The NIST Cybersecurity Framework (CSF) 2.0

National Institute of Standards and Technology
This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.29

February 26, 2024

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST サイバーセキュリティフレームワーク（CSF）2.0 版

米国国立標準技術研究所
本文書は無料で入手可能である: https://doi.org/10.6028/NIST.CSWP.29
2024 年 2 月 26 日

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Abstract

The NIST Cybersecurity Framework (CSF) 2.0 provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks. It offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization — regardless of its size, sector, or maturity — to better understand, assess, prioritize, and communicate its cybersecurity efforts. The CSF does not prescribe how outcomes should be achieved. Rather, it links to online resources that provide additional guidance on practices and controls that could be used to achieve those outcomes. This document describes CSF 2.0, its components, and some of the many ways that it can be used.

Keywords

cybersecurity; Cybersecurity Framework (CSF); cybersecurity risk governance; cybersecurity risk management; enterprise risk management; Profiles; Tiers.

Audience

Individuals responsible for developing and leading cybersecurity programs are the primary audience for the CSF. The CSF can also be used by others involved in managing risk — including executives, boards of directors, acquisition professionals, technology professionals, risk managers, lawyers, human resources specialists, and cybersecurity and risk management auditors — to guide their cybersecurity-related decisions. Additionally, the CSF can be useful to those making and influencing policy (e.g., associations, professional organizations, regulators) who set and communicate priorities for cybersecurity risk management.

Supplemental Content

NIST will continue to build and host additional resources to help organizations implement the CSF, including Quick Start Guides and Community Profiles. All resources are made publicly available on the NIST CSF website. Suggestions for additional resources to reference on the NIST CSF website can always be shared with NIST at cyberframework@nist.gov.

Note to Readers

Unless otherwise noted, documents cited, referenced, or excerpted in this publication are not wholly incorporated into this publication.

Before version 2.0, the Cybersecurity Framework was called the “Framework for Improving Critical Infrastructure Cybersecurity.” This title is not used for CSF 2.0.

2024 年 2 月 26 日

要旨

NIST サイバーセキュリティフレームワーク（CSF）2.0 版は、産業界、政府機関及び他の組織がサイバーセキュリティリスクを管理する際のガイダンスを提供するものである。これは、高レベルのサイバーセキュリティの成果に関するタクソノミー（分類法）を示すものであり、どのような組織でも規模、業界、または成熟度を問わず、それぞれのサイバーセキュリティへの取組みをより深く理解し、評価し、優先順位をつけ、各方面に周知するために利用することができる。CSF は、成果をどのように達成すべきかを規定するものではない。むしろ、それらの成果を達成するために利用できるプラクティスや制御に関する付加的ガイダンスを提供するオンラインリソースへのリンクを示すものである。本文書では、CSF 2.0 版、その構成要素及び CSF を利用できる多様な形態の一部を記述する。

キーワード

サイバーセキュリティ、サイバーセキュリティフレームワーク（CSF）、サイバーセキュリティリスクガバナンス、サイバーセキュリティリスクマネジメント、企業リスクマネジメント、プロファイル、ティア

対象者

サイバーセキュリティプログラムの開発と先導に責任を負う個人が、CSF の主たる対象者である。また、CSF は、リスクマネジメントに関与する他の人々（役員、取締役、調達専門家、技術専門家、リスクマネージャー、弁護士、人事スペシャリスト及びサイバーセキュリティ／リスクマネジメント監査人を含む）も、各自のサイバーセキュリティ関連の決断を下す際のガイダンスとして利用することができる。加えて、CSF は、ポリシーを立案する人々やポリシーに影響を及ぼす人々（例：各種団体、専門家組織、規制機関）がサイバーセキュリティリスクマネジメントにおける優先順位を決め、それらを周知する際にも役立つと考えられる。

補足的内容

NIST は、引き続き、クイックスタートガイドやコミュニティプロファイルを含め、組織が CSF を実施する際に役立つ付加的なリソースを構築し、保持する。リソースはすべて、NIST の CSF ウェブサイトで公開されている。NIST CSF ウェブサイトで参照すべき付加的リソースに関する提案があればいつでも、NIST と共有していただきたい（宛先：cyberframework@nist.gov）。

読者の皆様へ

別段に記載のない限り、本書において引用、参照または抜粋されている文書は、全体的に本書に組み込まれているわけではない。2.0 版より前は、サイバーセキュリティフレームワークは「重要インフラのサイバーセキュリティを改善するためのフレームワーク」と呼ばれていた。このタイトルは CSF 2.0 版では使用しない。

Acknowledgments

The CSF is the result of a multi-year collaborative effort across industry, academia, and government in the United States and around the world. NIST acknowledges and thanks all of those who have contributed to this revised CSF. Information on the CSF development process can be found on the NIST CSF website. Lessons learned about the use of the CSF can always be shared with NIST at cyberframework@nist.gov.

2024 年 2 月 26 日

謝辞

CSF は、米国及び世界中の産学官にまたがる長年に及ぶ協力の賜物である。NIST は、この改訂版 CSF に貢献していただいたすべての方々に感謝申し上げる。CSF 開発プロセスに関する情報は、NIST の CSF ウェブサイトに掲載されている。CSF の利用について学んだ教訓をいつでも NIST と共有していただきたい（宛先：cyberframework@nist.gov）。

Table of Contents

List of Figures

Table of Contents

List of Figures

Preface

The Cybersecurity Framework (CSF) 2.0 is designed to help organizations of all sizes and sectors — including industry, government, academia, and nonprofit — to manage and reduce their cybersecurity risks. It is useful regardless of the maturity level and technical sophistication of an organization's cybersecurity programs. Nevertheless, the CSF does not embrace a one-size-fits-all approach. Each organization has both common and unique risks, as well as varying risk appetites and tolerances, specific missions, and objectives to achieve those missions. By necessity, the way organizations implement the CSF will vary.

Ideally, the CSF will be used to address cybersecurity risks alongside other risks of the enterprise, including those that are financial, privacy, supply chain, reputational, technological, or physical in nature.

The CSF *describes* desired outcomes that are intended to be understood by a broad audience, including executives, managers, and practitioners, regardless of their cybersecurity expertise. Because these outcomes are sector-, country-, and technology-neutral, they provide an organization with the flexibility needed to address their unique risks, technologies, and mission considerations. Outcomes are mapped directly to a list of potential security controls for immediate consideration to mitigate cybersecurity risks.

Although not prescriptive, the CSF assists its users in learning about and selecting specific outcomes. Suggestions for how specific outcomes may be achieved are provided in an expanding suite of online resources that complement the CSF, including a series of Quick Start Guides (QSGs). Also, various tools offer downloadable formats to help organizations that choose to automate some of their processes. The QSGs suggest initial ways to use the CSF and invite the reader to explore the CSF and related resources in greater depth. Available through the NIST CSF website, the CSF and these supplementary resources from NIST and others should be viewed as a "CSF portfolio" to help manage and reduce risks. Regardless of how it is applied, the CSF prompts its users to consider their cybersecurity posture in context and then adapt the CSF to their specific needs.

Building on previous versions, CSF 2.0 contains new features that highlight the importance of *governance* and *supply chains*. Special attention is paid to the QSGs to ensure that the CSF is relevant and readily accessible by smaller organizations as well as their larger counterparts. NIST now provides *Implementation Examples* and *Informative References*, which are available online and updated regularly. Creating current and target state *Organizational Profiles* helps organizations to compare where they are versus where they want or need to be and allows them to implement and assess security controls more quickly.

Cybersecurity risks are expanding constantly, and managing those risks must be a continuous process. This is true regardless of whether an organization is just beginning to confront its cybersecurity challenges or whether it has been active for many years with a sophisticated, well-resourced cybersecurity team. The CSF is designed to be valuable for any type of organization and is expected to provide appropriate guidance over a long time.

2024 年 2 月 26 日

前文

サイバーセキュリティフレームワーク（CSF）2.0 版は、組織の規模や業界を問わず（産業界、学術界、政府及び非営利組織を含む）組織におけるサイバーセキュリティリスクのマネジメントと低減に役立つよう設計されている。これは、組織におけるサイバーセキュリティプログラムの成熟度や技術的洗練度に関係なく有用である。とは言え、CSF は万能のアプローチを包含するわけではない。各組織には共通するリスクと固有のリスクがあるほか、リスク選好度と許容度、具体的なミッション、そしてそれらのミッションの達成に向けた目的も様々である。必然的に、組織の CSF 実施形態も変わってくる。

理想的には、企業における他のリスク、例えば財政、プライバシー、サプライチェーン、評判、技術、または物理面の性質を帯びたリスクと並行して、サイバーセキュリティリスクにも対処できるよう、CSF を利用するのが望ましい。

CSF では、期待される成果を記述するが、そうした成果の意図は、役員、マネージャー及び実務者を含む広範囲に及ぶ対象者に、サイバーセキュリティに関する各自の専門知識に関係なく理解してもらうことにある。これらの成果は業界野、国、及び技術を問わず中立的であることから、組織が固有のリスク、技術及びミッションに関する検討事項に対処する上で必要とする柔軟性を組織にもたらす。成果は、サイバーセキュリティリスクの軽減策を即座に検討するための潜在的セキュリティ管理策のリストに直接マッピングされる。

規範的ではないものの、CSF は、ユーザが具体的な成果について学び、それらの成果を選択する際の支援となる。具体的な成果をどのように達成できるかに関する提言が、一連の「クイックスタートガイド」（QSG）を含め、CSF を補足する拡大する一連のオンラインリソースに記載されている。また、組織が有するプロセスの一部を自動化することを選択する際に役立つダウンロード可能なフォーマットも、様々なツールが提供する。QSG は、初期段階での CSF の使い方を提言すると共に、読者には CSF 及び関連リソースをより深く探究することを促す。NIST の CSF ウェブサイト経由で入手可能であるが、NIST 及びその他から提供される CSF とこれらの補足的リソースを、リスクのマネジメントと低減に役立つ「CSF ポートフォリオ」として捉えるべきである。適用方法に関係なく、CSF はユーザに対し、状況に応じてサイバーセキュリティへの取組みを検討し、次いで CSF を各自の具体的なニーズに合わせて適応させることを促すものである。

旧版を基礎として、CSF 2.0 版にはガバナンスとサプライチェーンの重要性を浮き彫りにする新たな特徴が盛り込まれている。大規模な組織と同様に、小規模な組織にとっても CSF が関連性を帯び、容易にアクセスできる状況を確保すべく、QSG には特別な注意が払われている。NIST は現在、「*実装例*」と「*参考情報*」を提供しており、これらはオンラインで入手可能で、定期的に更新される。現在の状態と目標とする状態を示す「*組織プロファイル*」を作成すれば、組織の現在の状態を、組織が望む状態またはそうなる必要のある状態と比較する上で役立ち、また組織がセキュリティ管理策をより素早く実施及び評価することが可能になる。

サイバーセキュリティリスクは絶えず拡大しており、それらのリスクのマネジメントは継続的プロセスでなければならない。これは、サイバーセキュリティにおける難題と対峙し始めたばかりの組織であれ、或いは既に長年にわたり、十分なリソースを有する洗練されたサイバーセキュリティチームを擁して活発に取り組んできた組織であれ、関係なく当てはまる。CSF は、どの種類の組織にも役立つよう設計されており、また、長期間にわたり適切なガイダンスを提供するであろうと予想される。

1. Cybersecurity Framework (CSF) Overview

This document is version 2.0 of the NIST Cybersecurity Framework (*Framework* or *CSF*). It includes the following components:

- ***CSF Core***, the nucleus of the CSF, which is a taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks. The CSF Core components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome. These outcomes can be understood by a broad audience, including executives, managers, and practitioners, regardless of their cybersecurity expertise. Because the outcomes are sector-, country-, and technology-neutral, they provide an organization with the flexibility needed to address its unique risks, technologies, and mission considerations.
- ***CSF Organizational Profiles***, which are a mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes.
- ***CSF Tiers***, which can be applied to CSF Organizational Profiles to characterize the rigor of an organization's cybersecurity risk governance and management practices. Tiers can also provide context for how an organization views cybersecurity risks and the processes in place to manage those risks.

This document describes *what* desirable outcomes an organization can aspire to achieve. It does not *prescribe* outcomes nor *how* they may be achieved. Descriptions of *how* an organization can achieve those outcomes are provided in a suite of online resources that complement the CSF and are available through the NIST CSF website. These resources offer additional guidance on practices and controls that could be used to achieve outcomes and are intended to help an organization understand, adopt, and use the CSF. They include:

- *Informative References* that point to sources of guidance on each outcome from existing global standards, guidelines, frameworks, regulations, policies, etc.
- *Implementation Examples* that illustrate potential ways to achieve each outcome
- *Quick-Start Guides* that give actionable guidance on using the CSF and its online resources, including transitioning from previous CSF versions to version 2.0
- *Community Profiles* and *Organizational Profile Templates* that help an organization put the CSF into practice and set priorities for managing cybersecurity risks

An organization can use the CSF Core, Profiles, and Tiers with the supplementary resources to understand, assess, prioritize, and communicate cybersecurity risks.

- **Understand and Assess:** Describe the current or target cybersecurity posture of part or all of an organization, determine gaps, and assess progress toward addressing those gaps.

1. サイバーセキュリティフレームワーク（CSF）の概要

本文書は NIST サイバーセキュリティフレームワーク（以下、単に「フレームワーク」または「CSF」）の 2.0 版である。本文書は、以下の構成要素を含む。

- ***CSF コア***： CSF の中核であり、これはどの組織においても自組織のサイバーセキュリティリスクのマネジメントに役立ち得る、高レベルのサイバーセキュリティの成果に関するタクソノミー（分類法）である。CSF コアの構成要素は、「機能」、「カテゴリー」及び個々の成果を詳述する「サブカテゴリー」から成る階層である。これらの成果は、役員、マネージャー及び実務者を含む広範囲に及ぶ対象者が、サイバーセキュリティに関する各自の専門知識に関係なく理解することができる。成果は、業界、国、及び技術を問わず中立的であることから、組織が固有のリスク、技術及びミッションに関する検討事項に対処する上で必要とする柔軟性を組織にもたらす。
- ***CSF 組織プロファイル***：これは組織における現在のまたは目標とするサイバーセキュリティへの取組みを、CSF コアの成果の観点から記述するためのメカニズムである。
- ***CSF ティア***：これを CSF 組織プロファイルに適用することにより、組織におけるサイバーセキュリティリスクのガバナンスとマネジメントプラクティスの厳密さを特徴付けることができる。また、ティアは、組織におけるサイバーセキュリティリスクの捉え方と、それらのリスクのマネジメントのために整備されるプロセスに対する文脈も提供する。

本文書では、組織が達成を切望し得る、期待される成果にはどのようなものがあるかを記述する。本文書では、成果を規定するわけでもなければ、成果の達成方法を記述するわけでもない。組織がそれらの成果を達成し得る*方法*については、CSF を補足する一連のオンラインリソースに記載されており、NIST の CSF ウェブサイト経由で入手可能である。これらのリソースは、成果を達成するために利用できるプラクティスや管理策に関する付加的ガイダンスを提供するものであり、組織が CSF を理解し、導入及び利用する際に役立ててもらうことを意図している。例として以下が挙げられる。

- *参考情報*：個々の成果に関して、既存のグローバルな標準、ガイドライン、フレームワーク、規制、ポリシーなどからのガイダンスの情報源を紹介する。
- *実装例*：個々の成果を達成するための潜在的な形態を例示する。
- *クイックスタートガイド*：CSF 及び CSF オンラインリソースに関して、CSF の旧版から 2.0 版への移行を含め、すぐに実践可能なガイダンスを示す。
- *コミュニティプロファイル及び組織プロファイルテンプレート*：組織が CSF を実用化し、サイバーセキュリティリスクマネジメントにおける優先事項を決める際に役立つ。

組織は CSF のコア、プロファイル及びティアを、補足的リソースと併せて利用することにより、サイバーセキュリティリスクを理解し、評価し、優先順位を決め、周知することができる。

- **理解し評価する**：組織の一部または全体におけるサイバーセキュリティへの現在のまたは目標とする取組みを記述し、ギャップを判断し、それらのギャップへの対処に向けた進捗状況を評価する。

- **Prioritize:** Identify, organize, and prioritize actions for managing cybersecurity risks that align with the organization's mission, legal and regulatory requirements, and risk management and governance expectations.
- **Communicate:** Provide a common language for communicating inside and outside the organization about cybersecurity risks, capabilities, needs, and expectations.

The CSF is designed to be used by organizations of all sizes and sectors, including industry, government, academia, and nonprofit organizations, regardless of the maturity level of their cybersecurity programs. The CSF is a foundational resource that may be adopted voluntarily and through governmental policies and mandates. The CSF's taxonomy and referenced standards, guidelines, and practices are not country-specific, and previous versions of the CSF have been leveraged successfully by many governments and other organizations both inside and outside of the United States.

The CSF should be used in conjunction with other resources (e.g., frameworks, standards, guidelines, leading practices) to better manage cybersecurity risks and inform the overall management of information and communications technology (ICT) risks at an enterprise level. The CSF is a flexible framework that is intended to be tailored for use by all organizations regardless of size. Organizations will continue to have unique risks — including different threats and vulnerabilities — and risk tolerances, as well as unique mission objectives and requirements. Thus, organizations' approaches to managing risks and their implementations of the CSF will vary.

The remainder of this document is structured as follows:

- Section 2 explains the basics of the CSF Core: Functions, Categories, and Subcategories.
- Section 3 defines the concepts of CSF Profiles and Tiers.
- Section 4 provides an overview of selected components of the CSF's suite of online resources: Informative References, Implementation Examples, and Quick Start Guides.
- Section 5 discusses how an organization can integrate the CSF with other risk management programs.
- Appendix A is the CSF Core.
- Appendix B contains a notional illustration of the CSF Tiers.
- Appendix C is a glossary of CSF terminology.

- **優先順位を決める**: 組織のミッション、法的要求事項と規制上の要求事項、そしてリスクマネジメントとリスクガバナンスにおける期待事項と整合的なサイバーセキュリティリスクマネジメントのための行動を識別し、組織化し、優先順位を決める。
- **周知する**: サイバーセキュリティリスク、能力、ニーズ及び期待事項に関する情報を組織の内外に周知するための共通の言語を提供する。

CSF は、産業界、学術界、政府及び非営利組織を含め、あらゆる規模、あらゆる業界の組織がそれぞれのサイバーセキュリティプログラムの成熟度に関係なく利用できるよう設計されている。CSF は、自主的に、あるいは政府の政策や付託を通じて採用可能な基礎的なリソースである。CSF のタクソノミー及び参照される標準、ガイドライン及びプラクティスは国別に特有のものではなく、旧版の CSF を多数の国々の政府や、他にも米国の内外を問わず様々な組織が成功裏に活用している。

サイバーセキュリティリスクマネジメントを改善し、情報通信技術（ICT）リスクの企業レベルでの全体的なマネジメントの情報源として利用できるよう、CSF を他のリソース（例：フレームワーク、標準、ガイドライン、主導的プラクティス）と併用すべきである。CSF は、規模に関係なくあらゆる組織が利用できるよう調整されることを意図する、柔軟性のあるフレームワークである。組織は、今後も引き続き、固有のリスク（様々な脅威や脆弱性を含む）を抱え、リスク許容度を有するほか、固有のミッションに関する目的と要求事項を有することになる。したがって、組織のリスクマネジメントに対するアプローチと CSF の実施形態も異なってくる。

本文書の残り部分の構成は、以下の通りである。

- セクション 2 は、CSF コアの基礎である機能、カテゴリー及びサブカテゴリーを説明する。
- セクション 3 は、CSF プロファイルと CSF ティアの概念を定義する。
- セクション 4 は、CSF に関する一連のオンラインリソースの代表的な構成要素、即ち参考情報、実装例及びクイックスタートガイドの概要を紹介する。
- セクション 5 は、組織が CSF を他のリスクマネジメントプログラムと統合し得る形態について論ずる。
- Appendix A は、CSF コアの説明である。
- Appendix B は、CSF ティアの概念的図解を記載する。
- Appendix C は、CSF 用語集である。

2. Introduction to the CSF Core

Appendix A is the CSF Core — a set of cybersecurity outcomes arranged by Function, then Category, and finally Subcategory, as depicted in Fig. 1. These outcomes are not a checklist of actions to perform; specific actions taken to achieve an outcome will vary by organization and use case, as will the individual responsible for those actions. Additionally, the order and size of Functions, Categories, and Subcategories in the Core does not imply the sequence or importance of achieving them. The structure of the Core is intended to resonate most with those charged with operationalizing risk management within an organization.

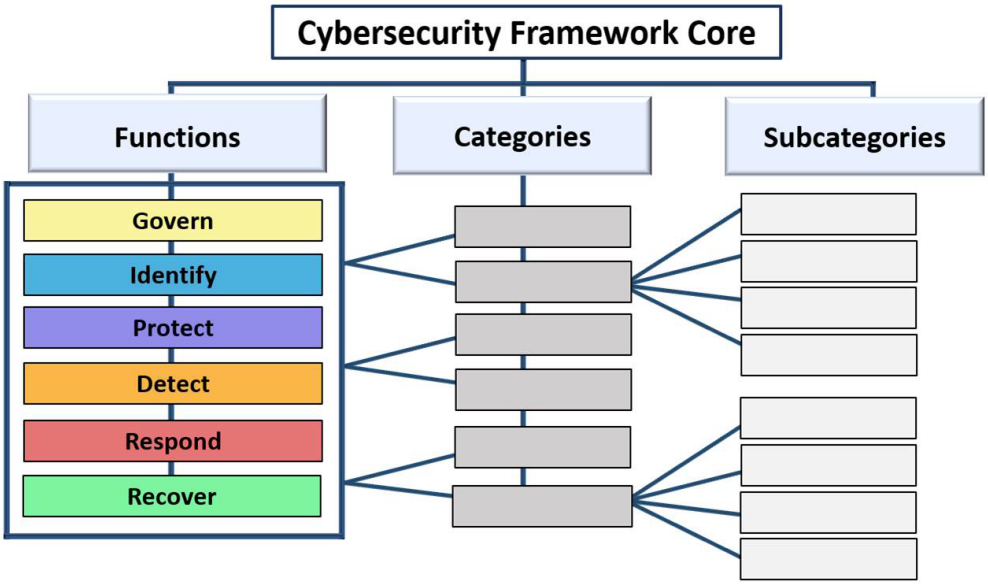

Fig. 1. CSF Core structure

The CSF Core Functions — GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER — organize cybersecurity outcomes at their highest level.

- **GOVERN (GV)** — *The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.* The GOVERN Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management (ERM) strategy. GOVERN addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.
- **IDENTIFY (ID)** — *The organization's current cybersecurity risks are understood.* Understanding the organization's assets (e.g., data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs identified under GOVERN. This Function also includes the identification of

2. CSF コアの紹介

Appendix A で CSF コアを説明するが、これは図 1 に描かれている通り、サイバーセキュリティにおける一連の成果を機能別に、次いでカテゴリー別に、そして最後にサブカテゴリー別に整理したものである。これらの成果は実行すべき措置のチェックリストではない。或る成果を達成するために講じられる具体的な措置は組織やユースケースによって異なり、同様にそれらの措置の責任者も異なってくる。加えて、コアにおける機能、カテゴリー、及びサブカテゴリーの順序と規模は、成果達成の順序または重要性を暗に意味するわけでもない。コアの構造は、組織内でのリスクマネジメント運用を担当する人々の共感を最も呼ぶことを意図している。

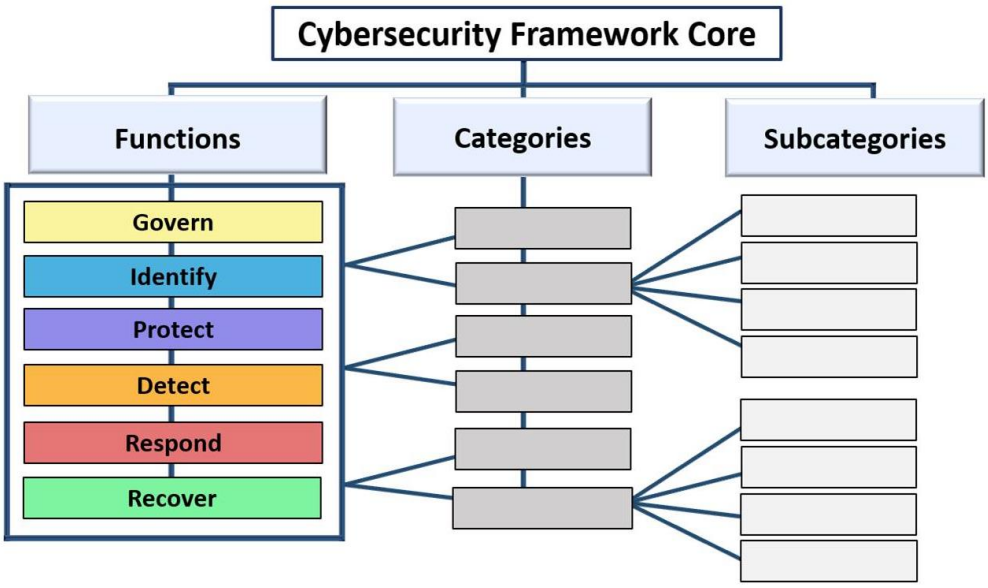

図 1. CSF コアの構造

CSF コアの諸機能（統制、識別、防御、検知、対応、及び復旧）は、サイバーセキュリティの成果をそれぞれの最も高いレベルで体系化するものである。

- **統制（GV：GOVERN）** — *組織におけるサイバーセキュリティリスクマネジメントの戦略、期待事項及びポリシーを確立し、周知し、モニタリングする。*統制機能は、組織のミッションと利害関係者の期待事項を背景に、他の 5 つの機能における成果の達成と優先順位決めに際して組織が何を行うことができるかについての情報源となる成果を提供する。統制活動は、組織のより広範な企業リスクマネジメント（ERM）戦略にサイバーセキュリティを組み入れる上で重要である。統制機能では、組織の状況の理解、サイバーセキュリティ戦略とサイバーセキュリティサプライチェーンリスクマネジメントの確立、役割／責任／権限、ポリシー、及びサイバーセキュリティ戦略の監督に対処する。
- **識別（ID：IDENTIFY）** — *組織の現在のサイバーセキュリティリスクを理解する。*組織の資産（例：データ、ハードウェア、ソフトウェア、システム、施設、サービス、人員）、サプライヤー及び関連するサイバーセキュリティリスクを理解すれば、自組織のリスクマネジメント戦略と、統制機能の下で識別されるミッションニーズと整合的な取組みを優先することができる。

improvement opportunities for the organization's policies, plans, processes, procedures, and practices that support cybersecurity risk management to inform efforts under all six Functions.

- **PROTECT (PR)** — *Safeguards to manage the organization's cybersecurity risks are used.* Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events, as well as to increase the likelihood and impact of taking advantage of opportunities. Outcomes covered by this Function include identity management, authentication, and access control; awareness and training; data security; platform security (i.e., securing the hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure.
- **DETECT (DE)** — *Possible cybersecurity attacks and compromises are found and analyzed.* DETECT enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring. This Function supports successful incident response and recovery activities.
- **RESPOND (RS)** — *Actions regarding a detected cybersecurity incident are taken.* RESPOND supports the ability to contain the effects of cybersecurity incidents. Outcomes within this Function cover incident management, analysis, mitigation, reporting, and communication.
- **RECOVER (RC)** — *Assets and operations affected by a cybersecurity incident are restored.* RECOVER supports the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts.

> While many cybersecurity risk management activities focus on preventing negative events from occurring, they may also support taking advantage of positive opportunities. Actions to reduce cybersecurity risk might benefit an organization in other ways, like increasing revenue (e.g., first offering excess facility space to a commercial hosting provider for hosting their own and other organizations' data centers, then moving a major financial system from the organization's in-house data center to the hosting provider to reduce cybersecurity risks).

Figure 2 shows the CSF Functions as a wheel because all of the Functions relate to one another. For example, an organization will categorize assets under IDENTIFY and take steps to secure those assets under PROTECT. Investments in planning and testing in the GOVERN and IDENTIFY Functions will support timely detection of unexpected events in the DETECT Function, as well as enabling incident response and recovery actions for cybersecurity incidents in the RESPOND and RECOVER Functions. GOVERN is in the center of the wheel because it informs how an organization will implement the other five Functions.

この機能には、6 つの機能すべての下での取組みの情報源としてサイバーセキュリティリスクマネジメントの支援となる組織のポリシー、計画、プロセス、手順、及びプラクティスを改善する機会の識別も含まれる。

- **防御（PR: PROTECT）** — *組織のサイバーセキュリティを管理するための保護対策を用いる。*資産とリスクが識別され、優先順位が決まったら、防御機能は、有害なサイバーセキュリティ事象の発生可能性とその影響を防止または低減する能力はもとより、機会を活用する可能性とその効果を高める能力も支援する。この機能の対象となる成果の例として、アイデンティティ管理／認証／アクセス制御、意識向上とトレーニング、データセキュリティ、プラットフォームセキュリティ（即ちハードウェア、ソフトウェア、物理的プラットフォームと仮想プラットフォームのサービスの保安）、及び技術インフラのレジリエンスが挙げられる。
- **検知（DE: DETECT）** — *サイバーセキュリティに対して起こり得る攻撃や侵入を発見し、分析する。*検知機能は、異常事態、侵入の兆候、及びその他、サイバーセキュリティ攻撃やインシデントが発生していることを示唆し得る潜在的な有害イベントの兆候の適時な発見と分析を可能にする。この機能はインシデント対応と復旧活動の成功を支援する。
- **対応（RS: RESPOND）** — *検知されたサイバーセキュリティインシデントに関する措置を講じる。*対応機能は、サイバーセキュリティインシデントの影響を封じ込める能力を支援する。この機能に該当する成果の対象は、インシデントの管理、分析、軽減、報告及びコミュニケーションである。
- **復旧（RC: RECOVER）** — *サイバーセキュリティインシデントの影響を受けた資産や運用が復旧する。*サイバーセキュリティリスクマネジメント活動の多くは、悪影響を及ぼす事象の発生防止に焦点を当てる一方、プラスの効果を得る機会の活用も支援し得る。

サイバーセキュリティリスクを低減するための措置は、収益の増加など、他にも様々な形で組織に恩恵をもたらす可能性がある（例：まず、自社や他の組織のデータセンターをホスティングするために余剰施設スペースを商用ホスティングプロバイダーに提供し、次にサイバーセキュリティリスクを軽減するために主要な会計システムを組織の社内データセンターからホスティングプロバイダーに移行します）。

図 2 では、CSF の諸機能を車輪に例えて示しているが、これらの機能はすべて互いに関連するからである。例えば、或る組織は資産を識別機能に分類し、それらの資産を防御機能の下で保安するための措置を講じる。統制機能と識別機能における計画作成とテストへの投資は、検知機能における予想外の事象の適時な検知の支援に繋がるほか、対応機能と復旧機能におけるサイバーセキュリティインシデントに対するインシデント対応措置と復旧措置を可能にする。統制機能が車輪の中央に位置するのは、他の 5 つの機能を組織が実施する際の情報源になるからである。

Fig. 2. CSF Functions

The Functions should be addressed concurrently. Actions that support GOVERN, IDENTIFY, PROTECT, and DETECT should all happen continuously, and actions that support RESPOND and RECOVER should be ready at all times and happen when cybersecurity incidents occur. All Functions have vital roles related to cybersecurity incidents. GOVERN, IDENTIFY, and PROTECT outcomes help prevent and prepare for incidents, while GOVERN, DETECT, RESPOND, and RECOVER outcomes help discover and manage incidents.

Each Function is named after a verb that summarizes its contents. Each Function is divided into *Categories*, which are related cybersecurity outcomes that collectively comprise the Function. *Subcategories* further divide each Category into more specific outcomes of technical and management activities. The Subcategories are not exhaustive, but they describe detailed outcomes that support each Category.

The Functions, Categories, and Subcategories apply to all ICT used by an organization, including information technology (IT), the Internet of Things (IoT), and operational technology (OT). They also apply to all types of technology environments, including cloud, mobile, and artificial intelligence systems. The CSF Core is forward-looking and intended to apply to future changes in technologies and environments.

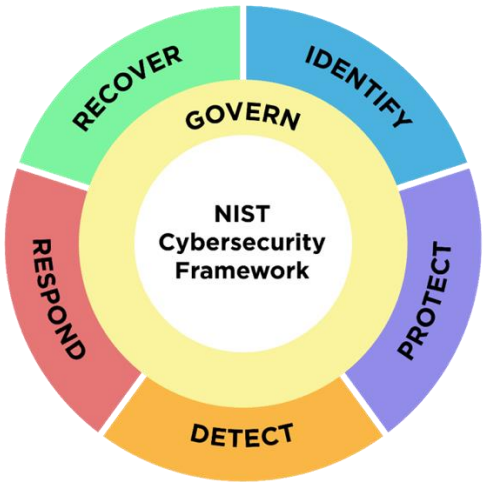

図 2. CSF の諸機能

これらの機能に同時に対処すべきである。統制、識別、防御、及び検知を支援する措置はすべて連続的に講じられるべきであり、対応と復旧を支援する措置は常に準備が整っている状態で、サイバーセキュリティインシデントの発生時に講じられるべきである。すべての機能が、サイバーセキュリティインシデントとの関連で不可欠な役割を担う。統制、識別、及び防御の成果はインシデントの防止やインシデントへの備えに役立つ一方、統制、検知、対応、及び復旧の成果はインシデントの発見と管理に役立つ。

各機能は、それぞれの内容を要約する動詞に因んで命名されている。各機能は、複数のカテゴリーに分けられ、これらのカテゴリーは集合的にその機能の構成要素として関連するサイバーセキュリティの成果を指す。サブカテゴリーは、各カテゴリーを更に、技術的活動や管理活動のより具体的な成果へと細分化したものである。サブカテゴリーは網羅的ではなく、各カテゴリーを支援する詳細な成果を表す。

機能、カテゴリー、及びサブカテゴリーは、情報技術（IT）、モノのインターネット（IoT）、及び運用技術（OT）を含め、組織が利用するあらゆる ICT に当てはまる。また、クラウドシステム、モバイルシステム、及び人工知能システムを含め、あらゆる種類の技術環境にも当てはまる。CSF コアは先を見越して、将来における技術や環境の変化に適用されることを意図するものである。

3. Introduction to CSF Profiles and Tiers

This section defines the concepts of CSF Profiles and Tiers.

3.1. CSF Profiles

A *CSF Organizational Profile* describes an organization's current and/or target cybersecurity posture in terms of the Core's outcomes. Organizational Profiles are used to understand, tailor, assess, prioritize, and communicate the Core's outcomes by considering an organization's mission objectives, stakeholder expectations, threat landscape, and requirements. An organization can then prioritize its actions to achieve specific outcomes and communicate that information to stakeholders.

Every Organizational Profile includes one or both of the following:

1. A *Current Profile* specifies the Core outcomes that an organization is currently achieving (or attempting to achieve) and characterizes how or to what extent each outcome is being achieved.
2. A *Target Profile* specifies the desired outcomes that an organization has selected and prioritized for achieving its cybersecurity risk management objectives. A Target Profile considers anticipated changes to the organization's cybersecurity posture, such as new requirements, new technology adoption, and threat intelligence trends.

> A *Community Profile* is a baseline of CSF outcomes that is created and published to address shared interests and goals among a number of organizations. A Community Profile is typically developed for a particular sector, subsector, technology, threat type, or other use case. An organization can use a Community Profile as the basis for its own Target Profile. Examples of Community Profiles can be found on the NIST CSF website.

The steps shown in Fig. 3 and summarized below illustrate one way that an organization could use an Organizational Profile to help inform continuous improvement of its cybersecurity.

Fig. 3. Steps for creating and using a CSF Organizational Profile

3. CSF プロファイルと CSF ティアの紹介

本セクションでは、CSF プロファイルと CSF ティアの概念を定義する。

3.1. CSF プロファイル

CSF 組織プロファイルは、組織の現在のまたは目標とするサイバーセキュリティへの取組みを、コアの成果に関して表すものである。組織プロファイルは、組織のミッションの目的、利害関係者の期待事項、脅威の情勢、及び要求事項を検討することによる、コアの成果の理解、調整、評価、優先順位決め、及び周知に利用される。その後、組織は具体的な成果を達成するための措置の優先順位を決め、その情報を利害関係者に周知することができる。

組織プロファイルはすべて、以下のいずれかまたは両方を含む。

1. *現在のプロファイル*では、組織が現在達成しつつある（または達成を試みている）コアの成果を具体的に示し、個々の成果の達成形態または達成の度合いを特徴付ける。
2. *目標のプロファイル*では、組織が自組織のサイバーセキュリティリスクマネジメントの目的を達成するために選択し優先順位を付けた期待する成果を具体的に示す。目標のプロファイルでは、組織のサイバーセキュリティへの取組みにおいて予想される変化、例えば新たな要求事項、新たな技術の採用、及び脅威インテリジェンスの動向などを検討する。

> コミュニティプロファイルは、多数の組織の間で共有される利益と目標に対処するために作成及び公表される、CSF の成果のベースラインである。コミュニティプロファイルは典型的に、特定の業界、従属業界、技術、脅威の種類、または他のユースケースを考慮して開発される。組織はコミュニティプロファイルを、固有の目標のプロファイルの基礎として利用できる。コミュニティプロファイルの例は、NIST の CSF ウェブサイトに掲載されている。

図 3 に記載されている通り、以下に要約される手順は、組織のサイバーセキュリティの継続的な改善に役立つ情報源として組織プロファイルを利用できる一形態の例示である。

図 3. CSF 組織プロファイルを作成及び利用する際の手順

1. **Scope the Organizational Profile.** Document the high-level facts and assumptions on which the Profile will be based to define its scope. An organization can have as many Organizational Profiles as desired, each with a different scope. For example, a Profile could address an entire organization or be scoped to an organization's financial systems or to countering ransomware threats and handling ransomware incidents involving those financial systems.
2. **Gather the information needed to prepare the Organizational Profile.** Examples of information may include organizational policies, risk management priorities and resources, enterprise risk profiles, business impact analysis (BIA) registers, cybersecurity requirements and standards followed by the organization, practices and tools (e.g., procedures and safeguards), and work roles.
3. **Create the Organizational Profile.** Determine what types of information the Profile should include for the selected CSF outcomes, and document the needed information. Consider the risk implications of the Current Profile to inform Target Profile planning and prioritization. Also, consider using a Community Profile as the basis for the Target Profile.
4. **Analyze the gaps between the Current and Target Profiles, and create an action plan.** Conduct a gap analysis to identify and analyze the differences between the Current and Target Profiles, and develop a prioritized action plan (e.g., risk register, risk detail report, Plan of Action and Milestones [POA&M]) to address those gaps.
5. **Implement the action plan, and update the Organizational Profile.** Follow the action plan to address the gaps and move the organization toward the Target Profile. An action plan may have an overall deadline or be ongoing.

Given the importance of continual improvement, an organization can repeat these steps as often as needed.

There are additional uses for Organizational Profiles. For example, a Current Profile can be used to document and communicate the organization's cybersecurity capabilities and known opportunities for improvement with external stakeholders, such as business partners or prospective customers. Also, a Target Profile can help express the organization's cybersecurity risk management requirements and expectations to suppliers, partners, and other third parties as a target for those parties to achieve.

3.2. CSF Tiers

An organization can choose to use the Tiers to inform its Current and Target Profiles. *Tiers* characterize the rigor of an organization's cybersecurity risk governance and management practices, and they provide context for how an organization views cybersecurity risks and the processes in place to manage those risks. The Tiers, as shown in Fig. 4 and notionally illustrated in Appendix B, reflect an organization's practices for managing cybersecurity risk as Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4). The Tiers describe a progression from informal, ad hoc responses to approaches that are agile, risk-informed, and

1. **組織プロファイルの範囲を決める。**プロファイルの範囲を定義する際の基礎となるハイレベルの事実と想定を文書化する。組織は希望通りの数の、それぞれ範囲が異なる組織プロファイルを定めることができる。例えば、或るプロファイルにおいて、組織全体を対象にする、或いは組織の会計システムまたはランサムウェアの脅威に対する対策や、それらの会計システムが関係するランサムウェアインシデントの処理を対象範囲とすることができる。
2. **組織プロファイルの準備に必要な情報を集める。**情報の例として、組織のポリシー、リスクマネジメントの優先事項とリソース、企業リスクプロファイル、ビジネス影響分析（BIA）登録簿、組織がサイバーセキュリティに関して遵守する要求事項や標準、様々なプラクティスやツール（例：手順や保護対策）、及び作業分担が挙げられる。
3. **組織プロファイルを作成する。**選択した CSF の成果についてプロファイルに含めるべき情報の種類を判断し、必要な情報を文書化する。目標のプロファイルの計画作成と優先順位決めの情報源となる、現在のプロファイルにおけるリスクの意味合いを検討する。更に、目標のプロファイルの基礎としてコミュニティプロファイルを利用することも検討する。
4. **現在のプロファイルと目標のプロファイルの間のギャップを分析し、行動計画を作成する。**ギャップ分析を実施して、現在のプロファイルと目標のプロファイルの間のギャップを識別及び分析し、そして優先される行動計画を立案する（例：リスク登録簿、リスク詳細報告書、それらのギャップに対処するための行動計画・マイルストーン（POA&M））。
5. **行動計画を実施し、組織プロファイルを更新する。**行動計画に従ってギャップに対処し、目標のプロファイルに向けて組織を動かす。行動計画は全体的な期限を定めてもよいし、継続的な計画としてもよい。

継続的な改善の重要性を踏まえ、組織はこれらの手順を必要に応じて何度も繰り返すとよい。

例えば、現在のプロファイルを利用して、組織のサイバーセキュリティ能力や改善に向けた既知の機会を文書化し、それをビジネスパートナーや見込み客など外部の利害関係者に周知することができる。また、目標のプロファイルは、組織のサイバーセキュリティリスクマネジメントにおける要求事項と期待事項をサプライヤーやパートナーなどの第三者に達成してもらいたい目標として表明する上でも役立つと考えられる。

3.2. CSF ティア

組織は、現在のプロファイル及び目標のプロファイルの情報源として、ティアを使うことを選択できる。ティアは、組織のサイバーセキュリティにおけるリスクガバナンスとリスクマネジメントのプラクティスの厳格さを特徴付け、組織におけるサイバーセキュリティリスクの捉え方と、それらのリスクを管理するために整備されるプロセスに文脈を与えるものである。

ティアは図 4 に記載の通り、また Appendix B で概念的に例示されている通り、組織におけるサイバーセキュリティリスクマネジメントのプラクティスを「部分的である」（ティア 1）、「リスク情報を活用している」（ティア 2）、「繰り返し適用可能である」（ティア 3）、及び「適応的である」（ティア 4）として反映する。これらのティアは、非形式的な一時的対応から、迅速でリスク情報を活用する継続的な改善に当たるアプローチに至るまでの進捗を表す。

continuously improving. Selecting Tiers helps set the overall tone for how an organization will manage its cybersecurity risks.

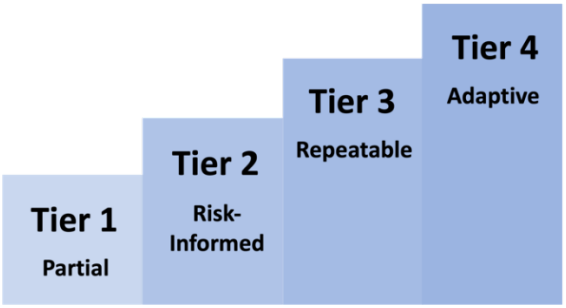

Fig. 4. CSF Tiers for cybersecurity risk governance and management

Tiers should complement an organization's cybersecurity risk management methodology rather than replace it. For example, an organization can use the Tiers to communicate internally as a benchmark for an organization-wide[1] approach to managing cybersecurity risks. Progression to higher Tiers is encouraged when risks or mandates are greater or when a cost-benefit analysis indicates a feasible and cost-effective reduction of negative cybersecurity risks.

The NIST CSF website provides additional information on using Profiles and Tiers. It includes pointers to NIST-hosted Organizational Profile templates and a repository of Community Profiles in a variety of machine-readable and human-usable formats.

[1] For the purposes of this document, the terms "organization-wide" and "enterprise" have the same meaning.

ティアの選択は、組織における今後のサイバーセキュリティリスクマネジメントの全体的なトーンを定める上で役立つ。

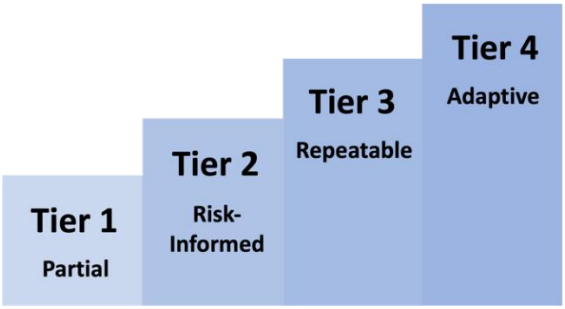

図 4. サイバーセキュリティリスクのガバナンスとマネジメントのための CSF ティア

ティアは、組織におけるサイバーセキュリティリスクマネジメント手法に取って代わるのではなく、むしろそれを補うものであるべきである。例えば、組織はティアを利用して、それをサイバーセキュリティリスクマネジメントに対する組織全体[1]でのアプローチのベンチマークとして内部で周知することができる。より上位のティアへの前進が奨励されるのは、リスクまたは義務が増大した場合、或いは費用便益分析の結果、悪影響を及ぼすサイバーセキュリティリスクの費用効果的な低減が実現可能であることが示唆される場合である。

NIST の CSF ウェブサイトに、プロファイルとティアの利用に関する付加的情報が掲載されている。NIST が収録している組織プロファイルのテンプレートや、多様な機械可読型フォーマット及び人間が利用できるフォーマットでのコミュニティプロファイルのリポジトリを検索できるポインターもある。

[1] 本文書の目的上、「組織全体」と「企業」は同じ意味である。

4. Introduction to Online Resources That Supplement the CSF

NIST and other organizations have produced a suite of online resources that help organizations understand, adopt, and use the CSF. Since they are hosted online, these additional resources can be updated more frequently than this document, which is updated infrequently to provide stability to its users, and be available in machine-readable formats. This section provides an overview of three types of online resources: Informative References, Implementation Examples, and Quick Start Guides.

Informative References are mappings that indicate relationships between the Core and various standards, guidelines, regulations, and other content. Informative References help inform how an organization may achieve the Core's outcomes. Informative References can be sector- or technology-specific. They may be produced by NIST or another organization. Some Informative References are narrower in scope than a Subcategory. For example, a particular control from SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, may be one of many references needed to achieve the outcome described in one Subcategory. Other Informative References may be higher-level, such as a requirement from a policy that partially addresses numerous Subcategories. When using the CSF, an organization can identify the most relevant Informative References.

Implementation Examples provide notional examples of concise, action-oriented steps to help achieve the outcomes of the Subcategories. Verbs used to express Examples include share, document, develop, perform, monitor, analyze, assess, and exercise. The Examples are not a comprehensive list of all actions that could be taken by an organization to achieve an outcome, nor do they represent a baseline of required actions to address cybersecurity risks.

Quick-Start Guides (QSGs) are brief documents on specific CSF-related topics and are often tailored to specific audiences. QSGs can help an organization implement the CSF because they distill specific portions of the CSF into actionable "first steps" that an organization can consider on the path to improving their cybersecurity posture and management of associated risks. The guides are revised in their own time frames, and new guides are added as needed.

Suggestions for new Informative References for CSF 2.0 can always be shared with NIST at olir@nist.gov. Suggestions for other resources to reference on the NIST CSF website, including additional QSG topics, should be directed to cyberframework@nist.gov.

4. CSF を補足するオンラインリソースの紹介

NIST 及び他の様々な組織が、組織による CSF の理解、採用及び利用に役立つ一連のオンラインリソースを生み出してきた。オンラインでホストされていることから、これらの付加的リソースは、ユーザに安定感を与えるためにさほど頻繁には更新されない本文書よりも高頻度で更新され、機械可読フォーマットで入手可能である。本セクションでは 3 種類のオンラインリソース、即ち参考情報、実装例、及びクイックスタートガイドの概要を示す。

*参考情報*は、コアと様々な標準、ガイドライン、規制及び他の内容の間の関係を示すマッピングである。参考情報は、組織がコアの成果をどのように達成できるかについての情報源として役立つ。参考情報は、業界固有の場合もあれば技術固有の場合もある。また、NIST が作成する場合もあれば他の組織が作成する場合もある。参考情報は、時々、サブカテゴリーより範囲が狭いこともある。例えば、SP 800-53、「*情報システム及び組織向けのセキュリティとプライバシーの管理策*」に記載されている特定の管理策は、或るサブカテゴリーに記載の成果を達成するために必要な多数の参考資料の 1 つと考えられる。他の参考情報は、より高レベルと考えられ、例えば多数のサブカテゴリーに部分的に対処するポリシーからの要求事項などがそうである。CSF を利用する場合、組織は最も関連性の高い参考情報を識別できる。

*実装例*は、サブカテゴリーの成果達成に役立つ簡潔な行動指向の手順の概念的な例を示すものである。実装例の表現に使用される動詞の例として、共有する、文書化する、開発する、実行する、モニタリングする、分析する、評価する、演習する、などが挙げられる。実装例は、組織が或る成果の達成に向けて講じることができるあらゆる措置の包括的リストでもなければ、サイバーセキュリティリスクへの対処に必要な措置のベースラインを表すものでもない。

*クイックスタートガイド（QSG）*は、具体的な CSF 関連のトピックを簡潔にまとめた文書であり、特定の対象者に合わせて調整されることが多い。QSG は、CSF における特定の部分を抜き出し、組織がサイバーセキュリティへの取組みや付随するリスクのマネジメントの改善に向けた途上で検討し得る、すぐに実施可能な「初期段階」に組み入れることから、組織が CSF を実施する際に役立つと考えられる。これらのガイドは、それぞれ固有の時間枠で改訂され、新規のガイドが必要に応じて追加される。

CSF 2.0 版向けに新たな参考情報の提言があれば、いつでも NIST と共有していただきたい（宛先：olir@nist.gov）。ST の CSF ウェブサイトで参照すべき他のリソースの提言があれば、付加的な QSG のトピックを含め、cyberframework@nist.gov 宛にお送りいただきたい。

5. Improving Cybersecurity Risk Communication and Integration

The CSF's use will vary based on an organization's unique mission and risks. With an understanding of stakeholder expectations and risk appetite and tolerance (as outlined in GOVERN), an organization can prioritize cybersecurity activities to make informed decisions about cybersecurity expenditures and actions. An organization may choose to handle risk in one or more ways — including mitigating, transferring, avoiding, or accepting negative risks and realizing, sharing, enhancing, or accepting positive risks — depending on the potential impacts and likelihoods. Importantly, an organization can use the CSF both internally to manage its cybersecurity capabilities and externally to oversee or communicate with third parties.

Regardless of the CSF's utilization, an organization may benefit from using the CSF as guidance to help it understand, assess, prioritize, and communicate cybersecurity risks and the actions that will manage those risks. The selected outcomes can be used to focus on and implement strategic decisions to improve cybersecurity postures and maintain continuity of mission-essential functions while taking priorities and available resources into account.

5.1. Improving Risk Management Communication

The CSF provides a basis for improved communication regarding cybersecurity expectations, planning, and resources. The CSF fosters bidirectional information flow (as shown in the top half of Fig. 5) between executives who focus on the organization's priorities and strategic direction and managers who manage specific cybersecurity risks that could affect the achievement of those priorities. The CSF also supports a similar flow (as shown in the bottom half of Fig. 5) between managers and the practitioners who implement and operate the technologies. The left side of the figure indicates the importance of practitioners sharing their updates, insights, and concerns with managers and executives.

Fig. 5. Using the CSF to improve risk management communication

5. サイバーセキュリティリスクコミュニケーションと統合の改善

CSF の用途は、組織の固有のミッションやリスクに基づいて変動する。利害関係者の期待事項や、リスク選好度と許容度を理解することにより（統制機能の説明で概要が示されている通り）、組織は、サイバーセキュリティ関連の支出と措置について情報に基づく決定を下すために、サイバーセキュリティ活動の優先順位を決めることができる。組織は、潜在的な影響や発生可能性に応じて、1 つまたは複数の形態（悪影響を及ぼすリスクの軽減、移転、回避または許容、及びプラスの効果をもたらすリスクの実現、共有、拡充または許容を含む）でのリスクの取扱いを選ぶことができる。重要な点として、組織は、CSF を内部で利用して自組織のサイバーセキュリティ能力を管理することができると同時に、対外的に利用して第三者を監督したり、第三者とコミュニケーションを行うことができる。

CSF の活用形態を問わず、組織は、サイバーセキュリティリスクやそれらのリスクを管理するための行動を理解、評価、優先順位付け及び周知する上で役立つガイダンスとして CSF を利用することが有益である。選択される成果を利用して、サイバーセキュリティへの取組みを改善するための戦略的決定に焦点を当て、それを実施し、そして優先事項と利用可能な資源を考慮に入れながらミッションに欠かせない機能の継続性を維持することができる。

5.1. リスクマネジメントコミュニケーションの改善

CSF は、サイバーセキュリティの期待事項、計画作成、及びリソースに関するコミュニケーションを改善するための基礎を提供する。CSF は、組織の優先事項や戦略的方向性に焦点を当てる役員と、それらの優先事項の達成に影響を及ぼす可能性のある具体的なサイバーセキュリティリスクを管理するマネージャーの間での、双方向の情報の流れ（図 5 の上半分に記載の通り）を促進する。また、CSF は、マネージャーと、技術を実装・運用する実務者の間での同様の流れ（図 5 の下半分に記載の通り）も支援する。図の左側では実務者が最新情報、見識及び懸案事項をマネージャーや役員と共有することの重要性を示している。

図 5. リスクマネジメントコミュニケーションを改善するための CSF の利用

Preparing to create and use Organizational Profiles involves gathering information about organizational priorities, resources, and risk direction from executives. Managers then collaborate with practitioners to communicate business needs and create risk-informed Organizational Profiles. Actions to close any gaps identified between the Current and Target Profiles will be implemented by managers and practitioners and will provide key inputs into system-level plans. As the target state is achieved throughout the organization — including through controls and monitoring applied at the system level — the updated results can be shared through risk registers and progress reports. As part of ongoing assessment, managers gain insights to make adjustments that further reduce potential harms and increase potential benefits.

The GOVERN Function supports organizational risk communication with **executives**. Executives' discussions involve strategy, particularly how cybersecurity-related uncertainties might affect the achievement of organizational objectives. These governance discussions support dialogue and agreement about risk management strategies (including cybersecurity supply chain risk); roles, responsibilities, and authorities; policies; and oversight. As executives establish cybersecurity priorities and objectives based on those needs, they communicate expectations about risk appetite, accountability, and resources. Executives are also responsible for integrating cybersecurity risk management with ERM programs and lower-level risk management programs (see Sec. 5.2). The communications reflected in the top half of Fig. 5 can include considerations for ERM and the lower-level programs and, thus, inform managers and practitioners.

The overall cybersecurity objectives set by executives are informed by and cascade to **managers**. In a commercial entity, these may apply to a line-of-business or operating division. For government entities, these may be division- or branch-level considerations. When implementing the CSF, managers will focus on how to achieve risk targets through common services, controls, and collaboration, as expressed in the Target Profile and improved through the actions being tracked in the action plan (e.g., risk register, risk detail report, POA&M).

Practitioners focus on implementing the target state and measuring changes in operational risk to help plan, carry out, and monitor specific cybersecurity activities. As controls are implemented to manage risk at an acceptable level, practitioners provide managers and executives with the information (e.g., key performance indicators, key risk indicators) they need to understand the organization's cybersecurity posture, make informed decisions, and maintain or adjust the risk strategy accordingly. Executives can also combine this cybersecurity risk data with information about other types of risk from across the organization. Updates to expectations and priorities are included in updated Organizational Profiles as the cycle repeats.

5.2. Improving Integration with Other Risk Management Programs

Every organization faces numerous types of ICT risk (e.g., privacy, supply chain, artificial intelligence) and may use frameworks and management tools that are specific to each risk. Some organizations integrate ICT and all other risk management efforts at a high level by using ERM, while others keep the efforts separate to ensure adequate attention on each. Small

組織プロファイルの作成と利用の準備に際し、組織の優先事項、リソース、及び役員からのリスク関連指示に関する情報を収集する必要がある。次いでマネージャーは実務者と協力してビジネスニーズを周知し、リスク情報に基づいた組織プロファイルを作成する。現在のプロファイルと目標のプロファイルの間で識別されたギャップを埋めるための措置は、マネージャーと実務者が実施し、それらの措置はシステムレベルでの計画に組み入れる主要なインプットを提供する。目標とする状態が組織全体にわたり達成されると（システムレベルで適用される管理策やモニタリングを通じた達成を含む）、リスク登録簿や進捗報告書を通じ、更新された結果を共有できる。継続的なアセスメントの一環として、マネージャーは、潜在的な危害を更に低減すると共に潜在的な便益を増大させる調整を行うための見識を得る。

統制機能は、役員との組織的なリスクコミュニケーションを支援する。役員の議論には戦略が関係するが、特に、サイバーセキュリティ関連の不確実性が組織の目的の達成に影響を及ぼし得る形態が関係する。ガバナンスに関するこれらの議論は、リスクマネジメント戦略（サイバーセキュリティサプライチェーンリスクを含む）、役割／責任／権限、ポリシー、及び監督に関する対話と合意の支援になる。役員はこれらのニーズに基づいて役員がサイバーセキュリティの優先事項と目的を定めたら、リスク選好度、説明責任及びリソースに関する期待事項を周知する。また役員は、サイバーセキュリティリスクマネジメントを ERM プログラムや、より低レベルのリスクマネジメントプログラムと統合する責任も負う（セクション 5.2 参照）。図 5 の上半分に反映されているコミュニケーションには、ERM やより低レベルのプログラムの検討を含めることができ、それらは結果としてマネージャーと実務者の情報源になり得る。

役員が定める全体的なサイバーセキュリティの目的について**マネージャー**から情報が提供されたり、マネージャーに周知されたりする。民間事業体では、これらが事業部門または運営部門に当てはまる場合もある。政府機関の場合、これらは部門レベルまたは部課レベルでの検討事項になり得る。CSF を実施する際、マネージャーは共通のサービス、管理策及び協力を通じてリスク目標を達成する方法に焦点を当てることになるが、これは目標のプロファイルにおいて表明され、行動計画において追跡調査される措置（例：リスク登録簿、リスク詳細報告書、POA&M）を通じて改善される通りである。

実務者は、目標とする状態の実施と運用上のリスクの変化の測定に焦点を当て、それを具体的なサイバーセキュリティ活動の計画作成、実行及びモニタリングに役立てる。許容可能なレベルでのリスク管理策が実施されると、実務者はマネージャーと役員が組織のサイバーセキュリティへの取組みを理解し、情報に基づいた決定を下し、相応にリスク戦略を維持または調整するために必要な情報（例：主要業績指標、主要リスク指標）をマネージャーと役員に提供する。役員は、このサイバーセキュリティリスクデータを、他の種類のリスクについて組織全体から寄せられる情報と組み合わせることもできる。期待事項と優先事項の最新情報は、サイクルの反復に応じて更新後の組織プロファイルに含まれる。

5.2. 他のリスクマネジメントプログラムとの統合の改善

あらゆる組織が非常に多様な ICT リスク（例：プライバシー、サプライチェーン、人工知能）に直面し、そして個々のリスクに特有のフレームワークやマネジメントツールを利用し得る。一部の組織は ICT と他のあらゆるリスクマネジメントの取組みを、ERM の活用によって高いレベルで統合する一方、他の組織はそうした取組みを別個のものとして維持し、それぞれに対する適切な配慮を確保する。小規模組織は、本質的に、企業レベルでリスクをモニタリングできる一方、比較的大規模の会社は別々のリスクマネジメントの取組みを ERM に統合することができる。

organizations by their nature may monitor risk at the enterprise level, while larger companies may maintain separate risk management efforts integrated into the ERM.

Organizations can employ an ERM approach to balance a *portfolio* of risk considerations, including cybersecurity, and make informed decisions. Executives receive significant input about current and planned risk activities as they integrate governance and risk strategies with results from previous uses of the CSF. The CSF helps organizations to translate their terminology for cybersecurity and cybersecurity risk management into general risk management language that executives will understand.

NIST resources that describe the mutual relationship between cybersecurity risk management and ERM include:

- *NIST Cybersecurity Framework 2.0 – Enterprise Risk Management Quick-Start Guide*
- NIST Interagency Report (IR) 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*
- IR 8286A, *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management*
- IR 8286B, *Prioritizing Cybersecurity Risk for Enterprise Risk Management*
- IR 8286C, *Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight*
- IR 8286D, *Using Business Impact Analysis to Inform Risk Prioritization and Response*
- SP 800-221, *Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio*
- SP 800-221A, *Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio*

An organization may also find the CSF beneficial for integrating cybersecurity risk management with individual ICT risk management programs, such as:

- **Cybersecurity risk management and assessment:** The CSF can be integrated with established cybersecurity risk management and assessment programs, such as SP 800-37, *Risk Management Framework for Information Systems and Organizations*, and SP 800-30, *Guide for Conducting Risk Assessments* from the NIST Risk Management Framework (RMF). For an organization using the NIST RMF and its suite of publications, the CSF can be used to complement the RMF's approach to selecting and prioritizing controls from SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*.
- **Privacy risks:** While cybersecurity and privacy are independent disciplines, their objectives overlap in certain circumstances, as illustrated in Fig. 6.

組織は、ERM アプローチを採用して、サイバーセキュリティを含むリスク関連の検討事項のポートフォリオのバランスを取り、情報に基づいた決定を下すことができる。役員は、ガバナンス戦略やリスク戦略を過去における CSF の利用からの結果と統合する過程で、現在のリスク対策と計画上のリスク対策に関する有意義なインプットを受け取る。CSF は、組織がサイバーセキュリティやサイバーセキュリティリスクマネジメントに関する用語を、役員が理解できる一般的なリスクマネジメント用語に置き換える上で役立つ。

サイバーセキュリティリスクマネジメントと ERM の間の相互関係を記述する NIST のリソースの例として以下が挙げられる。

- *NIST Cybersecurity Framework 2.0 – Enterprise Risk Management Quick-Start Guide*
- NIST Interagency Report (IR) 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*
- IR 8286A, *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management*
- IR 8286B, *Prioritizing Cybersecurity Risk for Enterprise Risk Management*
- IR 8286C, *Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight*
- IR 8286D, *Using Business Impact Analysis to Inform Risk Prioritization and Response*
- SP 800-221, *Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio*
- SP 800-221A, *Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio*

また、組織は、サイバーセキュリティリスクマネジメントを以下のような個別の ICT リスクマネジメントプログラムと統合する場合にも、CSF が有益であることが分かると考えられる。

- **サイバーセキュリティリスクのマネジメントとアセスメント**: CSF は、サイバーセキュリティリスクに関して確立されたマネジメントプログラムやアセスメントプログラム、例えば NIST リスクマネジメントフレームワーク（RMF）からの SP 800-37、「*情報システム及び組織のためのリスクマネジメントフレームワーク*」や、SP 800-30、「*リスクアセスメント実施ガイド*」と統合することができる。NIST RMF や関連する一連の刊行物を利用している組織の場合、CSF を利用して、SP 800-53、「*情報システム及び組織のためのセキュリティ管理策とプライバシー管理策*」からの管理策の選択と優先順位付けに対する RMF のアプローチを補うことができる。
- **プライバシーリスク**: サイバーセキュリティとプライバシーはそれぞれ独立した分野である一方、図 6 に図示されている通り、状況によっては目的が重なる。

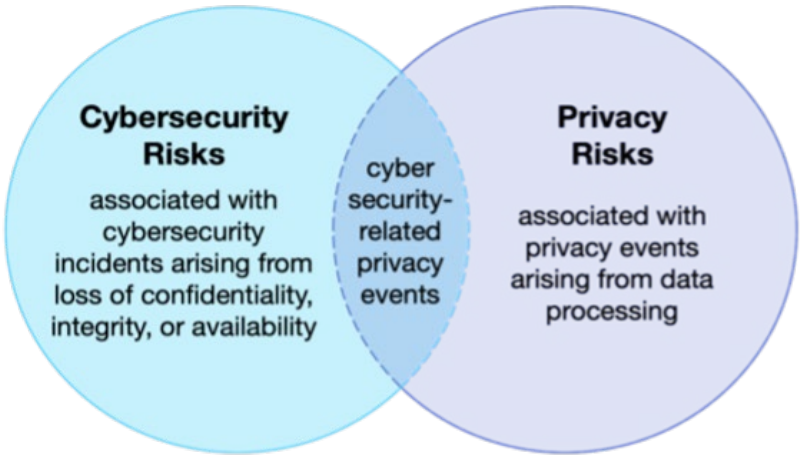

Fig. 6. Cybersecurity and privacy risk relationship

Cybersecurity risk management is essential for addressing privacy risks related to the loss of the confidentiality, integrity, and availability of individuals' data. For example, data breaches could lead to identity theft. However, privacy risks can also arise by means that are unrelated to cybersecurity incidents.

An organization processes data to achieve mission or business purposes, which can sometimes give rise to *privacy events* whereby individuals may experience problems as a result of the data processing. These problems can be expressed in various ways, but NIST describes them as ranging from dignity-type effects (e.g., embarrassment or stigma) to more tangible harms (e.g., discrimination, economic loss, or physical harm). The NIST Privacy Framework and Cybersecurity Framework can be used together to address the different aspects of cybersecurity and privacy risks. Additionally, NIST's Privacy Risk Assessment Methodology (PRAM) has a catalog of example problems for use in privacy risk assessments.

- **Supply chain risks:** An organization can use the CSF to foster cybersecurity risk oversight and communications with stakeholders across supply chains. All types of technology rely on a complex, globally distributed, extensive, and interconnected supply chain ecosystem with geographically diverse routes and multiple levels of outsourcing. This ecosystem is composed of public- and private-sector entities (e.g., acquirers, suppliers, developers, system integrators, external system service providers, and other technology-related service providers) that interact to research, develop, design, manufacture, acquire, deliver, integrate, operate, maintain, dispose of, and otherwise utilize or manage technology products and services. These interactions are shaped and influenced by technologies, laws, policies, procedures, and practices.

  Given the complex and interconnected relationships in this ecosystem, supply chain risk management (SCRM) is critical for organizations. Cybersecurity SCRM (C-SCRM) is a systematic process for managing exposure to cybersecurity risk throughout supply chains and developing appropriate response strategies, policies, processes, and procedures. The Subcategories within the CSF C-SCRM Category [GV.SC] provide a connection between outcomes that focus purely on cybersecurity and those that focus

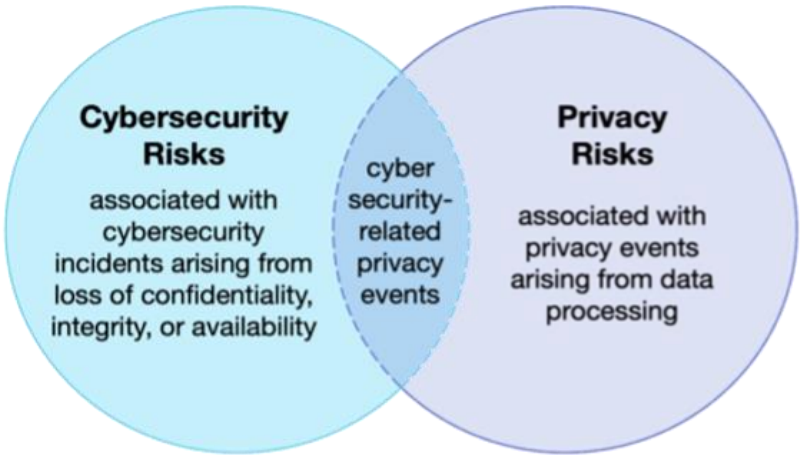

図 6. サイバーセキュリティリスクとプライバシーリスクの関係

サイバーセキュリティリスクマネジメントは、個人のデータの機密性、完全性、及び可用性の喪失に関連するプライバシーリスクへの対処に不可欠である。例えば、データ侵害は個人情報漏洩に繋がる恐れがある。しかし、プライバシーリスクは、サイバーセキュリティインシデントとは無関係の手段によって生じる可能性もある。

組織は、ミッションまたはビジネス上の目的を達成するためにデータを処理するが、それが時々、プライバシー事象の原因になることにより、個人がデータ処理の結果として問題に見舞われる可能性がある。これらの問題は様々な形で表すことができるが、NIST は、それらを尊厳型の影響（例：困惑または汚名）から、より有形の危害（例：差別、経済的損失、または身体的危害）に至る範囲のものとして表す。NIST の「プライバシーフレームワーク」と「サイバーセキュリティフレームワーク」を一体的に利用して、サイバーセキュリティリスクとプライバシーリスクにおけるそれぞれ異なる側面に対処することができる。加えて、NIST の「プライバシーリスクアセスメント方法論（PRAM）」にはプライバシーリスクアセスメントに利用するための問題事例のカタログが記載されている。

- **サプライチェーンリスク**：組織は、CSF を利用して、サプライチェーン全体にわたるサイバーセキュリティリスクの監督及び利害関係者とのコミュニケーションを促進することができる。あらゆる種類の技術が頼りとするのは、複雑で全世界的に分散し、広範囲にわたり相互に繋がるサプライチェーンエコシステムであり、その経路は地理的に多様で、複数レベルのアウトソーシングを伴う。このエコシステムは、官民の両業界の事業体（例：調達者、サプライヤー、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の技術関連サービスプロバイダ）から成り、それらが相互に作用して、技術製品やサービスの研究、開発、設計、製造、調達、納入、統合、運用、保守、処分を行ったり、別の形で活用または管理する。こうした相互作用は、技術、法律、ポリシー、手順及びプラクティスによって形成され、影響を受ける。

  このエコシステムにおける複雑で相互に繋がった関係を踏まえ、サプライチェーンリスクマネジメント（SCRM）は組織にとって重要である。サイバーセキュリティ SCRM（C-SCRM）は、サプライチェーン全体にわたるサイバーセキュリティリスクに曝される状況を管理し、適切な対応戦略、ポリシー、プロセス、及び手順を開発するための、体系的プロセスである。CSF C-SCRM のカテゴリー［GV.SC］に該当するサブカテゴリーは、純粋にサイバーセキュリティに焦点を当てる成果と、C-SCRM に焦点を当てる成果の間に繋がりをもたらす。SP 800-161r1（改訂第 1 版）、「*システムと組織のためのサイバーセキュリティサプライチェーンリスクマネジメントプラクティス*」は、C-SCRM に関する詳細な情報を提供する。

on C-SCRM. SP 800-161r1 (Revision 1), *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, provides in-depth information on C-SCRM.

- **Risks from emerging technologies:** As new technologies and new applications of technology become available, new risks become clear. A contemporary example is artificial intelligence (AI), which has cybersecurity and privacy risks, as well as many other types of risk. The NIST Artificial Intelligence Risk Management Framework (AI RMF) was developed to help address these risks. Treating AI risks alongside other enterprise risks (e.g., financial, cybersecurity, reputational, and privacy) will yield a more integrated outcome and organizational efficiencies. Cybersecurity and privacy risk management considerations and approaches are applicable to the design, development, deployment, evaluation, and use of AI systems. The AI RMF Core uses Functions, Categories, and Subcategories to describe AI outcomes and help manage risks related to AI.

- **新興技術からのリスク**：新たな技術や技術の新たな用途が利用可能となるにつれ、新たなリスクが明らかになってくる。最新の例は人工知能（AI）であり、これはサイバーセキュリティリスクとプライバシーリスクに加え、他にも多数の種類のリスクを抱える。NIST の「人工知能リスクマネジメントフレームワーク（AI RMF）」は、こうしたリスクへの対処に役立つよう開発された。AI リスクを他の企業リスク（例：財務、サイバーセキュリティ、評判、及びプライバシー）と並列で扱えば、より統合された成果と組織的効率性の実現に繋がる。サイバーセキュリティとプライバシーに関するリスクマネジメント上の検討事項やアプローチは、AI システムの設計、開発、展開、評価及び利用にも適用可能である。AI RMF コアでは機能、カテゴリー及びサブカテゴリーを利用して AI の成果を記述し、これらは AI に関連するリスクのマネジメントに役立つ。

Appendix A. CSF Core

This appendix describes the Functions, Categories, and Subcategories of the CSF Core. Table 1 lists the CSF 2.0 Core Function and Category names and unique alphabetic identifiers. Each Function name in the table is linked to its portion of the appendix. The order of Functions, Categories, and Subcategories of the Core is not alphabetical; it is intended to resonate most with those charged with operationalizing risk management within an organization. The numbering of the Subcategories is intentionally not sequential; gaps in numbering indicate CSF 1.1 Subcategories that were relocated in CSF 2.0.

Table 1. CSF 2.0 Core Function and Category names and identifiers

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

The CSF Core, Informative References, and Implementation Examples are available on the CSF 2.0 website and through the CSF 2.0 Reference Tool, which allows users to explore them and export them in human- and machine-readable formats. The CSF 2.0 Core is also available in a legacy format similar to that of CSF 1.1.

Appendix A. CSF コア

本付録では CSF コアの機能、カテゴリー及びサブカテゴリーを記述する。表 1 は、CSF 2.0 版におけるコア機能とカテゴリーの名称及び固有のアルファベット識別子の一覧である。表に記載された各機能の名称は、付録の該当部分にリンクされている。機能、カテゴリー及びサブカテゴリーの順序は、アルファベット順ではない。これは組織内でのリスクマネジメント運用を担当する人々の共感を最も呼ぶことを意図している。サブカテゴリーの採番は意図的に不連続になっている。採番にギャップがある箇所は、CSF2.0 において移動された CSF1.1 サブカテゴリーを示している。

表 1. CSF 2.0 コア機能、カテゴリー名、カテゴリー識別子

機能	カテゴリー	カテゴリー識別子
統制 (GV)	組織的文脈	GV.OC
	リスクマネジメント戦略	GV.RM
	役割／責任／権限	GV.RR
	ポリシー	GV.PO
	監督	GV.OV
	サイバーセキュリティサプライチェーンリスクマネジメント	GV.SC
識別 (ID)	資産管理	ID.AM
	リスクアセスメント	ID.RA
	改善	ID.IM
防御 (PR)	アイデンティティ管理とアクセス制御	PR.AA
	意識向上及びトレーニング	PR.AT
	データセキュリティ	PR.DS
	プラットフォームセキュリティ	PR.PS
	技術インフラのレジリエンス	PR.IR
検知 (DE)	継続的モニタリング	DE.CM
	有害イベントの分析	DE.AE
対応 (RS)	インシデントマネジメント	RS.MA
	インシデント分析	RS.AN
	インシデント対応の報告とコミュニケーション	RS.CO
	インシデント軽減	RS.MI
復旧 (RC)	インシデント復旧計画の実行	RC.RP
	インシデント復旧のコミュニケーション	RC.CO

CSF コア、参考情報、及び実装例は、CSF 2.0 版のウェブサイト上で入手可能であり、またユーザがそれらを探究したり人間可読及び機械可読のフォーマットでそれらをエクスポートすることを可能にする CSF 2.0 版参照ツールを通じて入手可能である。CSF 2.0 版のコアは、CSF 1.1 のフォーマットに似た旧式フォーマットでも入手可能である。

GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored

- **Organizational Context (GV.OC):** The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood
  - **GV.OC-01:** The organizational mission is understood and informs cybersecurity risk management
  - **GV.OC-02:** Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered
  - **GV.OC-03:** Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed
  - **GV.OC-04:** Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated
  - **GV.OC-05:** Outcomes, capabilities, and services that the organization depends on are understood and communicated
- **Risk Management Strategy (GV.RM):** The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions
  - **GV.RM-01:** Risk management objectives are established and agreed to by organizational stakeholders
  - **GV.RM-02:** Risk appetite and risk tolerance statements are established, communicated, and maintained
  - **GV.RM-03:** Cybersecurity risk management activities and outcomes are included in enterprise risk management processes
  - **GV.RM-04:** Strategic direction that describes appropriate risk response options is established and communicated
  - **GV.RM-05:** Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties
  - **GV.RM-06:** A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated
  - **GV.RM-07:** Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions

統制（GV）：組織のサイバーセキュリティリスクアセスメント戦略、期待事項、及びポリシーが確立、周知、モニタリングされている。

- **組織的文脈（GV.OC）**：組織のサイバーセキュリティリスクマネジメントの判断を巡る状況（ミッション、利害関係者の期待事項、依存性、並びに法的要求事項、規制上の要求事項、及び契約上の要求事項）が理解されている。
  - GV.OC-01：組織のミッションが理解され、サイバーセキュリティリスクマネジメントについて伝えている。
  - GV.OC-02：内部と外部の利害関係者が理解され、サイバーセキュリティリスクマネジメントに関するそれら利害関係者のニーズと期待事項が理解及び考慮されている。
  - GV.OC-03：サイバーセキュリティに関する法的要求事項、規制上の要求事項、及び契約上の要求事項（プライバシーと市民的自由の義務を含む）が理解され管理されている。
  - GV.OC-04：外部の利害関係者が組織に依存または期待する重要な目的、能力及びサービスが理解され周知されている。
  - GV.OC-05：組織が依存する成果、能力、及びサービスが理解され周知されている。
- **リスクマネジメント戦略（GV.RM）**：組織の優先事項、制約、リスク許容度、リスクに対する姿勢の表明、及び想定が、組織のリスク判断の支援のために確立、周知、利用されている。
  - GV.RM-01：リスクマネジメントの目的が確立され、組織の利害関係者によって合意されている。
  - GV.RM-02：リスク選好度とリスク許容度に関する表明が確立、周知、維持されている。
  - GV.RM-03：サイバーセキュリティリスクマネジメントの活動と成果が企業リスクマネジメントプロセスに含まれている。
  - GV.RM-04：適切なリスク対応オプションを表す戦略的方向性が確立、周知されている。
  - GV.RM-05：サプライヤー及び他の第三者からのリスクを含め、サイバーセキュリティリスクに関するコミュニケーション系統が組織全体にわたり確立されている。
  - GV.RM-06：サイバーセキュリティリスクの計算、文書化、分類、及び優先順位付けのための標準化された方法が確立、周知されている。
  - GV.RM-07：戦略的機会（即ちプラスの効果をもたらすリスク）が特徴付けられ、組織のサイバーセキュリティリスクに関する議論に含まれている。

- **Roles, Responsibilities, and Authorities (GV.RR):** Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated
  - **GV.RR-01:** Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving
  - **GV.RR-02:** Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced
  - **GV.RR-03:** Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies
  - **GV.RR-04:** Cybersecurity is included in human resources practices
- **Policy (GV.PO):** Organizational cybersecurity policy is established, communicated, and enforced
  - **GV.PO-01:** Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced
  - **GV.PO-02:** Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission
- **Oversight (GV.OV):** Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy
  - **GV.OV-01:** Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction
  - **GV.OV-02:** The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks
  - **GV.OV-03:** Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed
- **Cybersecurity Supply Chain Risk Management (GV.SC):** Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders
  - **GV.SC-01:** A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders
  - **GV.SC-02:** Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally
  - **GV.SC-03:** Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes
  - **GV.SC-04:** Suppliers are known and prioritized by criticality

- **役割／責任／権限**（GV.RR）：説明責任、実績アセスメント、及び継続的改善のためのサイバーセキュリティにおける役割／責任／権限が確立、周知されている。
  - GV.RR-01：サイバーセキュリティリスクについて組織の指導者が責任と説明責任を負い、リスクを意識した、倫理的で継続的な改善に取り組む文化を促進している。
  - GV.RR-02：サイバーセキュリティリスクマネジメントに関連する役割／責任／権限が確立、周知、理解、執行されている。
  - GV.RR-03：サイバーセキュリティリスクに関する戦略／役割／責任／ポリシーと一致する適切な資源が配分されている。
  - GV.RR-04：サイバーセキュリティが人事プラクティスに含まれている。
- **ポリシー**（GV.PO）：組織のサイバーセキュリティポリシーが確立、周知、執行されている。
  - GV.PO-01：サイバーセキュリティリスクを管理するためのポリシーが組織的文脈、サイバーセキュリティ戦略及び優先事項に基づいて確立、周知、執行されている。
  - GV.PO-02：サイバーセキュリティリスクを管理するためのポリシーが、要求事項、脅威、技術、及び組織のミッションの変化を反映する形でレビュー、更新、周知、執行されている。
- **監督**（GV.OV）：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活動と実行の結果がリスクマネジメント戦略の情報提供、改善、及び調整に利用されている。
  - GV.OV-01：サイバーセキュリティリスクマネジメント戦略の成果がレビューされ、戦略と方向性を調整するための情報源として利用されている。
  - GV.OV-02：サイバーセキュリティリスクマネジメント戦略がレビューされ、組織の要求事項とリスクを確実にカバーするよう調整されている。
  - GV.OV-03：組織のサイバーセキュリティリスクマネジメントの実績が、必要な調整のために評価及びレビューされている。
- **サイバーセキュリティサプライチェーンリスクマネジメント**（GV.SC）：サイバーサプライチェーン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、確立、管理、モニタリング、改善されている。
  - GV.SC-01：サイバーセキュリティサプライチェーンリスクマネジメントのプログラム、戦略、目的、ポリシー、及びプロセスが、組織の利害関係者によって確立、合意されている。
  - GV.SC-02：サプライヤー、顧客、及びパートナーがサイバーセキュリティに関して負う役割と責任が確立、周知され、内部と外部で調整が図られている。
  - GV.SC-03：サイバーセキュリティサプライチェーンリスクマネジメントが、サイバーセキュリティと企業におけるリスクマネジメント、リスクアセスメント、及び改善のプロセスに統合されている。
  - GV.SC-04：サプライヤーが把握され、重要性に応じて優先順位が付けられている。

- **GV.SC-05:** Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties
- **GV.SC-06:** Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships
- **GV.SC-07:** The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship
- **GV.SC-08:** Relevant suppliers and other third parties are included in incident planning, response, and recovery activities
- **GV.SC-09:** Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle
- **GV.SC-10:** Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement

IDENTIFY (ID): The organization's current cybersecurity risks are understood

- **Asset Management (ID.AM):** Assets (e.g., data, hardware, software, systems, facilities, services, people) 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-01:** Inventories of hardware managed by the organization are maintained
  - **ID.AM-02:** Inventories of software, services, and systems managed by the organization are maintained
  - **ID.AM-03:** Representations of the organization's authorized network communication and internal and external network data flows are maintained
  - **ID.AM-04:** Inventories of services provided by suppliers are maintained
  - **ID.AM-05:** Assets are prioritized based on classification, criticality, resources, and impact on the mission
  - **ID.AM-07:** Inventories of data and corresponding metadata for designated data types are maintained
  - **ID.AM-08:** Systems, hardware, software, services, and data are managed throughout their life cycles
- **Risk Assessment (ID.RA):** The cybersecurity risk to the organization, assets, and individuals is understood by the organization
  - **ID.RA-01:** Vulnerabilities in assets are identified, validated, and recorded

- GV.SC-05：サプライチェーンにおけるサイバーセキュリティリスクに対処するための要求事項が確立され、優先順位が付けられ、サプライヤー及びその他の関連する第三者との契約や他の種類の合意に統合されている。
- GV.SC-06：サプライヤーまたは他の第三者との正式な関係を締結する前に、リスクを低減するための計画作成と適正評価が実行されている。
- GV.SC-07：サプライヤー、それらの製品やサービス、及び他の第三者によってもたらされるリスクが理解され、記録され、優先順位が付けられ、評価され、それらの当事者との関係の過程にわたりモニタリングされている。
- GV.SC-08：関連するサプライヤー及び他の第三者がインシデントの計画作成、対応、及び復旧活動に含まれている。
- GV.SC-09：サプライチェーンセキュリティプラクティスがサイバーセキュリティと企業のリスクマネジメントプログラムに統合され、それらの実施状況が技術製品やサービスのライフサイクル全体にわたりモニタリングされている。
- GV.SC-10：サイバーセキュリティサプライチェーンリスクマネジメント計画において、パートナーシップまたはサービス合意の締結後に発生する活動に関する規定が含まれている。

識別（ID）：組織の現在のサイバーセキュリティリスクが理解されている。

- **資産管理（ID.AM）**：組織のビジネスの目的達成を可能にする資産（例：データ、ハードウェア、ソフトウェア、システム、施設、サービス、人員）が識別され、組織の目的とリスク戦略に対する相対的重要性と整合的な形で管理されている。
  - ID.AM-01：組織が管理するハードウェアの目録（インベントリ）が維持されている。
  - ID.AM-02：組織が管理するソフトウェア、サービス、及びシステムの目録（インベントリ）が維持されている。
  - ID.AM-03：組織が認可したネットワーク通信及び内部と外部のネットワークデータフローの表明が維持されている。
  - ID.AM-04：サプライヤーが提供するサービスの目録（インベントリ）が維持されている。
  - ID.AM-05：資産の優先順位が、分類、重要性、リソース、及びミッションに対する影響に基づいて決められている。
  - ID.AM-07：指定されたデータ型のデータとそれに呼応するメタデータの目録（インベントリ）が維持されている。
  - ID.AM-08：システム、ハードウェア、ソフトウェア、サービス、及びデータが、それらのライフサイクル全体にわたり管理されている。
- **リスクアセスメント（ID.RA）**：組織、資産、及び個人に対するサイバーセキュリティリスクを組織が理解している。
  - ID.RA-01：資産における脆弱性が識別、検証、記録されている。

- **ID.RA-02:** Cyber threat intelligence is received from information sharing forums and sources
- **ID.RA-03:** Internal and external threats to the organization are identified and recorded
- **ID.RA-04:** Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded
- **ID.RA-05:** Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization
- **ID.RA-06:** Risk responses are chosen, prioritized, planned, tracked, and communicated
- **ID.RA-07:** Changes and exceptions are managed, assessed for risk impact, recorded, and tracked
- **ID.RA-08:** Processes for receiving, analyzing, and responding to vulnerability disclosures are established
- **ID.RA-09:** The authenticity and integrity of hardware and software are assessed prior to acquisition and use
- **ID.RA-10:** Critical suppliers are assessed prior to acquisition

- **Improvement (ID.IM):** Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions
  - **ID.IM-01:** Improvements are identified from evaluations
  - **ID.IM-02:** Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties
  - **ID.IM-03:** Improvements are identified from execution of operational processes, procedures, and activities
  - **ID.IM-04:** Incident response plans and other **c**ybersecurity plans that affect operations are established, communicated, maintained, and improved

PROTECT (PR): Safeguards to manage the organization's cybersecurity risks are used

- **Identity Management, Authentication, and Access Control (PR.AA):** Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access
  - **PR.AA-01:** Identities and credentials for authorized users, services, and hardware are managed by the organization
  - **PR.AA-02:** Identities are proofed and bound to credentials based on the context of interactions
  - **PR.AA-03:** Users, services, and hardware are authenticated
  - **PR.AA-04:** Identity assertions are protected, conveyed, and verified

- **ID.RA-02**：サイバー脅威インテリジェンスが情報共有フォーラム及び情報源から寄せられている。
- **ID.RA-03**：組織に対する内部と外部からの脅威が識別、記録されている。
- **ID.RA-04**：脆弱性を利用する脅威の潜在的な影響と発生可能性が識別、記録されている。
- **ID.RA-05**：脅威、脆弱性、発生可能性、影響が、内在的なリスクの理解とリスク対応の優先順位付けに利用されている。
- **ID.RA-06**：リスク対応が選択、優先順位付け、計画、追跡、周知されている。
- **ID.RA-07**：変更と例外が管理され、リスクの影響について評価され、記録され、追跡されている。
- **ID.RA-08**：脆弱性開示情報の受領、分析、対応のためのプロセスが確立されている。
- **ID.RA-09**：ハードウェアとソフトウェアの真正性と完全性が調達と使用に先立って評価されている。
- **ID.RA-10**：調達に先立って重要サプライヤーが評価されている。

- **改善（ID.IM）**：組織のサイバーセキュリティリスクマネジメントのプロセス、手順及び活動の改善がすべての CSF 機能にまたがって識別されている。
  - **ID.IM-01**：改善が評価を基に識別されている。
  - **ID.IM-02**：サプライヤーや関連する第三者と調整の上で行われるものを含め、セキュリティテストと演習から改善点が識別されている。
  - **ID.IM-03**：運用のプロセス、手順及び活動の実行から改善点が識別されている。
  - **ID.IM-04**：運用に影響を及ぼすインシデントへの対応計画及び他のサイバーセキュリティ計画が確立、周知、維持、改善されている。

防御（PR）：組織のサイバーセキュリティリスクを管理するための保護対策が利用されている。

- **アイデンティティ管理／認証／アクセス制御（PR.AA）**：物理的資産と論理的資産へのアクセスが、認可されたユーザ、サービス及びハードウェアに限定され、無許可アクセスについて評価されたリスクと整合的に管理されている。
  - **PR.AA-01**：認可されたユーザ、サービス及びハードウェアのアイデンティティと証明書が組織によって管理されている。
  - **PR.AA-02**：アイデンティティが証明され、相互作用の文脈に基づく証明書に限定されている。
  - **PR.AA-03**：ユーザ、サービス及びハードウェアの認証が行われている。
  - **PR.AA-04**：ID アサーションが保護、周知、検証されている。

- **PR.AA-05:** Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties
- **PR.AA-06:** Physical access to assets is managed, monitored, and enforced commensurate with risk

- **Awareness and Training (PR.AT):** The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks
  - **PR.AT-01:** Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind
  - **PR.AT-02:** Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind

- **Data Security (PR.DS):** Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information
  - **PR.DS-01:** The confidentiality, integrity, and availability of data-at-rest are protected
  - **PR.DS-02:** The confidentiality, integrity, and availability of data-in-transit are protected
  - **PR.DS-10:** The confidentiality, integrity, and availability of data-in-use are protected
  - **PR.DS-11:** Backups of data are created, protected, maintained, and tested

- **Platform Security (PR.PS):** The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability
  - **PR.PS-01:** Configuration management practices are established and applied
  - **PR.PS-02:** Software is maintained, replaced, and removed commensurate with risk
  - **PR.PS-03:** Hardware is maintained, replaced, and removed commensurate with risk
  - **PR.PS-04:** Log records are generated and made available for continuous monitoring
  - **PR.PS-05:** Installation and execution of unauthorized software are prevented
  - **PR.PS-06:** Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle

- **Technology Infrastructure Resilience (PR.IR):** Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience
  - **PR.IR-01:** Networks and environments are protected from unauthorized logical access and usage

- PR.AA-05：アクセス許可、資格付与及び認証がポリシーにおいて定義され、管理、執行、レビューされ、最小権限の原則と職務の分離の原則を組み入れている。
- PR.AA-06：資産への物理的アクセスがリスクと整合的に管理、モニタリング、執行されている。

- **意識向上とトレーニング**（PR.AT）：組織の人員は各自のサイバーセキュリティ関連職務を遂行できるよう、サイバーセキュリティに関する意識向上とトレーニングを受けている。
  - PR.AT-01：人員は、サイバーセキュリティリスクを念頭に置きながら一般的な職務を遂行するための知識とスキルを持てるよう、意識向上とトレーニングを受けている。
  - PR.AT-02：特殊な役割を担う個人は、サイバーセキュリティリスクを念頭に置きながら関連職務を遂行するための知識とスキルを持てるよう、意識向上とトレーニングを受けている。

- **データセキュリティ**（PR.DS）：情報の機密性、完全性及び可用性を保護するため、組織のリスク戦略と整合的にデータが管理されている。
  - PR.DS-01：保存されているデータの機密性、完全性及び可用性が保護されている。
  - PR.DS-02：伝送中のデータの機密性、完全性及び可用性が保護されている。
  - PR.DS-10：使用中のデータの機密性、完全性及び可用性が保護されている。
  - PR.DS-11：データのバックアップが作成、保護、維持、テストされている。

- **プラットフォームセキュリティ**（PR.PS）：物理／仮想プラットフォームのハードウェア、ソフトウェア（例：ファームウェア、オペレーティングシステム、アプリケーション）及びサービスが、それらの機密性、完全性及び可用性を保護するよう、組織のリスク戦略と整合的に管理されている。
  - PR.PS-01：構成設定管理プラクティスが確立、適用されている。
  - PR.PS-02：ソフトウェアは、リスクと整合的に維持、代替、削除されている。
  - PR.PS-03：ハードウェアは、リスクと整合的に維持、代替、削除されている。
  - PR.PS-04：ログ記録が生成され、継続的モニタリング向けに利用可能な状態にされている。
  - PR.PS-05：未認可のソフトウェアのインストールや実行が防止されている。
  - PR.PS-06：セキュアなソフトウェア開発プラクティスが統合され、ソフトウェア開発ライフサイクル全体にわたりそれらのパフォーマンスがモニタリングされている。

- **技術インフラレジリエンス**（PR.IR）：資産の機密性、完全性、可用性、及び組織のレジリエンスを保護するための組織のリスク戦略に従ってセキュリティアーキテクチャが管理されている。
  - PR.IR-01：ネットワークと環境が未認可の論理アクセスと使用から保護されている。

- **PR.IR-02:** The organization's technology assets are protected from environmental threats
- **PR.IR-03:** Mechanisms are implemented to achieve resilience requirements in normal and adverse situations
- **PR.IR-04:** Adequate resource capacity to ensure availability is maintained

DETECT (DE): Possible cybersecurity attacks and compromises are found and analyzed

- **Continuous Monitoring (DE.CM):** Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events
  - **DE.CM-01:** Networks and network services are monitored to find potentially adverse events
  - **DE.CM-02:** The physical environment is monitored to find potentially adverse events
  - **DE.CM-03:** Personnel activity and technology usage are monitored to find potentially adverse events
  - **DE.CM-06:** External service provider activities and services are monitored to find potentially adverse events
  - **DE.CM-09:** Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events
- **Adverse Event Analysis (DE.AE):** Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents
  - **DE.AE-02:** Potentially adverse events are analyzed to better understand associated activities
  - **DE.AE-03:** Information is correlated from multiple sources
  - **DE.AE-04:** The estimated impact and scope of adverse events are understood
  - **DE.AE-06:** Information on adverse events is provided to authorized staff and tools
  - **DE.AE-07:** Cyber threat intelligence and other contextual information are integrated into the analysis
  - **DE.AE-08:** Incidents are declared when adverse events meet the defined incident criteria

- **PR.IR-02**：組織の技術資産が環境的脅威から保護されている。
- **PR.IR-03**：通常の状況と緊急時におけるレジリエンス要求事項を達成するためのメカニズムが実装されている。
- **PR.IR-04**：可用性を確保するための適切なリソース容量が維持されている。

検知（DE）：サイバーセキュリティに対して起こり得る攻撃や侵入が発見され分析されている。

- **継続的モニタリング（DE.CM）**：情報資産は、異常事態、侵入の痕跡及びその他の潜在的な有害イベントを発見するよう、モニタリングされている。
  - **DE.CM-01**：潜在的な有害イベントを発見するよう、ネットワークとネットワークサービスがモニタリングされている。
  - **DE.CM-02**：潜在的な有害イベントを発見するよう、物理的環境がモニタリングされている。
  - **DE.CM-03**：潜在的な有害イベントを発見するよう、人員の活動や技術の使用状況がモニタリングされている。
  - **DE.CM-06**：潜在的な有害イベントを発見するよう、外部のサービスプロバイダによる活動とサービスがモニタリングされている。
  - **DE.CM-09**：潜在的な有害イベントを発見するよう、コンピューティングハードウェアとソフトウェア、ランタイム環境、及びそれらのデータがモニタリングされている。
- **有害イベント分析（DE.AE）**：事象の特徴付け及びサイバーセキュリティインシデントの検知のため、異常事態、侵入の兆候及び他の潜在的な有害イベントが分析されている。
  - **DE.AE-02**：付随する活動の理解を向上させるため、潜在的な有害イベントが分析されている。
  - **DE.AE-03**：多様な情報源からの情報が相関付けされている。
  - **DE.AE-04**：有害イベントの推定上の影響と範囲が理解されている。
  - **DE.AE-06**：有害イベントに関する情報が、認可された職員とツールに提供されている。
  - **DE.AE-07**：サイバー脅威インテリジェンス及び他の文脈的情報が分析に統合されている。
  - **DE.AE-08**：定義されたインシデント基準に有害イベントが当てはまる場合、インシデントが宣言されている。

RESPOND (RS): Actions regarding a detected cybersecurity incident are taken

- **Incident Management (RS.MA):** Responses to detected cybersecurity incidents are managed
  - **RS.MA-01:** The incident response plan is executed in coordination with relevant third parties once an incident is declared
  - **RS.MA-02:** Incident reports are triaged and validated
  - **RS.MA-03:** Incidents are categorized and prioritized
  - **RS.MA-04:** Incidents are escalated or elevated as needed
  - **RS.MA-05:** The criteria for initiating incident recovery are applied
- **Incident Analysis (RS.AN):** Investigations are conducted to ensure effective response and support forensics and recovery activities
  - **RS.AN-03:** Analysis is performed to establish what has taken place during an incident and the root cause of the incident
  - **RS.AN-06:** Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved
  - **RS.AN-07:** Incident data and metadata are collected, and their integrity and provenance are preserved
  - **RS.AN-08:** An incident's magnitude is estimated and validated
- **Incident Response Reporting and Communication (RS.CO):** Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies
  - **RS.CO-02:** Internal and external stakeholders are notified of incidents
  - **RS.CO-03:** Information is shared with designated internal and external stakeholders
- **Incident Mitigation (RS.MI):** Activities are performed to prevent expansion of an event and mitigate its effects
  - **RS.MI-01:** Incidents are contained
  - **RS.MI-02:** Incidents are eradicated

RECOVER (RC): Assets and operations affected by a cybersecurity incident are restored

- **Incident Recovery Plan Execution (RC.RP):** Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents
  - **RC.RP-01:** The recovery portion of the incident response plan is executed once initiated from the incident response process

対応（RS）： 検知されたサイバーセキュリティインシデント関する措置が講じられている。

- **インシデントマネジメント（RS.MA）：** 検知されたサイバーセキュリティインシデントへの対応が管理されている。
  - **RS.MA-01：** インシデントが宣言されたら、関連する第三者と調整を図った上でインシデント対応計画が実行されている。
  - **RS.MA-02：** インシデント報告の対応順位が決められ、検証されている。
  - **RS.MA-03：** インシデントが分類され優先順位が付けられている。
  - **RS.MA-04：** インシデントは必要に応じて順位が引き上げられている。
  - **RS.MA-05：** インシデント復旧の開始基準が適用されている。
- **インシデント分析（RS.AN）：** 有効な対応を確保し、フォレンジック活動と復旧活動を支援するための調査が実施されている。
  - **RS.AN-03：** インシデント発生中に起こった状況及びインシデントの根本原因を立証するための分析が実施されている。
  - **RS.AN-06：** 調査中に実施された措置が記録され、記録の完全性と出所が保持されている。
  - **RS.AN-07：** インシデントのデータとメタデータが収集され、それらの完全性と出所が保持されている。
  - **RS.AN-08：** インシデントの規模が推定され、検証されている。
- **インシデント対応の報告とコミュニケーション（RS.CO）：** 法律、規制またはポリシーによって要求される通り、対応活動について内部と外部の利害関係者との調整が図られている。
  - **RS.CO-02：** 内外の利害関係者にインシデントが通知されている。
  - **RS.CO-03：** 情報は、指定された内外の利害関係者と共有されている。
- **インシデント軽減（RS.MI）：** 事象の拡大防止と事象の影響軽減のための活動が実施されている。
  - **RS.MI-01：** インシデントが封じ込められている。
  - **RS.MI-01：** インシデントが封じ込められている。

復旧（RC）： サイバーセキュリティインシデントの影響をうけた資産と運用を復旧する。

- **インシデント復旧計画実行（RC.RP）：** サイバーセキュリティインシデントの影響を受けたシステムやサービスの運用上の可用性を確保するための復旧活動が実施されている。
  - **RC.RP-01：** インシデント対応プロセスが開始された後、インシデント対応計画における復旧部分が実行されている。

- **RC.RP-02:** Recovery actions are selected, scoped, prioritized, and performed
- **RC.RP-03:** The integrity of backups and other restoration assets is verified before using them for restoration
- **RC.RP-04:** Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms
- **RC.RP-05:** The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed
- **RC.RP-06:** The end of incident recovery is declared based on criteria, and incident-related documentation is completed

- **Incident Recovery Communication (RC.CO):** Restoration activities are coordinated with internal and external parties
  - **RC.CO-03:** Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders
  - **RC.CO-04:** Public updates on incident recovery are shared using approved methods and messaging

- **RC.RP-02**：復旧措置が選択され、範囲が設定され、優先順位が付けられ、実施されている。
- **RC.RP-03**：バックアップ及び他の修復資産が復旧のために使用される前に、それらの完全性が検証されている。
- **RC.RP-04**：インシデント後の運用規範を確立するため、重要なミッション機能とサイバーセキュリティリスクマネジメントが考慮されている。
- **RC.RP-05**：回復した資産の完全性が検証され、システムとサービスが回復し、正常な運用状態が確認されている。
- **RC.RP-06**：基準に基づいてインシデント復旧の終結が宣言され、インシデント関連資料の作成が完了している。

- **インシデント復旧コミュニケーション（RC.CO）**：復旧活動について内部と外部の当事者との調整が図られる。
  - **インシデント復旧コミュニケーション（RC.CO）**：復旧活動について内部と外部の当事者との調整が図られる。
  - **RC.CO-04**：承認された方法とメッセージングを用いて、インシデント復旧に関する公開最新情報が共有されている。

Appendix B. CSF Tiers

Table 2 contains a notional illustration of the CSF Tiers discussed in Sec. 3. The Tiers characterize the rigor of an organization's cybersecurity risk governance practices (GOVERN) and cybersecurity risk management practices (IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER).

Table 2. Notional Illustration of the CSF Tiers

Tier	Cybersecurity Risk Governance	Cybersecurity Risk Management
Tier 1: Partial	Application of the organizational cybersecurity risk strategy is managed in an ad hoc manner. Prioritization is ad hoc and not formally based on objectives or threat environment.	There is limited awareness of cybersecurity risks at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis. The organization may not have processes that enable cybersecurity information to be shared within the organization. The organization is generally unaware of the cybersecurity risks associated with its suppliers and the products and services it acquires and uses.
Tier 2: Risk Informed	Risk management practices are approved by management but may not be established as organization-wide policy. The prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.	There is an awareness of cybersecurity risks at the organizational level, but an organization-wide approach to managing cybersecurity risks has not been established. 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. Cybersecurity information is shared within the organization on an informal basis. The organization is aware of the cybersecurity risks associated with its suppliers and the products and services it acquires and uses, but it does not act consistently or formally in response to those risks.
Tier 3: Repeatable	The organization's risk management practices are formally approved and expressed as policy. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements, threats, and technological landscape.	There is an organization-wide approach to managing cybersecurity risks. Cybersecurity information is routinely shared throughout the organization. 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 the cybersecurity risks of assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risks. Executives ensure that cybersecurity is considered through all lines of operation in the organization.

Appendix B. CSF ティア

表 2 にセクション 3 で論じた CSF ティアの概念的例示が記載されている。ティアは、組織のサイバーセキュリティリスクガバナンスプラクティス（統制）及び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（識別、防御、検知、対応、復旧）の厳格さを特徴付けるものである

表 2. CSF ティアの概念的例示

ティア	サイバーセキュリティリスクガバナンス	サイバーセキュリティリスクマネジメント
ティア 1：部分的である（Partial）	組織のサイバーセキュリティリスク戦略の適用が一時的な形で管理されている。 優先順位付けは一時的であり、目的または脅威環境に正式に基づくわけではない。	組織レベルではサイバーセキュリティリスクに対する意識が限定的である。 組織は、サイバーセキュリティリスクマネジメントを、通常外で個別の状況に応じて実施する。 組織は、組織内でのサイバーセキュリティ情報の共有を可能にするプロセスを有していない可能性がある。 一般的に組織は、サプライヤーや、自組織が調達し利用する製品やサービスに付随するサイバーセキュリティリスクを意識していない。
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ラクティスは経営陣から承認されるが、組織全体のポリシーとして確立されない場合がある。 サイバーセキュリティ活動と保護ニーズの優先順位付けは、組織のリスク関連の目的、脅威環境、またはビジネス／ミッションの要求事項が直接の情報源となる。	組織レベルでサイバーセキュリティリスクに対する意識はあるが、サイバーセキュリティリスクの管理に対する組織全体でのアプローチがまだ確立されていない。 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。 サイバーセキュリティ情報は、組織内で非公式に共有されている。 組織は、自組織のサプライヤーや調達及び利用する製品やサービスに付随するサイバーセキュリティリスクを意識しているが、それらのリスクへの対応に一貫してまたは正式に行動するわけではない。
ティア 3：繰り返し適用可能である（Repeatable）	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。 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。 組織のサイバーセキュリティプラクティスは、ビジネス／ミッションの要求事情、脅威、及びテクノロジー状	サイバーセキュリティリスクのマネジメントに対する組織全体でのアプローチが存在している。サイバーセキュリティ情報は、日常的に組織全体にわたり共有されている。 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。 資産のサイバーセキュリティリスクを、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。役員は、組織

Tier	Cybersecurity Risk Governance	Cybersecurity Risk Management
		The organization risk strategy is informed by the cybersecurity risks associated with its suppliers and the products and services it acquires and uses. Personnel formally act upon those risks through mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring. These actions are implemented consistently and as intended and are continuously monitored and reviewed.
Tier 4: Adaptive	There is an organization-wide approach to managing cybersecurity risks that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risks and organizational objectives is clearly understood and considered when making decisions. Executives monitor cybersecurity risks in the same context as financial 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. It evolves from an awareness of previous activities and continuous awareness of activities on organizational systems and networks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated.	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 that incorporates advanced cybersecurity technologies and practices, the organization actively adapts to a changing technological landscape and responds in a timely and effective manner to evolving, sophisticated threats. The organization uses real-time or near real-time information to understand and consistently act upon the cybersecurity risks associated with its suppliers and the products and services it acquires and uses. Cybersecurity information is constantly shared throughout the organization and with authorized third parties.

ティア	サイバーセキュリティリスクガバナンス	サイバーセキュリティリスクマネジメント
	況の変化に対する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。	内のあらゆる業務系統を通じてサイバーセキュリティが考慮される状況を確保している。 組織のリスク戦略は、自組織のサプライヤーや調達及び利用する製品やサービスに付随するサイバーセキュリティリスクが情報源である。人員は基本的な要求事項、ガバナンス構造（例：リスク評議会）、及びポリシーの実施とモニタリングを周知するため、書面での合意などのメカニズムを通じ、それらのリスクに対して正式に行動する。それらの措置は一貫して、意図された通りに実施され、継続的にモニタリング及びレビューされる。
ティア 4：適応している（Adaptive）	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。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。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、組織の文化の一部である。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。	組織は、過去と現在のサイバーセキュリティ活動（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プラクティスを適応させる。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。 組織が調達及び利用する製品やサービスに付随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、また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。 サイバーセキュリティ情報は、絶えず組織全体にわたり共有されると共に、認可された第三者とも共有されている。

Appendix C. Glossary

CSF Category
A group of related cybersecurity outcomes that collectively comprise a CSF Function.

CSF Community Profile
A baseline of CSF outcomes that is created and published to address shared interests and goals among a number of organizations. A Community Profile is typically developed for a particular sector, subsector, technology, threat type, or other use case. An organization can use a Community Profile as the basis for its own Target Profile.

CSF Core
A taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks. Its components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome.

CSF Current Profile
A part of an Organizational Profile that specifies the Core outcomes that an organization is currently achieving (or attempting to achieve) and characterizes how or to what extent each outcome is being achieved.

CSF Function
The highest level of organization for cybersecurity outcomes. There are six CSF Functions: Govern, Identify, Protect, Detect, Respond, and Recover.

CSF Implementation Example
A concise, action-oriented, notional illustration of a way to help achieve a CSF Core outcome.

CSF Informative Reference
A mapping that indicates a relationship between a CSF Core outcome and an existing standard, guideline, regulation, or other content.

CSF Organizational Profile
A mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes.

CSF Quick Start Guide
A supplementary resource that gives brief, actionable guidance on specific CSF-related topics.

CSF Subcategory
A group of more specific outcomes of technical and management cybersecurity activities that comprise a CSF Category.

CSF Target Profile
A part of an Organizational Profile that specifies the desired Core outcomes that an organization has selected and prioritized for achieving its cybersecurity risk management objectives.

CSF Tier
A characterization of the rigor of an organization's cybersecurity risk governance and management practices. There are four Tiers: Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4).

Appendix C. 用語集

CS カテゴリー
CSF 機能を集合的に構成する、一連の関連するサイバーセキュリティ成果。

CSF コミュニティプロファイル
多数の組織間で共有される利益と目標に対処すべく創出され公表される、CSF の成果のベースライン。コミュニティプロファイルは、典型的に特定の業界、従属業界、技術、脅威の種類、または他のユースケースを想定して開発される。組織は、コミュニティプロファイルを、固有の目標のプロファイルの基礎として利用できる。

CSF コア

どの組織においても自組織のサイバーセキュリティリスクのマネジメントに役立ち得る、ハイレベルのサイバーセキュリティ上の成果に関するタクソノミー（分類法）。その構成要素は、機能、カテゴリー、及び各成果を詳述するサブカテゴリーから成る階層である。

CSF 現在のプロファイル
組織プロファイルの一部であり、組織が現在達成しつつある（または達成を試みている）コアの成果を具体的に示し、個々の成果の達成形態または達成の度合いを特徴付ける部分。

CSF 機能
サイバーセキュリティの成果に関する最も高いレベルの組織。統制、識別、防御、検知、対応、復旧の 6 つの CSF 機能がある。

CSF 機能実装例
CSF コアの成果の達成に役立つ形態の、簡潔な行動指向の概念的な例示。

CSF 参考情報
CSF コアの成果と、既存の標準、ガイドライン、または他の内容の間の関係を示すマッピング。

CSF 組織プロファイル
組織における現在の及び／または目標とするサイバーセキュリティへの取組みを、CSF コアの成果に関して記述するためのメカニズム。

CSF クイックスタートガイド
具体的な CSF 関連のトピックに関する簡潔な、すぐに実施できるガイダンスを示す補足的リソース。

CSF サブカテゴリー
CSF カテゴリーを構成する技術やマネジメントに関するサイバーセキュリティ活動の、より具体的な成果から成る集合。

CSF 目標のプロファイル
組織プロファイルの一部であり、組織が自組織のサイバーセキュリティリスクマネジメントの目的を達成するために選択し優先順位を付けた所望のコアの成果を具体的に示す部分。

CSF ティア
組織におけるサイバーセキュリティリスクのガバナンスとマネジメントのプラクティスの厳格さを特徴付けるもの。「部分的である」（ティア 1）、「リスク情報を活用している」（ティア 2）、「繰り返し適用可能である」（ティア 3）、及び「適応している」（ティア 4）の 4 通りのティアがある。

Certain commercial equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

How to Cite this NIST Technical Series Publication:
National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

Contact Information
cyberframework@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

All comments are subject to release under the Freedom of Information Act (FOIA).

実験的手順を適切に指定できるよう、本書では、一部の民間の機器、装置、ソフトウェアまたは材料を、商業的であるか否かを問わず、特定している。係る特定は、任意の製品またはサービスの NIST による推奨または是認を意味するわけではなく、また特定された材料または機器が必然的に目的に対して利用可能な最良のものであることを意味するわけでもない。

NISTNIST技術シリーズポリシー
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

このNIST技術シリーズ刊行物の引用方法：
National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29.
https://doi.org/10.6028/NIST.CSWP.29

問い合わせ先
cyberframework@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

コメントはすべて、情報公開法（FOIA）に基づき公表される。