HITACHI
Inspire the Next

工場セキュリティソリューション
ご説明資料

株式会社 日立ソリューションズ・クリエイト

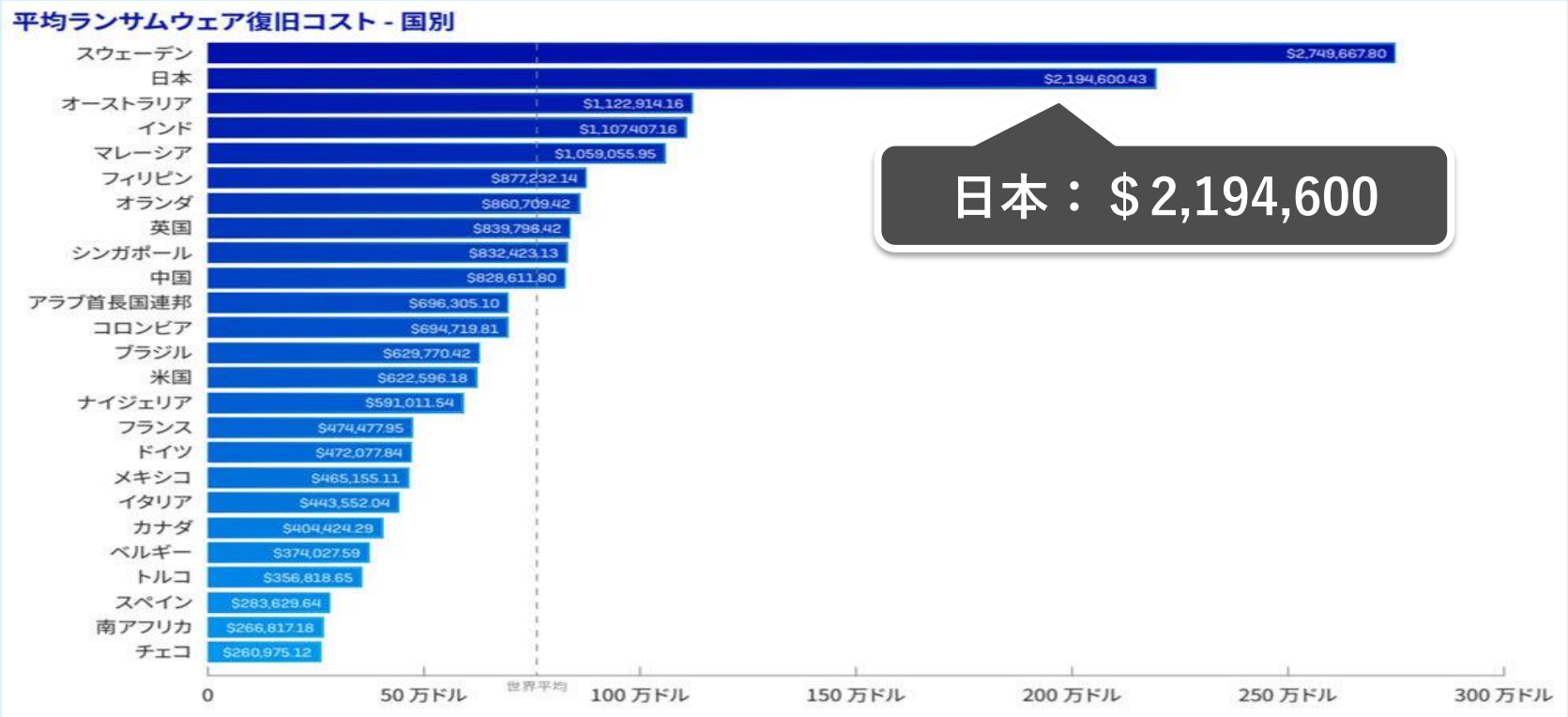
1.　近年の環境の変化

HITACHI
Inspire the Next

サイバーセキュリティ上の脅威が悪質・巧妙になり、その被害が深刻化

ランサムウェアによる事業停止によって発生する損失や運用コストなど、
損失額の平均は140万ドル、日本は約219万ドル（2億3,500万）
※被害後のデータ復元を引き換えに、支払いを要求される身代金支払いを除く

2020年1月から2月の期間、日本を含む26カ国のIT幹部5,000人を対象に実施したアンケート



出典：サイバーセキュリティ総研　日本企業のランサムウェア被害額世界で2位　Sophos調査レポート

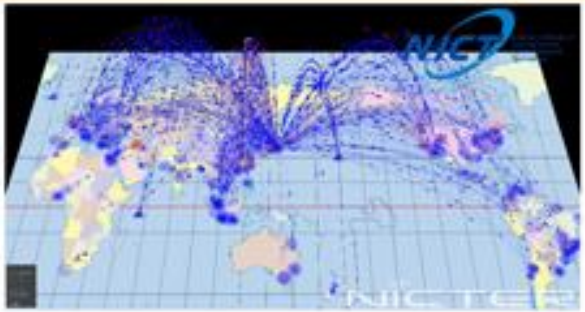
1.　近年の環境の変化

HITACHI
Inspire the Next

サイバーセキュリティ上の脅威が悪質・巧妙になり、その被害が深刻化

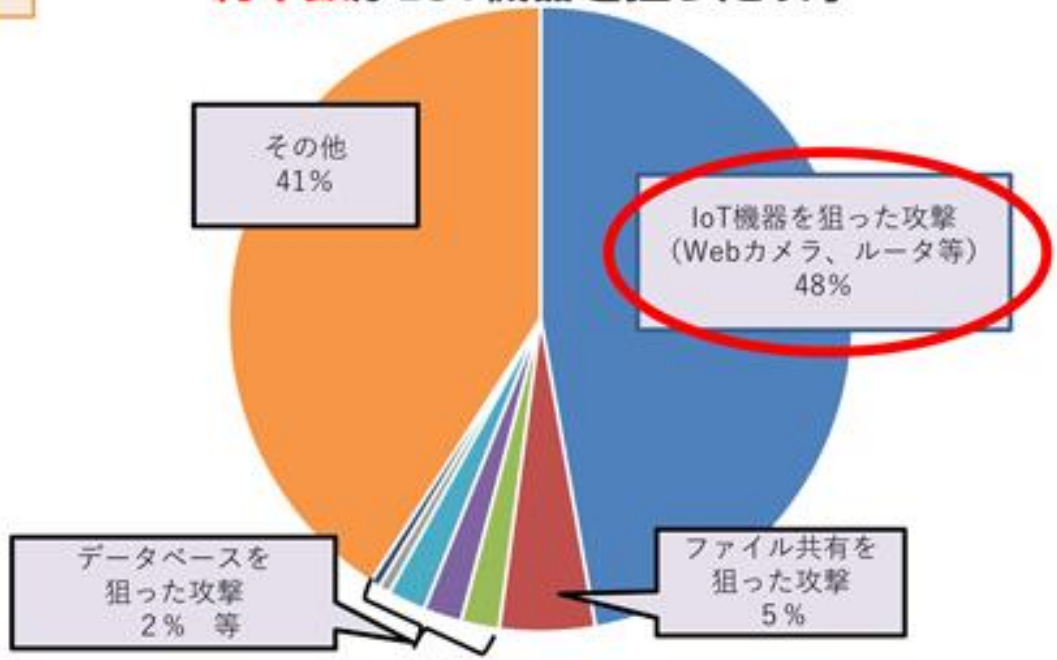
IoT機器を狙ったサイバー攻撃の状況（国立研究開発法人情報通信研究機構（NICT）発表）

NICTERにより観測されるサイバー攻撃の様子



NICTERで１年間に観測された
サイバー攻撃関連通信数

約半数がIoT機器を狙った攻撃



（注１）　NICTERで観測されたパケットのうち、サービスの種類（ポート番号）ごとに割合の多い上位から30位までを分析したもの。

（注２）　IoT機器を狙った攻撃は多様化しており、ポート番号だけでは分類しにくいものなど、「その他」に含まれているものもある。

2．工場、制御向けシステムの課題

近年、システム開発コストの削減や生産性の向上を目的とした
制御システムのオープン化が進んでいます
制御システムも情報システムと同じように、サイバー攻撃の脅威に晒されています

しかし、これまでクローズドなシステム環境は安全性が高いと信じられていたため
セキュリティへの認識が低いのが現実です

**リムーバブルメディアや外部機器、インターネット・イントラネット経由で
ウイルスに感染する事例が急増しています**

出典：IPA 『ドイツBSI　産業用制御システム(ICS)のセキュリティ −10大脅威と対策2019-』から

オープン化に向けたセキュリティ対策が重要課題

3． 制御システムの脅威とセキュリティリスク

HITACHI
Inspire the Next

セキュリティ被害を引き起こした原因は主に4ケースに分類され、端末や制御機器のぜい弱性が修正されてない場合に、被害を受けます

USBメモリー

- USBメモリーからのウイルス感染事例は頻繁に発生
- しかし、USBポートは運用上、メンテナンス上からも、なくすことは困難

リモートメンテナンス回線

- リモートメンテナンス回線の先の端末から、不正アクセス・ウイルス混入が発生

操作端末の入れ替え/保守用端末の管理

- 操作端末は汎用PCであることが一般的であり、入れ替え時にウイルスに感染していた端末から被害が発生
- システムに接続する保守用端末が原因

内部犯行・工業用無線LANなど

- 内部犯行者による物理セキュリティのすり抜け
- 工業用無線LANからの侵入
- PCのIDやパスワードの共通化、メモ書きの貼り付けなどは、悪用されやすく危険な運用

出典：IPA 『制御システム利用者のための脆弱性ガイド 重大な経営課題となる制御システムのセキュリティリスク』から

4．当社の制御システムのセキュリティリスク対策

HITACHI
Inspire the Next

お客さまの制御システムを守ります

■ラインやプラントの停止を防ぐ
可用性を維持し、制御システムの生産性を下げません

■人的損傷や環境破壊発生を防ぐ
悪意のある攻撃から制御システムを守ります

■経済的な損害発生を防ぐ
事業継続により、経済的損害を減らします

■信頼の失墜を防ぐ
お客さまのブランドや社会的信用を守ります

工場セキュリティソリューション

STEP1	STEP2	STEP3
課題抽出、対策立案	導入	運用・モニタリング
● IT/OT資産の可視化 ● リスク洗い出し ● 対応計画	● ガバナンス対策 ● 入口・出口対策 ● マルウェア対策 ● IoT監視＆検知　など	● IoT機器設定見直し

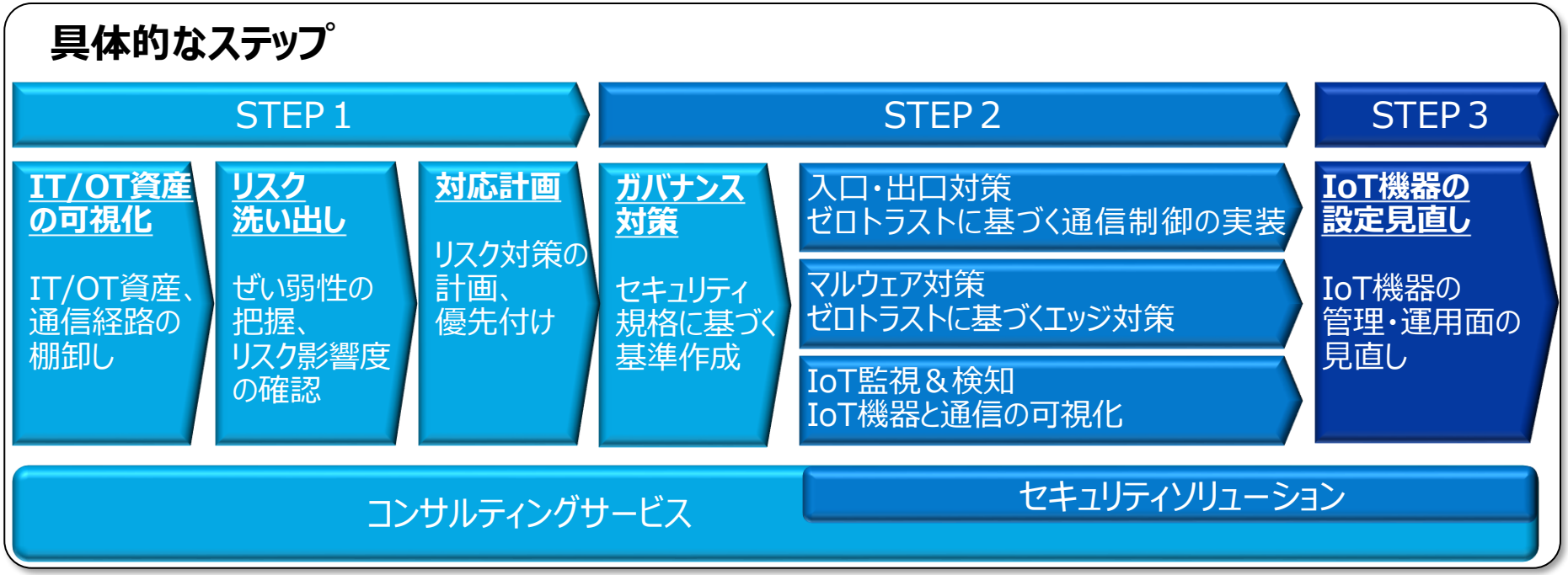
5．当社のサービスの特長

HITACHI
Inspire the Next

お客さまのニーズに合わせた最適なソリューションを提供

豊富な経験を有したコンサルタントが提供するコンサルティングサービスと、課題に合った適切なセキュリティソリューションの提供を通じて、お客さまの工場・制御システムのセキュリティ強化を支援します。

具体的なステップ



6-1. 当社のコンサルティングサービスの特長

HITACHI
Inspire the Next

経営者のビジョンとセキュリティ担当者の目標を考慮したコンサルティング

ISO※1/IEC※2のマネジメントシステムに精通し、ISMS※3のみならずQMS※4、ITSMS※5、BCMS※6などの多岐にわたる知見を強みに支援を行います。

コンサルティングサービス

IT/OT資産の可視化	リスク洗出し	対応計画	ガバナンス対策
IT/OT資産、通信経路の棚卸し	ぜい弱性の把握、リスク影響度の確認	リスク対策の計画、優先付け	セキュリティ規格に基づく基準作成
工場内情報セキュリティ現状調査	調査結果分析	情報セキュリティ対応計画策定支援	ガバナンス対策支援

※1 ISO : 国際標準化機構（International Organization for Standardization）
※2 IEC : 国際電気標準会議（International Electrotechnical Commission）
※3 ISMS : ISO/IEC 27001:2013（情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項）
※4 QMS : ISO 9001:2015（品質マネジメントシステム－要求事項）
※5 ITSMS : ISO/IEC 20000-1:2018 （情報技術－サービスマネジメント－第1部：サービスマネジメントシステム要求事項）
※6 BCMS : ISO 22301:2019（セキュリティおよびレジリエンス－事業継続マネジメントシステム－要求事項）

6-2. 工場内情報セキュリティ現状調査

HITACHI
Inspire the Next

工場内情報セキュリティ現状調査

～ コンサルティングサービス　現状調査 ～

設備観点、情報資産観点での現状資産および環境の調査を支援します

特長

①文書確認

生産現場におけるセキュリティ関連文書および運用関連文書についての調査

②設備および情報資産の整理

利用または管理対象となっている設備および情報資産を確認し整理

■文書確認

お客さまには、必要な文書を開示いただき、文書体系や文書の概要説明をお願いさせていただきます。
以下の確認および一覧表の作成を支援します。

- 管理方針
- セキュリティ関連規則
- 運用関連文書
- その他管理文書　など

■設備および情報資産の整理

保有している設備および情報資産を確認し整理一覧表の作成を支援します。

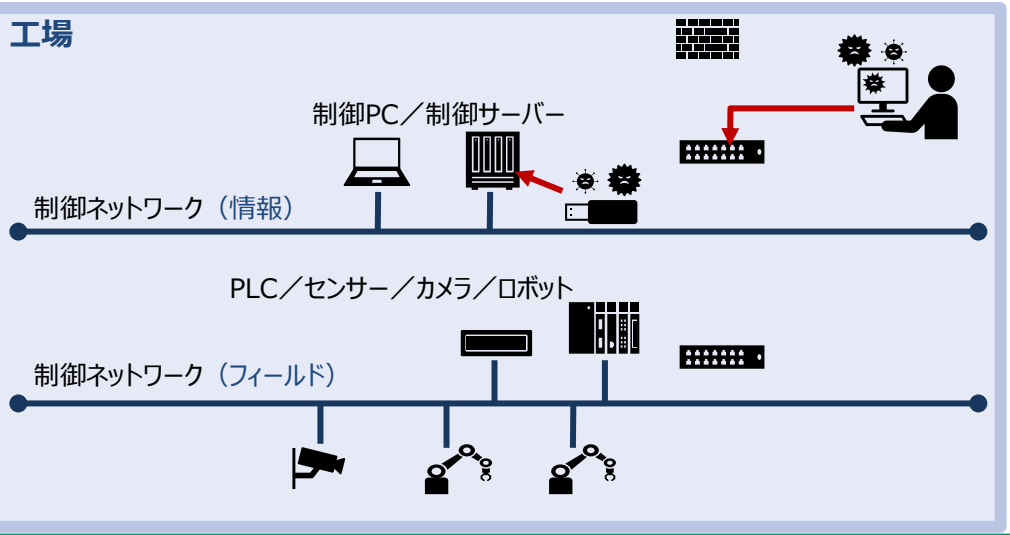
- 生産関連設備（PLC／センサー／カメラ／ロボットなど）
- サーバー／パソコン
- ネットワーク環境（クラウド環境を含む）

■ヒアリングの実施

- アンケートを実施し、現状調査結果を確認します。

現状を可視化することにより管理するための情報一覧を作成します。

IT部門は製造現場を把握できていない傾向があります



6-3. 調査結果分析

HITACHI
Inspire the Next

調査結果分析

～ コンサルティングサービス　調査結果分析 ～

現状調査の結果を基に、セキュリティの問題点の洗い出しを行います

特長

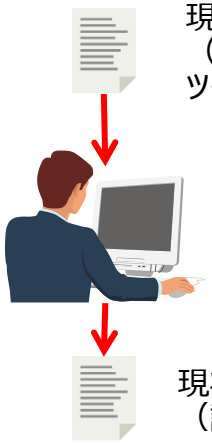
①リスクの分析、ぜい弱性の把握、リスク影響度の確認

現状調査の結果からリスク事項の洗い出し/ぜい弱性の把握と、各リスク事項に対する影響度の確認、
発生頻度から評価結果の定義

②課題事項の優先度の決定

各リスク事項に対し、当社見解による優先度（案）の作成

サービスの流れ



現状調査結果
（資産一覧、記入済ヒアリングシート、診断ツールの結果レポート など）

・評価・分析を行い、結果を評価値やコメントの作成
・評価値を定量的に表やグラフで整理

分析は、リスクを評価することが重要

現状評価報告書
（課題一覧、分析結果記入済の調査結果など）

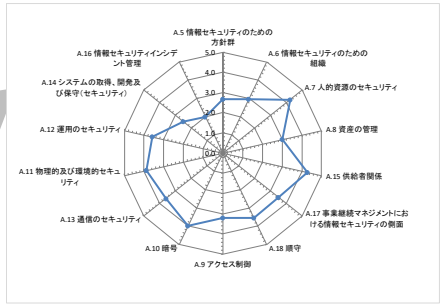
※打ち合わせを通じて、実態を良く理解・反映した評価・分析を実施
※ベースラインを踏まえた評価基準に照らして、お客さまに
分かりやすい評価値（記号・数値など）で評価結果を記載

現状評価報告書　記載イメージ

評価の観点	概要	ISMS 管理策の分類	管理策別評価	評価観点別評価
組織的対策	組織体制づくりや事業継続管理、コンプライアンスなど、組織として体系的に実施するセキュリティ対策	A.5 情報セキュリティのための方針群	2.7	3.3
		A.6 情報セキュリティのための組織	3.0	
		A.7 人的資源のセキュリティ	4.3	
		A.8 資産の管理	3.0	
		A.15 供給者関係	4.3	
		A.17 事業継続マネジメントにおける情報セキュリティの側面	3.5	
		A.18 順守	3.5	

経験に基づく優先度の観点を提供

評価の観点を定め、
セキュリティ管理観点の
内訳毎に評価（点）を整理



全ての評価の観点をグラフ化し、
リスクを見える化

6-4. 情報セキュリティ対応計画策定支援

HITACHI
Inspire the Next

情報セキュリティ対応計画策定支援

～ コンサルティングサービス　対応計画策定 ～

分析結果を基に、お客さまの今後のセキュリティ対応計画策定を支援します

特長

①対策案の検討

リスク分析結果を基に、課題・問題点に対する対策案の検討および優先度の確認

②対応計画案の策定

対策案について、優先度を考慮し対応計画案を策定

■対策案検討の観点

- 組織的対策　・ポリシーの見直し、セキュリティ体制の整備
- 人的対策　・セキュリティ教育や訓練の実施
- 物理的対策　・入退室管理システムの導入や特定区域での監視カメラの設置
- 技術的対策　・マルウェア対策やシステム監視、ログ取得・分析などによる入口・内部・出口における多層防御対策
  ・ネットワーク管理ツールなどを用いた対策

■対応計画の策定支援
対策案を基に、優先度を考慮し、
対応計画を策定します。

■以下が重要です
・対策案の観点をバランスよく計画すること
・段階的に整備し、継続的に見直していくこと

6-5. ガバナンス対策支援

HITACHI
Inspire the Next

ガバナンス対策支援

～ コンサルティングサービス　ガバナンス対策 ～

対応計画を基に、セキュリティ規格に基づく基準の作成を支援します

セキュリティの管理活動においてよりどころとなる規則の整備は最重要。
マネジメントシステムを利用することで継続的改善の仕組みの構築を支援します

特長

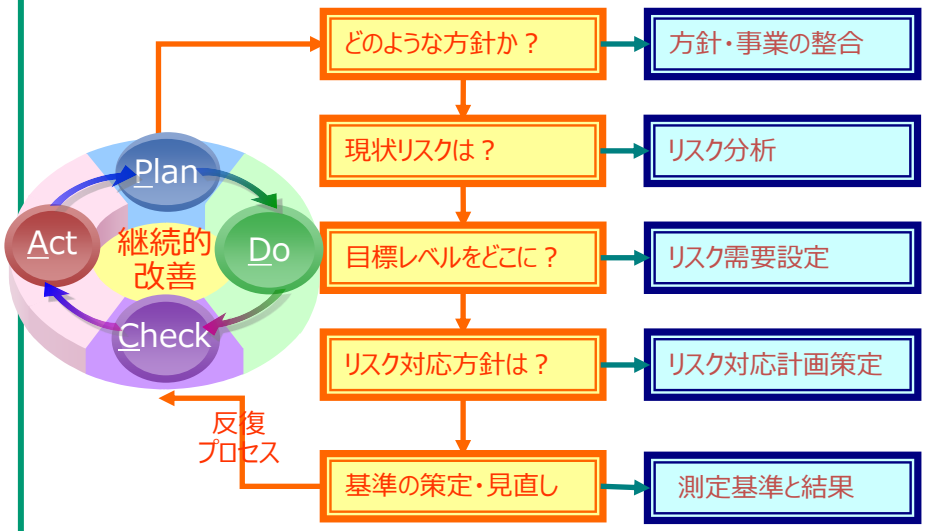
①ガバナンス状況の確認

対応計画などから、組織的なガバナンスの観点での確認を行い管理体制について検討

②お客さまに最適な基準の作成支援

数多くの業種、業態に合わせた基準の作成経験を踏まえ、お客さまの課題や要望を整理し、最適な基準の作成を支援
また、ISO関連のマネジメントシステム構築経験の視点から、必要な基準のレベルや深さについてアドバイスを実施

ガバナンス対策の活動



セキュリティ規格に基づく基準策定の効果

主要セキュリティ規格

IEC62443	NIST SP 800-82
NIST SP 800-171	ISO27001

- ◆ 現状の問題点を把握
- ◆ ポリシーの文書化と宣言
  - 方針を明文化し、従業員の意識を高める
- ◆ リスク評価に基づく適切な対策の選択と実施
  - 対策の漏れやアンバランスを防ぐ
  - 投資費用・人的資源の無理、無駄のない対策
- ◆ 企業の事業継続に影響を与えるリスクを低下

7-1. セキュリティソリューションの特長

HITACHI
Inspire the Next

コンサルティングからセキュリティ対策、運用、モニタリングまでトータルで支援

コンサルティングで明確になったお客さまの課題に対し、リスクの発生頻度と影響度を勘案して適切なセキュリティソリューションを提案し、セキュリティのリスクを軽減

セキュリティソリューション

入口・出口対策

ゼロトラストに基づく
通信制御の実装

ぜい弱性攻撃対策

Barracuda Web
Application Firewall

マルウェア対策

ゼロトラストに基づく
エッジ対策

**標的型攻撃対策
ソリューション**

AppGuard®

IoT監視＆検知

IoT機器と通信の可視化

**制御システム脅威
検知ソリューション**

Tripwire® Industrial
Visibility™

**ぜい弱性・リスク管理
ソリューション**

Tripwire® IP360™

7-2. セキュリティソリューション（製品概要）

HITACHI
Inspire the Next

Barracuda Web Application Firewall

～ ぜい弱性攻撃対策 ～

WEBアプリケーションへの攻撃から大切な情報を守ります

WAF
Barracuda Web Application Firewall

Barracuda.
Your journey, secured.

特長

①日本語GUIからの簡単チューニング

攻撃ログからボタン一つで定義の修正ができ、チューニングが簡単に実施可能

②ぜい弱性レポートのインポートで定義自動作成

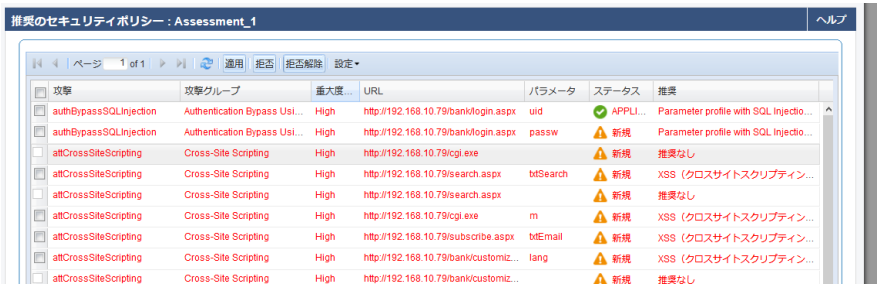
ぜい弱性診断結果をインポートすることにより、ポリシー作成から適用までを簡単に作成

ボタン一つでチューニング

- わかりやすい日本語GUIから検知した攻撃内容の確認が可能
- 修正ボタンからの簡単なチューニング作業

ポリシー自動作成

- さまざまなぜい弱性診断レポートの診断結果をインポートするだけでポリシーを自動で作成でき、定義も簡単
- アプリケーション開発中の段階から、チューニングが可能



7-3．セキュリティソリューション（製品概要）

HITACHI
Inspire the Next

AppGuard®

～　標的型攻撃対策ソリューション　～

APPGUARD

従来の検知型対策製品で検知することができない未知のマルウェアを含め、悪意のある不正プログラムの実行を防止

特長

①ファイルスキャンや定義ファイルのアップデートが不要で、システムへの負荷が少ない

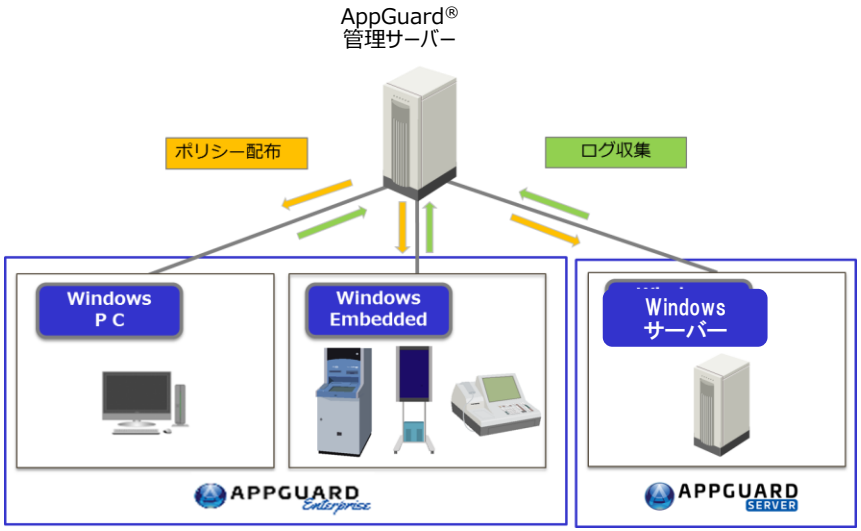
ITシステムはもちろんのこと、環境のオープン化に向けて対策が急務とされている制御システムの標的型攻撃対策にも有効

②攻撃の段階で脅威を遮断する新概念により、定期的なセキュリティポリシーの更新は不要

従来の検知型対策製品から置き換えた場合には、定義ファイルの更新などの保守・運用費用の削減が可能

AppGuard ®の技術

標的型攻撃対策ソリューション



7-4．セキュリティソリューション（製品概要）

HITACHI
Inspire the Next

Tripwire® Industrial Visibility™

～　制御システム脅威検知ソリューション　～

ネットワークへの負荷を抑制しながら自動的に可視化し、資産管理と脅威検知が可能

TRIPWIRE® INDUSTRIAL VISIBILITY

特長

①ネットワークへの負荷を抑制しながら、資産の可視化が可能

ネットワークや生産プロセスへの影響を抑制しながら、資産を自動的に抽出しネットワークマップを作成、稼働状況を可視化

②異常な挙動をいち早く検知

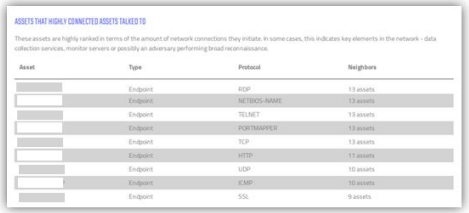
100種類を超える産業用プロトコルのパケット検査が可能、構成の不適切な変更や異常な指示など、異変をいち早く検知

ネットワークへの負荷を抑制しながら、資産の可視化

レガシーテクノロジーが混在する制御システムのネットワークは、遅延や帯域幅の変化の影響を受けやすいため、エージェントレス型とスキャンパケットを送らないパッシブスキャン方式を採用、ネットワークへの負荷を抑制しながら自動的に資産を可視化

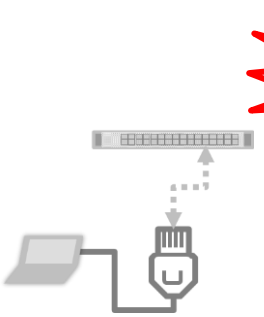
トポロジー・マップ

管理画面

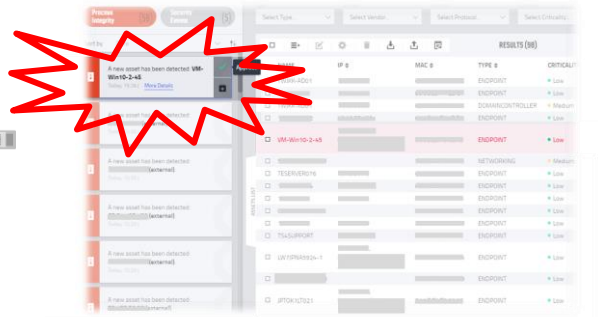


異常な挙動をいち早く検知

100種類を超える産業用プロトコルの詳細なパケット検査後、機械学習により制御システムのネットワーク上の「通常の状態」を安全のベースラインとして定義します。ベースライン情報で認識していない予期しない動作が発生した場合は、自動でアラートを作成



未登録デバイスの接続



管理画面

7-5．セキュリティソリューション（製品概要）

HITACHI
Inspire the Next

Tripwire® IP360™

～ ぜい弱性・リスク管理ソリューション ～

ぜい弱性診断・ぜい弱性リスク管理双方にバランスの取れたソリューション提供

TRIPWIRE® IP360

特長

①ぜい弱性診断のコンサルティング

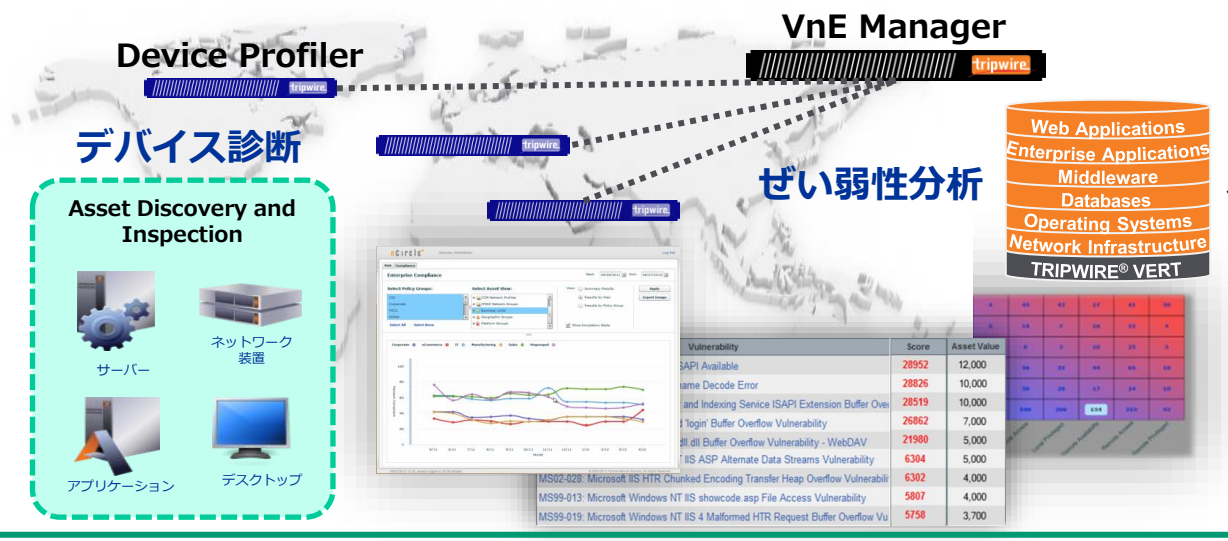
ネットワーク内のホストに関する膨大なデータを検出、収集したデータから最も効果的なリスク管理が可能

②ネットワーク上のすべてのIT資産を自動検出

資産価値およびぜい弱性スコアを組み合わせた高度な優先順位評価基準にて、評価と管理を効率良く実現

③包括的なネットワークセキュリティ管理

ネットワークやシステムへの負荷を抑えた監視や管理が可能、大規模で分散されたネットワークにおいても迅速な導入と容易な管理を実現



完全オンプレミスのエージェントレス型の製品であり、デバイスをルールに基づいて診断するスキャナ「Device Profiler」と、「Device Profiler」へのぜい弱性診断ルールの配信、診断結果の収集、台帳化、リスク分析管理を行う管理コンソール「VnE Manager」の2種類のアプライアンス（物理/仮想）から構成されます。

お問い合わせ

HITACHI
Inspire the Next

株式会社 日立ソリューションズ・クリエイト

Webでのお問い合わせ

www.hitachi-solutions-create.co.jp/inq.html

お問い合わせページより、商品・サービスをお選びください。

メールでのお問い合わせ

hsc-contact@mlc.hitachi-solutions.com

他社商品名、商標などの引用に関する表示

HITACHI
Inspire the Next

■他社商品名、商標などの引用に関する表示

- BarracudaNetworksおよびBarracuda Networks社ロゴは米国Barracuda Networks, Inc.の登録商標です。
- AppGuard® 、AppGuard®のロゴ は米国法人AppGuard, Inc. 、または株式会社Blue Planet-works及びその関連会社の、米国、日本またはその他の国における登録商標、または、商標です。
- Tripwire®は、Tripwire Inc.の登録商標です。
- 本資料に記載の会社名、製品名などは、それぞれの会社の商標または登録商標です。

■サービス・製品の仕様に対する表示

本資料に記載しているサービス・製品の仕様は、2021年3月現在のものです。
サービス・製品の改良などにより予告なく記載されている仕様が変更になることがあります。

■お問い合わせ情報について

ご相談、ご依頼いただいた内容は、回答などのため、当社の関連会社
（日立ソリューションズグループ会社）および株式会社日立製作所に提供（共同利用含む）する
ことがあります。
取り扱いには十分注意し、お客さまの許可なく他の目的に使用することはありません。


HITACHI
Inspire the Next