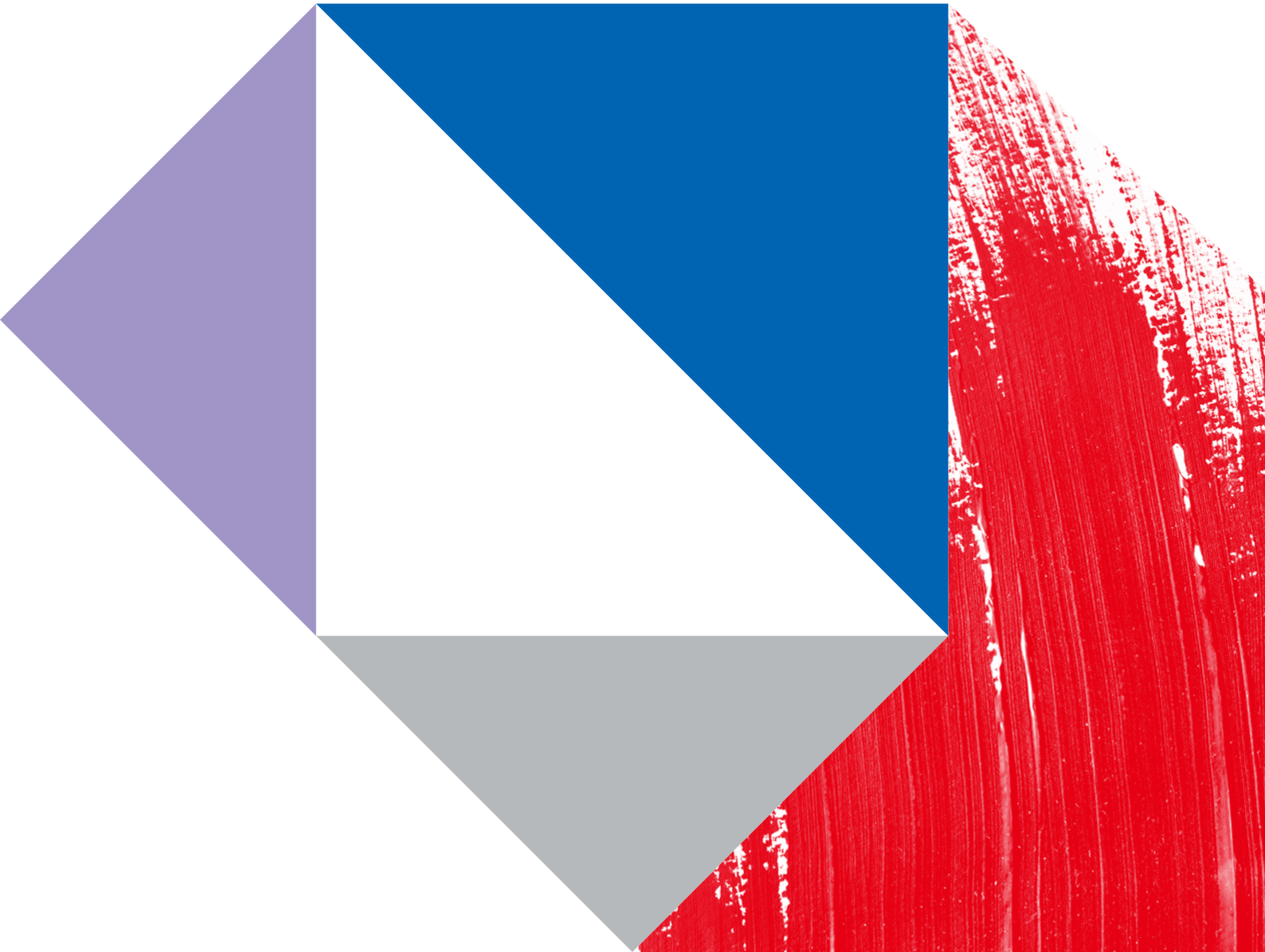
TOSHIBA

2020 サイバーセキュリティ報告書

Cyber Security Report



最高情報セキュリティ責任者（CISO）メッセージ

サイバーとフィジカルの安心・安全を、すべての人に

近年、ICT技術はあらゆる分野において高度に進化、あるいは深化しつつ、人々の暮らしを支えています。なかでも、デジタル技術は物理空間を超えた情報共有・コミュニケーションを可能にし、我々のライフスタイルや社会インフラに大きな変革をもたらしています。東芝グループは、1875年の創業以来、145年間継続している「ものづくり」で得た知見と経験にこのデジタル技術を組み合わせ、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を中心とした事業に取り組んでいます。これらの事業運営にあたり、最も優先すべきことは「すべての人々に安心・安全をお届けすること」であると考えています。

インターネットをはじめとする仮想世界（サイバー空間）と、人々が暮らす実世界（フィジカル空間）は、IoT技術の発展とともに融合しつつあります。こうした社会システムの変化を踏まえ、東芝グループは、“サイバー・フィジカル・システム（CPS）テクノロジー”で人々の暮らしを支えることを目標に掲げています。フィジカル空間で得たさまざまな情報をサイバー空間で分析し、価値あるインテリジェンスを新たに生み出し、それを再びフィジカル空間で活用するCPSにおいて、「サイバー空間のセキュリティを守ること」は、同時に「フィジカル空間のセキュリティを守ること」につながると考えています。高度化、多様化するサイバー攻撃に対して、セキュアにCPSを構築・提供することにより、社会をサイバー犯罪から守り、人々に安心・安全をお届けしていきたいと考えています。

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
執行役常務・CISO

石井 秀明

TOSHIBA

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**安心と安全**を提供してまいりました。140年以上の歴史を持つモノづくり企業として、電力供給や公共交通などの設計・運用や、半導体部品、大型プラントなどの製品開発で培った経験と知識は、サイバー犯罪に立ち向かう大きな武器となります。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するとともに、情報漏えい・不正利用を防止します。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。

2020 サイバーセキュリティ報告書
Cyber Security Report

目次

Chapter 1

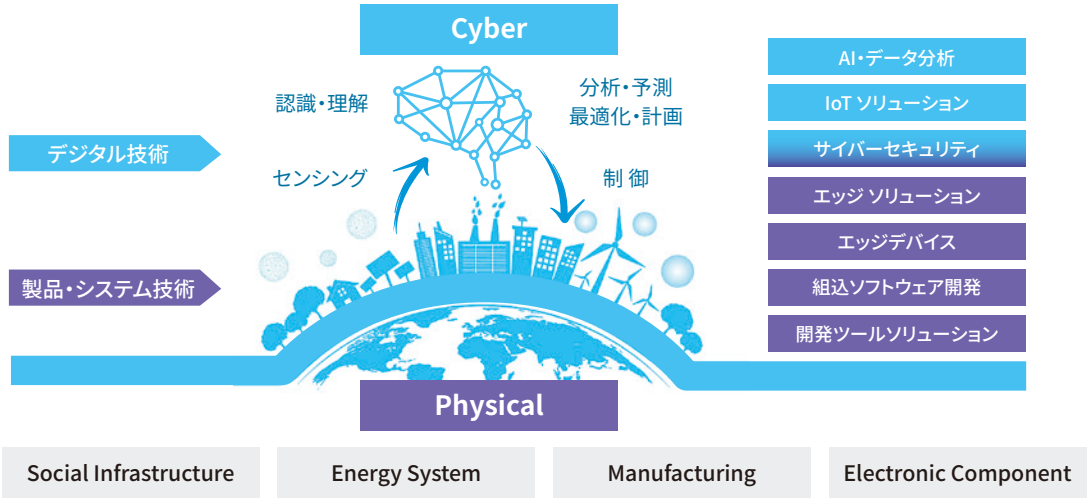
ビジョン・戦略

東芝グループは、サイバーとフィジカル（実世界）が融合した技術で社会課題を解決する、世界有数のCPSテクノロジー企業をめざしています。一方で、IoT（Internet of Things）を活用したデジタルトランスフォーメーションの進展を背景に、実世界のさまざまなモノがネットワークにつながることで、サイバー攻撃の脅威が情報システムだけでなく制御システムや製品にもおよび、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ます。

東芝グループは、サイバーとフィジカルの融合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フィジカルの知見と、約13万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、製品・システム・サービスの安心と安全の提供、事業の継続性確保をめざした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

東芝グループがめざすCPSテクノロジー企業



CPSとは、フィジカル（実世界）におけるデータを収集し、サイバー空間でデジタル技術などを用いて分析したり、活用しやすい情報や知識に加工してフィジカル側にフィードバックしたりすることで、新しい価値を創造する仕組みです。

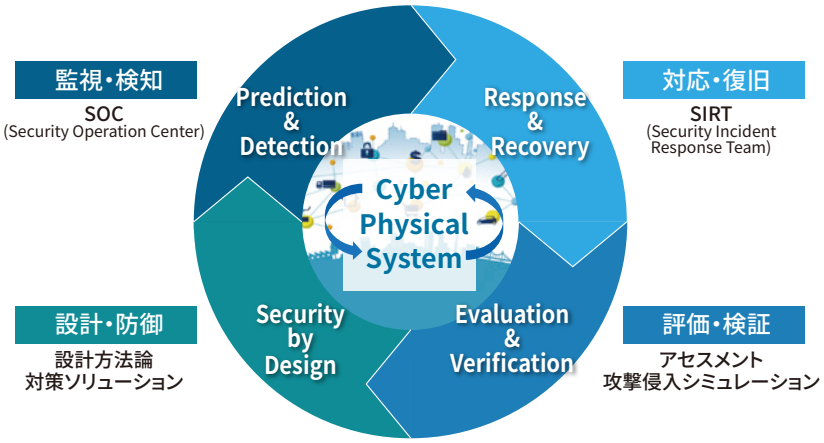
東芝グループは、さまざまな社会インフラ事業を中心に膨大な知見を持ち、長年の事業活動で蓄積したデータを持っています。また、世界をけん引してきたハイレベルなサイバー技術も保有しています。このようなことから、創業以来の歴史で培われたフィジカルの技術力とサイバー技術を融合することで新しい価値を創造するCPSを実現し、多様な分野で技術革新を起こすCPSテクノロジー企業をめざしています。そして、社会インフラのデジタルトランスフォーメーションを推進し、エネルギー需要増加、資源の枯渇、気候変動、都市への人口集中、物流の拡大、高齢化や労働力不足といった社会課題を解決していきます。

東芝グループのサイバーセキュリティビジョン

産業や社会の幅広い分野で、IoT、AI、クラウドなどのデジタル技術を活用したCPSによるデジタルトランスフォーメーションが進展する一方、モノがネットワークにつながることで、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、物理的な被害に遭うリスクが増大しています。そのような状況でも、東芝グループの使命はこれまでと変わらず、お客さまの事業継続を支え、安心で安全な社会を実現することです。そのためには、CPS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、サービスのセキュリティを確保する取り組みを進めています。さらに、設計・開発におけるSecurity by Design※に基づく防御にとどまらず、常に社内外の脅威を監視することでリスクを予測し、インシデント発生時には迅速な対応で被害の最小化と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、設計・開発にフィードバックしていく「セキュリティライフタイムプロテクション」で持続的なセキュリティ確保を実現します。

※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

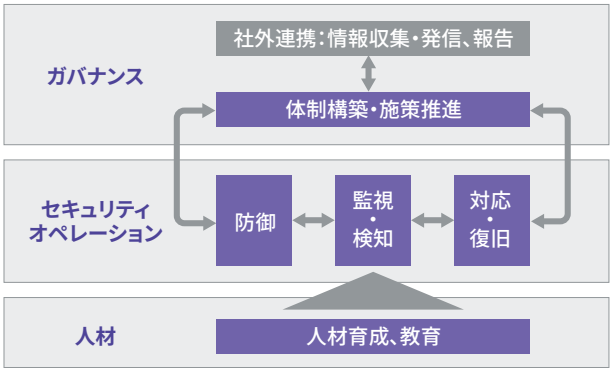
東芝グループでは、この「セキュリティライフタイムプロテクション」の実現に向け、サイバーセキュリティマネジメントプロセスを「ガバナンス」「防御」「監視・検知」「対応・復旧」「評価・検証」「人材」の6つの機能が有機的に結合したプロセスとして定義しました。そして、めざすゴールを「東芝サイバーセキュリティビジョン」として定めました。これにより、東芝グループの製品やサービスを安心してご利用いただけるようサイバーセキュリティの取り組みを強化し、信頼されるパートナーとなるように努めてまいります。

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
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が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

サイバーセキュリティマネジメントプロセスの持続的な運用と、継続的な強化をめざし、東芝グループのセキュリティ態勢強化に向けた戦略を推進しています。ここでの“セキュリティ態勢”とは、広く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、意思決定・指揮系統を明確化するガバナンス、監視・検知／対応・復旧／防御などのセキュリティオペレーション、そして、これらを運用・発展していく人材の3つの要素から構成され、これら要素を十分連携・活用できるよう強化、常態化することです（右図参照）。



サイバーセキュリティマネジメントプロセス

ガバナンスの強化では、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（当時は東芝社長、現在はCEO）から権限移譲され、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、東芝グループ会社への対応指示を迅速かつ適切に実施する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、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。さらに、CSIRT／PSIRT両者の対応プロセスや人材の共通化、ノウハウの共有化により、製造業としての高度なサイバーセキュリティをめざしています。そして、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、社内外の情報共有も積極的に推進しています。ほかにも、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、ガバナンス強化を推進しています。

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、セキュリティ運用基盤CDMP（Cyber Defense Management Platform）の構築を進めています。東芝グループを取り巻くセキュリティの脅威は増大する一方であり、保護すべき対象は、社内ITインフラだけでなく、工場などの生産設備やお客さまに提供する製品・システム・サービスをはじめ、将来的にはお客さまやお取引先さまのシステムにまで広がっています。しかし、セキュリティオペレーション人材には限りがあり、少ない人材でも精度の高いセキュリティオペレーションを実現するための運用基盤が必要です。そこで、さまざまな保護対象のセキュリティ監視や、セキュリティリスクの検知・予測、検知されたインシデントへの対応・復旧を自動化するためにCDMPの構築を進めています。さらに、社内外の脅威インテリジェンスの収集活用やナレッジの蓄積、AI活用を積極的に進め、検知・対応の迅速性と正確性を向上させるとともに、サイバー攻撃に対するリアクティブな対応からプロアクティブな予測・対応への転換を図り、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。

人材育成の強化では、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ました。同センターは、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、運用支援までを一貫して行う組織です。「サイバーセキュリティセンター」と連携し、製品開発におけるセキュリティ技術支援や共通セキュリティ基盤技術の開発・整備を行うとともに、専門人材の育成と強化を推進しています。また、東芝グループ全体のセキュリティレベルの向上をめざし、社内のセキュリティ教育体系を整備するとともに、個人情報を含む情報の管理・保護を目的とした情報セキュリティ教育、製品・システム・サービスに関する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。

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

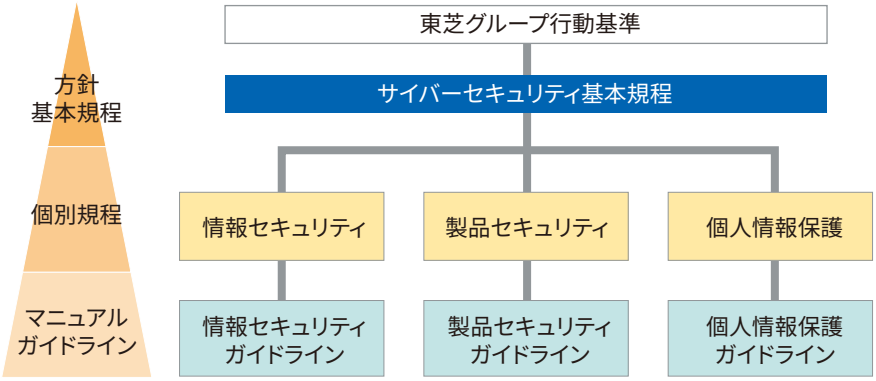
※1 Computer Security Incident Response Team
※2 Product Security Incident Response Team

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、安心・安全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。

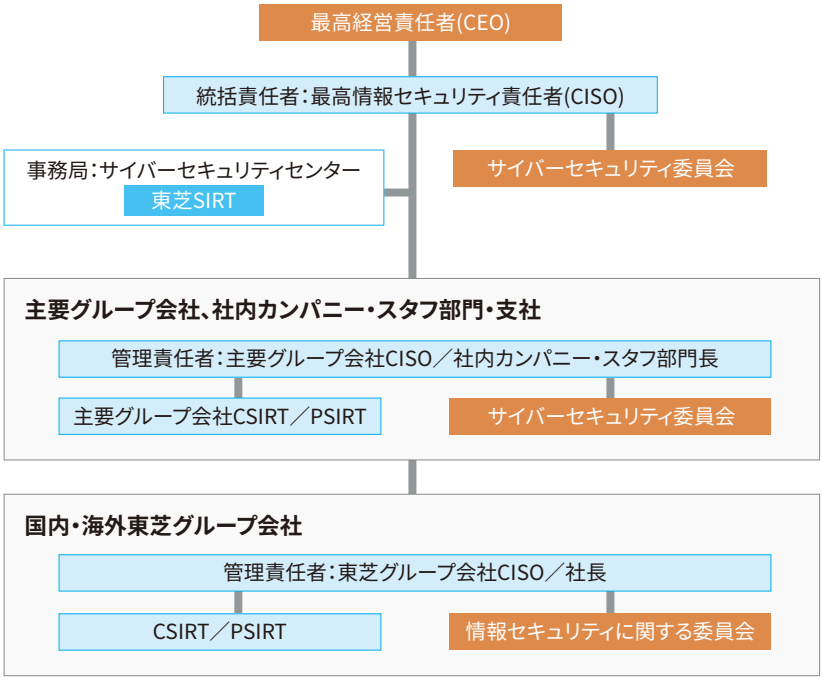
東芝個人情報保護方針（全文） http://www.toshiba.co.jp/privacy

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、サイバーセキュリティにかかわる体制や施策を検討・立案し、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。サイバーセキュリティ委員会では、東芝グループ全体のサイバーセキュリティ管理の徹底に必要な事項および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審議を行います。

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、主要グループ会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。さらに、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対応などに加えて、また、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

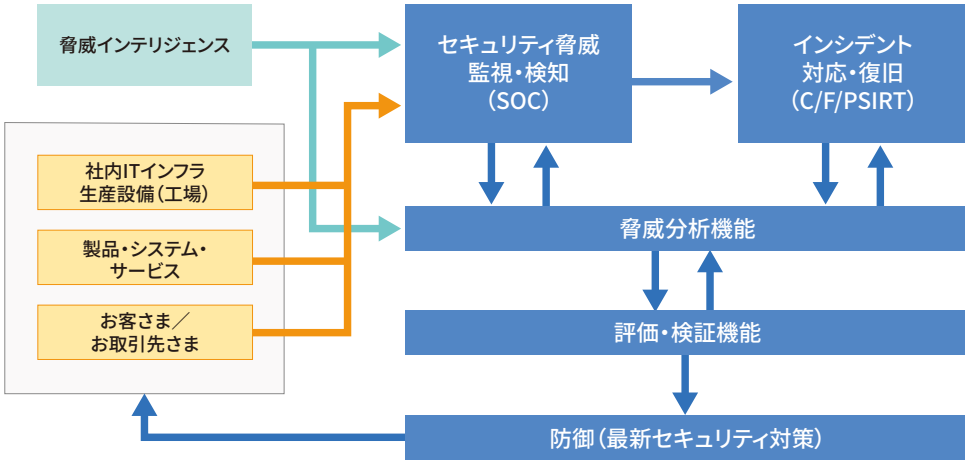
セキュリティオペレーション

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、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と呼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、セキュリティに対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。



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

CDMP (Cyber Defense Management Platform)

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.11参照)
・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.13、P.22参照)
・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止(P.19参照)
	⇒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.14参照)
・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.16参照)

東芝グループ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) と呼ばれる自動化プラットフォームの導入を進めています。

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。東芝グループでは、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るほか、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も進めています。

情報セキュリティ・個人情報保護教育

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に対する意識を高く持つことが重要です。日本がEUから受けた個人データの移転に関する十分性認定など、最新情報を取り込んだe-Learning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、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。さらに、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情報セキュリティ・個人情報保護教育を実施しています。

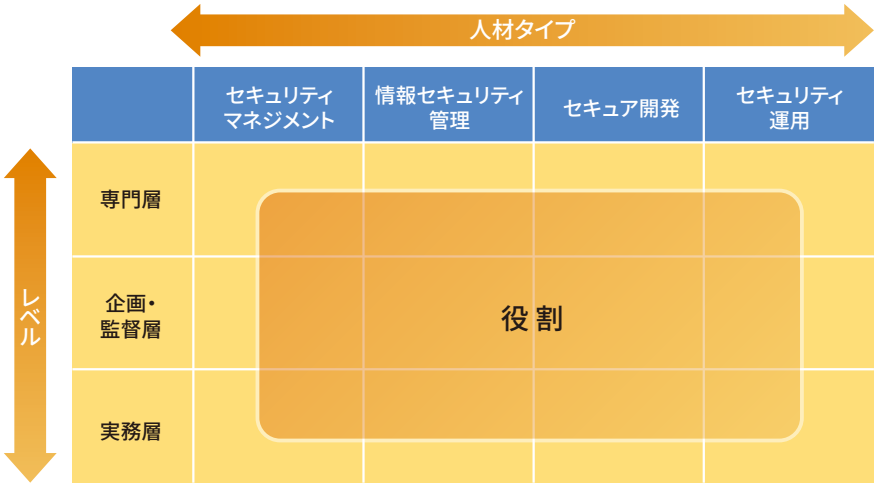
また、従業員一人ひとりが東芝グループの規程やルールを十分理解したうえで行動できるよう、日常業務のなかで理解すべきルールや注意点を平易にまとめた情報セキュリティハンドブックを作成しています。

製品セキュリティ教育

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、実践する必要があると考えています。そこで、情報セキュリティ教育と同様に、東芝グループのすべての役員と従業員を対象に、毎年製品セキュリティに関するe-Learningを実施しています。

高度なセキュリティ人材の育成

上記の教育のほか、東芝グループとして必要なセキュリティ人材像を定義し、担当業務に応じた人材タイプや役割レベルに応じて育成しています。専門知識や技術を持つ人材だけでなく、日々の業務において、製品開発時のセキュリティ向上、脆弱性やインシデントにすばやく対応できる人材の育成、管理職向けの製品セキュリティ教育なども行っています。



セキュリティ人材像

Chapter 2

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・サービスに分けてご紹介します。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

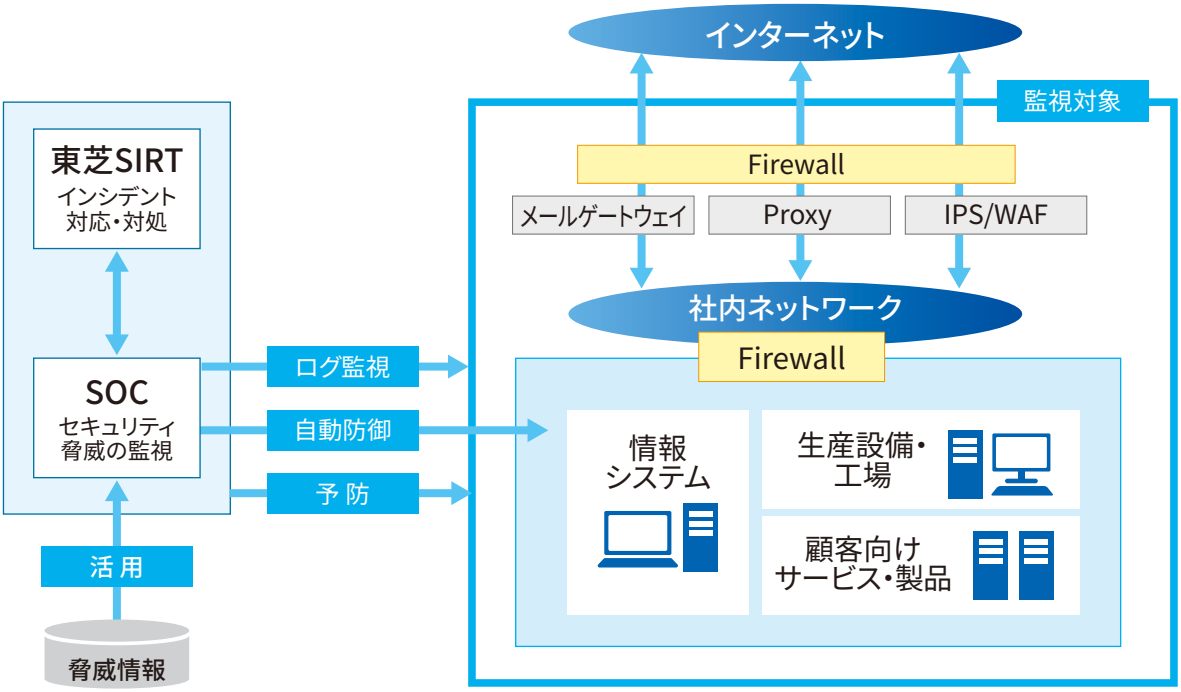
サイバー攻撃が巧妙化・高度化するなか、SOC（Security Operation Center）によるセキュリティ脅威の監視・検知、CSIRTによるインシデント対応・復旧を行い、お客さまの情報資産を適切に管理しています。また、毎年国内外の東芝グループ全組織に対し自主監査・アセスメントを行い、指導しています。

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Firewall、IPS、Proxy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っています。しかも、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ねらった計画的で標的型の攻撃に変化していることから、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。セキュリティリスクを早く、しかも正確に検知するため、SOCがインターネットの出入口、社内のPCおよびサーバ等のITシステム、工場、顧客向けサービスを監視し、アラートを検知した場合に速やかに対処し、被害最小化をめざします。また、外部の脅威情報を活用し、攻撃の予防と東芝グループ全組織のセキュリティ強化につなげます。

具体的には、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ひとつで、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)：Web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

インシデント対応への取り組み

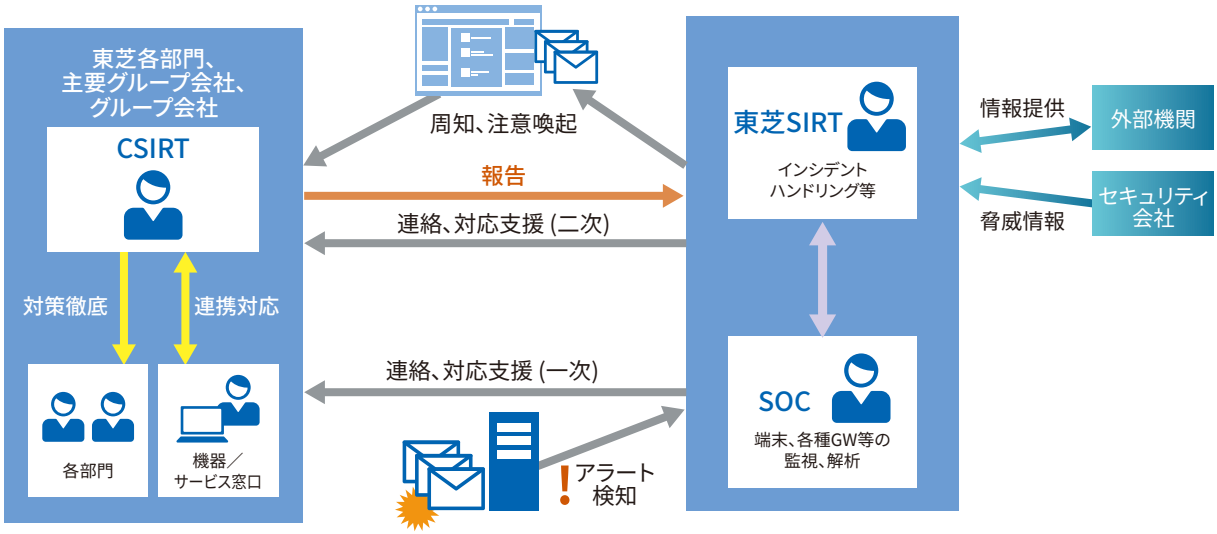
対応
復旧

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は、確実で速やかに対応が行われるようにしています。SOCがアラートを検知した場合は、東芝SIRTとの連携はもとより、該当する各部門・各社のCSIRTへも直接連絡し、より迅速な対応を可能としています。

※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、各部門および各社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、各部門や各社の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の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し、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、ウイルス拡散時のネットワーク遮断など、事業に影響を及ぼす対策であっても、実施内容や実施基準を明確化し、あらかじめ東芝グループ内に周知することで迅速な対応ができ、被害の最小化を図っています。

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。

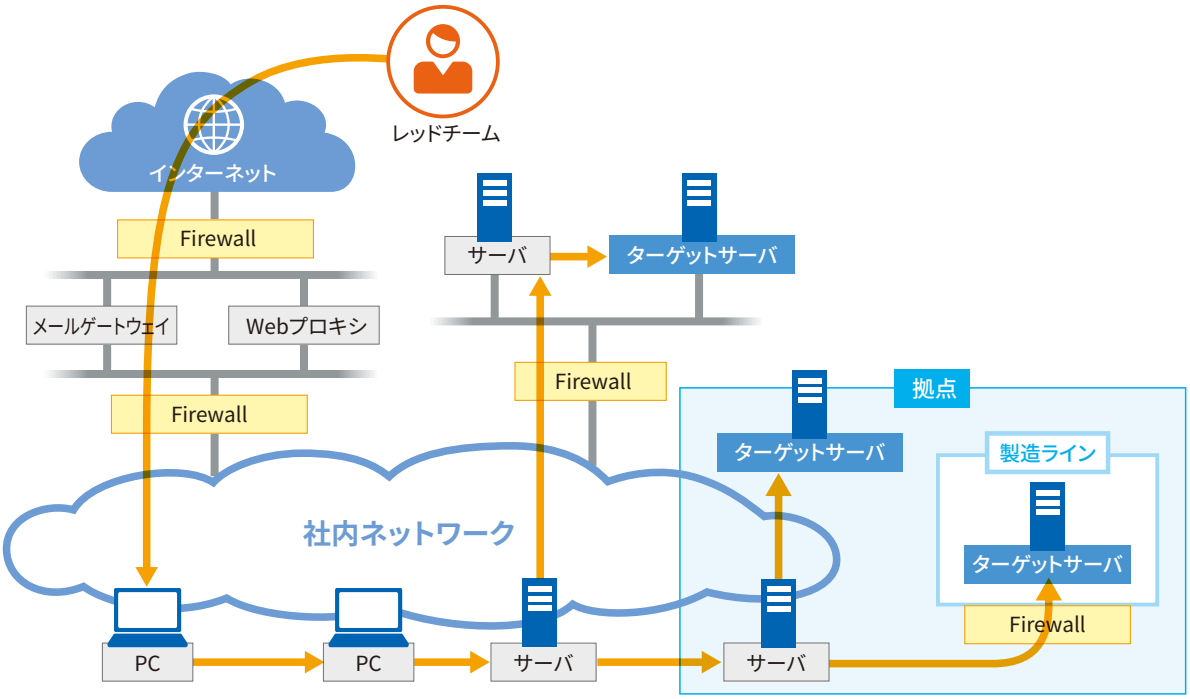
ハッカー視点の高度な攻撃・侵入テスト

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・侵入テストを実施し、東芝グループのセキュリティ施策の実効性を確認しています。今後も定期的に実施してまいります。

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。

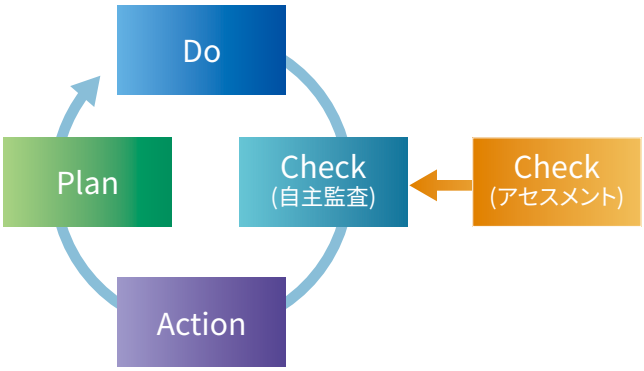
※レッドチーム：攻撃者がどのように対象組織を攻撃するかの観点で、セキュリティ体制や対策の有効性を確認するチーム



自主監査・アセスメント

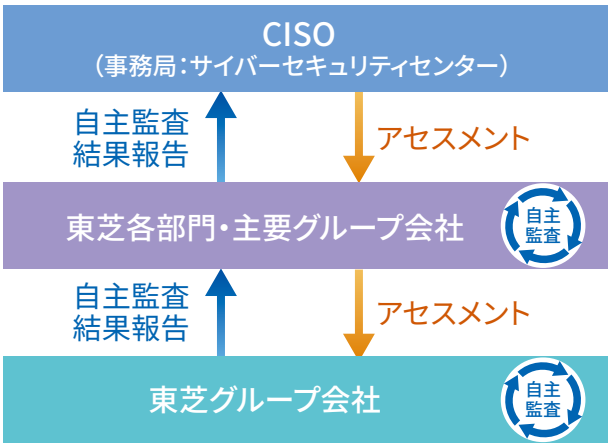
評価
検証

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。



自主監査・アセスメントを軸にPDCAサイクルを回す

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・支援します。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、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。

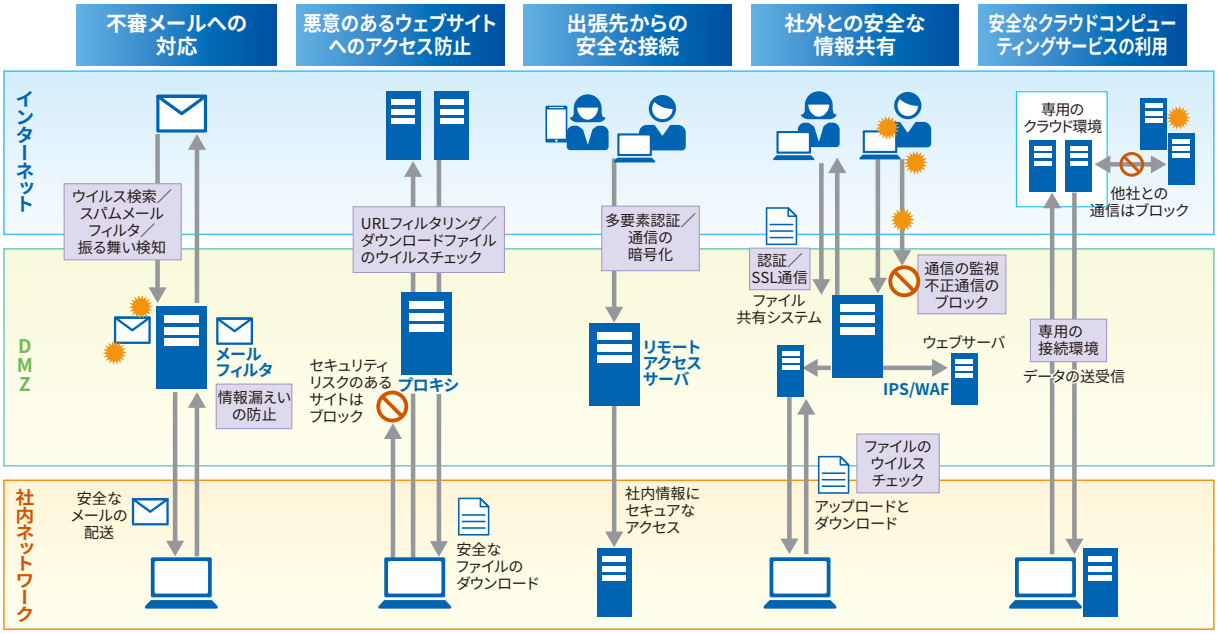


東芝グループ全体で自主監査・アセスメントを実施

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1日平均約250万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で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。



- 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)：Web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外部からの脅威と内部から発生する情報漏えいなどの二方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、1日平均約50万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フィルタを使い、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。また、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、通信の暗号化を実践しています。また、在宅勤務やテレワークにも仮想デスクトップと併わせて活用し、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うえで、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。

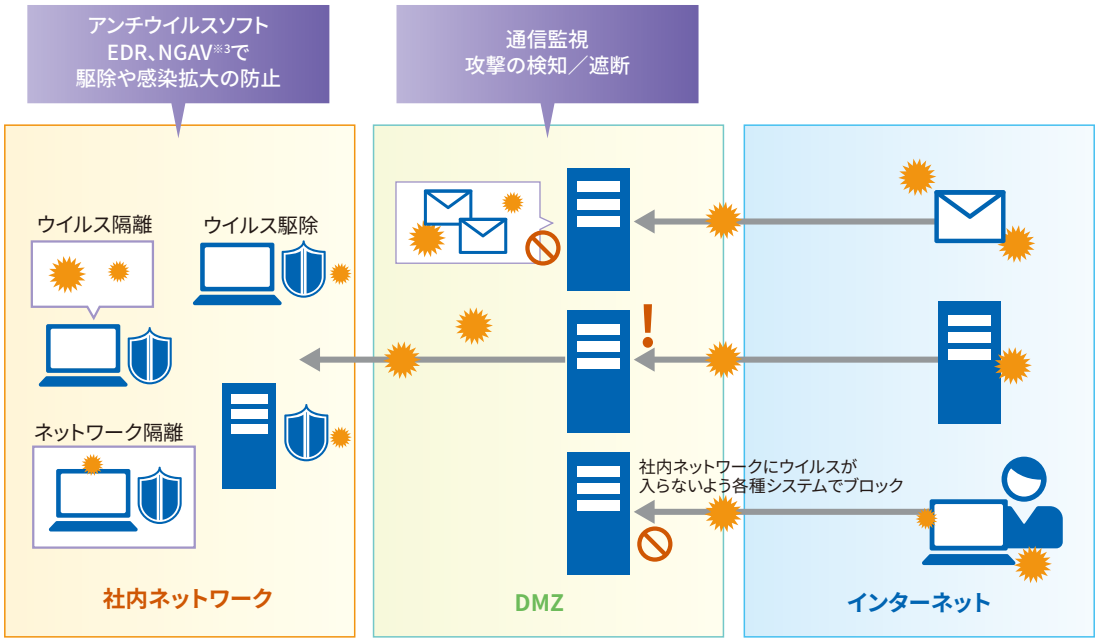
上記の東芝グループ共通のセキュリティ対策のほかに、個別にインターネット接続点を持っている拠点では、セキュリティ機器の設定や重要拠点におけるネットワークログを監視しています。共通施策だけではなく、事業や情報の重要度に合わせた対策を行うことで攻撃からの防御を徹底しています。現在は、情報システムの対策を中心に行っていますが、今後はそのノウハウを活用し、工場や顧客向けサービスなどのセキュリティ対策強化に取り組みます。

EDR※1ツールによるエンドポイント※2対策の強化

設計
防御

これまでの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、EDRツールの導入を進め、国内のPC、サーバへの展開が完了しました。引き続き海外へのツール展開を進めています。

・従来のウイルス対策製品で検出できない未知ウイルス感染等による不審な挙動の検知
・感染端末をネットワークから外すことなく、SOCがリモートで隔離
・収集した操作ログから、原因や被害範囲の追跡



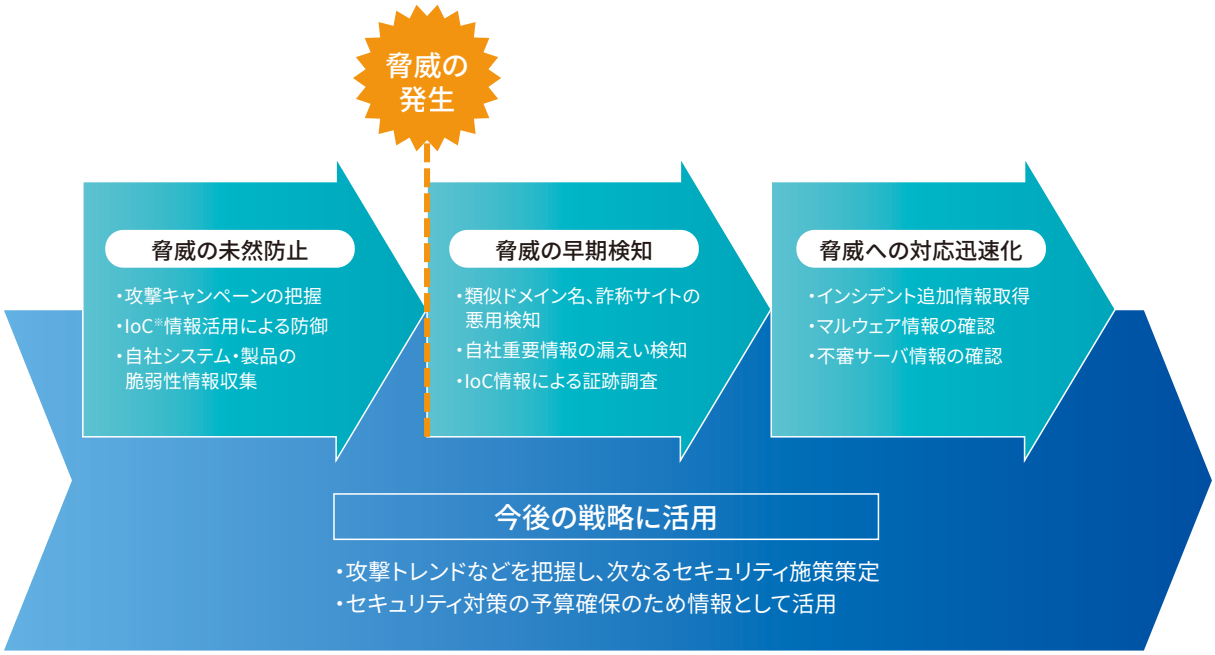
EDRツールの導入イメージ

※1 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
※3 NGAV：Next Generation Anti-Virus（次世代アンチウイルス）

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は、東芝グループを取り巻く脅威に対する未然防止、脅威発生後の早期検知と対応の迅速化に活用しています。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

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。

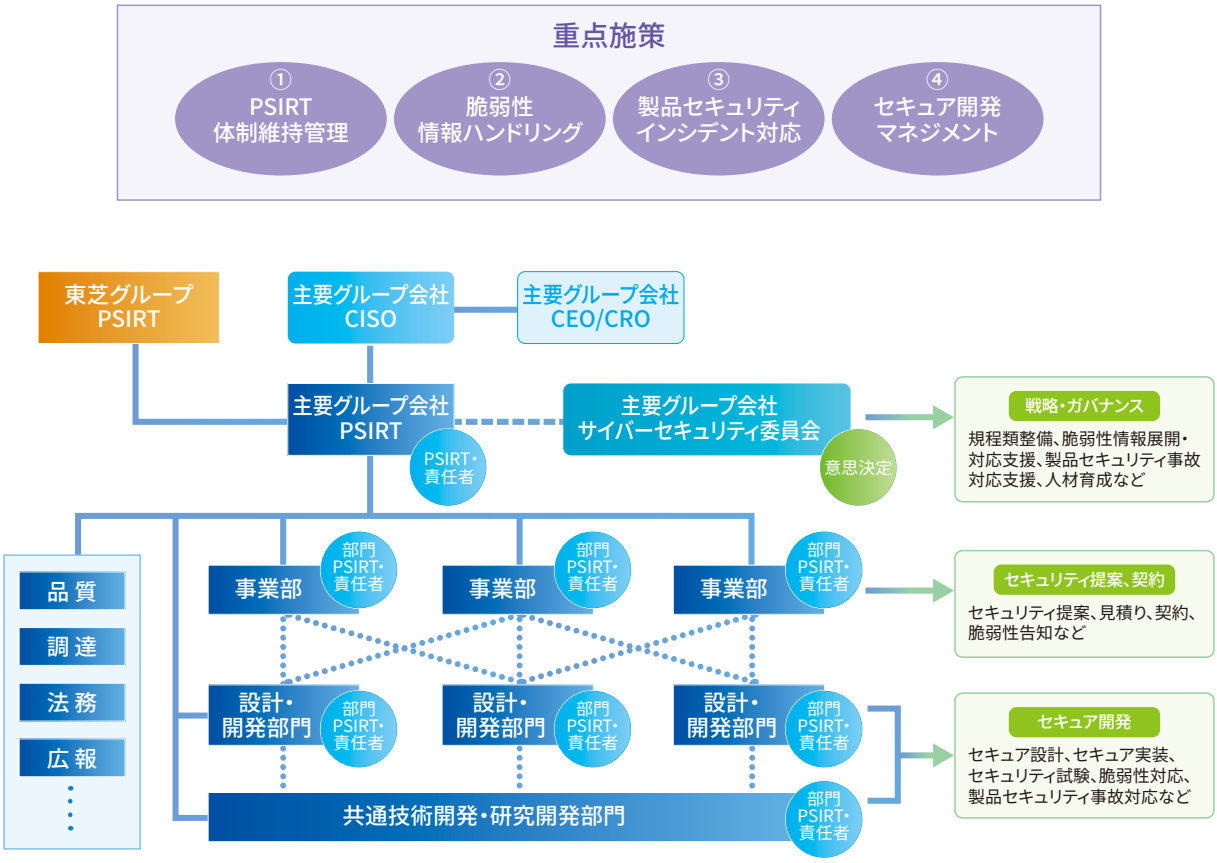
製品セキュリティを確保するための取り組み

設計 防御

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、東芝製品で利用される外部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

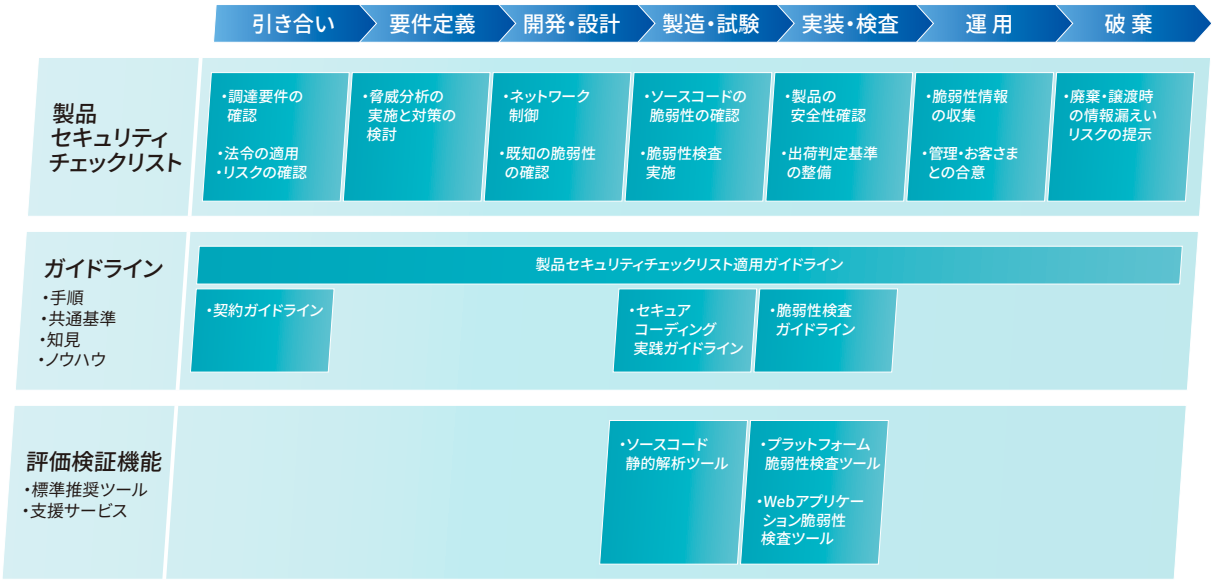
東芝グループの製品セキュリティ強化のため、4項目の重点施策を定義し、各社で構成する製品セキュリティマネジメント体制のもと、リスクベースの優先順位付けに基づく製品セキュリティ態勢強化計画を策定しました。これにより、全社施策を開発現場である各社の事業部門、設計・開発部門まで確実に行き渡らせる実効性と、自律的組織運営を実現します。



製品セキュリティリスクマネジメント体制

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、チェック項目をまとめた「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する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、東芝グループで一貫した製品セキュリティの確保を進めています。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きます。



「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）」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、「お取引先様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

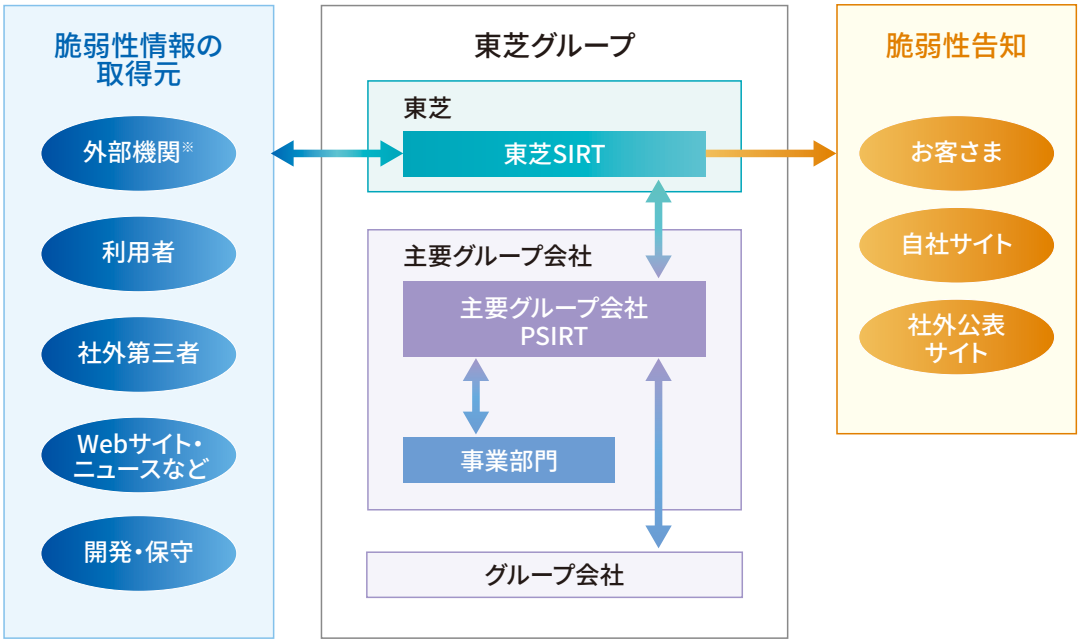
対応
復旧

東芝グループ全体で、一貫した迅速な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「ソフトウェ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。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。

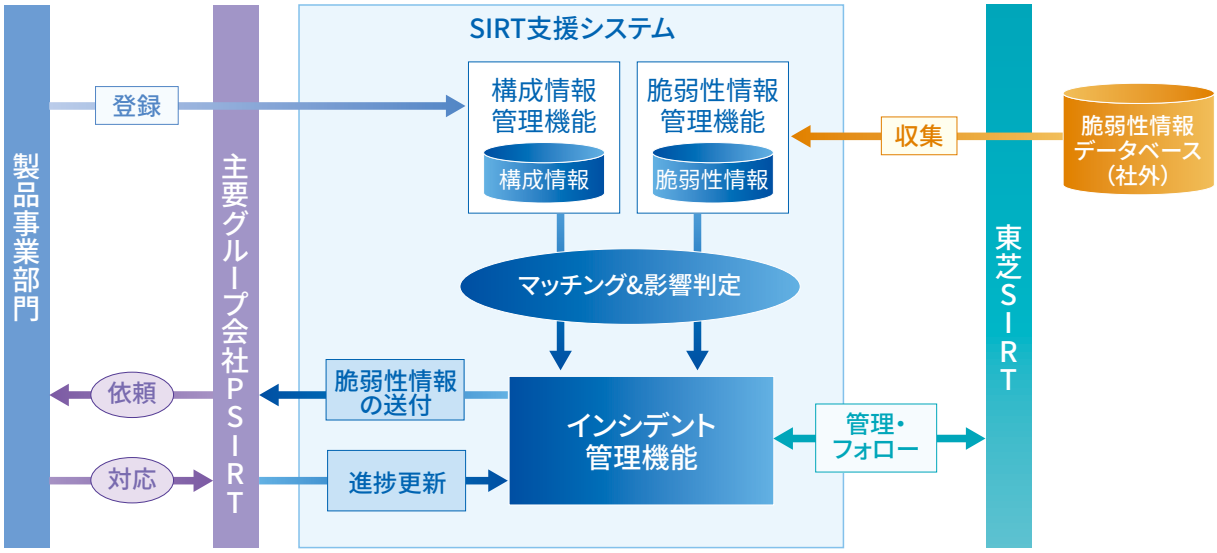


※外部機関：JPCERT/CC、JVN、ICS-CERTなど

東芝グループ脆弱性対応の体制

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、および影響レベルを判定し、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

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。

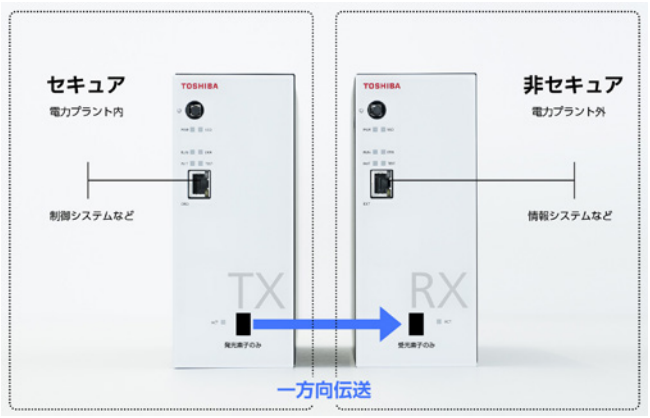
一方向伝送装置　TOSMAP-DS™／LX OWB

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

ISASecure®EDSA※1認証を取得した産業用コントローラ「ユニファイドコントローラnvシリーズ type2」

東芝インフラシステムズ(株)

近年、重要インフラを標的としたサイバー攻撃報告が増加し、基幹である制御システムのセキュリティ対策や管理の重要性が高まっています。東芝インフラシステムズ(株)の「ユニファイドコントローラnvシリーズ」は、社会インフラや産業システムなどの分野において多くの納入実績があります。そのなかでtype2は、一般産業システム分野向けに当社が展開している計装制御システム「CIEMAC™-DS/nv」のなかで使用される計装用コントローラです。このユニファイドコントローラにセキュリティ機能を実装し、セキュアな制御システムを実現しました。

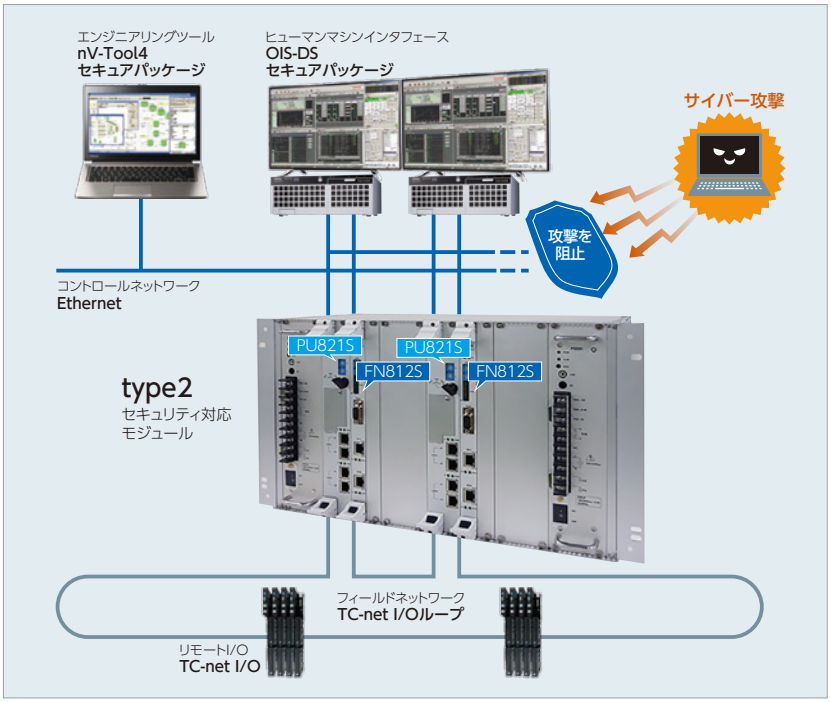
米国ISCI※2がスキームオーナーであるISASecure®EDSA認証は、制御機器(組み込み機器)のセキュリティ保証に関する認証制度で、事業者の調達要件として盛り込まれる傾向にあります。同認証は国際規格IEC 62443シリーズに統合される見込みでもあり、さまざまな業界から注目されています。EDSA認証の評価は、「ソフトウェア開発の各フェーズにおけるセキュリティ評価(SDSA※3)」「セキュリティ機能の実装評価(FSA※4)」「通信の堅牢性テスト(CRT※5)」という3つの評価項目からなっています。ユニファイドコントローラnvシリーズtype2は、国際的に認められた第三者認証機関であるCSSC※6認証ラボラトリーによる審査に合格し、ISASecure®EDSA認証を取得しました。

ユニファイドコントローラnvシリーズtype2のセキュリティ対応モジュールは、通信路／制御データ・パラメータの暗号化、認証などのセキュリティ機能を搭載しています。これらのセキュリティ機能により、外部攻撃者からのサイバー攻撃に耐え、エンジニアリングツール、ヒューマンマシンインタフェースとは通信を継続し、制御動作も確実に行います。

ユニファイドコントローラ
nvシリーズ type2

EDSA認証を取得したtype2を採用いただくことで、計装制御システム「CIEMAC™-DS/nv」を、よりセキュアに構築することが可能です。

IoT時代の到来により、制御システムやコンポーネントに対して期待される機能や役割が拡大し、安全かつセキュアなシステム構築の重要性が増しています。今後もセキュアで信頼性の高い製品のラインアップを拡充し、安心・安全で信頼できる持続可能な社会の実現に向けて貢献していきます。



制御システムの構成例

※1　ISASecure®EDSA：ISAセキュリティ適合性協会によるEDSA(Embedded Device Security Assurance)制御機器のセキュリティ保証に関する認証制度
※2　ISCI：ISA Security Compliance Institute(ISAのメンバーのコンソーシアムにより創設されたEDSA認証の制度運営元)
※3　SDSA：Software Development Security Assessment(ソフトウェア開発の各フェーズにおけるセキュリティ評価)
※4　FSA：Functional Security Assessment(機能セキュリティ評価)
※5　CRT：Communication Robustness Testing(通信の堅牢性テスト)
※6　CSSC：Control System Security Center(制御システムセキュリティセンター)

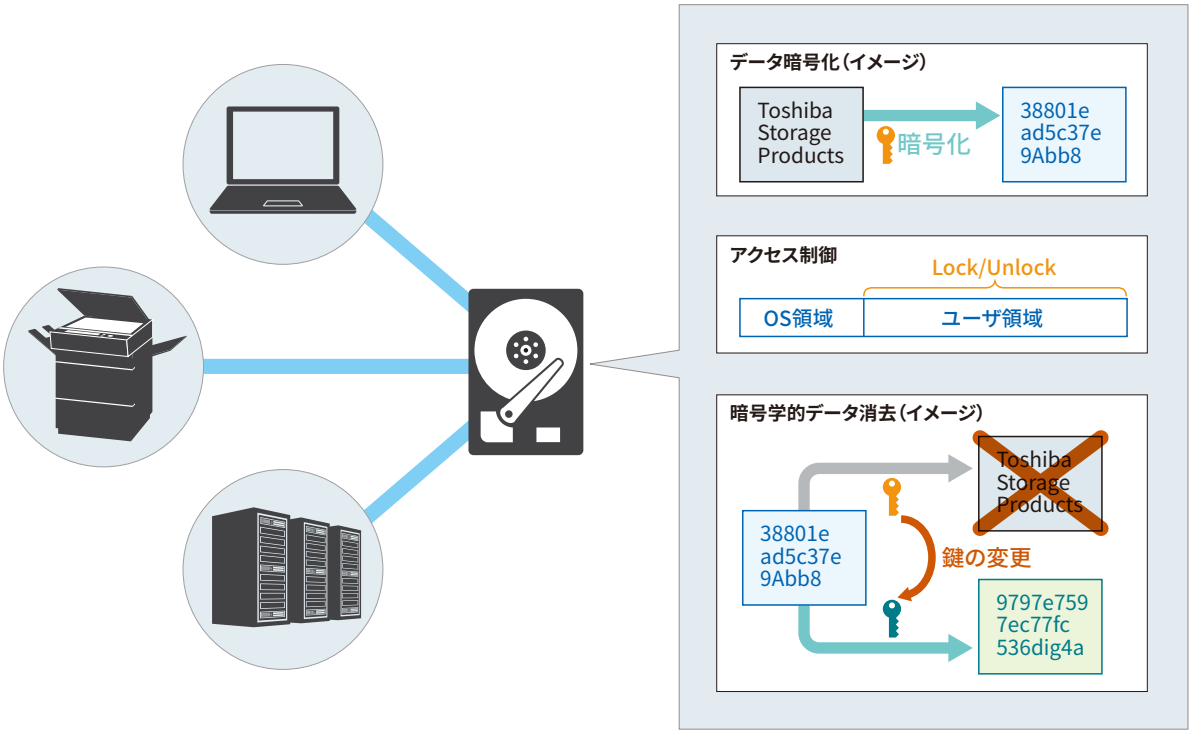
ストレージ製品へのセキュリティ機能の実装

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。東芝デバイス&ストレージ(株)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。当社ではこうしたお客さまのニーズに応えるため、自己暗号化ドライブ(SED※1)を開発し、提供しています。MQ01ABU***BWシリーズ※2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※3(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※4を用いています。またATA※5 Security Feature SetやTCG※6 Opal SSC※7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)や、当社独自暗号技術であるWipe Technology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。本製品は、米国政府および日本政府それぞれの暗号モジュール認証であるCMVP※8認証(#2082)とJCMVP(Japan CMVP)認証(#F0022)を取得しており、高い信頼性を第三者評価によって保証されています。これらの認証は、デジタル複合機向け暗号HDDのセキュリティ要件でもあり、デジタル複合機ベンダーのセキュリティ認証取得を容易にする効果もあります。



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 MQ01ABU***BWシリーズ: MQ01ABU050BW/MQ01ABU032BW
※3 NIST: National Institute of Standards and Technology
※4 AES: Advanced Encryption Standard
※5 ATA: Advanced Technology Attachment
※6 TCG: Trusted Computing Group
※7 SSC: Security Subsystem Class
※8 CMVP: Cryptographic Module Validation Program

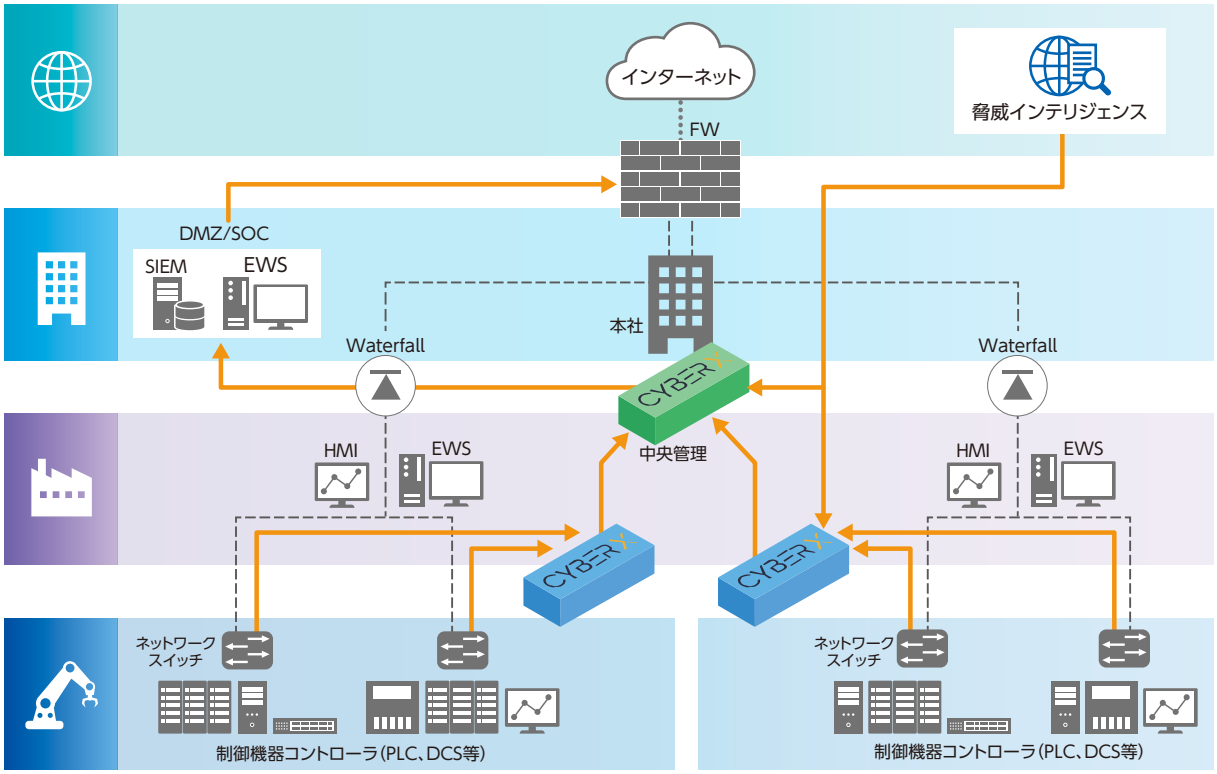
制御システム向けサイバーセキュリティ・プラットフォーム「CyberX Platform」

東芝デジタルソリューションズ（株）

「CyberX Platform」は、制御システムの資産識別、サイバーセキュリティ対策、統合管理を実現するソリューションで、世界で3000ヶ所以上のエネルギー、産業等の社会インフラで導入実績がある制御システム向けサイバーセキュリティ・プラットフォームです。

「CyberX Platform」は、これまでドキュメントで管理されていた制御ネットワークの最新状況の把握から、不正接続の監視、異常通信の検出、異常通信の原因分析までをリアルタイムに実施し、資産管理コストの削減とダウンタイムの予防を実現します。

特徴としては、①資産識別と可視化による通信トラフィック分析により情報資産を学習、自動でデバイスを検出し、トポロジー表示を行います。ネットワークに接続されたデバイスを自動検出し、ネットワークの接続関係をリアルタイムに可視化します。②脆弱性レポート自動生成として、システム全体の脆弱性情報をレポート形式で把握できます。必要なときに情報を収集・分析し、脆弱性情報を要約したレポートを自動生成できます。資産リスト、デバイスの脆弱性、ネットワークの脆弱性、個別の対応策が集約されたレポートの自動生成が可能です。③セキュリティ・設備の脅威・異常検出として、制御プロトコルに対応した異常検出、インシデント分析支援による迅速なオペレーションを実現し、制御システムを狙った脅威・異常を検出します。④攻撃経路予測と対策支援として、すべての資産の脆弱性情報をもとに危険な攻撃経路を予測します。システム全体の状態を把握し、制御システムに潜む攻撃経路を見つけ出すことで、リスクへの対策を支援します。



「CyberX Platform」システムの構成例

- CyberX PlatformはCyberX Inc.の製品です。
- SIEM（Security Information and Event Management：セキュリティ情報のイベント管理）
- DMZ（DeMilitarized Zone：非武装地帯）
- Waterfall 一方向セキュリティゲートウェイの開発元は、Waterfall Security Solutions Ltd.です。

決済端末 CT-5100シリーズ

東芝テック(株)

決済に用いられる方法は多様化しており、その代表的なものがICカードによるクレジットカード決済です。クレジットカード決済ではクレジットカード番号、個人情報等のセンシティブな情報が扱われており、サイバー攻撃によりこれらの情報が漏えいし悪用されるとクレジットカード利用者に多大な損害が発生する可能性があります。このため、日本政府は、クレジットカード決済を国民生活に重大な影響を与える重要インフラ14分野の1つとして指定しています。

従来、開発・製造を行うメーカーは、それぞれ独自のセキュリティ基準の決済端末を製造・販売していましたが、2006年には5つの国際ペイメントブランドによってPCIセキュリティ基準審議会(PCI SSC:Payment Card Industry Security Standards Council)が設立され、国際セキュリティ基準が制定されました。その規格の1つにPCI PTS(Payment Card Industry PIN Transaction Security)があります。PCI PTSはPIN(暗証番号)入力を行う決済端末に求められる高難易度のセキュリティ認定です。

決済端末CT-5100シリーズへ接続するPINパッド「PADCT-5100」は、クレジットカード決済を安全に行うためのPCI PTS Ver4.1認定を取得済みです。PCI PTSは決済端末で必要となるソフトウェアやハードウェアのセキュリティ機能や製品管理などの要件が幅広く規定されています。また、本体の「CT-5100」も、AndroidやLinux等のオープンなOSではなくクローズドなOSを採用し、搭載される全てのソフトウェアに認証および暗号機能を搭載していますので、外部からのハッキングに対して強固なセキュリティ性を保持しています。また、外部からの不正なアタックに対する耐タンパー機能も備えていますので、安心して利用できます。

2018年6月に施行された改正割賦販売法では、加盟店によるカード情報保護対策実施が義務化されております。対面加盟では、カード情報の非保持化(非保持と同等/相当を含む)またはPCI DSS準拠の必要があります。非保持化としては、加盟店で保有するPOS機器・ネットワークにカード情報を通過させないでカード会社で処理する“外回り方式”と、加盟店で保有するPOS機器・ネットワークにカード情報が通過するが、暗号化等の処理によりカード番号を特定できない状態、かつ、加盟店で復号できない仕組みを持ち、カード会社で処理し、非保持化と同等/相当の措置を行う“内回り方式”があり、決済端末CT-5100/PADCT-5100はどちらの方式にも対応可能です。

左:CT-5100(本体)
右:PADCT-5100(ICカードリーダライタ付PINパッド)

研究開発

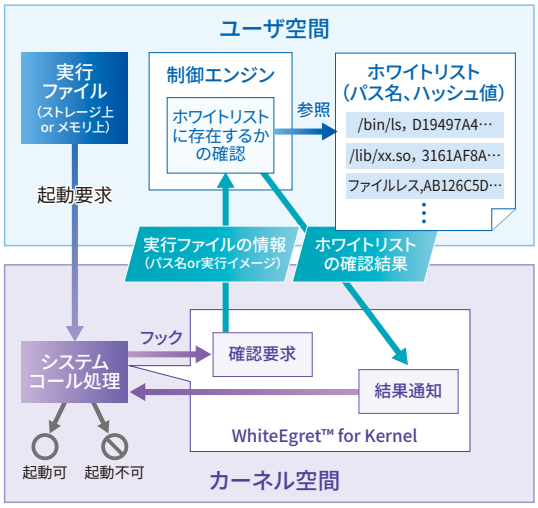
IoTやサイバー・フィジカル・システム（CPS）の進展にともないサイバー攻撃の高度化・多様化トレンドが拡大しています。ゼロトラストの環境下でも未知の脅威から社会基盤を守り続け安全で安心できる社会を実現するために、東芝ではセキュリティ脅威分析・予測・評価に基づき最新対策技術の導入を進めています。さらに、インシデント監視・検知、対応・復旧などの先進的セキュリティマネジメント技術、並びにそれらを支える基盤となる先端攻撃や先端暗号に関する研究開発にも取り組んでいます。サイバー攻撃脅威の進化を先取りしたプロアクティブな対応で、社会インフラ事業で築き上げた東芝基準の安心安全品質を提供し続けます。

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ねらうマルウェアが登場し、サイバー攻撃への適用事例が報告されるなど、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ホワイト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未知を含むマルウェアからの防御を可能にしています。ファイルとしての実体を持つマルウェアからの保護に加えて、従来技術では検出が困難で近年流行の兆しを見せる「ファイルレスマルウェア」からの保護も実現しています。

出典：春木洋美他、インフラの安心・安全な長期運用を支える制御システムセキュリティー技術／東芝レビューVol.73 No.5（2018年9月）より

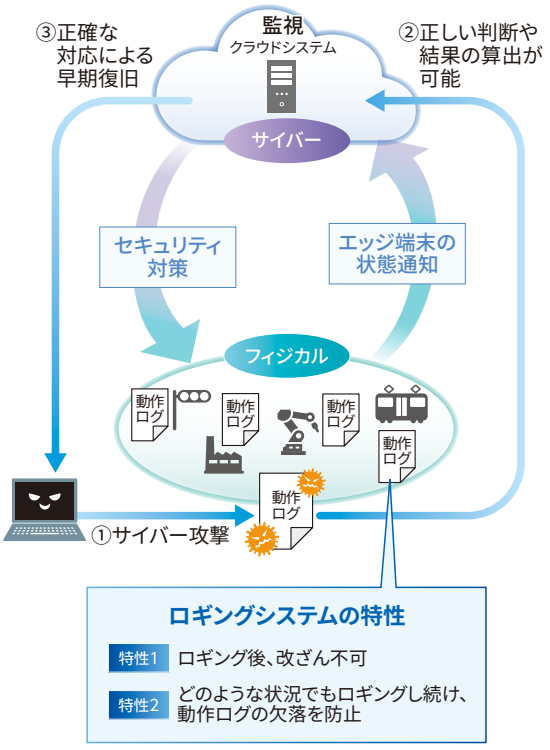


組込みロギングシステム

長期間の安定稼働が求められる社会インフラシステムでは、故障など稼働を妨げる事象の兆候を捉えるため、現場にあるエッジ機器の動作ログを収集しクラウドに統合して遠隔監視しています。社会インフラシステムがサイバー攻撃を受けると、稼働情報といった機密度の高い情報を奪われるだけではなく、動作ログが改ざんされ正確な状況がつかめなくなり、システム全体の不安定な状態を捉えることができず事故を起こしてしまうおそれがあります。

そこで東芝は、サイバー攻撃による動作ログの改ざんや欠落に耐性のあるエッジ機器向けのロギングシステムを、仮想化技術を応用して開発しました。

出典：蒋丹他、“組み込み機器向けセキュアロギングシステムの提案”、SCIS2020

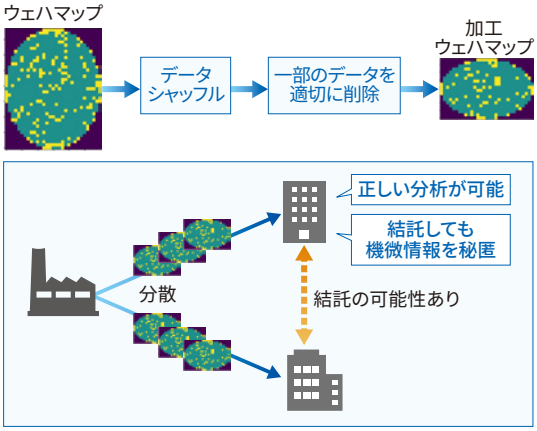


安全性と有用性を兼ね備えるデータ加工技術

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、安全性と有用性を両立するデータ加工方法の開発を進めています。一部のデータをシャッフルするとともに適切に削除することで、開示先が結託したとしても機微情報を守ることができる技術を開発しました。

出典：和田紘帆他、“半導体ウェハの品質検査データに対する安全性と有用性を両立可能なデータ加工方法の初期検討”、SCIS2020

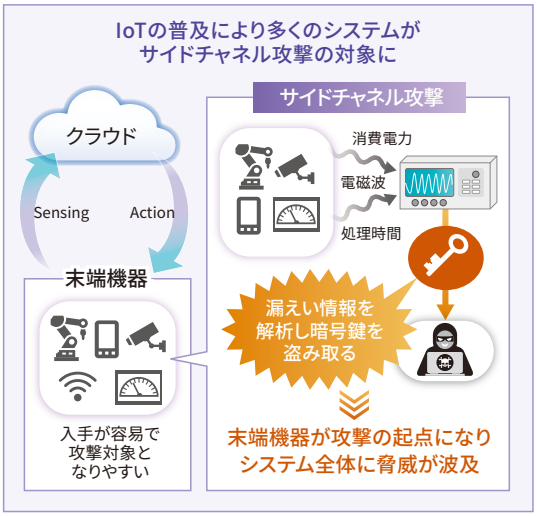


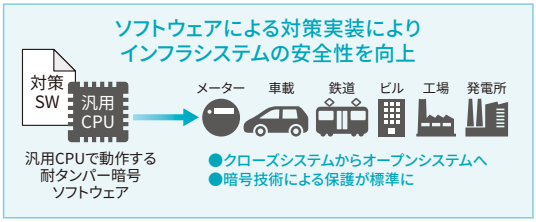
攻撃評価技術

サイバー攻撃や物理的攻撃などの攻撃技術は日々進化、多様化しています。このような未知の脅威から社会基盤（CPS）を正しく守り続けるためには攻撃技術を我々自身がつぶさに「知る」必要があります。

そこで東芝は、制御システムに対するリモートからのサイバー攻撃やCPS機器を物理的に不正解析するサイドチャネル攻撃など、リアルなモノやシステムへの攻撃手法を評価・分析する攻撃評価技術を開発しています。さらに、プロアクティブなセキュリティ対策の実現をめざして攻撃評価技術を自社製品の開発プロセスに取り入れ、サイバー攻撃に対抗する不正プログラム実行制御技術や、サイドチャネル攻撃に対して耐性がある耐タンパー実装技術などを研究開発しています。

出典：駒野雄一他、“IoT端末へのサイドチャネル攻撃の脅威評価～攻撃環境の変遷と対策技術の展望～”、SCIS2019



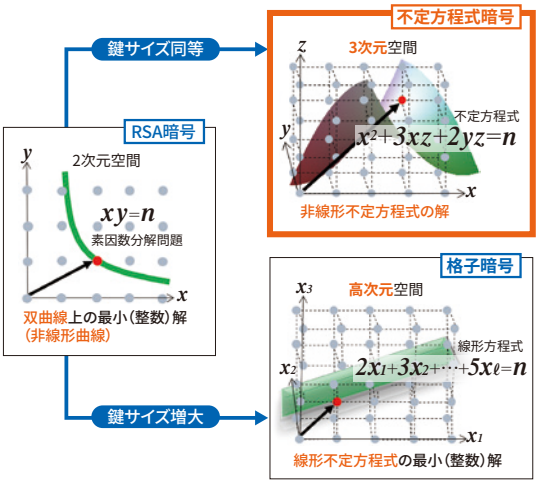


耐量子計算機暗号

量子コンピュータが現在よりも大きなデータを処理できるようになると、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公開鍵暗号の導入をめざします。

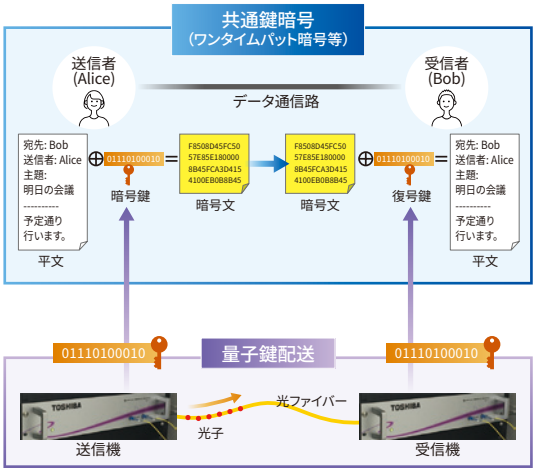
出典：Koichiro Akiyama et al. “A Public-key Encryption Scheme Based on Non-linear Indeterminate Equations (Giophantus)”, https://eprint.iacr.org/2017/1241 (2017)



量子暗号通信

東芝は、量子力学の原理に基づく次世代の暗号技術である量子暗号技術の研究開発にも取り組んでいます。光の最小単位である「光子」の検出回路と制御回路を高速、効率的、安定的に駆動する技術などを開発し、世界初となる10Mbpsを超える速度での量子暗号鍵生成を実現しました。医療・金融・通信インフラなどの多様なアプリケーション・ユースケースでの実用化をめざし、日本や英国にてさまざまな運用実証を進めています。また、ITU-TやISO/IEC JTC1, ETSI等にて、量子暗号関連技術の国際標準化にも取り組んでいます。

出典：http://www.toshiba.co.jp/qkd/index_j.htm



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.8参照）が中心とな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。特にリスクの高い個人情報を取り扱う部門やグループ会社に対しては現地確認を実施し、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り、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

2018年5月に欧州でGDPRが全面適用されたことを受け、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）などのGDPR対応を実施しています。また、国内東芝グループの全従業員に対して、GDPRの概要や域外移転における注意点などについて教育しています。

※General Data Protection Regulation

中国サイバーセキュリティ法への対応

2017年6月に施行された中国サイバーセキュリティ法の下部規則、ガイドラインの整備が進み、法執行も活発になっています。これらの法令などに対して、中国の地域総括現地法人を中心に情報把握、対応を進めています。

タイ個人情報保護法への対応

2019年5月に公布されたタイ個人情報保護法に対応するため、規程類のひな型を作成して現地法人に提供し、規程類の整備を進めています。

社外活動

2020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

主なデジ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 JTC 1（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2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 TC68/SC2、SC6、SC7　金融業務に利用される情報セキュリティ技術
- 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
- IEEE（The Institute of Electrical and Electronics Engineers, Inc.）802.21 WG　マルチキャスト通信のセキュリティ認証
- 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。

- 独立行政法人情報処理推進機構（IPA）10大脅威執筆者会 ほか
- 一般社団法人日本電気計測器工業会（JEMIMA）
- 一般社団法人電子情報技術産業協会（JEITA）個人データ保護専門委員会 ほか
- 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
- 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

ほか

第三者評価・認証

2020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ITサービス（株）
東芝情報システム（株）
東芝インフラシステムズ（株）
東芝デジタルソリューションズ（株）
東芝テックソリューションサービス（株）
日本システム（株）
九州東芝エンジニアリング（株）
イー・ビー・ソリューションズ（株）
中部東芝エンジニアリング（株）
東芝テック（株）
東芝デベロップメントエンジニアリング（株）
テックインフォメーションシステムズ（株）
東芝インフォメーションシステムズ（株）
東芝デジタルマーケティングイニシアティブ（株）

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）

東芝情報システム（株）
東芝プラントシステム（株）
東芝デジタルソリューションズ（株）
九州東芝エンジニアリング（株）
東芝テックソリューションサービス（株）
東芝ITサービス（株）
東芝インフォメーションシステムズ（株）
東芝情報システムプロダクツ（株）
東芝自動機器システムサービス（株）
東芝オフィスメイト（株）
東芝デジタルマーケティングイニシアティブ（株）
東芝アイエス・コンサルティング（株）
東芝ビジネスエキスパート（株）
東芝健康保険組合
東芝インフラシステムズ（株）

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（2020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-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-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	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+
TOSMART-P080 ePassport 01.06.04 + NVM Ver.01.00.01	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+
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）」または米国National Institute of Standards and Technology（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（2020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 C	2769	Level2
Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX model) Type A	2709	Level2
Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX model) Type B	2707	Level2
Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX04S model) Type A	2521	Level2
Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX04S model) Type B	2520	Level2
Toshiba TCG Enterprise SSC Self-Encrypting Hard Disk Drive (AL14SEQ model)	2508	Level2
Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX model NA02)	2410	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：セキュリティ技術ー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 Communication 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

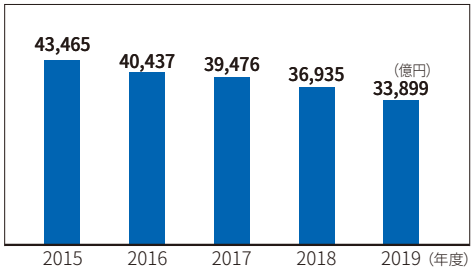
2020年3月31日現在

会社概要

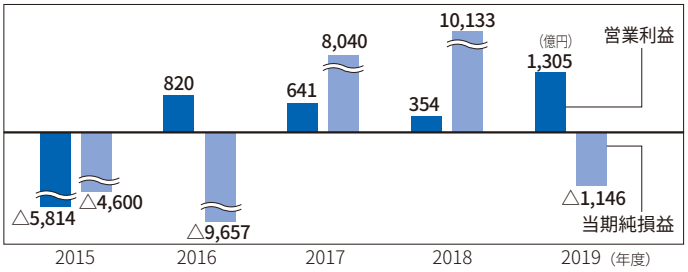
社　　名	株式会社 東芝 (TOSHIBA CORPORATION)
本社所在地	東京都港区芝浦1-1-1
創　　業	1875年（明治8年）7月
資 本 金	2,001億7,500万円
連結売上高	3兆3,899億円
連結従業員数	125,648人
発行済株式総数	4億5,500万株
上場証券取引所	東京、名古屋

業績（連結）

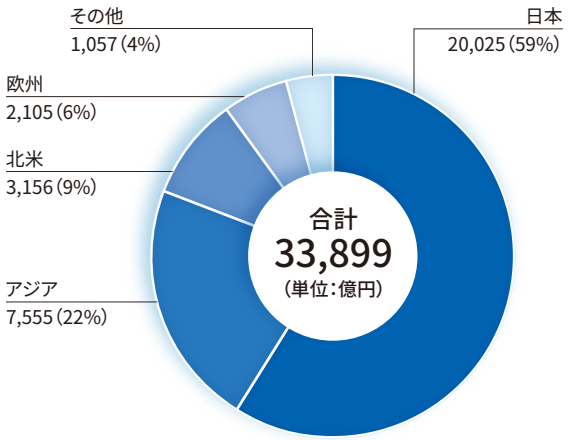
売上高の推移



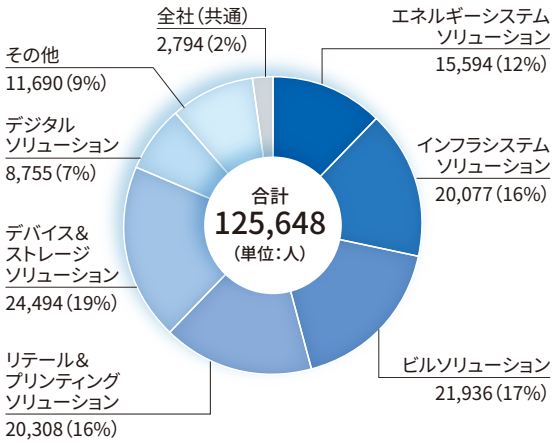
営業利益／当期純利益（損失）の推移



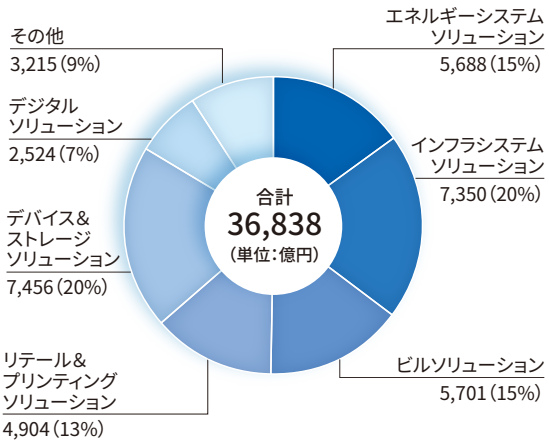
地域別売上高



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2,939億円含む）

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.toshiba.co.jp/security/

2020年6月発行

Printed in Japan