NRI グループからのお知らせ
Notification from NRI Group

Nomura Research Institute Group

2020 年 5 月 20 日

NRI セキュアテクノロジーズ株式会社

NRI セキュア、防衛産業サプライチェーン向けガイドライン「NIST SP800-171」に準拠するための支援サービスを強化

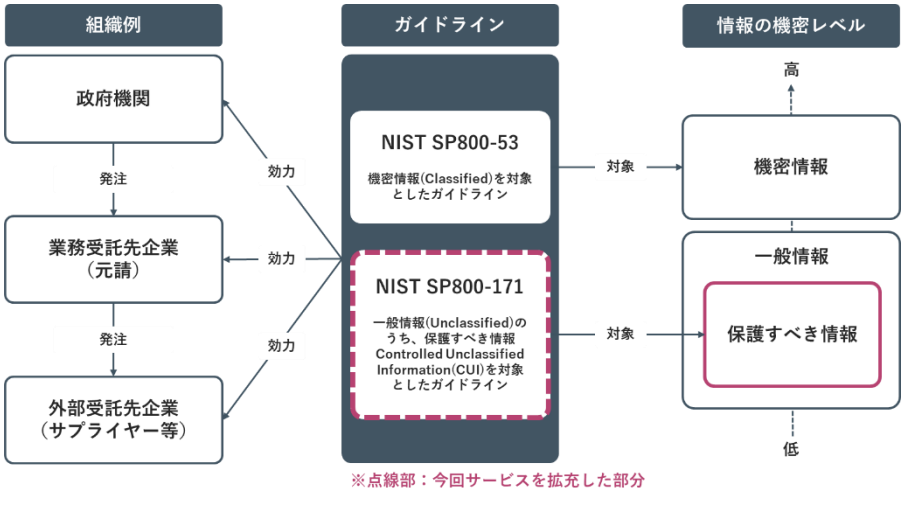
NRI セキュアテクノロジーズ株式会社（以下「NRI セキュア」）は、企業の情報セキュリティ対策状況を可視化するために独自に開発する標準化フレームワーク「NRI Secure Framework（以下「NSF」）」[1]において、米国立標準技術研究所（NIST）[2]が発行するガイドライン「NIST SP800-171」[3]に対応した、「NSF for NIST SP800-171」を新たに策定しました。NRI セキュアは、このフレームワークを活用することで、NIST SP800-171 の準拠を目指す企業に対し、「セキュリティ対策状況可視化サービス（以下「本サービス」）」の提供内容を強化します。

■ 防衛産業サプライチェーンを取り巻く背景

NIST SP800-171 は、「連邦政府外のシステムと組織における管理された非格付け情報の保護」と題されたガイドラインです。米国防総省では、全世界の取引先に対して NIST SP800-171 への準拠を求めています。具体的な要件は、ガバナンス体制の確立、管理体制の構築、システムへのセキュリティ対策の導入と運用、監査の実施など、多岐にわたります（要件の概要は、「ご参考」を参照）。

日本の防衛省も、2019 年 5 月に NIST SP800-171 相当のセキュリティ要求事項を調達基準に盛り込みました。現在影響を受けているのは、日米の防衛産業サプライチェーンに含まれる、製造業・重工業・建機メーカーなどの元請け企業や、これらの企業に対して部品などを提供するメーカーなどが主ですが、今後は他の産業にも同様の基準が適用されていくと考えられています。

図：情報の保護に関する NIST のガイドラインと、対象組織、情報の機密レベルの関係図



■ 本サービスの概要と特長

NSF for NIST SP800-171 は、NIST の各種ガイドラインを熟知したセキュリティコンサルタントが、200 社以上の利用実績を持つ NSF に、NIST SP800-171 の要件を組み込み、策定したフレームワークです。このフレームワークを用いて、「誰が」「何に対し」「どのような対策」を実施すべきである、などの具体的な提言をはじめ、準拠に向けたロードマップ策定からセキュリティ対策の実行までを幅広く支援します。

NIST SP800-171 を正確に解釈するには、事前知識やノウハウが必要です。本サービスをご利用いただくことで、難解な要件の解釈にお客さまの労力をかけることなく、自社の準拠状況を迅速かつ確実に可視化でき、セキュリティ対策の検討にかかる時間を大幅に短縮できます。また、企業の海外拠点に対しても、野村総合研究所グループの海外現地法人などと連携し、国内と同様の支援を行うことが可能です。お客さまのグループ全体での準拠を支援することができます。

本サービスは、以下の 3 つの内容から構成されます。

① NIST SP800-171 準拠状況の可視化および対策を提示

NSF for NIST SP800-171 やそのほかの関連するガイドライン[4]と照らし合わせ、お客さまのセキュリティ対策がどの程度 NIST SP800-171 に準拠しているのか、現状把握・分析を行い、準拠のために必要なセキュリティ対応策を提示します。

② セキュリティ対策のロードマップ策定支援

NIST SP800-171 準拠状況の可視化後、準拠に必要な対策を確実に実行するために、整備が必要な社内規程や運用体制、人員・設備面、技術対策など、セキュリティ対策の整理を行います。そして整理されたセキュリティ対策について優先度を定義した上で、お客さまに適した実効性のある計画策定を支援します。

③ セキュリティ対策の実行支援

ロードマップ上の施策が実行完了するまで、一気通貫で支援します。お客さまの要望や課題に応じて、最適なセキュリティソリューションの提示から、運用設計支援、セキュリティ対策導入時の PMO（プロジェクト・マネジメント・オフィス）支援、継続的なセキュリティ監視体制のアドバイザリなどが含まれます。

さらに、セキュリティ対策実装に関する当社独自の知見を用いて、プラットフォームや WEB アプリケーションを対象にした技術的な診断や、情報システムに対する実機での評価（脆弱性診断）なども、オプションとして提供します。

本サービスの詳細については、以下の Web サイトをご参照ください。

https://www.nri-secure.co.jp/service/consulting/nist-sp800-171

NRI セキュアは、今後も、企業・組織の情報セキュリティ対策を支援するさまざまな製品・サービスを提供し、グローバルな規模で安全な情報システム環境と社会の実現に貢献していきます。

---

[1] 「NRI Secure Framework（NSF）」：
組織・拠点ごとに利用する情報システムや体制のセキュリティレベルを横断的に評価するために、NRI セキュアが策定した標準化フレームワーク。NSF は、NRI セキュアが長年にわたるコンサルティングで培ってきたノウハウと、国内及び海外の著名なセキュリティ対策基準で掲げられている要求を解釈し、ここ数年のサイバーセキュリティトレンドや脅威の動向を踏まえて継続更新されています。金融、運輸、製造、エネルギー、商社、不動産など、多様な業界の多くの企業に対して、NSF を活用したセキュリティコンサルティングサービス（セキュリティ対策状況可視化サービス）の提供実績があります。NSF の詳細については、次の Web サイトをご参照ください。
https://www.nri-secure.co.jp/service/consulting/security_visualization

[2] 米国立標準技術研究所（NIST）：
National Institute of Standards and Technology の略称。科学技術分野における計測と標準に関する研究を行うアメリカ商務省に属する政府機関。

[3] 「NIST SP800-171」：
米国政府は 2010 年に公布した大統領行政命令 13556 により、連邦政府が取り扱う「一般情報（Unclassified）」のうち、一部を「保護すべき情報（Controlled Unclassified Information：CUI）」として管理を求めるようにしました。この CUI を管理することを目的として、NIST が策定したガイドラインが NIST SP800-171 です。NIST SP800-171 の要件は、ガバナンス体制の確立、管理体制の構築、システムへのセキュリティ対策の導入と運用、監査の実施などテーマが幅広いことが特徴。

[4] 関連するガイドライン：
NIST SP800-171A（「Assessing Security Requirements for Controlled Unclassified Information」）、NIST SP800-53（「連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策」）、NIST SP800-37（「連邦政府情報システムに対するリスクマネジメントフレームワーク適用ガイド：セキュリティライフサイクルによるアプローチ」）、NIST Handbook162（「NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements」）、ISO/IEC27001（「情報セキュリティマネジメントシステム(ISMS)認証」）など。

【お知らせに関するお問い合わせ先】

NRI セキュアテクノロジーズ株式会社　広報担当

TEL：03-6706-0622　E-mail：info@nri-secure.co.jp

【ご参考】

■ NIST SP800-171 の要件概要

分類	タイトル	概要
ガバナンス	意識向上と訓練	セキュリティポリシーを遵守すること
	リスク評価	情報資産のリスクを適切に評価すること
	セキュリティ評価	セキュリティ管理策を定期的に評価すること
セキュリティ対策の導入と運用	アクセス制御	システムへアクセスできる人/機能を制限すること
	構成管理	システムを構成する機器に求められるセキュリティ構成設定を確立すること
	識別と認証	システム利用者、デバイスを識別すること
	メンテナンス	組織のシステムのメンテナンスを行うこと
	記憶媒体の保護	CUIをセキュアに格納すると共にアクセスできるものを制限すること
	物理的保護	組織のシステム、装置等への物理的アクセスを制限すること
	システムと通信の保護	システムの通信を監視し、制御し、保護すること
	システムと情報の完全性	脆弱性情報の収集、監視、パッチ適用などの活動を通してタイムリーにシステムと情報の完全性を担保すること
管理体制	インシデント対応	インシデントの追跡、報告ができること
	要員のセキュリティ	システムへのアクセスを行う個人を審査すること
監査	監査と説明責任	システムの監査を行うとともに責任の追及ができること

■ 「セキュリティ対策状況可視化サービス」の流れ