News Release

2017 年 3 月 6 日
NRI セキュアテクノロジーズ株式会社

最適なセキュリティ対策を実現する「IoT セキュリティコンサルティングサービス」を提供開始
～IoT や制御システムのセキュリティ状況を可視化～

NRI セキュアテクノロジーズ株式会社（本社：東京都千代田区、代表取締役社長：小田島 潤、以下「NRI セキュア」）は、IoT（モノのインターネット）やそれに関わる制御システムを対象とするセキュリティ対策について、状況把握から最適なセキュリティ対策の実行までを支援する「IoT セキュリティコンサルティングサービス」（以下、「本サービス」）を、本日、提供開始します。

■ 独自開発したフレームワーク「NSF for IoT」を用いて、セキュリティ対策の定量評価を可能に

本サービスは、NRI セキュアが独自に開発した、IoT や制御システムに特化したセキュリティ状況の可視化フレームワーク「NRI Secure Framework(NSF) for IoT」を用いて提供します。このフレームワークは、国内外の複数の関係機関がそれぞれ発行する IoT に関するガイドラインなど※1 の要求事項を、NRI セキュアの専門家が解釈して選択・統合するとともに、IoT に関するサイバー攻撃の傾向や脅威を踏まえた上で作成されています。また、各企業における IoT に関するセキュリティの定義に関係なく、同じ物差しで他社比較を含むセキュリティ対策レベルの定量評価ができます。

本サービスでは、このフレームワークを用いて、NRI セキュアが当該企業の IoT および制御システムに関するセキュリティの状況を網羅的かつ具体的に把握、評価し、課題を抽出します。そして、事業の種類や環境、対象となる技術や機器などに応じた最適な対応策を提示します。

NRI セキュアは、これまで電気やガス、水道、石油などの重要インフラのシステムや、グローバル製造業のデバイス機器や工場のシステムなどを対象として、セキュリティの確保・向上を目的とするコンサルティングを行ってきました。また、IoT や制御システムの標準化活動なども行っており、これらを通じて培った知見が「NSF for IoT」に活かされています。「NSF for IoT」は、重要インフラ分野や製造業の IoT に関するセキュリティ対策立案などで、既に多くの利用実績があります。

■ 本サービスを構成する 4 つのメニュー

1. 現状課題の把握、セキュリティリスクの可視化と対策ロードマップの策定
   本サービスを導入する企業の IoT および制御システムについて、セキュリティの現状を「NSF for IoT」を使用して把握し、可視化します。その後、組織・拠点ごとのセキュリティの実態を横断的に評価・分析し、セキュリティ対策の立案とロードマップの策定を行います。
2. ポリシー・ガイドライン策定
   順守すべき IoT セキュリティの要件や、ルール、ガイドラインなどを策定します。対象事業全般に共通する汎用的なものから、事業特性に応じたポリシー・ガイドラインに至るまで策定が

可能です。

3. セキュリティに関する脆弱性診断

   IoT で使われる制御機器や組み込みデバイスなどを対象に、脆弱性が残存していないかについて実機評価を行います。アキレス認証※2 サービスにも対応できます。

4. 実行支援

   「NSF for IoT」で整理・立案した対策・ロードマップを元に、施策の実行支援を行います。具体的には、IoT における CSIRT※3 構築支援や、ソリューション・サービスの要件整理・導入実行支援など、幅広く対応します。

「IoT セキュリティコンサルティングサービス」の詳細は、以下の URL をご参照ください。
https://www.nri-secure.co.jp/service/consulting/iot_security.html

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 IoT に関するガイドラインなど：
IoT 推進コンソーシアム「IoT セキュリティガイドライン」、NIST「Cybersecurity Framework」、NIST「NISTIR 7628」、OWASP「IoT Security Guidance」、ISMS「ISO/IEC 27001」、「CSMS 認証基準（IEC 62443-2-1）」など。

※2 アキレス認証：
GE デジタル傘下のワールドテックが策定した産業用制御デバイスの認証プログラム。NRI セキュアは、日本で初めての本プログラムを提供する第三者機関となった。未知のセキュリティ脆弱（ぜいじゃく）性を検出するためのロバストネス検証（開発者にとって想定外の異常データを自動生成して送信し、対象の挙動の変化を確認する検証手法）を、制御デバイスに特化して行うツールである Achilles Testing Platform (ATP) を用い、一定のセキュリティ水準を満たすと認証を取得することが可能。

※3 CSIRT（Computer Security Incident Response Team）：
組織内において、情報セキュリティの問題に対して専門に対応する組織。

【ニュースリリースに関するお問い合わせ】
株式会社野村総合研究所　コーポレートコミュニケーション部　海藤、松本
TEL：03-5877-7100　E-mail：kouhou@nri.co.jp

【サービスに関するお問い合わせ】
NRI セキュアテクノロジーズ株式会社　ストラテジーコンサルティング部　山口、金子
広報　根本
TEL：03-6706-0622　E-mail：info@nri-secure.co.jp