重要インフラのサイバーセキュリティを向上させるためのフレームワーク

1.0 版

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

2014 年 2 月 12 日

目次

図

表

エグゼクティブサマリー

アメリカ合衆国（以下、米国）の国家安全保障と経済安全保障は、重要インフラが確実に機能することに依存している。サイバーセキュリティ上の脅威は、重要インフラシステムがより複雑になり、他システムとの接続も増えていることを巧みに利用して、国家の安全保障、経済、そして市民の安全と健康を危険に晒している。金銭的リスクや評判に関わるリスクと同様に、サイバーセキュリティを脅かすリスク（以下、サイバーセキュリティリスク）は企業の損益に影響を与える。たとえば、コストを跳ね上がらせたり、収益を圧迫したりする。また、企業を革新し、顧客を獲得・維持する能力に悪影響を及ぼすこともある。

このようなリスクへの対処を強化するために、大統領は 2013 年 2 月 12 日に Executive Order（以下、大統領令）第 13636 号「Improving Critical Infrastructure Cybersecurity（重要インフラのサイバーセキュリティの向上）」を発布した。この大統領令は、「米国の重要インフラのセキュリティとレジリエンスを高め、安全、セキュリティ、企業機密、プライバシー、および市民の自由を守ると同時に効率性、イノベーション、および経済繁栄を促進するサイバー環境を維持するための我が国のポリシーである」と規定している。本ポリシーを実施するにあたって、大統領令は、企業におけるサイバーセキュリティリスクの管理を支援するための、業界標準およびベストプラクティスをまとめた自主参加型の、リスクベース・アプローチに基づく「サイバーセキュリティフレームワーク（以下、本フレームワーク）」を策定することを要求している。政府と民間部門との連携により策定された本フレームワークは、企業に新たな規制を課すことなく、ビジネスニーズに基づいてコスト効率よくサイバーセキュリティリスクに対処し、そうしたリスクを管理するための「共通言語」を記している。

本フレームワークは、サイバーセキュリティへの取組を企業にとってのビジネス上のモチベーションにつながるものにすることと、サイバーセキュリティリスクを企業のリスク管理プロセスの一環としてとらえることに重きを置いている。本フレームワークは、以下の 3 つの要素で構成されている：フレームワークコア(Framework Core)、フレームワークプロファイル(Framework Profile)、およびフレームワークインプレメンテーションティア(Framework Implementation Tier)。フレームワークコアは、すべての重要インフラ分野に共通となるサイバーセキュリティ対策のベストプラクティス、期待される成果、参考情報をまとめており、企業が各々のプロファイルを作成するにあたっての詳細なガイダンスを提供している。プロファイルは、プロファイルを作成・活用することで、企業におけるサイバーセキュリティ対策やビジネス要件、リスク許容度、割当可能なリソースのバランスを鑑みるのに役立つ。フレームワークインプレメンテーションティアは、サイバーセキュリティリスクを管理する上で、自組織のアプローチの特徴を確認し、理解するための仕組みを提供する。

また、大統領令では、本フレームワークに対して、重要インフラに携わる企業がサイバーセキュリティ対策を行うにあたって、個人のプライバシーと市民の自由を保護するための方法論を示すよう定めている。プロセスや既存のニーズは企業によって異なるだろうが、本フレームワ

ークは、企業がプライバシーと市民の自由を包括的なサイバーセキュリティプログラムの一環として組み入れるのを支援する。

本フレームワークは、企業の規模、サイバーセキュリティリスクの程度、またはサイバーセキュリティの複雑さに関わらず、重要インフラのセキュリティとレジリエンスを向上させるためのリスク管理原則およびベストプラクティスを企業が適用できるようにする。本フレームワークは、現在、産業界で効力を発揮している標準、ガイドライン、およびベストプラクティスを集約することで、現在ある多様なサイバーセキュリティアプローチを体系化・構造化し、企業に示している。さらに、本フレームワークは、世界的に認められているサイバーセキュリティ標準をベースにしているため、米国外に所在する企業が利用することも可能であり、重要インフラのサイバーセキュリティを強化するための国際協力モデルとしても役立てることができる。

本フレームワークは 、重要インフラに対するサイバーセキュリティリスクを管理するための、万能サイズ的（どの規模の企業にも適用可能）なアプローチではない。各企業には、異なる脅威、異なる脆弱性、異なるリスク許容度に基づくそれぞれ特有のリスクがあり、本フレームワークが示す対策をどのように導入するかも多岐に渡る。企業は、重要サービスを提供する上で必要な対策を特定し、優先順位を決めて投資することで、それぞれの投資の効果を最大限に引き出すことができる。本フレームワークでは、最終的に、サイバーセキュリティリスクを低減すること、およびより適切に管理することを目標としている。

本フレームワークは、現時点でのものであり、実施に関する産業界からのフィードバックに基づいて更新・改良されていく。また、本フレームワークが利用されるにつれて得られる教訓は、将来のバージョンに反映される。これにより、新たな脅威やリスク、解決策が次々に浮上するダイナミックで課題の多い環境に身を置く重要インフラ事業者や運用者のニーズを満たすことができる。

個々の企業にガイダンスを提供し、米国の重要インフラのサイバーセキュリティ意識を総じて向上させる、こうした自主参加型のフレームワークの活用は、米国の重要インフラのサイバーセキュリティを向上させるための新たなステップとなる。

1.0　本フレームワークの紹介

米国の国家安全保障と経済安全保障は、重要インフラが確実に機能することに依存している。重要インフラのレジリエンスを高めるために、オバマ大統領は 2013 年 2 月 12 日に大統領令第 13636 号「Improving Critical Infrastructure Cybersecurity（重要インフラのサイバーセキュリティの向上）」を発布した。[1] 大統領令は、重要インフラサービスの提供に直接関わるプロセス、情報、システムに対するサイバーセキュリティリスクの管理を可能にする、「優先順位付けができ、柔軟性があり、繰り返し適用することが可能で、成果ベースの、費用対効果の高いアプローチ」を実現する、自主参加型のフレームワークの策定を指示している。産業界との連携により策定された本フレームワークは、サイバーセキュリティリスクの管理にあたってのガイダンスを提供する。

大統領令では、重要インフラを「物理的存在か、仮想的存在かに関わらず、米国にとって必要不可欠なシステムや資産で、これらのシステムや資産が利用不能な状態になったり、破壊された場合、米国の国家安全保障、経済安全保障、国民の健康や安全、またはこれらの問題のうち複数、あるいはすべてに悪影響を与える可能性があるもの」と定義している。外部からの脅威と内部からの脅威の両方が増大する中、重要インフラに責任を担う企業は、サイバーセキュリティリスクを特定、アセスメントし、管理するための、一貫性のある繰り返し適用可能なアプローチを必要とする。こうしたアプローチが、企業の規模、晒されている脅威、または今日のサイバーセキュリティの複雑さに関わらず必要である。

重要インフラコミュニティには、公共および民間の事業者や運用者（以下、事業者）、および国のインフラの安全性を守る役割を担う、その他の関係者が含まれる。各重要インフラ分野の事業者は、情報技術（IT）および産業用制御システム（ICS）によって支えられ、各々の役割を果たしている。[2] IT／ICS の技術と、それらが提供する通信機能や相互接続性への依存は、重要インフラ事業における潜在的な脆弱性を変化・拡大させ、運用上の潜在的リスクを増大させた。例えば、ICS や ICS によって生成されたデータが、重要インフラサービスの提供やビジネス上の意志決定に活用されるようになるにつれ、サイバーセキュリティインシデントが企業の業務資産、従業員の健康と安全、そして環境に与える潜在的な影響を考慮することが必要となっている。サイバーセキュリティリスクを管理するためには、リスク管理を行うビジネス上のモチベーション、その企業における IT／ICS の使い方に即したセキュリティ上の考慮事項を明確に理解することが必須となる。個々の企業によって IT／ICS の使い方も、リスクも固有であるため、本フレームワークが記述する成果の達成に使用されるツールや手法も変わってくる。

プライバシーと市民の自由の保護が国民の信頼を得るのに果たす役割を認識した上で、大統領令では本フレームワークに対して、重要インフラに携わる企業がサイバーセキュリティ対策を行うにあたって、個人のプライバシーと市民の自由を保護するための方法論を示すよう定めている。多くの企業には、既にプライバシーと市民の自由の保護のためのプロセスが存在する。

---

[1] 大統領令第 13636 号, *Improving Critical Infrastructure Cybersecurity*, DCPD-201300091, 2013 年 2 月 12 日。http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[2] DHS Critical Infrastructure プログラムは、重要インフラの各業界と、それらの業界が果たす重要な役割とバリューチェーン（価値連鎖）の一覧を記している。http://www.dhs.gov/critical-infrastructure-sectors

本フレームワークが示す方法論は、既存のプロセスを補完し、企業のサイバーセキュリティリスク管理アプローチと整合性の取れたプライバシーリスク管理を容易にするためのガイダンスを提供するものである。プライバシーとサイバーセキュリティの統合は、顧客の信頼を向上させ、より標準化された情報共有を可能にし、また、様々な法体制に跨る重要インフラの運用を容易にすることを通じて、企業に利をもたらしてくれる。

拡張性を確保し、技術革新を可能にするため、本フレームワークは技術的に中立なものとなっている。本フレームワークは、重要インフラ事業者によるレジリエンスの実現を可能にするための、様々な既存の標準、ガイドライン、ベストプラクティスを拠り所にしている。このような、産業界によって作成・運用・更新されてきたグローバルな標準、ガイドライン、ベストプラクティスを拠り所にすることにより、本フレームワークが示す成果の達成に使用されるツールや手法は、国境を超え、サイバーセキュリティリスクのグローバルな性質を反映し、技術の進歩やビジネス要件と共に発展すると思われる。既存の標準や新たな標準の活用は、規模の経済（スケールメリット）を可能にし、市場のニーズに合った効果的な製品、サービス、ベストプラクティスの開発を推進する。また、利害関係者を通じて、市場競争がそうして生まれた技術やベストプラクティスのより迅速な普及、および多くのメリットの実現を促進する。

本フレームワークはそうした標準、ガイドライン、ベストプラクティスを基に作り上げられ、企業が以下を実施するための一般的な分類法および手法を提供している。:

1) 現行のサイバーセキュリティへの取組を書き出す;
2) 目標とするサイバーセキュリティ対策の実施状態を書き出す;
3) 継続的かつ繰り返し実施可能なプロセスを通じ、サイバーセキュリティ改善の機会を見つけ、実行にあたっての優先順位付けを行う;
4) 目標達成までの進捗を評価する;
5) 社内外の利害関係者とサイバーセキュリティリスクについて情報交換を行う。

本フレームワークは、企業のリスク管理プロセスおよびサイバーセキュリティプログラムを補完するものであり、取って代わるものではない。企業は現在のプロセスを利用しつつ、本フレームワークを活用し、業界のベストプラクティスを考慮しながらサイバーセキュリティリスクの管理の強化および関係者間の意志疎通を図ることができる。また、サイバーセキュリティプログラムを持たない企業は、本フレームワークを参考にしてプログラムを立ち上げることができる。

本フレームワークが特定の業界に特化していないように、本フレームワークが示す標準、ガイドライン、ベストプラクティスの一般的な分類法も特定の国に特化したものではない。米国外に所在する企業でも自社のサイバーセキュリティ対策の強化に本フレームワークを利用することが可能であるほか、本フレームワークは重要インフラのサイバーセキュリティに関する国際協力にあたっての共通言語の確立にも寄与できる。

1.1　フレームワークの概要

本フレームワークはサイバーセキュリティリスクを管理するためのリスクベース・アプローチであり、以下の 3 つの要素で構成されている：フレームワークコア、フレームワークインプレメンテーションティア、およびフレームワークプロファイル。各要素は、サイバーセキュリティへの取組

とビジネス上のモチベーションの結び付きを強くするものである。これらの要素の詳細を以下に記す。

- フレームワークコア（以下、コア）は、すべての重要インフラ分野に共通となるサイバーセキュリティ対策のベストプラクティス、期待される成果、適用可能な参考情報をまとめたものである。コアは業界標準、ガイドライン、ベストプラクティスを集約して、サイバーセキュリティ対策と期待される成果について、経営レベルから実施／運用レベルまで、企業全体で共有できる形で示す。コアは、同時的・連続的に実行される 5 つの機能 ― 「特定（Identify）」、「防御（Protect）」、「検知（Detect）」、「対応（Respond）」、「復旧（Recover）」で構成される。これらの機能をまとめて考慮することによって、企業のサイバーセキュリティリスク管理ライフサイクルを、ハイレベルで、戦略的にとらえることが可能になる。コアは次にこれらの各機能の内容を鍵となるカテゴリー、サブカテゴリーに細分化して、各サブカテゴリーの実装の参考となる既存の標準、ガイドライン、ベストプラクティスを参考情報に例示し、対応付けている。
- フレームワークインプレメンテーションティア（以下、ティア）は、企業がサイバーセキュリティリスクをどのようにとらえているか、また、そうしたリスクを管理するためにどのようなプロセスを実施しているかを示す。ティアは企業のサイバーセキュリティリスク管理対策が、本フレームワークで定義されている特性（例：リスクおよび脅威に対する意識が高い、繰り返し適用可能である、適応している）をどの程度まで達成できているかも示す。ティアはその企業の取組がティア 1（「部分的である」）からティア 4（「適応している」）までのいずれの段階にあるかを示す。これらのティアは、特に手順化されていない場当たりな事後的対応から、迅速でリスク情報を活用したアプローチまでの進展を反映している。ティアの選定プロセスにおいて、企業は現行のリスク管理対策、脅威環境、法規制上の要求事項、事業目的／ミッション、自組織に課せられている制約を考慮する必要がある。
- フレームワークプロファイル（以下、プロファイル）は、本フレームワークのカテゴリーおよびサブカテゴリーから企業が選択した、ビジネスニーズを基にした期待される成果（セキュリティ対策の実施状態）を表している。プロファイルは、コアが示す標準、ガイドライン、ベストプラクティスを、特定の実施シナリオ（企業のセキュリティ対策実施方針）に合わせて整理したものと言える。プロファイルはまた、「現在の」プロファイル（「今の」状態）」と「目標」プロファイル（「目指す」状態）」を比較することにより、サイバーセキュリティ対策を向上させる機会を見つけるために使用できる。プロファイルを策定するにあたって、企業はコアのすべてのカテゴリーとサブカテゴリーを見直して、ビジネス上のモチベーションとリスクアセスメント結果を基にして最も対策が必要なリスクを決定することができる。また、企業のリスクに対処するために、必要に応じてカテゴリーとサブカテゴリーを追加することができる。これにより企業は「現在のプロファイル」を使用して、費用対効果やイノベーションを含むその他のビジネスニーズを考慮した上で、「目標のプロファイル」へ向けての対策の優先順位付けと進捗の測定を行うことができる。また、プロファイルを使用すれば、自己アセスメントを実施して、企業内または企業間で結果を共有することが可能になる。

1.2　リスク管理とサイバーセキュリティフレームワーク

リスク管理はリスクの特定、アセスメント、対処を繰り返すプロセスである。リスクを管理するために、企業はセキュリティ上の「イベント」が発生する可能性と、その結果としてもたらされる影響を把握する必要がある。この情報により、企業は提供するサービスに関して許容できるリスクレベルを決定し、リスク許容度として表すことができる。

リスク許容度を把握できれば、サイバーセキュリティ対策の優先順位付けが可能になり、サイバーセキュリティへの投資について十分な情報を得た上での決断が可能になる。リスク管理プログラムの実施は、企業がサイバーセキュリティプログラムを定量化し、どのような調整を行ったかについて伝達できるようにする。企業には、重要サービスの提供にもたらされる影響に基づいてリスクを低減するか、リスクを移転するか、リスクを回避するか、あるいはリスクを受け入れるかなど、リスクの対処に関して多様な選択肢が与えられている。

本フレームワークはリスク管理プロセスを通じて、企業がサイバーセキュリティに関する決定事項を伝達し、優先順位付けを行えるようにする。本フレームワークは期待される成果を得るためのサイバーセキュリティ対策を企業が選択できるよう、繰り返し適用可能なリスクアセスメントと、ビジネス上のモチベーションの確立をサポートしている。したがって、本フレームワークは IT／ICS 環境に対するサイバーセキュリティリスク管理アプローチを動的に選択し、改善する能力を企業に与える。

本フレームワークは柔軟性のある、リスクに基づいた実施が可能なため、広範囲のサイバーセキュリティリスク管理プロセスに使用できる。サイバーセキュリティリスク管理プロセスには、たとえば国際標準化機構（ISO）31000:2009[3]、ISO/IEC 27005:2011[4] 、NIST Special Publication 800-39[5]、*Electricity Subsector Cybersecurity Risk Management Process* (RMP)ガイドライン [6]がある。

1.3　本文書の概要

本文書は以降、以下のセクションと付録で構成されている:

- セクション 2 は、本フレームワークの以下の 3 要素について説明する:コア、ティア、プロファイル。
- セクション 3 は、本フレームワークの使い方の例を示す。

---

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

[4] 国際標準化機構／国際電気標準会議, *Information technology – Security techniques – Information security risk management*, ISO/IEC 27005:2011, 2011 年。http://www.iso.org/iso/catalogue_detail?csnumber=56742

[5] Joint Task Force Transformation Initiative, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication 800-39, 2011 年 3 月。 http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

[6] 米エネルギー省, *Electricity Subsector Cybersecurity Risk Management Process*, DOE/OE-0003, 2012 年 5 月。 http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

- 付録 A は、コアについて以下の項目を表で示す：機能、カテゴリー、サブカテゴリー、参考情報。
- 付録 B は、一部の用語の定義を示す。
- 付録 C は、本文書で使用されている略語の定義を示す。

2.0　本フレームワークの基本的な考え方

本フレームワークは内外のサイバーセキュリティリスクを把握・管理し、表現するための共通言語を提供する。本フレームワークはサイバーセキュリティリスクを低減するためのアクションの特定と優先順位付けに使用できるものであり、また、そうしたリスクを管理できるようポリシー、ビジネスアプローチ、技術的アプローチを調整するためのツールでもある。本フレームワークは関連する企業全体にわたってのサイバーセキュリティリスクを管理するために使用することもできれば、企業内の重要サービスの提供に焦点を絞ることもできる。また、業界をまとめる役割を担う業界団体、協会、企業などの異なるタイプの組織が「共通のプロファイル」を作成する場合など、本フレームワークはさまざまな目的に使用することができる。

2.1　フレームワークコア

コアはサイバーセキュリティ成果を達成するための対策と、それらの成果の達成のための参考情報をまとめたものである。コアは実施すべき対策のチェックリストではない。コアはサイバーセキュリティリスクを管理する上で役に立つことが産業界によって認められた、サイバーセキュリティの主な成果について述べる。コアは**図1**で示されるように、以下の 4 つの要素で構成されている：機能、カテゴリー、サブカテゴリー、参考情報。

図 1: フレームワークコアの構造

コアの各要素は、以下のように連携する：

- **機能**は、基本的なサイバーセキュリティ対策の最も上位を構成する要素である。ここでいう機能とは、「特定」、「防御」、「検知」、「対応」、「復旧」である。これらの機能は情報を整理し、リスク管理上の意思決定を可能にし、脅威に対処し、過去の対策から学んだ教訓を基に改善を行うことにより、企業がサイバーセキュリティリスクをどう管理しているか表現するのに役立つ。また、これらの機能はインシデント管理のための既存の手法と紐付け、サイバーセキュリティへの投資効果を示すのに役立てることができる。たとえば、計画および実施への投資はタイムリーな対応と復旧活動を支援するため、結果としてサービスの提供に対する影響も軽減される。

- **カテゴリー** は、機能をサイバーセキュリティ成果グループ別に細分化したものであり計画に基づいたニーズや特定の対策と密接に結びついている。カテゴリーには、たとえば「資産管理」、「アクセス制御」、「検知プロセス」などがある。
- **サブカテゴリー**は、カテゴリーを技術的な対策や管理面での対策がもたらす成果別に詳細化したものである。サブカテゴリーは、包括的なものではないが、所属するカテゴリーの成果の達成に必要な、個々の成果をまとめたものである。サブカテゴリーには、たとえば「外部情報システムの一覧を作成している」、「保存されているデータを保護している」、「検知システムからの通知を調査している」などがある。
- **参考情報**は、すべての重要インフラ分野に共通となる標準、ガイドライン、ベストプラクティスをまとめたセクションであり、各サブカテゴリーについて期待される成果を達成するための方法を示す。コアが記す参考情報は、あくまでも例を示すためのものであり、包括的ではない。参考情報は本フレームワークを構築するプロセスにおいて最も頻繁に参照される、重要インフラ分野を跨いだガイダンスをベースにしている。[7]

コアを構成する 5 つの機能の定義を以下に示す。これらの機能は連続した工程を形成することや、静的な、期待される最終状態へと導くことを意図しているわけではない。むしろ、これらの機能は動的なサイバーセキュリティリスクに対処できる運用文化の形成を目的として、同時的・連続的に実行することができる。コアの完全な一覧表に関しては、付録 A を参照のこと。

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

  「特定」機能における対策は、本フレームワークを効果的に使用する上で基本となる。企業はビジネスを取り巻く状況、重要な事業をサポートするリソース、および関連するサイバーセキュリティリスクを理解することで、自組織のリスク管理戦略とビジネスニーズに適合するように取り組みの対象を絞って、優先順位付けを行うことが可能になる。「特定」機能の成果カテゴリーには、たとえば以下がある：資産管理; ビジネス環境; ガバナンス、リスクアセスメント; リスク管理戦略。

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

  「防御」機能は、発生する可能性のあるサイバーセキュリティイベントがもたらす影響を抑えるのを支援する。「防御」機能の成果カテゴリーには、たとえば以下がある：アクセス制御; 意識向上およびトレーニング; データセキュリティ; 情報を保護するためのプロセスおよび手順; 保守; 保護技術。

- **検知** – サイバーセキュリティイベントの発生を検知するための適切な対策を検討し、実施する。

---

[7] NIST は情報依頼書に記載されている情報、サイバーセキュリティフレームワーク研究会、本フレームワークの策定プロセスに関与した利害関係者から得られた参考情報の一覧表を作成した。この一覧表には導入を支援する標準、ガイドライン、ベストプラクティスも含まれている。この一覧表は包括的なものとなることを意図しているわけではなく、むしろ利害関係者からの情報をベースにした出発点となることを意図している。この一覧表と補足資料に関しては、以下のウェブサイトを参照のこと：http://www.nist.gov/cyberframework/

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

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

  「対応」機能は、発生する可能性のあるサイバーセキュリティイベントがもたらす影響を封じ込めるのを支援する。「対応」機能の成果カテゴリーには、たとえば以下がある: 対応計画の作成; 伝達; 分析; 低減; 改善。

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

  「復旧」機能は、サイバーセキュリティイベントがもたらす影響を軽減するための、通常の運用状態へのタイムリーな復旧を支援する。「復旧」機能の成果カテゴリーには、たとえば以下がある: 復旧計画の作成; 改善; 伝達。

2.2　フレームワークインプレメンテーションティア

ティアは、企業がサイバーセキュリティリスクをどのようにとらえているか、また、そうしたリスクを管理するためにどのようなプロセスを実施しているかを示す。ティアには、ティア 1(「部分的である」)からティア 4(「適応している」)までの段階があり、それぞれの段階はサイバーセキュリティリスク管理対策がどの程度厳密で、高度なものか、そしてサイバーセキュリティリスク管理がビジネスニーズにどの程度基づいていて、企業の全体的なリスク管理対策にどの程度組み入れられているかを、段階的に表している。リスク管理において考慮すべき事項は、企業によるサイバーセキュリティリスクの管理やリスクの対処に、プライバシーと市民の自由に関する考慮事項がどの程度組み入れられているかなどの、サイバーセキュリティの幅広い側面を含む。

ティアの選択プロセスでは、企業の現行のリスク管理対策、脅威環境、法規制上の要求事項、事業目的／ミッション、企業に課せられている制約を考慮する。企業は、適切なティア、すなわち自組織の目標に見合うレベルであり、実施可能で、かつ重要な資産とリソースに対するサイバーセキュリティのリスクを企業の許容レベルまで低減できるティアを選択する必要がある。企業は、適切なティアを選択するにあたって、連邦政府の各部局、情報共有分析センター(ISAC)、既存の成熟度モデルなどから得られるガイダンスの活用を検討すべきである。

ティア 1(「部分的である」)にあたる企業は、ティア 2 以上を目指すことが推奨されるが、だからといってティアが成熟度を表しているわけではない。より高位のティアに進むことが推奨されるのは、それによってサイバーセキュリティリスクが低減され、費用効率も高くなる場合である。本フレームワークの導入の成否は、ティアの選択に左右されるわけではなく、当該企業が「目標のプロファイル」に定めた成果を達成できるかどうかによって決まる。

以下に、ティアの定義を示す:

ティア 1: 部分的である（Partial）

- リスク管理プロセス –企業のサイバーセキュリティリスク管理対策は確立されておらず、リスクは場当たり的に、場合によっては事後に対処される。サイバーセキュリティ対策の優先順位付けは、企業のリスク目標、脅威環境、またはビジネス／ミッション要件に基づいていない。
- 統合されたリスク管理プログラム – 組織レベルでのサイバーセキュリティリスク意識が不足していて、サイバーセキュリティリスクを管理するための組織全体にわたる取組は確立されていない。企業は外部情報源から得たさまざまな経験や情報に基づいてサイバーセキュリティリスクを管理しているため、管理は不規則であり、かつケースバイケースで実施されている。企業はサイバーセキュリティ情報を企業内で共有するためのプロセスを持っていない場合がある。
- 外部からの参加 – 企業は外部関係者と協調または協力し合うためのプロセスを持っていない場合がある。

ティア 2: リスク情報を活用している（Risk Informed）

- リスク管理プロセス – リスク管理対策は経営層によって承認されているが、企業全体にわたるポリシーとして確立されていない場合がある。サイバーセキュリティ対策の優先順位付けは、企業のリスク目標、脅威環境、またはビジネス／ミッション要件に基づいている。
- 統合されたリスク管理プログラム – 組織レベルでのサイバーセキュリティリスク意識はあるが、サイバーセキュリティリスクを管理するための組織全体にわたる取組は確立されていない。リスク情報を活用した、経営層によって承認されたプロセスおよび手順が定義され、実施されており、従業員にはサイバーセキュリティ上の役割を果たす上で十分なリソースが割り当てられている。サイバーセキュリティ情報は非形式的に企業内で共有されている。
- 外部からの参加 – 企業は、より大きなエコシステムにおける自組織の役割を理解しているが、外部と情報をやりとりしたり、共有する能力は確立していない。

ティア 3: 繰り返し適用可能である（Repeatable）

- リスク管理プロセス – 企業のリスク管理対策は正式に承認され、ポリシーとして述べられている。企業のサイバーセキュリティ対策は、ビジネス／ミッション要件の変化と、脅威およびテクノロジー状況の変化に対応するためのリスク管理プロセスの適用に基づいて、定期的に更新されている。
- 統合されたリスク管理プログラム – サイバーセキュリティリスクを管理するための企業全体にわたる取組が確立されている。リスク情報を活用したポリシー、プロセス、および手順が定義され、意図した通りに実施され、レビューされている。リスクの変化に効果的に対処するための一貫性のある手法が用意されている。職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有する。

- 外部からの参加 – 企業は自組織の依存関係とパートナーを把握しており、それらのパートナーから情報を得ている。このため、イベント発生時に彼らと協力して、リスク情報を活用した管理判断を行える状態にある。

ティア 4: 適応している（Adaptive）

- リスク管理プロセス – 企業は過去と現在のサイバーセキュリティ対策から学んだ教訓と、それらの対策から得た兆候を基に、サイバーセキュリティ対策を調整する。企業は最新のサイバーセキュリティ技術および対策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状況に進んで順応し、進化／高度化する脅威にタイムリーに対応する。
- 統合されたリスク管理プログラム – 発生する可能性のあるサイバーセキュリティイベントに対処するためのリスク情報を活用したポリシー、プロセス、手順を用いた、サイバーセキュリティリスクを管理するための企業全体にわたる取組が確立されている。サイバーセキュリティリスクの管理は組織文化の一部となっていて、以前の対策から得た教訓、他の関係者との間で共有されている情報、企業のシステムとネットワーク上の活動を継続的にモニタリングした結果に基づいて進化する。
- 外部からの参加 – 企業はサイバーセキュリティイベントが発生する前に、サイバーセキュリティを向上させるために、正確で最新の情報が配布され、活用されることを目的として、リスクを管理し、パートナーとの情報共有を積極的に行う。

2.3　フレームワークプロファイル

プロファイルは、企業のビジネス要件、リスク許容度、割当可能なリソースに基づいて調整された機能、カテゴリー、サブカテゴリーをまとめたものである。プロファイルは、法規制上の要求事項と業界のベストプラクティスを考慮して作成され、リスク管理上の優先事項を反映することを可能にし、企業の目標のみならず、業界の目標も踏まえた、サイバーセキュリティリスクを低減するためのロードマップの確立を可能にする。 最近は複雑な組織体系の企業が多いことから、特定の事業部門に合わせて調整された、個々のニーズを反映する複数のプロファイルを企業が用意することも考えられる。

プロファイルは、サイバーセキュリティ対策の現在の状態と目指す目標の状態を記述するのに使用できる。「現在のプロファイル」は、現時点で達成されているサイバーセキュリティ成果を示す。「目標のプロファイル」は、サイバーセキュリティリスク管理上の目指す目標を達成するのに必要な成果を示す。プロファイルは ビジネス／ミッション要件を踏まえ企業内および企業間でのリスクについての伝達を支援する。本フレームワークでは、実施に関して柔軟性を持たせることを意図して、プロファイルのひな形は規定しない。

プロファイルの比較（例：「現在のプロファイル」と「目標のプロファイル」との比較）は、サイバーセキュリティリスク管理上の目標を果たすために対処が必要なギャップを浮き彫りにする。これらのギャップを埋めるための行動計画は、上述のロードマップの作成に役立つ。ギャップを埋める作業の優先順位付けは、企業のビジネスニーズとリスク管理プロセスから導出される。このリスクベース・アプローチは、企業がサイバーセキュリティ目標をコスト効率よく、かつ優先順位けがなされる形で達成するために必要なリソース（例：人員、資金）の割出しを可能にする。

2.4　フレームワークインプレメンテーションの調整

図 2 は企業内の以下の各レベルにおける情報と意思決定の一般的な流れを示している:

- 経営レベル
- ビジネス／プロセスレベル
- 実施／運用レベル

経営レベルはビジネス／プロセスレベルに対してミッションの優先順位、割当可能なリソース、および全体的なリスク許容度を伝達する。ビジネス／プロセスレベルはこの情報をリスク管理プロセスへの入力情報として使用して、実施／運用レベルと連携してビジネスニーズを伝達し、プロファイルを作成する。実施／運用レベルはビジネス／プロセスレベルに対してプロファイルの実施の進捗状況を伝達する。ビジネス／プロセスレベルはこの情報を使用して影響のアセスメントを実施する。ビジネス／プロセスレベルの管理者は経営レベルに対して影響のアセスメント結果を報告し、企業の全体的なリスク管理プロセスに情報を報告する一方で、実施／運用レベルに対してビジネスに対する影響を伝達する。

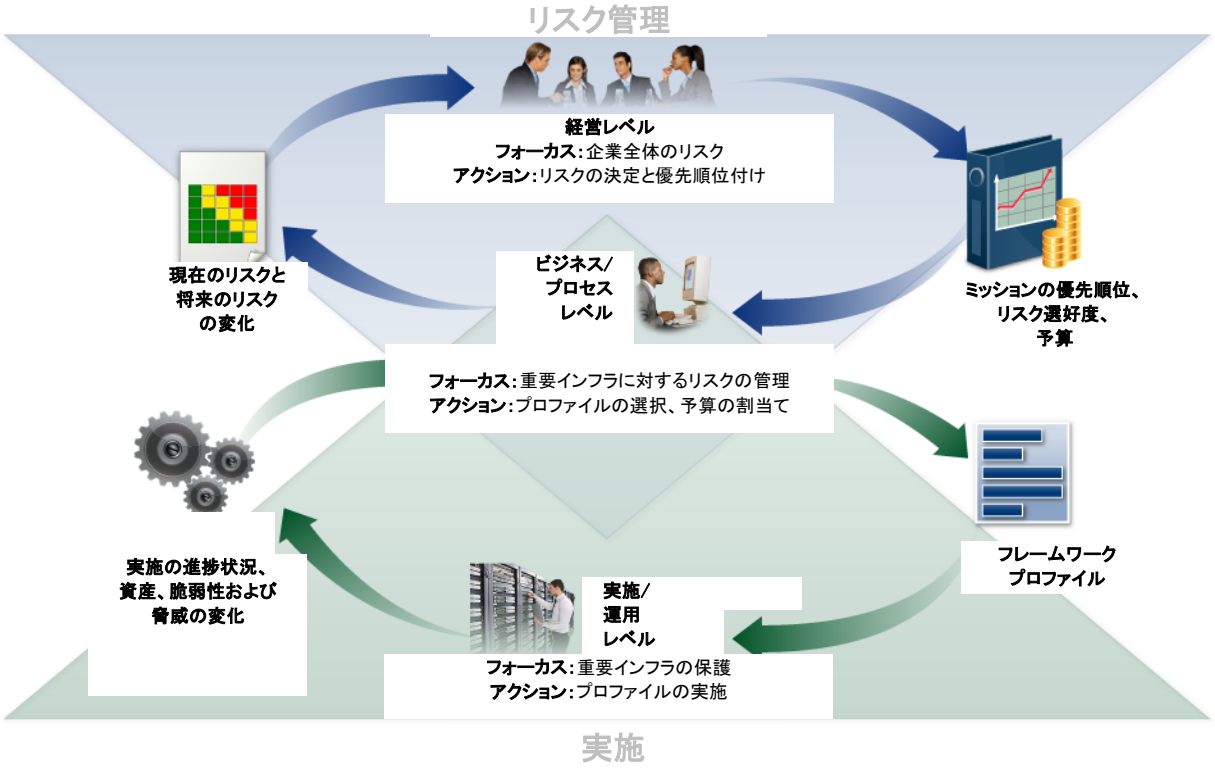

図 2: 企業内の情報と意思決定の流れ(概念図)

3.0　本フレームワークの使い方

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

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

以下のセクションでは、企業が本フレームワークをどのように使用できるかといった観点から、様々な使途を示す。

3.1　サイバーセキュリティ対策の簡単なレビュー

本フレームワークは、コアに記述されているサイバーセキュリティ対策と、現行のサイバーセキュリティ対策を比較するために使用できる。「現在のプロファイル」を作成することで、企業は「特定」、「防御」、「検知」、「対応」、「復旧」の 5 つのハイレベルの機能の観点から、コアのカテゴリーおよびサブカテゴリーに記述されている成果が、どの程度達成されているかを検証できる。企業が既知のリスクに見合うサイバーセキュリティの管理を実施していて、期待される成果を既に達成している場合がある。反対に、改善の余地がある（または改善が必要である）と企業が判断する場合がある。企業は既存のサイバーセキュリティ対策を強化し、サイバーセキュリティリスクを低減するための行動計画を作成する際に、そうした情報を活用できる。また、企業が特定の成果を達成するために過剰な投資を行っていると判断する場合がある。この情報は、企業が他のサイバーセキュリティ対策を強化するために、リソースの優先順位付けをやり直す際に活用できる。

これらの 5 つのハイレベルの機能は、リスク管理プロセスに取って代わるものではないが、上級役員やその他の従業員がサイバーセキュリティリスクの基本概念を簡単につかめるようにするためのものであり、これにより従業員は、特定されたリスクがどのように管理されているかをアセスメントし、既存のサイバーセキュリティ標準、ガイドライン、ベストプラクティスに照らし合わせて高位のレベルに達するための自組織の取組を評価できる。また本フレームワークは、企業が「我々の取組は十分であるか？」などの基本的な質問に答えるのに役立つ。それによ

り、サイバーセキュリティ対策の強化が必要な箇所に必要なタイミングで、十分な情報に基づいた強化対策を実施できるようになる。

3.2　サイバーセキュリティプログラムの立ち上げまたは改良

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

ステップ 1: 優先順位付けを行い、範囲を決定する。 企業は事業目的／ミッションと、企業のハイレベルでの優先事項を決定する。この情報に基づいて、企業はサイバーセキュリティの実施に関する戦略的な意思決定を行い、対策すべきビジネスラインまたはプロセスを支援するシステムや資産の範囲を特定する。本フレームワークは、企業内のビジネスニーズと関連するリスク許容度が異なる、さまざまなビジネスラインまたはプロセスを支援するように調整できる。

ステップ 2: 方向付けを行う。 ステップ 1 で選択されたビジネスラインまたはプロセスに対するサイバーセキュリティプログラムの範囲が決定された後に、企業は関連するシステムと資産、規制上の要求事項、および全体的なリスクアプローチを特定する。その後、企業はそれらのシステムと資産に対する脅威と、それらのシステムと資産の脆弱性を特定する。

ステップ 3: 「現在のプロファイル」を作成する。 企業はコアのカテゴリーとサブカテゴリーの成果の内、現時点でどれが達成されているかを示す「現在のプロファイル」を作成する。

ステップ 4: リスクアセスメントを実施する。 リスクアセスメントは、企業の全体的なリスク管理プロセスによって、または過去のリスクアセスメント活動によって導出される場合がある。企業はサイバーセキュリティイベントが発生する可能性と、そのイベントが企業にもたらす影響を把握するために、運用環境を分析する。企業にとって新たなリスク、脅威、脆弱性に関するデータを取り入れることは、サイバーセキュリティイベントが発生する可能性と、その結果としてもたらされる影響を確実に理解するためにも重要である。

ステップ 5: 「目標のプロファイル」を作成する。 企業は自組織の期待されるサイバーセキュリティ成果について記述する、本フレームワークのカテゴリーとサブカテゴリーのアセスメントに焦点を当てて「目標のプロファイル」を作成する。また、自組織に固有のリスクに対処するために、独自のカテゴリーやサブカテゴリーを作成・追加してもよい。また、「目標のプロファイル」を作成する際に、業界関係者、顧客、ビジネスパートナーなどの外部利害関係者がもたらす影響と、彼らの要求事項を考慮する場合がある。

ステップ 6: ギャップを特定・分析し、優先順位付けを行う。 企業は「現在のプロファイル」と「目標のプロファイル」を比較してギャップを特定する。次に企業はそれらのギャップを埋めるための、優先順位付けがなされた行動計画を作成する。この計画は、ミッション上のモチベーション、費用対効果分析、そして「目標のプロファイル」に記述されている成果の達成に必要なリスクの判断に基づいて作成されなければならない。その後、企業はギャップを埋めるのに必要なリソースを決定する。プロファイルをこのように使用することで、サイバーセキュリティ対策に関し

て十分な情報に基づいた意思決定が可能になり、リスク管理も容易になり、費用対効果の高い、目標とされる改善対策を実施できるようになる。

ステップ 7: 行動計画を実施する。企業はステップ 6 で特定されたギャップ（もしあればだが）に対して取るべき行動を決定する。次に企業は、「目標のプロファイル」に照らし合わせて、現行のサイバーセキュリティ対策をモニタリングする。その他のガイダンスとして、本フレームワークは、カテゴリーとサブカテゴリーに関する参考情報の例を示している。しかしながら、企業は業界固有のものを含め、どの標準、ガイドライン、ベストプラクティスが自組織のニーズに最適であるかを決定する必要がある。

企業が自組織のサイバーセキュリティを継続的にアセスメントし、改善するためには、上述のステップを必要なだけ繰り返す必要がある。たとえば、ステップ 2「方向付けを行う」をより頻繁に実施することで、リスクアセスメントの質が向上する場合がある。さらに、「現在のプロファイル」が更新される度に、「現在のプロファイル」と「目標のプロファイル」を比較することによって、進捗状況のモニタリングが可能になる。企業はまた、この進捗状況を活用して、自組織のサイバーセキュリティプログラムを企業が選択したティアに合わせて調整してもよい。

3.3　サイバーセキュリティ上の要求事項を利害関係者に伝える

本フレームワークは、不可欠な重要インフラサービスの提供に責任を担う、互いに依存する利害関係者間での要求事項の伝達を可能にする共通言語を提供する。例としては以下が挙げられる:

- 企業は外部サービスプロバイダ（例:データをエクスポートしているクラウドプロバイダ）に対してサイバーセキュリティリスク管理上の要求事項を伝えるために、「目標のプロファイル」を使用できる。
- 企業はサイバーセキュリティの状態を報告したり、調達要件と比較できるようにするために、「現在のプロファイル」を使用してサイバーセキュリティの状態を表すことができる。
- 重要インフラ事業者／運用者は、そのインフラが依存する外部パートナーを特定した上で、必要な対策（カテゴリーとサブカテゴリー）を伝えるために「目標のプロファイル」を使用できる。
- 重要インフラ分野は、構成企業が活用できる初期プロファイルとして、業界独自の「目標のプロファイル」を作成してもよい。

3.4　新たな参考情報または改訂された参考情報の活用

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

3.5　プライバシーと市民の自由を保護するための方法論

本セクションは、大統領令に定められているような、サイバーセキュリティ活動が個人のプライバシーと市民の自由にもたらす影響に対処するための方法を記述する。この方法はプライバシーと市民の自由に対する影響について考慮すべき事項と、そうした考慮事項に対処するためのプロセスの一般的な例をまとめたものである。なぜ一般的な例であるかと言うと、プライバシーと市民の自由に対する影響は業界ごとに異なったり、時間の経過とともに変わる可能性があり、企業によっては技術的実装の範囲内でそうした考慮事項やプロセスに対応することが考えられるからである。とはいえサイバーセキュリティプログラム内のすべての活動が、そうした考慮を必要とするとは限らない。セクション 3.4 に記載されているように、技術的プライバシー標準、ガイドライン、追加のベストプラクティスの作成が、技術的実装の改善を支援するためにも必要である。

プライバシーと市民の自由に対する影響は、企業のサイバーセキュリティ対策に関連して個人情報が使用、収集、処理、保持、または開示される場合に発生する。プライバシーや市民の自由に対する考慮を必要とする活動には、たとえば以下がある：個人情報の過剰収集または過剰保持につながるサイバーセキュリティ対策; サイバーセキュリティ対策とは無関係な個人情報の開示または使用; 表現の自由または結社の自由に影響を与える類のインシデント検知／モニタリングなど、サービス妨害または類似の悪影響を及ぼすサイバーセキュリティ対策。

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

プライバシーに対する影響に対処するために、企業は、対策が適切である状況において、自組織のサイバーセキュリティプログラムがどのようにして、以下をはじめとするプライバシーの原則を取り入れることが可能であるかを検討すべきである：サイバーセキュリティインシデントに関連する個人情報を含む資料を収集、開示、保持する際には、データを最小限に抑える; サイバーセキュリティ対策のために収集された情報の、サイバーセキュリティ対策以外の目的での使用を制限する; 特定のサイバーセキュリティ対策の透明性を確保する; 個人情報をサイバーセキュリティ対策に使用することに関して、個人の同意を得て、悪影響が及んだ場合の救済措置を用意する; データの質、完全性、セキュリティを確保する; 説明責任と監査が行われるようにする。

企業が 付録 A を参照してコアをアセスメントする際には、上述のプライバシーと市民の自由に対する影響に対処する手段として、以下のプロセスと活動を検討する可能性がある：

サイバーセキュリティリスクのガバナンス

- 企業によるサイバーセキュリティリスクのアセスメントと、潜在的リスクへの対応では、自組織のサイバーセキュリティプログラムがプライバシーにもたらす影響を考慮すること。

- サイバーセキュリティ関連のプライバシー問題に責任を負う個人は、十分な訓練を受けた者とし、適切な管理者層への報告を行うこと。
- サイバーセキュリティ対策がプライバシーに関して適用される法律、規制、憲法上の要求事項を遵守するのを支援するためのプロセスが存在すること。
- 前述の対策とコントロールの実施をアセスメントするためのプロセスが存在すること。

企業の資産とシステムをアクセスする個人を特定し、権限を与えるためのアプローチ

- 個人情報の収集、開示、または使用を伴うアクセス制御における、プライバシーに対する影響を特定し、対処するための措置をとること。

意識向上およびトレーニング対策

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

異常な活動の検知と、システムおよび資産のモニタリング

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

情報共有、またはその他の低減対策を含む、対応活動

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

付録 A: フレームワークコア

本付録はコア、すなわち、すべての重要インフラ分野に共通となる、サイバーセキュリティ対策のベストプラクティスとなる機能、カテゴリー、サブカテゴリー、参考情報の一覧を示す。本付録のコアの記載書式は、実施に関して具体的な順番を示しているわけではなく、記載されているカテゴリー、サブカテゴリー、参考情報が重要度が高くなる順に記載されているわけでもない。本付録に示されているコアは、サイバーセキュリティリスクを管理するための対策の一般的な例である。本フレームワークは包括的なものではないが、拡張可能であり、企業、業界、その他の関係者が、費用対効果が高く効率的なサブカテゴリーと参考情報を活用できるようにし、サイバーセキュリティリスクを管理できるようにする。対策はプロファイル作成時にコアから選択でき、追加のカテゴリー、サブカテゴリー、参考情報をプロファイルに追加することもできる。企業のリスク管理プロセス、法規制上の要求事項、事業目的／ミッション、企業に課せられている制約は、プロファイル作成時の上述の活動の選択に影響を与える。個人情報は、セキュリティリスクと保護対策をアセスメントする際に、カテゴリーで参照されるデータまたは資産の1つの要素である。

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

使いやすさのため、コアの各コンポーエントには一意の識別子が割り当てられている。表 1 に示されているように、機能とカテゴリーにはそれぞれアルファベットで記された一意の識別子が割り当てられている。表 2 の各カテゴリー内のサブカテゴリーには数字の、一意の識別子が割り当てられている。

本フレームワークに関連する補足資料に関しては、下記の NIST ウェブサイトを参照のこと。
http://www.nist.gov/cyberframework/

表 1: 機能の一意の識別子とカテゴリーの一意の識別子

機能の一意の識別子	機能	カテゴリーの一意の識別子	カテゴリー
ID	特定	ID.AM	資産管理
		ID.BE	ビジネス環境
		ID.GV	ガバナンス
		ID.RA	リスクアセスメント
		ID.RM	リスク管理戦略
PR	防御	PR.AC	アクセス制御
		PR.AT	意識向上およびトレーニング
		PR.DS	データセキュリティ
		PR.IP	情報を保護するためのプロセスおよび手順
		PR.MA	保守
		PR.PT	保護技術
DE	検知	DE.AE	異常とイベント
		DE.CM	セキュリティの継続的なモニタリング
		DE.DP	検知プロセス
RS	対応	RS.RP	対応計画の作成
		RS.CO	伝達
		RS.AN	分析
		RS.MI	低減
		RS.IM	改善
RC	復旧	RC.RP	復旧計画の作成
		RC.IM	改善
		RC.CO	伝達

表 2: フレームワークコア

機能	カテゴリー	サブカテゴリー	参考情報
特定 （ID）	**資産管理（ID.AM）:** 組織が事業目的を達成することを可能にするデータ、職員、デバイス、システム、施設を特定し、事業目標と自組織のリスク戦略との相対的重要性に応じて管理している。	**ID.AM-1**: 企業内の物理デバイスとシステムの一覧を作成している。	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: 企業内のソフトウェアプラットフォームとアプリケーションの一覧を作成している。	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: 企業内の通信とデータの流れの図を用意している。	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: 外部情報システムの一覧を作成している。	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: リソース（例：ハードウェア、デバイス、データ、ソフトウェア）を、分類、重要度、ビジネス上の価値に基づいて優先順位付けしている。	• **COBIT 5** APO03.03, APO03.04, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6: すべての従業員と第三者である利害関係者（例：供給業者、顧客、パートナー）に対して、サイバーセキュリティ上の役割と責任を定めている。	• **COBIT 5** APO01.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1

機能	カテゴリー	サブカテゴリー	参考情報
			• **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
	ビジネス環境（ID.BE）: 自組織のミッション、目標、利害関係者、活動を理解し、優先順位付けを行っている; この情報はサイバーセキュリティ上の役割、責任、リスク管理上の意思決定を伝達するために使用される。	**ID.BE-1:** サプライチェーンにおける企業の役割を特定し、伝達している	• **COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 • **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 • **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: 重要インフラとその産業分野における企業の位置付けを特定し、伝達している。	• **COBIT 5** APO02.06, APO03.01 • **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: 企業のミッション、目標、活動に関して優先順位を定め、伝達している。	• **COBIT 5** APO02.01, APO02.06, APO03.01 • **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 • **NIST SP 800-53 Rev. 4** PM-11, SA-14
		ID.BE-4:重要サービスを提供する上での依存関係と重要な機能を把握している。	• **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 • **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: 重要サービスの提供を支援する、レジリエンスに関する要求事項を定めている。	• **COBIT 5** DSS04.02 • **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 • **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14
	ガバナンス（ID.GV）: 自組織に対する規制、法律、リスクと、自組織の環境、運用上の要求事項を管理しモニタリングするためのポリシー、手順、プロセスを理解しており、サイバーセキュリティリスクの管理者に伝達している。	**ID.GV-1:** 自組織の情報セキュリティポリシーを定めている。	• **COBIT 5** APO01.03, EDM01.01, EDM01.02 • **ISA 62443-2-1:2009** 4.3.2.6 • **ISO/IEC 27001:2013** A.5.1.1 • **NIST SP 800-53 Rev. 4** -1 controls from all families
		ID.GV-2: 情報セキュリティ上の役割と責任について、内部と外部パートナーとで調整・連携している。	• **COBIT 5** APO13.12 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1 • **NIST SP 800-53 Rev. 4** PM-1, PS-7
		ID.GV-3: プライバシーや市民の自由に関する義務を含む、サイバーセキュリティ	• **COBIT 5** MEA03.01, MEA03.04

機能	カテゴリー	サブカテゴリー	参考情報
		に関する法規制上の要求事項を理解し、管理している。	• **ISA 62443-2-1:2009** 4.4.3.7 • **ISO/IEC 27001:2013** A.18.1 • **NIST SP 800-53 Rev. 4** -1 controls from all families (except PM-1)
		ID.GV-4: ガバナンスとリスク管理プロセスがサイバーセキュリティリスクに対応している。	• **COBIT 5** DSS04.02 • **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 • **NIST SP 800-53 Rev. 4** PM-9, PM-11
	リスクアセスメント（ID.RA）: 企業は自組織の業務（ミッション、機能、イメージ、評判を含む）、自組織の資産、個人に対するサイバーセキュリティリスクを把握している。	**ID.RA-1:** 資産の脆弱性を特定し、文書化している。	• **CCS CSC** 4 • **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 • **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: 情報共有フォーラム／ソースより、脅威と脆弱性に関する情報を入手している。	• **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **ISO/IEC 27001:2013** A.6.1.4 • **NIST SP 800-53 Rev. 4** PM-15, PM-16, SI-5
		ID.RA-3: 内外からの脅威を特定し、文書化している。	• **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
		ID.RA-4: ビジネスに対する潜在的な影響と、その可能性を特定している。	• **COBIT 5** DSS04.02 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-9, PM-11, SA-14
		ID.RA-5: リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮している。	• **COBIT 5** APO12.02 • **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16

機能	カテゴリー	サブカテゴリー	参考情報
		ID.RA-6: リスクに対する対応を定め、優先順位付けしている。	• **COBIT 5** APO12.05, APO13.02 • **NIST SP 800-53 Rev. 4** PM-4, PM-9
	リスク管理戦略（ID.RM）: 自組織の優先順位、制約、リスク許容度、想定を定め、運用リスクの判断に利用している。	**ID.RM-1:** リスク管理プロセスが自組織の利害関係者によって確立、管理され、承認されている。	• **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 • **ISA 62443-2-1:2009** 4.3.4.2 • **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2: 自組織のリスク許容度を決定し、明確にしている。	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.3.2.6.5 • **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-3: 企業によるリスク許容度の決定が、重要インフラにおける自組織の役割と、その分野に特化したリスク分析の結果に基づいて行われている。	• **NIST SP 800-53 Rev. 4** PM-8, PM-9, PM-11, SA-14
防御（PR）	**アクセス制御（PR.AC）:** 資産および関連施設へのアクセスを、承認されたユーザ、プロセス、またはデバイスと、承認された活動およびトランザクションに限定している。	**PR.AC-1:** 承認されたデバイスとユーザの識別情報と認証情報を管理している。	• **CCS CSC** 16 • **COBIT 5** DSS05.04, DSS06.03 • **ISA 62443-2-1:2009** 4.3.3.5.1 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 • **NIST SP 800-53 Rev. 4** AC-2, IA Family
		PR.AC-2: 資産に対する物理アクセスを管理し、保護している。	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 • **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 • **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
		PR.AC-3: リモートアクセスを管理している。	• **COBIT 5** APO13.01, DSS01.04, DSS05.03 • **ISA 62443-2-1:2009** 4.3.3.6.6 • **ISA 62443-3-3:2013** SR 1.13, SR 2.6

機能	カテゴリー	サブカテゴリー	参考情報
			• **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-17, AC-19, AC-20
		PR.AC-4: 最小権限および職務の分離の原則を取り入れて、アクセス権限を管理している。	• **CCS CSC** 12, 15 • **ISA 62443-2-1:2009** 4.3.3.7.3 • **ISA 62443-3-3:2013** SR 2.1 • **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 • **NIST SP 800-53 Rev. 4** AC-2, AC-3, AC-5, AC-6, AC-16
		PR.AC-5: 適宜、ネットワークの分離を行って、ネットワークの完全性を保護している。	• **ISA 62443-2-1:2009** 4.3.3.4 • **ISA 62443-3-3:2013** SR 3.1, SR 3.8 • **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, SC-7
	意識向上およびトレーニング（PR.AT）: 自組織の職員およびパートナーに対して、関連するポリシー、手順、契約に基づいた、情報セキュリティに関連する義務と責任を果たせるようにするために、サイバーセキュリティ意識向上教育と、十分なトレーニングを実施している。	**PR.AT-1:** すべてのユーザに情報を周知し、トレーニングを実施している。	• **CCS CSC** 9 • **COBIT 5** APO07.03, BAI05.07 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.7.2.2 • **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: 権限を持つユーザが役割と責任を理解している。	• **CCS CSC** 9 • **COBIT 5** APO07.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 • **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-3: 第三者である利害関係者（例：供給業者、顧客、パートナー）が役割と責任を理解している。	• **CCS CSC** 9 • **COBIT 5** APO07.03, APO10.04, APO10.05 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 • **NIST SP 800-53 Rev. 4** PS-7, SA-9

機能	カテゴリー	サブカテゴリー	参考情報
		PR.AT-4: 上級役員が役割と責任を理解している。	• **CCS CSC** 9 • **COBIT 5** APO07.03 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, • **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-5: 物理セキュリティおよび情報セキュリティの担当者が役割と責任を理解している。	• **CCS CSC** 9 • **COBIT 5** APO07.03 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, • **NIST SP 800-53 Rev. 4** AT-3, PM-13
	データセキュリティ(PR.DS): 情報と記録(データ)を情報の機密性、完全性、可用性を保護するために定められた自組織のリスク戦略に従って管理している。	**PR.DS-1:** 保存されているデータを保護している。	• **CCS CSC** 17 • **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS06.06 • **ISA 62443-3-3:2013** SR 3.4, SR 4.1 • **ISO/IEC 27001:2013** A.8.2.3 • **NIST SP 800-53 Rev. 4** SC-28
		PR.DS-2: 伝送中のデータを保護している。	• **CCS CSC** 17 • **COBIT 5** APO01.06, DSS06.06 • **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** SC-8
		PR.DS-3: 資産について撤去、譲渡、廃棄プロセスを正式に管理している。	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4. 4.3.3.3.9, 4.3.4.4.1 • **ISA 62443-3-3:2013** SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 • **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
		PR.DS-4: 可用性を確保するのに十分な	• **COBIT 5** APO13.01

機能	カテゴリー	サブカテゴリー	参考情報
		容量を保持している。	• **ISA 62443-3-3:2013** SR 7.1, SR 7.2 • **ISO/IEC 27001:2013** A.12.3.1 • **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: データ漏えいに対する保護対策を実施している。	• **CCS CSC** 17 • **COBIT 5** APO01.06 • **ISA 62443-3-3:2013** SR 5.2 • **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: ソフトウェア、ファームウェア、および情報の完全性の検証に、完全性チェックメカニズムを使用している。	• **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 • **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** SI-7
		PR.DS-7: 開発・テスト環境を実稼働環境から分離している。	• **COBIT 5** BAI07.04 • **ISO/IEC 27001:2013** A.12.1.4 • **NIST SP 800-53 Rev. 4** CM-2
	情報を保護するためのプロセスおよび手順（PR.IP）:（目的、範囲、役割、責任、経営コミットメント、組織間の調整を扱う）セキュリティポリシー、プロセス、手順を維持し、情報システムと資産の保護の管理に使用している。	**PR.IP-1:** 情報技術／産業用制御システムのベースラインとなる設定を定め、維持している。	• **CCS CSC** 3, 10 • **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 • **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 • **ISA 62443-3-3:2013** SR 7.6 • **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: システムを管理するためのシステム開発ライフサイクルを導入している。	• **COBIT 5** APO13.01 • **ISA 62443-2-1:2009** 4.3.4.3.3

機能	カテゴリー	サブカテゴリー	参考情報
			• **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 • **NIST SP 800-53 Rev. 4** SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
		PR.IP-3: 設定変更管理プロセスを導入している。	• **COBIT 5** BAI06.01, BAI01.06 • **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 • **ISA 62443-3-3:2013** SR 7.6 • **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
		PR.IP-4: 情報のバックアップを定期的に実施、保持し、テストしている。	• **COBIT 5** APO13.01 • **ISA 62443-2-1:2009** 4.3.4.3.9 • **ISA 62443-3-3:2013** SR 7.3, SR 7.4 • **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 • **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
		PR.IP-5: 自組織の資産の物理的な運用環境に関するポリシーと規制を満たしている。	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 • **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 • **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: ポリシーに従ってデータを破壊している。	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4.3.4.4.4 • **ISA 62443-3-3:2013** SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 • **NIST SP 800-53 Rev. 4** MP-6
		PR.IP-7: 保護プロセスを継続的に改善している。	• **COBIT 5** APO11.06, DSS04.05 • **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3,

機能	カテゴリー	サブカテゴリー	参考情報
			4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: 保護技術の有効性について、適切なパートナーとの間で情報を共有している。	• **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: 対応計画（インシデント対応および事業継続）と復旧計画（インシデントからの復旧および災害復旧）を実施し、管理している。	• **COBIT 5** DSS04.03 • **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 • **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2 • **NIST SP 800-53 Rev. 4** CP-2, IR-8
		PR.IP-10: 対応計画と復旧計画をテストしている。	• **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 • **ISA 62443-3-3:2013** SR 3.3 • **ISO/IEC 27001:2013** A.17.1.3 • **NIST SP 800-53 Rev.4** CP-4, IR-3, PM-14
		PR.IP-11: 人事に関わる対策にサイバーセキュリティ（例：アクセス権限の無効化、従業員に対する審査）を含めている。	• **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 • **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 • **ISO/IEC 27001:2013** A.7.1.1, A.7.3.1, A.8.1.4 • **NIST SP 800-53 Rev. 4** PS Family
		PR.IP-12: 脆弱性管理計画を作成し、実施している。	• **ISO/IEC 27001:2013** A.12.6.1, A.18.2.2 • **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	保守（PR.MA）: 産業用制御システムと情報システムのコンポーネントの保守と修理をポリシーと手順に従って実施している。	**PR.MA-1:** 自組織の資産の保守と修理は、承認・管理されたツールを用いて、タイムリーに実施し、ログを記録している。	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4.3.3.3.7 • **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5 • **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5
		PR.MA-2: 自組織の資産に対する遠隔保守は、承認を得て、ログを記録し、不正ア	• **COBIT 5** DSS05.04 • **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8

機能	カテゴリー	サブカテゴリー	参考情報
		クセスを防げる形で実施している。	• **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 • **NIST SP 800-53 Rev. 4** MA-4
	保護技術（PR.PT）: 関連するポリシー、手順、契約に基づいて、システムと資産のセキュリティと耐性・復旧力を確保するための、技術的なセキュリティソリューションを管理している。	**PR.PT-1:** ポリシーに従って監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューしている。	• **CCS CSC** 14 • **COBIT 5** APO11.04 • **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 • **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 • **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 • **NIST SP 800-53 Rev. 4** AU Family
		PR.PT-2: ポリシーに従って取り外し可能な外部記録媒体を保護し、そうした媒体の使用を制限している。	• **COBIT 5** DSS05.02, APO13.01 • **ISA 62443-3-3:2013** SR 2.3 • **ISO/IEC 27001:2013** A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 • **NIST SP 800-53 Rev. 4** MP-2, MP-4, MP-5, MP-7
		PR.PT-3: 最小機能の原則を取り入れて、システムと資産に対するアクセスを制御している。	• **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 • **ISO/IEC 27001:2013** A.9.1.2 • **NIST SP 800-53 Rev. 4** AC-3, CM-7
		PR.PT-4: 通信ネットワークと制御ネットワークを保護している。	• **CCS CSC** 7 • **COBIT 5** DSS05.02, APO13.01

機能	カテゴリー	サブカテゴリー	参考情報
			• **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 • **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7
検知（DE）	**異常とイベント（DE.AE）:** 異常な活動をタイムリーに検知し、イベントがもたらす可能性のある影響を把握している。	**DE.AE-1:** ネットワーク運用のベースラインと、ユーザとシステム間の予測されるデータの流れを特定し、管理している。	• **COBIT 5** DSS03.01 • **ISA 62443-2-1:2009** 4.4.3.3 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: 攻撃の標的と手法を理解するために、検知したイベントを分析している。	• **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 • **ISO/IEC 27001:2013** A.16.1.1, A.16.1.4 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: イベントデータを複数の情報源やセンサーから収集し、相互に関連付けている。	• **ISA 62443-3-3:2013** SR 6.1 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: イベントがもたらす影響を特定している。	• **COBIT 5** APO12.06 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI - 4
		DE.AE-5: インシデント警告の閾値を定めている。	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.2.3.10 • **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	セキュリティの継続的なモニタリング (DE.CM): サイバーセキュリティイベントを検知し、保護対策の有効性を検証するために、	**DE.CM-1:** 発生する可能性のあるサイバーセキュリティイベントを検知できるよう、ネットワークをモニタリングしている。	• **CCS CSC** 14, 16 • **COBIT 5** DSS05.07 • **ISA 62443-3-3:2013** SR 6.2 • **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7,

機能	カテゴリー	サブカテゴリー	参考情報
	情報システムと資産を離散間隔でモニタリングしている。		CM-3, SC-5, SC-7, SI-4
		DE.CM-2: 発生する可能性のあるサイバーセキュリティイベントを検知できるよう、物理環境をモニタリングしている。	• **ISA 62443-2-1:2009** 4.3.3.3.8 • **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: 発生する可能性のあるサイバーセキュリティイベントを検知できるよう、個人の活動をモニタリングしている。	• **ISA 62443-3-3:2013** SR 6.2 • **ISO/IEC 27001:2013** A.12.4.1 • **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: 悪質なコードを検出できる。	• **CCS CSC** 5 • **COBIT 5** DSS05.01 • **ISA 62443-2-1:2009** 4.3.4.3.8 • **ISA 62443-3-3:2013** SR 3.2 • **ISO/IEC 27001:2013** A.12.2.1 • **NIST SP 800-53 Rev. 4** SI-3
		DE.CM-5: 悪質なモバイルコードを検出できる。	• **ISA 62443-3-3:2013** SR 2.4 • **ISO/IEC 27001:2013** A.12.5.1 • **NIST SP 800-53 Rev. 4** SC-18, SI-4. SC-44
		DE.CM-6: 発生する可能性のあるサイバーセキュリティイベントを検知できるよう、外部サービスプロバイダの活動をモニタリングしている。	• **COBIT 5** APO07.06 • **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 • **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: 権限のない従業員、接続、デバイス、ソフトウェアのモニタリングを実施している。	• **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: 脆弱性スキャンを実施している。	• **COBIT 5** BAI03.10 • **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 • **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** RA-5
	検知プロセス（DE.DP）: 異常なイベントをタイムリーに、かつ正	**DE.DP-1:** 説明責任を果たせるよう、検知に関する役割と責任を明確に定義してい	• **CCS CSC** 5 • **COBIT 5** DSS05.01

機能	カテゴリー	サブカテゴリー	参考情報
	確に検知するための検知プロセスおよび手順を維持し、テストしている。	る。	• **ISA 62443-2-1:2009** 4.4.3.1 • **ISO/IEC 27001:2013** A.6.1.1 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: 検知活動は必要なすべての要求事項を満たしている。	• **ISA 62443-2-1:2009** 4.4.3.2 • **ISO/IEC 27001:2013** A.18.1.4 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14, SI-4
		DE.DP-3: 検知プロセスをテストしている。	• **COBIT 5** APO13.02 • **ISA 62443-2-1:2009** 4.4.3.2 • **ISA 62443-3-3:2013** SR 3.3 • **ISO/IEC 27001:2013** A.14.2.8 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
		DE.DP-4: イベント検知情報を適切な関係者に伝達している。	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.3.4.5.9 • **ISA 62443-3-3:2013** SR 6.1 • **ISO/IEC 27001:2013** A.16.1.2 • **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: 検知プロセスを継続的に改善している。	• **COBIT 5** APO11.06, DSS04.05 • **ISA 62443-2-1:2009** 4.4.3.4 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

機能	カテゴリー	サブカテゴリー	参考情報
対応（RS）	**対応計画（RS.RP）:** 検知したサイバーセキュリティイベントにタイムリーに対応できるよう、対応プロセスおよび手順を実施し、維持している。	**RS.RP-1:** イベントの発生中または発生後に対応計画を実施している。	• **COBIT 5** BAI01.10 • **CCS CSC** 18 • **ISA 62443-2-1:2009** 4.3.4.5.1 • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	伝達（RS.CO）: 法執行機関からの支援を必要に応じて得られるよう、内外の利害関係者との間で対応活動を調整している。	**RS.CO-1:** 対応が必要になった時の自身の役割と行動の順番を従業員は認識している。	• **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 • **ISO/IEC 27001:2013** A.6.1.1, A.16.1.1 • **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: 定められた基準に沿って、イベントを報告している。	• **ISA 62443-2-1:2009** 4.3.4.5.5 • **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 • **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: 対応計画に従って情報を共有している。	• **ISA 62443-2-1:2009** 4.3.4.5.2 • **ISO/IEC 27001:2013** A.16.1.2 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: 対応計画に従って、利害関係者との間で調整を行っている。	• **ISA 62443-2-1:2009** 4.3.4.5.5 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: サイバーセキュリティに関する状況認識を深めるために、外部利害関係者との間で任意の情報共有を行っている。	• **NIST SP 800-53 Rev. 4** PM-15, SI-5
	分析 (RS.AN): 適切な対応を確実にし、復旧活動を支援するために、分析を実施している。	**RS.AN-1:** 検知システムからの通知を調査している。	• **COBIT 5** DSS02.07 • **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISA 62443-3-3:2013** SR 6.1 • **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-

機能	カテゴリー	サブカテゴリー	参考情報
			5, PE-6, SI-4
		RS.AN-2: インシデントがもたらす影響を把握している。	• **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: フォレンジクスを実施している。	• **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 • **ISO/IEC 27001:2013** A.16.1.7 • **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: 対応計画に従ってインシデントを分類している。	• **ISA 62443-2-1:2009** 4.3.4.5.6 • **ISO/IEC 27001:2013** A.16.1.4 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
	低減（RS.MI）: イベントの拡大を防ぎ、その影響を緩和し、インシデントを根絶するための活動を実施している。	**RS.MI-1:** インシデントを封じ込めている。	• **ISA 62443-2-1:2009** 4.3.4.5.6 • **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-2: インシデントを低減している。	• **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 • **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 • **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-3: 新たに特定された脆弱性に関して、許容できるリスクである場合にはその旨を文書化し、そうでない場合には低減している。	• **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	改善（RS.IM）: 現在と過去の意思決定／対応活動から学んだ教訓を取り入れることで、自組織の対応活動を改善している。	**RS.IM-1:** 学んだ教訓を対応計画に取り入れている。	• **COBIT 5** BAI01.13 • **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: 対応戦略を更新している。	• **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
復旧（RC）	**復旧計画（RC.RP）:** サイバーセキュリティイベントによる影響を	**RC.RP-1:** イベントの発生中または発生後に復旧計画を実施している。	• **CCS CSC** 8 • **COBIT 5** DSS02.05, DSS03.04

機能	カテゴリー	サブカテゴリー	参考情報
	受けたシステムや資産をタイムリーに復旧できるよう、復旧プロセスおよび手順を実施し、維持している。		• **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	改善（RC.IM）: 学んだ教訓を将来的な活動に取り入れることで、復旧計画およびプロセスを改善している。	**RC.IM-1:** 学んだ教訓を復旧計画に取り入れている。	• **COBIT 5** BAI05.07 • **ISA 62443-2-1:2009** 4.4.3.4 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: 復旧戦略を更新している。	• **COBIT 5** BAI07.08 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	伝達（RC.CO）: コーディネーティングセンター、インターネットサービスプロバイダ、攻撃システムのオーナー、被害者、その他のCSIRT、ベンダなどの、内外の関係者との間で復旧活動を調整している。	**RC.CO-1:** 広報活動を管理している。	• **COBIT 5** EDM03.02
		RC.CO-2: イベント発生後に評判を回復している。	• **COBIT 5** MEA03.02
		RC.CO-3: 復旧活動について内部利害関係者と役員、そして経営陣に伝達している。	• **NIST SP 800-53 Rev. 4** CP-2, IR-4

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

- Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
- Council on CyberSecurity (CCS) Top 20 Critical Security Controls (CSC): http://www.counciloncybersecurity.org
- ANSI/ISA-62443-2-1 (99.02.01)-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*: http://www.isa.org/Template.cfm?Section=Standards8&Template=/Ecommerce/ProductDisplay.cfm&ProductID=10243
- ANSI/ISA-62443-3-3 (99.03.03)-2013, *Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels*: http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=13420
- ISO/IEC 27001, *Information technology -- Security techniques -- Information security management systems -- Requirements*: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534

- NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, 2013 年 4 月（2014 年 1 月 15 日時点での更新内容を含む）. http://dx.doi.org/10.6028/NIST.SP.800-53r4.

本付録に示されているコアのサブカテゴリーと参考情報のセクションとの対応付けは、おおまかな対応を示すものであり、参考情報のセクションが、サブカテゴリーに記述されている期待される成果達成を必ずしも約束するものではない。

付録 B: 用語集

本付録は、本文書で使用されている一部の用語の定義を示す。

Category **（カテゴリー）**	機能をサイバーセキュリティ成果グループ別に細分化したものであり、計画に基づいたニーズや特定の対策と密接に結びついている。カテゴリーには、たとえば「資産管理」、「アクセス制御」、「検知プロセス」がある。
Critical Infrastructure **（重要インフラ）**	物理的存在か、仮想的存在かに関わらず、米国にとって必要不可欠なシステムや資産で、これらのシステムや資産が利用不能な状態になったり、破壊された場合、米国のサイバーセキュリティ、経済安全保障、国民の健康や安全、またはこれらの問題のうち複数、あるいはすべてに悪影響を与える可能性があるもの。
Cybersecurity **（サイバーセキュリティ）**	攻撃を防止、検知し、攻撃に対応することにより情報を保護するプロセス。
Cybersecurity Event **（サイバーセキュリティイベント）**	企業の業務（ミッション、能力、評判を含む）に影響を及ぼす可能性のある、サイバーセキュリティに関わる変化。
Detect (function) **（検知（機能））**	サイバーセキュリティイベントの発生を検知するための適切な対策を検討し、実施すること。
Framework **（フレームワーク）**	サイバーセキュリティリスクを低減するためのリスクベース・アプローチであり、以下の 3 つの要素で構成されている：フレームワークコア、フレームワークプロファイル、フレームワークインプレメンテーションティア。「サイバーセキュリティフレームワーク」としても知られている。
Framework Core **（フレームワークコア）**	すべての重要インフラ分野に共通となるサイバーセキュリティ対策のベストプラクティス、期待される成果、参考情報をまとめたもの。フレームワークコアは以下の 4 つの要素で構成されている：機能、カテゴリー、サブカテゴリー、参考情報。
Framework Implementation Tier **（フレームワークインプレメンテーションティア）**	企業の、リスクに対するアプローチの特徴、すなわち、企業がサイバーセキュリティリスクをどのようにとらえているか、また、そうしたリスクを管理するためにどのようなプロセスを実施しているかを確認するための仕組み。

Framework Profile **（フレームワークプロファイル）**	本フレームワークのカテゴリーおよびサブカテゴリーから特定のシステムまたは企業が選択した、期待される成果を表すもの。
Function **（機能）**	本フレームワークの主要構成要素の一つ。機能は基本的なサイバーセキュリティ対策の最も上位を構成する要素であり、カテゴリーやサブカテゴリーにて詳細化される。機能は以下の 5 つの要素で構成されている:「特定」、「防御」、「検知」、「対応」、「復旧」。
Identify (function) **（特定（機能））**	システム、資産、データ、機能に対するサイバーセキュリティリスクの管理に必要な理解を深めること。
Informative Reference **（参考情報）**	すべての重要インフラ分野に共通となる標準、ガイドライン、ベストプラクティスをまとめたセクションであり、各サブカテゴリーに対応する、期待される成果を達成するための方法を示す。
Mobile Code **（モバイルコード）**	異なるプラットフォームに変更を加えることなく実装され、同一の方法で実行可能なプログラム（例:スクリプト、マクロ、またはその他の移植性のある命令文）。
Protect (function) **（防御（機能））**	重要インフラサービスの提供を確実にするための適切な保護対策を検討し、実施すること。
Privileged User **（権限を持つユーザ）**	通常のユーザの場合は実行する権限のない、セキュリティ関連機能を実行する権限のある（＝信頼されている）ユーザ。
Recover (function) **（復旧（機能））**	レジリエンスを実現するための計画を策定・維持し、サイバーセキュリティイベントによって阻害されたあらゆる機能やサービスを復旧するための適切な対策を検討し、実施すること。
Respond (function) **（対応（機能））**	検知されたサイバーセキュリティイベントに対処するための適切な対策を検討し、実施すること。
Risk **（リスク）**	発生しうる状況またはイベントによって、あるものが脅かされる程度の尺度であり、通常、(i) 当該の状況またはイベントが発生した場合にもたらされると考えられる悪影響と、(ii) 発生の可能性との計算式（関数）によって求められる。
Risk Management **（リスク管理）**	リスクを特定、アセスメントし、リスクに対応するプロセス。

Subcategory **（サブカテゴリー）**	カテゴリーを技術的な対策や管理面での対策がもたらす成果別に細分化したもの。サブカテゴリーには、たとえば「外部情報システムの一覧を作成している」、「保存されているデータを保護している」、「検知システムからの通知を調査している」などがある。

付録 C: 略語

本付録は、本文書で使用されている一部の略語の定義を示す。

CCS	Council on CyberSecurity
COBIT	Control Objectives for Information and Related Technology
DCS	Distributed Control System
DHS	Department of Homeland Security
EO	Executive Order
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IR	Interagency Report
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
IT	Information Technology
NIST	National Institute of Standards and Technology
RFI	Request for Information
RMP	Risk Management Process
SCADA	Supervisory Control and Data Acquisition
SP	Special Publication