

### ネットワーク通信先管理、認証機能による アクセス制限でサイバー攻撃をフィルタリング！



NEW

産業用マネージドハブ  
**EDS-G4008**シリーズ  
8ポートマネージドハブ (MOXA Inc.製)

マネージド  
ハブ

- **ネットワークフィルタ機能**  
(IPアドレス / MACアドレス / ポートなど)
- **認証機能 (ID・PW認証)**  
→ アクセス可能な端末を制限し、なりすまし攻撃を抑制

- **外部からのネットワーク侵入を防止**  
宛先および送信元のIPアドレス・TCP/UDPポート・MACアドレス、IP DSCP値、入力ポート等の情報の組み合わせにより、当該製品を通過する通信の許可・拒否を柔軟に制御。
- **IDによる認証により管理者以外のアクセスを制御**  
ID、パスワードによる認証機能実装により、当該スイッチへの意図しないアクセスによる誤操作の防止。また、マルウェアに乗っ取られたシステム内の機器からのなりすまし攻撃等の抑制が可能。
- **DoS攻撃への対策**  
各ポートで受信した通信に対して帯域の制限をかけたり、1秒あたりに受信可能なフレーム数の閾値を設定することが可能。(想定外帯域の利用制限、ブロードキャストストームの影響軽減)
- **Syslogによるイベントログの送信に対応。**  
指定したイベントについて、SNMPやメールで外部にアラートを上げることが可能。本体内蔵の端子からの出力(リレー出力)も可能。

### ネットワーク通信内容の監視とアクセス制限で サイバー攻撃から製造現場をしっかりとガード！



産業用セキュリティボックス  
**IEC-G102-BP**シリーズ  
IPS/IDS付き産業用超小型セキュリティボックス (MOXA Inc.製)

セキュリティ  
ボックス

- **IPS<sup>※1</sup>/IDS<sup>※2</sup>機能**  
→ 通信挙動監視によるDoS攻撃防止
- **ファイアウォール機能**  
→ ルールに基づくマルウェア<sup>※3</sup>・ランサムウェア<sup>※4</sup>の侵入防止
- **セキュリティパッチ機能**  
→ 端末機器にパッチを当てることが可能

- **ネットワークセキュリティを一元管理し、OT<sup>※5</sup>の可視性を向上**  
セキュリティ管理プラットフォームである「Security Dashboard Console」に接続すると、すべての侵入防止システムを単一のスペースで、効果的に管理・監視可能。
- **悪意のあるサイバー脅威の活動をダイナミックに防止**  
ネットワークトラフィックを分析し、詳細な行動監視とサイバークティビティの制御を提供。監視モードでは、管理者はサイバー脅威の活動を完全に可視化。
- **産業用プロトコルのホワイトリストコントロール**  
制御システムトラフィックのきめ細かいコマンドを提供する、産業用プロトコル認識機能を装備。
- **仮想パッチ適用とインテリジェントな脅威保護**  
仮想パッチは、エージェントレスの緊急セキュリティツールとして機能。

※1:IPS (Intrusion Prevention System):不正侵入防止システム  
※2:IDS (Intrusion Detection System):不正侵入検知システム  
※3:ウイルスやワームといった悪意のあるコードやソフトウェアの総称

※4:パソコンに保存されていたファイルを暗号化し開けなくした上で、ファイルを元に戻すことと引き換えに身代金を要求するマルウェア  
※5:OT (Operational Technology):工場などの製造現場で利用されている、設備やシステムを動かすための制御技術

## 1 想定するFAシステムへのサイバー攻撃

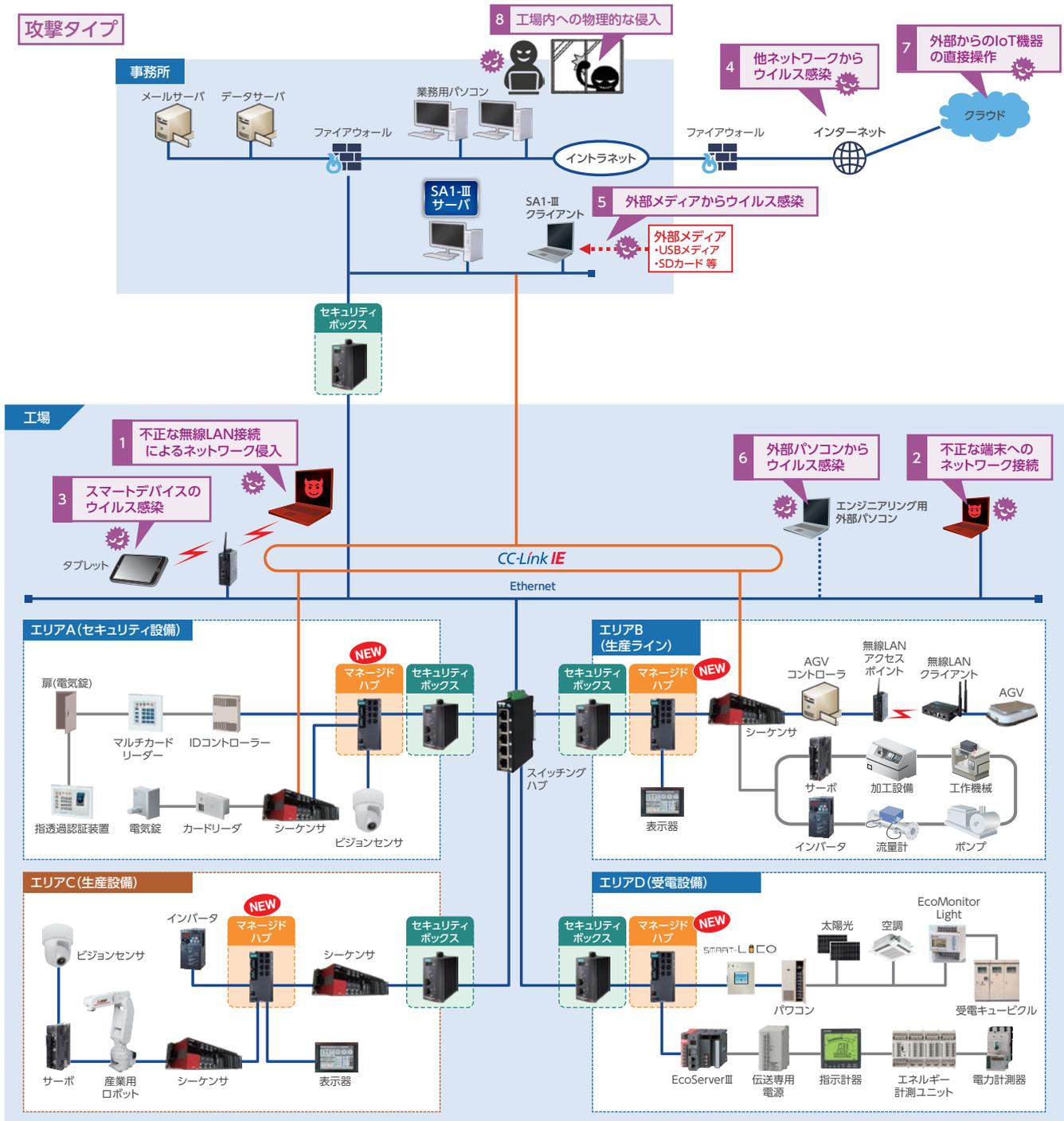
セキュリティボックス

マネージドハブ

### 工場内の設備・FA機器には様々なパターンでサイバー攻撃を受ける可能性があります

製造業はDXの推進により、外部ネットワークとの接続点が増加したことも相まって、標的型攻撃の対象となりやすくなっています。サイバー攻撃の影響は一社だけに留まるものではなく、情報漏洩や操業停止といった事態が発生すれば、その被害はサプライチェーン全体に広がる可能性も高くなります。

#### 攻撃タイプ



#### ゾーニング/システム構成例

### ゾーニングによるセキュリティ対策で、他エリアへの感染拡散を防止します！

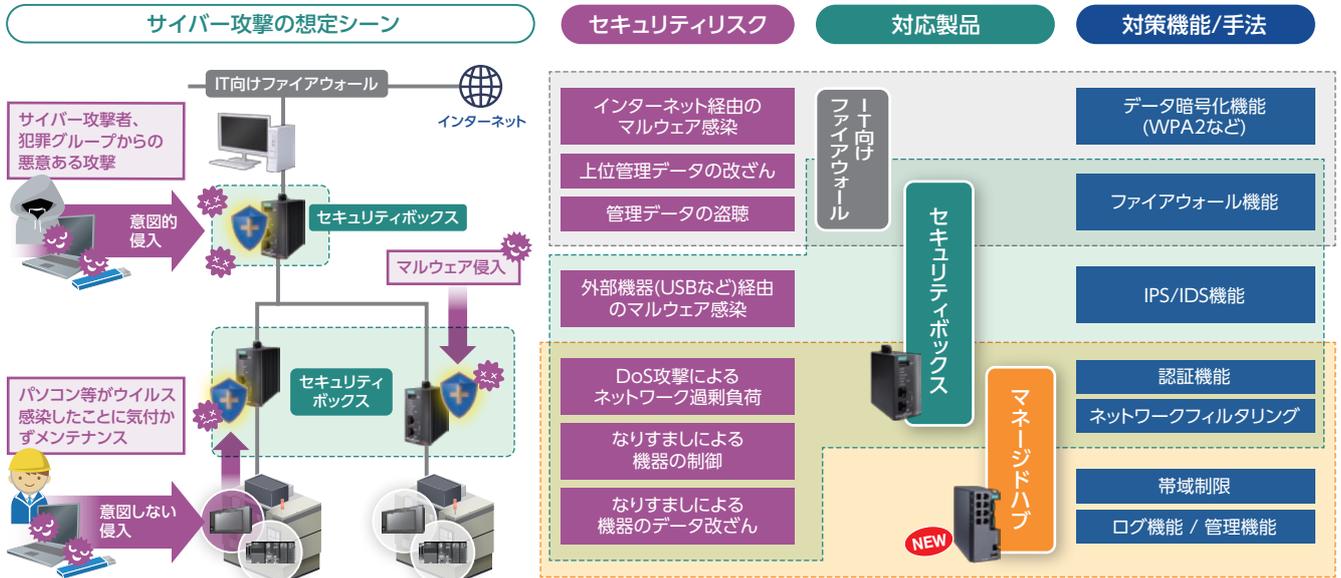
ゾーニングとは、システム・機械・装置の用途や脅威を考慮した区分でネットワークを分割することです。これにより、それぞれのエリアのリスク運用に応じたセキュリティ対策が考えやすくなります。前頁のように様々な攻撃ルートが考えられますが、以下の構成はゾーニングし、ウイルス感染した場合に他エリアに拡散しないよう、セキュリティ対策を施した一例です。

## 2 製造業に広がるサイバー攻撃への対策

セキュリティ  
ボックス

マネージド  
ハブ

外部からの様々なサイバー攻撃に対して、対策が可能です



セキュリティ  
ボックス

### 仮想パッチ適用によるサイバー攻撃対策



産業用セキュリティボックス IEC-G102-BPシリーズでは、パッチを適用できない環境でも、パッチを当てたかのようなサイバー攻撃対策が可能です。

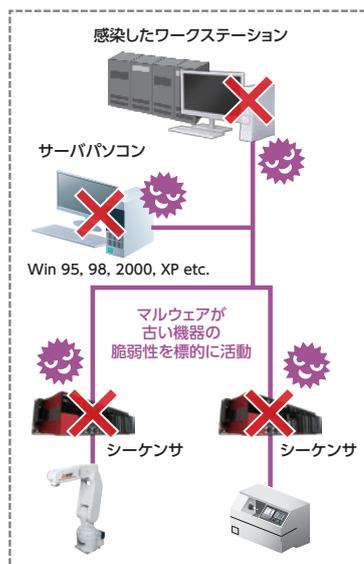
#### パッチ管理ができないデバイスを“Virtual Patch”で守る

##### ポイント

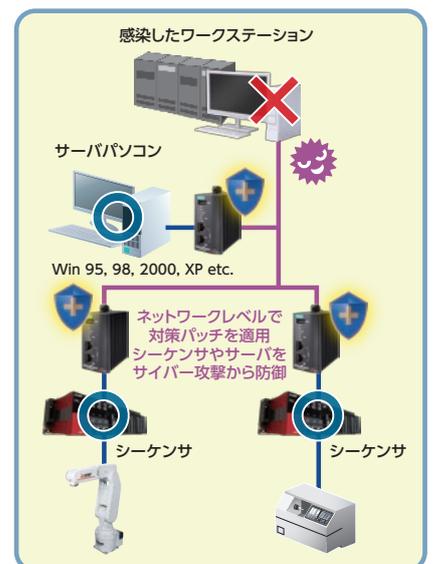
エンドポイントへのパッチが難しい場合に、**ネットワークレベルで脆弱性の悪用を防止**

- 新たな脅威が見つかった場合、ネットワーク機器のシグネチャを更新し、攻撃からエンドポイントを防御。
- シーケンサや古いWindows等、エンドポイントへのウイルス対策ソフトウェアの導入が難しい場合にも導入可能。
- ウィルス対策ソフトウェアのパッチは、システムへの影響を事前検証する前にも、ネットワーク上のパッチ適用は可能。

パッチの適用できない環境から



パッチを当てたかのような環境に (仮想パッチ)



## 3 サイバー攻撃へのセキュリティ対応

セキュリティ  
ボックス

マネージド  
ハブ

### サイバー攻撃検知仕様比較

項目		セキュリティ ボックス	マネージドハブ	セキュリティ ソフトウェア
対象	サイバー攻撃監視方法	ネットワーク (通信内容)	ネットワーク (通信内容)	エンドポイント (端末)
機能	検知	○	-	○
	攻撃パケット検知 (シグネチャ型攻撃検知)：シグネチャと呼ばれる検出ルールやパターンをあらかじめ登録しておき、 通信パケットをシグネチャとマッチングさせることで、不正なアクセスや 異常なトラフィックを検出します。	○	-	○
ネットワーク 管理	正常ではないパケット通信のふるまい検知 アノマリ型攻撃検知：○○○	○	-	○
	ポート管理機能 (Port Disable、IP管理) VLAN機能 (ネットワークの分離)	- -	○ ○	- -
攻撃検知状態 外部出力		専用管理ソフトウェア	接点出力	-

◎：防止可能-攻撃による被害の未然防止が可能  
△：検知可能-攻撃の検知が可能、早期対応により被害拡大を防止  
×：検知不可-攻撃の検知不可能

### セキュリティ製品別の対応について

No.	攻撃	攻撃ルート	攻撃対象		システムへの影響	攻撃種別	セキュリティ ボックス	マネージドハブ	セキュリティ ソフトウェア
			パソコン	制御機器					
1	不正な無線LAN接続による ネットワーク侵入	不正端末 → Wi-Fi	●	●	情報・制御プログラムの 改変 ・生産品質低下 ・生産性の喪失	不正アクセス	◎	◎	△
2	不正な端末へのネットワーク接続	不正端末 → Ethernet	●	●		ウイルス感染 ・生産性の喪失	DoS攻撃	◎	◎
3	スマートデバイス(スマホ等)の ウイルス感染	スマートデバイス → Ethernet	●	●	ウイルス感染 ・生産性の喪失		なりすまし マルウェア 脆弱性攻撃	△	△
4	他ネットワークからウイルス感染	外部ネットワーク → Ethernet	●	-		△		△	◎
5	外部メディアからウイルス感染	USBメモリ → パソコン接続	●	-		△		△	◎
6	外部パソコンからウイルス感染	不正端末 → Ethernet	●	-	△	△	◎		
7	外部からのIoT機器の直接操作	外部ネットワーク → Ethernet	-	●	制御機器直接操作 ・生産性の喪失 ・生産設備破損	不正アクセス	◎	◎	×

## 4 仕様

セキュリティ  
ボックス

マネージド  
ハブ

### 産業用マネージドハブ EDS-G4008 シリーズ

#### 基本仕様

形名		EDS-G4008-LV
イーサネット インターフェース	10/100/1000BaseT(X) Ports	8
	規格	IEEE 802.3 for 10BaseT, IEEE 802.3u for 100BaseT(X), IEEE 802.3ab for 1000BaseT(X), IEEE 802.3x for flow control, IEEE 802.3ad for Port Trunk with LACP, IEEE 802.1Q for VLAN Tagging, IEEE 802.1D-2004 for Spanning Tree Protocol, IEEE 802.1w for Rapid Spanning Tree Protocol, IEEE 802.1p for Class of Service, IEEE 802.1X for authentication
USBインターフェース	USBコネクタ	USB Type A
LEDインターフェース	LEDインジケータ	PWR1, PWR2, STATE, FAULT, MSTR/HEAD, CPLR/TAIL, SYNC
イーサネット ソフトウェアの特徴	フィルター	GMRP, GVRP, GARP, 802.1Q VLAN, IGMP Snooping v1/v2/v3, IGMP Querier
	マネージメント	IPv4/IPv6, Flow control, Back Pressure Flow Control, DHCP Server/Client, ARP, RARP, LLDP, Port Mirror, Linkup Delay, SMTP, SNMP Trap, SNMP Inform, SNMPv1/v2c/v3, RMON, TFTP, SFTP, HTTP, HTTPS, Telnet, Syslog, Private MIB
	MIB	P-BRIDGE MIB, Q-BRIDGE MIB, IEEE8021-SPANNING-TREE-MIB, IEEE8021-PAE-MIB, IEEE8023-LAG-MIB, LLDP-EXT-DOT1-MIB, LLDP-EXT-DOT3-MIB, SNMPv2-MIB, RMON MIB Groups 1, 2, 3, 9
	冗長プロトコル	STP, RSTP, Turbo Ring v2, Turbo Chain, Ring Coupling, Dual-Homing, Link Aggregation, MSTP
	セキュリティ	Broadcast storm protection, Rate Limit, Trust access control, Static Port Lock, MAC Sticky, HTTPS/SSL, SSH, RADIUS, TACACS+, Access control list, Login and Password Policy
システム電源	入力電圧	12~48VDC
	入力電流	12-48 VDC, 1.50-0.40A or 24 VDC, 0.70A
	最大電力量	8.84 W
筐体	寸法	55 × 140 × 120 mm (DINレール、電源コネクタ除く)
	固定方法	DINレールマウント、ウォールマウント (オプションキット)
環境要件	動作温度	-10~60°C (14~140°F)
	保管温度	-40~85°C (-40~185°F)
	湿度	5~95% (結露なきこと)

### 産業用セキュリティボックス IEC-G102-BPシリーズ

#### 基本仕様

形名		IEC-G102-BP-Pro-H-ME
イーサネット インターフェース	10/100/1000BaseT(X) Ports	2
	規格	IEEE 802.3 for 10BaseT IEEE 802.3ab for 1000BaseT(X) IEEE 802.3u for 100BaseT(X)
LEDインターフェース	LEDインジケータ	PWR1, PWR2, MANAGED, IPS/IDS, USB/F, BYPASS, 10/100/1000M
DoS and DDoS保護	テクノロジー	ICMP Flood, IGMP Flood, UDP Flood, UDP port scan, TCP SYN Flood, TCP Port SYN Scan, TCP Port FIN Scan, TCP Port NULL Scan, TCP Port Xmas Scan
ファイアウォール	IPSスループット	> 200 Mbps
	レイテンシ	< 500 microseconds
	同時接続 (TCP)	30000
	Deep Packet Inspection	Modbus TCP, Modbus UDP, EtherNet/IP, PROFINET-DCP, CIP, Omron FINS, Mitsubishi SLMP, Siemens S7 Comm., Siemens S7 Comm. Plus, With more available through firmware update
リアルタイム ファイアウォール/ VPNイベントログ	ポリシー登録数	512 rules
	ICS Protocol Filter Profiles	32 profiles
システム電源	入力電圧	12~48VDC
	入力電流	0.605A @ 12VDC, 0.297A @ 24VDC, 0.143A @ 48VDC
筐体	寸法	40 × 70 × 83mm (DINレール、電源コネクタ除く)
	固定方法	DINレールマウント、ウォールマウント (オプションキット)
環境要件	動作温度	-10~60°C (14~140°F)
	保管温度	-40~85°C (-40~185°F)
	湿度	5~95% (結露なきこと)
ソフトウェア	SDC (Security Dashboard Console)	○
	バーチャルパッチ自動アップデート	○
	バーチャルパッチ手動アップデート	○

#### 性能および制限事項

##### (1) スループット/遅延

RFC2544 双方向の  
UDPスループットの packets loss 0%

フレームサイズ (byte)	合計スループット (Mbps)	平均遅延時間 (μs)
64	114.780	351.728
128	217.983	365.955
256	420.303	427.211
512	812.026	437.810
1024	1508.458	645.332
1518	1827.038	658.157

IPS(prevention)+DoS(prevention)  
+ Policy Enforcement(64policies)設定時

##### (2) 同時接続

最大: 10,000セッション  
超過時: DROP

##### (3) 保護機能 (IPS、IDS、ファイアウォール)

最大: 50unique IP/MAC  
超過時: ACCEPT

##### (4) ファイアウォール

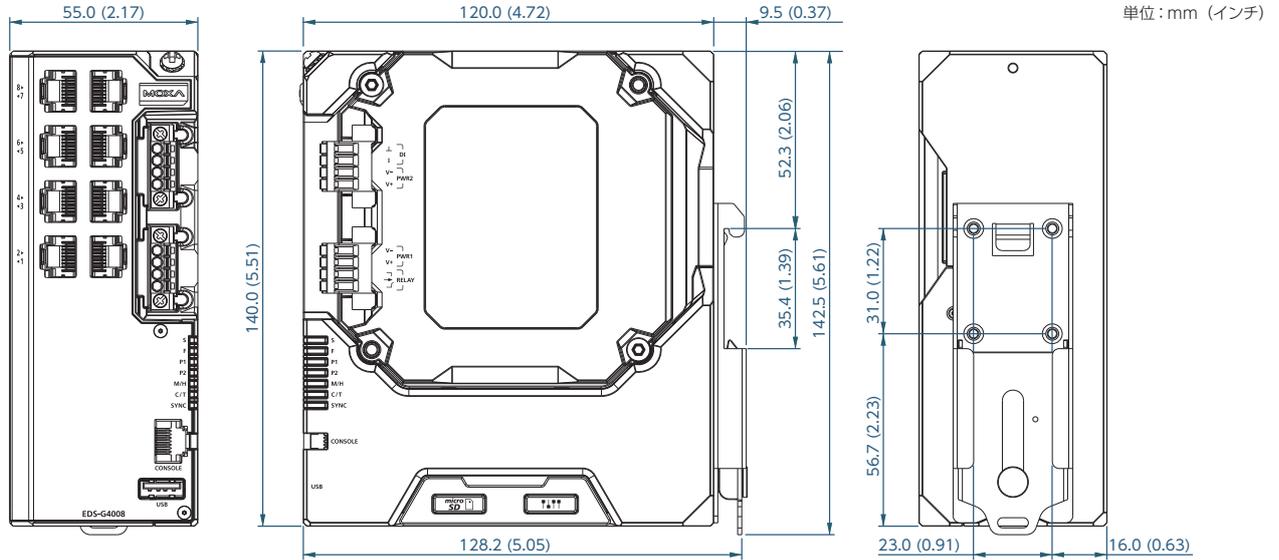
最大: 64ルール  
最大: 32object profiles/type

## 5 外形寸法図

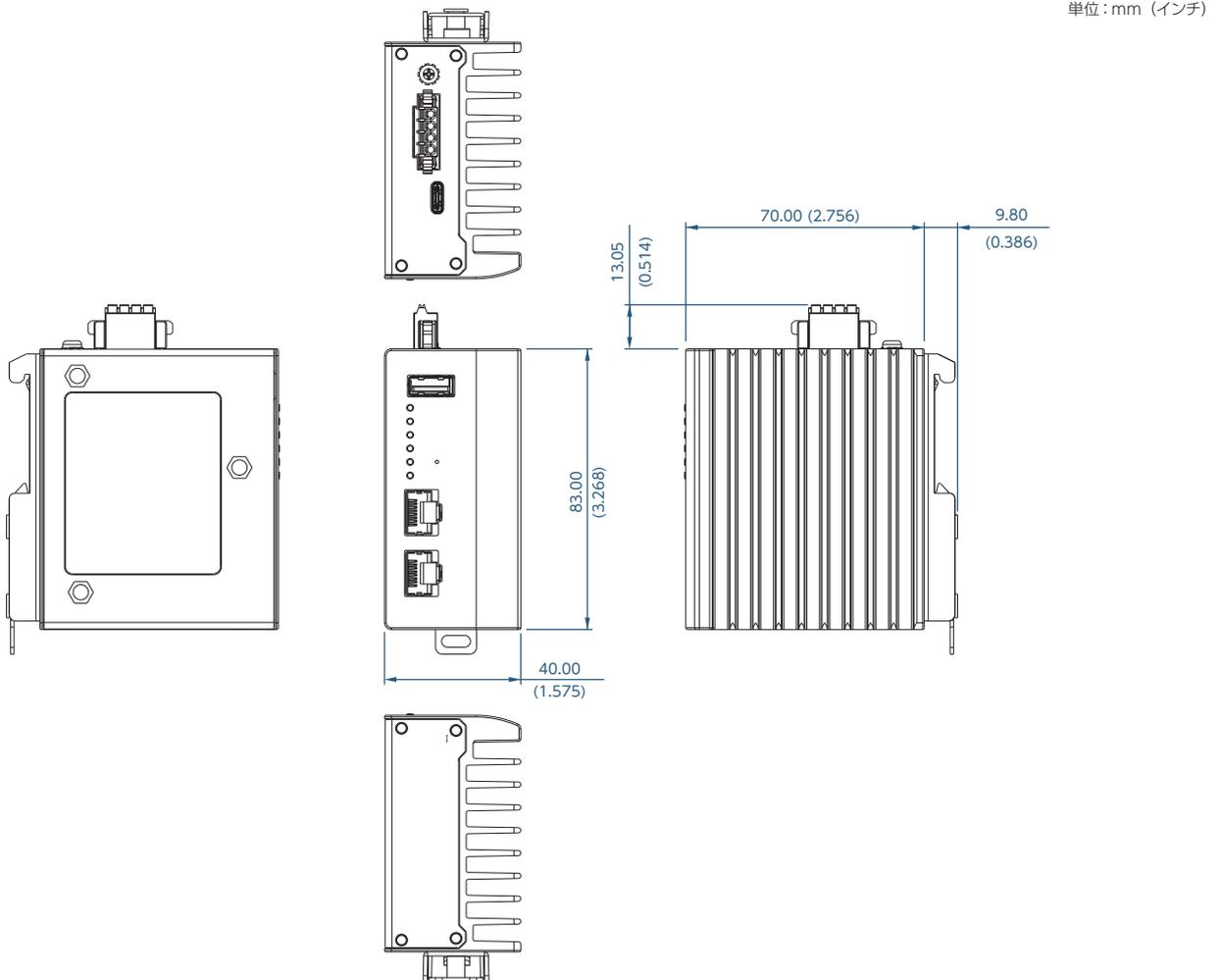
セキュリティ  
ボックス

マネージド  
ハブ

### 産業用マネージドハブ EDS-G4008シリーズ



### 産業用セキュリティボックス IEC-G102-BPシリーズ



## 6 価格表

セキュリティ  
ボックス

マネージド  
ハブ

### 産業用マネージドハブ EDS-G4008シリーズ

品名	形名	標準価格	備考
産業用マネージドハブ	EDS-G4008-LV	オープン価格	-10~60℃

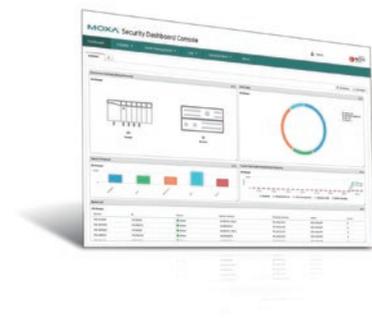
※価格、納期につきましてはお取引先へお問合せください。

### 産業用セキュリティボックス IEC-G102-BPシリーズ

品名	形名	標準価格	備考
本体	産業用セキュリティボックス (IECライセンス3年間付)	IEC-G102-BP-Pro-H-ME	オープン価格 産業用IPSシステム IECライセンス3年間付 -10~60℃
ライセンス	IECライセンス1年延長用	LIC-IEC-RENEW-1Y-XN-SR	オープン価格 セキュリティボックス ライセンス延長用(1年間)
	SDCライセンス1年間	LIC-SDC-NEW-1Y-XN-SR	オープン価格 1年間
	SDCライセンス3年間	LIC-SDC-NEW-3Y-XN-SR	オープン価格 3年間
	SDCライセンス5年間	LIC-SDC-NEW-5Y-XN-SR	オープン価格 5年間
	SDCライセンス1年延長用	LIC-SDC-RENEW-1Y-XN-SR	オープン価格 延長用(1年間)

※ IEC ライセンス：最新パターンファイルを適用できるライセンス。  
※価格、納期につきましてはお取引先へお問合せください。

## SDC ライセンスについて



### 製品概要

Security Dashboard Console (SDC) ソフトウェアは、ネットワーク上の IEC-G102-BP シリーズ産業用次世代 IPS を管理し、OT サイバー脅威を監視することで、継続的な生産ライン稼働を確保する一元化されたセキュリティプラットフォームです。

### 導入メリット

重要な資産の可視性、ネットワーク分析、および自動パターン更新を一元化することにより、より一層のネットワーク保護を提供します。

### 主な機能

- ①一元管理されたネットワークセキュリティ  
単一のプラットフォームからすべての IEC-G102-BP シリーズをより効率的で一元的に管理・監視することができます。
- ② OT ネットワークの可視性の強化  
必要な情報を提供するようにカスタマイズでき、データを視覚化できます。
- ③利便性と相互接続性を向上する  
さまざまな施設のセキュリティネットワークをリモートでトラブルシューティングし、メンテナンスコストを削減します。

# OTセキュリティソリューション

イーサネット、ETHERNET は富士フイルムビジネスイノベーション株式会社の登録商標です。  
本文中における会社名、商品名は、各社の商標または登録商標です。

## お問合せ先

三菱電機システムサービス株式会社 [www.melsc.co.jp/](http://www.melsc.co.jp/)

〒154-8520 東京都世田谷区太子堂4-1-1 キャロットタワー20階



北日本支社	〒983-0013	宮城県仙台市宮城野区中野1-5-35	機電営業課	(022) 353-7814
北海道支店	〒004-0041	札幌市厚別区大谷地東2-1-18	機電営業課	(011) 890-7515
首都圏第2支社	〒108-0022	東京都港区海岸3-9-15 LOOP-Xビル11階	製品販売課	(03) 3454-5511
			システム営業課	(03) 3454-1561
中部支社	〒461-8675	名古屋市東区大幸南1-1-9	機電営業課	(052) 722-7602
			機電システム課	(052) 722-7603
北陸支店	〒920-0811	金沢市小坂町北255	機電営業課	(076) 252-9519
関西支社	〒531-0076	大阪市北区大淀中1-4-13	営業一課・二課	(06) 6458-9738
中四国支社	〒732-0802	広島市南区大州4-3-26	機電フィールドエンジニアリング課	(082) 285-2111
			機電ソリューションエンジニアリング課	(082) 285-2112
四国支店	〒760-0072	高松市花園町1-9-38	機電フィールドエンジニアリング課	(087) 831-3186
			機電ソリューションエンジニアリング課	(087) 831-3190
九州支社	〒812-0007	福岡市博多区東比恵3-12-16 東比恵スクエアビル	機電営業課	(092) 483-8208

お問い合わせ、ご相談は信用とサービスの行き届いた当店へどうぞ