# インダストリアルIoTに向けたセキュリティー技術

## Security Technologies for Industrial IoT Systems

大矢　章晴　　中溝　孝則　　松下　達之
■OYA Toshiharu　■NAKAMIZO Takanori　■MATSUSHITA Tatsuyuki

**製造業を中心に，IIoT（インダストリアルIoT（Internet of Things））が注目されている。一方で，IoT機器や制御システムが情報システムとつながることによって，サイバー攻撃の攻撃箇所が増加するリスクが高まっている。**

**東芝デジタルソリューションズ（株）は，IIoTに向けたセキュリティー対策として，IIoTシステムを構成する制御システムや機器をセキュア化するために，セキュリティー認証取得支援技術を開発している。更に，セキュリティーの国際標準規格に基づき，対象とする制御システム・機器の特性を考慮して効率的に脅威分析を行うツール SecuScopeを開発している。これらを用いることで，対象の制御システム・機器の認証取得作業を軽減するとともに，IIoTにおけるセキュリティー品質を確保できる。**

Industrial Internet of Things (IIoT) systems have recently been attracting attention, particularly in the manufacturing industry. However, since IoT equipment and control systems are connected to information systems in such IIoT systems, the risk of cyberattacks increases.

To enhance the security of IIoT systems, Toshiba Digital Solutions Corporation has developed support technologies for the acquisition of security certifications to secure the equipment and control systems constituting IIoT systems. We have also developed SecuScope, a tool that facilitates the efficient analysis of security threats by taking the characteristics of the target equipment and control systems into consideration based on international security standards. These technologies make it possible to reduce the work required for the acquisition of security certifications for such equipment and control systems and to ensure security for IIoT systems.

## 1　まえがき

工場や社会インフラなどの幅広い分野において，あらゆるモノがネットワークにつながるIoTを活用する動きが進んでいる。

製造業を中心とした分野における制御システムでは，多種多様なデータを活用し，生産技術を高度化させることを目的とするIIoTが注目されている。例えば，プラント内に設置されたセンサーから取得した情報を，クラウドシステムで集積し分析することにより，設備の稼働状況の見える化とそれを活用した効率的な保守業務が行われている。

IIoTの活用によるメリットが得られる一方，ネットワークカメラなどのIoT機器や，OT（Operation Technology）としての制御システム，IT（情報技術）としての情報システムが相互に接続されるため，サイバー攻撃の経路が増えることに起因したリスクが高まっている。制御システムで利用されるPLC（Programmable Logic Controller）に関しては，“国内メーカー製のPLCなどを標的とした悪意を持った探索行為が行われている可能性がある”ことが，警視庁から報告されている[(1)]。更に，サイバー攻撃による被害も報告されており，脅威が現実的なものとなっている（**表1**）。

IIoTシステムへのサイバー攻撃による影響は，一つの工場や企業だけでなく，社会全体に及ぶ可能性があるため，セキュリティー対策が必要不可欠である。

**表1．サイバー攻撃事例**
Examples of cyberattacks

| 報告年 | 攻撃対象 | 説明 |
|---|---|---|
| 2016年 | ネットワークカメラなどのIoT機器 | マルウェアにより，数十万台の機器が感染してボットネットを形成し，DDoS攻撃に悪用された。 |
| 2016年 | IoT機器とネットサービス | 乗っ取りにより，攻撃の踏み台にされ，大手ネットサービスが5時間にわたり接続困難になった。 |
| 2015年 | 電力システム | 標的型攻撃により，ウクライナ西部の都市約140万世帯が数時間停電した。（2016年末にも同様の事件がウクライナで発生した。） |
| 2015年 | 交通システム | 不正アクセスにより，ロサンゼルスの交通情報の電光掲示板データが改ざんされた。 |

DDoS : Distributed Denial of Service Attack

東芝デジタルソリューションズ（株）は，IIoTに向けたセキュリティー対策では制御システム・機器の特性を考慮することが重要であると考え，制御システム・機器の開発プロセス全体にわたるセキュア化技術を開発するとともに，その中でも重要な脅威分析ツールの開発と適用に取り組んでいる。

## 2　IIoTにおけるセキュリティーの課題

### 2.1　IIoTの動向

IIoTは，顧客の要求に個々に応える製品の生産や使用価値の向上など，ビジネスモデルの変革を実現するものとして期待が高まっており，IIoTの実現に向けて様々なコンソーシアムが設

立されている。特にドイツの国家プロジェクトIndustrie 4.0や米国企業を中心としたIndustrial Internet Consortium（IIC）が注目されている。

Industrie 4.0では，産業製造分野の活性化に向け，垂直方向（一つの製品で異なる工程の業務を担う企業間のバリューチェーン）と水平方向（企業・分野の境界を越えたバリューチェーン）の連携を推し進めている。この連携を実現するには，バリューチェーン全体でのセキュリティー確保が重要であり，そのためには，開発プロセスの早期の段階でセキュリティーを検討するセキュリティーバイデザインが必要不可欠である[2]。

我が国においても，経済産業省から，我が国の産業が目指す姿を示すコンセプトとして“Connected Industries”が発表されており，この実現に向けた各種の施策が推進されていく予定となっている[3]。一方，セキュリティーの観点では，2015年9月に閣議決定された「サイバーセキュリティ戦略」[4]に基づき，安全な社会の実現に向けた基準整備として，IoT機器や，システム，サービスの提供にあたって，ライフサイクル（方針，分析，設計，構築・接続，運用・保守）におけるセキュリティー対策の指針を定めた「IoTセキュリティガイドライン」[5]が策定された。

このような動向を踏まえ，当社は，社会インフラや製造などの事業で培ってきた技術や知見と，IoTやAIなどの先進技術を駆使し，東芝IoTアーキテクチャーSPINEX™の開発などで，IIoTビジネスに取り組んでいる。

### 2.2　セキュリティー対策の課題

実世界の製品や，部品，設備，人，業務プロセスなどから膨大なデータをリアルタイムでクラウドシステムに集積し，デジタル化することでデジタル空間に現実の製造工程を再現する。そして，それらを分析することにより，現実世界で何をすべきかフィードバックし，生産の最適化を行うのがデジタルツインである（**図1**）。IIoTでこれを実現するためには，制御システムと情報システムのシームレスな連携が必要である。

IIoTにおいて，異なる性質を持つ制御システムと情報システムを連携させるためには，各々が持つ異なるリスクについて考える必要がある。

制御システムでは，情報システムで求められるCIA（Confidential，Integrity，Availability）のセキュリティーリスクに加え，事業リスクとしてのHSE（Health，Safety，Environment）も考慮する必要があり，就業者及び周辺コミュニティの健康及び安全性の保護や，高い環境レベルの管理・維持を行う責任が求められる[6]。このため，情報の機密性が求められる情報システムと比較して，制御システムは，連続稼働や安全性が優先されるなど異なる特性のセキュリティーが要求される。したがって，制御システムの安全性を考慮に入れた上で，IIoTシステムのセキュリティーを確保する必要がある。

また，システム同士を接続するには，セキュリティーをどのように担保しているのか，システムオーナー同士で相互に評価・確認を行う必要があり，それに利用できる共通指標としてセキュリティーの国際標準規格や認証制度がある。IIoTは，特定の分野だけでなく，製造や社会インフラなどの幅広い分野の制御システムで利用されるため，共通指標としては，汎用的な制御システムに適用可能なものが望ましい。

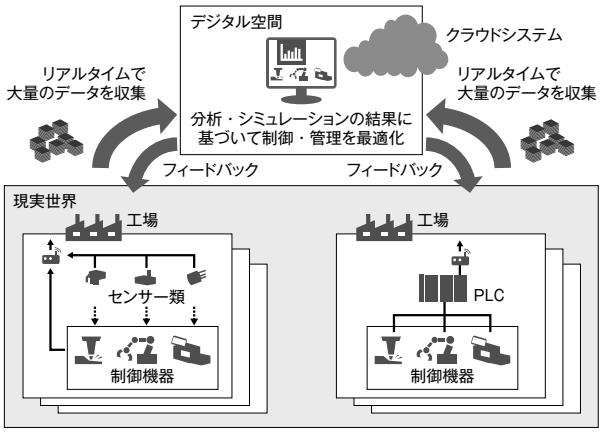



**図1．制御システムと情報システムが連携したデジタルツイン** ― 現実世界の情報をクラウドシステムに吸い上げてデジタル空間に現実世界を再現し，それを用いた分析やシミュレーションに基づいて制御・管理を最適化し，現実世界にフィードバックする。

Cooperation of control and information systems

加えてIIoTでは，様々なシステムや機器がつながるため，サイバー攻撃の対象となり得る領域が増え，どこに脅威が存在するのか把握することが難しくなるという問題がある。例えば，脆弱（ぜいじゃく）性のある機器を経由した攻撃がほかのシステムに対して行われるなどの脅威を把握する必要があり，把握できないと効果的な対策を立案することが難しくなる。

これらを踏まえると，IIoTにおけるセキュリティー対策の課題は主に三つあると考えられる。

(1)　課題1　　制御システムでは安全性を考慮する必要がある。

(2)　課題2　　セキュリティー対策の妥当性を担保するための共通指標に基づいた開発が必要となる。

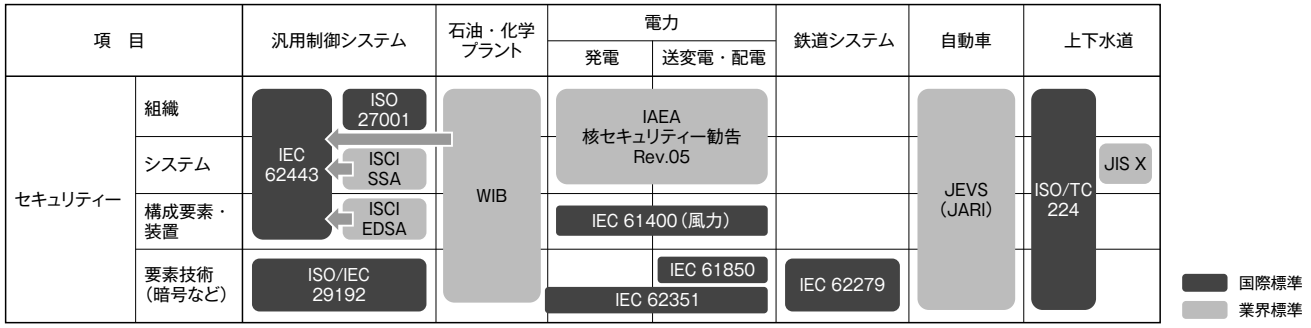
(3)　課題3　　どこに脅威が存在するのか把握し，効果的な対策を施す必要がある。

これら三つの課題を解決するための当社の取り組みに関し，3章では共通指標を活用した制御システム・機器向けのセキュア化技術について，4章ではどこに脅威が存在しどのような対策をすべきかを分析する脅威分析ツールとその適用例について述べる。

## 3　制御システム・機器のセキュア化への取り組み

### 3.1　セキュリティーの国際標準規格

制御システム分野のセキュリティー標準には，組織，システ




ISO：国際標準化機構　IAEA：国際原子力機関　JEVS：日本電動車両規格　JARI：一般財団法人 日本自動車研究所　TC：Technical Committee　JIS：日本工業規格

**図2．制御システムのセキュリティーに関する国際標準と業界標準** ― 分野ごとに国際標準や業界標準が定められているが，汎用的な国際標準としてIEC 62443シリーズが策定されつつある。

International and industrial standards related to security of control systems

ム，装置に対応したものや，業種，業界に対応したものなど，様々な標準・基準が策定されている（**図2**）。

こうした中で，汎用的な標準として国際電気標準会議（IEC）の規格IEC 62443シリーズ(注1)が策定されつつあり，一部事業者の調達要件にもなっている[7]。

IEC 62443シリーズは，制御システムを運用する組織マネジメント，システム，構成要素・装置の全レイヤーとプレーヤーをカバーした規格であり，以下の4部から構成されている。

(1)　第1部　　用語，コンセプト，モデルの定義などの構成全体に関する規格

(2)　第2部　　セキュリティーの管理・運用・プロセスなど，組織に関する規格

(3)　第3部　　セキュリティー技術・システムに関する規格で，ゾーン設計における安全性保証やセキュリティー機能要件などを規定

(4)　第4部　　構成要素・装置に関する規格で，開発プロセスや安全性を加味したセキュリティー機能要件などを規定

IEC 62443シリーズは，汎用的な制御システム向けの国際標準規格なので，2章で述べた課題1と課題2を満たしている。

また，制御システムのための評価認証制度として先行している業界標準のISASecure認証及び国際装置ユーザー協会（International Instrument User's Association）のWIB認証がIEC 62443シリーズに統合されつつある。ISASecure認証は，ISA（国際計測制御学会）とその下部にあたる認証フレームワーク推進組織ISCI（ISA Security Compliance Institute）が主体の制御システム及び装置の認証であり，現在，構成要素・装置を対象としたEDSA（Embedded Device Security Assurance）認証[8]が施行されている。

(注1)　IEC 62443シリーズのうち，策定中の標準についてはベースになっているISASecure認証を参照した。

EDSA認証では，構成要素のソフトウェア開発プロセスセキュリティー評価（SDLA），セキュリティー機能評価（FSA），通信ロバストネス試験（CRT）の三つの観点でセキュリティーを評価する。

制御システムのセキュリティーを評価するSSA（System Security Assurance）認証[9]も，EDSA認証と同様の三つの観点で評価を行う仕組みとして，認証制度が始まっている。

SDLAがIEC 62443-4-1，制御システムにおけるシステムのFSAがIEC 62443-3-3[10]，構成要素・装置のFSAがIEC 62443-4-2に対応している。

IEC 62443-4-1では，開発プロセスの中の要求分析フェーズにおいて脅威分析を実施することを定めているため，脅威分析を適切に実施すれば，2章で述べた課題3も解決できる。

これらのことから，IIoTにおけるセキュリティーの妥当性を評価し確認するための共通指標として，IEC 62443シリーズ及びこれに対応するISASecure認証は有力な候補であると考える。

当社は，制御システム・機器をセキュア化する技術として，第三者による認証プログラムであるEDSA認証及びSSA認証に準拠するためのセキュリティー認証取得支援技術，及びIEC 62443シリーズのセキュリティー機能要件を脅威分析に取り込むことにより，制御システムの特性を考慮したより妥当性のある分析結果となるような脅威分析ツールの開発を進めている。

### 3.2　セキュリティー認証取得支援技術

制御システム・機器向けのセキュリティー認証を取得するためには，システム・機器の企画段階からセキュリティー品質を作り込み，それらを維持する必要があるが，初めて認証取得を行う製品や新しい規格に対応する際，開発者には次のような課題がある。

(1)　認証取得の全体像が分からない。

(2)　要件を満たしているかどうかの判断が難しい。

(3)　開発のどの段階で，どのようなセキュリティー対策を実施すべきか分からない。

(4) どのような成果物を作成すればよいのか分からない。
(5) 認証取得作業を効率化したい。

このような課題を解決し，認証取得作業を軽減するため，製品開発者が認証取得で求められる作業を支援するための技術（**表2**）を開発している。

具体的には，EDSA認証とSSA認証ごとの教育資料，チェックリスト，ガイド，テンプレート，ツールであり，認証の三つの観点での評価に対応することで，製品開発者が，何に対してどのように取り組めばよいかを支援する技術となっている（**図3**）。

教育資料は，認証取得を考えている開発部門が，認証制度と必要な作業について理解するために，それらについての概要をまとめたものである。

チェックリストは，開発システム・機器が認証の要求項目を満たしているかを，リスト形式で確認できるようにしたもので，確認すべき項目と，どのように確認を行うかの方法についてまとめてある。これを利用することで，既存の制御システム・機器で実施しているセキュリティー対策と，認証のセキュリティー要件とのギャップを調べることができる。

ガイドは，認証の要求項目を，項目ごとに詳細に説明したもので，理解しづらい要求項目に対する解説や，要求項目に対応する際に間違いやすいポイントと対応の具体例，ベストプラクティスなどについて記載してある。

**表2．認証取得支援技術**
Support technologies for acquisition of security certifications

| 認証取得支援技術名 | 内　容 |
|---|---|
| 教育資料 | 認証の概要，行うべき作業をまとめたもの |
| チェックリスト | 要求項目を満たしているかをリスト形式で確認できるようにしたもの |
| ガイド | 要件の解説，対策の具体例などをまとめたもの |
| テンプレート | 認証に必要なドキュメント類のテンプレート |
| 脅威分析ツール | 脅威分析の効率化を行うツール（SecuScope） |

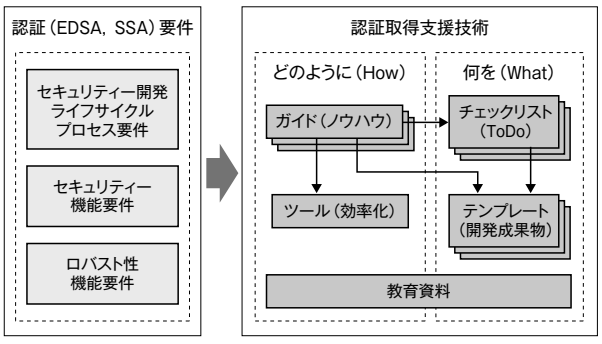



**図3．認証要件と認証取得支援技術との関係** — EDSA認証とSSA認証の要件に対し，製品開発者がどのように取り組めばよいかを支援する。
Relationship between security certification requirements and support technologies for acquisition of security certifications

テンプレートは，認証で必要となる各種ドキュメント類をテンプレート化したもので，ドキュメントの章立てと，各章に記載すべき内容について記載してある。テンプレートを利用することで，認証で必要となる事項が漏れなくドキュメント類に反映されることを目的として作成したものである。

ツールは，認証で必要となる作業を効率化するために作成したもので，認証の要求項目を満たすために必要な，制御システム・機器の脅威分析を支援するためのツール SecuScope[11]を提供している。

これらの支援技術を活用することで，制御システム・機器向けの認証取得を行う開発部門の作業を効率化するとともに，IIoTにおけるセキュリティー品質を確保できる。

## 4　脅威分析ツール SecuScope

3章で述べたように，IIoTのセキュリティーに関する共通指標としてIEC 62443シリーズが利用できるため，IEC 62443-3-3に記載されているシステムのセキュリティー機能要件を活用することにより，SecuScopeをIIoT向けのツールとするための開発を行っている。

### 4.1　SecuScope

SecuScopeは，脅威分析の作業を効率化するとともに，分析者による分析精度のばらつきを無くすことを目的として開発しているツールである。**図4**に脅威分析の流れを示す。まず，分析対象システムの仕様を分析し，以下を定義する。

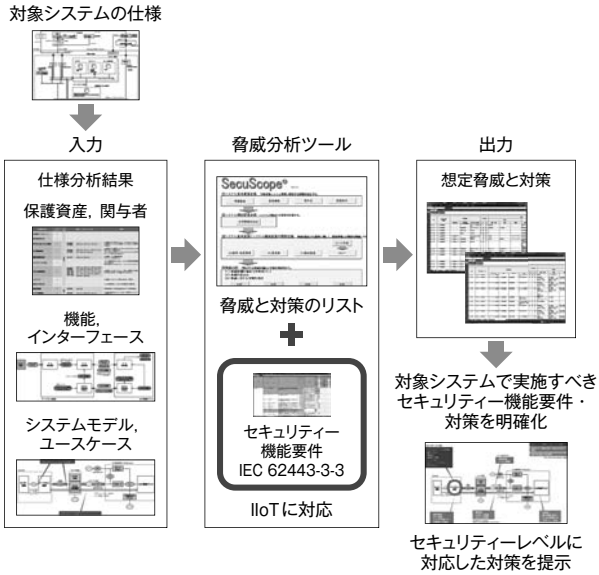



**図4．SecuScopeによるセキュリティー脅威分析** — 国際標準規格のセキュリティー機能要件と，それに対応するセキュリティーレベルごとの対策リストを作成し，SecuScopeの持つ脅威と対策のリストに組み込むことで，セキュリティー機能要件とリンクした対策を出力する。
Analysis of security threats using SecuScope

(1)　システム基本要素である，保護資産，関与者，業務機能，及び分析の前提となる条件
(2)　システム構成要素である，運用・物理環境，通信路，構成要素，及びインターフェースに関する情報
(3)　システム基本要素とシステム構成要素との関係

次に，仕様分析結果をSecuScopeに入力する。SecuScopeは，入力された仕様分析結果と，SecuScope内に保持している典型的な脅威と対策のリストを用いることにより，対象システムにおいて，脅威がどこに存在するかを自動的に洗い出し，それに対応する対策を提示する。これにより，どこでどのような対策をするべきか判断できる。

脅威と対策のリストは，セキュリティーの専門家が蓄積してきたノウハウに基づいて構築されている。日々変化する脅威や対策技術をリストに追加していくことで，最新の脅威に対応した分析が可能である。

### 4.2　IEC 62443シリーズへの対応

IIoT向けの出力結果とするため，分析結果として出力される対策にIEC 62443シリーズのセキュリティー機能要件を対応付けし，SecuScopeがIEC 62443シリーズの要件を満たす対策を提示するように開発を行っている。

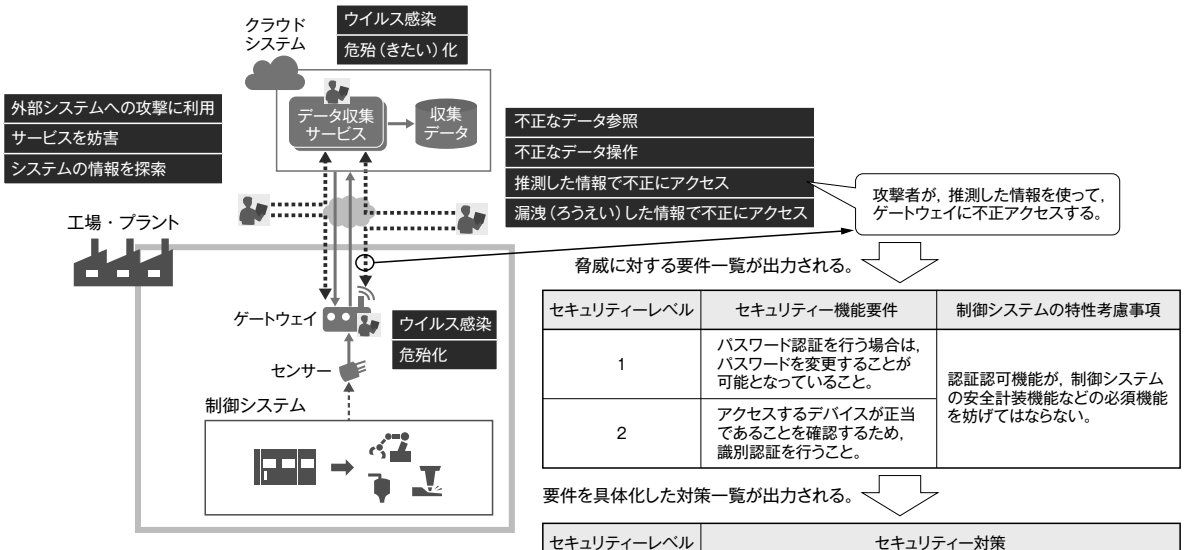
IEC 62443シリーズのセキュリティー機能要件は，抽象的に表現されているため，セキュリティーの専門家が補足説明を付けて具体化する。そして，要件を満たす対策を要件に対応付けし，要件と対策のリストを作成する。更に，これを脅威と対策のリストに対応付けることで，脅威-要件-対策リストを構築する。これにより，特定した脅威に対し，対応するIEC 62443シリーズのセキュリティー機能要件と対策が分かるため，対策の妥当性を担保できる。

セキュリティー機能要件には，対象システムに特有な影響（負の影響）を調整したベースライン（セキュリティーレベル）がレベル0から4まで設定されている。レベル付けは，攻撃者が持つ攻撃資源，産業制御システムに特有のスキルを攻撃者が持っているか否か，攻撃者のモチベーションと攻撃スキルの高さ，攻撃が意図的なものかどうかによって定められている[12]。セキュリティーレベルを活用することにより，対象システムのリスクレベルに合わせたセキュリティー機能要件の策定が可能となる。

### 4.3　適用例

SPINEX™の一つのサービスとして，製造業などでグローバルに点在する装置に対する見える化や遠隔監視を行う“IoTスタンダードパック”を提供している。このIoTスタンダードパックにSecuScopeを適用した結果の一部を**図5**に示す。

IoTスタンダードパックは，工場の制御システムにある機器に外付けされたセンサーからのデータを，ゲートウェイを介して送信し，クラウドシステムで収集することによって遠隔地から工場の機器の稼働状況を可視化するシステムである。4.1節で述べたように，システム基本要素などをSecuScopeに入力すると，例えば“攻撃者が推測した情報を使って，ゲートウェイに不正アクセスする”といった脅威が構成要素のインターフェースなどに抽出される。この脅威に対応するセキュリティー要件一覧を参照すると，セキュリティーレベル1では，“パスワード認証




| セキュリティーレベル | セキュリティー機能要件 | 制御システムの特性考慮事項 |
|---|---|---|
| 1 | パスワード認証を行う場合は，パスワードを変更することが可能となっていること。 | 認証認可機能が，制御システムの安全計装機能などの必須機能を妨げてはならない。 |
| 2 | アクセスするデバイスが正当であることを確認するため，識別認証を行うこと。 | |

| セキュリティーレベル | セキュリティー対策 |
|---|---|
| 1 | パスワードを初期設定から変更すること。 |
| 2 | クライアント証明書を用いたデバイス認証を実施すること。 |

**図5．SecuScopeの適用例** — システム基本要素などをSecuScopeに入力すると，脅威発生箇所とセキュリティー機能要件のレベルに応じた対策を出力する。
Example of application of SecuScope to IIoT system

を行う場合は，パスワードを変更することが可能となっていること”が必要な要件であると分かり，その要件を具体化した対策が“パスワードを初期設定から変更すること”であると分かる。更に，IEC 62443シリーズには，制御システム特有の考慮しなければならない事項が記載されているため，“認証認可機能が制御システムの安全計装機能などの必須機能を妨げてはならない”といった考慮すべき事項を把握することができる。

脅威−要件−対策リストでは，発生箇所（どこで），保護資産（何を），関与者（誰が），脅威内容（どうする）の形で脅威が表現され，その脅威への対策（どう守る）がセキュリティー要件のレベルごとに表現されている。

このように，IEC 62443シリーズで規定されたセキュリティー機能要件を対応付けした脅威−要件−対策リストをSecuScopeに組み込むことにより，対象システムのどこでどのような対策を備えておくべきか，また強化すべきかを，国際標準規格のセキュリティー機能要件に基づいて判断することができる。

## 5　あとがき

当社は，幅広い分野で制御システムと情報システムが融合していくIIoTシステムの実現に向けたセキュリティー課題を整理し，その課題を解決するための第一歩として，制御システム・機器をセキュアにするために，セキュリティー認証取得支援技術及び脅威分析ツール SecuScopeを開発している。

今後，SPINEX™をはじめとするIIoTシステムにもこれらの技術の適用を進め，得られた知見を利用して更に実践的な技術とすることで，便利，かつ安全・安心な社会の実現に貢献していく。

## 文　献


(1) 警察庁情報通信局情報技術解析課．情報技術解析平成27年報 ～平成27年中のインターネット観測結果等～．警察庁，2016，37p．<https://www.npa.go.jp/cyberpolice/detect/pdf/H27_nenpo.pdf>，（参照 2017-06-28）．

(2) 日本貿易振興機構ベルリン事務所海外調査部欧州ロシアCIS課．インダストリー4.0実現戦略 プラットフォーム・インダストリー4.0 調査報告．日本貿易振興機構，2015，97p．<https://www.jetro.go.jp/ext_images/_Reports/01/c982b4b54247ac1b/20150076.pdf>，（参照 2017-06-28）．

(3) 経済産業省製造産業局．“Connected Industries”～我が国産業が目指す姿（コンセプト）～．経済産業省，2017，1p．<http://www.meti.go.jp/press/2016/03/20170320001/20170320001-1.pdf>，（参照 2017-06-28）．

(4) 内閣サイバーセキュリティセンター．サイバーセキュリティ戦略．2015，41p．<http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku.pdf>，（参照 2017-06-28）．

(5) 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，2016，60p．<http://www.soumu.go.jp/main_content/000428393.pdf>，（参照 2017-06-28）．

(6) IEC 62443-2-1:2010. Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program.

(7) 小林偉昭．国際的な標準・認証の動向 ～制御システムのセキュリティ評価・認証への取り組み～ ～IEC/ISA/ISCIとISASecure®の最新動向～．制御システムセキュリティセンター，2014，20p．<http://www.css-center.or.jp/sympo/2015/documents/20150514-22_03kobayashi.pdf>，（参照 2017-06-28）．

(8) ISASecure. "IEC 62443 - EDSA Certification". ISASecure. <http://www.isasecure.org/en-US/Certification/IEC-62443-EDSA-Certification>, (accessed 2017-06-28).

(9) ISASecure. "IEC 62443 - SSA Certification". ISASecure. <http://www.isasecure.org/en-US/Certification/IEC-62443-SSA-Certification>. (accessed 2017-06-28).

(10) IEC 62443-3-3 Ed. 1.0:2013. Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels.

(11) 小田原育也，小島健司．スマートコミュニティシステムのためのセキュアシステム構築技術 セキュアSITM．東芝レビュー．2011，**66**，11，p.10－13．

(12) ISA, ISA-62443-3-2 draft 7, Ed. 1:2017. Security for industrial automation and control systems Security Risk Assessments, System Partitioning and Security Levels. <http://isa99.isa.org/Public/Series/Documents/ISA-62443-3-2-Public.pdf>, (accessed 2017-06-28).



大矢　章晴　OYA Toshiharu
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.

中溝　孝則　NAKAMIZO Takanori
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.

松下　達之　MATSUSHITA Tatsuyuki, Ph.D.
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
博士（情報理工学）　IEEE・電子情報通信学会会員
Toshiba Digital Solutions Corp.