トレンド

東芝のサイバーセキュリティー強化への取り組み

Toshiba's Approach to Strengthening of Cybersecurity

天野　隆 AMANO Takashi

デジタルトランスフォーメーションの急速な進展を背景に，あらゆるモノがネットワークにつながり，社会環境やビジネスに変化が起こりつつある。これに伴い，サイバー攻撃による脅威が，情報システムだけでなく，製品と，それに付随するシステムやサービスにまで広がり，社会インフラや製造設備が物理的な被害に遭うリスクが増大している。これに対し，国内外でサイバーセキュリティーへの関心が高まり，新たな規制やガイドラインの制定が進められている。

東芝グループは，企業としてのセキュリティー体制を強化し，製品などの運用段階まで含めたセキュリティー対応や，サプライヤーなどのサプライチェーンネットワークを含めたセキュリティー対策を進めている。

With billions of devices now connected to the Internet due to the rapid progress of digital transformation, social and business environments are changing. At the same time, the danger of cyberattacks is increasing, exposing not only information systems but also all connected products and services to a new level of threats. This is also increasing the risk of physical damage to social infrastructure and manufacturing facilities. New regulations and guidelines are consequently being established both in Japan and abroad.

The Toshiba Group is further strengthening its security systems in response to this situation. As part of these efforts, we are expanding the focus of security to include the design and manufacturing stages taking the operation of products into consideration, and are collaborating with suppliers to enhance the security of supply chain networks.

特集の概要図．デジタルトランスフォーメーションを支えるセキュリティー技術
Security technologies to support digital transformation

1. はじめに

IoT（Internet of Things）技術を活用したデジタルトランスフォーメーション(注1)の進展を背景に，様々なモノがネットワークにつながりつつある。これに伴い，サイバー攻撃の脅威が情報システムだけでなく製品，システムやサービスにも広がり，社会インフラが物理的な被害に遭うリスクが増大している。世界各国から多くの人々が集まるイベントを狙ったサイバー攻撃なども懸念される中，企業には自社内外のシステムや自社製品のセーフティーとセキュリティーに関するリスク評価を厳密に行って未然に様々なリスクに備え，インシデント発生時には迅速に対応することが求められている。

サイバー攻撃の内容も進化，多様化しており，2015年と2016年には，海外の重要インフラシステムの制御系がサイバー攻撃を受け，大規模停電が発生するなどのインシデントが発生した。また，2017年には，OS（基本ソフトウェア）の脆弱（ぜいじゃく）性を狙ったランサムウェアへの感染が，サプライチェーン経由で世界各国の企業に広がり，結果的に少なくとも150か国で関連インシデントが発生した。

このように脅威を増すサイバー攻撃に対し，デジタルトランスフォーメーションを進める企業は，どのような考えの下に，どのように取り組んでいくか，その方法論の策定が求められている。

2. 海外の動向

米国は，2017年に，防衛調達に参加する全ての企業に対して，セキュリティー対策としてNIST（米国国立標準技術研究所）のSP800-171の遵守を義務化し，2018年には，NISTが策定したガイドラインである「サイバーセキュリティフレームワーク(1)」に，サイバーサプライチェーンリスクマネジメントを追加している。

欧州では，2016年に，エネルギーなどの重要インフラ事業者に対して，NIS（Network and Information Security）指令に沿ったセキュリティー対策を義務化し，2017年には，単一のサイバーセキュリティー市場を目指して，ネットワークにつながる機器の認証フレームワークの導入検討を発表した。また，2018年から，EU（欧州連合）の顧客データを扱う企業に，データ処理制限などを新たに義務付けるGDPR（General Data Protection Regulation）の運用を開始し，ドイツではルーターのセキュリティーに関するテクニカルガイドラインの策定を進めている。

このように，世界中でサイバーセキュリティーに対する関心が高まっており，グローバルなサプライチェーンの中で信用を得るには，サイバーセキュリティー対策に注力する必要がある。

3. 我が国の取り組み

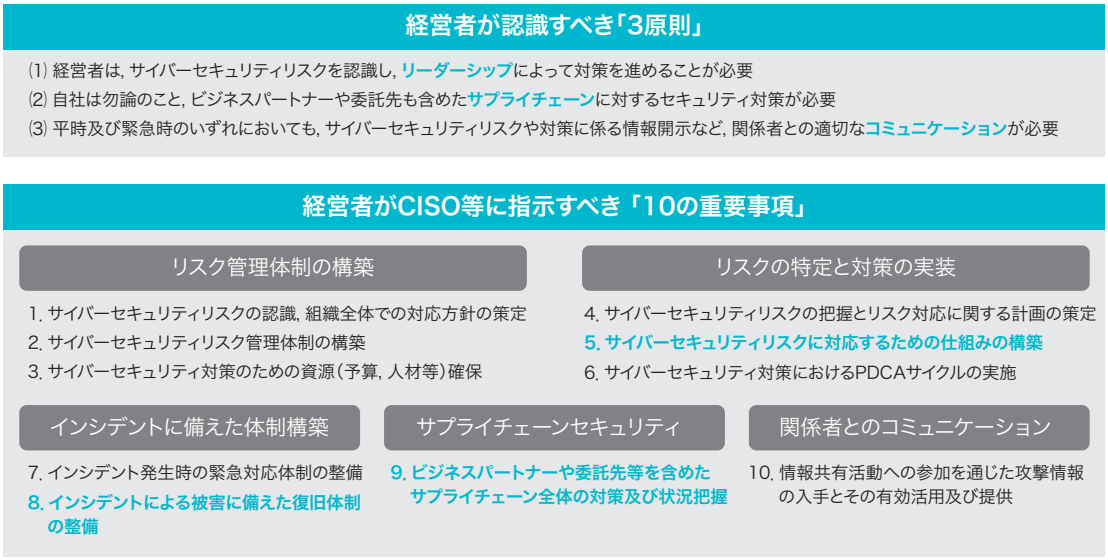
2014年11月，我が国において「サイバーセキュリティ基本法(2)」が制定された。同法は，サイバーセキュリティーという概念を法的に定義し，国や地方公共団体といった関係者の責務を明確化するとともに，「サイバーセキュリティ戦略本部」をサイバーセキュリティー政策に係る政府の司令塔と位置付け，国の行政機関に対する勧告権などの権限を付与した。「内閣サイバーセキュリティセンター（NISC）」では，同法の規定に基づき，「サイバーセキュリティ戦略(3)」を定めている。

サイバーセキュリティ戦略は，2020年代初頭までの将来を見据えつつ，基本的な施策の方向性を示すものである。そして，「本戦略の中で，サイバー空間に対する我が国の方針を内外に明確化するとともに，本戦略の実践により，積極的に「自由，公正かつ安全なサイバー空間」の創出に努め，「経済社会の活力の向上及び持続的発展」，「国民が安全で安心して暮らせる社会の実現」，「国際社会の平和・安定と我が国の安全保障」に寄与する。」としている。

経済産業省は，企業のサイバーセキュリティー対策を推進するため，独立行政法人 情報処理推進機構（IPA）とともに，サイバーセキュリティ基本法及びサイバーセキュリティ戦略に基づき，「サイバーセキュリティ経営ガイドライン(4)」を策定した。これは，大企業，及び小規模事業者を除く中小企業のうち，IT（情報技術）に関するシステムやサービスなどを供給する企業，及び経営戦略上ITの利活用が不可欠である企業の経営者を対象に，特に経営者のリーダーシップを求める内容となっている。サイバー攻撃から企業を守る観点で，経営者が認識する必要のある「3原則」，及び経営者が情報セキュリティー対策を実施する上での責任者となる担当幹部（CISO（最高情報セキュリティ責任者）など）に指示すべき「重要10項目」をまとめている（**図1**）。

サイバーセキュリティ基本法の下，経済産業省と総務省は，IoTを活用した革新的なビジネスモデルを創出していくとともに，国民が安全で安心して暮らせる社会を実現するために，必要な取り組みなどについて検討を行うことを目的として，「IoT推進コンソーシアム IoTセキュリティワーキンググルー

（注1） スウェーデン・ウメオ大学のエリック・ストルターマン教授が，2004年に提唱した「ITの浸透が，人々の生活をあらゆる面でより良い方向に変化させる」という概念。



経済産業省，IPA「サイバーセキュリティ経営ガイドライン」[4]を基に作成

図1. サイバーセキュリティ経営ガイドラインの概要
企業がサイバーセキュリティーを推進するために，経営者のリーダーシップが不可欠である。
Overview of cybersecurity management guidelines

プ」を開催してきた。同ワーキンググループは，2016年に「IoTセキュリティガイドライン ver 1.0[5]」を策定した。

このガイドラインは，IoT 機器やシステム，サービスの供給者及び利用者を対象として，適切なサイバーセキュリティー対策を検討するための考え方を，分野を特定せずにまとめたものである。供給者及び利用者は，サイバー攻撃などによる新たなリスクが，モノやその利用者の安全，及び個人情報・技術情報などの重要情報の保護に影響を与える可能性があることを認識した上で，IoT機器や，システム，サービスに対して，リスクに応じた対策を講じる必要がある。このガイドラインを活用することにより，IoT 機器や，システム，サービスの供給者や利用者が，自己の役割を認識しつつ，分野ごとの性質に応じたセキュリティー確保の取り組みを促進することを期待したものである。

4. 東芝の取り組み

東芝は，サイバーセキュリティー体制の強化を目的として，2017年に“サイバーセキュリティセンター”を設立した。CISOのリーダーシップの下，情報セキュリティーと製品セキュリティーの機能を統合した実行体制をスタートし，「東芝グループサイバーセキュリティマニフェスト」を策定した。

東芝グループサイバーセキュリティマニフェストでは，サイバーセキュリティー体制強化において東芝グループが目指すゴールを，(1)ガバナンス，(2)防御，(3)監視・検知，(4)対応・復旧，及び(5)人財の五つの視点で定めた。

(1) ガバナンス　　サイバーセキュリティーマネジメントのPDCA（Plan-Do-Check-Act）が回り，常に成熟度が向上している。
(2) 防御　　脆弱性が入り込まない製品，システム，サービスの設計，開発，構築のプロセスが運用できている。
(3) 監視・検知　　東芝グループの製品，システム，サービスに関わる社内外のセキュリティー脅威が，リアルタイムに把握できる。
(4) 対応・復旧　　インシデント発生時に，迅速に被害を局所化し，事業復旧できる。
(5) 人財　　必要なセキュリティー人財が，育成，強化できている。

また，これら五つの視点を有機的に結合し，事業に求められるセキュリティーマネジメントプロセスを定義した（**図2**）。サイバーセキュリティセンターは，東芝グループの各事業においてこのセキュリティーマネジメントプロセスが継続的に運用できるよう，各視点での支援を進めている。具体的には，社外セキュリティー機関との連携，東芝グループのガバナンスコーディネーション，セキュア開発・評価基盤構築，セキュリティー運用監視基盤構築，リスク管理基盤構築，イ

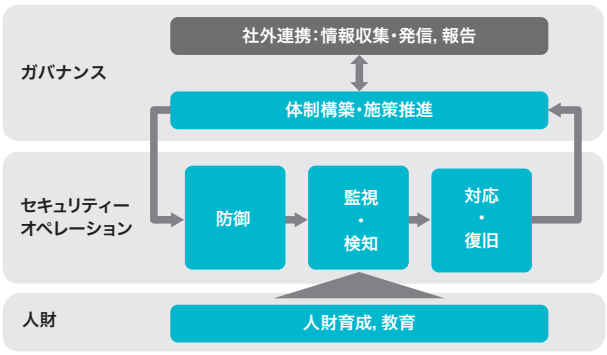


図2. セキュリティーマネジメントプロセス

サイバーセキュリティー体制の強化のために，東芝グループが目指すゴールを五つの視点でマネジメントプロセスとして定めた。

Security management process

ンシデント対応支援，教育プログラム策定と資格認定制度の制定である。

サイバーセキュリティセンターは，CISOの強力なリーダーシップの下，これらの具体的な取り組みを確実に実行して，東芝グループのサイバーセキュリティー体制の強化を推進している。

5. 東芝のセキュリティー技術

特集の概要図は，“セキュリティーライフタイムプロテクション”の概念であり，四つのフェーズから成るサイクルを回すことで，製品，システム，サービスに対するセキュリティーを継続的に維持・強化するものである。

この特集では，ライフタイムの各フェーズに適用した技術を紹介している。

設計・防御フェーズでは，インダストリアルIoTセキュリティーの方法論と製品のセキュリティーライフタイムプロテクション（この特集のp.6–10参照），及びソースコード解析ツールを活用したセキュリティー脆弱性対策の取り組みと，その内容や導入成果（同p.19–22参照）について述べる。

運用・監視フェーズでは，制御システムに求められる長期の安心・安全を実現する，ホワイトリスト型実行制御技術（同p.11–14参照）を紹介する。

インシデント対応・復旧フェーズは，この論文でサイバーセキュリティー体制強化について述べる。

評価・検証，教育フェーズでは，ISASecure® EDSA（Embedded Device Security Assurance）認証を取得したユニファイドコントローラ nvシリーズ type2の特長とEDSA認証に関する内容とその対応について（同p.15–18参照），及び容易にシステム構成を変更でき実システムに近い環境でセキュリティー試験を行える制御システム仮想化テストベッド技術（同p.23–27参照）を紹介する。

6. 今後の展望

デジタルトランスフォーメーションの進展により，製品，システム，サービスは，運用段階でも，日々進化するサイバー攻撃に対する備えを継続しなければならない。製品の出荷後，システムの構築後，及びサービスの開始後にも，それらに関わるセキュリティー脅威の監視・検知が重要になる。また，万が一インシデントが発生した際には，その影響範囲を迅速に局所化し，事業活動を復旧するための体制が必要である。一方，これらを実行する高度専門家の育成や，製品，システム，サービスへの攻撃・侵入の演習などによる対応スキルの向上も，進める必要がある。

デジタルトランスフォーメーションが，パートナー企業やサプライヤーと相互にデータを利活用する段階へ進むと，バリューチェーン全体で同じレベルのセキュリティーの担保を考慮する必要がある。今後は，製品，システム，サービスだけでなく，バリューネットワークでつながる，組織，人，データなども考慮して，サイバーセキュリティーへの対応を強化していく。

文　献

(1) NIST. 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. IPA 翻訳監修. 2014, 41p. <https://www.ipa.go.jp/files/000038957.pdf>, (参照 2018-06-01).
(2) 総務省. サイバーセキュリティ基本法. 国民のための情報セキュリティサイト. <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/legal/11.html>, (参照 2018-06-01).
(3) NISC. サイバーセキュリティ戦略. 2015, 40p. <https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf>, (参照 2018-06-01).
(4) 経済産業省, IPA. サイバーセキュリティ経営ガイドライン Ver 2.0. 2017, 32p. <http://www.meti.go.jp/press/2017/11/20171116003/20171116003-1.pdf>, (参照 2018-06-01).
(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. 2016, 60p. <http://www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf>, (参照 2018-06-01).

天野　　隆　AMANO Takashi
技術・生産統括部 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