米国国立標準技術研究所
サイバーセキュリティフレームワーク（CSF）2.0

米国国立標準技術研究所
https://doi.org/10.6028/NIST.CSWP.29.jpn より無料でご利用いただけます。
2024 年 2 月 26 日

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

概要

米国国立標準技術研究所（NIST）サイバーセキュリティフレームワーク（CSF）2.0 は、産業界、政府機関、及びその他の組織が、サイバーセキュリティリスクを管理するためのガイダンスを提供する。このフレームワークは、規模や分野、成熟度に関係なく、あらゆる組織がサイバーセキュリティの取り組みをよりよく理解し、アセスメントし、優先順位を付け、伝達するために使用できる、ハイレベルなサイバーセキュリティの成果の分類法を提供する。CSF は、成果をどのように達成することが望ましいかを規定するものではない。むしろ、これらの成果を達成するために使用できるプラクティス及び管理策に関する追加ガイダンスを提供するオンラインリソースにリンクしている。本文書では、CSF 2.0、そのコンポーネント、及び CSF 2.0 の様々な使用方法について説明する。

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、事業体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策定及び指導に責任を負う個人が、CSF の主な対象者である。また、経営幹部、取締役会、取得専門家、技術専門家、リスクマネージャー、弁護士、人事専門家、サイバーセキュリティ及びリスクマネジメント監査人など、リスクマネジメントに携わる人々も、サイバーセキュリティに関連する意思決定の指針として CSF を利用することができる。さらにCSF は、サイバーセキュリティリスクマネジメントの優先順位を設定し、伝達するポリシーを決定し、影響を与える人々（例えば、協会、専門組織、規制当局）にとっても有用である。

補足コンテンツ

NIST は、クイックスタートガイドやコミュニティプロファイルなど、組織が CSF を実装するのに役立つ追加リソースを構築し運用することを継続する。すべてのリソースは、NIST CSF ウェブサイトで公開される。NIST CSF ウェブサイトで参照するその他のリソースに関する提案は、いつでもNIST 宛て（cyberframework@nist.gov）のメールで伝えることができる。

読者への注意

特に断りのない限り、本書で引用、参照、抜粋された文書は、そのすべてが本書に組み込まれているわけではない。

バージョン 2.0 より前の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（Framework for Improving Critical Infrastructure Cybersecurity）」と呼ばれていたが、CSF 2.0 ではこの名称を使用していない。

謝辞

CSF は、米国及び世界中の産学官にわたる複数年にわたる共同作業の成果である。NIST は、本 CSF の改訂に貢献したすべての関係者に謝意を表する。CSF 策定プロセスに関する情報は、NIST CSF ウェブサイトに掲載されている。CSF の使用に関して得られた教訓は、いつでもNIST 宛て（cyberframework@nist.gov）のメールで共有することができる。

Translated by Mr. Matsushima, Information-technology Promotion Agency, Japan.
Translated with permission courtesy of the National Institute of Standards and Technology (NIST).
Translation reviewed on behalf of NIST by TaikaTranslations LLC under contract {133ND23PNB770271}.
Official U.S. Government Translation. All rights reserved, US Secretary of Commerce.

翻訳者：情報処理推進機構、松島氏。米国国立標準技術研究所（NIST）の許可を得て翻訳。翻訳は、契約書 {133ND23PNB770271} に基づき、NIST に代わって TaikaTranslations LLC が確認。米国政府公式翻訳。
著作権はすべて米国商務長官に帰属。

目次

1. サイバーセキュリティフレームワーク（CSF）の概要 1
2. CSF コアの概論 3
3. CSF プロファイル及びティアの概論 6
3.1. CSF プロファイル 6
3.2. CSF ティア 7
4. CSF を補足するオンラインリソースの紹介 9
5. サイバーセキュリティリスクのコミュニケーションと統合の改善 10
5.1. リスクマネジメントコミュニケーションの改善 10
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 11
附属書 A. CSF コア 15
附属書 B. CSF ティア 24
附属書 C. 用語集 26

図表一覧

図1. CSF コアの構造 3
図2. CSF の機能 5
図3. CSF 組織プロファイルの作成と使用の手順 6
図4. サイバーセキュリティリスクガバナンスとマネジメントのための CSF の階層 8
図5. リスクマネジメントコミュニケーション向上のための CSF の活用 10
図6. サイバーセキュリティとプライバシーリスクの関係 13

序文

サイバーセキュリティフレームワーク（CSF）2.0は、産業界、政府機関、学術機関、非営利団体など、あらゆる規模及び分野の組織が、サイバーセキュリティのリスクを管理し、軽減することを支援するために設計されている。組織の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。とはい　え、CSF は万能のアプローチを採用しているわけではない。各組織には共通のリスクと固有のリスクの両方があり、リスク選好度や許容度、特定のミッション、ミッションを達成するための目的も様々である。必然的に、組織がCSFを実装する方法も異なってくる。

理想的には、CSF は、財務、プライバシー、サプライチェーンリスク、評判、技術的リスク、 物理的リスクなど、事業体の他のリスクとともに、サイバーセキュリティリスクに対処するために使用される。

CSF は、サイバーセキュリティの専門知識の有無にかかわらず、経営幹部、管理職、実務者など、 幅広い対象者に理解されることを意図した望ましい成果を記述している。これらの成果は業種、国、技術にとらわれないため、組織独自のリスク、技術、ミッションに対処するために必要な柔軟性を提供する。成果は、サイバーセキュリティリスクを軽減するために直ちに検討する可能性があるセキュリティ管理策のリストに直接マッピングされている。

CSF は規範的なものではなく、ユーザーが具体的な成果について学び、選択することを支援するものである。具体的な成果をどのように達成するかについての提案は、一連のクイックスタートガイド（QSG）など、CSF を補完する一連のオンラインリソースの中で提供されている。また、プロセスの一部を自動化することを選択した組織を支援するために、様々なツールがダウンロード可能なフォーマットで提供されている。QSG は、CSF の最初の使用方法を提案し、読者に CSF と関連リソースをより深く探求するよう促している。NIST CSF ウェブサイト を通じて入手可能な CSF と、NIST 等が提供するこれらの補足リソースは、リスクの管理と低減を支援する「CSF ポートフォリオ」として捉えることが望ましい。どのように適用するかにかかわらず、CSF は、ユーザーが自社のサイバーセキュリティ態勢を状況に応じて検討し、CSF を特定のニーズに適合させるよう促している。

CSF 2.0は、旧バージョンをベースに、統治とサプライチェーンの重要性を強調する新機能を盛り込んでいる。QSG には特に注意が払われており、大規模な組織だけでなく、小規模な組織も CSF に関連性があり、容易に使用可能であることを確かなものにしている。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、定期的に更新されている。現状と目標の状態の組織プロファイルを作成することで、組織が現状とあるべき姿を比較し、より迅速にセキュリティ管理策を実装し、アセスメントすることができる。

サイバーセキュリティリスクは絶えず拡大しており、そのリスクを管理するプロセスは、継続的でなければならない。このことは、組織がサイバーセキュリティの課題に直面し始めたばかりであるか、あるいは高度で十分なリソースを備えたサイバーセキュリティチームを擁して長年活動してきたかに関係なく当てはまる。CSFは、あらゆるタイプの組織にとっても価値があるように設計されており、長期にわたって適切なガイダンスを提供することが期待されている。

1. サイバーセキュリティフレームワーク（CSF）の概要

この文書は、NIST サイバーセキュリティフレームワーク（フレームワーク 又は *CSF*）のバージョン 2.0 である。これには、以下のコンポーネントが含まれている。

- ***CSF*** コア：CSF の中核であり、あらゆる組織のサイバーセキュリティリスクマネジメントに役立つ、ハイレベルなサイバーセキュリティの成果の分類法である。CSF コアのコンポーネントは、各成果の詳細を示す機能、カテゴリー、サブカテゴリーの階層構造になっている。これらの成果は、サイバーセキュリティの専門知識の有無にかかわらず、経営幹部、管理職、実務者など、幅広い層が理解することができる。成果は、セクター、国、テクノロジーに中立であるため、組織固有のリスク、テクノロジー、及びミッションの考慮事項に対処するために必要な柔軟性を組織に提供する。
- ***CSF*** 組織プロファイル：組織の現在のサイバーセキュリティ態勢と目標のサイバーセキュリティ態勢を、CSF コアの成果の観点から説明するための仕組みである。
- ***CSF*** ティア：CSF 組織プロファイルに適用することで、組織のサイバーセキュリティリスクガバナンスとプラクティスマネジメントの厳格さを特徴付けることができる。また、ティアは、組織がサイバーセキュリティリスクをどのように捉えているか、また、それらのリスクを管理するためにどのようなプロセスを実施しているかについて、そのコンテキストを提供することもできる。

この文書は、組織がどのような望ましい成果を達成することを目指すことができるかを説明するものである。成果やその達成方法を規定するものではない。組織がこれらの成果を達成する方法については、本 CSF を補完する一連のオンラインリソースに記載されており、NIST CSF ウェブサイト から入手可能である。これらのリソースは、成果を達成するために使用できるプラクティスや管理策に関する追加的なガイダンスを提供し、組織が CSF を理解し、採用し、使用することを支援することを意図している。これらのリソースには、以下が含まれる。

- 既存のグローバル標準、ガイドライン、フレームワーク、規制、ポリシーなどから、各成果に関するガイダンスの情報源を指し示す参考文献。
- 各成果を達成する潜在的な方法を示す実装例
- CSF の旧バージョンからバージョン 2.0 への移行を含め、CSF 及びそのオンラインリソースの使用に関する実用的なガイダンスを提供するクイックスタートガイド。
- 組織が CSF を実践し、サイバーセキュリティリスクマネジメントの優先順位を設定するのに役立つ、コミュニティプロファイルと組織プロファイルのテンプレート

組織は、サイバーセキュリティリスクを理解し、アセスメントし、優先順位を付け、伝達するために、CSF コア、プロファイル、ティア、及び補足リソースを使用することができる。

- 理解し、アセスメントする：組織の一部または全部のサイバーセキュリティ態勢の現状または目標を説明し、ギャップを特定し、そのギャップへの対処に向けた進捗をアセスメントする。

- 優先順位を付ける：組織のミッション、法的及び規制要件、リスクマネジメント及びガバナンスの期待に沿ったサイバーセキュリティリスクを管理するためのアクションを識別し、整理し、優先順位を付ける。
- コミュニケーションを図る：サイバーセキュリティのリスク、ケイパビリティ（能力）、ニーズ、期待について、組織内外でコミュニケーションするための共通言語を提供する。

CSF は、サイバーセキュリティプログラムの成熟度に関係なく、産業界、政府機関、学術機関、非営利団体など、あらゆる規模及び分野の組織が使用できるように設計されている。CSF は、自主的に、及び政府のポリシーと義務を通じて採用することができる基礎的なリソースである。CSF の分類法及び参照される標準、ガイドライン、プラクティスは国を特定するものではなく、CSF の旧バージョンは、米国内外の多くの政府やその他の組織によって活用され、成功を収めている。

CSF は、サイバーセキュリティリスクをより適切に管理し、事業体レベルの情報通信技術（ICT）リスクの全体的なマネジメントに反映させるために、他の情報リソース（例えば、フレームワーク、標準、ガイドライン、リーディングプラクティス）と組み合わせて使用することが望ましい。CSF は柔軟なフレームワークであり、規模の大小にかかわらず、すべての組織が使用できるようテーラリングされることを意図している。組織には、様々な脅威及び脆弱性を含む固有のリスクとリスク許容度、及び固有のミッション目的と要件が引き続き存在する。したがって、組織がリスクを管理するためのアプローチとCSFを実装する組織は様々であろう。

この文書の残りの部分は、以下のように構成されている：

- セクション2では、CSF コアの基本について説明する：機能、カテゴリー、サブカテゴリー。
- セクション3では、CSF プロファイルとティアの概念を定義する。
- セクション4では、CSFの一連のオンラインリソースの選択コンポーネントの概要を示す：参考情報、実装例、クイックスタートガイド。
- セクション5では、組織がCSFを他のリスクマネジメントプログラムと統合する方法について述べている。
- 附属書 A は、CSFコアである。
- 附属書 B は、CSF ティアの概念的な実例を示している。
- 附属書 C は、CSF用語集である。

2. CSF コアの概論

附属書 A は CSF コアで、図1に示すように、機能、カテゴリー、サブカテゴリーの順に並べた、一連のサイバーセキュリティの成果である。これらの成果は、実行すべきアクションのチェックリストではない。成果を達成するために行う具体的なアクションは、組織やユースケースによって異なり、それらのアクションに責任を負う個人によっても異なるであろう。さらに、コアにおける機能、カテゴリー、サブカテゴリーの順番や大きさは、それらを達成する順序や重要性を意味するものではない。本コアの構成は、組織内でリスクマネジメントの運用を担当する者に最も共感されるように意図されている。

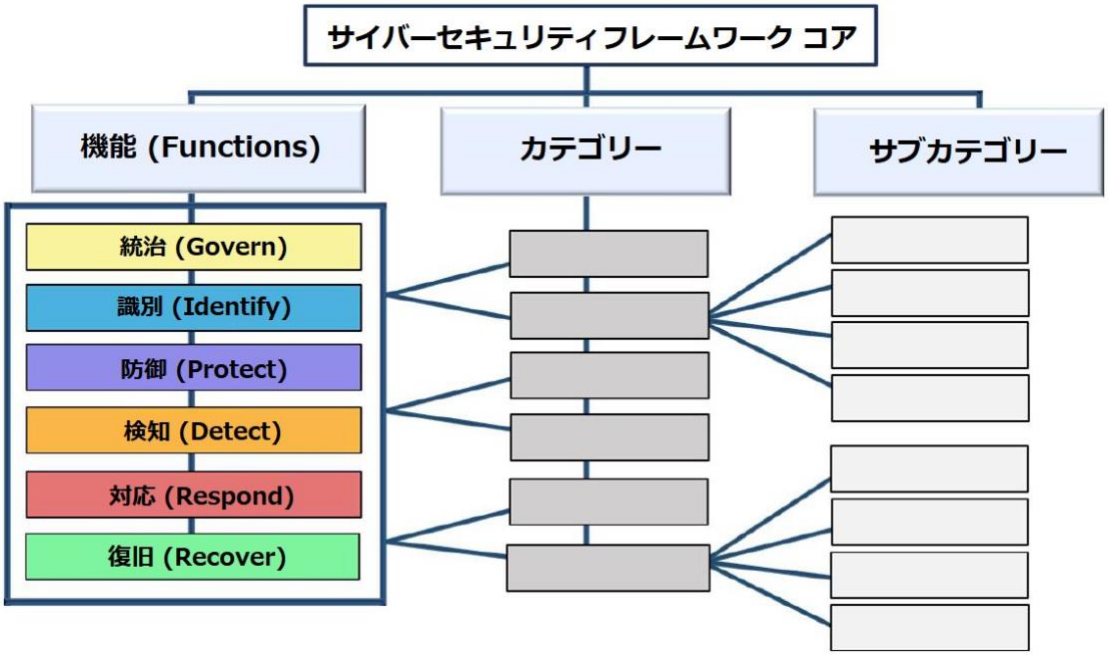

図1. CSFコアの構造

統治（GOVERN）、識別（IDENTIFY）、防御（PROTECT）、検知（DETECT）、対応（RESPOND）、復旧（RECOVER）という CSF コア機能は、最上位レベルでサイバーセキュリティの成果を体系化している。

- 統治（GV）－組織のサイバーセキュリティリスクマネジメント戦略、期待、ポリシーを確立され、伝達され、監視（モニタリング）される。統治機能は、組織のミッション及びステークホルダーの期待に照らして、他の5つの機能の成果を達成し、優先順位をつけるために組織が何をすべきかを知らせるための成果を提供する。統治活動は、サイバーセキュリティを組織の広範なエンタープライズリスクマネジメント（ERM）戦略に組み込むために重要である。統治は、組織の背景の理解、サイバーセキュリティ戦略及びサイバーセキュリティサプライチェーンのリスクマネジメントの確立、役割、責任、権限、ポリシー、サイバーセキュリティ戦略の監視に取り組む。
- 識別（ID）－組織の現在のサイバーセキュリティリスクが識別されている。組織の資産（例えば、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）、サプライヤ、及び関連するサイバーセキュリティリスクを識別することで、リスクマネジメント戦略及び統治で特定されたミッションのニーズに合致した取り組みに優先順位を付けることができる。

この機能には、サイバーセキュリティのリスクマネジメントを支援する組織のポリシー、計画、プロセス、手順、及びプラクティスの改善機会を識別し、6つの機能すべてにおける取り組みに情報を提供することも含まれる。

- 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セーフガード（セキュリティ対策）が使用される。資産及びリスクが特定され、優先順位が付けられると、防御は、有害なサイバーセキュリティ事象の起こりやすさ及びインパクトを防止又は低減するためだけでなく、機会をうまく利用する可能性と効果を高めるために、それらの資産をセキュアにする能力をサポートする。この機能によってカバーされる成果には、ID管理、認証、アクセス管理策、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（例えば、物理及び仮想プラットフォームのハードウェア、ソフトウェア、サービスのセキュア化）、技術インフラのレジリエンスが含まれる。
- 検知 (DE) – 起こり得るサイバーセキュリティ攻撃及び侵害の可能性が発見され、分析される。検知は、サイバーセキュリティ攻撃及びインシデントが発生していることを示す異常、侵害の指標、及びその他の潜在的な有害事象のタイムリーな発見及び分析を可能にする。この機能は、インシデント対応及び復旧活動の成功を支援する。
- 対応 (RS) – 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アクションが実行される。対応は、サイバーセキュリティインシデントの影響を抑制する能力をサポートする。この機能の成果には、インシデント管理、分析、軽減、報告、コミュニケーションが含まれる。
- 復旧 (RC) – 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及び業務が復旧される。復旧は、サイバーセキュリティインシデントの影響を低減し、復旧作業中の適切なコミュニケーションを可能にするために、通常業務のタイムリーな復旧を支援する。

多くのサイバーセキュリティリスクマネジメント活動は、ネガティブな事象の発生を防止することに重点を置いているが、ポジティブな機会の活用を支援することもある。サイバーセキュリティリスクを低減するためのアクションは、収益を増加させるなど、他の方法で組織に利益をもたらす可能性がある（例えば、まず余剰の施設スペースを商用ホスティングプロバイダに提供し、自社や他の組織のデータセンターをホスティングしてもらい、その後、サイバーセキュリティリスクを低減するために、主要な財務システムを組織内のデータセンターからホスティングプロバイダに移転する）。

図 2 は、すべての機能が互いに関連しているため、CSF の機能を車輪のように示している。例えば、組織は識別（IDENTIFY）で資産を分類し、防御（PROTECT）でそれらの資産をセキュア化するための措置を講じる。統治（GOVERN）機能と 識別（IDENTIFY）機能での計画とテストへの投資は、検知（DETECT） 機能での予期せぬ事象のタイムリーな検知をサポートし、対応（RESPOND）機能と復旧（RECOVER）機能での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と復旧活動を可能にする。統治（GOVERN）は、組織が他の5つの機能をどのように実装するかを示す情報であるため、車輪の中心に位置する。

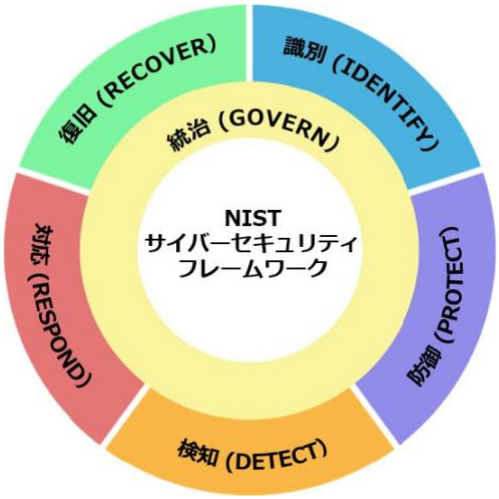

図2. CSFの機能

機能は同時に対処することが望ましい。統治、識別、防御、及び検知を支援するアクションはすべて継続的に行われることが望ましく、対応と復旧を支援するアクションは常に準備されており、サイバーセキュリティインシデントが発生したときに行われることが望ましい。すべての機能には、サイバーセキュリティインシデントに関連する重要な役割がある。統治、識別、防御の成果はインシデントの予防と準備に役立ち、統治、検知、対応、復旧の成果はインシデントの発見と管理に役立つ。

各機能には、その内容を要約する動詞の名前が付けられている。各機能は、関連するサイバーセキュリティの成果である「カテゴリー」に分けられ、そのカテゴリーが集合的に機能を構成する。サブカテゴリーは、各カテゴリーをさらに技術的・管理的活動のより具体的な成果に分割する。サブカテゴリーは網羅的ではないが、各カテゴリーをサポートする詳細な成果を記述している。

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）、及び制御・運用技術（OT）を含む、組織が使用するすべてのICTに適用される。また、クラウド、モバイル、人工知能システムを含む、あらゆる種類のテクノロジー環境にも適用される。CSFコアは将来を見据えたものであり、将来の技術や環境の変化に適用することを意図している。

3. CSF プロファイル及びティアの概論

このセクションでは、CSF プロファイル及び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、コアの成果という観点から、組織の現在及び／または目標とするサイバーセキュリティ態勢を記述するものである。組織プロファイルは、組織のミッション目的、ステークホルダーの期待、脅威の状況、要件を考慮して、コアの成果を理解、調整、アセスメント、優先順位付け、伝達するために使用される。組織は、特定の成果を達成するためのアクションに優先順位を付け、その情報をステークホルダーに伝えることができる。

すべての組織プロファイルには、以下のいずれか、又は両方が含まれる:

1. 現状プロファイルは、組織が現在達成している（または達成しようとしている）コアの成果を特定し、各成果がどのように、又はどの程度達成されているかを特徴づけるものである。
2. 目標プロファイルは、組織が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、優先順位をつけた望ましい成果を特定するものである。目標プロファイルは、新たな要件、新技術の採用、脅威情報の動向など、組織のサイバーセキュリティ態勢に予想される変化を考慮する。

コミュニティプロファイル（*Community Profile*）は、CSF の成果のベースラインであり、多数の組織間で共有される関心や目標に対応するために作成、公表される。コミュニティプロファイルは通常、特定のセクター、サブセクター、技術、脅威の種類、その他のユースケースを対象として策定される。コミュニティプロファイルファイルを独自の目標プロファイルの基礎として使用することができる。
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 に示し、以下に要約するステップは、組織がサイバーセキュリティの継続的改善に役立てるために組織プロファイルを使用する方法の1つを示している。

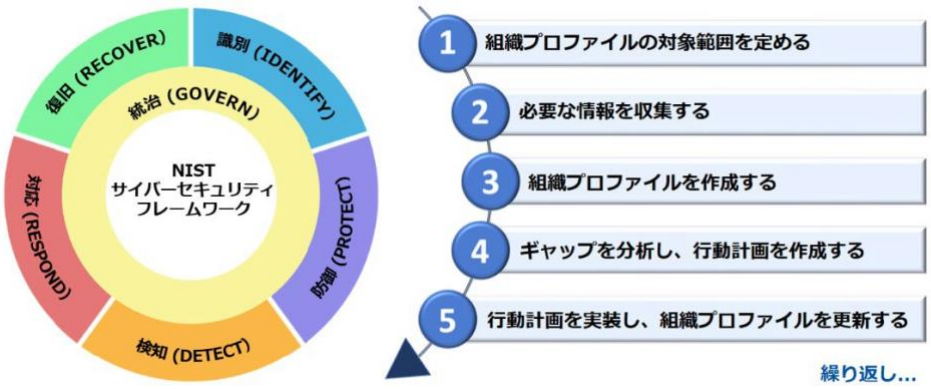

図3. CSF 組織プロファイルの作成と使用手順

1. 組織プロファイルの対象範囲を定める。プロファイルの対象範囲を定義するために、プロファイルの基礎となるハイレベルの事実と前提条件を文書化する。組織は希望する数の組織プロファイルを持つことができ、それぞれが異なる対象範囲を持つ。例えば、プロファイルは組織全体を対象とすることもできるし、組織の財務システムを対象とすることも、ランサムウェアの脅威への対策や財務システムに関わるランサムウェアインシデントへの対応を対象とすることもできる。
2. 組織プロファイルの準備に必要な情報を収集する。情報の例としては、組織のポリシー、リスクマネジメントの優先順位とリソース、事業体リスクプロファイル、ビジネスインパクト分析（BIA）登録簿、組織が従うサイバーセキュリティ要件及び標準、プラクティス及びツール（例えば、手順及びセーフガード）、業務の役割などが考えられる。
3. 組織プロファイルを作成する。選択した CSF の成果に対して、プロファイルに含めることが望ましい情報の種類を決定し、必要な情報を文書化する。目標プロファイルの計画と優先順位付けに情報を与えるため、現状プロファイルのリスクへの影響を検討する。また、目標プロファイルの基礎として地域社会のプロファイルを使用することも検討する。
4. 現状プロファイルと目標プロファイル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、現状プロファイルと目標プロファイルの差異を識別・分析し、そのギャップに対処するための優先順位をつけた行動計画（例えば、リスク登録簿、リスク詳細報告書、行動計画及びマイルストーン[POA&M]）を策定する。
5. 行動計画を実装し、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、組織を目標プロファイルに向けて前進させる。行動計画には、全体的な期限が設けられている場合もあれば、継続的な場合もある。

継続的改善の重要性を考えれば、組織はこれらのステップを必要に応じて何度でも繰り返すことができる。

組織プロファイルには他にも用途がある。例えば、現状プロファイルは、組織のサイバーセキュリティケイパビリティ（能力）と既知の改善機会を文書化し、ビジネスパートナーや見込み顧客などの外部のステークホルダーに伝えるために使用できる。また、目標プロファイルは、組織のサイバーセキュリティリスクマネジメントの要件と期待を、サプライヤ、パートナー、その他の第三者に対して、それらの関係者が達成すべき目標として表現するのに役立つ。

3.2. CSF ティア

組織は、ティアを使用して、現状プロファイル及び目標プロファイルを通知することを選択できる。ティアは、組織のサイバーセキュリティリスクガバナンスと管理プラクティスの厳しさを特徴付けるものであり、組織がサイバーセキュリティリスクをどのようにとらえ、 それらのリスクを管理するために実施されているプロセスについての状況を示す。ティアは、図 4 に示すように、また、附属書 B に概念的に示すように、サイバーセキュリティリスクを「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）、「反復可能である」（ティア 3）、「適応している」（ティア 4）として管理するための組織のプラクティスを反映している。ティアは、非公式で場当たり的な対応から、機敏で、リスクが伝達され、継続的に改善するアプローチへの段階を表している。ティアを選択することで、組織がサイバーセキュリティリスクをどのように管理するかについて、全体的な方向性を定めることができる。

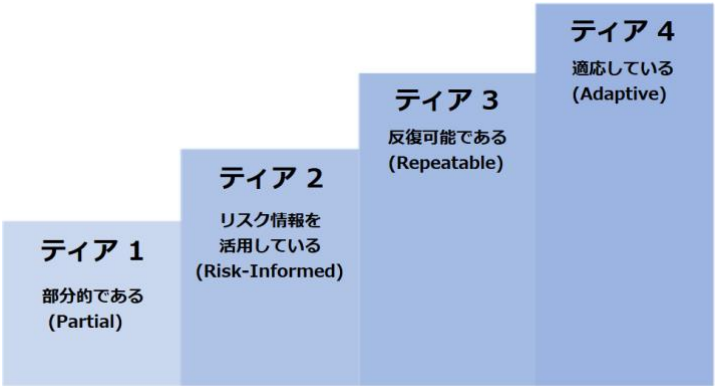

図4. サイバーセキュリティリスクのガバナンスとマネジメントのための CSF ティア

ティアは、組織のサイバーセキュリティリスクマネジメント手法を置き換えるのではなく、補完することが望ましい。例えば、組織はサイバーセキュリティリスクを管理するための組織全体[1]のアプローチのベンチマークとして、ティアを内部コミュニケーションに使用することができる。リスクまたは義務付けがより大きい場合、または費用対効果分析によってサイバーセキュリティの負のリスクを実現可能かつ費用対効果的に低減できることが示された場合には、より高いティアに進むことが推奨される。

NISTの CSF ウェブサイトでは、プロファイルとティアの使用に関する追加情報を提供している。これには、NISTが提供している組織プロファイルテンプレートへのポインタや、機械可読で人間が使用できる様々な形式のコミュニティプロファイルのリポジトリが含まれている。

[1]本文書では、「組織全体」と「事業体」という用語は同じ意味を持つ。

4. CSF を補足するオンラインリソースの紹介

NISTと他の組織は、組織が CSF を理解し、採用し、利用するのに役立つ一連のオンラインリソースを作成している。これらの追加リソースはオンラインで提供されているため、ユーザーに安定性を提供するために更新頻度が低い本文書よりも頻繁に更新され、機械可読形式で利用することができる。このセクションでは、3種類のオンラインリソース（参考情報、実装例、クイックスタートガイド）の概要を説明する。

参考情報（*Informative References*）は、コアと様々な標準、ガイドライン、規制、その他の内容と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達成するための情報提供に役立つ。参考情報は、分野や技術に特化したものとすることができる。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。参考情報の中には、サブカテゴリーよりも範囲が狭いものもある。例えば、SP800-53「情報システム及び組織のためのセキュリティ及びプライバシー管理策」の特定の管理策は、あるサブカテゴリーに記述されている成果を達成するために必要な多くの参考情報の一つである場合がある。その他の参考情報は、多くのサブカテゴリーに部分的に対応するポリシーの要件など、より高いレベルのものである。CSF を使用する場合、組織は最も関連性の高い参考情報を識別することができる。

実装例は、サブカテゴリーの成果を達成するための、簡潔でアクション指向のステップの想定例を提供する。実施例を表現するために使用される動詞には、共有する、文書化する、開発する、実行する、監視する、分析する、アセスメントする、行使する、などがある。実装例は、成果を達成するために組織が取り得るすべてのアクションの包括的なリストではなく、サイバーセキュリティリスクに対処するために必要なアクションのベースラインを示すものでもない。

クイックスタートガイド（*QSG*）は、特定の CSF 関連トピックに関する簡潔な文書であり、多くの場合、特定の対象者向けにテーラリングされる。QSG は、CSF の特定の部分を、組織がサイバーセキュリティ態勢と関連リスクの管理を改善するために検討できる、実行可能な「最初の一歩」に集約しているため、組織が CSFを実装する際に役立つ。QSGはそれぞれのタイムリーな時期に改訂され、必要に応じて新しいガイドが追加される。

CSF 2.0のための新たな参考情報についての提案は、いつでもNIST（olir@nist.gov）に伝えることができる。QSG の追加トピックを含め、NISTの CSF ウェブサイトで参照すべきその他のリソースに関する提案は、cyberframework@nist.gov 宛てに送付することが望ましい。

5. サイバーセキュリティリスクのコミュニケーションと統合の改善

CSF の使用は、組織固有のミッションとリスクによって異なる。ステークホルダーの期待、リスク選好度、許容度（「統治」で概説）を理解することで、組織はサイバーセキュリティに関する支出及びアクションについて情報に基づいた意思決定を行うために、サイバーセキュリティ活動を優先順位付けすることができる。組織は、潜在的なインパクトや起こりやすさに応じて、ネガティブなリスクの軽減、移転、回避、受容、又はポジティブなリスクの実現、共有、強化、受容など、1つまたは複数の方法でリスクに対処することを選択できる。重要なことは、組織が CSF を内部的に使用してサイバーセキュリティのケイパビリティ（能力）を管理することも、外部的に使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したりすることもできるということである。

CSF の利用に関係なく、組織は、サイバーセキュリティリスクとそのリスクを管理するためのアクションを理解し、アセスメントし、優先順位を付け、伝達するためのガイダンスとして CSF を使用することで、恩恵を受けることができる。選択された成果は、優先順位と利用可能なリソースを考慮しながら、サイバーセキュリティ態勢を改善し、ミッションに不可欠な機能の継続性を維持するための戦略的な意思決定に焦点を当て、実装するために使用することができる。

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に対する期待、計画、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盤となる。CSF は、組織の優先順位と戦略的方向性を重視する経営幹部と、それらの優先順位の達成に影響を及ぼす可能性のある特定のサイバーセキュリティリスクを管理するマネージャーとの間で、（図 5 の上半分に示すような）双方向の情報の流れを促進する。CSF はまた、マネージャーと、技術を実装・運用する実務者の間でも同様の流れ（図 5 の下半分）をサポートする。図の左側は、実務者が最新情報、知見、及び懸念をマネージャーや経営幹部と共有することの重要性を示している。

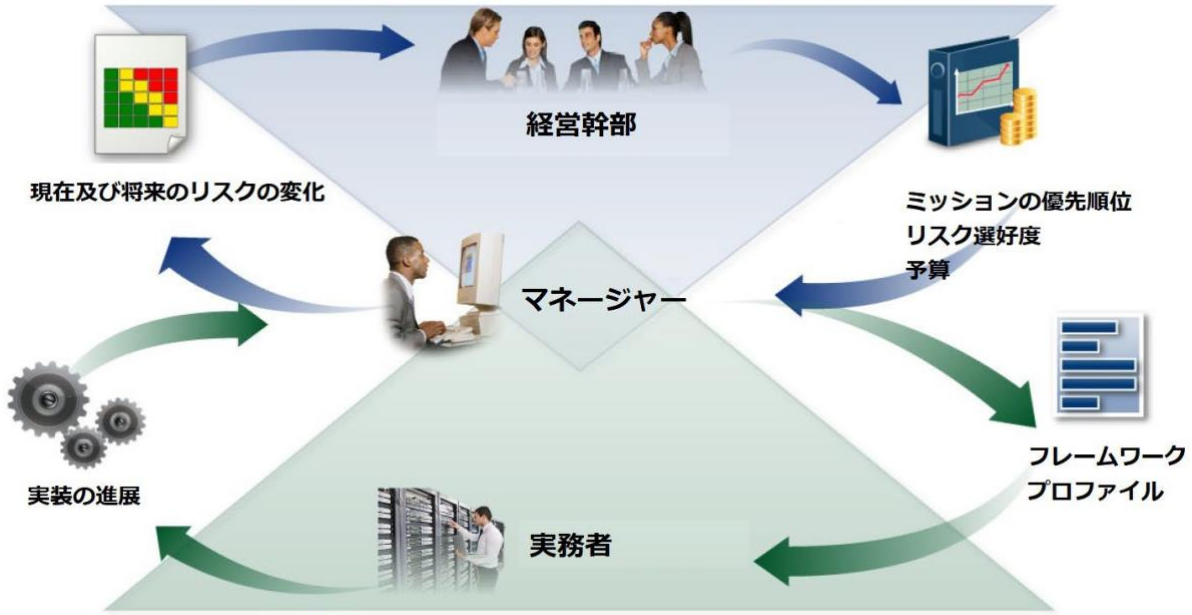

図5. リスクマネジメントコミュニケーション向上のためのCSFの活用

組織プロファイルの作成と使用の準備には、組織の優先順位、リソース、リスクの方向性に関する情報を経営幹部から収集することが含まれる。次に、マネージャーは実務者と協力して、ビジネスニーズを伝え、リスク情報を活用したプロファイルを作成する。現状プロファイルと目標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アクションは、マネージャーと実務者によって実施され、システムレベルの計画に重要なインプットを提供する。システムレベルで適用される管理策や監視（モニタリング）を含め、組織全体で目標状態が達成されると、更新された結果はリスク登録簿や進捗報告書を通じて共有することができる。継続的なアセスメントの一環として、マネージャーは、潜在的な危害をさらに低減し、潜在的な便益を増大させる調整を行うための知見を得る。

統治機能は、経営幹部との組織的なリスクコミュニケーションをサポートする。経営幹部による議論には、戦略、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達成にどのような影響を及ぼす可能性があるかが含まれる。これらのガバナンスに関する議論は、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をサポートする。経営幹部は、これらのニーズに基づいてサイバーセキュリティの優先順位と目的を設定する際に、リスク選好度、説明責任、リソースに関する期待を伝達する。また、経営幹部は、サイバーセキュリティリスクマネジメントをERM プログラムや下位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（第 5.2 節を参照）。図 5 の上半分に示されているコミュニケーションには、ERM や下位レベルのプログラムに関する考慮事項を含めることができ、それによりマネージャーや実務者に情報が提供される。

経営幹部が設定する全体的なサイバーセキュリティの目的は、マネージャーによって情報提供され、マネージャーに伝達される。営利企業の場合は、これらは基幹業務部門又は事業部門に当てはまる場合がある。政府機関の場合は、部門レベル又は部課レベルの検討事項となる可能性がある。CSF を実装する場合、マネージャーは、目標プロファイルに示され、行動計画（例えば、リスク登録簿、リスク詳細報告書、POA&M）で追跡されるアクションを通じて改善される、共通サービス、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。

実務者は、特定のサイバーセキュリティ活動の計画、実行、監視に役立てるために、目的状態の実装と運用リスクの変化の測定に重点を置く。受容可能なレベルでリスクを管理するための管理策が実装されると、実務者は、組織のサイバーセキュリティ態勢を理解し、十分な情報に基づいた意思決定を行い、それに応じてリスク戦略を維持又は調整するために必要な情報（例えば、主要業績評価指標、主要リスク指標）をマネージャーと経営幹部に提供する。経営幹部は、このサイバーセキュリティリスクデータを、組織全体からの他の種類のリスクに関する情報と組み合わせることもできる。期待と優先順位の更新は、サイクルが繰り返される中で、更新された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

あらゆる組織は、多くの種類のICTリスク（例えば、プライバシー、サプライチェーン、人工知能）に直面しており、各リスクに固有のフレームワークやマネジメントツールを使用している可能性がある。一部の組織は、ERMを使用することで、ICTと他のすべてのリスクマネジメントの取り組みを高いレベルで統合しているが、一方で、それぞれの取り組みに確実に十分な注意を払うために、取り組みを別個のものとして維持している組織もある。小規模組織は、本質的に、事業体レベルでリスクを監視（モニタリング）することができる一方、大企業ではERMに統合された個別のリスクマネジメントを維持する場合がある。

組織は、サイバーセキュリティを含むリスク考慮事項のポートフォリオのバランスを取り、情報に基づいた意思決定を行うために、ERM アプローチを採用することができる。経営幹部は、ガバナンスとリスク戦略を 過去のCSF の使用結果と統合する際に、現在及び計画中のリスク活動に関する重要な情報を得る。CSF は、組織がサイバーセキュリティと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、経営幹部が理解できる

一般的なリスクマネジメント用語に置き換えるのに役立つ。

サイバーセキュリティリスクマネジメントと ERM の相互関係を説明しているNISTのリソースには、以下のものがある。

- *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、次のような個別の ICT リスクマネジメントプログラムと統合する際に、CSF が有益であると考える場合がある。

- サイバーセキュリティリスクマネジメントとアセスメント：CSF は、SP800-37「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」及び NIST のリスクマネジメントフレームワーク（RMF）の SP800-30「リスクアセスメント実施ガイド」など、確立されたサイバーセキュリティリスクマネジメント及びアセスメントプログラムと統合することができる。NIST の RMF 及びその一連の出版物を使用する組織の場合、CSFは、SP 800-53「情報システム及び組織のためのセキュリティ及びプライバシー管理策（*Security and Privacy Controls for Information Systems and Organizations*）」の管理策の選択及び優先順位付けに関するRMFのアプローチを補完するために使用することができる。
- 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独立した分野であるが、図6に示すように、ある特定の状況では目的が重複する。

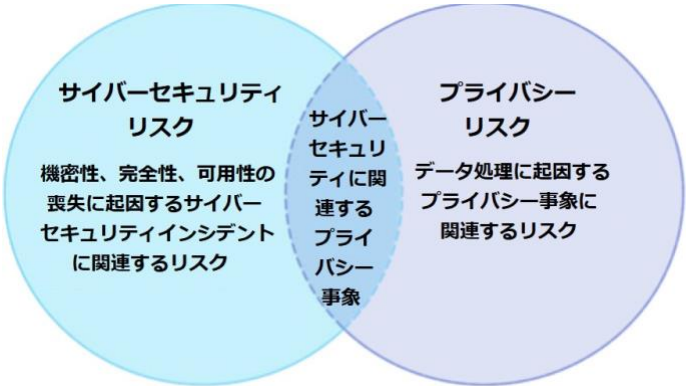

図6. サイバーセキュリティリスクとプライバシーリスクの関係

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に対処するために不可欠である。例えば、データ侵害は、個人情報の盗難につながる可能性がある。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な手段によっても生じる可能性もある。

組織は、ミッションやビジネスの目的を達成するためにデータを処理するが、その結果、個人が問題を経験する場合があるプライバシー事象が生じる可能性がある。これらの問題は様々な形で表現され得るが、NISTは、これらの問題を、尊厳に関わる影響（例えば、困惑又は汚名）から、より具体的な被害（例えば、差別、経済的損失、身体的被害）にまで及ぶと説明している。NIST のプライバシーフレームワーク及びサイバーセキュリティフレームワークは、サイバーセキュリティリスク及びプライバシーリスクの異なる側面に対処するために併用することができる。さらに、NIST のプライバシーリスク アセスメント手法（PRAM）には、プライバシーリスクアセスメントで使用する問題例の一覧がある。

- サプライチェーンリスク：組織は、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の監視とステークホルダーとのコミュニ ケーションを促進するために、CSF を利用することができる。あらゆる種類の技術は、地理的に多様なルートと複数の外部委託レベルを持つ、複雑で、グローバルに分散し、広範で、相互接続されたサプライチェーンのエコシステムに依存している。このエコシステムは、技術製品及びサービスの研究、開発、設計、製造、調達、納入、統合、運用、保守、廃棄、及びその他の、利用又は管理のために相互作用する官民の事業体（例えば、取得者、サプライヤ、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、その他の技術関連サービスプロバイダ）によって構成されている。これらの相互作用は、技術、法律、ポリシー、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結びついた関係を考慮すると、サプライチェーンの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のサイバーセキュリティリスクへの曝露を管理し、適切な対応戦略、ポリシー、プロセス、及び手順を策定するための体系的なプロセスである。CSF　C-SCRM　カテゴリー　[GV.SC] 内のサブカテゴリーは、純粋にサイバーセキュリティに焦点を当てた成果と、C-SCRM　に焦点を当てた成果の繋がりを提供する。

SP 800-161r1（改訂第 1 版）「システム及び組織におけるサプライチェーンの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」は、C-SCRM に関する詳細な情報を提供している。

- 新興技術によるリスク：新たな技術や技術の新たな応用が利用可能になるにつれて、新たなリスクが明らかになる。最近の例は人工知能（AI）であり、サイバーセキュリティリスク及びプライバシーリスクだけでなく、その他多くの種類のリスクが存在する。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、これらのリスクへの対処に役立てるために策定された。AIリスクを他の企業リスク（例えば、財務、サイバーセキュリティ、評判、プライバシー）と並行して扱うことで、より統合された成果と組織の効率化をもたらす。サイバーセキュリティとプライバシーのリスクマネジメントの考慮事項とアプローチは、AIシステムの設計、開発、展開、評価、及び利用に適用できる。AI RMF コアは、機能、カテゴリー、サブカテゴリーを用いてAIの成果を説明し、AIに関連するリスクの管理に役立つ。

附属書 A. CSF コア

この附属書では、CSF コアの機能、カテゴリー、及びサブカテゴリーについて説明する。表 1 に、CSF 2.0コアの機能及びカテゴリーの名称及び一意のアルファベット識別子を示す。表中の各機能名は、附属書の該当部分にリンクされている。コアの機能、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く、組織内でリスクマネジメントの運用を担当する者が最も共感を呼ぶように意図されている。

表 1.CSF 2.0 コア機能及びカテゴリーの名称と識別子

機能	カテゴリー	カテゴリー識別子
統治（GV）	組織の状況	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、認証、アクセス制御	PR.AA
	意識向上とトレーニング	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）	継続的監視	DE.CM
	有害事象の分析	DE.AE
対応（RS）	インシデント管理	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
	インシデントの軽減	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、実装例は、CSF 2.0 Web サイト及び CSF 2.0 リファレンス・ツールから入手可能であり、ユーザーはそれらを調査し、人間及び機械が読み取り可能な形式でエクスポートすることができる。CSF 2.0 コアは、CSF 1.1 と同様のレガシー・フォーマットでも利用可能である。

統治（GV）：組織のサイバーセキュリティリスクマネジメント戦略、期待、 及びポリシーが確立され、周知され、 監視されている。

- 組織の状況（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意思決定を取り巻く状況（ミッション、ステークホルダーの期待、依存関係、法的要求事項、規制上の要件、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情報を提供している。
  - GV.OC-02: 社内外のステークホルダーが理解され、サイバーセキュリティリスクマネジメントに関する彼らのニーズと期待が理解され、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、規制上の要件、及び契約上の要求事項（プライバシー及び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：外部ステークホルダーが組織に依存または期待する重要な目的、ケイパビリティ（能力）、及びサービスが理解され、伝達されている。
  - GV.OC-05：組織が依存する成果、ケイパビリティ（能力）、サービスを理解が理解され、伝達されている。

- リスクマネジメント戦略（GV.RM）：運用リスクの意思決定を支援するために、組織の優先順位、制約条件、リスク許容度、リスク選好度の表明、及び前提条件が確立され、伝達され、使用されている。
  - GV.RM-01：リスクマネジメントの目的が確立され、組織のステークホルダーによって合意されている。
  - GV.RM-02：リスク選好度及びリスク許容度が確立され、伝達され、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及び成果が、事業体のリスクマネジメントプロセスに含まれている。
  - GV.RM-04：適切なリスク対応のオプションを表す戦略的方向性が確立され、伝達されている。
  - GV.RM-05：サプライヤ及びその他の第三者によるリスクを含む、サイバーセキュリティリスクに関する組織全体にわたるコミュニケーション系統が確立されている。
  - GV.RM-06：サイバーセキュリティリスクの計算、文書化、分類、優先順位付けのための標準化された方法が確立され、伝達されている。
  - GV.RM-07: 戦略的機会(すなわちプラスに働くリスク)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。

- 役割、責任、権限（GV.RR）：説明責任、実績アセスメント、継続的改善を促進するためのサイバーセキュリティの役割、責任、権限が確立され、伝達されている。
  - GV.RR-01：組織のリーダーシップが、サイバーセキュリティリスクに対する責任と説明責任を負い、リスクを認識し、倫理的で、継続的に改善する文化を育んでいる。
  - 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、権限が確立され、伝達され、理解され、実施されている。
  - GV.RR-03：サイバーセキュリティリスク戦略、役割、責任、ポリシーに見合った適切なリソースが割り振られている。
  - 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され、伝達され、実施されている。
  - GV.PO-01：サイバーセキュリティリスクマネジメントのポリシーが、組織の状況、サイバーセキュリティ戦略、優先順位に基づいて策定され、伝達され、実施されている。
  - GV.PO-02：サイバーセキュリティリスクマネジメントのポリシーが、要件、脅威、技術、組織のミッションの変化を反映するようレビューされ、更新され、伝達され、実施されている。

- 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活動及び実行の結果が、リスクマネジメント戦略への情報提供、改善、調整に使用されている。
  - GV.OV-01：戦略と方向性に情報を与え調整するために、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ている。
  - GV.OV-02: 組織の要件とリスクを確実にカバーするために、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、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され、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、組織のステークホルダーによって識別され、確立され、管理され、監視され、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、及びプロセスが確立され、組織のステークホルダーによって合意されている。
  - GV.SC-02：サプライヤ、顧客、パートナーに対するサイバーセキュリティの役割と責任が確立され、伝達され、社内及び社外で調整されている。
  - 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及び事業体のリスクマネジメント、リスクアセスメント、改善プロセスに統合されている。
  - GV.SC-04：サプライヤが把握され、重要度によって優先順位が付けられている。

- 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件が確立され、優先順位が付けられ、サプライヤやその他の関連する第三者との契約やその他の種類の合意に統合されている。
- GV.SC-06：サプライヤまたはその他の第三者との正式な関係を結ぶ前に、リスクを低減するための計画と適正評価が実施されている。
- GV.SC-07：サプライヤ、その製品及びサービス、並びにその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、アセスメントされ、対応され、その関係継続中に監視されている。
- GV.SC-08：関連するサプライヤ及びその他の第三者が、インシデントの計画、対応、及び復旧活動に含まれている。
- GV.SC-09：サプライチェーンのセキュリティプラクティスが、サイバーセキュリティ及び事業体のリスクマネジメントプログラムに統合され、その実行が、技術製品及びサービスのライフサイクルを通じて監視されている。
- 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、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）：組織のビジネス目的の達成を可能にする資産（例えば、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、人材）が識別され、組織の目的及びリスク戦略に対する相対的な重要性に整合して管理されている。
  - ID.AM-01：組織が管理するハードウェアのインベントリ（一覧）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、及びシステムのインベントリ（一覧）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のデータフローの描写が維持されている。
  - ID.AM-04：サプライヤが提供するサービスのインベントリ（一覧）が維持されている。
  - ID.AM-05：資産は、分類、重要度、リソース、及びミッションへのインパクトに基づいて優先順位付けされている。
  - ID.AM-07：指定されたデータタイプのデータ及び対応するメタデータのインベントリ（一覧）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、ライフサイクル全体を通じて管理されている。

- 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：資産の脆弱性が識別され、妥当性が確認され、記録されている。
- 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や情報源から入手されている。
- ID.RA-03：組織に対する内部及び外部の脅威が識別され、記録されている。
- ID.RA-04：脆弱性を悪用する脅威の潜在的インパクトと起こりやすさが識別され、記録されている。
- ID.RA-05：脅威、脆弱性、起こりやすさ、及びインパクトが、内在するリスクを理解し、リスク対応の優先順位付けに情報を提供するために使用されている。
- ID.RA-06：リスク対応が選択され、優先順位付けされ、計画され、追跡され、伝達されている。
- ID.RA-07：変更及び例外が管理され、リスクのインパクトがアセスメントされ、記録され、追跡されている。
- ID.RA-08：脆弱性開示情報を受領し、分析し、対応するプロセスが確立されている。
- ID.RA-09：ハードウェア及びソフトウェアの真正性と完全性が、取得及び使用前にアセスメントされている。
- ID.RA-10：取得前に重要なサプライヤがアセスメントされている。

- 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プロセス、手順、及び活動の改善が、すべての CSF 機能にわたって識別されている。
  - ID.IM-01：改善点が評価から識別されている。
  - ID.IM-02：サプライヤ及び関連する第三者と協力して実施されるものを含め、セキュリティテスト及び演習から改善点が識別されている。
  - ID.IM-03：運用プロセス、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対応計画及びその他のサイバーセ　キュリティ計画が策定され、伝達され、維持され、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使用されている。

- アイデンティティ管理、認証、アクセス制御（PR.AA）：物理的及び論理的資産へのアクセスが、認可されたユーザー、サービス、及びハードウェアに限定され、アセスメントされた不正アクセスのリスクに応じて管理されている。
  - PR.AA-01: 認可されたユーザー、サービス、及びハードウェアの ID 及び認証情報が、組織によって管理されている。
  - PR.AA-02:　相互作用の文脈に基づいてIDが証明され、認証情報に結びつけられている。
  - PR.AA-03：ユーザー、サービス、及びハードウェアが認証されている。
  - PR.AA-04：ID アサーションが保護され、伝達され、検証されている。

- PR.AA-05：アクセス許可、資格の付与、及び認可がポリシーで定義され、管理され、実施され、レビューされ、最小特権と職務分離の原則が組み込まれている。
- PR.AA-06：資産への物理的なアクセスが、リスクに応じて管理され、監視され、実施されている。

- 意識向上とトレーニング（PR.AT）：サイバーセキュリティ関連の職務を遂行できるように、組織の人員に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が提供されている。
  - PR.AT-01：サイバーセキュリティリスクを念頭に置いて一般的な職務を遂行するための知識とスキルを有するよう、人員に意識向上とトレーニングが提供されている。
  - PR.AT-02：サイバーセキュリティリスクを念頭に置いて関連職務を遂行するための知識とスキルを有するよう、専門的な役割を担う個人に意識向上とトレーニングが提供されている。

- 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に、組織のリスク戦略に基づいて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され、保護され、維持され、テストされている。

- プラットフォームセキュリティ（PR.PS）：物理プラットフォーム及び仮想プラットフォームのハードウェア、ソフトウェア（例えば、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、機密性、完全性、及び可用性を保護するための組織のリスク戦略に沿って管理されている。
  - PR.PS-01：構成管理のプラクティスが確立され、適用されている。
  - PR.PS-02: ソフトウェアはリスクに応じて保守され、交換され、削除されている。
  - PR.PS-03：ハードウェアはリスクに応じて保守され、交換され、削除されている。
  - PR.PS-04：ログ記録が生成され、継続的監視のために利用可能となっている。
  - PR.PS-05：認可されていないソフトウェアのインストール及び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、その実行がソフトウェア開発ライフサイクル全体を通じて監視されている。

- 技術インフラのレジリエンス（PR.IR）：セキュリティアーキテクチャが、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とともに管理されている。
  - PR.IR-01：ネットワーク及び環境が認可されていない論理アクセス及び使用から保護されている。

- PR.IR-02：組織の技術資産が環境上の脅威から保護されている。
- PR.IR-03：通常時及び困難な状況でのレジリエンス要件を達成するためのメカニズムが実装されている。
- PR.IR-04：可用性を確実にするために十分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攻撃及び侵害の可能性が発見され、分析されている。

- 継続的監視（DE.CM）：異常、侵害の痕跡、及びその他の潜在的な有害事象を発見するために、資産が監視されている。
  - DE.CM-01：潜在的な有害事象を発見するために、ネットワーク及びネットワークサービスが監視されている。
  - DE.CM-02：潜在的な有害事象を発見するために、物理的環境が監視されている。
  - DE.CM-03：潜在的な有害事象を発見するために、人員の活動及び技術の利用が監視されている。
  - DE.CM-06：潜在的な有害事象を発見するために、外部サービスプロバイダの活動及びサービスが監視されている。
  - DE.CM-09：潜在的な有害事象を発見するために、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監視されている。

- 有害事象の分析（DE.AE）：異常、侵害の痕跡、及びその他の潜在的な有害事象が、事象を特徴付け、サイバーセキュリティインシデントを検知するために分析されている。
  - DE.AE-02：関連する活動をよりよく理解するために、潜在的な有害事象が分析されている。
  - DE.AE-03：情報は複数の情報源から相互に関連付けられている
  - DE.AE-04：有害事象の推定されるインパクトと範囲が理解されている。
  - DE.AE-06：有害事象に関する情報が、認可されたスタッフ及び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その他の文脈的情報が分析に統合されている。
  - DE.AE-08：有害事象が、定義されたインシデント基準を満たす場合に、インシデントが宣言される。

対応（RS）：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が講じられている。

- インシデント管理（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ると、関連する第三者と連携してインシデント対応計画が実行されている。
  - RS.MA-02：インシデント報告がトリアージされ、妥当性が確認されている。
  - 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エスカレーションまたは昇格されている
  - RS.MA-05：インシデントの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）：効果的な対応を確実にし、フォレンジック活動及び復旧活動をサポート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何が起こったのか、及びインシデントの根本原因を特定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アクションが記録され、記録の完全性と来歴が保持されている。
  - RS.AN-07：インシデントのデータ及びメタデータが収集され、その完全性と来歴が保持されている。
  - RS.AN-08：インシデントの規模が推定され、妥当性が確認されている。

- 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、またはポリシーの要件に従って、対応活動を社内外のステークホルダーと調整する。
  - RS.CO-02：社内外のステークホルダーにインシデントを通知する。
  - RS.CO-03：指定された社内外のステークホルダーと情報を共有する。

- インシデント軽減（RS.MI）：事象の拡大防止と影響を軽減する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-02：インシデントが根絶されている。

復旧（RC）：サイバーセキュリティインシデントの影響を受けた資産及び業務を復旧させる。

- インシデント復旧計画の実行（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及びサービスの運用可用性を確実にするための復旧活動が実施されている。
  - RC.RP-01：インシデント対応計画の復旧に関する部分が、インシデント対応プロセスから取り組み

が開始されると実行されている。

- RC.RP-02：復旧活動が選択され、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：バックアップ及びその他の復旧資産の完全性が、復旧に使用する前に検証されている。
- RC.RP-04：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、インシデント後の運用規範を確立するために考慮されている。
- RC.RP-05：復旧した資産の完全性が検証され、システム及びサービスが復旧し、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了が宣言され、インシデント関連の文書の作成が完成している。

- インシデント復旧のコミュニケーション（RC.CO）：復旧活動は社内外の関係者と調整される。
  - RC.CO-03：復旧活動及び運用ケイパビリティ（能力）復旧の進捗状況が、指定された社内外のステークホルダーに伝達されている。
  - RC.CO-04：インシデント復旧に関する公開最新情報は、承認された方法及びメッセージングを使用して共有されている。

附属書 B. CSF ティア

表 2 は、第 3 章で説明した CSF ティアの概念的な実例を示している。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のプラクティス（統治）と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（識別、防御、検知、対応、復旧）の厳格さを特徴づけるものである。

表2.CSFティアの概念的な実例

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場当たり的な方法で管理されている。 優先順位付けは場当たり的で、目的又は脅威環境に正式に基づくものではない。	組織レベルでのサイバーセキュリティリスクの意識向上は限定的である。 組織は、サイバーセキュリティリスクマネジメントを、不規則に、個々の場合に応じて実装している。 サイバーセキュリティ情報を組織内で共有できるプロセスが組織にない可能性がある。 組織は一般的に、サプライヤ及び取得し使用する製品及びサービスに関連するサイバーセキュリティリスクを認識していない。
第2段階：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によって承認されるが、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及び保護ニーズの優先順位付けは、組織のリスク目的、脅威環境、又はビジネス／ミッション要件によって直接伝達される。	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見られるが、サイバーセキュリティリスクを管理するための組織全体でのアプローチは確立されていない。 組織の目的及びプログラムにおけるサイバーセキュリティの考慮は、組織のすべてのレベルではなく、一部のレベルで行われている可能性がある。組織の資産及び外部資産のサイバーリスクアセスメントは実施されているが、通常、繰り返し実施可能、又は再び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、サプライヤ及び取得し使用する製品及びサービスに関連するサイバーセキュリティリスクを意識しているが、それらのリスクに対応するための一貫した行動や正式な行動を取っていない。
ティア3：反復可能である（Repeatable）	組織のリスクマネジメントのプラクティスは正式に承認され、ポリシーとして表明されている。 リスク情報を活用したポリシー、プロセス、手順が定義され、意図した通りに実装され、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／ミッション要件、脅威、及び技術状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。	サイバーセキュリティリスクを管理するための組織全体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が、組織全体で日常的に共有されている。 リスクの変化に効果的に対応するための一貫した方法が存在している。人員は、任命された役割及び責任を果たすための知識とスキルを有している。 組織が資産のサイバーセキュリティリスクを一貫して正確に監視している。サイバーセキュリティ担当の経営幹部とその他の幹部が、サイバーセキュリティリスクに関して、定期的にコミュニケーションを行っている。経営幹部は、組織内の全業務系統を通じてサイバーセキュリティが考慮されていることを確実にしている。

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
		組織のリスク戦略は、サプライヤ及び取得し使用する製品及びサービスに関連するサイバーセキュリティリスクから情報を得ている。人員は、ベースライン要件を伝達するための書面による合意、ガバナンス構造（例えば、リスク評議会）、及びポリシーの実装と監視などの仕組みを通じて、これらのリスクに正式に対処する。これらのアクションは一貫して意図した通りに実装され、継続的に監視及びレビューされる。
ティア 4：適応している（Adaptive）	潜在的なサイバーセキュリティ事象に対処するための、リスク情報に基づいたポリシー、プロセス、及び手順を用いたサイバーセキュリティリスクを管理する組織全体のアプローチがある。サイバーセキュリティリスクと組織の目的との関係が明確に理解され、意思決定の際に考慮されている。経営幹部が、財務リスクやその他の組織リスクと同じ文脈でサイバーセキュリティリスクを監視している。組織の予算が、現在及び予測されるリスク環境とリスク許容度の理解に基づいている。 事業部門は、経営陣のビジョンを実行し、組織のリスク許容度という観点でシステムレベルのリスクを分析している。 サイバーセキュリティリスクマネジメントは組織文化の一部である。~~サイバーセキュリティリスクマネジメントは、組織文化の一部である~~。それは、これまでの活動に対する認識、及び組織のシステムとネットワークにおける活動の継続的な認識から発展している。組織は、リスクへのアプローチ方法及び伝達方法において、ビジネス／ミッションの目的の変更を迅速かつ効果的に説明することができる。	組織は、過去及び現在のサイバーセキュリティ活動（そこから得られた教訓及びや予測指標を含む）に基づいて、サイバーセキュリティのプラクティスを適応させている。 高度なサイバーセキュリティ技術及びプラクティスを取り入れた継続的改善プロセスを通じて、組織は変化する技術状況に積極的に適応し、進化する高度な脅威に対してタイムリーかつ効果的な方法で対応している。 組織は、リアルタイム又はリアルタイムに近い情報を使用して、サプライヤ及び取得し使用する製品及びサービスに関連するサイバーセキュリティリスクを理解し、一貫してそれに対応している。 サイバーセキュリティ情報は、組織全体及び認可された第三者と常に共有されている。

附属書 C. 用語集

CSF 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の成果。

CSF コミュニティプロファイル
多くの組織間で共通の利害や目標に対処するために作成され公表されるCSF の成果のベースライン。コミュニティプロファイルは通常、特定の分野、下位分野、技術、脅威の種類、又はその他のユースケースのために策定される。組織は、コミュニティプロファイルを独自の目標プロファイルの基礎として使用することができる。

CSF コア
あらゆる組織のサイバーセキュリティリスクマネジメントに役立つ、ハイレベルなサイバーセキュリティ成果の分類法。そのコンポーネントは、各成果の詳細を示す機能、カテゴリー、サブカテゴリーの階層である。

CSF 現在のプロファイル
組織プロファイルの一部で、組織が現在達成している（又は達成しようとしている）コアの成果を詳述し、各成果がどのように、又はどの程度達成されているかを特徴付ける。

CSF 機能
サイバーセキュリティの成果に関する最高レベルの組織。CSF には、統治、識別、防御、検知、対応、回復の6つの機能がある。

CSF 実装例
CSF　コアの成果の達成を支援するための、簡潔でアクション指向の概念的な実例。

CSF 参考情報
CSF　コアの成果、及び既存の標準、ガイドライン、規制、又はその他の内容との関係を示すマッピング。

CSF 組織プロファイル
組織の現在のサイバーセキュリティ態勢、及び／又はまたは目標とするサイバーセキュリティ態勢を、CSF コアの成果の観点から説明するための仕組み。

CSF クイックスタートガイド
CSFに関連する特定のトピックについて、簡潔ですぐに使用可能なガイダンスを提供する補足資料。

CSF サブカテゴリー
CSF　カテゴリーを構成する技術的及び管理的なサイバーセキュリティ活動の、より具体的な成果のグループ。

CSF 目標プロファイル
組織プロファイルの一部であり、組織が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、優先順位をつけた望ましいコアの成果を詳述する。

CSF ティア
組織のサイバーセキュリティリスクガバナンスとマネジメントのプラクティスの厳格さの特性化。部分的である（ティア 1）、リスク情報が活用されている（ティア 2）、反復可能である（ティア 3）、適応的である（ティア 4）の4つのティアがある。

本書では、実験手順を適切に特定するために、商用、非商用を問わず、特定の商用機器、装置、ソフトウェア、または材料を識別している。このような識別は、NISTによるいかなる製品又はサービスの推奨または保証を意味するものではなく、又、識別した材料又は機器が必ずしもその目的にとって最良のものであることを意味するものでもない。

NIST 技術シリーズのポリシー

Copyright, Use, and Licensing Statements

NIST Technical Series Publication Identifier Syntax

米国国立標準技術研究所発行の本書の引用方法：

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 jpn.
https://doi.org/10.6028/NIST.CSWP.29.jpn

連絡先情報
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

すべてのコメントは情報公開法（FOIA）に基づき公開される。