トレンド

社会インフラや産業システムのCPSを支える東芝グループのサイバーセキュリティサービス・技術

Toshiba Group's Cybersecurity Services and Technologies Supporting CPS in Social Infrastructure and Industrial Systems

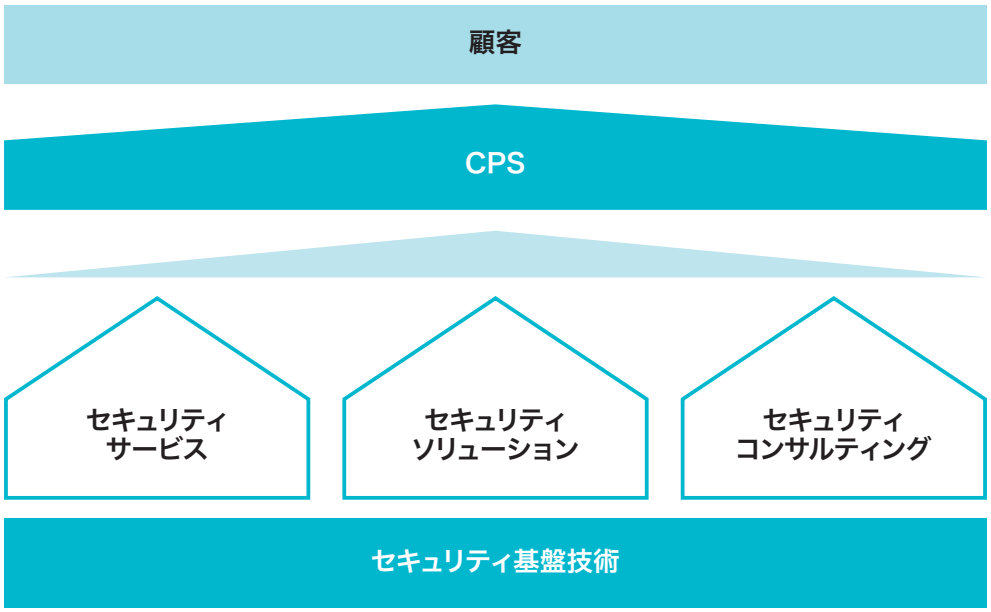
天野　隆 AMANO Takashi　　岡田　光司 OKADA Koji

持続可能な社会の実現に向け，東芝グループは，デジタル技術を活用して社会インフラや産業システムの進化を支える企業を目指している。近年，サイバー空間とフィジカル空間の技術が融合するCPS（サイバーフィジカルシステム）の進展とともに，従来の情報システムだけでなく，制御システムへもサイバー攻撃の脅威が高まっている。

このような状況の中，社会インフラや産業システムに対応可能なサイバーセキュリティマネジメント体制を強化するとともに顧客やパートナーと連携することで，システム開発から運用までサプライチェーン全体を支えるサイバーセキュリティを実現するサービスや技術の開発に取り組んでいる。

To contribute to the realization of a sustainable society, the Toshiba Group has set the goal of becoming a company supporting the evolution of social infrastructure and industrial systems through the utilization of digital technologies. In this context, the ongoing shift to cyber-physical systems (CPS) that fuse cyberspace and physical space technologies has led to a recent trend in which not only conventional information technology (IT) systems but also operational technology (OT) systems are facing growing threats from cyberattacks on physical space via cyberspace.

We are responding to this situation by making efforts to enhance our cybersecurity management systems so as to cater to the needs of social infrastructure and industrial systems, while developing cybersecurity services and technologies so as to support the entire supply chain from system development to operation in cooperation with our customers and partners.



特集の概要図．CPSの進化を支えるサイバーセキュリティサービス・技術
Cybersecurity services and technologies supporting evolution of CPS

1. 社会インフラ・産業システムのデジタル化とセキュリティ脅威の高まり

社会インフラや産業システムなどの制御システムは，旧来，独自システムと閉じたネットワーク環境で開発・運用されていた。しかし近年，情報システムで用いられてきた汎用的なOS（基本ソフトウェア），通信プロトコル，SW（ソフトウェア）が用いられるようになるとともに，生産管理システムなどの情報システムとの接続や，クラウドシステムでの製造・運用データの活用などのデジタル化が進み，インターネットへの接続も加速している。

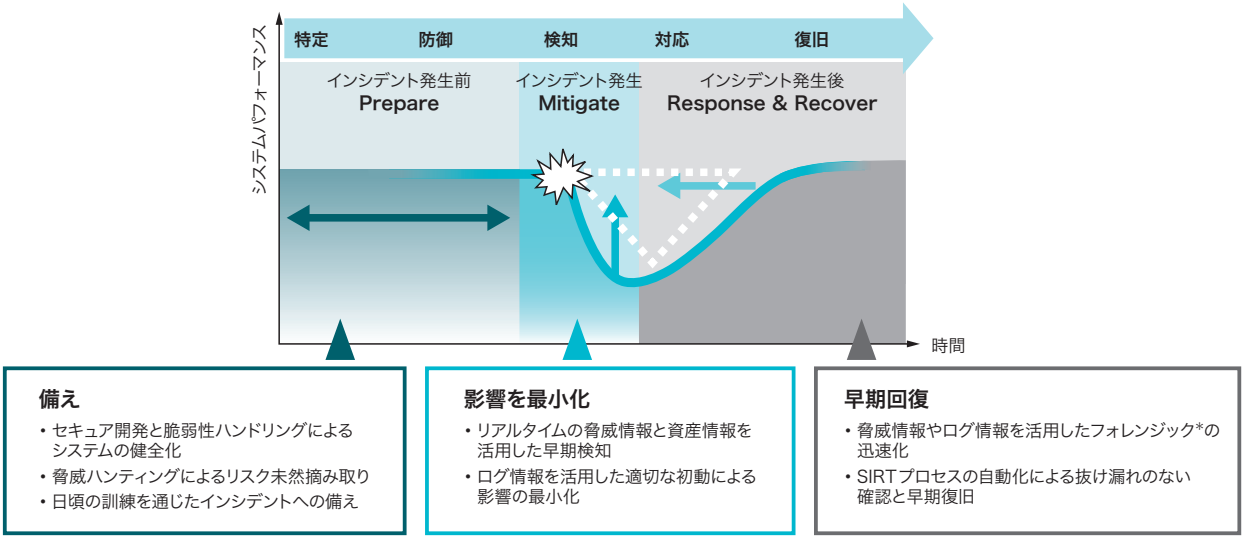
一方で，これまで閉じた環境で運用されていた制御システムが情報システムと接続・融合したことにより，これまで情報システムで起こっていたサイバー攻撃の脅威が社会インフラや産業システムにも及んでいる。最近では，ランサムウェアにより米国の石油パイプラインや国内の自動車工場が停止し，多額の損害が発生したことは記憶に新しい。これらは直接制御システムに対する攻撃ではなかったものの，情報システムと融合した産業システムが身の代金要求ビジネスの手段とされているのは明らかである。更に，2009年から2010年にイラン核燃料施設のプラント操業停止を発生させたStuxnetや，2015年から2016年にウクライナの電力システムを狙い大停電を発生させたサイバー攻撃のように，制御システムそのものに対する攻撃もこれまでに数多く発生している。このため，今後社会インフラや産業システムを狙った攻撃が，更に高度化することが予想される。

前述の自動車工場の例では，自動車会社本体ではなく関連部品会社への攻撃に端を発しており，サプライチェーン全体で対策をしていくことがいかに難しいかが明らかになった。また，2021年に発覚したRipple20のように，様々な機器やシステムに組み込まれたSWで脆弱（ぜいじゃく）性が発覚すると，その影響範囲の特定や対応が自社だけでは極めて困難な状況も生じている。そのため，サプライヤーの製造過程から顧客でのシステム運用まで，サプライチェーン全体で一貫したセキュリティ対策の必要性が求められている。

ここでは，東芝グループのサイバーセキュリティへの取り組みとして，社会インフラや産業システムを進化させる，CPSのレジリエンス向上のためのセキュリティサービス，ソリューション，コンサルティング，及び基盤技術について述べる（**特集の概要図**）。

2. サイバーセキュリティへの取り組み

東芝グループでは，自社の情報システムや，工場・設備などの生産システム，更には社会インフラ・産業分野において顧客に提供する製品・システム・サービスのサイバー攻撃に対するレジリエンスを向上させるため，“サイバーレジリエンス”のコンセプトを掲げている（**図1**）[1]。サイバーレジリエンスは，“インシデントに備え，その影響を最小化し，早



SIRT：Security Incident Response Team

＊セキュリティ事故発生時に，原因究明のためにコンピューターに残された証拠を調査すること

図1. サイバーレジリエンスのコンセプト

サイバー攻撃に対するレジリエンスを向上させるため，インシデントに備え，その影響を最小化し，早期に回復する能力と成熟度の向上を目指している。

Concept of cyber resilience against incidents caused by cyberattacks

期に回復する能力”のことであり，インシデント発生前，発生時，発生後のそれぞれにおいて，以下に示すような，システムパフォーマンスを最大化する取り組みで，レジリエンスの能力と成熟度の向上を目指している。

(1) インシデント発生前（Prepare：備え）　脆弱性の混入しないセキュアな設計・構築や，脅威ハンティングによるリスクの未然摘み取り，日々のインシデント対応訓練など，いわゆるサイバーハイジーンにつながる取り組みの強化

(2) インシデント発生時（Mitigate：影響を最小化）　脅威情報や収集したログを速やかに分析してインシデントの影響範囲を特定し，侵害の拡大を早期に抑え，影響を最小化するための取り組みの強化

(3) インシデント発生後（Response & Recover：早期回復）　ログの活用による根本原因の究明と，速やかな恒久対策

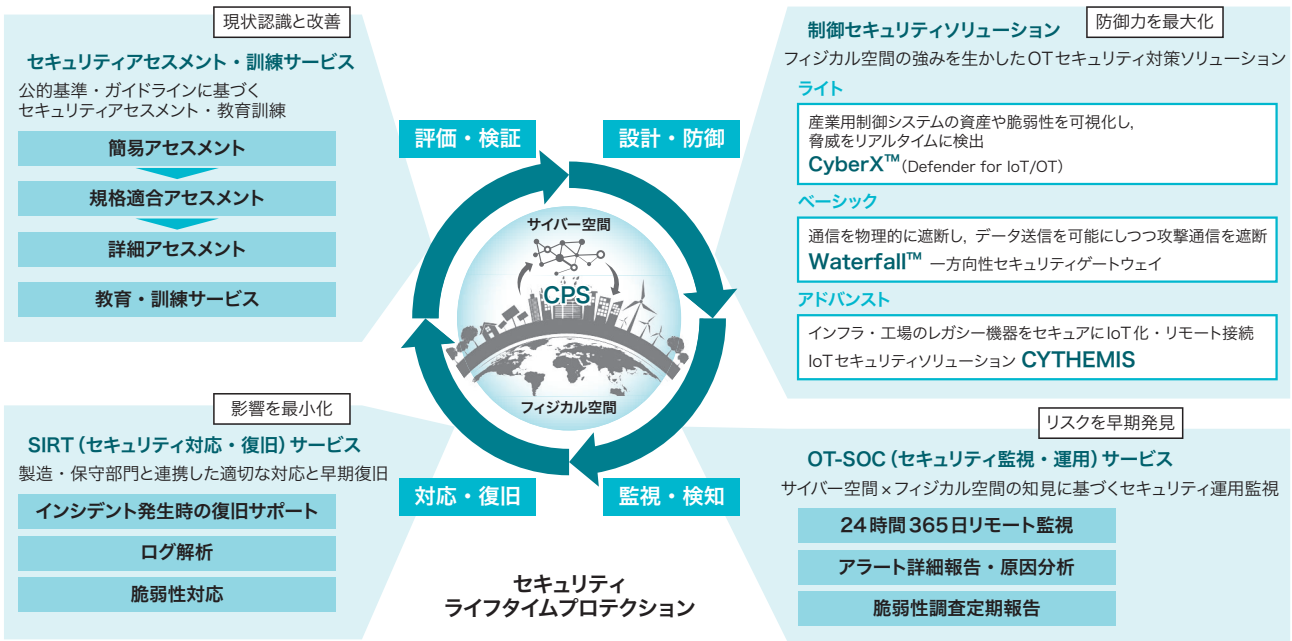
これらのうち，特にインシデントの影響を最小化するための早期検知・対処，そして早期回復するための自動化を実現する“セキュリティ運用”が重要な鍵となる。

東芝グループでは，このセキュリティ運用を持続的に回していくために，“セキュリティライフタイムプロテクション”のビジョンを掲げ，自社システムや工場などの生産システム，及び顧客に提供する社会インフラ・産業分野のCPSを対象に，技術開発や実践を行っている。セキュリティライフタイムプロテクションでは，これまでのシステムの設計・防御の対策だけでなく，システム運用中の監視・検知，インシデント発生時の対応・復旧，そしてアセスメントや脆弱性の評価・検証を行い，新たなシステム設計・防御にフィードバックすることで，レジリエンスの能力と成熟度の持続的な向上を目指すビジョンである。東芝グループは，長年培ってきた制御システムの開発・保守運用の技術ノウハウと，東芝グループ12万人のIT（情報技術）インフラのセキュリティ運用の実績を基に，制御システム運用とセキュリティ運用を統合した技術の開発と実践に取り組んでいる。更に，これら実践において開発した技術や得られたノウハウを，セキュリティサービス・ソリューションとして提供している（**図2**）。CPSの開発から顧客の環境での運用まで一貫したセキュリティ支援を行うことで，CPSのサイバーレジリエンス向上を目指している。

3. CPSを支えるサイバーセキュリティサービス・技術

3.1 セキュリティサービス

東芝グループのセキュリティ運用サービスを進化・高度化するための技術開発について，以下に述べる。



OT：Operational Technology　SOC：Security Operation Center

図2. 東芝グループのセキュリティライフプロテクションのコンセプトとCPSを支えるサイバーセキュリティサービス・ソリューション
評価・検証，設計・防御，監視・検知，対応・復旧のサイクルで，CPSのサイバーレジリエンスを支え，持続的なセキュリティを提供する。
Toshiba Group's “Security Lifetime Protection” concept and cybersecurity services and solutions supporting CPS

(1)　制御システム向けセキュリティ監視サービスの提供を可能にする不正アクセス検知技術　　情報システム向けに提供してきたセキュリティ監視サービスを制御システム向けに展開するために，情報システム向けのIDS（Intrusion Detection System：不正侵入検知システム）を応用し，制御システムの不正アクセスなどを検知するための技術を開発した（この特集のp.7–10参照）。

(2)　制御システム向けセキュリティ監視サービスの高度化　　制御システムのセキュリティ監視において課題となっている偽陽性アラートを絞り込むために，監視対象であるセキュリティセンサーから発せられたアラートの原因分析とリスク判定の精度を高める監視技術を開発し，この技術を検証するため，発電・変電システムのシミュレーターを用いた検証環境を構築した（同p.11–14参照）。

3.2　セキュリティソリューション

制御システムを中心とした，CPSのセキュリティソリューションの技術開発について，以下に述べる。

(1)　グローバルな脅威に対応した管理・運用を実現する制御システム向け統合セキュリティ管理ソリューション　　各国で整備が進むガイドラインや最前線で実績を重ねる対策技術などの動向を踏まえ，制御システム向けの資産・脅威の可視化と異常検知のソリューションや，物理的な一方向通信を用いた境界防御のソリューションを採用し，国内の制御システムやその運用環境に適応したセキュリティ管理・運用を実現した（同p.15–18参照）。

(2)　ユーザー，デバイス，データを認証するセキュリティソリューション　　長年のICカードや周辺システムの開発で培った認証・暗号化・鍵管理技術をベースに，ユーザー，デバイス，プログラム（データ）の認証やセキュリティを強化するソリューションとして，BISCADE，CYTHEMIS，AKTEGRISを開発した。これにより，多要素認証や，セキュリティ対策が難しいレガシー機器のネットワーク化，機器SW更新時の正当性の確保などを実現した（同p.19–23参照）。

(3)　コンテナ型仮想化技術のセキュリティリスクに対応した許可リスト型実行制御ソリューションWhiteEgret　　制御システムのセキュリティ対策として開発した長期的安定運用が容易なWhiteEgretをDocker™に対応させた。柔軟なプログラム更新など，コンテナ型仮想化技術の特長を生かしながら，コンテナ上でのマルウェア実行を防止し，CPSの長期安定運用を実現した（同p.24–28参照）。

3.3　セキュリティコンサルティング

制御システムやCPS向けに取り組んでいるセキュリティコンサルティングサービスの方法論・技術開発の取り組みと実践について，以下に述べる。

(1)　CPSのセキュリティを担保するリスクアセスメント手法　　CPSを提供する事業者は，システム及びサービスのライフサイクル全体を通したリスクマネジメントが社会的責務となっている。東芝グループは，リスクの特定，分析，及び評価を行うリスクアセスメントの手法とツールを開発し，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ように支援できる手法を実現した（同p.29–33参照）。

(2)　セキュリティの脆弱性評価技術とサイバー攻撃エミュレーション技術　　セキュリティリスクを正しく評価するため，対象の制御システムに実際に攻撃を行い，その影響度や攻撃難易度などを評価する，サイバー攻撃耐性評価の自動化技術の開発に取り組んでいる。今回，東芝グループの複合機（MFP）サービスをモチーフに，専門家が評価を実践してセキュリティ対策の有効性を検証するとともに，評価の自動化について考察を行った（同p.34–37参照）。

3.4　セキュリティ基盤技術

更なるDX（デジタルトランスフォーメーション）進化による産業データの利活用や，量子計算機の出現による暗号危殆（きたい）化に対して，先行的に取り組んでいる基盤技術開発について，以下に述べる。

(1)　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　　CPSの開発・運用アーキテクチャーを定めた“Toshiba IoT Reference Architecture（TIRA）”では，セキュリティ標準規格である米国国立標準技術研究所（NIST）のFramework for Improving Critical Infrastructure Cybersecurity（CSF）[2]や経済産業省の「サイバー・フィジカル・セキュリティ対策フレームワーク」[3]に準拠したセキュリティアセスメントと対策を実施している。しかし，産業分野ごとに準拠すべき基準が異なることから，今回，エネルギー分野をモチーフに，標準規格と業界基準で共通の評価プロファイルを開発した。これにより，各業界基準に基づいた顧客とのリスクコミュニケーションが可能となった（同p.38–41参照）。

(2)　セキュアなデータサービスを支えるデータ管理プラットフォーム　　フィジカル空間で得られたデータを利活用して新たな付加価値を創造するデータサービスでは，国や，地域，事業分野などによって，異なる法令や規

制を遵守したデータの管理・利活用が必要である。今回，データ管理を担うプラットフォームのセキュリティ要件と参照モデルを定め，それらに基づいた，先端医療向けデータサービスの一部機能を試作し，動作を確認した（同p.42–46参照）。

⑶　量子計算機でも破れない耐量子セキュリティ技術

量子計算機の出現により，暗号技術の危殆化が始まっている。そこで，高度な機密性を持つデータの安全な送信を可能とする量子鍵配送（QKD）と，ローエンドデバイスにも搭載可能で軽量な耐量子計算機暗号（PQC）を開発した。これらを駆使して，耐量子計算機からローエンドデバイスまでを含め，トータルなセキュリティを担保するための技術開発を進めている（同p.47–51参照）。

4. 今後の展望

今後，CPSの更なる進化により，オフィスから工場，社会インフラまで様々なものがクラウドシステムにつながり，業務システムなどの情報システムだけでなく，社会インフラや産業に関わる開発環境や生産・運用システム，更には制御システムの一部もクラウドシステムにシフトして，クラウドシステム（サイバー）からフィジカル空間を制御する世界がやってくると予想される。その際，これまでの境界型の防御は限界となり，境界レスでセキュリティを実現する“ゼロトラストアーキテクチャー”[4]の導入が必須となるであろう。実際に米国では，石油パイプラインのインシデントをきっかけに，ゼロトラストアーキテクチャーの導入を求める大統領令[5]が発令され，連邦政府サイバーセキュリティ強化を加速させている。

また，社会インフラ・産業分野でもゼロトラストアーキテクチャーの導入が進むと考えられるが，ネットワークにつながるあらゆるものを認証・監視するゼロトラストアーキテクチャーでは，セキュリティ運用の自動化・高度化が必須となる。これらの課題に対しても，早期に取り組み実践することで，社会インフラ・産業分野のCPSの進化を支える新たなセキュリティサービス・技術を創出していく。

文　献

⑴ 東芝．サイバーセキュリティ報告書 2021．東芝，2021，40p．<https://www.global.toshiba/content/dam/toshiba/jp/cybersecurity/corporate/report/pdf/CyberSecurityReport2021.pdf>，（参照 2022-02-04）．

⑵ NIST. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1, NIST, 2018, 54p.

⑶ 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，経済産業省，2019，261p.

⑷ Rose, S. et al. NIST Special Publication 800-207 Zero Trust Architecture. NIST, 2020, 57p.

⑸ Biden, J. R. "Executive Order on Improving the Nation's Cybersecurity". The White House. <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>, (accessed 2022-02-04).

・CyberXは，CYBERX ISRAEL LTD.の商標。

・Waterfallは，Waterfall Security Solutions Ltd.の商標。

・Dockerは，Docker, Inc.の商標。

天野　　隆　AMANO Takashi
技術企画部
サイバーセキュリティセンター
電子情報通信学会会員
Cyber Security Center

岡田　光司　OKADA Koji, D.Eng.
研究開発センター
サイバーセキュリティ技術センター
博士（工学）　電子情報通信学会会員
Cyber Security Technology Center