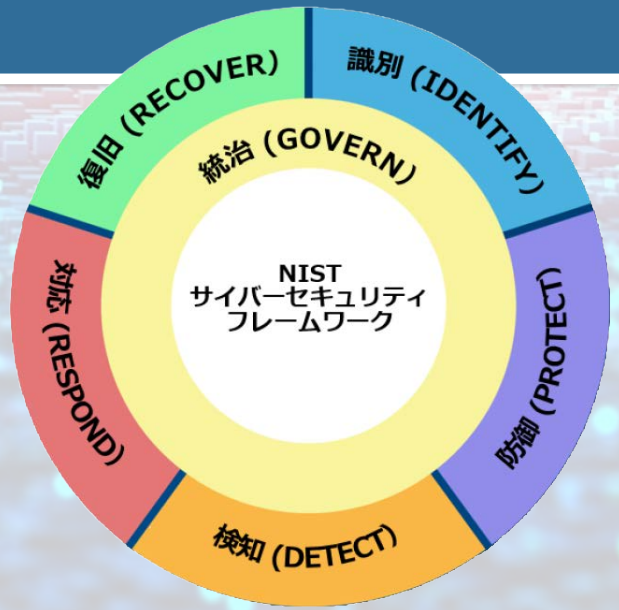
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

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



NIST Special Publication
NIST SP 1302 jpn (初期公開ドラフト)
https://doi.org/10.6028/NIST.SP.1302.jpn
コメントは cyberframework@nist.gov まで送付のこと
2024年2月

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 CSF 2.0: CSF ティアの活用

クイックスタートガイド

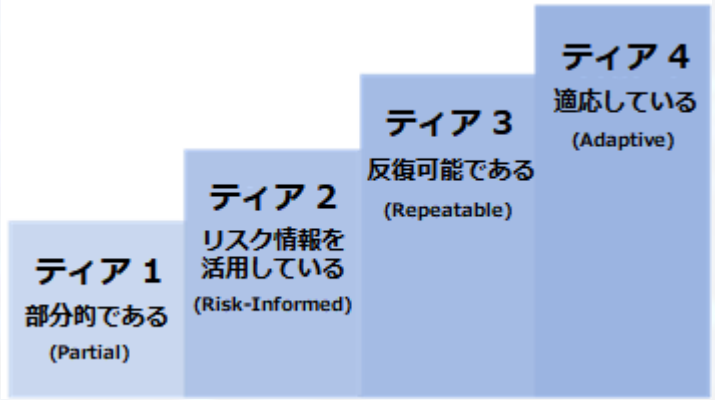
CSF ティア

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 の概念的な記述を再利用することもできるし、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したりすることもできる。



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、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メ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: CSF ティアの活用

クイックスタートガイド

ティアをプロファイルに適用する

ティアを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、サプライヤおよび取得及び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）