HITACHI
Inspire the Next

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

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
Inspire the Next

Contents

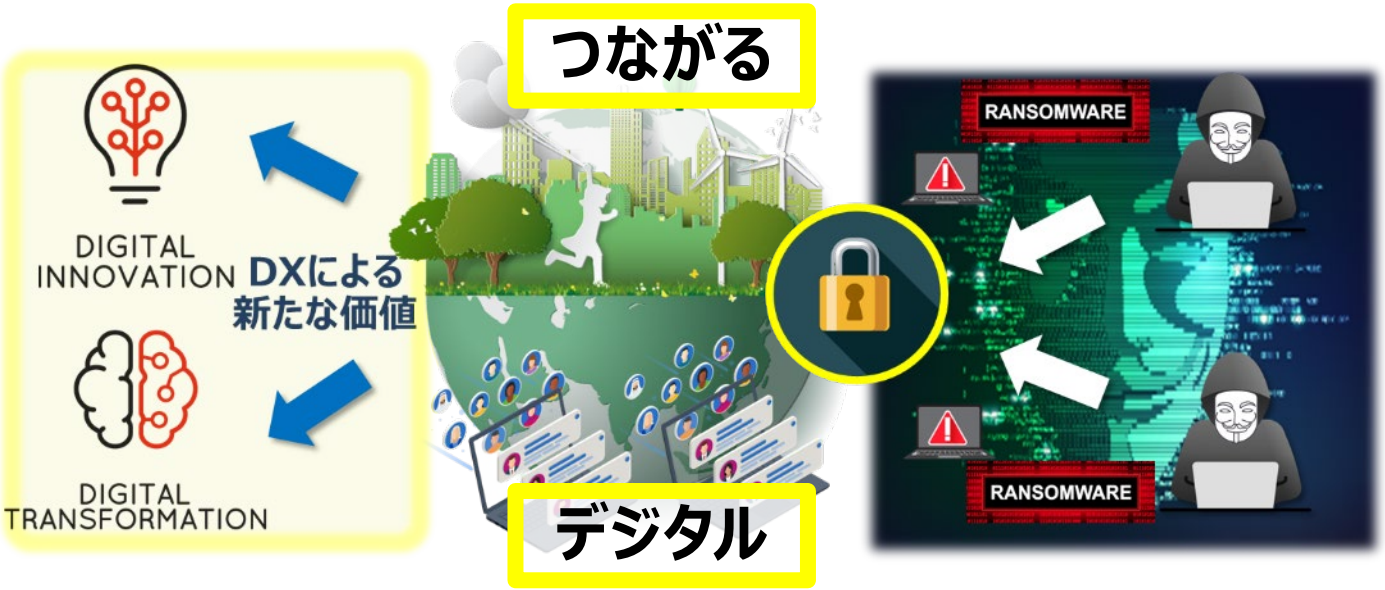
HITACHI
Inspire the Next

1．世の中のサイバーセキュリティ動向

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～

HITACHI
Inspire the Next

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

最近のセキュリティの脅威を振り返ってみる

HITACHI
Inspire the Next

世の中のセキュリティ動向

- 世界情勢に乗じたサイバー攻撃が激化
- 社会インフラを狙った攻撃も発生
- 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
- 不適切な情報公開/顧客情報漏えい
- 内部不正による情報漏えい
- テレワークなどのニューノーマルな働き方を狙った攻撃

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

いま考えるべきこと

HITACHI
Inspire the Next

- 世の中の潮流(DX,働き方改革)へ対応するために、早急なサイバー対策整備が必要
- サイバー攻撃が事業へ影響を及ぼすことが明らか

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
Inspire the Next

2. サイバーレジリエンス強化への取り組み

サイバーセキュリティビジョン

HITACHI
Inspire the Next

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	従業員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

サイバーセキュリティビジョンを実現するために

HITACHI
Inspire the Next

Cyber Security Frameworkの構成要素の観点で
対応できるよう、ITもプロセスもヒトも準備を行う
＝有事の際には、効果的に対応できるようにしておくこと

NIST Cyber Security Framework*の構成要素

- 特定(Identify)
- 防御(Protect)
- 検知(Detect)
- 対応(Respond)
- 復旧(Recover)

これらの
要素の観点で
対応できるように！

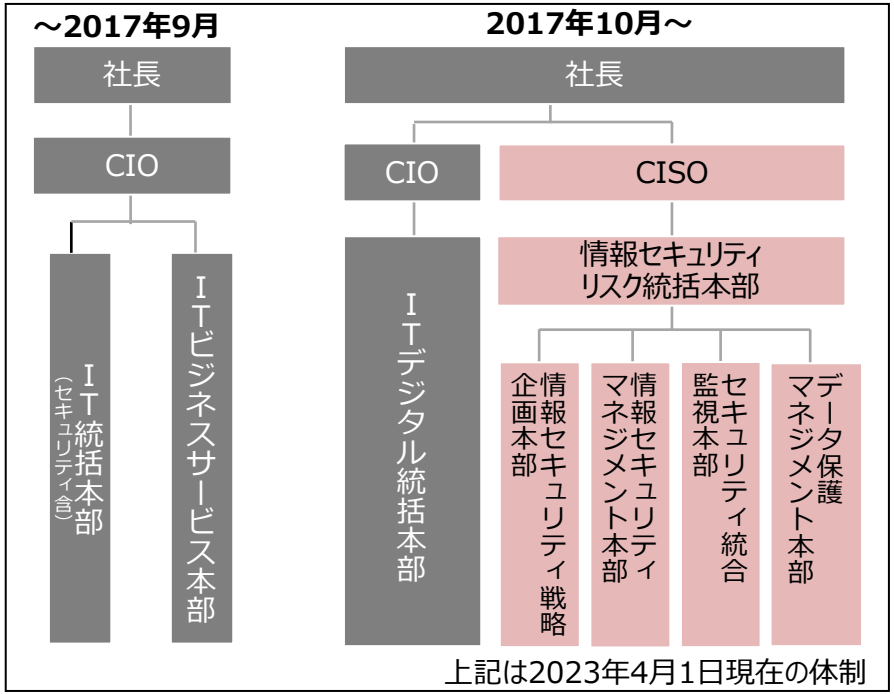
リスク管理の一環として、準備すること

＊米国国立標準研究所が発行したサイバー攻撃対策に特化した、サイバーセキュリティ対策のフレームワーク　NIST：National Institute of Standards and Technology

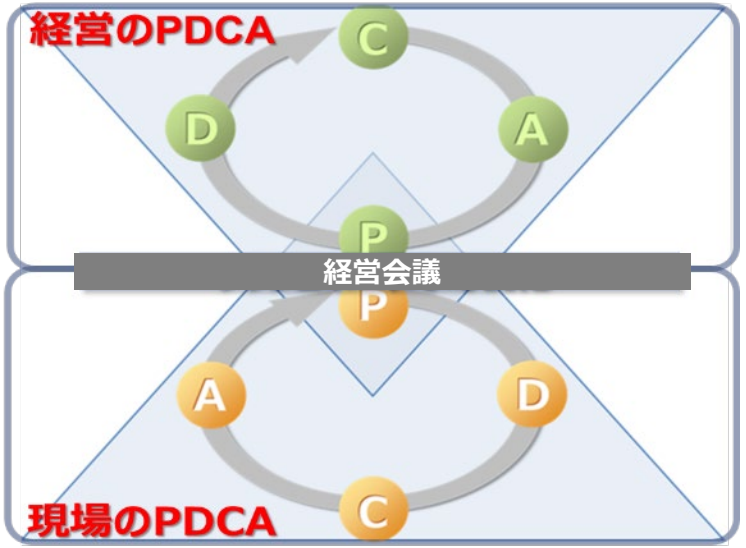
セキュリティガバナンス組織の設置

HITACHI
Inspire the Next

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CISOを設置し、セキュリティガバナンスの更なる徹底を開始



経営と現場をつなぐセキュリティガバナンスを推進

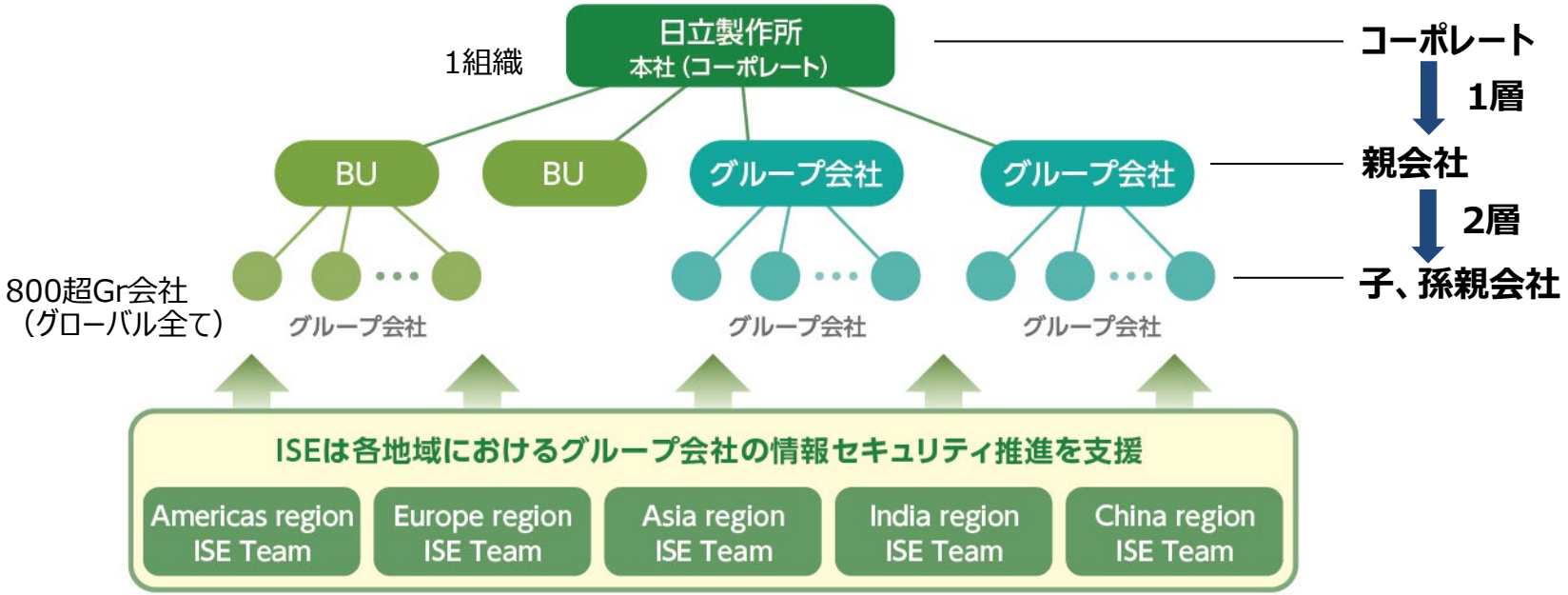


CIO：Chief Information Officer　CISO：Chief Information Security Officer

グローバル情報セキュリティガバナンス体制

HITACHI
Inspire the Next

- 情報セキュリティガバナンスは、2階層構造で推進
  （1層：コーポレート→親会社、2層：親会社→子会社、孫会社）
- 各リージョンに各社の情報セキュリティ推進を支援するISEを設置



(ISE: Information Security Expert)⇒コーポレートが任命

セキュリティガバナンス組織のミッション

HITACHI
Inspire the Next

平時の対応

・やるべきことはなにかをきめる・計画する（＝Plan)

⇒人(トレーニング・アウェアネス)
⇒技術(ITアーキテクチャー、モニタリング、インシデントレスポンス)
⇒規則・プロセス・組織

・やるべきことやる（＝Do)

⇒事業部門への実行指示、IT部門/QA部門等とのコーポ部門との連携

・できているかどうかを確認する（＝Check)

⇒セルフアセスメント(情報セキュリティ監査):1st ディフェンス
⇒コーポ部門評価＋オンサイトリスクアセスメント:2nd ディフェンス
⇒内部監査:3rd ディフェンス

・なにをすべきかを考察して、評価する（＝Act）

⇒残存リスク・リスク対処方法の決定・経営インパクト分析(経済損失)
⇒経営会議への対策案の答申

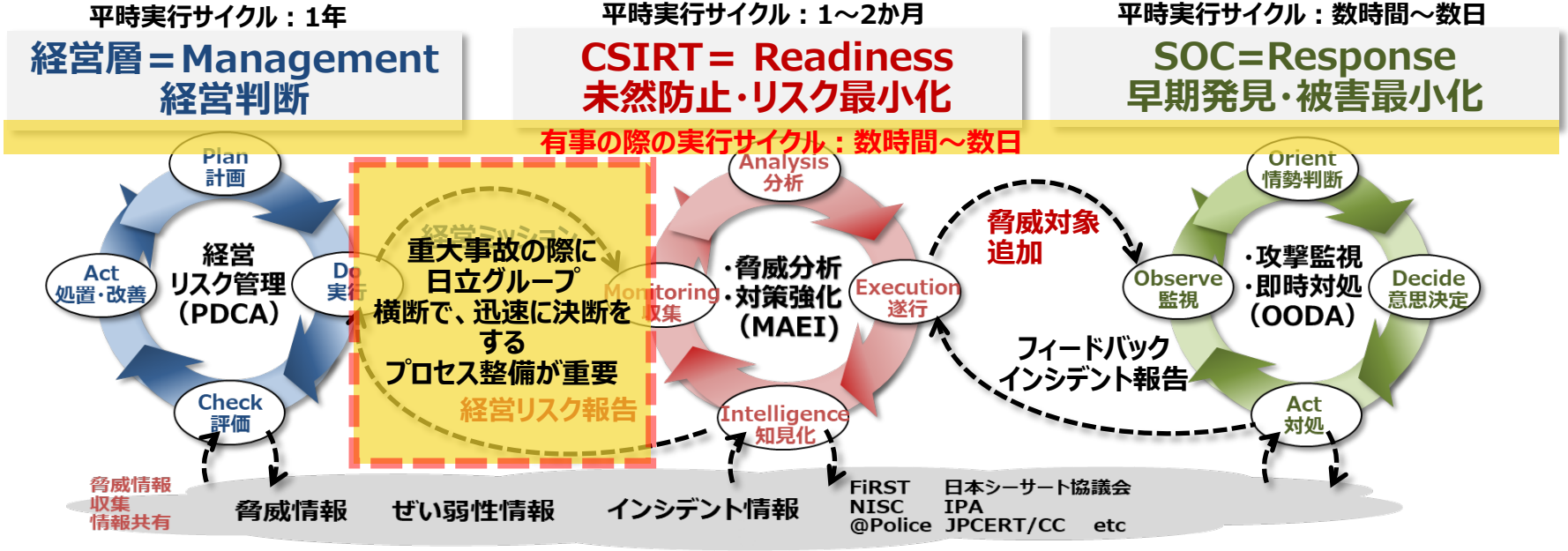
有事の対応

・被害局所/極小化に関する実行指示をする

⇒迅速なインシデントレスポンス
⇒緊急対策本部の設置
⇒サイバーBCPの発動

有事に向けた迅速な意思決定するためのプロセス整備

- **経営層** :PDCAベースでの「経営リスク管理」
- **CSIRT**:脅威情報の収集、平時/有事の「脅威分析」「対策強化」
- **SOC** :「攻撃監視」および有事の際の「即時対処」



SOC:Security Operation Center CSIRT:Computer Security Incident Response Team FIRST : Forum of Incident Response and Security Teams NISC : National center of Incident readiness and Strategy for Cybersecurity
IPA : Information-technology Promotion Agency,Japan JPCERT/CC : Japan Computer Emergency Response Team/Coordination Center

HITACHI
Inspire the Next

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。

取り組みの変化

HITACHI
Inspire the Next

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

2011年度のサイバーセキュリティ戦略

HITACHI
Inspire the Next

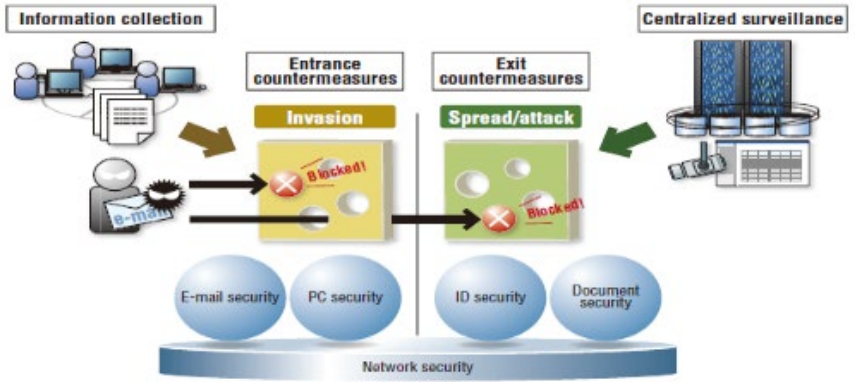
世の中の動向と同様に、
日立グループにおいても多くの
標的型攻撃を観測

**2011年度よりサイバー攻撃対策を
本格的に開始(施策拡充と体制整備)**

**既存のITセキュリティ対策に、昨今の標的型攻撃に代表される
サイバー攻撃への取り組みを追加**

サイバー攻撃対策の重点ポイント

1. **多層防御**
   (入口・出口・内部拡散対策)
2. **早期検知**
   (脅威情報共有・集中監視・分析)
3. **早期対応**
   (インシデントレスポンス強化)



2017年度のサイバーセキュリティ戦略 - WannaCry被害 -

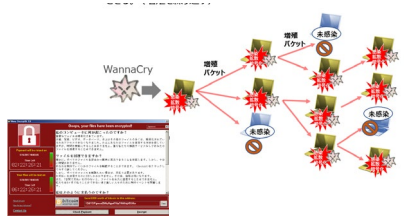
HITACHI
Inspire the Next

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（想定）
- 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
Inspire the Next

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』**

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

WannaCry被害への再発防止策

HITACHI
Inspire the Next

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、工場、製品サービス、サプライチェーン全体まで視野へ） 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)

SOC : Security Operation Center

WannaCry以降のサイバー攻撃対策の取り組み

HITACHI
Inspire the Next

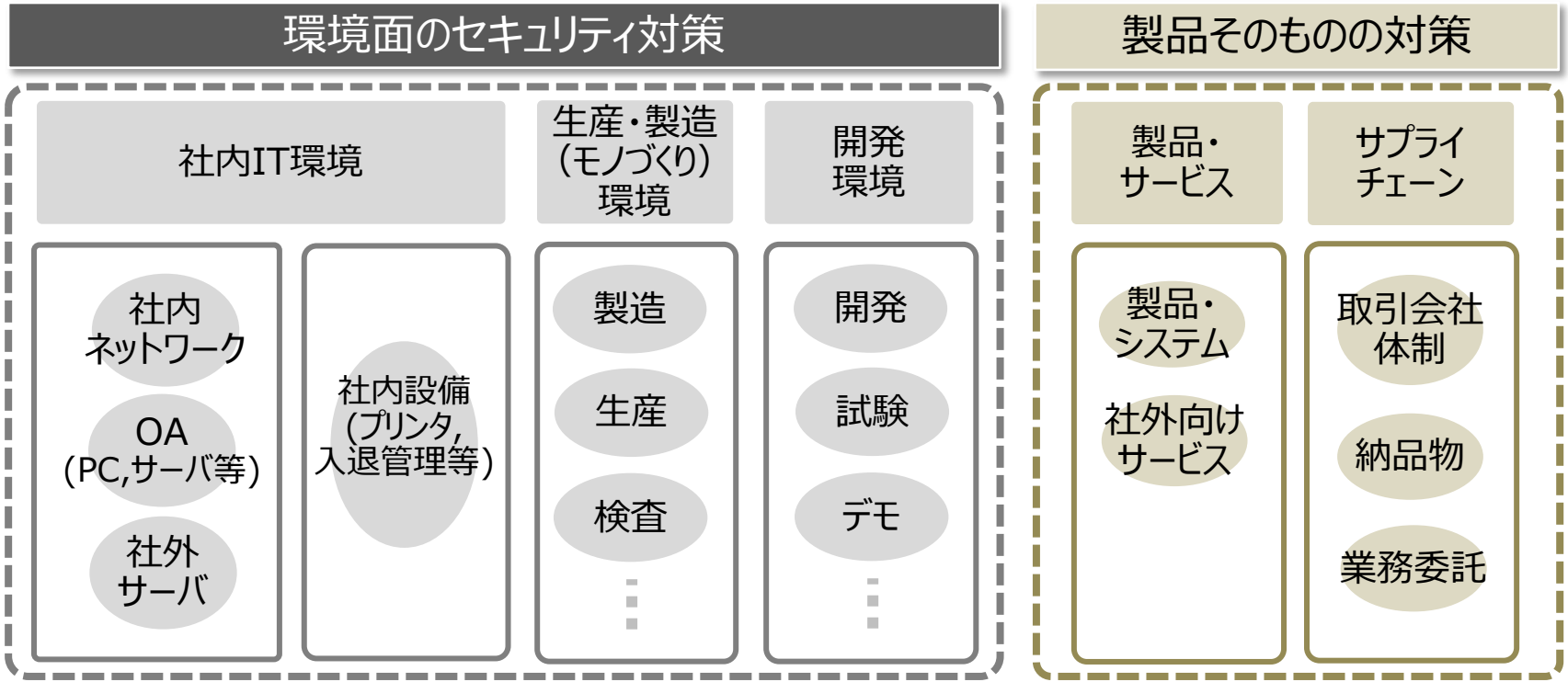
2017年5月のWannaCry被害を契機に、運用・技術・組織面でサイバー対策を強化

	2017年度	2018年度	2019年度	2020年度	2021年度～
運用面	規則面	**セキュリティ対策範囲拡大*1に併せたガイドライン・人財育成**策定と展開			
		サイバーBCPガイドライン見直し・拡充・定期訓練実施			
		*1 社内IT、製造現場、開発現場、製品サービス、サプライチェーン		**データプロテクション規則**制定・展開	
				M＆Aガイドライン策定・展開	
	実行面	**オンサイトリスクアセスメント**(現場確認)開始			
			サイバー訓練拡充と定期的な実施		
			グローバルセキュリティ対応開始(グローバル地域でのセキュリティサポート部隊発足)		
技術面		**グローバルNWセキュリティ監視** [1センター(日本)で24H365H]		**端末監視(エンドポイント強化)** **認証強化(監視・システム強化)**	
		脅威情報収集/分析によるレディネス機能設置～既存施策へのフィードバック			
		社内ネットワーク対策強化[バックアップ強化、データセンタ堅ろう化、**コンパートメント化**、**ゼロトラスト**]			
組織面	▲ 2017/10月 **コーポレート統制機能強化(CISO・専任組織設置)**,BU各社体制強化				
		▲2018/4月 セキュリティ対策範囲拡大*1にむけた各種**専門部会設置**			
			▲ 2019/4月 海外5拠点に**セキュリティサポート部隊設置**		
	サイバーセキュリティ**監視専任部隊**設置、**データプロテクション体制**強化 2022/4月 ▲				

セキュリティガバナンスの対象範囲

HITACHI
Inspire the Next

・セキュリティ対策の範囲を社内IT以外の製品、製造等環境へ拡大
・18年度から横断的な活動を開始



サイバーBCP整備とインシデント訓練・演習

HITACHI
Inspire the Next

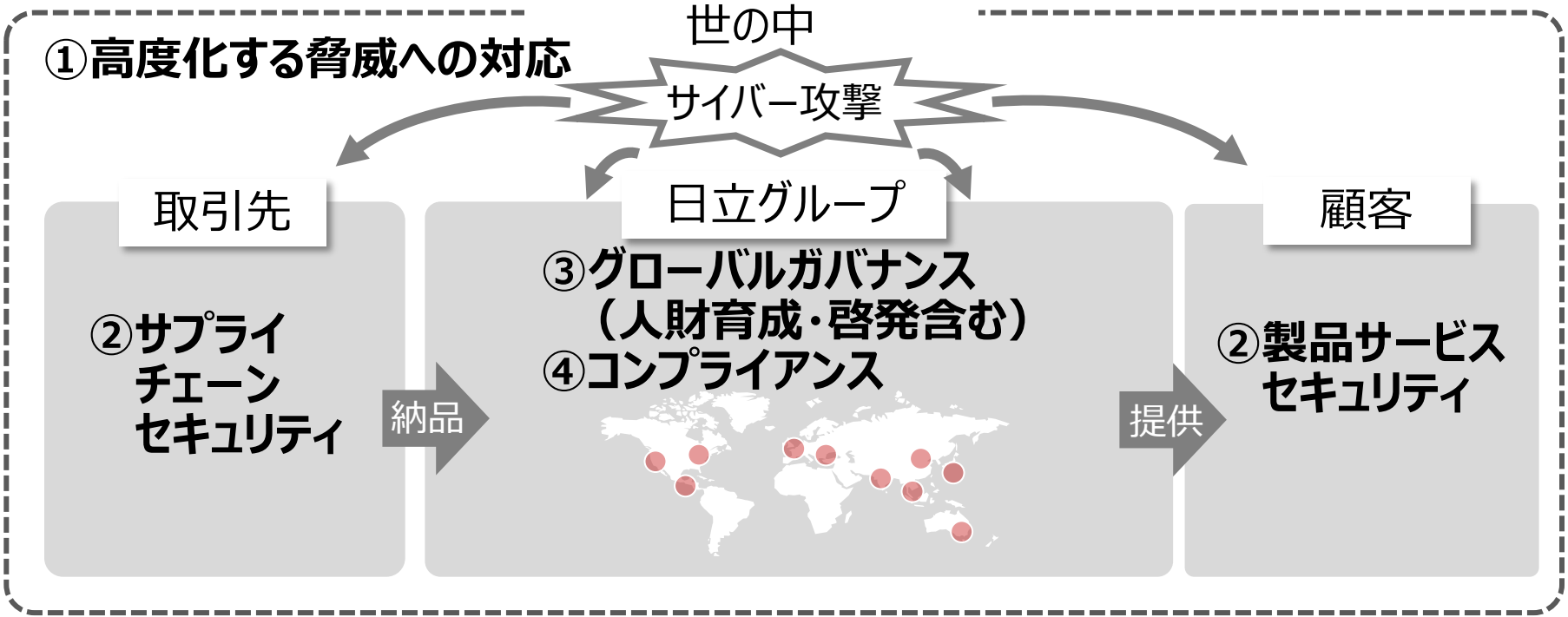
サイバーBCPの教訓：平時の活動は、有事のために。
いつでも緊急対応ができるスキル習得・意識の維持・計画整備

- **サイバー攻撃のシナリオ拡充**
  ⇒ **ケーススタディの整備と、リスクベースでの仮説立て**
- **シナリオ毎の実行手順書 (リスクに応じたプレイブック)整備**
- **インシデント訓練による実行力向上**
  ⇒緊急時にしっかりと動けるようになるために重要な要素
  ⇒最初はたいしたことがないインシデントレスポンスでも、大きな事案に
  つながっていく可能性があることを常に念頭においた対応
- **演習によるサイバーBCPの定期見直し**
  ⇒技術チーム/**有事の際の関連部門**、机上/実機、オープン/ブラインド

2020年度以降のサイバーセキュリティ戦略

HITACHI
Inspire the Next

- 2017年以降進めてきた体制・IT施策・プロセス整備等の更なる深堀
- ゼロトラスト・セキュリティの推進と、サイバーインテリジェンスの更なる強化

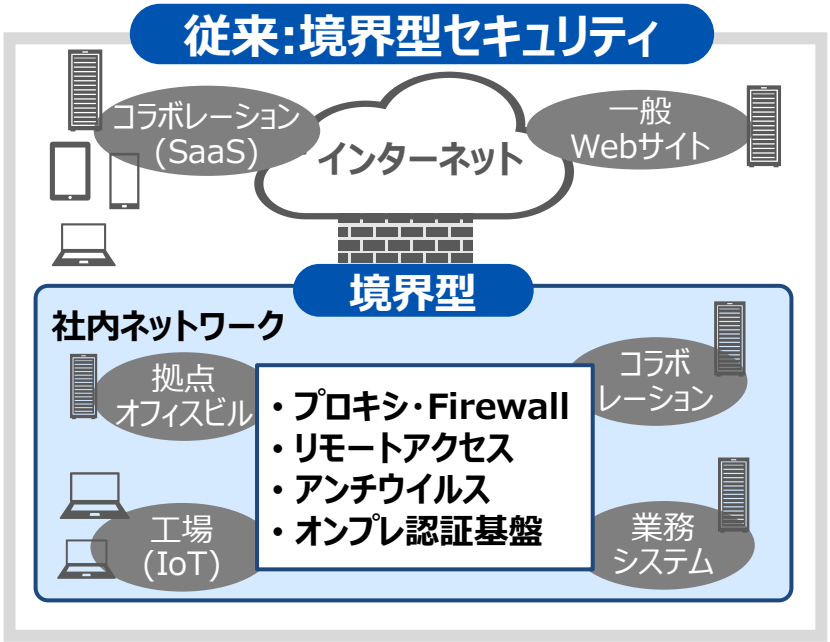


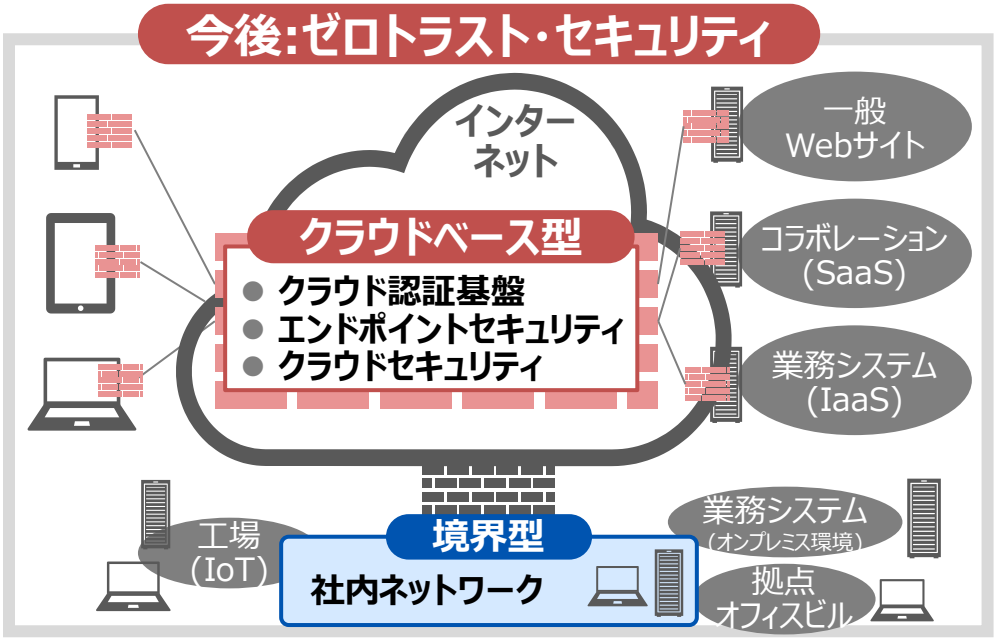
ゼロトラスト・セキュリティの考え方

HITACHI
Inspire the Next

業務システムのクラウド化・スマートフォン活用など
これからのデジタル社会を考えたDX/働き方改革に対応したセキュリティ対策が必須

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





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

ゼロトラスト・セキュリティの重要な要素

HITACHI
Inspire the Next

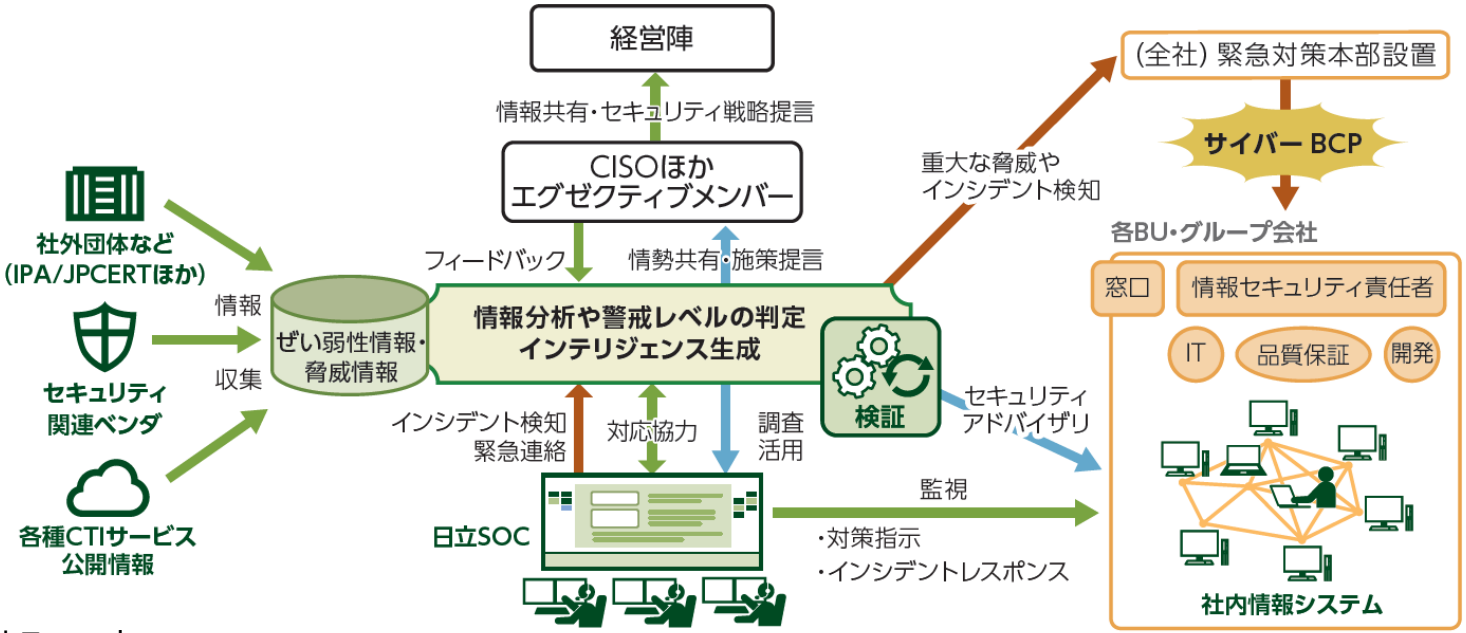
**認証およびエンドポイントの検知/対応をより強固にし、
クラウドアーキテクチャー全体のサイバー監視を実現する**

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)

サイバーセキュリティインテリジェンス強化

HITACHI
Inspire the Next

社内外の様々なセキュリティ動向・インシデントを収集し、各種アラートの発出、迅速な脆弱性対策、ITセキュリティ施策へのフィードバックなどを実施



BU：ビジネスユニット

HITACHI
Inspire the Next

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
Inspire the Next

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. **モノが「つながる」**
2. **人・組織が「つながる」**
3. **社会が「つながる」**

HITACHI
Inspire the Next

いままでつながっていなかったモノが「つながる」

セキュリティ確保のために、企業内において各事業部門が、相互に協力して推進することが必要

人・組織が「つながる」

人・組織がモノのつながりを介して「つながる」

立場、組織の垣根を越えたコミュニティづくり

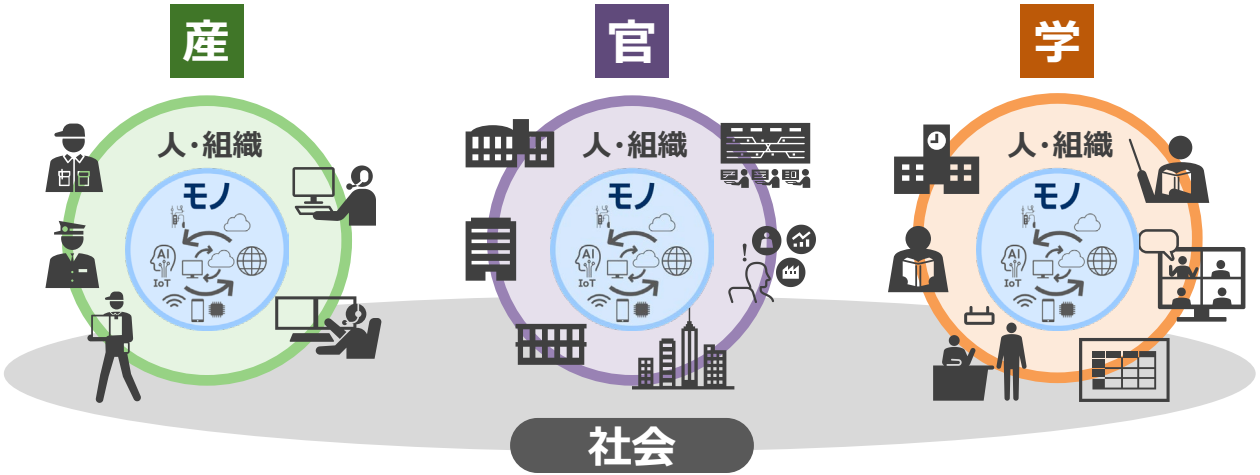
セミナーやワークショップの開催
- 自身の役割を再認識
- 周囲との連携深化

HITACHI
Inspire the Next

高度化・多様化するサイバー攻撃への対処

脅威情報や対策実行時の課題共有など、枠組を超えたコミュニティの形成が必要不可欠

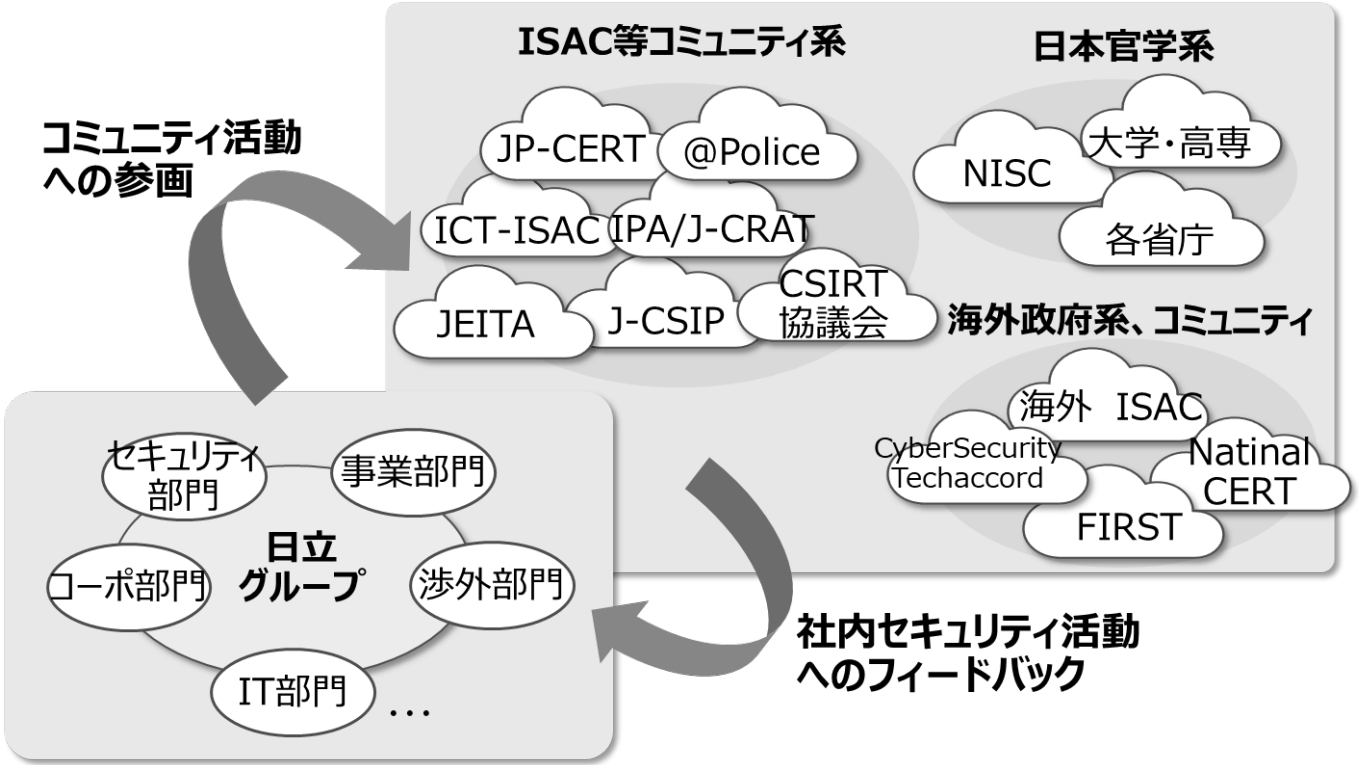
社会が「つながる」



③社会が「つながる」-産官協創-

HITACHI
Inspire the Next

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

③社会が「つながる」-産産協創-

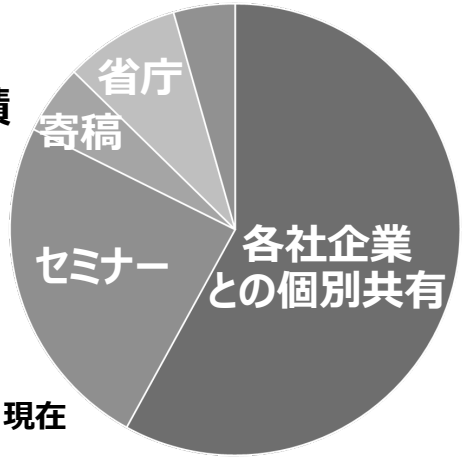
HITACHI
Inspire the Next

【他社との情報共有】
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

【グローバルコミュニティへの参画】
・日本企業として初めて、「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)

他社との
情報共有の実績
(合計:182回)



2023年3月現在

HITACHI
Inspire the Next

自分ゴト化

従業員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
Inspire the Next

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、なにかが足りない・・・・

**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」

従業員へ共感を得るための新たなセキュリティ啓発活動を開始

HITACHI
Inspire the Next

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」
「従業員が心から共感すること」

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
Inspire the Next

3. まとめ

まとめ

日立は、自社における**統制**を行うとともに、社外への活動などを通し、産・官・学が連携および**協創**した社会全体でのセキュリティエコシステムの構築を推進します。

また、組織を守る大きな砦をつくるために、**自分ゴト化**を推進し、従業員一人ひとりがセキュリティを正しく理解し、あるべき姿に向かって働くことができる意識づくりをめざします。

これらを実現することで、新しい日常をより安心・安全で快適に過ごせるように、また、そこに潜むリスクを回避できるように、日立は**サイバーレジリエンスの強化**に取り組みます。

HITACHI
Inspire the Next

END

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

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 Social Innovation is
POWERING GOOD