考情報*を含む、本*フレームワーク*に関連する補足資料に関しては、下記の NIST ウェブサイトを参照すること。http://www.nist.gov/cyberframework/

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

表 1: 機能とカテゴリーの識別子

機能の識別子	機能	カテゴリーの識別子	カテゴリー
ID	識別	ID.AM	資産管理
		ID.BE	ビジネス環境
		ID.GV	ガバナンス
		ID.RA	リスクアセスメント
		ID.RM	リスクマネジメント戦略
		ID.SC	サプライチェーンリスクマネジメント
PR	防御	PR.AC	アイデンティティ管理とアクセス制御
		PR.AT	意識向上およびトレーニング
		PR.DS	データセキュリティ
		PR.IP	情報を保護するためのプロセスおよび手順
		PR.MA	保守
		PR.PT	保護技術
DE	検知	DE.AE	異常とイベント
		DE.CM	セキュリティの継続的なモニタリング
		DE.DP	検知プロセス
RS	対応	RS.RP	対応計画の作成
		RS.CO	コミュニケーション
		RS.AN	分析
		RS.MI	低減
		RS.IM	改善
RC	復旧	RC.RP	復旧計画の作成
		RC.IM	改善
		RC.CO	コミュニケーション

Table 2: Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03

表 2:フレームワークコア

機能	カテゴリー	サブカテゴリー	参考情報
識別（ID）	**資産管理**（**ID.AM**）: 自組織が事業目的を達成することを可能にするデータ、人員、デバイス、システム、施設が、識別され、組織の目的と自組織のリスク戦略における相対的な重要性に応じて管理されている。	**ID.AM-1:** 自組織内の物理デバイスとシステムが、目録作成されている。	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: 自組織内のソフトウェアプラットフォームとアプリケーションが、目録作成されている。	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: 組織内の通信とデータフロー図が、作成されている。	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: 外部情報システムが、カタログ作成されている。	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: リソース（例:ハードウェア、デバイス、データ、時間、人員、ソフトウェア）が、それらの分類、重要度、ビジネス上の価値に基づいて優先順位付けられている。	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: 全労働力と利害関係にある第三者（例:サプライヤー、顧客、パートナー）に対してのサイバーセキュリティ上の役割と責任が、定められている。	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03

Function	Category	Subcategory	Informative References
		third-party stakeholders (e.g., suppliers, customers, partners) are established	**ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1 **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** BAI03.02, DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the	**ID.GV-1:** Organizational cybersecurity policy is established and communicated	**CIS CSC** 19 **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 **ISA 62443-2-1:2009** 4.3.2.6 **ISO/IEC 27001:2013** A.5.1.1 **NIST SP 800-53 Rev. 4** -1 controls from all security control families

機能	カテゴリー	サブカテゴリー	参考情報
			ISA 62443-2-1:2009 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1 **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
	ビジネス環境（ID.BE）: 自組織のミッション、目標、利害関係者、活動が、理解され、優先順位付けが行われている。この情報は、サイバーセキュリティ上の役割、責任、リスクマネジメント上の意思決定を伝えるために使用されている。	**ID.BE-1:** サプライチェーンにおける自組織の役割が、識別され、周知されている。	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: 重要インフラとその産業分野における自組織の位置付けが、識別され、周知されている。	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** 4.1 項 **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: 組織のミッション、目標、活動の優先順位が、定められ、周知されている。	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
		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機能が、定められている。	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: 重要サービスの提供を支援するレジリエンスに関する要求事項が、すべてのオペレーション状況（例：脅迫・攻撃下、復旧時、通常時等）について定められている。	**COBIT 5** BAI03.02, DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14
	ガバナンス（ID.GV）: 自組織に対する規制、法律、リスク、環境、運用上の要求事項を、管理し、モニタリングするためのポリシー、手順、プロセスが理解されており、経営層にサイバーセキュリティリスクについて伝えている。	**ID.GV-1:** 組織のサイバーセキュリティポリシーが、定められ、周知されている。	**CIS CSC** 19 **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 **ISA 62443-2-1:2009** 4.3.2.6 **ISO/IEC 27001:2013** A.5.1.1 **NIST SP 800-53 Rev. 4** すべてのセキュリティ管理策ファミリの「XX-1」管理策

Function	Category	Subcategory	Informative References
	management of cybersecurity risk.	**ID.GV-2:** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	**CIS CSC** 19 **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	**CIS CSC** 19 **COBIT 5** BAI02.01, MEA03.01, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.7 **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 **NIST SP 800-53 Rev. 4** -1 controls from all security control families
		ID.GV-4: Governance and risk management processes address cybersecurity risks	**COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 **ISO/IEC 27001:2013** Clause 6 **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	**CIS CSC** 4 **COBIT 5** BAI08.01 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15, PM-16

機能	カテゴリー	サブカテゴリー	参考情報
		ID.GV-2: サイバーセキュリティ上の役割と責任が、内部の担当者と外部パートナーとで調整・連携されている。	**CIS CSC** 19 **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2
		ID.GV-3: プライバシーや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規制上の要求事項が、理解され、管理されている。	**CIS CSC** 19 **COBIT 5** BAI02.01, MEA03.01, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.7 **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 **NIST SP 800-53 Rev. 4** すべてのセキュリティ管理策ファミリの「XX-1」管理策
		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処している。	**COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 **ISO/IEC 27001:2013** 6 項 **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11
	リスクアセスメント（ID.RA）: 自組織は、（ミッション、機能、イメージ、評判を含む）組織の業務、組織の資産、個人に対するサイバーセキュリティリスクを把握している。	**ID.RA-1:** 資産の脆弱性が、識別され、文書化されている。	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: サイバー脅威に関する情報が、複数の情報共有フォーラムおよび複数のソースから入手されている。	**CIS CSC** 4 **COBIT 5** BAI08.01 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15, PM-16

Function	Category	Subcategory	Informative References
		ID.RA-3: Threats, both internal and external, are identified and documented	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** Clause 6.1.2 **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Potential business impacts and likelihoods are identified	**CIS CSC** 4 **COBIT 5** DSS04.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.16.1.6, Clause 6.1.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	**CIS CSC** 4 **COBIT 5** APO12.02 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
		ID.RA-6: Risk responses are identified and prioritized	**CIS CSC** 4 **COBIT 5** APO12.05, APO13.02 **ISO/IEC 27001:2013** Clause 6.1.3 **NIST SP 800-53 Rev. 4** PM-4, PM-9
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	**CIS CSC** 4 **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3, Clause 9.3 **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	**COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.2.6.5 **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 **NIST SP 800-53 Rev. 4** PM-9

機能	カテゴリー	サブカテゴリー	参考情報
		ID.RA-3: 内部および外部からの脅威が、識別され、文書化されている。	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** 6.1.2 項 **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
		ID.RA-4: ビジネスに対する潜在的な影響とその発生可能性が、識別されている。	**CIS CSC** 4 **COBIT 5** DSS04.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.16.1.6, 6.1.2 項 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11
		ID.RA-5: 脅威、脆弱性、発生可能性、影響が、リスクを判断する際に使用されている。	**CIS CSC** 4 **COBIT 5** APO12.02 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
		ID.RA-6: リスク対応が、識別され、優先順位付けされている。	**CIS CSC** 4 **COBIT 5** APO12.05, APO13.02 **ISO/IEC 27001:2013** 6.1.3 項 **NIST SP 800-53 Rev. 4** PM-4, PM-9
	リスクマネジメント戦略（ID.RM）: 自組織の優先順位、制約、リスク許容度、想定が、定められ、運用リスクに対する意思決定を支援するために利用されている。	**ID.RM-1:** リスクマネジメントプロセスが、組織の利害関係者によって定められ、管理され、承認されている。	**CIS CSC** 4 **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** 6.1.3 項, 8.3 項, 9.3 項 **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2: 組織のリスク許容度が、決定され、明確に表現されている。	**COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.2.6.5 **ISO/IEC 27001:2013** 6.1.3 項, 8.3 項 **NIST SP 800-53 Rev. 4** PM-9

Function	Category	Subcategory	Informative References
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	**COBIT 5** APO12.02 **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 **NIST SP 800-53 Rev. 4** SA-14, PM-8, PM-9, PM-11
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	**CIS CSC** 4 **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	**COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	**COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM-9
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	**COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 **ISA 62443-2-1:2009** 4.3.2.6.7 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2

機能	カテゴリー	サブカテゴリー	参考情報
		ID.RM-3: 自組織によるリスク許容度の決定が、重要インフラにおける組織の役割と、その分野に特化したリスク分析の結果に基づいて行われている。	**COBIT 5** APO12.02 **ISO/IEC 27001:2013** 6.1.3 項, 8.3 項 **NIST SP 800-53 Rev. 4** SA-14, PM-8, PM-9, PM-11
	サプライチェーンリスクマネジメント（ID.SC）: 自組織の優先順位、制約、リスク許容度、想定が、定められ、サプライチェーンリスクマネジメントに関連するリスクに対する意思決定を支援するために利用されている。自組織は、サプライチェーンリスクを識別し、分析・評価し、管理するためのプロセスを定め、実装している。	**ID.SC-1:** サイバーサプライチェーンのリスクマネジメントプロセスが、組織の利害関係者によって、識別され、定められ、評価され、管理され、承認されている。	**CIS CSC** 4 **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: 情報システム、コンポーネント、サービスのサプライヤーと第三者であるパートナーが、識別され、優先順位付けられ、サイバーサプライチェーンのリスクアセスメントプロセスにより評価されている。	**COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.SC-3: サプライヤーおよび第三者であるパートナーとの契約が、組織のサイバーセキュリティプログラムやサイバーサプライチェーンのリスクマネジメント計画の目的を達成するための適切な対策の実施に活用されている。	**COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM-9
		ID.SC-4: サプライヤーおよび第三者であるパートナーが、監査、テストの結果、またはその他の評価に基づき、契約上の義務を満たしているか、定期的に評価されている。	**COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 **ISA 62443-2-1:2009** 4.3.2.6.7 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2

Function	Category	Subcategory	Informative References
			NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	**CIS CSC** 1, 5, 15, 16 **COBIT 5** DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.5.1 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: Physical access to assets is managed and protected	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.AC-3: Remote access is managed	**CIS CSC** 12 **COBIT 5** APO13.01, DSS01.04, DSS05.03 **ISA 62443-2-1:2009** 4.3.3.6.6 **ISA 62443-3-3:2013** SR 1.13, SR 2.6 **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1

機能	カテゴリー	サブカテゴリー	参考情報
			NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.SC-5: 対応・復旧計画の策定とテストが、サプライヤーおよび第三者プロバイダーと共に行なわれている。	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
防御（PR）	**アイデンティティ管理、認証／アクセス制御（PR.AC）:** 物理的・論理的資産および関連施設へのアクセスが、認可されたユーザ、プロセス、デバイスに限定されている。また、これらのアクセスは、認可された活動およびトランザクションに対する不正アクセスのリスクアセスメントと一致して、管理されている。	**PR.AC-1:** 認可されたデバイス、ユーザ、プロセスのアイデンティティと証明書が、発行、管理、検証、取り消し、監査されている。	**CIS CSC** 1, 5, 15, 16 **COBIT 5** DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.5.1 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: 資産に対する物理アクセスが、管理され、保護されている。	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.AC-3: リモートアクセスが、管理されている。	**CIS CSC** 12 **COBIT 5** APO13.01, DSS01.04, DSS05.03 **ISA 62443-2-1:2009** 4.3.3.6.6 **ISA 62443-3-3:2013** SR 1.13, SR 2.6 **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1

Function	Category	Subcategory	Informative References
			NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	**CIS CSC** 3, 5, 12, 14, 15, 16, 18 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.7.3 **ISA 62443-3-3:2013** SR 2.1 **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	**CIS CSC** 9, 14, 15, 18 **COBIT 5** DSS01.05, DSS05.02 **ISA 62443-2-1:2009** 4.3.3.4 **ISA 62443-3-3:2013** SR 3.1, SR 3.8 **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9

機能	カテゴリー	サブカテゴリー	参考情報
			NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: アクセスの許可および認可が、最小権限の原則および役割の分離の原則を組み入れて、管理されている。	**CIS CSC** 3, 5, 12, 14, 15, 16, 18 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.7.3 **ISA 62443-3-3:2013** SR 2.1 **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		PR.AC-5: ネットワークの完全性が、保護されている（例：ネットワークの分離、ネットワークのセグメント化）。	**CIS CSC** 9, 14, 15, 18 **COBIT 5** DSS01.05, DSS05.02 **ISA 62443-2-1:2009** 4.3.3.4 **ISA 62443-3-3:2013** SR 3.1, SR 3.8 **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7
		PR.AC-6: ID は、ID 利用者の本人確認がなされ、証明書に紐付けられ、インタラクションで使用されている。	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: ユーザ、デバイス、その他の資産は、トランザクションのリスク（例：個人のセキュリティおよびプライバシー上のリスク、その他組織にとってのリスク）の度合いに応じた認証（例：一要素、多要素）が行われている。	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9

Function	Category	Subcategory	Informative References
			ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	**CIS CSC** 17, 18 **COBIT 5** APO07.03, BAI05.07 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: Privileged users understand their roles and responsibilities	**CIS CSC** 5, 17, 18 **COBIT 5** APO07.02, DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	**CIS CSC** 17 **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16
		PR.AT-4: Senior executives understand their roles and responsibilities	**CIS CSC** 17, 19 **COBIT 5** EDM01.01, APO01.02, APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	**CIS CSC** 17 **COBIT 5** APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2

機能	カテゴリー	サブカテゴリー	参考情報
			ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
	意識向上およびトレーニング（PR.AT）: 自組織の人員およびパートナーは、関連するポリシー、手順、契約に基づいた、サイバーセキュリティに関する義務と責任を果たせるようにするために、サイバーセキュリティ意識向上教育とトレーニングが実施されている。	**PR.AT-1:** すべてのユーザは、情報が周知され、トレーニングが実施されている。	**CIS CSC** 17, 18 **COBIT 5** APO07.03, BAI05.07 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: 権限を持つユーザが、自身の役割と責任を理解している。	**CIS CSC** 5, 17, 18 **COBIT 5** APO07.02, DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-3: 第三者である利害関係者（例：サプライヤー、顧客、パートナー）が、自身の役割と責任を理解している。	**CIS CSC** 17 **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16
		PR.AT-4: 上級役員（セキュリティ担当役員）が、自身の役割と責任を理解している。	**CIS CSC** 17, 19 **COBIT 5** EDM01.01, APO01.02, APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-5: 物理セキュリティおよびサイバーセキュリティの担当者が、自身の役割と責任を理解している。	**CIS CSC** 17 **COBIT 5** APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2

Function	Category	Subcategory	Informative References
			NIST SP 800-53 Rev. 4 AT-3, IR-2, PM-13
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	**CIS CSC** 13, 14 **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 **ISA 62443-3-3:2013** SR 3.4, SR 4.1 **ISO/IEC 27001:2013** A.8.2.3 **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28
		PR.DS-2: Data-in-transit is protected	**CIS CSC** 13, 14 **COBIT 5** APO01.06, DSS05.02, DSS06.06 **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	**CIS CSC** 1 **COBIT 5** BAI09.03 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
		PR.DS-4: Adequate capacity to ensure availability is maintained	**CIS CSC** 1, 2, 13 **COBIT 5** APO13.01, BAI04.04 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: Protections against data leaks are implemented	**CIS CSC** 13 **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 **ISA 62443-3-3:2013** SR 5.2 **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4,

機能	カテゴリー	サブカテゴリー	参考情報
			NIST SP 800-53 Rev. 4 AT-3, IR-2, PM-13
	データセキュリティ(PR.DS): 情報と記録(データ)が、情報の機密性、完全性、可用性を保護するための自組織のリスク戦略に従って管理されている。	**PR.DS-1:** 保存されているデータが、保護されている。	**CIS CSC** 13, 14 **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 **ISA 62443-3-3:2013** SR 3.4, SR 4.1 **ISO/IEC 27001:2013** A.8.2.3 **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28
		PR.DS-2: 伝送中のデータが、保護されている。	**CIS CSC** 13, 14 **COBIT 5** APO01.06, DSS05.02, DSS06.06 **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12
		PR.DS-3: 資産は、撤去、譲渡、廃棄に至るまで、正式に管理されている。	**CIS CSC** 1 **COBIT 5** BAI09.03 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
		PR.DS-4: 可用性を確保するのに十分な容量が、維持されている。	**CIS CSC** 1, 2, 13 **COBIT 5** APO13.01, BAI04.04 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: データ漏えいに対する防御対策が、実装されている。	**CIS CSC** 13 **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 **ISA 62443-3-3:2013** SR 5.2 **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4,

Function	Category	Subcategory	Informative References
			A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	**CIS CSC** 2, 3 **COBIT 5** APO01.06, BAI06.01, DSS06.02 **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 **NIST SP 800-53 Rev. 4** SC-16, SI-7
		PR.DS-7: The development and testing environment(s) are separate from the production environment	**CIS CSC** 18, 20 **COBIT 5** BAI03.08, BAI07.04 **ISO/IEC 27001:2013** A.12.1.4 **NIST SP 800-53 Rev. 4** CM-2
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	**COBIT 5** BAI03.05 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISO/IEC 27001:2013** A.11.2.4 **NIST SP 800-53 Rev. 4** SA-10, SI-7
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	**CIS CSC** 3, 9, 11 **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	**CIS CSC** 18 **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 **ISA 62443-2-1:2009** 4.3.4.3.3

機能	カテゴリー	サブカテゴリー	参考情報
			A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: 完全性チェックメカニズムが、ソフトウェア、ファームウェア、および情報の完全性を検証するために使用されている。	**CIS CSC** 2, 3 **COBIT 5** APO01.06, BAI06.01, DSS06.02 **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 **NIST SP 800-53 Rev. 4** SC-16, SI-7
		PR.DS-7: 開発・テスト環境が、実稼働環境から分離されている。	**CIS CSC** 18, 20 **COBIT 5** BAI03.08, BAI07.04 **ISO/IEC 27001:2013** A.12.1.4 **NIST SP 800-53 Rev. 4** CM-2
		PR.DS-8: 完全性チェックメカニズムが、ハードウェアの完全性を検証するために使用されている。	**COBIT 5** BAI03.05 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISO/IEC 27001:2013** A.11.2.4 **NIST SP 800-53 Rev. 4** SA-10, SI-7
	情報を保護するためのプロセスおよび手順（PR.IP）:（目的、範囲、役割、責任、経営コミットメント、組織間の調整について記した）セキュリティポリシー、プロセス、手順が、維持され、情報システムと資産の防御の管理に使用されている。	**PR.IP-1:** 情報技術/産業用制御システムのベースラインとなる構成は、セキュリティ原則（例：最低限の機能性の概念）を組み入れて、定められ、維持されている。	**CIS CSC** 3, 9, 11 **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: システムを管理するためのシステム開発ライフサイクルが、実装されている。	**CIS CSC** 18 **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 **ISA 62443-2-1:2009** 4.3.4.3.3

Function	Category	Subcategory	Informative References
			ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
		PR.IP-3: Configuration change control processes are in place	**CIS CSC** 3, 11 **COBIT 5** BAI01.06, BAI06.01 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
		PR.IP-4: Backups of information are conducted, maintained, and tested	**CIS CSC** 10 **COBIT 5** APO13.01, DSS01.01, DSS04.07 **ISA 62443-2-1:2009** 4.3.4.3.9 **ISA 62443-3-3:2013** SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Data is destroyed according to policy	**COBIT 5** BAI09.03, DSS05.06 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 **NIST SP 800-53 Rev. 4** MP-6

機能	カテゴリー	サブカテゴリー	参考情報
			ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
		PR.IP-3: 構成変更管理プロセスは、策定されている。	**CIS CSC** 3, 11 **COBIT 5** BAI01.06, BAI06.01 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
		PR.IP-4: 情報のバックアップが、実施され、維持され、テストされている。	**CIS CSC** 10 **COBIT 5** APO13.01, DSS01.01, DSS04.07 **ISA 62443-2-1:2009** 4.3.4.3.9 **ISA 62443-3-3:2013** SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
		PR.IP-5: 組織の資産の物理的な運用環境に関するポリシーと規制が、満たされている。	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: データは、ポリシーに従って破壊されている。	**COBIT 5** BAI09.03, DSS05.06 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 **NIST SP 800-53 Rev. 4** MP-6

Function	Category	Subcategory	Informative References
		PR.IP-7: Protection processes are improved	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 **ISO/IEC 27001:2013** A.16.1.6, Clause 9, Clause 10 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Effectiveness of protection technologies is shared	**COBIT 5** BAI08.04, DSS03.04 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	**CIS CSC** 19 **COBIT 5** APO12.06, DSS04.03 **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
		PR.IP-10: Response and recovery plans are tested	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	**CIS CSC** 5, 16 **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21

機能	カテゴリー	サブカテゴリー	参考情報
		PR.IP-7: 防御プロセスは、改善されている。	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 **ISO/IEC 27001:2013** A.16.1.6, 9 項, 10 項 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: 防御技術の有効性に関する情報が、共有されている。	**COBIT 5** BAI08.04, DSS03.04 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: （インシデント対応および事業継続）対応計画と（インシデントからの復旧および災害復旧）復旧計画が、策定され、管理されている。	**CIS CSC** 19 **COBIT 5** APO12.06, DSS04.03 **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
		PR.IP-10: 対応計画と復旧計画が、テストされている。	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14
		PR.IP-11: サイバーセキュリティには、人事に関わるプラクティス（例:アクセス権限の無効化、人員のスクリーニング）が含まれている。	**CIS CSC** 5, 16 **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21

Function	Category	Subcategory	Informative References
		PR.IP-12: A vulnerability management plan is developed and implemented	**CIS CSC** 4, 18, 20 **COBIT 5** BAI03.10, DSS05.01, DSS05.02 **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	**COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.7 **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5, MA-6
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	**CIS CSC** 3, 5 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 **NIST SP 800-53 Rev. 4** MA-4
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	**CIS CSC** 1, 3, 5, 6, 14, 15, 16 **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 **ISA 62443-2-1:2009** 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 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 **NIST SP 800-53 Rev. 4** AU Family
		PR.PT-2: Removable media is protected and its use restricted according to policy	**CIS CSC** 8, 13 **COBIT 5** APO13.01, DSS05.02, DSS05.06 **ISA 62443-3-3:2013** SR 2.3 **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9

機能	カテゴリー	サブカテゴリー	参考情報
		PR.IP-12: 脆弱性管理計画が、作成され、実装されている。	**CIS CSC** 4, 18, 20 **COBIT 5** BAI03.10, DSS05.01, DSS05.02 **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	保守（PR.MA）: 産業用制御システムと情報システムのコンポーネントの保守と修理が、ポリシーと手順に従って実施されている。	**PR.MA-1:** 組織の資産の保守と修理は、承認・管理されたツールを用いて実施され、ログが記録されている。	**COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.7 **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5, MA-6
		PR.MA-2: 組織の資産に対する遠隔保守は、承認を得て、ログが記録され、不正アクセスを防止した形式で実施されている。	**CIS CSC** 3, 5 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 **NIST SP 800-53 Rev. 4** MA-4
	保護技術（PR.PT）: 技術的なセキュリティソリューションが、関連するポリシー、手順、契約に基づいて、システムと資産のセキュリティとレジリエンスを確保するために管理されている。	**PR.PT-1:** 監査記録/ログ記録の対象が、ポリシーに従って決定され、文書化され、実装され、その記録をレビューされている。	**CIS CSC** 1, 3, 5, 6, 14, 15, 16 **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 **ISA 62443-2-1:2009** 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 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 **NIST SP 800-53 Rev. 4** AU ファミリ
		PR.PT-2: リムーバブルメディアは、保護され、その使用がポリシーに従って制限されている。	**CIS CSC** 8, 13 **COBIT 5** APO13.01, DSS05.02, DSS05.06 **ISA 62443-3-3:2013** SR 2.3 **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9

Function	Category	Subcategory	Informative References
			NIST SP 800-53 Rev. 4 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	**CIS CSC** 3, 11, 14 **COBIT 5** DSS05.02, DSS05.05, DSS06.06 **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 **ISO/IEC 27001:2013** A.9.1.2 **NIST SP 800-53 Rev. 4** AC-3, CM-7
		PR.PT-4: Communications and control networks are protected	**CIS CSC** 8, 12, 15 **COBIT 5** DSS05.02, APO13.01 **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	**COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 **ISA 62443-2-1:2009** 4.3.2.5.2 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected	**DE.AE-1:** A baseline of network operations and expected data flows for	**CIS CSC** 1, 4, 6, 12, 13, 15, 16 **COBIT 5** DSS03.01 **ISA 62443-2-1:2009** 4.4.3.3

機能	カテゴリー	サブカテゴリー	参考情報
			NIST SP 800-53 Rev. 4 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
		PR.PT-3: 最低限の機能性の原則が、必須の機能のみ提供するようにシステムを構成することによって組み入れられている。	**CIS CSC** 3, 11, 14 **COBIT 5** DSS05.02, DSS05.05, DSS06.06 **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 **ISO/IEC 27001:2013** A.9.1.2 **NIST SP 800-53 Rev. 4** AC-3, CM-7
		PR.PT-4: 通信（情報）ネットワークと制御ネットワークが、保護されている。	**CIS CSC** 8, 12, 15 **COBIT 5** DSS05.02, APO13.01 **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
		PR.PT-5: メカニズム（例：フェールセーフ、ロードバランシング、ホットスワップ）が、平時及び緊急時においてレジリエンスに関する要求事項を達成するために実装されている。	**COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 **ISA 62443-2-1:2009** 4.3.2.5.2 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
検知（DE）	**異常とイベント（DE.AE）:** 異常な活動は、検知されており、イベントがもたらす潜在的な影響が、把握されている。	**DE.AE-1:** ネットワーク運用のベースラインと、ユーザとシステムで期待されるデータフローが、定められ、管理されている。	**CIS CSC** 1, 4, 6, 12, 13, 15, 16 **COBIT 5** DSS03.01 **ISA 62443-2-1:2009** 4.4.3.3

Function	Category	Subcategory	Informative References
	and the potential impact of events is understood.	users and systems is established and managed	**ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	**CIS CSC** 3, 6, 13, 15 **COBIT 5** DSS05.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors	**CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 **COBIT 5** BAI08.02 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is determined	**CIS CSC** 4, 6 **COBIT 5** APO12.06, DSS03.01 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Incident alert thresholds are established	**CIS CSC** 6, 19 **COBIT 5** APO12.06, DSS03.01 **ISA 62443-2-1:2009** 4.2.3.10 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	**CIS CSC** 1, 7, 8, 12, 13, 15, 16 **COBIT 5** DSS01.03, DSS03.05, DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4

機能	カテゴリー	サブカテゴリー	参考情報
			ISO/IEC 27001:2013 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: 検知したイベントは、攻撃の標的と手法を理解するために分析されている。	**CIS CSC** 3, 6, 13, 15 **COBIT 5** DSS05.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: イベントデータは、複数の情報源やセンサーから収集され、相互分析されている。	**CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 **COBIT 5** BAI08.02 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: イベントがもたらす影響が、判断されている。	**CIS CSC** 4, 6 **COBIT 5** APO12.06, DSS03.01 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4
		DE.AE-5: インシデント警告の閾値が、定められている。	**CIS CSC** 6, 19 **COBIT 5** APO12.06, DSS03.01 **ISA 62443-2-1:2009** 4.2.3.10 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	セキュリティの継続的なモニタリング（DE.CM）: 情報システムと資産は、サイバーセキュリティイベントを識別し、保護対策の有効性を検証するために、モニタリングされている。	**DE.CM-1:** ネットワークは、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。	**CIS CSC** 1, 7, 8, 12, 13, 15, 16 **COBIT 5** DSS01.03, DSS03.05, DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4

Function	Category	Subcategory	Informative References
	the effectiveness of protective measures.	**DE.CM-2:** The physical environment is monitored to detect potential cybersecurity events	**COBIT 5** DSS01.04, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2 **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	**CIS CSC** 5, 7, 14, 16 **COBIT 5** DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Malicious code is detected	**CIS CSC** 4, 7, 8, 12 **COBIT 5** DSS05.01 **ISA 62443-2-1:2009** 4.3.4.3.8 **ISA 62443-3-3:2013** SR 3.2 **ISO/IEC 27001:2013** A.12.2.1 **NIST SP 800-53 Rev. 4** SI-3, SI-8
		DE.CM-5: Unauthorized mobile code is detected	**CIS CSC** 7, 8 **COBIT 5** DSS05.01 **ISA 62443-3-3:2013** SR 2.4 **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	**COBIT 5** APO07.06, APO10.05 **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	**CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 **COBIT 5** DSS05.02, DSS05.05 **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Vulnerability scans are performed	**CIS CSC** 4, 20

機能	カテゴリー	サブカテゴリー	参考情報
		DE.CM-2: 物理環境は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。	**COBIT 5** DSS01.04, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2 **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: 人員の活動は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。	**CIS CSC** 5, 7, 14, 16 **COBIT 5** DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: 悪質なコードは、検知されている。	**CIS CSC** 4, 7, 8, 12 **COBIT 5** DSS05.01 **ISA 62443-2-1:2009** 4.3.4.3.8 **ISA 62443-3-3:2013** SR 3.2 **ISO/IEC 27001:2013** A.12.2.1 **NIST SP 800-53 Rev. 4** SI-3, SI-8
		DE.CM-5: 不正なモバイルコードは、検知されている。	**CIS CSC** 7, 8 **COBIT 5** DSS05.01 **ISA 62443-3-3:2013** SR 2.4 **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44
		DE.CM-6: 外部サービスプロバイダの活動は、潜在的なサイバーセキュリティイベントを検知できるようにモニタリングされている。	**COBIT 5** APO07.06, APO10.05 **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: 権限のない人員、接続、デバイス、ソフトウェアのモニタリングが、実施されている。	**CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 **COBIT 5** DSS05.02, DSS05.05 **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: 脆弱性スキャンが、実施されている。	**CIS CSC** 4, 20

Function	Category	Subcategory	Informative References
			COBIT 5 BAI03.10, DSS05.01 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-5
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	**CIS CSC** 19 **COBIT 5** APO01.02**,** DSS05.01, DSS06.03 **ISA 62443-2-1:2009** 4.4.3.1 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: Detection activities comply with all applicable requirements	**COBIT 5** DSS06.01, MEA03.03, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.2 **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		DE.DP-3: Detection processes are tested	**COBIT 5** APO13.02, DSS05.02 **ISA 62443-2-1:2009** 4.4.3.2 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.14.2.8 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.DP-4: Event detection information is communicated	**CIS CSC** 19 **COBIT 5** APO08.04, APO12.06, DSS02.05 **ISA 62443-2-1:2009** 4.3.4.5.9 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Detection processes are continuously improved	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

機能	カテゴリー	サブカテゴリー	参考情報
			COBIT 5 BAI03.10, DSS05.01 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-5
	検知プロセス（DE.DP）: 検知プロセスおよび手順が、異常なイベントに確実に気付くために維持され、テストされている。	**DE.DP-1:** 検知に関する役割と責任は、説明責任を果たせるように明確に定義されている。	**CIS CSC** 19 **COBIT 5** APO01.02**,** DSS05.01, DSS06.03 **ISA 62443-2-1:2009** 4.4.3.1 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: 検知活動は、該当するすべての要求事項を準拠している。	**COBIT 5** DSS06.01, MEA03.03, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.2 **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		DE.DP-3: 検知プロセスが、テストされている。	**COBIT 5** APO13.02, DSS05.02 **ISA 62443-2-1:2009** 4.4.3.2 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.14.2.8 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.DP-4: イベント検知情報が、周知されている。	**CIS CSC** 19 **COBIT 5** APO08.04, APO12.06, DSS02.05 **ISA 62443-2-1:2009** 4.3.4.5.9 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: 検知プロセスが、継続的に改善されている。	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

Function	Category	Subcategory	Informative References
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**RS.RP-1:** Response plan is executed during or after an incident	**CIS CSC** 19 **COBIT 5** APO12.06, BAI01.10 **ISA 62443-2-1:2009** 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	**CIS CSC** 19 **COBIT 5** EDM03.02, APO01.02, APO12.03 **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Incidents are reported consistent with established criteria	**CIS CSC** 19 **COBIT 5** DSS01.03 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: Information is shared consistent with response plans	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.2 **ISO/IEC 27001:2013** A.16.1.2, Clause 7.4, Clause 16.1.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** Clause 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	**CIS CSC** 19 **COBIT 5** BAI08.04 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15

機能	カテゴリー	サブカテゴリー	参考情報
対応（RS）	**対応計画（RS.RP）:** 対応プロセスおよび手順が、検知したサイバーセキュリティインシデントに対応できるように実施され、維持されている。	**RS.RP-1:** 対応計画が、インシデントの発生中または発生後に実行されている。	**CIS CSC** 19 **COBIT 5** APO12.06, BAI01.10 **ISA 62443-2-1:2009** 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	コミュニケーション（RS.CO）: 対応活動が、内外の利害関係者との間で調整されている（例：法執行機関からの支援）。	**RS.CO-1:** 人員は、対応が必要になった時の自身の役割と行動の順序を認識している。	**CIS CSC** 19 **COBIT 5** EDM03.02, APO01.02, APO12.03 **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: インシデントが、定められた基準に沿って報告されている。	**CIS CSC** 19 **COBIT 5** DSS01.03 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: 対応計画に従って、情報が共有されている。	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.2 **ISO/IEC 27001:2013** A.16.1.2, 7.4 項, 16.1.2 項 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: 利害関係者との間で調整が、対応計画に従って行なわれている。	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** 7.4 項 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: サイバーセキュリティに関する状況認識を広げるために、外部利害関係者との間で自発的な情報共有が行なわれている。	**CIS CSC** 19 **COBIT 5** BAI08.04 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15

Function	Category	Subcategory	Informative References
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	**CIS CSC** 4, 6, 8, 19 **COBIT 5** DSS02.04, DSS02.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: The impact of the incident is understood	**COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: Forensics are performed	**COBIT 5** APO12.06, DSS03.02, DSS05.07 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 **ISO/IEC 27001:2013** A.16.1.7 **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: Incidents are categorized consistent with response plans	**CIS CSC** 19 **COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NIST SP 800-53 Rev. 4** SI-5, PM-15
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-1:** Incidents are contained	**CIS CSC** 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5

機能	カテゴリー	サブカテゴリー	参考情報
	分析（RS.AN）: 分析は、効果的な対応を確実にし、復旧活動を支援するために実施されている。	**RS.AN-1:** 検知システムからの通知は、調査されている。	**CIS CSC** 4, 6, 8, 19 **COBIT 5** DSS02.04, DSS02.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: インシデントがもたらす影響は、把握されている。	**COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: フォレンジックが、実施されている。	**COBIT 5** APO12.06, DSS03.02, DSS05.07 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 **ISO/IEC 27001:2013** A.16.1.7 **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: インシデントは、対応計画に従って分類されている。	**CIS CSC** 19 **COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: プロセスは、内外のソース（例：内部テスト、セキュリティ情報、セキュリティ研究者）から報告された脆弱性情報を、自組織が受け取り、分析し、対応するために定められている。	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NIST SP 800-53 Rev. 4** SI-5, PM-15
	低減（RS.MI）: 活動は、イベントの拡大を防ぎ、その影響を緩和し、インシデントを解決するために実施されている。	**RS.MI-1:** インシデントは、封じ込められている。	**CIS CSC** 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5

Function	Category	Subcategory	Informative References
			NIST SP 800-53 Rev. 4 IR-4
		RS.MI-2: Incidents are mitigated	**CIS CSC** 4, 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	**CIS CSC** 4 **COBIT 5** APO12.06 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	**COBIT 5** BAI01.13 **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: Response strategies are updated	**COBIT 5** BAI01.13, DSS04.08 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident	**CIS CSC** 10 **COBIT 5** APO12.06, DSS02.05, DSS03.04 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	**COBIT 5** APO12.06, BAI05.07, DSS04.08 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	**COBIT 5** APO12.06, BAI07.08 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8

機能	カテゴリー	サブカテゴリー	参考情報
			NIST SP 800-53 Rev. 4 IR-4
		RS.MI-2: インシデントは、緩和されている。	**CIS CSC** 4, 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-3: 新たに識別された脆弱性は、許容できるリスクである場合にはその旨を文書化され、そうでない場合にはリスクが緩和されている。	**CIS CSC** 4 **COBIT 5** APO12.06 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	改善（RS.IM）: 組織の対応活動は、現在と過去の検知/対応活動から学んだ教訓を取り入れることで改善されている。	**RS.IM-1:** 対応計画は、学んだ教訓を取り入れられている。	**COBIT 5** BAI01.13 **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, 10 項 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: 対応戦略は、更新されている。	**COBIT 5** BAI01.13, DSS04.08 **ISO/IEC 27001:2013** A.16.1.6, 10 項 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
復旧（RC）	**復旧計画（RC.RP）:** 復旧プロセスおよび手順は、サイバーセキュリティインシデントによる影響を受けたシステムや資産を復旧できるよう実行され、維持されている。	**RC.RP-1:** 復旧計画が、サイバーセキュリティインシデントの発生中または発生後に実施されている。	**CIS CSC** 10 **COBIT 5** APO12.06, DSS02.05, DSS03.04 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	改善（RC.IM）: 復旧計画およびプロセスが、学んだ教訓を将来の活動に取り入れることで改善されている。	**RC.IM-1:** 復旧計画は、学んだ教訓を取り入れている。	**COBIT 5** APO12.06, BAI05.07, DSS04.08 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, 10 項 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: 復旧戦略は、更新されている。	**COBIT 5** APO12.06, BAI07.08 **ISO/IEC 27001:2013** A.16.1.6, 10 項 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8

Function	Category	Subcategory	Informative References
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**RC.CO-1:** Public relations are managed	**COBIT 5** EDM03.02 **ISO/IEC 27001:2013** A.6.1.4, Clause 7.4
		RC.CO-2: Reputation is repaired after an incident	**COBIT 5** MEA03.02 **ISO/IEC 27001:2013** Clause 7.4
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	**COBIT 5** APO12.06 **ISO/IEC 27001:2013** Clause 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4

Information regarding Informative References described in Appendix A may be found at the following locations:

- Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
- CIS Critical Security Controls for Effective Cyber Defense (CIS Controls): https://www.cisecurity.org
- American National Standards Institute/International Society of Automation (ANSI/ISA)-62443-2-1 (99.02.01)-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731
- ANSI/ISA-62443-3-3 (99.03.03)-2013, *Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels*: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785
- ISO/IEC 27001, *Information technology -- Security techniques -- Information security management systems -- Requirements*: https://www.iso.org/standard/54534.html
- NIST SP 800-53 Rev. 4 - NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (including updates as of January 22, 2015). https://doi.org/10.6028/NIST.SP.800-53r4. Informative References are only mapped to the control level, though any control enhancement might be found useful in achieving a subcategory outcome.

Mappings between the Framework Core Subcategories and the specified sections in the Informative References are not intended to definitively determine whether the specified sections in the Informative References provide the desired Subcategory outcome.

Informative References are not exhaustive, in that not every element (e.g., control, requirement) of a given Informative Reference is mapped to Framework Core Subcategories.

機能	カテゴリー	サブカテゴリー	参考情報
	コミュニケーション（RC.CO）: 復旧活動は、内外の関係者（例：コーディネーティングセンター、インターネットサービスプロバイダ、攻撃システムのオーナー、被害者、他組織の CSIRT、ベンダ）との間で調整されている。	**RC.CO-1:** 広報活動が、管理されている。	**COBIT 5** EDM03.02 **ISO/IEC 27001:2013** A.6.1.4, 7.4 項
		RC.CO-2: 評判は、インシデント発生後に回復されている。	**COBIT 5** MEA03.02 **ISO/IEC 27001:2013** 7.4 項
		RC.CO-3: 復旧活動は、内外の利害関係者だけでなく役員と経営陣にも周知されている。	**COBIT 5** APO12.06 **ISO/IEC 27001:2013** 7.4 項 **NIST SP 800-53 Rev. 4** CP-2, IR-4

付録 A に記載されている*参考情報*に関する情報は、以下のサイトを参照のこと:

- Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
- CIS Critical Security Controls for Effective Cyber Defense (CIS Controls): https://www.cisecurity.org
- American National Standards Institute/International Society of Automation (ANSI/ISA)-62443-2-1 (99.02.01)-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731
- ANSI/ISA-62443-3-3 (99.03.03)-2013, *Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels*: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785
- ISO/IEC 27001, *Information technology -- Security techniques -- Information security management systems -- Requirements*: https://www.iso.org/standard/54534.html
- NIST SP 800-53 Rev. 4 - NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, 2013 年 4 月（2015 年 1 月 22 日時点での更新内容を含む）. https://doi.org/10.6028/NIST.SP.800-53r4. *参考情報*は制御水準に対して作成したものだが、これよりさらに制御を強化することが、サブカテゴリーに記載された成果の達成に役立つ場合もある。

*フレームワークコアサブカテゴリー*と*参考情報*に記載されたセクションとの位置付けは、*参考情報*の当該セクションが、サブカテゴリーに記載された成果の達成可否を絶対的に決定することを示すものではない。

記載された*参考情報*のすべての要素（例：制御、要求事項）が*フレームワークコアサブカテゴリー*に対して作成されているわけではないという点で、*参考情報*は完全な情報を提供するものではない。

Appendix B: Glossary

This appendix defines selected terms used in the publication.

Table 3: Framework Glossary

Buyer	The people or organizations that consume a given product or service.
Category	The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management," "Identity Management and Access Control," and "Detection Processes."
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters.
Cybersecurity	The process of protecting information by preventing, detecting, and responding to attacks.
Cybersecurity Event	A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).
Cybersecurity Incident	A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.
Detect (function)	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Framework	A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the "Cybersecurity Framework."
Framework Core	A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.
Framework Implementation Tier	A lens through which to view the characteristics of an organization's approach to risk—how an organization views cybersecurity risk and the processes in place to manage that risk.

付録 B: 用語集

本付録は、本文書で使用されている一部の用語の定義を示す。

表 3: フレームワーク用語集

バイヤー	製品またはサービスを消費する人または組織。
カテゴリー	*機能*をサイバーセキュリティ成果グループ別に細分化したものであり、計画上のニーズや個別の対策と密接に結びついている。*カテゴリー*には、たとえば「*資産管理*」、「*アイデンティティ管理とアクセス制御*」、「*検知プロセス*」がある。
重要インフラ	物理的存在か、仮想的存在かに関わらず、米国にとって必要不可欠なシステムや資産で、これらのシステムや資産が利用不能な状態になったり、破壊された場合、米国のサイバーセキュリティ、経済安全保障、国民の健康や安全、またはこれらの問題のうち複数、あるいはすべてに悪影響を与える可能性があるもの。
サイバーセキュリティ	攻撃を防止、検知し、攻撃に対応することにより情報を保護するプロセス。
サイバーセキュリティイベント	組織の業務（ミッション、能力、評判を含む）に影響を及ぼす可能性のある、サイバーセキュリティに関わる変化。
サイバーセキュリティインシデント	サイバーセキュリティイベントのうち、自組織に影響を及ぼすと判断されたもので、対応と復旧の必要が生じるもの。
検知（機能）	サイバーセキュリティイベントの発生を識別するのに適した対策を検討し、実施すること。
フレームワーク	サイバーセキュリティリスクを低減するためのリスクベースアプローチであり、以下の 3 つの要素で構成されている：*フレームワークコア*、*フレームワークプロファイル*、*フレームワークインプリメンテーションティア*。「*サイバーセキュリティフレームワーク*」としても知られている。
フレームワークコア	すべての重要インフラ分野に共通し、個別の成果を得られるようまとめられたサイバーセキュリティ対策と参考資料。*フレームワークコア*は以下の 4 つの要素で構成されている：*機能*、*カテゴリー*、*サブカテゴリー*、*参考情報*。
フレームワークインプリメンテーションティア	リスクに対する組織のアプローチの特徴（組織がサイバーセキュリティリスクをどのようにとらえているか、また、そうしたリスクを管理するためにどのようなプロセスが存在しているか）を考察する上での視点。

Framework Profile	A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.
Function	One of the main components of the Framework. Functions provide the highest level of structure for organizing basic cybersecurity activities into Categories and Subcategories. The five functions are Identify, Protect, Detect, Respond, and Recover.
Identify (function)	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
Informative Reference	A specific section of standards, guidelines, and practices common among critical infrastructure sectors that illustrates a method to achieve the outcomes associated with each Subcategory. An example of an Informative Reference is ISO/IEC 27001 Control A.10.8.3, which supports the "Data-in-transit is protected" Subcategory of the "Data Security" Category in the "Protect" function.
Mobile Code	A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics.
Protect (function)	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
Privileged User	A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
Recover (function)	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
Respond (function)	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Management	The process of identifying, assessing, and responding to risk.
Subcategory	The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated."

フレームワークプロファイル	個別のシステムまたは組織が*フレームワークカテゴリー*および*サブカテゴリー*から選択した成果を表すもの。
機能	*フレームワーク*の主要構成要素の一つ。*機能*は基本的なサイバーセキュリティ対策の最も上位を構成する要素であり、*カテゴリー*や*サブカテゴリー*にて詳細化される。機能は以下の 5 つの要素で構成されている: *識別*、*防御*、*検知*、*対応*、*復旧*。
識別（機能）	システム、資産、データ、機能に対するサイバーセキュリティリスクの管理に必要な理解を深めること。
参考情報	すべての重要インフラ分野に共通となる基準、ガイドライン、プラクティスをまとめたセクションであり、各*サブカテゴリー*に関連する、期待される成果を達成するための方法を示す。*参考情報*の一例を挙げると、ISO/IEC 27001 Control A.10.8.3 は、「防御」機能の「データセキュリティ」カテゴリーの「伝送中のデータを保護している」サブカテゴリーをサポートするものである。
モバイルコード	異なるプラットフォームに変更を加えることなく実装され、同一の意味で実行可能なプログラム（例:スクリプト、マクロ、またはその他の移植性のある命令文）。
防御（機能）	重要インフラサービスの提供を確実にするための適切な保護対策を検討し、実施すること。
権限を持つユーザ	通常のユーザの場合は実行することが認可されない、セキュリティ関連機能を実行することが認可された（すなわち、信頼されている）ユーザ。
復旧（機能）	レジリエンスを実現するための計画を策定・維持し、サイバーセキュリティイベントによって阻害されたあらゆる機能やサービスを元に戻すための適切な対策を検討し、実施すること。
対応（機能）	検知されたサイバーセキュリティイベントに対処するための適切な対策を検討し、実施すること。
リスク	発生しうる状況またはイベントによって、あるものが脅かされる程度の尺度であり、通常、(i) 当該の状況またはイベントが発生した場合にもたらされると考えられる悪影響と、(ii) 発生の可能性との計算式（関数）によって求められる。
リスクマネジメント	リスクを識別、評価し、対応するプロセス。
サブカテゴリー	*カテゴリー*を技術的な対策や管理面での対策がもたらす成果別に細分化したもの。*サブカテゴリー*には、たとえば「外部情報システムが、カタログ作成されている」、「保存されているデータが、保護されている」、「検知システムからの通知は、調査されている」などがある。

Supplier	Product and service providers used for an organization's internal purposes (e.g., IT infrastructure) or integrated into the products of services provided to that organization's Buyers.
Taxonomy	A scheme of classification.

サプライヤー	組織の内部目的のために利用される製品およびサービス（例：IT インフラ）を提供する者、または組織の*バイヤー*に提供された製品またはサービスに含まれる製品およびサービスを提供する者。
タクソノミー	分類法。

Appendix C: Acronyms

This appendix defines selected acronyms used in the publication.

ANSI	American National Standards Institute
CEA	Cybersecurity Enhancement Act of 2014
CIS	Center for Internet Security
COBIT	Control Objectives for Information and Related Technology
CPS	Cyber-Physical Systems
CSC	Critical Security Control
DHS	Department of Homeland Security
EO	Executive Order
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IoT	Internet of Things
IR	Interagency Report
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
ISO	International Organization for Standardization
IT	Information Technology
NIST	National Institute of Standards and Technology
OT	Operational Technology
PII	Personally Identifiable Information
RFI	Request for Information
RMP	Risk Management Process
SCRM	Supply Chain Risk Management
SP	Special Publication

付録 C: 略語

本付録は、本文書で使用されている一部の略語の定義を示す。

ANSI	American National Standards Institute
CEA	Cybersecurity Enhancement Act of 2014
CIS	Center for Internet Security
COBIT	Control Objectives for Information and Related Technology
CPS	Cyber-Physical Systems
CSC	Critical Security Control
DHS	Department of Homeland Security
EO	Executive Order
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IoT	Internet of Things
IR	Interagency Report
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
ISO	International Organization for Standardization
IT	Information Technology
NIST	National Institute of Standards and Technology
OT	Operational Technology
PII	Personally Identifiable Information
RFI	Request for Information
RMP	Risk Management Process
SCRM	Supply Chain Risk Management
SP	Special Publication