鉄道におけるサイバーセキュリティ

通信ネットワークの保護

EBCワークショップ、2023年2月

ノキア・ソリューションズ&ネットワークス合同会社

本セッションの内容：

1. サイバーセキュリティの世界は変化している
2. 近年の鉄道事業者へのサイバー攻撃
3. 標準化とレギュレーション
4. DXとサイバーセキュリティに投資するメリット
5. 鉄道ITシステムを効果的かつ効率的に保護する方法
6. 鉄道のサイバーセキュリティに対するノキアの貢献
7. 鉄道の未来はデジタル!共に行動しよう!

サイバーセキュリティの世界は変わりつつある

セキュリティ運用チームが大量のデータに溺れている

技術シフト

新技術の採用により新たなセキュリティの課題が生じる

アタッカーシフト

サイバー犯罪者はもっと高度な技術、組織的で金銭的動機がある

脅威シフト

脅威の状況が大きく悪化し、従来のセキュリティ対策が無効になる

コンプライアンスの義務化

規制上の罰金は、大規模なグローバル企業には数十億ドルかかる可能性がある

スキル不足

2022年に180万人のサイバーセキュリティ職が未充足

ツールが多すぎる

組織はさまざまなツールで多くのベンダーを使用している

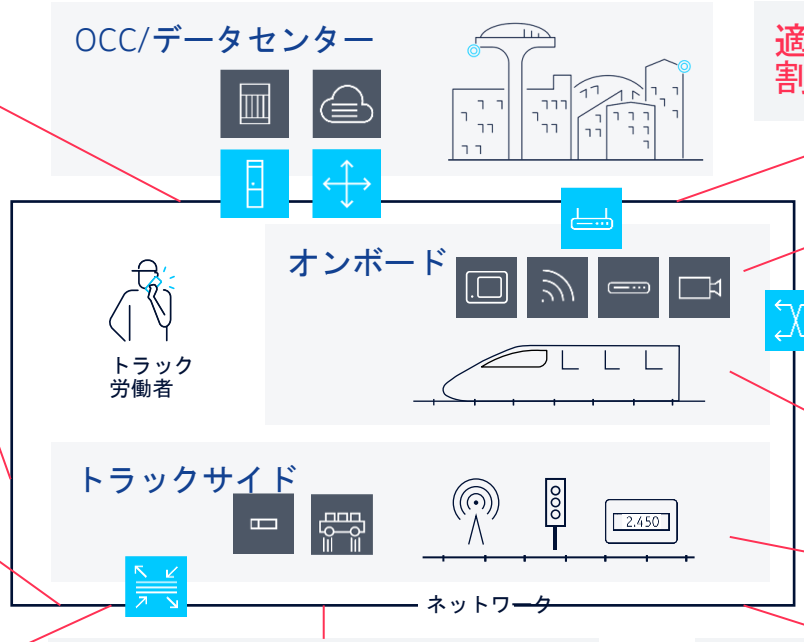
鉄道インフラにおけるサイバーセキュリティの脅威

適切な権限管理なし

外部メンテナンスアクセスが分離されていない

脆弱性の悪用

直接アクセス



適切なゾーン分割なし

弱偏析

セッション監視/ログ記録なし

信号IDSなし

物理アクセス

サイバーセキュリティ対策はオプション(任意)ではない、安全で効率的な鉄道運用のための要件(必須項目)である。

収益と財産の損失	復旧・復元費用	訴訟の可能性と罰則	ブランド力の低下

我々は誰と戦っている?
リスクはどこにでもある...そして多面的である

日常業務

稀だが致命的なインシデント

犯罪者
ハッキングが大きなビジネスになった-売却可能なデジタル資産を狙う

- 個人情報
- クレジットカード・デビットカード情報
- 知的財産

MALICE (悪意)
技術力と動機が組み合わさった、組織に反感を持つ者

- 不満を持つ社員
- 悪質プログラム
- 反社会的な攻撃
- 能力の証明

テロリスト
重要インフラのハッキング
テロリストにとって魅力的な選択肢となる

- インフラの混乱
- 経済への影響
- 器物損壊
- 人命の損失

政治的、国家戦略
最も洗練され、技術的に可能な脅威

- 攻撃能力
- 軍事作戦
- 国家秘密の漏洩 、営業秘密の取得、知的財産
- スパイ活動

考えられる結果:

- **データ盗難**
- **運用・サービス遅延**
- **恐喝**
- **貨物/物理システムの損傷**
- **乗客の負傷・喪失**

投資vs利益
自動化と特権アクセス管理の価値

IT/ICTシステム導入と運用コストの1~2%をCyber Securityに充てる事で、完全なセキュリティを担保できる。

392万ドル

の平均コスト
データ侵害

+95%

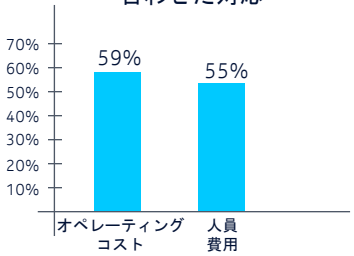
自動化が実装されていない場合、データ侵害のコストが高くなる

279日間

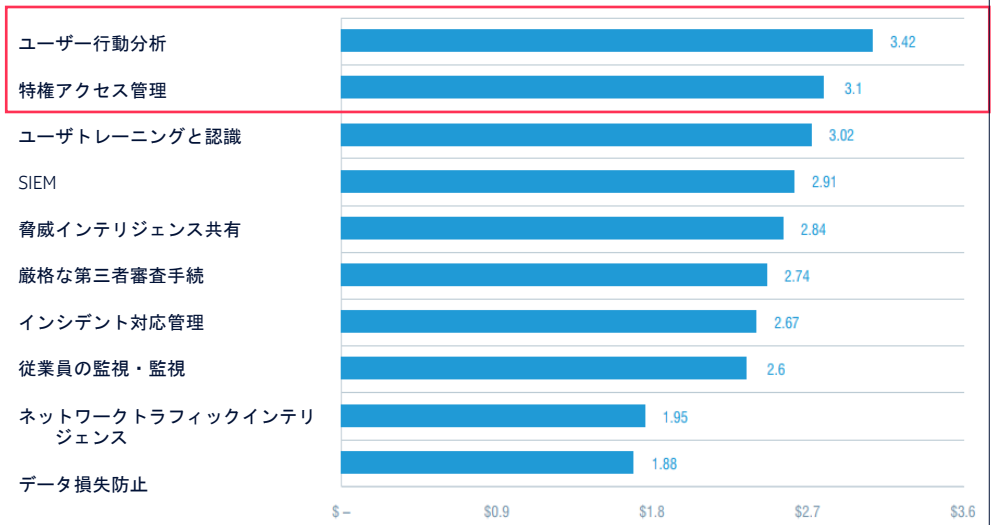
識別する時間と
データ侵害を含む

- 30% アラートのうち調査される
- 72% 調査されるアラームは偽
- 54% 正当な警報改善されない
- 53% 時間が費やされる検出

サイバーオートメーションはコストを削減する
強く同意し同意する
合わせた対応



の導入によるコスト削減
サイバーリスク低減ツールと活動



出典: Ponemon, 2020 cost of insider threat; Ponemon, 2019 cost of data breachesデータ侵害; Ponemon, 2018 cost benefitsサイバーオートメーション

主な国際標準とベスト・プラクティス
最も重要な例...

ISO 2700 x
情報セキュリティ管理システム
(ISO/IEC 27001は、情報セキュリティマネジメントシステム (ISMS) の要件を提供するファミリの中で最もよく知られた標準である)。

ITU-T X .805
システムのセキュリティアーキテクチャ
エンドツーエンド通信

IEC 62443 (-2-4)
産業用自動化制御システムのセキュリティ

EN 50126
信頼性、可用性、保守性と安全性 (RAMS)
(EN 50126はIEC 61508の鉄道部門固有のアプリケーションである。)

EN 50128
通信、信号および処理システム–鉄道の制御および保護システムのソフトウェア

EN 50129
通信、信号および処理システム–信号用の安全関連電子システム

EN 50159について
鉄道用途-通信、信号と処理システム-
伝送システムにおける安全関連通信

規制圧力の高まり

EUのサイバーセキュリティ戦略
市民を守るための行動,
役割・責任。

一般的なデータ保護規制
の大幅な締め付け
データプライバシー要件

ミッション・クリティカル通信
重要な通信システムのセキュリティを確保するためのベスト・プラクティスと標準を開発し、促進する。

APTAセキュリティ
プログラムとリソース
交通機関がセキュリティの維持と改善に成功していることを確認するのに役立ちます。

各政府の法律
事業者は、重要なサービスだけでなくデータプライバシーを保護するために、セキュリティ要件へのコンプライアンスを監視し、セキュリティ侵害を報告する必要がある

社会インフラを守るには。。。
ガイドラインに従って、信頼パートナーと協力・行動

ベストプラクティス

法律、指令、規範および勧告

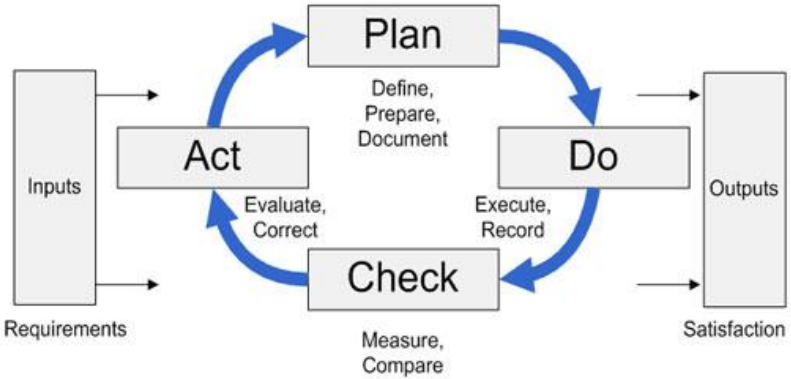
特定の業界/セキュリティニーズによって推進される

そのほとんどは、サイバー犯罪と戦うためには、**積極的な**関与と継続的な改善が必要であるという共通点がある。

例

ISO 27001の枠組みにおける**代表的な安全方法**

交通システムのリスク態勢を継続的に改善する



1. コンテキストの確立
2. リスク識別
3. リスク推定
4. リスク処理
5. リスク受容
6. リスクコミュニケーション

鉄道網向けノキアのサイバーセキュリティ

セキュリティ業務

セキュリティ業務の分析とレポート作成を自動化し、ビジネス上の意思決定を向上

IP/MPLSセキュリティ

ネットワークグループ暗号化

IPSec

ファイアウォール

光通信

レイヤ1トランスポート暗号化

鍵の集中管理

無線とコア

GSM-R, LTE, 5G, IoT, C-ITS, A2G, T2G

無線暗号化

IMS暗号化

エンドポイントセキュリティ

脅威の検出と暗号化、署名と認証を含むエンドポイント。

IoTデバイス

Nokiaのセキュリティサービス

セキュリティリスクインデックス評価フレームワーク

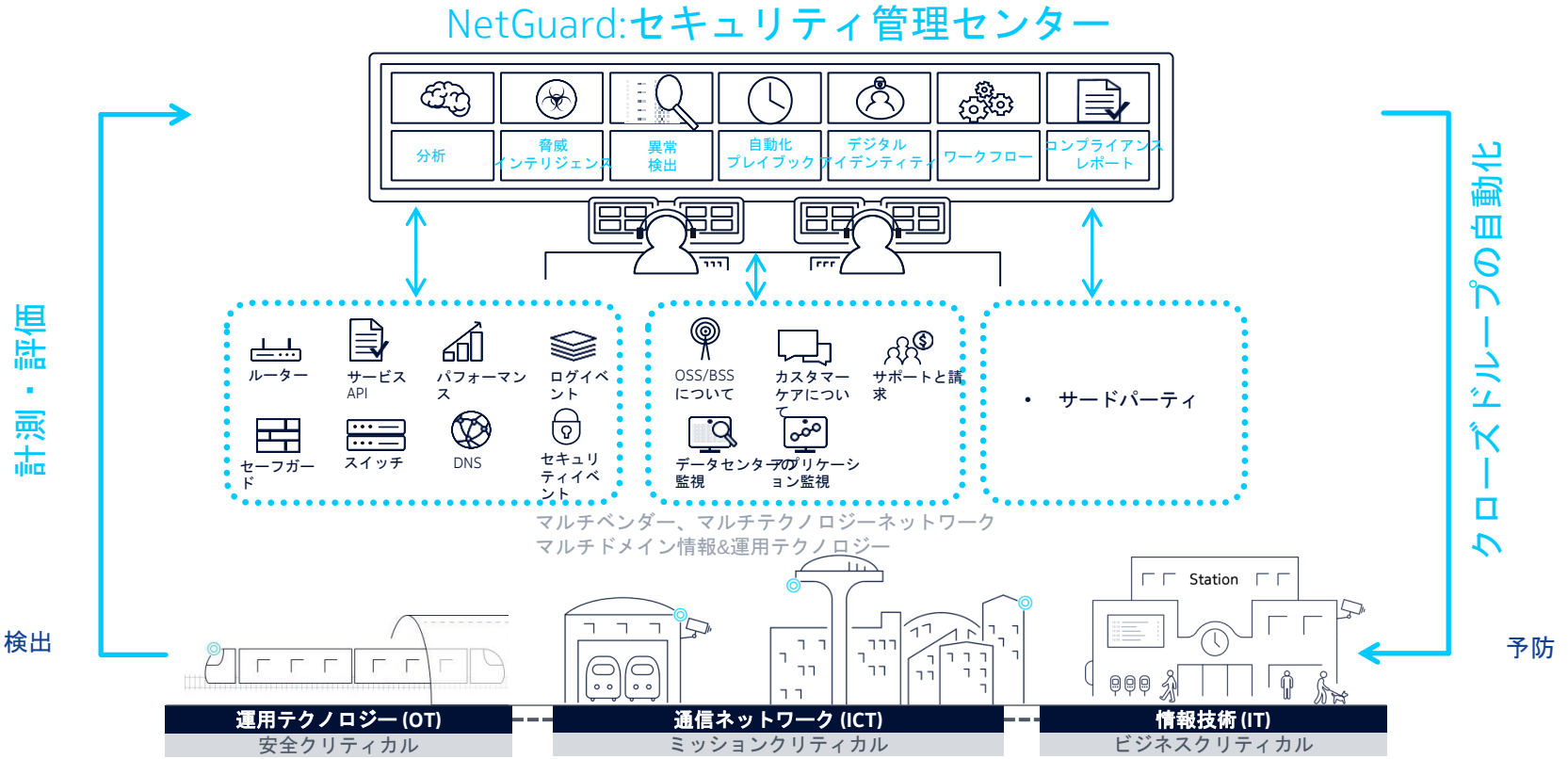
ソリューション検証およびセキュリティコンサルティングサービス

マルチベンダーネットワーク向けのマネージドセキュリティサービス

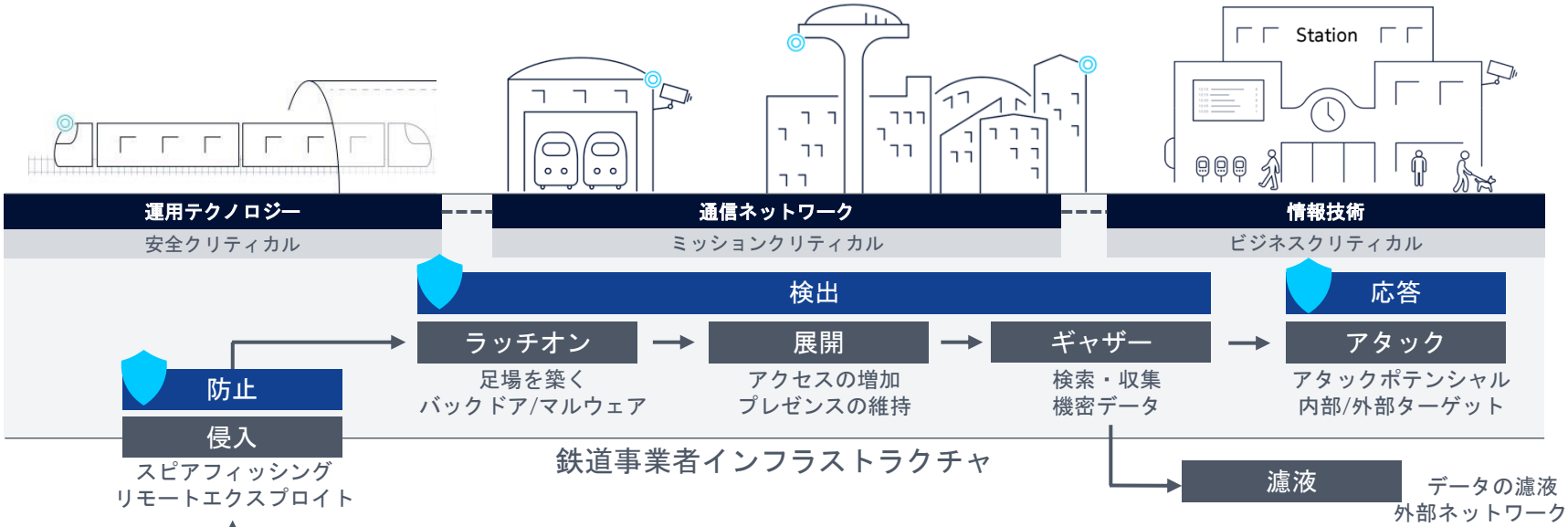
NetGuard

Security you can rely on

Nokia ACTIVEセキュリティ
E2E分析と自動化によるセキュリティ



脅威の軽減
悪サイクルにブレーキをかける



- **OTネットワークは社会に重要な価値と重要役割を持つ。**
- **OTネットワークを保護する事は必要不可欠。鉄道運用会社の使命。**

徹底したセキュリティの必須要素

セキュリティプロセスの自動化

攻撃の急増に対応

数千のアラートの優先順位付けと処理

応答時間の短縮

エンドツーエンドの保護

IPとLTE

シグナリングとコア

デバイスセキュリティ(IoTなど)

ネットワークセグメンテーション

トラフィックの分離

不正なトラフィックを制限するファイアウォール

セキュリティ分析

ネットワークとデバイス間でデータを相関させる

異常を特定し、対応を推奨する

機械学習

暗号化データの保護

侵入された場合でも機密性と完全性を確保する

多層IP/MPLSと光暗号化

冗長性

運用ネットワークと輸送の安定性

あらゆる攻撃からの迅速な回復

アクティブなセキュリティ管理

セキュリティの集中管理システム

自動化、分析、レポート作成

標準・規格

ISO 2700 x

ITU-T X .805

IEC 62443 (-2-4)

EN 50126/28/29/59

固定通信、モバイル、IoTセキュリティで実績のあるリーダー

500+
セキュリティプロジェクト

350+
セキュリティ認定・資格専門家

30+
グローバル運用ネットワーク管理、TelcoおよびEnterprise

#1
セキュリティ保護された
GSM-R, LTE, 5G, FRMCS

10+
主要なセキュリティ標準の確立における積極的な役割

グローバル
顧客現場の知見と経験

セキュリティ監視センター
専用ビジネスユニット

研究開発
Bell Labs中央研究所
4つのBUのR&Dセンター

NOKIA

結論

- 既存システムと新しいインフラを保護するのに遅すぎる事はない。
- サイバーセキュリティは複雑ではなく、高価でもない。必要な投資。
- DXに自信を持ち、5 G、IP-MPLS、IoT、クラウド、AIを安心に実装。
- サイバーセキュリティの知識を得て、段階的な対策、準備、安全を確保。
- サイバーセキュリティは新しい文化、習慣、基本知識。関係者全員。
- 信頼できる責任ある機器ベンダー、業界団体、標準化組織、規制委員会のコミュニティに参加。
- 技術の進化にアップデート。 孤立しない、無視しない、出遅れない事。
- セキュリティは日本経済の発展の為、国際競争力向上のチャンス！

安全・安心なデジタルスマート鉄道の実現

NOKIA

All aboard. All connected. All secure.

連絡先:
masayuki.1.sato@nokia.com
運輸セグメント営業部

hiroto.goya@nokia.com
グローバルエンタープライズ事業CTO