protiviti®
Global Business Consulting

NISTがサイバーセキュリティフレームワーク（CSF）バージョン2.0をリリース：企業にとって何を意味するのか

2024
2月28日

背景

2024年2月26日、米国国立標準技術研究所（NIST）は、広く利用されているサイバーセキュリティフレームワーク（CSF）のバージョン2.0を発表しました。このCSFの最新版は、サイバーセキュリティの洗練度に関係なく、あらゆる対象者、業種、組織の種類を対象として設計されています。

「CSFは多くの組織にとって不可欠なツールであり、サイバーセキュリティの脅威を予測し、対処するのに役立っている。」とローリー・E・ロカシオ商務次官（標準・技術担当）兼NIST長官は述べています。「CSF 2.0は、旧バージョンを基にしたものであり、単なる1つの文書ではない。組織のサイバーセキュリティのニーズが変化し、その能力が進化するにつれて、個別に、あるいは組み合わせてカスタマイズして使用することができる一連のリソースである。」

CSFのバージョン2.0で、NISTはその中核となるガイダンスを拡大するためにフレームワークを更新し、利用者がCSFを最大限に活用するのに役立つリソースを開発しました。NIST CSF 2.0は、あらゆる規模・セクターの組織がサイバーセキュリティリスクを管理・低減できるよう、対象範囲を拡大しています。ガバナンスとサプライチェーンの重要性を強調し、組織がサイバーセキュリティ戦略について充分な情報に基づいて意思決定を行い、実行する方法を網羅しています。

NIST CSF 2.0開発の経緯

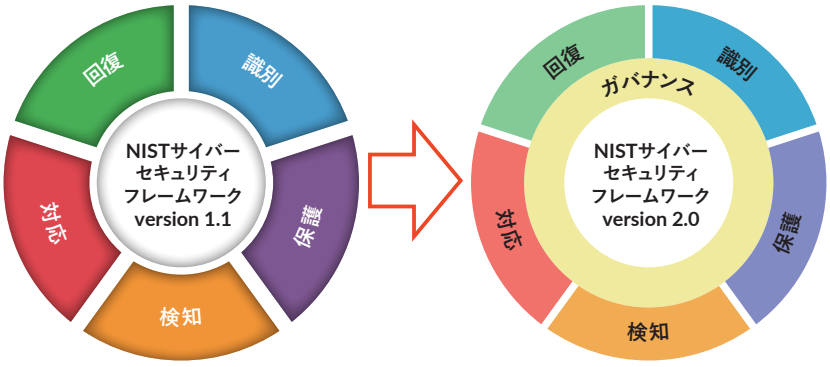
NISTは2023年8月8日にNIST CSF 2.0のドラフト版を発表し、主要な利害関係者、複数の業界や組織からコメントを集めました。また、NISTは2022年8月から複数のワークショップを開催し、バージョン2.0を複数の業界やあらゆる規模の企業で導入しやすくすることを意図して、CSFを更新するための共同プロセスを開発しました。コメントは2023年11月まで受け付けられ、NIST CSF 2.0の最終版に反映されました。

NIST CSF 2.0の新項目

NIST CSF 2.0は、旧バージョンのCSFを基礎とし、フレームワークをより包括的なものとするために、いくつかの新しい概念や要素を導入しています。以前のCSFには次の5つの中核機能がありました。識別（Identify）、保護（Protect）、検知（Detect）、対応（Respond）、回復（Recover）です。NIST CSF 2.0では、これらの5つの機能に情報を提供し、支援する新たな中核機能「ガバナンス」が追加されています。

NIST CSF 2.0は、フレームワークの基礎要素として「ガバナンス」機能を導入している。

出典：米国立標準技術研究所：
www.nist.gov/cyberframework



CSFコアは、あらゆる組織がサイバーセキュリティリスクを管理するのに役立つ、高レベルのサイバーセキュリティ成果の分類法であり、フレームワークの基礎となっています。NISTは、NIST CSF 1.1フレームワークを構成する機能、カテゴリー、サブカテゴリーを評価し、NIST CSF 2.0の構築の一環として、新たなカテゴリーの追加、類似のサブカテゴリーの統合、その他のサブカテゴリーの廃止を行いました。その結果、NIST CSF 2.0は、カテゴリーを23から22に、サブカテゴリーを108から106に削減しています。

最も注目すべき変更点は以下の通りです。

- **ガバナンス機能**：ガバナンス機能は、組織の目標と利害関係者の期待に照らして、他の5つの機能のイニシアチブを達成し、その優先順位をつけるために、組織が行うべきことを示すガイダンスを提供するものです。ガバナンス機能は、NIST CSF 2.0フレームワークの基盤を成す組織の背景、サイバーセキュリティ戦略およびサイバーセキュリティ・サプライチェーン・リスク管理の確立、役割、責任、権限、方針、サイバーセキュリティ戦略の監督をカバーします。

- **サイバーセキュリティのサプライチェーンリスク管理**：新しいガバナンス機能では、（NISTの最新ガイダンスを反映した）サイバーセキュリティ・サプライチェーン・リスク管理と安全なソフトウェア開発に重点が置かれています。NISTが組織に対して提案している新しいプラクティスには、以下のようなものがあります。

  - サイバーセキュリティ・サプライチェーン・リスク管理（C-SCRM）戦略、目的、方針、プロセスを策定すること。

  - 組織のテクノロジー・サプライヤーを特定し、それぞれが組織にとってどの程度重要であるかを判断すること。

  - C-SCRMの役割と要件を確立し、組織内外に伝達すること。

- **リファレンスツールの更新**：新しく包括的なオンラインNIST CSF 2.0リファレンスツールにより、ユーザーはキーワードや語句を使用してNIST CSF 2.0を簡単に探索し、サブカテゴリーや実装例のリファレンスを素早く見つけることができるようになっています。また、このツールはミッション・ステートメント、利害関係者の期待、法的要件、規制上の説明責任、契約上の義務といった要素を強調することで、組織のプロフィールや状況についてユーザーの理解を促進します。更新され最新化されたリファレンスツールは、NIST CSF 2.0で概説されているサイバーセキュリティのベストプラクティスを理解し、実施するための貴重なリソースとなります。

- **サイバーセキュリティリスク低減に関するガイダンス**：このフレームワークには、クイックスタートガイドが含まれており、多数の事例や、産業界、政府機関、教育機関、医療機関、あらゆる規模の企業（サイバーセキュリティ・プログラムが成熟していない中小企業を含む）など、多くの事業体に適用可能で詳細なガイダンスが記載されています。このガイダンスは、サイバーセキュリティのリスクを効果的に低減し、ベストプラクティスを開発することに重点を置いています。

- **プロファイル・ガイダンスの拡充**：組織の目標や利害関係者の期待、脅威の状況、要件に基づいて、サイバーセキュリティの成果を理解し、調整し、評価し、その優先順位をつけるためのガイダンスを提供するために、組織とコミュニティのプロフィールが大幅に改訂され、拡張されました。これらのプロファイルは、目標とする成果の進捗状況を評価し、関係者に適切な情報を伝えるために使用することができます。

- **CSF段階の拡張**：CSFの階層を組織のプロファイルに適用することで、組織のサイバーセキュリティリスクガバナンスと管理の成果の厳格さを特徴付けることができます。NIST CSF 2.0では、2つのCSF層が定義されています。サイバーセキュリティリスクガバナンスはガバナンス機能に相当し、サイバーセキュリティリスクマネジメントは残り5つのCSF機能に相当します。これらのCSF階層はそれぞれ、組織の目標達成を支援する独自のガイダンスを持っています。

前述のとおり、NIST CSF 2.0は、NIST CSF 1.0およびNIST CSF 1.1を基に作成されており、これらは既にかなり包括的なものでした。とはいえ、NIST CSF 2.0全体を通じて大幅な更新が行われており、提供されるメリットを完全に実現させるように心がける必要があります。注目すべき変更点としては、対象範囲が拡大され、重要な部門で活動する組織以外にも適用されるようになったことが挙げられます。NIST CSF 2.0は、サイバーセキュリティのリスク管理を組織全体のリスク管理プロセスに統合することも強調しています。

今何をすべきか？

NIST CSF 2.0が最終化された今、組織は新しいフレームワークのコンポーネントを導入する前に、いくつかの準備段階を踏む必要があります。以下のステップは、主要なフレームワーク要素の採用を容易にし、組織が潜在的な利益を引き出すためのスタートを切るのに役立ちます。

1. NIST CSF 2.0への移行を監督する部門横断的なサイバー・タスクフォースを導入することで、サイバーセキュリティ部門とその他の事業部門との間の連携とコミュニ

ケーションを可能にします。サイバー・タスクフォースは、組織の取締役会や幹部との対話を促進し、サイバーセキュリティ・プログラムと全体的な組織戦略への影響の理解を促す必要があります。

2. NIST CSF 2.0クイックスタートガイドをレビューし、組織が新しいフレームワークの主要部分を実施することを支援します。

3. 現在のポリシー、プロセス、手順、およびコントロールをNIST 2.0フレームワークの要素に照らして見直し、特にガバナンス機能と組織への影響に焦点を当て、組織の関連文書とコントロールの説明が必要に応じて更新されていることを確認します。

4. サイバーセキュリティリスクガバナンスとサイバーセキュリティリスクマネジメントに関する新しい階層化ガイダンスを見直します。これらの項目にはそれぞれ特定の階層格付け要件と目標があるためです。

5. NIST CSF 2.0に対するギャップ分析を実施し、発見された不備に対処するためのアクションプランを策定します。

6. 重要な資産およびリソース全体にわたって望ましいリスク態勢を達成するのに役立つよう、適切なCSFの実施階層を検討し、特定します。

プロティビティの支援

プロティビティは、お客様がビジネスとテクノロジーの総合的なアプローチでリスク態勢を把握し、現在のサイバーセキュリティ能力を評価できるよう支援します。プロティビティは、新しいNIST CSF 2.0フレームワークと当社の深い専門知識を組み合わせることで、お客様の現在のサイバーセキュリティ能力とビジネス推進要因を理解し、目標とする明確なセキュリティ運用モデルに向けて組織を推進するためにカスタマイズされたサイバープログラムのロードマップを作成します。

プロティビティは、既存のフレームワーク、リスク管理プログラム、統制の設計、監査手法を改訂し、新基準に適合させることで、3つの防衛ライン全体で関係者を支援しています。プロティビティは、お客様固有のリスク状況やサイバーセキュリティの成熟度を把握することで、取締役会や経営幹部がビジネスリスクを理解・評価し、お客様にサービスを提供することにより、ビジネスを成長させるための賢明なサイバーセキュリティ戦略投資を行うためのアドバイスを提供します。

protiviti®