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

Nomura Research Institute Group

2020 年 9 月 24 日
NRI セキュアテクノロジーズ株式会社

NRI セキュアのセキュリティ対策実行支援プラットフォーム「Secure SketCH」が、米国の 2 ガイドラインに対応

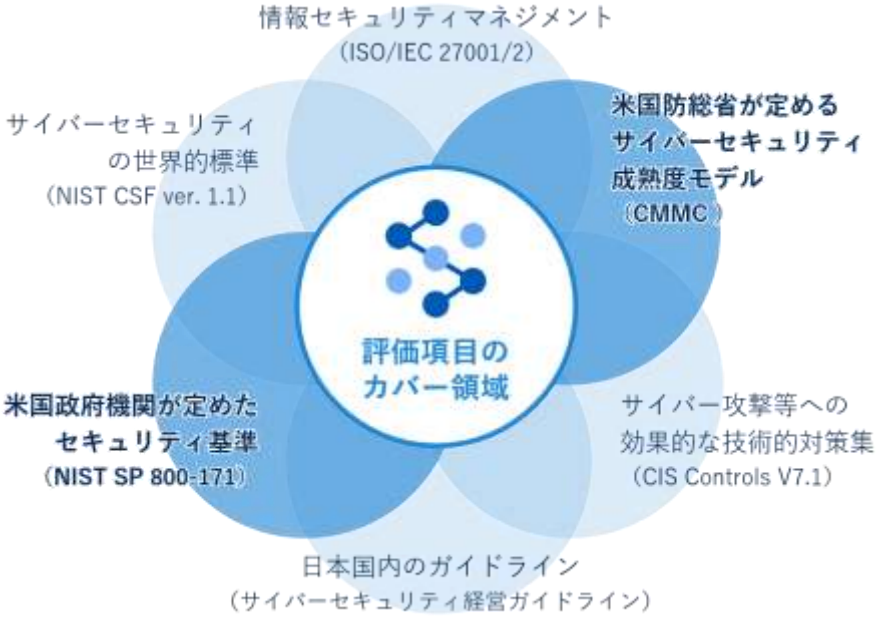
～ 米国防総省 CMMC と NIST SP800-171 への準拠状況が把握可能に ～

NRI セキュアテクノロジーズ株式会社（以下「NRI セキュア」）は、企業による情報セキュリティ対策の実行を支援するプラットフォーム「Secure SketCH（セキュア スケッチ）」において、有償の「PREMIUM プラン」で提供している「ガイドラインチェック機能」の対象として、新たに 2 つのガイドラインを追加し、本日提供を開始します。

「Secure SketCH」は、企業の情報セキュリティ担当者が Web 上で約 80 の設問に回答することで、自社におけるセキュリティ対策の状況を定量的に可視化し、必要な対策の把握と推進に役立てることができるプラットフォーム型のサービスです。本年 9 月 24 日現在、無償プランも含め 1,700 以上[1]の企業等に利用されており、そのうち有償プランの利用組織数は 300 を超え[2]、組織の規模や業種を問わず利用されています。

2019 年 4 月より提供している「ガイドラインチェック機能」は、自社のセキュリティ対策状況が国内外の各種セキュリティガイドラインにどの程度準拠しているかを分析し、その準拠状況を確認するための機能です。業種を問わない最大公約数の評価項目となるように、主要なガイドラインを幅広く参照しており、これまで、「NIST Cybersecurity Framework Version 1.1」[3]、「経済産業省 サイバーセキュリティ経営ガイドライン Ver 2.0」[4]および「経済産業省 情報セキュリティ管理基準（平成 28 年改正版）」[5]、「CIS Controls V7.1」[6]に対応してきました。

図：Secure SketCH が対応しているガイドライン



※太字が今回追加したガイドライン

昨今、企業のサプライチェーンを狙ったサイバー攻撃が増加しており、実際に被害が発生した事例も明らかになっています。このため、サプライチェーン上に存在するすべての関連企業や業務委託先にとって必要な、セキュリティ対策への関心や検討意欲が高まっています。

このような背景から、このたび、サプライチェーンのセキュリティ対策に対応している「米国防総省 CMMC」[7]および「NIST SP 800-171」[8]を、新たに追加しました。これにより、Secure SketCH の設問に回答するだけで、米国政府がサプライチェーン内の請負業者に対して求めるセキュリティ要件について、自社の準拠状況を自動的に算出・表示することが可能になります（表示イメージは、文末の「ご参考」を参照ください）。

Secure SketCH の詳細については、次の Web サイトをご参照ください。

https://www.secure-sketch.com/

NRI セキュアは今後も、Secure SketCH の機能強化・品質維持向上に努め、グローバルな規模で安全・安心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] 無償の「FREE プラン」と、有償の「STANDARD プラン」「PREMIUM プラン」「GROUPS プラン」の利用組織数の合計です。

[2] 有償の「STANDARD プラン」「PREMIUM プラン」「GROUPS プラン」の利用組織数の合計です。

[3] NIST Cybersecurity Framework Version 1.1：
米国国立標準技術研究所（NIST：National Institute of Standards and Technology）が発行する「重要インフラのサイバーセキュリティを改善するためのフレームワーク 1.1 版」を指します。ビジネスと組織の両方のニーズに基づいた、費

用対効果の高いサイバーセキュリティリスク対策・管理について記されています。重要インフラ向けに作成されたものですが、あらゆる業界で利用可能で、日本語訳が情報処理推進機構（IPA）より、次の Web サイトで公開されています。https://www.ipa.go.jp/files/000071204.pdf

[4] 経済産業省 サイバーセキュリティ経営ガイドライン Ver 2.0：
経済産業省が IPA とともに策定したガイドラインです。サイバー攻撃から企業を守る観点で、経営者が認識する必要のある「3 原則」と、企業の最高情報セキュリティ責任者（CISO）などの担当幹部に経営者が指示すべき「重要 10 項目」をまとめています。

[5] 経済産業省 情報セキュリティ管理基準（平成 28 年改正版）：
同じく経済産業省が策定したガイドラインです。情報セキュリティマネジメントシステム（ISMS）に関する国際規格「ISO/IEC 27001」と整合が取られた、情報セキュリティマネジメント体制を構築し、適切な管理策を整備・運用するための実践的な規範です。

[6] CIS Controls V7.1：
米国の産官学から成る非営利団体 The Center for Internet Security（CIS）が管理するフレームワークです。サイバーセキュリティに関する技術分野に焦点を当て、現在発生しているサイバー攻撃や近い将来に発生が予測される攻撃の傾向を踏まえ、多岐にわたる対策の中から、自社（組織）が実施すべき対策と、その優先順位を導くためのアプローチを提示しています。なお、NRI セキュアは、V3 以降、日本語への翻訳を担当しています。日本語版は次の Web サイトからご覧いただけます。https://learn.cisecurity.org/control-download

[7] 米国防総省 CMMC：
米国防総省（DoD：United States Department of Defense）が発行する、サイバーセキュリティ成熟度モデル認証（Cybersecurity Maturity Model Certification）のフレームワークで、主に DoD が請負業者に調達する際の要件として認証取得を促すものです。2020 年 1 月に v1.0 が公開されました。

[8] NIST SP 800-171：
米国国立標準技術研究所（NIST：National Institute of Standards and Technology）が発行する「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。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（CUI：Controlled Unclassified Information）」として管理することを目的に、2015 年 6 月に発行されました。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、DoD 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。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。

【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】

■ 「ガイドラインチェック機能」の画面