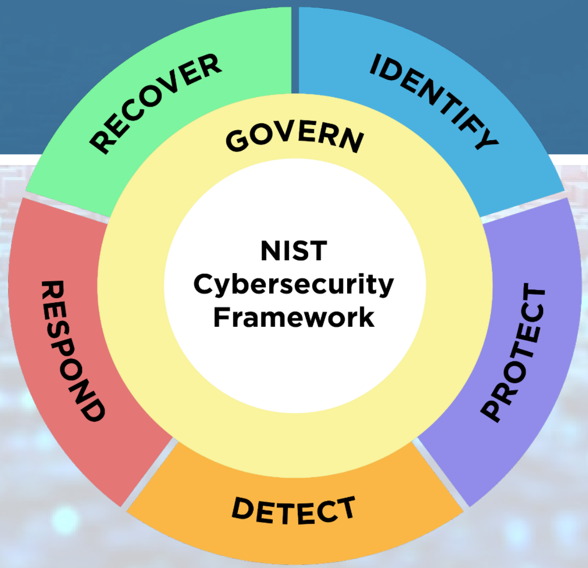
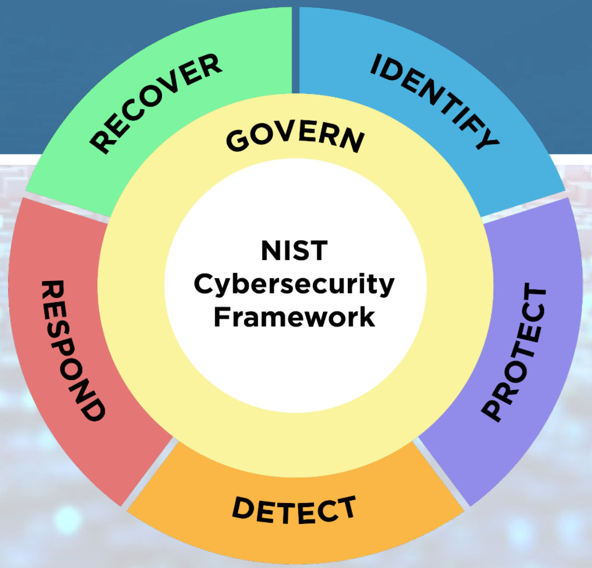
NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE



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:
CSF ティアの活用
クイックスタートガイド



¦ɸ{ɸ 5ŜLJI·ǊűƳŜyű ƻŦ /ƻƳƳŜǊŎŜ
DǺyI· aɸ wI·ǺƳƻyŘƻΣ {ŜŎǊŜǘŀǊȅ
bI·ǘǺƻyI·f LyǎǘǺǘdzǘŜ ƻŦ {ǘI·yŘI·ǊŘǎ I·yŘ ¢ŜŎKyƻfƻƎȅ
[I·dzǊǺŜ 9ɸ [ƻŎI·ǎŎǺƻΣ bL{¢ 5ǺǊŜŎǘƻǊ I·yŘ ¦yŘŜǊ {ŜŎǊŜǘI·Ǌȅ ƻŦ /ƻƳƳŜǊŎŜ Ŧƻǎ {ǘI·yŘI·ǊŘǎ I·yŘ ¢ŜŎKyƻfƻƎȅ

bL{¢ {LJŜŎǺI·f tdzōfǺŎI·ǘǺƻy
bL{¢ {t молн
ƘǘǘLJǎΥƪƪŘƻǺΦƻǊƎкмлΦслнукbL{¢Φ{tΦмолн
コメントは cyberframework@nist.gov まで送付のこと
2024年10月

NIST CSF 2.0: USING THE CSF TIERS

A QUICK-START GUIDE

Cybersecurity Framework (CSF) Tiers

CSF Tiers can be applied to CSF Organizational Profiles to characterize the rigor of an organization's cybersecurity risk governance and management outcomes. This can help provide context on how an organization views cybersecurity risks and the processes in place to manage those risks. The Tiers can also be valuable when reviewing processes and practices to determine needed improvements and monitor progress made through those improvements.

Appendix B of the CSF contains a notional illustration of the CSF Tiers. In that illustration, each Tier has separate descriptions for Cybersecurity Risk Governance (corresponding to the Govern Function) and Cybersecurity Risk Management (for the other five CSF Functions: Identity, Protect, Detect, Respond, and Recover).

The Tiers capture an organization's outcomes over a range: Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4). They reflect a progression from informal, ad hoc responses to approaches that are agile, risk-informed, and continuously improving.

An organization wanting to use the CSF Tiers can reuse the notional descriptions from Appendix B of the CSF. Alternatively, they can customize those descriptions, create new ones, or use a set of descriptions they already have in place.

Selecting Tiers

Selecting the CSF Tiers that your organization should be meeting in its cybersecurity risk governance and management activities is generally performed by organization leadership.

Here are tips for selecting Tiers:

- Selecting Tiers overall or at the Function or Category level will provide a better sense of the organization's current cybersecurity risk management practices than selecting Tiers at the lower Subcategory level.
- You can use one of the two Tier components (governance or management descriptions) if you want to focus on a subset of the CSF Functions. For example, if your scope is governance only, you can omit the Cybersecurity Risk Management descriptions.
- When selecting Tiers, consider the following aspects of the organization:
    - current risk management practices
    - threat environment
    - legal and regulatory requirements
    - information sharing practices
    - business and mission objectives
    - supply chain requirements
    - organizational constraints, including resources
- Ensure that the Tiers being selected help to meet organizational goals, are feasible to implement, and reduce cybersecurity risks to critical assets and resources to levels that are acceptable to the organization.
- Progression to higher Tiers is encouraged when needed to address risks or mandates.

NIST CSF 2.0: CSF ティアの活用

クイックスタートガイド

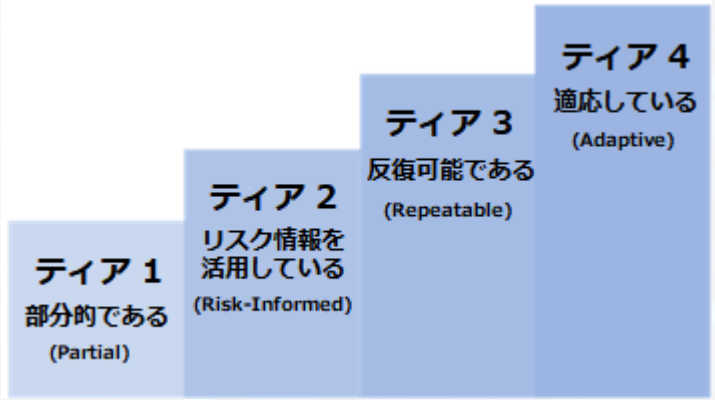
サイバーセキュリティフレームワーク（CSF） ティア

CSF ティアをCSF組織プロファイルに適用して、組織のサイバーセキュリティリスクガバナンス（統治）及びサイバーセキュリティリスクマネジメント（管理）の成果の厳密性を特徴付けることができる。これは、組織がサイバーセキュリティリスクをどう捉えているか、及びそれらのリスクを管理するためにどのようなプロセスを実施しているかについてのコンテキストを提供するのに役立つ。またティアは、必要な改善を判断し、それらの改善を通じて達成された進捗を監視するためのプロセス及びプラクティスをレビューする際にも役立つ。

CSFの付属書 B には、CSF ティアの概念図が含まれている。この図には、各ティアに、サイバーセキュリティリスクガバナンス（「統治」機能に対応している）、及びサイバーセキュリティリスクマネジメント（「識別」、「防御」、「検知」、「対応」、「復旧」の5つのCSF機能）の個別の説明がある。

ティアは、部分的である（ティア 1）、リスク情報を活用している（ティア 2）、反復可能である（ティア 3）、適応している（ティア 4）の範囲で、組織の成果を捉えている。これらは、非公式で場当たり的な対応から、アジャイルで、リスク情報を活用して、継続的に改善するアプローチへの進展を反映している。

CSF ティアの使用を希望する組織は、CSFの付属書Bの概念的な記述を再利用することができる。あるいは、それらの記述をカスタマイズしたり、新たな記述を作成したり、既存の一連の記述を使用することもできる。



ティアを選択する

サイバーセキュリティリスクガバナンス及びサイバーセキュリティリスクマネジメント活動において組織が満たすことが望ましいCSFティアの選択は、通常、組織のリーダーによって実行される。

ティアを選択する際のヒントを以下に示す。

- ティアを全体、又は機能レベルあるいはカテゴリーレベルで選択すると、下位のサブカテゴリーレベルで選択するよりも、組織の現在のサイバーセキュリティリスクマネジントのプラクティスを把握しやすくなる。
- CSFの機能のサブセットに焦点を当てたい場合は、2つのティアコンポーネント（ガバナンス又はマネジメントの説明）のいずれかを使用することができる。例えば、「統治」のみが対象範囲の場合は、サイバーセキュリティリスクマネジメントの記述を省くことができる。
- ティアを選択する場合は、組織の以下の側面を考慮する。
    - 現在のリスクマネジメントのプロセス
    - 脅威の環境
    - 法的及び規制上の要件
    - 情報共有のプラクティス
    - ビジネス及びミッションの目的
    - サプライチェーンの要件
    - リソースを含む組織上の制約
- 選択するティアが、組織の目標を達成するのに役立ち、実装することが可能であり、重要な資産及びリソースに対するサイバーセキュリティリスクを組織が受容可能なレベルまで軽減できることを確実にする。
- リスク又は義務に対処するために必要な場合は、より高いティアへの移行が推奨される。

NIST CSF 2.0: USING THE CSF TIERS

A QUICK-START GUIDE

APPLYING TIERS TO ORGANIZATIONAL PROFILES

Applying Tiers to Organizational Profiles

Once your organization's Tier selections have been made, you can use them to help inform your Current and Target Profiles.

For example, if leadership has determined that your organization should be at Tier 2 (Risk Informed) for the Identify and Protect Functions, then your Current Profile would reflect how well the Tier 2 Cybersecurity Risk Management characteristics are currently being achieved for each CSF Category within those two Functions. Similarly, the Target Profile would reflect any improvements to Identity and Protect outcomes needed to fully achieve the Tier 2 description. The table excerpt below shows the relevant part of the Tier 2 description.

Tiers should be used to **guide and inform** an organization's cybersecurity risk governance and management methodologies rather than take their place.

Tier	Cybersecurity Risk Governance	Cybersecurity Risk Management
Tier 1: Partial	…	…
Tier 2: Risk Informed	…	There is an awareness of cybersecurity risks at the organizational level, but an organization-wide approach to managing cybersecurity risks has not been established. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs but is not typically repeatable or reoccurring. Cybersecurity information is shared within the organization on an informal basis. The organization is aware of the cybersecurity risks associated with its suppliers and the products and services it acquires and uses, but it does not act consistently or formally in response to those risks.
Tier 3: Repeatable	…	…
Tier 4: Adaptive	…	…

Additional Resources

- *Quick-Start Guide for Creating and Using Organizational Profiles* (includes taking CSF Tiers into account in Current and Target Profiles)
- Organizational Profile notional template
- *A Guide to Creating CSF 2.0 Community Profiles* (includes using CSF Tiers to inform the development of Community Profiles)

NIST CSF 2.0: CSF ティアの活用

クイックスタートガイド

ティアを組織プロファイルに適用する

ティアを組織プロファイルに適用する

組織のティアの選択を完了したら、それを現状プロファイル及び目標プロファイルの通知に役立てることができる。

例えば、組織が「識別」機能及び「防御」機能について、ティア 2（リスク情報を活用している）が望ましいとリーダーが決定した場合、現状プロファイルには、これら2つの機能内のCSFカテゴリーについて、ティア 2のサイバーセキュリティリスクマネジメントの特性が現在どの程度達成されているかを反映する。同様に、目標プロファイルには、ティア 2の記述を完全に達成するために必要な「識別」及び「防御」の成果の改善を反映する。以下の表の抜粋は、ティア 2の記述の関連部分を示している。

ティアは、組織のサイバーセキュリティリスクガバナンス及びサイバーセキュリティリスクマネジメントの手法の代わりに使用するのではなく、**手引きし通知する**ために使用されることが望ましい。

ティア	サイバーセキュリティリスクガバナンス	サイバーセキュリティリスクマネジメント
ティア 1: 部分的である	…	…
ティア 2: リスク情報を活用している	…	組織レベルでは、サイバーセキュリティリスクに対しての認識はあるが、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のアプローチは確立されていない。 組織の目的及びプログラムにおけるサイバーセキュリティの考慮は、組織の一部のレベルでは行われているが、すべてのレベルでは行われていない。組織の資産及び外部の資産のサイバーリスクアセスメントが行われているが、通常、反復可能ではない、又は繰り返し行われていない。 サイバーセキュリティ情報が、組織内で非公式に共有されている。 組織は、サプライヤ及び取得・使用する製品とサービスに関連するサイバーセキュリティリスクを認識しているが、それらのリスクに対応するための一貫した、又は正式な行動をとっていない。
ティア 3: 反復可能である	…	…
ティア 4: 適応している	…	…

補足リソース

- *Quick-Start Guide for Creating and Using Organizational Profiles* (現状プロファイル及び目標プロファイルを考慮することを含む)
- Organizational Profile notional template
- *A Guide to Creating CSF 2.0 Community Profiles* (コミュニティプロファイルにCSFティアを使用することを含む)