日本の産業サイバーセキュリティの現在地とこれから

Nov 7 2019 | 9:00- | Prince Park Tower Tokyo

Hiroshi Sasaki
Sr. Security Advisor – McAfee Japan

佐々木　弘志
シニア・セキュリティ・アドバイザー　マカフィー株式会社

VUCAの時代

2016年11月9日：トランプ大統領選勝利
https://www.asahi.com/special/timeline/20161109-trump-history/

Volatility（変動性・不安定さ）
Uncertainty（不確実性・不確定さ）
Complexity（複雑性）
Ambiguity（曖昧性・不明確さ）

分断/格差の時代

AI台頭で消える職業

SNS、フェイクニュース、ポリコレ棒

昭和の価値観（精神論）の崩壊

災害時に露呈する「想定外」

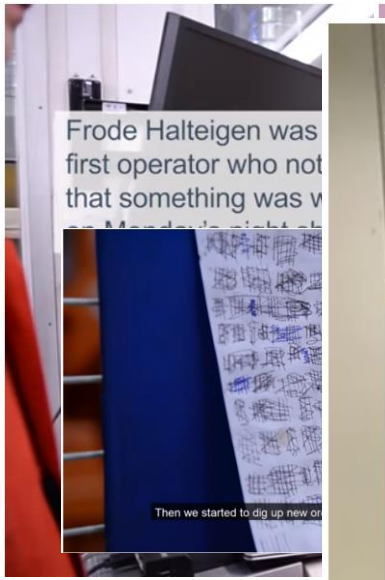
サイバー攻撃の報復がミサイル

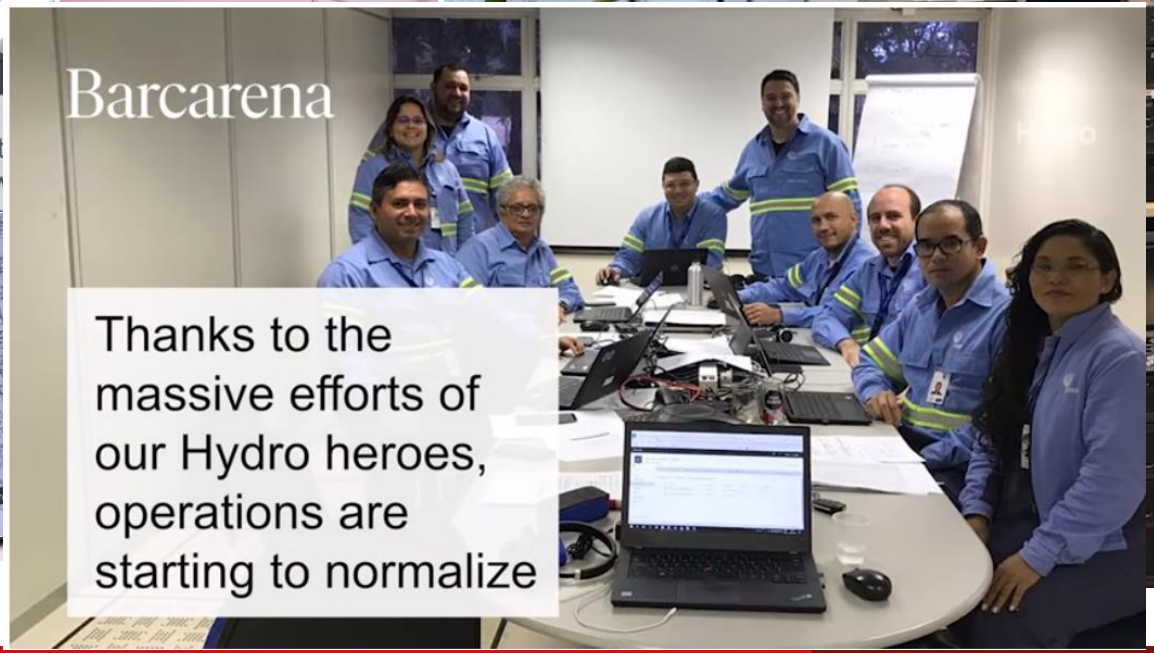
グローバル化、技術の進歩により、様々な事象が予想できない形で起こる時代

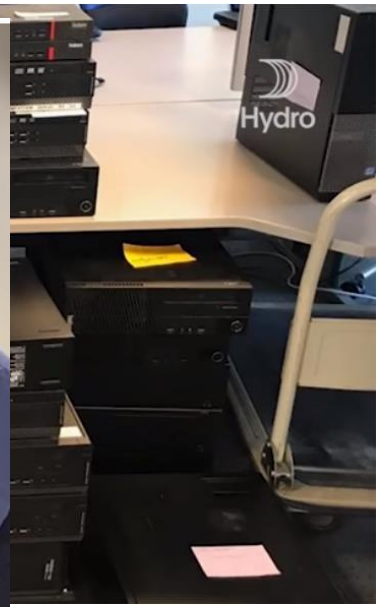
SNS時代のインシデント対応広報の在り方

ノルウェーのアルミニウム製造大手 Norsk Hydro（世界40か国、従業員3.5万人以上）は2019年3月19日未明にRansomwareによるサイバー攻撃を受けた。最初の1週間（3月25日時点）で3億～3億5000万ノルウェークロネ（4000万ドル相当）に達したと推定。**事件直後からFacebookで情報公開。状況を説明する広報動画も作成。**

https://www.youtube.com/watch?v=S-ZlVuM0we0







Speakers

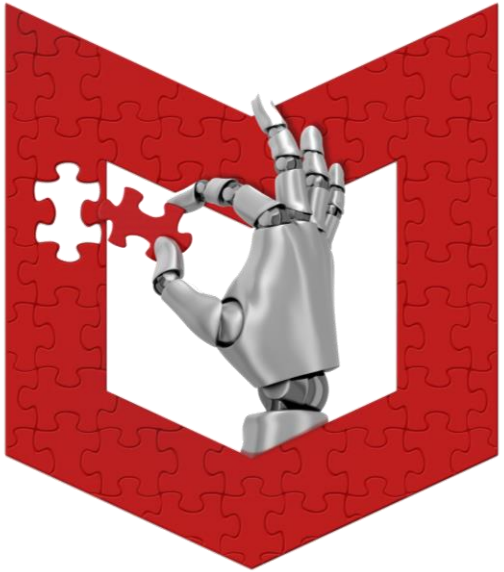
佐々木　弘志
シニア・セキュリティ・アドバイザー
CISSP
サイバー戦略室
マカフィー株式会社

CIP/IoTセキュリティの文化醸成をミッションとしている

・産業制御システム開発者（14年）
・マカフィー株式会社
　産業制御システムセキュリティのコンサルタント（6年~）
　講演、執筆多数。
・IPA 産業サイバーセキュリティセンター サイバー技術研究室 専門委員（2017年7月～）
・経済産業省の非常勤アドバイザー 情報セキュリティ対策専門官（2016年5月～）

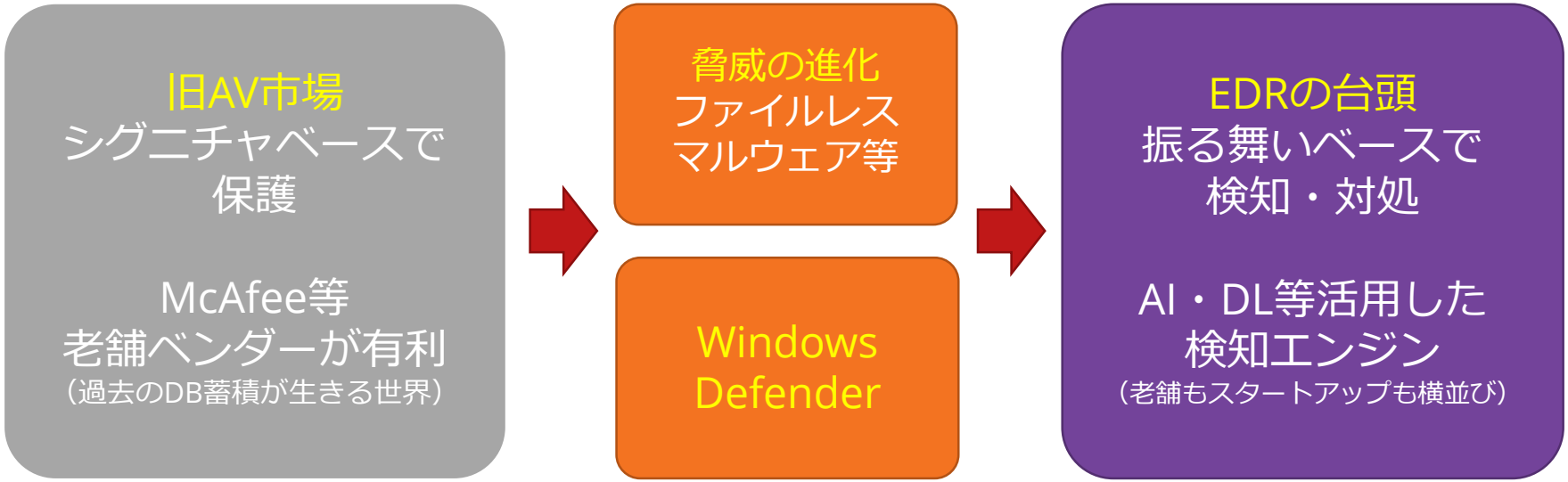
Agenda

- 日本の産業サイバーセキュリティの現在地とこれから
  - サイバーセキュリティもVUCA の時代
  - DX＆ゼロトラストネットワーク
  - 産業サイバーセキュリティの基本的な考え方
  - ４P対策の現状と課題
  - ４P対策のこれから



サイバーセキュリティもVUCAの時代

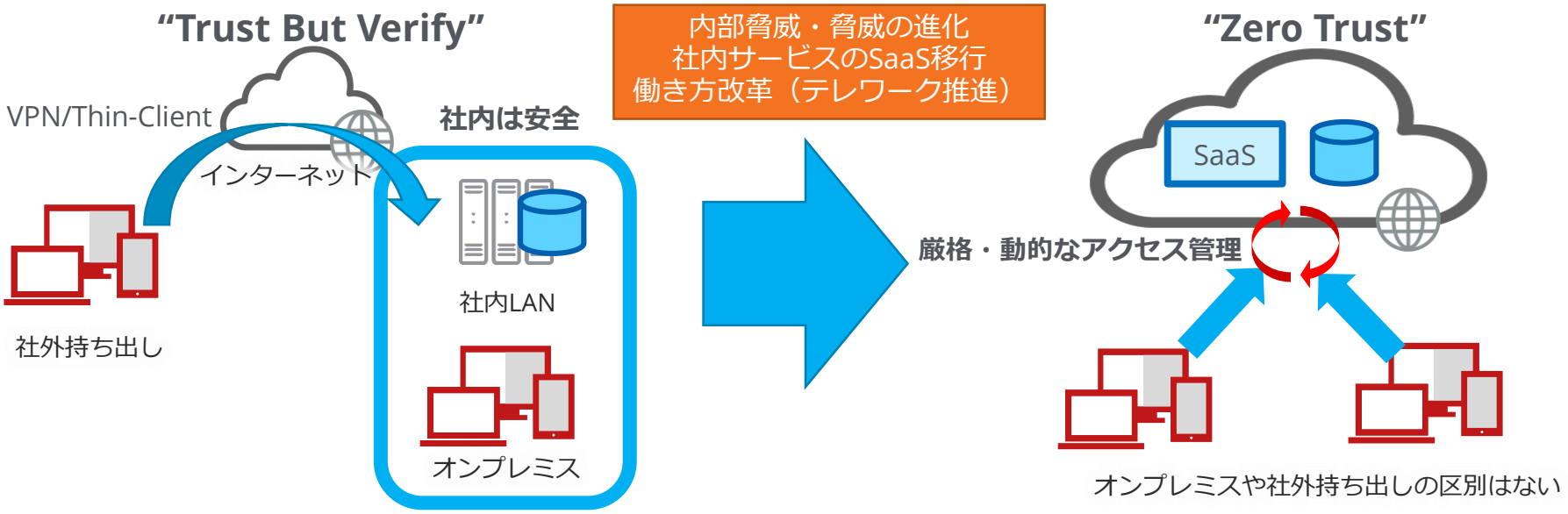
エンドポイントセキュリティの世界に起こったゲームチェンジ



大きなゲームチェンジが、予想できない形で、短サイクルで起こり、
旧ビジネスが一瞬で終わってしまう時代（**損切りできないと負ける**）

ゼロトラストネットワークとは？

Forrester Researchが2010年に提唱した考え方で、“社内（ネットワーク内）は安全である”という前提に立って境界を守るやり方では守れなくなった現状を踏まえ、「信頼しないことを前提とし、全てのトラフィックを検査、ログ取得を行う」という性悪説のアプローチ



https://www.itmedia.co.jp/enterprise/articles/1809/27/news011.html

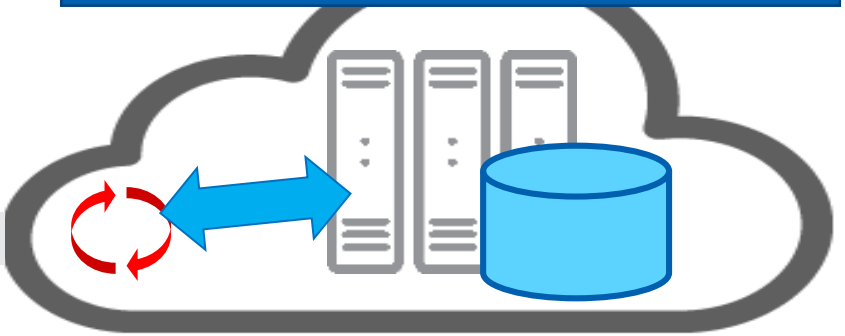
ゼロトラストネットワークに必要な機能

マルウェア対策

認証を確立しさえすれば
コンテンツは暗号化される

&Sf12d!”d%a&LoK~s2SAd+Qs/…

クラウド上のデータ保護（SaaS）
設定管理（IaaS/PaaS）



厳密・動的なアクセス管理

- アクセスポリシーの定義
- 管理デバイス？OSパッチ？AV？HDD暗号化？アクセス場所等状況に応じて、リソースにアクセスできる権限を制御する

オンプレミスのネットワーク製品はやがて廃れていくものと考えられる

ゼロトラストネットワークへの移行はDXのひとつの形態である

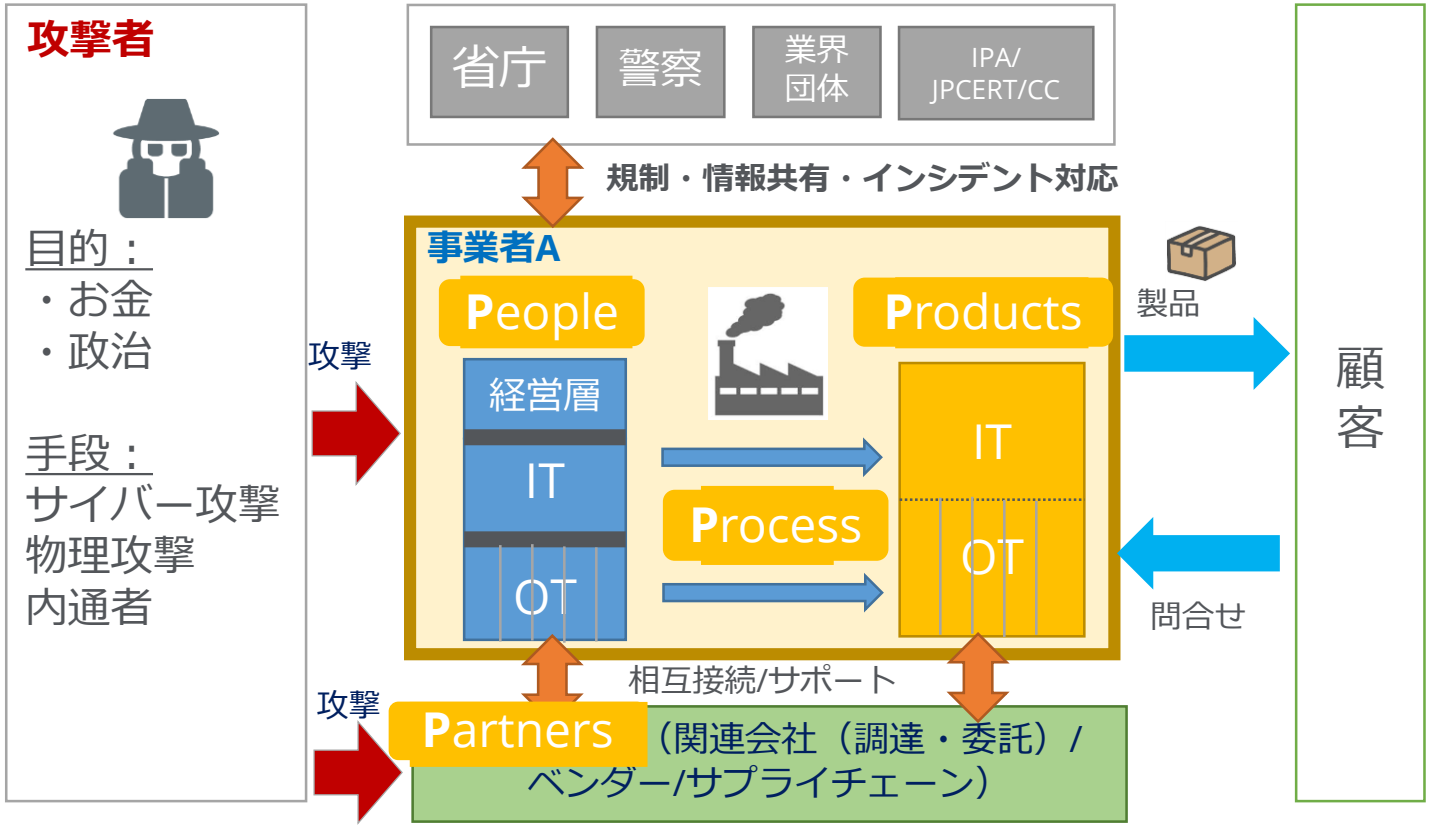
DXの定義

外部変化（顧客、市場）
↓
内部変化
（組織、文化）
↓
プラットフォーム活用
（クラウド、モビリティ等）
↓
新サービス・ビジネスモデル
↓
顧客に対する価値の創出
↓
企業が競争力をもって生き残ること

ゼロトラストNW移行

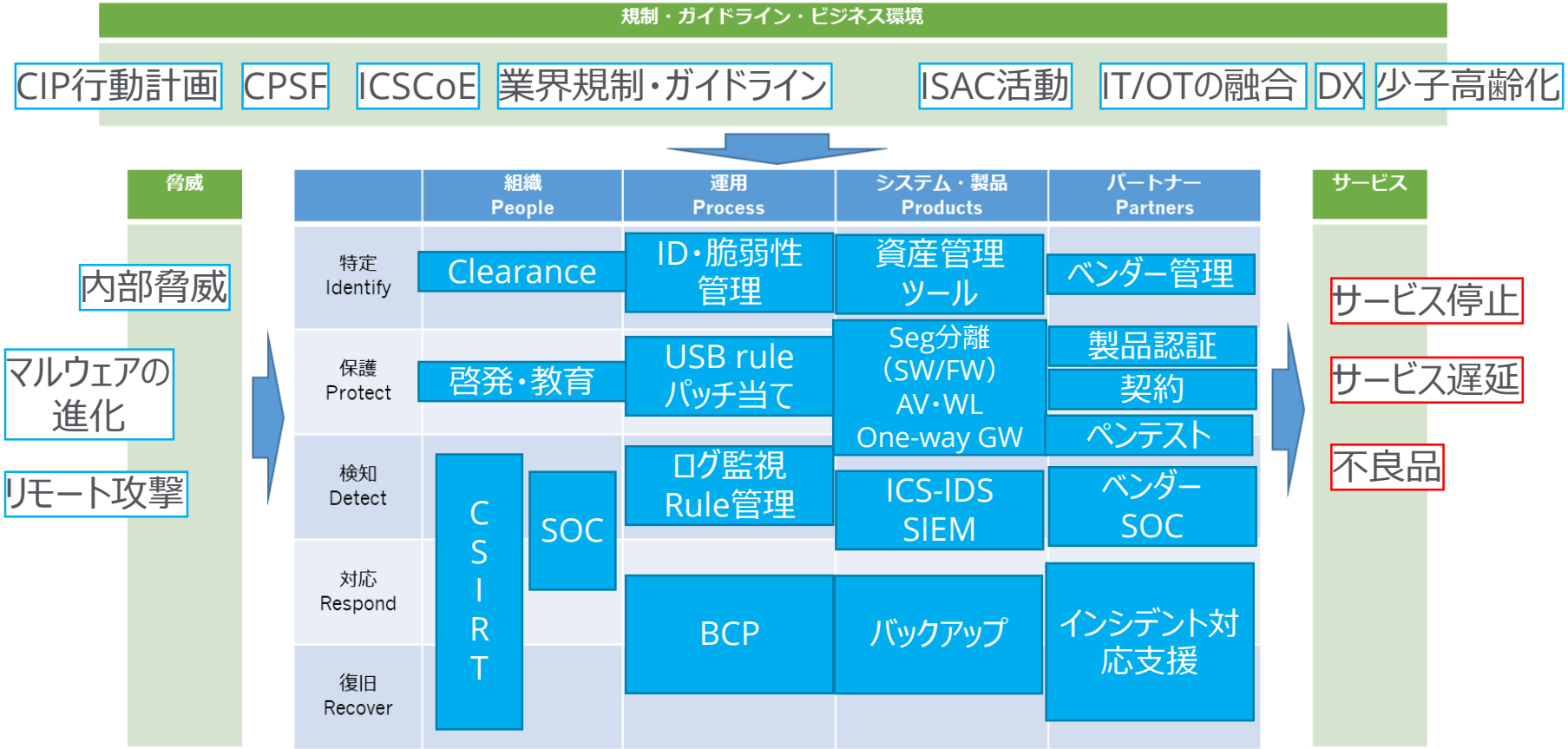
外部変化（脅威の進化）
↓
内部変化
（テレワーク推進・働き方改革）
↓
クラウド移行に伴う
動的で厳格なアクセス管理・データ保護
↓
新しい働き方のモデル
↓
社員の作業効率化・モチベーション向上
↓
企業が競争力をもって生き残ること

産業サイバーセキュリティの基本的な考え方



産業サイバーセキュリティ検討のためのフレームワーク

産業サイバーセキュリティにおける現状の対策整理



４P対策の現状の課題

People（組織）

- 経営層の理解不足
- 現場の理解不足
- 教材・外部/内部トレーニング不足
- サイバー演習のノウハウ不足
- IT/OTセキュリティ人材不足

Products（システム）

- 可用性重視のため既存システムへの対策が困難（旧Windows等）
- 新システムのセキュリティ・バイデザインのノウハウ不足
- OT対応製品の少なさ⇒高価

Process（運用）

- 既存BCPのサイバー対応の困難さ
- OT向け検知ルール作成の困難さ
- ポリシー/標準/ルールの更新頻度
- 業界ごとの違いで自動化が難しい
- IT/インターネット接続の管理負担

Partners（パートナー）

- 2nd ティア問題
- 高価なセキュリティ認証
- ガイドライン・標準がない
- 各自バラバラのチェックリスト
- 対策コスト・効果バランスが悪い

産業サイバーセキュリティの文化が育っていないための悪循環が発生

４P対策のこれから（People）

リソースシェア

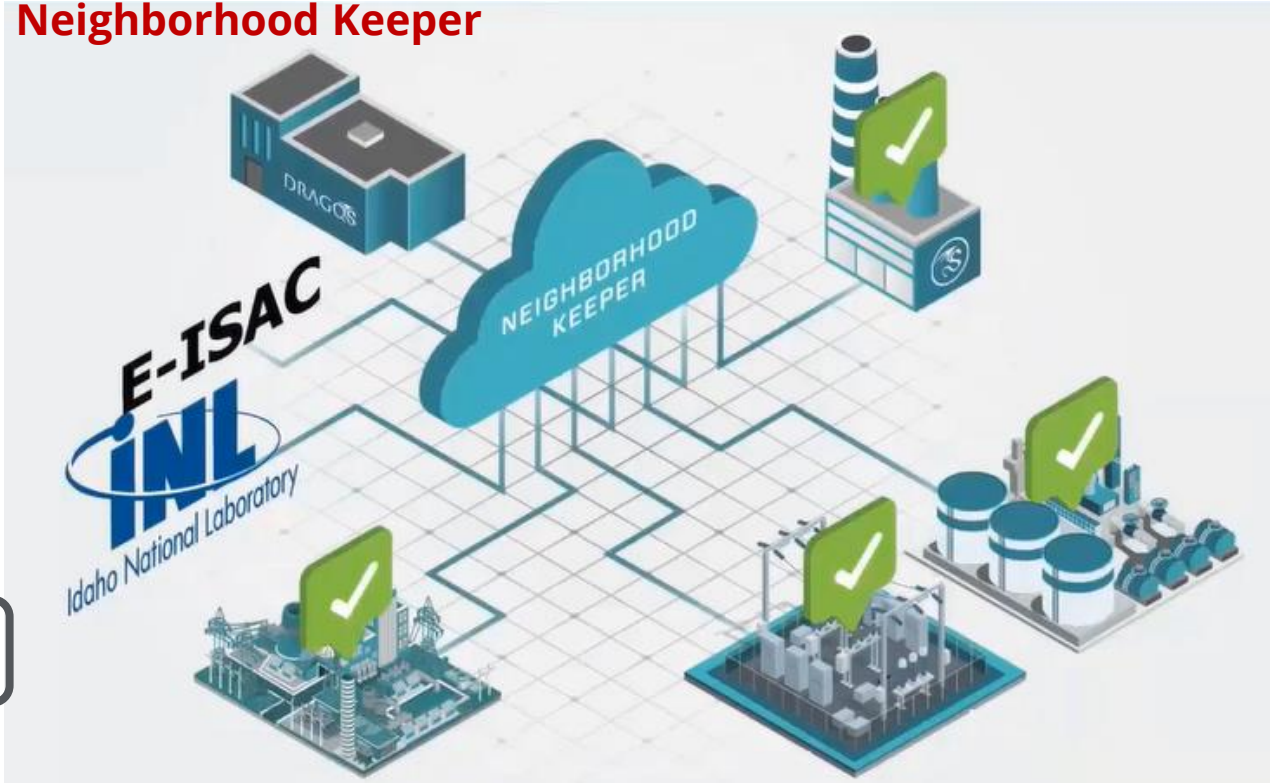
人材不足はすぐには解消しない
OTは業界知識が必要

↓

同業界での**ノウハウシェア**
（ISAC）

↓

同業界での**人材リソース**シェア



https://vimeo.com/318813654

４P対策のこれから（Process）

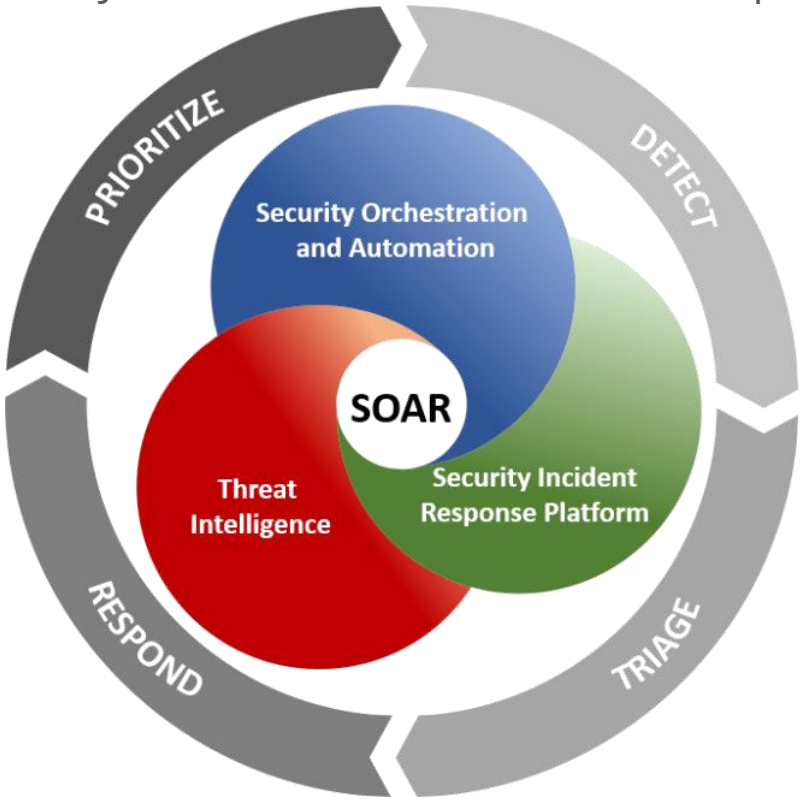
自動化

人材不足はすぐには解消しない
オペレータへの教育は大変

OTインシデント対応の自動化

「OTのIT化」の進展
仮想化・５G活用によるクラウド化
OT版のSOAR

SOAR(Security Orchestration, Automation, Response)



https://source44.net/security-orchestration-automation-response-soar/

４P対策のこれから (Products)

セキュリティ・バイ・デザイン

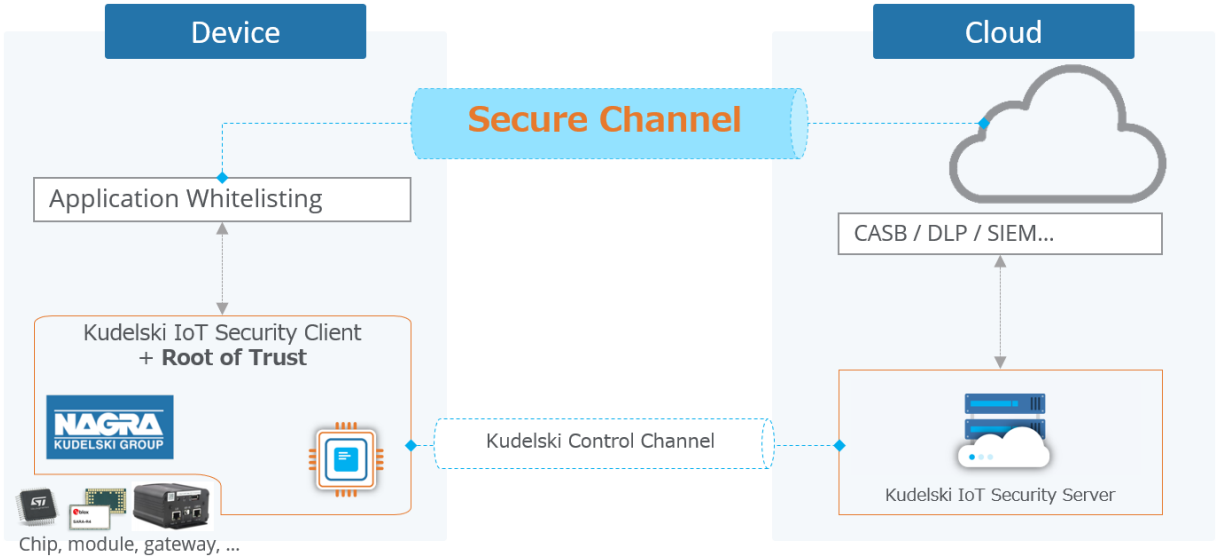
新規産業システムを開発時には
最初からセキュリティを
考慮することで**結果的に安価に**

例）

チップレベルの
End to End 保護
ソリューションの導入

https://vimeo.com/318813654

チップレベルの通信コンテンツ保護の例



- 安価なデバイスにも適用可能（OS依存しない）
- ファームウェアのアップデートが安全にできる
- チップレベルの「Root of Trust」なので改ざんが困難
- **ゼロトラストネットワーク**と近いコンセプト

基本的なIoTセキュリティのアプローチ

Simple. Secure. Sustainable.

Design & Evaluation

1. DESIGN

Design a secure IoT solution tailored to your business needs

Security Platform

2. RUN

Manage and control all your key IoT assets with simple APIs

Managed Services

3. SUSTAIN

Maximize ROI by managing your device and security lifecycle

https://youtu.be/k6O2oMX3BR4

Secure video surveillance

新規または既存のカメラインフラの安全なビデオ監視の実現

-安全性の確保
-プライバシーの保護
-エビデンスの生成

NAGRA
KUDELSKI GROUP

Use case: 連邦政府機関での実装例

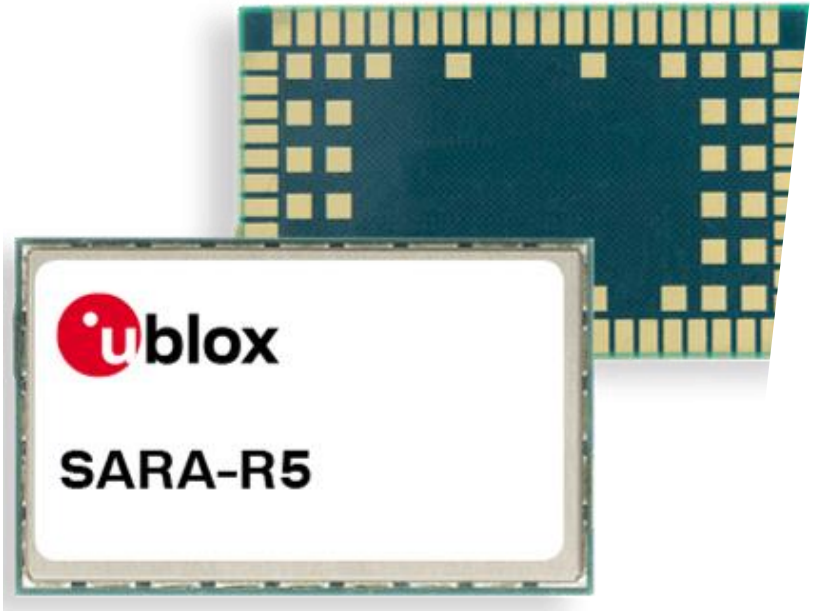
- **Site surveillance to secure physical access**
- Protect existing video surveillance equipment
- Enable intelligence close to the camera

顧客の決定理由

- Support for **legacy and deployed cameras**
- **Low-latency real-time** content encryption
- Protect privacy **to prevent information leaks**

顧客の利益

- End-to-end video encryption
- Dynamic access control for video decryption
- **Data integrity** to satisfy **legal evidence rules**



Wearable healthcare devices

エンドツーエンドの
セキュリティを備えた
ウェアラブル医療センサー
からの継続的なデータ記録
により、**データの機密性**を
確保し、**患者の安全**を保護
します.

NAGRA
KUDELSKI GROUP

Use case: Leikr 社 U-blox スマートメディカル時計

- **A wireless gateway for medical data**
- U-blox module with embedded Kudelski RoT
- Sends data from multiple sensors to Cloud

顧客の決定理由

- **Low-power, bandwidth efficient**
- Strong signal & interference management
- End-to-end security

顧客の利益

- **Simple & secure data** from different devices
- **Reliable connectivity** so vital data is not lost
- **Encryption protects patient safety & privacy**

https://www.youtube.com/watch?v=cdncs6r25aw

４P対策のこれから (Partners)

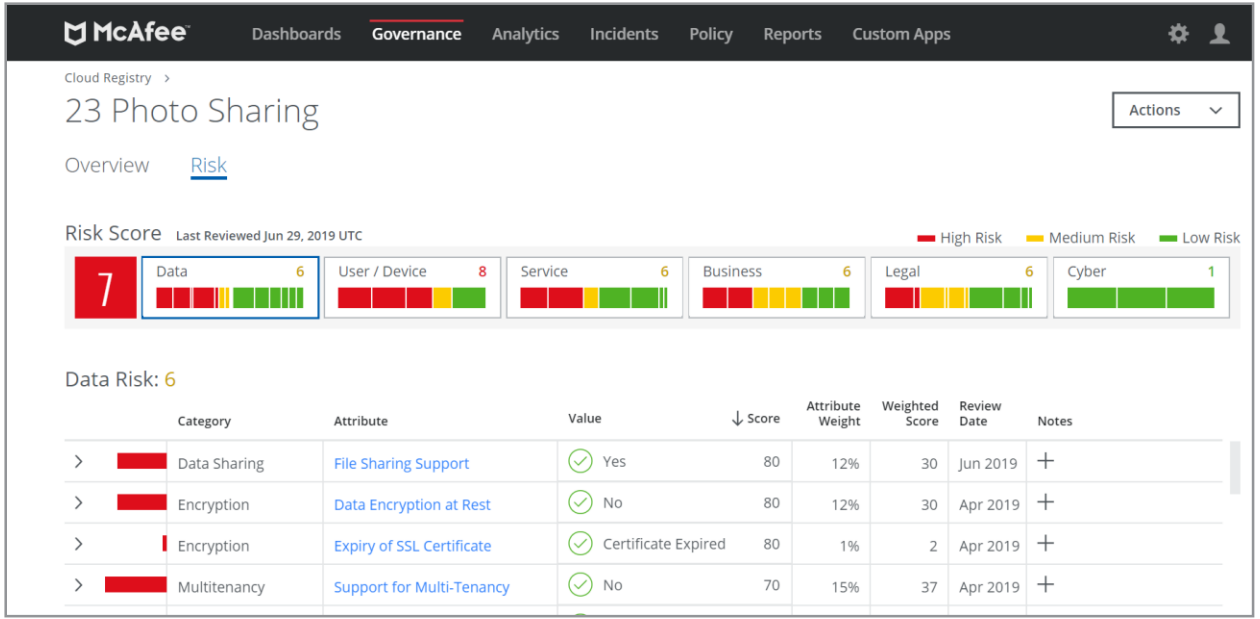
動的リスク評価

通常の静的な製品**認証**では
脅威の進化に対応できない

エンドユーザ・ベンダーが
契約時に毎回別のフォーマットを
用いるのは無駄

動的な製品・
ソリューションリスク評価
（レーティング）

MVision Cloud Cloud Registry 機能



- クラウドサービスの動的な安全性評価
- 項目に応じて、リスクの重みづけがされている
- 非開示項目はリスク高く評価される⇒ベンダーの情報開示へ
- ベンダーの改善が早く評価に反映される

https://vimeo.com/318813654

日本の産業サイバーセキュリティのこれから

「リソースシェア」・「自動化」・
「セキュリティ・バイ・デザイン」・「動的リスク評価」

一番大事なのは、必要なセキュリティ対策を
（VUCA時代の）ビジネス環境に応じて柔軟に採用できる
経営判断の「速度（Agility）」