\Orchestrating a brighter world

NEC

JDSF2019新春セミナー 講演資料

これからのデジタル社会を見据えたサイバーセキュリティのあり方

2019年2月1日

日本電気株式会社
サイバーセキュリティ戦略本部
事業開発G　伊藤大輔（CISSP、情報処理安全確保支援士）

Orchestrating a brighter world

未来に向かい、人が生きる、豊かに生きるために欠かせないもの。
それは「安全」「安心」「効率」「公平」という価値が実現された社会です。

NECは、ネットワーク技術とコンピューティング技術をあわせ持つ
類のないインテグレーターとしてリーダーシップを発揮し、
卓越した技術とさまざまな知見やアイデアを融合することで、
世界の国々や地域の人々と協奏しながら、
明るく希望に満ちた暮らしと社会を実現し、未来につなげていきます。

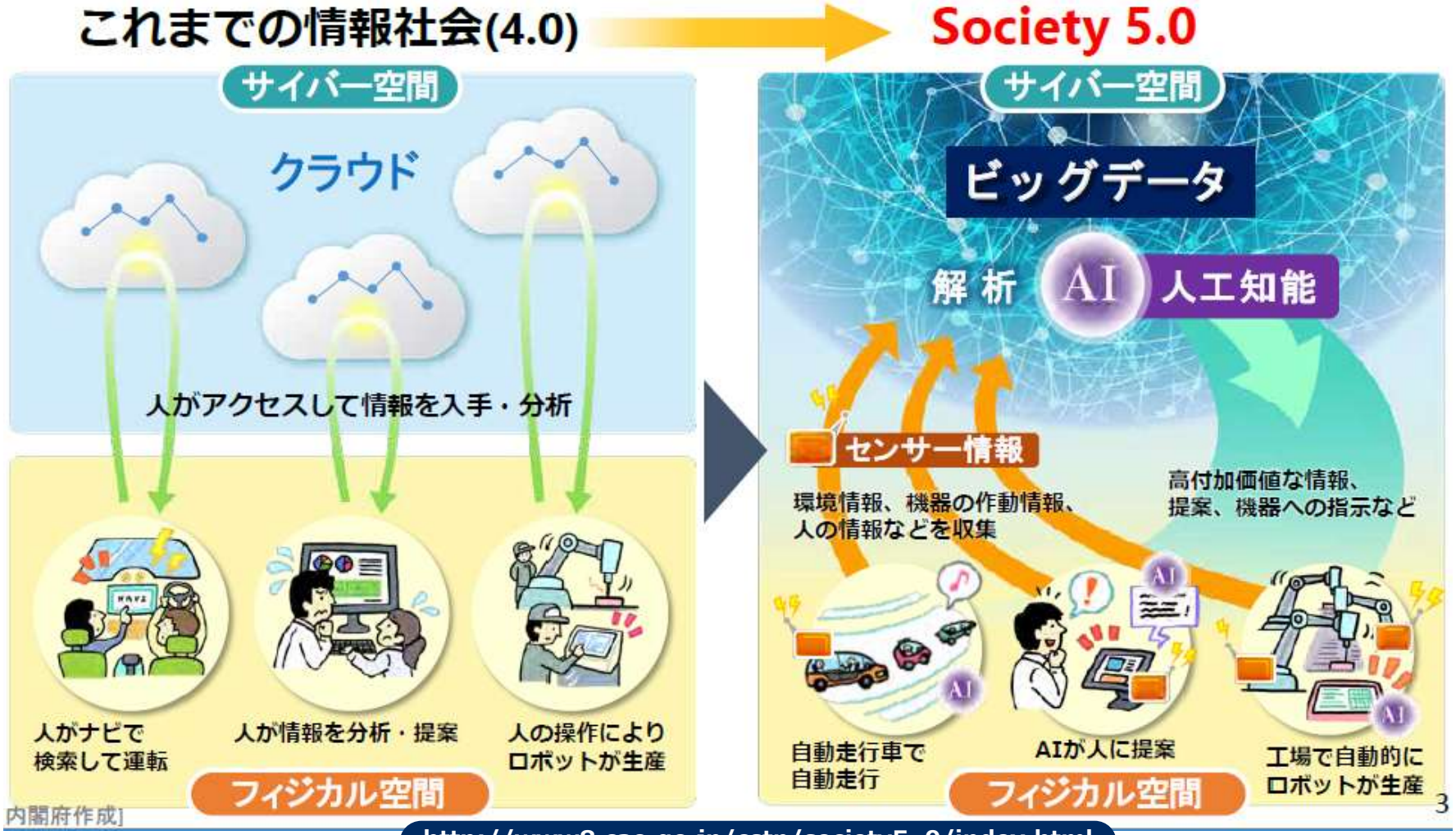
アジェンダ

1. Society5.0の進展とサイバーセキュリティ
2. NECの考えるサイバーセキュリティ
3. サイバーセキュリティに対するNECの取り組み
4. これからのサイバーセキュリティ対策のアプローチ

1.Society5.0の進展とサイバーセキュリティ

政府の取り組み（Society 5.0）

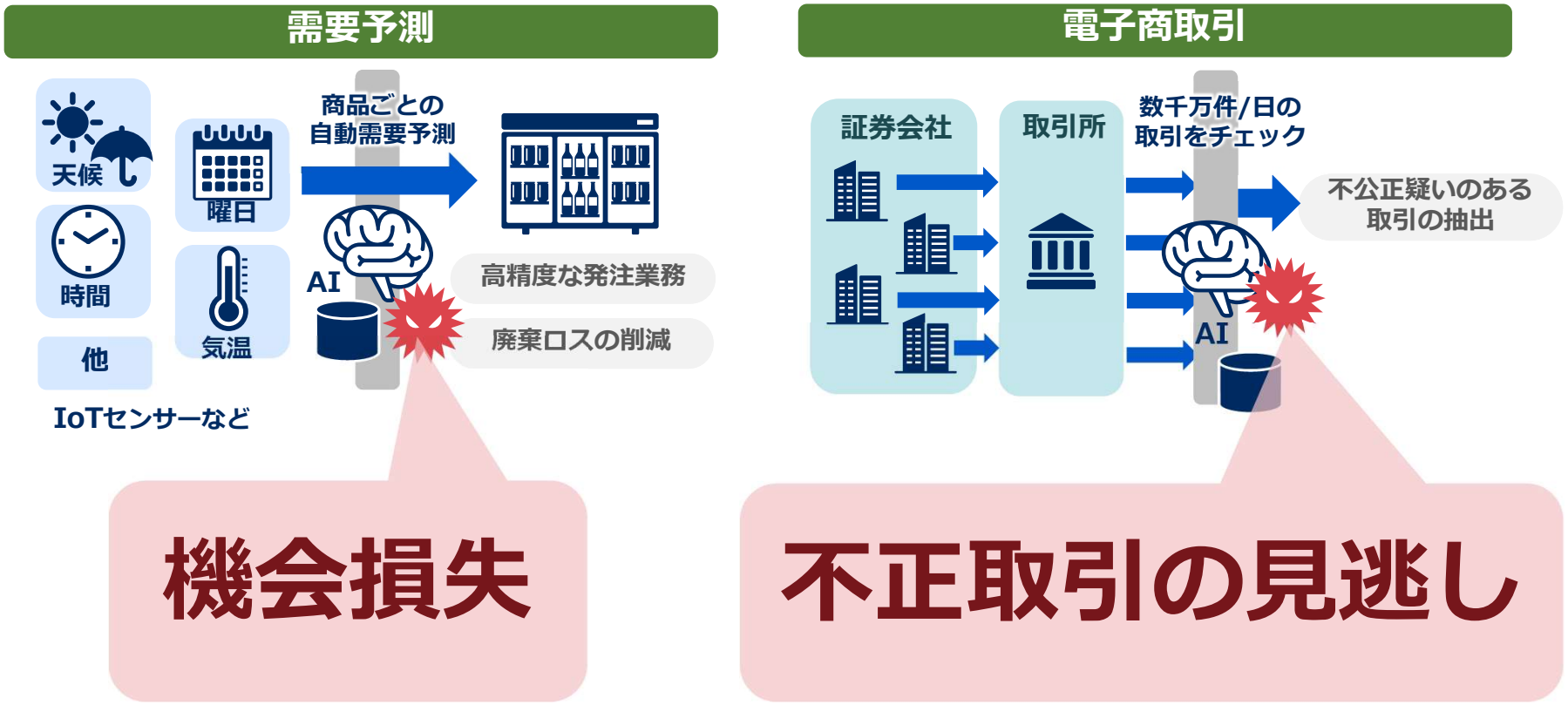
AIとIoT技術を基にサイバー空間とフィジカル空間を高度に融合させた
スマートシステムを利用した社会



http://www8.cao.go.jp/cstp/society5_0/index.html

AI/IoTの活用による企業活動の変化とサイバー攻撃のリスクの拡大

AI/IoTの活用が経営やビジネス成長の源泉になる一方
サイバー攻撃の対象となる箇所が増える



サイバー攻撃によりビジネスに影響が生じた例（1/2）

セキュリティパッチ未適用の端末に感染したランサムウェアの被害により、
病院業務や工場ラインなどが停止

WannaCry (2017年5月)

150か国で20万台以上が感染

既知の脆弱性に未対応だった Windows端末が感染 → 脆弱性管理の問題

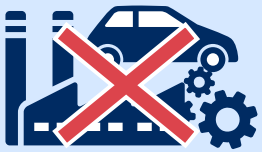
医療関係施設(約50団体)

救急搬送患者の受け入れ不可

心臓手術中止

患者の受診を制限

大手自動車メーカー



車の生産ライン停止

石油関連企業

ガソリンスタンドの電子決済が停止

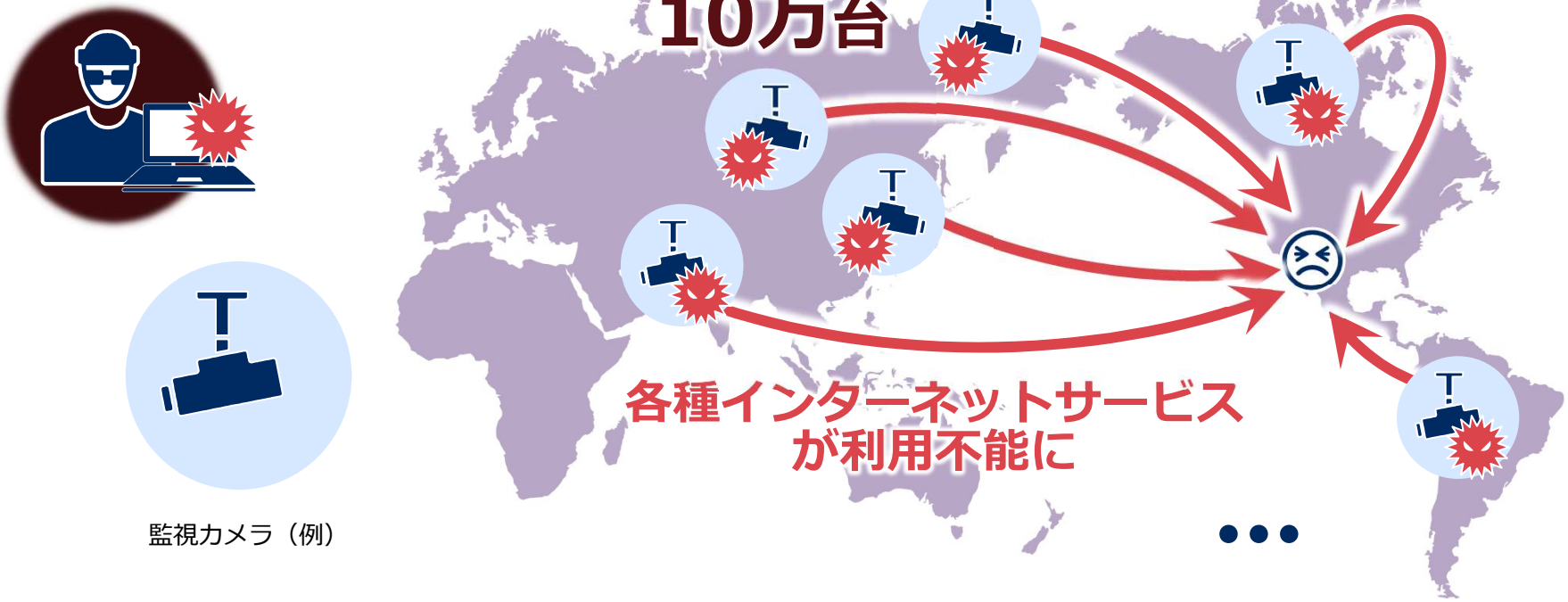
サイバー攻撃によりビジネスに影響が生じた例（2/2）

製品仕様そのものが脆弱なIoT機器を踏み台にした
大規模なサイバー攻撃により米東海岸のWebサービスに被害

Mirai (2016年10月)

世界各地のインターネット機器(監視カメラ等)を乗っ取り、攻撃に悪用

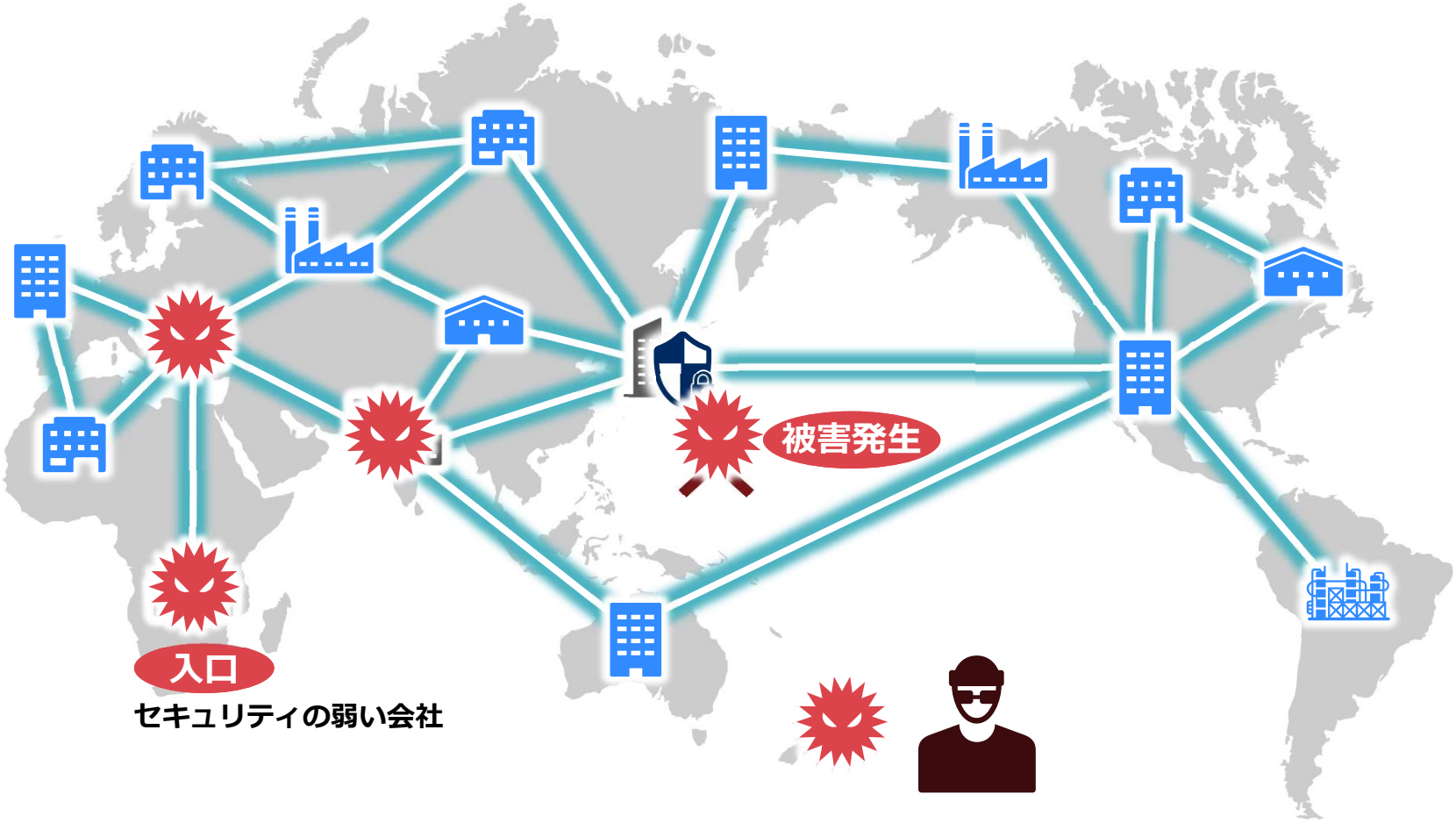
デフォルトのID/PWのまま
使用されているIoT機器(Webカメラ等)に感染 → **製品設計の問題**



監視カメラ（例）

サプライチェーン型攻撃の増加

セキュリティ対策が弱い会社を”入口”にして
サイバー攻撃をしかける手口が増加



日本政府のセキュリティに対する取り組み

官民連携でサイバーセキュリティ向上への取り組みを加速

サイバーセキュリティの課題解決のための官民連携のWGを設置

サイバーセキュリティ協議会の発足

電気通信事業法に基づく省令改正（総務省）

2020年4月以降は不正アクセスを防ぐ機能を設けることを義務化

サイバー・フィジカル・セキュリティ対策フレームワークの策定

三層構造でセキュリティを考える

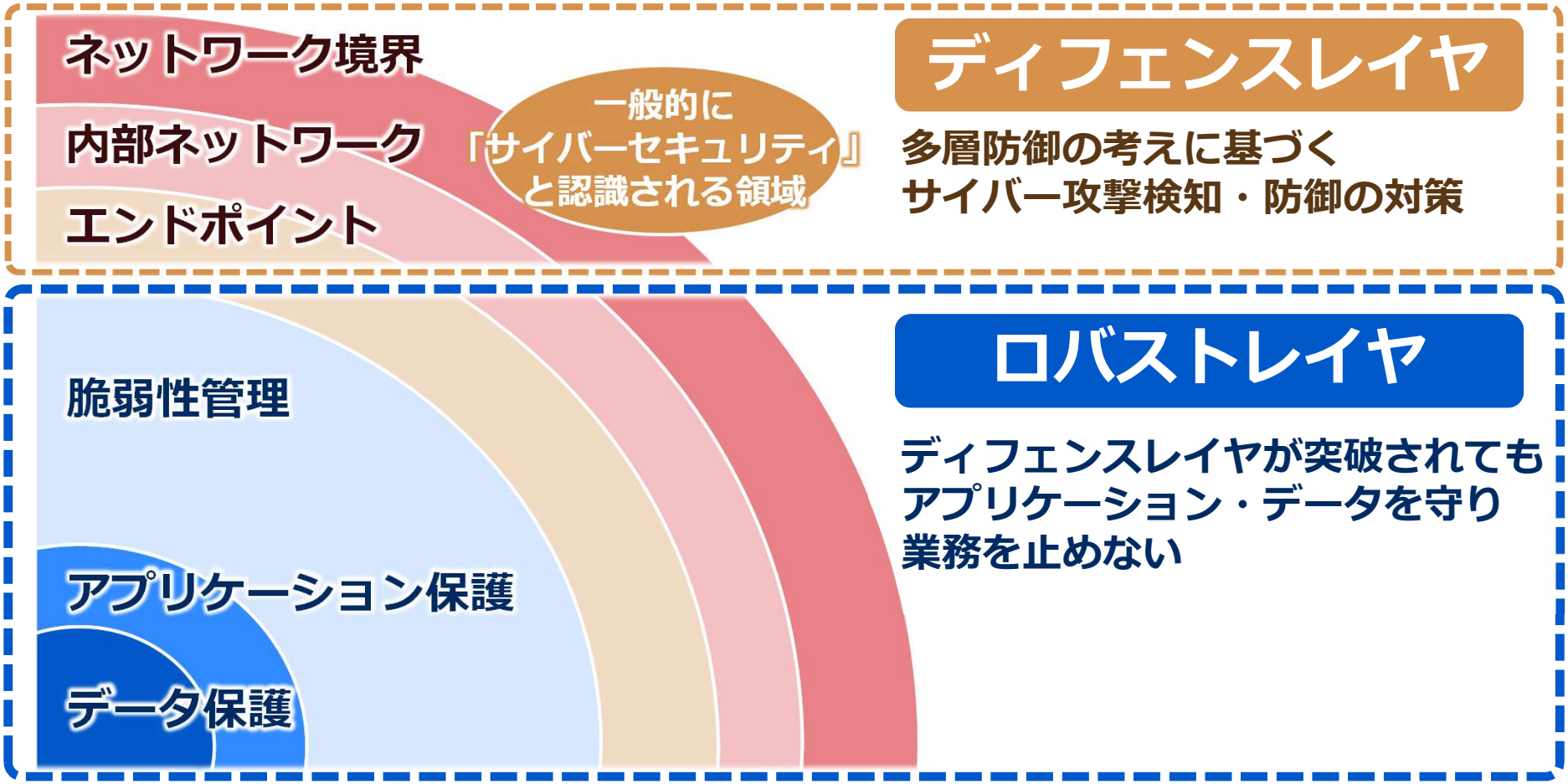
- 企業間のつながり（従来型サプライチェーン）
- フィジカル空間とサイバー空間のつながり
- サイバー空間におけるつながり

2.NECの考えるサイバーセキュリティ

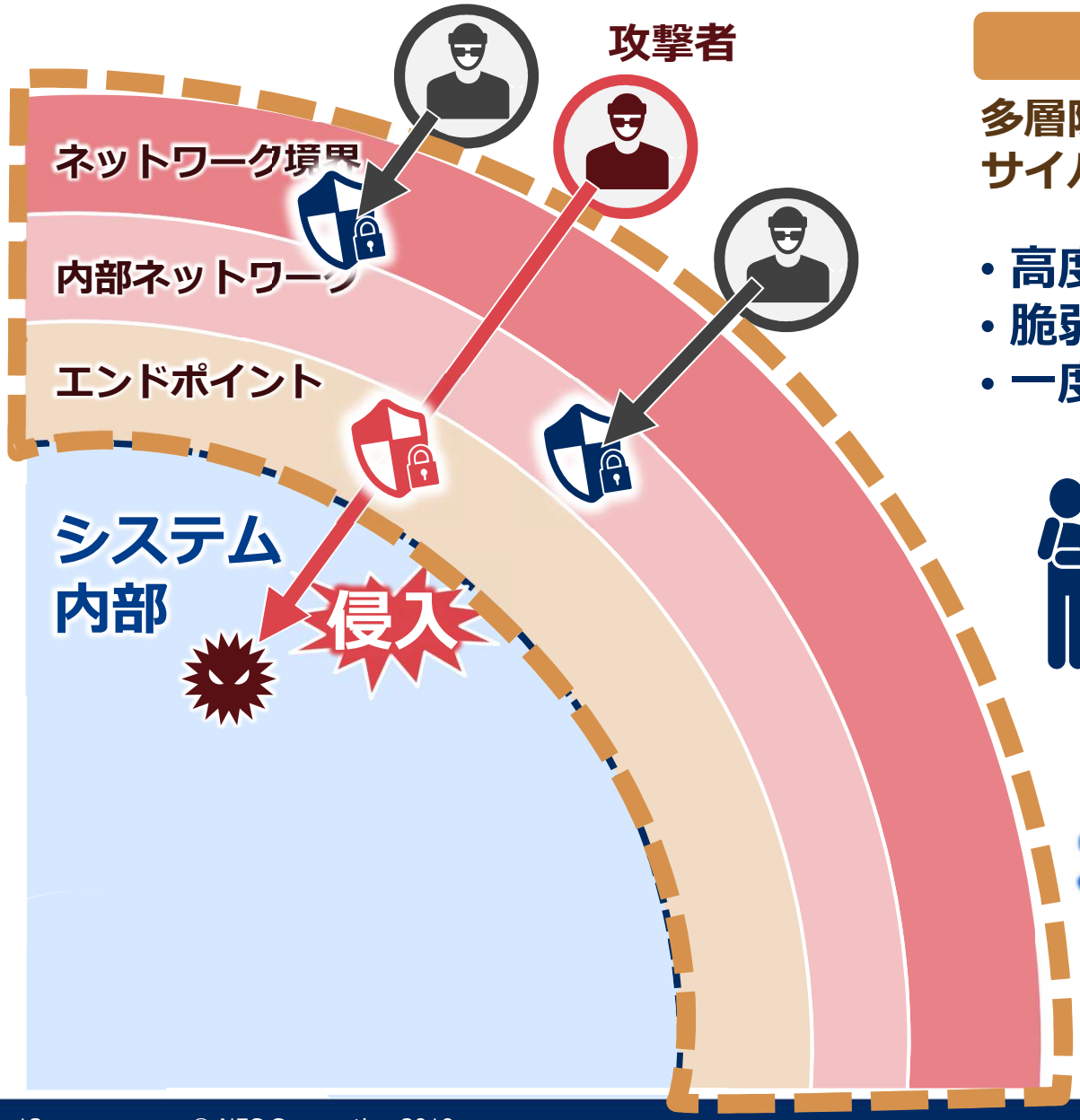
サイバーセキュリティ対策 2つのアプローチ

Society5.0の進展に伴うセキュリティ脅威の増大に対し
NECでは多層防御モデルを大きく２つのレイヤに分けアプローチ

多層防御モデル



ディフェンスレイヤの課題



ディフェンスレイヤ

多層防御の考えに基づく
サイバー攻撃検知・防御の対策

- 高度な標的型攻撃
- 脆弱な機器を探すワーム機能
- 一度でもミスすると侵入成功

デジタル化やIoTにより
攻撃される対象が激増

万が一突破されても
業務が止まらない
対策が必要

ロバストレイヤの必要性

ロバストレイヤ

ディフェンスレイヤが突破されても
アプリケーション・データを守り
業務を止めない

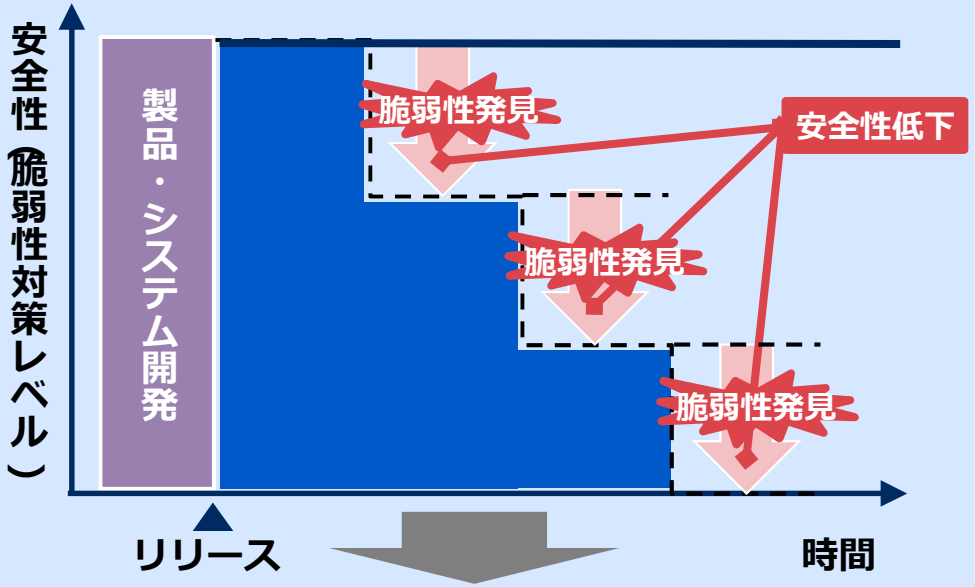
近年は脆弱性を狙う攻撃が大多数

**「脆弱性」を見える化し
機器内に弱点を
残さないことで
大部分の攻撃に対処可能**

脆弱性管理による安全性の確保

「脆弱性対策」された状態を維持

リリース直後は安全性の高い製品・システムも
脆弱性対策を怠ると、徐々に安全性を損ない
サイバー攻撃の被害を受けるリスクが高まる



ロバストに作る

ロバストを維持する

- 脆弱性情報を収集、分析
- 機器の脆弱性を見える化
- 脆弱性への対処実行

NECの考えるサイバーセキュリティ

多層防御によるシステム全体のセキュリティ対策と
それを実現するセキュリティ人材の育成

①多層防御

ディフェンス×ロバストにより
高度化する攻撃に対応

②サプライチェーン防御

サプライチェーンまで含めた
システム全体のセキュリティ対策

③セキュリティ人材の育成

サイバーセキュリティを
支える人材の育成

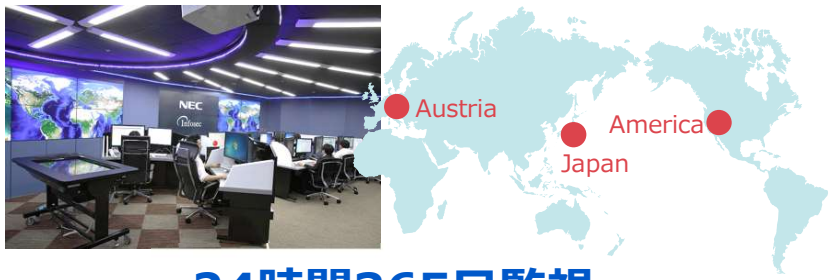
3.サイバーセキュリティに対する NECの取り組み

ディフェンスレイヤにおけるNECの主な取り組み

最新のサイバー攻撃動向の知見に基づき対策を強化

- ディフェンスレイヤにおける従来のIDSやEDR等の対策は必要
- 高度な攻撃への対処、検知後の対応復旧が重要

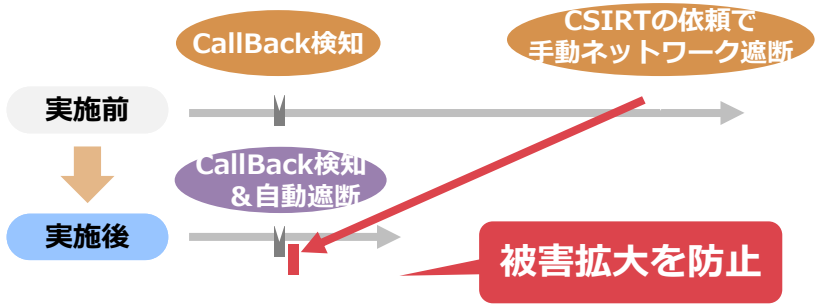
監視サービスの展開



24時間365日監視

サイバーセキュリティ対策の中核拠点として「NECサイバーセキュリティ・ファクトリ」運用中

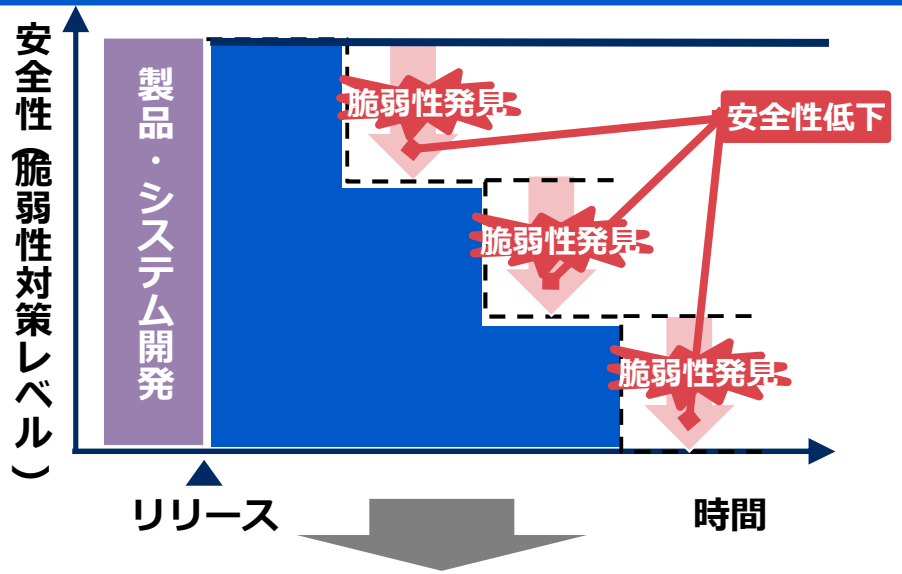
SDN×サイバー攻撃対策連携



NECイントラネットでサイバー攻撃リスク極小化に向け、SDNによる感染端末の自動遮断を実施

ロバストレイヤにおけるNECの主な取り組み

ロバストに作る取り組みとロバストを維持する取り組みを実践



ロバストに作る

“セキュリティ・バイ・デザイン”

ロバストを維持する

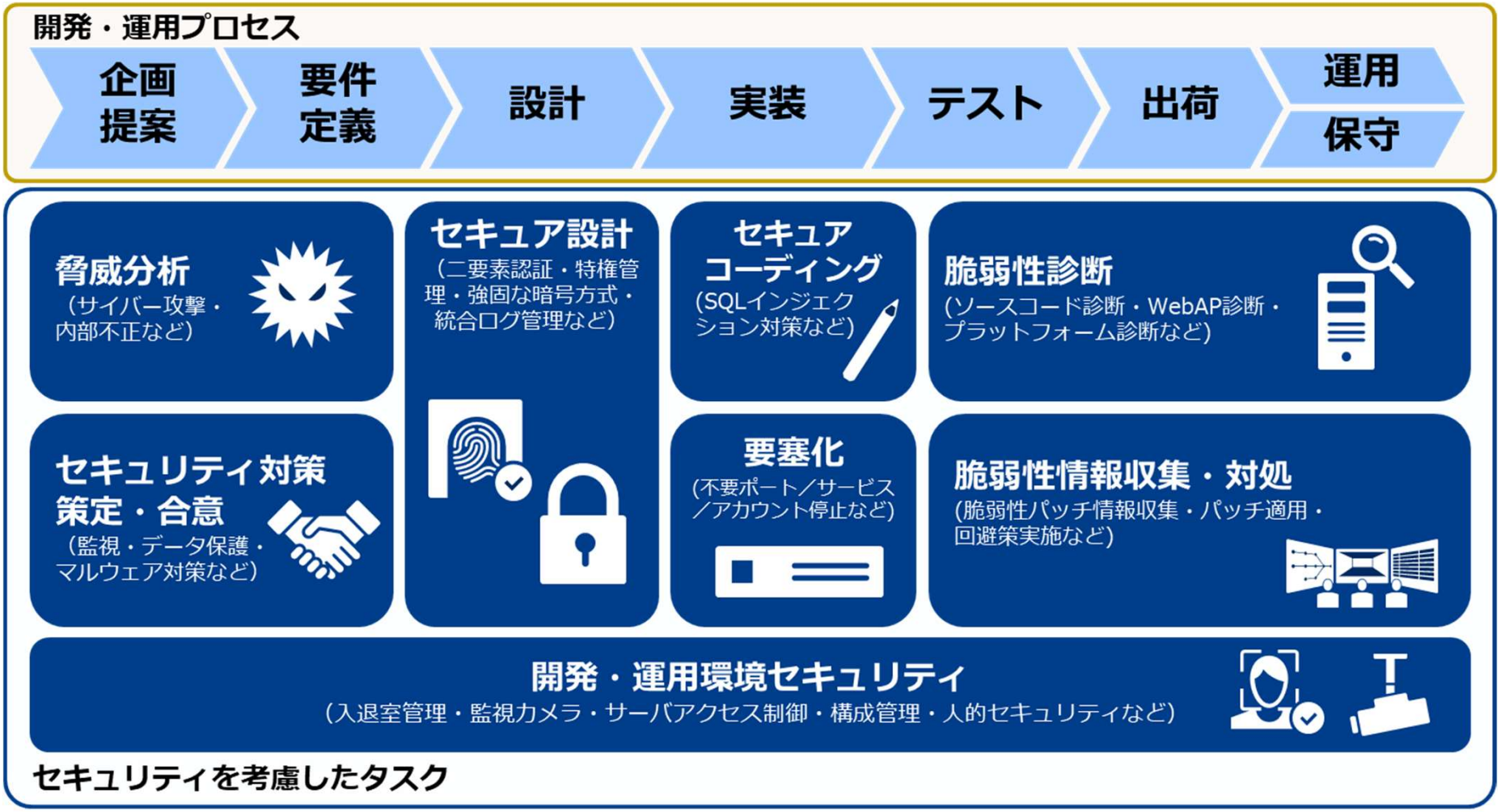
- 脆弱性情報を収集、分析
- 機器の脆弱性を見える化
- 脆弱性への対処実行

“サイバーセキュリティインテリジェンス”

仮想パッチ

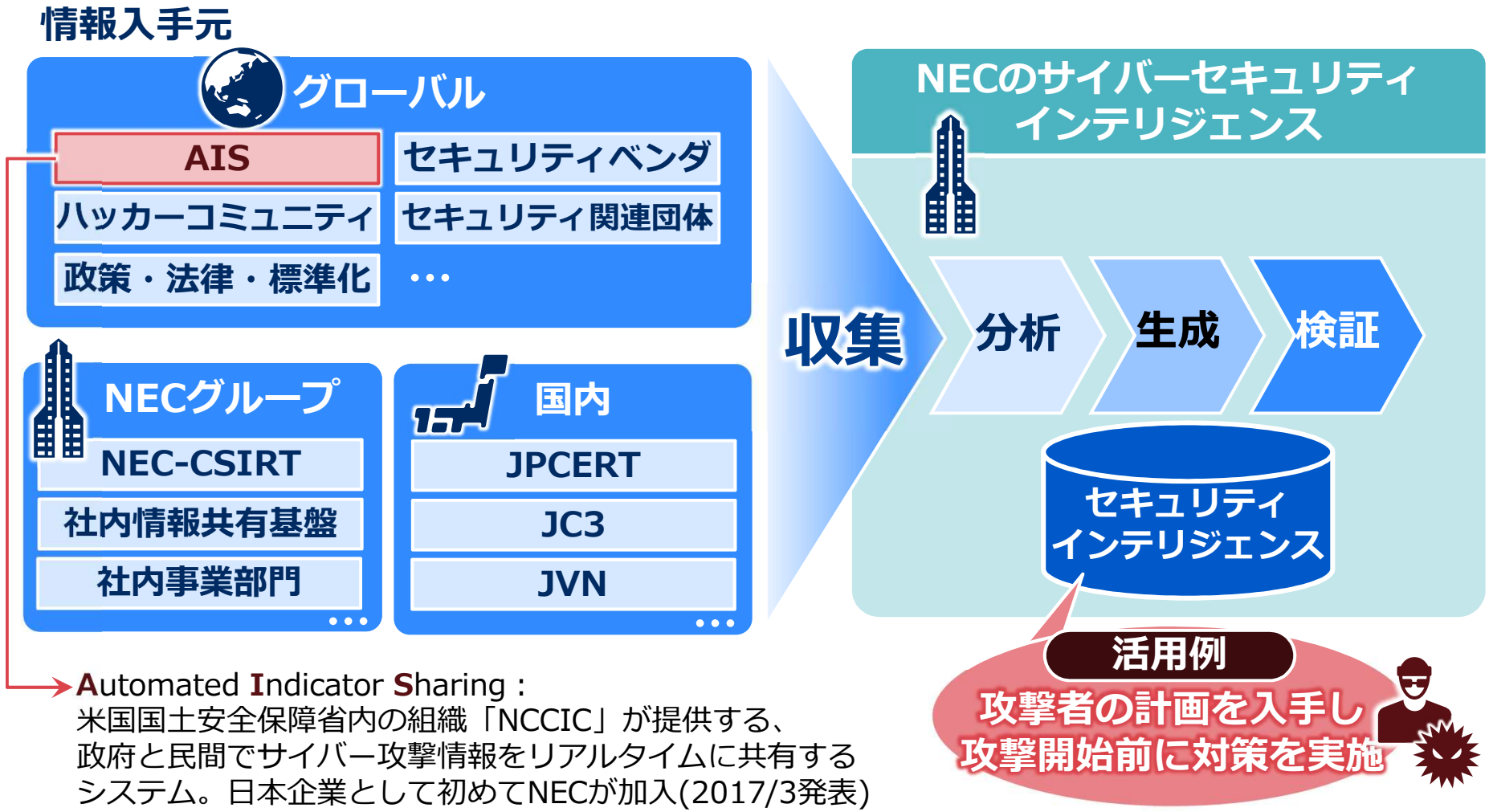
セキュリティ・バイ・デザイン

システム・サービス・製品の企画設計段階から
セキュリティを考慮したプロセスを実践



サイバーセキュリティインテリジェンス

国内外の多様な情報ソースからインテリジェンスを収集・分析・生成した
セキュリティインテリジェンスを、脆弱性管理等に活用



Automated **I**ndicator **S**haring：
米国国土安全保障省内の組織「NCCIC」が提供する、
政府と民間でサイバー攻撃情報をリアルタイムに共有する
システム。日本企業として初めてNECが加入(2017/3発表)

仮想パッチ

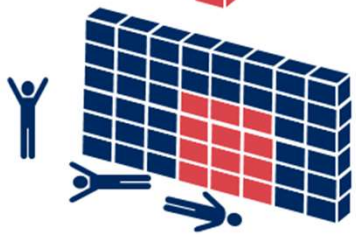
業務システムへのセキュリティパッチ適用には多くの時間とコストが必要
「仮想パッチ」によるシステムが危険な状況を大幅に短縮

本格対応(システム改修)イメージ

穴(脆弱性)を発見

穴を塞ぐ方法を検討し
工事(システム改修)
を人手をかけて
急ピッチで実行

穴を塞いで対応完了

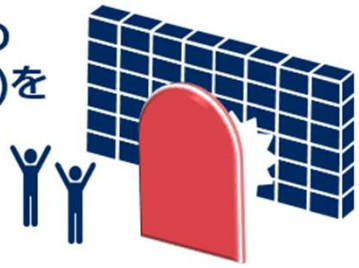


- 時間がかかり攻撃を受ける危険が増す
- コストが高くなる
- 緊急対応となり関係者の負荷が高い

仮想パッチによる対応イメージ

穴(脆弱性)を発見

即座に壁(システム)の
外側に盾(仮想パッチ)を
設置して対応完了



改修計画を立て本来の対応

- 本格対応に比べ短期間で対応可能
- 本格対応に比べ低コスト
- SWの設定で対応するため負荷が低い

セキュリティ人材の育成

NECのサイバーセキュリティを支える人材の育成

セキュリティ公的資格の取得促進

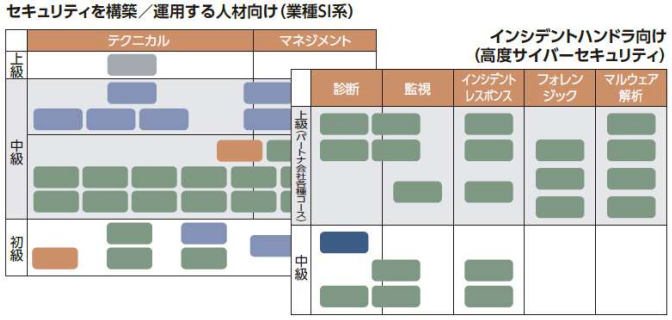
情報セキュリティに関するスキル、業務経験、資格を有している者が核となり、お客様への最適なソリューションの提供に貢献

- **CISSP※1**
- **情報処理安全確保支援士**

有資格者数は国内トップクラス

※1 CISSP®- Certified Information Systems Security Professional

セキュリティ人材育成



セキュリティスキルチャレンジ

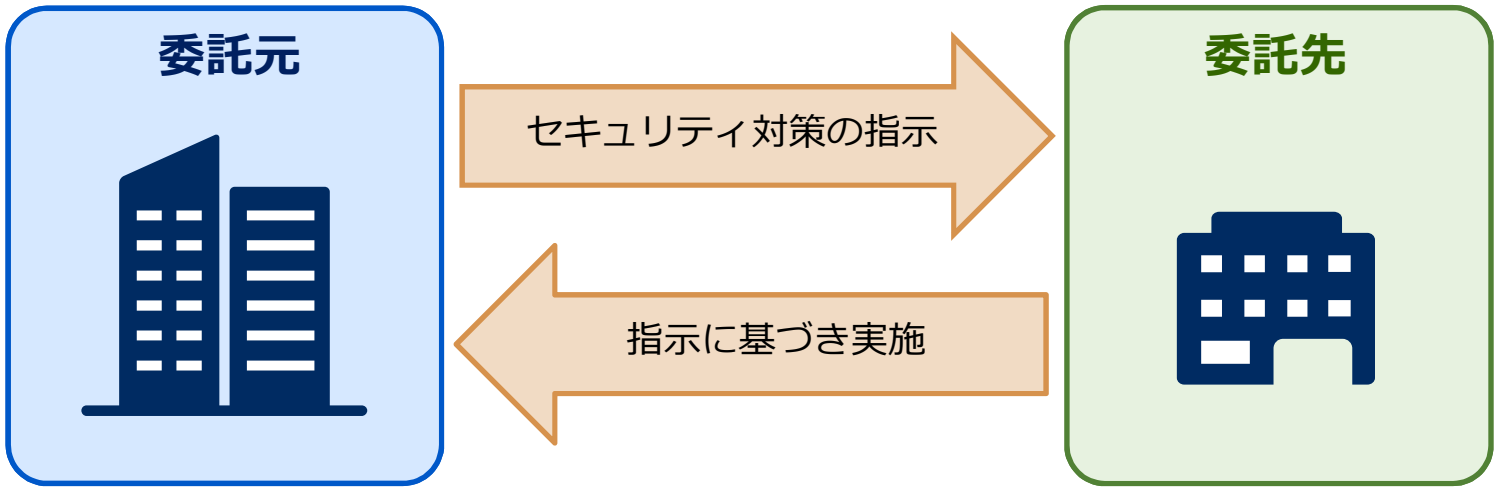
グループ内のセキュリティ人材発掘のため社内セキュリティコンテスト※2を毎年実施

※2 NECグループを対象にCTF（Capture The Flag）競技を開催

SE・開発者、先端・中核技術者の育成を目的としたプログラムの展開

サプライチェーンにおけるセキュアシステム設計

委託先等も含めたサプライチェーンに対するセキュリティ対策が重要に
NECではセキュア開発・運用に関わるガイド類を整備し委託先に指示



NECの取り組み事例

委託業務における
セキュア開発・運用実施要領

お取引先様向け
セキュア開発・運用実施要領

お取引先様向け
セキュア運用・保守ガイド

など

対象はお客様向け製品・システム・サービスの開発・運用

4.これからのサイバーセキュリティ対策のアプローチ

まとめ

Society5.0の進展により

- **つながる機器や情報量が激増することで攻撃対象が拡大**
- **サイバー攻撃によりシステムの可用性が損なわれ事業継続性に影響**

サイバーセキュリティは事業継続性を
重視した対応が不可欠

これからのサイバーセキュリティ対策は

ディフェンスレイヤ　**ロバストレイヤ**

の２つのアプローチで考え、
それらを支える人材の育成やサプライチェーンに対する取り組みも重要

問い合わせ先：NEC サイバーセキュリティ戦略本部
E-mail: info@cybersecurity.jp.nec.com


Orchestrating a brighter world
NEC