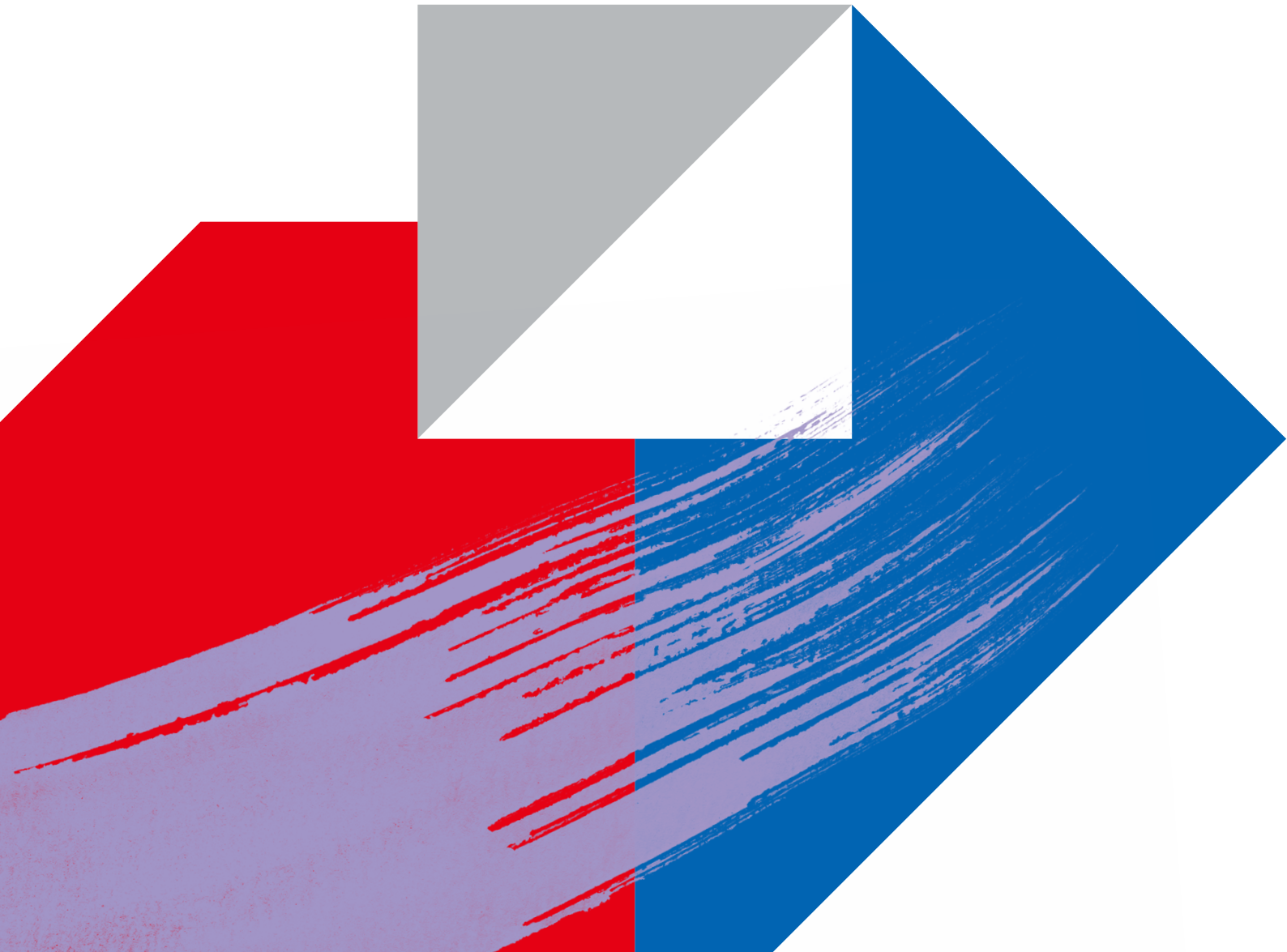
TOSHIBA

# 2021 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

# リモートでつながる世界に、安心を届けたい

新型コロナウイルス感染症（COVID-19）によって、世界は大きな変革を迫られました。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終息を願わずにはいられませんが、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」な社会をめざす考え方もあります。

この1年を振り返ると、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」であると言えるでしょう。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、「リモートでつながる世界」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言えます。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を中心とした事業に取り組み、皆さまの暮らしを支える「インフラサービスカンパニー」へと変革を進めています。1875年の創業以来、145年間継続している「ものづくり」で得た知見と経験を活かし、現実世界だけでなく、「リモートでつながる世界」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**安心と安全**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。

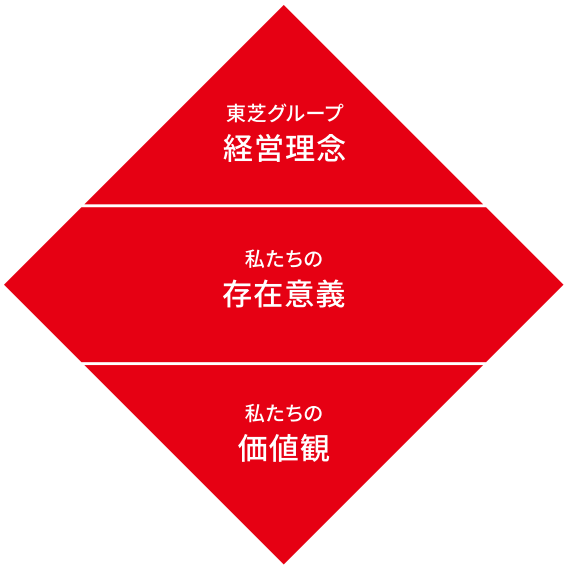
見えざる脅威から社会を守るため、東芝はグループ一丸となって**サイバーセキュリティ体制**を構築し、関連法令の遵守やセキュリティ人材の育成に努めることはもちろん、お客さまへの情報開示に向けて、積極的かつ誠実に取り組んでまいります。

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。

# 2021 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（仮想世界）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テクノロジー企業としての飛躍に向けて、インフラサービスカンパニーをめざしています。サイバー・フィジカル・システム（CPS）とは、フィジカル（実世界）から生じるさまざまなデータを収集し、それらをクラウドなど大量の計算機資源が存在するサイバー（仮想世界）でAIなどの分析技術を用いて分析し、活用しやすい情報に加工してフィジカルにフィードバックすることで、効率的で持続可能な社会を実現していく仕組みです。しかし、その一方でCPSでは、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、145年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、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インフラサービスカンパニー

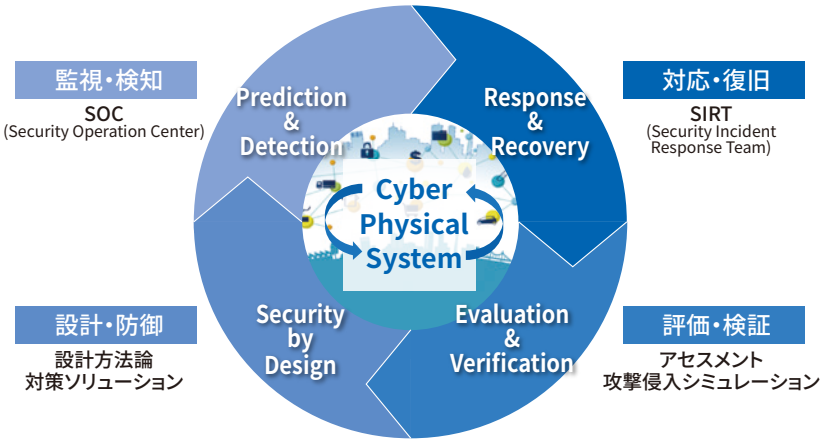

東芝グループには、社会インフラ事業を中心に膨大な知見と、それを裏付けるデータの蓄積があります。また、東芝グループは世界をけん引してきたハイレベルな情報処理やデジタル・AIといったサイバー技術を保有しています。創業以来、培われてきたフィジカルの強い技術力と、世界最先端のサイバー技術との融合から生まれるCPSテクノロジー、および新しい価値を創造するインフラ事業における豊富な知見で、人類が直面しているさまざまな社会課題を解決する社会インフラサービスの実現をめざします。そして、この社会インフラにデジタルトランスフォーメーションを導入することで、地球温暖化や気候変動、自然災害、インフラ老朽化、ニューノーマル対応、高齢化や労働力不足といった世界に山積する具体的な問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、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、サービスのセキュリティを確保する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、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、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」「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、皆さまの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<br>常に成熟度が向上している |
| 防御 | 脆弱性が入り込まない<br>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<br>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<br>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<br>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 |

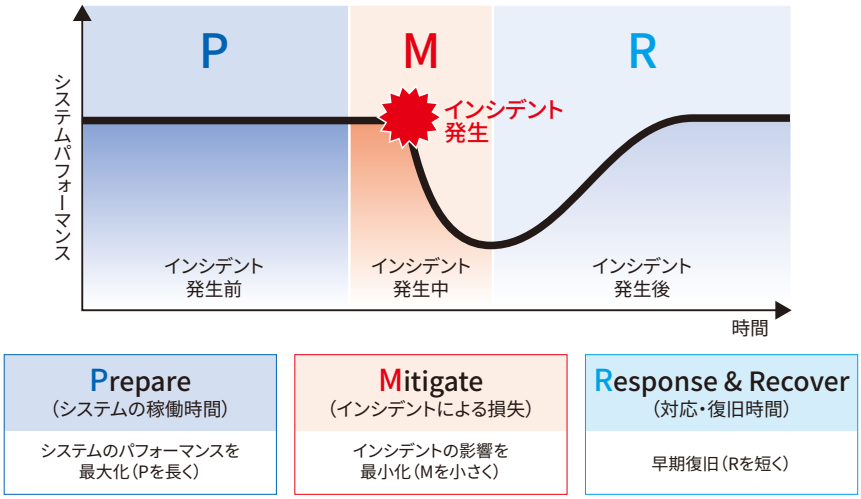
東芝グループがめざすゴール

# サイバーセキュリティ態勢強化に向けた戦略

東芝グループの事業の中心となるインフラサービスにおいて、セキュリティのスコープも変化しています。組織内ネットワークやPC、サーバといった情報セキュリティ、プロダクトのセキュリティ品質を高める製品セキュリティに加え、産業インフラの現場における制御セキュリティ、さらに現実社会で生成される情報をサイバー空間であつかうためのデータセキュリティへと拡大しています。

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ーを定義しています。パラメーターは、システムの稼働時間「Prepare（P）」、インシデントによる損失「Mitigate（M）」、そして対応・復旧時間「Response ＆ Recover（R）」の3つで、それぞれ、「Pを長く」「Mを小さく」「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

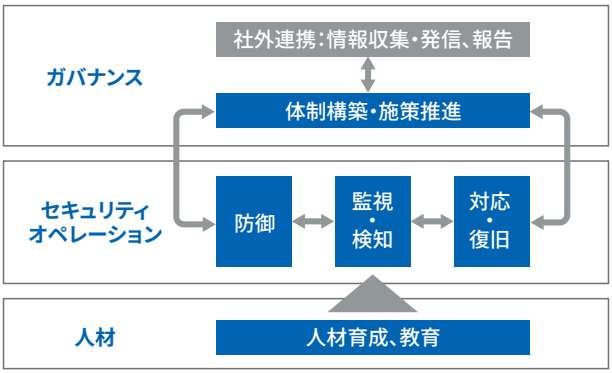
東芝グループでは、サイバーレジリエンスの実現に向けたセキュリティ態勢強化の戦略を推進しています。ここでの“セキュリティ態勢”とは、セキュリティリスクに対する十分な準備を備えた状態を意味します。具体的には、「Pを長く」「Mを小さく」するために意思決定・指揮系統を明確化するガバナンス、「Mを小さく」「Rを短く」するための監視・検知／対応・復旧／防御を行うセキュリティオペレーション、そして、これらを運用し発展させていく人材の3つが十分に連携・活用できるよう強化され、常態化されていることを意味します。

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（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。また、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、ガバナンス強化を推進しています。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、社内外の情報共有も積極的に推進しています。

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、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。

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。東芝グループ全体のセキュリティ人材育成の促進に向けては、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プロセス**

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。

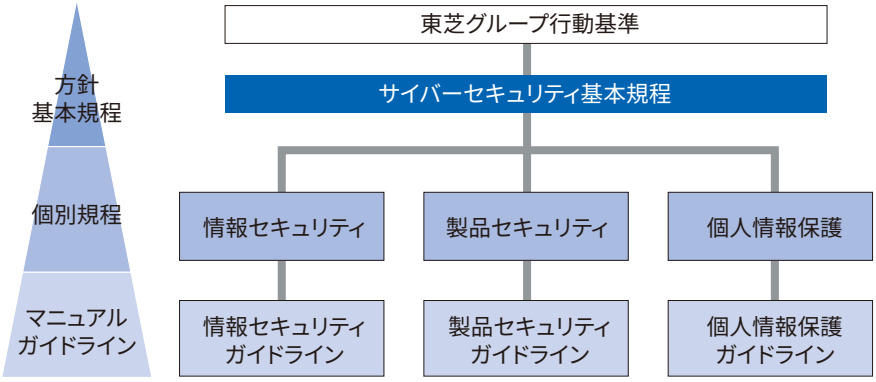
※1 CSIRT：Computer Security Incident Response Team
※2 PSIRT：Product Security Incident Response Team
※3 CDMP：Cyber Defense Management Platform
※4 脅威インテリジェンス：世の中のセキュリティにかかわる脅威動向やハッカーの攻撃活動など、セキュリティに対する意思決定を支援する情報の総称

# 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。

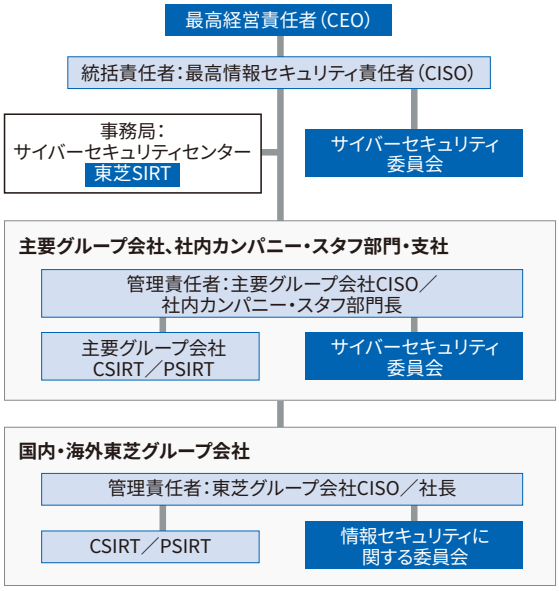
**東芝個人情報保護方針（全文）** https://www.global.toshiba/jp/privacy/corporate.html

## 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、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

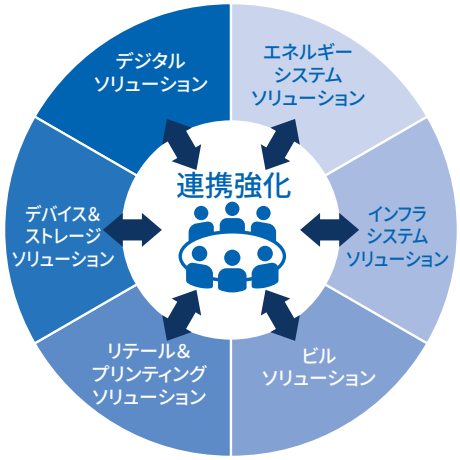



サイバーセキュリティマネジメント体制

## 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。

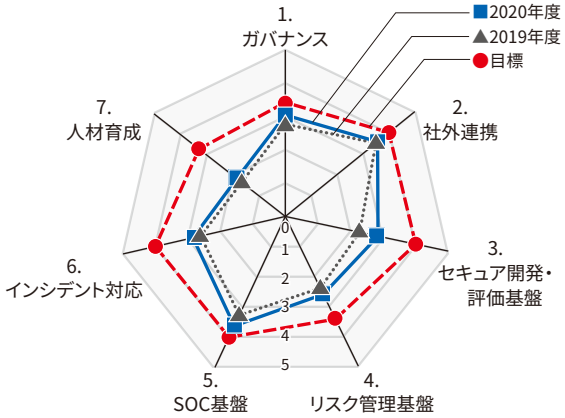


## 成熟度自己評価

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年度は海外東芝グループ会社の成熟度自己評価も実施し、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。



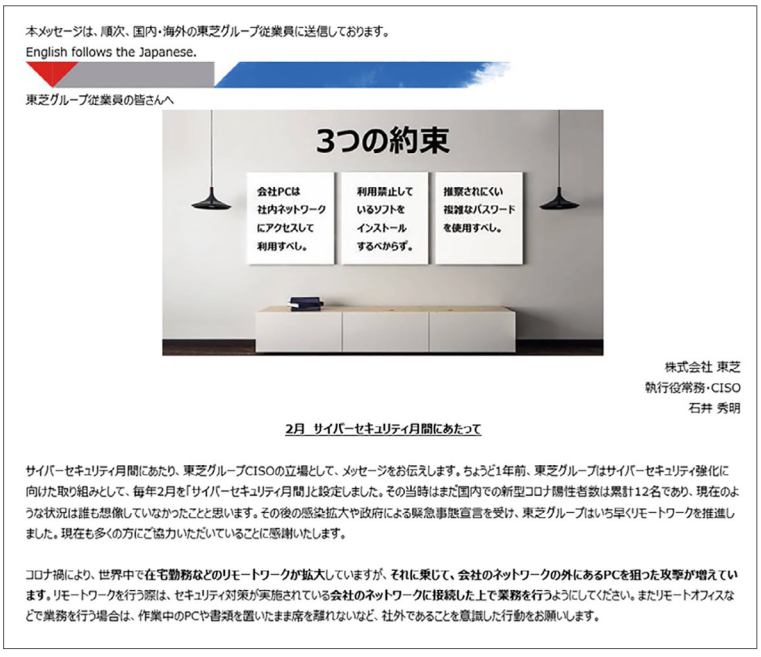

成熟度自己評価結果のグラフ

※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、ポスターを制作して各事業場や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おります。
English follows the Japanese.

東芝グループ従業員の皆さんへ




株式会社 東芝
執行役常務・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の立場として、メッセージをお伝えします。ちょうど1年前、東芝グループはサイバーセキュリティ強化に向けた取り組みとして、毎年2月を「サイバーセキュリティ月間」と設定しました。その当時はまだ国内での新型コロナ陽性者数は累計12名であり、現在のような状況は誰も想像していなかったことと思います。その後の感染拡大や政府による緊急事態宣言を受け、東芝グループはいち早くリモートワークを推進しました。現在も多くの方にご協力いただいていることに感謝いたします。

コロナ禍により、世界中で**在宅勤務などのリモートワークが拡大**していますが、**それに乗じて、会社のネットワークの外にあるPCを狙った攻撃が増えています。**リモートワークを行う際は、セキュリティ対策が実施されている**会社のネットワークに接続した上で業務を行う**ようにしてください。またリモートオフィスなどで業務を行う場合は、作業中のPCや書類を置いたまま席を離れないなど、社外であることを意識した行動をお願いします。

サイバーセキュリティ月間　CISO配信メッセージ

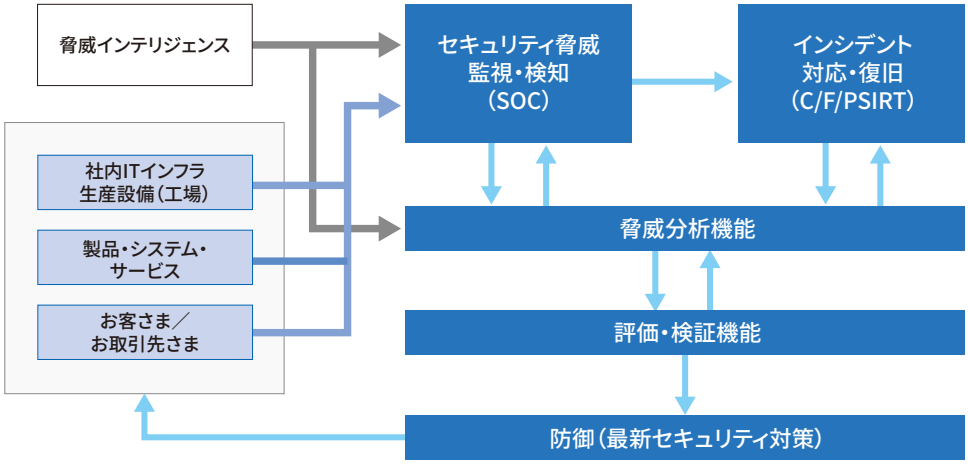
# セキュリティオペレーション

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。




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.15参照） |
| ・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.17、P.23参照） |
| ・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.20参照） |
| | ⇒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.18参照） |
| ・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.19参照） |

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、ダッシュボードによる情報共有、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、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。

# 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。また、人材育成促進のために、東芝グループ内のセキュリティ資格・認定制度を展開しています。

## 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。テレワークを行う際のセキュリティ上の注意点など、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上で行動できるよう、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

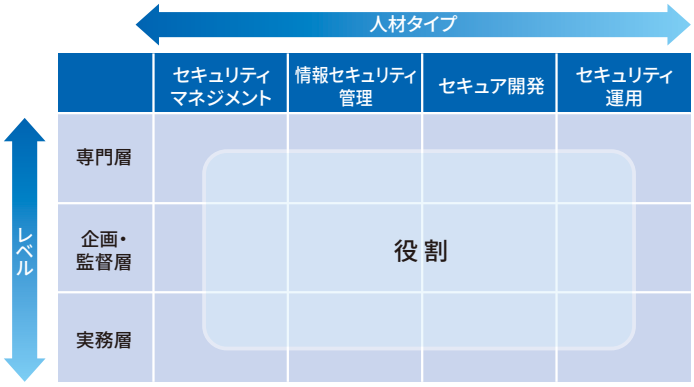
お客さまに提供する製品・システム・サービスのセキュリティを確保するためには、営業、調達、設計、開発、品質、保守など製品にかかわる全員が、製品にセキュリティ脆弱性が発生するリスクの重大性と、製品開発段階でのセキュリティ脆弱性混入の防止、および出荷済み製品のセキュリティ脆弱性への迅速な対応の重要性を理解し、実践する必要があると考えています。そこで、情報セキュリティ教育と同様に、東芝グループのすべての役員と従業員を対象に、毎年製品セキュリティに関するe-Learningを実施しています。

## 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。

## セキュリティ資格・認定制度

上記のセキュリティ人材像を踏まえ、人材タイプと役割レベルそれぞれの組み合わせごとに、セキュリティに関する知識、技術を有していることを認定する、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、社内外で開催されている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、およびその人材タイプと役割レベル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。




セキュリティ人材像

# プライバシーガバナンス※1の取り組み

東芝グループでは、今後、データサービスを展開していきますが、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ます。

データサービスを行う東芝データ(株)では、先行して以下の取り組みを行っています。

## 東芝データ(株)のプライバシーガバナンスの取り組み紹介

(株)東芝の100%子会社である東芝データ(株)は、東芝テック(株)が展開する「スマートレシート®」※2により収集した購買データをはじめとする人材、健康や行動など実社会で発生したデータを、生活者から同意を得た上で、付加価値をつけて実社会に還元することで、豊かな未来の創造をめざしています。同社が扱うデータの適正かつ適切なプライバシー保護を実施するため、東芝グループ内で先駆けて下記のようなプライバシーガバナンスの取り組みを進めています。

### プライバシーに関する社外有識者会議(2020年3月25日 第1回会議開催)※3

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社外有識者会議」を設置し、プライバシー保護の観点から助言を受けています。

＜社外有識者会議の構成員＞

議長　佐藤 一郎 氏　(所属:国立情報学研究所 教授)【専門:情報制度】

構成員　生貝 直人 氏　(所属:東洋大学経済学部総合政策学科准教授　～2021年3月
2021年4月～　一橋大学大学院法学研究科 准教授)【専門:情報政策】

構成員　日置 巴美 氏　(所属:三浦法律事務所 弁護士)【専門:データビジネス】

構成員　山本 龍彦 氏　(所属:慶應義塾大学大学院法務研究科 教授)【専門:憲法学】

構成員　奥原 早苗 氏　[2020年10月1日開催の第3回会議から参加]
(所属:公益社団法人 日本消費生活アドバイザー・コンサルタント・相談員協会 顧問)
【専門:消費者政策】

※1 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

※2 スマートレシート(東芝テック株式会社の登録商標) https://www.smartreceipt.jp/
お客さまが店舗で会計をする際に、電子化されたレシートデータをスマートフォンで受け取れるシステム

※3 東芝 ニュースリリース(2020-03-25):プライバシーに関する社外有識者会議の設置について
https://www.global.toshiba/jp/news/corporate/2020/03/pr2501.html

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。

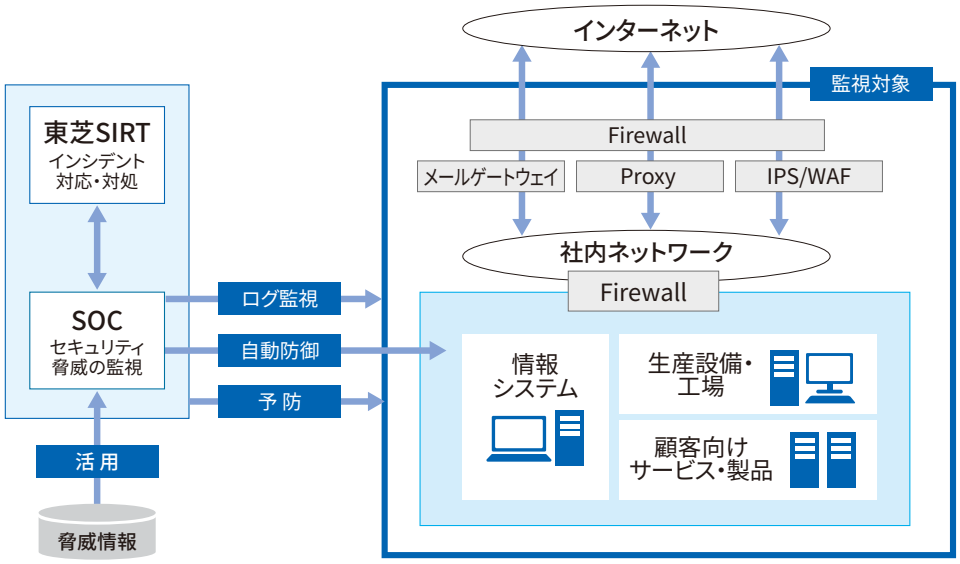
## 社内ITインフラへの対策

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。そこで、セキュリティリスクを早く、さらに正確に検知し、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)：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

## EDR※1ツールによるエンドポイント※2対策の強化

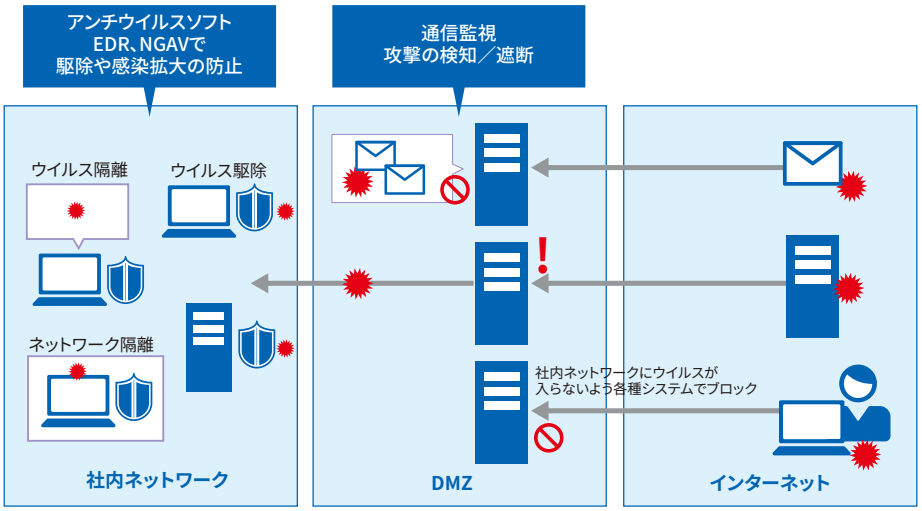
監視 検知

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感染等によるエンドポイントの不審な挙動の検知
- 感染端末をネットワークから外すことなく、SOCがリモートでエンドポイントをネットワークから隔離、脅威の駆除
- 収集した操作ログから、原因や被害範囲の追跡

※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

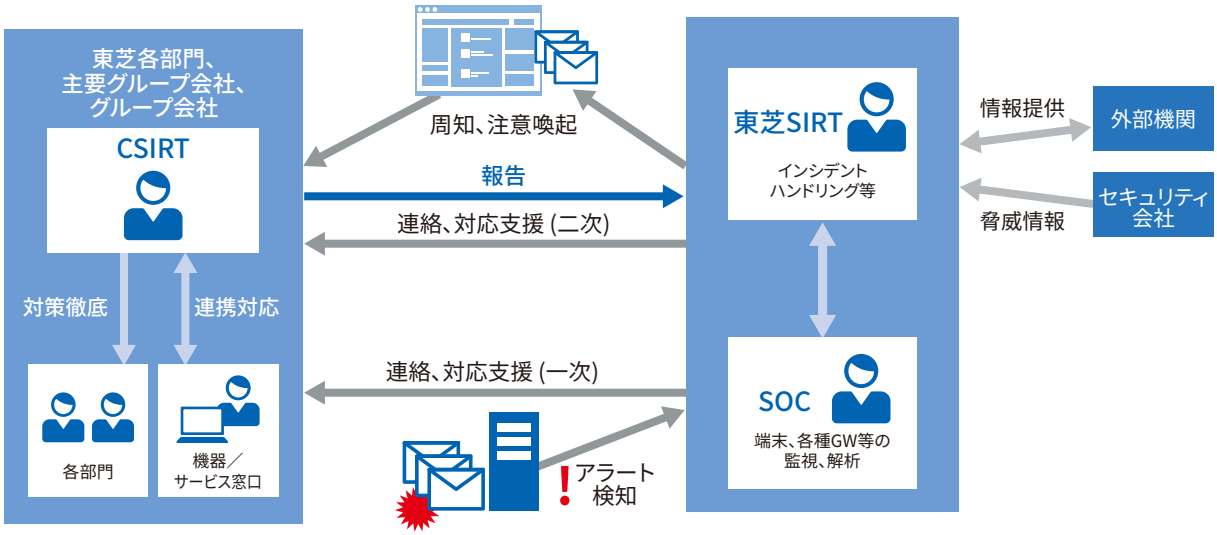
対応
復旧

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態勢を整えています。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、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これを周知することで迅速な対応が可能となり、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。

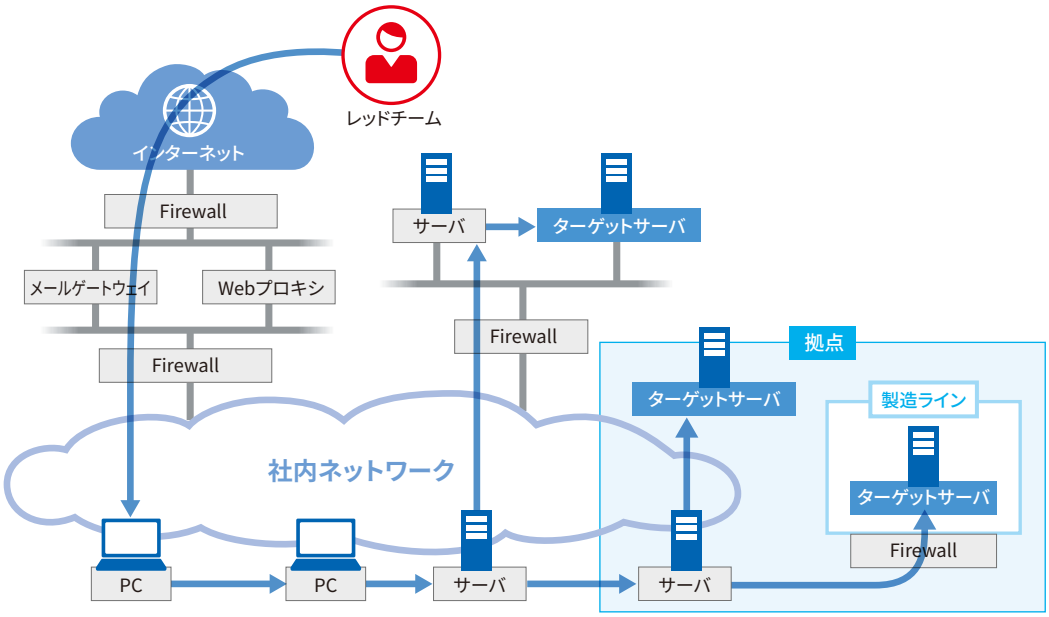
# ハッカー視点の高度な攻撃・侵入テスト

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を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

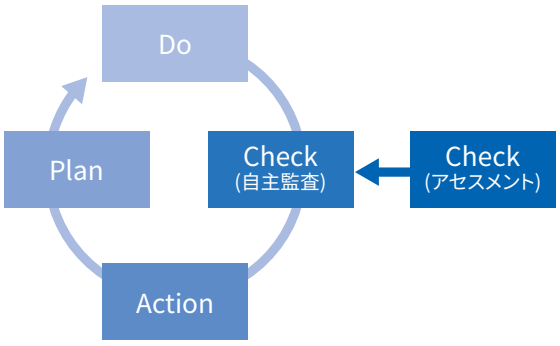



# 自主監査・アセスメント

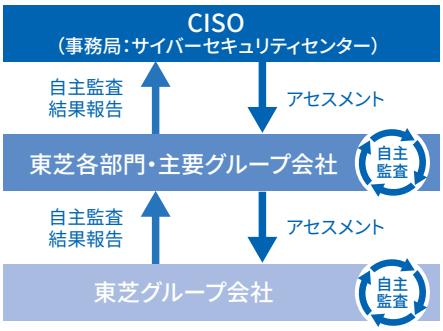
評価検証

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。

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

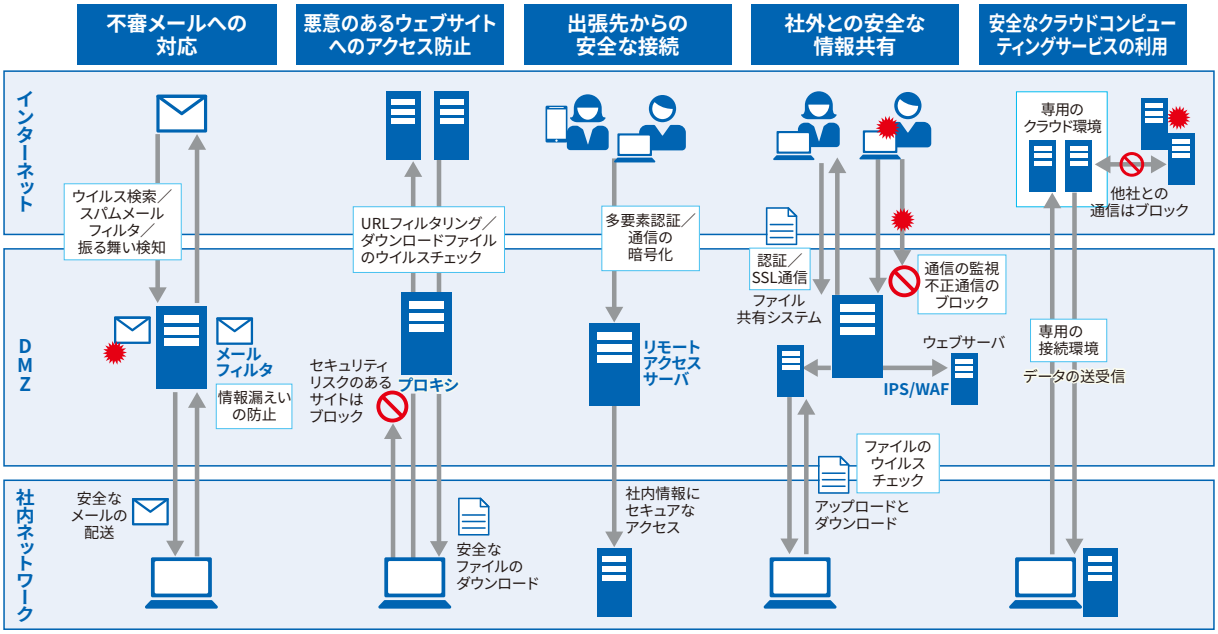



東芝グループ全体で自主監査・アセスメントを実施

# 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、情報漏えいなど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。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

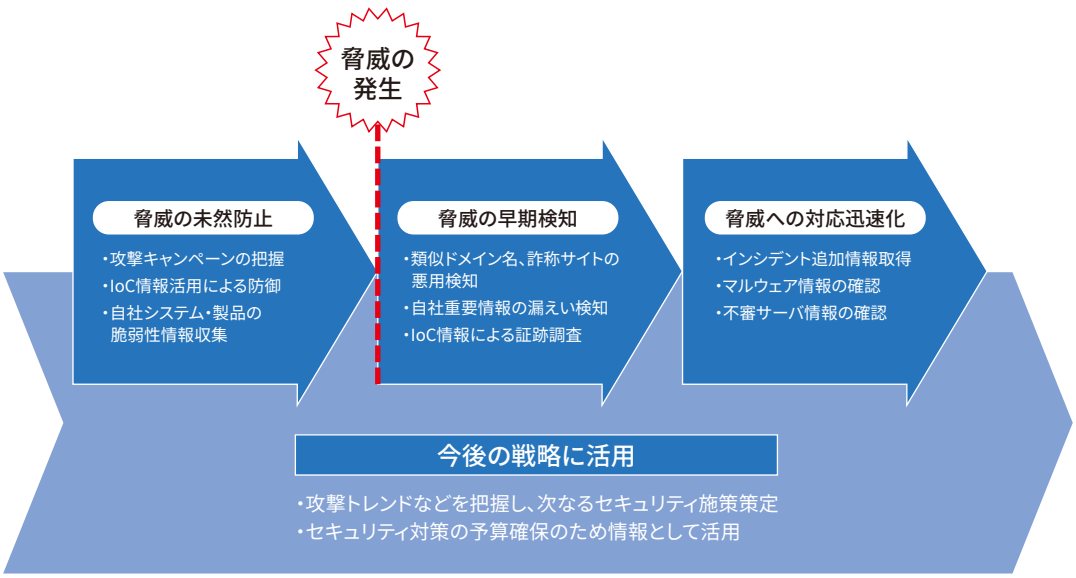
業務効率化のため、クラウドコンピューティングサービスを利用する機会が増えていると同時に、情報漏えい、不正アクセス、誤設定など危険も増えています。そのため、さまざまな危険から重要情報を守り、安全に利用できるプライベートクラウド環境を構築しています。一方、パブリッククラウドサービスの利用は申請制とし、東芝グループのセキュリティポリシーを満たしているか確認した上で、利用を許可しています。また、定期的に利用機能や方法に変更がないか確認しています。

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。

# 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

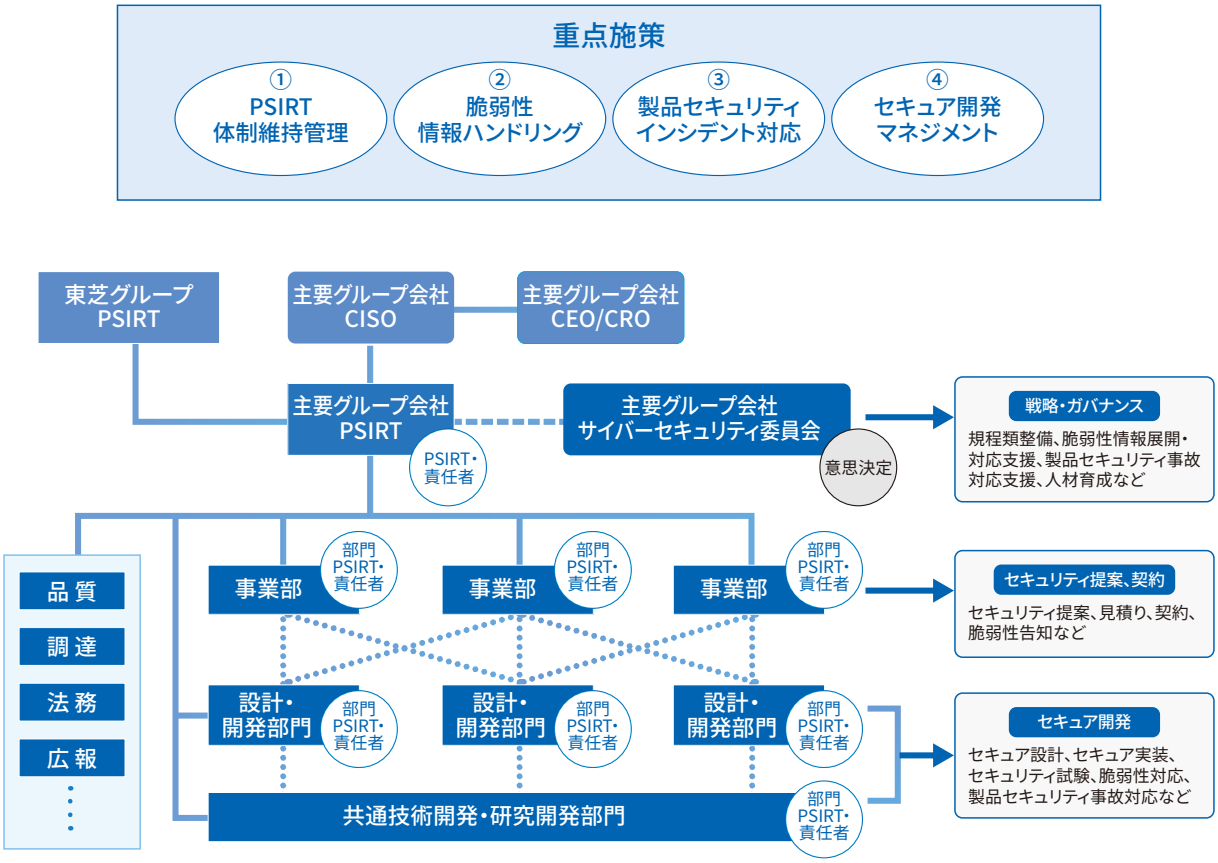
東芝グループでは、お客さまへ提供する製品・システム・サービスに対するセキュリティ品質を確保するため、さまざまな活動に取り組んでいます。また、PSIRT（Product Security Incident Response Team）体制を確立し、社外機関との連携により自社製品の脆弱性への迅速な対応を行っています。

## 製品セキュリティを確保するための取り組み


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

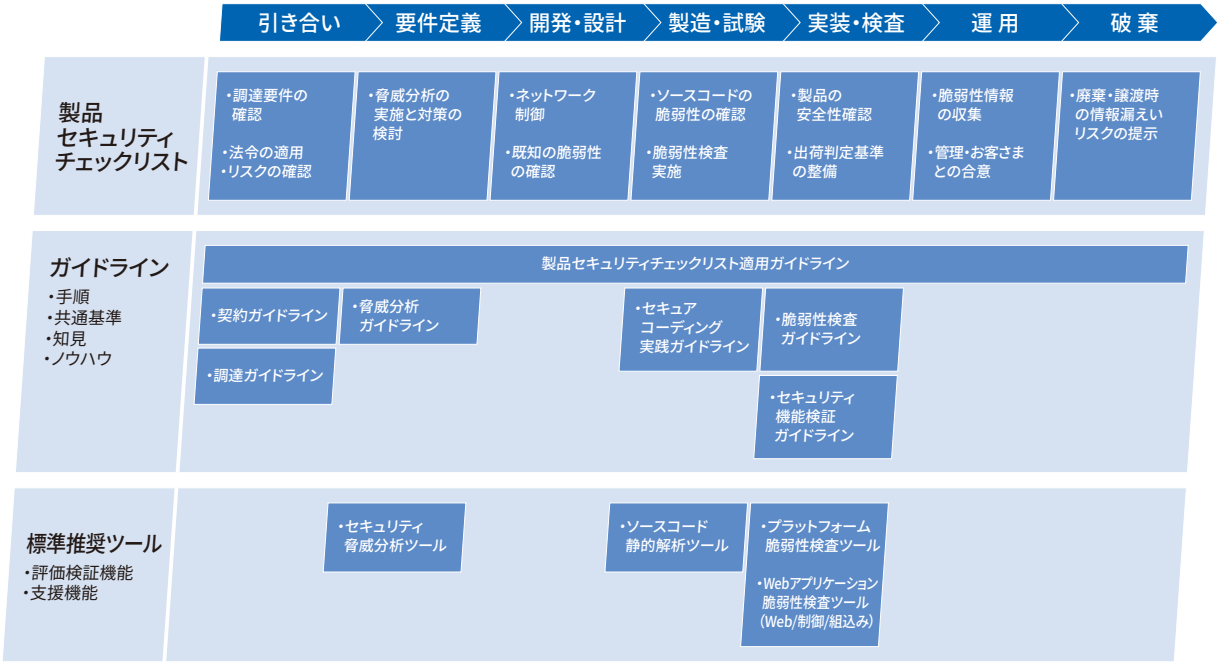
東芝グループの製品セキュリティ強化のため、4項目の重点施策を定義し、グループ各社で構成する製品セキュリティマネジメント体制のもと、リスクベースの優先順位付けに基づく製品セキュリティ態勢強化計画を策定しました。これにより、全社施策を開発現場であるグループ各社の事業部門、設計・開発部門まで確実に行き渡らせる実効性と、自律的組織運営を実現します。




製品セキュリティマネジメント体制

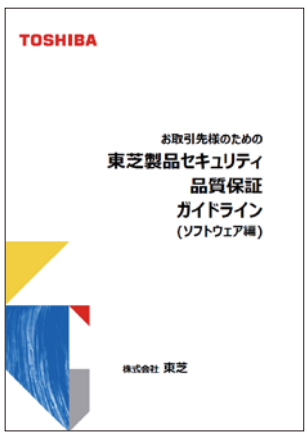
## 製品セキュリティチェックリスト、およびガイドライン・標準推奨ツールの整備

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

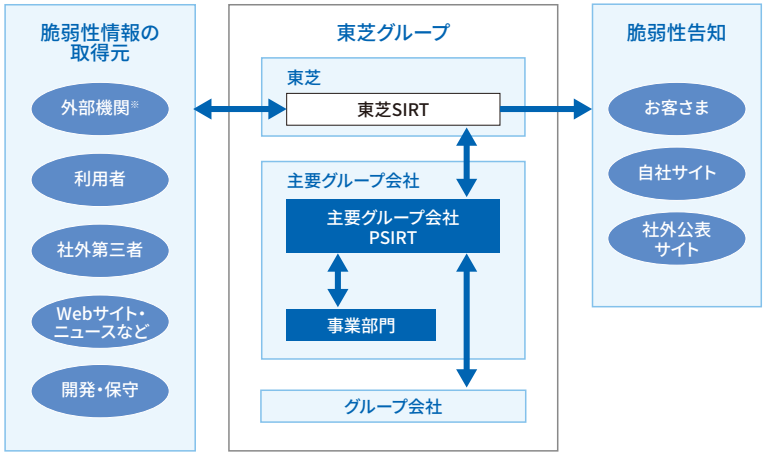
対応 復旧

東芝グループ全体で、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。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。

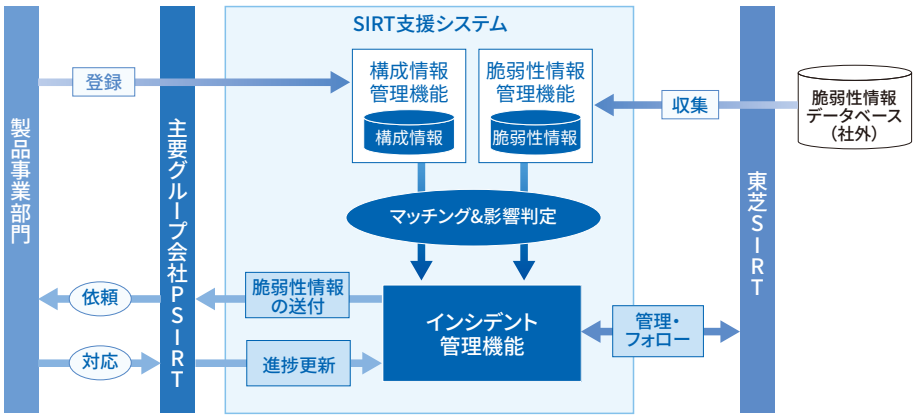



※外部機関：JPCERT/CC、JVN、ICS-CERTなど

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

# コラム

## サプライチェーンにおけるサイバーセキュリティ対策

新型コロナウイルスの感染拡大により、企業・個人ともに物理的な行動制限を余儀なくされました。さまざまなIT技術が社会に浸透したことで、コロナ禍においても市民生活が抱える不便さを解決してきましたが、多様なITの活用は新たなリスクの増大につながったとも言えます。

World Economic Forumが今年1月に発表した“The Global Risks Report 2021”※1によると、今後2年の短期的リスクで、「サイバーセキュリティ対策の失敗」が4位として位置付けられ、直近のリスクの高さが見て取れます※2。


**グローバルリスクの展望**

将来、重大な世界的脅威となりうるリスク（リスク意識調査回答者による）

Source: World Economic Forum, The Global Risks Report 2021

### サプライチェーンがサイバー攻撃のターゲットに

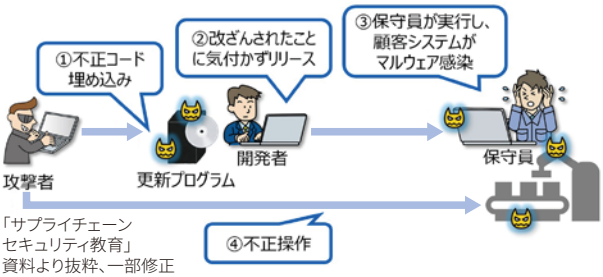
昨今はサプライチェーン※3の弱点を狙った攻撃が増え、経済産業省は昨年6月に「昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性について」を発表し、大企業から中小企業までサプライチェーン全体のサイバーセキュリティ対策の強化が急務であると警告しました※4。これは、日本だけのことではなく、EUも昨年12月に新たに発表したCybersecurity Strategy※5で、さらなるレジリエンスの強化の一つにサプライチェーンセキュリティ対策の必要性について言及しているように、世界各国で重要な政策課題の一つとして認識が高まっています。

サプライチェーンにかかわる攻撃では、その手法の一つとして、攻撃者は攻撃目標とする企業の周辺をまず狙います。セキュリティ対策が十分ではない海外拠点、グループ会社や子会社、取引先にまず侵入し、そこを足掛かりに、攻撃目標へと侵入します。そのため、自組織や本社だけのセキュリティ対策では不十分で、一人ひとりが意識を高め、サプライチェーンにかかわるプロセス全体を通じた対策が重要になってきます。

### 東芝グループの取り組み

東芝グループでは、サプライチェーンにおける製品セキュリティリスクに備えるため、従業員に対するe-Learningを積極的に実施し、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。それは、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必要があると考えるからです。また、e-Learningだけではなく、具体的に実行するための製品セキュリティに関する規程やガイドラインを整備し、取引する相手とのセキュリティ要求事項の明確化や、取引先の意識を高めるためにセキュリティレベルの定量評価を継続的に実施し、委託先を選定するように心がけています。

このような取り組みを通じて、サプライチェーンにかかわるプロセス全体としてのセキュリティ向上に努めています。




**サプライチェーンにかかわる攻撃の例（更新ソフトウェアによるマルウェア感染）**

※1 http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf
※2 https://jp.weforum.org/press/2021/01/jp-healing-of-social-fractures-seen-as-key-to-brighter-future/
※3 サプライチェーンとは、一般的に、ある製品の原材料が生産されてから、最終消費者に届くまでのプロセスを意味する
※4 https://www.meti.go.jp/press/2020/06/20200612004/20200612004-1.pdf
※5 https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

# 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。

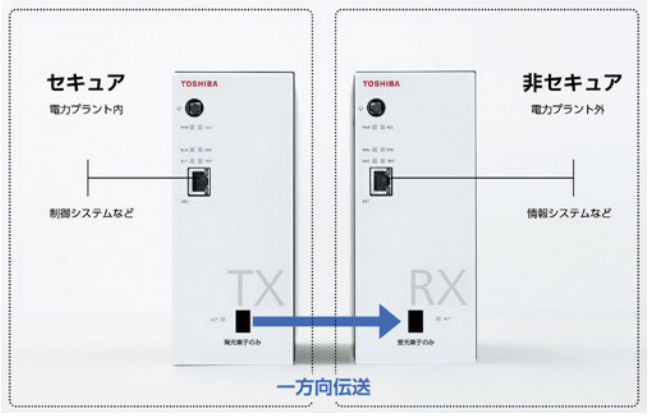
## 一方向伝送装置　TOSMAP-DS™／LX OWB

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。

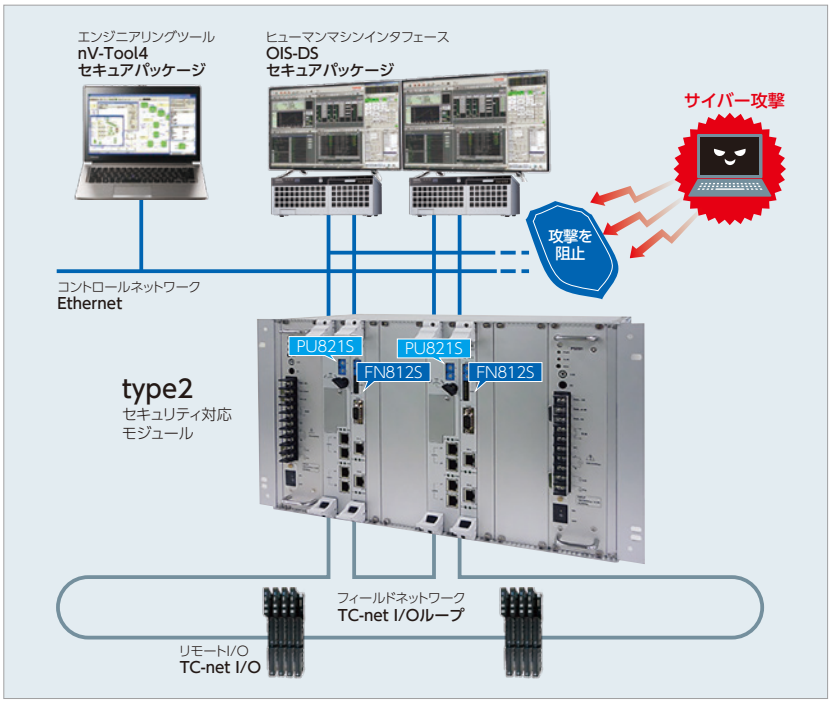
米国ISCI※2がスキームオーナーであるISASecure®EDSA認証は、制御機器（組み込み機器）のセキュリティ保証に関する認証制度で、事業者の調達要件として盛り込まれる傾向にあります。同認証は国際規格IEC 62443シリーズに統合される見込みでもあり、さまざまな業界から注目されています。EDSA認証の評価は、「ソフトウェア開発の各フェーズにおけるセキュリティ評価（SDSA※3）」「セキュリティ機能の実装評価（FSA※4）」「通信の堅牢性テスト（CRT※5）」という3つの評価項目からなっています。ユニファイドコントローラnvシリーズtype2は、国際的に認められた第三者認証機関であるCSSC※6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

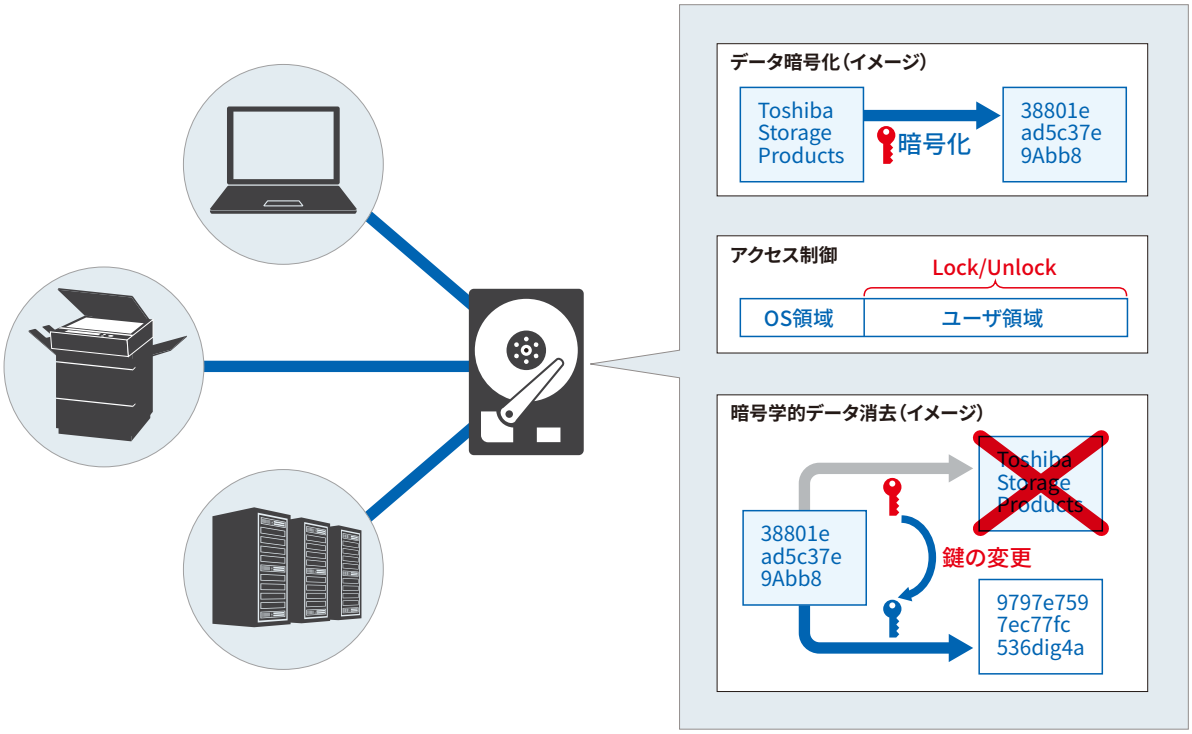
## ストレージ製品へのセキュリティ機能の実装

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

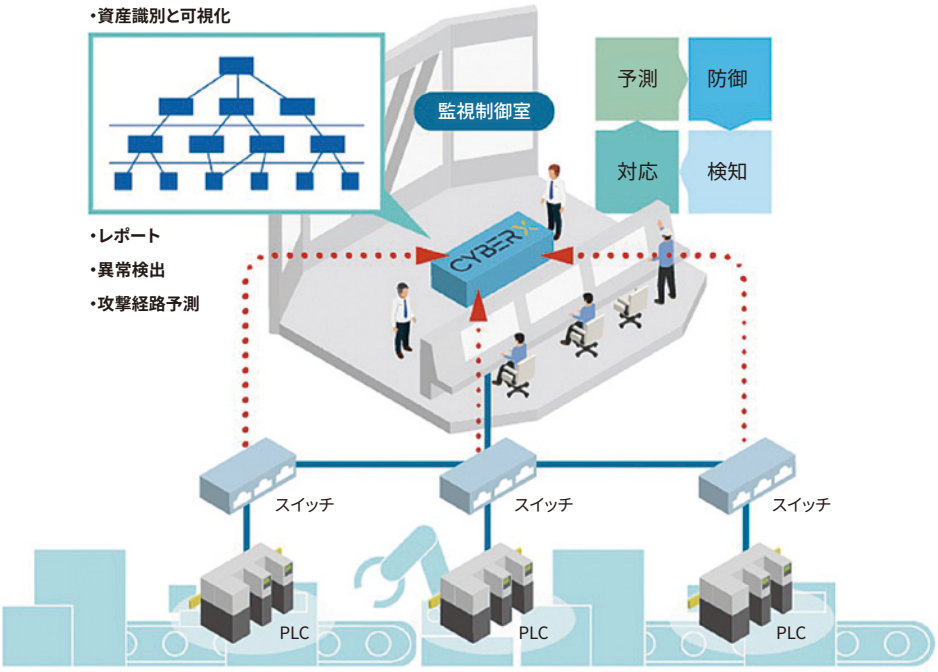
※1 SED: Self-Encrypting Drive
※2 MQ01ABU***BWシリーズ: MQ01ABU050BW/MQ01ABU032BW
※3 NIST: National Institute of Standards and Technology
※4 AES: Advanced Encryption Standard
※5 ATA: Advanced Technology Attachment
※6 TCG: Trusted Computing Group
※7 SSC: Security Subsystem Class
※8 CMVP: Cryptographic Module 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（Defender for IoT）』

東芝デジタルソリューションズ（株）

産業や社会の幅広いフィールドへデジタル化が広がり、これまで外部のネットワークから隔離されていた制御システムがIoTネットワークとつながることで、エネルギーや製造、交通、医療機関など重要な社会インフラでのセキュリティリスクが高まっています。一方、産業現場では所有している機器やネットワーク、潜んでいるリスクを正確に把握することが難しいのが現状です。これらの課題を解決するのが、世界3000カ所以上の制御システムでの導入実績を誇る、CyberX（Defender for IoT）です。当社は日本国内の販売代理店として、東芝の有する豊富な社会インフラ、設備管理ノウハウを用いて最適なシステムを構築し、導入、運用支援、保守サポートまでをワンストップでご提供しています。

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（Defender for IoT）』システムイメージ

●CyberX（Defender for IoT）は米マイクロソフト社の製品です。

## 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。

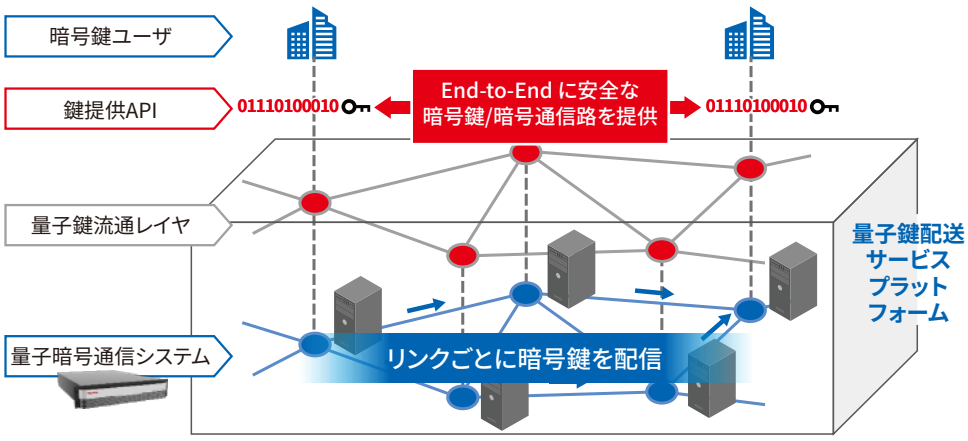
これに対抗する技術が、量子暗号通信です。量子コンピュータのようなどんなに高速なコンピュータが現れようとも、「理論上絶対に破られない」暗号通信技術です。暗号通信を行うための暗号鍵を、光の最小単位である光子にのせて通信することで、通信途中で暗号鍵が漏えいすることを、量子力学の原理により防ぎます。

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、将来にわたって安全に暗号鍵を供給することのできる量子暗号通信システムの、PoCユーザ向けへの提供を開始しました。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

## 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

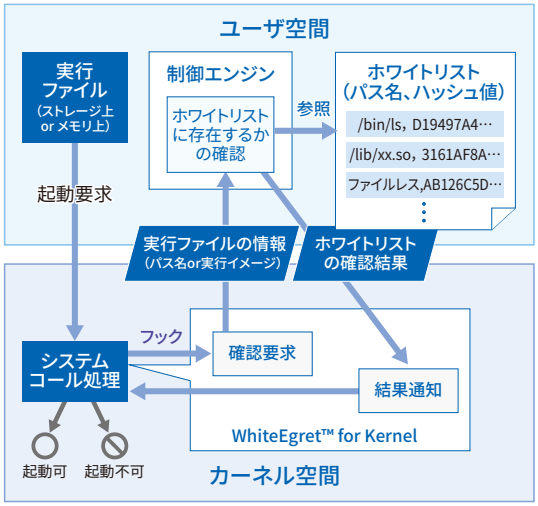
高度化、多様化するサイバー攻撃から社会基盤を守り続けるため、東芝では先進的セキュリティマネジメント技術や、それらを支える先端攻撃や先端暗号に関する研究開発に取り組んでいます。サイバー攻撃の進化を先取りしたプロアクティブな対応で、社会インフラ事業で築き上げた東芝基準の安心安全品質を提供し続けます。

## 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。

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

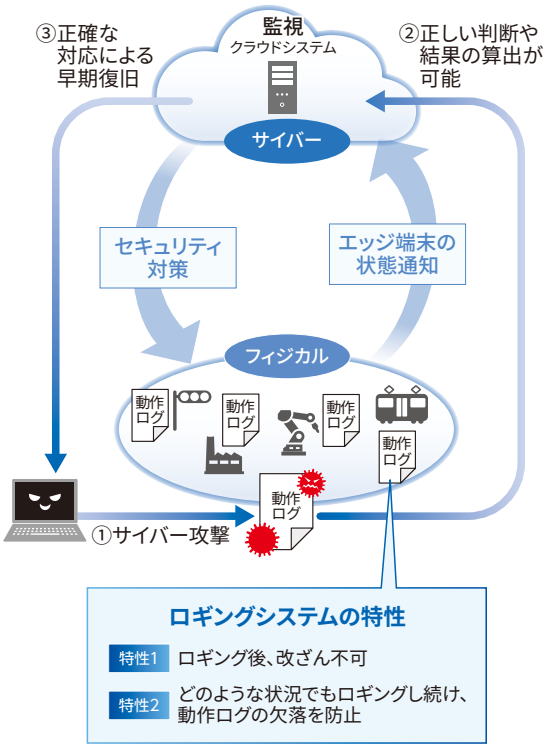



## 組込みロギングシステム

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兆候を捉えるため現場にあるエッジ機器の動作ログを用いてクラウドから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動作ログが改ざんされると、正確な状況を認識できずシステムが不安定な状態となり事故につながるおそれがあります。

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



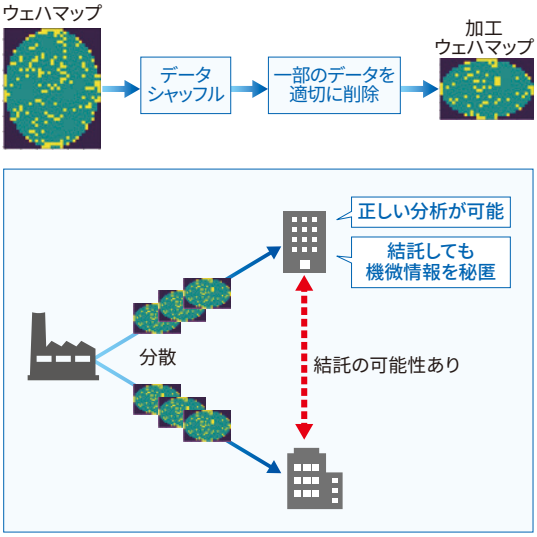
## 安全性と有用性を兼ね備えるデータ加工技術

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

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

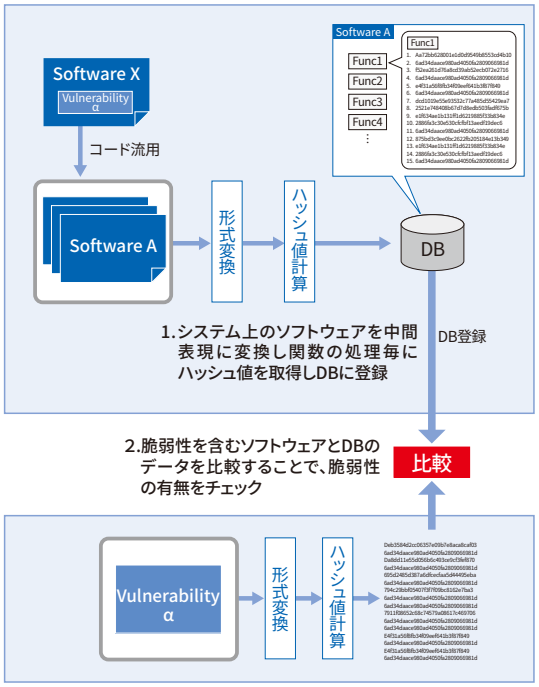



## 脆弱性検査技術

ソフトウェアの脆弱性を放置すると、サイバー攻撃の起点となりシステムへの甚大な被害につながります。そのため、脆弱性の見落としを防ぐ必要がありますが、近年はソフトウェアの外部導入が進んでおりソースコードを持たない場合があります。

そこで東芝は、バイナリコードを解析する脆弱性検知技術を開発しました。入力バイナリからビルド・実行環境を推測できないため、ソースコード形式に戻し共通化することで解析しています。外部導入したバイナリコードに脆弱性が含まれていても検出することができます。

出典：藤松由里恵他、“バイナリ脆弱性検知ツールVulneraBinの評価”、SCIS2021

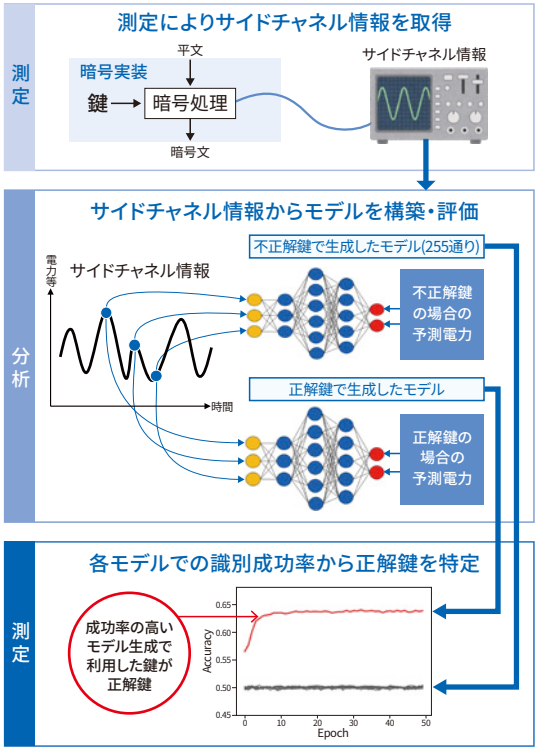


## 攻撃評価技術

さまざまな機器が接続する社会基盤（CPS）においては、日々進化、多様化する攻撃による脅威が増しています。このような脅威に対応するためには、我々自身がつぶさに攻撃技術を「知る」必要があります。

そこで東芝は、CPSを構成するリアルなモノを物理的に解析する手法を開発し、製品開発プロセスに取り入れて自社製品の評価を実施しています。AIを用いたサイドチャネル攻撃などの最先端技術を取り入れた攻撃手法とともに、これら攻撃への耐性を有する耐タンパー実装技術なども開発しています。

出典：前田智紀他、“ディープラーニングを用いた非プロファイリングサイドチャネル攻撃を可能にするハイパーパラメータと効率的な攻撃手法の提案”、SCIS2021

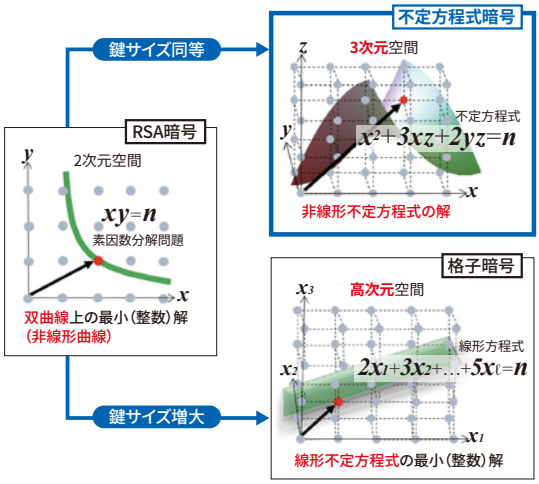



## 耐量子計算機暗号

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。

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)



# 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、グループ各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。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。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。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

2021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。

- 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
- 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
- デジタルトラスト協議会

ほか

# 第三者評価・認証

2021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
東芝デジタル＆コンサルティング株式会社
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
東芝ライフスタイル株式会社
日本システム株式会社
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
九州東芝エンジニアリング株式会社（本社事業所）
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）

九州東芝エンジニアリング株式会社
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（2021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<br>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SYS V1.0 | 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/<br>ファクスユニット（GD-1370J/GD-1370NA/GD-1370EU）および<br>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Ⅰ（GD-1370J/<br>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Ⅰ（GD-1370J/<br>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Ⅰ（GD-1370J/<br>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Ⅰ（GD-1370J/<br>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<br>MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V1.0 | デジタル複合機 | C0566 | EAL2※3+ |
| TOSHIBA e-STUDIO5508A/6508A/7508A/8508A MULTIFUNCTIONAL<br>DIGITAL SYSTEMS SYS V1.0 | デジタル複合機 | C0529 | EAL3+ |
| TOSHIBA e-STUDIO5506AC/6506AC/7506AC MULTIFUNCTIONAL<br>DIGITAL SYSTEMS SYS V1.0 | デジタル複合機 | C0528 | EAL3+ |
| TOSHIBA e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A<br>MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V1.0 | デジタル複合機 | C0524 | EAL3+ |
| TOSHIBA e-STUDIO2505AC/3005AC/3505AC/4505AC/5005AC<br>MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V1.0 | デジタル複合機 | C0523 | EAL3+ |
| TOSHIBA e-STUDIO2000AC/2500AC MULTIFUNCTIONAL<br>DIGITAL SYSTEMS SYS V1.0 | デジタル複合機 | C0522 | EAL3+ |
| TOSHIBA e-STUDIO5560C/6560C/6570C MULTIFUNCTIONAL<br>DIGITAL SYSTEMS SYS V3.0 | デジタル複合機 | C0491 | EAL3+ |
| TOSHIBA e-STUDIO557/657/757/857 MULTIFUNCTIONAL<br>DIGITAL SYSTEMS SYS V3.0 | デジタル複合機 | C0490 | EAL3+ |
| TOSHIBA e-STUDIO207L/257/307/357/457/507<br>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-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（2021 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 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

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は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

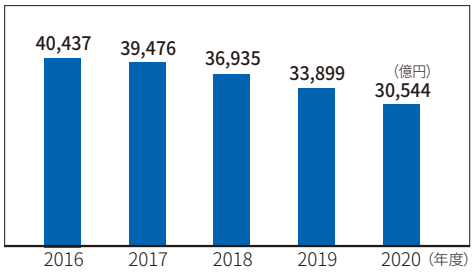
2021年3月31日現在

## 会社概要

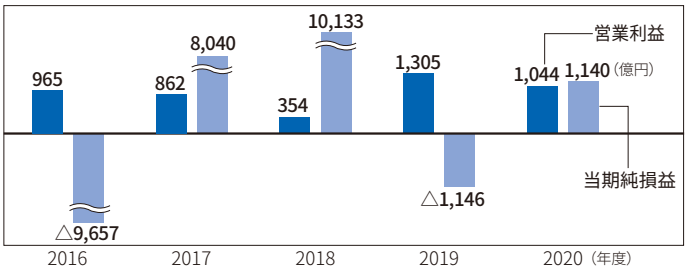
| | |
|---|---|
| 社　　名 | 株式会社 東芝<br>(TOSHIBA CORPORATION) |
| 本社所在地 | 東京都港区芝浦1-1-1 |
| 創　　業 | 1875年（明治8年）7月 |
| 資 本 金 | 2,005億5,800万円 |
| 連結売上高 | 3兆544億円 |
| 連結従業員数 | 117,300人 |
| 発行済株式総数 | 4億5,528万株 |
| 上場証券取引所 | 東京、名古屋 |

## 業績（連結）

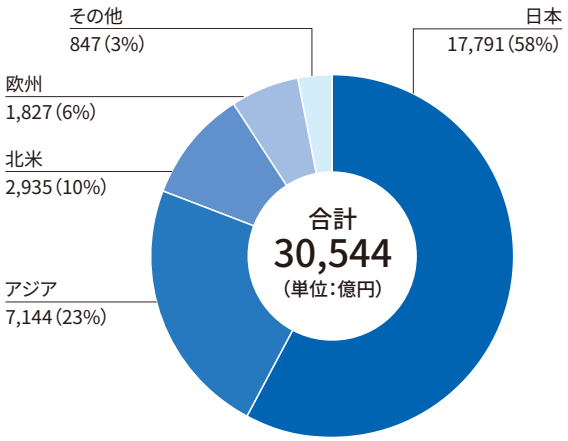
### 売上高の推移



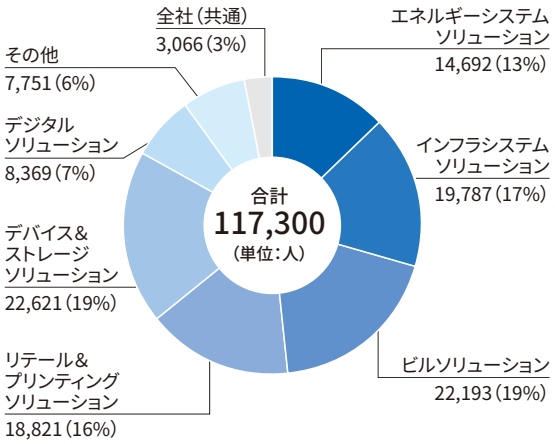

### 営業利益／当期純利益（損失）の推移



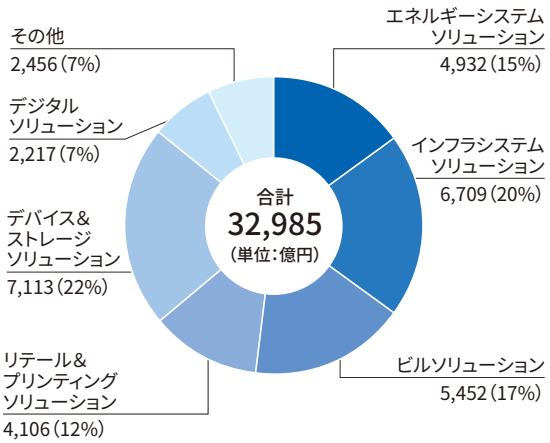

### 地域別売上高




### 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2,442億円含む）

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


**2021年6月発行**

**Printed in Japan**