医療機関向け無線LAN環境サイバーセキュリティ対策ご案内

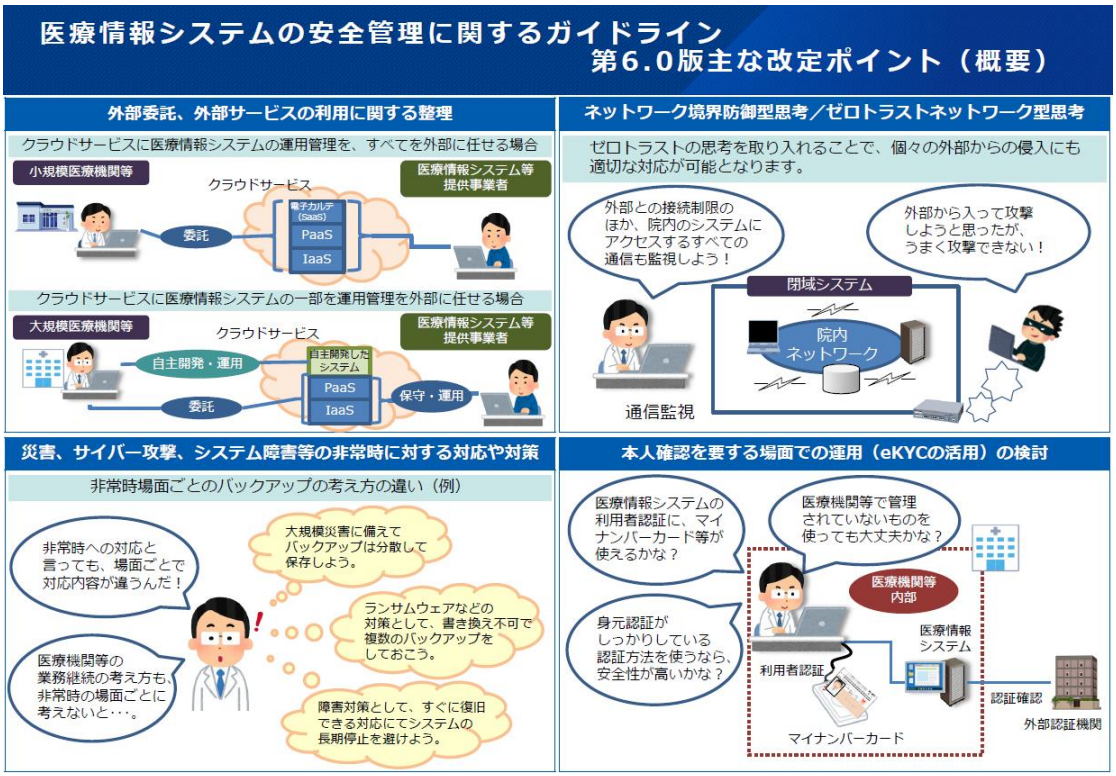
手を緩めることが出来ない高度化・巧妙化したサイバー攻撃への対策は医療機関の皆様にとって日々の課題となっております。

医療機関を狙ったサイバー攻撃は、2021年頃から増加傾向にあります、そのなかでも、電子カルテなどを標的とするランサムウェアによる攻撃が増加しています。
(警察庁の統計によりますと、2022年に報告されたランサムウェアの被害件数230件のうち、医療機関は20件)

これらランサムウェアなどのサイバー攻撃は、無線LANを経由した侵入も報告されております、皆様が実施しておられるサイバー攻撃対策への見直し等に本内容をご検討いただければ幸いです。

背景：厚生労働省　医療情報システムの安全管理に関するガイドライン　第6版

厚生労働省は2023年(令和5年)からマイナンバーを健康保険証として利用するためのオンライン資格の導入を義務化したことにより、医療業界におけるサイバー攻撃対策の重要性を呼びかけています。
これに関連して、「医療情報システムの安全管理に関するガイドライン第6版」が発行されました。



出典:https://www.mhlw.go.jp/content/10808000/001102597.pdf

株式会社 アイサン情報システム
〒103-0016　東京都中央区日本橋小網町6番1号　山万ビル12階
Tel: 03-5614-5177　| E-mail: cyber@aisan-is.jp

ガイドライン：ネットワーク境界防御型思考/ゼロトラストネットワーク型思考の実装

医療機関においても無線LANを日常的にご利用されている一方で、管理者が認識していない端末(無線LAN機能も持った医療機器等)やゲスト無線LAN環境などの状況把握については、十分ではないことが現状です。

ソリューションのご紹介 (AirEye)

aireye | The **Leader** in Network Airspace Control and Protection (NACP)

無線LAN環境の可視化と無線LANを使ったサイバー攻撃の防御

すべての無線LANを監視
すべての無線通信をリアルタイムで監視、分析

特定と分類
端末等とネットワークを分類

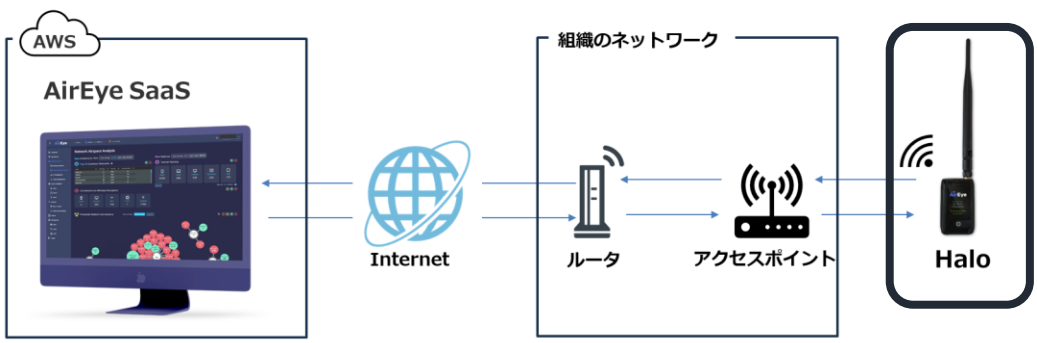
コントロール
セキュリティのルール違反を検出し、デバイス間の危険な接続を自動的に切断

防御
悪意のある接続を検出し、攻撃を停止

フォレンジック
攻撃の詳細と関与するデバイスを特定

AirEyeの構成と設置

既存の環境に「Halo」を設置するだけで構築完了です !!



株式会社 アイサン情報システム
〒103-0016 東京都中央区日本橋小網町6番1号 山万ビル12階
Tel: 03-5614-5177 | E-mail: cyber@aisan-is.jp

教育機関向け無線LAN環境サイバーセキュリティ対策ご案内

ICTを活用した教育の効果を上げるため、大学などの高等教育機関のキャンパスにおいてはBYOD(Bring Your Own device)による授業に移行しているケースの多く見られます。このような環境を支えているインフラストラクチャとして無線LAN環境が大きな存在となっています。

また、情報セキュリティ対策により、重要情報を内部・外部の脅威から守りながら、教育環境を質を下げない取り組みも推進しなければなりません。

昨今のサイバー攻撃対象の80%は教育機関に何らか関係しているとのデータもあります。本ソリューションは教育機関における継続したサイバーセキュリティ対策として活用いただけます。

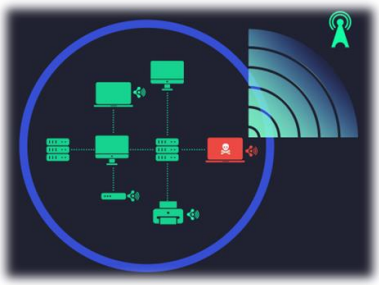
データ：公表されている大学のサイバーセキュリティインシデント

全国大学法人数790に対して、
2022年度は約20大学法人がインシデント発生を公表

*インターネット上など、パブリック情報として公表されたものを独自にカウント

市場トレンド：無線LANを経由したサイバー攻撃の可能性

組織ネットワークへの不正アクセス



データ漏洩

ネットワーク機器の乗っ取り

無線LAN環境に対する、
可視性およびコントロールの向上の必要性が高まっています。

株式会社 アイサン情報システム
AISAN

〒103-0016　東京都中央区日本橋小網町6番1号　山万ビル12階
Tel: 03-5614-5177　| E-mail: cyber@aisan-is.jp

aireye | The **Leader** in Network Airspace Control and Protection (NACP)

無線LAN環境の可視化と無線LANを使ったサイバー攻撃の防御

すべての無線LANを監視
すべての無線通信をリアルタイムで監視、分析

特定と分類
端末等とネットワークを分類

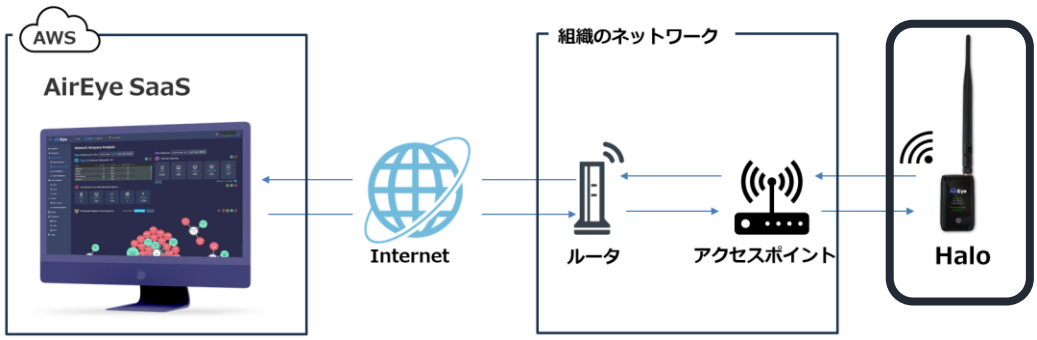
コントロール
セキュリティのルール違反を検出し、デバイス間の危険な接続を自動的に切断

防御
悪意のある接続を検出し、攻撃を停止

フォレンジック
攻撃の詳細と関与するデバイスを特定

AirEyeの構成と設置

既存の環境に「Halo」を設置するだけで構築完了です !!



株式会社 アイサン情報システム
〒103-0016 東京都中央区日本橋小網町6番1号 山万ビル12階
Tel: 03-5614-5177 | E-mail: cyber@aisan-is.jp

工場システム向け無線LAN環境サイバーセキュリティ対策ご案内

工場システムはインターネットへ直接接続されないことを前提に設計されていました。しかしながら、昨今のDXやスマートファクトリーの流れを受け、工場システムにおいて、IoTなどの利用が進んできたことによるインターネットへの接続が定常的に必要になっています。

一方で、これら新しい環境において、手を緩めることできないサイバーセキュリティ対策を同時に検討する必要が出てきております。

本ご案内は、工場システムで稼働する無線LAN環境へのサイバーセキュリティ対策にフォーカスを当てた内容となっております。

背景：経済産業省　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

2022年11月に経済産業省より、工場でのIoT化によりネットワーク(インターネット)接続機会の増加によりサイバー攻撃のリスクが増加していることに対するガイドラインとして発行されました。

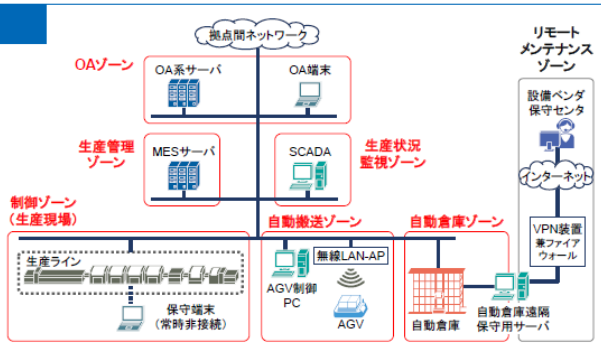
ガイドラインの目的

- 工場をインターネット等のネットワークにつなぐことによるセキュリティリスクが増加。
- 工場DXに伴い、クラウドやサプライチェーンのシステムと直接接続された工場におけるセキュリティも考慮する必要。
- インターネット接続の機会に乏しい工場についても不正侵入者等による攻撃を受ける場合もある。
- 攻撃の態様により、特定の工場が狙われる場合もあれば、たまたま攻撃した先が工場である場合もある。

→ したがって、いかなる工場においても、サイバー攻撃を受ける可能性があることを認識する必要がある。

また、本ガイドラインにおける工場システムとは下記図を想定構成および要素としてあります。

想定システム、ゾーン



想定業務

- 生産計画設定
- 生産(＋検査)
- 生産状況監視(現場)
- 部材補充(現場へ)
- 部材購入(倉庫へ)
- 生産性分析
- トレーサビリティデータ参照
- メンテナンス
- リモートメンテナンス

想定データ

- 生産計画
- 生産指示(生産機種・量)
- 生産レシピ
- 生産実績(トレサビデータ)
- 設備状態
- 設備プログラム・パラメタ・図面
- 部材在庫量(現場)
- 部材在庫量(倉庫)

工場システム例における構成要素

- ネットワーク
  - 設備系ネットワーク※
  - 生産管理系ネットワーク※
  - 情報系ネットワーク
- 装置・機器（機能・プログラム）
  - VPN装置兼ファイアウォール
  - 無線LAN-AP
  - MESサーバ
  - 生産ライン
  - SCADA
  - 保守端末（常時非接続）
  - AGV制御PC
  - AGV
  - 自動倉庫
  - 自動倉庫遠隔保守用サーバ
  - OA系サーバ
  - OA端末

※近年、設備系ネットワークや生産情報系ネットワークから情報系ネットワークを経由することなく、直接インターネットに接続できる経路も増えているが、そのような場合でも、本ガイドラインに示したステップや対策は活用可能。

https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline_gaiyou.pdf より抜粋

株式会社 アイサン情報システム
〒103-0016　東京都中央区日本橋小網町6番1号　山万ビル12階
Tel: 03-5614-5177　| E-mail: cyber@aisan-is.jp

ガイドラインで求められている無線LANに対するチェック項目

本ガイドライン　付録Eチェックリスト 項目2-7において下記内容となっております。
「工場内に無線LANを導入している場合、ネットワークへの接続を許可された機器の台帳を作成し、無許可の機器を拒否する仕組みがある。」

ソリューションのご紹介 (AirEye)

aireye | The **Leader** in Network Airspace Control and Protection (NACP)

無線LAN環境の可視化と無線LANを使ったサイバー攻撃の防御

すべての無線LANを監視
すべての無線通信をリアルタイムで監視、分析

特定と分類
端末等とネットワークを分類

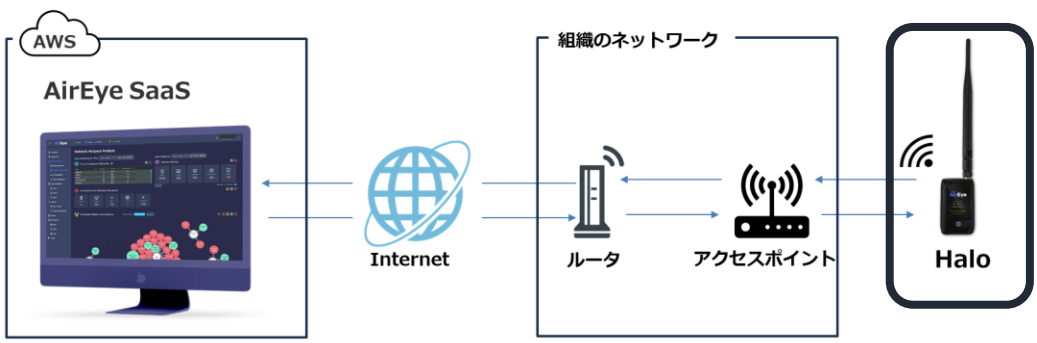
コントロール
セキュリティのルール違反を検出し、デバイス間の危険な接続を自動的に切断

防御
悪意のある接続を検出し、攻撃を停止

フォレンジック
攻撃の詳細と関与するデバイスを特定

AirEyeの構成と設置

既存の環境に「Halo」を設置するだけで構築完了です　!!



株式会社 アイサン情報システム
〒103-0016　東京都中央区日本橋小網町6番1号　山万ビル12階
Tel: 03-5614-5177　| E-mail: cyber@aisan-is.jp