スマート製造セキュリティソリューション

作成:趙科強　セキュリティソリューションアーキテクト

日付:2023.4

Security Level:

HUAWEI

目次

生産業務を効果的に保護するすべく、セキュリティ関連政策や条例が相次ぎ施行

全人代(国会)

『中国サイバーセキュリティ法』

国は、重要な業種や分野、および破壊、機能喪失、データ漏洩により、国家安全保障、国民経済、国民生活、公共利益に重大な危害を与える可能性のある重要な情報インフラに対して、サイバーセキュリティ等級保護制度に基づいて重点的な保護を実施する。

第59条ネットワーク運営者が本法第21条、第25条に定められているネットワーク安全保護義務を果たせない場合、管轄部門が是正を命じ、警告を与える。是正を拒否した場合、またはネットワークの安全性を損なうなどの結果をもたらした場合、1万元以上10万元以下の罰金を科し、直接責任を負う責任者に対して5000元以上5万元以下の罰金を科す。

国务院
WWW.GOV.CN

国務院(内閣)

重要情報インフラのセキュリティ保護条例

重要インフラセキュリティ認定基準:

(3)5人以上が死亡、または50人以上が重傷者が出た場合
(4)5000万元以上の経済的損失を直接引き起こした場合
(8)社会的・経済的秩序に重大な損害を与え、または国家安全保障を危険にさらした場合。

情報化と産業化の高度の融合を推進する中で、**「スマート製造の産業制御システム（PLC）のセキュリティ保障能力構築を強化し、総合的な保障体系を健全化する」と提言。**

「インターネット+製造業」の深化と産業インターネットの発展に関する指導意見」

「セキュリティ保護の強化」を理念とし、「高い安全性と信頼性」を基本原則とし、**「産業用インターネットのセキュリティ保護システムの構築、と能力向上」**の目標を明確化。

公安部(警察庁)

「サイバーセキュリティ等級保護基本要件」

セキュリティ等級保護制度1.0をベースに重要な情報インフラの保護に関する要件をさらに強化

基本的な要件を踏まえ、PLCシステム専用技術とアプリケーションに適用されるセキュリティ拡大要件をまとめた

中华人民共和国工业和信息化部

工業情報化部

PLCシステムの情報セキュリティ保護に関するガイドライン

セキュリティソフトウェアの選定と管理、設定とパッチ管理、境界セキュリティ保護、物理、環境のセキュリティ保護、ID認証、遠隔アクセスセキュリティ、セキュリティ検出と緊急時対応計画訓練、資産セキュリティ、データセキュリティ、サプライチェーン管理、責任の実施に関する11のガイドラインを明確化。これは、産業制御セキュリティ分野における国家サイバーセキュリティ法のセキュリティ要件を反映している。

『PLCシステム情報セキュリティインシデント緊急管理業務ガイド』

『PLCシステム情報セキュリティ保護能力評価業務管理方法』

『PLCシステムの情報セキュリティ行動計画』

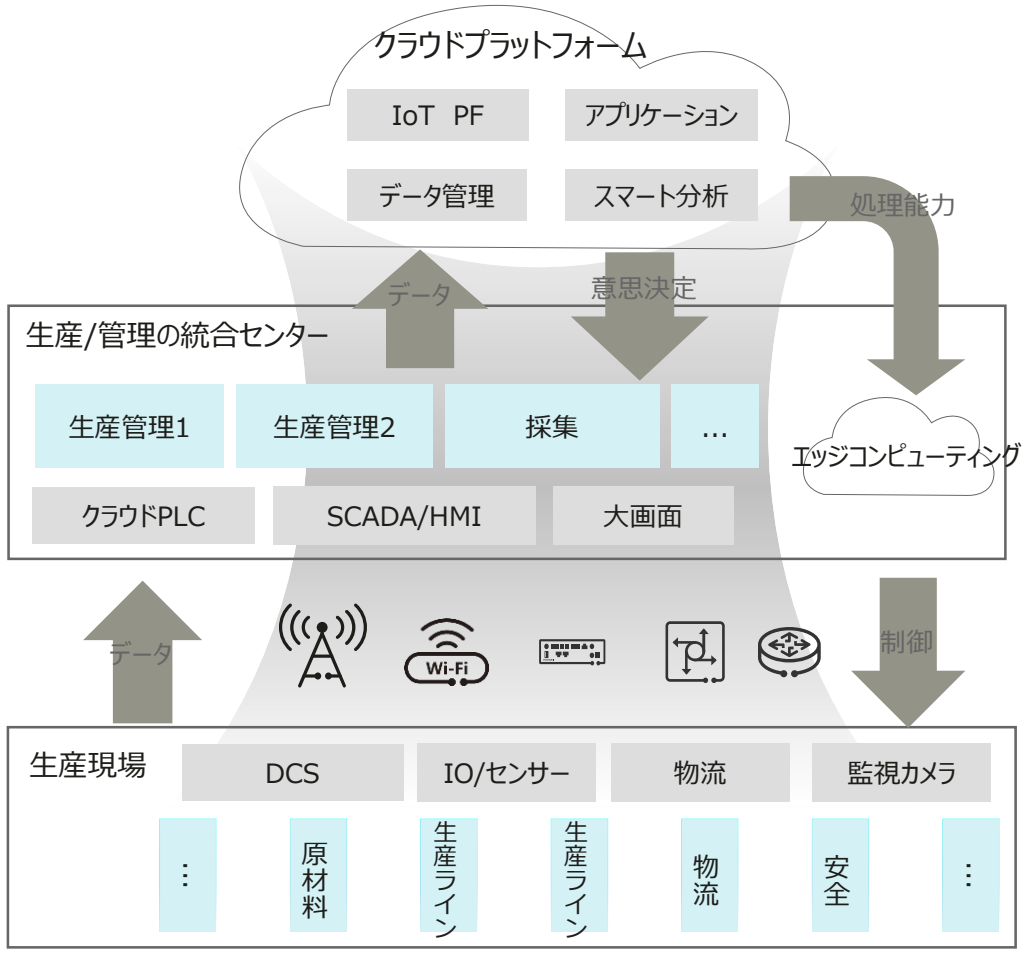
『産業用インターネットのセキュリティ強化に関するガイドライン』

……

- **第21条:政府は等級保護制度を実施し、法律面から企業主体に等級保護の構築を求める。**
- **第38条:関連機関は重要な情報システムに対して定期的に等級保護評価を行う。**
- **第59条:等級保護を怠ることは違法であり、企業トップの責任の追及、生産停止・過料。**

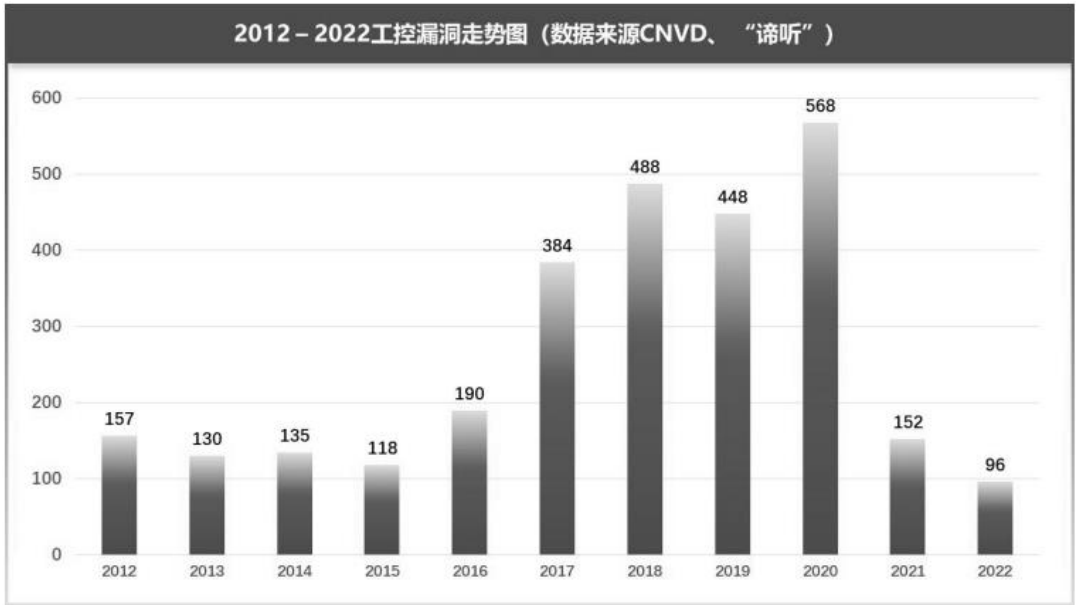
HUAWEI

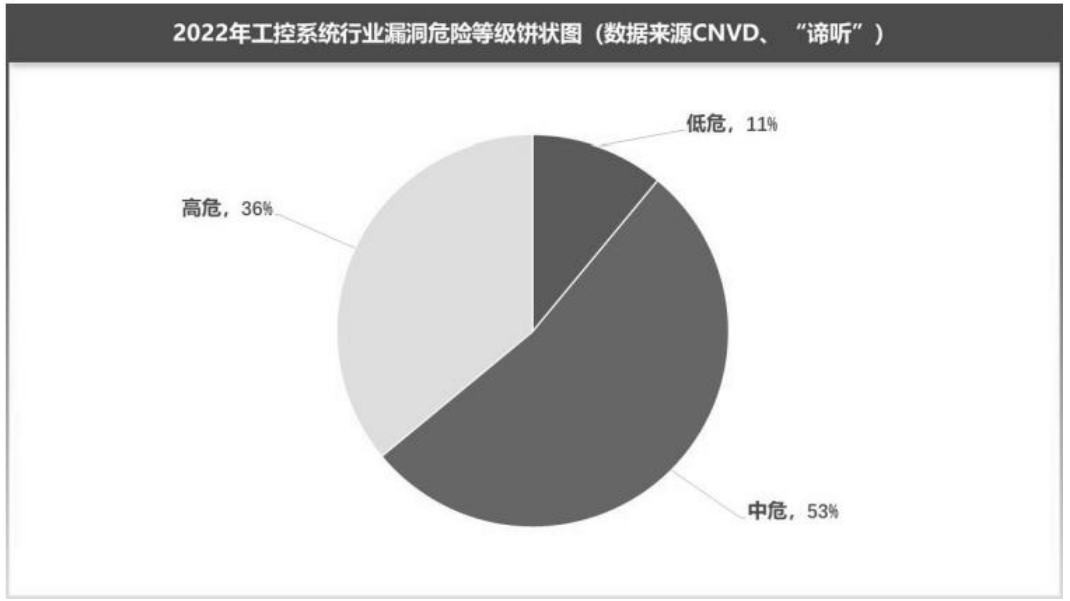
企業のデジタル変革がもたらす新たなセキュリティ課題



- **融合:**ITリスクがOTネットワークにもたらされた場合、生産が中断されないようにする方法とは
- **ネットワーク化、IoT化:**ネットワークアクセス端末が急増、端末のなりすましと場所移動
- **クラウド化:**頻繁な業務変更、ネットワークの境界が曖昧になり、クラウド内のアプリケーションをどう保護するか
- **スマート化:**ビッグデータ+AI、データ価値が急増、どう重要データを保護するか
- **統合管理:**SCADAとHMIのリモート化、不正コマンドや不正操作をどう検知するか

脆弱で攻撃されやすい生産システム、セキュリティ状況がいっそう深刻化





『2022年産業制御におけるサイバーセキュリティ状況に関するホワイトペーパー』

- PLCシステムには多くの脆弱性があり、**98%以上**がハッカーに悪用される中・高リスクの脆弱性
- 2010年以降、**APT攻撃は**顕著な増加がみられ、高度標的型攻撃で、長期持続的な攻撃で甚大な被害に
- 2017年以降、**ランサムウイルス**が急増し、ファイルの暗号化、システムの破壊などの被害は、生産現場を直撃

セキュリティインシデントの教訓

ドイツの製鉄所がAPT攻撃で生産停止、高炉に被害

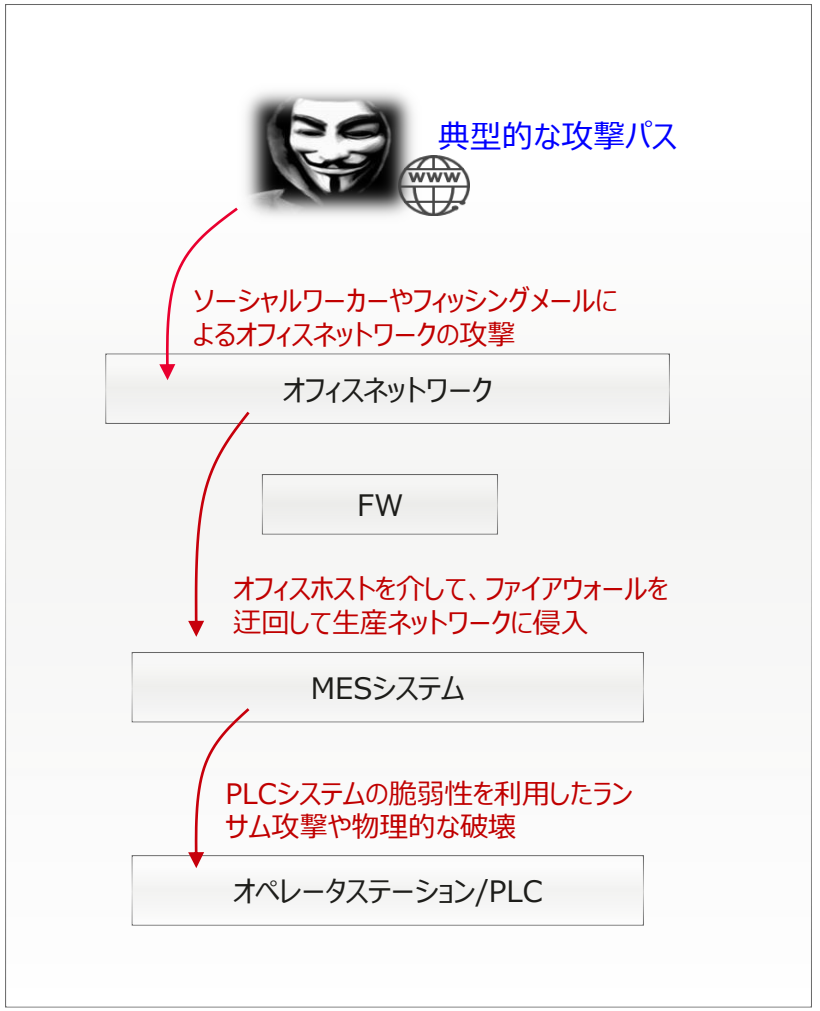
2014年12月には、ドイツの製鉄所が**APT**によるサイバー攻撃を受け、重大被害を受けた。攻撃者はフィッシングメールやソーシャルワーカーの手法を使ってオフィスネットワークに侵入し、そこから生産ネットワークに侵入。PLCシステムに精通している攻撃者の頻繁な破壊によってシステムが故障し、高炉が非常閉鎖しなければならず、設備が損傷し、甚大な損失をもたらした。

半導体メーカーがランサム攻撃を受け、3日間で17億ドル損失

2018年、台湾の半導体メーカーはランサムウイルスに感染し、生産ネットワークに未知のランサムウイルスを搭載した新しい機器を導入したが、脅威検知とセキュリティゾーニングの不備で、ウイルスは生産ネットワークに急速に拡散し、3つの生産拠点が停止に追い込まれ、3日間で17億元もの損失が発生。

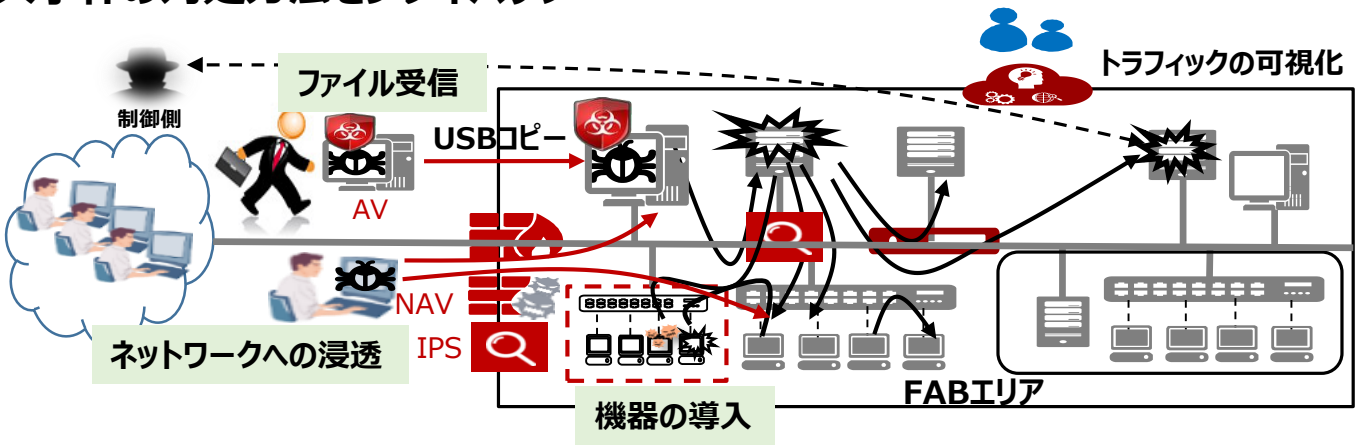
教訓

1.従業員の安全意識を高め、フィッシングメールを警戒する。
2.オフィスネットワークと生産ネットワークのセキュリティゾーニングを行い、オフィスネットワークを介した侵入を防ぐ



セキュリティ構築の教訓と提言

- 2つの脅威侵入事件の対処方法をプレイバック



2017

- ファイルのインポート。AVは未知のウイルスを検出できず…
- イントラネットAVはウイルスを検知・駆除できず。
- イントラネットで拡散。管理者が不審なトラフィックを発見
- IDSには特徴がなく検出できないためパッチも対処できない
- 少数のホストのBSOD状態。管理者が異常を発見し、原因を分析
- 管理者は不審なトラフィックを発見し、該当ホストを遮断し、ワームの拡散を防ぐ
- 被害ホストは、バックアップを使用してシステムを復元。
- 感染したホストはウイルスを駆除した後、1台ずつ復旧、トラフィック監視により、動作を保証(復旧までX時間がかかり、業務損失をほぼゼロに抑えた)

2018

- ウイルスが潜伏している無症状の新設備がウイルスをもたらす…
- ウイルスはイントラネットに拡散し、既存設備に感染
- 管理者が検知できず…
- ウイルスは生産ライン、エリアを横断して拡散
- ウイルスにより、複数の工場の生産ラインが停止
- 管理者がトラブルシューティングを実施したが、すでに手遅れ。
- 故障分析により原因を洗い出し
- 生産ラインを復旧(復旧までX日がかかり、業務損失が10億以上)

- 教訓と提言

教訓:
1. 攻撃はイントラネットに直接侵入し、発見は手遅れ。
2. 未知の脅威に対する防御能力に不備
3. 内部で防御できず、脅威拡散に対する制御能力と感知能力が不足

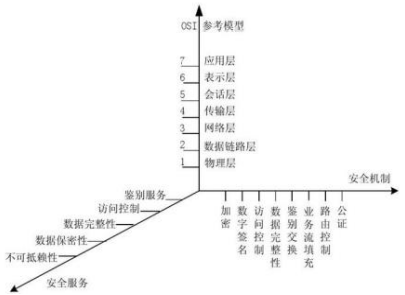
提言:
1. セキュリティゾーニングを構築し、ITリスクがOTに入るのを阻止し、踏み台攻撃を減らす。
2. 検知システム、プローブ、サンドボックスを実装し、ランサムなどの未知の脅威に対処。
3. ゾーニングとセキュリティ分離を強化することで、ウイルスと脅威の水平方向拡散を阻止

目次

産業用インターネットセキュリティの枠組み、３つの視点からセキュリティリスクに包括的に対処

OSIセキュリティシステム

ネットワーク層に応じたセキュリティ対策

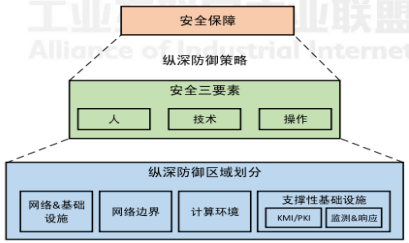


P2DRモデル

動的なセキュリティ保護、脅威の継続的な監視と対応

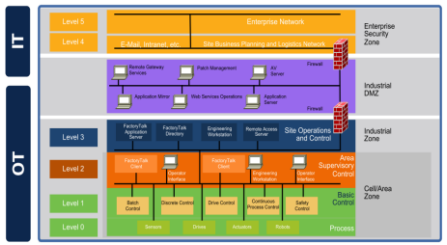
IATF情報保証技術の枠組み

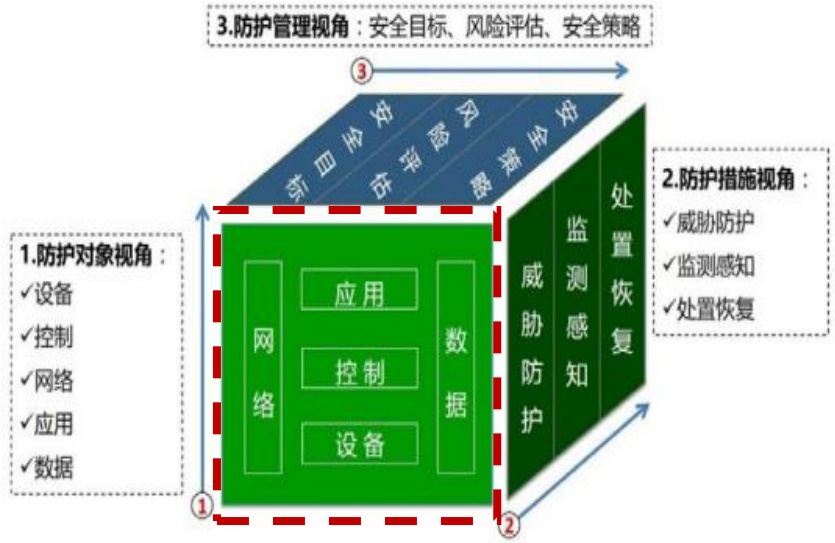
多層防御により、技術と管理を強化



IEC 62443

垂直階層化、水平方向のゾーニング



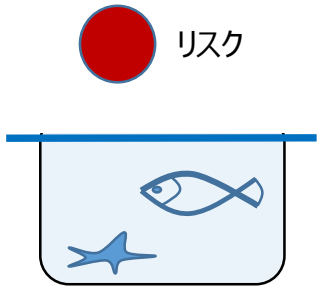


産業用インターネットセキュリティの枠組み–AII 2018

- 保護対象、保護措置と保護管理の3つの視点から構築し、保護対象に応じた措置を講じ、システムの安全問題をリアルタイムに監視し、タイムリーに対応。
- セキュリティ管理を強化し、セキュリティ目標に基づいてセキュリティポリシーを指定し、継続的に改善し、産業ネットワークのセキュリティを確保。

セキュリティ設計理念:ベストエフォート型防御から確実なサービス保証へ転換
3次元の強靭なセキュリティ保護の枠組みを築く

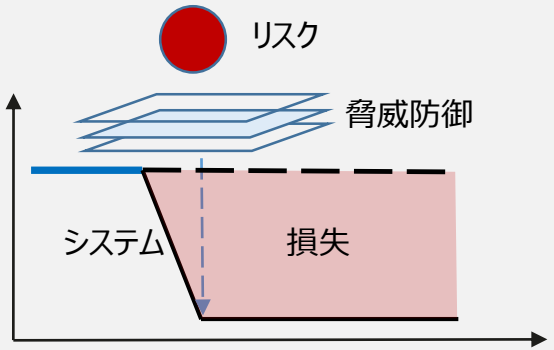
AS-IS:一次元線形型防御



「脆弱性丸見え、防御手段がなく、脅威不明」では、産業システムの安全性をどう確保する？

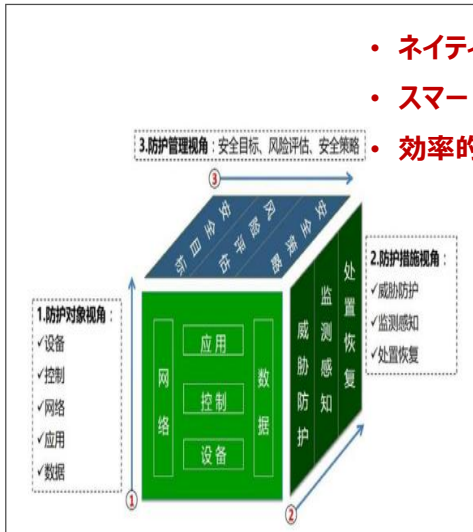
- **脆弱性丸見え:**システムは古く、脆弱性を改善できず、ウイルス感染されても継続利用
- **防御手段なし:**遅延/ジッタを増やすことができず、設備保守リスクが高く、防御技術の導入が困難
- **未知の脅威:**APT攻撃とランサム攻撃には、未知の脅威と高度な脅威が多数含まれている

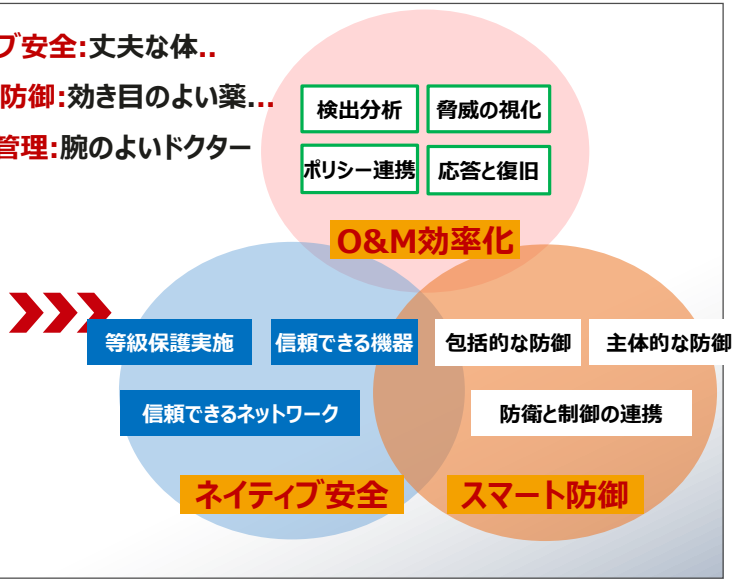
ベストエフォート型では脅威に対処できない



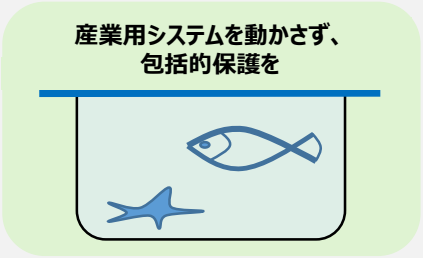
TO-BE:3次元靭性保護

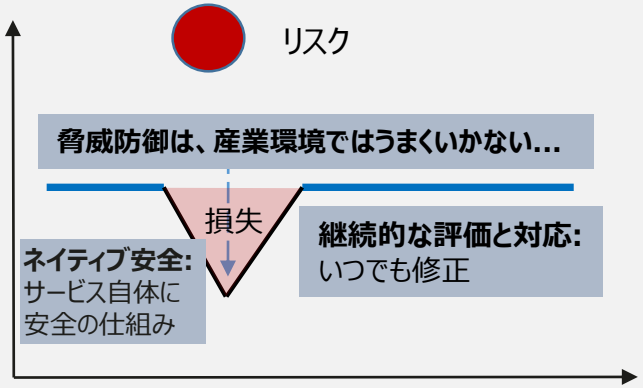
- **ネイティブ安全:**丈夫な体..
- **スマート防御:**効き目のよい薬...
- **効率的管理:**腕のよいドクター





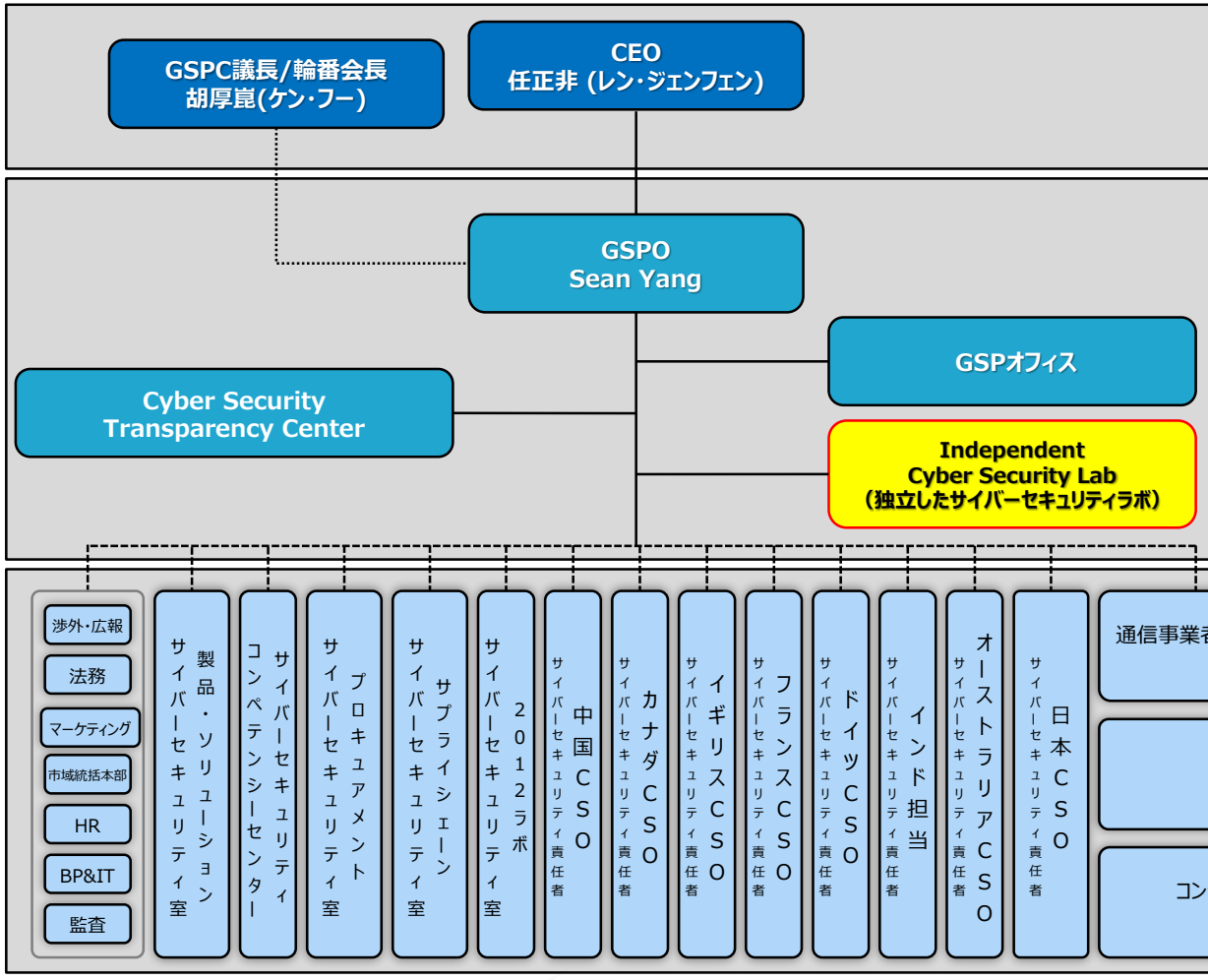
包括的保護と確実なサービス保証





ファーウェイのサイバーセキュリティ戦略は、統制、監査、ビジネスプロセス、政策、手順、標準、目標など、全ての活動に【組み込まれている Built-in 】（強力な保証システムを可能にするガバナンス体制）

- GSPC、GSPO、GSPO office、ICSL LAB、RSPO、CSPOセキュリティ組織
- ICSLでの審査に合格すると、GSPO（John Suffolk英国政府で情報セキュリティ責任者を歴任）へ上申され、GSPOでの審査に合格すると、CSOへ報告される仕組みとなっている



GSPC：Global Cyber Security & User Privacy Protection Committee
戦略的方向性を策定。戦略、計画、指針、ロードマップ、投資について合意し、戦略の実施、優先順位における競合の解消、監査に責任を負います。

GSPO：Global Cyber Security & User Privacy Protection Officer
（セキュリティ戦略の策定、サイバーセキュリティ保証システムの社内での確立を取りまとめ、ステークホルダーとのコミュニケーションや、お客様のサイバーセキュリティシステムの確立をサポートします、ファーウェイのグローバル・サプライチェーンに関わるセキュリティをあらゆる側面から監視・改善を図るとともにサイバー・セキュリティ保証システムの強化および実行を監督します。

GSPOオフィス：Global Cyber Security オフィス
関連部署を調整して詳細な運用規則と実務内容を整備し、戦略とその実行をサポートするとともに、適用推進、監査、実行状況の追跡を実施します。

地域/BG/BU CSO

地域・部署レベルのセキュリティオフィス：GSPOと連携し、サイバーセキュリティ戦略とその要件が各地域・部門に十分に浸透し、必要に応じて更新されるよう、部門や事業部レベルのプロセスをどのように変更すればよいかを判断し、実施を監督することに責任を負います。セイバーセキュリティ責任者は、戦略全般の策定と改善に取り組みます。さらに、各部門もそれぞれ専任の専門家を擁しています。

3800+セキュリティと個人情報保護専任担当者

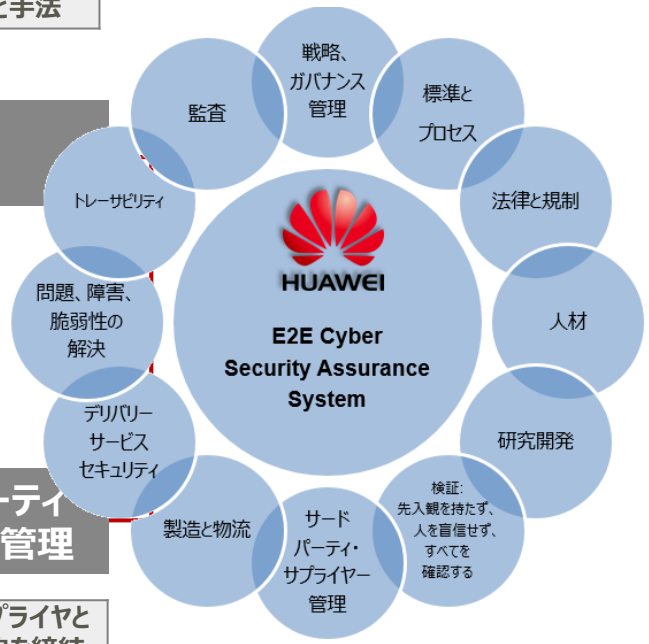
全社、全従業員を対象としたE2Eのサイバーセキュリティ保護システム

- HUAWEI End-to-End サイバー・セキュリティ保証システムに含まれる12分野
- サイバーセキュリティは**ソフトウェア、ハードウェア**など技術だけでなく、**戦略や組織、人材、テクノロジー、プロセス**なども大きく関わっています。言い換えればファーウェイ全体、そして従業員一人ひとりと切っても切れない関係にあります

戦略、ガバナンス管理	標準とプロセス	法律と規制	人材	研究開発	検証
最高指針 GSPC	最適な基準を採用 ビルトイン	コンプライアンス 800+法律専門家	100%BCG署名率 違反処分制度 キーポジション管理	信頼できる CSへ7.5億ドルの投資 ソフトウェアエンジニアリング能力開発に20億ドル	テストしか信用しない 多様な視点と手法

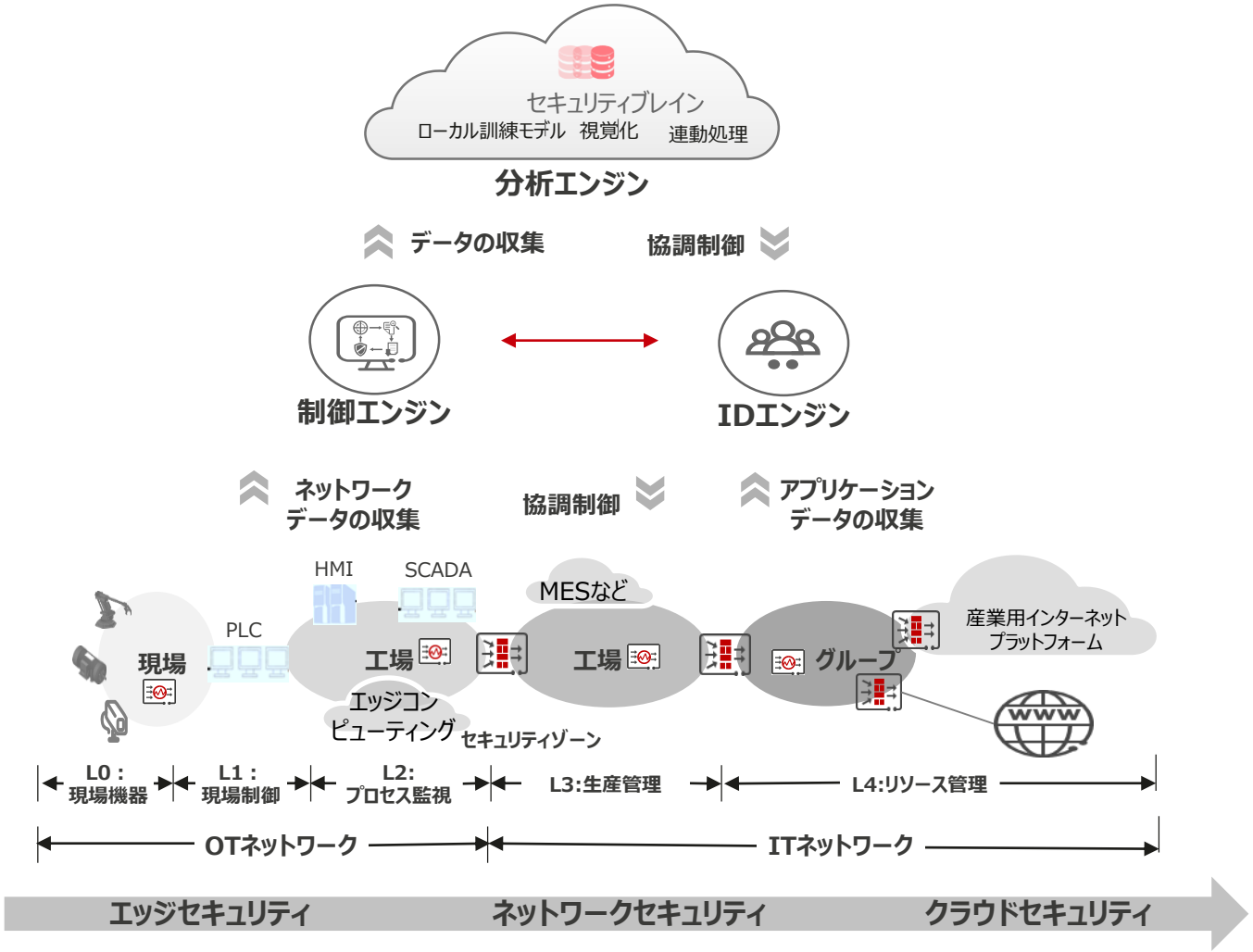
人材、テクノロジー、プロセス

監査	トレーサビリティ	問題、障害 脆弱性対策	安全なサービスデリバリー	製造と物流	サードパーティサプライヤ管理
内部監査 第三者による監査 お客様の監査	ソフトウェア:1時間 ハードウェア:4時間	セキュリティ脆弱性管理センター(HVMC) 責任ある開示	3つの審査 安全な遠隔アクセスPF セキュリティ就業証明書	ISO 28000、C-TPAT、TAPAなど 自動テスト装置(ATE) デジタル署名	3,855社のサプライヤとセキュリティ契約を締結 サプライヤ認定 部品部材受入テスト



目次

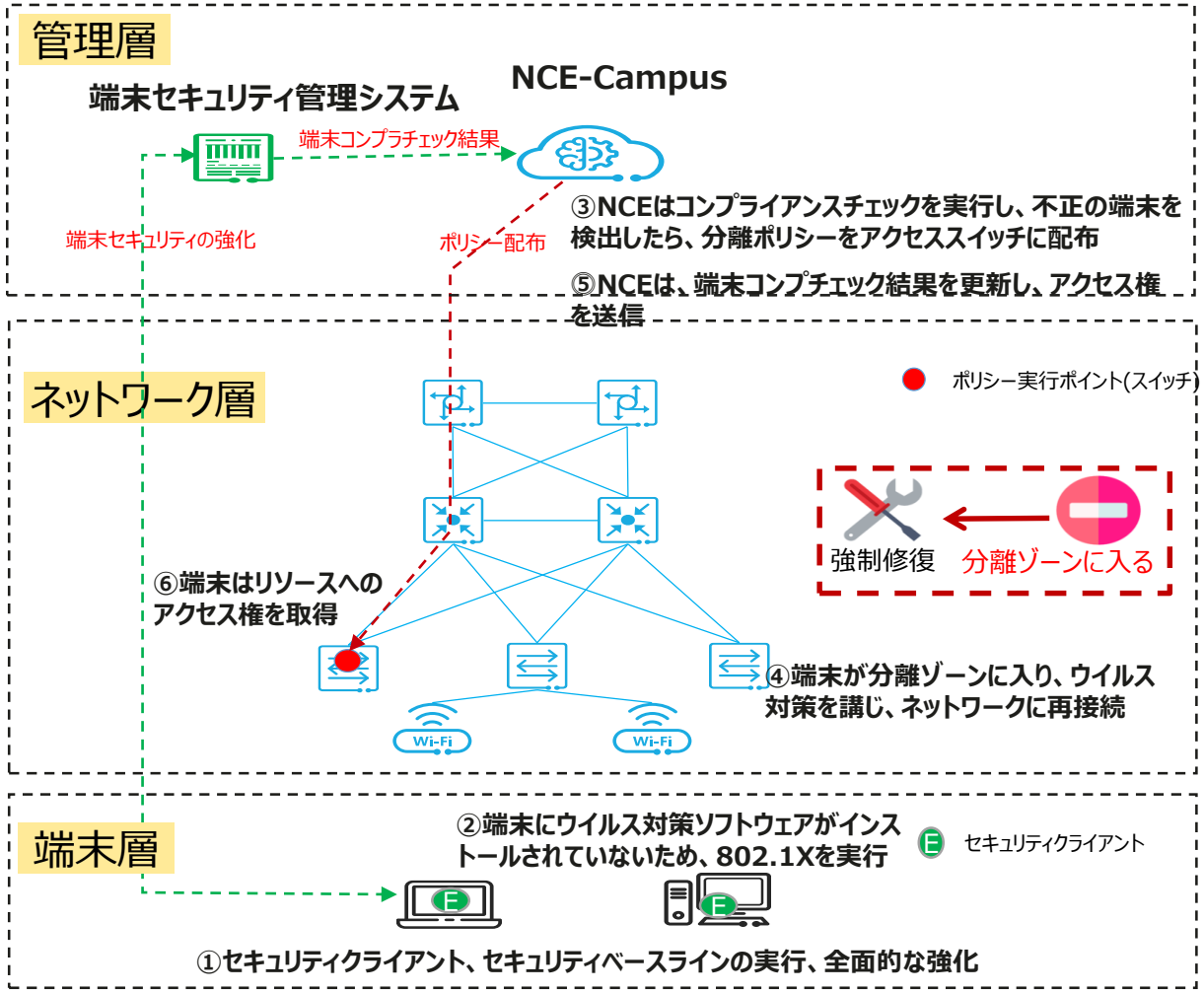
セキュリティ指向ネットワーク:多層防御、ネットとセキュリティ連動、IT/OTの包括的安全を確保



多層防御、ネットとセキュリティ連動、包括的セキュリティ

- **IT/OTの3級多層防御、等級保護と法順守**
  - **PLC:**トラフィックを解析し、PLCのホワイト環境を構築し、3級保護を実現
  - **セキュリティゾーン:**生産作業変更不要。一元構築でコスト削減。オンデマンドのセキュリティ機能展開。ITからOTへの侵入を効果的に防ぐ。
  - **多層防御:**IT境界+セキュリティゾーン+OT境界で3級保護体系の多層防御を確立し、重要な業務とデータを効果的に保護。
- **クラウド/ネットワーク/セキュリティを包括的、主体的に防御、安全運営レベルを向上**
  - **完全監視:**ネット/エッジ/エンドの全量収集、能動的検出、「死角なし」のセキュリティ監視。
  - **スマート分析:**セキュリティビッグデータのAI分析により、未知の脅威と高度な脅威を検知。
  - **迅速な処理:**脅威可視化、ネットワーク・セキュリティ連動、自動処理、セキュリティ問題を数分で解決。
- **ゼロトラスト、ローカルとリモートユーザーによるアプリケーションとデータへの信頼できるアクセス**
  - **SDPゼロトラスト:**継続的な認証、きめ細かな権限制御でローカル/リモートでの企業アプリケーションへのアクセスを安全かつ効率的に
  - **アクセス制限:**同時にアクセスできるのが一つのネットワークだけで、根本から踏み台攻撃を食い止める
  - **セキュリティサンドボックス:**不審なアプリケーションのアクセスを感知し、自動的にローカルサンドボックスアクセス環境を起動し、データをサンドボックスから取り出すことができないようデータの安全性を確保。

オフィス端末のネットワークアクセスにおけるセキュリティ



包括的ヘルスチェック、セキュリティ強化

- 端末のセルフチェック:パッチ、弱いパスワード、共有ディレクトリ…
- セキュリティ強化:DNS、DHCP、ソフトウェアのホワイトリスト…

セキュリティチェック、正常アクセス

- 認証に成功すると、NCE-Campusは端末セキュリティ管理システムからコンプライアンスチェックの結果を取得
- 準拠していない端末は、分離ゾーンに隔離し、修復する

継続的な監視、動的許可

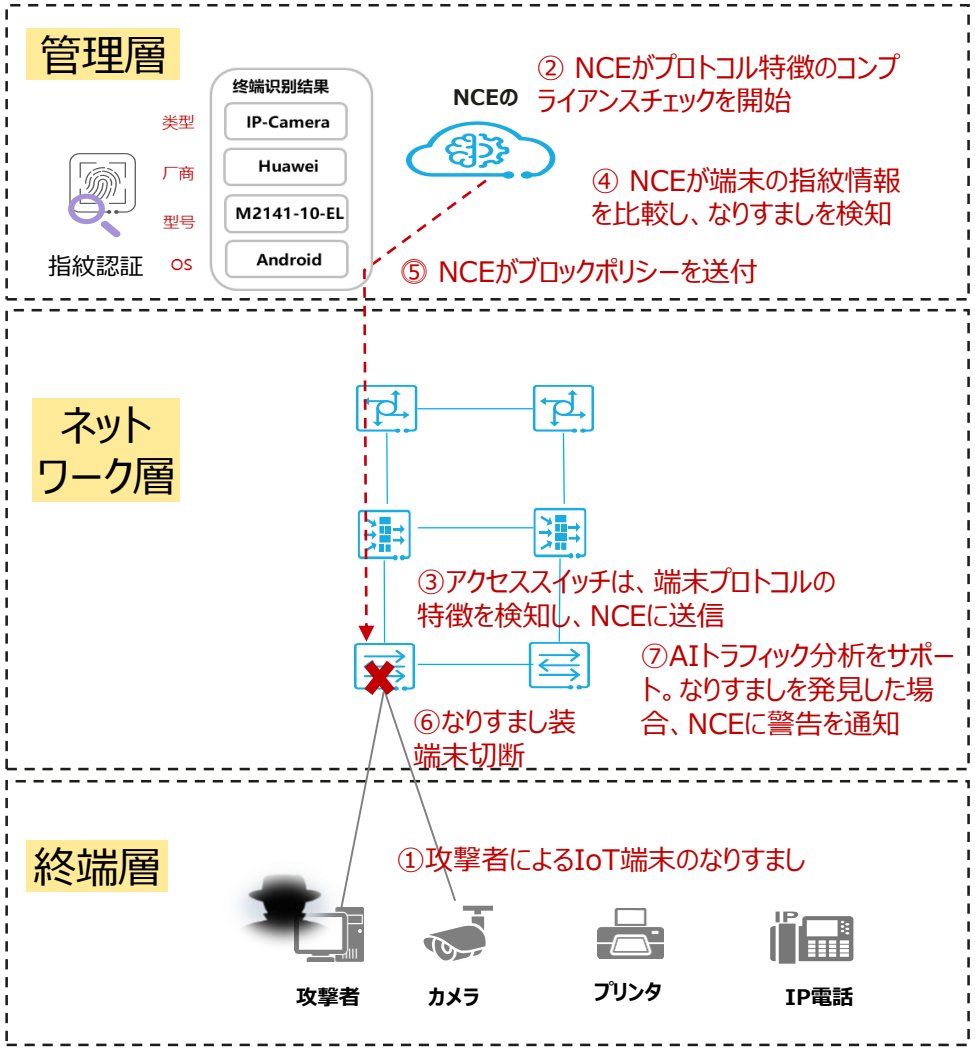
- NCE-Campusは端末セキュリティ管理システムから端末セキュリティコンプラチェック結果をリアルタイムで同期
- NCE-Campusは、セキュリティコンプラチェック結果に基づいてセキュリティポリシーを更新し、スイッチに配信し、端末のアクセス権限を動的に更新

ポートフォリオ:NCE-Campus+セキュリティクライアント

ソリューションの特徴:ネットワーク接続と端末セキュリティが連動し、安全な端末だけがネットワークに接続可能

HUAWEI

信頼できるIoT端末アクセス



ポートフォリオ:HiSec Insight+NCE-Campus+スイッチ
ソリューションの特長:プロトコル指紋認証+トラフィック挙動分析、なりすまし端末の発見と隔離

IoT端末の正確な識別

- **多様な方法:**4種類の検知方式:nmapアクティブスキャン、プロトコル指紋ライブラリ比較、カスタム検知ルール、手動マーキング。
- **豊富な種類:**1.8万種類の端末タイプを検知可能。タイプ、メーカー、モデル、OSなどのフィールド検知可能
- **速い:**デバイスがオンラインになるとすぐに検知が始まる。
- **高精度:**多種の認識方式を総合的判断し、検知精度が高く、顔認証100%成功。
- **きめ細かい:**端末タイプに応じてセキュリティポリシーを配信。

IoT端末の不正アクセス防止

1. **未使用ポートを閉鎖:**スイッチにアクセスされていない端末のポートをシャットダウン。
2. **MAC認証:MACを設定し、**不正端末の接続を防止。1つのポートに1つの端末のみがアクセスでき、ハブへの不正アクセスを防ぐ。
3. **ポートバインドルール:**ポートをMACとIPにバインドするように設定。攻撃者はMACをスニッフィングしても、IPアドレスがわからないため、ネットワークにアクセスできない。

IoT端末のなりすまし防止

1. **よくあるなりすまし:**NCEはプロトコル指紋を比較することにより、なりすまし端末を発見し、アラームをトリガし、ブロックポリシーを送付。
2. **高度なりすまし:**スイッチ/HiSecのInsightは、AIトラフィック分析でなりすましを検知し、アラームをトリガし、ブロックポリシーを送付。

IoT端末のハイジャック防止

1. **リスクの検知:**オープンサービスとセキュリティの脆弱性をスキャン。
2. **脅威検出:**トラフィックを収集し、AI脅威モデリングを行い、なりすまし端末検出、クラッキング、リモートコントロール、データ漏洩などのセキュリティインシデントを検知。
3. **迅速な対処:**ネットワークとセキュリティが連動し、迅速に対処。

モバイル端末セキュリティ管理

不明アプリをインストールすると、セキュリティリスクが発生する。

機器の持ち出し、データ漏えい。

不正なネットワークに接続し、機密データを流出。

ポートフォリオ:MDMセキュリティクライアント+MDMセキュリティコントローラ

ソリューションの特徴:モバイル端末の徹底管理と制御により、ネットワーク攻撃とデータ漏洩を防ぐ。

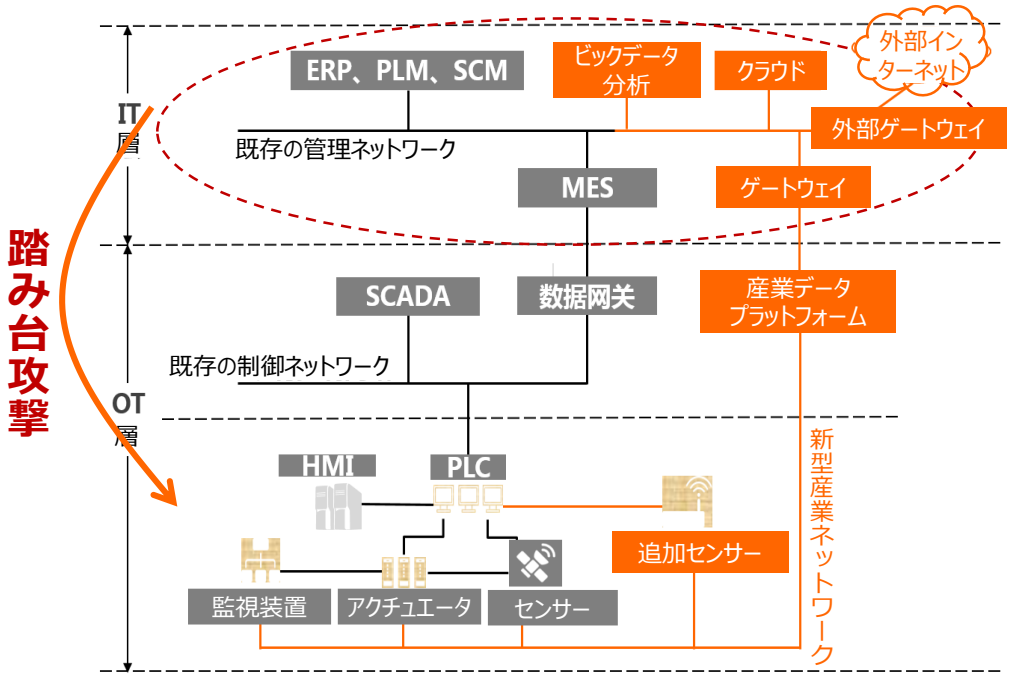
ソリューション設計

- モバイル端末に**セキュアクライアント**をインストールし、携帯電話、タブレット、PDA、コードスキャナなどのモバイルデバイスに対応、**Android、IOS**の主流OSをサポート。
- モバイル端末とアプリケーションシステムとの間でデジタル証明書を用いて身元を検証し、全過程を暗号化して伝送する。
- **APPのブラックリストとホワイトリスト**をカスタマイズし、不正APPをインストールすることを禁止。
- GPSとネットワークホットスポットに基づいてデジタルフェンスを定義し、モバイル端末が指定エリアを離れた後、システムを自動的にロックして通報する。
- **監視カメラは、**従業員が特定のエリアに入ると、管理者はコードをスキャンしてカメラを無効にし、退場後に再度コードをスキャンしてカメラを有効化。
- モバイル端末は指定された**SSID**のネットワークのみにアクセスできる。私的に外部の不正なネットワークに接続することを許可しない。
- **セキュアデスクトップ**でシステム設定をロックし、定義されたセキュリティポリシーを使用し、**Bluetooth、カメラ、USBストレージなどを無効化。**
- データの暗号化保存が可能で、**透かし、遠隔データ消去**などをサポートし、データの安全性を保証。

HUAWEI

PLCならではのセキュリティ特性:業務継続性最優先のため、閉鎖的システム、丸見えるの脆弱性、隙だらけの保護対策

オフィスネットワークの脅威は生産ネットワークに浸透し、被害甚大...

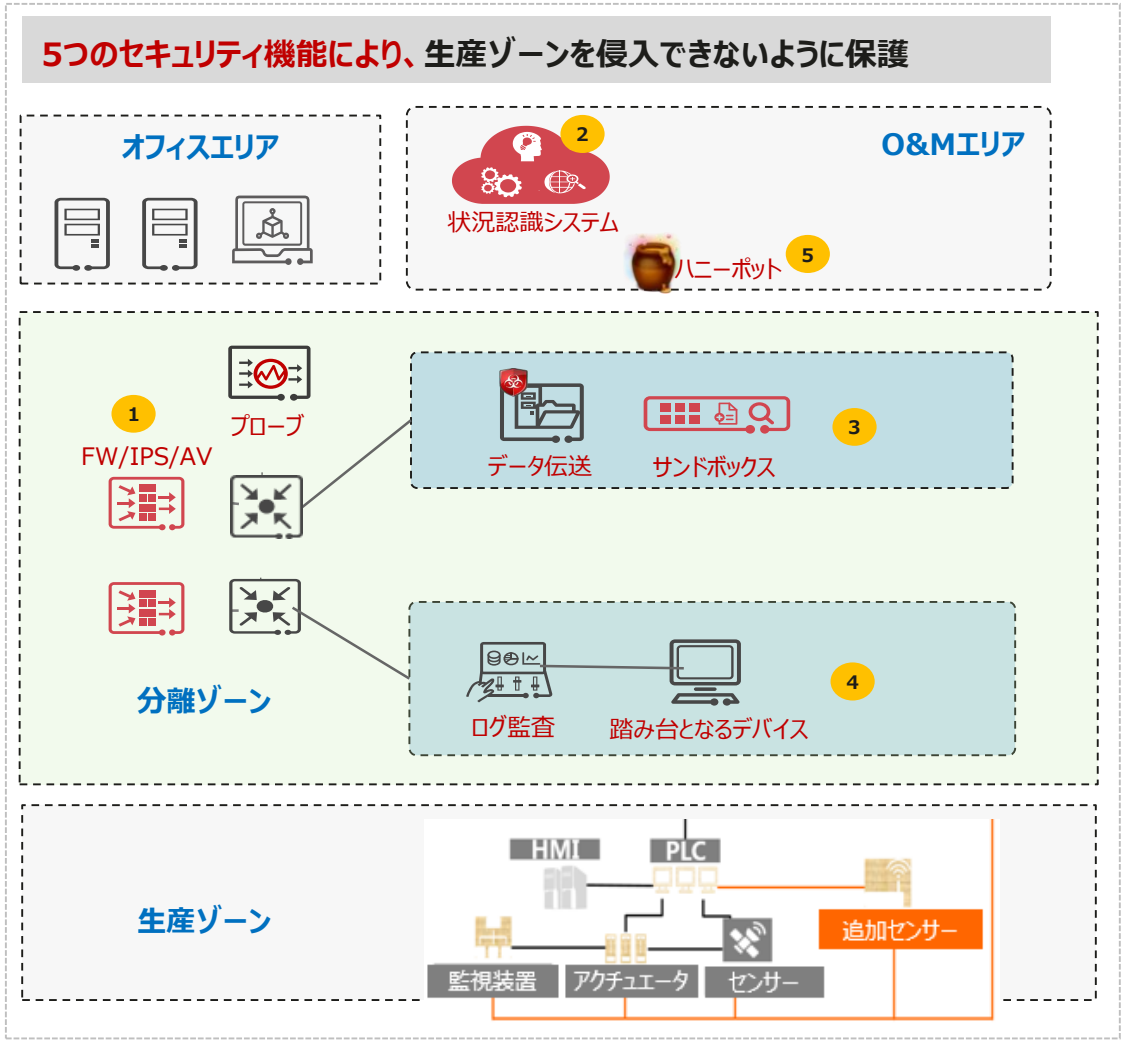


- **業務継続性最優先:**可用性がセキュリティより優先度が高く、ファイアウォールやウイルス対策などの防御手段が不足。
- **専用プロトコル/脅威検知困難:**プロトコル、技術アーキテクチャなどさまざまな脅威があり、一般的な脅威情報は有用性が低く、個別の脅威の特定が困難。
- **丸見えの脆弱性、隙だらけの保護:**重要なシステムのため、サードパーティのセキュリティパッチをインストールできない。20年以上の老朽設備は、脆弱性が丸見え。

- 工業情報化部の『産業用インターネットセキュリティ状況報告書』：最大の被害をもたらす脅威は、ランサムウェアなどの高度なITリスクが産業システムへの侵入である。
- **企業のITは、脅威が生産OTに侵入するために必ず通る道。高度な脅威を阻止するためには、ITとOTの境界で効果的なアイソレーションが必要。**

分離ゾーン:ITリスクのOT侵入を効果的に阻止

分離ゾーン



セキュリティリスク

- 悪意のある攻撃者がオフィスネットワークに侵入した後、生産ネットワークに踏み台攻撃を行い、生産の中断とデータ漏洩を引き起こす。
- オフィス端末がフィッシングメールまたは悪意のあるウェブサイトにアクセスしてウイルスに感染した後、ウイルスが生産ネットワークに入り、生産が中断される。
- ユーザーは生産エリアでUSBディスクを使用してファイルをコピーし、ランサムウイルスが生産ネットワークで急速に拡散し、生産が中断されました。
- メーカーのリモートまたは工場で設備を運用し、メンテナンスする場合、誤操作、悪意のある操作、機密データの漏洩のリスクがあり、追跡が困難です。

ソリューション

1. **境界防御能力**:生産ネットワークの境界にファイアウォールを実装し、IPSとNAV機能を有効化。
2. **未知脅威の検出能力**:セキュリティアナライザーとプローブを実装し、トラフィックを収集する。これらデータを包括的に分析し、未知の脅威を検出。
3. **不正ファイル検知能力**:データ転送とサンドボックスを実装し、USBメモリのインポートとネットワーク転送によって持ち込まれた不正ファイルを検出。
4. **O&M監査能力**:CBHとログ監査を実装し、不正操作と誤操作を防ぐ。
5. **ネットワークトラップ機能**:ハニーポットシステムを導入し、攻撃が発生する前に脅威を検出してブロック

お客様の価値:

- **生産業務変更不要。**
- **一元的構築、投資削減**
- **充実したセキュリティ機能、オンデマンド導入。**

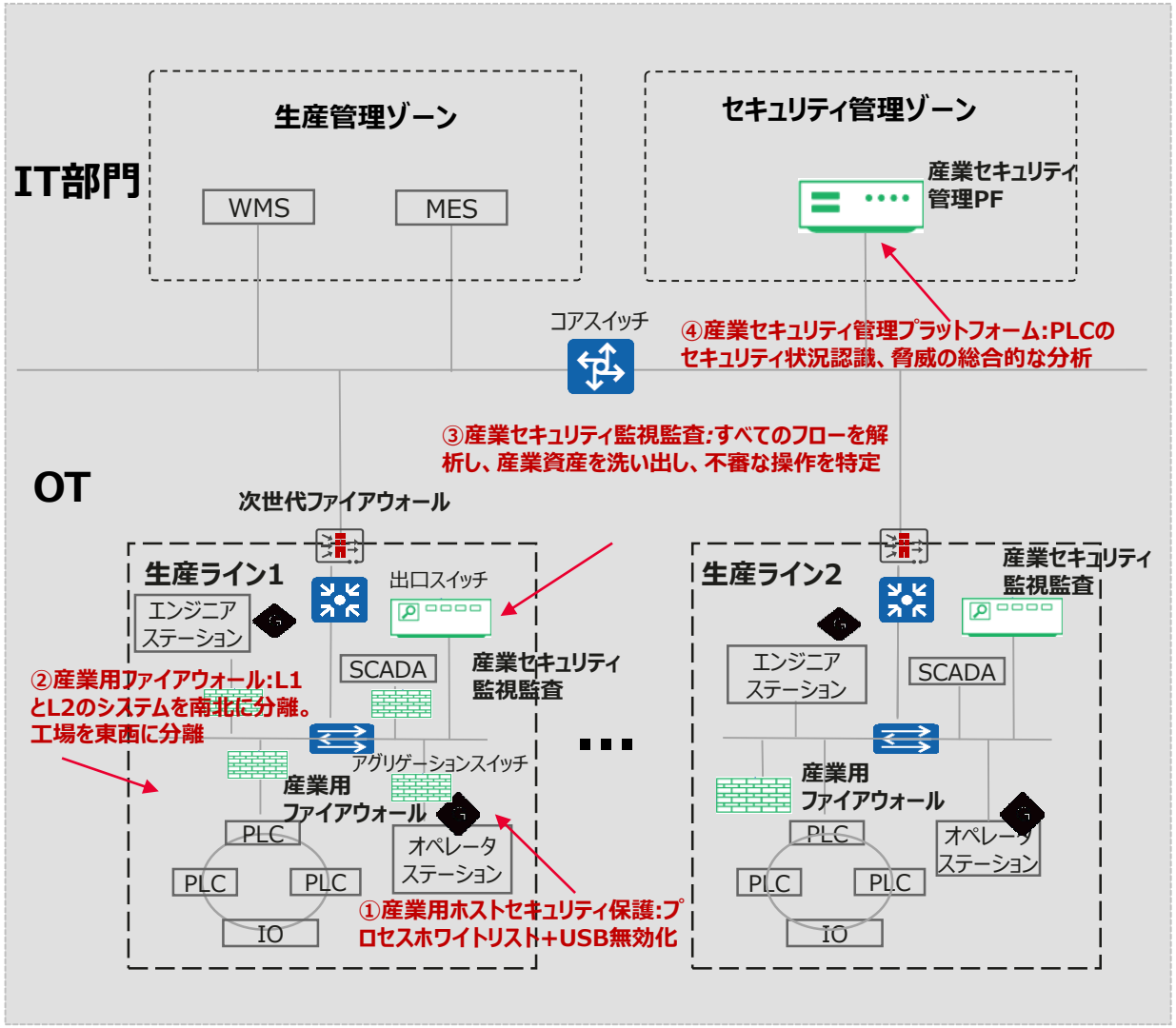
製品構成

- **必須:ファイアウォール、サンドボックス、プローブ、状況認識システム。**
- **オプション:ハニーポット、データ伝送、踏み台マシン、ログ監査。**

HUAWEI

PLCセキュリティ等級保護:セキュリティ4点セットで安全生産の「ホワイト環境」を構築

PLC等級保護3級、スマート製造能力成熟度5級を満たす



PLCセキュリティ保護スキーム

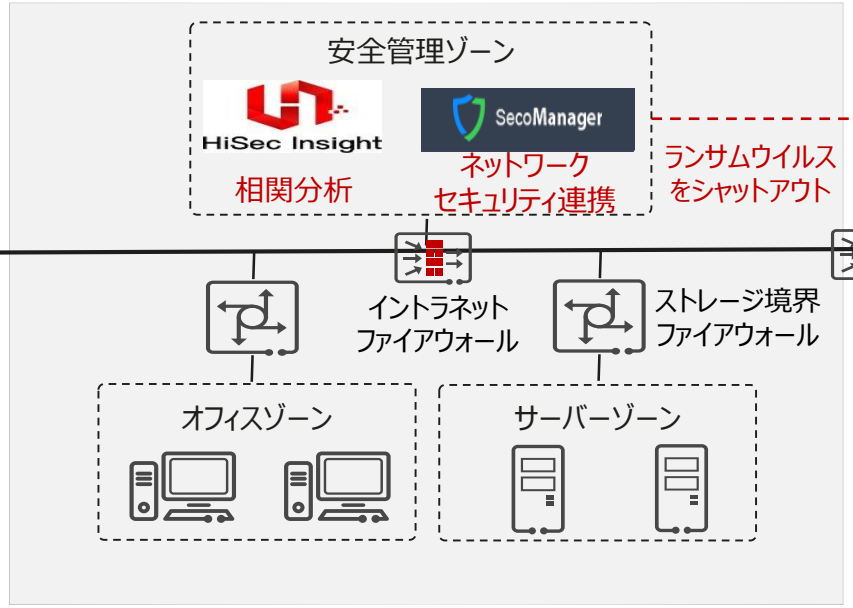
- **セキュリティゾーン境界:**ファイアウォールで分離し、垂直方向の階層化、水平方向のゾーンニング原則に従い、L1及びL2システムの間に産業ファイアウォールを実装する。産業プロトコルを解析したうえで、L１及びL2システムの南北方向の分離と工場ネットワーク間の東西方向の分離を実現する。工場の出口に次世代ファイアウォールを実装し、L２とL3システムの南北方向の分離と工場ネットワーク間の東西方向の分離を実現。ITリスクがOTに侵入し、ランサムウイルスが工場をまたがって拡散することを防ぐ。
- **安全な通信ネットワーク:**L1システムとL2システムに接続されているスイッチに産業セキュリティ監視監査システムを実装し、以下の機能を実現する：
  - 産業資産とPLCの抜け穴を発見し、台帳を明確にする。
  - 通信トポロジーを作成し、不正通信を検知する。
  - 機械学習、ワンクタップでのホワイトリスト作成、不審な操作を検知。
  - IPSルールをプリセットし、トラフィックを分析し、悪意のある攻撃を検出すると警告を通知。
  - O&M監査:設定変更や設備のO&Mなどの重要な操作を記録。
- **安全なコンピューティング環境:**産業用ホストセキュリティガードを設置。ホワイトリストで指定されたプロセスのみが起動でき、USBと不要な通信ポートを無効にする。共通のセキュリティポリシーを適用して、ホストセキュリティガードをインストールできない産業用ホストをアップグレードして交換。
- **セキュリティ管理センター:セキュリティ管理ゾーンに産業セキュリティ管理PFを配置。**
  - サウスバウンドでは、産業用セキュリティ監視監査システムと産業用ファイアウォールからセキュリティログを収集し、生産ネットワーク内の脅威を特定し、OTセキュリティ状況を大画面で表示。
  - ノースバウンドではIT状況検知システムと連携し、ITのOT資産への不正アクセス、OT資産の不正外部接続などのエンドツーエンドの脅威をすばやく検知・対処する。ITとOTの脅威は一体で可視化、分析、対処可能。

HUAWEI

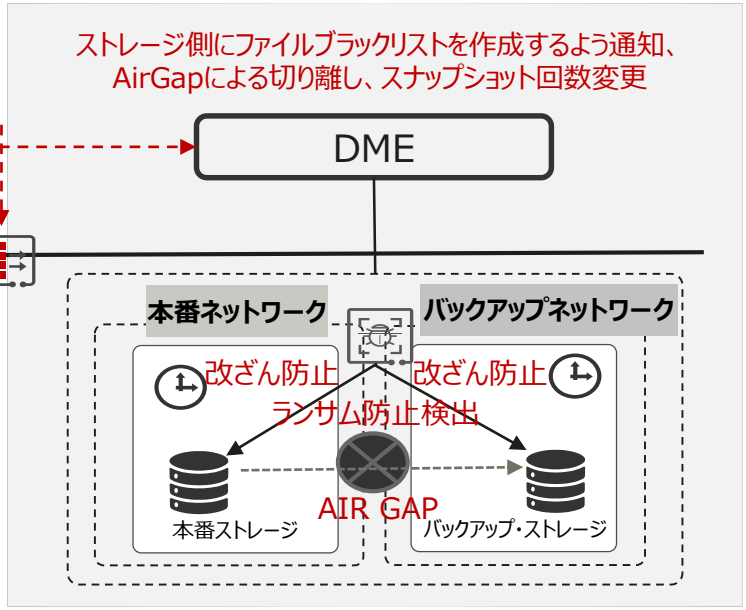
業界初のネットワーク・ストレージ連動ランサム対策を打ち出し、企業の安全を保護

侵入前:正確な境界侵入対策

侵入前:すばやく拡散防止



侵入前:確実にデータ暗号化防止



- ウイルス検出率

80% → 90%

- トレーサビリティ処理時間

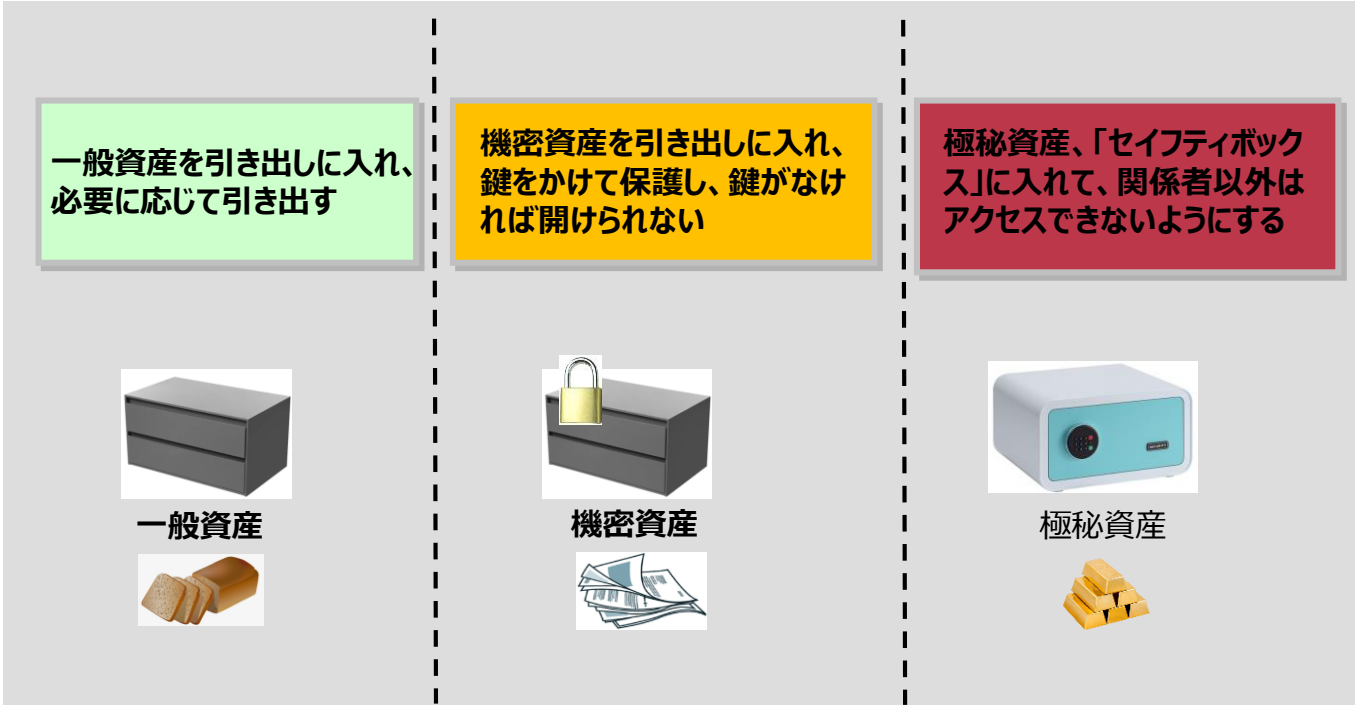
日 → 分

- データリカバリ速度

30TB/h → 170TB/h

HUAWEI

内外の脅威に直面している企業、データ漏洩を食い止める方策とは



資産の重要性によりセキュリティ保護のレベルを選ぶべき

リスクの課題:

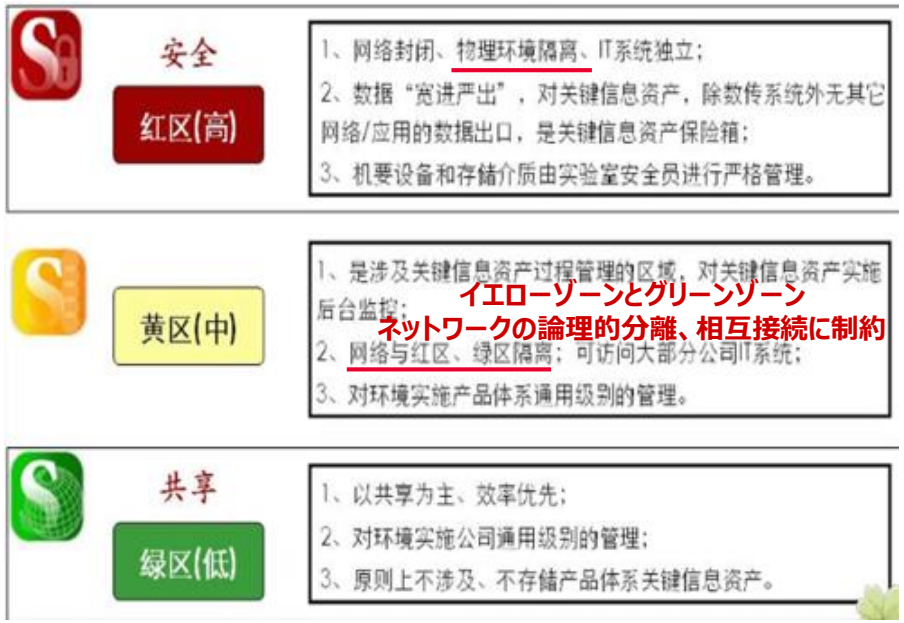
1. 内外の脅威:侵入、特権濫用、情報漏えい。
2. 売上が重要だが、それを守ることがより重要。
3. 絶対的な安全はなく、安全性は費用対効果を考慮する必要がある。
4. データはセキュリティを確保すると同時に十分に流通しなければならない。データが流通してはじめて価値が生まれる。

セキュリティポリシー:

1. データを分類して階層化し、セキュリティゾーニングでセキュリティポリシーを制定する。
2. セキュリティは費用対効果を考慮する必要があり、重要データは機密領域に入れ、重点的に保護する必要がある。
3. セキュリティは業務上必要性に応じて、セキュリティと効率を両立させ、セキュリティの必要性を踏まえ対策を講じる。
4. 技術と管理の両方を重視し、多層防御で外部の脅威を効果的に遮断。

具体的な取り組み:技術と管理の両輪で階層化、分離、正確な制御で保護

レッドゾーン：物理的分離



イエローゾーンとグリーンゾーン
ネットワークの論理的分離、相互接続に制約

厳し管理により環境の物理的分離を実現

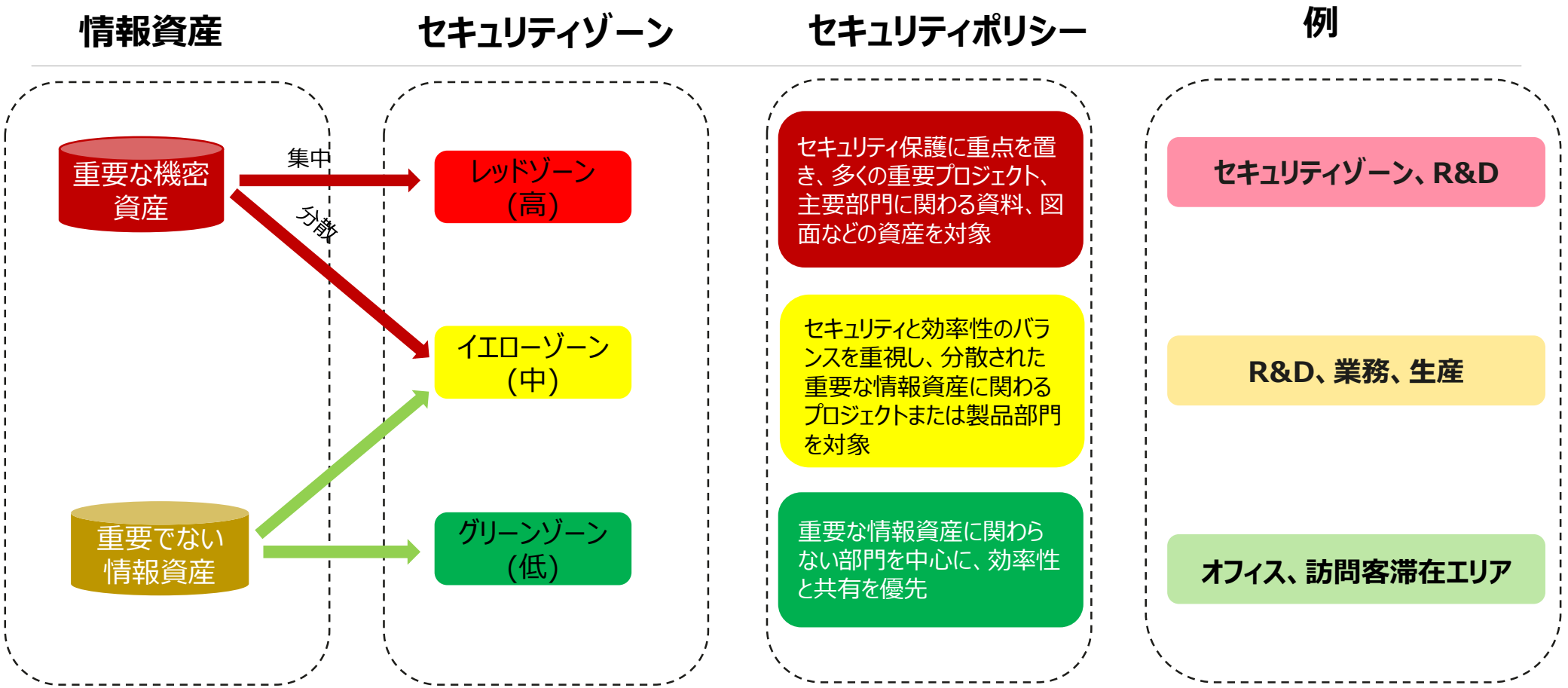
1. 物理的分離により、各フロアを色で区分けし、警備員と入退出制御を設置。
2. 厳格な管理システムを実行し、レッドゾーンは携帯電話やPCを持ち込むことはできない。イエローゾーンは写真撮影は禁止されている。
3. 360度のカメラ監視。
4. レッドゾーンの持ち込みと持ち出しはできない。イエローゾーンからストレージメディアを持ち出すには、承認と封印が必要。

高度な技術手段により、ネットワークを論理的に分離

1. レッドゾーンネットワークは物理的に分離され、ITシステムは独立している。イエローゾーンとグリーンゾーンは、VLAN/VPNなどのネットワーク技術により論理的に分離されたネットワークパーティションを実装。
2. イエローゾーンではデスクトップクラウドを使用できるが、データはローカルに移せない。
3. 高機密性から低機密性へのデータ伝送は、必ず責任者の承認を経て、データ伝送チャネル(eTrans)を通じて伝送し、ITが定期的に監査。

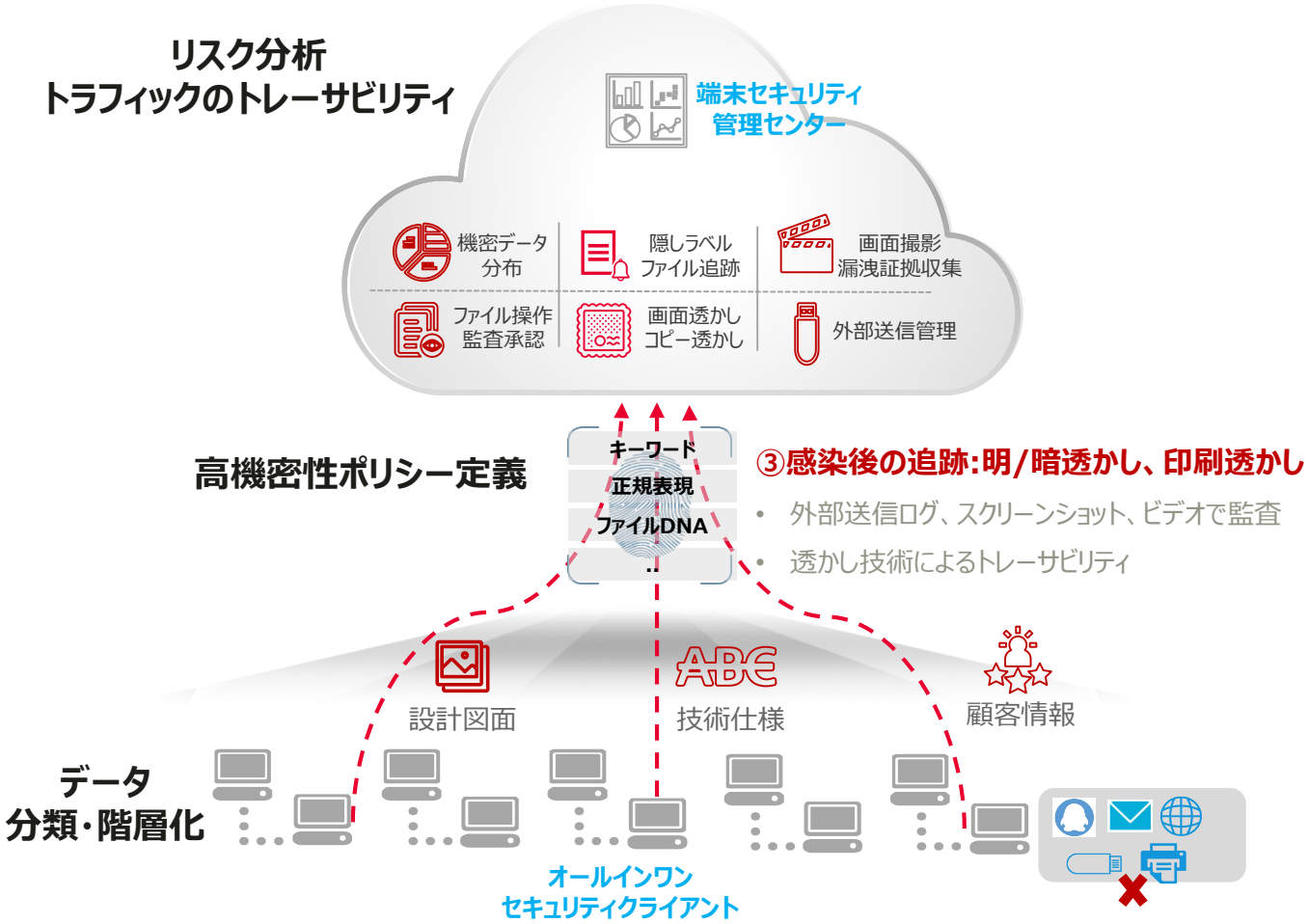
HUAWEI

ゾーンニング原則:資産の重要性と保護要件に基づきゾーンを分け、安全性と効率性を両立



業務にかかわる資産の重要性、保護と共有ニーズに応じて、赤、黄、緑の3つの区画に分け、それぞれ高、中、低の3つの情報セキュリティ管理レベルに対応する。

重要データの漏洩防止:内部の漏洩防止、外部の窃取防止



①検出:機密データを自動的に検知・警告

- ユーザーによる機密データの不正取得と保存

②感染中管理:機密データの発信禁止

- ユーザーは、必要に応じてUSBポートとメール送信権限を申請。
- ユーザー権限とファイルの機密レベルにより、許可、ブロック、承認を実行。
- USB、プリント、ネットワーク経由での機密ファイルのブロックと監査

- **感染前検出**

端末セキュリティ管理センターはデータ分類階層化ルールを定義し、端末に配信。

端末DLPは自動的にホスト側に分散して格納されたデータを整理し、資産とリスクを可視化。

- **遮断**

ユーザーがUSBメモリ、メール、IM、Web、プリンタなどの送信方法を介して機密ファイルを送信しないようにする。

ファイルのイントラネットでの移動はアクセス制御と承認プロセスを経る必要がある。

ファイルのネットワーク横断交換は、安全なデータ伝送システムによってフィルタリングされ、承認・ウイルススキャンと駆除が行われなければならない。

- **監査**

従業員による機密データの操作と送信、ログ記録、自動監査で、「意図的」と意図的でない」データ漏えいを検出。

従業員の端末操作行動を分析し、リスクを予測。

- **追跡**

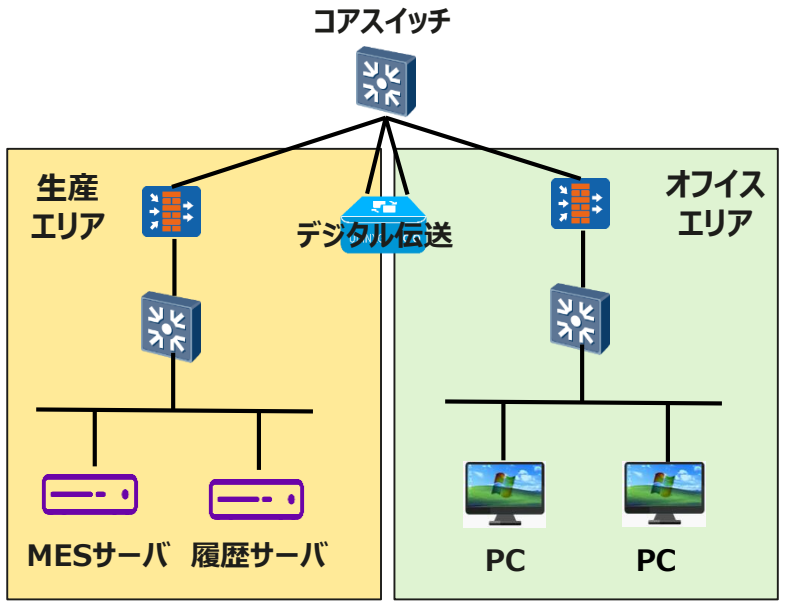
ファイル透かし、スクリーン透かし、プリント透かしなどの技術を使用して、漏洩者を特定し、ログを通じて攻撃を監査・追跡。

- **データ漏えいの脅威の85%以上が社内から発生。**
- **従業員の安全意識の研修、技術的手段を通じて「手を伸ばしたらかならず捕まる」という抑制力を働かせる。**

HUAWEI

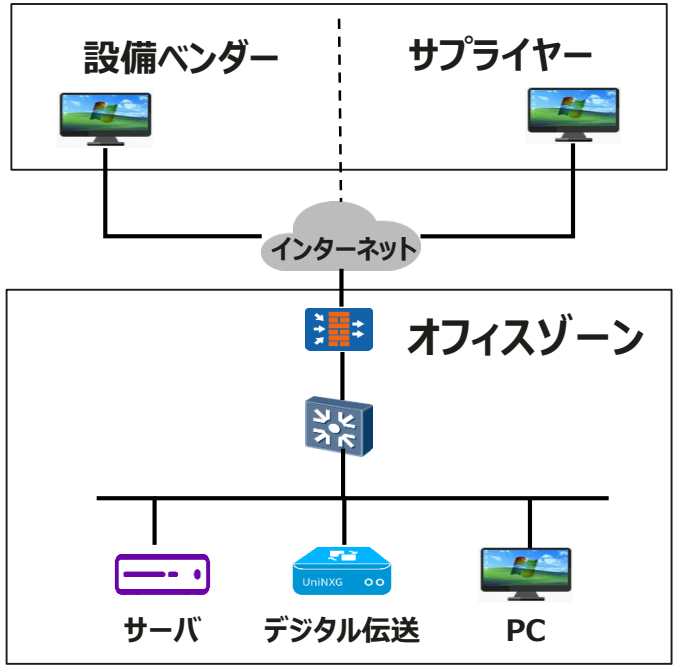
データ伝送システム:クロスネットワークファイルの安全な交換

①セキュリティゾーン間のファイルの安全な交換



- 高機密性ネットワークと低機密性ネットワークを通じて、ファイルの受け渡しだけを許可し、ネットワーク通信を許可しないことにより、ネットワーク攻撃を効果的に遮断。
- ファイルは転送と保存の全プロセスで暗号化され、より安全である。
- 機密ファイルを検出した場合、自動的に承認プロセスに入って、OAシステムと接続する。プロセスが完全に自動化され、ファイルの転送がより効率化。
- ファイル交換プロセスを完全に記録し、トレサビリティを可能に。

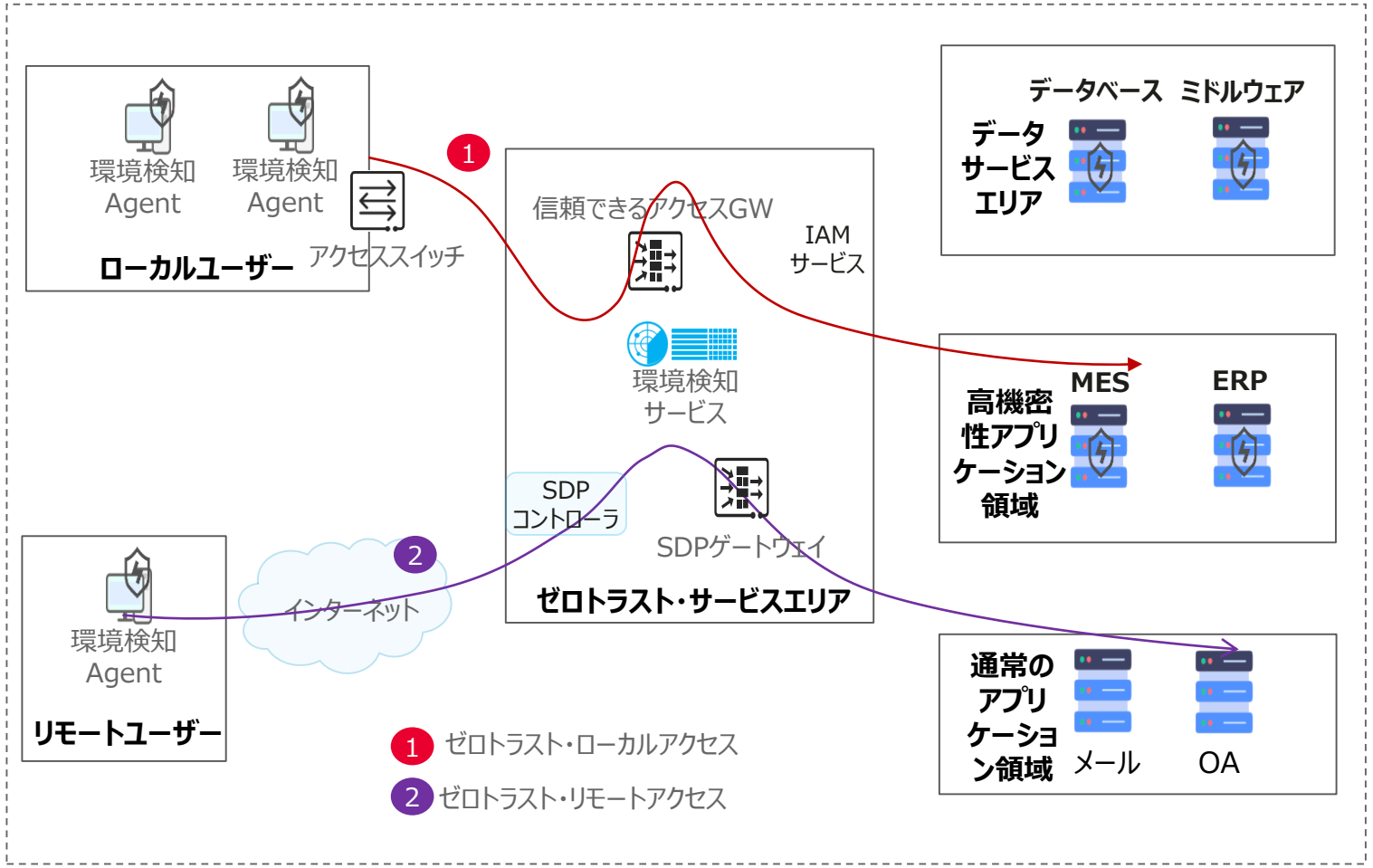
②インターネット経由ファイルの安全な送受信



- 外部ファイルリンク技術を通じて、サプライヤーとの間のファイルの安全な送受信を実現。
- インターネットでファイル共有する際に、HTTPS暗号化技術を使用し、大容量ファイルの転送とダウンロード再開がサポートするため、より効率的でファイル転送を実現。
- データ転送で受信したファイルを、ローカルでウイルススキャン、安全性を確保した後、クラウドにコピー。
- 権限管理、高機密ファイルを送受信して画面録画をトリガーし、トレサビリティを確保。

HUAWEI

ゼロトラスト:ローカルとリモートユーザーが安全にアプリケーションとデータにアクセスできる



ゼロトラストの概念

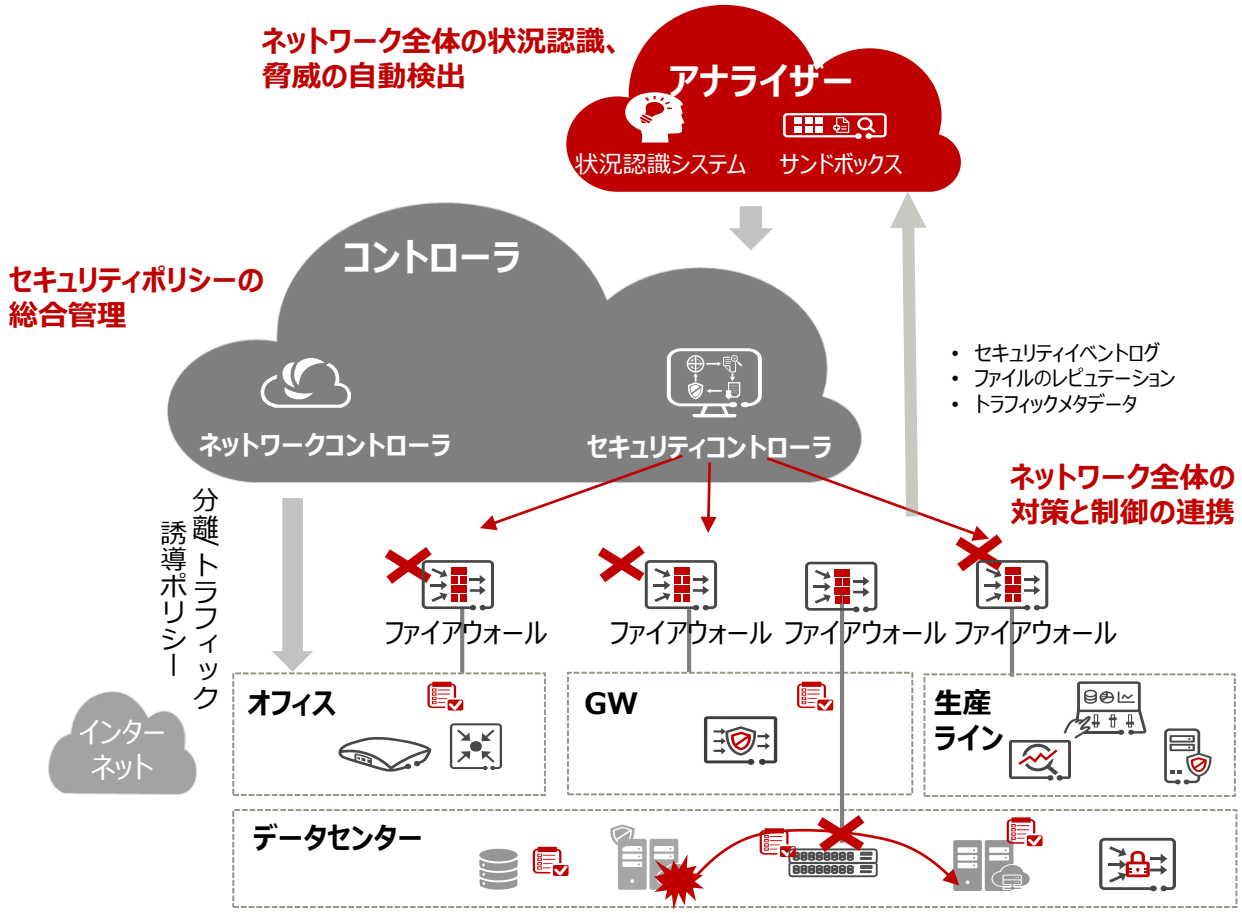
IDを中心とし、信頼できないネットワーク環境において、持続的な環境検知と動的ポリシー管理により、きめ細かなアクセス制御を実現し、エンドポイント、ユーザー、ネットワーク、アプリケーション、データからエンドツーエンドの信頼チェーンを構築し、信頼できるデータ転送を実現。

ソリューション

- ✓ **ゼロとロスト・ローカルアクセスアプリケーション:** ローカルユーザーはまず信頼できるアクセスGWによって認証を行い、ユーザートークンとアプリケーショントークンを取得する。アクセスGWはトークンを携帯してIAMに検証要求を開始し、IAMはエンドポイントセキュリティスコアと権限情報を確認し、アクセス権限があればアクセスGWに許可を通知する。
- ✓ **ゼロトラスト・リモートアクセスアプリケーション:** SDPコントローラを実装し、認証してからアクセスする。正当な端末は効率的にアクセスし、不正端末は遮断される 。

HUAWEI

スマートQ&M:多層防御、脅威の迅速な検知と対処、生産安全を確保



脅威の迅速な追跡、発生源近くで遮断

ソリューション

全量収集、リアルタイム監視:プローブは全域流量を収集する。サンドボックスでリアルタイムに報告されたファイルをチェック/分析。状況認識システムはセキュリティログを受信し、未知の脅威を検出。

ネットワークセキュリティ連動、数分で遮断:状況認識システムによりネットワーク全体のログ、トラフィックメタデータ、ファイルを収集し、ファーウェイ特許のAIアルゴリズムを使用して未知の高度な脅威と攻撃源を迅速に検知。ネットワークコントローラとセキュリティコントローラに連動ポリシーを配信し一元的なスケジューリングとオーケストレーションを行う。さらにセキュリティポリシーをスイッチとファイアウォールに送信し、発生源で遮断し、脅威の拡散範囲を抑える。

ランサムウイルス検出例：

1、インターネットからメール経由でランサムウイルスを送信する。

2、ファイアウォールはトラフィックの監視により、感染ファイルをサンドボックスに連携。

3、サンドボックスで脅威分析を行い、変異ウイルスがPC1に侵入。

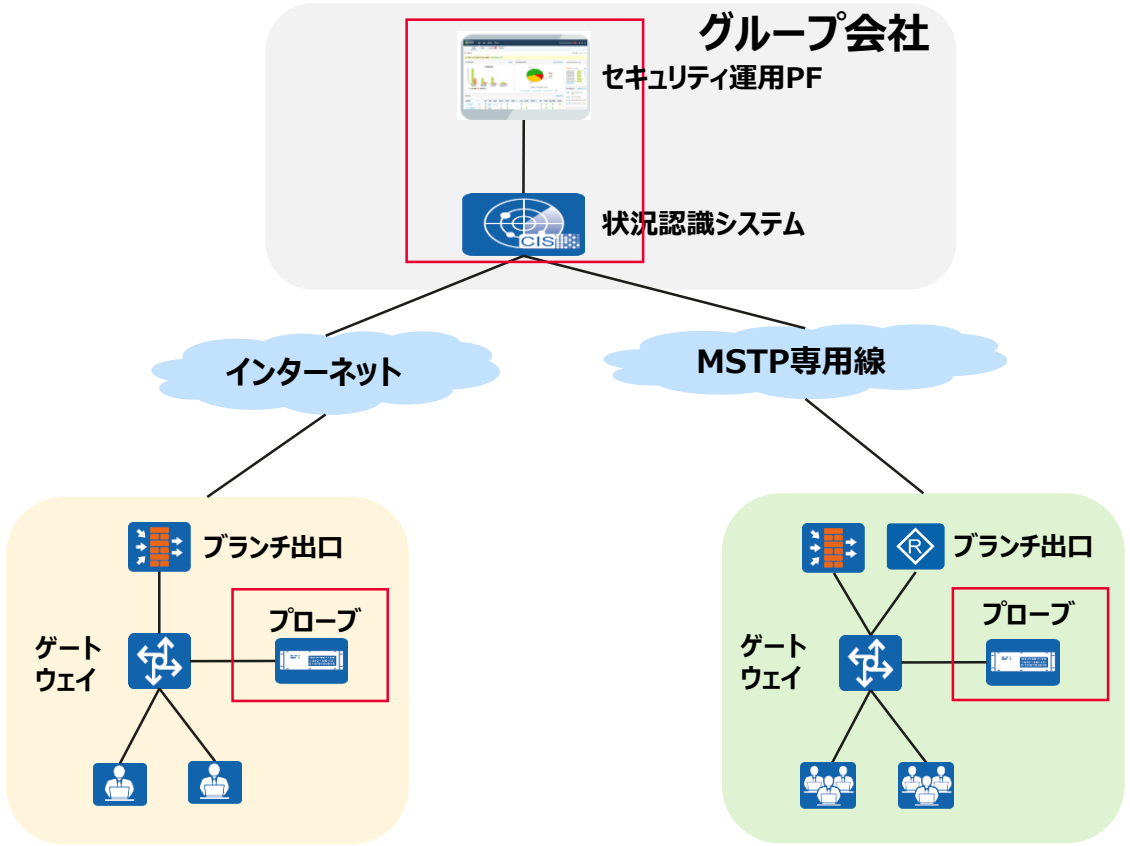
4、ファイアウォールとEDRはサンドボックスから検出結果を取得する。

5、ファイアウォールは同期結果に基づいて後続の攻撃を遮断し、EDRはネットワーク全体で不正ファイルを遮断・除去。

HUAWEI

ブランチのセキュリティ:セキュリティ状況全般の画面表示、連携対処できるため、グループ全体のセキュリティレベルを高めている

- グループ会社は状況認識システムとセキュリティ運用プラットフォームを配置し、作業指示システムと連携させる。ブランチにはプローブを実装する。
- ビッグデータとAI技術を活かして、早期警報、通報、緊急指令機能を一体化し、本社と支社間の一元的セキュリティ運用管理プラットフォームを構築。



セキュリティソリューション

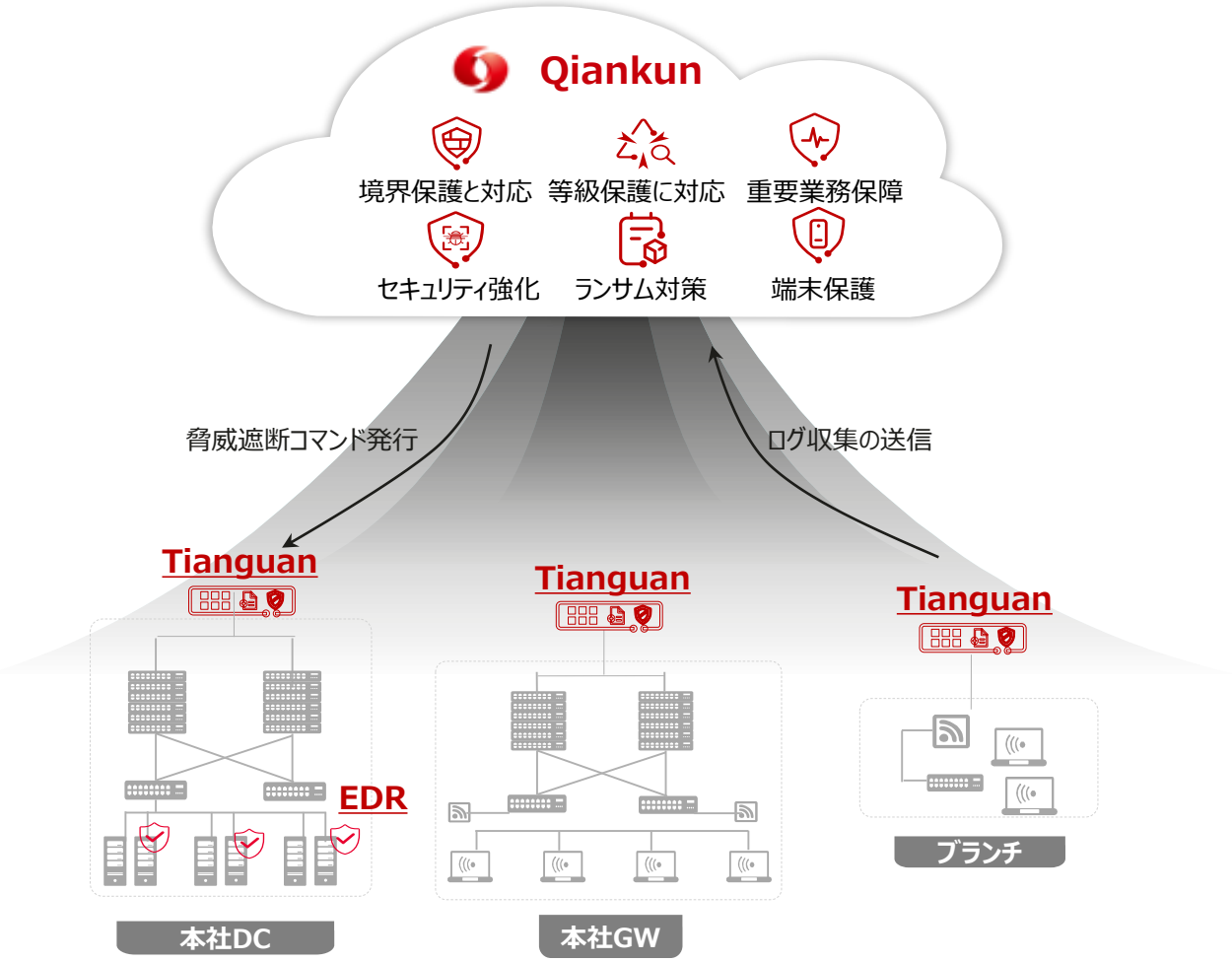
- **プローブ**をコアスイッチの隣に配置し、コアスイッチにポートミラーリングを設定し、東西トラフィックと南北トラフィックをプローブにミラーリングする。
- プローブはトラフィックに対して脅威検出と不審トラフィック分析を行い、侵入とウイルスの拡散などを検知し、脅威ログとトラフィックのメタデータを生成・暗号化して本社の状況認識システムに送信。状況認識システムはAIアルゴリズム、脅威情報分析などにより、ランサム攻撃やAPT攻撃などの高度な脅威を検出する。
- アナライザーによって脅威が検出された後、プローブはフォレンジック機能を起動し、生成された攻撃メッセージをグループの状況認識システムに送信してセキュリティ分析及びフォレンジックを行う。

お客様の価値:

- **ブランチトラフィックを収集し、脅威イベントを検出。**
- **作業指示システムと連携してすばやく処理、収束させる。**
- **フォレンジック調査で、ブランチのセキュリティ構築を促進。**

HUAWEI

Qiankun（乾坤）セキュリティサービス:クラウド・エッジ・エンドポイントの一体化構造、オンデマンドでサービス購入、脅威の自動処理を可能に



乾 Huawei Qiankun

スマート分析+脅威情報+クラウドエキスパート

- **スマート分析:**セキュリティログとフォレンジックファイルの関連分析により、攻撃イベントを正確かつ迅速に処理。
- **セキュリティサービス:**実際のセキュリティニーズに基づいて、様々なセキュリティクラウドサービスを継続的に進化させる。
- **クラウド専門家:**セキュリティエキスパート、7*24時間連続オンラインサービス。

坤 Tianguan+EDR

エンドポイント保護+トラフィック検出+自動処理

- **境界防御(Tianguan、天関):**シグネチャDBのリアルタイム更新。外部からの攻撃や故障したホストを検出し、自動的にブロック。
- **エンドポイント検出と対処(EDR):**資産管理、ウイルス対策、ランサム対策、侵入検知、攻撃からの復旧。

お客様の価値:

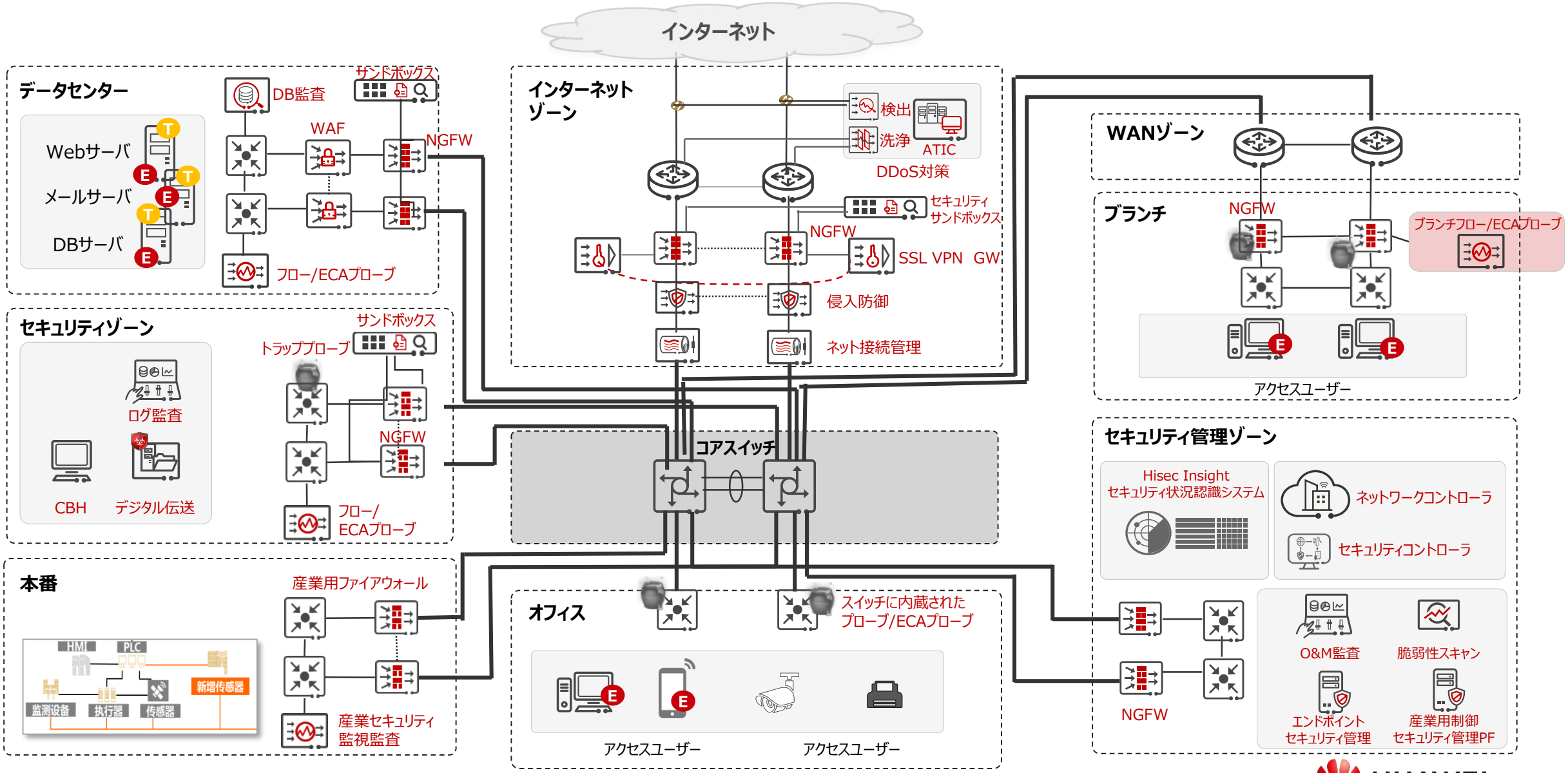
- 一台で等級保護要件2級を満たす。
- 脅威の自動処理、人の操作が不要。
- セキュリティのサービス化、セキュリティ機能のオンデマンド購入。

製品構成

- 製品:Tianguan、EDR
- サービス:境界安全(必須)、脆弱性スキャン(推奨)、重点業務保障(推奨)、ランサム対策(推奨)。

HUAWEI

スマート製造セキュリティソリューションの導入全容



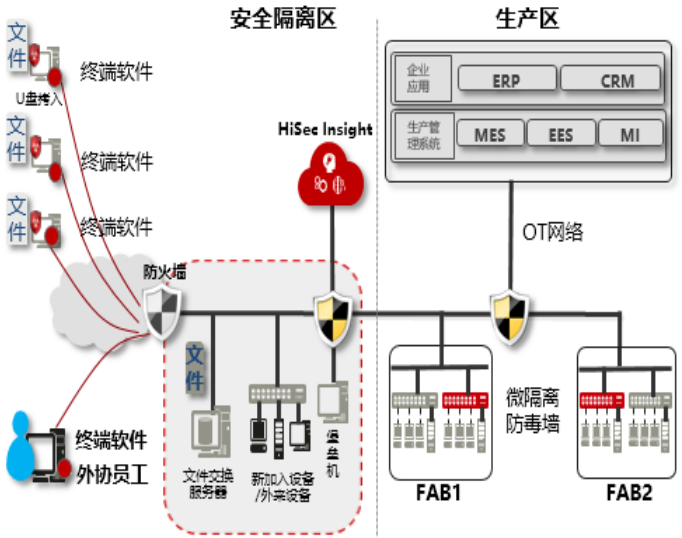
HUAWEI

事例:XX南方工場、産業用インターネットセキュリティにおける取り組み

課題

- **難しい検知:**未知のマルウェア、0dayの脆弱性を悪用し、検知が難しい。
- **すばやい拡散:**マルウェアが侵入すると、ワームはイントラネット内ですばやく広まる。
- **長時間化:**攻撃を検出してからリスクをブロックするまでに時間がかかりすぎる。

ネットワークトポロジー



ソリューション

予知保全:AIFW+マイクロ隔離+サンドボックス、事前に保護措置を取り、ハッカーの侵入を食い止めるか、攻撃時間を遅らせる。

リアルタイム監視:グローバルな状況認識、インシデント中の監視、ハッカーの挙動の可視化、攻撃行動をすばやく発見。

善後策:ネットワーク・セキュリティの連携、善後策、調査、追跡、セキュリティポリシーの最適化、保護レベルの向上。

お客様の価値

平均検出率:	60% [シグネチャベース]	96% 【AI】
迅速な検出:	日レベル	分レベル
追跡処理:	日レベル	秒レベル

Thank you.

把数字世界带入每个人、每个家庭、
每个组织、构建万物互联的智能世界。

Bring digital to every person、 home and organization for a fully connected、 intelligent world.