業界トップクラスのサイバーセキュリティーサービス

IIFES2024

シュナイダーエレクトリック
サービス事業部　インダストリーサービス

Life Is On Schneider Electric

Schneider Electric のサイバーセキュリティーソリューション

自社工場で採用し、培ったノウハウやソリューションをお客様にも提供

現状把握 ▶ **監視** ▶ **保全**

マネージドセキュリティーサービス（MSS）

シュナイダーが自社工場用に構築したCCSH (OT-SoC)の機能を
アセスメントから監視・対応まで一気通貫で顧客向けに提供

サイバーセキュリティー アセスメントサービス（CAS）
設備の現状把握/評価を行うサービス

サイバーセキュリティーアプリケーションプラットフォーム（CAP）
社内ネットワーク等に対する不正アクセス等を防ぐサービスプラットフォーム
（不正侵入検知システム）

セキュアリモートアクセス（SRA）
資産へリモートアクセスする場合の管理と操作記録を行うサービス

Life Is On Schneider Electric

現状把握 ▶ 監視 ▶ 保全

マネージドセキュリティーサービス（MSS）

シュナイダーが自社工場用に構築したCCSH (OT-SoC)の機能を
アセスメントから監視・対応まで一気通貫で顧客向けに提供

**サイバーセキュリティー
アセスメントサービス（CAS）**

設備の現状把握/評価を行うサービス

**サイバーセキュリティーアプリケー
ションプラットフォーム（CAP）**

社内ネットワーク等に対する不正アクセス等を防ぐサービスプラットフォーム
（不正侵入検知システム）

**セキュアリモートアクセス
（SRA）**

資産へリモートアクセスする場合の管理と操作記録を行うサービス

サイバーセキュリティーアプリケーション プラットフォーム（CAP）

Life Is On Schneider Electric

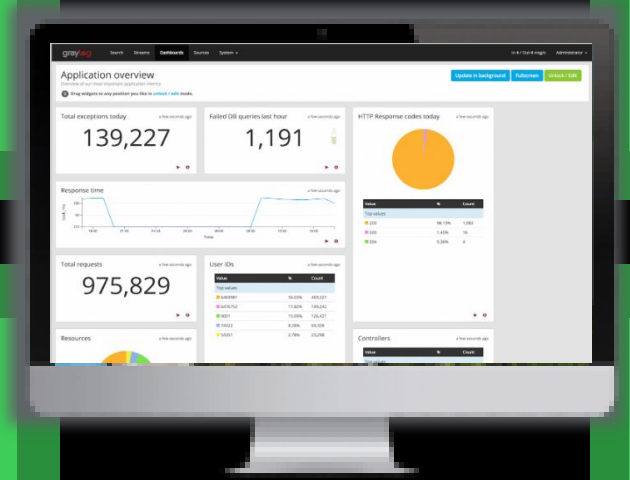
現状把握
監視
保全

サイバーセキュリティーアプリケーションプラットフォーム（CAP）

必要なデータを一元管理するアドバイザープラットフォーム

OT資産と
ネットワーク通信の
可視化

CVEに基づく
脆弱性アセスメント



脅威・異常の
検知・検出

リアルタイムな
リスクモニタリング

CVEとは、Common Vulnerabilities and Exposures の略称で、日本語では**「共通脆弱性識別子」**と表します。
一般公開されている**情報セキュリティの脆弱性をデータベース化**したもので、それぞれ固有の名前やID番号が付けられています。

Life Is On Schneider Electric

攻撃検知の仕組み

Layer 4
コーポレートITネットワーク

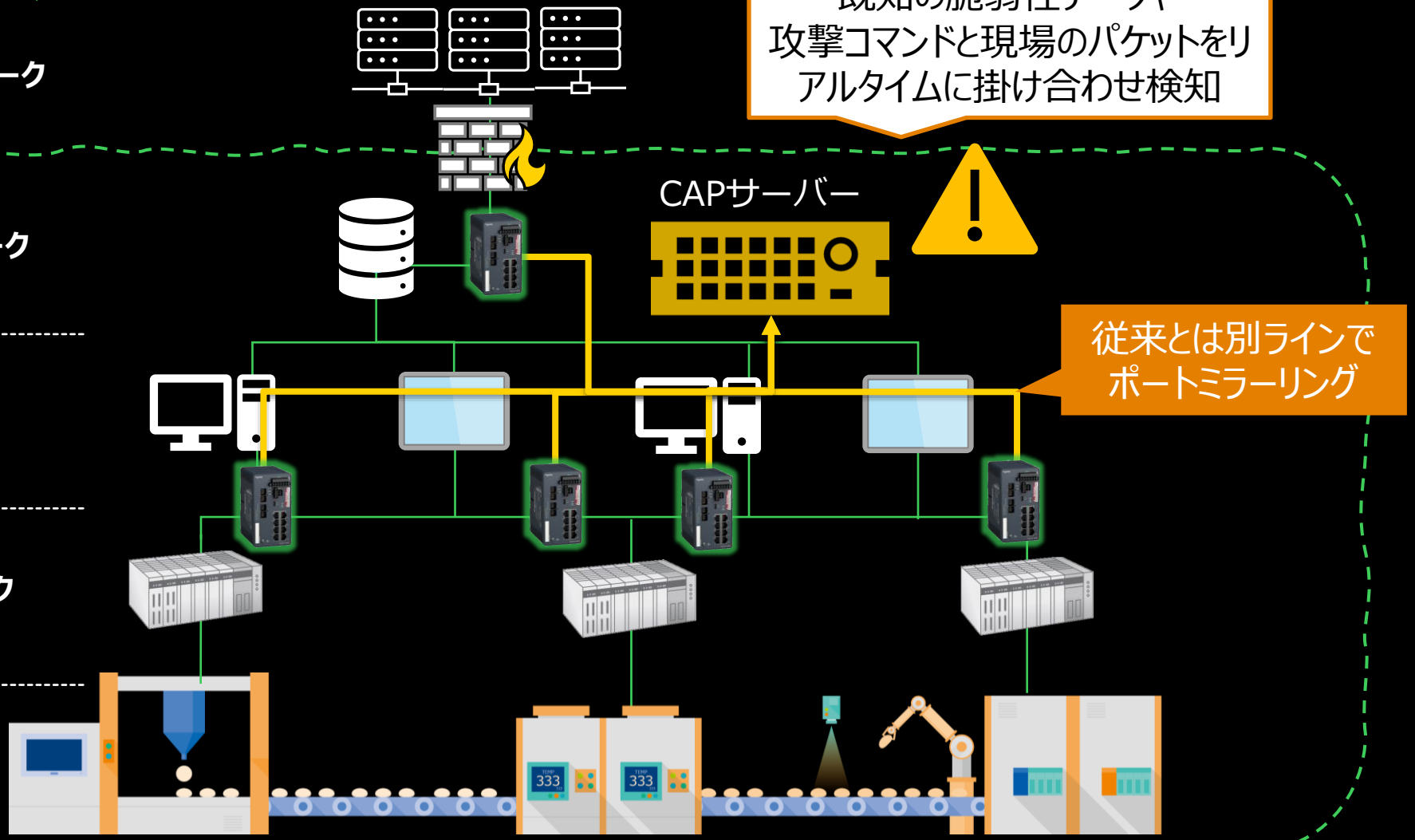
Layer 3
オペレーションネットワーク

Layer 2
プロセスネットワーク

Layer 1
コントロールネットワーク

Layer 0
現場機器

工場内



Life Is On Schneider Electric

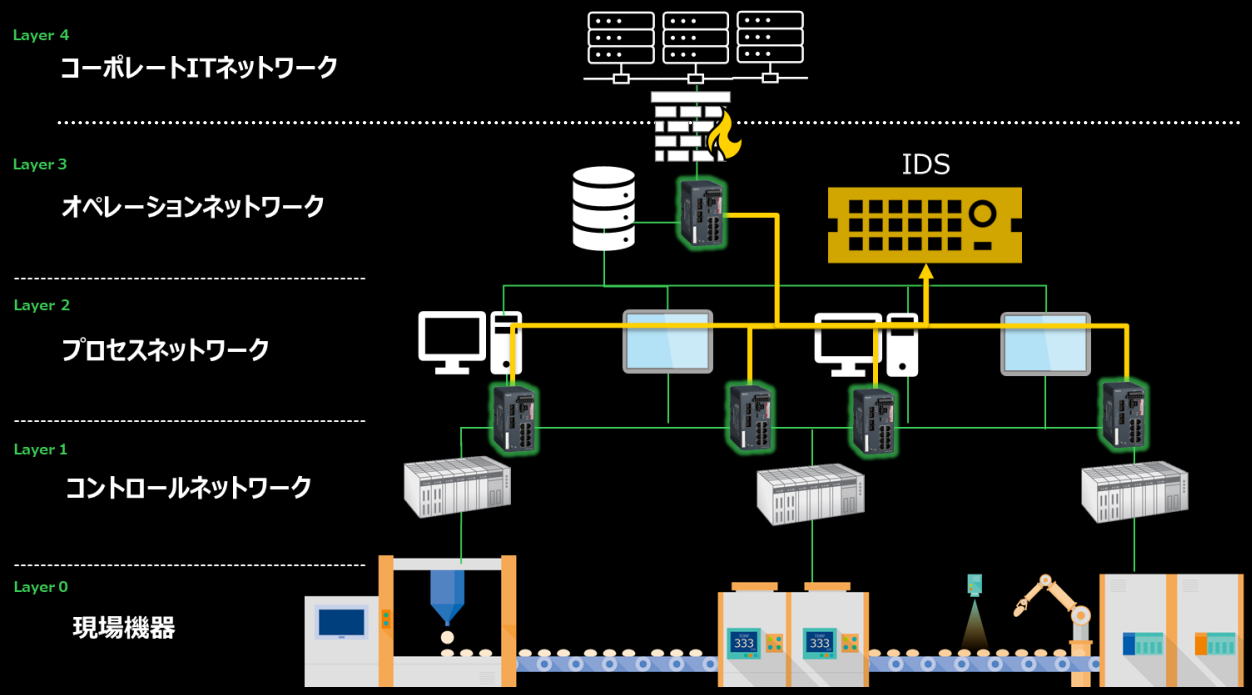
Schneider Electric のCAPがOTに特化している理由

一般的なIDS

- マネージドスイッチやファイアウォールなど経由したリアルタイムなパケットデータを、直接IDSに取り込み、既知の攻撃コマンドやマルウェアのパケット情報と掛け合わせた分析を行い、攻撃を検知します。

  例えば…
  スキャンコード、偵察コマンド、特権コマンド、既知の攻撃コマンドなど

- PLCについては、メーカー名、IPアドレス、MACアドレス程度の情報



Schneider Electric のCAPがOTに特化している理由

CAPは一般的なIDS機能に加え、PLCの見える化にも注力！

通信情報からデータを受けるだけでなく、PLCなどのPJファイルを解析して情報を得ています。(ファームウェアVer、型式、シリアルNo.、プロトコルなど)

詳細なPJファイル分析で出来ることは…

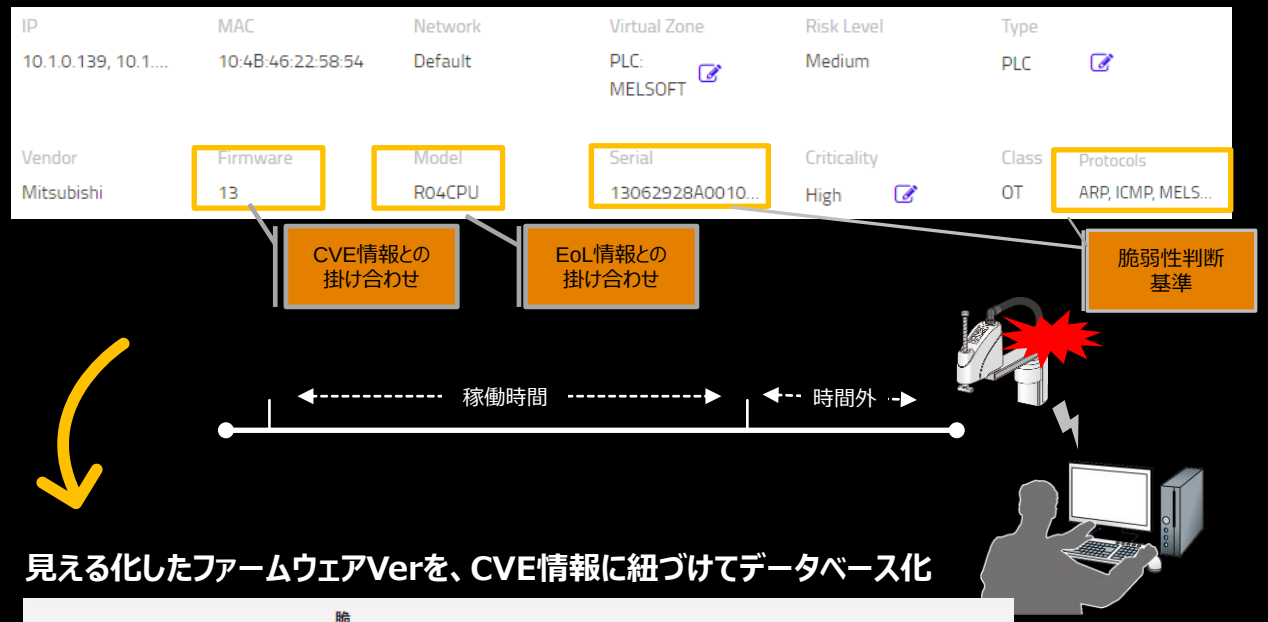
- **承認した時間外でのPLCへのアクセスを検知**
- **PLCラダーのオンライン変更を検知**
  →例：何らかの攻撃を仕掛けた可能性を把握

- **遠隔からのPLCへのRUN/STOPなどのモード変更を検知**
  →例：コマンドの稼働時間外利用を把握

- **PLCの生産中止情報を見える化**
  →例：生産中止の製品は入手不可で、復旧のための準備ができる

- **PLCのファームウェアVerを把握**
  → 例：Verに該当する公開済み脆弱性情報によりパッチ対策ができる

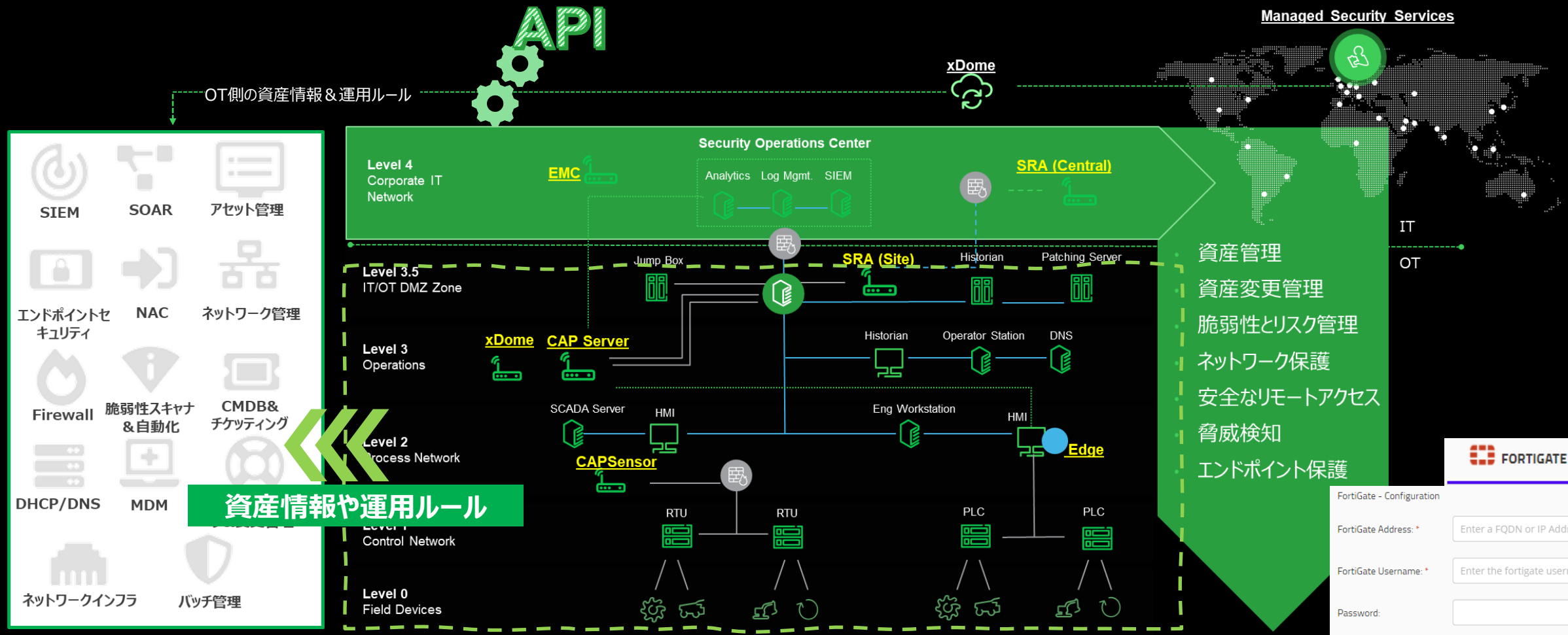
CAPは一般的なIDSの機能に加え、
事前に脆弱性を判断し、対策を打つことが可能！



見える化したファームウェアVerを、CVE情報に紐づけてデータベース化

脆弱性名	脆弱性	CVE	説明
ICSA-23-061-01	OT	CVE-2023-0457	CVE-2023-0457 - MELSEC iQ-F シリーズには、パスワードの平文保存による情報漏えいの脆弱性 (CWE-2561)が存在します。認証されていない攻…
ICSA-20-324-05	OT	CVE-2020-5668	CVE-2020-5668 - モジュールが悪意のある攻撃者から特別に細工された SLMP パケットを受信すると、モジュールは DoS 状態に入る可能性があり…
ICSA-20-303-01	OT	CVE-2020-5652	CVE-2020-5652 - CPU モジュールが悪意のある攻撃者から特別に細工されたパケットを受信すると、イーサネット通信が DoS 状態になる可能性があ…

Schneider Electric のCAPがIT系の方にも好まれる理由



現在ご使用しているITセキュリティコンポーネントへOTの資産情報をリンクできます。
これにより、ITとOTで管理の分断されていたツールや人員やプロセスを統一できるようになります。

現状把握 ▶ 監視 ▶ 保全

マネージドセキュリティーサービス（MSS）

シュナイダーが自社工場用に構築したCCSH (OT-SoC)の機能を
アセスメントから監視・対応まで一気通貫で顧客向けに提供

**サイバーセキュリティー
アセスメントサービス（CAS）**

設備の現状把握/評価を行うサービス

**サイバーセキュリティーアプリケー
ションプラットフォーム（CAP）**

社内ネットワーク等に対する不正アクセス等を防ぐサービスプラットフォーム
（不正侵入検知システム）

**セキュアリモートアクセス
（SRA）**

資産へリモートアクセスする場合の管理と操作記録を行うサービス

マネージドセキュリティーサービス（MSS）

Life Is On Schneider Electric

OTサイバーセキュリティー業界が抱える３つの大きな課題

IT/OTセキュリティーの経験を有する専門家が限られる

IT/OT両方の技術力を持った人材は市場では少ないが、需要と人件費はかなりの勢いで上がっている。

OTサイバーセキュリティーに割り当てられる予算が限られる

セキュリティー要件は日々増加していますが、設備投資と給与増が優先で、実被害を受けていない企業ではセキュリティー費用が捻出しにくい。

セキュリティー管理の投資収益率低下

セキュリティー系の人員計画を立てても、サイバー攻撃の技術度が上がり続けていて、更なる教育も必要で、投資への収益率が見込めない。

だから…

お客様のIT部門の人員はそのままに、今後増えていくリスクを「人員増」で考えるのではなく、専門家に任せて「費用」と「時間」と「リスク」を抑えましょう。 これがSEの「MSS」です。

Life Is On Schneider Electric

Schneider Electric のグローバルにおけるサイバーセキュリティーチームを活用

社内で培ってきた、これらの技術/人/経験値を使って、
全世界のお客様へ、このMSSと言うサービスを提供しています。

220 拠点

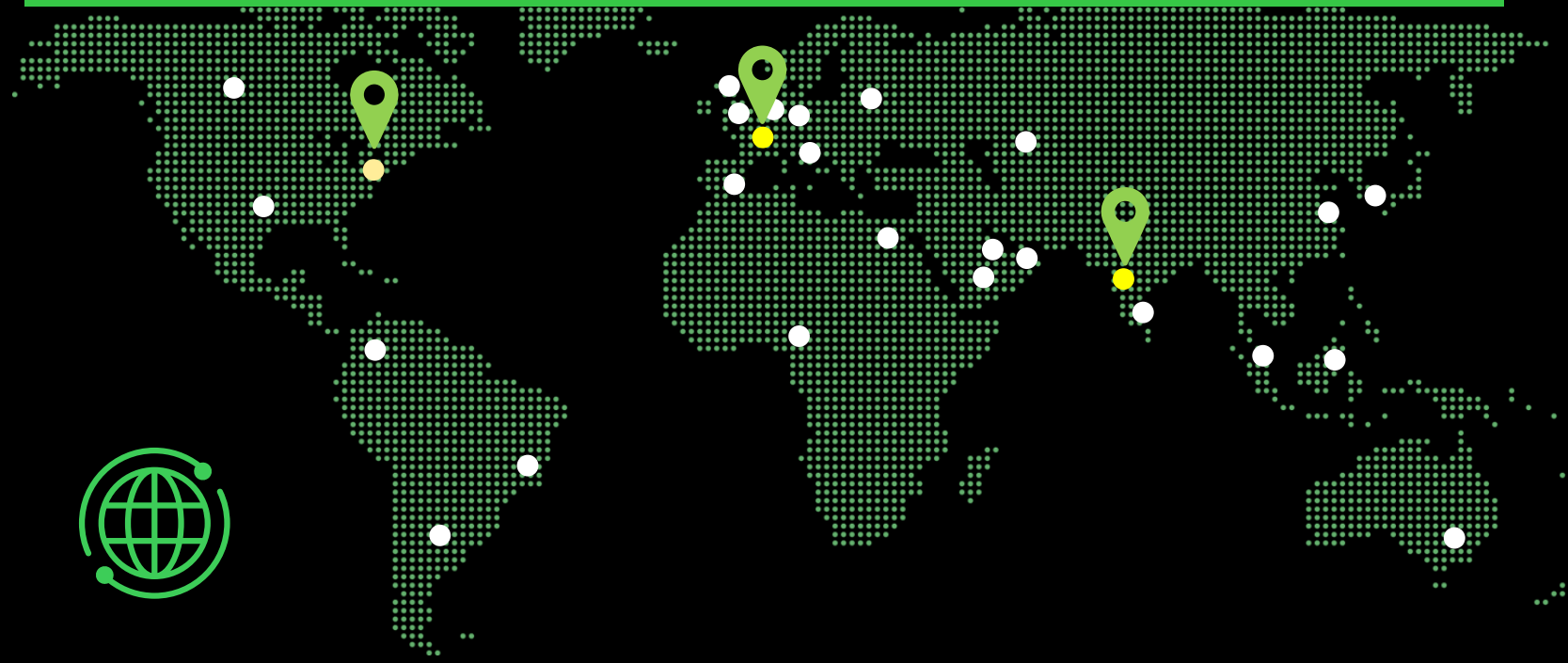
全世界220の
シュナイダー拠点をサポートする
セキュリティーエキスパート

100 名以上

認定資格を持つ
OTサイバーコンサルタント

3,500 名以上

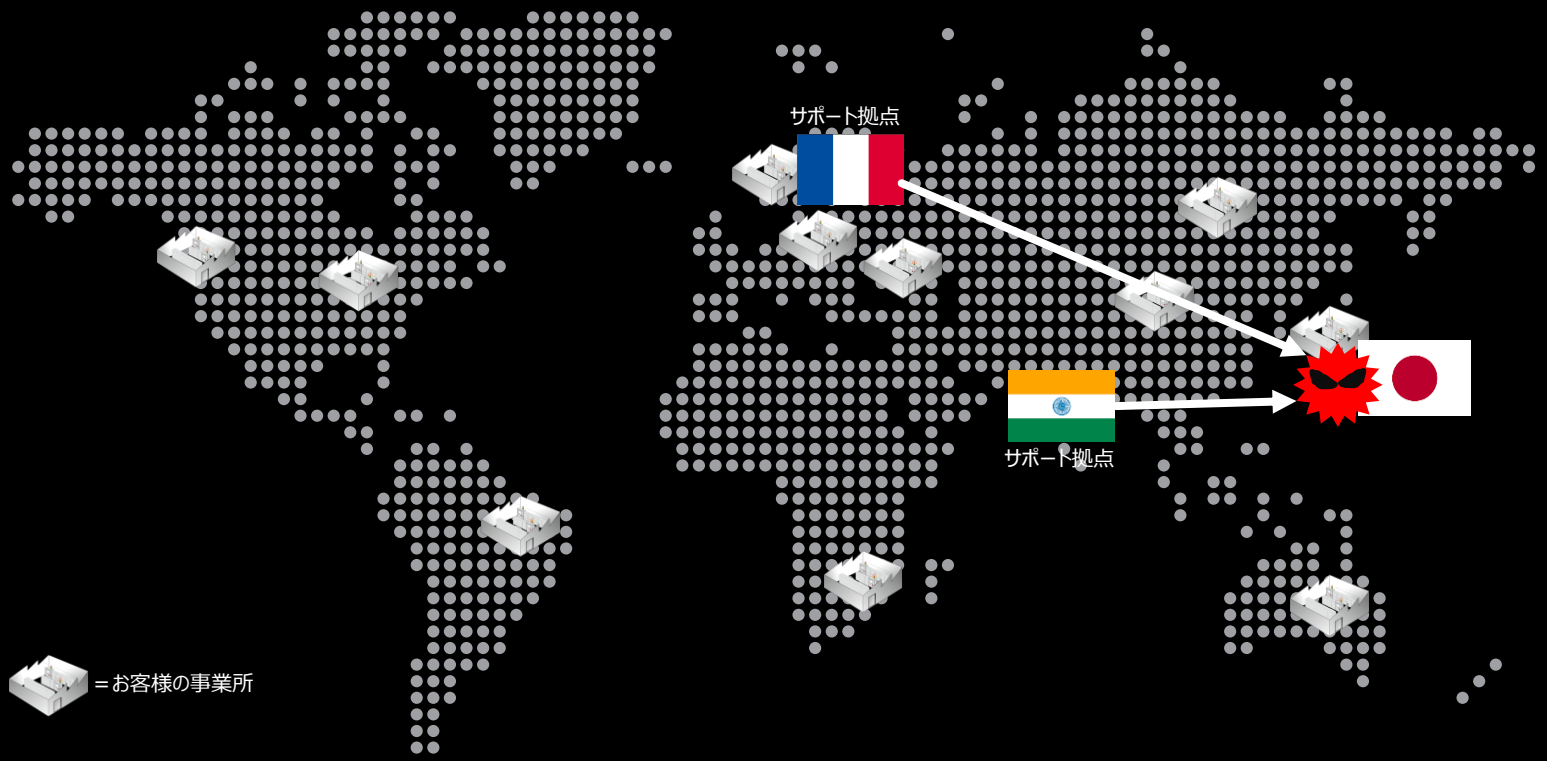
認定サイバートレーニングを受けた
サービスエンジニア



ISA CISSP CISM CISA IEC CompTIA Security+ GPEN 27001 GICSP NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION CEH LPT CHFI

Life Is On Schneider Electric

マネージドセキュリティーサービス（MSS）の全体像



サービス概要

CAP（不正侵入検知システム）の情報を基に・・・

導入時
- **セキュリティーKPIをお客様とSEで協議して決定**
- **お客様へセキュリティー対応のトレーニング（継続可）**

毎月・四半期毎
- **KPIをベースに脆弱状況報告と回避策のアドバイス(報告書)**

インシデント発生時
- **プライオリティ高のインシデントに対して、アドバイスを行う**

  ※作業自体はお客様が担当

- **ランサムウェア等がいつ、どこを経由して感染したのか？NW上で何が起こったのか？を専用ソフトやSRA等を使用して調査＆報告**

MSS：マネージドセキュリティーサービス - 提供までの流れ

Life Is On Schneider Electric

CAPに情報を集めるマネージドスイッチの紹介

Modiconマネージドスイッチ

Life Is On Schneider Electric

Modiconマネージドスイッチ

1 大きく改善したサイバーセキュリティー

- MACアドレスベース-ポートセキュリティー / ポートベース アクセスコントロール
- **DDoS攻撃** 防御
- ローカルロールベースドアクセスコントロール（L-RBAC)
- ACLs

2 ネットワークの信頼性の向上

- さらなる冗長性の確保

3 あらゆる産業現場で適用できる堅牢な設計

- **耐環境モデルのラインアップ**
- **使用周囲温度範囲を拡大したPoE対応モデル**

4 過去のシステムとのインターオペラビリティ

- 過去のConneXium モデルからのリニューアルも簡単

5 デジタル入力による柔軟なアラーム管理

- **デジタル入力がONされるとSNMPメッセージを出力**

6 より簡単に改善された管理プロセス

- **USB Type Cポートを備えた、簡単ブラウザ設定**
- HTML5 ウェブインターフェイス (JAVA ベースインターフェイスでは無い)

7 プラグアンドワーク：各ポートでRSTPがデフォルトで有効

Life Is On Schneider Electric

Modiconマネージドスイッチラインアップ

ノーマル
10/100BASE-T


4TX


8TX


16TX

ノーマル(耐環境モデル)
10/100BASE-T＆-40~+70℃＆絶縁保護コーティング


8TX

ギガビットイーサ対応
10/100BASE-T+10/100/1000BASE-TX


8TX+4GE

10/100BASE-T+SFP GE


8TX+4SFP GE


16TX+4SFP GE


20TX+4SFP GE

FX光ファイバー対応
10/100BASE-T+100BASE-FX


4TX+1MM


4TX+1SM


4TX+2MM


4TX+2SM


8TX+1MM


8TX+1SM


8TX+2MM


8TX+2SM

PoE対応
10/100/1000BASE-TX（PoE)


8GE(PoE)

10/100/1000BASE-TX（PoE)＆-40~+70℃


8GE(PoE)

FX光ファイバー対応(耐環境モデル)
10/100BASE-T+100BASE-FX＆-40~+70℃＆絶縁保護コーティング


8TX+2MM


8TX+2SM

TX：ファーストイーサネット*10/100 Base*
*MM:*光ファイバーマルチモード
*SM:*光ファイバーシングルモード
SFP：光ファイバートランシーバー
GE：ギガビットイーサネット*10/100/1000 Base-TX*
PoE:Power on Ethernet

20種のラインアップ

Life Is On Schneider Electric

Life Is On | Schneider Electric

se.com