トレンド

デジタル化で進化する社会のサイバーレジリエンスを強化するセキュリティ技術

Security Technologies for Enhancing Cyber Resilience of Society amidst Progress of DX

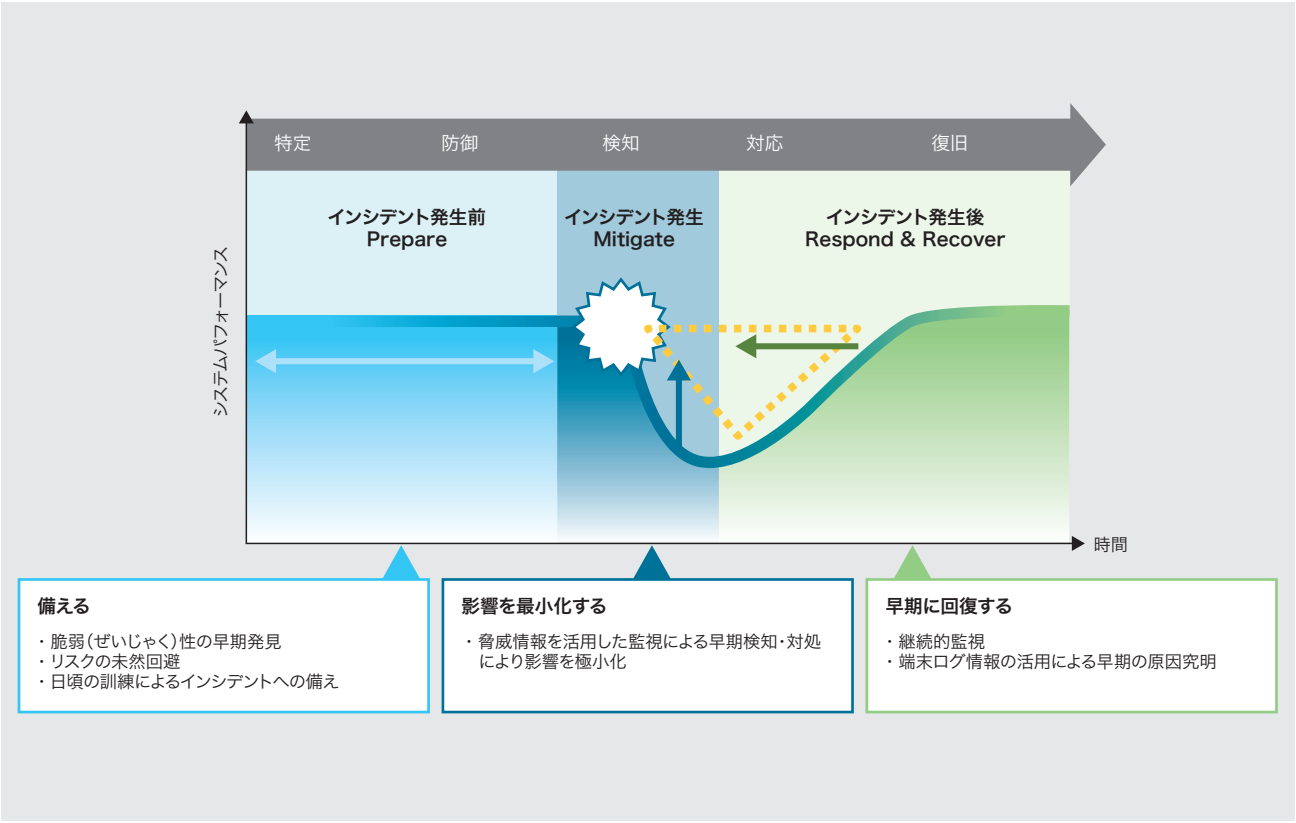
岡田　光司 OKADA Koji　　下田　秀一 SHIMODA Shuichi

社会インフラや製造業のデジタル化により，サイバーとフィジカルが融合するサイバーフィジカルシステム（CPS）の構築が進んでいる。一方で，様々なシステムがつながることで新たなサイバーセキュリティリスクが増加し，社会インフラや製造業へのサイバー攻撃が激化している。更に，量子時代に向けた技術革新が進む中，それに伴う新たなセキュリティリスクへの備えも大きな社会課題となっている。

東芝グループは，カーボンニュートラル・サーキュラーエコノミーに向けた，つながるデータ社会を見据え，レジリエントな社会を実現するためのセキュリティ技術の開発と実践に取り組んでいる。

Cyber-physical systems (CPS) that fuse cyberspace and physical space technologies at a high level have been introduced with the expansion of digital transformation (DX) in production facilities and the social infrastructure field. On the other hand, the connection of various systems via the network has recently been accompanied by higher cybersecurity risks of such CPS systems, leading to the intensification of cyberattacks. Furthermore, demand has also been increasing for new security measures accompanying the technological innovations in the field of quantum computers.

The Toshiba Group has been taking the initiative in developing and implementing necessary security measures to enhance cyber resilience of a connected society through the use of safe and secure data so as to help realize carbon neutrality and a circular economy.



特集の概要図．サイバーレジリエンスのコンセプト

Cyber resilience and security incident response processes

1. 社会インフラや製造業を取り巻くサイバーセキュリティの動向

近年，社会インフラや製造業のサプライチェーンを標的としたランサムウェア（身の代金要求型ウイルス）によるサイバー攻撃が急増している。2010年にイランの核施設を狙ったスタックスネットをはじめ，旧来の社会インフラへの攻撃は政治的な目的が主であった。しかし，2010年代後半からはランサムウェアによる経済目的のサイバー攻撃が急増し，現在ではその多くが社会インフラや製造業を標的にしているといわれている。その要因の一つとして，社会インフラや製造業は，サイバー攻撃によりその稼働が阻害されることで，社会生活への影響や多額の事業損失が生じるなど被害の影響が非常に大きいことが挙げられる。特に，近年のデジタル化の進展によって社会インフラや製造業の調達から製造，販売，そして運用までのサプライチェーンがつながることで，一部の企業への攻撃がサプライチェーン全体に影響し，被害が拡大する。しかし，多くの企業や拠点が複雑に関わるサプライチェーンでは，企業や拠点ごとのセキュリティレベルが異なるため，サプライチェーン全体のセキュリティ対策を強化することが難しく，攻撃者の格好のターゲットになっている。

このように，デジタル化により社会インフラや製造業が進化する一方で，AIをはじめとしたデジタル技術の活用によりサイバー攻撃も巧妙さを増しており，企業や社会全体のリスクが高まっている。これに対応するため，各国がサイバーセキュリティ規制を強化する動きがある。特に，社会インフラの中でも電力や石油・ガス，電気通信などの重要インフラの保護は国家の安全保障に関わる重要課題と認識され，規制が強化されている。欧州連合（EU）のNetwork and Information Systems Directive 2（NIS2）[(1)]は，サイバー攻撃に対するEU全体の耐性を向上させることを目的としている。エネルギーや，運輸，上下水道などの重要インフラ分野を対象として，罰則の強化とインシデント発生時の報告義務が課されている。NIS2は，企業が包括的なサイバーセキュリティリスク管理策を実施し，経営陣がその責任を負うことを求めている。一方国内でも，2024年5月に施行された経済安全保障推進法[(2)]で，基幹インフラ事業の事業者（特定社会基盤事業者）が特定重要設備の導入・維持管理などの委託をしようとする際に，事前に届け出を行い，審査を受けることが，定められた。また，サイバーセキュリティ経営ガイドラインVer 3.0[(3)]には，自社へのリスク波及と他社の2次被害を防ぐ観点から，サプライチェーン全体での対策を経営者に求める旨が，新たに記載された。

更に，社会インフラに限らず，デジタル製品に対するセキュリティ規制も強化されてきた。EUで2024年12月に発効されたサイバーレジリエンス法（CRA）[(4)]は，EU域内に上市するデジタル要素を含む製品のセキュリティ強化を目的としている。ほかのデバイスやネットワークに直接又は間接的に接続される（有線・無線を含む）製品の製造業者と小売業者に対して，サイバーセキュリティ要件の適用が2027年12月から義務付けられる。国内でも，IoT（Internet of Things）製品のセキュリティ向上のために，2024年8月に経済産業省が公表した「IoT製品に対するセキュリティ適合性評価制度構築方針」[(5)]に基づき，IoT製品の「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」[(6)]が2025年3月に始まった。この制度は，IoT製品のセキュリティ機能を評価し，適合基準に基づいて「★1（レベル1）」から「★4（レベル4）」までの適合ラベルを付与することで，製品のセキュリティ対策を可視化することを目的としている。適合ラベルは，製品が最低限のセキュリティ要件を満たすことを示しており，調達者や消費者は製品のセキュリティ情報を取得できる。

東芝グループは，このような状況を踏まえ，社会インフラシステムやデジタル製品を提供する製造業として，サイバーセキュリティに関する様々な施策や研究開発に取り組んでいる[(7)]。特に，サイバー攻撃によるインシデントの発生を前提としたサイバーレジリエンスの向上を方針に据えて，サイバーセキュリティ対策を進めている。東芝グループは，サイバーレジリンスを“インシデントに備え，影響を最小化し，早期に回復する能力”と定義し，その能力と成熟度の向上を図っている（**特集の概要図**）。対象システムのシステムパフォーマンスを最大化するために，そのシステム能力が毀損している時間（黄色の三角形の面積）を最小化することを目的として，インシデント発生前にインシデントの発生を抑える取り組みに加え，インシデントが発生した場合もその影響を最小化して，早期に回復する取り組みが重要である。

2. 制御システムのセキュリティ強化の取り組み

近年の社会インフラや製造業へのサイバー攻撃に対し，そのOT（制御・運用技術）システムのサイバーレジリエンス強化は喫緊の課題である。これまで業務系IT（情報技術）システムとOTシステムを分離・防御することで対策してきたが，デジタル化の進展により，遠隔での保守・制御や，稼働データを収集・分析して稼働を最適化する取り組みが進むことで，もはやその垣根はなくなりつつある。しかし，長期稼働が求められるOTシステムではレガシー機器や独自プロトコルが多く用いられており，直接的な対策が難しい。そ

のため，OTシステムの状態を常に可視化・監視して，これまで想定していなかったセキュリティインシデントが発生した際に，人的対応も含めていかに早く稼働を復旧するかという，正にサイバーレジリエンスの向上が求められている。その中でも，OTシステムに用いられるソフトウェアの脆弱（ぜいじゃく）性は，攻撃者の格好の標的となることから，脆弱性の管理が最重要課題であり，1章に記載したCRAでもSBOM（Software Bill of Materials）の管理と提出が求められている。このような状況に対し，東芝グループは，OTシステムのセキュリティ強化に向けた技術開発を進めている。

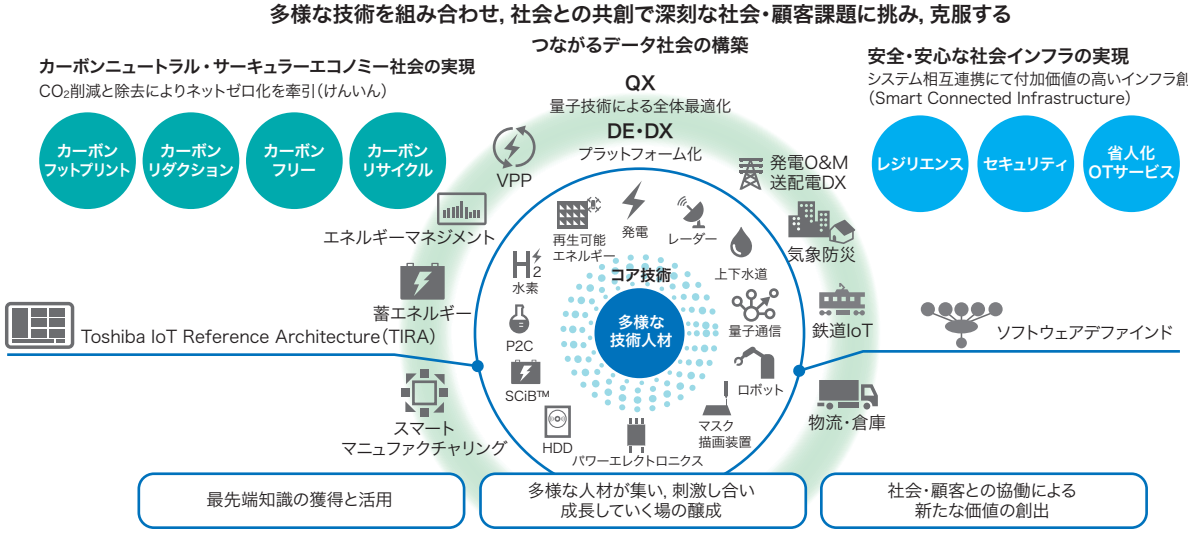
まず，東芝グループのOTシステムに関する高度な制御技術と豊富な運用実績を基に，OTシステムのリスクアセスメントからセキュリティソリューションの導入・運用に至るまで，ライフサイクル全体を通じたセキュリティ対策を体系的にワンストップで提供できる統合コンサルティングプロセス手法を開発した。この手法では，レガシー機器や独自プラットフォームの利用や，システムの可用性や安全性の確保といったOTシステム固有の制約も考慮しており，顧客のシステムに合わせて最適化した持続可能なOTシステムセキュリティを提供できる（この特集のp.11–15参照）。

また，インシデントが発生しても早期に検知して復旧可能な顧客システムの運用を目指し，OTシステム向けセキュリティ訓練システムを開発した。これは，OTシステムのシミュレーターを用いたロールプレイング方式で，訓練や，教育へ取り入れて実践演習ができるものである。サービス妨害攻撃やランサムウェアなどのサイバー攻撃が起こった際に，システムの操作や通信データ・ログの解析を行い，組織的に連携して対応することを模擬して，攻撃の検知・分析から，対応，システムの復旧までをリアルに体験できる（同p.16–19参照）。

更に，前述のCRAでも対応が求められているSBOMの管理と脆弱性への対応（脆弱性ハンドリング）についても，東芝グループで取り組みを進めている。様々かつ大規模なシステムを取り扱う東芝グループでは管理の効率化が必須であることから，SBOMと脆弱性情報の照合結果に基づいて迅速かつ確実に脆弱性に対応するためのPSIRT（Product Security Incident Response Team）支援システムを導入した。脆弱性が対象製品で悪用可能かどうかを判定するスクリーニング技術や，製品のセキュリティ対策に基づいてリスクを評価する環境評価技術を開発し，東芝グループ内での実践を通じて脆弱性ハンドリングの更なる効率化に取り組んでいる（同p.20–23参照）。

3. 社会インフラのデジタルトランスフォーメーションに向けたセキュリティ対策

東芝グループは，カーボンニュートラル・サーキュラーエコノミーと，安全・安心な社会インフラの実現を目指し，社会インフラシステムのデジタルエボリューション（DE：Digital Evolution），デジタルトランスフォーメーション（DX：Digital Transformation），及びクオンタムトランスフォー



CO_2：二酸化炭素　VPP：バーチャルパワープラント　O&M：運用・メンテナンス　P2C：Power to Chemicals　SCiB™：東芝リチウムイオン二次電池
HDD：ハードディスクドライブ

図1. 技術・イノベーションビジョン
カーボンニュートラル・サーキュラーエコノミーと，安全・安心な社会インフラの実現を目指して，様々な社会課題解決に向けた研究開発を行っている。
Technology and innovation visions

メーション（QX：Quantum Transformation）による，更なる進化に向けた技術開発に取り組んでいる（**図1**）。

このような社会インフラのデジタル化の進展，そしてつながるデータ社会の実現により，カーボンニュートラルやインフラ運用の最適化など，様々な社会課題の解決が期待される一方で，サイバーとフィジカルが融合した様々なシステムがつながることで，サイバー攻撃のリスクが増すことは避けられない。そのため，それらの新たなリスクに対して常にレジリエントなサイバーセキュリティ対策を実現していくことが，社会インフラを進化させる東芝グループとして必須の取り組みである。

東芝グループは，これまで信頼性の高いハードウェア製品を数々開発してきたが，その機能をソフトウェアデファインド化してクラウドシフトすることで，遠隔での制御や機能のアップデートなど，新たな価値を創出するCPSの構築を進めている。その一方で，クラウドシステムや通信路へのサイバー攻撃に対しても，社会インフラの稼働を最優先に考えたレジリエントなサイバーセキュリティ対策が必要となる。

東芝グループは，産業用コントローラーとして用いるPLC（Programmable Logic Controller）をクラウドシステム上に実装することで，顧客のリモート作業や外部サービス連携を可能とする計装クラウドサービスを提供し，製造現場への適用を進めている。このサービスでは，制御データをインターネット経由で共有するため，従来のシステム構成とはセキュリティ要件が大きく異なることから，脅威分析結果とゼロトラストアーキテクチャーに基づいたセキュリティ対策を実施している（この特集のp.24–28参照）。

また，エレベーターの制御にもソフトウェアデファインド技術を適用し，ELCLOUD（エルクラウド）サービスの提供を開始した。ELCLOUDには，警備・清掃・搬送などを行うロボットと連携する“ロボット連携サービス”，利用者のスマートフォンからエレベーターを呼び出す“スマホ呼びサービス”，及びビル管理会社向けの“管理支援サービス”がある。昇降機は利用者の安全・安心を最優先とする社会インフラシステムであるため，サイバー攻撃によって運行に影響を与えないセキュリティ設計・実装を実現した（同p.29–32参照）。

更に，社会インフラの様々なシステムがつながり，産業データが連携・流通することで，サプライチェーン・バリューチェーン全体でのシステム稼働の最適化による新たな価値の創出や，環境負荷を低減するためのサーキュラーエコノミーの加速が期待されている。現在，サプライチェーンでのカーボンフットプリントのデータ連携や，資源や素材のサーキュラーエコノミーに向けたデジタルプロダクトパスポート（DPP）などの製品情報を連携・公開する取り組みが進んでいる。しかし，連携先の事業者から入手するデータが本当に正しいのか，その信頼性（トラスト）を確認・確保する仕組みが世界的にもまだ確立されておらず，東芝グループは，その仕組み作りにいち早く取り組んでいる。

具体的には，東芝グループも参画する日本とドイツの産業団体が連携し，事業者間でデータの授受を行う際にトラスト関係を構築するための仕組みを開発し，現在，国際標準への提案を進めている。更に，この仕組みをベースに，不特定多数の事業者間でデータ共有をするためのトラストフレームワークの構築と，実現に向けたルール作りと技術開発に取り組んでいる（同p.33–36参照）。

4. 安全・安心な量子社会の実現

近い将来，量子計算機が実用化されることで，複雑な社会問題の解決や社会全体の最適化が期待される。一方で，これまでセキュアな通信やデータ保護に用いられてきた公開鍵暗号が量子計算機により解かれてしまうこと（暗号の危殆（きたい）化）が大きな社会問題となっている。東芝グループは，量子暗号通信と耐量子計算機暗号（PQC）をハイブリッドに組み合わせた，量子計算機に対しても安全な情報通信システムの実現を目指している。

量子暗号通信は，既に世界各国で高機密ネットワークの社会実装が進んでおり，東芝グループも様々なパートナーと社会実証を進めている。今後高機密ネットワークの運用が始まると，各鍵管理拠点での運用コストが課題となることから，その対策技術の開発に取り組んでいる。また，量子暗号通信のネットワークが拡大するとユーザーや拠点間の認証が必要となることから，このネットワークの認証にPQCを導入したハイブリッドシステムを開発した。今後も，量子暗号通信とPQCの組み合わせ，又は使い分けにより，量子計算機実用化以降のセキュアネットワークを実現する（この特集のp.37–41参照）。

5. 今後の展望

東芝グループは，社会インフラのDEから，データ社会の実現に向けたDX，そして量子社会を実現するQXを目指している。それらの技術と社会システムの進化に伴って新たなセキュリティリスクが出現しても，常に安全・安心かつレジリエントな社会インフラを実現することを目指し，今後も新たなセキュリティ技術の開発とサイバーセキュリティの取り組みを，顧客及び社会とともに進めていく。

文　献

(1) Directive (EU) 2022/2555 of the European Parliament and of the Council. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>, (accessed 2025-04-18).
(2) 内閣府. “経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（経済安全保障推進法）”. <https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/suishinhou.html>, (参照 2025-04-18).
(3) 経済産業省，情報処理推進機構. サイバーセキュリティ経営ガイドラインVer 3.0. 2023, 53p. <https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf>, (参照 2025-04-18).
(4) Regulation (EU) 2024/2847 of the European Parliament and of the Council. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847&qid=1733552498245>, (accessed 2025-04-18).
(5) 経済産業省. IoT製品に対するセキュリティ適合性評価制度構築方針. 2024, 26p. <https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/pdf/20240823_1.pdf>, （参照 2025-04-18）.
(6) 情報処理推進機構. “セキュリティ要件適合評価及びラベリング制度（JC-STAR）”. 情報セキュリティ. <https://www.ipa.go.jp/security/jc-star/index.html>, （参照 2025-04-18）.
(7) 東芝. サイバーセキュリティ報告書2025. 2025, 26p. <https://www.global.toshiba/content/dam/toshiba/jp/cybersecurity/corporate/report/pdf/CyberSecurityReport2025_A3_rev02.pdf>, （参照 2025-07-09）.

岡田　光司　OKADA Koji, D.Eng.
総合研究所 AIデジタルR&Dセンター
博士（工学）
電子情報通信学会会員
AI Digital R&D Center

下田　秀一　SHIMODA Shuichi
技術企画部 サイバーセキュリティセンター
Cyber Security Center