インダストリアルIoTシステムに対応したセキュリティーアーキテクチャー

Industrial IoT Security Architecture

斯波　万恵 SHIBA Masue　　池田　竜朗 IKEDA Tatsuro　　岡田　光司 OKADA Koji

産業や社会インフラなどの幅広い分野で，IoT（Internet of Things）によるデジタル化が広がりを見せている。あらゆる“モノ”がネットワークにつながることにより，新たなビジネスモデルへの変革が進む一方で，サイバー攻撃のリスクが顕在化してきている。

東芝デジタルソリューションズ（株）は，重要インフラや産業制御システムの製品・システムをサイバー攻撃の脅威からライフサイクル全体にわたって守る“セキュリティーライフタイムプロテクション”のコンセプトを策定し，設計段階からIoTシステムの広がりや深さに応じて適切なセキュリティー対策を作り込んでいく“セキュリティーリファレンスアーキテクチャー”を整備した。このアーキテクチャーに基づいて，セキュリティーとコストのバランスを考慮したIoTシステムの構築に取り組んでいる。

Digital transformation is expanding in a wide range of fields in both industry and society via the Internet of Things (IoT). While the myriads of interconnected IoT devices are creating new business models, they are also exposed to an increased risk of cyberattacks.

To address this problem, Toshiba Digital Solutions Corporation has developed the concept of lifetime security protection, which emphasizes the protection of key products and systems of important infrastructure and industrial control systems throughout their life cycles, and a security reference architecture, which is designed to build robust security into IoT systems at their design stage in a flexible manner according to the breadth and depth of their utilization. We are now creating IoT systems using this architecture, taking the cost-security balance into consideration.

1. まえがき

産業や社会インフラなどの分野で，IoTによるデジタルトランスフォーメーションが広がっている。あらゆるモノがネットワークにつながり，情報システムと制御システムが接続される新しい世界は，ビジネスモデルの変革が加速される一方で，サイバー攻撃のリスクが増加している。例えば，機器の僅かな脆弱（ぜいじゃく）性を突いて社会インフラを狙うサイバー攻撃も，現実のものとなってきている。

東芝デジタルソリューションズ（株）は，情報システムと制御システムの両方でセキュリティーの運用管理を行ってきた経験から，インダストリアルIoTアーキテクチャーを開発し，東芝IoTアーキテクチャー“SPINEX”を支えるIoTセキュリティーの方法論として活用している。ここでは，当社が策定した“セキュリティーライフタイムプロテクション”のコンセプト，及びそれに基づいて整備した“セキュリティーリファレンスアーキテクチャー”の概要について述べる。

2. セキュリティーライフタイムプロテクション

情報システムでは，ISO/IEC（国際標準化機構／国際電気標準会議）が規定する“情報セキュリティマネジメントシステム”で認証制度が整備され，情報システムを運用する組織において“現状把握→予防→検知→対策”といったPDCA（Plan-Do-Check-Act）サイクルを持続的に回すことが求められている。このPDCAサイクルをインダストリアル領域のIoTシステムに適用するために，セキュリティーライフタイムプロテクションのコンセプトを策定した（**図1**）。

“設計・防御→運用・監視→インシデント対応・復旧→評価・検証，教育”のPDCAサイクルを回すことで，サイバー攻撃の高度化や巧妙化に伴って相対的にセキュリティーレベルの耐性が低下していくのを防ぎ，適切かつ継続的に維持する。

設計・防御フェーズでは，制御システムのセキュリティー国際標準規格IEC 62443に準拠した製品開発でセキュリティー品質を確保するとともに，製品の構成管理に基づく脆弱性やインシデントの監視基盤を開発した。運用面では，イ

図1. セキュリティーライフタイムプロテクション
IoTシステムのライフサイクル全体にわたってPDCAを回すことで，適切なセキュリティーレベルを継続的に維持する。
Lifetime security protection

ンシデントへの対応ルールとその優先順位，リスク管理ポリシーなどを社内規程で厳格に明文化することで，有事の際の復旧を効率化している。また，常に最新のセキュリティー評価・検証を行える環境や，演習・訓練によるセキュリティー人財の教育・育成を図るといった，環境面にも取り組んでいる。

このセキュリティーライフタイムプロテクションに基づいて，最適なセキュリティーレベルを継続的に維持することで，異常を早期に検知し，有事の際にも被害を最小限に抑えることが可能になる。更に，迅速な対応でセキュリティーインシデントを封じ込め，システムやサービスの停止期間を最小限にとどめる強固なセキュリティーを提供する。

3. デジタルトランスフォーメーションの進化に応じたセキュリティーリファレンスアーキテクチャー

IoTシステムのセキュリティー対策レベルの分類と，その対策レベルに応じたセキュリティーリファレンスアーキテクチャーを策定した（**図2**）。

IoTシステムのセキュリティーを適切に設計することは，容易ではない。これは，守る対象となる事業や，サービス，業務プロセス，接続される機器の種類と数，やり取りされる情報資産，セキュリティーインシデントの要因となるセキュリティーリスクといった，それぞれの要素がIoTシステムごとに異なるからである。また，国家レベルの組織から小さな犯罪組織，愉快犯といった全ての脅威に対して，一律の手法で

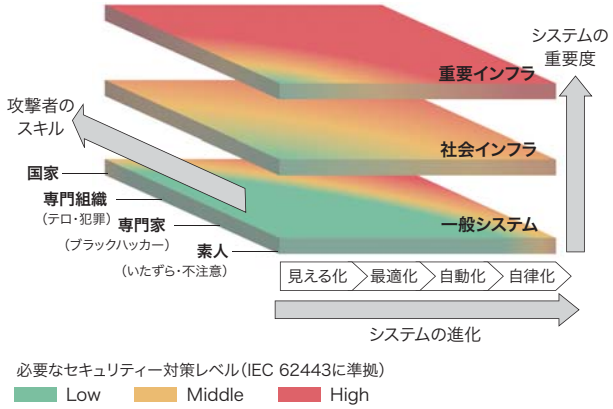


図2. セキュリティーリファレンスアーキテクチャー
Low，Middle，Highという3段階のセキュリティー対策レベルを設定し，システムの進化に応じて，コストバランスを重視した必要十分なセキュリティー対策を実行するためのアーキテクチャーモデルである。
Security reference architecture

対抗することは非合理的である。過剰な対策は，業務やシステム運用において効率の低下を招き，逆に不十分な対策では，後付けのセキュリティー対策に掛かるコストが増大してしまう。このため，IoTシステムのセキュリティーに関わる多種多様な技術要素を，システムの特性や進化に合わせて体系化した枠組みを整備した。デジタルトランスフォーメーションの進化に応じて，制御システムセキュリティーの国際標準であるIEC 62443や，ほかの規格，ガイドライン[1], [2]に準拠した，“Low”，“Middle”，“High”という3段階のセ

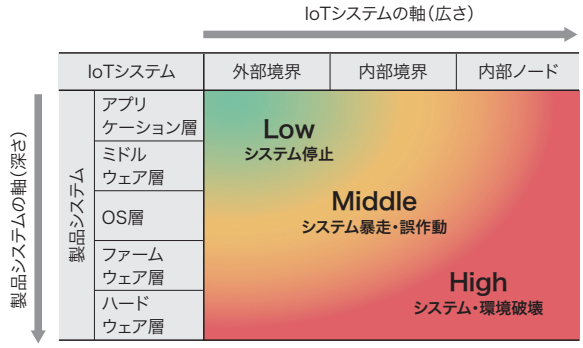


図3. 2軸の多層防御

IoTシステム軸（広さ）と製品システム軸（深さ）の2軸による多層防御で，セキュリティー対策の体系化を図った。

Two-axis multilayered defense

キュリティー対策レベルを設定した。各レベルを満たす技術的な対策を決定し，個別のシステムへの実装を図っている。

4. IoTシステムの広さと深さを軸とした多層防御

セキュリティーリファレンスアーキテクチャーに基づいてセキュリティー設計を行うにあたり，製品システムの“深さ”とIoTシステムの“広さ”という二つの軸で必要な対策の体系化を図った（**図3**）。

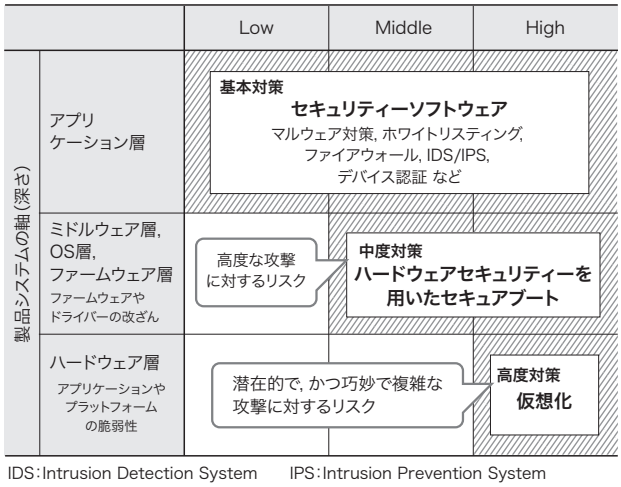
4.1 深さの多層防御

深さの軸では，システムを構成するアプリケーション層，ミドルウェア層，OS（基本ソフトウェア）層，ファームウェア層，及びハードウェア層の各層に対して，どのようなセキュリティー対策を実施すべきかを整理した（**図4**）。

一般的なアプリケーション層への脅威に対しては，ホワイトリストなどによるマルウェア対策や，ファイアウォールといったセキュリティーソフトウェアによる基本的な対策を実装すべきである。

ファームウェアやドライバーへの脅威としては，例えば，HDD（ハードディスクドライブ）やSSD（ソリッドステートドライブ）内に不可視でかつ削除も不可能な領域を作成し，そこを攻撃者の攻撃起点として利用することで，HDDやSSDのファームウェアを書き換えるという攻撃事例が報告されている。この攻撃では，システム起動時にマルウェアを読み込ませることで，確実にマルウェアを起動する。このような脅威は，一般のマルウェア対策ソフトウェアなどによる検知や駆除が極めて難しく，ファームウェアや，ブートコード，OSカーネル，デバイスドライバーなどの完全性を，起動シーケンスに沿って順次セキュリティー検証を行うことにより対策を行う。トラストアンカー（信頼の根拠）としてTPM（Trusted Platform Module）などのセキュリティーモジュールを実装し，セキュリティーモジュールに格納された署名データベースによりセキュリティー検証を行うといった手段が考えられる（**図5**）。

また，昨今のアプリケーションやOSでは，システムの複雑化やオープンソースの利用などで，脆弱性が混入したり残存したりするリスクが高い。未知の脆弱性（ゼロデイ攻撃）などを複数利用した“正規アプリケーションの権限利用”や



IDS：Intrusion Detection System　IPS：Intrusion Prevention System

図4. 製品システム軸のレベルごとの対策

各層について，攻撃の難度やリスクの程度に合わせたセキュリティーレベルごとの対策を整理した。

Security measures for each level of product and system axes

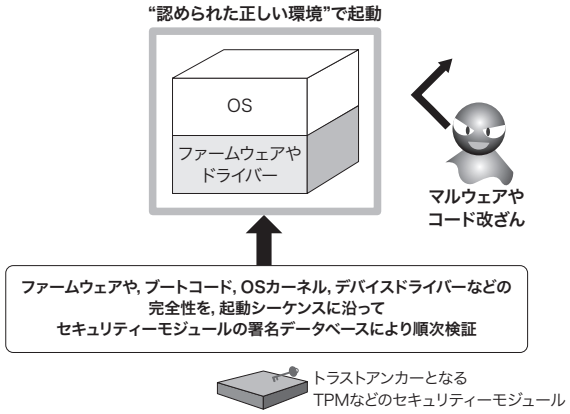


図5. ミドルウェア層，OS層，ファームウェア層の脅威への対策

一般のマルウェア対策ソフトウェアなどによる検知や駆除が極めて難しいので，セキュリティーモジュールを用いたセキュアブートにより対策を行う。

Security measures for threats against middleware, operating system (OS), and firmware layers

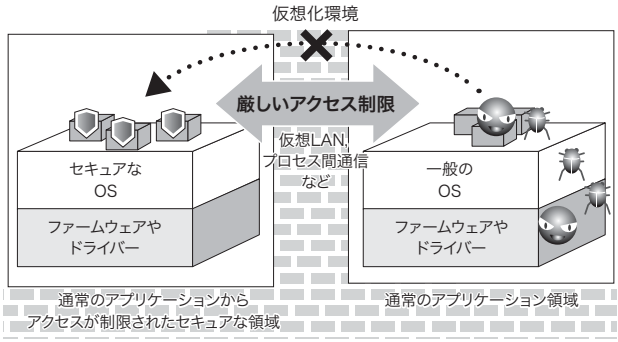


図6. ハードウェア層の脅威への対策

アクセスを制限したセキュアな領域に重要なセキュリティー機能やアプリケーションを置き，仮想化によってセキュリティー機能を分離することで，セキュリティー対策を行う。

Security measures against hardware and system-wide threats

“脆弱性による不正な権限取得”を活用して，セキュリティー対策ソフトウェアやOSのセキュリティー機能を停止，又は回避した後に攻撃を実行するといった高度な攻撃は，“正規アプリケーションの脆弱性”を利用しているため，セキュリティー対策ソフトウェアやセキュアブートなどでは対処が困難である。このような攻撃に対しては，TEE（Trusted Execution Environment）などの仮想化で対策を行う。この対策では，通常のアプリケーションからのアクセスを制限したセキュアな領域に重要なセキュリティー機能やアプリケーションを置き，通常のアプリケーション領域のリスクが混入しないように，チップレベルで分離する。また，厳しいアクセス制限を設けるため，通常アプリケーション領域でルート権限を奪取されたとしても，セキュリティー機能を無効化されることはない（**図6**）。

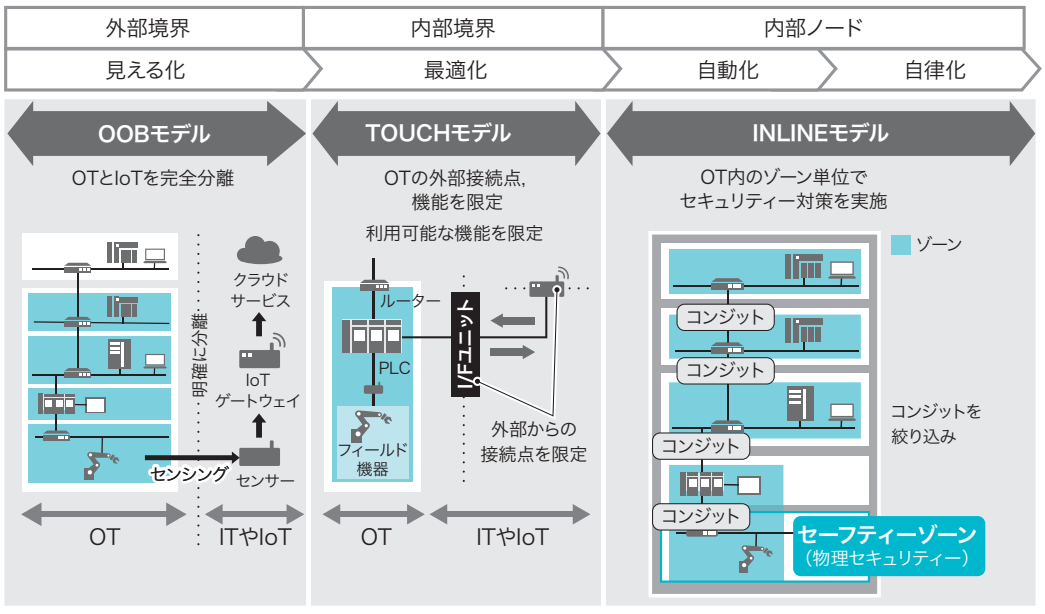
4.2 広さの多層防御

広さの軸では，IoTシステムの進化に伴い，対策をどの範囲まで行うべきかを明確にした。広さの多層防御を実現するために策定した，三つのセキュリティーモデルを**図7**に示す。

“見える化”の段階では，システムと外部との，物理的又はネットワーク的な境界を分離する“OOB（Out of Bound：完全分離）モデル”，“最適化”の段階に進んだ場合は，システム内部の各サブシステムにおける境界を限定してセキュアに管理する“TOUCHモデル”，そして“自動化”と“自律化”の段階では，各機器や装置といった内部ノードへの対策までを包括した“INLINEモデル”に分けて，セキュリティーモデルごとに実装すべき対策を明確にした。

4.3 三つのセキュリティーモデルと実装ソリューション

OOBモデルでは，情報システム（OT：運用技術）と制御システム（IT（情報処理）やIoT）を分離し，システム間の



I/F：インターフェース　PLC：Programmable Logic Controller

図7. IoTシステム軸（広さ）の進化に合わせたセキュリティーモデル

IoTシステムの進化に伴い，対策をどの範囲まで行うべきかを，三つのセキュリティーモデルで明らかにした。

Security model based on evolution of IoT system axis (breadth)

影響を可能な限り排除することに注力する。センシングしたフィールド機器に関するデータを送信する際，データの流れを制御システムから情報システムへの一方向に限定することで，制御システムのプロセスには直接影響を与えず，センシングデータの通信ラインから制御システムへのリスク発生を抑える。

TOUCHモデルでは，外部から接続できる機器を必要最低限に絞り込むことで，万一の場合にも制御システムの重要な機能には影響を与えないことを目指している。ホワイトリストにより実行できるプログラムをあらかじめ限定するほか，外部からリモートで制御機器をコントロールするコマンドを絞り込むなど，フィールド機器の分析や最適化に必要となるデータだけをオンデマンドに取得できる環境とする。

INLINEモデルでは，機能単位でゾーニングを行い，ゾーン間の接続点であるコンジットを絞り込むことで，制御システム全体のセキュリティーを確立する。情報システムに最も近いゾーンではAI を活用した次世代マルウェア対策を，情報システムゾーンと制御システムゾーンの接続点では一方向性セキュリティーゲートウェイであるデータダイオードを，また制御システムゾーンの内部にある組み込み機器にはホワイトリスト型マルウェア対策を，産業用コントローラー製品では国際的な認証制度であるISASecure® EDSA（Embedded Device Security Assurance）認証を取得した製品[3]を活用するなどの対策が考えられる。また，制御ネットワークやコンポーネントの異常な振る舞いを検知し，監視するソリューションなども加えて，ゾーンごとに最適な対策を組み合わせることで，重要インフラのセキュリティー要求を満たす対策を実装する必要がある。

産業用製造設備では，長期間にわたってシステムを稼働し続けることが多い。レガシーな制御システムを運用する場合に，インラインでセキュリティーを確保するためのソリューションも開発されている[4]。エンドポイントにある機器自体には手を加えず，機器と上位のネットワーク通信の間にセキュリティープロキシーデバイスを取り付けることで，セキュアな通信と機器間の相互認証を実現できる。これにより，システムの可用性を低下させることなく，データの機密性や完全性を確保できる。

5. あとがき

今回整備したセキュリティーリファレンスアーキテクチャーに基づいて，セキュリティーライフタイムプロテクションを推し進めながら，今後も，デジタルトランスフォーメーションの進化に対応できるセキュリティーソリューションを提供していく。また，日々巧妙化・高度化するセキュリティーの脅威に対して，技術要件を柔軟に更新して多様な仕組みを連動させることで，信頼性の高いIoTシステム向けセキュリティーの構築を目指していく。

文　献

(1) Stouffer, K. et al. Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800- 82 Revision 2, 247p. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>, (accessed 2018-06-01).
(2) IoT推進コンソーシアム，ほか．IoTセキュリティガイドライン ver 1.0. 総務省，経済産業省．2016，60p．<http://www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf>,（参照 2018-06-01）.
(3) CSSC認証ラボラトリー．EDSA認証済み製品．CSSC認証ラボラトリーウェブサイト．<http://www.cssc-cl.org/jp/certified_devices/index.html>,（参照 2018-06-01）.
(4) 友枝裕樹，ほか．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．東芝レビュー．2018, 73, 1, p.59–62. <http://www.toshiba.co.jp/tech/review/2018/01/73_01pdf/f06.pdf>.（参照2018-06-01）.

斯波　万恵　SHIBA Masue
東芝デジタルソリューションズ（株）
インダストリアル ICT セキュリティセンター
電子情報通信学会・情報処理学会会員
Toshiba Digital Solutions Corp.

池田　竜朗　IKEDA Tatsuro
東芝デジタルソリューションズ（株）
インダストリアル ICT セキュリティセンター セキュリティ技術部
Toshiba Digital Solutions Corp.

岡田　光司　OKADA Koji, D.Eng.
東芝デジタルソリューションズ（株）
インダストリアル ICT セキュリティセンター
博士（工学）　電子情報通信学会会員
Toshiba Digital Solutions Corp.