サイバーインテリジェンスを活用したNIST CSF 2.0への準拠

サイバーセキュリティはほとんどの組織にとって最優先事項であり、CEOの96％がビジネスの成功に不可欠と考えています。しかしその一方で、多くのCEOは、サイバー攻撃から組織を完全に守ることができないという悩みを抱えています。

組織におけるサイバーセキュリティ目標の達成を支援するため、米国国立標準技術研究所（NIST）は、広く採用されているサイバーセキュリティフレームワーク（CSF）を2024年2月に更新しました。NIST CSF 2.0は範囲が以前より拡大され、業種や業態を問わず全ての組織に適用できるようになりました。

NIST CSFとは

NIST CSFは、組織がサイバーリスクを最小限に抑えるためのサイバーセキュリティガイドラインとベストプラクティスをセットにしたもので、米国の全ての連邦政府機関と政府サプライヤーに義務付けられています。民間企業にとっては任意のフレームワークですが、セキュリティフレームワークを順守する組織の約74%がNIST CSFを使用しているという調査結果があります。

NIST CSFが広く採用されている理由は、その柔軟性にあるかもしれません。このフレームワークは、特定のツールやテクノロジーを指定するものではありません。その代わりに、ベストプラクティスのライブラリを提供しています。組織は、自社のリスクプロファイルや業界のニーズに最も適したプラクティスを選択することができます。

最近リリースされたCSFバージョン2.0は、業界や規模に関係なく、全ての組織にとってより柔軟で有用なフレームワークとなっています。このバージョンアップに伴い、NISTはフレームワークのコアガイダンスを更新し、組織やコミュニティ向けのCSF 2.0プロファイルテンプレートなど、いくつかのリソースを作成しました。

NIST CSF 2.0は拡張性も備えています。小企業は、このフレームワークの中核となる原則を活用して基本的なセキュリティ基盤を確立し、大企業は、このフレームワークに基づいてより洗練されたセキュリティプログラムを構築することができます。

NIST CSF 2.0の中核機能とは

NIST CSF 2.0は、効果的なサイバーセキュリティに不可欠な6つの中核機能（統治、識別、保護、検知、対応、回復）の概要を示しています。これらの機能は、組織が広範囲なセキュリティ戦略を構築するためのロードマップとなります。

- **統治：**これはNIST CSF 2.0の新機能で、明確なサイバーセキュリティガバナンス体制を確立することの重要性を強調するものです。これには、役割と責任の定義、サイバーセキュリティリスク管理戦略の策定、組織全体のセキュリティ対策の指針となるポリシーの策定などが含まれます。

- **識別：**このコア機能を通じて、組織は現在のサイバーリスクを把握することができます。これには、資産の棚卸し、脆弱性と脅威の検出、潜在的なサイバー脅威に関する情報の維持が含まれます。

- **保護：**ここでは、サイバー攻撃を防止し、その影響を軽減するための保護措置の導入に重点を置きます。この機能には、システムやデータの保護、アクセス制御の導入、ネットワークやデバイスの監視、従業員のトレーニングなどが含まれます。

- **検出：**セキュリティインシデントの早期発見は非常に重要です。この機能には、システムを継続的に監視し、攻撃を示す不審な活動を特定するためのセキュリティ対策を導入することが含まれます。

- **対応：**この機能は、セキュリティインシデントが発生した場合にとるべき行動につながります。インシデント対応の計画立案、被害拡大を防ぐインシデントの封じ込め、脅威の根絶、インシデントの報告などが含まれます。

- **回復：**組織は、サイバー攻撃を受けた後に通常業務を復旧できなければなりません。その中核となる機能は、事業継続性を確保する復旧計画の策定と維持です。これには、インシデント発生後に重要なシステムとデータを復元する手順が含まれます。

NIST CSF 2.0の仕組み

上記の6つのコア機能に加え、組織プロファイルも CSF 2.0の重要な要素です。組織プロファイルテンプレートはスプレッドシートで提供されます。組織が記入することで、現状と目標とするサイバーセキュリティプロファイルを決定することができます。このテンプレートには、各コア機能の下に約128のカテゴリとサブカテゴリがあり、それぞれに詳細なアウトカムの説明が記載されています。

例えば、Detect core機能には、Continuous Monitoring（DE.CM）とAdverse Event Analysis（DE.AE）の2つのカテゴリーがあります。DE.CMには5つ、DE.AEには6つのサブカテゴリーがあり、各サブカテゴリーは、特定のコア機能カテゴリーに落とし込むアウトカムと関連しています。サブカテゴリDE.AE-02のCSFアウトカムの説明は、「潜在的な有害事象を分析し、関連する活動をよりよく理解する」です。このようなアウトカムは、組織がサイバーセキュリティ態勢のあらゆる側面について深く考える上で役立ちます。

このテンプレートに記入する際、組織は適切と思われるカテゴリやサブカテゴリを含めたり除外したりできます。そして、各サブカテゴリのアウトカムを達成するために、特に以下の観点から、現在の、および目標とするサイバーセキュリティ対策を評価できます：

- 優先順位
- ステータス
- ポリシー、プロセス、手順
- 社内慣行
- 役割と責任
- 参考になる資料

プロファイルの完成後、組織は現状と目標としたサイバーセキュリティ態勢のギャップを分析し、目標に近づくための行動計画を立てることができます。行動計画が実行されると、プロファイルを再検討して更新し、その戦略が効果的であるかどうかを確認できます。

WhoisXML APIのインテリジェンスは、NIST CSF 2.0の実装にどのように役立つか

CSFの組織プロファイルテンプレートに目を通すと、組織は、ドメイン名、IPアドレス、DNSのデータを含む広範なインテリジェンスソースの必要性に気づくでしょう。こうしたサイバーインテリジェンスは、フレームワークの識別（ID）、保護（PR）、検知（DE）、対応（RE）の各機能で組織を支援することができます。以下は、WhoisXML APIのインテリジェンスが適応できるカテゴリの例です。

- **Asset Management (ID.AM):** 重要な資産を全て特定し、インベントリ化し、優先順位を付け、管理する必要があります。これらの資産には、企業が登録したドメイン名、ウェブサイトのメタデータ、SSL証明書、DNSレコードなど、WhoisXML APIが可視化できるものも含まれています。

- **Risk Assessment (ID.RA):** CSFの目的のひとつは、組織が直面するサイバーセキュリティリスクを理解することです。この目的を達成するためには、サイバー脅威につながる脆弱性やその他の弱点を特定する必要があります。WhoisXML APIのThreat Intelligence Data Feedは、特にID.RA-02（サイバー脅威インテリジェンスは、情報共有フォーラムや情報源から受信）を満たす上で役立ちます。さらに、ドメイン名、IPアドレス、DNSのデータポイントは、組織が見過ごす可能性のあるインフラの誤った設定を明らかにすることができます。

- **Identity Management, Authentication, and Access Control (PR.AA):** NISTはこのカテゴリのアウトカムについて、組織が資産へのアクセスを許可されたユーザー、サービス、ハードウェアに制限し、管理することであると説明しています。WhoisXML APIのIPインテリジェンスは、ここで役に立ちます。特に組織のサービスエリア外にあるデバイスや規制違反のIPアドレスを持つデバイスからの接続をブロックする際に有用です。組織が当社の脅威インテリジェンスソースを使う場合でも、悪意あるドメイン名、URL、IPアドレス、CIDR値、ハッシュをブロックすることができます。

- **Continuous Monitoring (DE.CM):** CSFのDetect機能の文脈では、継続的なモニタリングとは、異常、IoCを含む有害なイベントを見つけるために資産を追跡することを指します。このプロセスには、悪意あるインジケーターを探すためにネットワークやサードパーティサービスをスキャンすることが含まれますが、それはWhoisXML APIの脅威インテリジェンスデータをネットワークモニタリングツールに統合することで、より効果を上げることができます。

- **Adverse Event Analysis (DE.AE) とIncident Analysis (RS.AN):** 潜在的な悪意のリソースやイベントが検出されると、NIST CSF 2.0はさらに、DE.AEに基づいてそれらを分析することを組織に要求します。サイバーセキュリティインシデントが検出された場合も同様です（RS.AN）。特にパッシブDNSデータを使って収集した所有者、名前解決、設定、関連づけといった文脈情報を悪意あるインジケーターと照合することで、組織はこれらのアウトカムを達

成できるようになります。

まとめ

NIST CSFのコンプライアンスは、単にチェックボックスにチェックを入れれば完了ということにはなりません。顧客とビジネスを保護し、倫理的で責任ある運用の文化を醸成することが非常に重要です。組織のコンプライアンスを分析し、そのサイバーセキュリティ態勢がどの程度強固であるかを把握するためには、信頼できるサイバーインテリジェンスソースが必要になってきます。

NIST CSF 2.0の機能とカテゴリーを満たせるWhoisXML APIのサイバーインテリジェンスソースについて詳しくは、こちらにお問い合わせください。