ICカード技術を応用してセキュアなネットワークを実現するIoTセキュリティーソリューション

Security Solution for IoT Systems to Realize Secure Network Applying Smart Card Technologies

友枝　裕樹 TOMOEDA Yuki　　福岡　寛規 FUKUOKA Hiroki　　杉渕　慶 SUGIBUCHI Kei

近年，重要インフラの監視制御システム，及び製造業の製造拠点に対するサイバー攻撃のリスクが高まっている。海外では，サイバー攻撃によると思われる大規模停電が発生しており，我が国でも重要インフラなどにおけるセキュリティー確保に向けた各種の取り組みが行われている。

東芝インフラシステムズ（株）は，ICカード事業で培ったセキュリティー技術を応用したIoT（Internet of Things）セキュリティーソリューションの開発と製品化に取り組んでいる。ICカードに使う耐タンパー性の高いチップを実装したセキュリティープロキシーデバイスは，ネットワークを構成する様々な機器に外付けするだけで，セキュアな通信を実現する。IIoT（インダストリアルIoT）分野だけでなく，重要インフラなどのセキュリティー強化と最適なオペレーションに貢献できる。

The expansion of Internet of Things (IoT) systems in recent years has led to an increase in security risks from cyberattacks on monitoring and control systems for critical infrastructure systems and their components. Following reports in other countries of events believed to be due to cyberattacks including a large-scale blackout, various countermeasures against this growing threat have been introduced to improve cybersecurity in Japan.

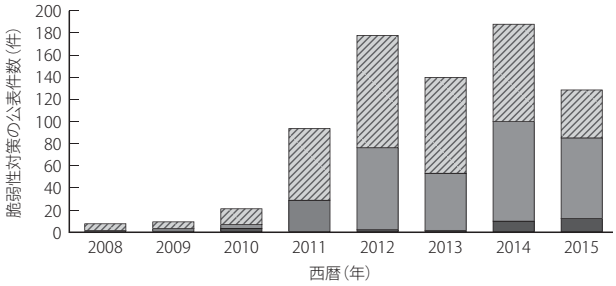
As part of its efforts in this field, Toshiba Infrastructure Systems & Solutions Corporation has developed and released an IoT security solution based on security technologies acquired through the development of smart cards. This solution achieves secure communication by externally connecting newly developed security proxy devices, which incorporate a chip with high tamper-resistance performance developed for smart cards, to each component in the network. It is expected to contribute to the strengthening of cybersecurity and optimal operation of critical infrastructure systems as well as industrial IoT systems.

1. まえがき

IIoTと呼ばれている産業分野のIoTでは，これまで収集できていなかった既存の機器やシステム内の情報を収集し，その中から意味のある情報を抽出して，サービスに利用したり，オペレーションの効率化に活用したりする取り組みが進められている。今後，収集した情報を基に，オペレーション効率を向上させる最適なデータを見いだし，機器やシステムにフィードバックするといったフェーズへ進化していくと考えられる。情報を機器やシステムから収集するフェーズでは，セキュリティーはそれほど重要視されていないが，機器やシステムへのフィードバックというフェーズでは，“データの完全性（改ざんされていないか）”，及び“機器やシステムの可用性（使いたいときにきちんと使えるか）”の確保という観点から，セキュリティーがより重要になってくる。

重要インフラについては，これまでベンダー独自のプロトコルで，物理的に完全に隔離された状態で運用されることが多かったが，機器の汎用化や，プロトコルのオープン化，IIoTを活用するためのネットワーク化が進み，様々な脆弱（ぜいじゃく）性が指摘されるようになってきている。例えば海外では，ネットワークが外部につながっていなくても，システムの可用性を低下させるセキュリティーインシデントが発生している。一方，我が国では，海外に比べるとセキュリティーリスクに対する意識がまだ低く，重要インフラをはじめとしてサイバー攻撃の対象になる可能性が高いため，政府を中心にサイバー攻撃の対策に関する取り組みが行われている。

図1に示すように，ここ数年で制御システムに関する脆弱性対策の公表件数は徐々に増えてきており[(1)]，この傾向は今後も続くと考えられる。セキュリティーは目に見えないため，対策の費用対効果が分かりにくいが，2017年5月に発生したランサムウェアWannaCryのように，感染すると対象システムを復元するために膨大な費用が発生する場合もある。



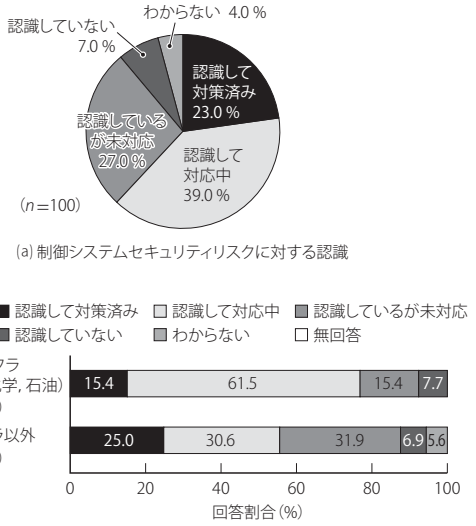
西暦（年）	2008	2009	2010	2011	2012	2013	2014	2015
深刻度Ⅲ（件）	6	6	14	64	101	86	87	43
深刻度Ⅱ（件）	2	4	4	29	74	52	90	73
深刻度Ⅰ（件）			4	1	3	2	11	13

＊独立行政法人 情報処理推進機構「制御システム利用者のための脆弱性対応ガイド 重大な経営課題となる制御システムのセキュリティリスク ～制御システムを運用する企業が実施すべきポイント～ 第3版」[1]を基に作成

図1. 脆弱性対策情報を公表した制御システムの年別公表件数

ここ数年，脆弱性対策の公表件数が増加する傾向にある。

Published number of security vulnerabilities of industrial control systems by year



n, *N*：件数

＊IPA「制御システムユーザ企業の実態調査報告書」[2]を基に作成

図2. IPAによる制御システムに関するアンケート結果1

重要インフラの方が，「認識して対策済み」と「認識して対応中」を合わせた回答の割合が高く，制御システムのセキュリティーリスクに対する意識が高いと考えられる。

Results of questionnaire (1) regarding industrial control systems reported by Information-technology Promotion Agency, Japan (IPA)

そのため，セキュリティーインシデントが起こる前にきちんと対策をしておくことが重要である。

ここでは，東芝インフラシステムズ（株）が開発した，様々な社会インフラのシステム全体をセキュアにすることができるIoTセキュリティーソリューションの概要と特長について述べる。

2. 社会インフラ分野でのセキュリティーへの取り組み

セキュリティーは，一部分だけを強固にしても，ほかの部分に脆弱性があれば，そこを攻撃されて全体のセキュリティーレベルが低下する。一般に，重要インフラをはじめとした社会インフラシステムでは，様々なベンダーの機器やシステムが混在し，OS（基本ソフトウェア）の種類やバージョンも複数存在する。サブシステムレベルで見ても，導入時期が異なり，運用年数も10年以上というものも多いため，全てを一度にリプレースすることは難しい。このような背景から，なかなかシステム全体をセキュアにするのは難しいという側面がある。また，IT（情報技術）分野とは異なり，社会インフラ分野では，どんなときでもシステムが確実に稼働することが求められるため，セキュリティーの3要素である“機密性（情報が漏えいしないこと）”，“完全性（情報が改ざんされないこと）”，“可用性（情報がいつでも使えること）”のうち，可用性が最優先される。したがって，タイムリーにセキュリティーパッチを適用できない，あるいは全く適用できないというケースも多い。

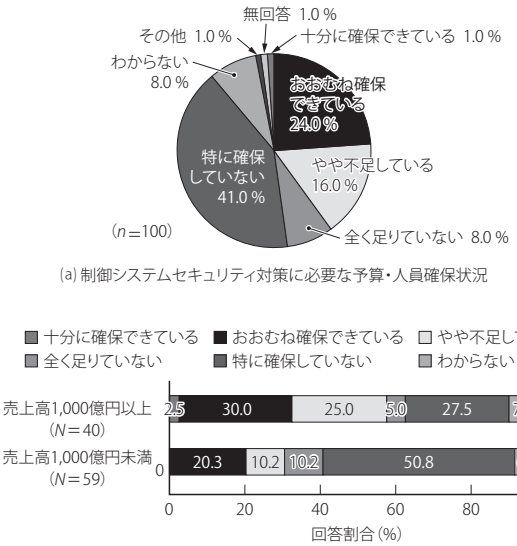
社会インフラ分野でも，生産性向上のためにICT（情報通信技術）化やIIoT化が急速に進んでいる。例えば，外部ネットワークに直接つながっていない制御システムや工場内ネットワークについても，インターネットやメールが使われる社内の業務ネットワークに対して標的型攻撃が行われ，数台のPC（パソコン）がマルウェアやランサムウェアに感染した場合，セキュリティーパッチが施されていない機器を含む上記のようなシステムに，社内ネットワークを介して感染が拡大するおそれがある。

IPA（独立行政法人 情報処理推進機構）によるアンケート結果[2]を見ると，ITシステムのセキュリティー対策はしっかりできていても，上記のような社会インフラシステムのセキュリティー対策は遅れ気味であることが分かる（**図2**，**図3**）。

3. IoT セキュリティーソリューション

当社は，2章で述べたような制約を考慮した，社会インフラ分野のシステム全体をセキュアにするソリューションを開発し，その製品化を進めている。

本来，ネットワークの終端に位置する機器（以下，エンドポイントと略記）そのものをセキュアにして，システム全体をセキュアにすることが王道と考えられるが，2章で述べた背



＊IPA「制御システムユーザ企業の実態調査報告書」[2]を基に作成

図3. IPAによる制御システムに関するアンケート結果2

予算・人員確保状況を売上高別に見ると，売上高1,000億円未満の企業では，「特に確保していない」の回答割合が50 %を超えている。

Results of questionnaire (2) regarding industrial control systems reported by IPA

景から全てのエンドポイントをセキュアにしていくことは難しい。ハードウェアでセキュリティーチップを追加実装するのはもちろん，ソフトウェアでセキュリティー機能を追加した場合でも，IT分野とは異なり，パフォーマンスへの影響やOSの対応バージョンに対するサポートの問題が出てくる。そこで当社は，エンドポイントに必要なセキュリティー機能を集約して代行する，外付けのデバイス（以下，セキュリティープロキシーデバイスと略記）を開発した（**図4**）。これは，エンドポイントのネットワークポート（イーサネット用ポート）に挟み込むだけなので，エンドポイント自体に手を加える必要が全くない。また，外付けにしたため，様々なベンダーの機器や，OSの対応バージョンにも依存せず，どんなものにも適用できるという利点がある。

＜セキュリティープロキシーデバイスの機能＞
- 通信先とのPKIベースの相互認証
- 通信データの機密性・完全性保護
- 鍵や証明書のセキュアな保持と更新機能
- 通信のホワイトリスト（プロトコルチェック，通信方向制御）
- 管理サーバーによるセキュリティーパッチ更新
- 管理サーバーへのネットワーク異常検知（相互認証異常，ホワイトリスト異常，物理的に外された場合など）
- 管理サーバーからの署名データの署名検証（アセットのファームウェアなどのセキュアアップデートに利用）

図4. 開発したセキュリティープロキシーデバイス

開発したセキュリティープロキシーデバイスは，既存のLANケーブルに挟み込んで使用する。

Newly developed security proxy device

このセキュリティープロキシーデバイスには，ICカードで使用されている，高い耐タンパー性を備えたセキュリティーチップが実装されており，PKI（公開鍵基盤）ベースのセキュリティーを実現するための鍵や証明書がセキュアに保管されている。これらによって，開発したセキュリティープロキシーデバイス間の通信では確実な相互認証が行われるため，Miraiウイルスなどで問題になったパスワードベースの簡易認証とは異なる，確実な機器間認証が実行され，かつ通信データの機密性や完全性が確保される。

したがって，システム内に管理されていないデバイスや機器があり，それらが何らかの理由（保守員の保守作業中のUSB（Universal Serial Bus）メモリーからの感染や，標的型攻撃により業務ネットワークがウイルスに感染して社内ネットワーク全体にまん延した場合など）でマルウェアやランサムウェアに感染したとしても，開発したセキュリティープロキシーデバイスが取り付けられているエンドポイント（以下，アセットデバイスと略記）は影響を受けない（**図5**）。

また，このセキュリティープロキシーデバイスにはホワイトリスト機能があるため，万一アセットデバイス自体がUSBメモリーなどからマルウェアに感染してしまった場合も，本来許可されていない通信（例えば，プロトコルなど）を検知できる。セキュリティープロキシーデバイスは，上位の管理システムで一括管理されているため，このホワイトリストでの検知や，前述の相互認証時の失敗など，ネットワーク内部の

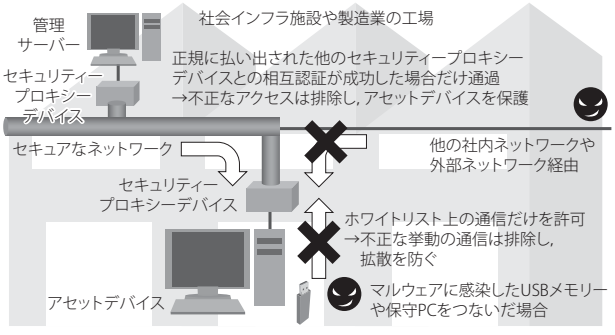


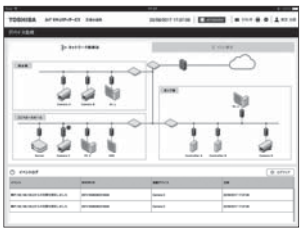
図5. 開発したセキュリティープロキシーデバイスによるセキュアなネットワーク

情報をやり取りする機器間だけのセキュアなネットワークを構築し，不要なアクセスを遮断する。

Secure network realized by security proxy devices

異常を検出して管理システムに即座に挙げるとともに，管理者に通知できる。

更に，セキュリティープロキシーデバイスは，管理システムによって常にセキュリティーパッチを最新の状態にすること



(a) 施設内のアセットデバイス全体の表示例
（不正アクセスを検知し，詳細ログも出力）

(b) アセットデバイスの構成管理情報や，
ホワイトリスト設定情報，
公開鍵証明書情報などの表示例

(c) アセットデバイスのリスト表示例
（証明書更新や，パッチ更新，
ファームウェアアップデートなどを一括実施）

図6. 開発したセキュリティープロキシーデバイスを用いた上位管理システムの表示例

管理下にある様々な機器の状態を，一括して監視できる。

Example of host management system using security proxy devices

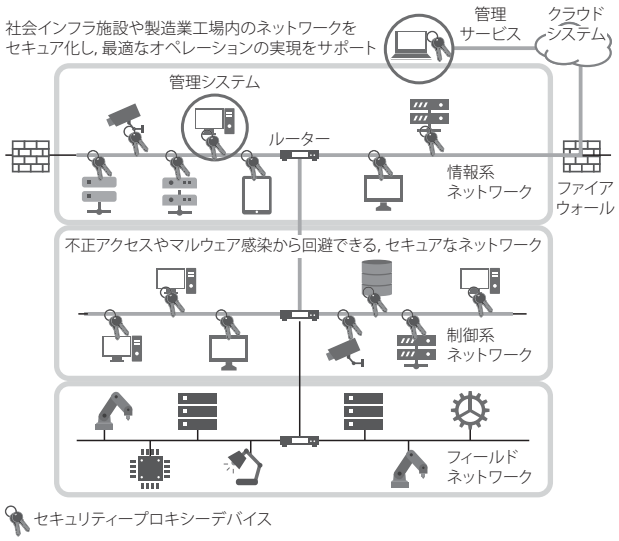


図7. IoTセキュリティーソリューションの全体像

レガシーな機器やシステムが含まれている環境下でも，システム全体をセキュアにできる。

Overview of IoT security solution

ができる。セキュリティープロキシーデバイスがエンドポイントのネットワークの入り口で防御していることになるため，アセットデバイスにセキュリティーパッチが施されていない状況でも，多くの脅威を回避できる。

そのほかにも，エンドポイントを個別のセキュリティープロキシーデバイスにより1対1で守っているメリットとして，システム全体のエンドポイントの状態やその構成管理，ファームウェアや設定情報などのセキュアなアップデートも，管理システム側から一括して行うことが可能である（**図6**）。

今後，IoTが更に進化して，上位側から下位側に情報をフィードバックするようなフェーズになったときにも，セキュリティープロキシーデバイスはセキュアな通信を行うことができ，システム全体の可用性を低下させることなく，最適なオペレーションを行うことができる（**図7**）。

4. あとがき

当社は，社会インフラのセキュリティー向上を実現できるIoTセキュリティーソリューションを開発した。今回開発したソリューションの検証を，CSSC（技術研究組合 制御システムセキュリティセンター）などで行う予定である。

今後，重要インフラだけでなく，IIoTを進めている製造業のセキュリティー強化にも貢献し，様々な分野への展開を図っていく。

文　献

(1) IPA. 制御システム利用者のための脆弱性対応ガイド 重大な経営課題となる制御システムのセキュリティリスク～ 制御システムを運用する企業が実施すべきポイント～ 第3版. 2017, 33p. <https://www.ipa.go.jp/files/000058489.pdf>, （参照2017-11-22）.

(2) IPA. 制御システムユーザ企業の実態調査報告書. 2016, 44p. <https://www.ipa.go.jp/files/000051551.pdf>, （参照2017-11-22）.

友枝　裕樹　TOMOEDA Yuki
東芝インフラシステムズ（株）
セキュリティ・自動化システム事業部 ICカードシステム営業部
Toshiba Infrastructure Systems & Solutions Corp.

福岡　寛規　FUKUOKA Hiroki, Ph.D.
東芝インフラシステムズ（株）
セキュリティ・自動化システム事業部 ICカードシステム営業部
博士（理学）
Toshiba Infrastructure Systems & Solutions Corp.

杉渕　　慶　SUGIBUCHI Kei
東芝インフラシステムズ（株）
小向事業所 ICカードシステム部
Toshiba Infrastructure Systems & Solutions Corp.