MITSUBISHI ELECTRIC
Changes for the Better

三菱電機サイバーセキュリティーソリューション
OTGUARD®

社会的背景と経営課題

「Society5.0」に向け社会が進化し、あらゆる面でIT※1との融合が進む一方、サイバー空間の秩序や安全に脅威を与えるような著しく悪意を持ったサイバー攻撃が多発しています。情報（IT）システムだけでなく、インフラ設備やプラント設備などの制御（OT※2）システムにも影響を与え、事業継続性が損なわれる事態が発生した場合、企業収益に甚大な影響を与える事例が増加しています。

経営者が適切なセキュリティー投資を行わずに社会に対して損害を与えてしまった場合、経営責任や法的責任が問われる可能性が指摘されており、今後さらに経営戦略としてのセキュリティー投資は必要不可欠になっています。

※1　IT（Information Technology）：情報技術
※2　OT（Operational Technology）：制御技術

相談事例

CASE 1　サイバー攻撃に対するリスクがどこにあるか把握しておらず、最適な対策方法がわからない

CASE 2　制御システムは更新せず継続利用して、現行の運用方法も維持したまま、セキュリティー対策だけ強化したい

CASE 3　セキュリティー対策実施後も継続した情報提供やインシデント発生時・機器故障時のサポートをしてほしい

このようなお悩みに、OT・ITを融合した最適なソリューションをご提供いたします。
三菱電機サイバーセキュリティーソリューション「OTGUARD®」は、
これまでの設備投資や蓄積した運用ノウハウ、しくみなどの経営資産を無駄にすることなく、
経営課題を解決いたします。

経営課題を解決する制御システムに最適かつ最も現実的な手段「OTGUARD®（オオティガード）」をご提供します。

三菱電機サイバーセキュリティーソリューション

OTGUARD

オオティガード

FEATURES 1
事業継続の健康診断、セキュリティーアセスメント

- OT・ITを融合した脆弱性診断によるリスクの見える化
- マルウェアの動きやクラッカー（コマンド）の攻撃手法に対応した対策立案

FEATURES 2
既存システムはそのままで強固なセキュリティー対策

- 既存システム機器を更新せず、セキュリティースイッチのアドオンで対策可能
- 不正プログラム（マルウェア、マルコード、等）を検知・遮断しサイバー攻撃を監視

FEATURES 3
管理業務を強力に支援する充実した運用サービス

- 機器故障時の迅速な対応や最新のセキュリティーエンジンへの更新サービス
- 定期診断によりシステム状態を診断し、最新の脅威や対策技術への改善・提案

FEATURES 1

事業継続の健康診断、セキュリティーアセスメント

経営課題のセキュリティー対策は、現状分析（リスクアセスメント）から始まり、
『OTGUARD®』によるサイバーセキュリティーのPDCAサイクルで対策・強化します。

制御システムは、建物の設備全体を動かすために必要なインフラ設備（電力供給、等）をコントロールしています。既存システムや今後運用を開始するシステムにおいて、脆弱性診断によるリスクの見える化や対策の立案などを行うセキュリティーアセスメントは、事業継続を行うために必要な経営資産です。

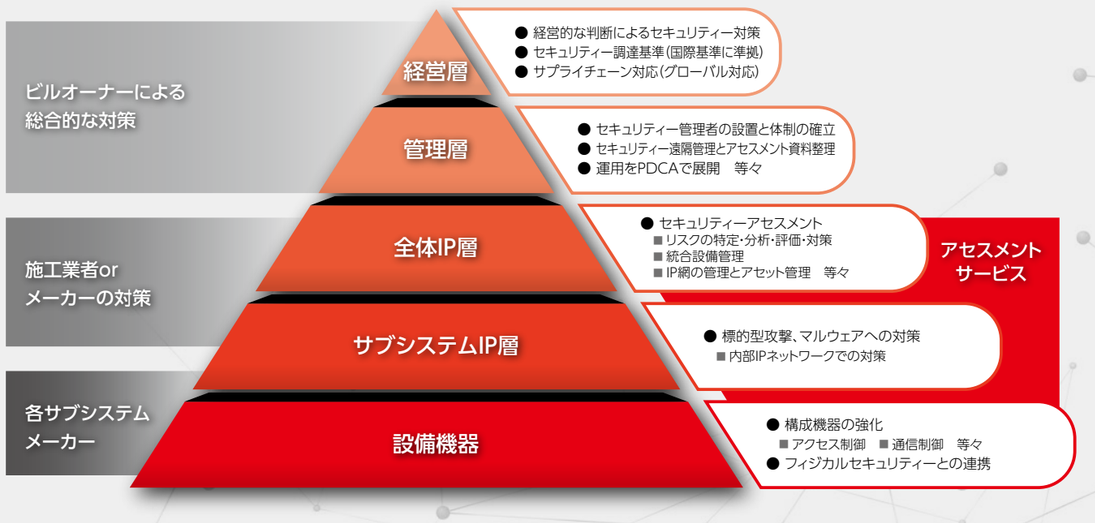
PDCAサイクル（経営方針への組み込み）

サイバーセキュリティー対策は一度行なったら終わりではありません。環境の変化に合わせて、積極的に対策を行い、新たな脅威に対応していく必要があります。設備全体のサイバーセキュリティー強化とともに、リスクの見える化によるインシデント発生要因の特定（計画・企画）、実施、点検・監査、見直し・改善というPDCAサイクルにもとづき、お客様のニーズに合わせた継続的な対策を支援します。

OT・ITを融合したセキュリティーアセスメント

制御システムへのサイバー攻撃対策は、現場（運用・管理）目線でのセキュリティーアセスメントが重要です。三菱電機は、重要インフラ向け制御（OT）システムにおける多数の納入実績を活かして、ユーザー視点に立った現場目線での「OT」とクラッカー（コマンド）の攻撃手法に対応した「IT」の特長を融合したセキュリティーアセスメントを実現いたします。

サイバーセキュリティーの組織体制とアセスメントサービスの位置付け



アセスメントサービスメニュー

サービスメニュー	概要	期間（目安）
セキュリティーアセスメント・ベーシック	限定した範囲で現状のセキュリティーレベルを短期間でチェック。リスクの見える化とインシデント発生要因の特定を実施します。	2ヶ月～
セキュリティーアセスメント・アドバンス	現状のセキュリティーリスクを可視化（見える化）した上で、綿密かつ中長期的なセキュリティー対策を提示します。	6ヶ月～

サービス内容	ベーシック	アドバンス
ヒヤリング、図面調査	○	◎
現地調査	○	◎
セキュリティーリスクの見える化	○	◎
インシデント発生要因の特定	○	◎
実ネットワークデータ採取	—	◎
脆弱性診断データ採取	—	◎
セキュリティー対策企画	—	◎

FEATURES 2

既存システムはそのままで強固なセキュリティー対策

OTGUARD®は、不正プログラム（マルウェア、マルコード、等）の検知・遮断を分散処理で実現する
セキュリティースイッチを適用した強固なサイバーセキュリティー対策です。

制御システムは10年から20年近くに渡って運用されるため、最新のセキュリティー対策を実装した機器で構成されたシステムに更新することが容易ではない場合があります。そのため、OSの最新化を行うことができない場合もあり、サポート切れのOSをそのまま使っているリスクが存在しています。また、CPUの稼働率が一時的に高まるマルウェア対策ソフトウェアを容易に導入できないリスクも存在しています。

OTGUARD®は、内部IPネットワーク機器であるセキュリティースイッチをアドオンで配置することにより、既存システムの資産を活かしたサイバーセキュリティー対策が可能です。

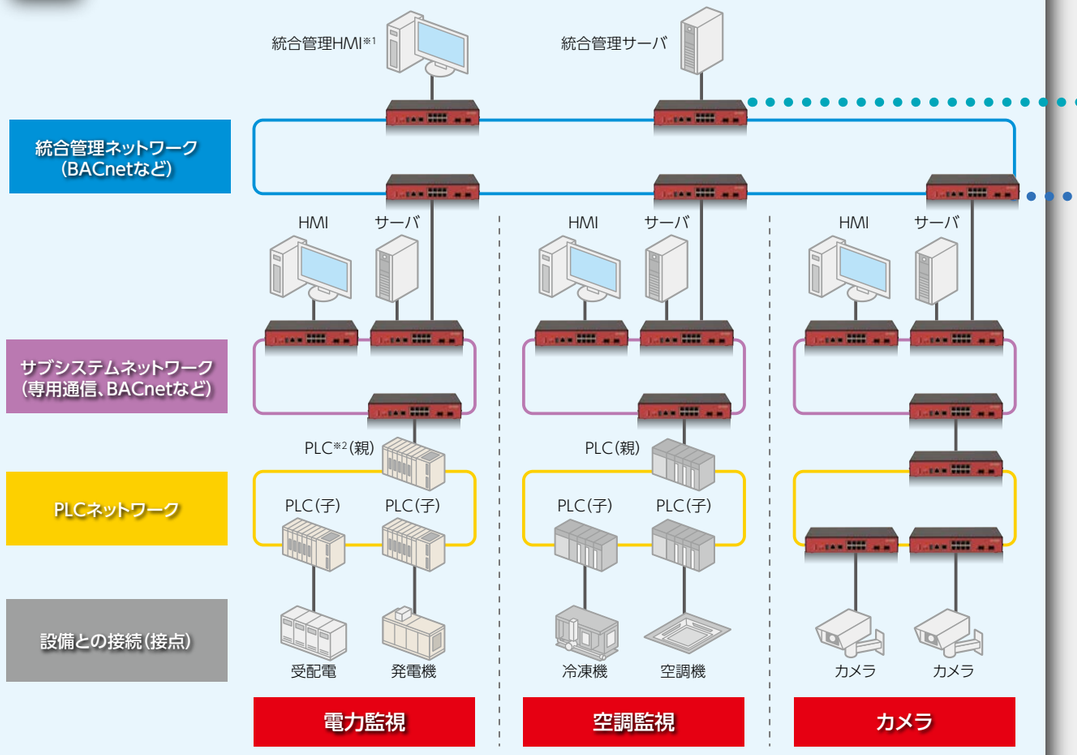
対策実行手順

お客様のシステムへの導入は3ステップで行います。

POINT!
お客様のセキュリティー要件に合わせて適用が可能!

ステップ1 セキュリティースイッチ適用

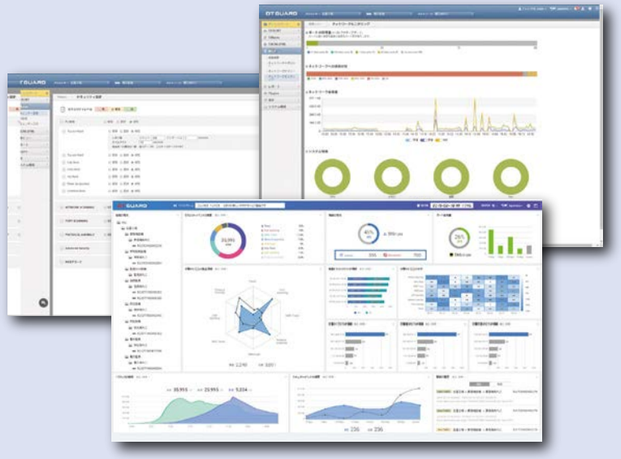
セキュリティーアセスメントの結果をもとに、最適な場所へセキュリティースイッチを配置します。



ステップ2 サイバー攻撃監視機能の実装【基本】

セキュリティースイッチの設定やスイッチ毎にアラートを表示します。

サイバー攻撃監視機能
- アラート表示
- スイッチ単位のトラフィック状態監視
- スイッチの基本設定
- セキュリティーエンジンの設定　等



セキュリティースイッチ
監視ネットワーク

サイバー攻撃
監視HMI

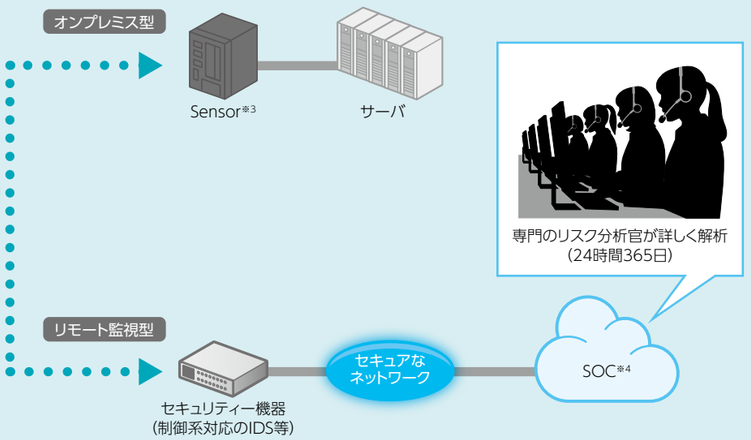
ステップ3 ネットワーク状態、接続機器管理機能の実装、リモート監視【オプション】

ネットワーク情報を起点とした接続機器管理を行います。
また、リモート監視サービスとして、専門のリスク分析官と連携し、インシデントが発生した場合に詳しく分析して、お客様の運用をサポートします。

接続機器管理機能
- IPアドレス管理
- 設置場所管理　等

ネットワーク状態管理機能
- 通信状態見える化
- サイバー脅威の検知・分析
- リモート監視　等

ミラーポート
接続



※お客様毎に最適な最新のセキュリティー製品を組合せご提案いたします。

※1　HMI（Human Machine Interface）：人間と機械が情報をやり取りするための装置
※2　PLC（Programmable Logic Controller）：制御装置
※3　Sensor ：監視対象の通信を取得できる場所に設置し、監視対象通信データの収集、パケットの分析、メタデータへの変換、および正常時のトラフィック・パターンを学習し、その結果をサーバへ送信する装置
※4　SOC（Security Operation Center）：セキュリティー監視を行う拠点

FEATURES 2

既存システムはそのままで強固なセキュリティー対策

制御システムは24時間365日連続した運用が求められます。
そのため、制御システムの構成品がマルウェアに感染しても運用の継続が必要です。

なぜ内部IPネットワークでのセキュリティー対策が必要か?

制御システムは、インターネットなど外部のネットワークに接続せずにクローズド環境で構成されているシステムが多く、サイバー攻撃に対して比較的安全とみなされ、セキュリティー機能の実装が不完全でした。

このような制御システムにおいて、近年、Stuxnetやランサムウェアの事例のように、マルウェアの侵入を許してしまうと、システムの運用に甚大な影響を与える事例が報告されています。また、近年増加しつつある脅威として、ファイルレスマルウェア※1のように、従来の対策だけではサイバー攻撃から防御することが困難な状況となっています。

さらに、マルウェアのみならず内部侵入者により物理的なセキュリティー対策が突破され、内部IPネットワークへの不正アクセスを起因とした攻撃により、システム運用に甚大な影響を及ぼす可能性が指摘されています。

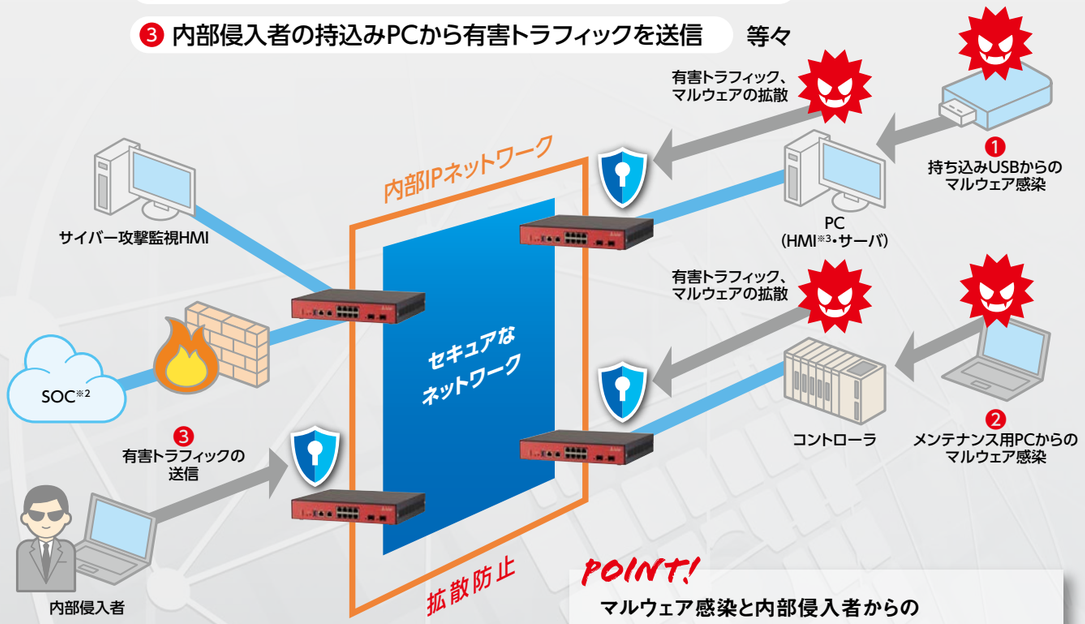
そのため、マルウェア感染や内部侵入者による攻撃を前提として、エンドポイント機器(PCやコントローラ、等)での対策のみではなく、システム全体に対策が可能な内部IPネットワークを含めた総合対策が必要となっています。

マルウェア感染・内部侵入者からの攻撃を前提とした内部対策

内部IPネットワークにセキュリティースイッチを配置することにより、マルウェアの拡散(ラテラルムーブメント)や内部侵入者からの攻撃それぞれに有効な対策が可能です。

脅威の例

1. 持込みUSBからPCにマルウェアが感染
2. メンテナンス用PCからコントローラ等にマルウェアが感染
3. 内部侵入者の持込みPCから有害トラフィックを送信　等々



POINT!
セキュリティースイッチ毎で分散処理を行っているため、
サイバー攻撃監視HMIがダウンしても防御可能!

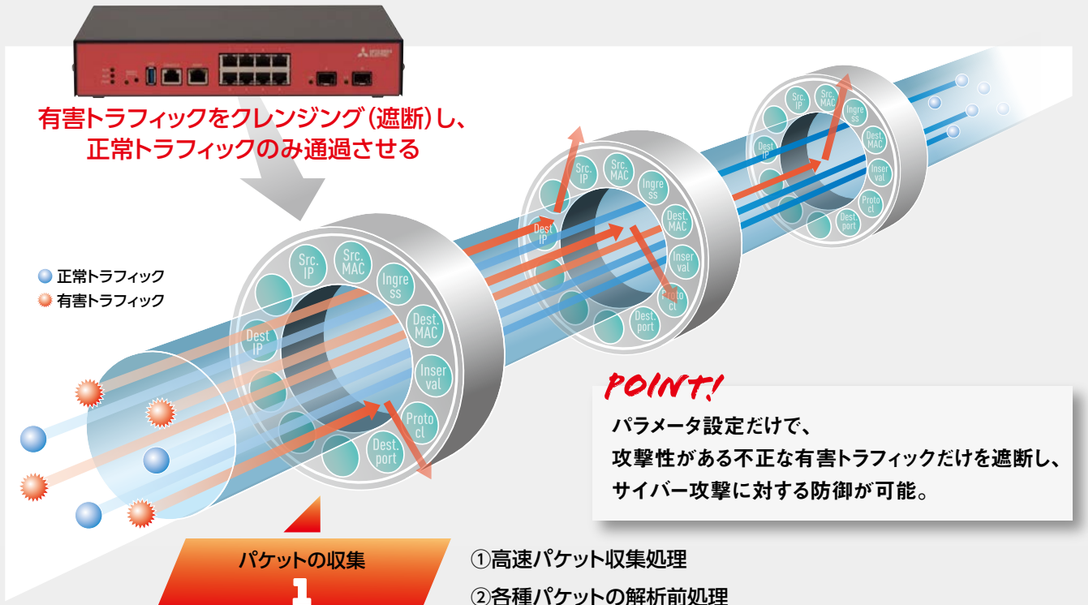
POINT!
マルウェア感染と内部侵入者からの
攻撃それぞれに有効な対策が同時に実現可能!

※1 ファイルレスマルウェア:実行ファイルがディスク上に保存されず、メモリ上で実行されるマルウェア
※2 SOC (Security Operation Center):セキュリティー監視を行う拠点
※3 HMI (Human Machine Interface):人間と機械が情報をやり取りするための装置

OTGUARD

セキュリティースイッチ機能

パケットの各要素(送信元IP、宛先IP、送信元MAC、宛先MAC、ポート番号、パケット数、タイムスタンプ、等)を活用して、それぞれの送信元/宛先別の使用頻度、パケットの間隔、隣接タイムのパケット情報などをリアルタイムに分析し、有害トラフィックをクレンジングすることにより、必要なトラフィックのみを通過させます。また、セキュリティースイッチの物理ポート毎にアクセスコントロールが可能です。



POINT!
パラメータ設定だけで、
攻撃性がある不正な有害トラフィックだけを遮断し、
サイバー攻撃に対する防御が可能。

1. パケットの収集
2. 有害トラフィックの分析
3. 有害トラフィックの遮断

①高速パケット収集処理

②各種パケットの解析前処理
- 攻撃トラフィックと業務トラフィックなどの仕分け(メタデータ化)

③脅威分析と検知処理
- 相関分析モデルをベースとした分析技術
- 相関分析モデル化されたメタデータから脅威トラフィックを分析
- 新たな脅威にも柔軟に対応可能

④設備機器管理(IP・Mac管理)と不正ネットワーク機器の検知処理

セキュリティー機能

分類	攻撃タイプ
サービス妨害攻撃(DoS 攻撃)	TCP syn flooding / TCP ack flooding / UDP flooding / ICMP flooding / ARP flooding / Mac flooding / Unknown flooding
サービス探索攻撃(Port Scan)	TCP syn scan / TCP ack scan / UDP scan / Stealth scan
ネットワークデバイス探索攻撃(Network Scan)	TCP network scan / UDP network scan / ICMP network scan / Non-echo ICMP network scan / ARP network scan
プロトコル異常検知	Land attack / Invalid TCP flags / ICMP fragments / TCP fragments / Smurf attack
なりすまし攻撃	ARP spoofing / IP spoofing
SMB通信	inv-access / Brute-force / SMB-Scan / SMB-Filter
フィルタリング	IPスクリーン / ドメインフィルター
IPv6	Host Scan / ネイバースプーフィング / DAD DoS / IPv6 filter

FEATURES 3

管理業務を強力に支援する充実した運用サービス

サポート窓口による技術支援や機器故障時の迅速な対応、最新セキュリティーエンジンへの更新や
定期的なネットワーク診断による最新脅威への対策支援を行い、システム管理・運用をサポートします。

システム運用支援からサイバーセキュリティー対策計画支援まで幅広いサポート

システムの構成変更や運用を取り巻く環境の変化、新たな脅威によるサイバー攻撃の進化に対応するため、サイバーセキュリティー対策を継続的に行い、信頼・資産を守る必要があります。

OTGUARD®は充実したサービスメニューにより、お客様のシステム管理・運用業務のサポートからサイバーセキュリティー対策計画までをトータルサポートします。

業務支援	システム管理業務における技術的支援、機器保守、ソフトウェア最新化
診断・評価	通信内容・機器状態確認、評価と報告
報告・提案	サポート対応や最新情報に基づく総合評価、改善提案

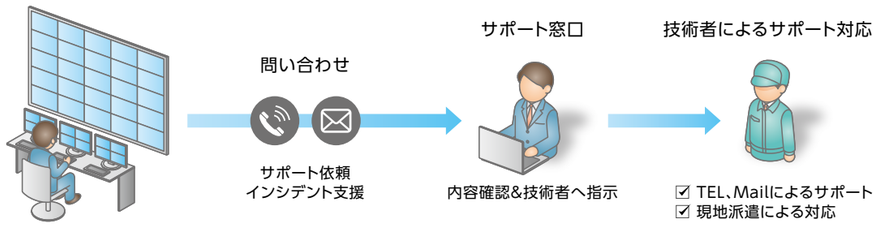
これらの総合的なサイバーセキュリティー対策のサポート(運用・保守サービス～評価・提案)を行うことにより、安心・安全なシステム運用が継続されるよう支援します。

7つの運用サービスメニュー

7つのサービスメニューによりお客様の管理業務をサポートします。

サービス 1　テクニカルサポートサービス

お客さまからの様々な問い合わせに対して技術者によるサポートやセキュリティースイッチの最新セキュリティーエンジンの適用要否の検討・報告を行うことによりシステム運用を支援します。
また、インシデント発生時には復旧支援を行い、対策計画についてサポートします。



サービス 2　最新脅威・対策技術提供サービス

サイバーセキュリティーに関する最新情報(社会的動向・脅威・技術　等)を提供することで、お客様のサイバーセキュリティー対策計画への支援を行います。

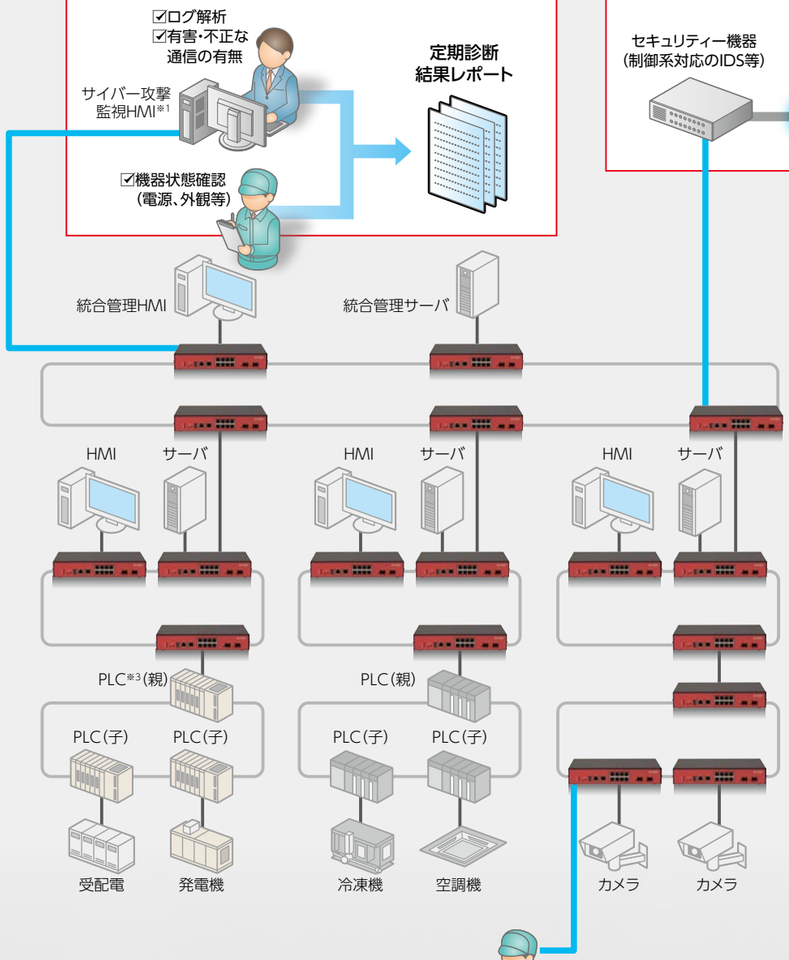
※1　HMI (Human Machine Interface)：人間と機械が情報をやり取りするための装置
※2　SOC (Security Operation Center)：セキュリティー監視を行う拠点
※3　PLC (Programmable Logic Controller)：制御装置

OTGUARD

サービス 3

定期診断サービス

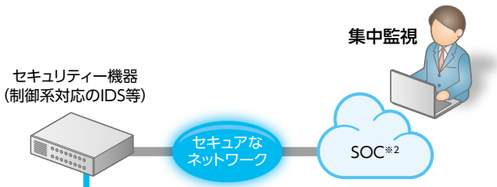
通信内容に関するログ解析・セキュリティースイッチの機器状態確認行います。
ログ解析による有害トラフィック・不正アクセスの有無および通信内容評価を行い、機器状態確認結果と併せて診断結果レポートとして提出します。



サービス 4

SOC(Security Operation Center)サービス

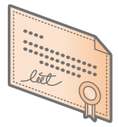
お客様のシステムを24時間365日体制で監視し、不正アクセスを検知した場合には専門のリスク分析官が詳しく解析し、インシデントへの対応のサポートを行います。
遠隔地で複数拠点を集中監視することが可能となります。



サービス 5

セキュリティーエンジン サブスクリプションサービス

最新のセキュリティーエンジンをお使い頂くための定額利用権に加え、セキュリティーエンジンが更新された場合、更新情報をメール等でご連絡するサービスです。



サービス 6

セキュリティースイッチ 故障対応サービス

機器故障時には修理・交換の迅速な対応により、システムの早期復旧をサポートします。納入後10年間の機器修理・交換に対応します。

サービス 7

セキュリティーエンジン更新サービス

サポート技術者によりセキュリティーエンジンの更新を行います。更新後にはシステムの健全性確認(機器状態確認・通信ログ確認等)を行い、システム運用に支障が無いことを確認します。

① スポット対応サービス(セキュリティーエンジンの更新があった場合に、都度契約します。)
② 年1回更新サービス(セキュリティーエンジンの更新がない場合は、動作状況のチェックを行います。)
③ セキュリティーエンジン更新毎対応サービス

三菱電機サイバーセキュリティーソリューション
OTGUARD®

OTGUARD®は経済産業省産業サイバーセキュリティー研究会ワーキング1(制度・技術・標準化)ビルサブワーキンググループから2019年6月17日に公表された「ビルシステムにおけるサイバー・フィジカル・セキュリティー対策ガイドライン第1版」および、情報処理推進機構セキュリティーセンター(IPA)から公開されている「制御システムのセキュリティー分析ガイド　第2版」に準拠したソリューション提供が可能です。

三菱電機株式会社　〒100-8310 東京都千代田区丸の内二丁目7番3号〈東京ビル〉

お問合せは下記へどうぞ

本社……〒100-8310 東京都千代田区丸の内2-7-3(東京ビル)……(03)3218-3218
北海道支社……〒060-8693 札幌市中央区北2条西4丁目1(北海道ビル)……(011)212-3724
東北支社……〒980-0013 仙台市青葉区花京院1-1-20(花京院スクエア)……(022)216-4567
北陸支社……〒920-0031 金沢市広岡3-1-1(金沢パークビル)……(076)233-5503
中部支社……〒450-6045 名古屋市中村区名駅一丁目1番4号(JRセントラルタワーズ)……(052)565-3101
関西支社……〒530-8206 大阪市北区大深町4-20(グランフロント大阪タワーA)……(06)6486-4132
中国支社……〒730-8657 広島市中区中町7-32(ニッセイ広島ビル)……(082)248-5275
四国支社……〒760-8654 高松市寿町1-1-8(日本生命高松駅前ビル)……(087)825-0005
九州支社……〒810-8686 福岡市中央区天神2-12-1(天神ビル)……(092)721-2176

⚠安全に関するご注意

●ご使用の前に取扱説明書をよくお読みの上、
正しくお使いください。

本品のうち、戦略物資(又は役務)に該当するものの輸出にあたっては、外為法に基づく経済産業大臣の輸出(又は役務取引)許可が必要です。

SE-L-970(IP)

この印刷物は、2022年3月の発行です。なお、お断りなしに仕様を変更することがありますのでご了承ください。

2022年3月作成