

2017 年 10 月 18 日

株式会社日立情報通信エンジニアリング

日立独自の「鍵付け替え技術」により、IoTシステムの高セキュア化を実現する データ保護ソリューション「IoTデータセキュリティ」のサービス提供を開始

株式会社日立情報通信エンジニアリング(代表取締役社長:岩崎 秀彦、本社:神奈川県横浜市)は、IoT^{*1}時代に求められる、より安心・安全なセキュリティニーズに対応するため、日立独自の「鍵付け替え技術」の採用により、安全なデータ共有とお客さまによる暗号鍵管理の運用負荷の軽減を可能にし、IoT システムの高セキュア化を実現する、IoT 機器組み込み型のデータ保護ソリューション「IoT データセキュリティ」のサービス提供を 10 月 20 日より開始します。

IoT 時代の到来により、さまざまな「モノ(Things)」がネットワークにつながるようになり、利便性が格段に向上する一方で、IoT 機器で取り扱う内部保持データに対する不正アクセスや情報漏えいなどのセキュリティリスクが急速に高まっています。そのため、データ共有シーンにおいて、安全で安心なセキュリティ対策を実現するサービス・ソリューションが強く求められています。

「IoT データセキュリティ」は、IoT 機器間(End to End)におけるシステムデータを暗号化によってガードするデータ保護ソリューションです。暗号データの共有化を安全に行うことができるデータ「暗復号ソフトウェア」と、お客さまによる暗号鍵管理の運用負荷を軽減する「鍵管理サービス」により、セキュアな環境構築をサポートします。

「暗復号ソフトウェア」は、株式会社日立製作所の「鍵付け替え技術 ^{*2}」の採用により、お互いの暗号鍵を共有することなく、データ利活用を可能にします。また、暗号データを平文化せずに異なる暗号鍵に付け替え(再暗号化)が可能のため、データ共有時の漏えいリスクを排除できます。また、IoT 機器への組み込みを考慮し、OS レスの処理性能の低い機器でも利用できる軽量・コンパクトなソフトウェアとしており、さまざまな用途でのセキュリティ強化に利用できます。

さらに、「鍵管理サービス」は、IoT 機器に組み込まれる暗号鍵の増加に伴い複雑化する暗号鍵の運用管理を一括管理し、お客さまの運用負荷を軽減します。

「IoT データセキュリティ」を導入することにより、これまでの安価なインターネット回線を高セキュア化できるため、安全性の担保が必要な制御データの保護や、組み込み機器のファームウェアの更新、暗号化されたデータのネットワーク上ストレージへの一時的保管など、製造業や公共、インフラをはじめ、さまざまな用途で、End to End のデータ共有を安全に行うことが可能になります。

なお、本ソリューションは、「Hitachi Social Innovation Forum 2017 TOKYO^{*5}」、ならびに「SCF2017/計測展 2017 TOKYO^{*6}」の日立ブースで展示紹介します。

社会の未来を変えるアイデアがここに

Hitachi Social Innovation Forum 2017 | TOKYO

*1 IoT: Internet of Things

2 株式会社日立製作所 特許技術(特許第 6033741 号)。共通鍵暗号方式の暗号アルゴリズム(AES)により、暗号化されたデータを平文にすることなく、異なる暗号鍵に再暗号化する技術で、CELLOS*⁴にて暗号プロトコルの安全性評価済。

*3 AES: Advance Encryption Standard、高度暗号化標準。

*4 CELLOS: Cryptographic protocol Evaluation toward Long-Lived Outstanding Security Consortium、暗号プロトコル評価技術コンソーシアム。

*5 2017 年 11 月 1 日(水)～2 日(木)開催@東京国際フォーラム

*6 2017 年 11 月 29 日(水)～12 月 1 日(金)開催@東京ビッグサイト

■主な特長

1. End to End で データを保護(IoT 機器間)

- ・IoT機器内部で、シームレスにデータの暗号化・復号化を実現します。
- ・OSレスでも実装可能な、軽量・コンパクトなアプリケーションソフトウェアを提供します。
- ・改ざん検知機能を「暗復号ソフトウェア」に実装しているため、データの不正な書き換えリスクを低減します。

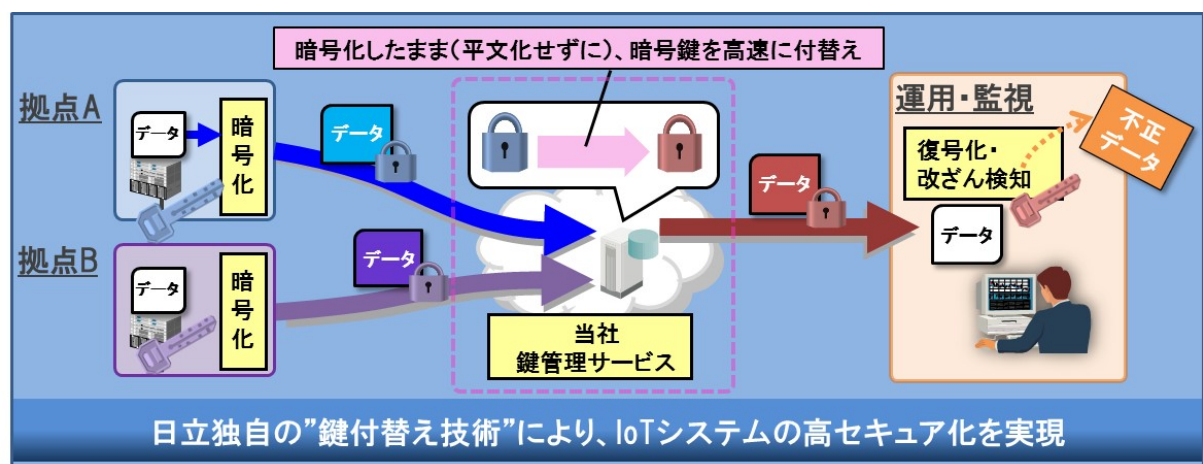
2 「鍵管理サービス」を提供

- ・複雑化する暗号鍵の運用管理を一括管理し、お客さまの運用負荷を軽減します。
- ・定期的な鍵更新作業を削減できるため、管理者の負担を低減します。

3. 暗号鍵の漏えいリスクを縮小化

- ・機器同士がデータを暗号したまま共有可能となり、データ漏えい脅威の影響範囲を縮小化します。
- ・一度も平文化せずにEnd to Endでデータの共有が可能のため、経路上におけるハッキングリスクの低減が可能です。

■「IoTデータセキュリティ」のイメージ図



■「IoTデータセキュリティ」の価格、および提供開始日について

品名	提供内容	標準価格(税別)	提供開始日
IoT データセキュリティ ソリューション	・ 暗復号ソフトウェア	16,000 円/装置	2017 年 10 月 20 日
	・ 鍵管理サービス	3,000 円/月・装置～	
	・ 実装サービス	個別見積もり	

■「IoT データセキュリティ」に関するホームページ

<http://www.hitachi-ite.co.jp/products/iotsec/index.html>

■「Hitachi Social Innovation Forum 2017 TOKYO」に関するホームページ

<http://hsiftokyo.hitachi/>

■「SCF2017／計測展 2017 TOKYO」に関するホームページ

<http://scfmcs.jp/>

■商標に関する表示

記載の会社名、製品名はそれぞれの会社の商標もしくは登録商標です。

■お客さまお問い合わせ先

株式会社 日立情報通信エンジニアリング 営業統括本部 営業戦略本部 [担当:川口]
〒220-6125 神奈川県横浜市西区みなとみらい 2 丁目 3 番 3 号 クイーンズタワーB 25 階
電話:050-3101-2429 (直通)

■報道機関お問い合わせ先

株式会社 日立情報通信エンジニアリング 経営・事業企画本部 企画部 [担当:中村]
〒220-6122 神奈川県横浜市西区みなとみらい 2 丁目 3 番 3 号 クイーンズタワーB 22 階
電話:050-3163-5726 (直通)

以上

このニュースリリース記載の情報(製品価格、製品仕様、サービスの内容、発売日、お問い合わせ先、URL 等)は、発表日現在の情報です。予告なしに変更され、検索日と情報が異なる可能性もありますので、あらかじめご了承ください。
