CPSのセキュリティを担保するリスクアセスメント手法

Risk Assessment Methods Ensuring Security of CPS

源島　朝昭 GENJIMA Tomoaki　　射水　　亮 IMIZU Ryo

CPS（サイバーフィジカルシステム）の進展に伴い，サイバー空間への攻撃がフィジカル空間まで到達し，生活者や企業の活動に影響を与えるセキュリティリスクが高まっている。また，CPSを実現するシステム及びサービスの提供事業者は，ライフサイクル全体を通したリスク管理が社会的責務となってきている。しかし，リスクの特定・分析・評価を行うリスクアセスメントの専門家が確保できないため，時間やコストを掛けられない，また同一手法を用いても経験やスキルによって分析結果が異なる，などの問題に直面している。

東芝グループは，これらの問題を解決するため，セキュリティの専門家でなくても一定のスキルがあれば，専門家と同等以上の結果を出せるリスクアセスメント手法の整備・改良を続けており，CPSのセキュリティ向上に貢献している。

Accompanying the expansion of cyber-physical systems (CPS), a strong need exists for the protection of people's lives and corporate activities against cyberattacks on the physical spaces of CPS via cyberspace. Demand has consequently arisen for risk management systems that can take responsibility for each phase of the life cycle of CPS systems and services. However, various problems must be overcome including a lack of experienced personnel in this field, costly and time-consuming analysis and estimation work, and differences in the analysis results obtained by personnel having different experience levels and skills even when the same method is used.

With this as a background, the Toshiba Group is continuously developing and improving risk assessment methods that allow even inexperienced personnel having a certain level of skill to obtain results equal to or better than those obtained by experienced personnel. These methods are expected to contribute to the realization of CPS with improved security.

1. まえがき

社会インフラが直面する様々な課題をデジタル技術で解決するCPSにより，これまで独立していたフィジカル空間（実世界）とサイバー空間（デジタル技術）を融合させることができる。これにより，実世界データの利活用が進み，新たなビジネス価値が創造される時代となっている。一方，サイバー空間への攻撃がフィジカル空間まで到達し，社会インフラなどの重要機能の維持が困難となり，生活者や企業の活動に影響を与えるリスクも高まってきている。

CPSを実現する製品，システム，及びサービスの提供事業者は，それらの開発，運用，及び廃棄といったライフサイクル全体を通してセキュリティを確保するために，サイバー攻撃によるインシデント発生後に対応するだけでなく，開発の設計段階からセキュリティ確保に向けた取り組みを行うことが，社会的な責務となっている。その責務を全うするためには，リスク管理が重要なポイントとなる。

リスクの特定・分析・評価を実施するリスクアセスメント手法（**図1**）は数多く存在するが，どのような場面でどの手法を用いるかは定まっていない。そのため，CPSを実現しようとする業界のセキュリティ基準，ガイドライン，及び企業ポリシーにより，CPS提供事業者と顧客との協議でその手法が決定されることが多い。また，その実行にあたっての課題として，セキュリティの専門家の確保，時間・コストの削減，

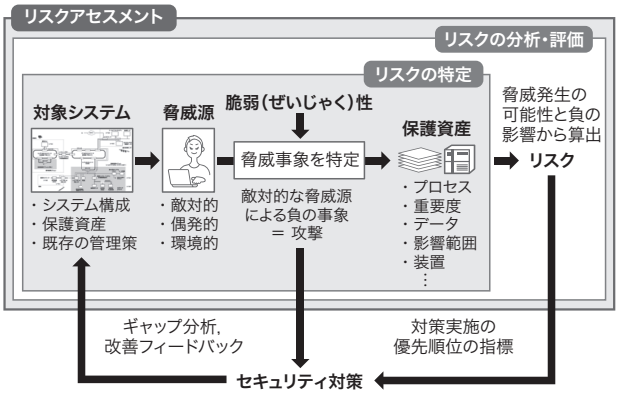


図1. リスクアセスメントのプロセス概念

リスクアセスメントは，特定した脅威に対して“リスク”という形でセキュリティ要件を決定するための判断基準を出力する，リスク管理プロセスの一部である。

Conceptual diagram of risk assessment processes

リスクアセスメント実施者の経験やスキルが違っても分析結果が同じになるようにする，といったことが挙げられる。

東芝グループは，これらの課題を解決するため，顧客要求に応じたリスクアセスメント手法を用いて，セキュリティの専門家がいない場合でも，一定のスキルがあれば，専門家と同等以上の結果を出せるリスクアセスメント手法を整備し，随時改良を進めている。ここでは，その取り組みについて述べる。

2. CPSのセキュリティを担保するリスクアセスメント手法とその課題

CPSを実現する製品，システム，及びサービスの提供事業者に求められる顧客からのリスクアセスメント要求は，その目的，分析対象物，及び適用するライフサイクルプロセスによって異なり，取り得るリスクアセスメント手法のアプローチも変わってくる。東芝グループは，IT（情報技術）セキュリティ管理のガイドラインであるISO/IEC TR 13335-3[1]（国際標準化機構／国際電気標準会議 技術報告書 13335-3）に示される四つのリスクアセスメント手法を，顧客要求に応じて使い分けている（**表1**）。

ベースラインアプローチは，一定の確保すべきセキュリティ基準を設定し，分析対象システムの適合性を評価する手法である。その基準は，分析対象システムが適用される用途や業界別の基準・ガイドラインなどが一般的であり，主に要件定義の段階で用いられる。例えば，産業用オートメーション及び制御システム用途であれば，その国際標準であるIEC 62443シリーズ[2]を基準としている。ベースラインアプローチは，第三者との合意形成が取りやすい反面，業界別に国際標準，基準，及びガイドラインがあり，そのセキュリティ要件の粒度も異なることから，リスクアセスメント実施者によってその解釈が異なり，評価結果にばらつきが生じるという問題がある。

詳細リスク分析アプローチは，構造化された評価指標に基づいて評価する手法である。独立行政法人 情報処理推進機構（IPA）発行の「制御システムのセキュリティリスク分析ガイド[3]」を用いて評価するケースが多く，主に運用中の社会インフラシステム向けの評価に用いられる。この手法は，分析対象システム自体に対する正確なリスク分析が可能な反面，セキュリティの専門家の確保が必要であり，多くの時間・コストが掛かるという問題がある。

非形式的アプローチは，専門家の知見や経験を活用して評価する手法である。経験値を活用するのでコストは抑えられるが，属人的であり継続的なセキュリティレベルの向上に課題がある。

最後の組み合わせアプローチは，ベースラインと詳細リスク分析を組み合わせて評価する手法である。

いずれの手法もセキュリティの専門家や分析対象システムの知識を持つ人の確保，時間及びコストの削減が必要で，実現に向けての障壁が高い。このような背景から，まずは顧客自身で速やかに分析対象システムのセキュリティ対策状況を把握できないかといった，要望が増えてきた。そこで東芝グループは，新たなアプローチとして，顧客自身が分析対象システムのセキュリティ対策の達成状況を簡易的に判定できるようにし，その結果を東芝グループのセキュリティの専門家が総合評価して顧客へフィードバックする，簡易リスク分析アプローチのツールを開発し，顧客に無償提供して

表1. リスクアセスメント手法

Risk assessment methods defined in International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) TR 13335 guidelines

リスクアセスメント手法	内　容
ベースラインアプローチ	既存の国際標準や業界基準に基づいて，分析対象システムに対してセキュリティ対策要件の適合性などをチェックする。
詳細リスク分析アプローチ	分析対象システムに対して，①重要度（あるいは損なわれた場合の事業被害レベル），②脅威レベル，③脆弱性レベルの三つの評価指標を用いて，リスク分析を実施する。
非形式的アプローチ	組織や担当者の経験や判断によって，リスクを評価する。
組み合わせアプローチ	複数の分析アプローチを併用し，作業の効率化や異なった評価視点の活用によって，分析精度の向上と作業工数増大の回避を図る。

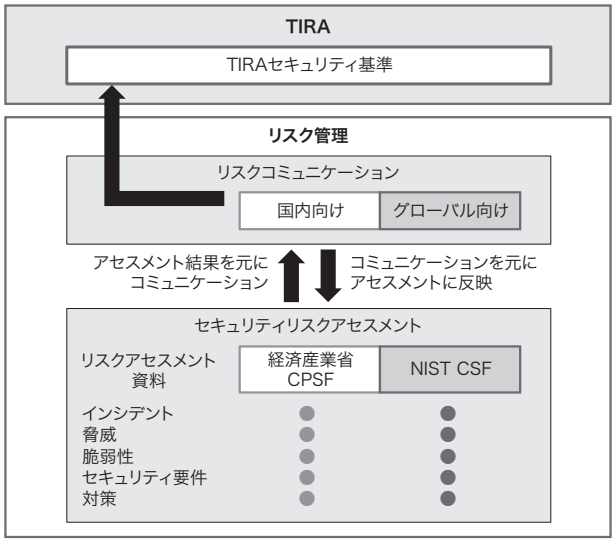


図2. TIRAセキュリティ基準

国内・グローバル向けの社会インフラに対応したセキュリティ基準を採用することで，提供するCPSのセキュリティ状況を客観的に評価し，顧客とのコミュニケーションが図れる。

Security criteria of Toshiba IoT Reference Architecture open and common framework for developing and operating Internet of Things (IoT) services as CPS

いる。

3章以降，特に使用頻度が高いベースラインアプローチと簡易リスク分析アプローチにおける課題への取り組みについて，説明する。

3. ベースラインアプローチ

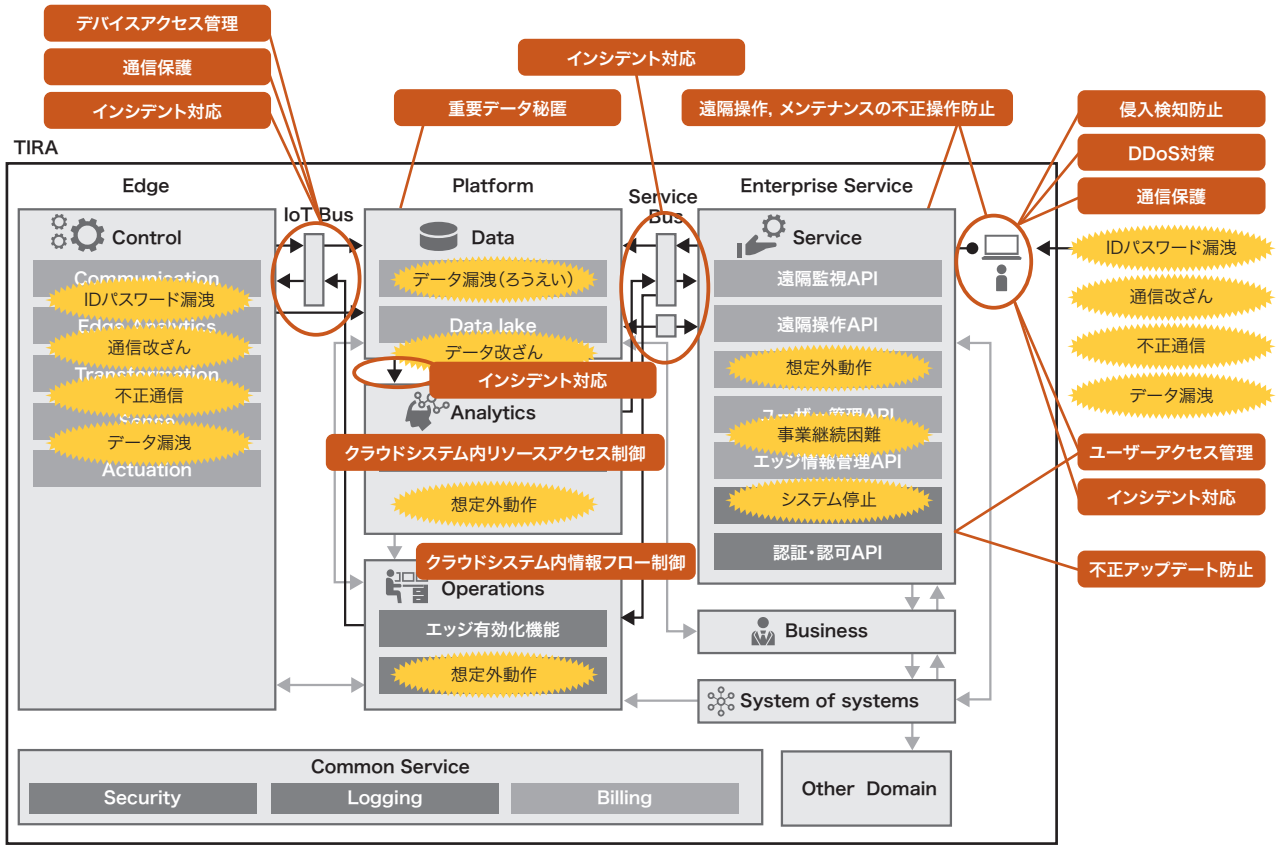
ベースラインアプローチの主な課題として，2章で述べたリスクアセスメント実施者による評価結果のばらつき抑制と，様々なシステム構成形態ごとにリスク特定・分析・評価に掛かるコストの削減がある。

これらの課題を解決するために，システム構成を分類・一般化したリファレンスアーキテクチャー，及びそのリスク評価結果から，必要なセキュリティ基準を事前に定義し，各CPSのリスクアセスメントに対してその結果を活用するというアプローチを考えた。

具体的には，東芝グループにおいてCPSを開発・運用するための共通フレームワークとして定めている，東芝IoT（Internet of Things）リファレンスアーキテクチャー（Toshiba IoT Reference Architecture，TIRAと略記）に対して，セキュリティ基準を策定した。その基準の策定においては，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）[4]」，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米国国立標準技術研究所（NIST）のFramework for Improving Critical Infrastructure Cybersecurity（CSF）[5]の要件を採用することで，網羅性を確保した。

以上のような取り組みにより，TIRA上で構築した様々なCPSに対して，共通のセキュリティ要件が抜け漏れなく定義でき，同様のシステム開発をする際にこれを用いることで，あらかじめセキュリティを考慮したシステム設計が可能となる（**図2**）。

また，セキュリティの専門家が実施したリスクアセスメント結果を東芝グループ内で共有することで，その再利用性を高め，コスト削減を図っている（**図3**）。



ID：識別情報　API：Application Programming Interface　DDoS：Distributed Denial of Service

図3. 遠隔管理アーキテクチャーのリスク分析例

TIRAのユースケース及びアーキテクチャーをパターン化し，セキュリティの専門家によるセキュリティ脅威と対策結果を示すことで，再利用性を高めている。

Example of risk analyses of remote management architecture

4. 簡易リスク分析アプローチ

簡易リスク分析アプローチは，顧客自身が分析対象のセキュリティ対策状況に対する設問項目に回答し，その回答結果を東芝グループの担当者が個別評価し，更にセキュリティの専門家が総合評価した結果を，顧客へフィードバックするフローとなる（**図4**）。その一連のフローで使用するツールの特長について述べる。

⑴ 設問回答内容の曖昧さの排除　　簡易リスク分析アプローチでは，分析対象システムのセキュリティ対策状況の設問を14項目に絞り込み，顧客側で現在のセキュリティ対策レベルを段階的に判定できるようにしている。その達成状況の網羅性を高めるために，一般社団法人JPCERTコーディネーションセンターが無償配布している「制御システムセキュリティ自己評価ツール（J-CLICS）[6]」の設問項目を参考とし，過去に東芝グループで実施した社会インフラ向けの詳細リスク分析で得た脅威と，その具体的な対策の知見を取り入れて開発した。

ここでは，設問回答の全てを自由記述から選択方式にすることで，顧客からの回答内容の曖昧さを排除し，個別評価者が機械的に評価できるようにした。顧客に対しても，設問ごとの具体的な実施例，その証明のための成果物，及びセキュリティ対策状況の成熟度を，3段階で判定できるようにし，それらを理解しやすい用語・表現で示すことで，専門家でなくても簡易に自己判定できるようにした（**図5**）。

⑵ 個別評価基準の共通化　　顧客から回収した設問回答がどの成熟度でも，個別評価者がそれぞれの成熟度に合致したセキュリティ対策案を示せるようにするために，セキュリティの専門家の知見を設問ごとにデータベース化した（**図6**）。それを東芝グループ内に共有することで，一定のスキルがあれば，専門家と同等以上の個別評価結果を出せるように工夫している。

⑶ 評価結果の有用性　　個別評価者が実施した評価結果を，最終的に東芝グループのセキュリティの専門家が再評価している。具体的には，レーダーチャートによるセキュリティ対策の総合評価結果をまとめ，脆弱（ぜいじゃく）な箇所については，記述式のアドバイスをフィードバックすることで，評価結果の有用性を確保している（**図7**）。

更に，この簡易アセスメントの利点は，現状のリスクアセスメントだけでなく定期的に実施することで，自己成熟度評価ツールとしても活用できることである。

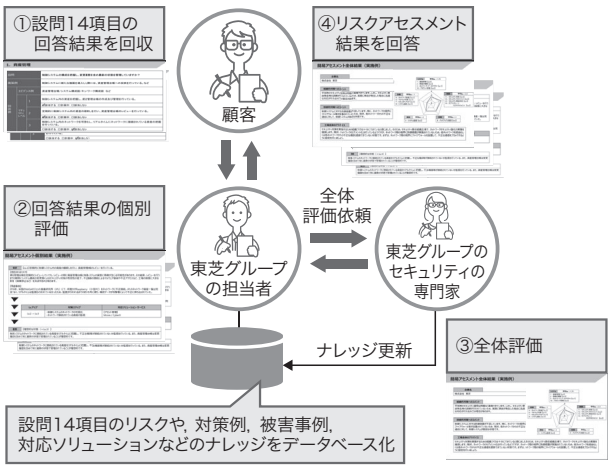


図4. 簡易リスク分析の概要

分析対象システムの運営者である顧客自身が，14個の設問に回答することで，現在のセキュリティ対策状況を網羅的に評価できる。

Overview of simplified risk assessment

実際に設問で問われている対策を実施している場合の，具体的な実施内容の例を示す。

実際に設問で問われている対策を実施している場合の，証明や成果物の例を示す。

3段階の成熟度（マチュリティーレベル）を“該当する”，“計画中”，及び“該当しない”の三つで評価する。

設問			取引先や関連企業に対して，セキュリティ要件を仕様書などで明示していますか？
施策例			調達時に自社が求めるセキュリティ要件を仕様書に含めている。など
回答例	エビデンス例		セキュリティ要件を含めた調達仕様書など
	マチュリティーレベル	1	取引先などに対して，セキュリティ要件を仕様書などで明確に提示している。
			☑該当する　□計画中　□該当しない
		2	取引先などから，セキュリティ対策の実施状況の報告（監査を含む）を受け，対策状況を把握している。
			☑該当する　□計画中　□該当しない
		3	取引先なども含めたセキュリティ事故発生時の対応手順を定め，定期的に確認を行っている。
			□該当する　□計画中　☑該当しない

図5. 設問回答内容の曖昧さの排除

組織のセキュリティ対策状況に関する設問項目の実施例である。評価対象システムについてのセキュリティ対策の現状に当てはまる選択肢にチェックすることで，曖昧さを排除する。

Expressions to eliminate ambiguous questions and answers

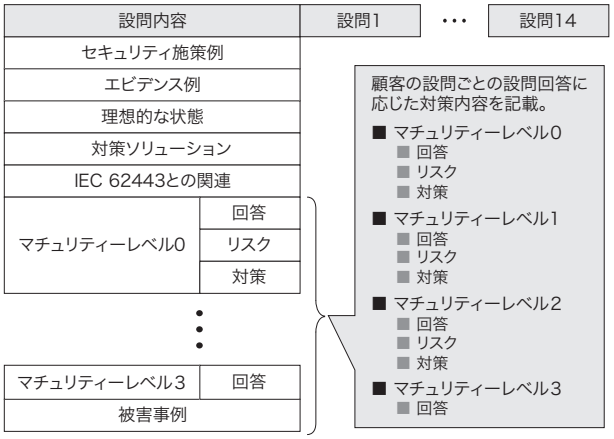


図6. 専門家の知見をベースにした個別評価基準の共通化

設問ごとのリスクや，対策例，被害事例，対応ソリューションなどのナレッジをデータベース化し，個別評価者に提供する。

Standardization of individual evaluation criteria based on knowledge of experienced personnel

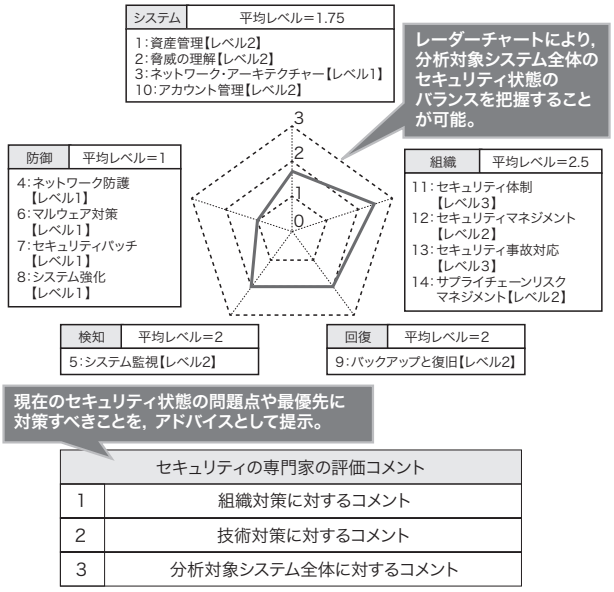


図7. セキュリティ対策の評価結果の例

セキュリティの専門家が再分析を行い，現状の分析対象システムのセキュリティ状態に対するコメントを，顧客にフィードバックする。

Example of results of evaluation of security measures

5. あとがき

CPSのライフサイクルのセキュリティ確保を目的とした，リスクアセスメントの取り組みについて述べた。セキュリティの専門家の知見を取り入れてCPS向けのリスクアセスメント手法を整備することで，東芝グループ内で複数のCPS開発が同時に進行する場合のセキュリティ要件定義の効率化や，顧客に納入した分析対象システムを含めたリスク評価結果のばらつき・評価コストの抑制効果などが得られた。一方，CPSはシステム構成や取り扱う資産が多様であり，かつそのリソースやスループットといった制約条件により，個々のリスクに対して導入できる対策が異なるという問題がある。更に，DX（デジタルトランスフォーメーション）の進展によりCPSが変容するとともにサプライチェーンが複雑化しており，実現するアーキテクチャーも変化し続けている。

今後は，システム制約を考慮した対策選定の導出技術の開発，並びに新たなシステム構成形態に対応した継続的なリスクアセスメント手法の改善を行い，東芝グループへの展開及び顧客へのアセスメントサービス提供により，CPSのセキュリティ向上に貢献していく。

文　献

(1) ISO/IEC TR 13335-3:1998. Information technology - Guidelines for the management of IT Security - Part 3 : Techniques for the management of IT Security. ISO.
(2) IEC. Understanding IEC 62443. <https://www.iec.ch/blog/understanding-iec-62443>, (accessed 2022-02-01).
(3) IPA. 制御システムのセキュリティリスク分析ガイド 第2版 ～セキュリティ対策におけるリスクアセスメントの実施と活用～. 2020, 384p. <https://www.ipa.go.jp/files/000080712.pdf>,（参照 2022-02-01）.
(4) 経済産業省 商務情報政策局 サイバーセキュリティ課. サイバー・フィジカル・セキュリティ対策フレームワーク Society5.0における新たなサプライチェーン（バリュークリエイションプロセス）の信頼性の確保に向けて Version 1.0. 経済産業省, 2019, 262p. <https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf>,（参照 2022-02-01）.
(5) NIST. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. 2018, 55p. <https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf>, (accessed 2022-02-01).
(6) JPCERTコーディネーションセンター. 制御システムセキュリティ自己評価ツール（J-CLICS）. <https://www.jpcert.or.jp/ics/jclics.html>,（参照 2022-02-01）.

源島　朝昭　GENJIMA Tomoaki
東芝デジタルソリューションズ（株）
ICT ソリューション事業部 制御セキュリティ事業推進部
Toshiba Digital Solutions Corp.

射水　　亮　IMIZU Ryo
東芝デジタルソリューションズ（株）
ICT ソリューション事業部 制御セキュリティ事業推進部
Toshiba Digital Solutions Corp.