工場セキュリティガイドライン

対応ソリューションマップ

1.00 版
2024 年 4 月 12 日

東京大学 グリーン ICT プロジェクト・
Edgecross コンソーシアム
合同

工場セキュリティ WG

ECD-TE4-0010-01-JA

改版履歴

版	発行日	改版概要
1.00	2024 年 4 月 12 日	初版

目次

1. はじめに

本ソリューションマップは、東京大学 グリーン ICT プロジェクト・Edgecross コンソーシアム合同 工場セキュリティ WG が発行した、工場セキュリティガイドラインに記載の各セキュリティ対策として、利用可能なセキュリティベンダのソリューション(サービス／製品)を対応付け整理したものです。

工場セキュリティガイドラインを参照し工場のセキュリティ対策を推進する際に、どのようなサービス／製品を選定するのが適しているかを検討するための一助になることを目的としています。

2. セキュリティ対策と対応サービス／製品

工場セキュリティガイドライン 概要編「8.1. チェックリスト」の各確認項目に対応する各社サービス／製品は、以下の対応表に整理したとおりです。

2.1 チェックリスト対応表

カテゴリ	番号	確認項目	対応サービス/製品
準備	0-1	工場システムにおけるセキュリティ対策の検討・企画に必要な経営目標、外部要件、内部要件／状況を整理する。	• 2.4.1.2 セキュリティリスクアセスメントサービス • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス
	0-2	工場システムにおける業務・保護対象の整理、及び重要度の設定を行う。この結果を踏まえゾーンを設定し、業務・保護対象を結びつけ、セキュリティ脅威による影響を整理する。	• 2.4.1.2 セキュリティリスクアセスメントサービス • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス

カテゴリ	番号	確認項目	対応サービス/製品
	0-3	工場システムに関する内外の要件や、業務・保護対象・ゾーン等の情報収集・整理結果に基づき、工場システムのセキュリティ対策方針を策定し、想定脅威に対する対策の対応づけを行う。	• 2.4.1.2 セキュリティリスクアセスメントサービス • 2.4.4.1　OT セキュリティアセスメントサービス、コンサルティングサービス
組織的対策	1-1	工場システムのセキュリティについて、決裁者（工場長、カンパニー長等）または経営層が脅威や必要性の認識をもっており、十分な予算・人員配置などの協力を得られる状態にある。	• 2.4.1.2 セキュリティリスクアセスメントサービス • 2.4.4.1　OT セキュリティアセスメントサービス、コンサルティングサービス
	1-2	工場システムのセキュリティ対応について情報システム部門との協力・連携態勢が取られている。	• 2.4.1.4 セキュリティインシデント対応 体制・プロセス整備支援サービス • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス
	1-3	工場システムのセキュリティ検討組織があり、担当者がアサインされており、責任と業務内容が明確化されている。	• 2.4.1.4 セキュリティインシデント対応 体制・プロセス整備支援サービス • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス
	1-4	工場のセキュリティ事故発生時の担当者がアサインされていて、責任と業務内容が明確化されている。	• 2.4.1.4 セキュリティインシデント対応 体制・プロセス整備支援サービス • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス

カテゴリ	番号	確認項目	対応サービス/製品
	1-5	工場セキュリティに関する脅威の動向などについて、定期的に情報提供を受けたり、勉強会を開いたりするなどの現場教育を行っている。	• 2.4.1.4 セキュリティインシデント対応 体制・プロセス整備支援サービス • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス
運用的対策	2-1	システムが侵害・停止した場合の事業に対するリスクを定量的に検討している。（リスクアセスメント実施）	• 2.4.1.2 セキュリティリスクアセスメントサービス • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス
	2-2	工場システムにおける専用のセキュリティポリシが規定されていて、認知されている。	• 2.4.1.3 ポリシー策定支援サービス • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス
	2-3	工場システムからの電子メールやインターネットアクセスはポリシによって禁止している。	• 2.4.1.3 ポリシー策定支援サービス • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス
	2-4	工場システムにおけるセキュリティの異常発生時の責任者の対応が明確化されている。	• 2.4.1.2 セキュリティリスクアセスメントサービス • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス
	2-5	工場システムにおけるセキュリティの異常発生時の対応方法を現場作業者が理解し、訓練を実施している。	• 2.4.1.4 セキュリティインシデント対応 体制・プロセス整備支援サービス • 2.4.1.5 制御システムセキュリティ研修 • 2.4.4.1　OT セキュリティアセスメントサービス、コンサルティングサービス

カテゴリ	番号	確認項目	対応サービス/製品
	2-6	情報資産の検出ツールを利用するなど、工場ネットワークに接続している機器（サーバ、クライアント端末、ネットワーク機器、設備等）の台帳を作成し、システム構成図が存在し、変更管理を実施している。	• 2.3.2.1 iNetSec FC • 2.3.2.2 iNetSec SF • 2.3.3.1 Cisco Cyber Vision • 2.3.3.4 Cisco Secure Network Analytics (SNA) • 2.3.3.5 Cisco Identity Services Engine (ISE) • 2.3.4.2 Deep Discovery Inspector • 2.3.5.2 FortiNAC • 3.3.6.1 xDome • 3.3.6.2 CTD • 2.4.1.3 ポリシー策定支援サービス • 2.4.2.1 OT セキュリティ関連サービス • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス
	2-7	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。	• 2.3.2.2 iNetSec SF • 2.3.5.2 FortiNAC • 2.4.1.3 ポリシー策定支援サービス • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス
	2-8	定期的な脆弱性診断やペネトレーションテスト（侵入可否検査）を実施して、システムへの侵入を成功させるために使用できる攻撃手法や脆弱性を特定している。	• 3.3.6.1 xDome • 3.3.6.2 CTD • 2.4.1.3 ポリシー策定支援サービス • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス

カテゴリ	番号	確認項目	対応サービス/製品
	2-9	工場内に外部記録媒体（USB メモリ、フラッシュカード）やポータルメディアの利用・持ち込みを制限している。	• 2.4.1.3 ポリシー策定支援サービス • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス
	2-10	工場内のシステムのパスワードの強度と有効期限を含むパスワードルールがある。（安全に関わる緊急対応を必要とする表示器などの端末は除く）	• 2.4.1.3 ポリシー策定支援サービス • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス
	2-11	工場内のシステムへのアクセス権で使用していない古いアカウント（退職者・異動者など）を削除している。	• 2.4.1.3 ポリシー策定支援サービス • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス
	2-12	工場ネットワーク内の接続機器について、事前にそれらがウイルスに感染していないことを確認する手順がある。	• 2.4.1.3 ポリシー策定支援サービス • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス
	2-13	システム機能の完全な復旧を想定したバックアップを行い、定期的にバックアップデータからの復旧テストを行っている。また、その手順が明確化されている。	• 2.4.1.3 ポリシー策定支援サービス • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス

カテゴリ	番号	確認項目	対応サービス/製品
技術的対策	3-1	ウイルス対策がインストールできる端末にはアンチウィルスソフトまたはアプリケーション許可リスト(ホワイトリスト)を導入し、インストール不可能な端末では何らかの代替策（USB 型のアンチウィルスなど）を導入している。	• 2.3.1.2 軽量プログラム改ざん検知 • 2.3.3.3 Cisco Secure Firewall ISA3000 • 2.3.4.3 Cloud One - Workload Security / Trend Micro Deep Security • 2.3.5.1 FortiGate • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス
	3-2	アプリケーション/オペレーティングシステム（OS）にはセキュリティパッチを適用している。もしくは代替策でリスクを低減させている。	• 2.3.3.3 Cisco Secure Firewall ISA3000 • 2.3.4.1 TippingPoint Threat Protection System • 2.3.4.3 Cloud One - Workload Security / Trend Micro Deep Security • 2.3.5.1 FortiGate • 3.3.6.1 xDome • 3.3.6.2 CTD • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス
	3-3	制御端末のオペレーティングシステムの使用サービスやアプリケーションは必要最小限とし、未使用のサービスやポートは停止・無効化している。	• 2.3.4.3 Cloud One - Workload Security / Trend Micro Deep Security • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス

カテゴリ	番号	確認項目	対応サービス/製品
	3-4	工場の重要設備への物理的なアクセスについてレベル分けなどの十分な対策を行っている。（例：監視カメラ、警報装置）入退室管理、外部の入室者への関係者の付き添いなど運用面で補完してもよい。	• 2.2.1.1 入退場管理ソリューション　SecureFrontia X • 2.2.1.2 人物行動分析システム FieldAnalyst for Scene Understanding • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス
	3-5	工場ネットワーク内において、セキュリティレベルに応じたネットワークセグメント管理を行っている。（VLAN 等）	• 2.3.1.3 SDN（UNIVERGE Network Operation Engine） • 2.3.3.2 Catalyst IE 3000 スイッチシリーズ • 2.3.3.3 Cisco Secure Firewall ISA3000 • 2.3.5.1 FortiGate • 3.3.6.1 xDome • 3.3.6.2 CTD • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス
	3-6	工場システムのリモートメンテナンスなどを目的とした外部からのインターネットアクセスが可能な場合、認証（2 要素認証が望ましい）やネットワーク侵入防護などの保護対策を行っている。	• 2.3.1.1 軽量暗号 • 2.3.5.2 FortiNAC • 3.3.6.3 SRA • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス

カテゴリ	番号	確認項目	対応サービス/製品
	3-7	工場内のネットワーク（情報システムとの境界含む）の不審な通信を特定するためのネットワーク検知/防護システムを導入している。	• 2.3.1.4 InfoCage 不正接続防止 • 2.3.1.5 OWL DualDiode • 2.3.1.6 Nozomi Networks Guardian • 2.3.1.7 ForeScout eyeInspect • 2.3.1.8 Darktrace • 2.3.3.1 Cisco Cyber Vision • 2.3.3.3 Cisco Secure Firewall ISA3000 • 2.3.3.4 Cisco Secure Network Analytics (SNA) • 2.3.3.5 Cisco Identity Services Engine (ISE) • 2.3.4.1 TippingPoint Threat Protection System • 2.3.4.2 Deep Discovery Inspector • 2.3.5.1 FortiGate • 2.3.5.2 FortiNAC • 2.3.5.4 FortiDeceptor • 3.3.6.1 xDome • 3.3.6.2 CTD • 2.4.2.1 OT セキュリティ関連サービス • 2.4.3.1 Trend Vision One • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス

カテゴリ	番号	確認項目	対応サービス/製品
	3-8	工場内システムのログイン、操作履歴などのイベントログを取得している。それらのログは定期的に分析するか必要日数保存している。	• 2.3.1.9 Splunk • 2.3.3.3 Cisco Secure Firewall ISA3000 • 2.3.5.3 FortiAnalyzer • 2.4.3.1 Trend Vision One • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス
工場システム・サプライチェーン管理	4-1	工場システムのセキュリティ事故発生時の制御システムベンダー・構築事業者との連絡・連携態勢が取られている。	• 2.4.1.4 セキュリティインシデント対応 体制・プロセス整備支援サービス • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス
	4-2	工場システムのメンテナンス等にかかわる外部事業者向けのセキュリティ教育を実施している。	• 2.4.1.5 制御システムセキュリティ研修 • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス
	4-3	納品された工場システムに関するセキュリティの脆弱性が発見された場合、その情報が速やかに共有されるように、制御システムベンダー・構築業者との関係を維持している。	• 2.4.1.4 セキュリティインシデント対応 体制・プロセス整備支援サービス • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス
	4-4	サプライチェーン（協力会社、生産子会社など）における工場システムの脅威、影響度、対応状況（監査実施など）を把握できている。	• 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス

カテゴリ	番号	確認項目	対応サービス/製品
	4-5	納入する工場システム機器に対して、一定のセキュリティ基準をみたしているかを判定するプロセス、または受け入れ検査がある。	• 2.4.1.3 ポリシー策定支援サービス • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス
	4-6	新規システム導入時の設計仕様要件にセキュリティに関する要求仕様が明確化されている。	• 2.4.1.3 ポリシー策定支援サービス • 2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス

上記の他にも、チェックリストの確認項目には含まれていないものの、工場のセキュリティ対策として必要になると考えられる下記サービス／製品を掲載しています。

- 2.2.2.1 部屋免震システム
- 2.2.2.2 防虫エンジニアリング

2.2 物理面での対策

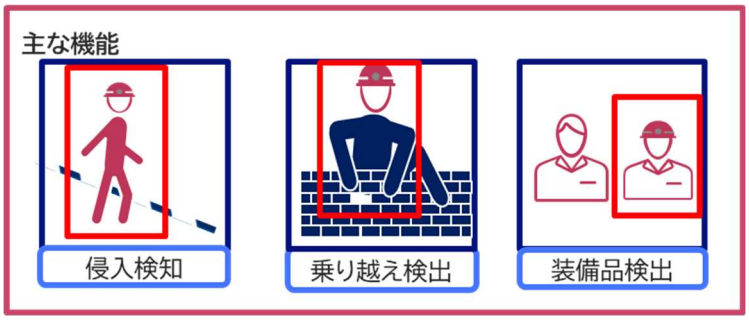
物理面での対策に対応する各社のサービス／製品は、下記となります。

2.2.1 NEC

2.2.1.1 入退場管理ソリューション SecureFrontia X

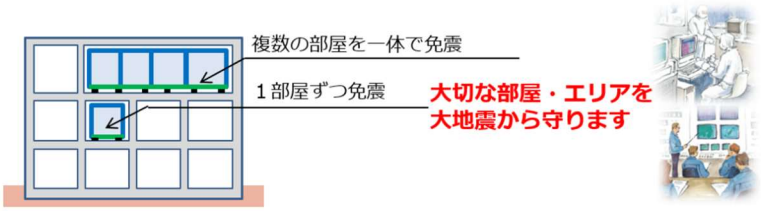
チェックリスト対応項目	3-4
ソリューション概要	IC カードをはじめ、生体認証との連携による入退管理で、工場における敷地内や建屋内各フロアへのセキュアな入場制限を実現します。 ① IC カードによる本人認証により、セキュリティを担保します。 ② 各種センサ、勤怠システム、マスタとの連携など既存の各種システムと連携やモニタ監視を行うことができます。 ③ 顔認証などの生体認証と連携し、より高度なセキュリティを実現します。  IC カード  顔認証  モニタ機能
製品詳細 URL	https://www.necplatforms.co.jp/solution/security/sfx/index.html

2.2.1.2 人物行動分析システム FieldAnalyst for Scene Understanding

チェックリスト対応項目	3-4
ソリューション概要	AI による監視カメラ映像のリアルタイム解析で、動く物体を人/クルマ/モノなどとして認識・追跡し、工場などの生産現場の安全を見守り、各種施設の強固なセキュリティ確立に貢献します。 ① 工場やプラントなどにおいて、危険なエリアへの立ち入りを監視し、作業員が誤って立入禁止区域へ侵入するとアラートを発報して警告します。 ② 機密を要するエリア、部外者の立入禁止区域などへの侵入を、行動検知と深層学習の組み合わせで防止し、セキュリティの向上を実現します。 ③ 工場やプラント、建設現場などで必須となる装備、ヘルメットやゴーグル、シールドなどの装着の有無を検知して、未装備の場合は警告します。 
製品詳細 URL	https://www.nec-solutioninnovators.co.jp/sl/fieldanalyst/fa_02/aisu/index.html

2.2.2 竹中工務店

2.2.2.1 部屋免震システム

ガイドライン 対応項目	5.2.2. 物理面での対策 5.2.2.1.建屋にかかわる対策
製品概要	「部屋免震システム」は、従来の建物免震構造よりローコストで、かつ同じように地震後の機能が維持できるように建物内の重要な部屋に限定して免震とする技術です。短い期間で簡易な工事により導入が可能です。 建物内の「部屋」を対象にした免震システムです。 新築でも改修でも、また１部屋から複数の部屋、大きなエリアまでフレキシブルに導入可能です。 コストの問題などで建物を免震構造とすることが難しく、地震時にこれだけは止められない、守りたいという重要な部屋をお持ちのお客様に幅広くお勧めしています。(例：災害対策室、手術室、代替のきかない製造施設、保管庫など) 
製品詳細 URL	https://www.takenaka.co.jp/solution/disaster/heyamenshin/

2.2.2.2 防虫エンジニアリング

ガイドライン 対応項目	5.2.2. 物理面での対策 5.2.2.1.建屋にかかわる対策
製品概要	虫を誘引させない、侵入させない技術 建物に虫が近接したり、虫が入り込む要因を排除します バグフラッシャー（フラッシング機能付きシートシャッター） シャッターの開口部の前に停滞する虫をきれいに吹き飛ばしてしまうことにより、建物への侵入を低減します。  バグバンパー（歩行虫進入阻止部材） 含有する昆虫忌避剤の効果とオーバーハングの形状により、歩行虫の侵入を防ぎます。 
製品詳細 URL	https://www.takenaka.co.jp/solution/environment/boutyu/

2.3 システム構成面での対策

システム構成面での対策に対応する各社のサービス／製品は、下記となります。

2.3.1 NEC

2.3.1.1 軽量暗号

チェックリスト 対応項目	3-6
製品概要	送受信データの暗号化、機器認証を後付け可能なソフトウェア。 ① 通信アプリケーションの改修を不要で後付けが可能 機器に搭載される通信アプリケーションのソースコードを改修することなくインストールするだけで、通信の暗号化が可能となり、暗号化のためのコストや手間を削減できます。 ② 柔軟な暗号化設定 暗号化対象とする通信と対象外とする通信とを設定により指定することが可能です。そのため、暗号化対象とする機器、対象外とする機器をシステム内に混在させることができます。 ③ 機器認証によるシステムの堅牢性強化 機器同士が暗号化通信を開始する前に、互いを自動的に認証します。これにより、不正な機器とは暗号化通信を行わず、信頼できる機器のみと行うように制限できます。
製品詳細 URL	https://jpn.nec.com/iot/platform/security/lcdk/

2.3.1.2 軽量プログラム改ざん検知

チェックリスト 対応項目	3-1
製品概要	不正プログラム(マルウェア感染、プログラム改ざん)の対策を後付け可能なソフトウェア。 ① 不正プログラム対策の常時実行 感染したマルウェアや改ざんされたプログラムファイルを検知して起動を抑止するだけでなく、実行中のメモリ上にあるマルウェアや改ざんされたプログラムを検知することもできます。これにより、不正プログラムの実行を防止して被害を最小限に抑える対処が可能になります。 ② コンテナの不正プログラム対策 コンテナを搭載した機器では、ホスト OS 上だけでなく、動作中のコンテナ内も不正プログラム対策ができます。 ③ 低負荷な動作 機器の稼働状況に合わせて低負荷に動作するため、長期間の稼働やリアルタイム性が要求されるプログラムの処理を妨げません。 ④ 極小フットプリント 不正プログラム対策に必要な最小限の処理に特化することで、フットプリントは約 100KB と極小です。これにより、メモリ・ディスク容量に制約のある機器にも適用できます。
製品詳細 URL	https://jpn.nec.com/iot/platform/security/lwtd/

2.3.1.3 SDN (UNIVERGE Network Operation Engine)

チェックリスト 対応項目	3-5
製品概要	情報系と制御系のネットワーク分離や生産ライン毎にネットワークを分割するなど、ネットワークをセキュアかつ柔軟に構築することができる SDN 製品です。 ① 物理的な機器の分離ではなく、仮想ネットワーク技術で、工場内ネットワークを論理的に分離可能です。 ② 仮想ネットワークによる分離により、セキュリティ被害を局所化できます。 ③ 物理/仮想のネットワーク構成や端末位置情報なども可視化可能です。
製品詳細 URL	https://jpn.nec.com/univerge/noe/

2.3.1.4 InfoCage 不正接続防止

チェックリスト 対応項目	3-7
製品概要	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します。 ① 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します。 ② 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することができます。 
製品詳細 URL	https://jpn.nec.com/infocage/prevention/

2.3.1.5 OWL DualDiode

チェックリスト対応項目	3-7
製品概要	データの流れを物理的に一方向に限定し、重要データの共有をセキュアに実現するデータダイオード製品 ① ダイオードの原理を応用した“一方向通信アーキテクチャ”により、通信を片方向のみに限定します。 ② ファイアウォールで防げないサイバー攻撃も確実に防御します。 ③ 通信プロトコルの終端機能により、FTP、HTTP などの通信でも一方向転送を実現します。 
製品詳細 URL	https://www.ncos.co.jp/products/ipss/owl/

2.3.1.6 Nozomi Networks Guardian

チェックリスト対応項目	3-7
製品概要	OT ネットワークの可視化・脅威検知を行う IDS 製品 ① 工場/プラント内ネットワークの通信を監視し、ネットワーク構成や内在する脆弱性を可視化します。 ② IT/OT アセットに対する脅威を deny list(拒否リスト)で検知、異常な通信を allow list（許可リスト）で検知します。 ③ OT プロトコルに対する不正な攻撃も検知します。 ④ 日本語 GUI に対応し、モニタ状況を把握するダッシュボードをユーザの好みにカスタマイズ可能です。 
製品詳細 URL	https://www.ncos.co.jp/products/ipss/nozomi/

2.3.1.7 ForeScout eyeInspect

チェックリスト	3-7
製品概要	OT ネットワークの可視化・脅威検知を行う IDS 製品 ① 工場/プラント内ネットワークの通信を監視し、ネットワーク構成や内在する脆弱性を可視化します。 ② IT/OT アセットに対する脅威を deny list(拒否リスト)で検知、異常な通信を allow list（許可リスト）で検知します。 ③ OT プロトコルに対する不正な攻撃も検知します。
製品詳細 URL	https://jpn.nec.com/datanet/silentdefense/

2.3.1.8 Darktrace

チェックリスト 対応項目	3-7
製品概要	自己学習型 AI による通信の分析により、未知のセキュリティ脅威なども検知可能な NDR 製品 ① ユーザ固有のふるまいやデバイスの通信パターンを分析し、定常状態を学習する事で、ネットワーク上の異常をリアルタイムに検知します。 ② 異常検知時に、自動的に該当通信を遮断することで、被害を局所化することが可能です。 ③ シグネチャ更新不要のため、運用負荷を低減でき、閉域ネットワークなどでも導入可能です。 
製品詳細 URL	https://www.nesic.co.jp/solution/Darktrace.html

2.3.1.9 Splunk

チェックリスト 対応項目	3-8
製品概要	ネットワークやシステムのログ、セキュリティ情報などを一元管理し、脅威の可視化とインシデント対応の効率化を実現する SIEM 製品 ① セキュリティイベントの一元管理や複数のセキュリティ機器のログを横断分析することができます。 ② 機器ごとのログを統合し、ネットワークやシステム状態を即座に把握します。 ③ ブラウザベースの GUI で、効率的かつ容易なログ分析が可能です。
製品詳細 URL	https://jpn.nec.com/soft/splunk/

2.3.2 PFU

2.3.2.1 iNetSec FC

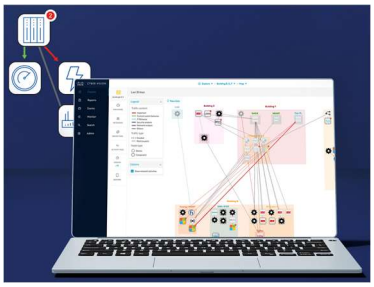
チェックリスト対応項目	2-6
製品概要/特徴	工場内の IT 機器とネットワークの見える化を簡単に実現し、セキュリティ対策に必要な現状把握を自動化します。 特徴①：機器とネットワーク構成を自動で見える化 ・ネットワーク接続機器のベンダー名や機器種別、OS 種別を判定 ・現在のネットワーク構成を自動で作図 ・IP アドレスを持たないスイッチングハブも検出可能 ・管理外セグメント機器も検知し LAN 内の全数把握を自動で実現 ・機器の設置場所「写真」も登録でき、機器を探す時間を大幅削減 特徴②：異常機器と影響範囲を見える化しトラブル対処を迅速化と未然防止 ・ネットワークマップ上にてネットワークエラーが発生している個所を表示し影響範囲を見える化し迅速な対処を実現 ・ネットワークスイッチの接続ポートごとの負荷状況や転送エラー数を見える化しトラブル予防や調査に活用可能 ・現在のネットワークマップを表示するだけでなくスナップショット保存が可能。トラブル発生時に過去の正常時の状態と比較し調査時間を大幅に削減が可能 特徴③：マルチベンター対応で環境を変えずに導入可能 ・様々なメーカーのネットワークスイッチと連携可能のためスイッチの入れ替え不要で導入が可能 
製品詳細 URL	https://www.pfu.ricoh.com/inetsec/products/fc/

2.3.2.2 iNetSec SF

チェックリスト 対応項目	2-6,2-7
製品概要/特徴	ネットワークに接続されるあらゆる IT 機器を手軽に「検知・遮断・管理」ができます。 特徴①：機器の見える化と自動遮断 ・ネットワーク接続機器を自動的に検出 ・機器のベンダー名や機器種別、OS 種別を判定 ・接続が許可されていない不正な機器を遮断 特徴②：複雑な IT 機器管理の負担を軽減 ・機器利用申請・承認のワークフローで社内の機器を手軽に管理 ・機器種別に応じて自動許可が可能 ・OS 種別の自動判定により古い OS の稼働を把握可能 ・ダッシュボードやレポーティング機能で運用者の負担軽減 ・ランダム MAC アドレスを検知し、遮断して警告画面表示することにより固有 MAC アドレスでの接続へ誘導 ・長期未接続機器を自動でリストアップし削除も可能 特徴③：様々な不正機器を検知し自動で遮断対処 ・マルウェアに感染した機器を検知・遮断し感染被害を局所化 ・業務で禁止されたアプリケーションを検知し機器を自動で遮断 ・他製品と連携しエッジ側の不正な機器を自動で遮断 
製品詳細 URL	https://www.pfu.ricoh.com/inetsec/products/sf/index.html

2.3.3 シスコシステムズ

2.3.3.1 Cisco Cyber Vision

チェックリスト 対応項目	2-6, 3-7
製品概要/特徴	Cisco Cyber Vision は、工場のセキュリティ態勢を詳細に把握できるようにする、大規模展開が非常に容易なソリューションです。 以下の特徴があります。 ■ 工場ネットワーク内の状況を把握 すべての産業用機器の資産情報を特定し、それらの通信状況を確認できます。Cyber Vision はネットワーク構成を可視化するため、大規模であっても簡単に展開できます。 ■ 工場の攻撃対象領域を縮小 工場ネットワークのセキュリティ態勢を把握することにより、優先すべきアクションが明確になります。Cyber Vision は、早急な対応が必要な機器に焦点を当てて解決策を提案します。 ■ 運用を効率化 工場内ネットワークのイベントの監視、通信問題の特定、および迅速な問題のトラブルシューティングにより、ダウンタイムを短縮してネットワークのパフォーマンスを向上させます。 ■ IT セキュリティを工場内ネットワークに拡張 Cyber Vision は、工場内機器の資産とイベントに関する情報を IT セキュリティツールに提供することにより、ネットワーク全体のリスクの管理とセキュリティポリシーの適用を容易にします。 
製品詳細 URL	https://www.cisco.com/site/jp/ja/products/security/industrial-security/cyber-vision/index.html

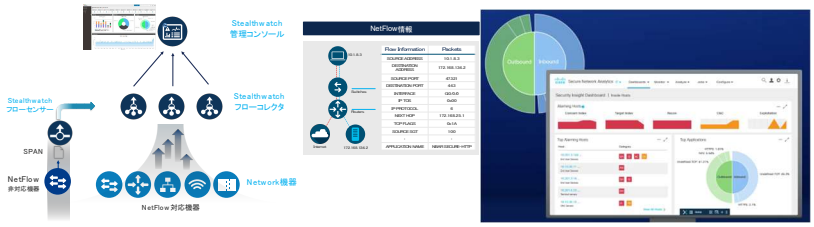
2.3.3.2 Catalyst IE 3000 スイッチシリーズ

チェックリスト対応項目	3-5, 3-7
製品概要	Catalyst IE 3000 シリーズは、過酷な環境でも耐えられる堅牢なハードウェア設計かつ高機能なセキュリティ機能を兼ね備えた製品です。 以下の特徴があります。 ■産業用途向け専用設計 過酷な環境での利用を想定した温度範囲（-40 ～ 75° C）に耐えられるファンレス設計および高度な産業用プロトコルに対応したセキュリティ機能を有しています。 ■セキュアブート機能 IE スイッチ自身のソフトウェアとハードウェアを相互認証し、不正な模造品やソフトウエアの使用を未然に防止する機能を有しています。 ■Cyber Vision 連携 IE スイッチの機能によりスイッチを通過する産業プロトコルに対して DPI（データ解析)を実施、これを Cyber Vision サーバ上で分析して脅威の検出を行います。 ■Secure Network Analytics 連携 IE スイッチの機能によりスイッチを通過するトラフィック情報を収集し、Secure Network Analytics サーバー上で分析して異常な振る舞いを検出する方式のため、専用のセンサーを設置することなくネットワーク全体を隅々まで脅威検出させることができます。またフロー情報のみを用いるため、未知のアプリケーション層プロトコルに対しても効果を発揮します。  
製品詳細 URL	https://www.cisco.com/c/ja_jp/products/switches/industrial-ethernet-switches/index.html

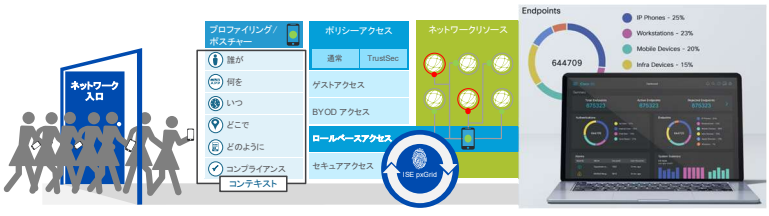
2.3.3.3 Cisco Secure Firewall ISA3000

チェックリスト対応項目	3-1, 3-2, 3-5, 3-7, 3-8
製品概要	過酷な環境でも耐えられる堅牢なハードウェア設計の産業用ファイアウォールで優れたエンドツーエンドのセキュリティを提供します。 以下の特徴があります。 ■産業用途向け専用設計 過酷な環境での利用を想定した温度範囲（-40 ～ 75° C）に耐えられるファンレスかつ DIN レールマウント設計の堅牢なアプライアンスです。 また、NERC-CIP、ISA99/IEC62443、CFATS、ANSI/AWWA G430 などのさまざまな産業標準、規制、およびガイドラインに準拠しており DNP3, Modbus, IEC 61850, Omron、Rockwell, GE, Schneider, Siemens など多様な産業用プロトコルおよびアプリケーションに対応したアクセス制御、脅威制御、アプリケーション制御を提供します。 ■多様な機能統合 いわゆるファイアウォール、シグネチャーに基づく侵入検知システム（IDS）/侵入防止システム（IPS）、ネットワークアドレス変換（NAT）、仮想プライベートネットワーク（VPN）、DNS/DHCP 等の機能を統合しています。 また Cyber Vision, Secure Network Analytics との連携が可能です。 ■用途及び規模に応じた柔軟な管理機能 単体の GUI 管理だけでなく数百台規模の集中設定、ログ管理、監視、およびレポート作成をオンプレミスもしくはクラウドで提供します。 
製品詳細 URL	https://www.cisco.com/c/ja_jp/products/security/industrial-security-appliance-isa/index.html

2.3.3.4 Cisco Secure Network Analytics (SNA)

チェックリスト 対応項目	2-6, 3-7
製品概要	Cisco Secure Network Analytics は、工場を含む企業全体のネットワークの可視化を実現し、脅威をリアルタイムで検出して対応する業界実績ナンバー 1 を誇る NDR(Network Detection and Response)ソリューションです。 以下の特徴があります。 ■ 高度な検知機能 強力な機械学習機能と独自の検知アルゴリズムにより、暗号化トラフィックを含むあらゆる通信を分析することが可能であると共に、重大な脅威に関する誤検出やアラームを大幅に削減しお客様のインシデント対応にかかる時間を大幅に削減します。 また Cisco Identity Services Engine (ISE) と連携することにより検知した端末をネットワークから隔離することも可能です。 ■ 投資を最大限に活用 工場ネットワークを構成する既存の NetFlow 対応スイッチ（Catalyst スイッチ）から収集するフロー情報を利用するため新たにセンサーを導入することなくネットワーク全体の可視化と脅威対策を実現できます。 ■ 長期データ保持 スケーラブルで長期的なテレメトリのストレージ機能により、フローコレクタを追加することなく、最大 1 ～ 2 年分のデータを長期間保持できます。 
製品詳細 URL	https://www.cisco.com/site/jp/ja/products/security/security-analytics/secure-network-analytics/index.html

2.3.3.5 Cisco Identity Services Engine (ISE)

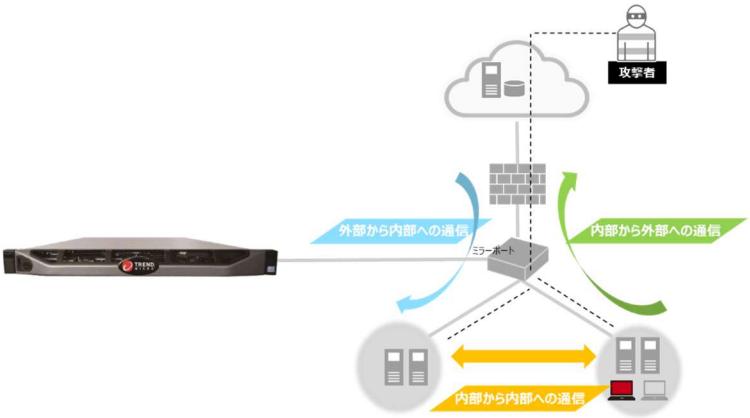
チェックリスト 対応項目	2-6, 3-7
製品概要	工場を含む企業ネットワークのセキュリティポリシー管理を合理化し、運用コストを削減するためのワンストップソリューションです。ISE を使用すると、工場ネットワークへの有線 LAN、無線 LAN、および VPN 接続を含むあらゆるアクセスをするユーザと機器の確認及び制御することができます。 以下の特徴があります。 ■高度なアクセスコントロール スイッチや無線 LAN アクセスポイントからのアクセス認証要求に対してアクセス可否を応答するたけでなく、認証されたユーザー毎に接続される VLAN やアクセス可能なサーバーを限定するアクセス制御リストを動的に適用するなど柔軟な接続制御が可能です。 ■機器のプロファイリング 工場で利用する機器をネットワークに接続した際に、管理者が定義したポリシーに基づき自動的に検出、分類、関連付けすることができます。 ■ネットワーク機器の認証 RADIUS および TACACS+ プロトコルを利用して工場ネットワークを構成するスイッチ、無線 LAN アクセスポイント、Firewall、VPN 機器などへのアクセス認証を集中管理することができます。 
製品詳細 URL	https://www.cisco.com/site/jp/ja/products/security/identity-services-engine/index.html

2.3.4 トレンドマイクロ

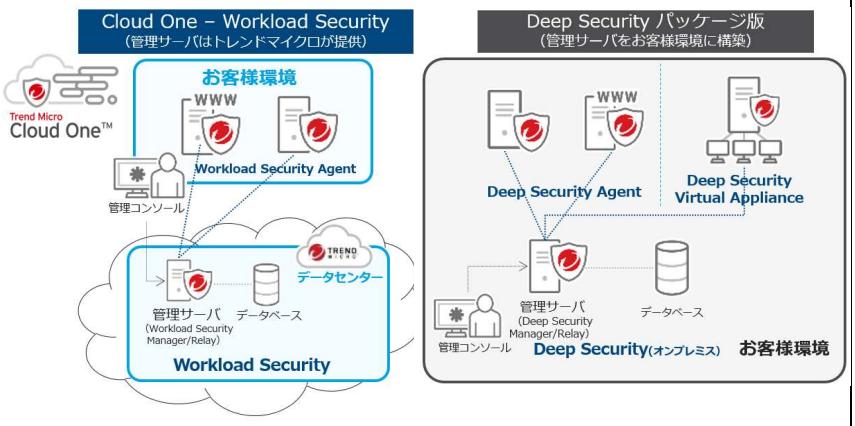
2.3.4.1 TippingPoint Threat Protection System

チェックリスト 対応項目	3-2, 3-7
製品概要/特徴	脆弱性を突いたウイルス侵入はもちろん、工場内部拡散も防御する次世代 IPS。 ■ ネットワークの入口・出口・ネットワーク内部の攻撃をブロック。※1 ■ ネットワーク単位で工場内生産設備の弱点（脆弱性）を保護。※2 ■ 推奨設定によりフィルタチューニングの工数を削減。リアルタイムで不正な通信をブロック。※1 ・ 脆弱性そのものを保護（仮想パッチ）し、攻撃をブロック※2 ・ IP アドレス/DNS ドメイン/URL の拒否リストで不正な通信をブロック ※1 すべての攻撃、不正な通信をブロックできるわけではありません。 ※2 すべての脆弱性を保護できるわけではありません。 
製品詳細 URL	https://www.go-tm.jp/tp

2.3.4.2 Deep Discovery Inspector

チェックリスト 対応項目	2-6, 3-7
製品概要/特徴	狙いを定めた企業/組織を狙う標的型攻撃の様々な攻撃を可視化する監視センサー。 ■ 見えざる攻撃から企業や組織を保護。 ■ ネットワーク内部に設置し全方位の通信を監視。 ■ 複数の兆候から不正な予兆を検知。 • 従来のウイルスパターンファイルでは見つからない機密データを盗み出すウイルスを検出できます。※ • すべてのネットワークポートと 105 種類を超えるプロトコルの 360 度にわたる可視化が単一のアプライアンスで実現します。 • 脅威の分析により生産設備をロックしたり、ファイルを暗号化したりすることで使用不能にし、元に戻すことと引き換えに「身代金」を要求する不正プログラム（ランサムウェア）を検出します。 ※すべての脆弱性を検出できるわけではありません。 
製品詳細 URL	https://www.go-tm.jp/dd

2.3.4.3 Cloud One - Workload Security / Trend Micro Deep Security

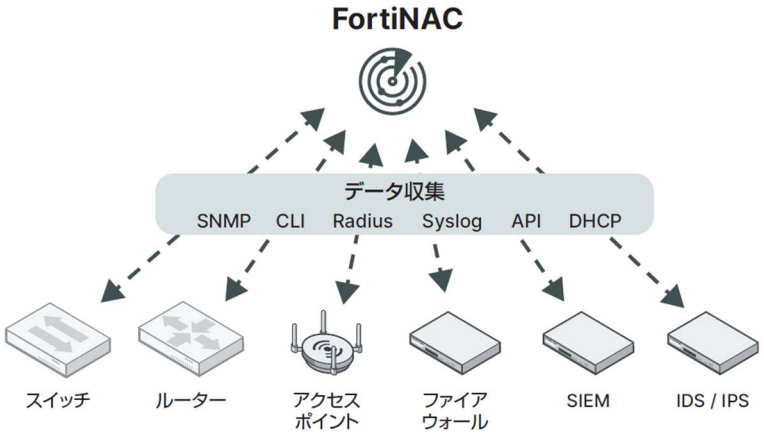
チェックリスト 対応項目	3-1, 3-2, 3-3
製品概要/特徴	物理・仮想・クラウドなど多様なサーバ環境に対応し、統一したセキュリティを提供することが可能な総合サーバセキュリティ対策製品。 ■ ひとつの Cloud One Workload Security / Trend Micro Deep Security エージェントに多彩なセキュリティ機能を実装。 ■ 工場内生産設備の弱点（脆弱性）を保護し、サポート終了 OS を使用したシステムの延命を支援。※ ■ コンプライアンス準拠を支援。 ■ クラウド環境にセキュリティを迅速に組込むことが可能。 ■ 下記の機能によりサーバを総合的に保護します。 • 不正プログラム対策 • IPS/IDS（侵入防御） • Web レピュテーション • ファイアウォール • アプリケーションコントロール • 変更監視 • セキュリティログ監視 
製品詳細 URL	www.go-tm.jp/c1ws www.go-tm.jp/tmds

2.3.5 フォーティネット

2.3.5.1 FortiGate

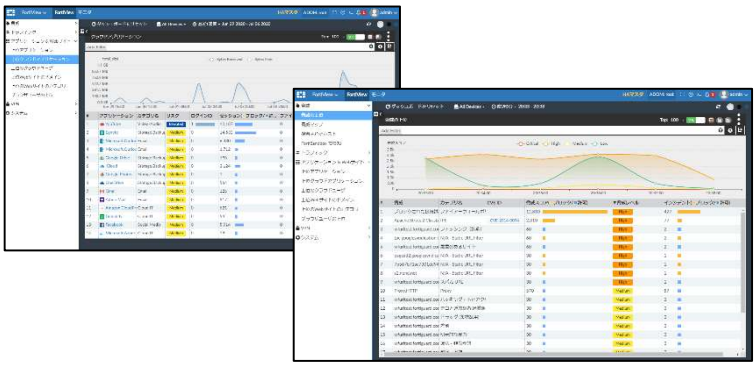
チェックリスト 対応項目	3-1, 3-2, 3-5, 3-7
製品概要/特徴	工場セキュリティガイドラインチェックリストを基に境界防御を始め、端末保護やネットワーク保護、そして Windows 端末 旧 OS や OT/IoT 機器脆弱性に対する仮想パッチの観点で OT セキュリティリスクの低減に寄与します。FortiGuard インダストリアルセキュリティサービスライセンスを活用することで OT プロトコルに特化した侵入防止システム（IPS）シグネチャ使用し、OT 環境におけるアプリケーション/デバイスを標的とした悪意のあるトラフィックを検知・排除します。本ライセンスを付加することで仮想パッチとして機能し、制御機器ベンダーのパッチ開発・適用よりも早くセキュリティ保護を可能とします。小型から大型まで多くの製品ラインアップを有し、自社開発 ASIC による高性能化、そして省電力で対環境面に大きく貢献します。  ※ この文書に記載されている仕様は、予告なしに変更されることがあります。この文書に含まれている情報の正確性および信頼性には万全を期しておりますが、Fortinet, Inc. は、いかなる利用についても一切の責任を負わないものとします。Fortinet®、FortiGate®、FortiCare®、および FortiGuard® は Fortinet, Inc. の登録商標です。その他記載されているフォーティネット製品はフォーティネットの商標です。
製品詳細 URL	https://www.fortinet.com/jp/products/next-generation-firewall

2.3.5.2 FortiNAC

チェックリスト 対応項目	2-6, 2-7, 3-6, 3-7
製品概要/特徴	工場セキュリティガイドラインチェックリストにおいては資産管理やネットワーク制御、保護の観点で OT セキュリティリスクの低減に寄与します。 特徴は以下、 可視化：PC やスマートフォンから IoT デバイスまで、ネットワーク接続されたエンドポイントをデバイスの IP アドレスや MAC アドレス、OS の種類はもちろん、デバイスの種類まで可視化可能 アクセス制御：ネットワークに接続するデバイスごとにネットワークのセグメンテーション、アクセスポリシー、ユーザ認証等により適切なアクセス制御が可能 自動レスポンス：セキュリティイベントに対するアクション(アラートメール、デバイス隔離など)の自動化で運用負荷を軽減 エージェントレススキャン：ネットワーク接続を試行するヘッドレスデバイスを検知し、識別 マルチベンダーサポート：2,350 以上のネットワーク機器（LAN スイッチやルータ)、170 以上のベンダーのネットワークデバイス（スイッチ、アクセスポイント、ファイアウォール、クライアント）との連携と構成をサポート FortiGate と連携：FortiGate で検知したインシデントを FortiNAC へ Syslog 通知し自動遮断/隔離が可能 

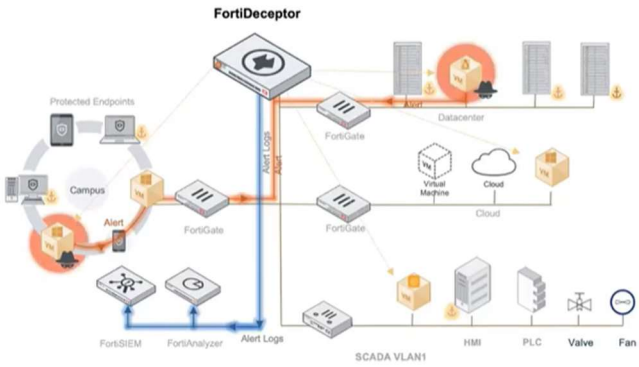
	※ この文書に記載されている仕様は、予告なしに変更されることがあります。この文書に含まれている情報の正確性および信頼性には万全を期しておりますが、Fortinet, Inc. は、いかなる利用についても一切の責任を負わないものとします。 Fortinet®、FortiGate®、FortiCare®、および FortiGuard® は Fortinet, Inc. の登録商標です。その他記載されているフォーティネット製品はフォーティネットの商標です。
製品詳細 URL	https://www.fortinet.com/jp/products/network-access-control

2.3.5.3 FortiAnalyzer

チェックリスト 対応項目	3-8
製品概要/特徴 	工場セキュリティガイドラインチェックリストにおいてはログ収集の観点で OT セキュリティリスクの低減に寄与します。 特徴は以下、 一元管理：すべてのフォーティネットセキュリティデバイスからログを自動的に収集、保存、分析します。大量のログを簡単に管理でき、さまざまな検索条件を使用して特定のイベントを検索することができます。単一の管理ポイントでの可視化と実用的な情報を提供し、潜在的なセキュリティ脅威を検知し、パフォーマンスを向上させ、ネットワークを最適化します。 統合アプローチ：MITRE ATT&CK®のユースケースにマッピングされた直感的なルールエディタを使用して、さまざまなタイプのログソースに対し、イベントを相関付けます。これにより、分析者は攻撃者に先んじて if-this-then-that（これがこうの場合はこうする）条件を設定し、対抗手段を講じることができます。 FortiGuard Labs との統合：新たな脅威や脆弱性に関する情報をリアルタイムで取り込むことで、正確な情報を得られるだけでなく、攻撃対象領域全体のリスク範囲を特定することができ、脅威  の検出を加速させ、早急な対応が必要な領域をピンポイントで特定することができます。

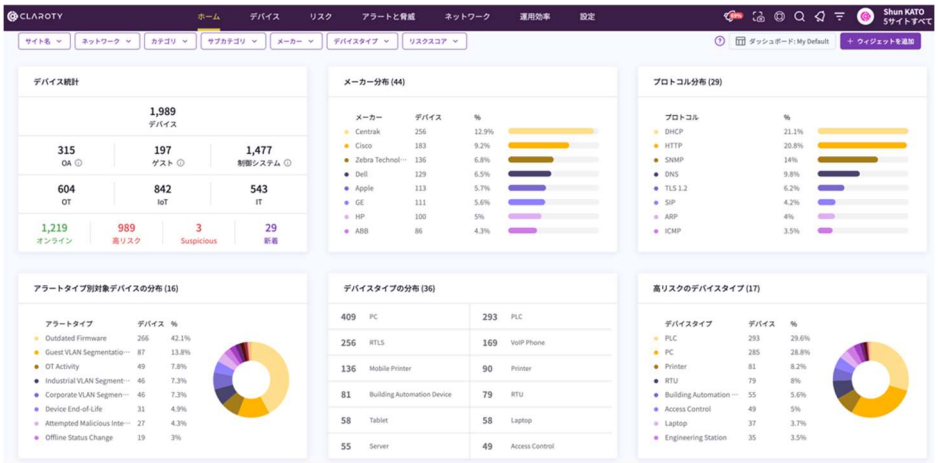
	※ この文書に記載されている仕様は、予告なしに変更されることがあります。この文書に含まれている情報の正確性および信頼性には万全を期しておりますが、Fortinet, Inc. は、いかなる利用についても一切の責任を負わないものとします。Fortinet®、FortiGate®、FortiCare®、および FortiGuard® は Fortinet, Inc. の登録商標です。その他記載されているフォーティネット製品はフォーティネットの商標です。
製品詳細 URL	https://www.fortinet.com/jp/products/management/fortianalyzer

2.3.5.4 FortiDeceptor

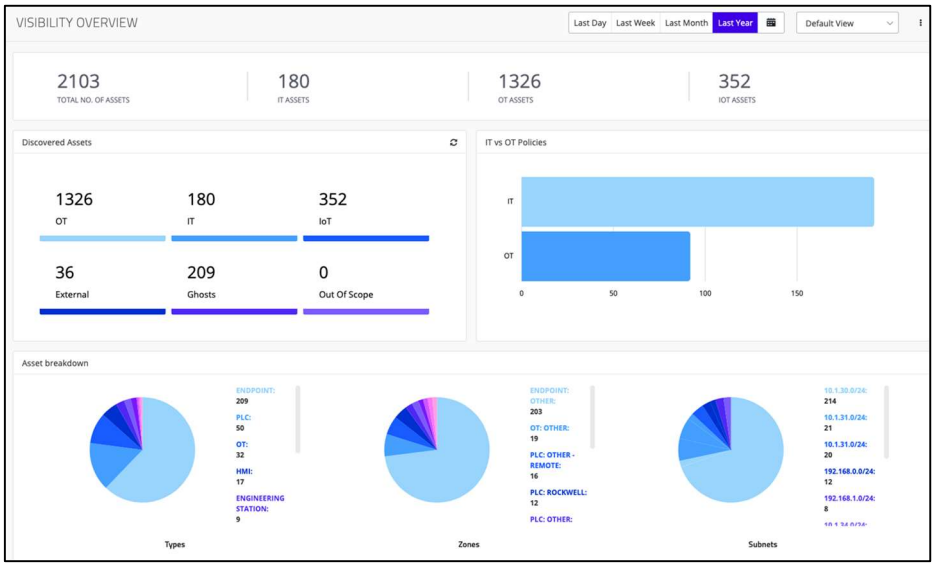
チェックリスト 対応項目	3-7(ネットワーク保護)
製品概要/特徴	工場セキュリティガイドラインチェックリストにおいてはデコイとルアーを使ったアクティブディフェンスによりネットワーク保護の観点で OT セキュリティリスクの低減に寄与します。 特徴は以下、豊富なデコイとルアー：お客様の環境に合わせて細かくカスタマイズされた IT/ OT/ IoT のデコイとルアーをウィザード形式でセットアップできるとともに、IT 環境と OT 環境にまたがって分散ディセプション導入環境を一元管理できます。 迅速な調査：アクセス、使用ツール、ラテラルムーブメントなどの全アクティビティの攻撃活動時系列にインシデントをインテリジェントに相関付けすることで迅速な調査を実現でき、FortiGuard Labs が提供するコンテキスト脅威インテリジェンスによって階層化されています。 フォーティネット製品との連携：FortiGate、FortiNAC、FortiSOAR、サードパーティを含むセキュリティファブリック統合によって初期段階の攻撃を排除します。FortiSIEM および FortiAnalyzer を通じて脅威の可視化と探索を強化します。  ※ この文書に記載されている仕様は、予告なしに変更されることがあります。この文書に含まれている情報の正確性および信頼性には万全を期しておりますが、Fortinet, Inc. は、いかなる利用についても一切の責任を負わないものとします。 Fortinet®、FortiGate®、FortiCare®、および FortiGuard® は Fortinet, Inc. の登録商標です。その他記載されているフォーティネット製品はフォーティネットの商標です。
製品詳細 URL	https://www.fortinet.com/jp/products/fortideceptor

2.3.6 クラロティ

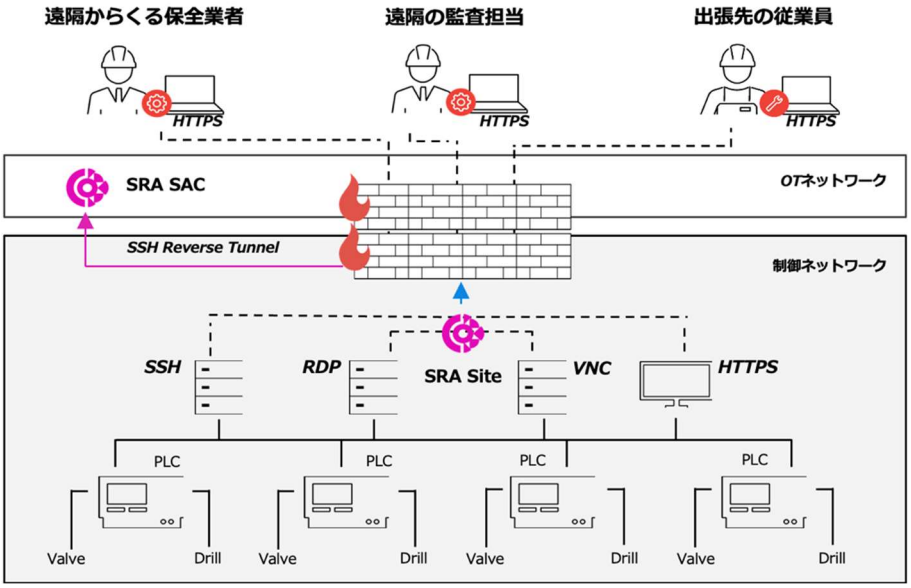
2.3.6.1 xDome

チェックリスト対応項目	2-6, 2-8, 3-2, 3-5, 3-7
製品概要/特徴	工場ネットワーク内につながる機器を 5 種類のデータ収集方法を活用することによって検出、台帳化します。資産台帳化された各機器については関連する公開脆弱性(CVE)との自動紐づけをモデル番号やファームウェアをベースに行い、定期評価に寄与します。 該当する脆弱性情報については、EPSS, KEV などの悪用可能性指標を元にした対応優先順位付け情報を提示し、対策の支援をします。 通信パケットから VLAN テーブル・マトリクスを自動作成することで、現状の VLAN セグメンテーションの状況把握や、推奨 ACL ポリシーの作成によるデバイス・ゾーンベースでのセグメンテーション管理を支援します。 既知の脅威コマンドに当てはまる通信パケットや、ポリシーに違反する通信が発信された場合にはアラート発報し、ユーザーに通知することができます。 
製品詳細 URL	https://discover.claroty.com/ja-jp/xiot/product/xdome

2.3.6.2 CTD

チェックリスト対応項目	2-6, 2-8, 3-2, 3-5, 3-7
製品概要/特徴	工場ネットワーク内につながる機器を 5 種類のデータ収集方法を活用することによって検出、台帳化します。資産台帳化された各機器については関連する公開脆弱性(CVE)との自動紐づけをモデル番号やファームウェアをベースに行い、定期評価に寄与します。 資産の情報や通信振る舞いベースにして仮想ゾーンを作成し、仮想ゾーン間の通信ポリシーを作成することができます。これにより重要度に応じたゾーンの定義やゾーン間の通信ルール作成することで、セグメント管理を支援します。 既知の脅威コマンドに当てはまる通信パケットや、ポリシーに違反する通信が発信された場合にはアラート発報し、ユーザーに通知することができます。 
製品詳細 URL	https://discover.claroty.com/ja-jp/xiot/product/ctd

2.3.6.3 SRA

チェックリスト 対応項目	3-6
製品概要/特徴	SRA は OT 環境特有の運用、管理、およびセキュリティのニーズに特化して構築され、セッションの承認、リアルタイム監視、録画などが可能なリモートアクセスソリューションです。以下の特徴があります。 - ２要素認証 - リモートユーザ毎の接続端末制限 - 接続可能時間の制限 - 接続中のライブ監視、内容の録画記録 - 管理者による接続の強制遮断 - 境界ファイヤーウォールのポート開放を最小化 
製品詳細 URL	https://discover.claroty.com/ja-jp/xiot/product/sra

2.4 ライフサイクル面での対策

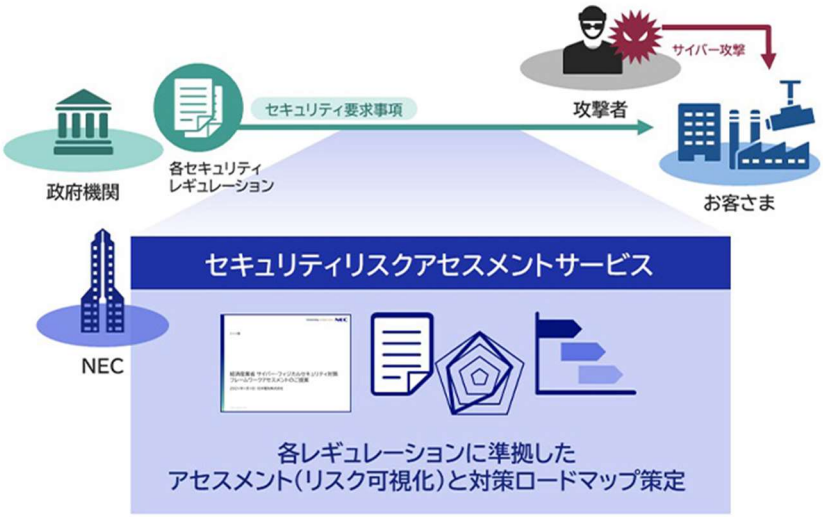
ライフサイクル面での対策に対応する各社のサービス／製品は、下記となります。

2.4.1 NEC

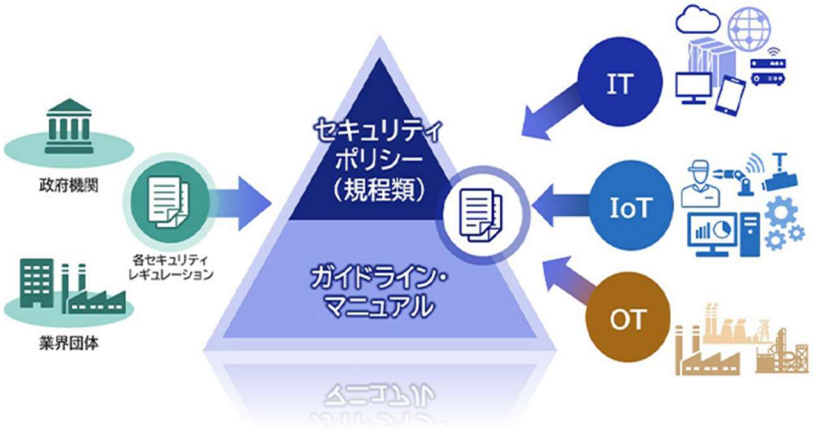
2.4.1.1 ActSecure セキュリティサービス

チェックリスト 対応項目	2-5
製品概要	サイバー攻撃の検知・分析を行うマネージド・セキュリティサービス ① 専門のアナリストがセキュリティログの分析を行い、検知した脅威インシデントをお客様管理者へ即座に通報します。 ② マルウェア侵入などの脅威発生時の迅速な対応が可能となります。 ③ お客様は、自社内に SOC(Security Operation Center)を構築することなく、安心・安全なセキュリティ環境を実現 できます。
製品詳細 URL	https://jpn.nec.com/actsecure/actsx_mss.html

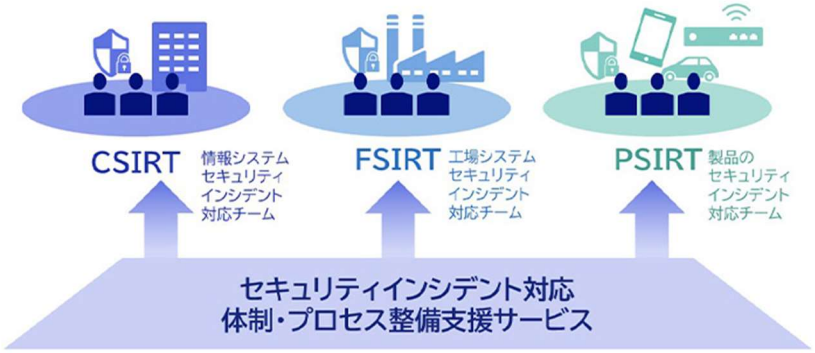
2.4.1.2 セキュリティリスクアセスメントサービス

チェックリスト 対応項目	0-1、0-2、0-3、1-1、2-1、2-4、4-4
製品概要	工場セキュリティガイドラインの内容に基づき、公開済みチェックリスト内容から更に詳細化した事項について確認。工場セキュリティの専門家が分析して、推進ロードマップを策定します。 ① 各種セキュリティレギュレーション・ガイドラインをベースにNEC が独自で作成したチェックリストにより、お客さまの課題を網羅的に抽出します。 ② 公的資格を有するセキュリティスペシャリストチームが多角的にインタビューと分析を実施し、現状のリスクを評価します。 ③ 各レギュレーションの要求事項ごとに最適なソリューションを紐づけており、優先順位を考慮して、改善や強化のための対策を提示します。 
製品詳細 URL	https://jpn.nec.com/cybersecurity/service/professional/consulting/risk_assessment/

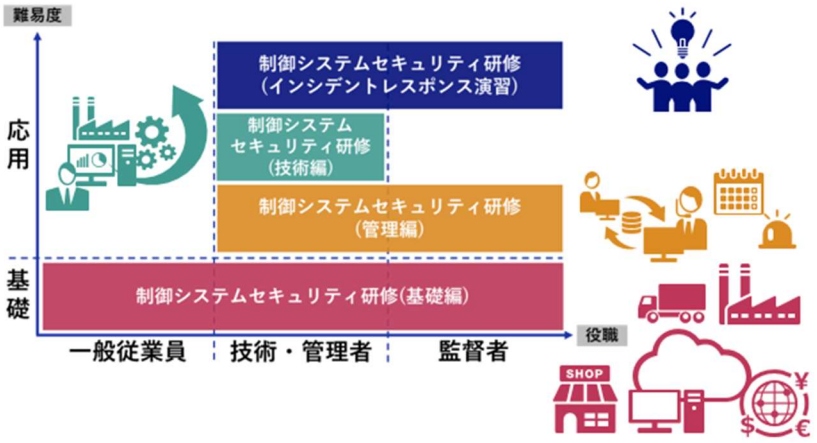
2.4.1.3 ポリシー策定支援サービス

チェックリスト対応項目	2-2、2-3、2-6、2-7、2-8、2-9、2-10、2-11、2-12、2-13、4-5、4-6
製品概要	工場におけるセキュリティ体制、システムへのセキュリティ整備方針、運用手順などを、工場セキュリティガイドラインの内容に基づき整備します。 ① 各種セキュリティレギュレーション・ガイドラインをベースに、お客さまの事業特性を踏まえたセキュリティポリシーを整備します。 ② 公的資格を有するセキュリティスペシャリストチームが、技術面・組織面から分析のうえ策定します。 ③ セキュリティポリシー策定後の運用支援やコンサルテーションの提供も可能です。 
製品詳細 URL	https://jpn.nec.com/cybersecurity/service/professional/consulting/policy/

2.4.1.4 セキュリティインシデント対応 体制・プロセス整備支援サービス

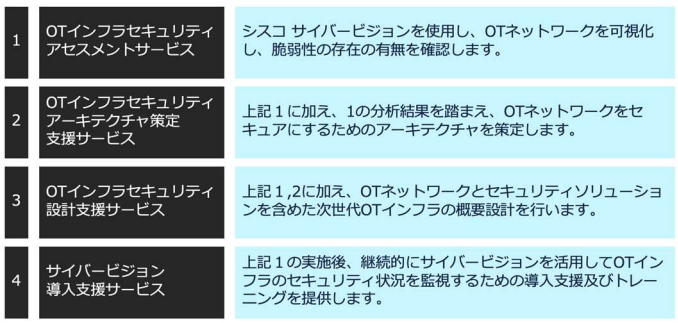
チェックリスト 対応項目	1-2、1-3、1-4、1-5、2-5、4-1、4-3、
製品概要	工場におけるインシデント発生時の被害最小化・迅速な復旧、脆弱性への迅速な対応が可能な組織体制づくりを支援します。 ① 10 数年にわたる、NEC-CSIRT/PSIRT の運用実績、ICT システムや運用サービスを提供してきた技術力・ノウハウを基に支援します。 ② 公的資格を有するセキュリティスペシャリストチームが、技術面・組織面から組織体制の構築、プロセス策定を支援します。 ③ プロセス策定後の運用支援やコンサルテーションの提供も可能です。 
製品詳細 URL	https://jpn.nec.com/cybersecurity/service/professional/consulting/incident_response/index.html

2.4.1.5 制御システムセキュリティ研修

チェックリスト 対応項目	1-5、2-5、4-2、
製品概要	制御システムのオープン化や攻撃の高度化・巧妙化に伴うサイバーリスクの増加へ対応するため、各々の役割に応じた制御システムセキュリティ対策の技術・知識の獲得をご支援します。 ① 一般従業員から管理者、監督者層まで様々な階層・目的・レベルに合わせた教育メニューを用意しています。 ② インシデント発生時の対応手順について演習形式で体験することにより、実業務への効果が期待できます。 ③ 教育以外のコンサルティング（アセスメント、ポリシー策定、等）やセキュリティ製品（OT-IDS、OT-FW、等）の提供も可能です。 
製品詳細 URL	（現在準備中）

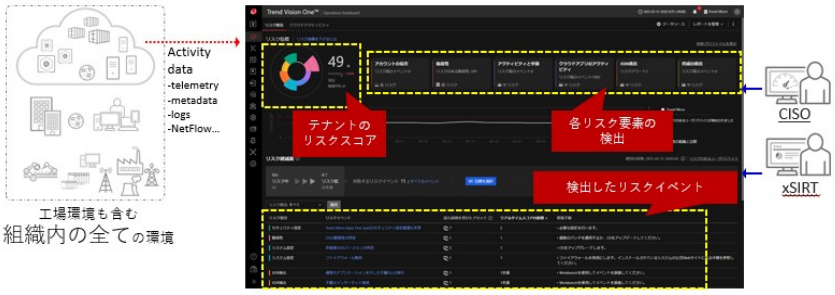
2.4.2 シスコシステムズ

2.4.2.1 OT セキュリティ関連サービス

チェックリスト 対応項目	2-6,3-7
製品概要/特徴	OT セキュリティ関連サービスは、OT セキュリティ対策を進める上で必要となる現状把握による As-Is から To-Be に向けたセキュリティアーキテクチャの策定と実装に向けた概要設計を支援します。 以下の特徴があります。 ■ Cisco Cyber Vision を使用して工場ネットワークの可視化を行い現状どのような脆弱性やセキュリティ課題があるか分析します。 ■ 明らかになったセキュリティ課題の分析結果からどのように工場ネットワークのセキュリティを実装するかアーキテクチャ方針を策定します。 ■ さらに策定されたアーキテクチャに準拠した工場ネットワークのセキュリティ実装に向けた概要設計を実施します。 ■ Cisco Cyber Vision による工場セキュリティ状況を定常的に監視するための導入支援及びトレーニングを提供します。 ・シスコCXのOTインフラセキュリティ強化支援サービス 
製品詳細 URL	https://www.cisco.com/c/ja_jp/solutions/internet-of-things/iot-security.html#~services

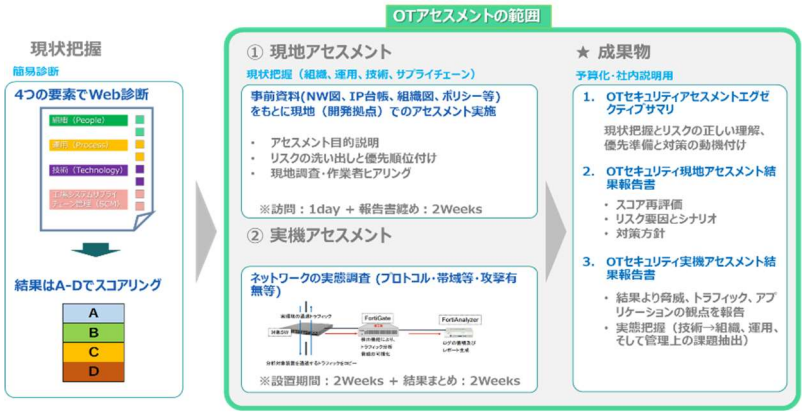
2.4.3 トレンドマイクロ

2.4.3.1 Trend Vision One

チェックリスト対応項目	3-7, 3-8
製品概要/特徴	DX が進む組織のセキュリティを支える新しいセキュリティプラットフォーム。 Trend Vision One は高度なスレットインテリジェンスと相関分析による迅速なインシデント対応、環境全体のリスクの可視化を提供し、 リスクに基づく動的なアクセス制御でゼロトラストの実現を支えるサイバーセキュリティプラットフォームです。 XDR により工場内で発生したセキュリティイベントを相関分析し脅威を可視化します。 
製品詳細 URL	https://www.trendmicro.com/ja_jp/business/products/one-platform.html

2.4.4 フォーティネット

2.4.4.1 OT セキュリティアセスメントサービス、コンサルティングサービス

チェックリスト対応項目	全項目 ※ 但し、アセスメントでは現状と OT リスクを把握することを目的としているため範囲は対策準備までとなります。継続コンサルティングサービスにて組織、運用の対策支援が可能です
製品概要/特徴	OT セキュリティアセスメントは、OT セキュリティ対策を進める上で、「どのように進めたらよいのか」、「どのような対策を実施すべきなのか」、「どこまでコストをかけて実施すべきなのか」などの課題に対し、本ガイドラインチェックリストを活用して、「現地アセスメント」と「実機アセスメント」を実施することでリスクに応じたあるべき姿の提案と対策支援指針を提供します。また、その後の組織、運用の建付け支援としてコンサルティングサービスを提供しています。特徴は以下、 ■ ガイドライン準拠社内外の説明責任を果たすことが可能 ■ 無償 Web 診断で簡易的に現状を把握可能 （本アセスメントへの準備） ■ 組織、運用、技術のバランス対応によって実効性を担保 ■ 現場ヒアリング、製造現場調査含む現地アセスメントと実機を活用した裏付けデータ取得の実機アセスメント 
製品詳細 URL	https://www.fortinet.com/jp/promos/ot-security-assessment

2.5 サプライチェーン面での対策

サプライチェーン面での対策に対応する各社のサービス／製品は、下記となります。

本版での掲載サービス／製品はありません。
次版以降に追記予定です。

3. 問合せ先

「2 セキュリティ対策と対応サービス／製品」に記載した各社の問い合わせ先は、下記のとおりです。(五十音順)

社名	URL	問い合わせ窓口	E-mail
日本電気株式会社	https://jpn.nec.com/	https://jpn.nec.com/contactus/business.html **（法人お問合せ窓口）**	-
株式会社 PFU	https://www.pfu.ricoh.com/	-	inetsec-pro@ml.ricoh.com
シスコシステムズ合同会社	https://www.cisco.com/c/ja_jp/buy.html	0120-092-255	-
トレンドマイクロ株式会社	www.trendmicro.com	03-5334-3601 （法人お問い合わせ窓口）	-
フォーティネットジャパン合同会社	www.fortinet.com/jp/promos/ot-security	-	-
クラロティ	https://discover.claroty.com/ja-jp/xiot	-	salesjp@claroty.com

4. 商標について

OWL ロゴ、OWL DualDiode は、Owl Cyber Defense Solutions, LLC の登録商標です。

Nozomi Networks ロゴ、Nozomi Networks Guardian は、Nozomi Networks, Inc.の登録商標です。

ForeScout eyeInspect は、ForeScout Technologis, Inc.の登録商標です。

Darktrace、Darktrace ロゴは、Darktrace Limited の登録商標です。

Splunk は、Splunk, Inc.の登録商標です。

iNetSec は、PFU の登録商標です。

Cisco Cyber Vision, Catalyst IE 3000, Cisco Secure Firewall ISA3000, Cisco Secure Network Analytics, Cisco Identity Services Engine は、シスコシステムズの登録商標です。

TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスタービジネスセキュリティサービス、SafeSync、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、SECURE CLOUD、Trend Micro VDI オプション、おまかせ不正請求クリーンナップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おもいでバックアップサービス、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンナップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルラ

以上