Check for updates

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

NIST Cybersecurity Framework 2.0:
Quick-Start Guide for Creating and Using Organizational Profiles

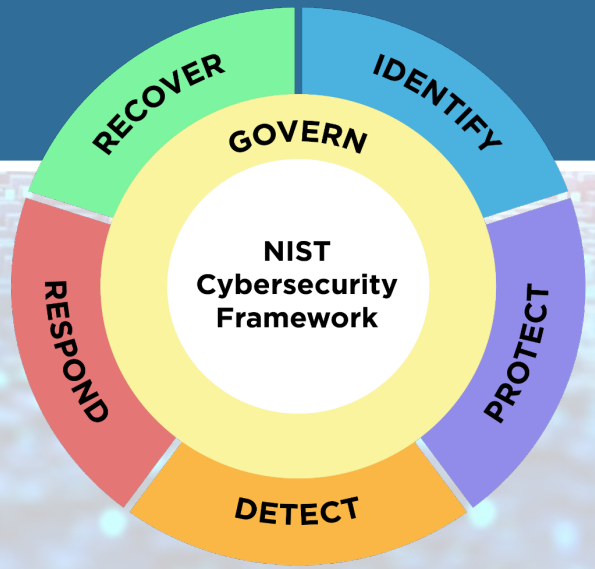
U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST Special Publication
NIST SP 1301
https://doi.org/10.6028/NIST.SP.1301
February 2024

Check for updates

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

NIST サイバーセキュリティ フレームワーク 2.0:
組織プロファイルの作成と使用のための
クイックスタートガイド



This translation is not an official U.S. Government or NIST translation.
The U.S. Government does not make any representations as to the accuracy of the translation.
The official English language version of this publication is available free of charge from the National Institute of Standards and Technology (NIST):
https://www.nist.gov/cyberframework

本翻訳は米国政府または NIST の公式な翻訳ではない。米国政府は、本翻訳の正確性に関していかなる表明も行っていない。
本出版物の公式な英語版は米国国立標準技術研究所（NIST：National Institute of Standards and Technology）から無料で入手可能である。
https://www.nist.gov/cyberframework

U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST Special Publication
NIST SP 1301
https://doi.org/10.6028/NIST.SP.1301
2024年2月

NIST CSF 2.0: CREATING AND USING ORGANIZATIONAL PROFILES

A QUICK START GUIDE

INTRODUCTION

Drive Progress Over Time with Organizational Profiles

An ***Organizational Profile*** describes an organization's current and/or target cybersecurity posture in terms of cybersecurity outcomes from the Cybersecurity Framework (CSF) Core. Organizational Profiles are used to understand, tailor, assess, and prioritize cybersecurity outcomes based on an organization's mission objectives, stakeholder expectations, threat landscape, and requirements. The organization can then act strategically to achieve those outcomes. These Profiles can also be used to assess progress toward targeted outcomes and to communicate pertinent information to stakeholders.

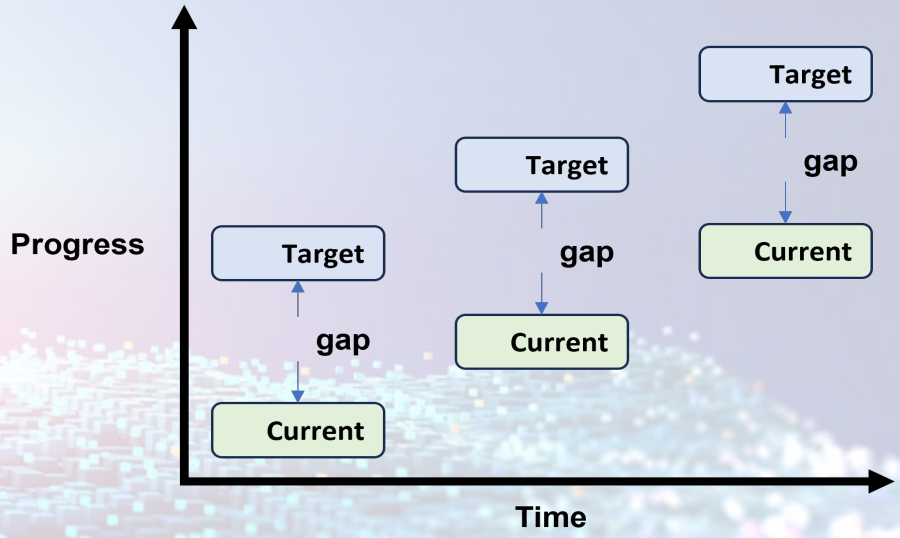
Organizational Profiles can be categorized as:

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

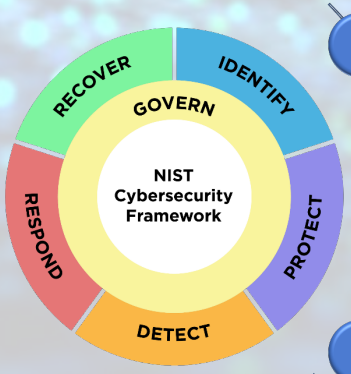
Create and Use Organizational Profiles with the CSF Five-Step Process

CSF 2.0 describes a five-step process for creating and using Organizational Profiles. More specifically, the process compares an aspirational Target Profile to an assessed Current Profile. Then, a gap analysis is performed, and an action plan is developed and implemented. This process naturally leads to refinements in the Target Profile to be used during the next assessment.

Drive Progress Over Time



Create and Use Organizational Profiles



1. Scope the Organizational Profile
2. Gather needed information
3. Create the Organizational Profile
4. Analyze gaps and create an action plan
5. Implement action plan and update Profile

Repeat...

NIST CSF 2.0: 組織プロファイルの作成と使用

クイックスタートガイド

はじめに

組織プロファイルを使用して時間の経過に伴った進捗を促進する

組織プロファイルは、サイバーセキュリティフレームワーク（CSF）コアのサイバーセキュリティ成果の観点から、組織の現在、及び／又は目標のサイバーセキュリティ態勢を記述したものである。組織プロファイルは、組織のミッションの目的、ステークホルダーの期待、脅威状況、要件に基づいて、サイバーセキュリティの成果を理解し、テーラリングし、アセスメントし、優先順位を付けるために使用される。その結果、組織は、これらの成果を達成するために戦略的に行動することができる。これらのプロファイルは、目標とする成果に向けた進捗状況をアセスメントし、ステークホルダーに適切な情報を伝達するためにも使用できる。

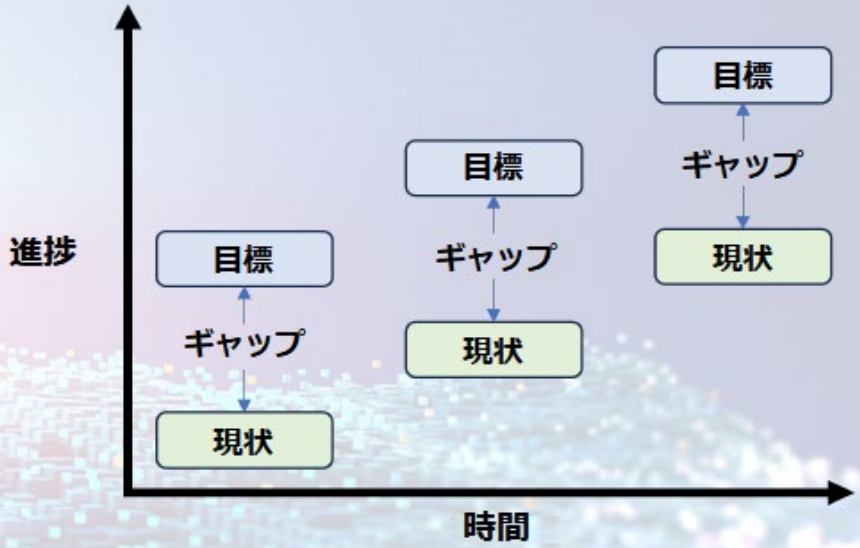
組織プロファイルは、次のように分類することができる。

- **現状プロファイル**：組織が現在達成しているCSF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付ける。
- **目標プロファイル**：組織がサイバーセキュリティリスクの管理目標を達成するために選択し、優先順付けした望ましいCSFの成果を特定する。目標プロファイルは、新たな要件、新技術の採用、及び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。

CSFの5つのステッププロセスを使用して組織プロファイルを作成し使用する

CSF 2.0は、組織プロファイルを作成して使用するための5つのステッププロセスを説明している。具体的には、このプロセスでは、所望の目標プロファイルをアセスメントされた現状プロファイルと比較する。その後、ギャップ分析を行い、行動計画を策定し、実装する。このプロセスは、必然的に、次回のアセスメントで使用する目標プロファイルの改良につながる。

時間の経過に伴った進捗を促進する



組織プロファイルの作成と使用

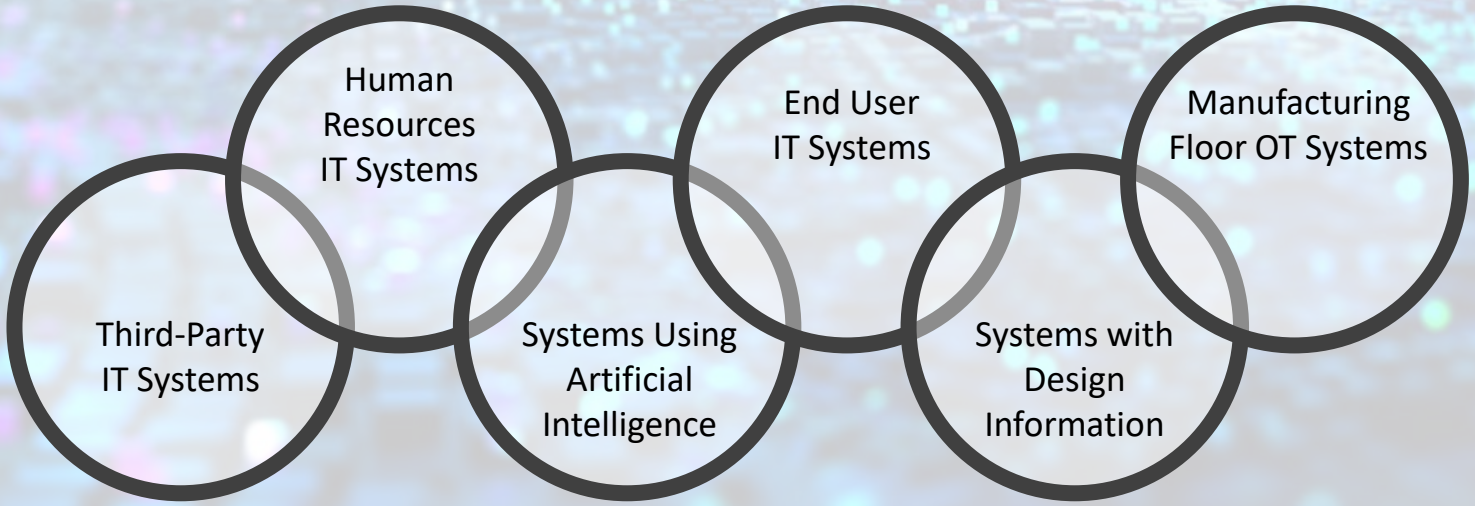
NIST CSF 2.0: CREATING AND USING ORGANIZATIONAL PROFILES

A QUICK START GUIDE

SCOPE THE ORGANIZATIONAL PROFILE

The scope defines the high-level facts and assumptions on which the Profiles will be based. You can have as many Organizational Profiles as desired, each with a different scope. Questions to answer as you scope your Profile include:

- What's the reason for creating the Organizational Profile?
- Will the Profile cover the entire organization? If not, which of the organization's divisions, data assets, technology assets, products and services, and/or partners and suppliers will be included?
- Will the Profile address all types of cybersecurity threats, vulnerabilities, attacks, and defenses? If not, which types will be included?
- Which individuals or teams will be responsible for developing, reviewing, and operationalizing the Profile?
- Who will be responsible for setting expectations for actions to achieve the target outcomes?



Organizational Profile Facts

Ways to Think about Profiles

A given organization may wish to use several Profiles.

Each Profile can have a distinct scope based on factors like:

- technology category (IT, OT)
- data types (PII, PHI, PCI)
- users (employees, third-parties)

The scope of a Profile determines the *applicability* of a given CSF outcome.

It may be helpful to combine two or more Profiles when scopes overlap.

NIST CSF 2.0: 組織プロファイルの作成と使用

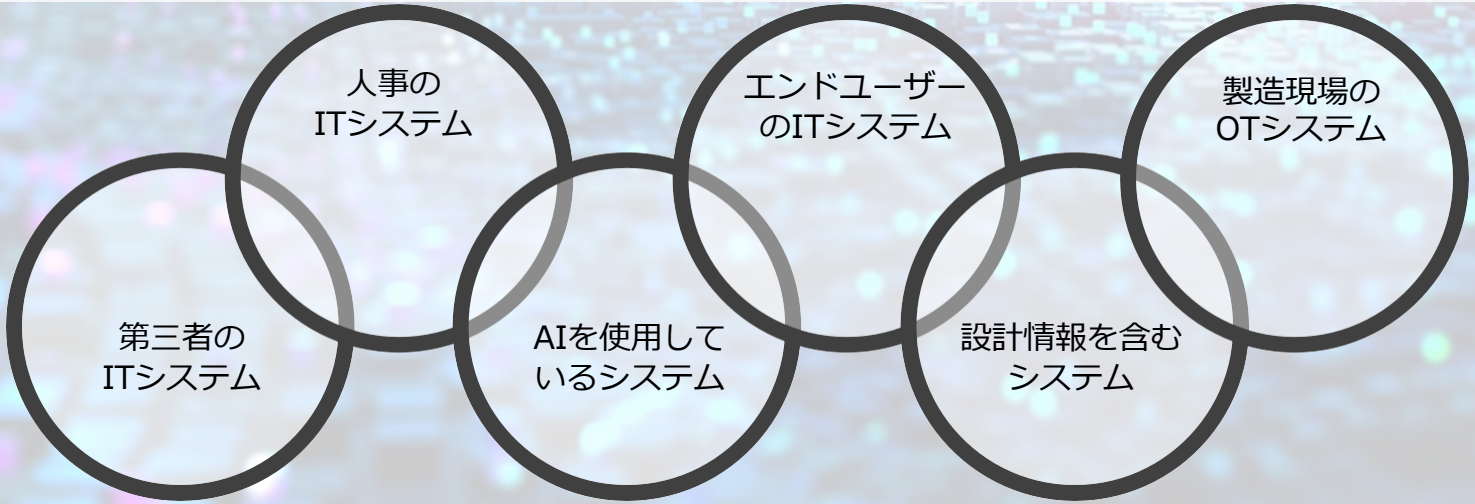
クイックスタートガイド

組織プロファイルの対象範囲を定める

プロファイルの基礎となるハイレベルの事実及び仮定を定義し、対象範囲を定める

組織プロファイルはいくつでも作成することができ、それぞれに異なる対象範囲を定めることができる。プロファイルの対象範囲を定める際には、次のような質問に回答する。

- 組織プロファイルを作成する理由は何か？
- プロファイルは組織全体をカバーしているか？そうでない場合は、組織のどの部門、データ資産、技術資産、製品及びサービス、及び／又はパートナーとサプライヤが含まれるか？
- プロファイルはあらゆる種類のサイバーセキュリティの脅威、脆弱性、攻撃、及び防御に対応しているか？そうでない場合は、どの種類が含まれるか？
- プロファイルを策定し、レビューし、運用する責任を負うのは、どの個人又はチームか？
- 目標の成果を達成する責任を負うのは誰か？



組織プロファイルの実際

プロファイルについての考え方

ある組織では、複数のプロファイルの使用を望む場合がある。

各プロファイルは、次のような要因に基づいて異なる対象範囲を定めることができる。

- 技術カテゴリー (IT, OT)
- データの種類 (PII, PHI, PCI)
- ユーザー (従業員、第三者)

プロファイルの対象範囲は、特定のCSFの成果の**適用可能性**を決定する。

対象範囲が重複する場合は、2つ以上のプロファイルを組み合わせると有用である可能性がある。

NIST CSF 2.0: CREATING AND USING ORGANIZATIONAL PROFILES

A QUICK START GUIDE

GATHER NEEDED INFORMATION

Examples of information may include organizational policies, risk management priorities and resources, cybersecurity requirements and standards... The sources of information needed will depend on the use case, the elements that the Profiles will capture, and the level of detail desired. Common sources of information include:

1. Community Profiles

A ***Community Profile*** is a baseline of CSF outcomes created and published to address *shared interests and goals among a number of organizations*. A Community Profile is typically intended for a particular sector or subsector, technology, threat type, or other use case.

An organization can use a Community Profile as the basis for its own Target Profile by copying the Community Profile into an Organizational Profile. A Community Profile can be adapted by:

- Adjusting the priorities of particular CSF outcomes
- Adding organization-specific Subcategories, Informative References, or implementation guidance

See *A Guide to Creating CSF 2.0 Community Profiles* for more information on creating and using Community Profiles.

2. NIST Organizational Profile Template

NIST provides a **CSF Organizational Profile template** as a Microsoft Excel spreadsheet. You can download it and fill it in to create Current and Target Profiles for your organization. The template facilitates side-by-side comparison of Current and Target Profiles to identify and analyze gaps. You can find the template on the CSF 2.0 website.

Prioritization

The Defining Feature of a Profile

The central notion of a Target Profile is to determine differing priorities for applicable CSF outcomes. Priorities help you determine parts of your cybersecurity program that should be resourced more, or less. Cybersecurity priorities are driven by strategic objectives, laws, regulations, and risk responses. To learn more, see SP 800-37 about organization-wide risk management tasks in the *Prepare Step*. IR 8286B offers information about how the CSF Core supports risk response decisions.

NIST CSF 2.0: 組織プロファイルの作成と使用

クイックスタートガイド

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及びリソース、サイバーセキュリティ要件及び標準などが考えられる。

必要な情報源は、ユースケース、プロファイルがキャプチャする要素、及び希望する詳細レベルによって異なる。一般的な情報源は、次の通り。

1. コミュニティプロファイル

コミュニティプロファイルは、多くの組織間で共通の利害及び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である。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を対象としている。

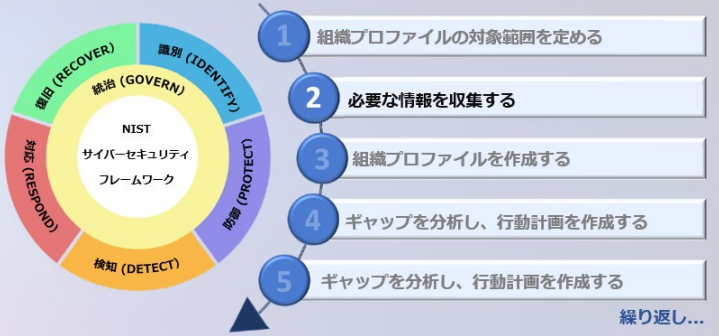
組織は、コミュニティプロファイルを組織プロファイルにコピーすることによって、コミュニティプロファイルを自らの目標プロファイルの基礎として使用することができる。コミュニティプロファイルは、次の方法で適用できる。

- CSFの成果の優先順位を調整する。
- 組織固有のサブカテゴリー、参考情報、又は実装ガイダンスを追加する。

コミュニティプロファイルの作成と使用の詳細については、*A Guide to Creating CSF 2.0 Community Profiles* を参照。

2. NIST 組織プロファイルのテンプレート

NISTは、**CSF 組織プロファイルのテンプレート** を Microsoft Excel スプレッドシートとして提供している。このテンプレートをダウンロードし、記入することで、組織の現状プロファイルと目標プロファイルを作成することができる。テンプレートは、ギャップを識別し分析するために、現状プロファイルと目標プロファイルを並べて比較する一助となる。CSF 2.0のウェブサイトからテンプレートを入手できる。



優先順位付け

プロファイルの定義的特徴

目標プロファイルの中心的な概念は、適用可能なCSFの成果に対して異なる優先順位を決定することである。優先順位は、サイバーセキュリティプログラムのうち、より多くのリソースを投入することが望ましい部分と、より少ないリソースを投入することが望ましい部分を決定するのに役立つ。
サイバーセキュリティの優先順位は、戦略的目的、法律、規制、及びリスク対応によって決まる。詳細については、準備ステップにおける組織全体のリスクマネジメントタスクに関する SP 800-37 を参照のこと。
IR 8286B では、CSFコアがリスク対応の決定をどのようにサポートするかについての情報を提供している。

NIST CSF 2.0: CREATING AND USING ORGANIZATIONAL PROFILES

A QUICK START GUIDE

CREATE THE ORGANIZATIONAL PROFILE – PART 1

Determine what types of supporting information each Profile should include for the selected CSF outcomes... Steps for creating an Organizational Profile are:

3a: Download the latest CSF Organizational Profile template spreadsheet and customize as desired.

3b: Include cybersecurity outcomes that apply to your use case, and document rationales as needed.

3c: Document current cybersecurity **Practices** in the Current Profile columns. More detailed entries may provide better insights for later steps.

3d: Document cybersecurity **Goals** and the plans for achieving them in the Target Profile columns. Entries may be based on CSF Informative References, new cybersecurity requirements, new technologies, and trends in cyber threat intelligence.

3e: Note the importance of each Goal using the **Priority** field.

CSF Outcomes		Current Profile			Target Profile	
Identifier	**Description**	**Practices**	**Status**	**Rating**	**Priority**	**Goals**
The identifiers and descriptions from the CSF Core – Functions, Categories, Subcategories. You can also add your own outcomes to address your organization's unique risks and requirements.		Policies, processes, procedures and other activities related to an outcome. May include artifacts that contain evidence of achieving an outcome.	The current state or condition of an outcome, such as whether it is being achieved and to what degree.	An assessment or evaluation of current practices using scales such as: • high/medium/low • 1-5 • 0-100%, • red/yellow/green	The relative importance of an outcome using scales such as: • Low/Medium/High • 1/2/3/4/5 • rankings (1, 2, 3…)	Such as: • Policies, Processes, and Procedures • Roles and Responsibilities Selected from: • Informative References - standards, guidance, and best practices

NIST CSF 2.0: 組織プロファイルの作成と使用

クイックスタートガイド

組織プロファイルを作成する – PART 1

選択したCSFの成果に関して、各プロファイルに含めることが望ましいサポート情報の種類を決定する。

組織プロファイルの作成ステップは以下の通りである。

3a: 最新の CSF 組織プロファイルのテンプレート・スプレッドシートをダウンロードし、必要に応じてカスタマイズする。

3b: ユースケースに適用するサイバーセキュリティの成果を含め、必要に応じて根拠を文書化する。

3c: 現在のサイバーセキュリティの**プラクティス**を 現状プロファイル 列に記入する。より詳細に記入することで、後のステップでより良い知見が得られる可能性がある。

3d: サイバーセキュリティの**ゴール**とそれを達成するための計画を、目標プロファイル 列に記入する。記入内容は、CSF 参考情報、新たなサイバーセキュリティ要件、新たな技術、及びサイバー脅威インテリジェンスの動向に基づく場合がある。

3e: **優先順位** 欄を使用して、各目標の重要性に言及する。

CSF の成果		現状プロファイル			目標プロファイル	
識別子	**説明**	**プラクティス**	**現状**	**評価**	**優先順位**	**ゴール**
CSF コアの識別子と説明 – 機能、カテゴリー、サブカテゴリー。組織固有のリスク及び要件に対応するために、独自の成果を追加することもできる。		成果に関するポリシー、プロセス、手順、及びその他の活動。成果達成の証拠を含む成果物を含む場合もある。	成果が達成されているかどうか、どの程度達成されているかなど、成果の現在の状態又は状況。	以下のような尺度を使用した、現在のプラクティスのアセスメント又は評価。 • 高／中／低 • 1-5 • 0-100%, • 赤／黄／緑	以下のような尺度を使用した、成果の相対的な重要性。 • 低／中／高 • 1／2／3／4／5 • ランキング (1, 2, 3…)	• ポリシー、プロセス、及び手順 • 役割及び責任 など 以下から選択 • 参考資料 – 標準、ガイダンス、ベストプラクティス

NIST CSF 2.0: CREATING AND USING ORGANIZATIONAL PROFILES

A QUICK START GUIDE

CREATE THE ORGANIZATIONAL PROFILE – PART 2

The table below shows a notional example of a single row from an Organizational Profile. This is meant for illustrative purposes only. Here are some tips drawn from the example:

- Add and remove columns from the Organizational Profile template to suite your needs. The CSF encourages users to record whatever information is significant and to use whatever format they prefer.
- The columns do not have to be the same for the Current Profile and the Target Profile.
- Include Informative References to understand differences between Practices and Goals. This example shows SP 800-53 controls in the square brackets.

CSF Outcomes		Current Profile			Target Profile	
Identifier	**Description**	**Practices**	**Status**	**Rating**	**Priority**	**Goals**
PR.PS-01	Configuration management practices are established and applied	Policy: Configuration Management policy version 1.4, last updated 10/14/22. Defines the configuration change control policy [**CM-1**]. Procedures: System owners and technology managers informally implement configuration management practices. Change control processes are not consistently followed. The CIO specifies configuration baselines [**CM-2**] for the IT platforms and applications most widely used within the organization, but baseline use is not monitored or enforced consistently across the organization.	Configuration management is partially implemented within the organization. Some systems do not follow available baselines and other systems do not have baselines, so they may have weak configurations that make them more susceptible to misuse and compromise. Unauthorized changes may go undetected. Some changes are not tested or tracked.	3 *out of 5*	High	Policy: The Configuration Management policy requires configuration baselines to be specified, used, enforced, and maintained for all commodity technologies used by the organization. The policy requires change control processes to be followed for all technologies within the organization [**CM-1**]. Procedures: Each division of the organization has a configuration management plan [**CM-9**], as well as maintains, implements, and enforces configuration baselines [**CM-2**] and settings [**CM-6**] for their systems. Baselines are applied to all systems before production release. All systems are continuously monitored for unexpected configuration changes, and tickets are automatically generated when deviations from baselines occur. Designated parties review change requests and corresponding impact analyses [**CM-4**] and approve or deny each [**CM-3**].

NIST CSF 2.0: 組織プロファイルの作成と使用

クイックスタートガイド

組織プロファイルを作成する – PART 2

以下の表は、組織プロファイルの単一行の概念的な実例を示している。

これは説明のみを目的としている。この例から得られる助言を以下に示す。

- 必要に応じて、組織プロファイルのテンプレートから列を追加したり削除したりする。CSFは、重要な情報は何でも記録し、好きなフォーマットを使用することを推奨している。
- 列は、現状プロファイルと目標プロファイルで同じである必要はない。
- プラクティスとゴールの違いを理解するための参考資料を含める。この例では、括弧内に SP 800-53 の管理策が示されている。

CSF の成果		現状プロファイル			目標プロファイル	
識別子	**説明**	**プラクティス**	**現状**	**評価**	**優先順位**	**ゴール**
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。	ポリシー: 構成管理ポリシー バージョン 1.4（更新日 2022年10月14日）。 構成変更の管理ポリシーを定義している [**CM-1**]。 手順: システム所有者及び技術マネージャーが、構成管理のプラクティスを非公式に実装している。変更管理策が一貫して守られていない。CIOが、組織内で最も広く使用されているITプラットフォーム及びアプリケーションのベースライン [**CM-2**] を定義しているが、ベースラインの使用は組織全体で一貫して監視又は実施されていない。	構成管理が、組織内で部分的に実装されている。一部のシステムは適用可能なベースラインに従っておらず、その他のシステムにはベースラインがないため、誤用や侵害を受けやすい脆弱な構成になっている可能性がある。認可されていない変更が、検出されない可能性がある。一部の変更は、テスト又は追跡されていない。	3 5段階評価	高	ポリシー: 構成管理ポリシーでは、組織が使用するすべての汎用技術について、構成ベースラインを規定し、使用し、実施し、維持することを求めている。このポリシーは、組織内のすべての技術について、変更管理ポリシーに従うことを求めている [**CM-1**]。 手順: 組織の各部門は、構成管理計画 [**CM-9**] を持つとともに、そのシステムの構成ベースライン [**CM-2**] 及び設定 [**CM-6**] を維持し、実装し、実施する。ベースラインは、本番リリース前にすべてのシステムに適用される。すべてのシステムは、予期しない構成変更について継続的に監視され、ベースラインからの逸脱が発生すると自動的にチケットが生成される。指定された関係者は、変更要求及びそれに対応するインパクトの分析 [**CM-4**] をレビューし、それぞれを承認または拒否する [**CM-3**]。

NIST CSF 2.0: CREATING AND USING ORGANIZATIONAL PROFILES

A QUICK START GUIDE

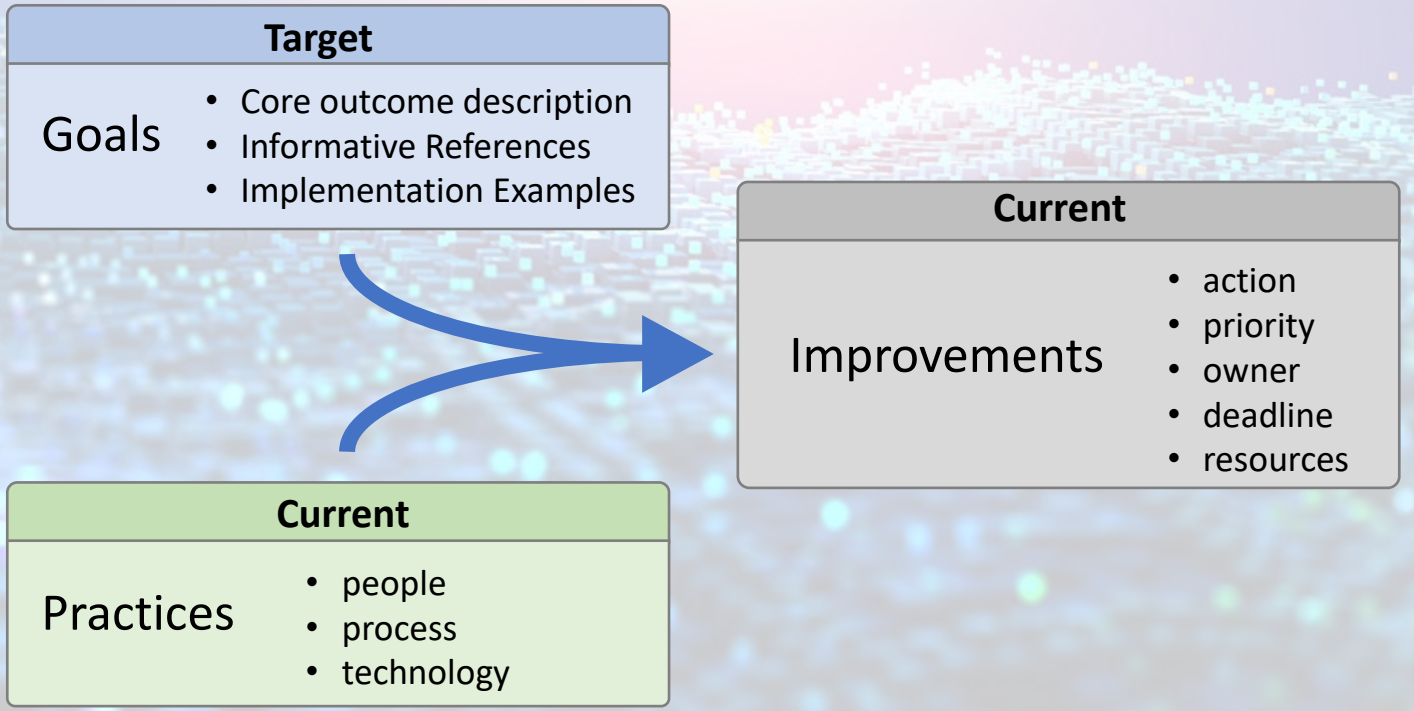
ANALYZE GAPS AND CREATE AN ACTION PLAN – PART 1

Identifying and analyzing the differences between the Current and Target Profiles enables an organization to find gaps and develop a prioritized action plan for addressing those gaps. Using Profiles in this manner helps your organization make better-informed decisions about how to improve cybersecurity risk management in a prioritized and cost-effective manner.

Step 4a

How to Analyze Gaps

Compare and contrast your current **practices**, across people, process, and technology, to the best practices described in CSF outcome descriptions, Informative References, and Implementation Examples. With those **goals** in mind, make observations about differences and document those items as candidate improvements.



Step 4b

How to Create Action Plans

The action plan is a list of pending **improvements** for your cybersecurity program. In addition to the Organizational Profile gap analysis, the action plan should consider mission drivers, benefits, risks, and necessary resources (e.g., staffing, funding). Action plans should have all the essential items in the graphic (left).

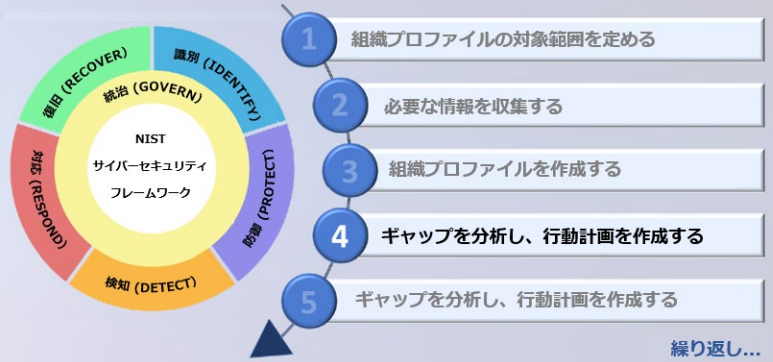
NIST CSF 2.0: 組織プロファイルの作成と使用

クイックスタートガイド

ギャップを分析し、行動計画を作成する – PART 1

現状プロファイルと目標プロファイルの差異を識別して分析することで、組織はギャップを発見し、そのギャップに対応するための優先順を付けた行動計画を策定することができる。

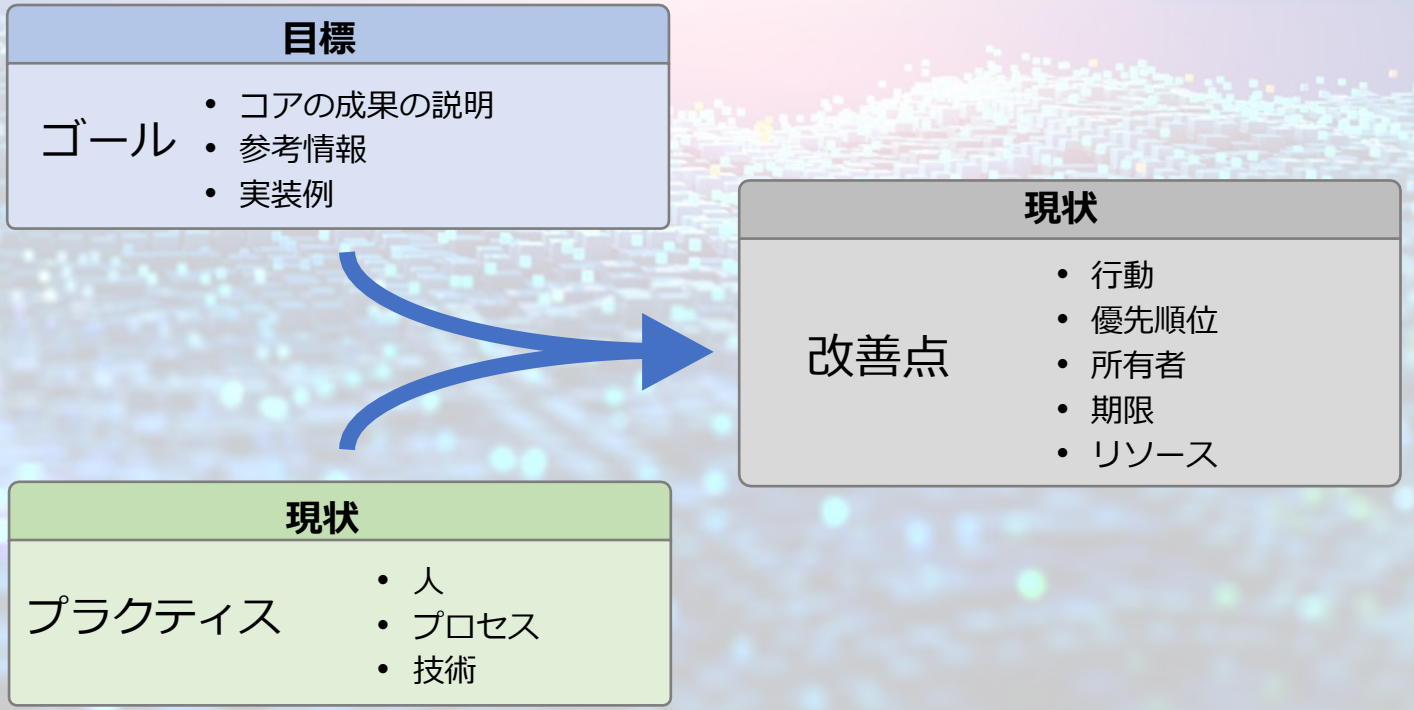
このようにプロファイルを使用することで、優先順位付けされた費用対効果の高い方法でサイバーセキュリティリスクマネジメントを改善する方法について、組織はより良い情報に基づいた意思決定を行うことができる。



ステップ 4a

ギャップの分析方法

人、プロセス、及び技術にわたる現在の**プラクティス**を、CSFの成果に関する記述、参考情報、及び実装例に記載されているベストプラクティスと比較する。これらの**ゴール**を念頭に置き、相違点について観察し、それらの項目を改善候補として文書化する。



ステップ 4b

行動計画の作成方法

行動計画は、サイバーセキュリティプログラムの保留中の**改善点**のリストである。組織プロファイルのギャップ分析に加え、行動計画では、ミッションの推進要因、メリット、リスク、及び必要なリソース（例えば、人員配置、資金調達）を考慮することが望ましい。行動計画は、左の図に示す必須項目がすべて含まれていることが望ましい。

NIST CSF 2.0: CREATING AND USING ORGANIZATIONAL PROFILES

A QUICK START GUIDE

ANALYZE GAPS AND CREATE AN ACTION PLAN – PART 2

Identifying and analyzing the differences between the Current and Target Profiles enables an organization to find gaps and develop a prioritized action plan for addressing those gaps. The CSF provides links to tools, controls, and implementation resources that will help you with analyzing gaps [**Step 4a**] and creating action plans [**Step 4b**]. A recommended approach for developing action plans is to use the NIST CSF 2.0 Reference Tool to follow the references from your Target Profile's pertinent Subcategories to the associated NIST SP 800-53 controls.

What Best Practices to Use

Informative References: relationships between the Core and various best practices, including standards, guidelines, regulations, and other resources. References help inform how an organization may achieve the CSF outcomes. They also help connect desired outcomes to other common cybersecurity documents, such as ISO/IEC 27001 and SP 800-53 which provides a catalog of security and privacy controls.

How to Implement Best Practices

Implementation Examples: notional descriptions of ways CSF outcomes can be fulfilled. The examples are not a comprehensive list of *all* actions that could be taken by an organization, nor are they a *baseline* of required actions; they are helpful ideas to get organizations thinking about concrete steps. The NIST CSF 2.0 Reference Tool allows users to explore the full CSF 2.0 Core and download in Excel and JSON formats.

Example of an Implementation Example

An Excerpt from the NIST CSF 2.0 Reference Tool

Subcategory

PR.PS-01: Configuration management practices are applied (formerly PR.IP-01, PR.IP-03, PR.PT-02, PR.PT-03)

Implementation Examples

Ex1: Establish, test, deploy, and maintain hardened baselines that enforce the organization's cybersecurity policies and provide only essential capabilities (i.e., principle of least functionality)

Ex2: Review all default configuration settings that may potentially impact cybersecurity when installing or upgrading software

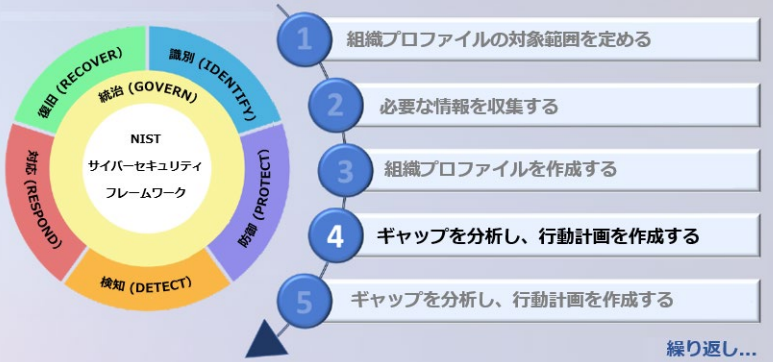
NIST CSF 2.0: 組織プロファイルの作成と使用

クイックスタートガイド

ギャップを分析し、行動計画を作成する – PART 2

現状プロファイルと目標プロファイルの差異を識別し、分析することで、組織はギャップを発見し、そのギャップに対処するための優先順位を付けた行動計画を策定することができる。

CSFでは、ギャップの分析 [**Step 4a**] 及びアクションプランの作成 [**Step 4b**] に役立つツール、管理策、及び実装リソースへのリンクを提供している。行動計画を策定するために推奨されるアプローチは、**NIST CSF 2.0 Reference Tool** を使用して、目標プロファイルの該当するサブカテゴリーから関連する NIST SP 800-53 の管理策への参照をたどることである。



使用するベストプラクティス

参考情報：コアと標準、ガイドライン、及びその他のリソースを含む様々なベストプラクティスとの関係。

参考情報は、組織がCSFの成果をどのように達成できるかを示すのに役立つ。また、セキュリティ及びプライバシー管理策のカタログを提供している ISO/IEC 27001 及び **SP 800-53** など、他の一般的なサイバーセキュリティ文書と望ましい成果を関連付けるのにも役立つ。

ベストプラクティスの実装方法

実装例：CSFの成果を達成する方法の概念記述。実装例は、組織が取り得るすべての行動を包括的なリストではなく、また、必要な行動のベースラインでもない。組織が具体的なステップについて考えるのに役立つアイディアである。NIST CSF 2.0 Reference Tool では、ユーザーがCSF 2.0 コアの全容を調べたり、Excel 及び JSON 形式でダウンロードしたりすることができる。

実装例の例

NIST CSF 2.0 Reference Tool からの抜粋

サブカテゴリー

PR.PS-01：構成管理のプラクティスが適用されている(旧 PT.IP-01、PR.IP-03、PR.PT-02、PR.PT-03)

実装例

例1: 組織のサイバーセキュリティポリシーを実施し、不可欠なケイパビリティのみを提供する強化されたベースラインを確立し、テスト、配備し、維持する（即ち、最小機能の原則）。

例2: ソフトウェアのインストール又はアップグレードの際に、サイバーセキュリティに潜在的なインパクトを与える可能性のあるすべてのデフォルト構成設定をレビューする。

NIST CSF 2.0: CREATING AND USING ORGANIZATIONAL PROFILES

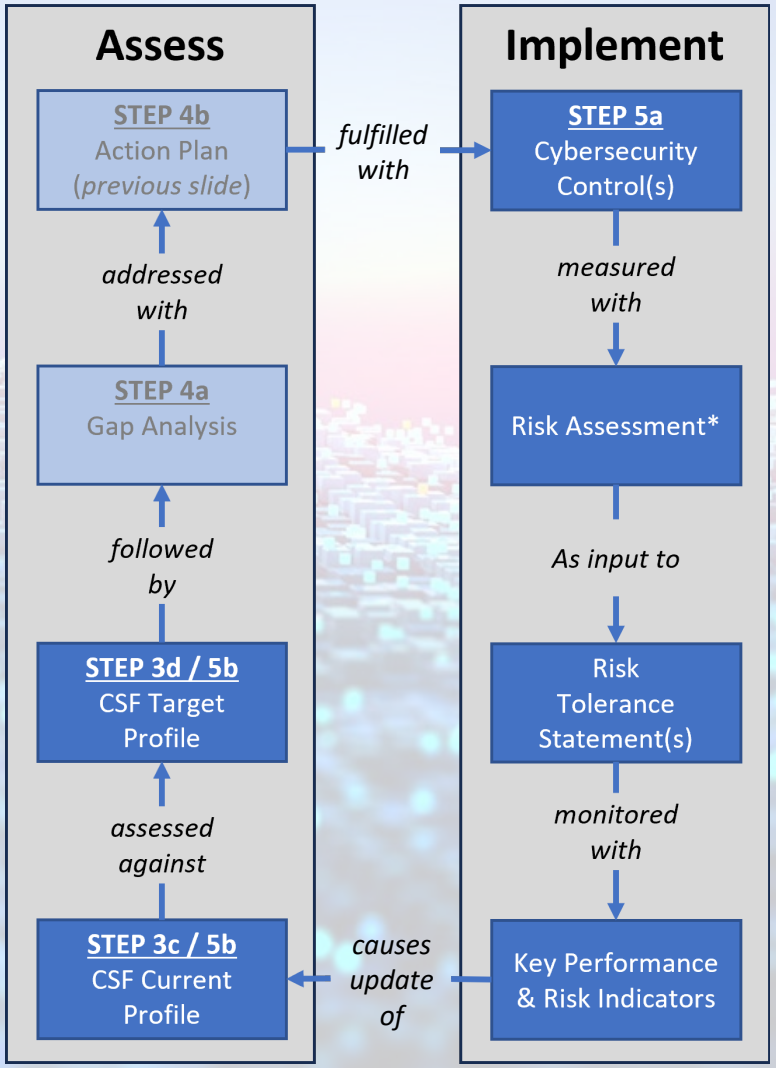
A QUICK START GUIDE

IMPLEMENT ACTION PLAN AND UPDATE PROFILE

Step 5a

Implementing Action Plans

The Action Plan is fulfilled through any combination of management, programmatic, and technical controls. As those controls are implemented, the Organizational Profile can be used to track implementation status. Subsequently, controls and associated risks can be monitored through Key Performance Indicators (KPI) and Key Risk Indicators (KRI). Cyber risks that fall beyond Risk Tolerance are observed through Risk Assessments. Risks beyond Risk Tolerance may prompt updates to the Action Plan, Organizational Profile, and/or Risk Tolerance statements. Gap Analysis may also result in the creation of POA&M for gaps that will take a longer remediation timeline. More information about KPI, KRI, Risk Tolerance, and POA&Ms can be discovered in IR 8286B and SP 800-37.



* Risk Assessment can occur at any time and can inform any step

Step 5b

Updating Your Profile

Implement activities that follow your Action Plan are a part of an ongoing cyber risk management program (feedback loops and lines of communication more nuanced than shown). Risk Assessments, as described in SP 800-30, can leverage Risk Tolerance statements when identifying risks, as well as determining likelihood and impact of those risks. The changing likelihood and impact are a measure of the effectiveness of the Action Plan and the discrete controls. Risk monitoring is also performed using KPI and KRI. Changes in risks, likelihoods, and/or impacts may all result in updates to the Organizational Profile.

NIST CSF 2.0: 組織プロファイルの作成と使用

クイックスタートガイド

行動計画を実装し、組織プロファイルを更新する

ステップ 5a

行動計画の実装

行動計画は、マネジメント、プログラム、及び技術管理策のあらゆる組み合わせによって達成される。これらの管理策が実装されると、組織プロファイルを使用して実装ステータスを追跡できる。

その後、管理策及び関連リスクは、重要業績評価指標 (KPI) 及び 重要リスク指標 (KRI) を通じて監視することができる。リスク許容度を超えるサイバーリスクは、リスクアセスメントを通じて観察される。

リスク許容度を超えるリスクは、行動計画、組織プロファイル、及び／又はリスク許容度ステートメントの更新を促す可能性がある。また、ギャップ分析により、修復に長期間を要するギャップのアクション計画とマイルストーン（POA&M）が作成される場合もある。KPI、KRI、リスク許容度、及び POA&M に関する詳細は、IR 8286B 及び SP 800-37 に記載されている。

ステップ 5b

プロファイルの更新

行動計画に従って**実装**する活動は、継続的なサイバーリスクマネジメントプログラムの一部である（フィードバックのループ及びコミュニケーションの経路は、図示されているものよりも微妙である）。

SP 800-30 に記載されているように、リスクアセスメントは、リスクを識別し、リスクの起こりやすさ及びインパクトを決定する際に、リスク許容度ステートメントを活用することができる。変化する起こりやすさ及びインパクトは、行動計画及び個別の管理策の有効性の尺度である。また、リスクの監視は、KPI及びKRIを用いても実施される。リスク、起こりやすさ、及び／又はインパクトの変化は、組織プロファイルの更新につながる可能性がある。

* リスクアセスメントはいつでも行うことができ、どのステップにも情報を与えることができる。

NIST CSF 2.0: CREATING AND USING ORGANIZATIONAL PROFILES

A QUICK START GUIDE

NEXT STEPS

What We Learned. This QSG explained the following terms:

Organizational Profile – CSF Core outcomes relevant for a specific organization

Community Profile – CSF Core outcomes that apply to multiple organizations

Current Profile – the cybersecurity outcomes that an organization is currently achieving

Target Profile – the desired outcomes an organization wants to achieve

Gap Analysis – determining the differences between the Current and Target Profiles

Informative References – best practices that implement various CSF Core outcomes

Implementation Examples – notional ways organizations can achieve CSF Subcategories

Action Plan – address gaps and move toward the Target Profile

What's Next. Here's a list of things you can do to move this QSG into practice:

- Familiarize yourself with the NIST CSF Organizational Profile template
- See if there is a Community Profile relevant for you at the NIST Community Profiles site
- Determine how many CSF Organizational Profiles you need [**Step 1**]
- Inventory your cybersecurity requirements
- Prioritize CSF outcomes in your Organizational Profiles [**Step 2**]
- Assess your Current Profile [**Step 3**]
- Read more about Informative References
- Improve your cybersecurity program over time [**Steps 4 & 5**]

Learning More

Reading

IR 8286B — NIST IR 8286B, *Prioritizing Cybersecurity Risk for Enterprise Risk Management*

SP 800-37 — NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems & Organizations*

SP 800-53 — NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems & Organizations*

SP 800-30 — NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*

Resources

Organizational Profile Template

NIST CSF 2.0 Reference Tool

Informative References

Implementation Examples

A Guide to Creating CSF 2.0 Community Profiles

Quick-Start Guide for Using the CSF Tiers

NIST CSF 2.0: 組織プロファイルの作成と使用

クイックスタートガイド

次のステップ

何を学んだか。

このクイックスタートガイドでは、下記の用語について説明した。

組織プロファイル – 特定の組織に関連するCSF コアの成果。
コミュニティプロファイル – 複数の組織に適用されるCSF コアの成果。
現状プロファイル – 組織が現在達成しているサイバーセキュリティの成果。
目標プロファイル – 組織が達成したい望ましい成果。
ギャップ分析 – 現状プロファイルと目標プロファイルの差異を特定する。
参考情報 – 様々なCSF コアの成果を実装するベストプラクティス。

実装例 – 組織がCSF サブカテゴリーを達成することができる概念的な方法。
行動計画 – ギャップに対処し、目標プロファイルに向けて前進する。

次は何をするか。

このクイックスタートガイドを実行に移すためにできることを以下に示す。

- NIST のCSF 組織プロファイルのテンプレートに慣れる。
- NIST の組織プロファイルサイトで、自分に関連するコミュニティプロファイルがあるかどうかを確認する。
- 必要な CSF 組織プロファイルの数を決定する。[**ステップ 1**]

- サイバーセキュリティ要件のインベントリを作成する。
- 組織プロファイルの CSF の成果に優先順位を付ける。[**ステップ 2**]
- 現状プロファイルをアセスメントする。[**ステップ 3**]
- Informative References を詳しく読む。
- サイバーセキュリティプログラムを時間の経過に伴って改善する。[**ステップ 4&5**]

さらに学ぶ

読み物

IR 8286B NIST IR 8286B, *Prioritizing Cybersecurity Risk for Enterprise Risk Management*

SP 800-37 NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems & Organizations*

SP 800-53 NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems & Organizations*

SP 800-30 NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*

リソース

Organizational Profile Template
NIST CSF 2.0 Reference Tool
Informative References
Implementation Examples
A Guide to Creating CSF 2.0 Community Profiles
Quick-Start Guide for Using the CSF Tiers