RESOURCE CENTER

NISTサイバーセキュリティフレームワークとは？究極のガイド

Get the full interactive view at
https://bitwarden.com/ja-jp/resources/nist-cybersecurity-framework/

bitwarden

NISTの歴史

米国国立標準技術研究所（NIST）は、企業、非営利団体、
その他の民間機関がサイバーセキュリティのリスク管理を改善するのを支援するため、
組織が従うべきガイダンスとベストプラクティスを提供している。NISTは米国商務省の一部であり、米国で最も古い（物理）
科学研究所のひとつである。

2013年、大統領は大統領令13636号を出した：

> **「国家の重要インフラのセキュリティと回復力を強化し、安全、セキュリティ、ビジネスの機密性、プライバシー、
> 市民の自由を促進しながら、効率性、革新性、経済的繁栄を促進するサイバー環境を維持することは、米国の政策である。**

この大統領令は、NISTがサイバーセキュリティ・フレームワークに適用する、以下のような一定の要件を定めた：

- 重要インフラの各部門に適用されるセキュリティ基準やガイドラインを特定する。
- 優先順位付けされた、柔軟で繰り返し可能な、パフォーマンスベースの、費用対効果の高いアプローチを提供する。
- 重要インフラの所有者および運営者がサイバーリスクを特定、評価、管理できるように支援する。
- 技術革新を可能にし、組織の違いを考慮する。
- 技術に中立的で、重要インフラ部門が製品やサービスの競争市場から利益を得られるようなガイダンスを提供する。
- サイバーセキュリティ・フレームワークの実施実績を測定するためのガイダンスを含める。
- 今後、特定のセクターや規格策定機関との協力を通じて取り組むべき改善分野を特定する。

なぜこのようなことが重要になってきたのか？

端的に言えば、増大するサイバーセキュリティの脅威は、企業やその他の組織に日々影響を与えている。単一の真実の情報源がなければ、
企業がセキュリティ・
リスクを軽減するための効果的な対策を実施するための徹底的で効果的な枠組みを構築することはほとんど不可能である。だからこそ、
NISTサイバーセキュリティ・フレームワークは企業にとって極めて重要なものとなっているのである。

目次

NISTサイバーセキュリティフレームワークとは？

基本的に、NISTサイバーセキュリティ・フレームワークは、あらゆる種類の組織がサイバーセキュリティ・リスクをよりよく理解し、管理し、低減するのに役立つ。このガイダンスに従うことで、ネットワークとデータの保護が向上する。NISTサイバーセキュリティ・フレームワークは、どのような企業や組織でも実施可能なように細分化されており、サイバーセキュリティ保護の改善のためにどこに時間とリソースを集中させるべきかをよりよく理解することができる。それは、企業が自社のデータ、顧客のデータ、ネットワーク、従業員をより効果的に保護できるようにすることだ。

NISTサイバーセキュリティ・フレームワークは米国内の組織によって開発されたが、世界的な普及を念頭に置いて作成された。そのため、多くの言語に翻訳され、世界中の政府、企業、団体に採用されている。

NISTサイバーセキュリティ・フレームワーク1.1以来、多くの組織や政府がこのフレームワークの採用に成功している：

- サウジアラムコ
- バミューダ政府
- イスラエル国家サイバー総局
- Cimpress-Fair
- 複数の州 - 情報共有・分析センター
- カンザス大学医療センター
- ピッツバーグ大学
- アイエスエーシーエー
- 日本異業種フォーラム
- シカゴ大学
- コロラド川下流河川局
- オプティック・サイバー・ソリューション

NISTサイバーセキュリティ・フレームワーク（CSF）の最新バージョンは、小規模の学校や非営利団体から大企業まで、あらゆる種類や規模の対象者、業種、組織を対象としている。このフレームワークは、サイバーセキュリティの洗練度に関係なく、どのような組織でもこのフレームワークが示す情報から利益を得られるように設計されている。

NIST理事兼標準技術担当商務次官のローリー・E・ロカシオによると

> 「CSFは多くの組織にとって重要なツールであり、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きた。
> 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、時間をかけて個別に、
> あるいは組み合わせてカスタマイズし、使用することができる一連のリソースのことである。

NISTサイバーセキュリティフレームワークの歴史を探る

また、NISTサイバーセキュリティフレームワークの最新の進化は、重要インフラに焦点を当てるにとどまらず、
あらゆるセクターのあらゆる組織（あらゆる規模）を包含している。

NISTサイバーセキュリティ・フレームワークが作成されたとき、その目標は政府、産業界、学界の利害関係者との継続的な関与にあった。
このフレームワークを作成するために、NISTは全米でアウトリーチやワークショップを行い、また情報提供要請（RFI）や意見募集（RFC）
を行った。当初の目標は3つあった：

- 既存のサイバーセキュリティ基準、ガイドライン、フレームワーク、ベストプラクティスを特定する。
- 優先順位の高いギャップを指定する。
- これらのギャップに対処するための行動計画を策定する。

情報収集のための意見募集期間は2013年4月8日に終了し、NISTは270件以上の回答を得た。これらの回答から、
NISTは最初のサイバーセキュリティ・フレームワーク・ワークショップのアジェンダを作成した。このワークショップは、関心を集め、
認識を高め、共同開発プロセスについての見識を深めることを目的として、ワシントンDCで開催された。ワークショップでは、大統領令、
開発目標、フレームワークの開発プロセスの再確認などが行われた。

2回目のワークショップは2013年5月29日から31日にかけてカーネギーメロン大学で開催され、最初のRFIの分析に基づいた議題が出された。
その目的は、彼らが受け取った情報をさらに定義し、明確にすること、そして、
セキュリティに基づくいくつかのトピックにわたって議論を促すことであった。このワークショップの終了後、NISTは収集した情報を分析し、
サマリーを作成して各業界と共有し、サイバーセキュリティ・フレームワークの初期草案の作成に使用した。

NISTサイバーセキュリティ・フレームワークの最初の草案は2013年7月2日に発表された。

NISTはリリース後、初期リリースの議論と改良を目的としたワークショップを数回開催した。2014年2月12日、
NISTサイバーセキュリティフレームワークのバージョン1.0がリリースされた。

NISTサイバーセキュリティフレームワークの中核機能

NISTサイバーセキュリティフレームワークは、ベストプラクティスの一般的な概要を示すいくつかのコア機能で構成されている。
これらの機能は、手続き的なステップと見なされることを意図しているのではなく、
むしろサイバーセキュリティリスクの動的な性質に対処するために使用される。

ガバナンス

この機能は、組織がその使命と利害関係者の期待に照らして、
残りの機能に優先順位をつけるために何ができるかを知らせるのに役立つ成果を提供する。

特定する

特定機能は、システム、資産、データ、能力に対するサイバーセキュリティ・リスクについて組織的な理解を深める必要性を訴えている。
この要素はビジネスに焦点を当てるもので、リスク管理戦略に合致した方法で取り組みの優先順位を決めることができる。

プロテクト

この機能は、資産を保護し、サイバーセキュリティ・イベントの可能性を防止または低下させ、
それによって生じる影響を軽減する組織の能力をサポートする。

検出

この機能により、サイバーセキュリティ・イベントが発生した、または発生する可能性があることを示す異常、侵害の指標、
その他の有害事象をタイムリーに発見し、分析することができる。

応答する

この機能は、インシデントの管理、分析、緩和、報告、および通信をカバーし、
サイバーセキュリティインシデントのあらゆる影響を抑制するのに役立つ。

回復する

この機能は、サイバーセキュリティインシデントの影響を軽減し、復旧中に必要な（そして適切な）コミュニケーションを可能にするために、
通常業務をタイムリーに復旧させることに重点を置いている。

これらの機能の最終的な目標は、組織がサイバーセキュリティ事象にどのように備え、どのように対応し、どのように回復するかについて、
ハイレベルで戦略的な視点を提供することである。

NISTサイバーセキュリティフレームワークの導入

NISTサイバーセキュリティ・フレームワークが何をするものなのか、そしてどのように進化してきたのかをしっかりと理解した上で、
それをどのように導入するのがベストなのか悩んでいることだろう。

NISTは、導入のための7段階のアプローチを推奨している：

1. **優先順位と範囲**– 組織の目的と保護すべき資産の優先順位を決める。
2. **オリエンテーション**– 対象範囲内のプロセス、システム、コンポーネント、および遵守すべき主要なコンプライアンス規制について、
   自分自身とチームをよく理解する。
3. **現在のプロファイルを作成する**– フレームワークのどの管理成果がすでに組織内で達成されているかを示し、
   次にまだ統合する必要があるもののリストを作成する。
4. **リスク・アセスメントの実施**– 業務環境を分析し、サイバーセキュリティ・イベントが発生する可能性とその影響を判断する。
5. **ターゲットプロファイルを作成する** – サイバーセキュリティフレームワークのカテゴリとサブカテゴリの評価に焦点を当て、
   望ましいサイバーセキュリティの成果を説明するのに役立てる。
6. **ギャップの特定、分析、優先順位付け**– 組織に存在するサイバーセキュリティのギャップを特定する。この分析から、
   それらのニーズに対処するための優先順位をつけた計画を立てることができる。
7. **行動計画を実行する**– これまでのステップで発見されたすべての問題に対処するため、作成した計画を実行に移す。

ひとつ覚えておいてほしいのは、フレームワークは柔軟性に欠けるということだ。実際、このフレームワークには十分な柔軟性があり、
既存のセキュリティ・プロセスと統合することができる。上記の7つのステップの中で、それがどのように機能するかがわかるはずだ。

NISTサイバーセキュリティフレームワーク採用のメリット

NISTがフレームワーク導入のための7つのステップを示しているため、組織は、どのようなリスクにさらされやすいか、
そのリスクに応じた計画をどのように立てるか、組織全体のコミュニケーションをどのように改善し、
コンプライアンスをどのように強化するかについて、広範な概観を得ることができる。組織の弱点とその緩和方法に関する教育は、
NISTフレームワークの重要な利点の一つである。

> 連邦取引委員会によると、NISTフレームワークは「あらゆる規模の企業がサイバーセキュリティ・リスクをよりよく理解、管理、低減し、ネットワークとデータを保護するのに役立つ」という。

NISTは、各組織が異なることを理解し、パスワードを安全に保つための3つのヒント（これは普遍的なものと考えるべきである）
を提供している。

フレームワーク採用における課題と考慮点

NISTサイバーセキュリティ・フレームワークは複雑である。上記の7つのステップに進む前に、
核となる機能を十分に理解しておくことが重要だ。永続的な成功を確実にするためには、
組織内にサイバーセキュリティ文化を奨励することが重要である。そうでなければ、
プロセスやシステムの劇的な変化に対する抵抗に直面することになる。

その他の課題は以下の通り：

- リソースの制約 - 現在、これらの変更を実施できるスタッフがいないかもしれない。
- ほとんどの場合、サイバーセキュリティ・
  フレームワークを自分の組織に合うようにカスタマイズするのに時間を費やす必要があるだろう。
- 脅威は常に進化しており、セキュリティ対策もそれに対応する必要がある。
- サイバーセキュリティ・フレームワークは、既存のプロセスと統合することが望ましい。
- 利害関係者の関与を促すことは、こうした要求に応えられるサイバーセキュリティ文化の醸成に直結するため、難しいかもしれない。

NISTサイバーセキュリティフレームワークのプロファイルと階層

NISTの実施段階は4つある：

- **Tier 1 Partial**- オンデマンドまたはゼロのセキュリティ手順を持つ企業。
- **ティア2 リスクに詳しい**企業 - 直面している脅威を認識しており、ある程度の方針を定めているが、連携した戦略がない。
- **Tier 3 Repeatable**- リスクマネジメントとサイバーセキュリティのベストプラクティスがあり、経営陣の承認を得ている企業。
  このような企業は、しばしば競合他社と比較して自らを評価し、さらには他の組織と連携して、その慣行が一致していることを確認する。
- **ティア4 適応型**- 厳しく規制される業界（銀行やヘルスケアなど）に属する企業で、日常的に広範なリスク認識に貢献している。

NISTによると、サイバーセキュリティ・フレームワーク・プロファイルとは、「機能、カテゴリー、サブカテゴリーを、組織のビジネス要件、リスク許容度、リソースと整合させること」である。これらのプロファイルは、
組織がサイバーセキュリティのリスクを低減するためのロードマップを確立するのに役立つ。

NISTは、カスタマイズ可能なサイバーセキュリティフレームワーク組織プロファイルテンプレートと、
使用可能なコミュニティプロファイルのリストを提供している。

NISTフレームワークの更新と進化

NISTサイバーセキュリティ・フレームワークは、刻々と変化するサイバーセキュリティの状況や新たな脅威を反映し、
定期的な更新に依存する生きた文書となるよう設計されていることを覚えておいてほしい。このため、
組織は常に最新の脅威に対応することが極めて重要であり、サイバーセキュリティ・フレームワークは現在のニーズに合わせて進化し、
継続的に改善されることになる。

あなたの組織がNISTサイバーセキュリティ・フレームワークとともに進化できるようにするには、サイバーセキュリティ・
フレームワークとともに進化できる最高のテクノロジーを活用できるようにする方法として、
あなたのビジネスに最適なサイバーセキュリティ技術スタックを構築する方法を検討するとよいだろう。

Bitwardenの活用でサイバーセキュリティ体制を強化

セキュリティが組織にとって最も重要な分野のひとつになっていることは言うまでもない。強固なサイバーセキュリティ・
リスク管理の実践がなければ、企業は野放しになっている数々の脅威の犠牲になる可能性がある。NISTサイバーセキュリティ・
フレームワークの助けを借り、入念な計画とコミュニケーションを行えば、組織のセキュリティは大幅に改善されるだろう。
NISTサイバーセキュリティ・フレームワークに徹底的に取り組み、7つのステップに従い、常に更新と進化に備えることで、
組織はサイバーセキュリティのリスクからよりよく守られるようになる。

今日から始める準備はできていますか？パスワード管理ソリューションの導入を検討し、組織を正しい方向にスタートさせましょう。
ビットワルデンのビジネスプランの確認、セールスへのお問い合わせ、プラン価格の比較。