第94回運輸政策セミナー

社会インフラを支える製造業における サプライチェーンセキュリティの取組
～サイバーレジリエンスの向上に向けて～

TOSHIBA

2024年12月13日

株式会社東芝　サイバーセキュリティ技術センター
古川　文路

Contents

01

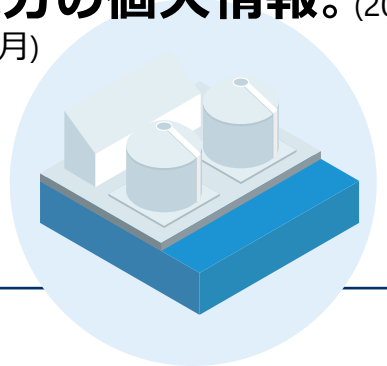
サプライチェーンセキュリティを取り巻く動向

サプライチェーンに起因するサイバーインシデント事例

製造業や社会インフラのサプライチェーンを標的とするランサムウェア攻撃が増加

サプライチェーンからの情報漏洩リスク

複数自治体の水道局やガス事業者から、業務委託先のネットワークが第三者から不正アクセスを受け、**約416万人分の個人情報。**(2024年7月)

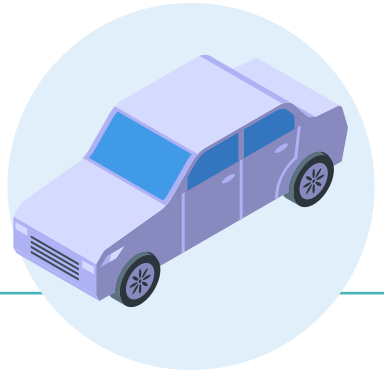


サプライチェーンからの不正侵入等リスク

公立病院がランサムウェア攻撃を受け、**電子カルテシステムに障害が発生。**(2022年10月)

サプライヤーの停止による事業継続リスク

自動車部品メーカーが、ランサムウェア攻撃を受けサーバがダウン。(2022年3月)



ソフトウェアを通じたサプライチェーンリスク

クラウドサービス提供事業者の**データセンターのサーバーが不正アクセスされ、ランサムウェアに感染。**(2023年6月)

狙われる重要インフラ

製造業が集積する中部地方の主要港名古屋港が
ランサムウェア攻撃で3日間停止

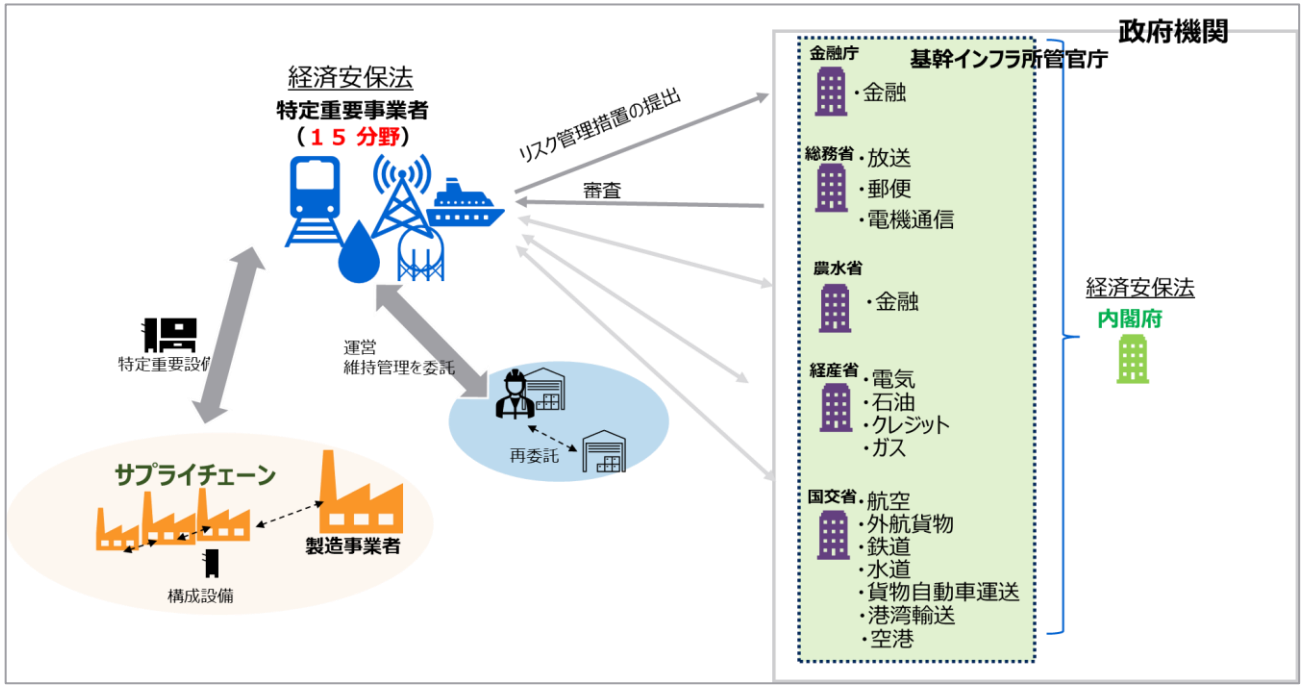
多数の荷主のサプライチェーンが途絶し、経済に多大な影響が生じる

サプライチェーンセキュリティに関する国内の政策事例

経済安全保障推進法に基づく届出はサプライチェーン全体で対応が必要

基幹インフラ役務の安定的な提供の確保に関する制度

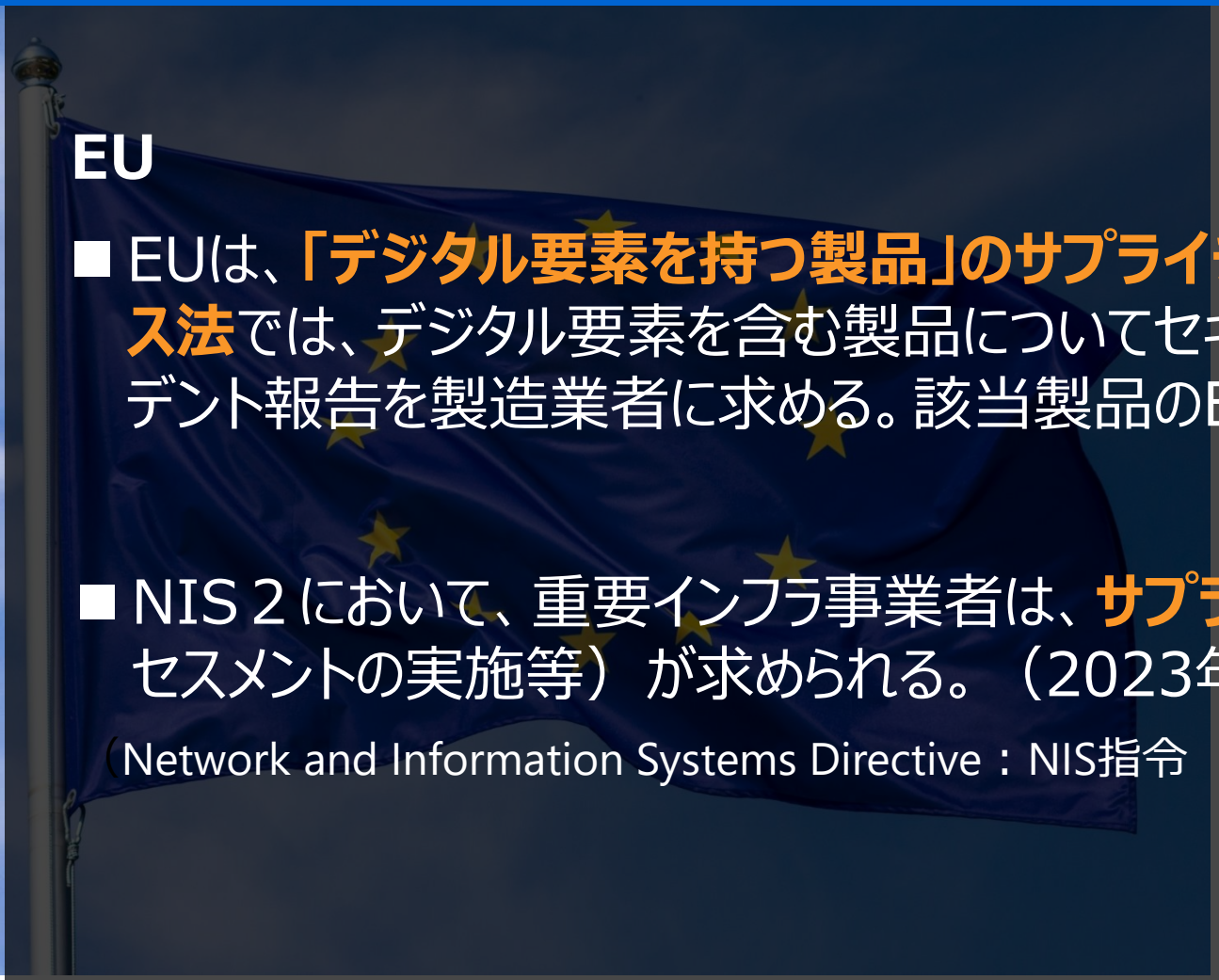
- サプライチェーンを狙った攻撃の増加を踏まえ、経済安全保障推進法の下、重要インフラ事業者の**特定重要設備**に対して**事前審査**を導入。2024年5月17日から施行。
- 役務の安定的な提供を妨害する行為の手段として使用されることを防止するため、**重要設備の導入・維持管理等の委託を事前に審査**。



https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/doc/infra_setsumeikai.pdf （内閣府の資料を基に作成）

EUのサプライチェーン強化に向けた規制の動向

EUでは2027年12月からサイバーレジリエンス法が全面適用に



EU

■ EUは、**「デジタル要素を持つ製品」のサプライチェーン対策**を重視。**EUサイバーレジリエンス法**では、デジタル要素を含む製品についてセキュリティ要件の実装、脆弱性の管理、インシデント報告を製造業者に求める。該当製品のEUへの上市にはCEマークが必須に。

■ NIS２において、重要インフラ事業者は、**サプライチェーンのセキュリティ対策状況の確認**（アセスメントの実施等）が求められる。（2023年1月16日に発効）

（Network and Information Systems Directive：NIS指令

※SBOM： Software Bill of Materials（ソフトウェア部品表）

工場・プラントのセキュリティ規制・標準化動向

自動車や半導体など重要産業への攻撃増加により、工場システム・装置に対する規制が強化

自動車
TISAX®

- 自動車サプライヤーに対する情報セキュリティ認証制度
- ドイツ自動車メーカーとの取引でサプライヤーが審査を受ける

*VDA（ドイツ自動車工業会）

半導体
SEMI E187

- 半導体製造装置のサイバーセキュリティ規格。製造装置に求める対策を定義
- 半導体工場が製造装置の購入契約における要求事項として使用

*SEMI：Semiconductor Equipment and Materials International（国際半導体製造装置材料協会）

経産省
工場セキュリティガイドライン

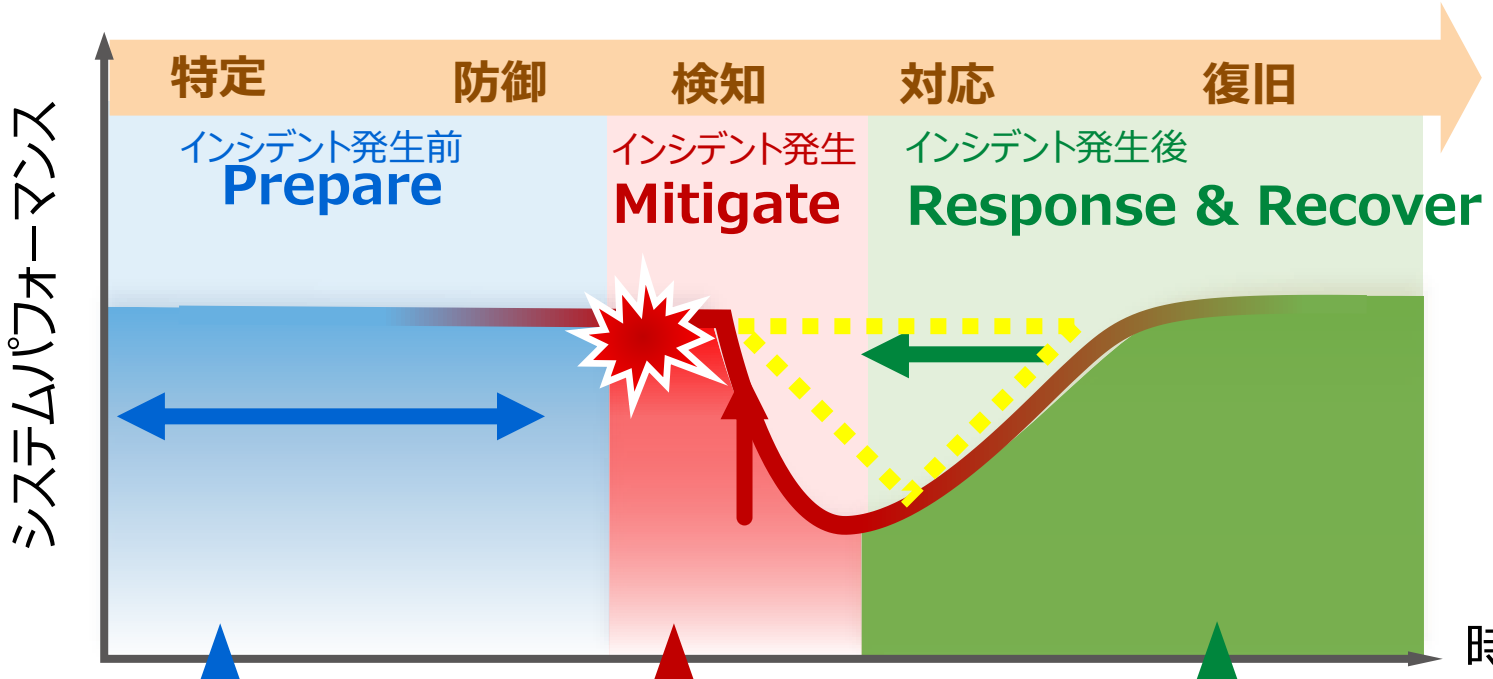
- 工場システムのDXを進める上で、セキュリティ対策を進める際の参考となる考え方やステップの手引き書

02

東芝グループのサプライチェーンセキュリティの取り組み

サイバーセキュリティ強化に向けた戦略 「サイバーレジリエンス」

インシデントに「備え」、「影響を最小化」し、「早期に回復」して、事業を継続する『能力』



備える

- 脆弱性を**早期に**発見
- リスクを**未然に**摘み取る
- 日頃の訓練を通じてインシデントに備える

影響を最小化する

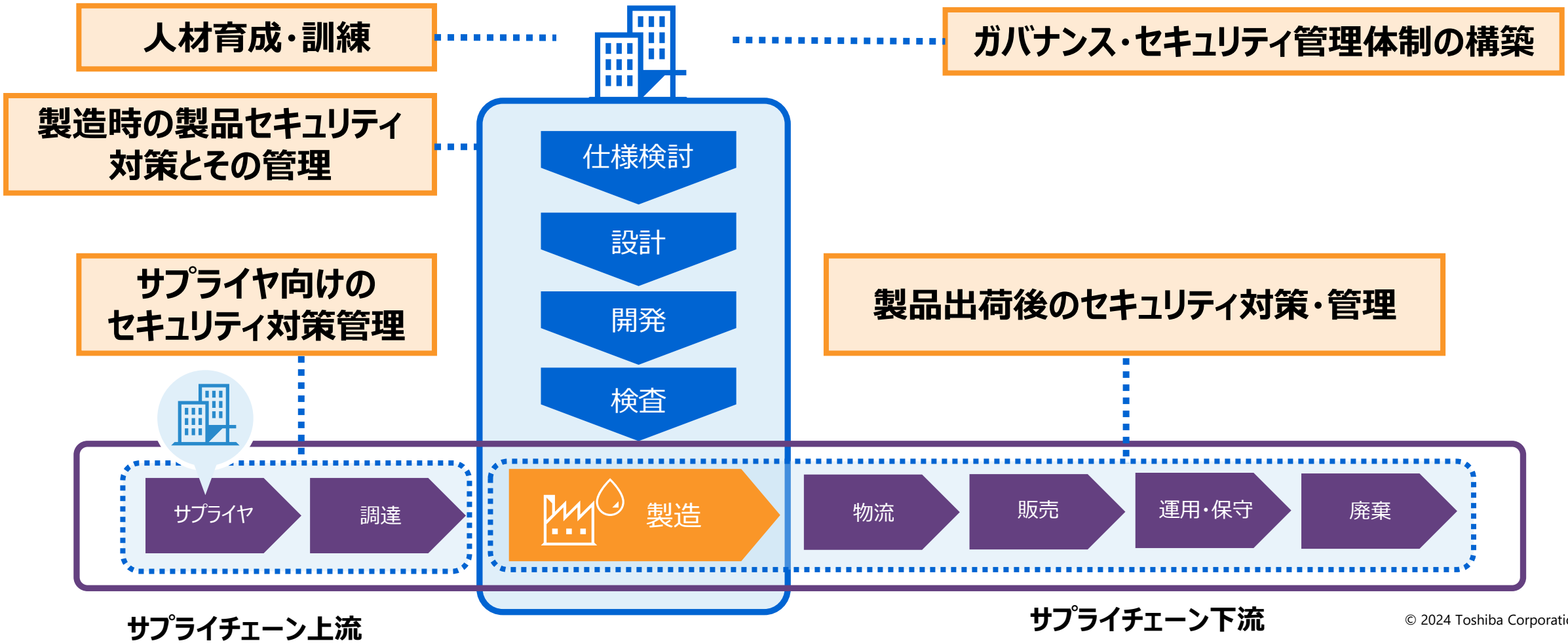
- 脅威情報を活用した**監視による早期検知・対処**により影響の極小化

早期に回復する

- **継続的監視**
- 端末ログ情報の活用による原因の早期究明

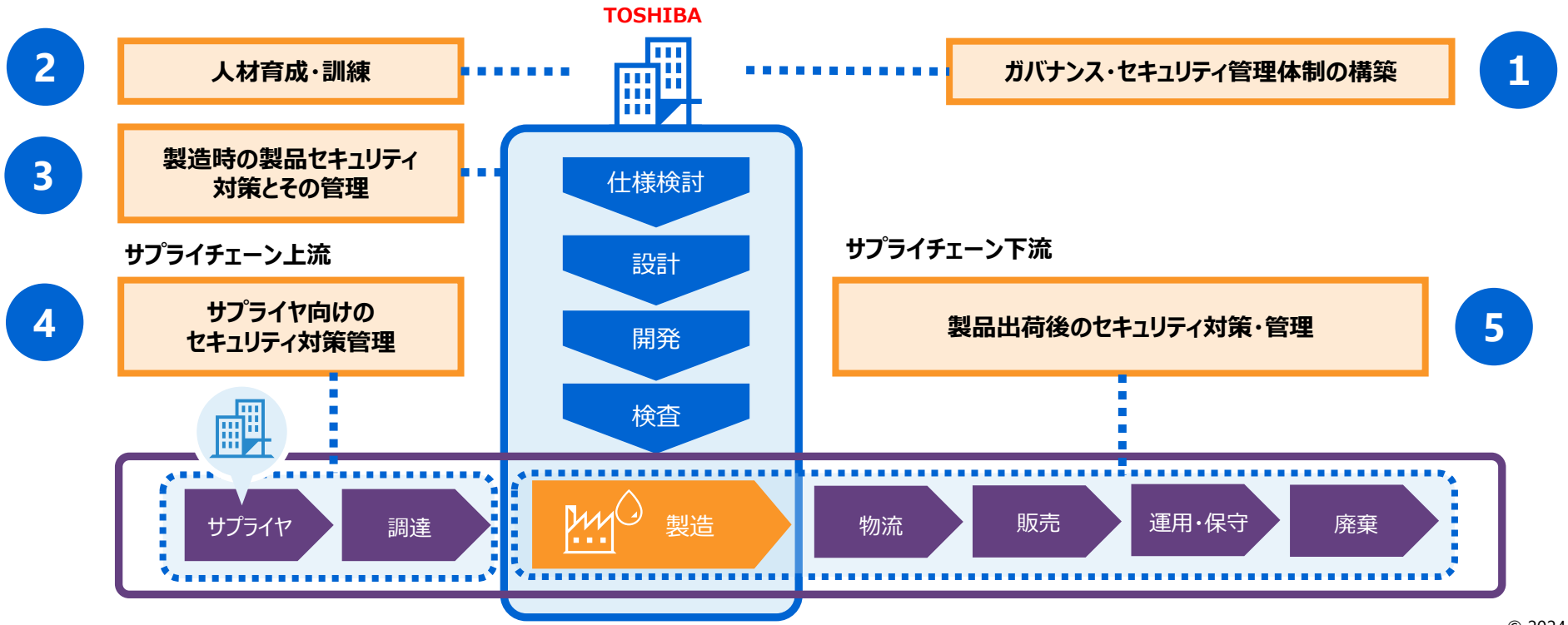
求められるサプライチェーンセキュリティ対策の全体像

自組織・製品のセキュリティ対策に加えサプライチェーン上流・下流の対策・管理も必須に



東芝のサプライチェーンセキュリティの取り組み

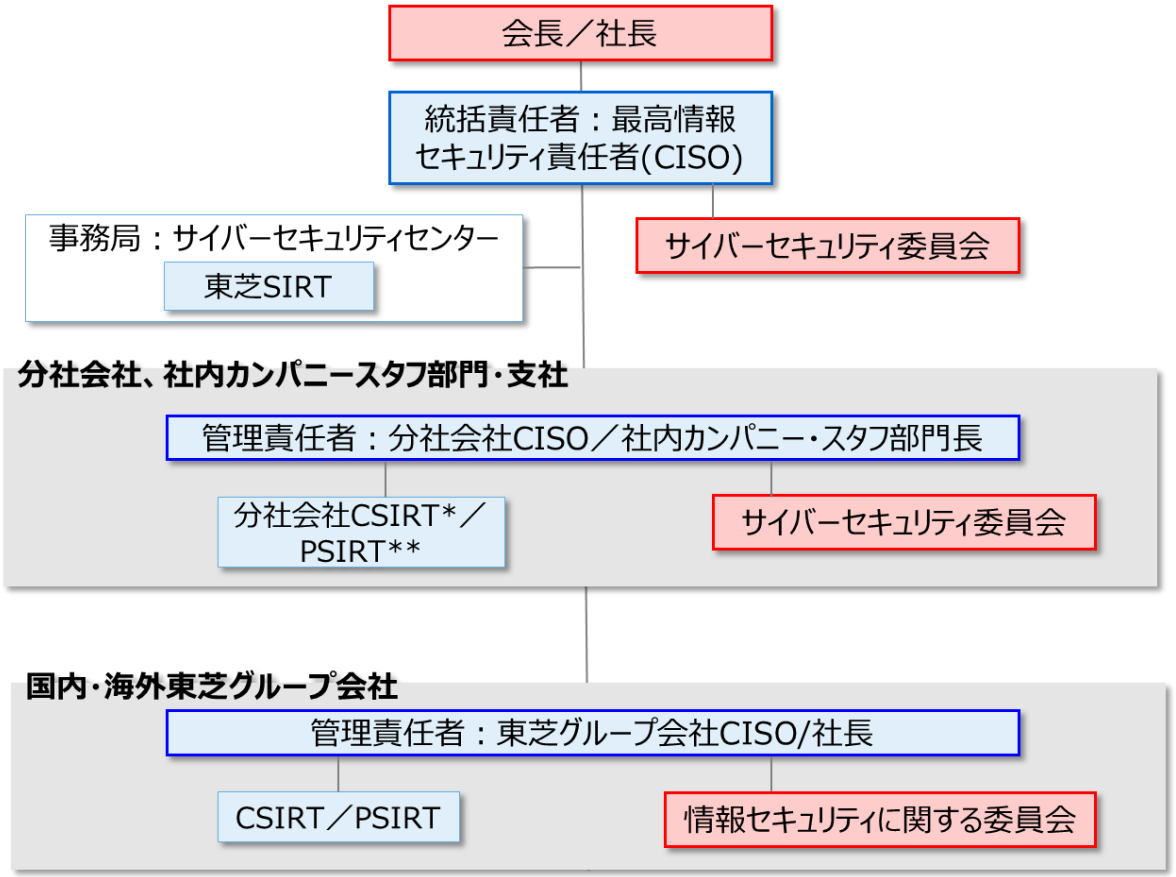
1. セキュリティガバナンス・運用体制の構築
2. 人材育成・訓練
3. 製品セキュリティ対策とその管理
4. サプライヤのセキュリティ対策管理
5. 製品出荷後のセキュリティ対策管理



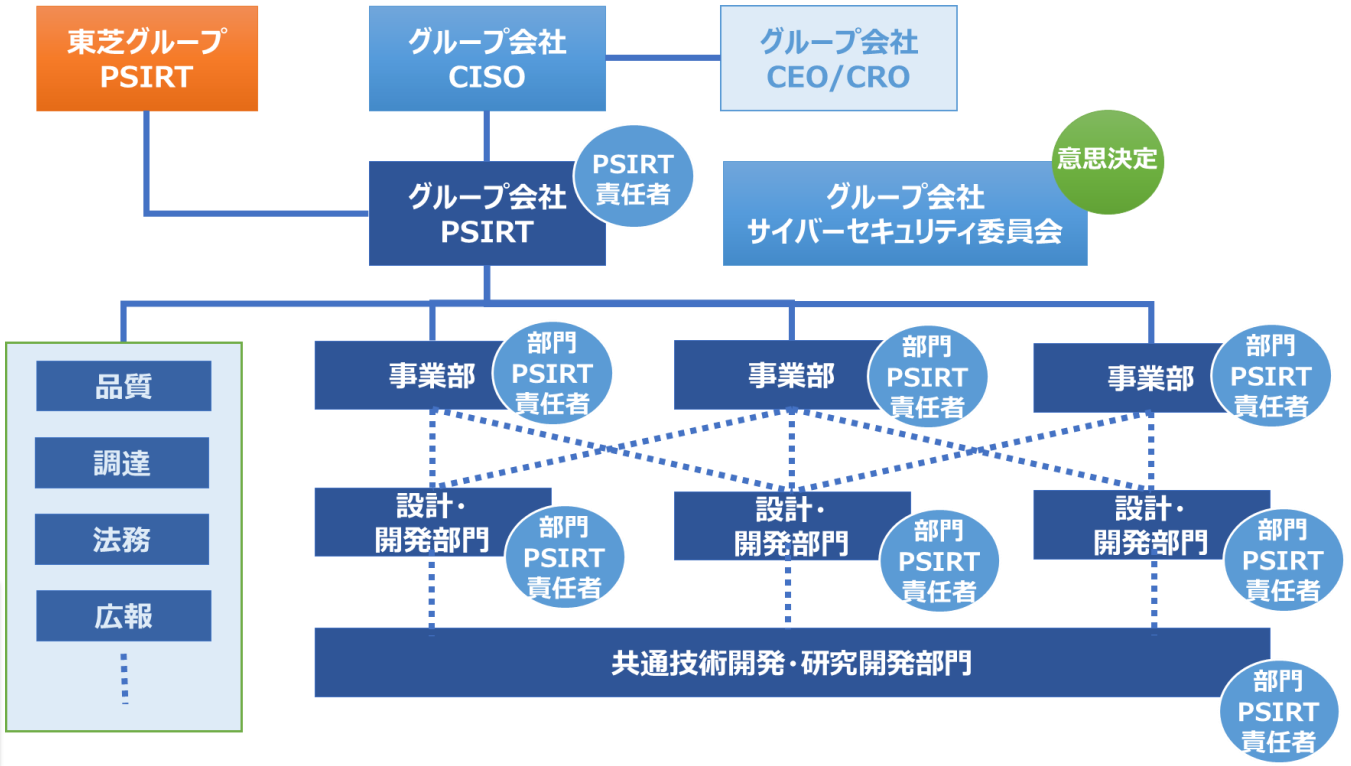
ガバナンス・セキュリティ管理体制の構築

①ガバナンス

ガバナンス組織としてのサイバーセキュリティセンターを中心に
東芝グループのITインフラと製品セキュリティリスクマネジメント体制を強化



サイバーセキュリティマネジメント体制



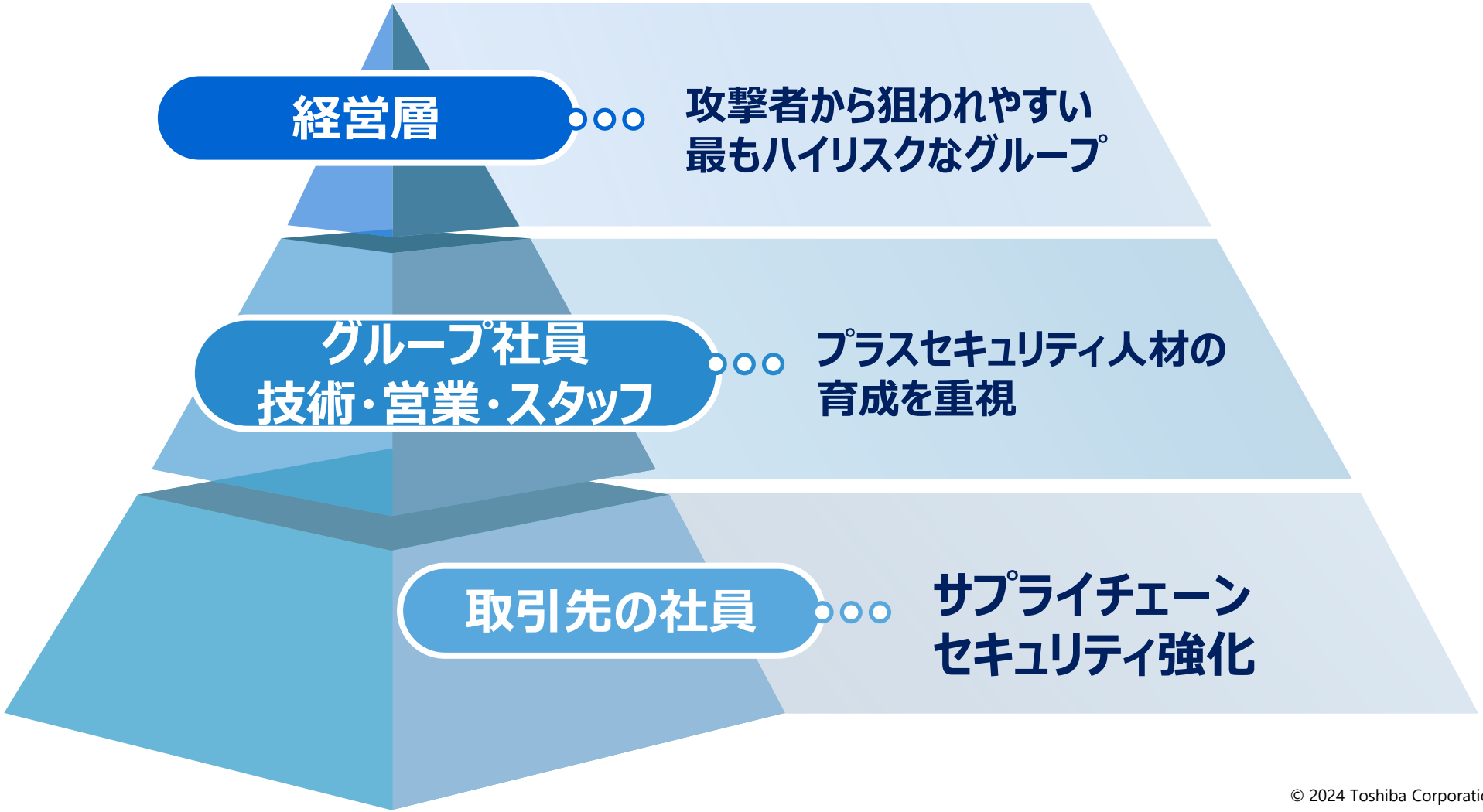
製品セキュリティリスクマネジメント体制

*CSIRT：Computer Security Incident Response Team，**PSIRT：Product Security Incident Response Team

人材育成・訓練：3階層で人材育成カリキュラム・教育訓練を推進

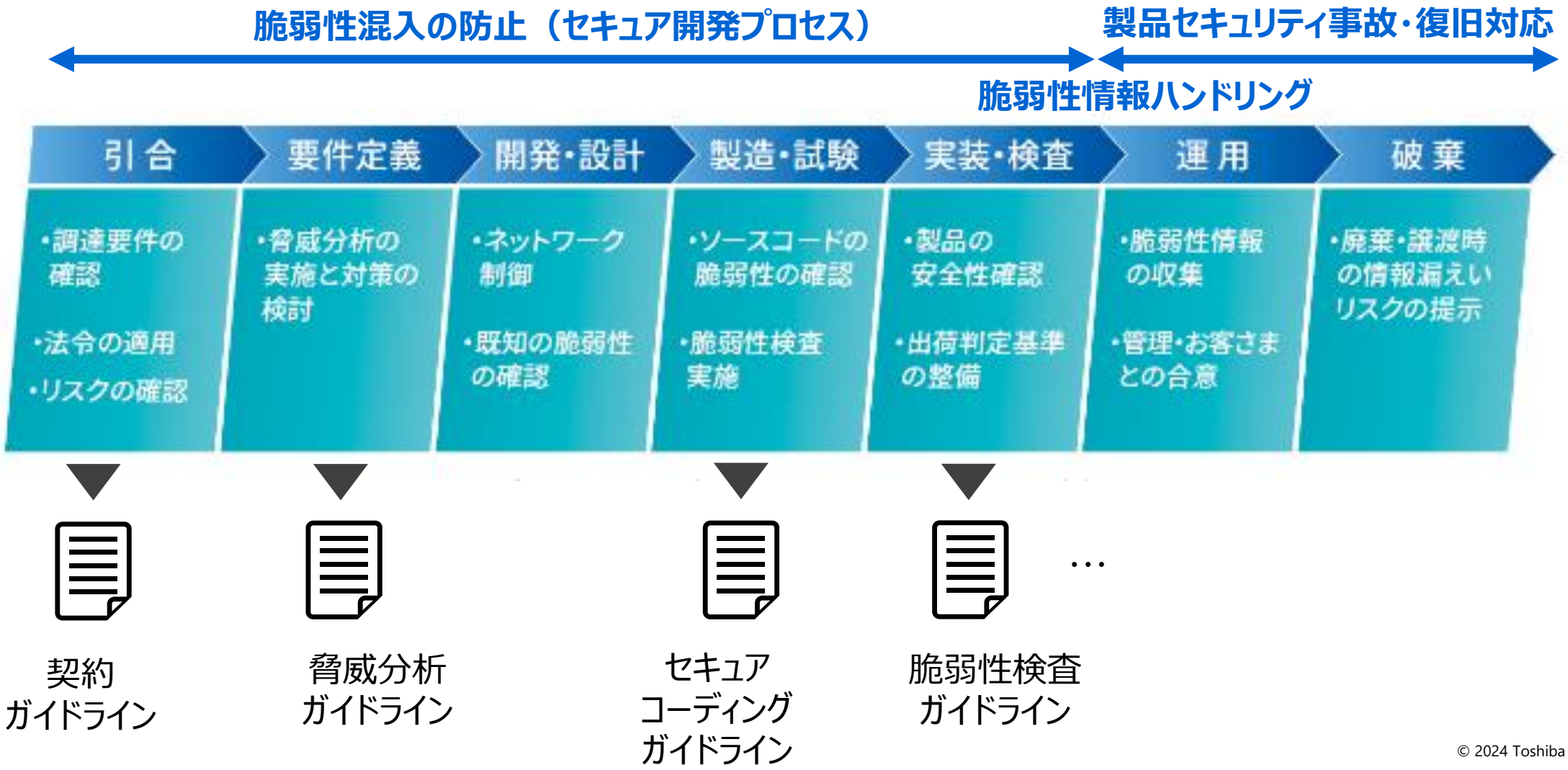
②人材

国内外の東芝グループだけでなく、取引先も含めたリテラシー向上と対策のフォローアップ



製品セキュリティ対策とその管理

製品ライフサイクルの各フェーズでガイドラインやチェックリストを整備、脆弱性混入を防止



サプライヤのセキュリティ対策管理

④サプライヤ

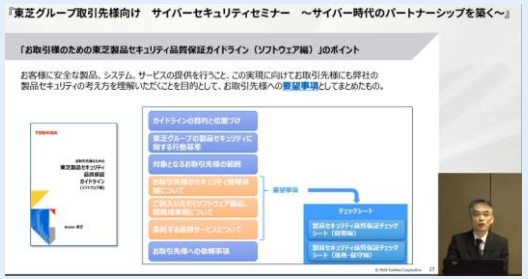
ビジネスパートナーや取引先等を含めたサプライチェーン全体のセキュリティ品質向上

1. 東芝製品セキュリティ品質保証ガイドラインを配付

「お取引先さまのセキュリティ管理体制」「ご納入いただくソフトウェア製品の開発成果物」「委託する運用サービス」の３点について、具体的なセキュリティ要望事項を定め、**取引開始時に配付**、周知し、東芝グループが求めるセキュリティ要望事項をご理解いただいています。

2. 東芝グループ取引先様向けサイバーセキュリティセミナー開催

お取引先さま向けの**相談窓口を開設**し、**調達部門と連携**して、東芝製品のセキュリティ品質保証に関するオンライン説明会を開催。約7,000社の東芝グループお取引先に向けて、セミナーを実施。



配信映像(イメージ)

アンケートで9割以上
が役に立つと回答

サプライヤのセキュリティ対策管理

④サプライヤ

**ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握に
アタックサーフェス調査を利用し可視化。リスクを把握し、是正への協力を依頼**

課題と対応策

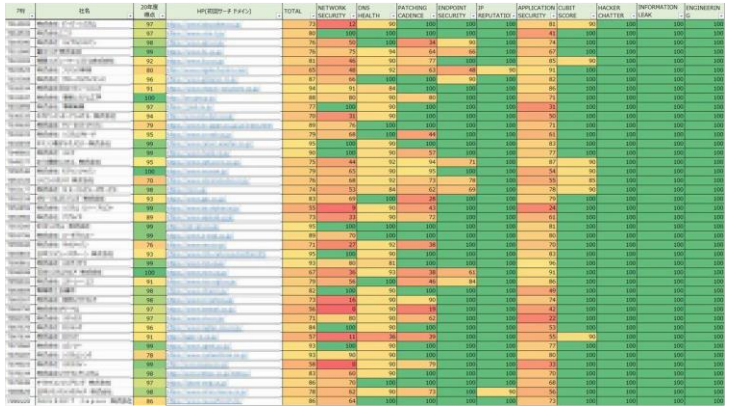
- 取引がある協力会社の規模は大小様々であるため、**点検を効率的**に行いたい。
- 従来の情報セキュリティ点検だけでは、**実際のセキュリティホールは見つからない**。
- **サプライチェーンからの情報漏えい**リスクが高まっている。

**協力会社への攻撃リスクを
客観的に評価する仕組みが必要**

取引先の手を煩わせることなく、短時間で脅威を把握できる手法として、**アタックサーフェス調査** に注目

アタックサーフェス調査結果例

協力会社の診断項目別のスコアー覧例



サプライヤのセキュリティ対策管理

④サプライヤー

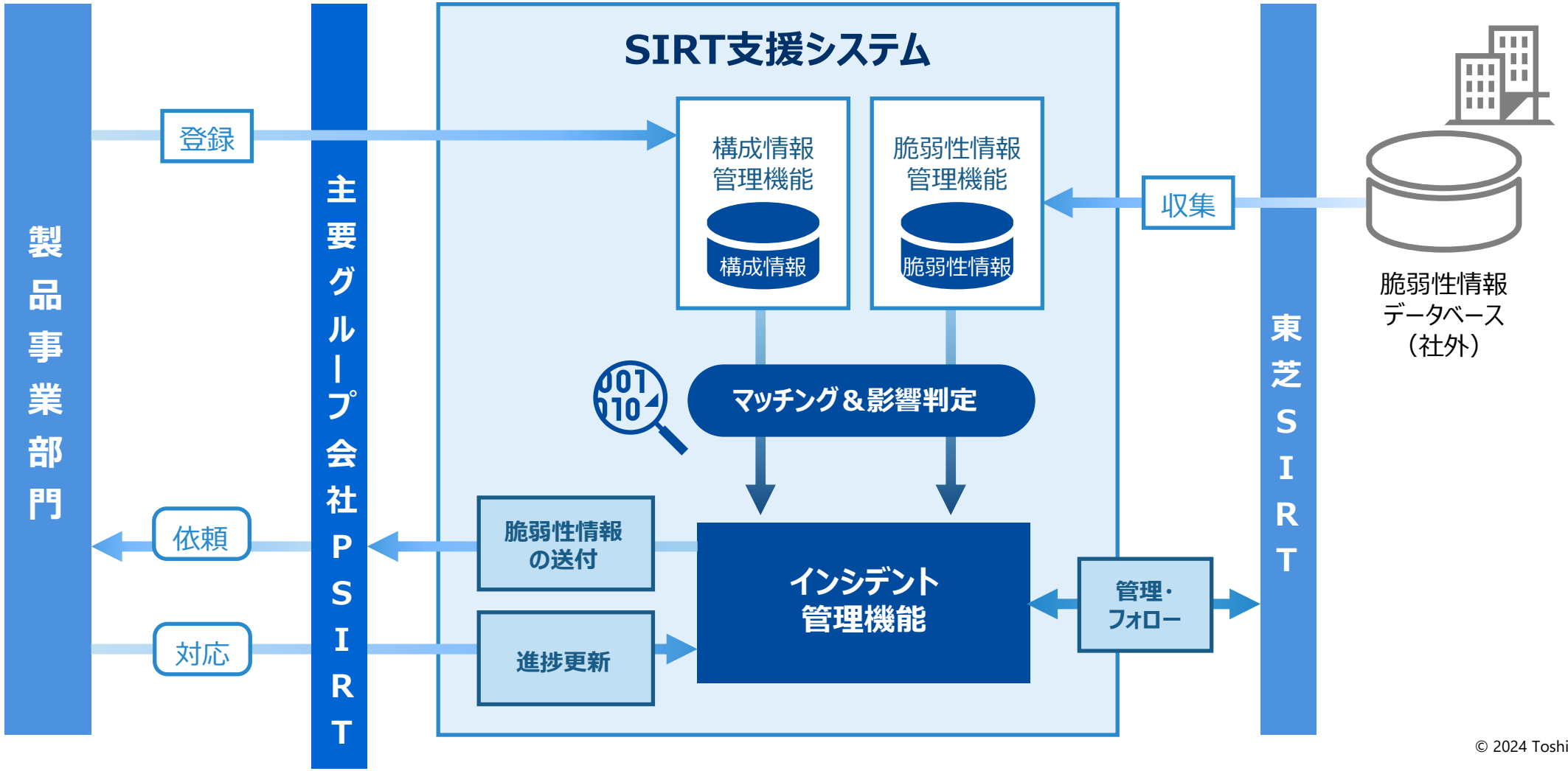
サプライチェーン企業が主体的、かつ真剣に取り組む必要がある

- チェックリストによる自主点検 ・・・ **オレオレ評価、実効性に疑問**
- 取引先への現地審査 ・・・ **コスト増、対応人材の確保**
- 導入ツール、対策の強制 ・・・ **下請法・独禁法抵触の恐れ**
- 導入ツール、施策提供 ・・・ **利益供与（資産贈与）**
- 価格転嫁 ・・・ **競争力低下、経営インパクト**

製品セキュリティ対策とその管理

⑤製品出荷後

SIRT支援システムにより製品出荷後の脆弱性ハンドリングを可視化・自動化



製品セキュリティインシデント

⑤製品出荷後

クラウド環境でのランサムウェア感染を題材とし、経営層、事業部、PSIRTが連携
インシデント対応の「初動対応」「緊急検討会議」「ケーススタディ」を行う実践的演習
（特に今後は取引先も含めた訓練を実施）

実践的演習の内容：

- 各部門のプロセスと役割を確認
- 演習では計3時間で約20枚の状況付与カードを付与
- 同じカードは必ずしも全てのチームには配布されず、情報量に偏りをもたせる

参加者の声：

- インシデント発生時の報告ルート、報告後の作業の流れが確認できた
- 自社のルールについても理解があいまいな部分があった
- 報告ルートなど、社内ルールの再点検をする必要がある

03

情報共有・情報発信の取組

東芝グループ、取引先への情報発信・共有

サイバーセキュリティ報告書を毎年発行、専門家を招いた講演会や四半期毎のCISO会議

社外の専門家を招いたセキュリティ講演会
（年３～４回実施）

- 欧州サイバーレジリエンス法の動向
- 生産性向上のためのセキュリティ対策の考え方等

サイバーセキュリティ報告書2024

東芝グループのサイバーセキュリティ活動に関する取組みとして年1回発行

四半期毎の東芝グループCISO会議

各事業体のインシデント情報、セキュリティの課題について議論

社外との情報交換とリテラシー向上に向けた社外活動

- サイバーセキュリティを**協調領域**と捉え、各企業や業界団体とオープンに情報交換
- 各種業界団体セミナーや、都内大学院での授業で**現役から次世代に向けた**啓発を実施

1. 情報交換

■ 社外との情報交換

- 各社セキュリティ担当との情報交換を定期的に実施
- 業界団体への参加を通じた情報交換

2. リテラシー向上

■ 業界団体での講演活動

- 大阪府工場協会様
- 千葉県経営者協会様
- 電力ISAC様

他、多数

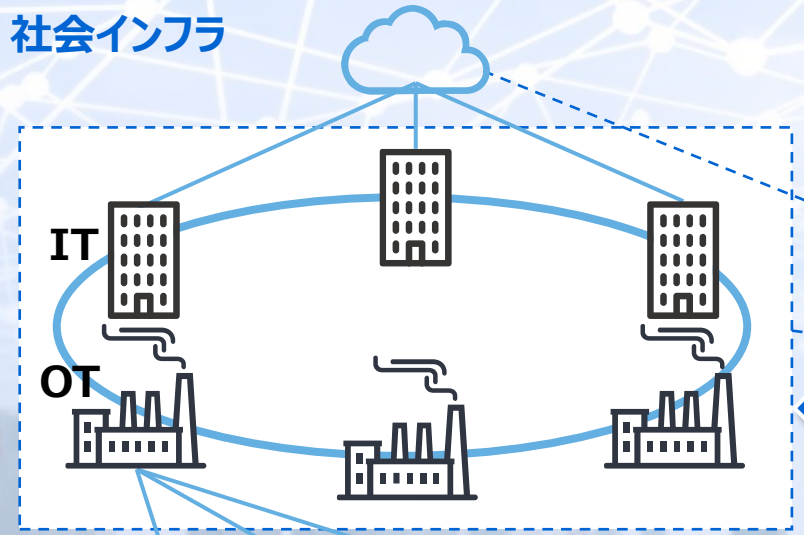
■ 次世代に向けた教育・啓発活動

- 大学院での授業
- うんこドリル

お子様向けの啓発として全国の小学校に83,000冊寄贈

最後に：サプライチェーンセキュリティ強化に向けて

サプライチェーン全体のセキュリティリテラシー向上、社会インフラのレジリエンス向上



TOSHIBA

東芝グループ経営理念

人と、地球の、明日のために。

Committed to People,
Committed to the Future.

TOSHIBA