TOSHIBA

サイバーセキュリティ報告書

2022

2022年3月31日現在

最高情報セキュリティ責任者（CISO）メッセージ

「つながる世界」に、安心を届けたい

新型コロナウイルス感染症との闘いが長期化し、仕事を含めたすべての生活面で影響が消えずにいます。人々の距離は感染防止のために遠ざけられ、当たり前だったことが制限される日常生活に不自由を感じておられる方も多いことでしょう。一刻も早いコロナ禍の収束を願いながら新型コロナウイルスと折り合いを付けつつ、共存する「ニューノーマル」な社会をめざして在り方を模索しています。

日々の暮らしで大きく進化したのは「デジタル技術を活用したサービス」であるといえるでしょう。SNSを利用した人同士のつながり、店へ出掛けることなく買い物ができるネットショッピングや宅配サービス、自宅でのオンライン授業、テレワーク主体のビジネスなどが当たり前となり、「つながる世界」があらゆる領域に広がっています。見方を変えれば、このような状況はインターネットなどを悪用する犯罪者にとっても好都合といえます。私たちはサイバー空間でのセキュリティを強化し、サイバー犯罪から社会を守らなければなりません。

東芝グループでは、経営理念「人と、地球の、明日のために。」のもと、1875年の創業以来、147年間継続している「ものづくり」で得た知見と経験を活かし、現実世界だけでなく、「つながる世界」にも安心を届けたいと考えております。

本書は、東芝グループが実践するサイバーセキュリティ強化への取り組みをご紹介し、お客さま、株主さま、お取引先さまを含めたすべての方々にご理解いただくことを目的としています。皆さまに安心して東芝製品・サービスをお選びいただけますよう、本書が一助になれば幸いです。

株式会社 東芝
執行役上席常務・CISO

石井 秀明

東芝グループ サイバーセキュリティ マニフェスト

『見えざる脅威から社会を守り抜く』揺るぎなき決意を持って

日常生活は急速にデジタル化が進み、それにともなってサイバー犯罪が蔓延しつつあります。誰もが、ある日突然、大切なものを奪われたり、理不尽な事件に巻き込まれたりする危険にさらされていると言ってもよいでしょう。

東芝グループは暮らしを支える企業として、社会とお客さまに**安全と安心**を提供してまいりました。145年以上の歴史を持つ企業として、豊富な経験と知識を活かした電力供給や公共交通などのインフラサービス、最先端のデジタル技術を利用したデータサービスをお届けすることにより、フィジカルとサイバーの両面から世界の人々の生活・文化に貢献したいと考えています。一方で、こうしたサービスはサイバー犯罪の対象にもなり得るため、セキュリティ強化は最重要課題のひとつです。

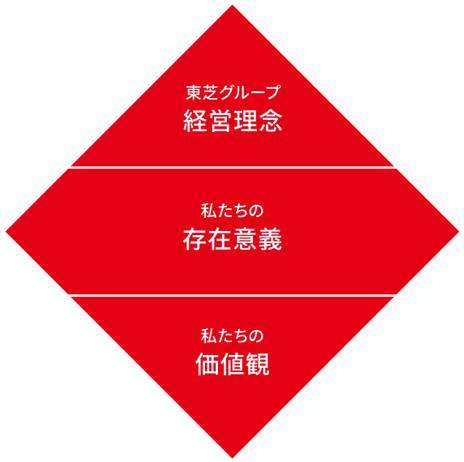
見えざる脅威から社会を守るため、東芝はグループ一丸となって**サイバーセキュリティ体制**を構築し、関連法令の遵守やセキュリティ人材の育成に努めることはもちろん、お客さまへの情報開示に向けて、積極的かつ誠実に取り組んでまいります。

また、事業を通じて得た個人情報を適切に管理し、情報漏えい・不正利用を防止することでお客さまのプライバシー保護を徹底いたします。万が一セキュリティ事故が発生した場合には、その**被害を最小限**に食い止め、原因究明と復旧に最善を尽くします。

『見えざる脅威から社会を守り抜く』、揺るぎなき決意を持って取り組んでまいります。

東芝グループ理念体系

東芝グループ理念体系は、
東芝グループの持続的な成長を支える基盤であり、
すべての企業活動の拠り所となるものです。



「東芝グループ経営理念」、「私たちの存在意義」、
「私たちの価値観」の3つの要素で構成されます。

東芝グループの変わらない信念である
「東芝グループ経営理念」を踏まえ、
東芝グループが社会において果たすべき役割を表した
ものが「私たちの存在意義」であり、
その存在意義を実行するために東芝グループが共有し
大切にするものが、「私たちの価値観」です。

東芝グループ経営理念

人と、地球の、明日のために。

東芝グループは、
人間尊重を基本として、豊かな価値を創造し、
世界の人々の生活・文化に
貢献する企業集団をめざします。

私たちの存在意義

世界をよりよい場所にしたい。
それが私たちの変わらない想いです。

安全で、よりクリーンな世界を。
持続可能で、よりダイナミックな社会を。
快適で、よりワクワクする生活を。

誰も知らない未来の姿。
その可能性を発見し、結果を描き、たどり着くための解を導き出す。
昨日まで想像もできなかった未来を現実のものにする。

私たち東芝グループは、培ってきた発想力と技術力を結集し、
あらゆる今と、その先にあるすべての未来に立ち向かい、
自分自身を、そしてお客様をも奮い立たせます。

新しい未来を始動させる。

それが私たちの存在意義です。

私たちの価値観

誠実であり続ける

日々の活動において、
人や地球に対する責任を自覚し、
つねに誠実な心で行動する。

変革への情熱を抱く

世界をよりよく変えていく熱い情熱を持ち、
そのために必要な変化を
自ら起こす。

未来を思い描く

社会に与える価値や意義を考え、
次の、さらにその先の世代の
ことまで見据える。

ともに生み出す

互いに協力し合い、
信頼されるパートナーとして
ともに成長し、新しい未来を創る。

2022 サイバーセキュリティ報告書
Cyber Security Report

目次

Chapter 1

ビジョン・戦略

東芝グループは、「人と、地球の、明日のために。」という経営理念のもと、一人ひとりの安全安心な暮らしを誰もが享受できるインフラの構築から、社会的・環境的な安定を実現する「繋がるデータ社会の構築」、そして「カーボンニュートラル」「サーキュラーエコノミー」の実現により持続可能な未来をめざしています。その実現に重要な手段が「デジタル」であり、デジタルエコノミーの発展に伴い、今後、様々な企業が産業の垣根を越えて繋がることで、新たな社会価値が創造されると考えています。

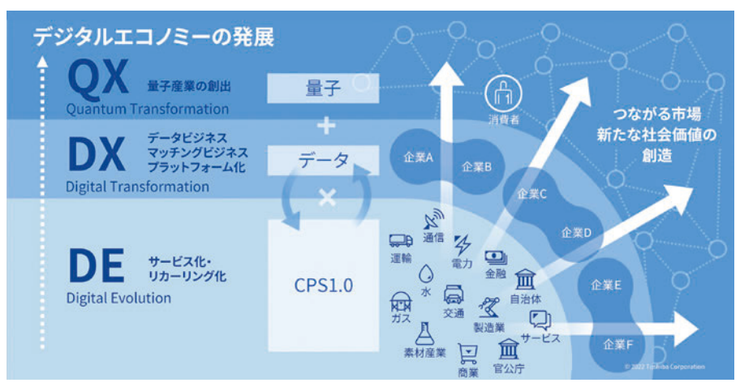
デジタルエコノミーの発展に必要不可欠なのがサイバーレジリエンスです。様々なインフラのデジタル化が進むことで、サイバー攻撃の脅威が社会インフラの物理的な被害にまで及ぶリスクが増大しています。また今後、様々な企業が産業を超えて繋がるためにはセキュリティの確保が必須であり、流通・活用されるデータの信頼性の確保も重要な課題です。さらには量子コンピュータの出現に対しても安全なネットワーク環境の実現が望まれています。

東芝グループは、デジタル化を推進する企業の責務として、140年以上の歴史で培われた幅広い事業領域に根差したインフラの知見と、約12万人の従業員を支える情報システムのセキュリティ運用のノウハウを融合し、安全安心なインフラの提供と、セキュアに繋がるデータ社会の構築により、持続可能なカーボンニュートラル・サーキュラーエコノミーの実現に貢献するサイバーセキュリティ強化に取り組んでいます。

東芝サイバーセキュリティビジョン

カーボンニュートラル・サーキュラーエコノミーの実現に向けたデジタル化戦略

東芝グループは、長年にわたり、電力や鉄道、上下水道など、国の重要インフラを支える事業に携わってきました。今後、カーボンニュートラル・サーキュラーエコノミーの実現に向けたデジタル化の変化に対応していくために、東芝グループではDE、DX、QXの3つの戦略を定めています。第一段階のデジタルエボリューション（DE）では、これらインフラのハードウェアとソフトウェアを分離してネットワークと接続し、様々なアプリケーションを追加していくことで、新たなサービスを生み出していきます。その次の段階は、このソフトウェアのレイヤーを標準化し、他社のハードウェアや他社のアプリとつながることでプラットフォーム化していくデジタルトランスフォーメーション（DX）です。プラットフォーム化により生み出される人のデータや産業のデータを活用し、更に新しいサービスを生み出すデータビジネスをめざします。さらにその先では、様々なプラットフォーム自体が業界を超えて繋がり、カーボンニュートラルなどの複雑な問題の最適解を見つけ出す量子の世界であるクオンタムトランスフォーメーション（QX）へ発展させることで、カーボンニュートラル・サーキュラーエコノミーの実現に貢献する企業をめざしています。



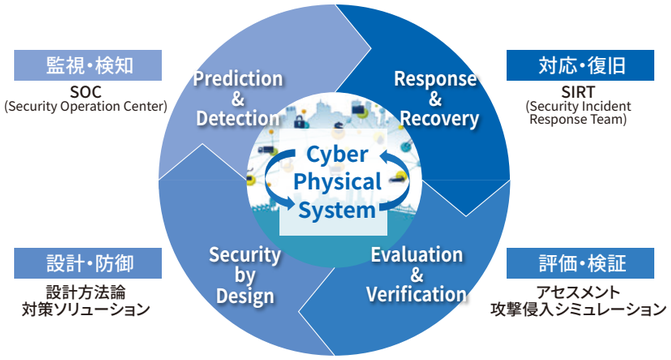
出典：2022年度 東芝グループ 経営方針説明会

東芝グループのサイバーセキュリティビジョン

近年、産業や社会の幅広い分野におけるデジタル化の進展に伴い、サイバー攻撃の脅威が社会インフラの制御システムや機器などにも広がり、制御システムが攻撃者に乗っ取られたり停止させられるなどの物理的な被害に遭うリスクが増大しています。そのような状況での東芝グループの使命は、これまで以上にお客さまの事業と社会を支え、安全安心で持続可能な社会を実現することです。そのためには、デジタル技術の利便性とサイバー攻撃の脅威によるリスクを正しく評価した上で、従来の防御を中心としたセキュリティ対策から、情報システムと制御システムを包括した持続的なセキュリティ確保への転換が不可欠です。

そこで、東芝グループは、自社内の情報システムや工場・設備などの生産システムだけでなく、お客さまに提供する製品・システム・サービスのデジタル化に対応したセキュリティ確保の取り組みを進めています。この取り組みは、設計・開発段階におけるSecurity by Design※に基づくセキュリティ構築にとどまらず、運用段階においては常に社内外の脅威を監視することでリスクを予測し、万が一のインシデント発生時には迅速な対応で被害の最小化と早期の事業復旧を図ります。また、最新の脅威と対策技術による評価・検証を行い、製品やサービスの設計・開発にフィードバックしていくことにより、「セキュリティライフタイムプロテクション」を実現し持続的なセキュリティを提供します。

※Security by Design：セキュリティを企画・設計段階から確保するための方策



セキュリティライフタイムプロテクション

東芝グループでは、この「セキュリティライフタイムプロテクション」の実現に向け、サイバーセキュリティマネジメントプロセスを「ガバナンス」「設計・防御」「監視・検知」「対応・復旧」「評価・検証」「人材」の6つの機能が有機的に結合したプロセスとして定義しました。そして、めざすゴールを「東芝サイバーセキュリティビジョン」として定めました。このビジョンの実現をめざしてサイバーセキュリティの取り組みを強化し、東芝グループの製品やサービスを通じて、皆さまに信頼されるパートナーであり続けられるように努めてまいります。

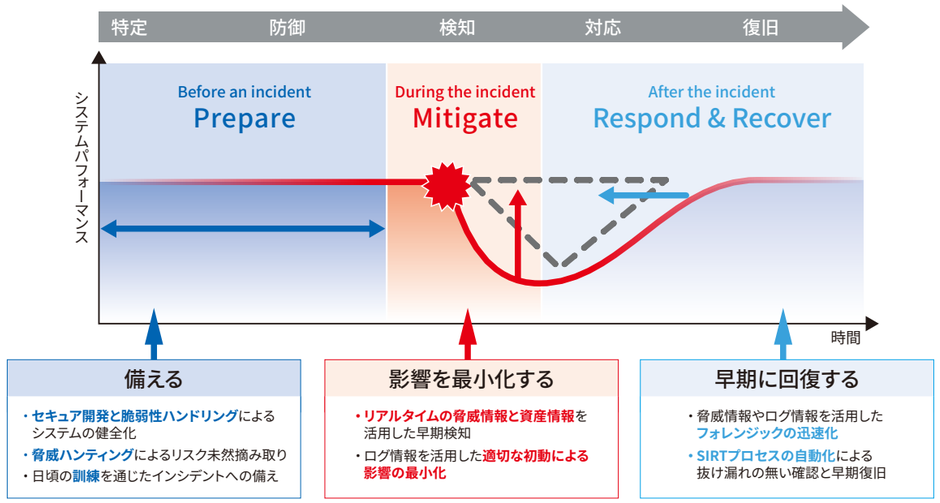
ガバナンス	サイバーセキュリティマネジメントのPDCAが回り 常に成熟度が向上している
設計・防御	脆弱性が入り込まない 製品開発／システム構築プロセスが運用できている
監視・検知	東芝グループおよび東芝製品にかかわる 社内外のセキュリティ脅威をリアルタイムに把握できる
対応・復旧	インシデント発生時に 迅速に被害を最小化し、事業復旧できる
評価・検証	製品／システムを評価・検証し 常に新たな脆弱性への対応ができている
人材	必要なセキュリティ人材が育成・強化できている

東芝グループがめざすゴール

サイバーセキュリティ態勢強化に向けた戦略

東芝グループでは、情報／製品／制御／データセキュリティをトータルで実現するために、「サイバーレジリエンス」という上位の考え方を取り入れました。レジリエンスは、「弾力」「復元力」「回復力」といった意味を持つ言葉です。サイバーレジリエンスは、サイバー攻撃などのセキュリティ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のことです。

私たちは、サイバーレジリエンスを実現するために、インシデントによるシステムへの影響を最小化するパラメータを定義しています。パラメータは、インシデントへの備え「Prepare（P）」、インシデントによる損失の軽減「Mitigate（M）」、そして対応・復旧時間「Respond & Recover（R）」の3つで、それぞれ、「Pを手厚く」「Mを十分に」「Rを短く」することが求められます。



サイバーレジリエンス

東芝グループでは、サイバーレジリエンスの実現に向けたセキュリティ態勢強化の戦略を推進しています。ここでの“セキュリティ態勢”とは、セキュリティリスクに対する十分な準備を備えた状態を意味します。具体的には、「Pを手厚く」「Mを十分に」するために意思決定・指揮系統を明確化するガバナンス、「Mを十分に」「Rを短く」するための監視・検知／対応・復旧／防御を行うセキュリティオペレーション、そして、これらを運用し発展させていく人材の3つが十分に連携・活用できるよう強化され、常態化されていることを意味します。

今後、CPSの進化により、情報システムだけでなく、社会インフラや産業にかかわる開発環境や生産・運用システム、さら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）からフィジカルを制御する世界がやってくると予想されます。その際、これまでのような社内に信頼できるネットワークを維持する境界型の防御は限界となり、「ネットワークはもはや信頼できるものではなくなった」という考え方のもと、人やモノといった資産単位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」の導入が必須となってきます。ネットワークにつながるあらゆるモノを認証・監視するゼロトラストアーキテクチャでは、セキュリティ運用の自動化・高度化が必要になるでしょう。東芝グループでは、これらの課題に対しても、早期に取り組みを行うことで、エネルギー×デジタル、インフラ×デジタルにおけるCPSの進化を支えてまいります。

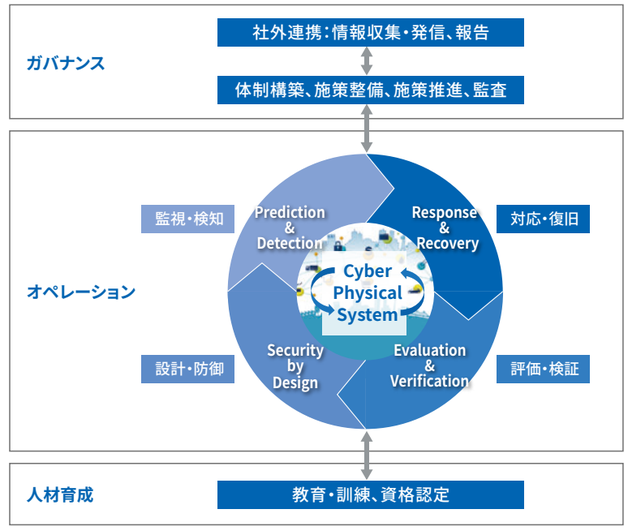
また、これらを実践するための組織強化も進めています。まず、ガバナンスの観点から、2017年11月に東芝グループの最高情報セキュリティ責任者（CISO）を設置しました。CISOは、最高経営責任者（CEO）から権限委譲され、サイバーセキュリティリスク管理の全責任を負うとともに、経営に影響を及ぼす重大なセキュリティインシデントへの意思決定を行います。これにより、東芝グループの全社に向けた対応指示を迅速かつ適切に行えるよう指揮系統を明確にしました。

また、専門組織として「サイバーセキュリティセンター」を設置しました。ここでは、社内情報システムにおける情報資産や個人情報などのセキュリティリスクに対応するCSIRT※1機能と、提供する製品・システム・サービスのセキュリティリスクに対応するPSIRT※2機能を集約しました。工場や設備などのシステムに関しても、CSIRT/PSIRT両面で抜けや漏れが無いようチェックしています。社内規程によるルールの明文化やグループ会社の体制整備を進め、製品開発段階や出荷済み製品について、セキュリティ上の脆弱性に対応するとともに、リスク判定ポリシーの共通化など、ガバナンスを強化しています。さらに、国内外のセキュリティ関連組織との窓口をこのセンターに一本化し、東芝グループ各社に設置した窓口との間で連携を図り、社内外の情報共有を積極的に行っています。

監視・検知、対応・復旧、防御といったセキュリティオペレーションの強化では、サイバーレジリエンス向上に向けたセキュリティリスクの検知・対応の迅速性および正確性向上を目的に、CDMP※3とよぶセキュリティ運用基盤の構築を進めています。CDMPでは、監視・検知、対応・復旧の自動化や脅威インテリジェンス※4の活用を積極的に進め、セキュリティリスクが企業活動に及ぼす影響の最小化をめざしています。

技術力強化の観点から、2019年4月に、東芝研究開発センターに「サイバーセキュリティ技術センター」を開設し、社内のセキュリティ専門人材を集めてサイバーセキュリティ技術に関する研究開発から技術支援、運用支援までを一気通貫で推進しています。

また、東芝グループ全体のセキュリティ人材の育成に向けては、従業員一人ひとりのセキュリティ意識の向上を図るため、情報セキュリティ・個人情報保護教育、製品セキュリティ教育を、全従業員を対象に実施しています。また、製品開発時のセキュリティ品質向上や、インシデント対応を担う高度なセキュリティ人材の育成のための教育とセキュリティ資格・認定制度を展開しています。



サイバーセキュリティマネジメントフレームワーク

以降で、ガバナンス、セキュリティオペレーション、人材育成の観点で、現在進めている具体的な施策についてご紹介します。

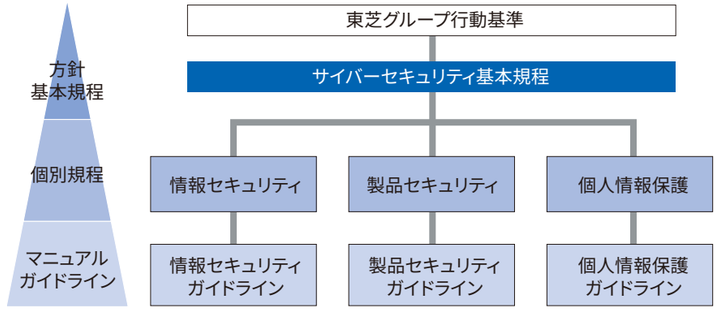
※1 CSIRT：Computer Security Incident Response Team
※2 PSIRT：Product Security Incident Response Team
※3 CDMP：Cyber Defense Management Platform
※4 脅威インテリジェンス：世の中のセキュリティにかかわる脅威動向やハッカーの攻撃活動など、セキュリティに関する意思決定を支援する情報の総称

ガバナンス

東芝グループの情報システムおよび製品・システム・サービス、個人情報保護におけるリスクに対し、グループとして一貫した対策を推進するため、「サイバーセキュリティ基本規程」を制定し、その下に情報セキュリティ／製品セキュリティ／個人情報保護の各規程を制定しています。これらの規程の基本方針およびマネジメント体制を紹介します。

基本方針

東芝グループは、企業経営に大きな影響を与えるサイバーセキュリティリスクを適切に管理し、さまざまなサイバー攻撃を想定したリスク管理体制を構築しています。また、安全・安心を追求する企業風土の醸成、お客さまやお取引先さまの情報、各種個人情報の保護を徹底することにより、社会的信用の維持、高品質な製品・システム・サービスの安定供給を行うサプライチェーンの実現をめざします。



東芝グループのサイバーセキュリティ関連規程体系

情報セキュリティ管理の基本方針

東芝グループは、「個人情報、お客さまやお取引先さまの情報、経営情報、技術・生産情報など、事業遂行過程で取り扱うすべての情報」の財産価値を認識し、これらを秘密情報として管理するとともに、その不適正な開示・漏えい・不当利用の防止および保護に努めることを基本方針としています。この方針は、東芝グループ行動基準の「情報セキュリティ」の項に規定し、東芝グループの全役員・従業員に周知しています。

製品安全・製品セキュリティに関する基本方針

東芝グループは、「製品安全・製品セキュリティに関する行動基準」を定め、関係法令遵守や、製品安全・製品セキュリティの確保に努めることはもちろん、お客さまへの安全情報の開示に積極的かつ誠実に取り組んでいます。また、製品提供先となる国や地域が規定している安全関連規格、技術基準（UL規格※1、CEマーキング※2など）を常に調査し、各規格・基準にしたがって安全関連規格の表示をしています。

※1 UL規格：材料・製品・設備などの規格を作成し、審査・認証する米国のUL LLCが発行する安全規格
※2 CEマーキング：製品が欧州連合（EU）共通の安全関連規格に適合していることを示すマーク。指定製品にこのマークがなければ欧州経済領域（EEA）で流通が認められない

個人情報保護方針

東芝グループが事業活動を通じてステークホルダーの皆さまから取得した個人情報は、皆さまの大切な財産であるとともに、東芝グループにとっても新たな価値創造の源泉となる重要資産であることを認識して、個人情報保護法および関連する法令、国が定める指針、そのほかの規範を遵守します。また、規程を制定し、個人情報保護マネジメントシステムを着実に実施し、維持するとともに、継続的な改善に努めます。

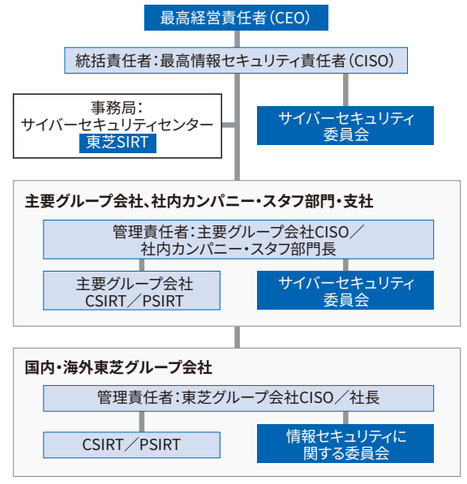
東芝個人情報保護方針（全文） https://www.global.toshiba/jp/privacy/corporate.html

マネジメント体制

東芝グループにおけるサイバーセキュリティ対策を推進するため、CISOの下でサイバーセキュリティマネジメント体制を構築しています。東芝SIRT※1はCISOを補佐し、東芝グループ全体のサイバーセキュリティリスク管理のための基本方針、推進体制、施策、重大クライシスリスクに発展するおそれのあるサイバーセキュリティインシデントへの対応について、サイバーセキュリティ委員会で審議します。また、東芝SIRTはCSIRTとPSIRTの両方の機能を持ち、東芝グループ全体のサイバーセキュリティ施策を統括し、国内・海外の東芝グループ会社を支援します。

また、東芝グループ全体へ一貫したセキュリティ対策を徹底させるために、グループ会社を所管する主要グループ会社に対して、CISOを設置し、各社のサイバーセキュリティマネジメント体制を整備しています。主要グループ会社のCISOは、自社とその国内および海外の傘下会社のサイバーセキュリティについて責任を負います。各社のCSIRTは、情報セキュリティにかかわる施策徹底や情報セキュリティインシデントへの対応などを行い、各社のPSIRTは製品セキュリティにかかわる施策徹底や製品脆弱性対応などを担当します。サイバーセキュリティ委員会※2では、主要グループ会社におけるサイバーセキュリティの徹底に必要な事項およびクライシスリスクに発展するおそれのあるサイバーセキュリティインシデントへの対応について審議を行います。

※1 SIRT：Security Incident Response Team
※2 同等の機能を有する会議体の場合もある

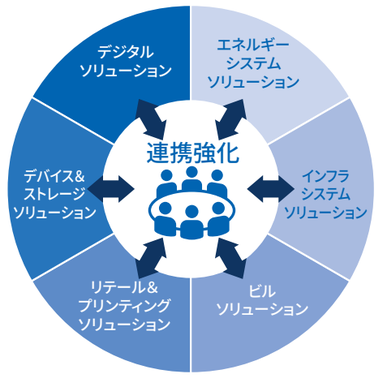


サイバーセキュリティマネジメント体制

東芝グループCISO会議

東芝グループのサイバーセキュリティ方針・施策を立案および評価する場として、東芝グループCISO会議を四半期ごとに開催しています。東芝グループは、エネルギー、社会インフラ、電子デバイス、デジタルソリューションという多様な事業を展開していることから、必要なサイバーセキュリティも異なります。そのため、本会議では東芝グループ全体のサイバーセキュリティ戦略や方針を議論するだけでなく、主要グループ会社のCISOがグループ各社での取り組みや課題を積極的に共有することで、自社の課題解決につなげています。

高度化するサイバー攻撃の脅威に立ち向かうため、主要グループ会社で組織を超えた横の連携を強化し、東芝グループ全体のサイバーセキュリティを強化していきます。

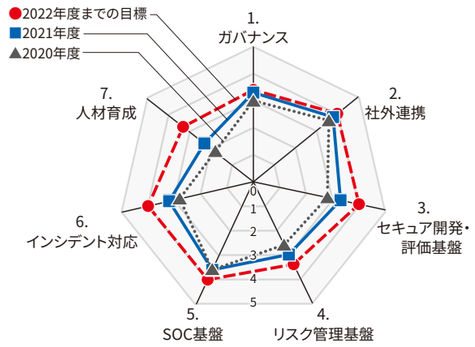


成熟度自己評価

東芝グループでは、サイバーセキュリティマネジメントの目標を設定し、目標に向けて管理レベルを高めるため、主要グループ会社を対象に毎年成熟度自己評価を実施しています。各社の成熟度を見える化することで、現在の状態を測定します。また、目標とのギャップを把握して具体的な施策を講じることで、各社のサイバーセキュリティ管理の確実なレベルアップを図ります。

成熟度自己評価の指標は、国内外で実績のあるセキュリティインシデントマネジメントの成熟度モデルSIM3※1や、経済産業省『サイバーセキュリティ経営ガイドライン』、NIST※2 “Cyber Security Framework”を参考にし、情報セキュリティ（CSIRT）、製品セキュリティ（PSIRT）の両方を評価します。評価レベルは5段階とし、ガバナンス、社外連携、セキュア開発・評価基盤、リスク管理基盤、SOC基盤、インシデント対応、人材育成のカテゴリ別に成熟度を評価します。

2020年度以降は成熟度自己評価の対象を海外東芝グループ会社にも拡大し、海外のサイバーセキュリティマネジメント体制の強化を推し進めています。



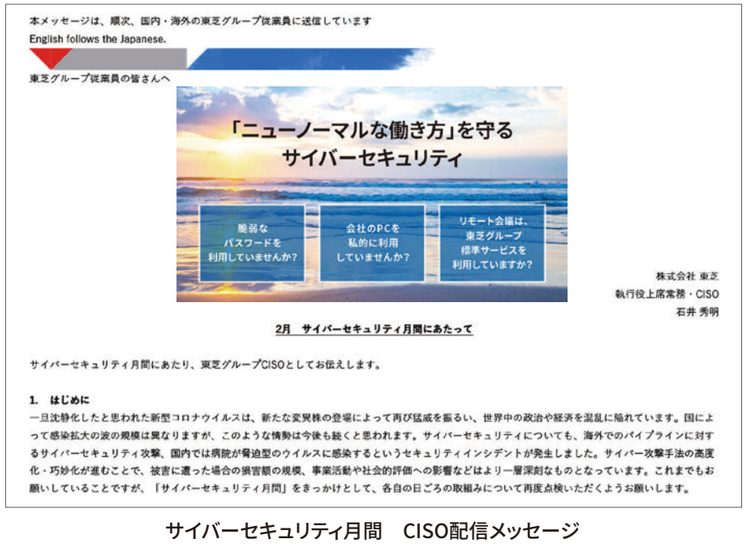
成熟度自己評価結果のグラフ

※1 SIM3：Security Incident Management Maturity Model
※2 NIST：National Institute of Standards and Technology（アメリカ国立標準技術研究所）

サイバーセキュリティ意識啓発活動

東芝グループでは、内閣サイバーセキュリティセンターのサイバーセキュリティ月間の取り組みに賛同し、2月を「サイバーセキュリティ月間」と定め、東芝グループCISOより全従業員に向けたメッセージを配信しています。メッセージの内容はその年のセキュリティ動向に合わせたテーマとしており、情報セキュリティで注意すべきことや、東芝グループが出荷する製品のセキュリティ対応などについても発信しています。また、ポスターを製作して社内ポータルなどに掲載し、従業員の意識啓発を促しています。

サイバーセキュリティでは常に最新の動向を把握し、情報連携することが大切です。そのため、情報発信・共有するコミュニティを作り、国内外のセキュリティニュースやベンダーレポート、業界団体・政策関連のニュース、報道発表などを日々発信・共有することで情報連携を図っています。


本メッセージは、順次、国内・海外の東芝グループ従業員に送信しています
English follows the Japanese.
東芝グループ従業員の皆さんへ
「ニューノーマルな働き方」を守る
サイバーセキュリティ
脆弱なパスワードを利用していませんか?
会社のPCを私的に利用していませんか?
リモート会議は、東芝グループ標準サービスを利用していますか?
株式会社 東芝
執行役上席常務・CISO
石井 秀明
2月　サイバーセキュリティ月間にあたって
サイバーセキュリティ月間にあたり、東芝グループCISOとしてお伝えします。
1. はじめに
一旦沈静化したと思われた新型コロナウイルスは、新たな変異株の登場によって再び猛威を振るい、世界中の政治や経済を混乱に陥れています。国によって感染拡大の波の規模は異なりますが、このような情勢は今後も続くと思われます。サイバーセキュリティについても、海外でのパイプラインに対するサイバーセキュリティ攻撃、国内では病院が脅迫型のウイルスに感染するというセキュリティインシデントが発生しました。サイバー攻撃手法の高度化・巧妙化が進むことで、被害に遭った場合の損害額の規模、事業活動や社会的評価への影響などはより一層深刻なものとなっています。これまでもお願いしていることですが、「サイバーセキュリティ月間」をきっかけとして、各自の日ごろの取組みについて再度点検いただくようお願いします。

サイバーセキュリティ月間　CISO配信メッセージ

グローバル対応体制

グローバルビジネスの推進にあたり、国内・海外東芝グループ全体で一貫したセキュリティ確保の取り組みがより重要になっています。実際に海外現地法人で発生したインシデントの影響が他国へおよぶ事例も発生しています。

東芝グループでは、サイバーセキュリティ施策の推進にあたり、サイバーセキュリティマネジメント体制（P.10参照）で臨んでいます。東芝グループ会社へは主要グループ会社経由で施策の提示・実行を進め、主要グループ会社各社は、自社とその傘下会社のサイバーセキュリティについて責任を負います。

社内ITインフラに対するセキュリティ脅威の監視とインシデントへの対応については、サイバーセキュリティマネジメント体制のように階層的な管理ではなく、SOCおよび東芝SIRTに集約したグローバルで一元的な体制で実施しています。これにより、社内ITインフラで発生している事象を相関的に分析するとともに、インシデント発生状況などの情報が集約でき、インシデントの早期検知と早期対応を可能にしています。

また、各地域や国ごとに、情報セキュリティや個人情報保護に関する法規制強化が進んでおり、場合によっては個別の施策が必要となるケースが生じています。各地域や国の法規制動向については継続的に調査を実施し、法規制の施行状況に合わせ、遅滞なく対応できるようにしています。

サプライチェーンのセキュリティリスクへの対応

昨今、サプライチェーンの弱点を狙った攻撃が増え、大企業から中小企業までサプライチェーン全体のサイバーセキュリティ対策の強化が急務です。

東芝グループでも、自社やグループ会社にとどまらず、情報を共有するパートナー企業を含むサプライチェーン全体のサイバーリスク対策のレベル向上を行うべく、ガバナンス、オペレーション、人材育成の3つの視点で対策を行っています。

（1）人材育成（e-Learning）

従業員に対するe-Learningを実施し、サプライチェーン上に存在する脅威はもちろん、想定されるリスクとその対策について学習する機会を設けています。ビジネスを推進していく上で、委託する立場、委託される立場、どちらの立場にもなることを想定し、立場ごとに異なるリスクを認識してそれに合わせた対策を講じることを目的としています。

（2）アセスメント

パートナー企業との共通システムやネットワーク構成の実態調査に関し、規程に定めたセキュリティ対策が施されているかを定期的にアセスメントしています。社内ネットワークに限らず、独立化されやすい工場・生産ラインへのアセスメントにも取り組み始めています。

（3）セキュリティレベルの定量評価（Security Risk Ratings）

一部のグループ会社において、パートナー企業を選定する際に、その企業のサイバーセキュリティを定量的に評価・可視化する取り組みを始めました。これは一般的に、Security Risk Ratingsとよばれる最近注目されている手法であり、サイバー攻撃を受けるリスクを可視化するものです。

攻撃者の視点に立って、実際に攻撃を行う初期段階の情報収集（初期偵察）を行い、対象会社のセキュリティ対策状況を定量評価（スコア化）します。取引開始の判断はこのスコアも参考に総合判断し、また取引中の会社に対しても定期的に診断を行い、発見された脆弱性に対しては、指導や是正支援を行います。

このような取り組みにより、パートナー企業を含むサプライチェーンのセキュリティ向上を図るとともに関係者の高いセキュリティ意識も醸成しています。

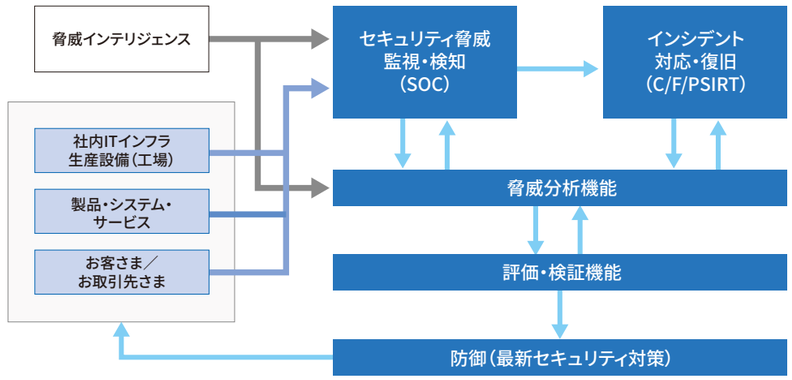
セキュリティオペレーション

東芝グループにおけるセキュリティオペレーションの高度化に向けた取り組みについて紹介します。現在東芝グループでは、レジリエンス向上に向けたセキュリティリスクの検知・対応の迅速性および正確性向上を目的に、CDMP※1とよぶセキュリティ運用基盤の構築を進めています。CDMPでは、監視・検知、対応・復旧の自動化や脅威インテリジェンス※2の活用を積極的に進め、セキュリティリスクが企業活動に及ぼす影響の最小化をめざしています。

※1 CDMP：Cyber Defense Management Platform
※2 脅威インテリジェンス：世の中のセキュリティにかかわる脅威動向やハッカーの攻撃活動など、セキュリティに関する意思決定を支援する情報の総称

CDMPの概要

CDMPでは、社内ITインフラだけでなく、工場などの生産設備、お客さまに提供する製品・システム・サービスをはじめ、将来的にはこれらに接続されるお客さまやお取引先さまのシステムも保護対象と考えています。具体的には、下図に示す機能群から構成されるセキュリティ運用基盤で、2019年1月から一部で運用を開始しています。



CDMP (Cyber Defense Management Platform)

•SOC：Security Operation Center
•C/F/PSIRT：Computer/Factory/Product Security Incident Response Team

CDMPは以下の機能で構成されます。

・セキュリティ脅威監視・検知（SOC）	⇒システムの状態監視によるセキュリティインシデントの検知（P.18参照）
・インシデント対応・復旧（C/F/PSIRT）	⇒発生したインシデントへの対応とシステムの復旧（P.14、20、26参照）
・脅威分析機能	⇒脅威インテリジェンスの活用による脅威未然防御（P.23参照）
	⇒ナレッジ蓄積、AI活用による精度向上
・評価・検証機能	⇒ハッカー視点での製品・システムの評価・検証（P.21参照）
・防御（最新セキュリティ対策）	⇒最新セキュリティ対策の適用による防御（P.22参照）

サイバー空間を取り巻く脅威は増大する一方です。対応できるリソースも限られており、検知されたインシデントへの対応・復旧の自動化、ナレッジの蓄積、AI活用を進め、少ないリソースでも精度の高いセキュリティ運用をめざします。自動化については、SOAR（Security Orchestration, Automation and Response）とよばれる自動化プラットフォームの導入を進め、SOAR上での脅威インテリジェンスの活用や、インシデント調査・対応の自動化を進めています。また、各社CISOやCSIRT/PSIRT関係者が自社のセキュリティ状況をリアルタイムに把握可能な、ダッシュボードの構築を進めています。ダッシュボードにより自社で発生しているインシデントやその対応状況を把握し、速やかな対応を促すことがその目的です。

インシデント対応迅速化

昨今のランサムウェア攻撃や情報窃取を狙った攻撃は、パソコンやサーバなどのエンドポイント※1が起点となるケースが多くみられます。一方、こうしたサイバー攻撃の巧妙化により、すべての攻撃からエンドポイントを完全に守ることは年々難しくなっています。そこで、インシデントの発生を前提とし、エンドポイントで何が起きているのか、状況を把握しその後の対応を迅速に行うことが重要となっています。

東芝グループでは、エンドポイントへの高度な攻撃を検知し、対応するためにEDR※2ツールの導入を進めてきました。（詳細は、Chapter 2 P.19「EDRツールによるエンドポイント対策の強化」参照）

EDRツールの導入により、

・強力な探索機能（クエリ機能）によりエンドポイントの「今」を把握（ベースラインの把握）
・エンドポイントに潜むマルウェアの不審な挙動を予兆段階で検知（早期検知）
・ネットワーク隔離によりマルウェアの他エンドポイントへの感染拡大防止（被害の最小化）

などといった点で、インシデント対応の迅速化に大きな効果が得られつつあります。

※1 エンドポイント：ネットワークに接続したパソコンやサーバ、情報機器
※2 EDR：Endpoint Detection and Response（エンドポイントでのセキュリティ脅威の検出と対応）

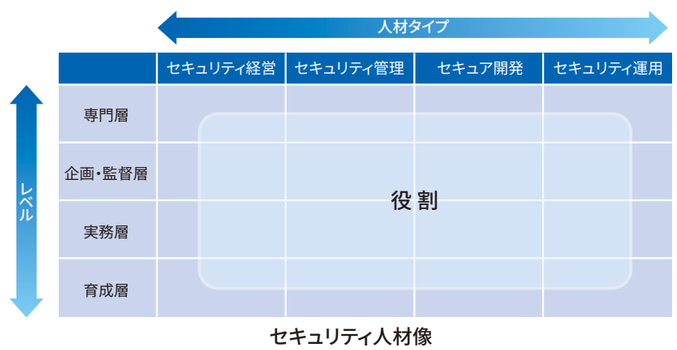
人材育成

東芝グループにおけるセキュリティ人材育成の取り組みについて紹介します。東芝グループに必要な「セキュリティ人材像」の定義、当該定義に基づく「セキュリティ教育プログラム」の提供、所定のセキュリティ知識・技術・実務スキルを有することを認定する「セキュリティ資格認定制度」による三位一体の取り組みを進めています。

セキュリティ人材像と資格認定制度

セキュリティ人材のレベルは、高度なセキュリティスキルを持った専門層からプラス・セキュリティ人材※1を含む育成層までがあります。また、セキュリティ人材のタイプは、セキュリティに関する経営、管理、開発、運用に分かれます※2。レベルとタイプそれぞれの組み合わせごとに、果たすべき役割を「セキュリティ人材像」としてまとめています。また、そのような人材を認定するセキュリティ資格認定制度を東芝グループ内で運用しています。認定には、社内外の所定のセキュリティ教育を受講していること、情報処理安全確保支援士などのセキュリティの資格を保有していること、および人材像に定義された役割を遂行するのにふさわしい業務経験を有していること、などの基準を設けています。これまでに約800名を認定しています。

※1 プラス・セキュリティ人材：セキュリティ対策を主たる目的とする業務としては明示的に位置付けられていないが、対策不十分な場合にセキュリティ上の問題が生じるような業務にセキュリティを意識して従事できる人材
※2 独立行政法人情報処理推進機構（IPA）取りまとめのスキル標準「ITSS+」等を参照



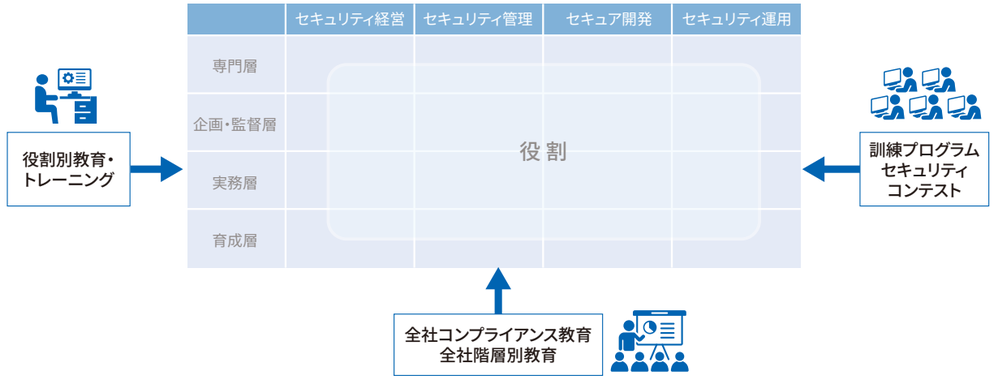
セキュリティ人材像

セキュリティ教育

情報漏えいを防ぐためには、従業員一人ひとりが日々の情報を適切に取り扱うための知識を身につけ、標的型攻撃などのセキュリティ脅威や、テレワークを行う際のセキュリティ上の注意点などに対する意識を高く持つことが重要です。また、お客さまに提供する製品・システム・サービスのセキュリティを確保するためには、営業、調達、設計、開発、品質、保守など製品にかかわる全員が、製品にセキュリティ脆弱性が発生するリスクの重大性と、製品開発段階でのセキュリティ脆弱性混入の防止、および出荷済み製品のセキュリティ脆弱性への迅速な対応の重要性を理解し実践する必要があります。そこで、一人ひとりのセキュリティ意識とリテラシーの向上を図るため、全社コンプライアンス教育（情報セキュリティ・個人情報保護教育、製品セキュリティ教育）を東芝グループすべての役員・従業員を対象に毎年実施しています。海外の従業員も受講できるよう多言語で展開しています。入社時や昇格時などの節目でも、それぞれの役割に応じた階層別教育を実施しています。

また、セキュリティ人材像に定義されたそれぞれの役割に基づく教育・トレーニングも提供しています。情報セキュリティ、製品セキュリティの基礎やサプライチェーンセキュリティの重要性を学ぶe-Learning、脅威分析やセキュア開発の手法を学ぶe-Learning、脆弱性検査の実務スキルを習得するハンズオントレーニング、脆弱性やインシデントにすばやく対応できる専門人材・高度人材の育成トレーニング、製品開発時のセキュリティ品質向上を担う管理職向けの製品セキュリティ教育などを提供するとともに、IPA産業サイバーセキュリティセンターが主催する中核人材育成プログラムなど、社外の実践的なトレーニングプログラムへの人材派遣も実施しています。

さらに、身につけた知識やスキルを常態化させるための訓練プログラム（例：インシデント対応訓練）や、セキュリティ技術の啓発・浸透・強化を目的とする東芝グループ従業員向けのセキュリティコンテストなどの取り組みも並行して実施しています。



プライバシーガバナンス※の取り組み

東芝グループでは、データサービスを展開していますが、社会的にパーソナルデータを利活用する事例が増えるとともに、プライバシー保護への要請が高まっています。

東芝グループでは、パーソナルデータを事業に活用する前にプライバシーリスクを特定・評価する仕組みとルールを作り、リスクを低減した上で事業に活用していきます。また、従業員に対してプライバシー保護の意識づけを図るための教育を実施しています。

プライバシーガバナンス規程の制定

東芝は2021年7月に「プライバシーガバナンス規程」を制定しました。パーソナルデータを利活用する事業においてプライバシー侵害のリスクがないか評価する手順を定めています。対象となる事業を計画する部門は、自社のCSIRTを通して、コーポレートスタフの関係部門から構成するプライバシーリスク評価委員会にかけて評価します。その際にプライバシーリスクが大きい案件については別途、外部有識者会議に諮問します。

プライバシー保護に関する全従業員教育

2021年度、個人情報保護の教育に併せて、プライバシー保護の重要性やプライバシーリスク評価の手順を周知する教育を東芝グループ従業員に対して実施しました。

プライバシーに関する外部有識者会議

会社から独立した中立・公正な社外構成員による「プライバシーに関する外部有識者会議」を設置しています。

※プライバシーガバナンス：プライバシーリスクを適切に管理し、組織全体でプライバシー問題に取り組むための体制を構築、機能させること

個人情報保護

東芝グループが事業活動を通じてステークホルダーの皆さまから取得した個人情報は、皆さまの大切な財産であるとともに、東芝グループにとっても新たな価値創造の源泉となる重要資産であることを認識して、個人情報の保護を適切に行っています。

社内規程、管理体制の整備と教育

東芝は、個人情報を適切に管理し、取り扱うため、社内規程「東芝個人情報保護プログラム」を制定しており、グループ会社においても各社で同様の規程を制定しています。規程で定めた事項を遵守し、運用するために、各組織で構築しているサイバーセキュリティマネジメント体制（P.10参照）によって個人情報保護を推進しています。また、個人情報の取り扱いや安全管理措置について意識づけを図るため、毎年、すべての役員・従業員・派遣社員を対象に教育を行っています。

個人情報の特定と管理

各組織が保有する個人情報を特定するため、「個人情報管理データベース（台帳）」を整備し、定期的に確認、更新しています。個人情報の内容と量に応じてリスクを判定し、リスクに応じて個人情報を管理しています。また、個人情報保護に関する自主監査結果を確認し、必要に応じてアセスメントを実施するとともに、要改善事項があれば是正しています。

個人情報の委託先の選定と監督

個人情報を取り扱う業務を社外に委託する場合、もし、委託先で個人情報の漏えいなどの事故が発生した場合、委託元の監督責任が問われます。特に、委託先からの漏えい事件が報道されて社会問題となって以来、委託元による委託先の監督が強く求められるようになりました。東芝グループでは、会社として適切なルールを整備し、安全に個人情報を管理できる委託先を選定するための基準を定め、一定の水準以上の会社に委託しています。また、委託後も、委託先に対して定期的に情報の管理、取扱状況を確認しています。

海外法令対応

近年、個人データ保護の法令を新たに制定したり、既存の法令を改定したりする動きが世界各国で顕著になっています。東芝グループでは、米国・中国・欧州・アジアにある地域総括現地法人を中心に、事業リスクに応じて各国における遵法活動を推進しています。

欧州一般データ保護規則（GDPR※）への対応　※General Data Protection Regulation

欧州GDPRに対応するため、東芝グループでは、欧州の地域総括現地法人を中心に、従業員の教育、規程類の整備、データ移転の状況把握（Data Mapping）などを実施しています。英国がEU から離脱し、2020 年12 月末で移行期間が終了したのに先立ち、2020年10月に欧州現法と日本の東芝グループ会社との間でIGDSA（TOSHIBA Intra-Group Data Sharing Agreement）を締結し、欧州と日本で個人データを共有する契約上の根拠を明確にしました。

中国個人情報保護法への対応

中国では、2017年6月に施行されたサイバーセキュリティ法に続き、2021年9月にデータセキュリティ法、11月に個人情報保護法が施行されました。これに対し、中国の地域総括現地法人を中心に情報把握を行い、規程類、契約書、教育資料などのひな型を作成して現地法人に展開するなどの対応を進めています。

タイ個人情報保護法への対応

2022年6月施行のタイ個人情報保護法に対応するため、アジアの地域総括現地法人を中心に規程類、契約書、教育資料などのひな型を作成して現地法人に提供し、体制を整備しています。

セキュリティ確保への取り組み

東芝グループでは、従来独立して推進してきた情報セキュリティと製品セキュリティの機能を集約し、セキュリティ強化に向けた取り組みを推進しています。本章では、セキュリティ強化に向けた取り組みとして、対象を社内ITインフラ、製品・システム・サービスに分けて紹介します。なお、社内ITインフラは東芝グループ内のPC・サーバ・ネットワークなどに加え、工場や生産設備も対象としています。

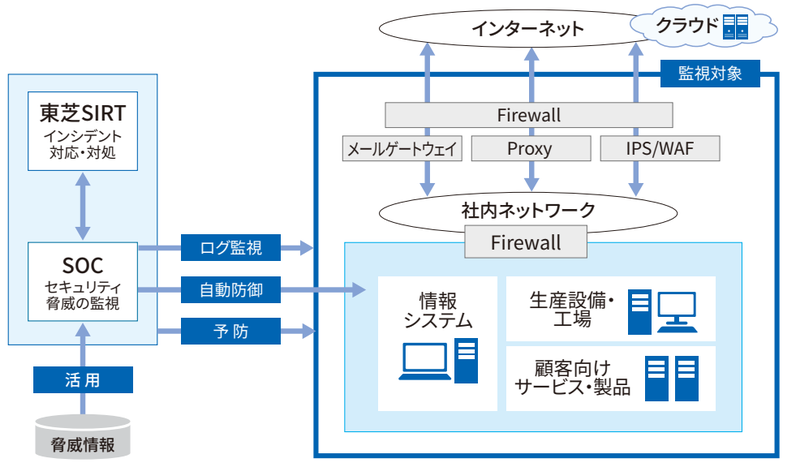
社内ITインフラへの対策

サイバー攻撃が巧妙化・高度化するなか、SOCによるセキュリティ脅威の監視・検知、CSIRTによるインシデント対応・復旧を行い、お客さまの情報資産を適切に管理しています。また、毎年国内外の東芝グループ全組織に対し自主監査・アセスメントを行い、指導しています。

監視・検知の強化

守るべき情報資産は社内ネットワーク内にあり、攻撃者を社内に侵入させないという考えから、これまではインターネットの出入口にファイアウォール、IPS、プロキシなどを設置して対策を講じてきました。しかし、業務の効率化や働き方改革により、パブリッククラウドの活用が増え、企業ネットワークにおける社内と社外の境界があいまいになり、その上、サイバー攻撃が、不特定多数をターゲットにしたものから、特定組織の機密情報や事業停止を狙った計画的で標的型の攻撃に変化し、ますますサイバー攻撃のリスクが増大するようになりました。そこで、セキュリティリスクをさらに早く、しかも正確に検知し、速やかに対処するため、以下の対策を強化しています。

・ITシステムに加え、工場・顧客向けサービスに監視範囲を拡大
・外部からの攻撃だけでなく、社内の侵害拡散や不審な振る舞いの通信を検知
・アラート検知後の対処の定型化と自動化
・外部の脅威インテリジェンス活用によるリスクベースのセキュリティマネジメント



SOCによるセキュリティ監視・検知の全体像

- SOC（Security Operation Center）：24時間365日体制でネットワークやデバイスを監視し、サイバー攻撃の検出や分析、対応策のアドバイスを行う組織
- Firewall：セキュリティ対策機能の一つで、意図しないソフトウェアが勝手に通信をしないように通信ポートを制御するもの
- ゲートウェイ：ネットワークとネットワークを接続するためのハードウェアやソフトウェアのこと
- Proxy：代理という意味があり、インターネットと内部ネットワークの間に置かれ、内部コンピュータの代理としてインターネット接続をする
- IPS（Intrusion Prevention System）：侵入防止システムとして、内部ネットワークへの不正侵入を検知し、遮断する
- WAF（Web Application Firewall）：ウェブアプリケーションのセキュリティの脆弱性を悪用した攻撃を検知し、遮断する

EDR※1ツールによるエンドポイント※2対策の強化

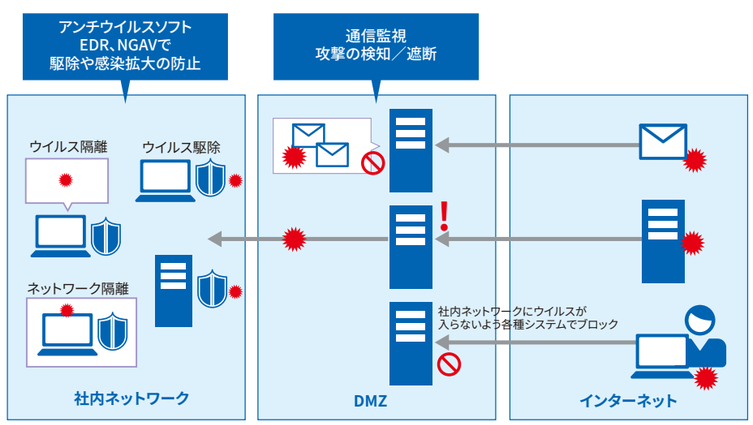
監視
検知

ウイルス対策ソフトで対応できない未知のウイルスや、ネットワークの出入口で検知できない高度な攻撃を検知し対応するため、国内・海外のパソコン・サーバなどのエンドポイントにEDRツールを導入しています。

EDRツールの導入イメージ

- 従来のウイルス対策製品で検出できない未知ウイルスの感染などによるエンドポイントの不審な挙動の検知、実行のブロック
- 感染端末をネットワークから外すことなく、SOCがリモートでエンドポイントをネットワークから隔離、脅威を駆除
- 収集した操作ログから、原因や被害範囲の追跡
- 外部の脅威インテリジェンスを活用し、エンドポイントの脆弱性の把握と対策徹底

※1　EDR：Endpoint Detection and Response（エンドポイントでのセキュリティ脅威の検出と対応）
※2　エンドポイント：ネットワークに接続したパソコンやサーバ、情報機器



EDRツールの導入イメージ

- NGAV（Next Generation Anti-Virus）：次世代アンチウイルス
- DMZ（DeMilitarized Zone）：インターネットなどセキュリティが確保されていないネットワークと、内部ネットワークなど保護されたネットワークの間に置かれるネットワーク領域

インシデント対応への取り組み

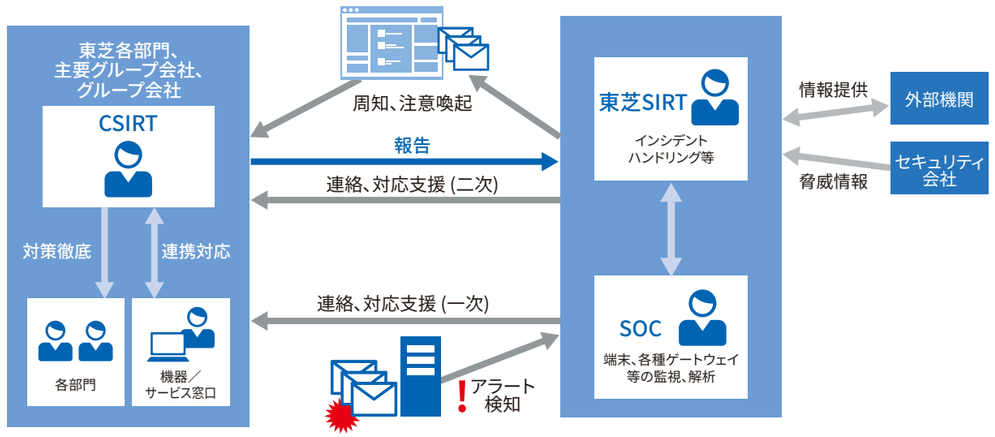
対応
復旧

サイバーセキュリティマネジメント体制のもと、東芝各部門、主要グループ会社、国内・海外グループ会社すべてにCSIRT※を設置し、インシデント発生時には、確実で速やかな対応が取れる体制を整えています。これによりSOCがアラートを検知した場合、東芝SIRTとの連携はもとより、該当する東芝の各部門・東芝グループ各社のCSIRTへも直接連絡が入り、より迅速な対応が実行できます。

※CSIRT：Computer Security Incident Response Team

CSIRTの役割

各システムの脆弱性対応やインシデント対応は、該当システムを所管する部門やグループ会社のCSIRTが責任を持ちます。IT部門や製造部門と連携して、脆弱性対応など各種セキュリティ施策の徹底や、インシデント対応を行います。東芝SIRTは、東芝の各部門および東芝グループ各社CSIRTと連携して、東芝グループ全体における各種セキュリティ施策の徹底やインシデント発生時の被害の最小化に責任を持ちます。特に、メールシステムなど、全社共通システムのインシデント対応、東芝の各部門や東芝グループ各社のCSIRT支援、複数部門が協調して行わなければならないインシデント対応を実行する役割を持っています。



インシデント対応の手順概要

インシデント対応への取り組み

ウェブサイトの改ざん、標的型メールやスパムメールの流入、未知ウイルスの侵入やウイルス拡散など、発生し得るインシデントに対しては、検知から終息までの対応手順書を用意するとともに、訓練や実際のインシデント対応を通して手順の確認や改善を実施しています。また、インシデント対応後は根本原因の追究および改善策の徹底を図り、再発防止を図っています。

自動化への取り組み

脆弱性やインシデントへの対応を24時間・365日で迅速かつ正確に行うために、脆弱性情報や脅威情報を入手した際、またアラートを検知した際の対応の自動化に取り組んでいます。入手情報や検知アラートを分類し、対応手順をパターン化することで、発生時間や対応者に関係なく対応できます。また、この取り組みを進めることで検知アラートの内容や関係する脅威情報などを相関分析し、真因の追究や、最適な対応手順を導くことをめざしています。

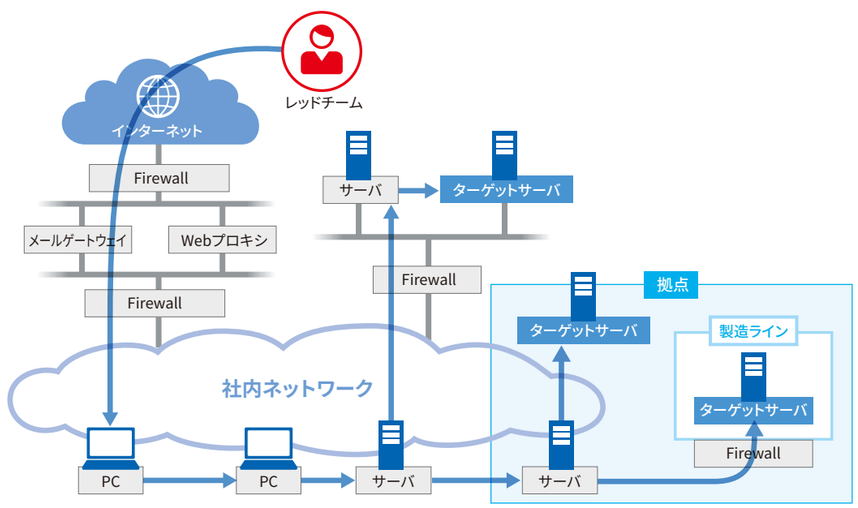
ハッカー視点の高度な攻撃・侵入テスト

評価
検証

特定の企業や組織の顧客情報や機密情報を不正に取得する標的型攻撃が増加しています。このような高度化するサイバー攻撃の脅威に対し、セキュリティ専門会社のレッドチーム※による攻撃・侵入テストを受診し、東芝グループのセキュリティ施策の実効性を定期的に確認しています。

この攻撃・侵入テストではレッドチームが実際の攻撃者と同じ高度な戦術や技術を用いて、東芝グループのネットワークへの侵入を試み、現実に即した疑似攻撃があらかじめ決めたターゲットサーバへ到達できるかを確認します。さらに、既存のセキュリティ対策における有効性の確認や、サイバー攻撃に対する弱点と追加施策を検討します。

※レッドチーム：攻撃者がどのように対象組織を攻撃するかの観点で、セキュリティ体制や対策の有効性を確認するチーム



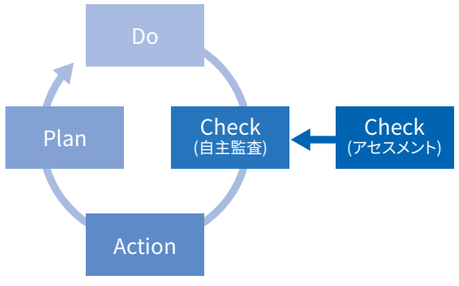
攻撃・侵入テストの概要

自主監査・アセスメント

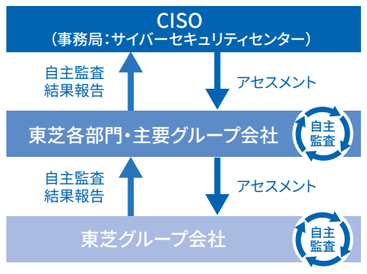
評価
検証

東芝グループには多様な事業分野があることから、東芝グループ全体の情報セキュリティを確保するためには、各部門が自律的にPDCAサイクルを回すことが大切です。そこで、すべての部門が、毎年社内ルールの遵守状況を自ら点検し、問題点の発見・改善に努めています。

各部門の点検結果や改善活動は、事務局である「サイバーセキュリティセンター」が評価し、是正が必要であれば指導・支援を行います。国内・海外の東芝グループ各社においても、毎年自主監査を行い、自主監査結果を第三者の視点で確認し妥当性を評価するアセスメントを事務局が実施することで、グループ各社の情報セキュリティレベルの向上につなげています。



自主監査・アセスメントを軸にPDCAサイクルを回す

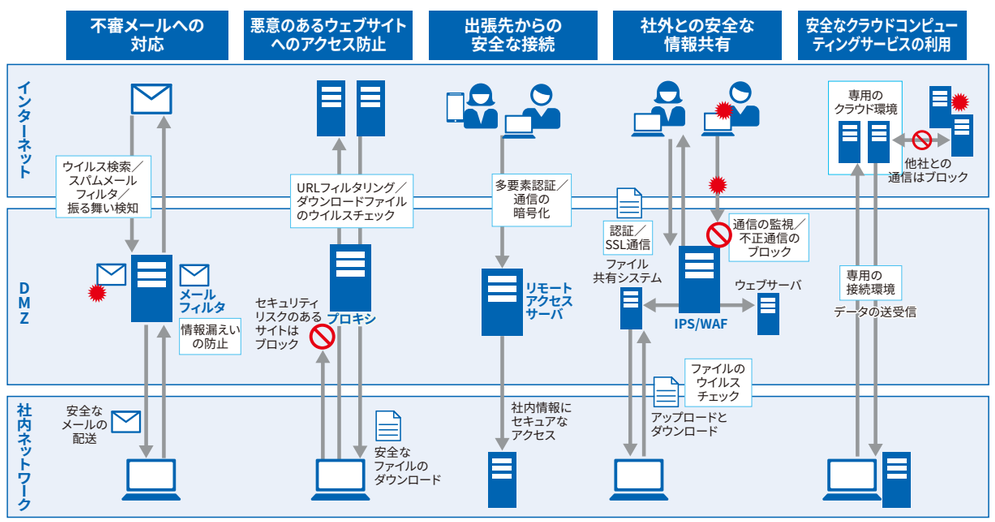


東芝グループ全体で自主監査・アセスメントを実施

インターネット接続点のセキュリティ対策

設計
防御

東芝グループでは毎日数千万件の攻撃を観測しており、外部インターネットと社内ネットワークの境界にWAF/IPSなどの各種セキュリティ機器を設置して監視や遮断を実行しています。ここでは各種リスクに対するインターネット接続点でのセキュリティ対策について紹介します。



インターネット接続点のセキュリティ対策

- DMZ（DeMilitarized Zone）：インターネットなどセキュリティが確保されていないネットワークと、内部ネットワークなど保護されたネットワークの間に置かれるネットワーク領域
- プロキシ：代理という意味があり、インターネットと内部ネットワークの間に置かれ、内部コンピュータの代理としてインターネット接続をする
- IPS (Intrusion Prevention System)：侵入防止システムとして、内部ネットワークへの不正侵入を検知し、遮断する
- WAF (Web Application Firewall)：ウェブアプリケーションのセキュリティの脆弱性を悪用した攻撃を検知し、遮断する
- スパムメール：無差別かつ大量に送られる迷惑メール

不審メールへの対応

ウイルスつきメールなどの外部からの脅威、情報漏えいなどの内部から発生する脅威の両面で対策を講じています。外部からの脅威では、ウイルスの流入対策として、受信メールの本文にあるリンクや添付ファイルを一度安全な環境で実行する「振る舞い検知」「送信ドメイン認証」「スパムメールフィルタ」を導入しています。これにより、毎日数十万通の不審メールをブロックしています。また、内部からの情報漏えいを防止するために、添付ファイルの暗号化や誤送信防止ツールを導入し、外部ドメイン宛のメール監視を実施しています。

悪意のあるウェブサイトへのアクセス防止

インターネットウェブアクセスにおけるリスク低減策として、プロキシサーバを導入しています。マルウェアのチェックやURLフィルタの活用、およびログ監視を行い、悪意のあるウェブサイトへのアクセスを防いでいます。不審な通信が発生した場合は、アクセスログから利用端末の特定を行います。一方、業務上必要なウェブサイトへは、ユーザ認証による制限でアクセスを許可し、業務の妨げにならないようにしています。

出張先からの安全な接続

営業担当者や出張者が、客先やホテルなどからインターネットを利用してパソコンやスマートデバイスを安全に社内ネットワークに接続できる環境を構築しています。多要素認証を用いて、不正アクセスを防止し、通信の暗号化を実施しています。また、在宅勤務やテレワークでも仮想デスクトップと併せて活用し、働き方改革を推進しています。

社外との安全な情報共有

社外との情報共有や情報発信にウェブサイトを活用しています。お取引先さまとのファイル交換にはアクセス制御やファイルのウイルスチェックを実施し、安全な環境を設けています。ウェブサイトや社外公開サーバはセキュリティ診断を定期的に行い、脆弱性のチェックや増大する脅威に対し、いち早く対策を行っています。

安全なクラウドコンピューティングサービスの利用

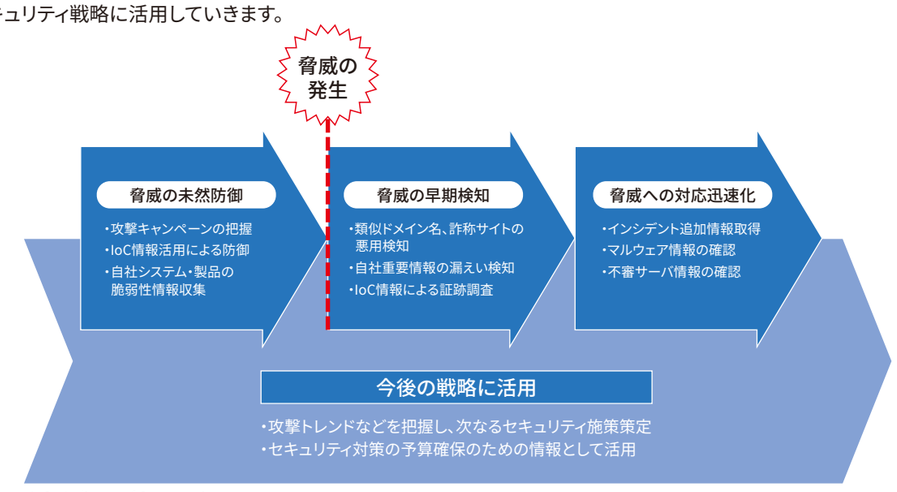
業務効率化のため、クラウドコンピューティングサービスを利用する機会が増えていると同時に、情報漏えい、不正アクセス、誤設定など危険も増えています。そのため、さまざまな危険から重要情報を守り、安全に利用できるプライベートクラウド環境を構築しています。一方、パブリッククラウドサービスの利用は申請制とし、東芝グループのセキュリティポリシーを満たしているか確認した上で、利用を許可しています。また、定期的に利用機能や方法に変更がないか確認しています。

上記の東芝グループ共通のセキュリティ対策のほかに、個別にインターネット接続点を持っている拠点では、セキュリティ機器の設定やログ監視をしています。共通施策だけではなく、事業や情報の重要度に合わせた対策を行うことで攻撃からの防御を徹底しています。現在は、情報システムの対策を中心に行っていますが、今後はそのノウハウを活用し、工場や顧客向けサービスなどのセキュリティ対策強化に取り組みます。

脅威インテリジェンスの活用

セキュリティオペレーションの高度化に向けた施策として、脅威インテリジェンスの活用を積極的に進めています。脅威インテリジェンスは、ハッカーの攻撃や脅威動向、脆弱性に関する情報など、脅威の防止や検知に利用できる情報の総称で、東芝グループでは、公的機関や外部の脅威インテリジェンス提供サービスなど、さまざまなソースからの情報を入手しています。

入手した脅威インテリジェンスに対し、東芝グループへの影響、緊急度などを分析し、必要に応じてプロキシやファイアウォール、EDRなどの機器に適用を行います。このように、東芝グループを取り巻く脅威に対する未然防御、脅威発生後の早期検知と対応の迅速化に脅威インテリジェンスを活用しています。また、攻撃トレンドなどの情報は、今後のセキュリティ戦略に活用していきます。



•IoC：Indicator of Compromise

脅威インテリジェンスの活用

製品・システム・サービスへの対策

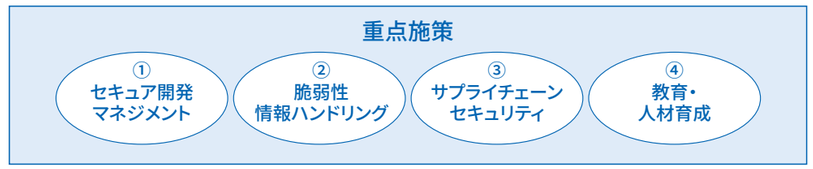
東芝グループでは、お客さまへ提供する製品・システム・サービスに対するセキュリティ品質を確保するため、さまざまな活動に取り組んでいます。また、PSIRT（Product Security Incident Response Team）体制を確立し、社外機関との連携により自社製品の脆弱性への迅速な対応を行っています。

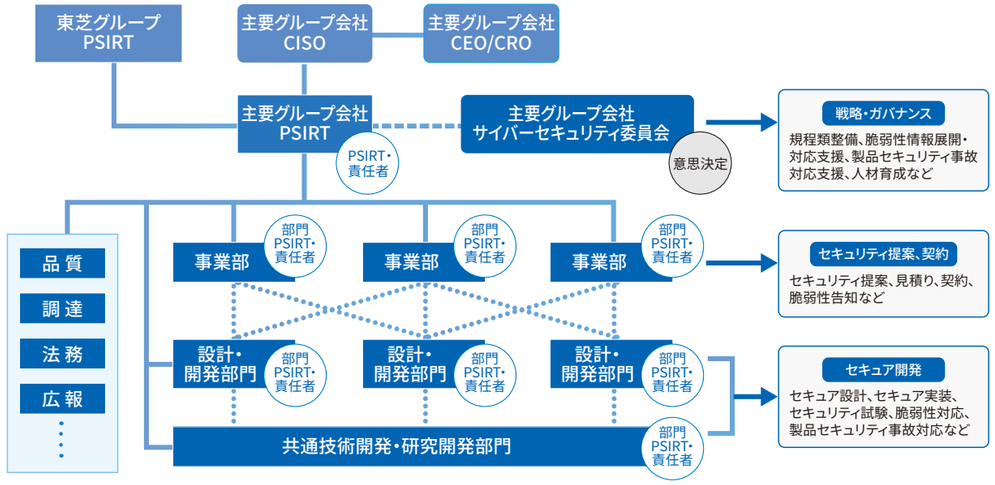
製品セキュリティを確保するための取り組み

お客さまへ提供する製品・システム・サービスに対するセキュリティを確保するため、サイバーセキュリティマネジメント体制の一部として構築した製品セキュリティマネジメント体制のもと、品質保証部門・調達部門と連携して、製品の開発プロセスにおけるセキュリティを確保するとともに、東芝グループ製品に利用される他社製品のセキュリティを確保しています。

製品セキュリティ態勢強化計画の策定

東芝グループの製品セキュリティ強化のための重点施策4項目について、昨今の製品セキュリティを取り巻く情勢と東芝グループの実情を鑑みて再定義し、東芝グループとしての中期的な達成目標を設定するとともに達成状況を可視化しました。これに基づき、グループ各社で構成する製品セキュリティマネジメント体制のもと、リスクベースの優先順位付けに基づく製品セキュリティ態勢強化計画を策定しました。これらにより、全社施策を開発現場であるグループ各社の事業部門、設計・開発部門まで確実に行き渡らせる実効性の確保と、自律的組織運営の早期かつ着実な実現をめざします。

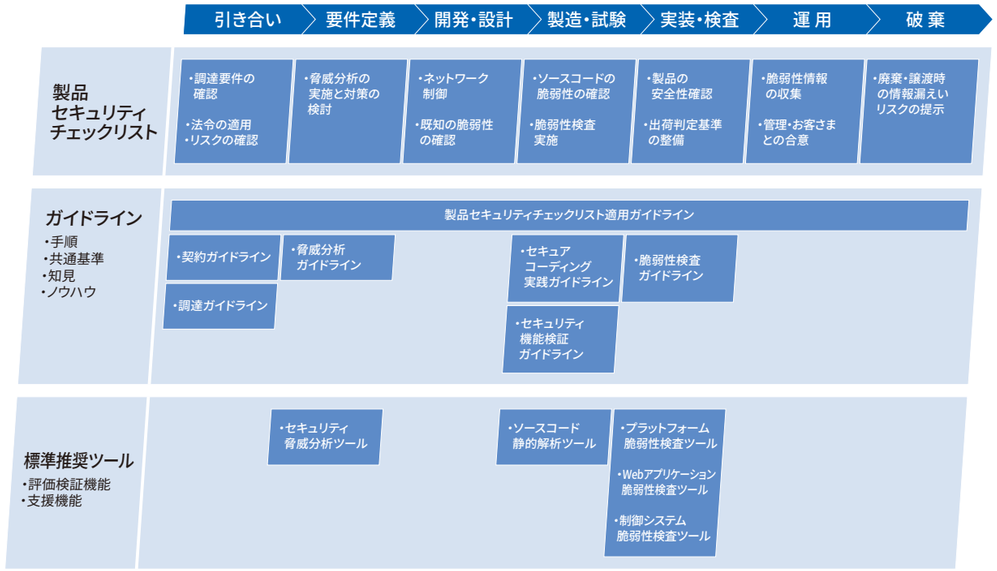




製品セキュリティマネジメント体制

製品セキュリティチェックリスト、およびガイドライン・標準推奨ツールの整備

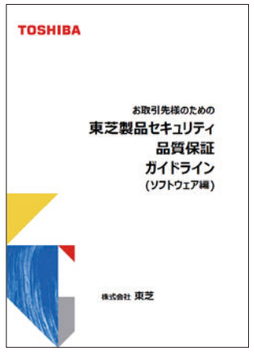
製品の開発プロセスの各フェーズでは、当該フェーズで確認すべき項目をまとめた「製品セキュリティチェックリスト」、チェックリストに対応した東芝グループ共通の「ガイドライン」「標準推奨ツール」の整備を進めています。これらを活用することで、考慮すべき内容の漏れを防止するだけでなく、経験・ノウハウ・習熟度の違いによる対応レベルの差を解消し、東芝グループとして一貫した製品セキュリティの確保を進めています。チェックリストで確認する上で有用な標準推奨ツールや関連する支援サービスなどについては、メニュー化した評価検証機能の一部として提供しています。



製品セキュリティチェックリスト、およびガイドライン・標準推奨ツールの整備

「お取引先様のための東芝製品セキュリティ品質保証ガイドライン（ソフトウェア編）」の制定

お取引先さまにも東芝グループの製品セキュリティの考え方を十分にご理解いただくとともに、安全な製品・システム・サービスの提供の実現にご協力いただく目的で、ガイドラインの整備を進めています。このガイドラインでは、「お取引先さまのセキュリティ管理体制」「ご納入いただくソフトウェア製品の開発成果物」「委託する運用サービス」の3点について、具体的なセキュリティ要望事項を定め、取引開始時に配布、周知することで、東芝グループが求めるセキュリティ要望事項を明らかにしています。



「お取引先様のための東芝製品セキュリティ品質保証ガイドライン（ソフトウェア編）」

迅速かつ確実な脆弱性への対応

対応
復旧

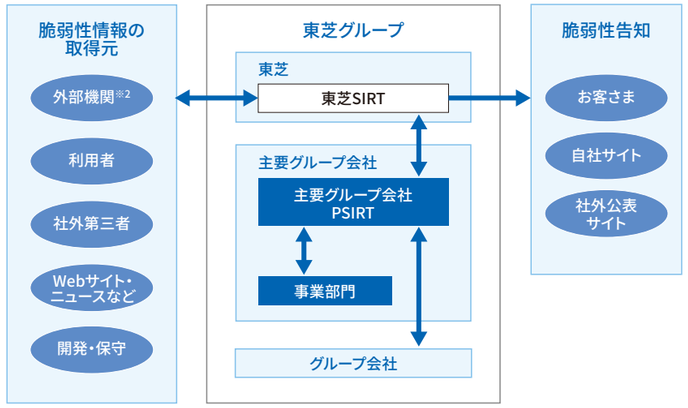
東芝グループ全体で、迅速かつ一貫した脆弱性対応を行うための体制を整備することにより、東芝グループの製品・システム・サービスをご活用いただいているお客さまの事業リスクの低減に貢献します。

東芝グループは、経済産業省告示「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」に基づく「情報セキュリティ早期警戒パートナーシップ」に参加し、外部機関と積極的に連携して、情報収集を行っています。また2021年6月よりCNA（CVE採番機関、CVE Numbering Authority）※1としてCVE®（Common Vulnerabilities and Exposures）プログラムに参画し、自社製品の脆弱性に対してより迅速に対応することが可能となりました。

全社で一貫した対応ができるよう、必要な対応手順で具体化した「製品セキュリティリスク対応マニュアル」を社内規程として策定するとともに、e-Learningを活用して製品ライフサイクルにかかわる全従業員の意識の向上を図っています。

脆弱性対応の体制

東芝グループが提供する製品・システム・サービスに対して、脆弱性対応のための体制「東芝SIRT」を整備しています。東芝グループの内外との脆弱性対応窓口機能を東芝SIRTに集約し、事業主体となる主要グループ会社の「主要グループ会社PSIRT」と連携して、迅速かつ一貫した脆弱性対応にあたります。脆弱性がお客さまの事業に深刻な影響を与えるおそれがあると判断した場合は、社会的影響を考慮して適切な手段で告知し、対応いたします。

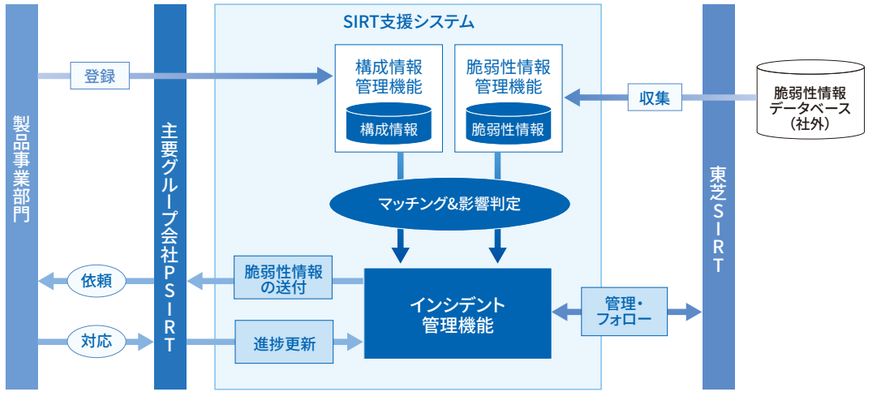


東芝グループ脆弱性対応の体制

※1 CNA：あらかじめ定めた範囲内の製品群における脆弱性に対するCVE ID割当てとそのCVE Recordの作成および公開を担当する組織
https://www.cve.org/About/Overview
※2 外部機関：JPCERT/CC、JVN、ICS-CERTなど

脆弱性ハンドリングのプロセス

外部から受け取った脆弱性情報は、製品事業部門を持つ主要グループ会社が影響を受ける製品を特定し、影響レベルを判定した上で、必要な対策を講じる必要があります。しかし、昨今脆弱性が急増したため、東芝グループではこれまでの脆弱性ハンドリングの知見から独自開発した「SIRT支援システム」を運用し、製品事業部門の迅速かつ確実な対応をめざします。



SIRT支援システムの概要

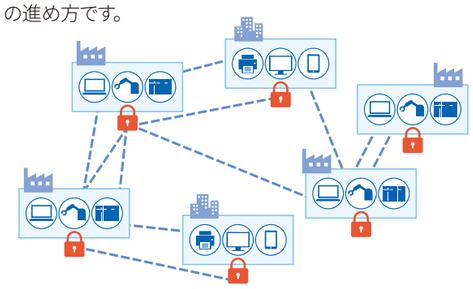
コラム

ニューノーマル時代のゼロトラストシフト

コロナ禍の日常は昨年と同様に続き、テレワーク、リモート会議など、オンラインでやり取りすることが当たり前になりました。働き方の環境の変化に応じて、サイバー攻撃の狙いも変化し、IPAが昨年出した「情報セキュリティ10大脅威2021」※1によると、“テレワークなどのニューノーマルな働き方を狙った攻撃”が新たに3位にランクインし、“ランサムウェアによる被害”が1位となっています。これは、攻撃者が環境変化に機敏に適応し、脅威を増大させていることを意味します。そのため、従来の守り方を考え直す必要性が出てきました。

今年1月、米国政府が出した覚書「Moving the U.S. Government Toward Zero Trust Cybersecurity Principles」※2が注目を集めました。米国政府は、「脅威が高まっている現状において、従来の“境界防御型”のセキュリティ対策に頼っていては、重要なシステムやデータを守ることができない」と述べており、ゼロトラストセキュリティモデルへと移行する戦略が提示されました。英国においても、NCSCが「Zero Trust architecture design principles」※3を昨年公開し、日本も昨年「サイバーセキュリティ2021」※4でゼロトラストの検討が言及されています。国内企業も、パロアルトの調査※5によると、ゼロトラストに注目する企業の割合が88%もあり、官民問わずその採用に関心が高まっています。

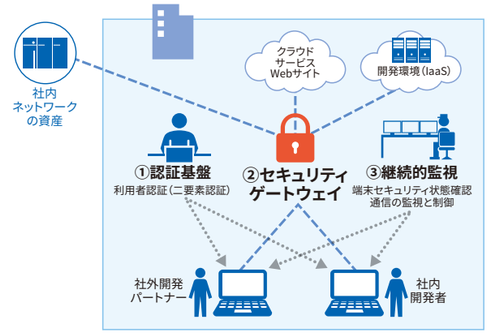
一方で、これまで構築してきた社内ネットワークの境界防御を一気に取り崩し、ゼロトラストへ移行することは、膨大なコストと作業負担を要することから困難です。そこで、まずは境界防御を維持しつつ、境界の中にあるゼロトラストの仕組みが導入しやすい部分や、一つのプロジェクトから始めていくことで移行へのリスクを減らし、周囲の理解を得ながら、ゼロトラストへシフトしていくことも一つの進め方です。



ゼロトラストネットワーク

東芝グループの取り組み

東芝デジタルソリューションズでは、社内ネットワークの中に多くのソフトウェア開発用のシステムや資産があるため、以前は強固なセキュリティ境界を設置し、社内と社外を完全に分離して安全を確保してきました。しかし、社外とのクラウドを活用した共同開発が増えて、ソフトウェア開発用にゼロトラストの環境を新たに構築しました。これにより、開発効率は向上しています。この社内事例で導入した東芝グループが考えるゼロトラストの3要素 ①認証基盤 ②セキュリティゲートウェイ ③継続的監視、を軸にセキュリティポリシーと運用体制を確立し、ゼロトラストシフトした要素を増やしていきたいと考えています。



ソフトウェア開発拠点のゼロトラストモデル

将来的には、境界防御の壁の有効性・必要性が薄れていき、社内にある工場や研究所などの部署、あるいは資産単位でゼロトラスト化し、企業はゼロトラスト化した要素の集合体となっていくでしょう。脅威は、内部犯、海外拠点や子会社、さらにはサプライチェーンから侵入します。ゼロトラストモデルでは、つながる相手の信頼性は全てその都度確認し、つながる対象は常に監視を行います。このため、ゼロトラスト化した要素の集合体は、リスクを最小化し、サプライチェーン全体で最適化されたセキュリティを構築することを可能にすると考えています。

※1 情報セキュリティ10大脅威2021
https://www.ipa.go.jp/security/vuln/10threats2021.html
※2 https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
※3 https://www.ncsc.gov.uk/collection/zero-trust-architecture
※4 https://www.nisc.go.jp/pdf/policy/kihon-s/cs2021.pdf
※5 https://www.paloaltonetworks.jp/company/press/2021/palo-alto-networks-surveys-japanese-organizations-on-zero-trust

セキュアな製品・システム・サービスの提供

東芝グループでは、エネルギー、社会インフラ、電子デバイスなど、各事業分野におけるセキュリティのニーズから、さまざまなセキュリティにかかわる製品・システム・サービスを提供しています。

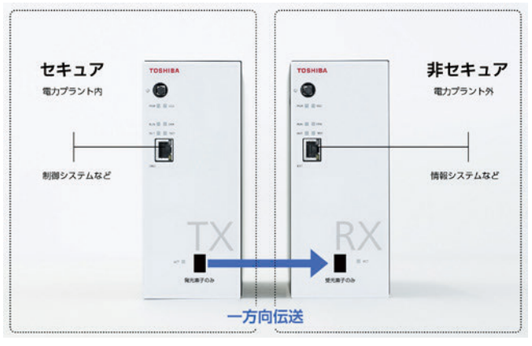
一方向伝送装置　TOSMAP-DS™／LX OWB

東芝エネルギーシステムズ（株）

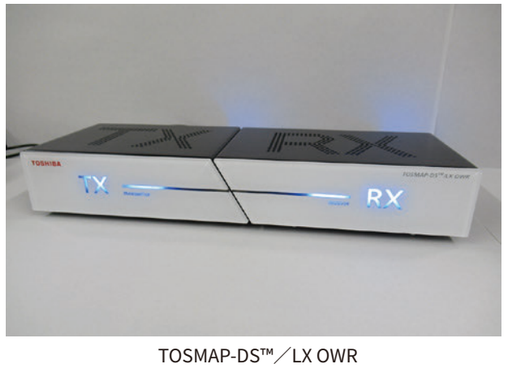
近年の電力市場自由化の流れのなかで、発電プラントの監視制御体系は多様化しており、監視操作の効率化や高度化などへの要望がますます強くなっています。その一例として、遠隔での統合監視やプラントの運転データなどを用いた高度な分析のニーズがあります。これを実行するためには、外部にデータを送信する必要がある一方で、発電所の監視制御は確実に守らなければなりません。

そこで、発電所内部のネットワークセキュリティを確実に担保する手段として、一方向伝送装置 TOSMAP-DS™／LX OWBを適用しています。外部からの通信を物理的に遮断することで、内部ネットワークを確実に保護しつつ、外部への単一方向にデータ送信を可能とすることで、強固なセキュリティを構築することができます。この製品は、発光素子しか持たないTX（Transmitter）と、受光素子しか持たないRX（Receiver）を「対」に存在させることで、物理的に一方向伝送を確保するとともに、区分けが明快にイメージできるようになっています。既存の発電プラントの制御システムにも容易に追加できる仕様で、セキュアな運転監視の高度化を実現できます。また、アキレスコミュニケーション認証（Achilles Communication Certification）Level 2を取得していますので、未知のセキュリティ脆弱性を検出するためのロバストネス性※も確保しています。さらに、より小型で高性能化を実現した、後継機種TOSMAP-DS™／LX OWRもリリースしました。

※さまざまな外部の影響による変化を受けにくい性質・頑強性



TOSMAP-DS™／LX OWB



TOSMAP-DS™／LX OWR

IoTセキュリティソリューション　CYTHEMIS™

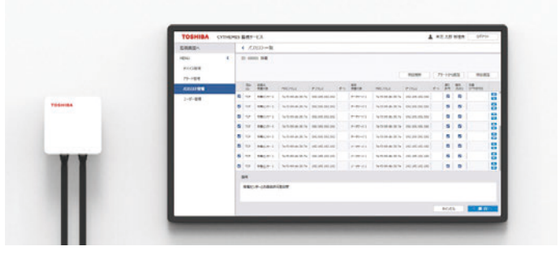
東芝インフラシステムズ（株）

近年、IoT化が盛んな工場だけでなく、マテリアルズインフォマティクスといった研究開発分野のIoT化の取組みも盛んになってきています。クラウド活用による分析の高度化、測定データの共用、研究装置の共同利用など、研究開発の効率化・加速化に向けた取組みですが、コロナ禍によるリモートワークや遠隔利用の加速といった背景もあります。そのためには、研究開発装置のネットワーク化が必須ですが、これらを制御するPCは用途向けにカスタマイズされているケースが多く、一般利用のPCと同じようなセキュリティ対策やOSのアップデートができず、ネットワークにつなげることが許容されないことが多々あります。そのために、上記のような取組みを諦めたり、データの移動にUSBメモリ等を使わざるを得なく、研究開発業務の効率化が進められない状況があります。東芝インフラシステムズ（株）が開発したCYTHEMIS™は、そのような装置のセキュリティを担保しながら、ネットワーク接続を可能とし、IoT化を後押しするソリューションになります。

CYTHEMIS™は、ネットワークに外付けできる小型のデバイスとそれを集中管理するシステムがパッケージとなったソリューションです。小型のデバイスは、装置個別のファイアウォールのようなもので、装置の代わりに、通信のフィルタリングや相互認証、暗号化の機能を代行し、許可された宛先だけに許可された通信だけを許容し、安全な通信を実現します。許可した通信以外は全て遮断するため、社内ネットワークに入り込んだマルウェアのラテラルムーブメントを防ぎ、万が一の場合でも、セキュリティ的に脆弱性が残っている装置に感染してしまうようなケースを防ぎます。また、保守作業等で、装置自身がマルウェア感染してしまい、その装置から社内ネットワークに拡散してしまうようなケースでも、管理システムとデバイスの連携により、拡散を抑え込むこともできます。その意味で、外付けのEDR的な役割も持っています。ネットワーク管理者の立場からは、既存のネットワーク環境はそのままに、これまで許可できなかった装置のネットワーク化を許容しつつ、セキュリティ的な運用管理業務を最小限に抑えることができます。

当面は組織内に閉じたデータ移動や装置の遠隔利用で活用するケースでも、管理システムの設定を変えるだけで、将来的なクラウド活用や組織外との連携も容易に実現できます。

本格的なIoT/CPS時代では、サイバー空間と物理空間のデータの正確な転写や通信相手の識別が必須になってきます。CYTHEMIS™は、これまでのようなネットワークの境界で守るやり方ではなく、通信に関与するそれぞれのエンティティをしっかり認証して、それぞれの通信をセキュアにすることで、安心・安全なIoT/CPS時代に貢献していきます。



CYTHEMIS™

ストレージ製品へのセキュリティ機能の実装

東芝デバイス&ストレージ（株）

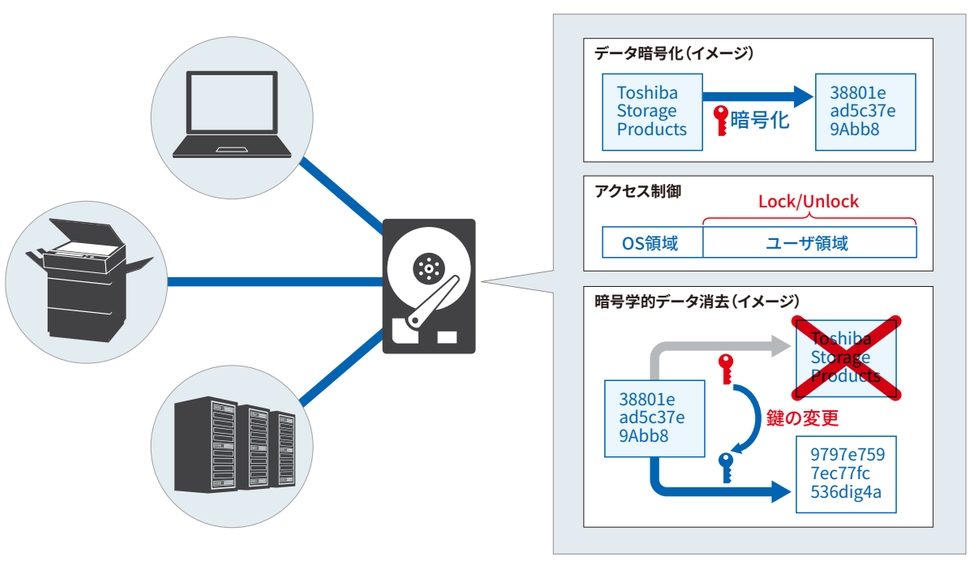
近年、個人情報保護に対する要求の高まりから、ストレージ製品の情報セキュリティが重要性を増しています。東芝のHDD製品は、個人ユースでのモバイル機器向け製品だけでなく、デジタル複合機向け製品やデータセンター向けをはじめとしたエンタープライズ製品など、各分野に適した製品をラインアップしており、各分野に合わせて適切な情報セキュリティ技術を備えたHDDを提供しています。

ストレージ製品に求められるセキュリティ要件として、まずHDDの盗難や紛失により発生するデータ流出の保護と抑止機能があります。また、廃却後にデータが流出することを防止するため、データを完全に消去する機能も求められています。

当社ではこうした顧客ニーズに応えるため、自己暗号化ドライブ（SED※1）を開発、提供しています。クラウドデータセンター用の大容量で高性能なニアラインHDDでは、データの書き込み時にHDD内で自動的に暗号化して保存します。データ暗号化にはNIST※2（アメリカ国立標準技術研究所）で定められた標準暗号規格であるAES※3を用いています。またATA※4Security Feature Set（ATA機の場合）やTCG※5 Opal SSC※6、TCG Enterprise SSCによるアクセス制御機能もサポートし、保護されたデータをパスワード認証なしに取得することを防止します。これら機能により、データ保護と流出抑止を実現しています。

さらに、廃却時のデータ完全消去についても、データの暗号化鍵を変更することで暗号学的に瞬時にデータ無効化できる技術（Cryptographic Erase）を搭載し、コストをかけてデータを上書きすることなく全データの無効化を実現しています。

本製品の暗号アルゴリズム実装は、米国政府の FIPS PUB 140-3 に基づく暗号アルゴリズム試験 CAVP※7 を取得（A1637, A1638, A1645）しており、高い信頼性が保証されています。更に MG09*CP18/16TA※8 製品では、2020 年から開始された米国政府の暗号モジュール認証、FIPS PUB 140-3 に基づく CMVP※9 の取得も進めており、暗号モジュールとしての HDD 全体の設計、実装、動作を第三者機関により多角的に評価しています。



ストレージ製品のセキュリティ機能のイメージ

※1　SED：Self-Encrypting Drive
※2　NIST：National Institute of Standards and Technology
※3　AES：Advanced Encryption Standard
※4　ATA：Advanced Technology Attachment
※5　TCG：Trusted Computing Group
※6　SSC：Security Subsystem Class
※7　CAVP：Cryptographic Algorithm Validation Program
※8　MG09*CP18/16TA：MG09SCP18TA, MG09ACP18TA, MG09SCP16TA, MG09ACP16TA
※9　CMVP：Cryptographic Module Validation Program

量子暗号通信システム

東芝デジタルソリューションズ（株）

昨今、インターネットなどの情報通信ネットワークは、私たちの生活には無くてはならないものとなりました。今後もIoT化の浸透などにより、ネットワークへの依存度はますます高まっていくと考えられます。

一方、近年、量子コンピュータの発展は目覚ましいものがあります。今後、大規模な量子コンピュータが登場すると、その圧倒的な計算能力により、インターネットなどで広く利用されている暗号通信が簡単に破られ、大事な情報が漏えいする危険性があります。

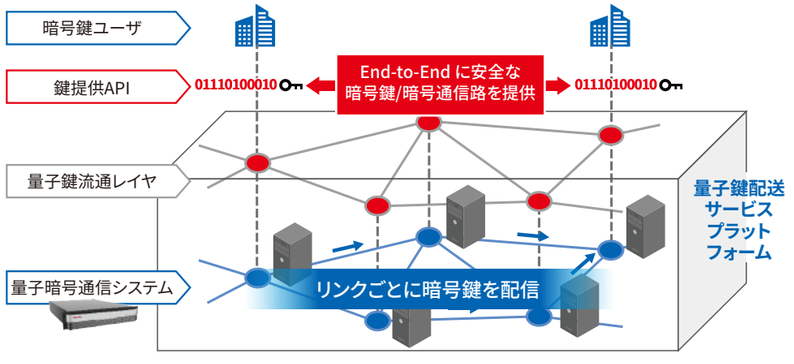
これに対抗する技術が、量子暗号通信です。量子コンピュータのようなどんなに高速なコンピュータが現れようとも、「理論上絶対に破られない」暗号通信技術です。暗号通信を行うための暗号鍵を、光の最小単位である光子にのせて通信することで、通信途中で暗号鍵が漏えいすることを、量子力学の原理により防ぎます。

東芝グループでは、量子暗号通信の研究を20年以上継続し、暗号鍵配信速度（単位時間あたりに配信できる暗号鍵の量）の世界最高を更新するなど、常にトップを走り続けてきました。そしてこの度、安全に暗号鍵を供給することのできる量子暗号通信サービスの実証を、世界の複数都市で開始しました。標準化されたAPI※を介して、安全な暗号鍵を簡単に利用することができます。

今後は大規模なネットワークへの展開を進め、多くのさまざまなお客さまにご利用いただける、暗号鍵供給サービスを提供してまいります。

※ ETSI GS QKD 014

量子暗号通信システム



量子鍵配送サービスプラットフォーム

デジタル複合機e-STUDIO5525AC/e-STUDIO5528Aシリーズ

東芝テック(株)

オフィス、店舗に設置されたデジタル複合機は、コピー機能だけでなく、ネットワークに接続され、クラウドサービスへのスキャンデータの保存やクラウドサービスからのプリント機能を備えています。サイバー攻撃を受け、複合機内の機密情報が漏えいする、改ざんされる、データが破壊される、複合機が利用できなくなる等の問題が発生しない様にするため、セキュリティ対策を講じる必要があります。

デジタル複合機e-STUDIOシリーズは、複合機として最新かつ最高レベルのセキュリティ基準HCD-PP※1に適合するべく、ISO/IEC15408※2認証(CC※3認証)を以前から取得しています。HCD-PPは暗号モジュールのセキュリティ要件として米国連邦標準規格FIPS 140-2※4と同等レベルの機能要件が規定されており、HCD-PPに適合することは最高レベルのセキュリティ認証取得に相当する対策が施された製品であることを意味しています。

デジタル複合機e-STUDIO5525AC/e-STUDIO5528Aシリーズでは、上記セキュリティ機能に加え、アンチマルウェア、TPM※5 2.0、セキュアブート、指紋認証等のセキュリティ機能を強化しました。

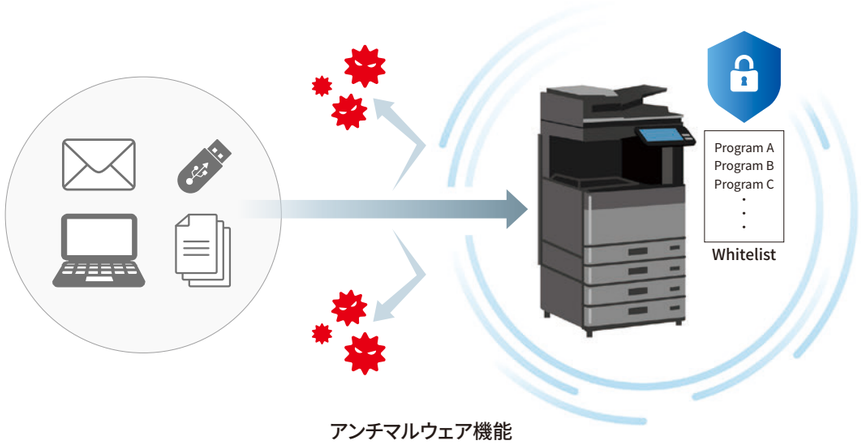
アンチマルウェア機能を利用することで、許可された安全なソフトウェアのみが動作可能となり、マルウェアのような不正ソフトウェアに感染することを防止することができます。

TPM2.0に対応することで、安全に暗号鍵を保存することができます。これによって記録メディアが盗まれた場合でも、暗号化されたデータの復号を防ぐことができ、複合機内の機密情報を守ることができます。セキュアブート機能により、万が一複合機内の起動プログラムが改ざんされた場合にも検出が可能です。

更に、従来のカード認証やNFC認証に加え、指紋認証による個人認証機能を追加しました。生体情報を利用することで、高速で安全な個人認証を可能としています。

これらのセキュリティ対策については、東芝研究開発センターにおけるサイバー攻撃評価により、セキュリティの専門技術者が想定するサイバー攻撃に耐えることを確認しました。

このように、デジタル複合機e-STUDIOシリーズは、これらの機能や対策によって、様々なセキュリティの脅威からお客様の情報資産を保護します。



アンチマルウェア機能

※1　HCD-PP：Hard Copy Device - Protection Profile
※2　ISO/IEC15408：国際標準化機構／国際電気標準会議規格15408
※3　CC：Common Criteria
※4　FIPS 140-2：Federal Information Processing Standard 140-2
※5　TPM：Trusted Platform Module

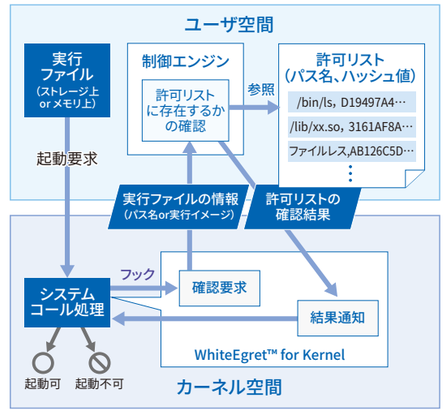
研究開発

高度化、多様化するサイバー攻撃から社会基盤を守り続けるため、東芝では先進的セキュリティマネジメント技術や、それらを支える先端攻撃や先端暗号に関する研究開発に取り組んでいます。サイバー攻撃の進化を先取りしたプロアクティブな対応で、社会インフラ事業で築き上げた東芝基準の安心安全品質を提供し続けます。

不正プログラム実行制御技術

電力システムなど重要インフラの制御システムを狙うマルウェアが登場し、サイバー攻撃に適用され、社会基盤が脅かされています。

そこで東芝は、Linux®標準機能を利用して実行プログラム起動の可否を決定する許可リスト型不正プログラム実行制御技術WhiteEgret™を開発しました。制御システムに適用可能で既知・未知を問わずマルウェアからの防御を可能にしています。さらに、制御システムへの適用が広がるコンテナ型仮想化技術や、新たな脅威であるファイルとしての実体を持たない「ファイルレスマルウェア」にも対応しています。

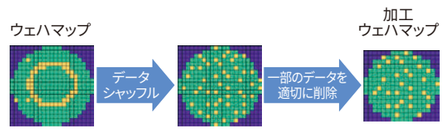


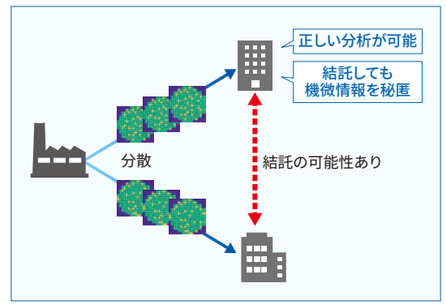
参考文献：金井遵他、“コンテナ型仮想化技術のリスクに対応した許可リスト型実行制御ソリューション”、東芝レビュー Vol.77, No.3 (2022年5月)

安全性と有用性を兼ね備えるデータ加工技術

半導体製造過程で得られるウェハマップ※などの産業データは、適切に分析し利活用することで生産効率向上などの価値をもたらします。しかし、利活用のために外部組織に開示すると産業データに含まれる機微情報の漏えいリスクが高まります。また、暗号化など安全性を高める手法を適用すると、高い自由度で分析することが困難になります。

そこで東芝は、安全性と有用性を兼ね備えるデータ加工技術を開発しました。データを適切にシャッフルや削除することで、開示先が結託したとしても機微情報を守ることができます。





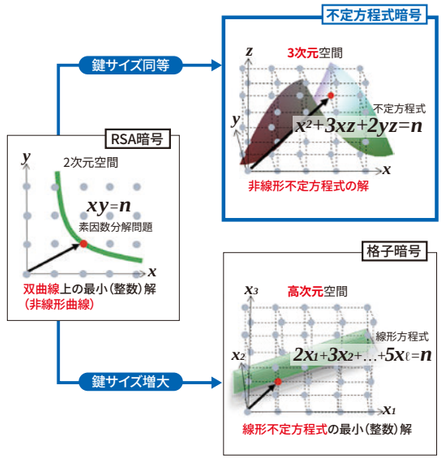
※ウェハマップ：シリコンウェハ上に作成されるチップの良品と不良品の分布を表したデータ
参考文献：花谷嘉一他、“安全性と有用性を両立する半導体ウェハマップのデータマスキングの検討”、SCIS2022

耐量子計算機暗号

大きなデータ処理が可能な量子コンピュータが出現すると、現在普及している公開鍵暗号が破られ、情報セキュリティは無力化される可能性があります。

そこで東芝は、現行のRSA方式で用いられている素因数分解問題よりもはるかに計算が困難な「不定方程式の求解問題」を安全性の根拠とする不定方程式暗号を開発しました。他方式よりも高い安全性を実現することで暗号鍵サイズを現行方式程度に抑えるとともに、高速処理も可能とし、計算機資源が限られるエッジ機器などへの耐量子計算機暗号の導入をめざします。

参考文献：Koichiro Akiyama et al., “A Public-key Encryption Scheme Based on Non-linear Indeterminate Equations (Giophantus)”, https://eprint.iacr.org/2017/1241 (2017)

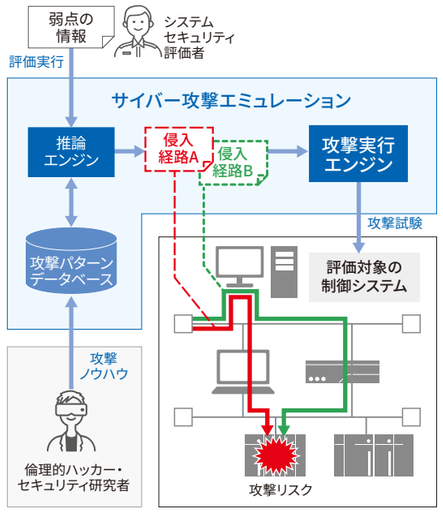


サイバー攻撃エミュレーション技術

社会インフラを支える制御システムに対するサイバー攻撃が激しさを増す中で、こうした攻撃のリスクを評価し、適切な対策をとることが重要になっています。

そこで東芝は、システム内に存在する弱点の情報にもとづいて実際に攻撃を受けるリスクを評価するサイバー攻撃エミュレーション技術を開発しました。この技術を用いることで、制御システムへの侵入経路を割り出し、その経路に沿って重点的なセキュリティ対策を行うことが可能になります。また実際に攻撃を行うことで、精度よく攻撃リスクを評価するとともに、セキュリティ対策の有効性を検証することができます。

参考発表：Fukutomo Nakanishi et al., “Automated Attack Path Planning and Validation (A2P2V)”, BlackHat USA Arsenal 2021
https://github.com/pentest-a2p2v/

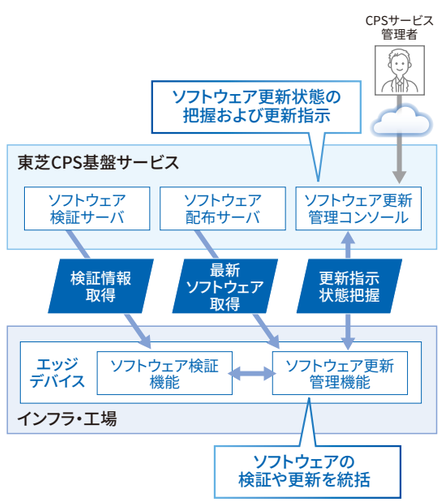


セキュアなソフトウェア更新技術

CPSにおいては、接続するエッジデバイスを、悪意ある第三者がインターネットを経由して攻撃する可能性が高まります。このような攻撃に備えるには、エッジデバイスのソフトウェアを常に最新版に更新しておく必要があります。一方、近年ではソフトウェア更新機能を悪用する攻撃事例が増えてきており、更新機能の仕様や実装には細心の注意が必要です。

そこで、東芝は既存のソフトウェア更新機能に対して脅威分析を行い、分析で得られた知見とオープンソース実装とを組み合わせてセキュアなソフトウェア更新技術を開発しました。

参考文献：南圭祐他、“HABANEROTSのエッジデバイス向けセキュリティー機能”、東芝レビュー Vol.76, No.5（2021年9月）



社外活動

2022年3月31日現在

東芝グループでは、サイバーセキュリティに関する各種標準化活動や社外活動に参画することにより、セキュアなサイバーフィジカル社会の実現のために活動しています。

国際標準化活動

主なデュール国際標準化活動として、ISO（International Organization for Standardization：国際標準化機構）とIEC（International Electrotechnical Commission：国際電気標準会議）があります。ISOとIECの合同技術委員会として、ISO/IEC JTC1（Joint Technical Committee 1：第 1 合同技術委員会）が設けられており、東芝グループは、ISO/IEC JTC1の3つのSC（Subcommittee:専門委員会）をはじめ、以下の国際標準化活動に参画しています。

- ISO/IEC JTC1/SC17　カードおよび個人識別用セキュリティデバイス
- ISO/IEC JTC1/SC27　ITセキュリティ技術
- ISO/IEC JTC1/SC41　IoTと関連技術
- ISO TC292/WG4　製品の偽造防止と信頼性
- IEC TC65/WG10　汎用制御システム
- ETSI（European Telecommunications Standards Institute）、SCP（Smart Card Platform）ヨーロッパの電気通信全般にかかわる標準化活動
- GlobalPlatform　マルチアプリケーションICカードの管理技術

SIRT活動

FIRST

FIRST（Forum of Incident Response and Security Teams）は、大学、研究機関、企業、政府機関などが加盟する信頼関係で結ばれたインシデント対応チームの国際コミュニティで、東芝グループは2019年1月に加盟しました。

日本シーサート協議会（NCA）

NCAは、コンピュータセキュリティにかかるインシデントに対処するための日本の組織で、東芝グループは2014年に加盟しました。

その他

セキュリティに関する情報共有や普及・啓発などを推進する各種社外活動へ参画しています。また、全国で開催される各種セミナー、学会などにおける講演も行っています。

- 一般社団法人情報通信ネットワーク産業協会（CIAJ）通信ネットワーク機器セキュリティ分科会 ほか
- 一般財団法人日本情報経済社会推進協会（JIPDEC）
- 特定非営利活動法人日本セキュリティ監査協会（JASA）
- サイバー情報共有イニシアティブ（J-CSIP）重要インフラ機器製造業者SIG
- 電子商取引安全技術研究組合（ECSEC）
- 技術研究組合制御システムセキュリティセンター（CSSC）
- ロボット革命・産業IoTイニシアティブ協議会 産業セキュリティアクショングループ
- 産業横断サイバーセキュリティ人材育成検討会
- 内閣サイバーセキュリティセンター（NISC）サイバーセキュリティ協議会
- 電力ISAC（Japan Electricity Information Sharing and Analysis Center）テクニカル会員
- 一般社団法人デジタルトラスト協議会
- 経済産業省　産業サイバーセキュリティ研究会　ワーキンググループ1（制度・技術・標準化）工場サブワーキンググループ ほか

第三者評価・認証

2022年3月31日現在

東芝グループでは、情報セキュリティマネジメント、個人情報保護、製品に関する第三者評価・認証の取得を推進しています。

ISMS認証取得状況（東芝グループ／東芝冠称会社）

東芝ITサービス株式会社
東芝インフォメーションシステムズ株式会社
東芝インフラシステムズ株式会社（小向事業所 SA部門）
東芝情報システム株式会社
東芝デジタルエンジニアリング株式会社（大分事業所）
東芝デジタルエンジニアリング株式会社（デジタルエンジニアリング第2事業部）
東芝デジタルエンジニアリング株式会社（本社 デジタルエンジニアリング第3事業部）
東芝デジタルソリューションズ株式会社
東芝デジタルマーケティングイニシアティブ株式会社
（ソリューション本部 Webプラットフォーム部 サーバサービス担当、アプリケーションサービス担当）
東芝デジタルマーケティングイニシアティブ株式会社
東芝テック株式会社（静岡事業所（三島））
東芝テック株式会社（静岡事業所（大仁））
東芝テックソリューションサービス株式会社
東芝デベロップメントエンジニアリング株式会社
東芝ビジネスエキスパート株式会社
（TBLS事業統括部 業務サポート事業部、人材開発事業部 芝大門塾）
東芝ライフスタイル株式会社
テックインフォメーションシステムズ株式会社
イー・ビー・ソリューションズ株式会社
SBS東芝ロジスティクス株式会社
中部東芝エンジニアリング株式会社（本社、横浜事業所）

プライバシーマーク取得状況（東芝グループ／東芝冠称会社）

東芝アイエス・コンサルティング株式会社
東芝ITサービス株式会社
東芝インフォメーションシステムズ株式会社
東芝インフラシステムズ株式会社
東芝健康保険組合
東芝自動機器システムサービス株式会社
東芝情報システム株式会社
東芝データ株式会社
東芝デジタルエンジニアリング株式会社
東芝デジタルソリューションズ株式会社
東芝デジタルマーケティングイニシアティブ株式会社
東芝テックソリューションサービス株式会社
東芝ビジネスエキスパート株式会社
東芝プラントシステム株式会社
みずほ東芝リース株式会社
UT東芝株式会社

ITセキュリティ評価・認証の取得状況

（独）情報処理推進機構（IPA）が運用するISO/IEC 15408※1に基づく「ITセキュリティ評価及び認証制度」または各国の認証制度によって認証された主な製品は、次のとおりです（2022年3月末現在）。

製　品	TOE※2種別	認証番号	適合するPP・保証要件
TOSHIBA e-STUDIO330AC/400AC ファクスユニットおよびFIPSハードディスクキット付モデル	デジタル複合機	C0684	PP適合(Protection Profile for HardcopyDevices 1.0 dated September 10, 2015)
TOSHIBA e-STUDIO2515AC/3015AC/3515AC/4515AC/5015AC/ ファクスユニット（GD-1370J/GD-1370NA/GD-1370EU）および FIPSハードディスクキット（GE-1230）付モデル	デジタル複合機	C0633	PP適合(Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015)
TOSHIBA e-STUDIO5516AC/6516AC/7516ACファクスユニット（GD-1370J/ GD-1370NA/GD-1370EU）およびFIPSハードディスクキット（GE-1230）付モデル	デジタル複合機	C0632	PP適合(Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015)
TOSHIBA e-STUDIO2018A/2518A/3018A/3518A/4518A/5018A ファクスユニット（GD-1370J/GD-1370NA/GD-1370EU）および FIPSハードディスクキット（GE-1230）付モデルSYS V1.0	デジタル複合機	C0631	PP適合（Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015）
TOSHIBA e-STUDIO5518A/6518A/7518A/8518A ファクスユニット（GD-1370J/ GD-1370NA/GD-1370EU）およびFIPSハードディスクキット（GE-1230）付モデル	デジタル複合機	C0630	PP適合（Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015）
TOSHIBA e-STUDIO2010AC/2510AC ファクスユニット（GD-1370J/ GD-1370NA/GD-1370EU）およびFIPSハードディスクキット（GE-1230）付モデル	デジタル複合機	C0629	PP適合（Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015）
TOSHIBA e-STUDIO3508LP/4508LP/5008LP、Loops LP35/LP45/LP50 MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V1.0	デジタル複合機	C0566	EAL2※3+
TOSHIBA e-STUDIO5508A/6508A/7508A/8508A MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V1.0	デジタル複合機	C0529	EAL3+
TOSHIBA e-STUDIO5506AC/6506AC/7506AC MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V1.0	デジタル複合機	C0528	EAL3+
TOSHIBA e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V1.0	デジタル複合機	C0524	EAL3+
TOSHIBA e-STUDIO2505AC/3005AC/3505AC/4505AC/5005AC MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V1.0	デジタル複合機	C0523	EAL3+
TOSHIBA e-STUDIO2000AC/2500AC MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V1.0	デジタル複合機	C0522	EAL3+
TOSHIBA e-STUDIO5560C/6560C/6570C MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V3.0	デジタル複合機	C0491	EAL3+
TOSHIBA e-STUDIO557/657/757/857 MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V3.0	デジタル複合機	C0490	EAL3+
TOSHIBA e-STUDIO207L/257/307/357/457/507 MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V3.0	デジタル複合機	C0489	EAL3+
TOSMART-GP1（Supporting PACE PP-0499）	ICs, Smart Cards and Smart Card-Related Devices and Systems	—	EAL4+
TOSMART-GP1（Supporting PACE and BAC PP-0500）	ICs, Smart Cards and Smart Card-Related Devices and Systems	—	EAL4+
Microcontrôleur sécurisé T6ND7 révision 4	ICs, Smart Cards and Smart Card-Related Devices and Systems	—	EAL4+
Toshiba T6NE1 HW version 4	ICs, Smart Cards and Smart Card-Related Devices and Systems	—	EAL4+
TOSMART-P080-AAJePassport	ICs, Smart Cards and Smart Card-Related Devices and Systems	—	EAL4+
TOSMART-P080 ePassport 01.06.04 + NVM Ver.01.00.01	ICs, Smart Cards and Smart Card-Related Devices and Systems	—	EAL4+
T6ND1 Integrated Circuit with Crypto Library v6.0	ICs, Smart Cards and Smart Card-Related Devices and Systems	—	EAL4+
FS Sigma Version 01.01.05	ICs, Smart Cards and Smart Card-Related Devices and Systems	—	EAL4+

※1　ISO/IEC 15408：情報技術セキュリティの観点から、情報技術に関連した製品およびシステムが適切に設計され、その設計が正しく実装されていることを評価するための国際標準規格です。
※2　TOE（Target Of Evaluation）：評価の対象となるソフトウェアやハードウェアなどの製品のことをTOEといいます。関連する管理者および使用者の手引書（利用者マニュアル、ガイダンス、インストール手順書など）を含むことがあります。
※3　EAL（Evaluation Assurance Level）：ISO/IEC 15408では、規定した評価項目（保証要件）に対する保証の度合いを、EAL1から7まで7段階のレベルで規定しており、段階が上がるごとに評価の内容が厳しくなります。

暗号モジュール試験・認証の取得状況

IPA が運用する ISO/IEC 19790※1 に基づく「暗号モジュール試験及び認証制度（JCMVP）」またはアメリカ国立標準技術研究所（NIST）とカナダ Communications Security Establishment（CSE）が運用する FIPS140-2※2 に基づく「Cryptographic Module Validation Program（CMVP）」によって認証された主な製品は、次のとおりです（2022年3月末現在）。

製　品	認証番号	レベル
暗号化機能搭載2.5型ハードディスクドライブ「MHZ2 CJ」シリーズ	J0006	Level1
東芝ソリューション暗号ライブラリ	F0001	Level1
Toshiba Secure TCG Opal SSC and Wipe technology Self-Encrypting Drive (MQ01ABU050BW, MQ01ABU032BW and MQ01ABU025BW)	F0022	Level2
Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (THNSB8 model)	2807	Level2
Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX model) Type B	2707	Level2
Toshiba TCG Enterprise SSC Self-Encrypting Hard Disk Drive (AL14SEQ model)	2508	Level2
Toshiba TCG Enterprise SSC Self-Encrypting Hard Disk Drive	2333	Level2
Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX model)	2262	Level2
Toshiba Secure TCG Opal SSC and Wipe technology Self-Encrypting Drive (MQ01ABU050BW, MQ01ABU032BW and MQ01ABU025BW)	2082	Level2

※1　ISO/IEC 19790：セキュリティ技術－暗号モジュールの試験および認証に関するセキュリティ要求事項を評価するための国際標準規格です。
※2　FIPS140-2：米国連邦政府の省庁等各機関が利用する、ハードウェアおよびソフトウェア両方を含む暗号モジュールに関するセキュリティ要件の仕様を規定する米国連邦標準規格です。

その他セキュリティ認証の取得状況

認証名称	製品名	レベル
アキレスコミュニケーション認証 (Achilles Communications Certification)	TOSMAP-DS/LX　OWB	Level2
	TOSMAP-DS/LX　OWR	Level2
ISA Secure® EDSA (Embedded Device Security Assurance) 認証	CIEMAC™-DS/nv（TOSDIC-CIEDS/nv）ユニファイドコントローラnvシリーズtype2	EDSA2010.1 Level1

持続可能な開発目標（SDGs）達成に向けて

世界経済フォーラムの2019年度版「グローバルリスク報告書」で、発生の可能性が高いグローバルリスクのトップ5に大規模なサイバー攻撃やデータの大量漏えいがあげられています。そのため、デジタルトランスフォーメーションを進める製造業においてもIT/OT（Operation Technology）/IoTのサイバーセキュリティに対する取り組みが必須です。東芝グループでは、製品やシステムのライフサイクル全体のセキュリティに対する考え方を示し、サイバーセキュリティ体制を強化するなかで、以下の4つの観点でSDGsに貢献します。

目標9：イノベーション
サイバー／フィジカル両面からのセキュリティ対策を進め、高度化するサイバー攻撃に対応します。

目標11：スマートな都市
スマートな都市を実現する社会インフラの安心・安全をセキュリティ技術で支えています。

目標12：持続可能な消費と生産
サプライチェーンの信頼性を確立し、グローバルなバリューチェーンの価値創造をめざします。

目標17：パートナーシップ
グローバルなセキュリティベンダーとのパートナーシップにより、常に最新のセキュリティ対策を取り入れます。

東芝グループの事業概要

2022年3月31日現在

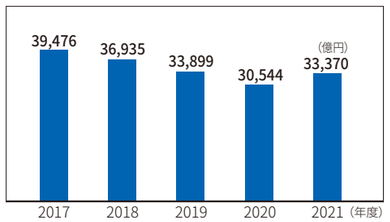
会社概要

社　　名　株式会社 東芝
（TOSHIBA CORPORATION）
本社所在地　東京都港区芝浦1-1-1
創　　業　1875年（明治8年）7月
資 本 金　2,008億6,900万円

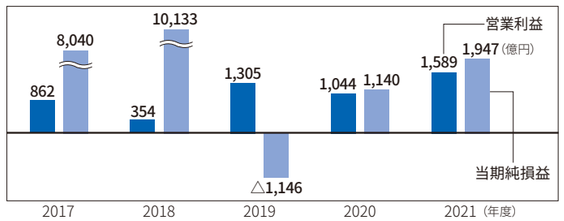
連結売上高　3兆3,370億円（2021年度）
連結従業員数　116,224人
発行済株式総数　4億3,314万株
上場証券取引所　東京、名古屋

業績（連結）

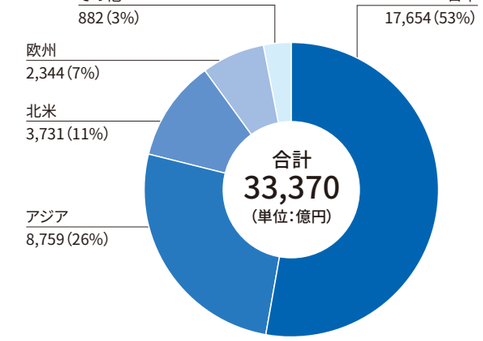
売上高の推移



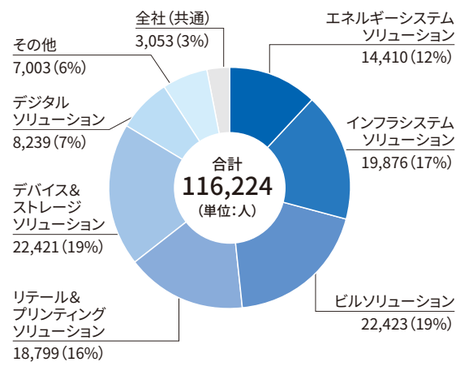
営業利益／当期純利益（損失）の推移



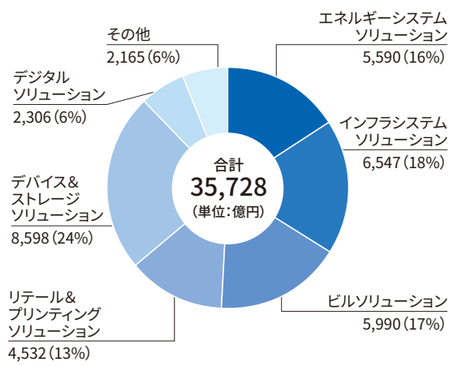
地域別売上高



セグメント別従業員数



セグメント別売上高



（セグメント間の内部売上高消去2,358億円含む）

人と、地球の、明日のために。

株式会社 東芝

〒105-8001 東京都港区芝浦1-1-1

お問い合わせ先

技術企画部　サイバーセキュリティセンター

TEL:03-3457-2128　FAX:03-5444-9213

e-mail : HDQ-TOSHIBA-SIRT@ml.toshiba.co.jp

東芝サイバーセキュリティ ウェブサイト

https://www.global.toshiba/jp/cybersecurity/corporate.html

2022年6月発行

Printed in Japan