複製・第三者への開示はご遠慮ください。

春光懇話会全体セミナー　資料

日立グループにおけるサイバーレジリエンス強化の取り組み

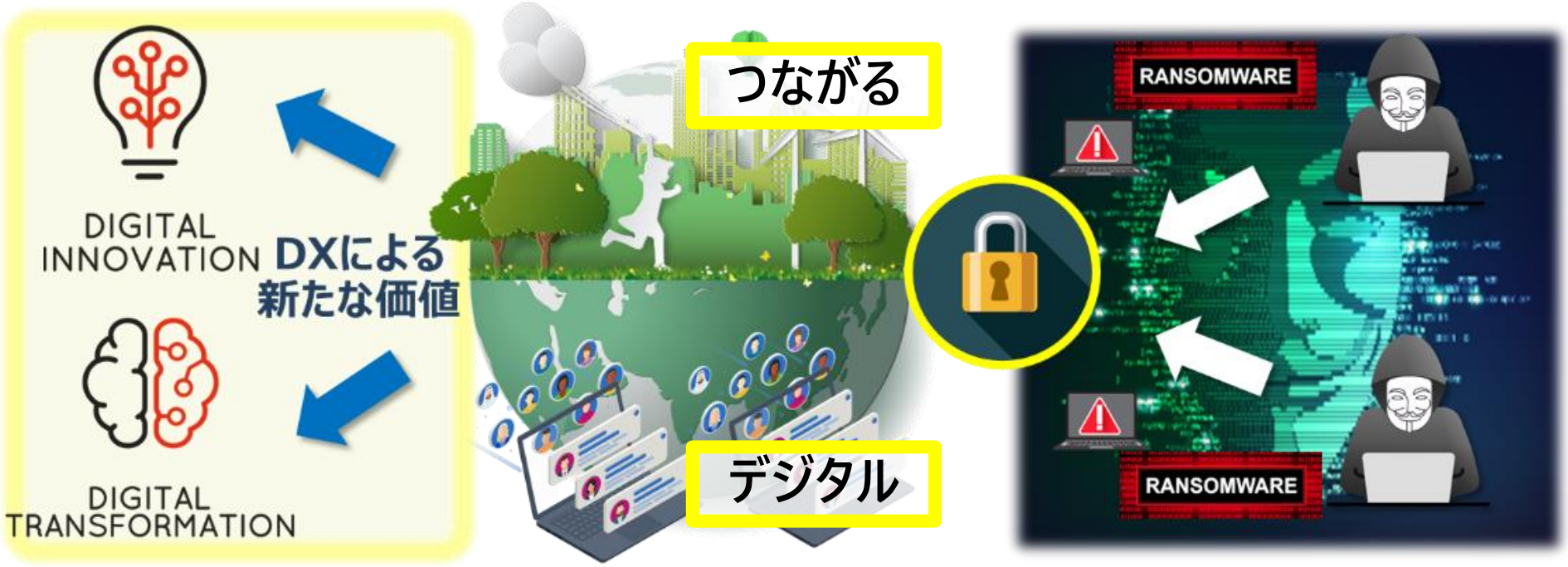
2025/7/23

株式会社 日立製作所　情報セキュリティリスク統括本部　村山 厚

©Hitachi, Ltd. 2025. All rights reserved

企業を取り巻く環境　～世の中の大きな2つの流れとリスク～

世の中を便利にする
新潮流デジタルトランスフォーメーション(DX)と働き方改革



最大のリスクは**サイバーセキュリティ**

©Hitachi, Ltd. 2025. All rights reserved

最近のセキュリティの脅威を振り返ってみる

世の中のセキュリティ動向

アタックサーフェスの拡大(攻撃の網羅性及び速度UP)

- DDoS攻撃による事業システム停止
- ランサムウェア、情報暴露等の攻撃がさらに増加
- サプライチェーンがサイバー攻撃を受け事業影響が発生
- ネットワーク機器の脆弱性を悪用した攻撃の増加
- クラウドサービスへの攻撃増加
- 生成AI系サービスにおける意図せぬ情報共有の顕在化

内部不正による情報漏えい

事象発生後の影響

- 事業中断
- 社内業務の停止
- ステークホルダーへの被害(迷惑)

事業そのものへ影響をおよぼしている

今まで以上に「経営」としてセキュリティを考えなければいけない状況

©Hitachi, Ltd. 2025. All rights reserved

サイバーセキュリティビジョン

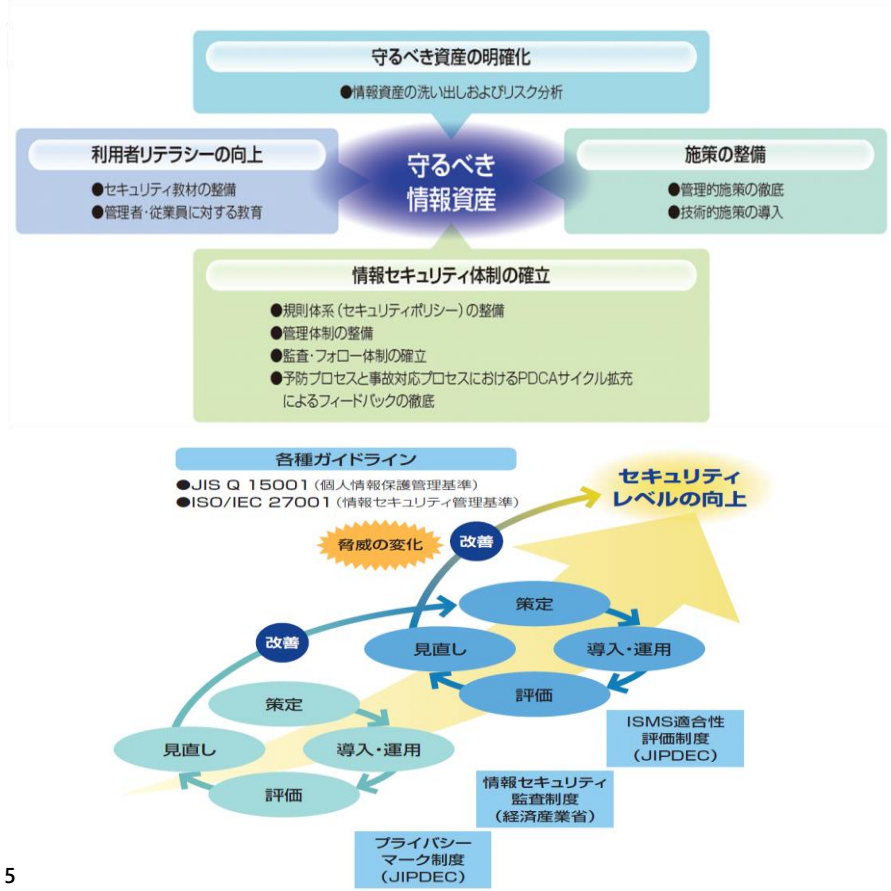
統制	サイバーセキュリティを経営課題として位置づけたセキュリティ対策を継続的かつ着実に実行する。 しかし、絶対の安全はない。 ゆえに、有事の際には、短い時間で回復できる抵抗力をつける。
協創	高度化/増加するサイバー攻撃へ対処するために、 社内コミュニケーションを拡充し、共感を得る。 さらには、社会全体でのセキュリティエコシステムを構築し、仲間を増やす。
自分ゴト化	一人ひとりがセキュリティを正しく理解・共感し、 自分ゴトとしてとらえて行動することができる意識づくりを醸成する。

サイバーレジリエンスの強化
➡ しなやかなセキュリティ耐性を身につける

©Hitachi, Ltd. 2025. All rights reserved

ビジョンを実現するために

リスクへ対応するためにやるべきことを決めて準備を行う
＝有事の際には、効果的に対応できるようにしておくこと



リスクへ対応するために準備行うことが重要

全ての活動は有事に備えた準備をすること

- 準備(Readiness)　予防準備
- 事象発生
- 対応(Response)　事象への対応
- 回復(Recovery)　システム復旧 再発防止

©Hitachi, Ltd. 2025. All rights reserved

統制

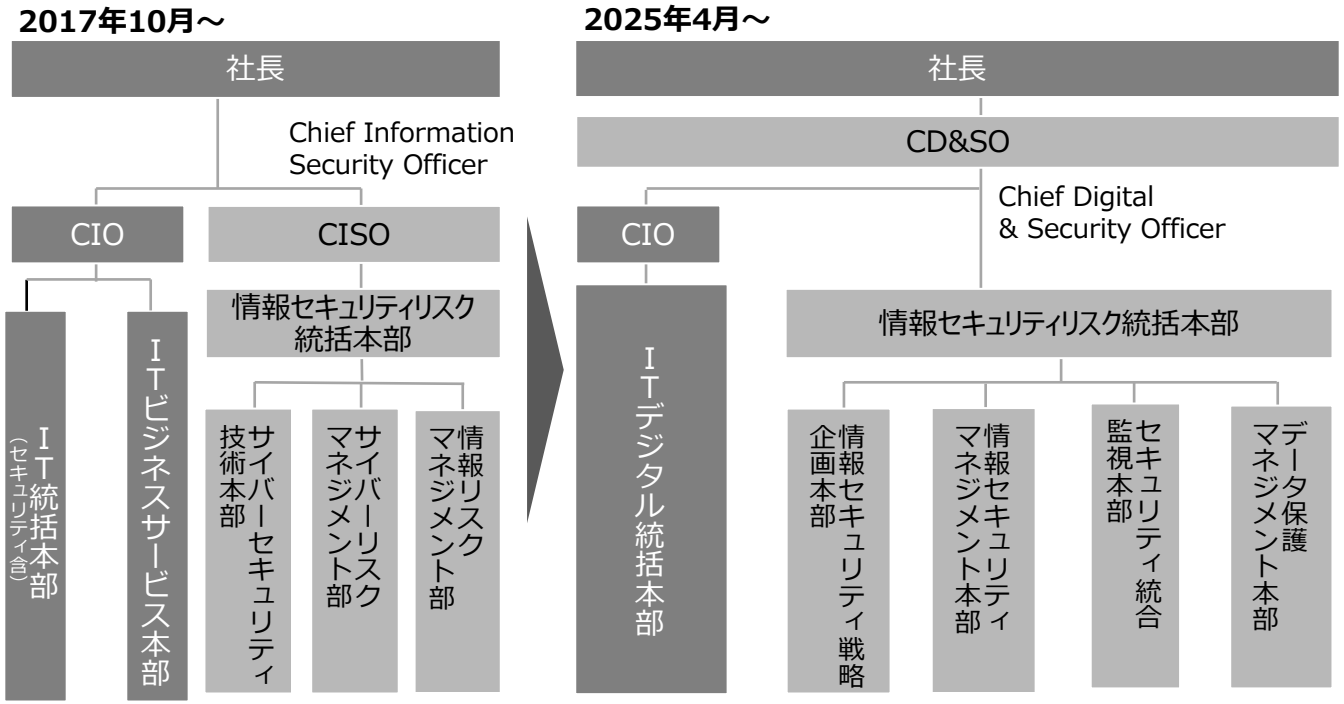
サイバーセキュリティを経営課題として
位置づけたセキュリティ対策を継続的
かつ着実に実行する。
しかし、絶対の安全はない。
ゆえに、有事の際には、短い時間で
回復できる抵抗力をつける。

©Hitachi, Ltd. 2025. All rights reserved

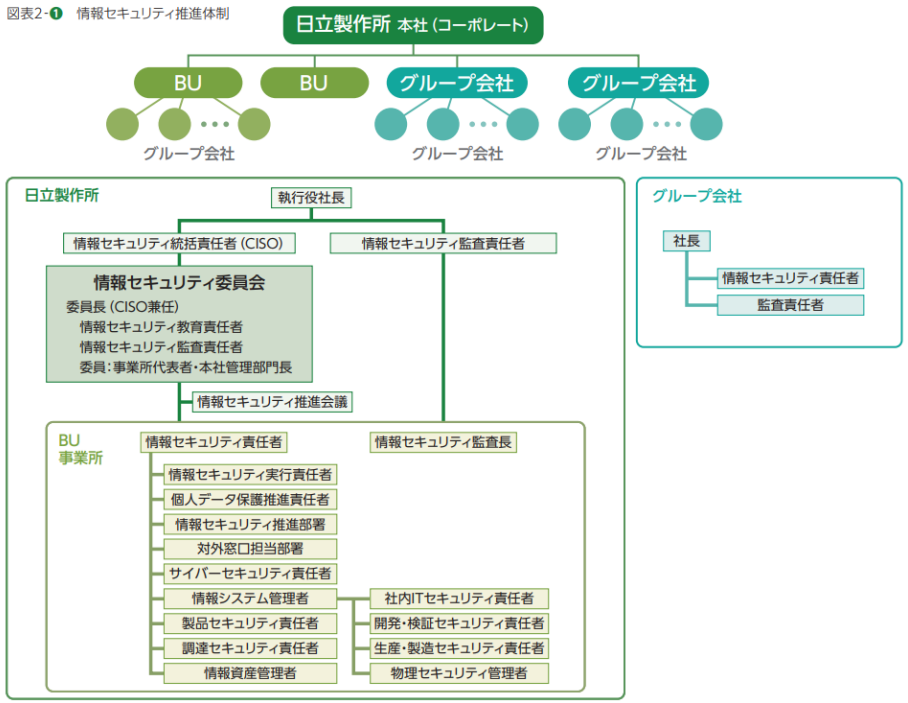
セキュリティガバナンス組織の設置

事業継続の担保、機密情報漏えいの防止、日立提供サービス経由による顧客感染の防止をするために、
サイバーセキュリティを経営課題と位置づけ2017年10月1日に、単独のセキュリティ部門を設置し、
セキュリティガバナンスの更なる徹底を開始

2017/10月までは、IT部隊配下にセキュリティ部隊を配置していたものを、
2017/10月からは、セキュリティ部隊が独立してセキュリティガバナンスを実行



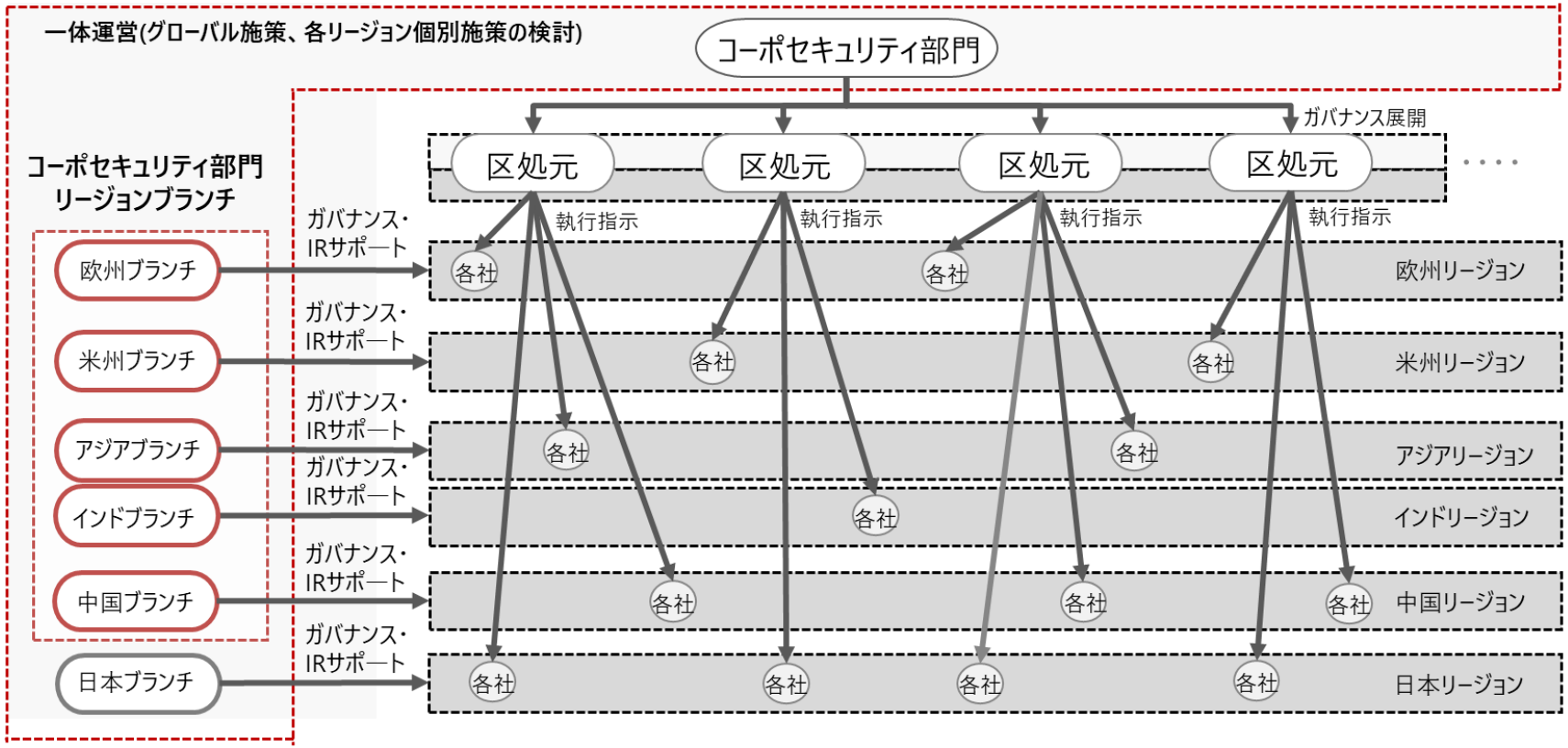
コーポレートは実行指示/モニタリングを実施し、BU各社の
事業特性を重視しつつ、委員会形式による合意制でガバナンス



グローバルセキュリティガバナンス体制

2023年～インシデントへの迅速な対応及び変化する地域法制への対応のため、平時の対応を強化

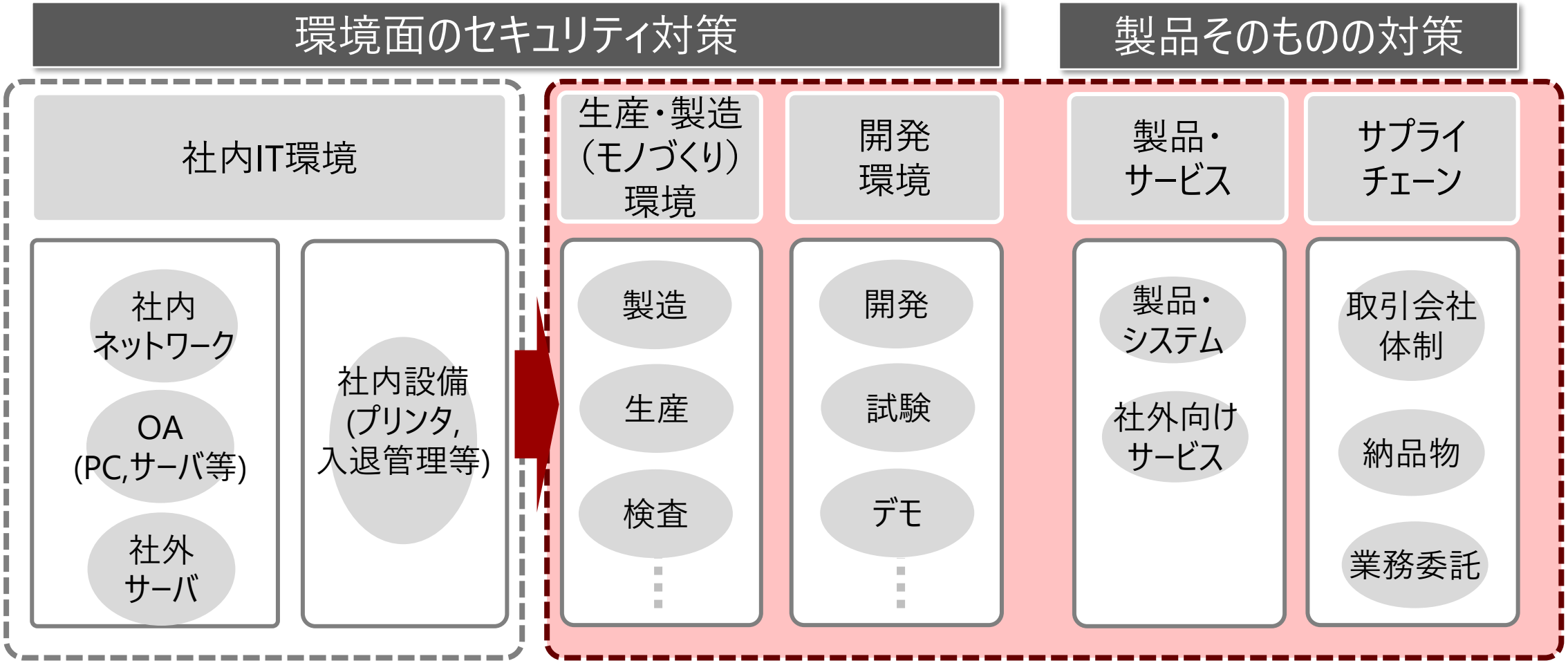
ブランチ設置目的		
1	**コミュニケーション強化**	⇒ 平時/有事における情報伝達度の底上げ
2	**インシデントマネジメント強化**	⇒ インシデント・法令対応窓口設置による対応迅速化
3	**マネジメントモニタリング強化**	⇒ モニタリング体制確立(3DL浸透)による対策定着化



©Hitachi, Ltd. 2025. All rights reserved

情報セキュリティ推進の対象範囲

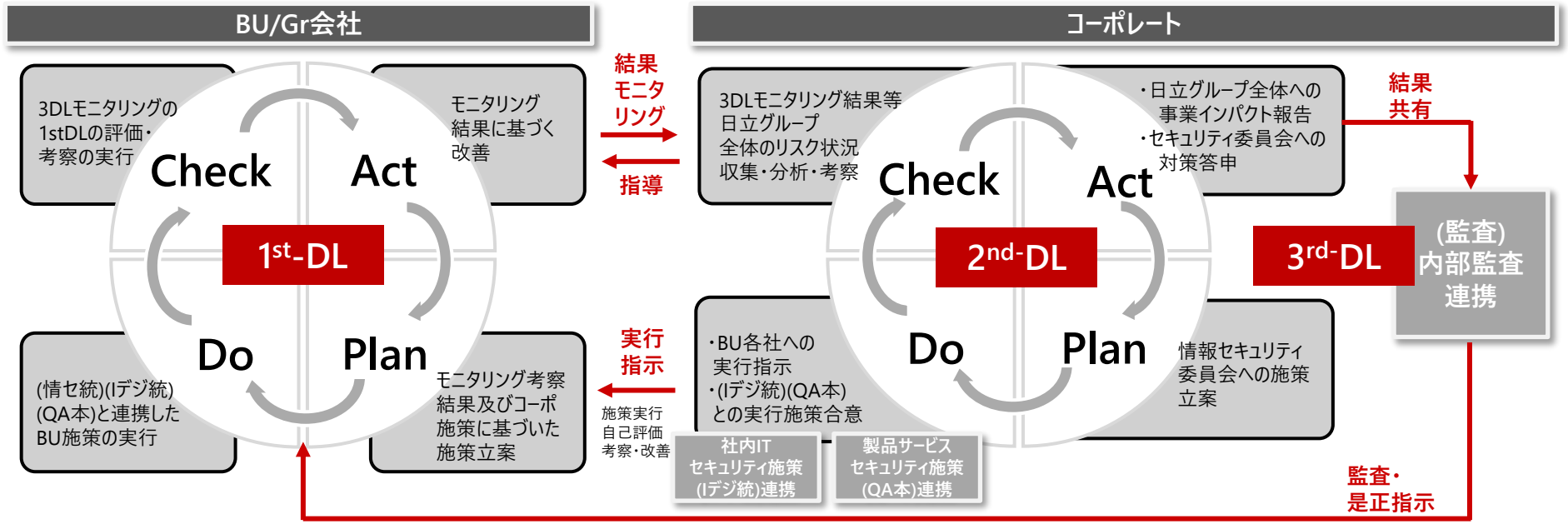
2017/下期以降、情報セキュリティガバナンスの範囲を社内IT以外の社内環境、製品にも拡大



©Hitachi, Ltd. 2025. All rights reserved

情報セキュリティマネジメントのPDCAサイクルモデル

活動の目的	製品サービスを作り出すための環境、プロセスまで領域を広げた網羅的なリスク低減
目指すべき姿	●1stDL：BU/Gr会社の自己点検実施後、各社の情報セキュリティ推進体制で結果を改善 ●2ndDL：コーポ主管部門から1stDLのBU/Gr会社への実行指示、および改善結果をモニタリング・指導 ●3rdDL：コーポレート監査部門がコーポ主管部門の2ndDLの結果をもとに、1stDLの監査・是正指示



©Hitachi, Ltd. 2025. All rights reserved

セキュリティ対策の取り組みの変化

フェーズ	潮流・攻撃の変化	具体的な強化策
2011年度~	増加する標的型攻撃 ⇒[情報窃取]型	**境界面での情報窃取対策** 多層防御(出入口対策) 早期検知(サイバー監視強化) 早期対応(IR強化)
2017年度~	WannaCry事案 ⇒[拡散+破壊]型	**システム破壊への対策** OTエリアのセキュリティ強化 パッチ適用徹底 サイバーBCP強化
2020年度~	• **新潮流DX** • **働き方改革** • **次世代高度標的型攻撃** **⇒[拡散+情報窃取＋破壊]型**	**ゼロトラスト・セキュリティ対応** **•認証/エンドポイントの検知/対応をより強固にする施策の推進** **•統合サイバー監視の実現**

IR：Incident response　OT：Operational Technology

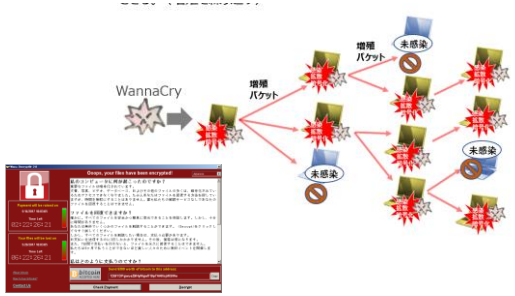
©Hitachi, Ltd. 2025. All rights reserved

11

2017年度のサイバーセキュリティ戦略　- WannaCry被害 -

きっかけは、自己増殖型ランサムウェアである「WannaCry」ウィルス感染事案

2017年5月12日深夜、日立グループ社内ネットワークのサーバーなどが、自己増殖型ランサムウェアである「**WannaCry**」ウイルスに**感染**し、**システム障害が発生**した。



●WannaCryの特長

Windowsのファイル共有機能の脆弱性を悪用して、自分自身を他の脆弱なWindowsシステムに感染させる**ネットワークワーム型のランサムウェア**

- 被害は社内ITだけでなく、生産・製造環境にも及んだ
- タイムリーにセキュリティパッチが適用できていなかったシステム系での被害が大多数
- 初期感染機器は、セキュリティ対策の意識されていない社内LANに接続されたデジタルマイクロスコープ
- バックアップからの復元に時間を要した
- 世の中脅威情報を上手に社内展開できていなかった

WannaCry感染

©Hitachi, Ltd. 2025. All rights reserved

12

2017年度のサイバーセキュリティ戦略 - 教訓 -

日立におけるWannaCry被害からの教訓

『絶対の安全はない。影響を限定し、いかに早く元に戻すかが大切』

教訓を元とした対策の考え方

事業継続の担保、機密情報漏えいの防止、日立提供サービス経由による顧客感染の防止をするために、**サイバーセキュリティを経営課題と位置づけ**、セキュリティガバナンスの徹底を推進する

特 定	①セキュリティ体制整備 ②セキュリティ対策範囲の拡大(社内ITだけではなく全体まで視野へ) ③脅威情報収集・分析 ④サイバーセキュリティ人財育成
防 御	⑤社内IT環境の堅ろう化 ⑥IoT/OTのセキュリティ対策
検 知	⑦サイバーセキュリティ監視拡充(SOC機能拡充)
対 応	⑧インシデント訓練と演習(迅速なインシデントレスポンス)
復 旧	⑨サイバーBCP整備(シナリオ拡充と復旧計画の整備)

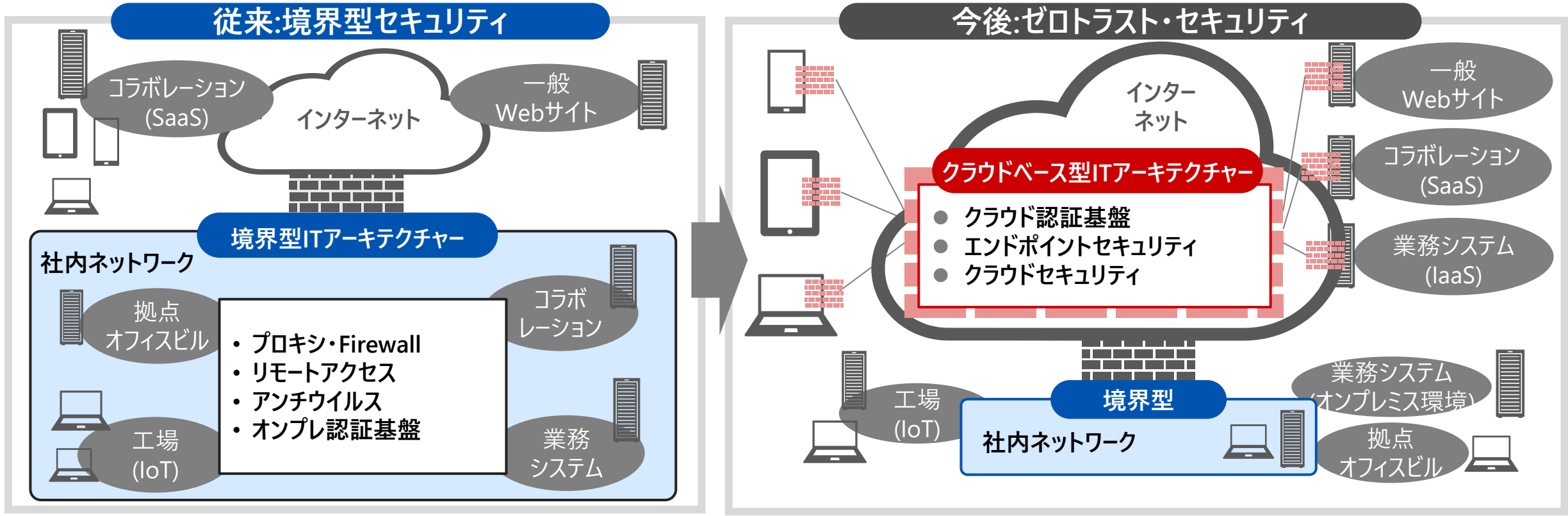
©Hitachi, Ltd. 2025. All rights reserved

13

2020年度以降のサイバーセキュリティ戦略

業務システムのクラウドシフトに伴い、境界型ITアーキテクチャーから
クラウドベース型ITアーキテクチャーへのシフトが今後必要

ITプラットフォームのクラウド化に伴うセキュリティ対策の実装＝ゼロトラスト・セキュリティ



SaaS：Software as a Service　IaaS：Infrastructure as a Service

©Hitachi, Ltd. 2025. All rights reserved

ゼロトラスト・セキュリティの重要な要素

**認証およびエンドポイントの検知/対応をより強固にし、
クラウドアーキテクチャー全体のサイバー監視を実現する**

認 証	認証強化（多要素認証）
エンドポイント	パソコン、サーバー、IoT機器、OT、スマートデバイス
クラウドセキュリティ	クラウド、アプリケーションセキュリティの強化 クラウドネットワークGWの併用によるさらなる強化 データセキュリティ(所在、データそのもののセキュリティ)強化
統合サイバー監視	既存ネットワーク系の監視に加えて、データ、認証、 エンドポイント、アプリケーション、クラウドを統合した監視 (シグネチャー、ふるまい、行動検知など)

©Hitachi, Ltd. 2025. All rights reserved

協創

高度化/増加するサイバー攻撃へ対処するために、社内コミュニケーションを拡充し、共感を得る。
さらには、社会全体でのセキュリティエコシステムを構築し、仲間を増やす。

©Hitachi, Ltd. 2025. All rights reserved

セキュリティエコシステムの構築

セキュリティエコシステムのコンセプト

セキュリティ活動という1つの目標に向かって相互に協力し、事業活動の維持・拡大をする

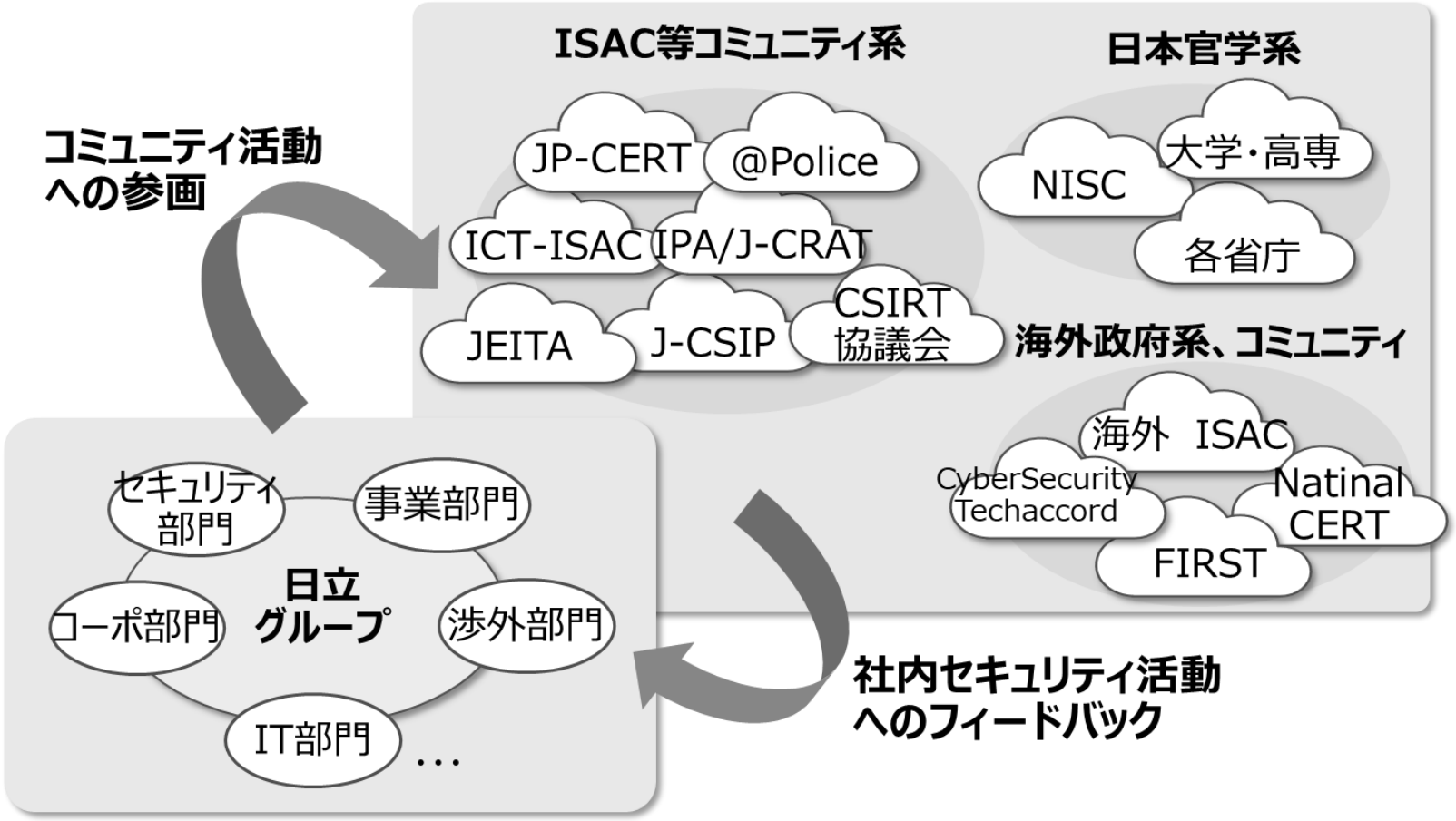
キーワード：3つの「つながる」

1. **モノ　　：デジタルの世界でモノが「つながる」**
2. **人・組織　：会社のなかの人・組織が垣根なく「つながる」**
3. **社会　　：社会全体が「つながる」**

©Hitachi, Ltd. 2025. All rights reserved

社会が「つながる」-産官協創-

省庁、ISAC、CSIRTコミュニティなどとの情報共有活性化



CERT：
Computer Emergency Response Team

ISAC：
Information Sharing and Analysis Center

JEITA：
Japan Electronics and Information Technology Industries Association

J-CSIP：
Initiative for Cyber Security Information sharing Partnership of Japan

J-CRAT：
Cyber Rescue and Advice Team against targeted attack of Japan

©Hitachi, Ltd. 2025. All rights reserved

社会が「つながる」-産産協創-

【社外組織との情報共有】

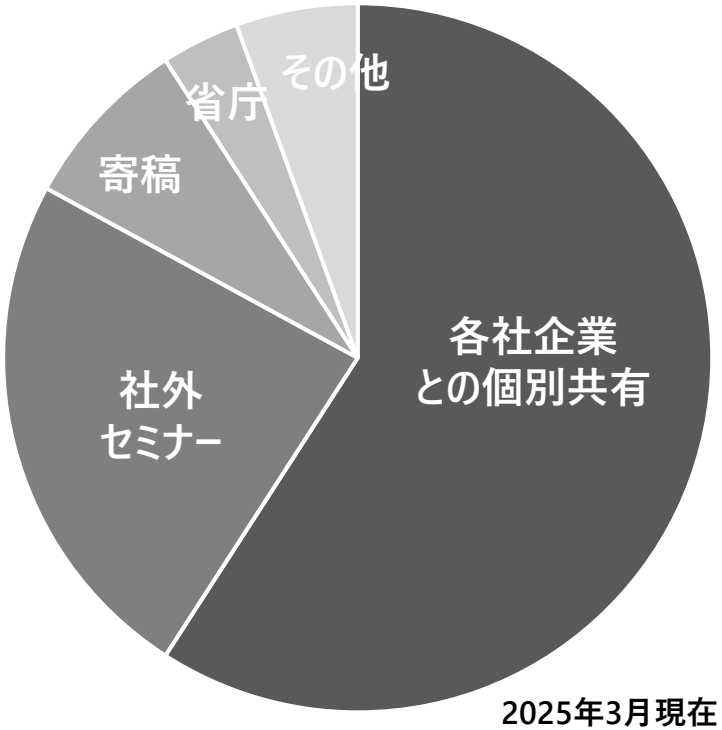
2017年10月以降、コーポレートセキュリティ部門にて、
WannaCry被害から学んだ教訓・対策・課題の共有
活動開始

⇒**特に課題共有は、一緒に知恵を出す
大変有意義な機会**

【各種社外コミュニティへの参画】

- 「Cybersecurity Tech Accord」に賛同表明
- Information Security Forum(ISF)への参画
- 日本シーサート協議会(NCA)、FIRST*1への参画

*1:FIRST(Forum of Incident Response and Security Teams)



社外組織との
情報共有
(合計:252回)

2025年3月現在

©Hitachi, Ltd. 2025. All rights reserved

自分ゴト化

一人ひとりがセキュリティを
正しく理解・共感し、
自分ゴトとしてとらえて行動すること
ができる意識づくりを醸成する。

©Hitachi, Ltd. 2025. All rights reserved

いままで足りなかったことはなにか？

いままでのセキュリティ対策の取り組み
今までも各種IT施策や教育等、網羅的な取り組みを実施
⇒しかし・・・

**共感を得て、
個人が納得しない限り
人の意識と行動が
変わることはない**

重要なこと
- 「押し付けではないこと」
- 「分かりやすいこと」
- 「それぞれの立場にたって考えること」
- 「共有ではなく、共感してもらうこと」

**セキュリティの取り組みそのものへの共感を得るために
新たな視点で活動を開始**

©Hitachi, Ltd. 2025. All rights reserved

新たなセキュリティ啓発活動のコンセプト

一人ひとりのセキュリティ意識の向上こそが重要

キーワード　「自分ゴト化」

取り組み1：意識の変革

1) 共感(認知/理解)を得る取り組み
　⇒セキュリティに興味を持ってもらう。
2) 自分ゴト化をする取り組み
　⇒身の回りのセキュリティを意識してもらう。

取り組み2：行動の変革

セキュリティを自分ゴトとしてとらえ、
従業員一人ひとりが自発的に
行動してもらう取り組み
⇒知識の習得・深堀・共有をしてもらう。

©Hitachi, Ltd. 2025. All rights reserved

©Hitachi, Ltd. 2025. All rights reserved