MANUFACTURING

製造業向け
ネットワーク
ソリューション
ガイド

製造DXに向けた工場インフラ構築とガイドラインに基づくセキュリティ対策

Allied Telesis

2023.08版

工場インフラの整備・活用に向けて

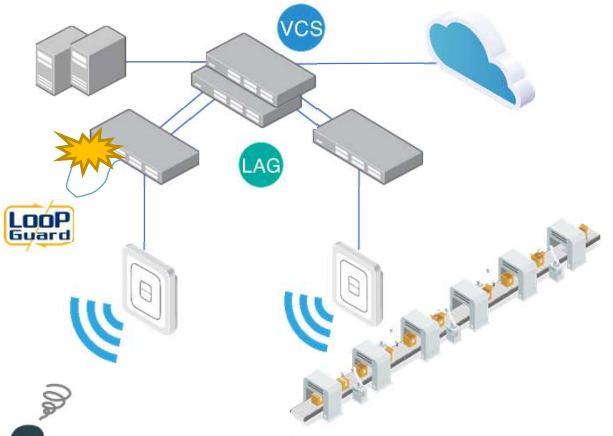
製造市場では、人口減少に伴う労働力不足を解決するために、「自動機やロボットの導入による自動化・省人化」や「IT・IoT・ビッグデータ・AIなどの活用による生産工程の合理化」など、製造DX推進に向けた取り組みが進められています。スマートファクトリーの実現には、IoTの導入や、それらの様々なデータを利活用できる安定したネットワーク環境の構築が不可欠です。

また、昨今の工場ネットワークはクラウドやサプライチェーンのシステムとの接続など、インターネット接続によるセキュリティリスクも増加しています。経済産業省より公表されている「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」に基づき、サイバー攻撃に備えた対策や運用も検討していく必要があります。

現状の課題と工場ネットワークに求められる要件

止まらないネットワーク

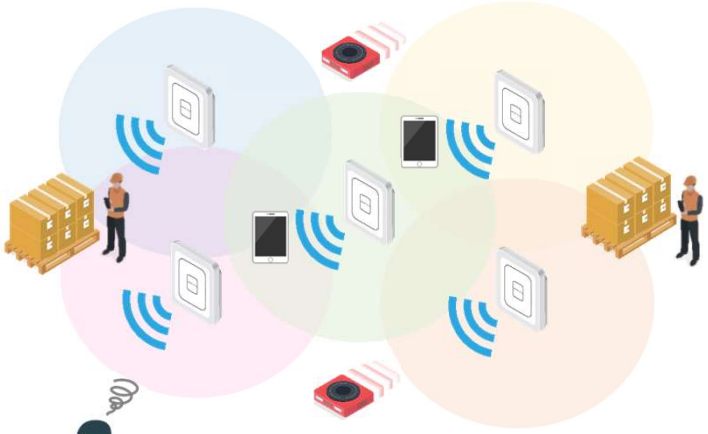
24時間365日生産ラインが止まらない
安定したネットワーク



情報系／設備系のネットワークともに
遅延や停止が許されない・・・

安定した無線LAN

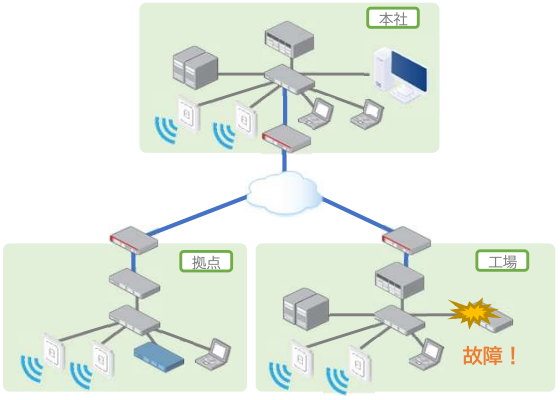
工場内の様々な電波との干渉を防ぎ
AGVなどの移動端末も最適に繋がるWi-Fi環境



電波干渉も気になる上、移動端末の通信
が途切れることも多々ある・・・

容易な運用管理

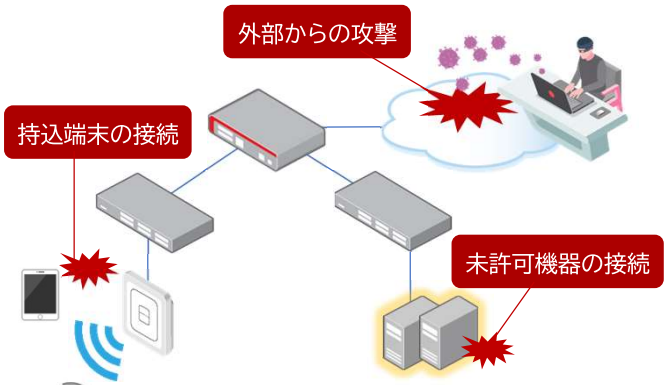
本社・拠点・工場など複数のネットワークを
まとめて管理し、管理者の負担を軽減



情報システム担当者が常時いないから
万一の時にすぐに対応できない・・・

セキュリティ対策

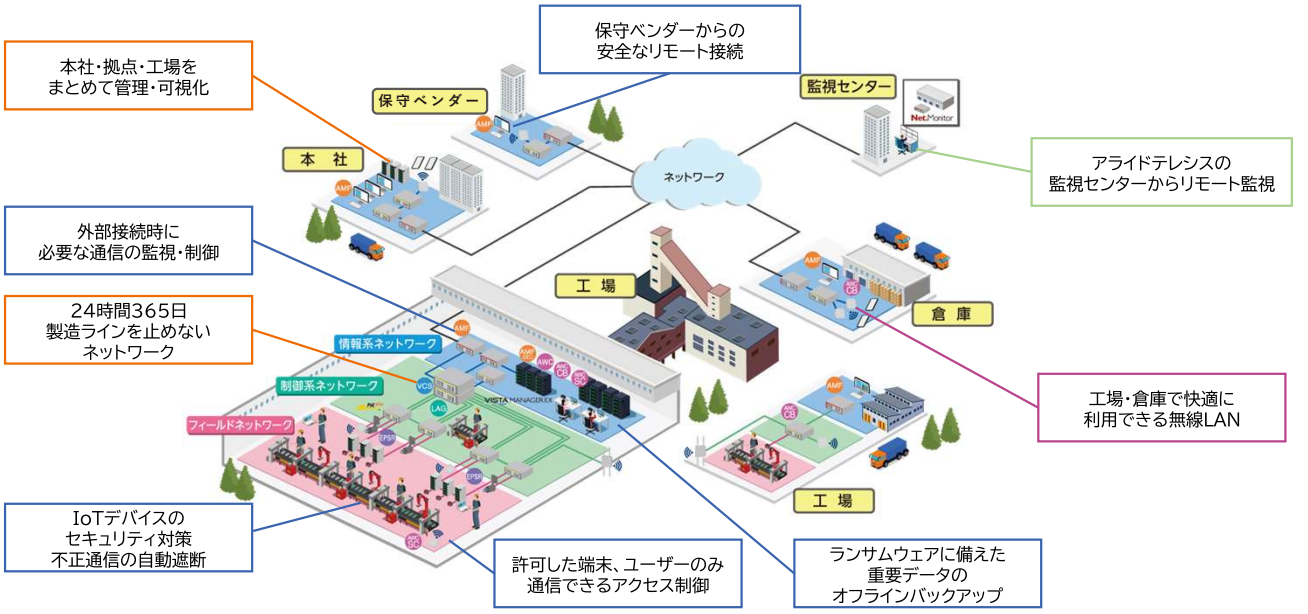
許可デバイスのみ接続させるアクセス制御と
多発するサイバー攻撃への対策



現状のネットワークでどこまでセキュリティ
対策が必要なのか分からない

Copyright© 2023 Allied Telesis K.K. All Rights Reserved.

工場ネットワークのポイント



Ⅰ 安定したインフラの構築

① 止まらないネットワーク
② 安定した無線LAN環境
③ ネットワークの運用管理

Ⅱ ガイドラインに基づくセキュリティ対策

① セキュリティ対策・企画導入の進め方
② ガイドラインで求められている対策
③ 運用体制の見直し・セキュリティ教育

Ⅰ 安定したインフラの構築

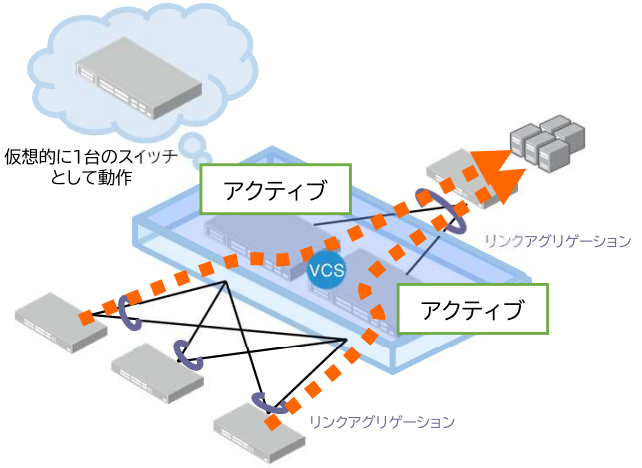
1 止まらないネットワーク

24時間365日生産ラインを止めないネットワーク技術

機器の冗長化（VCS）

VCS(Virtual Chassis Stacking)

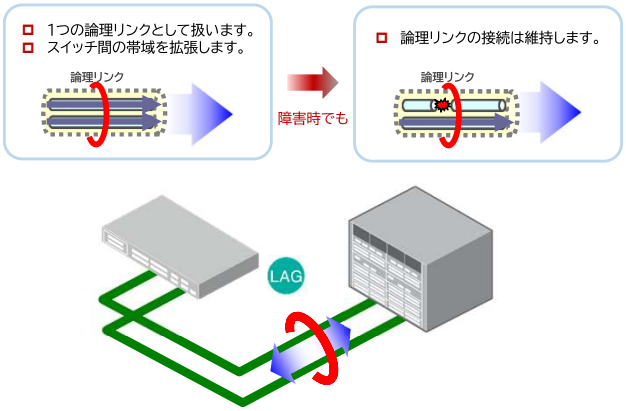
複数スイッチを仮想的に1台とすることで、低コストかつ簡単に負荷分散型冗長ネットワークを実現。経路の切り替わりが最短0.5秒で可能となり、ダウンタイムを最小化。



経路の冗長化（LAG）

LAG(Link Aggregation)

複数の物理ポートをグループ化することで、スイッチ間の帯域幅を拡大しつつ、リンクの冗長性を高める機能。



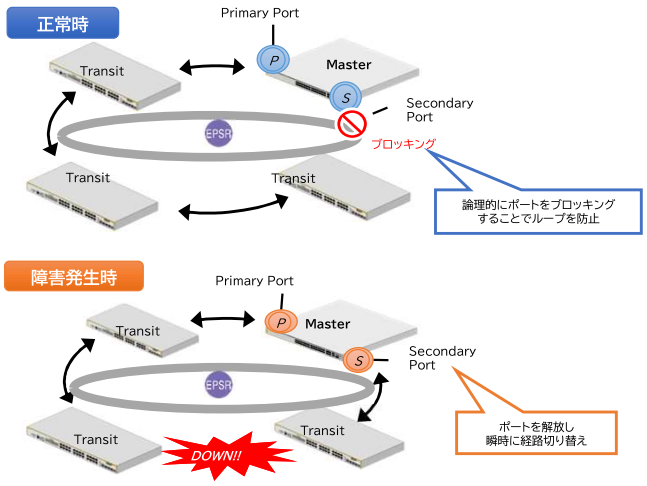
論理リンクを構成する物理リンクの一つが切断された場合も、残りの物理リンクにて通信を行なうことが出来ます。

Copyright© 2023 Allied Telesis K.K. All Rights Reserved.

経路の冗長化（EPSR）

EPSR(Ethernet Protected Switched Ring)

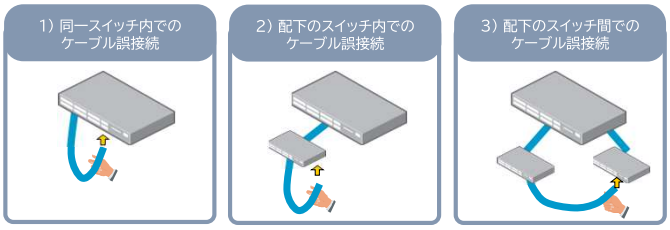
リング構成のネットワークに特化した レイヤー2のループ防止・冗長化機能。各スイッチの役割をあらかじめ固定しておくことで、障害の検出と経路の切替をより高速に実現。



ループ対策

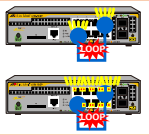
ループガード

特殊フレームを利用してネットワーク上のループを検出。ループが発生しているポートはLEDの特殊な点灯で分かりやすく通知。



機器単体でのループ以外の検出も可能

ループガードのアクション実行中のポートが赤や緑に点滅後、全ポートのLEDが赤や緑に点滅する等の動作を繰り返し、ループしている筐体とポートを知らせます。



2 安定した無線LAN環境

製造現場のDXを促進するIoT活用に欠かせないWi-Fi環境

作業の自動化・データの収集・蓄積・活用による生産性の向上を目指して様々なIoTデバイスの活用が進んでいます。これらのデバイスを安定利用するためには、最適な無線LAN設計が必要です。

AWC 「遅い」「途切れる」「つながらない」を解決〈自律型無線LAN〉

電波の自動調整

AWC CB 移動中も途切れず快適に〈シングルチャンネル無線LAN〉

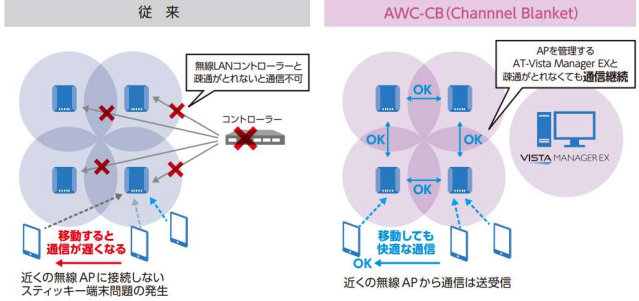
ブランケット方式
（アライド独自）
全ての無線APで同一チャンネル

単一チャンネルでローミング・電波干渉なしローミングのパケットロスや遅延はない
⇒ 移動端末には最適

ローミングレス

同一チャンネルを使いSSIDを同期し、仮想的な1台として動作

電波の強いAPが自動的にデータ転送を行い、同一チャンネル内の隣接しないAPであれば同時通信が可能



ポイント　従来の方式では、端末側がAPを選択して接続していましたが、AWC-CBでは端末の動作に依存せず、電波の強いAPが自動的にデータを転送するため、ローミングやスティッキー問題を解決します。

Copyright© 2023 Allied Telesis K.K. All Rights Reserved.

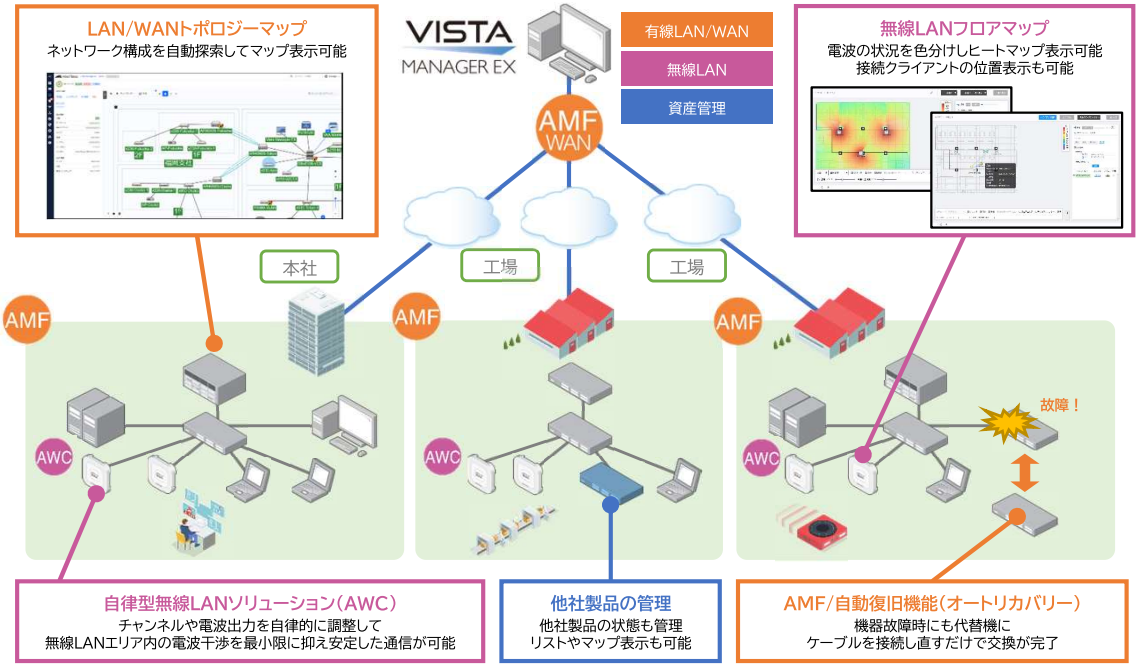
3 ネットワークの運用管理

ネットワーク統合管理機能 AMF

- 従来、個別に設定/管理していたネットワーク機器を一元管理する機能
- ネットワークの構築・運用・管理に必要となるコストや技術スキルを大幅削減

ネットワーク統合管理ソフトウェア Vista Managerシリーズ

- 大規模かつ複雑な工場のネットワーク状況をひと目で確認可能



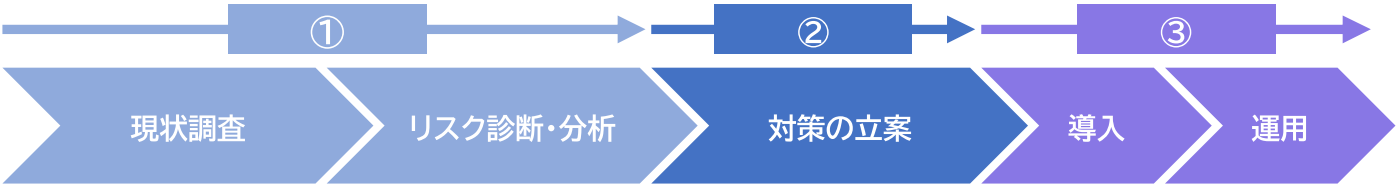
Ⅱ ガイドラインに基づくセキュリティ対策

1 ガイドライン対策・企画導入の進め方

各段階で定義されている内容に沿って調査・検討

工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン

①：工場内にあるデバイス、ネットワークの状況把握とリスク分析
②：セキュリティリスクに対する対策の具体的な検討
③：対策の導入と日々の運用・万一のインシデント発生時の体制整備



基本情報把握

- 業務内容の確認・整理
- 情報資産・現状把握
- デバイス/システム構成運用の確認
- 現状のセキュリティ体制・ポリシーの把握

リスクの洗い出し

- 現状の対策状況の可視化
- 保護対象の整理
- 現状の課題・存在するリスクの洗い出し

対策の検討

- 現状の対策とガイドラインに基づく対策との比較
- リスク評価と必要な対策の優先順位付け
- 対策の立案
- 対策の具体化

導入・運用

- 情報資産・デバイスの台帳化
- 定常的なモニタリング
- セキュリティ教育
- 定期的な脆弱性診断
- 取引先や調達先(サプライチェーン)への対策要請と状況確認

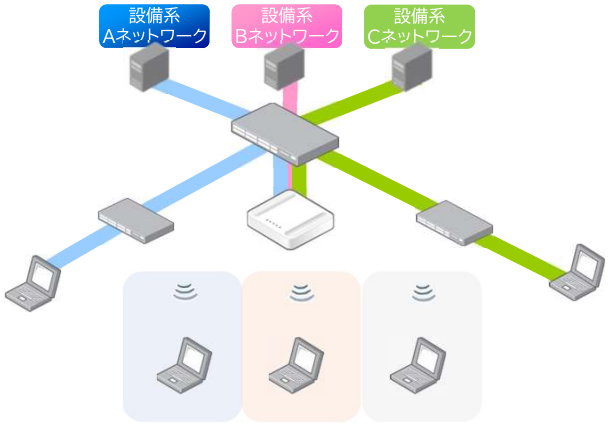
Copyright© 2023 Allied Telesis K.K. All Rights Reserved.

2 ガイドラインで求められている対策

ネットワークの論理分離

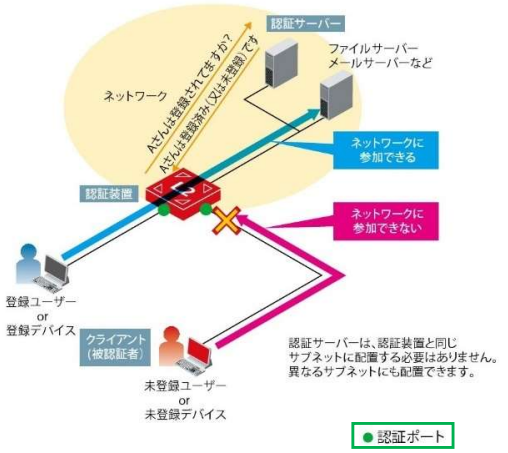
VLAN(Virtual LAN)

▸1台のスイッチで複数のネットワークを論理的に分離し物理分離よりも低い機器コストで構成が可能。
またセグメントを分割することでセキュリティも強化



端末/ユーザーの認証

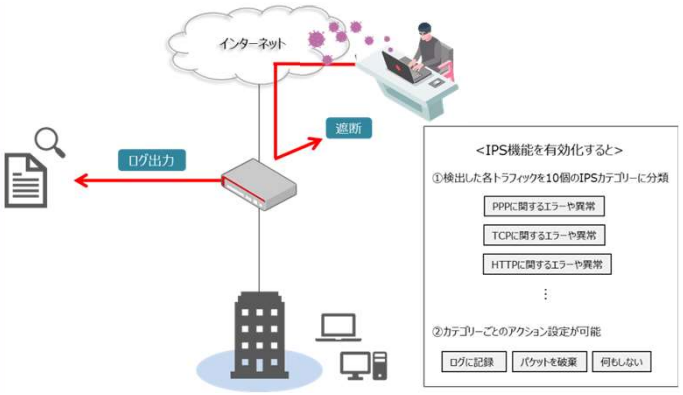
▸許可した端末/ユーザーのみ通信可能となるように制限
▸MACアドレス認証/Web認証/IEEE 802.1X認証/ワンタイムパスワード認証などがあり、端末によって認証方法を選択・組み合わせて設定



Firewall／UTM

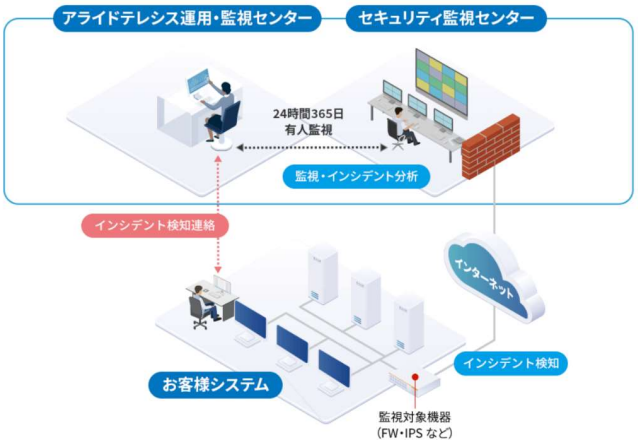
IDS(侵入検知)/IPS(侵入防止)

▸サービス妨害や不正アクセスを検知・防御するシステム
→“ログ出力”による検知や、通信遮断による外部の攻撃からの防御が可能に



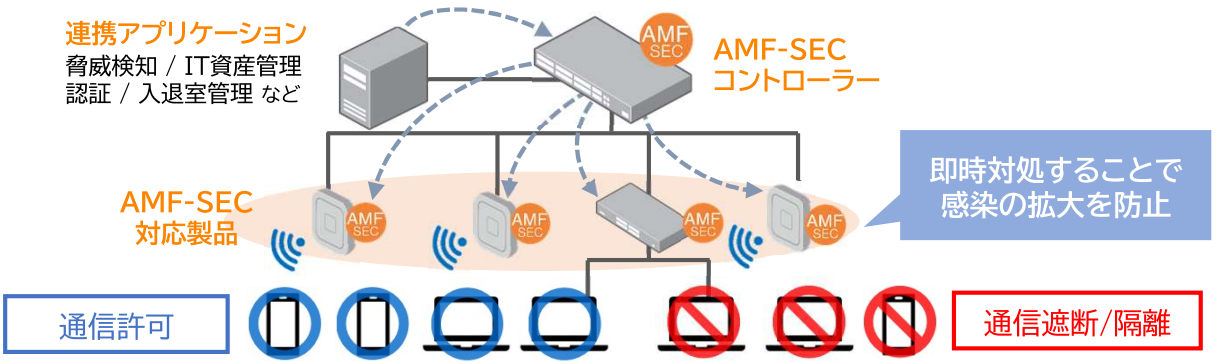
ログ管理(MSSサービス)

▸お客様ネットワーク内のセキュリティデバイスから出力される重要なログを、専門知識を持ったセキュリティアナリストが24時間365日リアルタイムで分析を行い、精度の高いインシデント対応情報を報告



ネットワーク自動制御ソリューション

▸ パートナー各社のアプリケーションと連携し、外部からのサイバー攻撃や内部犯行による情報漏えい対策として、「認証」「隔離」「遮断」などネットワークの自動制御を行う

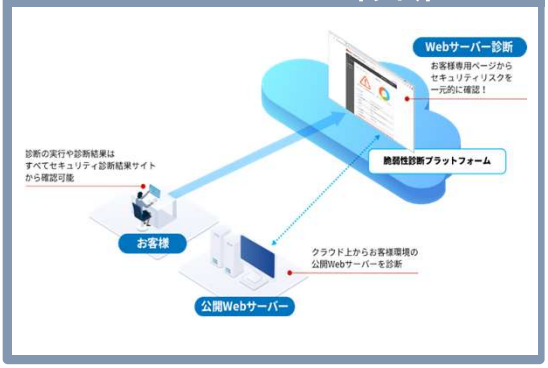


Copyright© 2023 Allied Telesis K.K. All Rights Reserved.

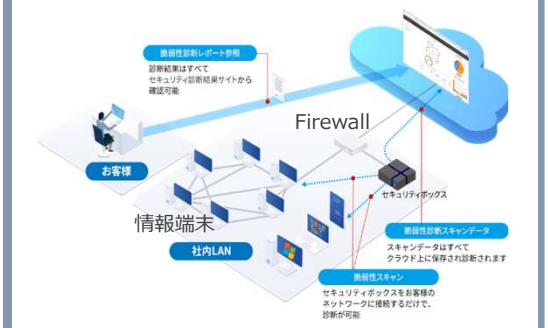
脆弱性診断・通知サービス

- クラウド上からお客様のWebサーバーやLANシステム内に接続されているIP機器の脆弱性を診断
- 脆弱性通知サービスでは、契約対象機器の脆弱性を検出し、お客様へメール通知も可能

Webサーバー診断



LANシステム診断

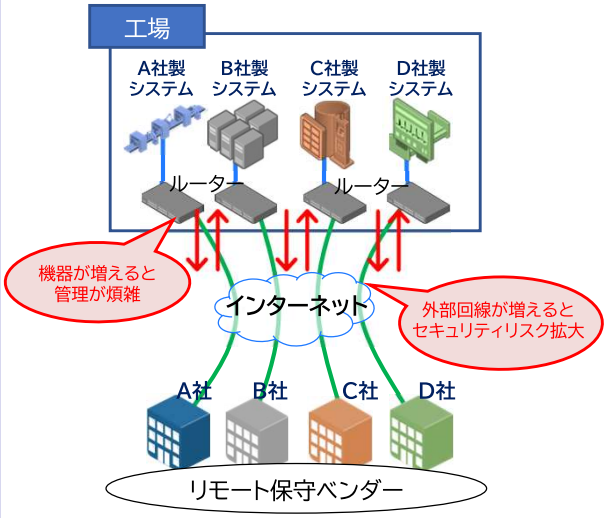


リモートメンテナンス環境の整備

- 外部接続点を集約することで、リモート接続を一括管理でき、接続ログの確認が用意に
- 脆弱性管理の対象数を限定することで、運用工数を大幅削減

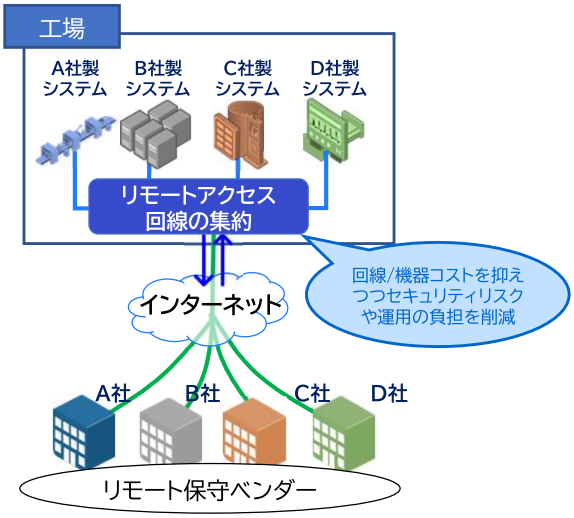
課題

保守ベンダーごとの環境で負担増加



対策

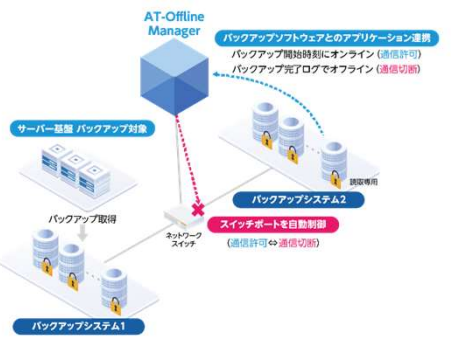
リモメン回線、装置を集約して負担軽減



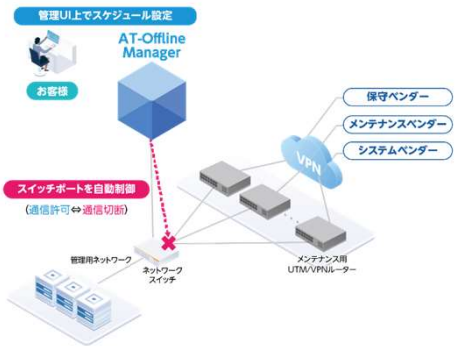
ランサムウェア対策 オフラインバックアップ

- 万一のインシデントや滅失に備えたデータバックアップソリューション
- バックアップ環境をネットワークで自動オフライン化することが可能に

日々のバックアップデータをオフライン化



メンテナンス環境をオフライン化



Copyright© 2023 Allied Telesis K.K. All Rights Reserved.

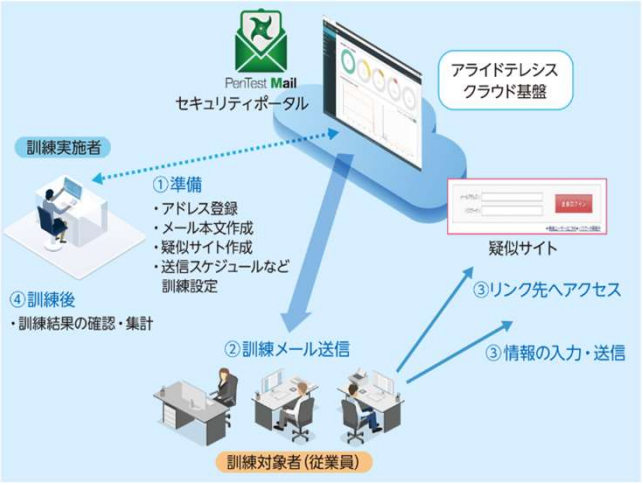
3 運用体制の見直し・セキュリティ教育

サイバー攻撃の早期認識と対処／従業員へのセキュリティ教育

運用・管理面のセキュリティ対策として、万一に備えたインシデント対応フローやセキュリティ教育が重要です。

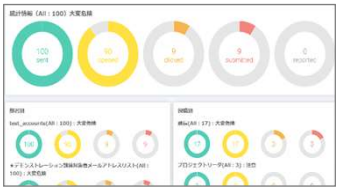
フィッシングメール訓練

- クラウド上に用意された管理画面（セキュリティポータル）から、訓練用のメールを送信
- フィッシングメール訓練を実施し、結果を即時集計・可視化することが可能



簡単訓練設定ウィザードですぐに訓練開始！
フィッシングメール雛形、疑似フィッシングサイトを用意

訓練結果がわかりやすいダッシュボード
部門別、役職別結果表示



情報セキュリティ研修

- 定期的な従業員へのセキュリティリテラシー教育の実施と組織におけるインシデント発生に備えた体制作り

Step 1 一般従業員向け情報セキュリティ基礎／フィッシングメール基礎／ランサムウェア基礎

Step 2 インシデント対応教育・訓練コース（全6コース）
予め決まった演習シナリオで
基礎フロー教育・訓練

Step 3 カスタマイズコース：団体全体向け
要件ヒアリング実施後、お客様環境に
合わせたシナリオ開発（2-3か月）

様々な受講形態

- 集合型研修
（講義・実機演習）
- オンライン研修
（講義のみ）
- e-learning研修
（動画教材の視聴）

幅広いコース提供

- 初級・中級・上級と
スキルアップを目指した
コースの受講が可能
- 専門的、技術的な
スキル取得が可能

LMSによる学習管理

- 受講コース一覧の表示
- テキストの配布
- 試験の実施・結果確認
- 合格証書
認定ロゴ提供
（※一部のコース）

ネットワーク構築などのご質問やご相談、その他のお問い合わせ
https://www.allied-telesis.co.jp/contact/

アライドテレシス株式会社
〒141-0031東京都品川区西五反田7-21-11 第2TOCビル TEL.03-5437-6000（大代表）
https://www.allied-telesis.co.jp/

●CentreCOM、SwitchBlade、Secure EnterpriseSDN、AMFramework、 AMFPlus、 VCStack、EPSRing、LoopGuard、AlliedView、AT-Vista Manager、AT-VA、AT-UWC、Allied Telesis Unified Wireless Controller、EtherGRID、Envigilant、Net.Service/ネット・ドット・サービス、Net.Cover、Net.Monitor、Net.Assist、アライド光は、アライドテレシスホールディングス（株）の登録商標です。●その他の会社名、商品名は、各社の商標または登録商標です。 ●内容は改良等のため予告なく変更される場合があります。●記載されている内容を許可なく使用、複製、複写、改変、加工、転載等することを禁じます。