



Nomura Research Institute Group

## NEWS RELEASE

2020年8月4日

NRI セキュアテクノロジーズ株式会社

### NRI セキュア、IoT 機器向けの開発ガイドラインを販売開始

～ コンサルティングと診断で培ったノウハウを盛り込み、国内外のセキュリティ標準を網羅 ～

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、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）機器を開発する企業向けに、開発時に組み込むべきセキュリティ要件をまとめた「IoT セキュア開発ガイドライン（以下「本ガイドライン」）」の販売を、本日開始します。

本ガイドラインは、NRI セキュアが長年にわたり実施してきた IoT 機器メーカーに対する開発支援コンサルティングと、IoT 機器に関する豊富なセキュリティ診断の経験で培ってきたノウハウ、および NIST（米国標準技術研究所）など、国内外の公的機関・団体などから発行されている IoT 関連のセキュリティ標準やガイドライン<sup>1</sup>で求められる対策を集約・統合したものです。最新の技術動向を取り込み、IoT 機器のセキュアな開発を支援します。

#### ■ 開発時点におけるセキュリティ対策の重要性

IoT が普及するにつれ、IoT 機器を狙ったサイバー攻撃や、セキュリティ上の脆弱性の報告件数が増加しています。背景には、開発工程で十分なセキュリティ対策がなされないまま、サイバー攻撃に対して脆弱な機器が多数出荷されていることが挙げられます。IoT 機器は、出荷された後では脆弱性の修正が困難な場合が多く、開発時点で製品特性に合わせたセキュリティ対策を講じることが重要です。

#### ■ 「IoT セキュア開発ガイドライン」の概要

本ガイドラインでは、IoT 機器開発に関する長年の支援実績を踏まえて、開発の工程ごとに実施すべき対策を取り上げ、実装方式や設定値の具体例を挙げながら解説しています。また、実際に発生したインシデント（事件・事案）の事例をもとに、各要件を取り込まない場合のリスクについても紹介しています。

本ガイドラインを活用することで、一定のセキュリティ水準を保ちながら、IoT 機器の設計・開発が可能になります。開発を社外に委託する場合においても、本ガイドラインを委託先と共有することにより、順守すべきセキュリティ基準を明確に示すことができます。また個別の企業ごとに、適合が求められる業界標準規格や社内ポリシーを取り入れ、カスタマイズしたガイドラインを策定することも可能です（オプションサービス）。

## ■ IoT システム全体のセキュリティをトータルで支援

NRI セキュアでは、「Web アプリケーション」および「スマートフォンアプリケーション」向けのセキュリティ開発ガイドラインも、それぞれ販売しています（下図を参照）。これらと本ガイドラインをあわせてご利用いただくことで、IoT システム全体のセキュアな設計・開発が可能となります<sup>2</sup>。このほか、上流工程における開発支援コンサルティングサービスやセキュリティ診断を組み合わせることで、セキュリティ水準の高い IoT システムの構築をトータルで支援します。

図：IoT システム全体のセキュリティを支える3つのガイドライン



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・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。

<sup>1</sup> 本ガイドラインは、以下のセキュリティ標準やガイドラインの項目を踏まえて作成しています。（2020年8月4日時点）

- NIST, NISTIR 8200 “Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT)”
- NIST, NISTIR 8228 “Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks”
- NIST, NISTIR 8259 (Draft) “Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline”

- NIST, NISTIR 8267 (Draft) “Security Review of Consumer Home Internet of Things (IoT) Products”
- NIST, White Paper (Draft) “Internet of Things (IoT) Trust Concerns”
- ENISA, “Good Practices for Security of IoT - Secure Software Development Lifecycle”

など

<sup>2</sup> Web アプリケーション、スマートフォンアプリケーション、IoT 機器のセキュア設計・開発ガイドラインの詳細については、次の Web サイトをご参照ください。<https://www.nri-secure.co.jp/service/assessment/guideline>

**【ニュースリリース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](mailto:info@nri-secure.co.jp)