政府情報システムにおける
サイバーセキュリティフレームワーク導入に関する
技術レポート

2023（令和 5）年 3 月 31 日

デジタル庁

〔標準ガイドライン群ＩＤ〕
DS-22X

〔キーワード〕
サイバーセキュリティフレームワーク

〔概要〕
サイバー攻撃の高度化・複雑化に伴い、サイバーレジリエンスの強化が求められており、脅威の侵入を前提とし、識別・防御に加え、検知・対応・復旧を認識することで、情報セキュリティ機密性・完全性・可用性を高めることがますます重視される中、NIST サイバーセキュリティフレームワークが世界的にも注目されている。
本技術レポートでは、サイバーセキュリティフレームワークについて解説し、政府情報システムに導入する上での要点を示すことを目的とする。

改定履歴

改定年月日	改定箇所	改定内容
2023年3月31日	-	・初版決定

目次

１　はじめに

社会全体のデジタルトランスフォーメーションが加速し、我々を取り巻く様々な分野においてデジタル技術の利活用が進んでいる。他方、サイバー攻撃はその発生頻度の増加と高度化が続く状況下にあり、サイバーセキュリティ対策のさらなる強化が不可欠となってきている。政府情報システムに対しても、今後、サイバー攻撃の脅威は高まっていくことが予想される。

こうした背景から、政府機関等に対するサイバー攻撃に対しても、それを防御することだけに注力するのではなく、攻撃の発生を速やかに検知し、対応することで被害を極小化し、正常状態に迅速に復旧することにも意識を向ける必要がある。

近年、包括的にサイバーセキュリティ態勢を構築するための代表的なツールとしてアメリカ国立標準技術研究所（以下、「NIST」という。）において、サイバーセキュリティフレームワークが開発され、国際的にもその利用や応用が進んでいる。

本文書はサイバーセキュリティフレームワークの基本的な考え方を解説した上で、政府機関や政府情報システムに対して当該フレームワークを導入するための方針、実施プロセスを示すと共に政府統一基準やその他のセキュリティに関する基準等との関係についても言及する。

１．１　背景と目的

本文書は、政府情報システムの開発や運用業務に従事する関係者に対して、サイバーセキュリティフレームワークの概要とその必要性、及びその特徴を示すことを主目的とする。

サイバーセキュリティ対策を講じる際には、特定のセキュリティ対策ソリューションを導入するだけでは不十分であり、サイバーセキュリティ態勢を構築・維持する上で構成される機能（「識別」「検知」「防御」「対応」「復旧」）に対して、組織及び情報システムのリスクに応じたセキュリティ対策を実施することが重要である。

サイバーセキュリティ対策の計画や実施の段階において、サイバーセキュリティフレームワークを参照し、導入することで、組織や情報システムにおけるサイバーセキュリティの各機能におけるサイバーセキュリティ対策のばらつきや不十分なリスク管理が解消され、政府機関並びに政府情報システムにおけるサイバーセキュリティの水準が向上することが期待される。

１．２　適用対象

本文書は、政府情報システムを適用対象として想定している。なお、本文書

はサイバーセキュリティフレームワークへの理解を深める参考文書であり、適用の遵守を求めるものではない。

１．３　位置づけ

本文書は、標準ガイドライン群の Informative（情報提供）のレベルの参考文書である。

１．４　本書の構成

第 2 章ではサイバーセキュリティフレームワークの概要を示し、サイバーセキュリティフレームワークの必要性と特徴について説明する。サイバーセキュリティフレームワークに関する知見がない読者は、本章を理解することで第 3 章以降の記載内容への理解を深めることができるため、一読することを推奨する。また、第 6 節ではサイバーセキュリティフレームワークの諸外国での活用状況について紹介する。

第 3 章ではサイバーセキュリティフレームワークを導入するためのプロセスについて、準備段階で実施すべき事項や導入段階で実施すべき事項を示すとともに、第 3 節ではサイバーセキュリティフレームワークを導入する際の留意事項についても説明する。

第 4 章ではサイバーセキュリティフレームワークと政府統一基準を筆頭に他のセキュリティの基準等との関係性について説明する。サイバーセキュリティフレームワークは、政府統一基準やその他のセキュリティに係る基準やフレームワークを排他するものではなく、政府機関は、政府統一基準および各政府機関の情報セキュリティポリシーに準拠した上で、サイバーセキュリティフレームワークを参照することが重要となる。

１．５　用語

本文書において使用する用語は、表１-1 及び本文書に別段の定めがある場合を除くほか、標準ガイドライン群用語集の例による。その他専門的な用語については、民間の用語定義を参照すること。

表 1-1 用語の定義

用語	意味
サイバーレジリエンス（サイバーレジリエント）	サイバーセキュリティ攻撃の影響を最小限に留めつつ、迅速に元の状態に回復、復元すること
サイバーセキュリティフレームワーク	NIST サイバーセキュリティフレームワーク(1.1 版)（NIST Cybersecurity Framework (Version 1.1)）
統一基準	政府機関等のサイバーセキュリティ対策のための統一基準（令和 3 年度版）
NIST	アメリカ国立標準技術研究所 National Institute of Standards and Technology

２サイバーセキュリティフレームワークの概要

２．１　サイバーセキュリティフレームワークの必要性

今日、サイバー空間は重要な公共空間であり、それなくしては我々の生活や経済活動は成り立たなくなっている。サイバー空間の拡大により生活の利便性は向上したが、その一方でそこで行われる攻撃や犯罪も増加している。特に近年は標的型攻撃のような特定の個人や組織を狙った攻撃や、国家に支援された犯罪集団による大規模分散型サービス不能（DDoS）攻撃など、サイバー空間における脅威の甚大化、被害の甚大化の一途をたどっている。

そのような環境の変化とは裏腹に、サイバー攻撃に対して「防御」を中心とした従来のセキュリティ態勢の構築が未だに続いている。しかしながら、昨今の高度化・複雑化するサイバー攻撃に対して、「防御」中心のサイバーセキュリティ対策だけでは、対処することが困難になってきている。そのため、サイバー攻撃は完全に防ぐことはできないという前提のもと、「防御」の対策だけではなく、サイバー攻撃を速やかに「検知」するとともに「対応」し、被害が発生した際には「復旧」するといったサイバーレジリエンスに関する対策にも注力すべきである。

サイバーセキュリティフレームワークはサイバーレジリエンスを含んだ包括的なサイバーセキュリティ態勢を構築するための代表的なフレームワークであり、サイバーセキュリティ態勢に必要な機能を定義したリスクベースアプローチのフレームワークである。また、業種業態、事業規模に問わず、幅広い組織で使えるような汎用性があるため、世界的に官民での活用が進んでいる。

２．２　サイバーセキュリティフレームワークの特徴

サイバーセキュリティフレームワークは組織のサイバーセキュリティリスクマネジメントを改善する目的で利用される。組織が直面するサイバーセキュリティリスクへの対応方針に応じてセキュリティ対策を継続的に改善するため、以下の３つの要素で構成されている。

（１）フレームワークコア（以下、「コア」という。）

（ア）すべての重要インフラ分野に共通するサイバーセキュリティ対策、期待される成果、適用可能な参考情報を定義したもの。

（イ）「識別」「防御」「検知」「対応」「復旧」の５つの機能に分類される。各機能の下には複数のカテゴリが存在し、各カテゴリはそれぞれ複数のサブカテゴリを有する。

（２）フレームワークインプリメンテーションティア（以下、「ティア」とい

う。）

（ア）組織におけるサイバーセキュリティリスクへの対応状況を評価する際の指標を定義したもの。

（イ）指標は 4 段階あり、次のとおり。

① ティア１：部分的である

② ティア２：リスク情報を活用している

③ ティア３：繰り返し適用可能である

④ ティア４：適応している

（3）フレームワークプロファイル（以下、「プロファイル」という。）

（ア）フレームワークのカテゴリ及びサブカテゴリに基づき、サイバーセキュリティリスクに対する期待される効果を現すもの。

（イ）サイバーセキュリティリスクへの対応状況として、「あるべき姿」と「現在の姿」をまとめたもの。

（ウ）「あるべき姿」の策定については、組織のビジネス上の要求、リスク許容度、割当可能なリソースに基づき、コアの機能、カテゴリ、サブカテゴリの到達地点を調整する。

２.３ コア -業種・業態を問わない、共通となるサイバーセキュリティ対策-

コアは、業種業態、企業規模に依存しない共通のサイバーセキュリティ対策を定義している。コアの構成は 5 つの機能、23 のカテゴリ、108 のサブカテゴリ、参考情報により構成されている。

1) 機能は、業種業態、企業規模に問わず実施すべきサイバーセキュリティ対策の最上位の概念であり、識別、防御、検知、対応、復旧の 5 機能が定義されている。

- 識別：組織の資産（情報システム、人、データ・情報など）、組織を取り巻く環境、重要な機能を支えるリソース、関連するサイバーセキュリティリスクを特定し理解を深める。
- 防御：重要サービスの提供が確実に行われるよう適切な保護対策を検討し実施する。
- 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。
- 対応：サイバーセキュリティインシデントに対処するための適切な対策を検討し実施する。
- 復旧：サイバーセキュリティインシデントにより影響を受けた機能

やサービスをインシデント発生前の状態に戻すための適切な対策を検討し実施する。これには、レジリエンスを実現するための計画の策定・維持も含む。

2) カテゴリは、機能を細分化しグループ化したものである。各機能に対して全 23 のカテゴリが紐付けられている。

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

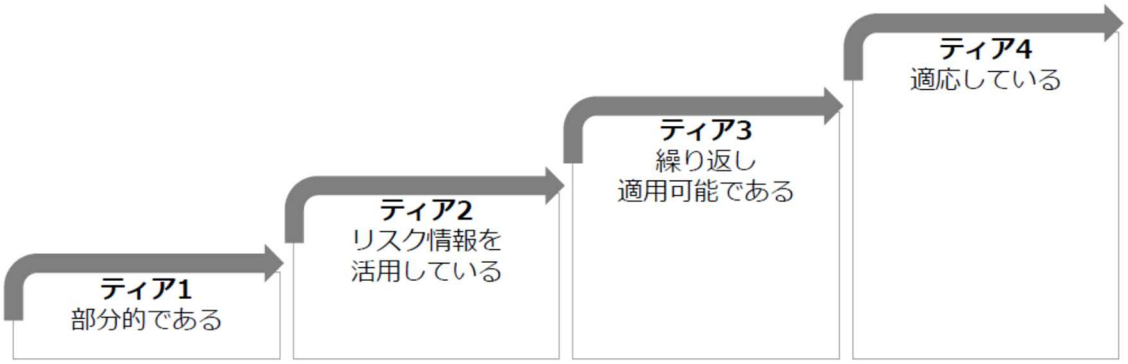
- サブカテゴリは、カテゴリを技術的観点、および管理的観点で更に細分化したもの。例えば資産管理（ID.AM）は次のようなサブカテゴリから構成されている。

カテゴリ	サブカテゴリ
資産管理（ID.AM）：自組織が事業目的を達成することを可能にするデータ、人員、デバイス、システム、施設が、識別され、組織の目的と自組織のリスク戦略における相対的な重要性に応じて管理されている。	ID.AM-1: 自組織内の物理デバイスとシステムが、目録作成されている。
	ID.AM-2: 自組織内のソフトウェアプラットフォームとアプリケーションが、目録作成されている。
	ID.AM-3: 組織内の通信とデータフロー図が、作成されている。
	ID.AM-4: 外部情報システムが、カタログ作成されている。
	ID.AM-5: リソース(例:ハードウェア、デバイス、データ、時間、人員、ソフトウェア)が、それらの分類、重要度、ビジネス上の価値に基づいて優先順位付けられている。
	ID.AM-6: 全労働力と利害関係にある第三者(例:サプライヤー、顧客、パートナー)に対してのサイバーセキュリティ上の役割と責任が、定められている。

- 参考情報は、サブカテゴリに関連するセキュリティの基準、ガイドラインやプラクティスをまとめたセクションである。次のような基準、ガイドライン、プラクティスとの関係が示されている。
  - ISO/IEC 27001:2013
  - NIST SP 800-53 rev4 連邦政府情報システム及び連邦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
  - CIS クリティカルセキュリティコントロール
  - COBIT 5
  - ISA/IEC 62443

２．４　ティア -対策の状況を数値化するための段階的な評価基準-

ティアは組織におけるサイバーセキュリティリスクへの対応状況を評価する際の指標を定義したものであり、ティア１からティア４までの 4 つの段階から構成されている。これは組織におけるサイバーセキュリティリスクへの対応状況がどの程度厳密で高度かを表すものであり、サイバーセキュリティ対策やサイバーセキュリティのリスク管理及び対処がどの程度導入されているかの判断を行うことにも活用できる。



ティア	説明
ティア 1：部分的である (Partial)	セキュリティ対策は経験に基づいて実施される。セキュリティ対策は組織として整備されておらず場当たり的に実施されている。
ティア 2：リスク情報を活用している (Ris Informed)	セキュリティ対策はセキュリティリスクを考慮して実施されているが、組織として方針や標準が定められてはいない、あるいは非公式に存在する。
ティア 3：繰り返し適用可能である (Repeatable)	セキュリティ対策は組織の方針・標準として定義、周知されており、脅威や技術の変化に伴い方針・標準は定期的に更新される。
ティア 4：適応している (Adoptive)	組織で標準化されたセキュリティ対策は、脅威や技術の変化、組織における過去の教訓やセキュリティ対策に関するメトリックスなどを参考に、継続的且つタイムリーに調整される。

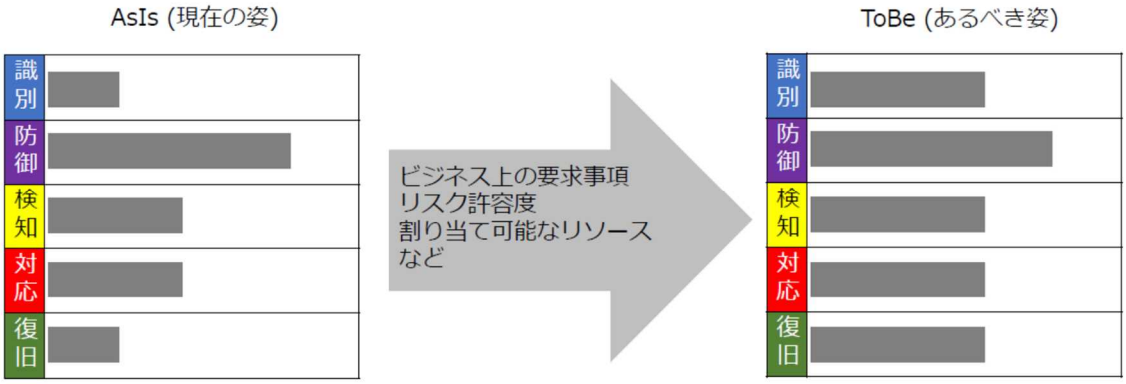
２．５　プロファイル –組織毎に調整された機能・カテゴリ・サブカテゴリ群–

プロファイルは、機能・カテゴリ・サブカテゴリについて組織毎に考慮すべき点を踏まえて調整し、整理したものである。組織毎に考慮すべき内容とは例えば、組織が事業を計画・実行する上で遵守すべき法令等の規制などの要求事項、組織や事業の特性を踏まえたリスク許容度、組織が保有する人的・金銭的・時間的リソースなどが考えられる。

また、プロファイルの作成にあたっては、昨今組織間の関係や構造が複雑化していることを踏まえると、組織に対して 1 対 1 でプロファイルを作成するのではなく、個別の事業部門ごとに、各々の要求を反映する形で複数のプロファイルを選択することも考えられる。

組織はプロファイルを用いることで、具体的なサイバーセキュリティ対策の「現在の姿」と「あるべき姿」を明らかにする事が可能となる。「あるべき姿」のプロファイルはサイバーセキュリティリスクマネジメントの目標を達成するために必要な成果を表している。プロファイルは組織が達成すべき要求事項の実現を支援し、組織の内外においてリスクコミュニケーションを行う上でも活用可能となる。サイバーセキュリティフレームワークにおいて、具体的なプロファイルの形は規定されていないが、本文書においては参考のため 3 章において一例を提示する。

また、「現在の姿」と「あるべき姿」についてプロファイルを比較することで、サイバーセキュリティマネジメント上の目標を達成する上で、解消が必要なギャップを明らかにすることが可能である。当該ギャップを解消するために必要な作業の優先順位付けを行うことが必要となるが、それは、組織における要求事項とリスクマネジメントプロセスにより導出されるものであり、同時に、ギャップの解消に必要なリソースの割り出しを可能にする。



２．６　諸外国における状況

2014 年に NIST が策定したサイバーセキュリティフレームワークは、2015 年には米国の組織の約 3 割で採用され、2020 年には半数に達すると推測されていた。米国以外の国においても、サイバーセキュリティフレームワークの活用事例は報告されており、国際的にも広く活用されているフレームワークであるといえる。例えば、2016 年にはイタリアにおいて、IACSF が開発され、これはサイバーセキュリティフレームワークを参考にしたものである。また、2017 年にはイスラエルにおいて国立サイバー総局（ICND）がサイバー防御方法論を公開しているが、これもサイバーセキュリティフレームワークを採用したものである。イギリスにおいても、2018 年に最小サイバーセキュリティ標準（MCSS）を導入しており、サイバーセキュリティフレームワークが採用され、英国向けに調整されている。

（参考）イスラエルにおける事例

イスラエル政府は 2002 年から重要インフラ（CII）のサイバーセキュリティを主導しており、2012 年には、官邸にサイバーセキュリティを推進する政府局を設立するなど、サイバーセキュリティ態勢を継続的に強化し、2017 年には、サイバーセキュリティフレームワークを採用した Israel Cyber Defense Methodology（ICDM)を策定した。

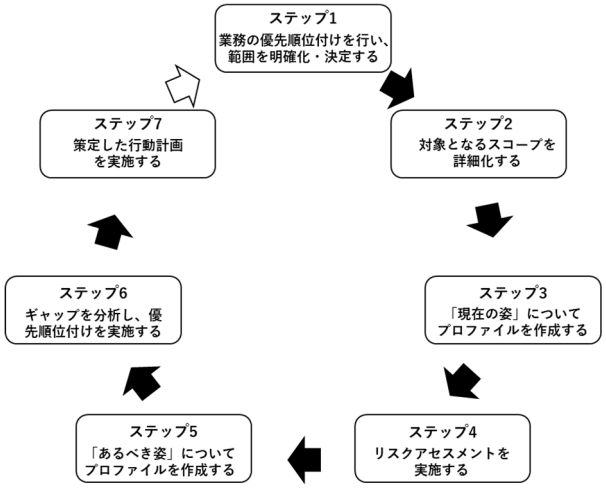
イスラエルでは、かねてより「特定」、「保護」、「復旧」による成果を重視していたが、「検知」、「対応」の検討を強化すべく、国際的な共通言語で構成され、国内外の標準に対応し、複数の規制に準拠することが可能な重要なフレームワークを求めており、結果として、サイバーセキュリティフレームワークの適用に至った。

ICDM においては、使いやすさを向上させるために多層構造をとっており、各セキュリティコントロールに対して、要件、説明と例、ベストプラクティスへのリンク、テンプレート、機密性/完全性/可用性との関係性、標準・規制との互換性などの情報を含んでいる。

ICDM は政府内のみならず、危険物を扱う企業に対してもその適用を義務づけており、健康、金融などの分野にも拡大しつつある。

3　サイバーセキュリティフレームワーク導入に向けたプロセス

本章では、各機関がサイバーセキュリティフレームワークを導入する上での具体的なプロセスを示す。紹介するプロセスは、次の 7 ステップから構成されており、各ステップでステークホルダーが担う役割と実施内容、実施する上で留意すべき点をまとめる。



3.1　準備編

本節では、組織がサイバーセキュリティフレームワークを導入するにあたり、事前に準備すべき事項を示す。

1)　コミュニケーションの調整機能を確保する

包括的なサイバーセキュリティ態勢を構築するためには、組織における意思決定者レベル、管理者レベル、業務の実施/運用者レベルでコミュニケーションを行い、リスクマネジメントに関する意思決定と対策の実施を図る必要がある。各レベル間でのコミュニケーションが円滑に実施されるよう、事務局的な位置づけを設置することで、意思決定者レベルから業務実施/運用者レベルまでの調整機能を確保することが重要となる。

2)　意思決定者を特定する

組織のリスクマネジメントプロセスにサイバーセキュリティリスクを組み込むことに関する意思決定を行い、リスクベースで業務全体の中から優先順位の高い業務を判断するなど実質的な意思決定が可能な環境を構築することが重要であり、そのための意思決定者を特定することが必要不可欠となる。

3)　情報収集機能を確保する

組織の資産に対する脅威と情報システム等の脆弱性を識別するために、脅威・脆弱性情報が利用可能である必要があるため、当該情報を継続的に入手するための体制を確保することが重要となる。一般的には、組織の CSIRT が平時の業務として当該機能を担うことが想定される。

３．２　導入編

本節では、各組織において政府統一基準や各組織のセキュリティポリシー等に従い、サイバーセキュリティリスクマネジメントプロセスが既に整備されていることを前提とし、既存プロセスを強化、改善する方法としてサイバーセキュリティフレームワークを導入する際の具体的なプロセスについて解説する。当該プロセスは一時的な活動ではなく、定期的かつ継続的に実施するものとして位置付けることで、サイバーセキュリティに関する継続的な改善が可能となる。

1)　業務の優先順位付けを行い、範囲を明確化・決定する

サイバーセキュリティフレームワークを導入し、サイバーセキュリティに関する改善を行う対象を業務単位で決定する。なお、行政サービスへの影響が軽微な業務については導入の優先順位を劣後させる、または導入の対象外とすることが考えられるが、それ以外は原則、各機関全体を対象とする。

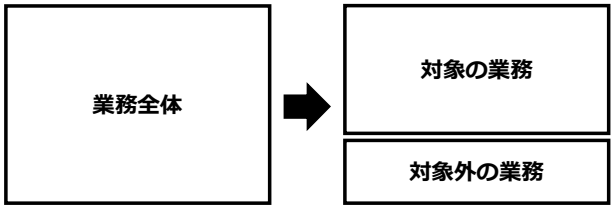


図 1　ステップ1

2)　対象となるスコープを詳細化する

1)において絞り込んだ対象業務に対して、関連する情報システムと資産、規制上の要求事項、全体的なリスクアプローチから脅威と脆弱性を特定する。

図 2　ステップ2

3)　「現在の姿」についてプロファイルを作成する

コアのサブカテゴリ単位で組織の現状について簡易分析を行い、現時点での達成状況を示すプロファイルを作成する。なお、既存のリスク評価結果が存在する場合、既存の評価項目とサイバーセキュリティフレームワークのサブカテゴリのマッピングを行うことなどにより、既存のリスク評価結果を活用することが考えられる。既存のリスク評価結果において、サイバーセキュリティフレームワーク上の項目が存在しない等の理由により、マッピングが困難な場合には、当該項目についてはサイバーセキュリティフレームワークのサブカテゴリに基づいてあらためて簡易分析を実施することが望ましい。

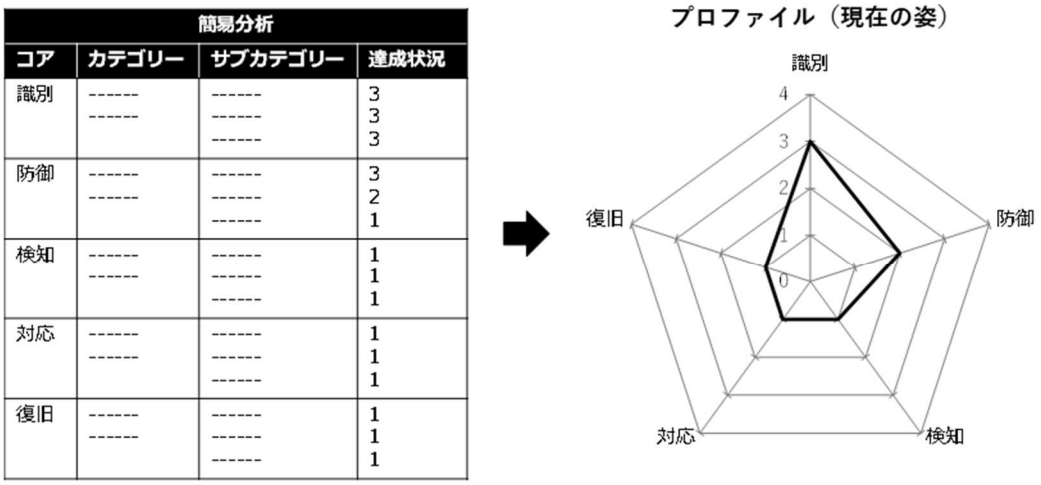


図 3　ステップ3

4)　リスクアセスメントを実施する

2)で特定した対象の情報システムとそれに関連する脅威、脆弱性からサイバーセキュリティ事案が発生する可能性とその影響、および自組織における重要システムを特定する。既存のリスクアセスメント結果が存在する場合、

当該アセスメント結果を活用することも考えられる。

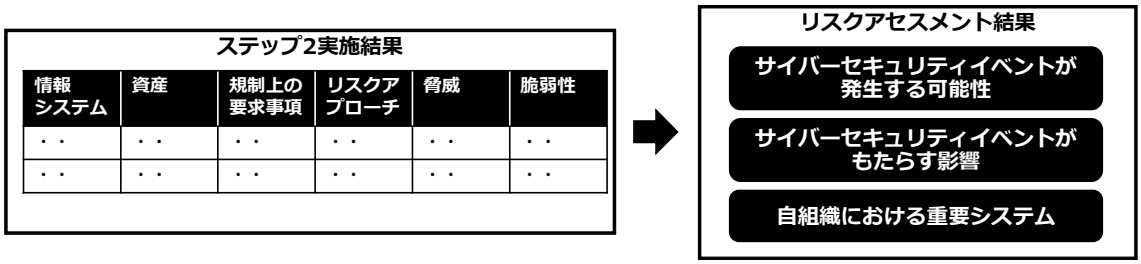


図 4　ステップ4

5)　「あるべき姿」についてプロファイルを作成する

4)の結果に基づき、保有する情報システムや資産を踏まえた目標のティアおよびプロファイルを決定する。ティア 3 は、一般的に「あるべき姿」を策定する上での 1 つの指標となると考えられるが、情報システムの重要性や、情報セキュリティ事案発生時の影響度やリスクの受容度に応じて、ティアは柔軟に設定することが可能である。

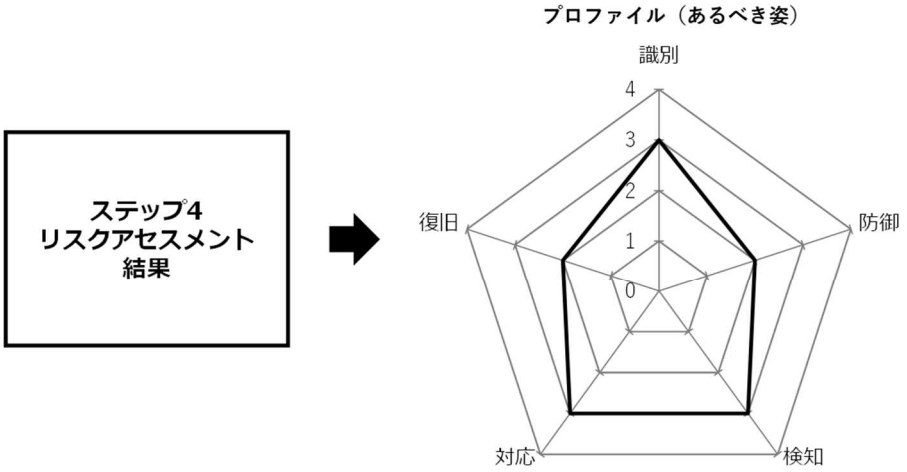


図 5　ステップ5

6)　「現在の姿」と「あるべき姿」についてギャップを分析し、優先順位付けを実施する

プロファイルについて、「現在の姿」と「あるべき姿」を比較し、両プロファイル間のギャップを分析する。「あるべき姿」のプロファイルを達成す

るために解消するべきギャップについて、何を取り組んでいくのか、優先順位をつけながら行動計画を策定する。

優先順位の検討にあたっては様々な視点で多角的にギャップを分析することが望ましい。例えば、セキュリティ対策を実施する上での実現可能性、人的・金銭的・時間的コスト、ギャップが引き起こすセキュリティリスク、既に計画・実施中のセキュリティ対策との親和性などの観点考えられる。また、同種の組織と比較を行う事で、自組織のセキュリティ対策の過不足を明らかにし、同種組織の標準的な水準を満たしていないセキュリティ対策を優先的に強化するという考え方もある。

行動計画は、サイバーセキュリティに係る意思決定を行う委員会等で審議し、組織の共通の課題として広く認識を図ることが重要である。

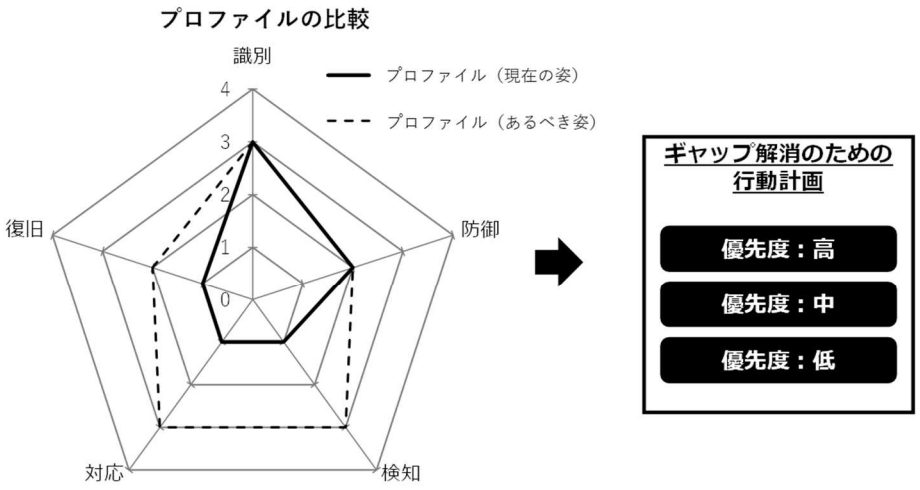


図 6　ステップ6

7)　策定した行動計画を実施する

6)において策定した行動計画に従い、サイバーセキュリティ対策に関する改善を行うための具体的な取り組みを実施する。また、計画の進行に伴い定期的かつ継続的に再評価を実施し、「現在の姿」のプロファイルを更新・把握することで、「あるべき姿」のプロファイルとの間のギャップが解消していくようフォローアップしていくことも重要である。再評価は外部環境（脅威や規制上の要求事項など）および内部環境（体制やシステムなど）に大きな変更があった場合、あるいは定期的実施の観点では少なくとも 1 年に 1 回以上実施する事が望ましい。

３．３　サイバーセキュリティフレームワーク導入時の留意点

1)　ティア 4 を組織の目標にする必要は無い

サイバーセキュリティフレームワークにおいては、最高位のティア 4 を全ての組織目標にする必要はなく、組織における業務や情報システムの重要性等に応じて、適切なティアを設定することが重要となる。サイバーセキュリティに関する取り組みが先進的な組織であっても、すべてのコアでティア 4 を達成することは困難であり、現実的には 3 かあるいはそれ以下の目標値が設定されることも少なくないと考えられる。したがって、サブカテゴリで示されるすべての管理策について網羅的に対応し、かつ、すべての管理策をティア 4 に設定するアプローチは現実的ではない。行動計画の実施フェーズにおいて、組織特性や求められるセキュリティ対策のレベル等を踏まえたうえで残存リスクについて、リスクを許容するのかどうか、あるいは代替策を講じるのかどうかなど、実現可能な対応を検討していくことが重要である。

2)フレームワークはツールとして活用し、既存プロセスを改善する

サイバーセキュリティフレームワークは、既存のサイバーセキュリティリスクマネジメントプロセスを改善するためのツールであり、サイバーセキュリティリスクマネジメントそのものを代替するものではないという点については留意する必要がある。すなわち、サイバーセキュリティフレームワークを導入する事で、政府統一基準や組織の情報セキュリティポリシーに従ったリスクマネジメントを実施することが不要となるわけではない。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マネジメントに関するベストプラクティスとしてのツールであり、既存のリスクマネジメントプロセスを補完する形で、現在から将来的にどのような形でサイバーセキュリティ対策を講じていけばよいのかどうかを明らかにしていくための取り組みの中で、採用する手段の１つであることを認識することが重要である。

3)外部評価を活用し、客観的な現状分析を行う

「現在の姿」をプロファイルする際に、自己評価を行う場合、近視眼的な評価結果となることは否めない。そのため、プロファイルを作成する際の簡易分析は、外部評価を活用することも考えられる。一般的に、外部評価を採用した場合、導出されるプロファイルは評価が低くなる傾向にある。

4)組織の特性に応じてコアやプロファイルを最適化する

サイバーセキュリティフレームワークで定めるコアは、あくまで重要イン

フラにおいて適用される汎用的な管理策であり、実際に組織で導入する際には、組織の特性を踏まえて管理策の最適化や、追加・削除を検討することが重要であることにも留意したい。当然、ティアやプロファイルにおいても組織特性を考慮した上で策定する必要がある。

４　サイバーセキュリティフレームワークと他の基準等との関係

政府機関においてはサイバーセキュリティ戦略本部により、政府機関等の情報セキュリティ水準を向上させるための統一的な枠組みとして、統一基準が定められており、政府機関等や政府機関等全体において統一基準に基づくサイバーセキュリティに係るPDCAサイクルを適切に運用することで、情報セキュリティの確保を図っている。

また、民間において広く活用されている、組織における情報セキュリティマネジメントシステムに関する国際規格であるISO/IEC27000シリーズが存在している。

これらの基準等はサイバーセキュリティフレームワークと共通点があるが、本節においては政府統一基準も含め、類似の情報セキュリティに関する基準等との関係について言及する。

４．１ 統一基準との関係

政府機関等が準拠すべきサイバーセキュリティに関する基準として、政府統一基準がサイバーセキュリティ基本法に基づき定められている。統一基準は政府機関等のサイバーセキュリティ水準を向上させることを目的に、情報セキュリティのベースラインや、高い水準の情報セキュリティを確保するための対策事項を規定しており、組織は PDCA サイクルの中でサイバーセキュリティを確保することが求められている。政府統一基準は、行政という特定の業態において、標準的な業務とそのリスクに応じた対策が策定されていることを考慮すれば、統一基準への準拠性評価により組織におけるサイバーセキュリティリスクアセスメントが可能である。

政府機関が自身のサイバーセキュリティ態勢を構築・改善する際、統一基準で定めるベースラインに準拠することは前提となるが、その際、サイバーセキュリティフレームワークを活用することで、サイバーセキュリティに係る 5 つの機能「識別」「防御」「検知」「対応」「復旧」の観点で、サイバーセキュリティ対策を捉えることが可能となる。各機関におけるサイバーセキュリティ態勢について、サイバーセキュリティフレームワークにおけるコアのカテゴリ及びサブカテゴリと照らし合わせ、どの程度達成されているかを検証することで、改善が必要なものを明確化し、組織におけるリソース分配の優先順位付けや対策実施時の取捨選択を行う際の情報として活用することが期待される。

４．２　その他の基準等との関係

サイバーセキュリティフレームワークとISO/IEC27000シリーズは、組織のサイバーセキュリティリスクマネジメントを改善するという目的において共通し

ている。ISO/IEC27000 シリーズは、情報セキュリティマネジメントシステムに関する規格群であり、電子情報のみならず、情報システム、記録媒体、紙や無形の情報も含めた、組織が保護すべき情報資産を管理するための枠組みを提供している。他方、サイバーセキュリティフレームワークは、情報技術、産業用制御システム、サイバーフィジカルシステム、或いは IoT といった重要インフラをサイバー攻撃から保護することに主な焦点を当てている。組織がリスクを識別、評価し、それに基づいてセキュリティ対策を選択し、優先順位を付け、導入し、継続的に改善するという一連のアプローチを提供している点では共通しているが、サイバーセキュリティフレームワークはその保護対象や脅威を具体化したものであるといえる。

また、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マネジメントを行うプロセスについて、具体的な手法を指定しておらず、手法の一例として、ISO31000,ISO/IEC27005,NIST SP800-39 等を示すにとどめている。これらのガイドラインでは、情報資産の重要度、脅威、脆弱性からリスクを分析し、対応、モニタリングする手法を示している。

また、他の基準等と比較し、サイバーセキュリティフレームワークは対応、復旧の領域においてより具体性を高めていることが特徴としてあげられる。これは、昨今よく言及されるように、サイバーセキュリティに対する脅威が高度化・複雑化すると共に、重要インフラの情報技術等への依存度が増していることを踏まえ、重要インフラがサイバーセキュリティの脅威に曝された場合においても、継続的な機能や障害発生時の早期復旧が重要であるという認識に基づくものだと考えられる。

参考資料１　サイバーセキュリティフレームワークと政府統一基準の対応関係

本文書では、サイバーセキュリティフレームワークの各カテゴリと政府統一基準の項番単位での対応関係を示すため、サイバーセキュリティフレームワークと政府統一基準の関係を表として整理した。政府機関等の各組織は、統一基準で定めるベースラインに準拠することが求められるが、サイバーセキュリティフレームワークを適切に導入することで、各組織におけるサイバーセキュリティ態勢を改善することが可能となる。

当該活動の中で、下表を活用する事でサイバーセキュリティフレームワークを導入する上で、各カテゴリの記載事項について、統一基準上の要求事項を参照しながら、カテゴリやサブカテゴリの内容を選択することが可能となる。

他方、サイバーセキュリティフレームワークはあらゆる業種・業態について、包括的なものではないため、政府機関等の各組織において、追加のカテゴリ、サブカテゴリ、参考情報を追加することも可能である。そのため、組織の特性に応じて追加のカテゴリ等が必要な場合は、適宜拡張して利用することを推奨する。

なお、サイバーセキュリティフレームワークコアの全容については、独立行政法人情報処理推進機構より公開されているもの[1]を参照されたい。

[1] 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　1.1 版　Core（https://www.ipa.go.jp/files/000071205.xlsx）

機能の識別子	機能	カテゴリの識別子	カテゴリ	政府統一基準 項番
ID	識別	ID.AM	資産管理	3.1.1 (1) (3) 5.1.1 (1) (2) 8.1.1 (1)
		ID.BE	ビジネス環境	2.1.2 (2) 5.3.1 (1) 7.3.2 (1)
		ID.GV	ガバナンス	2.1.1 (1) (2) (3) (4) (5) 2.1.2 (1) (2) 2.2.1 (1) (2) 2.4.1 (1) (2) 4.1.1 (1) 5.2.1 (1)
		ID.RA	リスクアセスメント	2.1.2 (1) 2.2.4 (2) 2.4.1 (1) (2) 5.2.1 (2) 6.2.1 (1) 6.2.4 (1)
		ID.RM	リスクマネジメント戦略	5.2.1 (1) 5.2.5 (1)
		ID.SC	サプライチェーンリスクマネジメント	4.1.1 (2) (3) 4.2.1 (1) (2) (3) (4) 4.2.2 (1) (2) 5.1.2 (1) 5.2.1 (3) (4) 5.2.2 (1) (3)

機能の識別子	機能	カテゴリの識別子	カテゴリ	政府統一基準 項番
PR	防御	PR.AC	アイデンティティ管理とアクセス制御	3.2.1 (1) (3) 5.2.2 (2) 6.1.1 (1) (2) 6.1.2 (1) 6.1.3 (1) 6.2.4 (1) 7.1.1 (1) 7.1.2 (1) 7.2.2 (1) 7.3.1 (1) (2) (4) 8.1.1 (3) (4) (5) (6) (8) 8.1.3 (1) (2) (3)
		PR.AT	意識向上およびトレーニング	2.2.3 (2)
		PR.DS	データセキュリティ	3.1.1 (4) (6) (7) (8) 5.2.1 (3) 5.2.4 (1) 6.1.5 (1) (2) 7.1.1 (3) (4) (5) 7.1.2 (1) (2) (3) 7.2.4 (1) 7.3.1 (1) (3) (4) 8.1.1 (2) (3) (6) 8.1.3 (2)

機能の識別子	機能	カテゴリの識別子	カテゴリ	政府統一基準 項番
		PR.IP	情報を保護するためのプロセスおよび手順	2.2.1 (1) 2.2.4 (1) 2.3.1 (2) (3) 3.1.1 (7) (8) 3.2.1 (1) 5.1.1 (1) (2) 5.2.2 (2) 5.3.1 (1) 6.1.1 (2) 6.1.3 (1) 6.2.1 (1) 6.2.2 (1) 6.2.4 (1) 7.1.1 (1) (2) (3) (4) (5) 7.1.2 (1) (2) (3) 7.1.3 (1) 7.2.2 (1) (2) 7.2.3 (1) 7.3.1 (3) 7.3.2 (1) 8.1.2 (1)
		PR.MA	保守	5.2.3 (1) 6.1.4 (1) 7.3.1 (1)
		PR.PT	保護技術	3.1.1 (3) (4) (6) 6.1.4 (1) 7.1.1 (2) (5) 7.2.3 (1) (2) 7.2.4 (1) 7.3.1 (1) (2) (4) 8.1.1 (1) (3) 8.1.2 (1)

機能の識別子	機能	カテゴリの識別子	カテゴリ	政府統一基準 項番
DE	検知	DE.AE	異常とイベント	2.2.4 (2) 5.2.1 (2)
		DE.CM	セキュリティの継続的なモニタリング	6.1.4 (1) 6.2.2 (1) 6.3.1 (2) 7.1.1 (1) (2) (4) (5) 7.1.2 (2) 7.2.2 (2) 7.3.1 (1) 7.3.2 (2) 8.1.1 (3) (4) (7)
		DE.DP	検知プロセス	8.1.1 (7) 8.1.2 (1)
RS	対応	RS.RP	対応計画の作成	2.2.4 (1)
		RS.CO	コミュニケーション	2.2.4 (2)
		RS.AN	分析	2.2.4 (2) 6.2.1 (1) 7.2.2 (2)
		RS.MI	低減	2.2.4 (2) 5.1.1 (1) (2) 6.2.1 (1)
		RS.IM	改善	2.2.4 (3)
RC	復旧	RC.RP	復旧計画の作成	2.2.4 (2)

機能の識別子	機能	カテゴリの識別子	カテゴリ	政府統一基準 項番
		RC.IM	改善	2.4.1 (1) (2)
		RC.CO	コミュニケーション	2.2.4 (2)

参考資料２　参考文献

(1) National Institute of Standards and Technology - Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
(2) National Institute of Standards and Technology - Success Story: Israel National Cyber Directorate Version 2.0 https://www.nist.gov/cyberframework/success-stories/israel-national-cyber-directorate-version-20
(3) IPA – 重要インフラのため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 https://www.ipa.go.jp/files/000071204.pdf
(4) CIS-Sapienza, Cybersecurity National Lab – National Framework for Cyber Security https://www.cybersecurityframework.it/
(5) UK Government – The Minimum Cyber Security Standard https://www.gov.uk/government/publications/the-minimum-cyber-security-standard