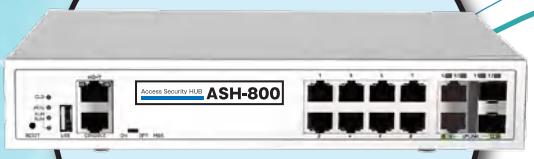
# 新しい「セキュリティ対策」のカタチ

対策が困難だった**「拡散防止」「二次被害防止」**に
最適な「Network Security Appliance」&「Security Access Point」




ASH-800

ASH-AP

Access Security HUB **ASH Series**

Fuva Brain

# 日々進化するサイバー攻撃から会社を守れますか?

ランサムウェアによる
データ暗号化

スマートフォンの
セキュリティ

Emotetウイルスによる
偽装メール拡散

USBメモリからの
ウイルス感染

テレワーク時の持出用
PCの帰還

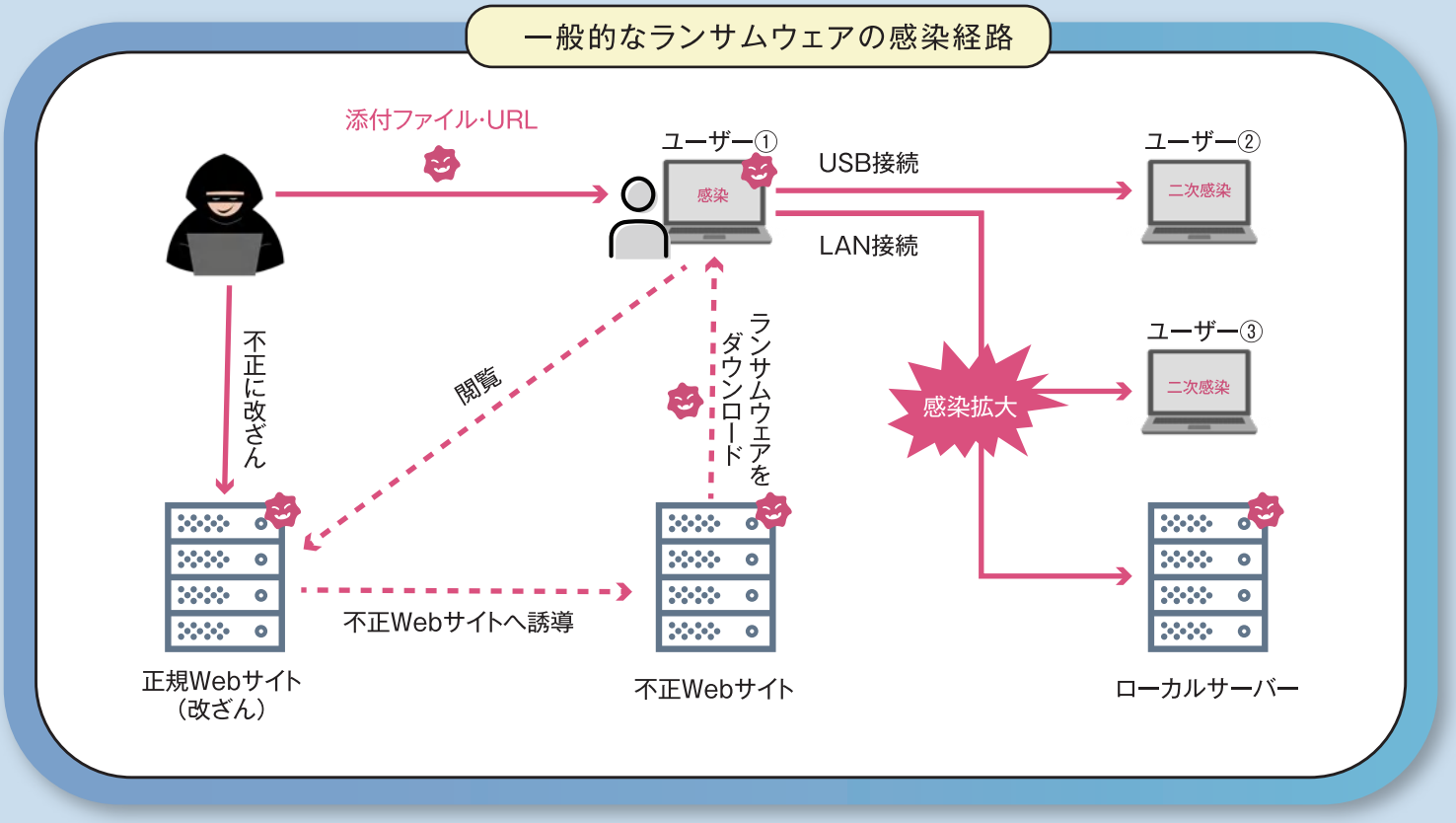
サプライチェーン
攻撃

VPN機器を狙った
サイバー攻撃

## これらの脅威が御社を脅かしています

ウイルス感染はネットワーク内での感染拡大による
被害をいかに最小限に食い止めることが出来るかが重要です

### 一般的なランサムウェアの感染経路

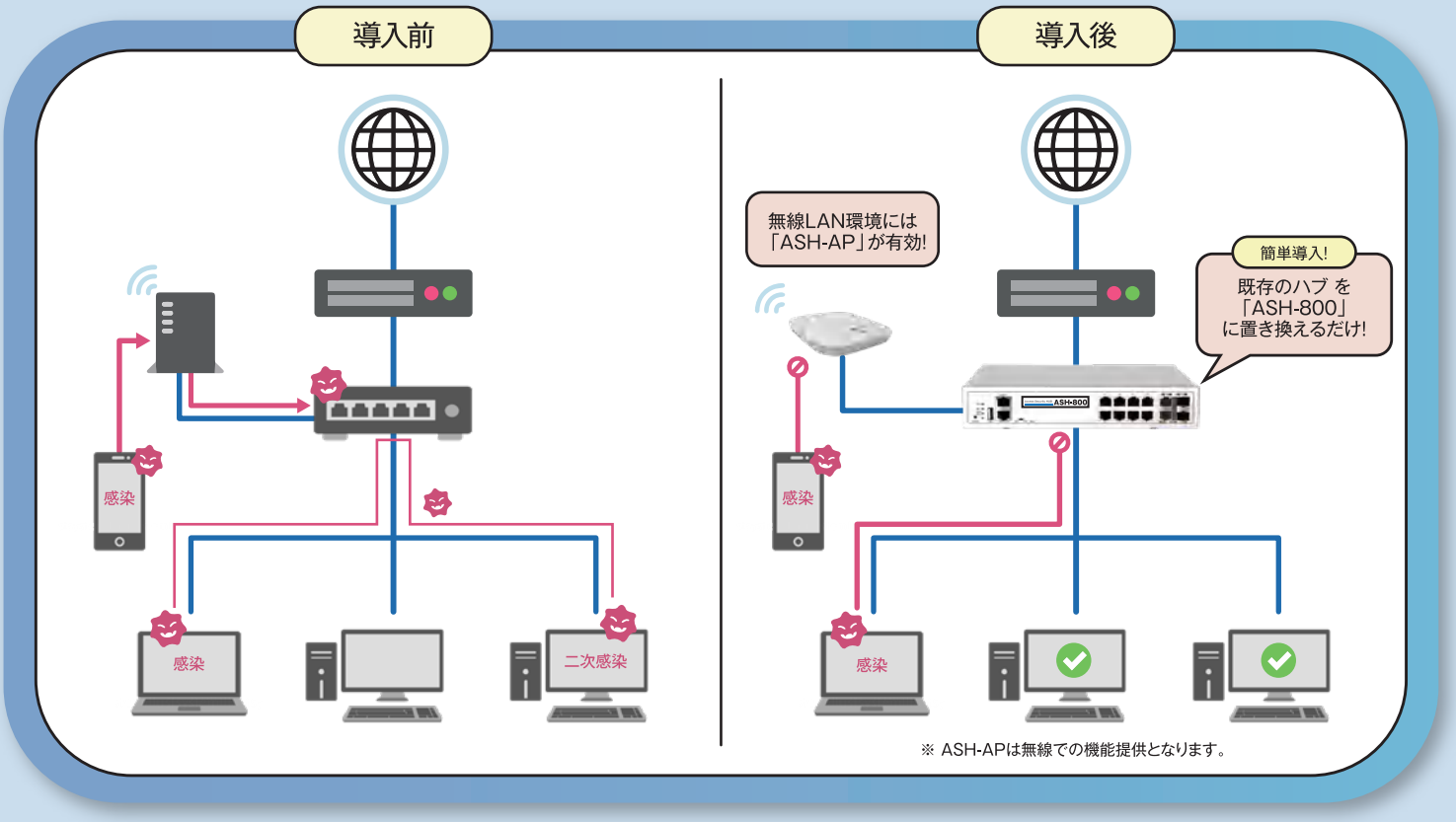


# ASH Series でできる！セキュリティ対策

＼その1.／

## できること　ウイルス拡散防止

振る舞い検知方式でウイルス拡散時の前兆動作をリアルタイムで検知･遮断し、二次感染や拡散の被害を最小限に抑えることができます



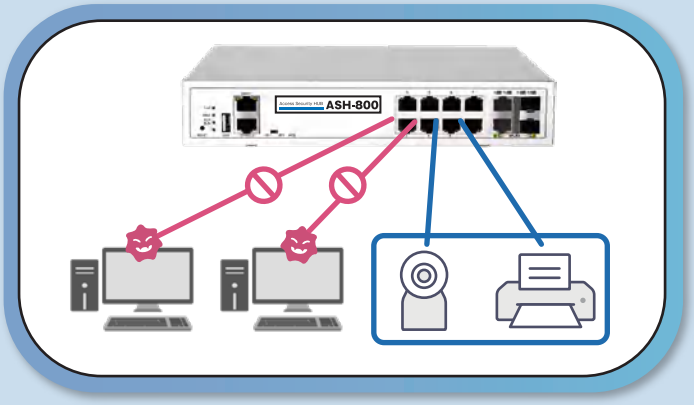

※ ASH-APは無線での機能提供となります。

＼その2.／

## できること　有害トラフィックの選別遮断

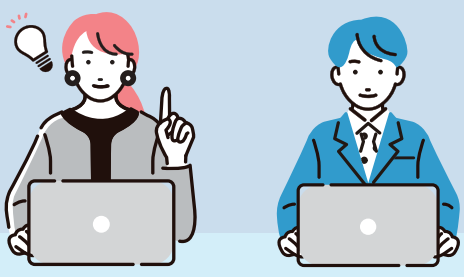
大量のパケットを送り、特定のマシン機能を停止させる
「DoS攻撃」や、ネットワークの負荷を上げるような攻撃など、
有害なパケットを検知し、遮断します。

■ 対策できる攻撃（例）
・DoS、DDoS攻撃　・IPスプーフィング
・ブロードキャスト攻撃　・DHCPフラッディング など




特許技術

「ＭＤＳエンジン」で、
有害トラフィック“だけ”を選別して
遮断できるから、通常業務にも支障なし!



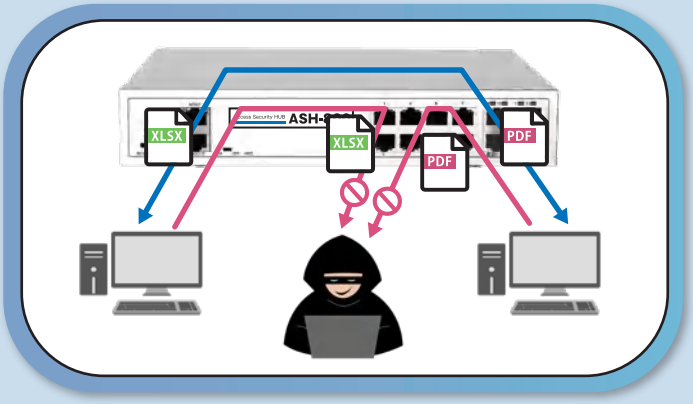
＼その3.／

できること

# ハッキングによる盗難･盗聴･情報漏洩防止

通信傍受の代表的な攻撃である「ARPスプーフィング攻撃」を
アクセスネットワーク層で検知･遮断できます。

■ 狙われている情報
･メールアカウントなどの認証情報　･IP電話の盗聴
･各種資料の情報　･マイナンバー　･テレビ会議の内容
･監視カメラデータ



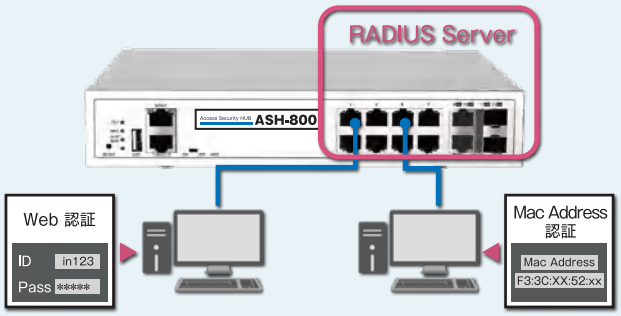

## 管理ソフト「VNM」で運用も安心･安全!

### ネットワークループの検知･遮断

スイッチのポート同士を誤って接続することで発生するネットワークループ。ASH-800 は、ネットワークループが発生した障害箇所を瞬時に特定･遮断し、ネットワーク全体に障害が波及することを防止します。

※ ASH-800 専用の機能となります。
※ VNM（Visual Node Manager）は、クライアントPCへのインストールが必要です。

### 不正端末の持ち込みを防ぐ強力な認証機能

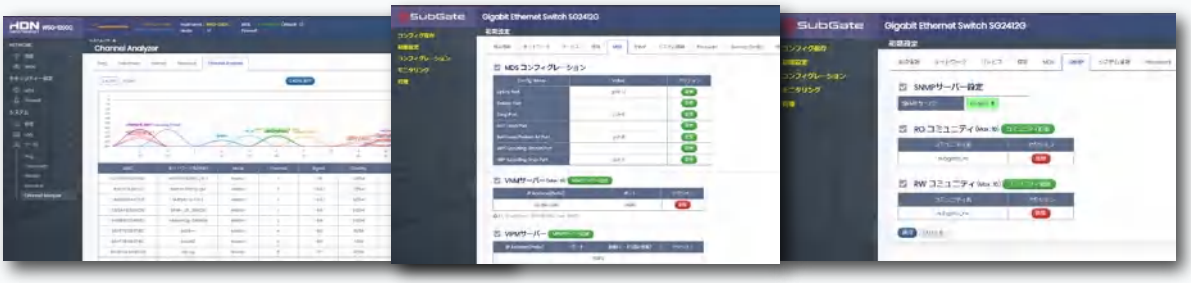



ASH-800 は、ユーザー認証を行うRADIUSサーバ機能を標準で搭載しているため、導入の手間が省けます。Web認証/MAC認証/802.1X認証をサポートしています。

※「ASH-800」は最大512ユーザー、「ASH-AP」は最大64ユーザーまで認証可能。

### 高機能GUIで操作性抜群!

APのチャンネルアナライザー機能　セキュリティ機能　VNMサーバ連携（SNMP）



直感的でわかりやすい日本語対応のGUIで操作が簡単!

# 「UTM」と「ASH Series」の違い

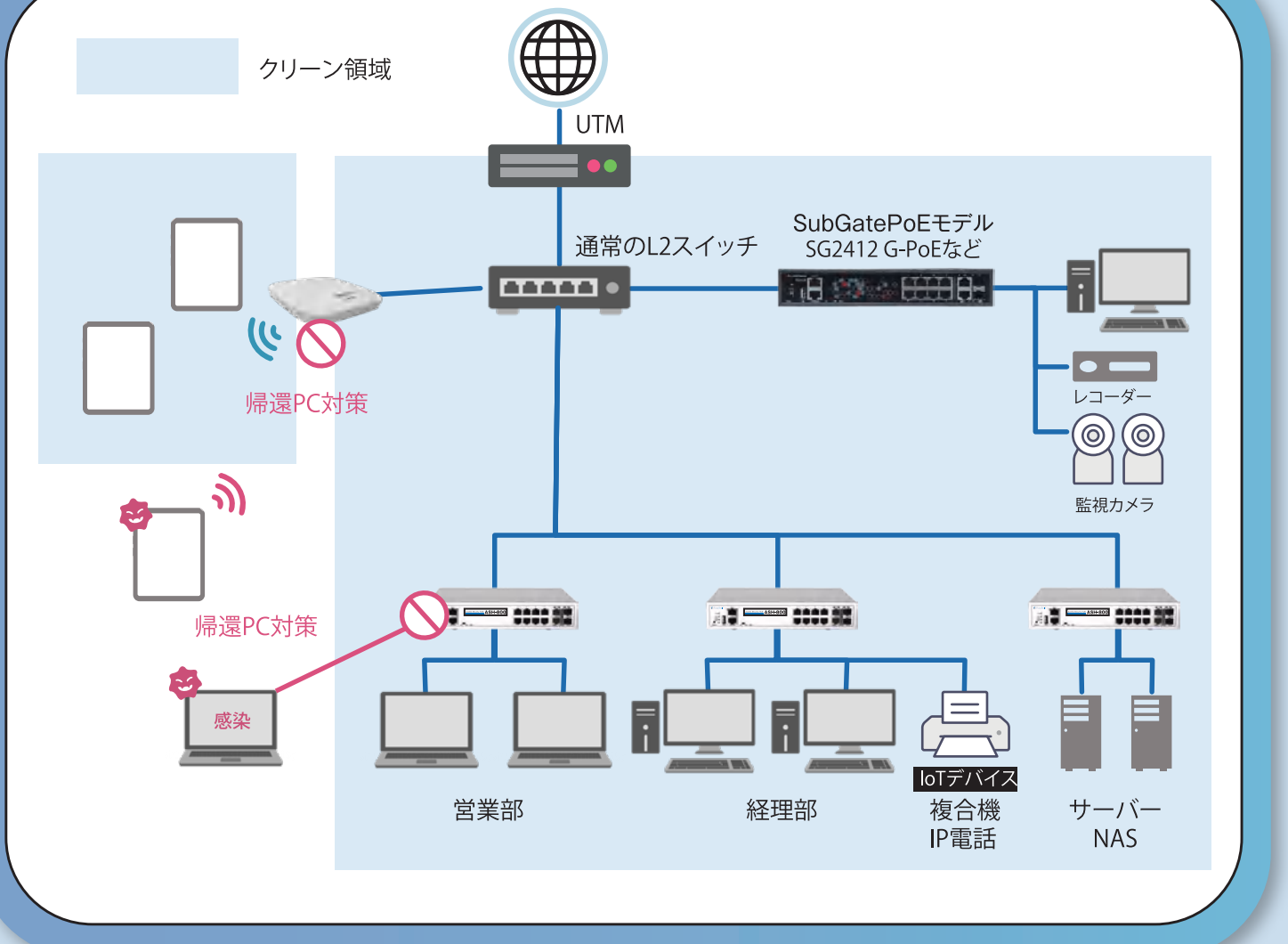
- 「UTM」と「ASH Series」とでは、セキュリティの守備位置が異なります。
- UTMはネットワークの入り口で監視し、外部からの脅威を検知しブロックします。
- それに対してASH Seriesは主に社内でウイルス感染が起こった場合に他のPCサーバへの拡散を防止します。
- UTMのセキュリティとは被ることがありませんので、お客様のセキュリティレベルを大きく上げる事が出来ます。

| UTM | | ASH |
|---|---|---|
| ○ | アンチウイルス(web) | - |
| ○ | スパムメール対策 | - |
| ○ | Webフィルタリング | - |
| ○ | ファイアウォール | - |
| ○ | 不正侵入 検知/防止 | - |
| ○ | C&Cサーバー通信対策 | - |
| - | ウイルス拡散防止 | ○ |
| - | 有害トラフィックによる攻撃遮断 | ○ |
| - | 情報窃盗遮断 | ○ |
| - | ループ検知/遮断 | ○ |

＼その4.／

できること　感染後の被害を最小化

構成イメージ



## ASH-800

| | |
|---|---|
| H/W | MAC アドレステーブル：16K　/　電源 ×1 |
| インターフェース | コンソールポート ×1　/　10/100/1000 Base-T ×10　/　1000 Base SX/LX/ZX ×2　/　利用可能ポート数（最大）：12 |
| 寸法 / 重量 | 消費電力 (W)：16.8　/　外形寸法 (mm)：W250 x H44 x D200　/　重量 (kg)：1.9 |

## ASH-AP

最大64台接続可能なWi-Fi アクセスポイントタイプ

| | |
|---|---|
| H/W | 内蔵アンテナ　/　電源：付属電源アダプタまたは PoE 給電 |
| インターフェース | コンソールポート ×1　/　10/100/1000 Base-T ×1 |
| ワイヤレス機能 | 対応プロトコル：802.11a/b/g/n/ac　/　セキュリティ：WPA/WPA2(PSK,Enterprise,Mixed Mode)　/<br>暗号化方式：CCMP(AES),TKIP |
| PoE | 802.3at(PD) |
| 寸法 / 重量 | 消費電力 (W)：18　/　外形寸法 (mm)：W210 x H30 x D210　/　重量 (kg)：0.5 |

## ASH Series 仕様詳細

| | |
|---|---|
| VLAN | 4K VLAN ID　/　802.1q ポートベース VLAN　/　プロトコル /IP サブネット /MAC ベース VLAN　/　シェアード VLAN　/<br>ハイブリッド VLAN　/　Voice VLAN　/　802.1ad VLAN スタッキング (QinQ) |
| 冗長性 / ループ検出 | STP/RSTP/MSTP　/　PVSTP　/　ERP(Ethernet Ring Protection)　/　セルフ・ループ・プロテクション　/<br>SPR(Smart Port Redundancy)　/　UDLD |
| リンク<br>アグリゲーション | IEEE 802.3ad LACP, スタティックチャンネルグループ　/　トランクグループ：最大 12 グループ（1 グループ最大 8 ポートまで） |
| 監視 | ポートミラーリング　/　1:1, N:1, N:N：TFM(Traffic Flow Monitoring) |
| L2 マルチキャスト | IPv4 IGMP スヌーピング (v1/v2/v3)　/　IPv6 MLD スヌーピング (v1/v2) |
| QoS | 最大 8 キュー（ポート毎）　/　Rate Limit(Ingress/Egress)　/　DiffServ　/　Auto QoS　/　SP, WRP, DRR　/　IPv6 QoS |
| 管理 | LLDP, LLDP-MED　/　RMON( グループ 1,2,3,9)　/　ローカル / リモート Syslog　/　USB インターフェースサポート　/<br>Auto Config 機能サポート　/　マルチ OS サポート　/　統合管理 ソフトウェア (VNM)　/　IPv4/IPv6 Telnet/SSH　/　IP SLA　/<br>ソフトウェアダウンロード：FTP, SFTP, TFTP, USB　/　DHCP サーバ / リレー　/　SNMP v1/v2/v3, Trap 対応　/<br>IPv4/IPv6 sFlow　/　NTP/SNTP　/　SIM(Single IP Management):　/　802.3az EEE |
| セキュリティ | セキュリティ専用 Engine　/　DHCP スヌーピング　/　ポートセキュリティ　/　ACL：① L2/L3/L4 ACL　②時間ベース ACL<br>③ VLAN ACL　④ Ingress/Egress ACL　⑤ CPU-ACL　/　IPv4/IPv6 DHCP/NetBIOS フィルタリング　/　ストーム制御　/<br>Embedded RADIUS サーバ　/　IP, MAC, IP + MAC 組み合わせ認証 (VIPM)　/　AAA 認証：ローカル , RADIUS, TACACS +認証　/<br>マルチ認証　/　802.1x：マルチホスト , MAC 認証バイパス , ゲスト VLAN, ダイナミック VLAN<br><br>有害トラフィック選別遮断　攻撃遮断：DoS/DDoS 攻撃 , DHCP 攻撃 , ICMP 攻撃 , ARP 攻撃<br>フラッディング遮断：TCP SYN フラッディング , UDP フラッディング , MAC フラッディング<br>スプーフィング遮断：ARP スプーフィング , IP スプーフィング<br>スキャニング遮断：ホストスキャン , ポートスキャン<br>IPv6 DAD 攻撃遮断：<br>自動検知 / 遮断 /QoS/Rate Limit 及び解除　/　有害トラフィック発生時アラート機能 |

お問い合わせ･ご購入は下記販売店まで

Fuva Brain
株式会社フーバーブレイン

本社 〒102-0094
東京都千代田区紀尾井町4-1
ニューオータニガーデンコート22F

www.fuva-brain.co.jp

1_2022.05