リスクコミュニケーションを容易にするTIRAのセキュリティプロファイル

TIRA Security Profiles Facilitating Risk Communication between Service Providers and Customers

川端　健 KAWABATA Takeshi

CPS（サイバーフィジカルシステム）の進展に伴い，サイバー空間のセキュリティ脅威がフィジカル空間の人や社会に影響を及ぼし始めている。セキュリティリスクを極力抑えるには，提供者と利用者の間でのリスクに関する情報交換（リスクコミュニケーション）が必要となるが，業界ごとに準拠するセキュリティの規格やガイドラインの表現が異なり，リスクコミュニケーションを困難にしていた。

東芝グループは，CPS開発・運用のための共通フレームワークである東芝IoTリファレンスアーキテクチャー（Toshiba IoT Reference Architecture，TIRAと略記）に，米国国立標準技術研究所（NIST）及び経済産業省が示すセキュリティ対策のフレームワーク要件を採用した独自のセキュリティ基準を設け，エネルギー分野に関わるサービスの評価プロファイルを整備した。このプロファイルでの表現を基本とすることで，TIRAに準拠した社会インフラ・産業システムのCPS サービスであるToshiba SPINEXでは，顧客とのリスクコミュニケーションが容易になる。

With the progress of cyber-physical systems (CPS), people and society in the physical space are facing security threats from cyberattacks via cyberspace. In order to minimize the effects of security risks, it is necessary to strengthen communication between service providers and customers by exchanging information associated with their risks. However, the difficulty encountered in such risk communication due to the different expressions of standards and guidelines adopted in each business field is a serious issue.

The Toshiba Group has created the Toshiba IoT Reference Architecture (hereafter abbreviated as TIRA) as a common platform to promote the development and operation of CPS, and has established its proprietary security standard for TIRA based on the Cybersecurity Framework (CSF) formulated by the National Institute of Standards and Technology (NIST) of the United States and the Cyber/Physical Security Framework (CPSF) formulated by the Ministry of Economy, Trade and the Industry (METI) of Japan. As part of these efforts, we have developed evaluation profiles compliant with TIRA for TOSHIBA SPINEX CPS products and services in the energy field so as to facilitate risk communication with customers.

1. まえがき

実世界のフィジカル空間とオンラインネットワーク上の仮想空間が融合するCPS化により，実世界の高度化・自動化が進み始めている。また，DX（デジタルトランスフォーメーション）により，CPSと人とのつながりが強まり，CPSを介した人と人のつながりも生まれ始めている。一方，セキュリティ脅威も，サイバー空間だけにとどまらず，フィジカル空間に影響を及ぼし，社会インフラや人の生活へ影響を及ぼし始めている。今まで，人は仮想空間の利用を一時停止するだけで，セキュリティ脅威を避けることができたが，段階的にそれも困難になることが予想される。

このような中，セキュリティ脅威への対策として，CPSの製品・システム・サービス提供者はリスク管理を行い，技術のセキュリティレベルを適切に維持し，プロセスのセキュリティ成熟度を高める取り組みを実施することが社会的な責務となっている。また，セキュリティ脅威は変化することから早めの取り組みとともに，顧客とセキュリティリスクに関する情報や意見を交換するリスクコミュニケーションを日々行う必要がある。

技術及びプロセスのセキュリティレベルを維持向上させる取り組みを実施する上で，共通の評価基準として用いられるのが，規格・ガイドラインなどに示されるセキュリティ要求事項である。この規格・ガイドラインは，業界・技術レイヤーごとに存在する。そのため，CPSの製品・システム・サービス提供者は，リスク管理の一環として，準拠する規格・ガイドラインの選定や，選定した規格・ガイドラインに準拠しているかどうかの評価（対応状況評価）に多くの時間を割いている。

東芝グループでは，CPSを開発・運用するための共通フレームワークとしてTIRAを定め，独自のセキュリティ基準を策定している。TIRAのセキュリティ基準は，CPSのサプライチェーン全体のサイバーセキュリティ確保を目的として策定された経済産業省の「サイバー・フィジカル・セキュリ

ティ対策フレームワーク（CPSF）[1]」，及び重要インフラのサイバーセキュリティを向上させるためのフレームワークであるNISTのFramework for Improving Critical Infrastructure Cybersecurity（CSF）[2]の要件を採用し，考慮すべき観点の網羅性を担保し，提供物・サービスに対する自己評価を顧客に提示できることとしている。

この取り組みは，規格・ガイドラインへの対応状況評価に多くの時間を割くのではなく，顧客に対して提供物のセキュリティのレベルや成熟度を適切に伝え，リスクコミュニケーションを行うことを念頭に置いている。ここでは，セキュリティに関する規格・ガイドラインの現状，リスクコミュニケーション上の問題点，及びこれを解決するための東芝グループの取り組みについて述べる。

2. 規格・ガイドラインにおける表現の多様性

CPS関連製品及びサービスにおけるセキュリティに関する代表的な規格・ガイドラインは，**図1**のように整理することができる。組織に関しては，組織体制や事業プロセスの要件が定められており，システム及びコンポーネントについては，技術レイヤーごとの技術要件が示されている。

各規格・ガイドラインで示される要件の表現は，抽象度が異なるため，複数の規格・ガイドラインへの対応状況評価を難しくしている。NIST CSFでは，他の主要な規格との参照関係が示されている。**表1**は，NIST CSFにある要件の一つであるID.AM-1を例に挙げて，IEC 62443（国際電気標準会議規格 62443）[3]やSP 800-53 rev.4[4]との表現の違いを比較して示している。IEC 62443及びSP 800-53の表現は，NIST CSFのAM-1の要件を目的とした場合の実現手段として捉えることができる。

このようにセキュリティ要件の表現は，目的要件，プロセス要件，設計要件，実装要件などに大別することができ，抽象度も様々である。また，一つの規格・ガイドラインでその抽象度が混在する場合もあり，理解を更に困難にしている。

表1. CSFの参照関係に基づく規格間における要件表現の違いの例

Differences in expression of similar requirements based on reference relationships between NIST CSF and other standards

規　格	ID	要　件
CSF	ID.AM-1	組織内の物理デバイスやシステムをリスト化する。
IEC 62443	2-1 4.2.3.4	組織は，各種IACSの識別子，装置に関するデータを収集し，セキュリティリスクの特性を識別し，それらの装置を論理的システムにグループ化しなければならない。
IEC 62443	3-3 SR7.8	制御システムは，インストールされたコンポーネントのリストと関連プロパティを報告する機能を提供しなければならない。
SP 800-53	CM-8	組織は，システムコンポーネント一覧を作成，文書化する。また，組織が定めた頻度でレビューし，更新する。
SP 800-53	PM-5	組織は，組織の情報システムの一覧を作成し，維持・管理する。

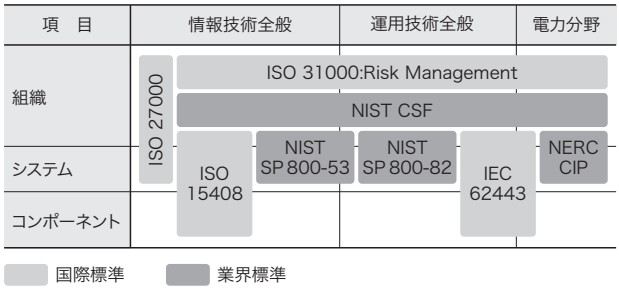
IACS：Industrial Automation and Control System（産業用オートメーション及び制御システム）

3. リスクコミュニケーション上の問題点

リスクコミュニケーションをする上で，提供製品・サービスに対するセキュリティ規格・ガイドラインへの対応状況評価を実施する必要があり，**図2**に示す①から③の手順で実施される。

リスク分析準備としてターゲットを識別する手順①では，提供製品・サービスに含まれる構成資産の識別を実施し，重要度を把握する。それらの構成資産の整理情報を基に，手順②のリスク分析を実施する。その分析整理結果を基に，規格・ガイドラインにある要件への対応状況を手順③で整理する。

リスクコミュニケーションに関わる問題点としては，多くの規格・ガイドラインの理解と対応コスト，組織に対する規格・ガイドライン準拠の必須化，及び規格・ガイドラインへの対応状況評価結果と遂行力のギャップの三つが挙げられる。



ISO：国際標準化機構　　NERC：北米電力信頼性評議会
CIP：重要インフラ保護基準

図1. CPSの製品・サービスに関わる代表的な規格・ガイドライン

CPSの製品・サービスに関するセキュリティ規格及びガイドラインを，組織，システム，コンポーネントに分けて整理して示した。

Typical standards and guidelines for CPS products and services

図2. 製品・サービスのセキュリティ規格・ガイドラインへの対応状況評価の手順

リスクコミュニケーションをする上で，セキュリティに関する規格・ガイドラインへの製品・サービスの対応状況を評価する必要があるが，規格・ガイドライン間の要件の違いを理解するのに多大な時間を要する。

Flow of processes for evaluation of CPS products and services corresponding to security standards and guidelines

⑴　多くの規格・ガイドラインの理解と対応コスト

２章で示した規格・ガイドラインの表現の多様なことや，前提とするアーキテクチャーの記載がないことから，個々のセキュリティ要件，及び規格・ガイドライン間の違いを理解するのに多大な時間・コストを要する。このようなセキュリティ対応が，セキュアなCPSサービスを次々と生み出し社会をより良くすることの足かせになりかねない。業界ごとに適切なポイントで，リスクコミュニケーションができないことが問題である。

⑵　組織に対する規格・ガイドライン準拠の必須化

従来，CPSの関連コンポーネント・システムは，提供物に対する技術レベルに関する規格・ガイドライン準拠だけが注目・要求される場合が多かった。これは，製品・システム間を接続する上で，各コンポーネント・システムが備えるセキュリティレベルを把握する必要があったからである。一方，フィジカル機器がサイバー空間に接続されることにより脅威の顕在化が進み，セキュリティパッチや脆弱性対応の要求が増加し始めている。そのため，従来は重視されない場合もあった開発・保守プロセスに関する組織体制及びプロセス整備の成熟度についての要求が，高まり始めている。また，CPSサービスにおいても同様である。

⑶　規格・ガイドラインへの対応状況評価結果と遂行力のギャップ　　セキュリティ規格・ガイドラインにおける対応評価までの段階では，リスクコミュニケーションを実施する事前準備ができたにすぎない。想定外のリスクへの対応能力として，技術レベルを維持し，組織・プロセス成熟度を高める努力を継続する遂行力が事業者にあるか否かを判断するには，リスクコミュニケーションを通して確認するしかない。

4. TIRAのセキュリティプロファイル整備の取り組み

顧客又は共創パートナーに対して提供サービスのセキュリティレベル・成熟度を適切に伝える上で，共通の指標が必要となる。この共通指標として用いられるのが，セキュリティ規格・ガイドラインである。一方，業界ごとに個別にCPSサービスを実現し業界間が排他的であるうちは，DX化が進まない。業界ドメインを越えてデータを流通させ，新しい価値を生む情報へと変換していくことが，必要となっている。そのためには，業界ごとに策定される規格・ガイドラインの差異を吸収していく必要がある。

そこで，今回はエネルギー分野での組織における共通プロファイルについて，NIST CSFをベースに，TIRAを前提とした考慮すべきプロファイルを整備した。検討ステップは４ステップである。

ステップ１：共通ミッションとその目標の設定　　リスクコミュニケーションをする上で，共通のミッションとそれに対する目標を共有し，目標達成に向けた議論にすることが重要である。ここでは，エネルギー分野におけるCPSサービスについての三つの共通ミッションに対して，目標を設定する（**表２**）。

ステップ２：目標に関連する規格・ガイドライン要件の抽出

各ミッションのセキュリティ目標に合わせるために，プロファイルに表記する要件に優先順位を付ける。具体的には，各ミッションに関連性の強いNIST CSFの要件を抽出し，最も重要な要件を太字として整理した。**表３**にその例を示す。

ステップ３：CPSサービスの影響レベルの定義　　ミッションごとにエネルギー分野におけるインシデントによる影響レベルのランク付けを，SP 800-82[5]を参考にして**表４**のように定義する。このランクごとに，次のステップ４で考慮すべき観点をプロファイルとして整理する。

ステップ４：CPSサービスプロファイルの作成　　**表５**に示すプロファイルは，CPSサービスのリスクを低減する

表２．エネルギー分野における共通のミッションとその目標

Typical missions and targets in energy field

ミッション	目　標
環境の安全性	エネルギー分野のサービスは，環境の安全性に悪影響を及ぼすセキュリティリスクに対応が求められる。
生産目標の確保	エネルギー分野のサービスは，生産目標の維持に悪影響を及ぼすセキュリティリスクに対応が求められる。
企業秘密の保護	エネルギー分野のサービスは，社会インフラに関わる企業秘密に悪影響を及ぼすセキュリティリスクに対応が求められる。

表３．各ミッションの目標と関連性の強いCSFの主な要件

Mission targets and relevant NIST CSF subcategories

ミッション	環境の安全性	生産目標の確保	企業秘密の保護
資産管理	**ID.AM-1**	**ID.AM-1**	**ID.AM-1**
	ID.AM-2	ID.AM-2	**ID.AM-2**
	ID.AM-3	ID.AM-3	**ID.AM-3**

表４．インシデントによるエネルギーサービスへの影響レベル

Impact levels of energy services at time of incident

影響レベルのランク	低	中	高
環境	一時的なダメージ	継続的なダメージ	甚大なダメージ
生産	一時的な削減	対応計画策定を要する一時的な削減	利用者への影響が避けられない大幅な削減
企業イメージ	一時的	継続的	完全な失墜

表5. エネルギーサービスのプロファイルの例

Examples of profiles for energy services based on NIST CSF

CSFの要件	影響レベル	エネルギープロファイル
ID.AM-1	低	エネルギーサービスを構成するシステムコンポーネントの資産を，HWコンポーネント資産として文書化する。例えば，TIRAのエッジ層にあるPLC，DCS，センサー，アクチュエーター，ネットワーク装置，保護リレー，表示器，計算機やプラットフォーム・エンタープライズ層にある計算機，クラウド環境などが含まれる。組織で定義されたプロセスに基づき，レビュー・更新される。また，コンポーネント資産の区別のため，マシン名，製造者，モデル，シリアル番号，設置場所などが含まれる。
	中	各資産の管理者をHWコンポーネント資産文書に追記する。
	高	未承認のハードウェアコンポーネント・ファームウェアを検出するためのメカニズムを特定する。また，検出メカニズムは自動化される。
ID.AM-2	低	エネルギーサービスを構成するシステムに含まれるソフトウェア及びファームウェアの資産を，ソフトウェア資産として文書化する。ソフトウェアは，OSやアプリケーションを含み，ライセンス情報・バージョン情報が含まれる。ソフトウェア文書一覧は，組織で定義されたプロセスに基づき，レビュー・更新される。
	中	ソフトウェアの管理者を特定し，文書化する。
	高	未承認のソフトウェアを検出するためのメカニズムを特定する。また，検出メカニズムは自動化される。

HW：ハードウェア　　PLC：Programmable Logic Controller
DCS：Distributed Control System　　OS：基本ソフトウェア

上で利用するだけでなく，共通のリスクコミュニケーションをする目的で，ランクごとに作成した。これは，従来の規格・ガイドラインの役割に代わることを目的としているのものではない。また，作成にあたりNIST CSFの参照関係を参考にし，TIRAに合わせた形で表現している。

このプロファイルを，TIRAに準拠した社会インフラ・産業システムにおけるCPSサービスである，Toshiba SPINEXにおけるリスクコミュニケーションのベースラインとすることで，業界ごとに異なる規格・ガイドラインを解釈する手間がポイントを押さえた上で削減でき，これを共通言語化することで，コミュニケーションが容易になる。

5. あとがき

CPSサービスにおけるリスクコミュニケーションを目的としたTIRAセキュリティプロファイル整備の取り組みについて述べた。今後，エネルギー業界をベースに作成したこのプロファイルを基に，異なる業界に対しても差分プロファイルを作成することで，業界間の差異も明確になり，業界間のコミュニケーションを容易にするものと考えている。

リスクコミュニケーションをする意義は，リスクの確率を下げるための議論をするだけでなく，合理的なリスクの受容を議論することであり，場合によっては納得のいく失敗もあり得る。また，リスクコミュニケーションは，全てクローズドな場で実施する必要はない。各製品・サービスレベルにおいても，オープンな場でリスクコミュニケーションを取り，よりリーズナブルなセキュリティ対応で安心・安全な社会を実現していくことが重要である。

今後，このTIRAのセキュリティプロファイルをオープンな場で議論していくことを，計画していく。

文　献

(1) 経済産業省．サイバー・フィジカル・セキュリティ対策フレームワーク Version 1.0. <https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html>,（参照 2022-03-01）.
(2) NIST. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. <https://www.nist.gov/cyberframework>, (accessed 2022-03-01).
(3) IEC. Understanding IEC 62443. <https://www.iec.ch/blog/understanding-iec-62443>, (accessed 2022-02-01).
(4) NIST. Security and Privacy Controls for Federal Information Systems and Organization SP 800-53 rev.4. <https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/archive/2015-01-22>, (accessed 2022-03-01).
(5) NIST. Guide to Industrial Control Systems（ICS）Security. Special Publication 800-82 Revision 2. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>, (accessed 2022-03-01).

川端　健 KAWABATA Takeshi
研究開発センター
サイバーセキュリティ技術センター
セキュリティ技術部
Security Technology Dept.