Edgecrossユーザ向けセキュリティガイドライン対応
セキュリティ製品/サービス

2022年3月版

Edgecrossコンソーシアム　テクニカル部会　セキュリティガイドライン策定WG

本書の目的

- Edgecrossコンソーシアムでは、Edgecrossを用いたシステムのユーザの皆様が安全・安心を確保できるように下記のガイドラインを発行しています。

  Edgecrossユーザ向けセキュリティガイドライン
  [URL] https://www.edgecross.org/ja/data-download/pdf/ECD-TE4-0006-01-JA.pdf

- 一方で、一般的に、セキュリティガイドラインに沿ってセキュリティ対策を導入する際、ガイドライン記載のセキュリティ対策に該当する製品/サービスを探すことは労力を要します。

- そこで、本書では、ユーザの皆様がこのような労力を減らすことができるように、Edgecrossユーザ向けセキュリティガイドライン記載の各種セキュリティ対策に該当する製品/サービスをリストアップしました。
  本セキュリティガイドラインに沿ってセキュリティ対策を導入する際に是非お役立てください。
  各製品についての質問は、資料内に記載の問い合わせ先へお問い合わせください。

- Edgecrossエコシステムソリューションに登録されている製品には右に示しましたロゴが表示されています。
  ロゴが付いている製品は、提供会員によるEdgecrossを使ったシステムでの動作確認が完了しています。

EDGECROSS
Ecosystem Solution

ガイドライン該当章	セキュリティ製品/サービス名	提供会社
3.3 セキュリティソフトウェア	McAfee Embedded Control / McAfee Integrity Control	マカフィー株式会社
	StellarProtect/StellarEnforce	トレンドマイクロ株式会社
	軽量暗号 開発キット	日本電気株式会社
	SecureWare/Credential Lifecycle Manager	日本電気株式会社
	IoT Device Security Manager	日本電気株式会社
	日立カメラ生体認証SDK for Windows フロントカメラ	株式会社日立製作所
	Blackberry Protect	株式会社日立ソリューションズ
	秘文　Device Control	株式会社日立ソリューションズ
	IoTセキュアライブラリ	株式会社日立ソリューションズ
	ファームウェアの脆弱性診断　Vdoo Vision	株式会社日立ソリューションズ

ガイドライン該当章	セキュリティ製品/サービス名	提供会社
3.5 ネットワーク	資産管理/IDS：eyeInspect	日本電気株式会社
	資産管理/IDS：Nozomi Guardian	日本電気株式会社
	資産管理・ネットワーク可視化：AX-Network-Manager (AX-NM)	日本電気株式会社
	ネットワーク不正接続検知：InfoCage不正接続防止	日本電気株式会社
	EdgeIPSシリーズ/EdgeFire/OT Defense Console	トレンドマイクロ株式会社
	Trend Micro Portable Security 3	トレンドマイクロ株式会社
	日立指静脈認証装置 C-1	株式会社日立製作所
	資産管理：JP1/ITDM2＋エージェントレス資産管理ソリューション	株式会社日立製作所
	不正通信監視：Hitachi Anomaly Detector	株式会社日立製作所
	サイバー防衛訓練サービス「オンラインNxSeTA」	株式会社日立製作所
	制御システム現状把握ソリューション	株式会社日立製作所
	産業用制御システム向けFW/UTM　FortiGate Rugged	株式会社日立ソリューションズ
	SCADAfence Platform	株式会社日立ソリューションズ
	OTネットワークセキュリティ可視化サービス	富士通株式会社
	Microsoft Defender for IoT	日本マイクロソフト株式会社

3.3 セキュリティソフトウェア
セキュリティ製品/サービス

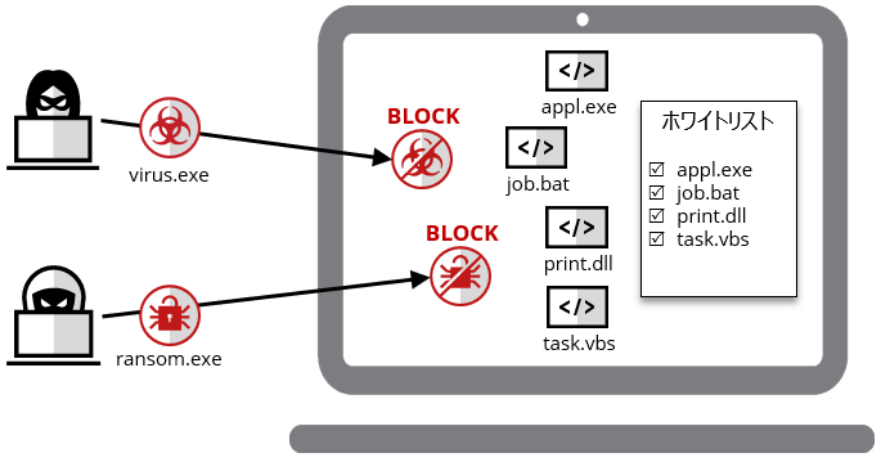
EDGECROSS CONSORTIUM

工場用オートメーションシステム向けセキュリティソフトウェア

McAfee Embedded Control / McAfee Integrity Control

- アプリケーションホワイトリスティングによる堅牢な保護
- 工場のセキュリティに必要な基本要件を網羅
  FA、産業用制御システムで多数の実績あり
- スキャン不要、定義ファイルの更新不要
  インターネット接続不要
- システムの停止や データ流出の原因となりうる
  マルウェアなどの未承認の実行ファイルをブロック
- ソフトウェアや設定に対する 未承認の変更を阻止、
  システムの完全性を確保
- 組み込みシステム向けに国内で125万ライセンス以上の導入実績

❖ ホワイトリスト型セキュリティ
- ホワイトリストに登録されたプログラム，スクリプトのみ実行できます
- 侵入してきたマルウエアは，ホワイトリストに登録されていないのでブロックされます



可用性・性能重視のシステム	組込み機器・レガシーOSのシステム	分散・独立したシステム
システム高負荷による処理遅延や停止を回避	ウイルス対策ソフトが非対応な環境にも対応	スタンドアロンでも強固なセキュリティを実装
定期的なスキャンが不要	**レガシーOSの延命 パッチ適用のコントロール**	**定義ファイルを使用することなく堅牢なセキュリティを実現**

McAfee

URL：https://www.mcafee.com/enterprise/ja-jp/products/embedded-control.html
問い合わせ先：McAfee Enterpise IoTソリューション営業部 奈良宛 junnosuke_nara@mcafee.com
TEL: 070-1369-0962

産業向けエンドポイントセキュリティ

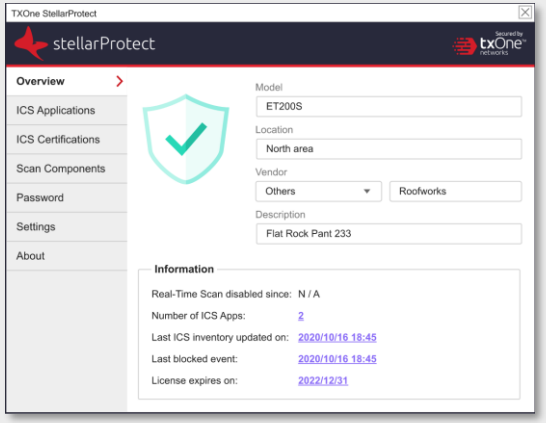
[トレンドマイクロ]

StellarProtect

OT環境向けの包括的なエンドポイントプロテクション

- 産業用次世代アンチウイルス
- オペレーション振る舞い検知
- ICSアプリケーションセーフガード
- USBデバイス制御

対象端末例：
- 産業用アプリケーション搭載端末
- OT環境に設置されているが、IT環境と連携したり、インターネット接続が発生する端末 (オンライン端末)
- 設定変更など頻繁に発生する端末



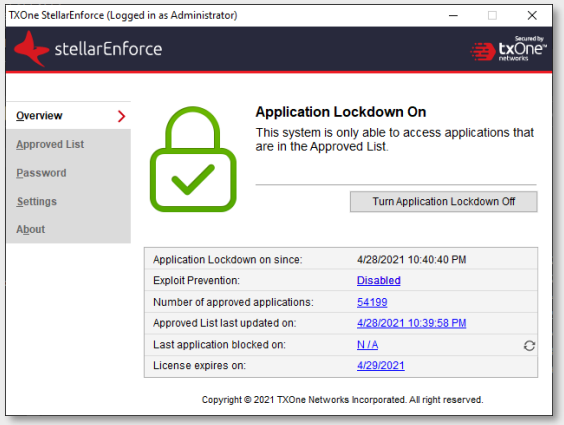
StellarEnforce

Trend Micro Safe Lockの後継製品

ロックダウンと変更管理によりOT環境のレガシーデバイスを守る

- パッチ適用が難しい端末の対策に最適
- Windows XP/2000サポート
- パターンファイル不要※1
- リソース負荷を最小限に抑制

対象端末例：
- レガシーOS端末
- インターネット接続が発生しない端末 (オフライン端末)
- リソース負荷を掛けたくない端末



※1 マルウェア対策を行うためのパターンファイルは不要です。ただし、一部機能を利用する際にパターンファイルが必要になります。

法人お問合せ窓口　https://www.trendmicro.com/ja_jp/contact/contact-us.html
TEL: 03-5334-3601

軽量・認証暗号化製品:軽量暗号 開発キット [NEC]

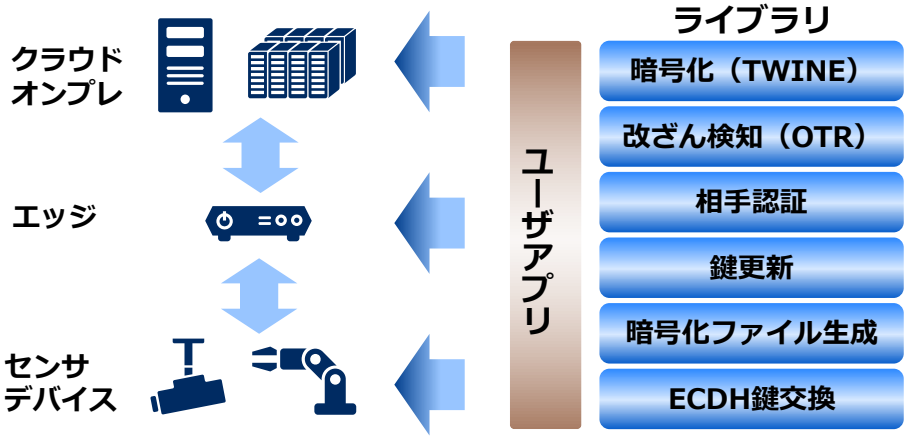
NEC独自開発の軽量暗号TWINE/認証暗号OTRにより
センサデバイスからクラウドまでEnd to Endのデータセキュリティを実現

Edgecrossにおけるファイルの暗号化に利用できます

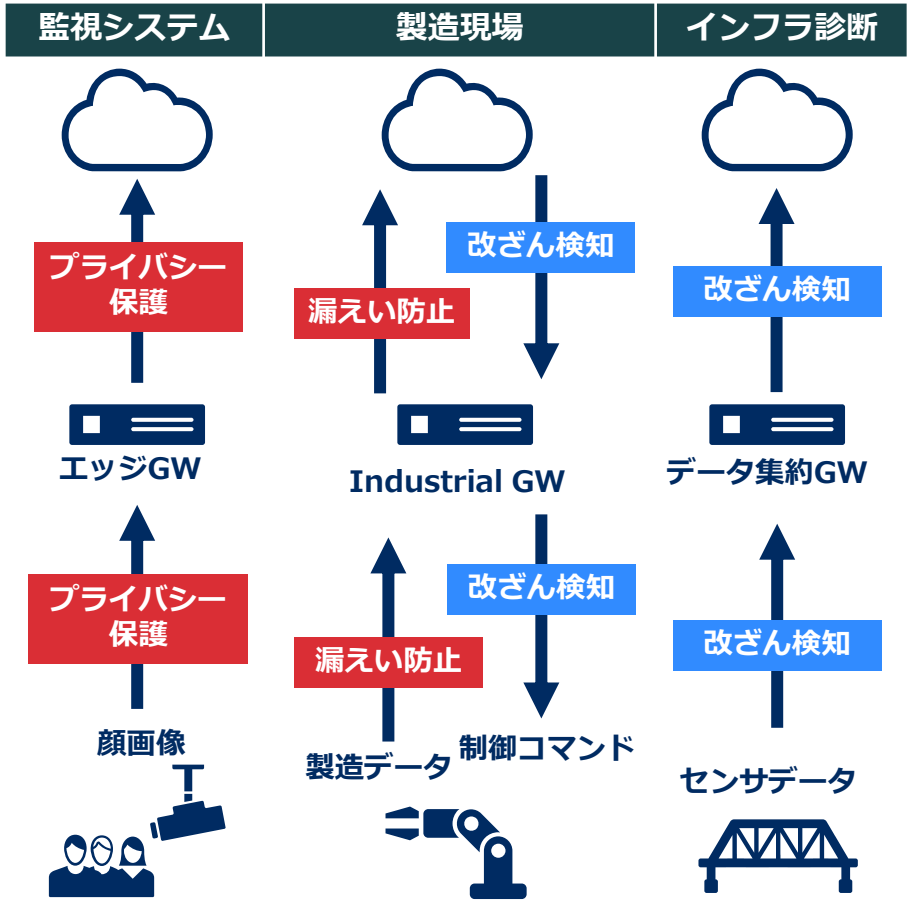
導入によるメリット

- **省リソース環境からデータ保護**
  センサデバイス用途の省リソースマイコンにも搭載可能な軽量ライブラリ
- **改ざん検知機能**
  OTRの改ざん検知機能により、暗号化だけでなくデータの正当性も保証
- **ファイル暗号化**
  コマンドとして実行可　※アプリケーションに組込み不要

商品情報



活用イメージ



NEC独自の暗号技術により、小容量メモリ(ROM:6KB, RAM:0.4KB)※でも高速に暗号化・復号処理が可能
秘匿化と同時に改ざん検知も軽量・高速に実現

※ECDH鍵交換は除く

URL・お問合せ先：https://jpn.nec.com/iot/platform/security/lcdk/index.html

デバイスID/鍵管理製品：SecureWare/Credential Lifecycle Manager [NEC]

エッジ/デバイスの認証情報(ID, 暗号鍵, 電子証明書)をリモートから専門スキル不要でセキュアかつ簡単に発行・自動配付/更新でき、デバイスに設定された暗号鍵や電子証明書の有効/無効状態を集中管理可能

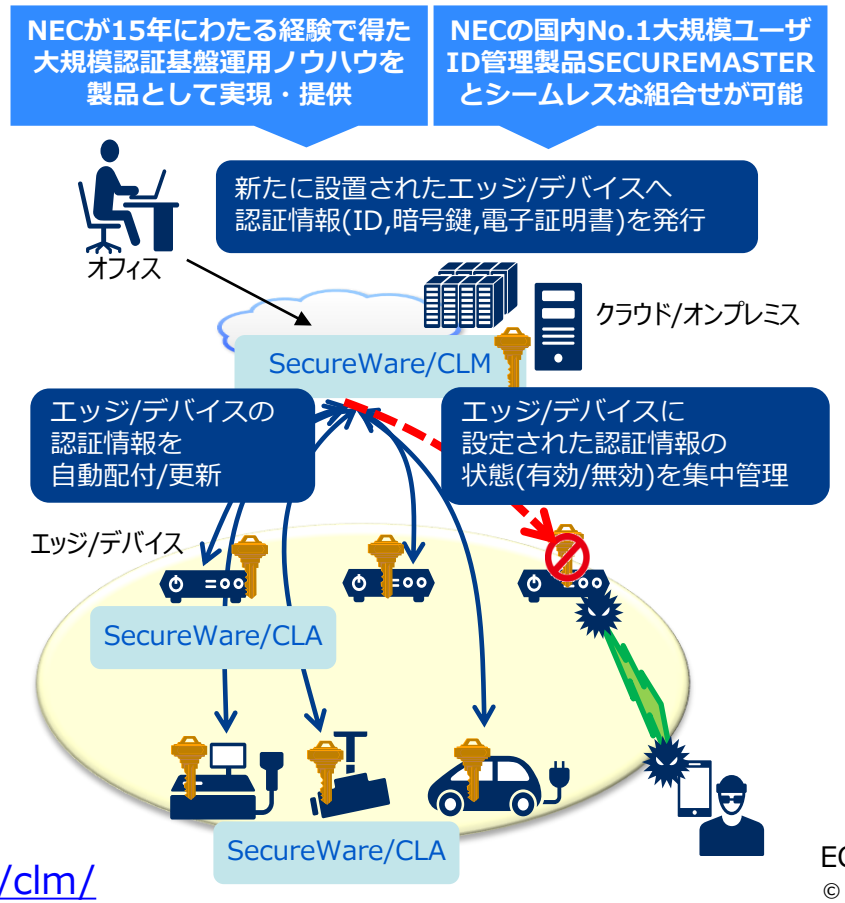
導入によるメリット

- **リモートからデバイスの認証情報を設定**
  エッジ/デバイスの認証情報(ID, 暗号鍵, 電子証明書)をリモートからセキュアに設定可能
- **セキュアかつ簡単な発行手順、自動配付/更新**
  簡単な手順で、セキュリティ強度の高い認証情報のリモート発行・自動配付/更新
- **デバイスの認証情報の状態を集中管理**
  デバイスに設定された認証情報の状態(有効/無効)をリモートから集中管理可能

商品情報

- クラウド/オンプレミス上で動作する**サーバ(CLM)**、及びエッジ/デバイス上で動作する**ツール(CLA)**からなる**ソフトウェア製品**

活用イメージ



URL・お問合せ先：https://jpn.nec.com/secureware/clm/

デバイス接続/通信アクセス制御・異常検知：IoT Device Security Manager [NEC]

不正なアクセス/接続の脅威からエッジ/デバイスを守る、
許可リスト型のアクセス制御・異常検知セキュリティ対策
リモートから脅威検知、許可リスト設定自動化で、簡単・セキュアな運用が可能

許可リスト

- IP通信だけではなく非IPのUSB, Bluetooth Low Energy デバイスも一括でアクセス制御
- アプリ名(※1)やホスト名(※2)により、容易なIP通信アクセス設定が可能

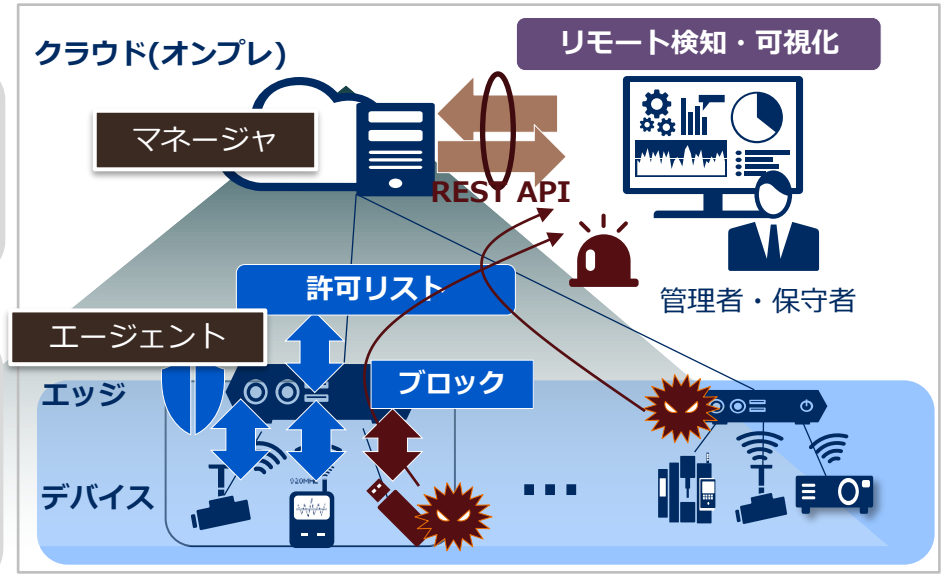
リモート検知・可視化

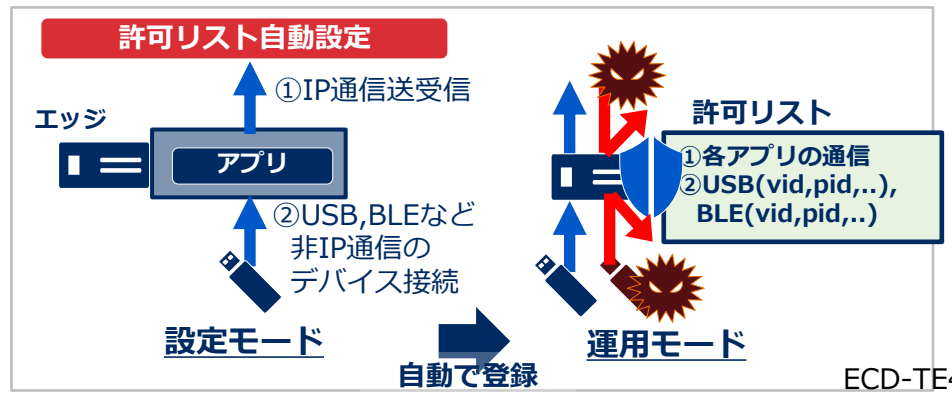
- 未知の通信/デバイスのアクセスや、リモートからの脅威検知により、大規模なIoTシステムでも監視の目が行き届く
- 異常が発生してもリモートから迅速に対処が可能なため、被害の拡大を防止

自動設定

- 専門的スキルが無くても適切な許可リストの設定が可能
- IP通信だけではなく、USB, Bluetooth Low Energy デバイスもまとめて自動で設定

(※1)エッジ上で実行されるアプリ名を指定（TCP/IP通信が対象）
(※2)FQDN(Fully Qualified Domain Name)名を指定





URL・お問合せ先：https://jpn.nec.com/iot/platform/security/whitelist/index.html

不正アクセス防止

ユーザ認証：日立カメラ生体認証SDK for Windows フロントカメラ [日立]

ITセキュリティ対応
日立カメラ生体認証 SDK for Windows フロントカメラ
C-N190C-1111

HITACHI
Inspire the Next

VeinID そして、安心のスタンダードへ 日立指静脈認証

製品に関する詳細・お問い合わせは下記へ

■製品情報サイト
https://www.hitachi.co.jp/veinid/

■インターネットでのお問い合わせ
https://www.hitachi.co.jp/veinid-inq/

かざした指が認証鍵になる　汎用カメラ向け指静脈認証SDK*1

PC内蔵カメラ・外付けカメラ*2を用いた指静脈認証ソフトウェア開発ライブラリ

*1 SDK: Software Development Kit　*2 2021年春サポート予定

静脈認証の特長

・身体の中にある静脈のパターンをデータとして利用するので、本人を識別するためのデータの偽装が難しく、第三者のなりすましが困難です。

・ICカードなどのように、盗難や紛失などの心配がなく、パスワードのように忘れたりすることがありません。

日立の指静脈認証技術

■ 公開型生体認証基盤(PBI)*3
■ 20年間の研究開発・販売実績
■ 国内シェアNo.1*4

*3 PBI: Public Biometric Infrastructure (https://www.hitachi.co.jp/securityauthentication-pbi/)
*4 富士経済「2020 セキュリティ関連市場の将来展望」調べ（金額ベース）

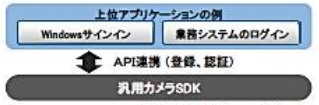
日立カメラ生体認証SDK for Windows フロントカメラ(汎用カメラSDK)の特長

PCの内蔵カメラ、または外付けカメラを用いた指静脈認証で、Windowsサインインや、業務システムへのログインを可能にします。

専用装置不要　完全非接触型　確実な本人意思確認　PC内蔵カメラ、または外付けカメラによる1:1認証が可能です。

機能

本SDKは上位アプリケーションに下記のAPI*5を提供します。
・登録（テンプレートの生成）
・認証（指定されたテンプレートとの照合結果通知）



*5 API: Application Programming Interface

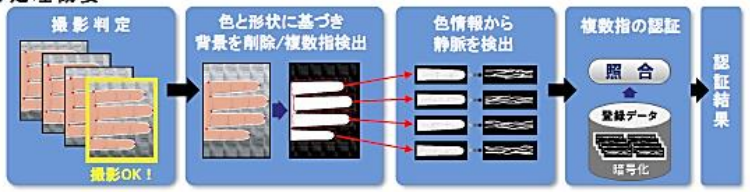
技術概要

かざした指の位置を正確に検出し、可視光の画像から静脈パターンだけを安定して抽出します。また、複数の指を用いることで認証の精度を高めます。

■開発技術

可視光の画像から静脈パターンだけを安定して抽出すること	色情報を用いた静脈パターンの抽出技術
かざした複数指の位置を正確に検出して高精度に認証すること	撮影画像からの指検出と複数指照合による認証の高精度化技術

■処理概要



指静脈認証の流れ

①指をかざす　②カメラが指の写真を撮影　③各指を検出　④指静脈パターン抽出　⑤複数の指を用いた認証処理　⑥ユーザー認証

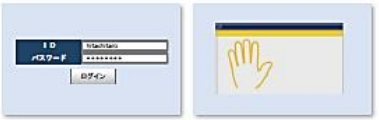
利用事例

■従業員のWindowsサインイン認証／ロック解除などに利用
・指静脈認証により、パスワード入力なくWindowsサインインが可能となります。
・ロック画面の解除も、パスワード入力の代わりに指静脈認証で行うことができます。

Windowsサインインのイメージ*6

(POINT)
パスワード入力する必要がなくなり、指をかざせばWindowsサインインができ、利便性が向上します。

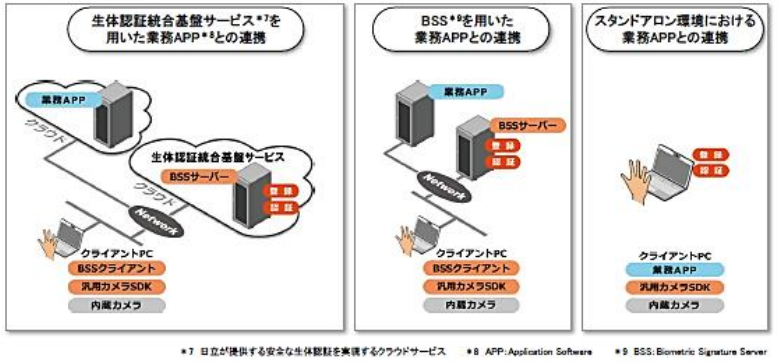
■多要素認証が必要とされる業務システムへのログイン認証に利用
銀行の取引システム、経理の取引システムなど高いセキュリティが要求される業務システムにて指静脈認証による多要素認証を実現します。
・ステップ1：パスワードによる1段目認証
・ステップ2：指静脈による2段目認証



(POINT)
・従業員：本人の生体情報を使用して多要素認証を行うため、PC紛失やパスワード盗難の場合でも、他人によるシステムログインのリスクが限りなく小さくなります。
・社内システム管理者：新規デバイスを導入することなく、多要素認証システムを構築することができます。

*6 日本マイクロソフト株式会社の許諾を得て使用しています。

システム構成例

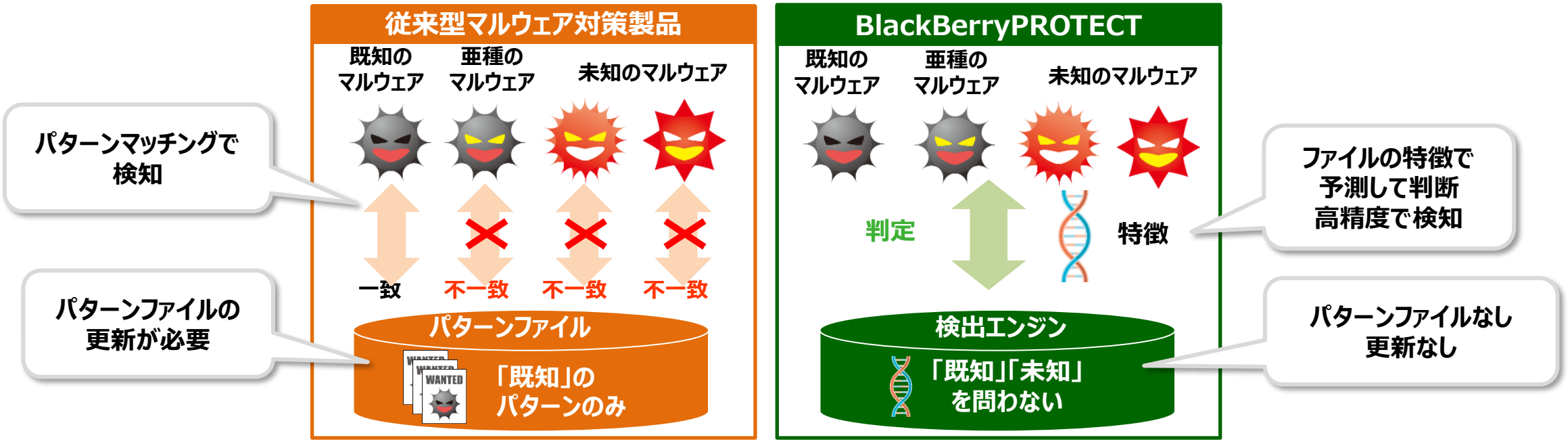


*7 日立が提供する安全な生体認証を実現するクラウドサービス　*8 APP: Application Software　*9 BSS: Biometric Signature Server

マルウェア対策

BlackBerryPROTECT

機械学習による先進的な検知エンジンを用いて既知・未知の区別なくマルウェアを検知可能な次世代マルウェア対策製品です。



マルウェア検知率

99%※以上

※ 2018 NSS Labs “ADVANCED ENDPOINT PROTECTION Cylance Security Value Map™(SVM)”

DNAレベルのマルウェア解析

パターンファイルの更新は不要

機械学習による先進的な検出エンジンで高精度にマルウェアを検知

問合せ先：https://www.hitachi.co.jp/security-inq

デバイス制御

秘文 Device Control

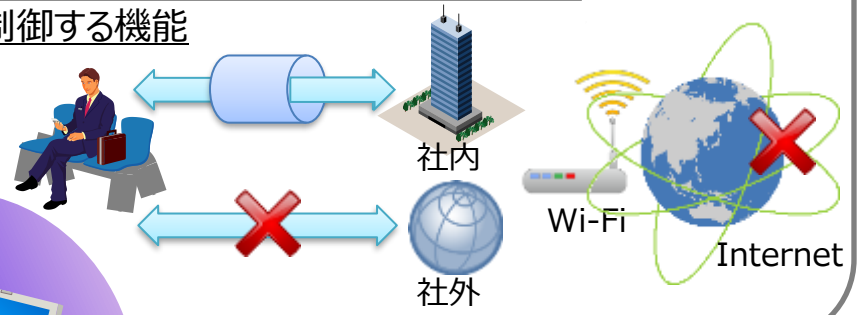
情報漏洩の経路となるスマートフォン、USBメモリー、SDカードなど、デバイスへの不正コピーを防止します。またスマートフォンのテザリング機能による未許可アクセスポイントへの接続を制御し、ネットワーク経由の情報漏洩を防止します。

① デバイス制御

外部デバイスへデータを持ち出しさせないための機能

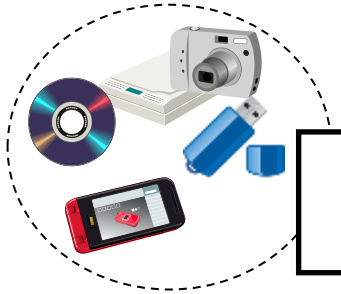
② ネットワーク制御

情報漏えいリスクのあるネットワーク利用を制御する機能

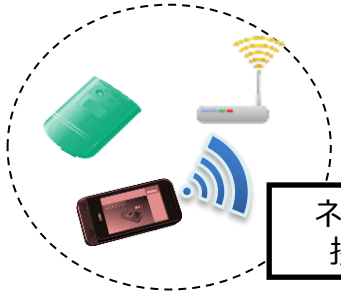


③ ログ取得・管理

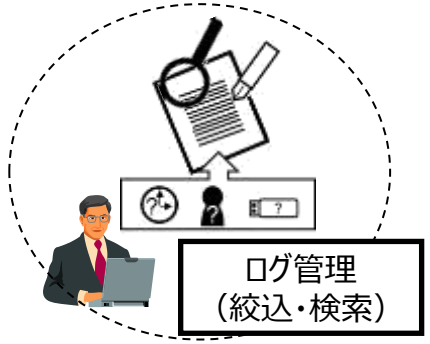
情報漏えい対策施策の確認、監査のための機能



デバイス接続
および
ファイル持ち出しログ



ネットワーク
接続ログ



ログ管理
（絞込・検索）

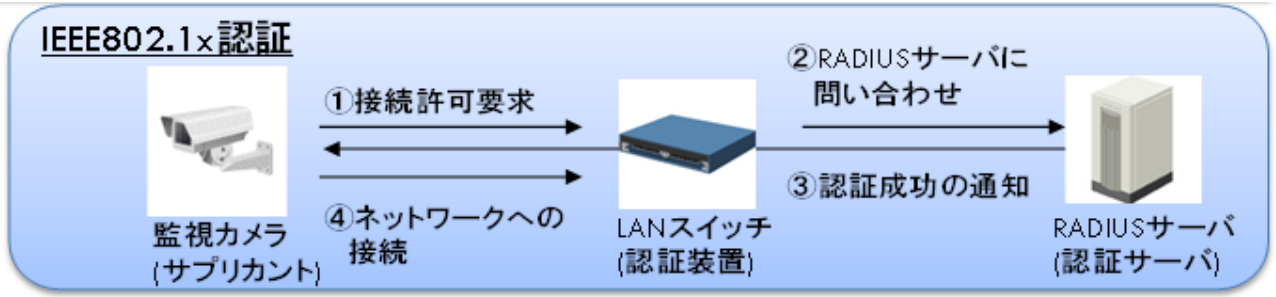
問合せ先：https://www.hitachi.co.jp/security-inq

認証強化・データ暗号化

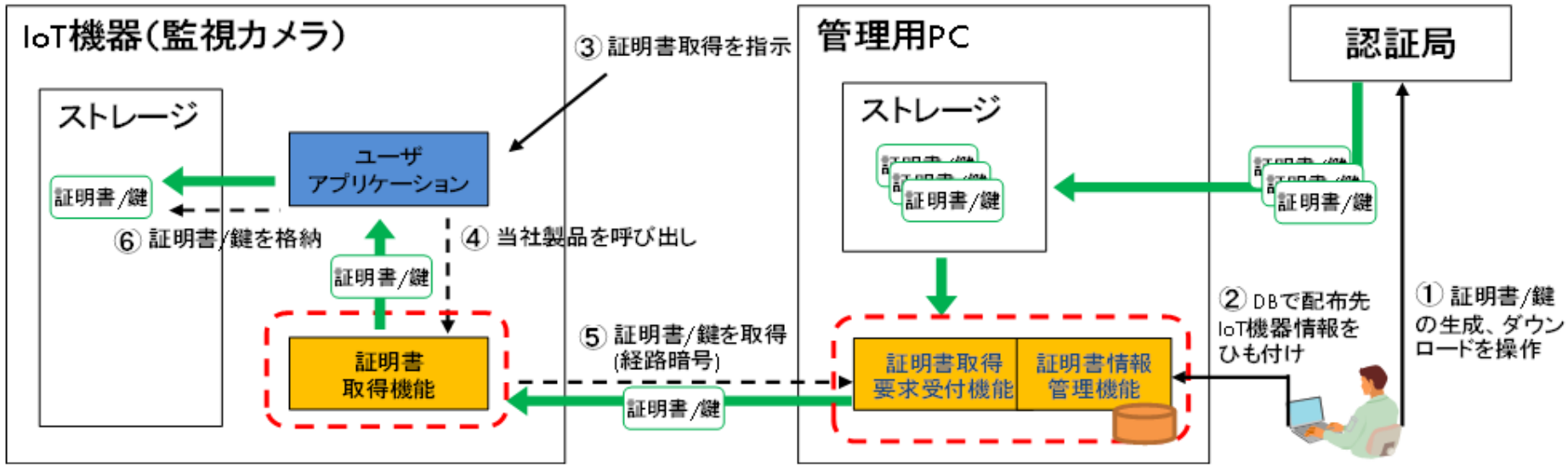
IoTセキュアライブラリ

IoTセキュリティライブラリは、不正なIoTデバイスの接続防止や、監視カメラなどがインターネット経由でデータ送信する際のデータ暗号化と改ざん検知を実現します。

監視カメラシステムへの適用例



当社製品によるクライアント証明書管理



- ✓ IoT機器(監視カメラ)にクライアント証明書を入れ、ネットワーク接続時に認証(IEEE802.1x)
- ✓ 取り扱うデータ（ドローンのデータやカメラ映像データ）の漏えい・改ざんを防止

問合せ先：https://www.hitachi.co.jp/security-inq

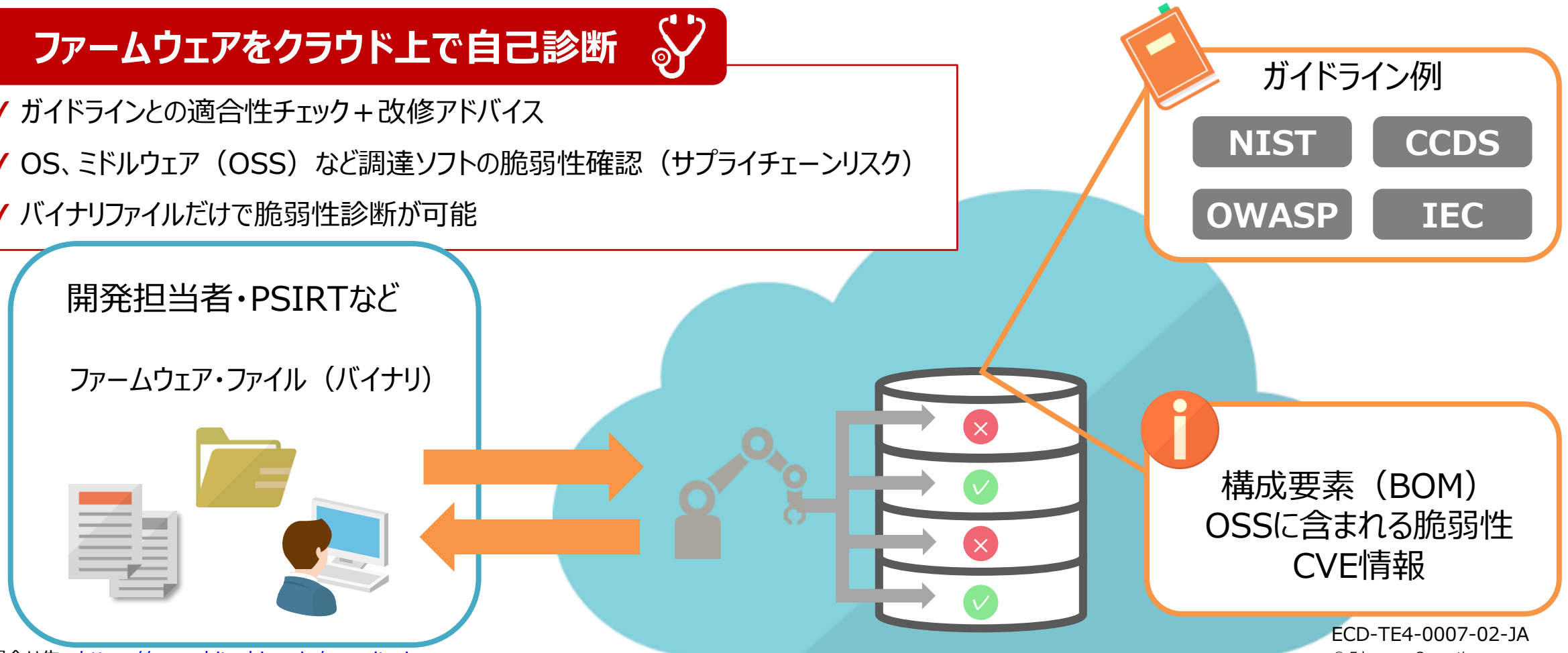
ファームウェアの脆弱性診断

Vdoo Vision

IoT機器ファームウェア(バイナリファイル)の静的な脆弱性診断を実施します。OS/OSS/アプリケーションに残存する既知の脆弱性や脆弱性となる設定、これらの改修方法をご確認いただけます。また、IEC62443/NIST SP800-171など規格・ガイドラインの要件に対して、適合状況を確認することができ、セキュアな開発を効率よく実施できます。

ファームウェアをクラウド上で自己診断

- ✓ ガイドラインとの適合性チェック＋改修アドバイス
- ✓ OS、ミドルウェア（OSS）など調達ソフトの脆弱性確認（サプライチェーンリスク）
- ✓ バイナリファイルだけで脆弱性診断が可能



問合せ先：https://www.hitachi.co.jp/security-inq

3.5 ネットワーク
セキュリティ製品/サービス

ネットワーク可視化・脅威検知（IDS）

資産管理/IDS：eyeInspect

製品概要

制御システムのネットワーク可視化・セキュリティ検知を実現するソフトウェア製品。パッシブ構成で動作するため、既存の制御システムに影響を与えずに導入可能。

導入効果と機能

● ネットワーク可視化
デバイスの種類と数、役割、サブネット、通信方向などを自動で視覚的に表示可能。最新のネットワーク構成図を自動で生成可能。

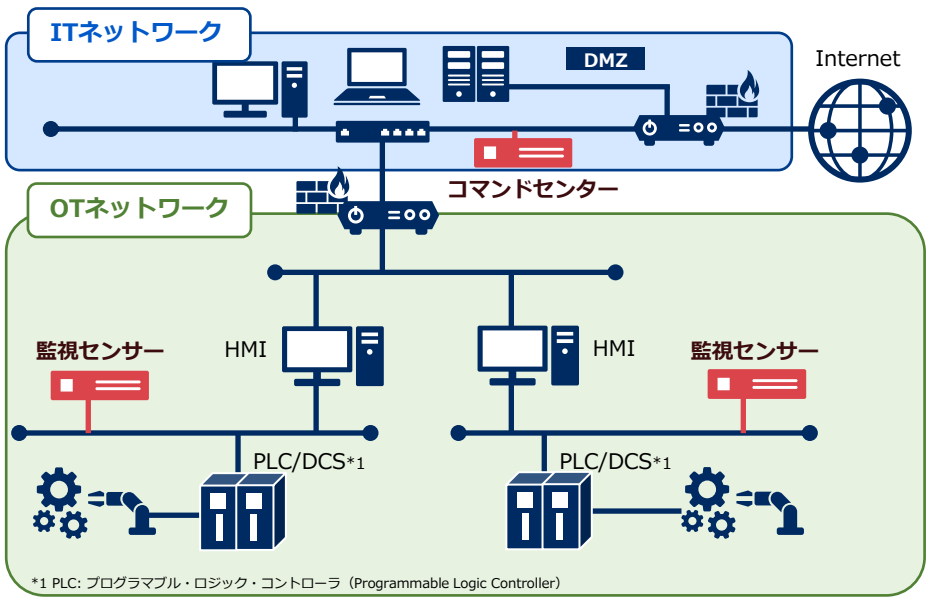
● アセット管理
モデル名、脆弱性情報、プロトコルなど詳細なアセット情報を表示・一覧化することが可能。脆弱性を持ったPLCやアクティブでないホストを見つけることが可能。

● セキュリティ検知
不正な通信・攻撃、内部犯行をブラックリストやホワイトリスト併用しセキュリティ検知。

● 独自プロトコルの検知ロジック開発
お客様自身でプロトコルの検知ロジックを開発可能。お客様の独自プロトコルも検知可能。

構成イメージ

FORESCOUT



画面イメージ

ネットワーク可視化

アセット管理情報

URL・お問合せ先：https://jpn.nec.com/datanet/silentdefense/index.html

ネットワーク可視化・脅威検知（IDS）

資産管理/IDS：Nozomi Guardian

製品概要

Guardianは、OTネットワーク通信環境の可視化とフィールドデバイスのリアルタイム状態監視により、セキュリティレベルを高めるソリューションです。電力・ガス・石油・化学プラント・製造・製薬など幅広い業種で導入が進んでいます。

導入効果と機能

● 導入・運用が容易

日本語GUIを提供しており容易に操作が可能。またアプライアンス1台で運用可能であるため導入のハードルが低い。さらにボタン1つで学習を行えるため運用負荷を低くすることが可能。

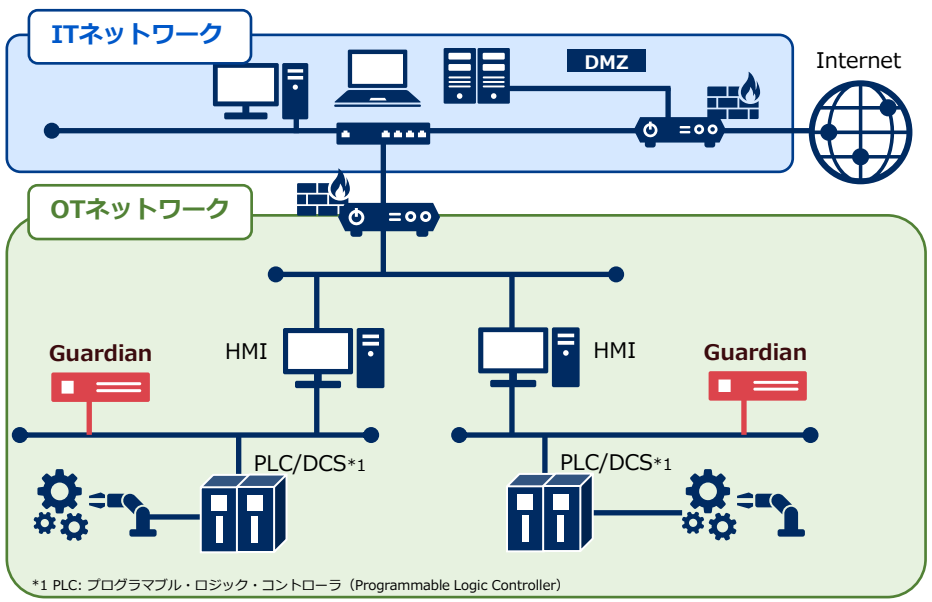
● ネットワーク・アセット可視化機能

工場/プラント内ネットワークの通信をモニタすることによりネットワークマップを自動で作成。情報を視覚的かつ一覧として表示可能。また、OT環境のアセットを洗い出し、ベンダ名、OS、プロトコルなど詳細なアセット情報を一覧化することが可能。

● セキュリティ検知

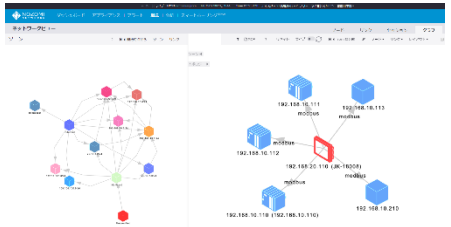
PLCなどのコントローラーで保持しているプロセス値を自動で学習してホワイトリスト化を行い、プロセスの異常な変化を検知することが可能。また、別観点として洗い出しを行ったアセット同士がどのようなプロトコルで通信を行っているかをホワイトリスト化し異常な通信を検知可能。

構成イメージ



画面イメージ

ネットワーク可視化



アセット管理情報

URL・お問合せ先：https://www.ncos.co.jp/products/ipss/nozomi/

資産管理・ネットワーク可視化：AX-Netwrok-Manager (AX-NM)

製品概要

ネットワーク接続状況の自動検出＆マップ表示、端末の位置情報管理機能を備えた運用管理者の負荷を軽減できるソフトウェア製品。
エージェントレスで導入でき、物理/論理構成などをとりまとめた情報を**ワンタッチでドキュメント出力**

導入効果と機能

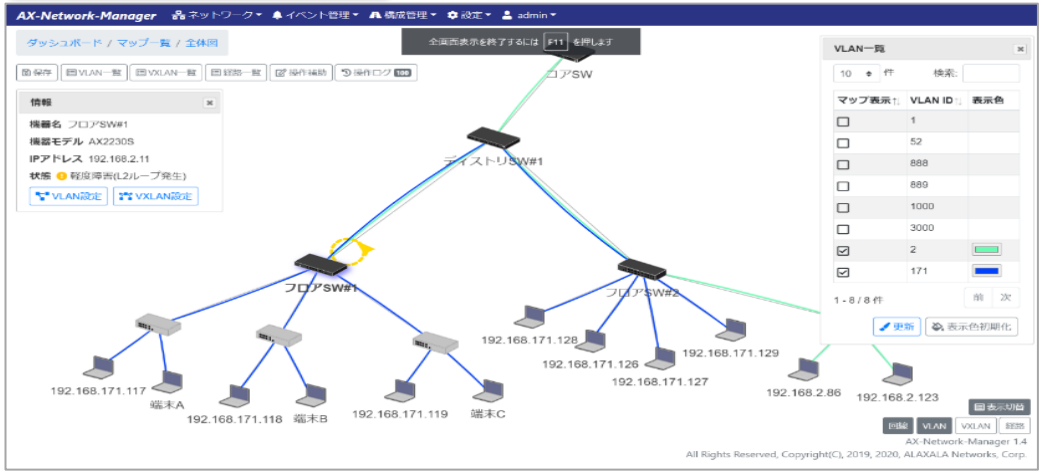
● **ネットワーク構成**
トポロジマップの自動作成で、ネットワーク機器の構成やネットワークに接続されている端末の位置が一目でわかる。

● **端末一覧**
登録された装置から情報を自動収集し、端末/ポートなどを一覧表示。履歴管理も可能で、**資産管理にかかる工数を削減**。

● **ドキュメント出力**
機器設定やネットワーク接続状態を**ワンタッチでドキュメント出力**可能で、完成図書として活用可能。

● **サイバー攻撃自動制御**
AlaxalAスイッチ及びセキュリティ製品と連携することで該当端末を隔離。攻撃の検知から初動までを自動化し、迅速な対応で被害を最小限に抑制。

ネットワーク構成



端末一覧

MACアドレス	ベンダ	接続先機器名	接続先ポート名	VLAN ID
0012.e23e.b365	ALAXALA Networks Corporation	フロアSW#3	GigabitEther 0/7	171
b068.e688.03c5	CHONGQING FUGUI ELECTRONICS CO.,LTD.	コアSW	GigabitEther 0/48	3000
a874.1d8a.8e06	PHOENIX CONTACT Electronics GmbH	ディストリSW#1	GigabitEther 1/0/2	2

ドキュメント出力

お問合せ先：https://jpn.nec.com/security/solution/ot_iot.html

ネットワーク不正接続検知：InfoCage不正接続防止 [NEC]

製品概要

InfoCage不正接続防止は、管理外の持込みPCやスマートフォン、タブレット端末などの接続を排除し、情報漏えいやウイルス感染のリスクを軽減。

導入効果と機能

●端末情報の自動収集
ネットワークに接続されている端末の情報を自動収集し、ネットワークを可視化
- ➢管理外の端末が接続されていないか確認
- ➢サポートの切れた古いOSの把握

●不正端末の遮断
未登録の端末やNG登録された端末の接続を防止し、不正端末による不正アクセスやウイルス感染からネットワークを保護

●簡単導入
- ➢エージェントレス：
  センサーが通信を監視するため、端末へのソフトウェアのインストールが不要
- ➢ネットワーク機器非依存：
  既存のネットワーク機器の入れ替えや設定変更が不要

●スマートデバイス対応
PC だけでなく、スマートフォンやタブレットなどのスマートデバイスも管理が可能

イメージ図

- ネットワーク機器の**空きポートに接続**
- ミラーポート不要

状態	MACアドレス	IPアドレス	機器種別	接続ポート	スイッチアドレス
OK	0A:00:01:0A:00:01	192.168.0.1	Windows XP	Fa/01	192.168.0.254
OK	0B:00:02:0B:00:02	192.168.0.2	Windows 7 SP1	Fa/02	192.168.0.254
OK	0C:00:03:0C:00:03	192.168.0.3	Windows 8	Fa/03	192.168.0.254
NG	0D:00:04:0D:00:04	192.168.1.1	Linux	Fa/01	192.168.1.254
NG	0E:00:05:0E:00:05	192.168.1.2	ネットワーク機器	Fa/02	192.168.1.254
NG	0F:00:06:0F:00:06	192.168.2.1	iOS	Fa/01	192.168.2.254

導入・運用実績

- 官公庁、製造など業種を問わず、豊富な導入実績（約1,300社）
- NECグループにて、10万台規模で現在運用中

不正接続防止領域 2016年度実績：シェアNo.1※

※出典：㈱富士キメラ総研 2017 ネットワークセキュリティビジネス調査総覧 <不正接続防止ツール>

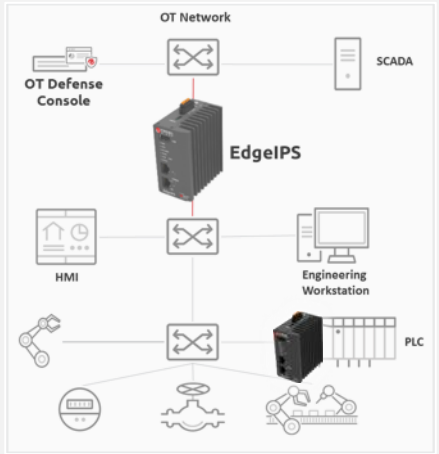
URL・お問合せ先：https://jpn.nec.com/infocage/prevention/index.html

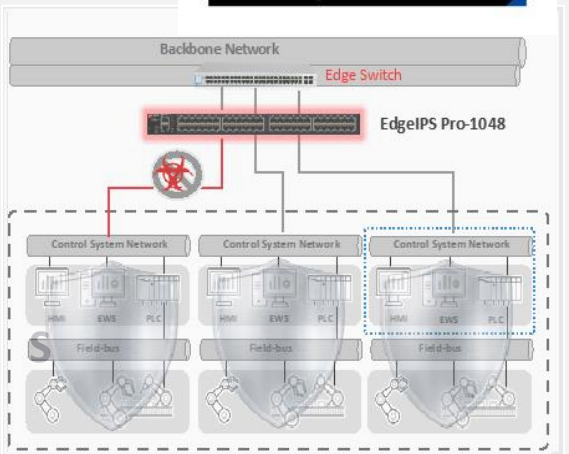
産業向けネットワークセキュリティ

[トレンドマイクロ]

EDGECROSS CONSORTIUM

EDGECROSS Ecosystem Solution





産業向け次世代IPS

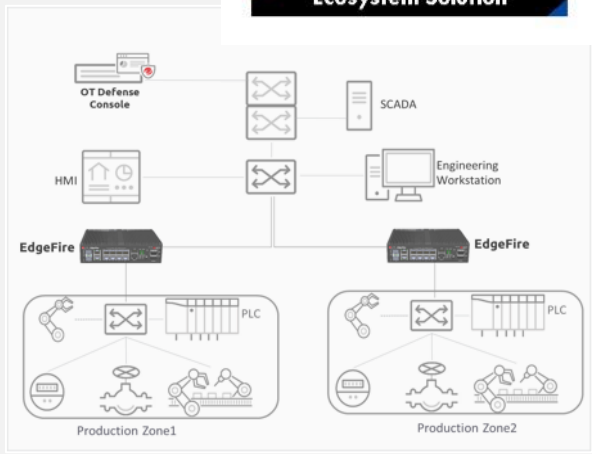
- 重要資産の前段で保護
- 後付けで導入
- 様々な産業機器の脆弱性を保護

- 重要資産をまとめて保護
- 様々な産業機器の脆弱性を保護
- 冗長化構成対応

EdgeIPS | EdgeIPS Pro

EdgeIPS シリーズ

EDGECROSS Ecosystem Solution

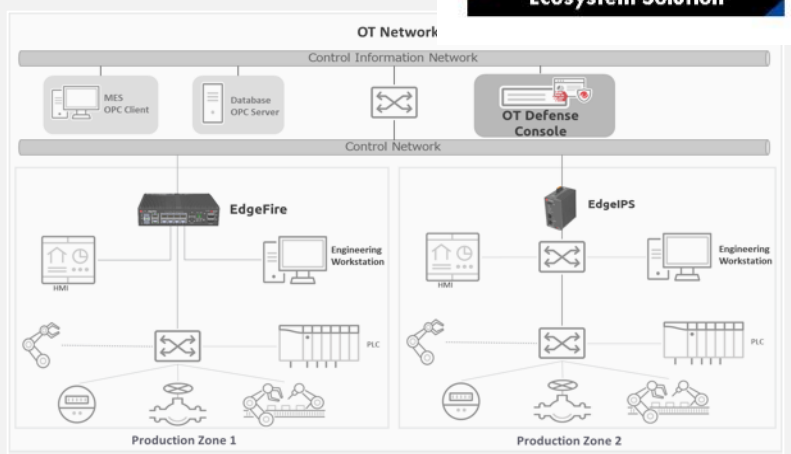


産業向け次世代FW

- ネットワークセグメンテーション
- 生産ライン単位で保護
- アクセス制御、脆弱性対策、NAT

EdgeFire

EDGECROSS Ecosystem Solution



産業向け集中管理コンソール

- EdgeIPSシリーズ、EdgeFireを集中管理
- ポリシーの一元管理
- 資産情報、トラフィック、イベントの可視化
- サードパーティ連携

仮想アプライアンス
(VMware Workstation Pro, ESXi)

OT Defense Console

法人お問合せ窓口 https://www.trendmicro.com/ja_jp/contact/contact-us.html
TEL: 03-5334-3601

Trend Micro Portable Security™ 3

クローズド環境やスタンドアロンPC向けのマルウェア検索・駆除ツール

Trend Micro Portable Security 3(TMPS3)は、WindowsまたはLinuxデバイスのUSBポートに差し込み、ソフトウェアをインストールせずにマルウェア検索・駆除が出来る持ち運び可能なツールです。

マルウェア検索が完了すると、LEDライトで検索結果を示します。デバイスのマルウェア検索中に資産情報も収集し、OTの可視性を向上させます。

TMPS3の集中管理が行える管理プログラムは、リモートまたは物理的に複数のTMPS3に検索設定を展開できます。また、複数のTMPS3から検索ログや資産情報を統合することが可能です。

法人お問合せ窓口
https://www.trendmicro.com/ja_jp/contact/contact-us.html
TEL: 03-5334-3601

不正アクセス防止

ユーザ認証：日立指静脈認証装置 C-1 [日立]

公開型生体認証基盤(PBI)対応
日立指静脈認証装置 C-1
PC-KCC300

HITACHI
Inspire the Next

そして、安心のスタンダードへ
VeinID 日立指静脈認証

製品に関する詳細・お問い合わせは下記へ
■製品情報サイト
https://www.hitachi.co.jp/veinid/
■インターネットでのお問い合わせ
https://www.hitachi.co.jp/veinid-inq/

指の静脈パターンが PKI*1認証の「秘密鍵」になる

PBI*2と複数指認証による高い安全性と認証精度により、大規模なユーザー数に対応可能な生体認証システムを実現します。
この生体認証システムにより、手ぶらでのキャッシュレス決済、入退管理、会員管理などに、利便性の高い生体認証を提供します。

*1 PKI：Public Key Infrastructure、公開鍵暗号基盤　*2 PBI：Public Biometric Infrastructure

静脈認証の特長

・身体の中にある静脈のパターンをデータとして利用するので、本人を識別するためのデータの偽装が難しく、第三者のなりすましが困難です。

・ICカードなどのように、盗難や紛失などの心配がなく、パスワードのように忘れたりすることがありません。

日立の指静脈認証技術

■ 公開型生体認証基盤(PBI)
■ 20年間の研究開発・販売実績
■ 国内シェアNo.1*3

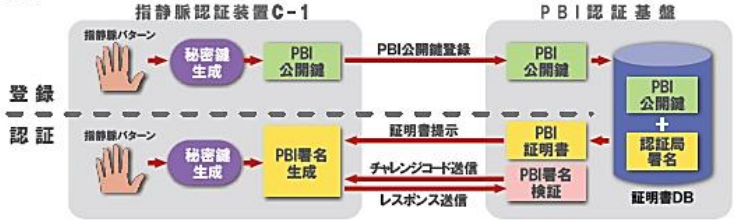
*3 富士経済『2020 セキュリティ関連市場の将来展望』調べ（金額ベース）

日立指静脈認証装置 C-1の特長

●高い安全性と認証精度

・PBIによる高い安全性

従来のPKIによる認証システムでは、ICカードなどに秘密鍵と電子証明書を鍵情報として格納し、厳重に管理する必要がありました。PBIを用いたシステムでは、指静脈パターンから秘密鍵を生成するため、ユーザーは鍵情報の管理が不要になります。また、サーバーに生体情報を保存せず、PBI公開鍵を保存する仕組みのため、生体情報が漏えいすることがありません。



・複数指による高い認証精度

認証精度*4	本人拒否率	他人受入率
	0.01%	0.0000016%

*4 1:1認証での測定値。バイオメトリクスの精度評価に関する国際規格ISO/IEC 19795-1:2006に基づいた測定方法で算出した精度。

●使いやすいデザイン

・指を浮かせた状態で認証可能（非接触）
・状態表示LEDにより、認証成功などの状態を表示可能
・内蔵スピーカーにより、音声でのガイダンスも可能

●バーコード読み取り機能

・スマートフォンの画面や紙媒体などに印刷されたバーコードに対応
・読み取り可能なバーコード
CODE39、CODE93、CODE128、JAN、DataBar、ITF
QRコード、SQRC*5*6

*5 SQRCを使用するには、別途、株式会社デンソーウェーブのソフトウェア購入とクラウドサービスの利用契約が必要です。
*6 オプションにて、2021年夏サポート予定

利用事例

決　済
スーパーマーケット、コンビニ、駐車場、ガソリンスタンドなどでのキャッシュレス決済

入退管理
店舗、スポーツ・コンサートなどのイベント会場、美術館、アミューズメント施設などでの入退管理

会員管理
スポーツジム、ゴルフ場、ホテル、VIPラウンジ、クラブなどでの会員管理

システム構成例

*7 BSS：Biometric Signature Server　*8 ネットワークに接続するには、別売りのUSB-LAN/USB－Wi-Fiアダプターが必要です。（2021年夏サポート予定）

各部詳細

資産管理：JP1/ITDM2＋エージェントレス資産管理ソリューション[日立]

JP1/ITDM2＋エージェントレス資産管理ソリューションは、工場内の産業用PCの管理にかかる労力を低減します。産業用PCの資産管理を徹底し、資産の運用時に必要となるセキュリティを確保するソリューションを提供します。

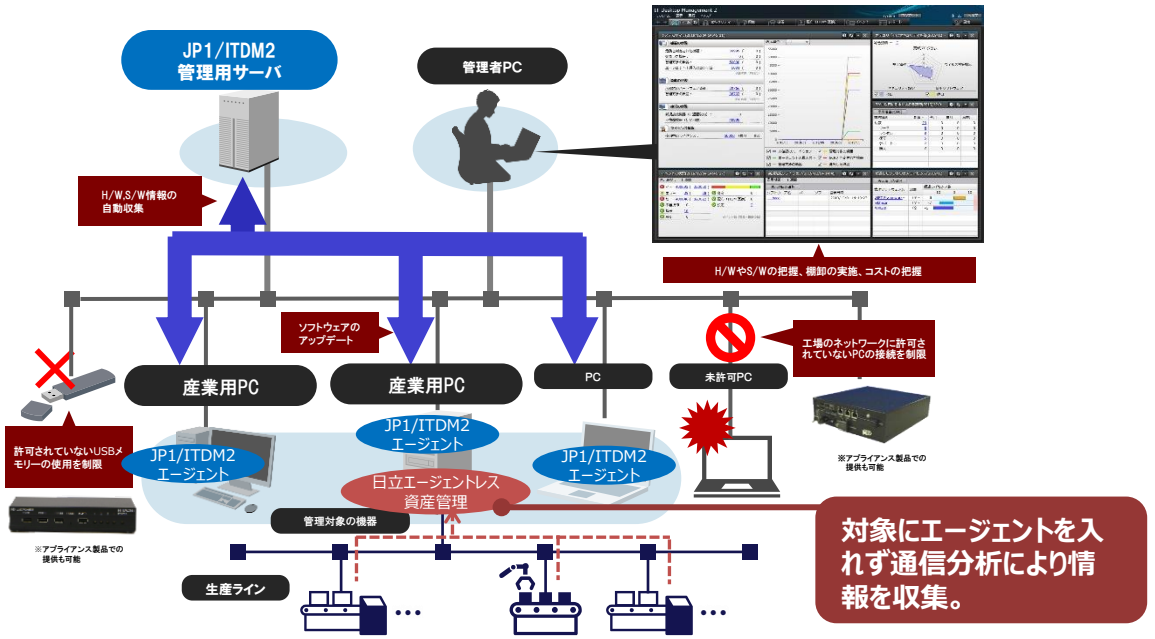
工場内にある産業用PCのセキュリティを確保

- 許可されていないUSBメモリーの使用を制限
- 工場ネットワークへの許可されていないPCの接続を制限
- 導入ソフトウェアのバージョンを把握し、脆弱性がないか確認

工場内にある産業用PCを容易に把握し管理コストを削減

- 産業用PCのハードウェア情報や導入しているソフトウェア情報を一元的に把握
- 産業用PCや導入ソフトウェアの棚卸やコスト把握を容易に実現
- 導入している各種ソフトウェアを最新のバージョンに一括アップデート
- エージェントが導入不可の機器についても通信分析により資産管理情報を収集

管理イメージ



特長

見やすい画面	様々な環境で活用	10年サポート
HTML5を使用したWebブラウザ画面で、グラフィカルにレポートを表示。ひとつの画面で、現状を把握できます。	管理エージェントが導入されたネットワーク接続機器だけでなく、ネットワークに接続されていない機器や管理エージェントが導入されていない機器も資産管理できます。	最大で10年間のサポートサービスを提供。標準サポートの5年間に加えて、限定サポートとして5年間サポートサービスを提供しています。

ユースケース例

産業用PCで使用を許可していないUSBメモリーを使わせたくない

USBメモリーから産業用PCへマルウェア感染するリスクを低減するために、管理者が許可していないUSBメモリーを産業用PCで使用できなくすることができます。

複数の産業用PCの棚卸に手間がかかっている

生産ラインごとに配置されている複数の産業用PCやその他の機器を棚卸する場合に、JP1/ITDM2＋エージェントレス資産管理で管理している機器は自動的に棚卸できるため、管理者の手間と多くの時間を削減することができます。

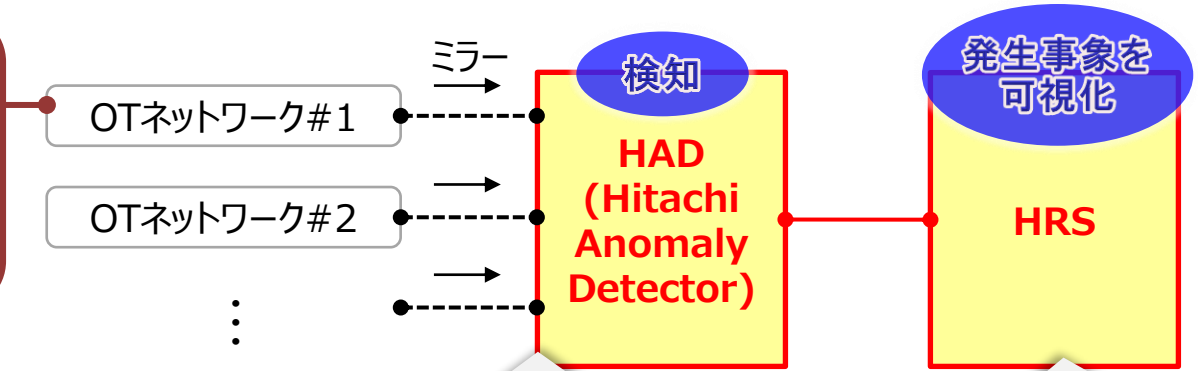
※ JP1/ITDM2 ： JP1/IT Desktop Management 2

問合せ先：https://www.hitachi.co.jp/security-inq

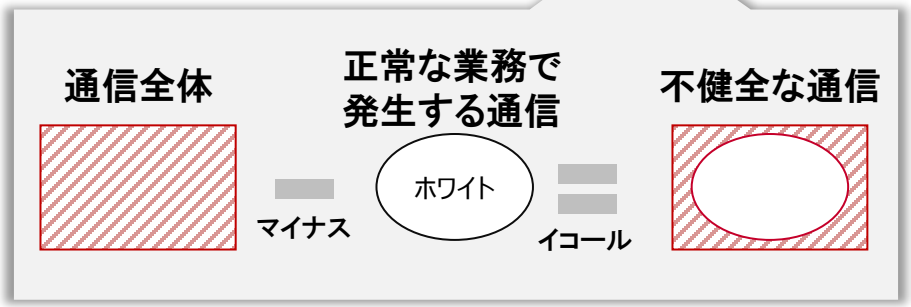
不正通信監視：Hitachi Anomaly Detector ［日立］

工場現場のネットワークパケットを解析し，現場ネットワークに影響を与えることなく、**Hitachi Anomaly Detector (HAD)** および **HRS がセキュリティインシデントを検知、可視化します。**

ネットワークのミラーポートからパケットを収集分析することで、対象に影響与えることなく、不正通信を検知可能



完全カスタマイズ可能な構成図により、どの機器でセキュリティインシデントが発生しているか。どの機器に対して影響を与えているかを直感的に把握可能



Hitachi Anomaly Detector (HAD)

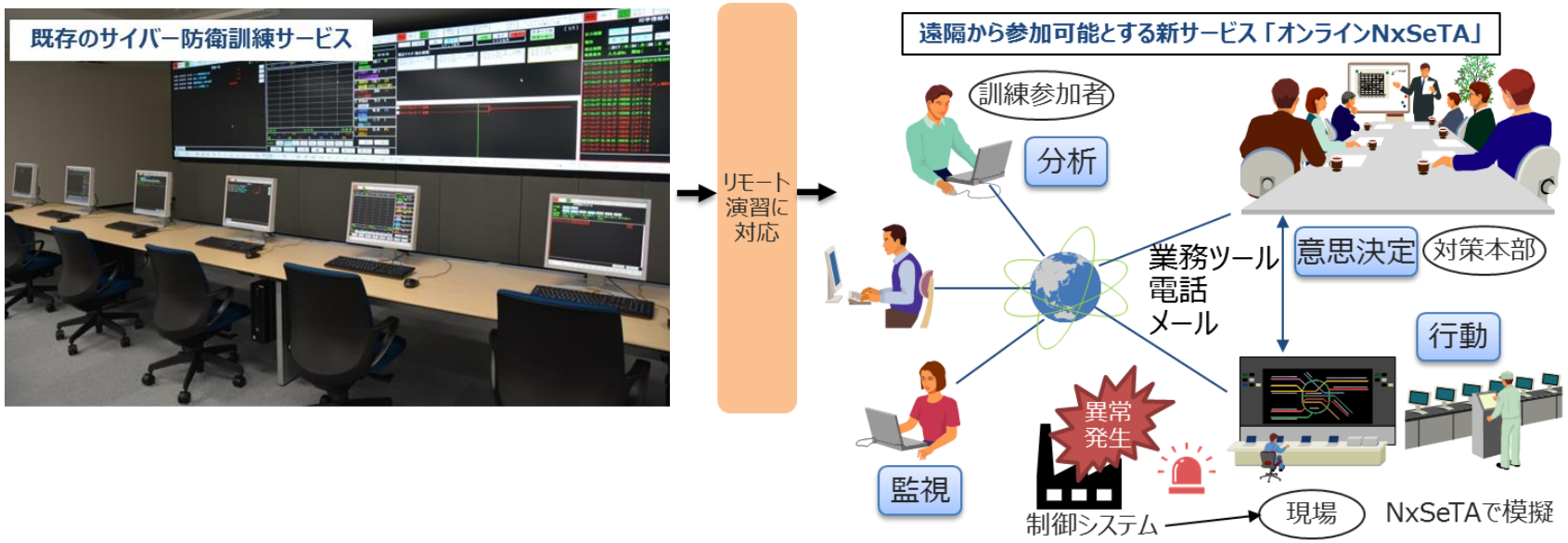
正常な通信を学習し、
正常から外れる通信を検知する不正通信監視製品

HRS (セキュリティ監視ダッシュボード)

発生した事象を分析し，
発生事象を分かりやすく可視化する製品

サイバー防衛訓練サービス「オンラインNxSeTA」

実際の現場に限りなく近い環境での訓練をリモート下でも提供



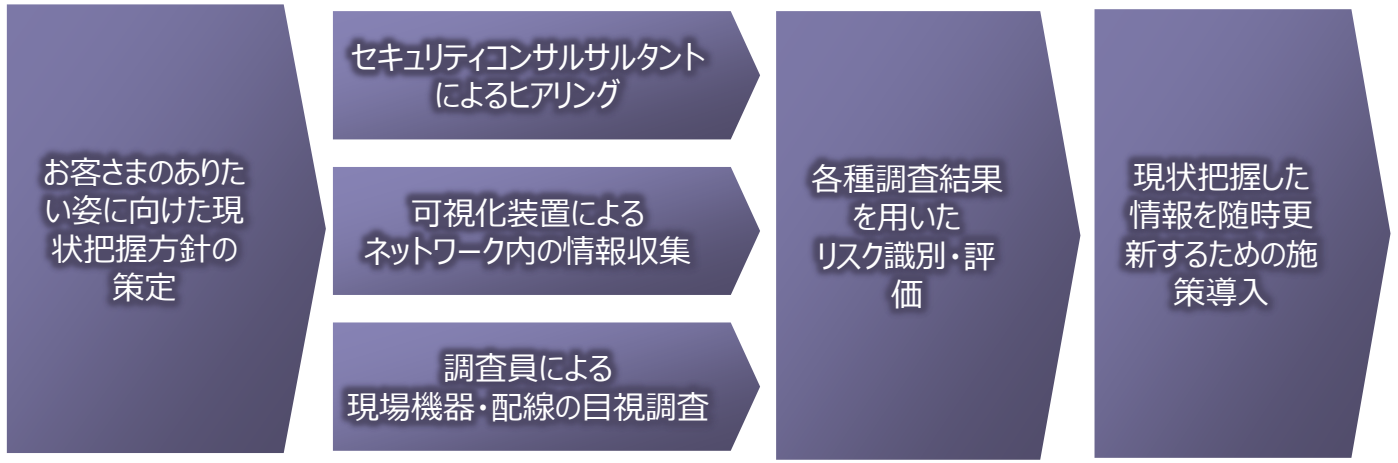
サービス名称	概要	イメージと適用例
オンラインNxSeTA	**遠隔からのオンライン参加方式** 受講者は、自宅または勤務先からNxSeTAにリモートでログインし演習に参加する。 リモートでの実業務で使用するツールを用いたコミュニケーションや連携方法についての支援も可能とする。	・リモート業務に対応した組織訓練 ・業務で用いる業務ツールの活用支援（連携支援） ・リモートワークショップ

問合せ先：https://www.hitachi.co.jp/security-inq

制御システム現状把握ソリューション

現場におけるセキュリティリスクの洗い出しを強化し、より正確な現状把握を行うことで、セキュリティ対策全体の効率化と省力化を実現し、お客さまの価値向上に貢献

ソリューションの全体像



サービス名称	概要	イメージと適用例
制御システム現状把握ソリューション	可視化装置よるネットワーク内の情報収集、調査員による現場調査、セキュリティコンサルタントのヒアリングを実施。 収集した資産情報および各資産のセキュリティ対策状況を元に現状の改善点やリスクの識別評価を実施。 お客様で監視・情報最新化できる仕組みを提案。	・長年稼働を続ける工場やプラントで、拡張・変更を繰り返してきたシステム全体のセキュリティ対策の実態把握。 ・デジタルトランスフォーメーション(DX)を進める際のセキュリティ対策の見直しで活用。 ・製造業の現場棚卸で活用。

可視化装置

NX UsbMonitor
機器のUSBポートを監視。
USBの利用状況を可視化。

NX NetMonitor
ネットワーク内の機器を監視。
稼働中の機器を可視化。

NX NetMonitor IDS+
ネットワーク内の通信を監視。
機器の通信を可視化。

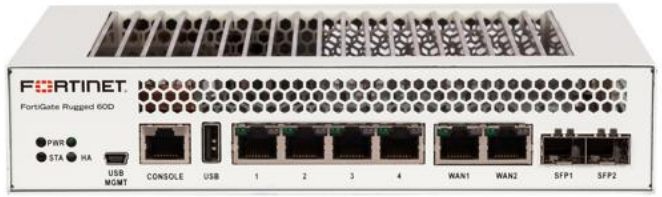
問合せ先：https://www.hitachi.co.jp/security-inq

産業用制御システム向けFW/UTM

FortiGate Rugged

FortiGate Ruggedシリーズは、産業用制御システムのネットワークに対する悪意のある攻撃からの保護を目的として特別に設計された、オールインワンのセキュリティアプライアンスです。産業用制御システムの設置環境に対応すべく、電気や無線の干渉、寒暖差による影響など、過酷な環境への耐性を持っています。

- **産業用制御システムの主要なプロトコルを網羅**
- **振動や寒暖差の大きい過酷な運用環境に対応**
- **電気や無線周波数の干渉が大きい環境に対応**
- **IEC 61850-3、IEEE 1613などの国際的な変電所オートメーション規格に準拠**
- **壁面やDINレールに設置可能**



60D

35D

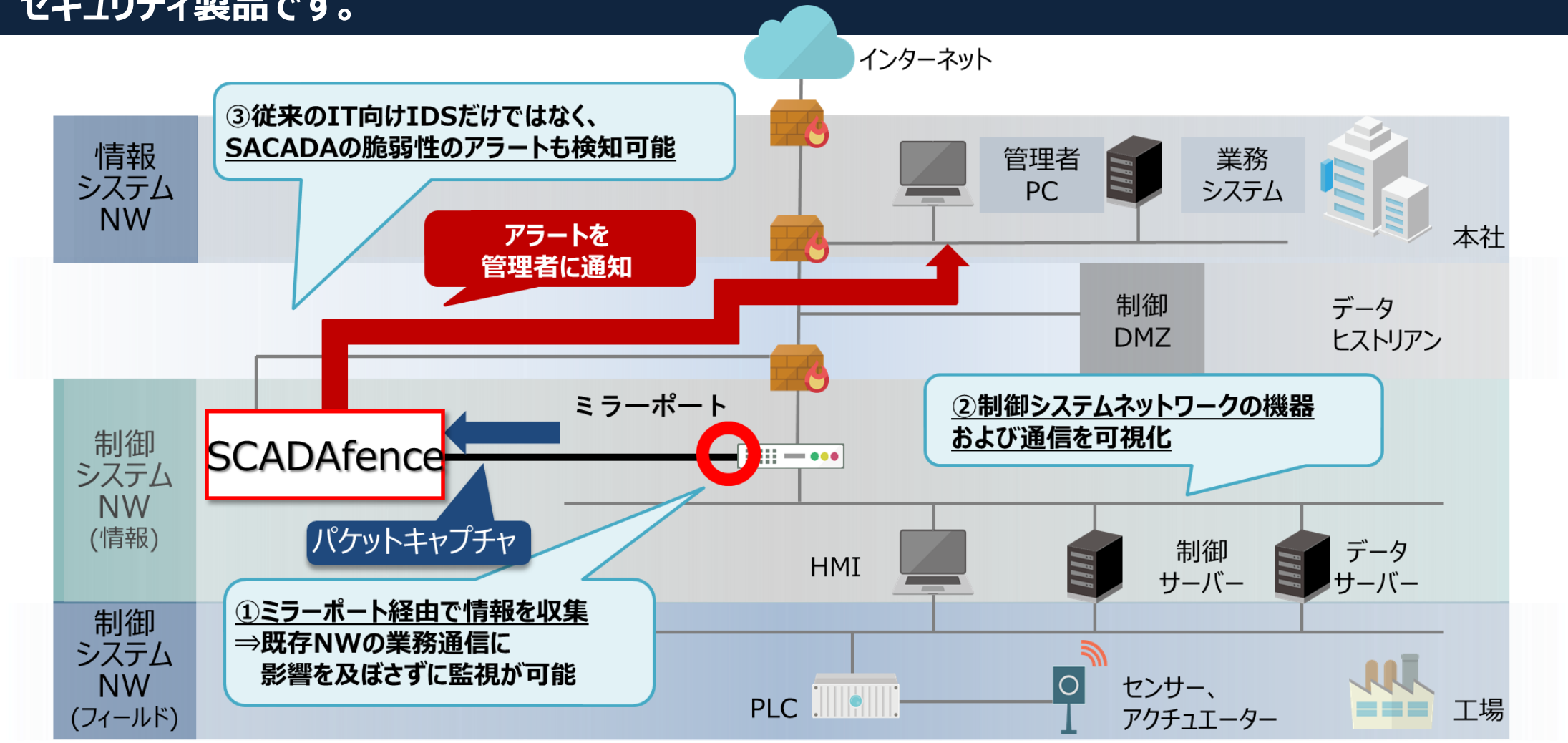
30D

耐久性を考慮した設計で過酷な環境に対応

問合せ先：https://www.hitachi.co.jp/security-inq

SCADAfence Platform

SCADAfence Platform は、工場やビルなどのIoT(Internet of Things)やOT(Operational Technology)のネットワークや資産を可視化、管理を容易にし、マルウェアや不正操作などから守るセキュリティ製品です。



IDS: Intrusion Detection System

OTネットワークセキュリティ可視化サービス

サービスカタログ

FUJITSU

OTネットワークセキュリティ可視化サービス

OTネットワーク・セキュリティ可視化サービス

近年、広範囲な**生産ライン停止**を含む、工場のOTネットワークでの**重篤なマルウェア感染被害**が増加しています。
従来感染リスクが少ないと考えられていた、工場のOTネットワークにおいても、**マルウェア感染リスクの低減**と、万が一感染した場合の**生産業務への被害・影響の極小化**が急務となっています。

※OT(Operational Technology)：各種生産設備及びそれらを制御するシステム

一般的な工場の声

① OTネットワークに接続されている機器や、その脆弱性を把握・管理がしたい。
② 産業用プロトコルも含めて、OTネットワーク上に流れる通信内容を可視化したい。
③ OTネットワークのセキュリティ強化として、どのようなツールを利用すれば良いかわからない。

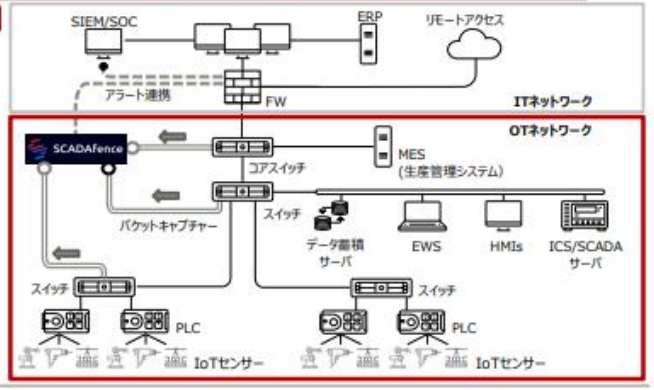
ご提供サービス（セキュリティセンサーによるOTネットワークの可視化）

お客様生産現場のネットワークにセキュリティセンサー(SCADAfenceプラットフォーム)を接続し、接続デバイス及びそれらが行っている通信内容、また、それらが持つセキュリティ脆弱性や異常通信を可視化・管理できる環境をご提供致します。

お客様メリット

① ネットワークの最新状況を自動で可視化することができ、従来かかっていた管理コストを削減できる
② セキュリティリスクの早期発見、及びその初動対応の迅速化により、生産業務への被害を低減できる
③ 大規模な環境であっても少人数で効率的、且つ、安価な運用の実現が可能

導入構成イメージ



shaping tomorrow with you
社会とお客様の豊かな未来のために

サービスカタログ

サービスの特長

特長1 OTネットワーク上の機器情報を自動収集。台帳管理や定期的な現場サーベイが不要

- 自動で検出した機器情報を一覧表示することができ、リアルタイムな資産管理を実現
- PLCやHMIなどの生産設備やIoT機器も識別し、IP/MACアドレスの他、機器の種別、属性、OS、ファームウェアバージョン情報などを収集
- CVE(共通脆弱性識別子)を基に機器の脆弱性を管理し、セキュリティ運用を効率化

特長2 OTネットワーク上の機器に対する脆弱性や通信内容を管理。異常発生時の対応リコメンドにより、早急にリスクを排除

- OTネットワークに特有の産業用プロトコルにも対応。PLCやDCSの通信状態を制御コマンドのレベルまで把握。通信状況を継続的に自動学習することで、変化の多いOTネットワークでも通常とは異なる振る舞いを迅速に検知
- 異常発生時の対応に関するリコメンドを提供し、被害発生・拡大を防止

特長3 国際・業界標準ガイドラインへの適合度合いをスコア化。取るべき対策とその効果が明確になり、効率よく高度化

- ホスト名やIPアドレスなどの機器情報とアラート情報、リスクレベルを拠点ごとに集約し、IEC-62443やNISTなどのOTネットワークにおける標準規格・ガイドラインへの適合度合いをスコアリング
- 規格やガイドラインが持つ各項目に対する適合度合いを把握することで、実施すべき対策とその優先順位が明確となり、対策後の効果を確認しながら実行が可能

サービスの位置づけ

工場における最大のセキュリティリスクは操業停止に陥ることであるため、工場内でセキュリティインシデントが発生した際に、如何に早く検知し、被害を最小化できるかが重要となってきます。
本サービスを導入することにより、生産現場を可視化し、継続的に監視できる環境を整備することで、セキュリティインシデントに対する早期発見と迅速な初動対応を可能にし、OTネットワークの安定稼働に必要となる運用の最適化を実現します。

お問合せ先

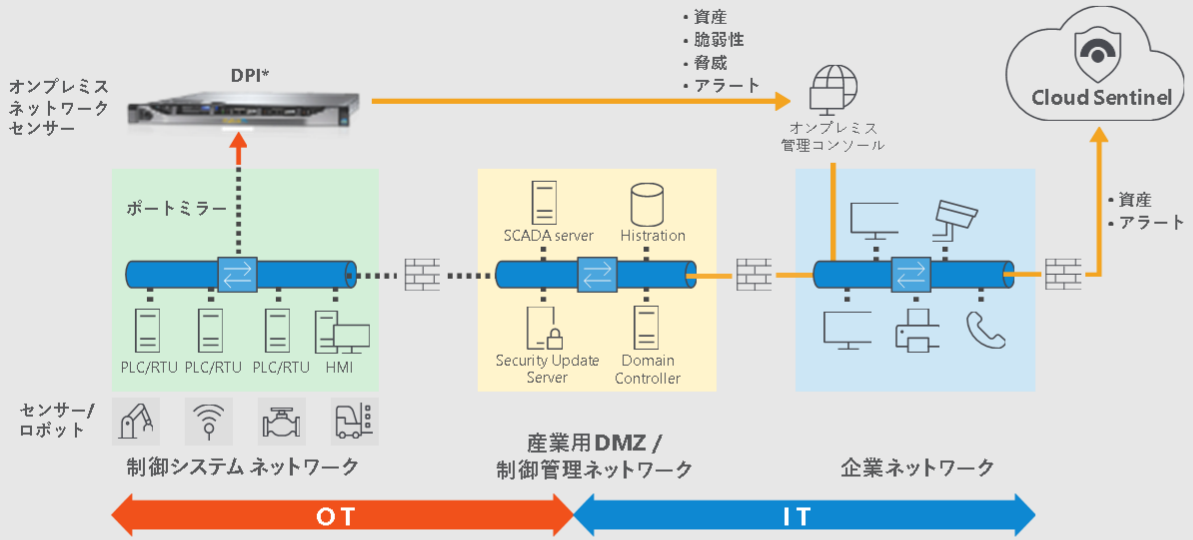
富士通コンタクトライン（総合窓口） 0120-933-200

受付時間 9:00～12:00および13:00～17:30（土・日・祝日・当社指定の休業日を除く）

富士通公開サイト https://www.fujitsu.com/jp/

Microsoft Defender for IoT

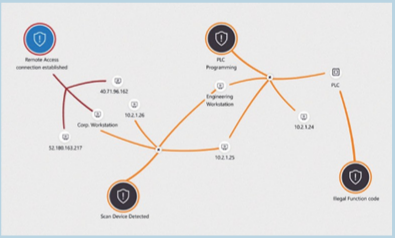
Microsoft Defender for IoT 制御ネットワークの可視化・異常検知



Azure Sentinel との連携

IT/OT の境界を越えた多段階攻撃を迅速に特定

Sentinel とネイティブに統合することができ、IT/OT のすべてから集約された情報をもとにセキュリティのモニタリングとガバナンス強化をすることができます。



Sentinel によるインシデントの分析画面

100% パッシブでパフォーマンスに影響を与えず導入

センサーをミラーポートに接続するだけで自動的にデバイスを検知して詳細情報を含む IoT/OT 資産を視覚的なネットワークマップとして表示できます。

セキュリティ リスク レポートをいつでも簡単に作成

お客様のネットワークのリスク スコアをまとめたレポートをその根拠となる脆弱性情報やその対応策を含めていつでも作成ができます。

すべてのベンダー固有プロトコルを認識

DPI* エンジンをプラグインとして追加することで、すべてのプロトコルに容易に対応することができます。

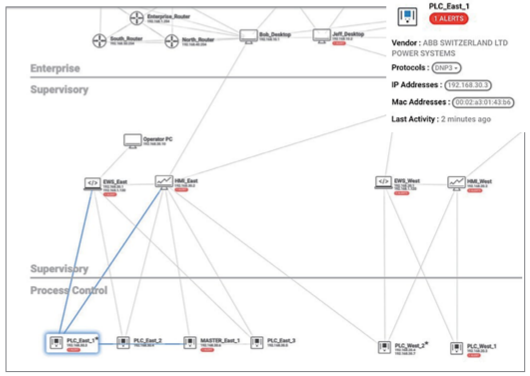
機械学習と IoT に対応した行動分析による脅威検知

特許取得済みのふるまい検知機能により、外部からの侵入やマルウェア感染 (ファイルレスを含む) などでネットワーク内で異常な行動があるとそれを即座に検知することができます。

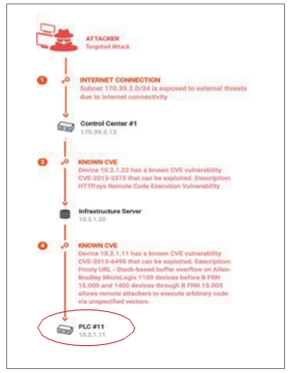
攻撃経路のシミュレーションによる重要デバイスへのリスクを予見

重要デバイスへの侵入経路をシミュレーションすることができるので、効果的な対応策を容易に判断することができます。

＊DPI (Deep Packet Inspection)：ネットワークを流れるパケットを解析する機能。接続されているデバイスの発見、異常や脅威の検知などを実施。



接続されているすべてのデバイスの通信を分析して自動的に階層に分類して表示



攻撃可能な経路のシミュレーション

Microsoft

問合せ先：edgecross_ms_desk@microsoft.com

改定履歴

Ver	改定内容	発行年月
2021年9月版	初版発行	2021年9月
2022年3月版	日本マイクロソフト社　Microsoft Defender for IoTを追加	2022年3月

https://www.edgecross.org/