Digital communications
株式会社デジタル・コミュニケーションズ

中小企業に最適な「拡散防止型」情報漏えい対策

Eye"24.7" AntiMalware D-Guard
HUB/AP Series

標的型攻撃も。顧客情報流出も。機密情報の持ち出しも。
情報漏えいリスクをまとめて減らすヒント、教えます。

ZERO TRUST

日々、増大するマルウェアの新種・亜種群。
従来のシグネチャベースでは
検知は追いつけない。

Cloud Mobile IoT

進化する脅威に対抗する

01 取り巻く環境の変化 内部への侵入リスクが拡大

クラウドサービスやモバイルデバイスの普及 -
働き方改革の推進によるテレワーク需要 -
IoT（モノのインターネット）の増加 -

02 攻撃者の組織化 ランサムウェアの産業化

サイバー攻撃のビジネス化で金銭目的が顕著に -
ランサムウェア攻撃の頻度は 3 倍に上昇 -

03 マルウェアの増大と 攻撃手法の高度化・複雑化

毎月 1200 万を超える新しい亜種のマルウェアの出現 -
1 秒に 11.6 個生成される新種のマルウェア -

ゼロトラストを前提としたリアルタイム監視。
進化する脅威を一貫して検出。

ATC（Advanced Threat Control：先進型振る舞い検知）は、PC やサーバー内のアプリケーションの動きを常時監視し、不正な動きを検知。既知、亜種、未知の脅威から保護します。

- 高度なヒューリスティック手法に基づく動的テクノロジーを採用。
- アプリケーションが行うすべての動作を監視し、未知の脅威を逃さず検出。

※ATC 機能は Windows OS に対応

BACKUP

データ消失によるビジネスへの影響を最小限に抑え、万が一の時の業務復旧時間を短縮。

※バックアップ機能はWindowsOSに対応

定期的に自動実行　**安全な領域でデータ保護**　**容易に復旧**

DATA SHIELD

指定フォルダを自動バックアップ
（更新データのみ）

差分バックアップにより、
バックアップ時間を短縮。

バックアップフォルダを
Eye“247”AntiMalware が保護。

スケジュールスキャン実施

スケジュールスキャンとバックアップ機能との連携により、重要情報を定期的に負荷なくバックアップ。

RESTORE

万が一、ランサムウェアなどの
被害が発生した場合

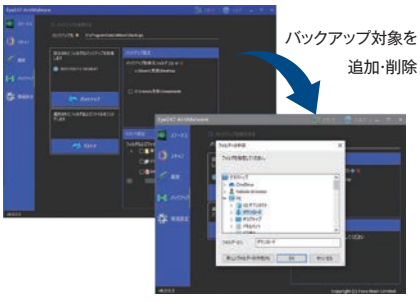
バックアップフォルダを
Eye“247”AntiMalware が保護。
不正な書き換え、暗号化など
の被害を受けません。

感染対応後、
バックアップフォルダから
ファイルの復旧が可能です。

管理Managerで全端末共通のバックアップ設定

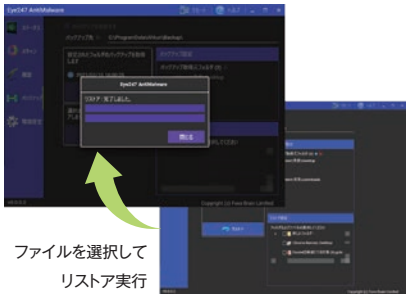
管理Managerでバックアップ対象のファイルパスを指定することで、全端末共通の領域に対してバックアップを取ることができます。

クライアントで個別にバックアップ設定も可能



日々、使用しているファイルの保存場所は利用者毎に異なるものです。Eye“247”AntiMalwareでは管理Managerで指定したファイルパスの他にPC毎に任意のファイルパスを指定できます。

クライアントでデータのリストアを簡単に実行



万が一、ランサムウェアに感染した場合でも、クライアントで簡単に直近のバックアップデータからリストア（復旧）できます。

セキュリティ対策の新しい考え方は「守る」＋「拡散を防ぐ」！
感染拡散防止 ＋ エンドポイントセキュリティという新しい多層防御のカタチで、社内クラスターから情報資産を守ります。

世界中の脅威情報を共有し、最新のセキュリティレベルを保ちます。クラウドでのPC集中管理にて、オフィス外にいても、最新のセキュリティレベルを共有することが可能です。

1 感染拡大を防ぐ

SubGate

世界初のセキュリティスイッチ「SubGate」で、ウイルス拡散時の前兆動作を検知・遮断を行い、二次被害を最小限に抑えます。また、有害トラフィックの遮断、ハッキングによる情報漏えいも防ぎます。

※D-Guard HUB/AP シリーズは、株式会社サブゲートの「SubGate」「SubGate AP」のOEM 製品です。

2 各PCで守る

Eye'24.7 AntiMalware

エンドポイントセキュリティ「Eye“247”AntiMalware」でウイルス検知時隔離、USB 接続時の自動スキャンなどを行い、各 PC を守ります。PC の一元管理や、持出し用 PC のセキュリティにも使えます。

3 業務可視化で守る

Eye'24.7 Work Smart Agent

業務可視化ソフトウェア「Eye “247” Work Smart Agent」にてウェブ閲覧履歴、USBやプリンタの利用履歴の確認が可能。USB・WPDの利用制限もでき、意図的な情報持ち出しの抑止にもなります。PC作業内容のメール自動送信機能も。

企業には企業のための最新セキュリティ！

Internet

SubGate

Eye'24.7 AntiMalware

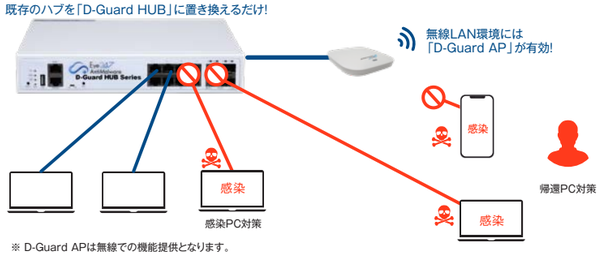
Eye'24.7 Work Smart Agent

拡散防止

ウイルス拡散防止

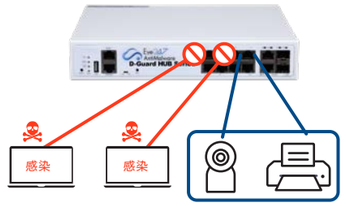
振る舞い検知方式でウイルス拡散時の前兆動作をリアルタイムで検知・遮断し、二次感染や拡散の被害を最小限に抑えることができます

既存のハブを「D-Guard HUB」に置き換えるだけ!



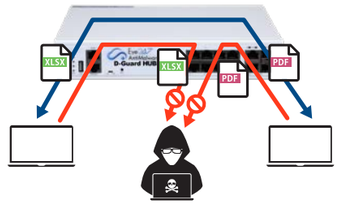
※ D-Guard APは無線での機能提供となります。

有害トラフィック選別遮断



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。

ハッキングによる盗難・盗聴・情報漏えい防止



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。

安全な社内ネットワーク

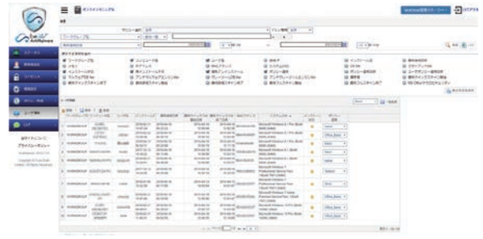
ウイルス拡散

DoS/DDoS攻撃

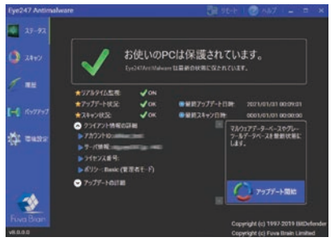
内部ハッキング

Eye'24.7 AntiMalware

操作しやすい管理画面
管理画面は操作しやすく、レポートの確認等も簡単。



わかりやすいクライアント画面
一目で自分のPC状況がわかり、何かあった時もすぐに対応可能に。



未知のマルウェア検知・隔離
ATC機能が未知のマルウェアを検知し、自動で隔離。

マルウェア検知・隔離
世界最高レベルの検知能力で、マルウェア実行前に挙動を検知し隔離。

バックアップリストア機能
保護領域に重要情報をバックアップ。万が一の時は、バックアップデータからリストア（復旧）。

USB自動スキャン
PC接続時にスキャンを実行。マルウェア発見時は拡散させず駆除。

Eye'24.7 Work Smart Agent

USB、プリンタ利用履歴記録
いつ、どのPCで、どのファイルをコピーしたかの管理が可能に。

USB・WPD利用制限
「使用禁止」「書き込みのみ禁止」といった設定が可能。

作業日報自動報告
毎日の作業内容を管理者に自動でメール送信。

ウェブ閲覧、利用アプリ記録
ウェブの閲覧履歴から利用したアプリまでしっかり記録。

店舗・倉庫

外出先

Fuva Brain

UPDATE

セキュリティ製品を組み合わせたソリューション

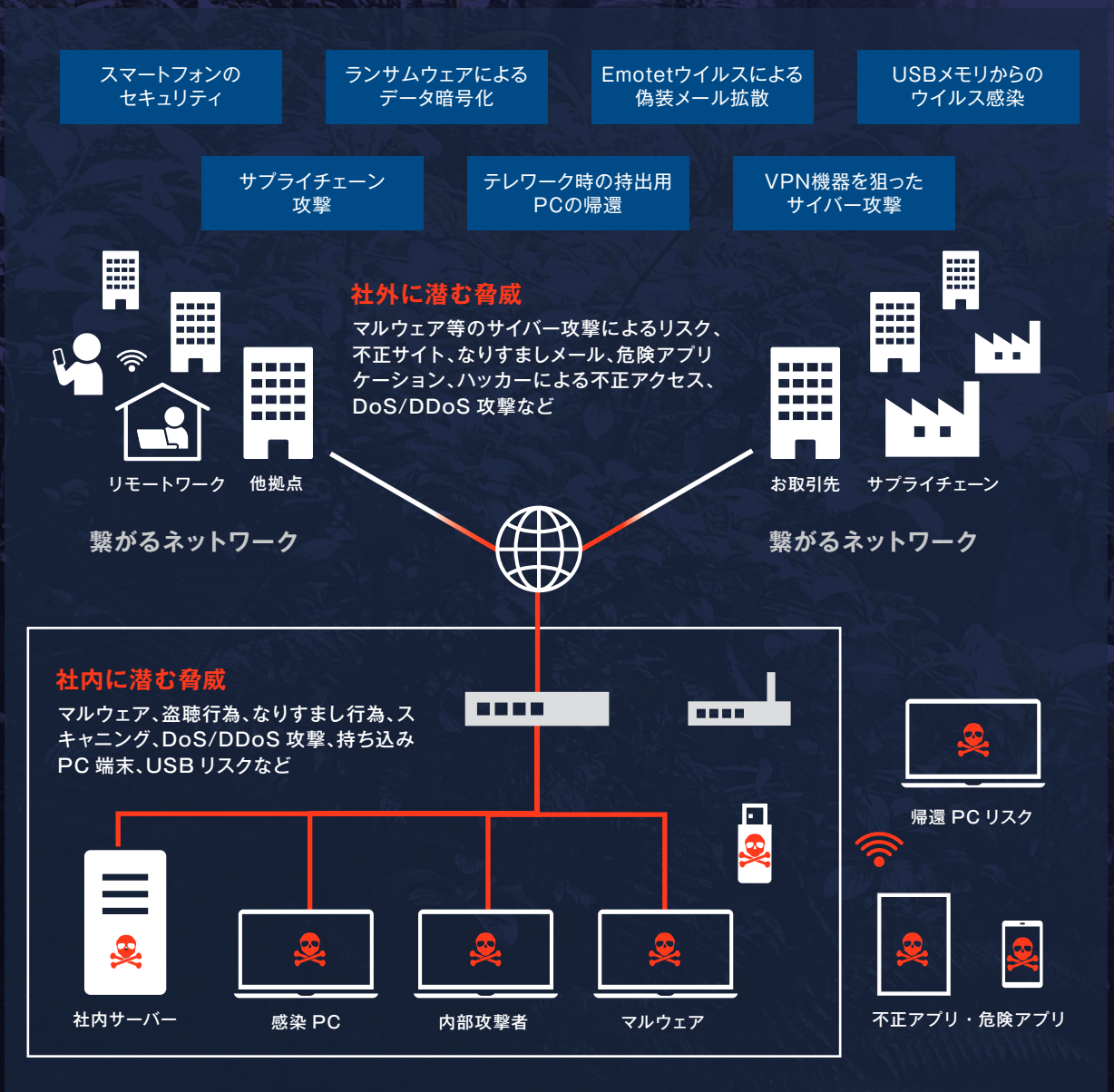
日々、進化するサイバー攻撃から会社を守れますか？

Eye“247”AntiMalware D-Guard HUB/AP シリーズは、世界初※のウイルスの拡散を防ぐ「SubGate」セキュリティインテリジェント L2 スイッチと Fuva Brain の提供するエンドポイントセキュリティ「Eye“247”AntiMalware」、業務可視化ソフトウェア「Eye“247”Work Smart Agent」3つのセキュリティで、従来型のセキュリティでは不可能だった多層防御型のセキュリティを実現し、企業の情報資産を外部・内部の脅威から守ります。

※サブゲート社が有する世界初の特許技術を搭載

ビジネスを脅かすセキュリティ脅威
ウイルス感染から「繋がったネットワーク」を守るために

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できるかが重要です。

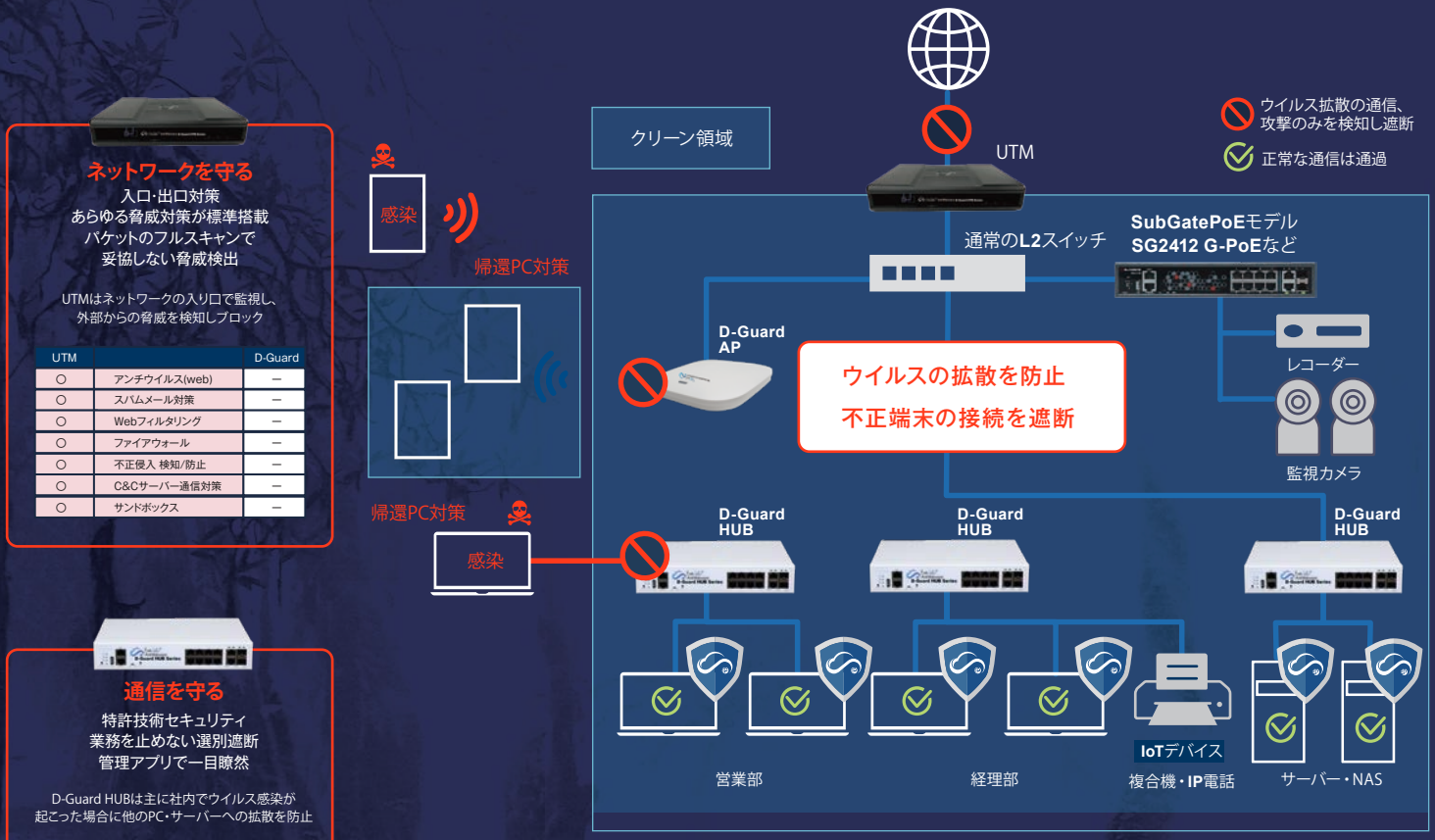


感染後のリスクを考えたことはありますか？

FuvaBrain推奨ネットワーク構成

D-Guard HUB と UTM では守備位置が異なるため、同時導入でセキュリティレベルが大きく上がります。

ネットワークの出入り口は UTM、エンドポイントはウイルス対策ソフト、
そして、万が一のウイルス感染時に感染拡大による被害を最小限に食い止めるため、セキュリティスイッチの導入を推奨しています。



ネットワークを守る

入口·出口対策
あらゆる脅威対策が標準搭載
パケットのフルスキャンで
妥協しない脅威検出

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

UTM		D-Guard
○	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	—
○	サンドボックス	—

通信を守る

特許技術セキュリティ
業務を止めない選別遮断
管理アプリで一目瞭然

D-Guard HUBは主に社内でウイルス感染が
起こった場合に他のPC・サーバーへの拡散を防止

UTM		D-Guard
—	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	○

エンドポイントを守る

Eye 24.7 AntiMalware

未知の脅威に強い振る舞い検知
サーバー設置不要で集中管理
わかりやすい管理画面と自動レポート

情報漏えい抑止

Eye 24.7 Work Smart Agent

操作ログ・業務把握

Eye “247” AntiMalware 管理Manager

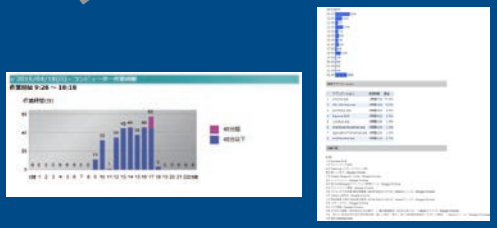
マルウェアの検知状況をリアルタイムに把握できる他、PC・サーバーの機器情報（OS やユーザー名等）、ソフトウェア情報の一元管理が可能です。

ユーザー情報

- マルウェアの検知状況の把握、自動レポート
- OS のバージョンや利用状況、アップデート状況の把握
- スケジュールスキャンの実施状況の把握

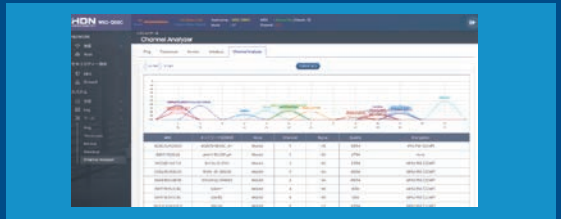
管理者端末

Eye “247” Work Smart Agent 業務日報



毎日の PC の作業内容が翌営業日に管理者にメールで送信されます。

D-Guard HUB統合モニタリング（VNM）



- 複数台の D-Guard HUB/AP 機器を一元管理
- リアルタイム有害トラフィック状況把握
- ネットワークトラフィック分析

※複数拠点の機器を管理する場合、VPN 環境が必要です
※Windows Server での運用を推奨します

型番

シリーズ		CL数	ライセンス期間
Eye"247" AntiMalware D-Guard HUB Series		~5	5年 / 6年 / 7年
		~10	
		~20	
		~50	
Eye"247" AntiMalware D-Guard AP Series		~70	
		~100	
		~150	
		~200	

ハードウェアスペック

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:16.8W / 外形寸法(mm):W250×H44×D200 重量:1.9Kg

ASH-AP	
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,Enterpreise,Mixed Mode) 暗号化方式: CCMP(AES),TKIP
PoE	802.3at(PD)
寸法 / 重量	消費電力:18W 外形寸法(mm): W210×H30×D210 / 重量:0.5Kg

ソフトウェア動作環境

Eye"247" AntiMalware クライアントプログラム		
対応OS (日本語/英語)	下記OSの32ビット、64ビット(×64)をサポートします。 Windows 11 / 10 Windows Server 2022 / 2019 / 2016 / 2012R2 / 2012 Windows Storage Server 2016 / 2012R2 / 2012 Windows Server IoT 2019 for storage ※本製品は、Microsoft .NET Framework4.5.2以上が必要です。 ※Windows11S/10Sは非対応です。	下記OSをサポートします。 macOS Monterey(12.0以上) macOS Big Sur(11.0以上) macOS Catalina (10.15以上) macOS Mojave (10.14以上) macOS High Sierra (10.13以上)
CPU	クロック周波数1.5GHz以上(推奨 2GHz以上) ※Windows11 は、1.5GHz(推奨2GHz以上)で2コア以上 ※IntelまたはAMDプロセッサに対応しています。 ARMプロセッサには対応しておりません。	クロック周波数 2GHz以上 ※Apple M1チップ Intelプロセッサに対応しています。
メモリ	2GB以上(推奨4GB以上) ※Windows11は、4GB以上(推奨8GB以上)	4GB以上
ハードディスク	インストール時に1GB以上の空き容量	インストール時に1GB以上 の空き容量
Eye"247" AntiMalware Manager		
Webブラウザ	Google Chrome(推奨)、Microsoft Edge	
画面解像度	1024×768以上(1280×1024推奨)	

Eye"247" Work Smart Agent	
対応OS	Windows 11 / 10 (32/64ビット版)
対応OS言語	日本語 / 英語
メモリ	4GB以上
ハードディスク	インストール時に500MB以上の空き容量

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LAN / シェアードVLAN / 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 / SPR(Smart Port Redundacy) / UDLD
リンクアグリゲーション	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 / 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 Telenet/SSH / IP SLA / 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 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: ①L2/L3/L4 ACL ②時間ベース ACL ③VLAN ACL ④Ingress/Egress ACL ⑤CPU-ACL IPv4/IPv6 DHCP/NetBiOS フィルタリング / ストーム制御 / 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 / 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 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 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 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 スキャニング遮断: ホストスキャン,ポートスキャン IPv6 DAD攻撃遮断 自動検知/遮断/QoS/Rare Limit 及び解除 / 有害トラフィック発生時アラート機能

※本製品の設置・ご使用に関しましては、製品に添付しております安全上の注意をよくご確認の上、必ずお守りください。※本製品は日本国外での使用については一切のサポート、保証をしておりません。
※記載内容は2023年2月現在のものです。※仕様は予告なく変更する場合がありますので、予めご了承ください。※記載されている製品名は各社の商標・登録商標です。

1_2023.02

お問い合わせ・ご購入はこちらの窓口まで

発売元 Digital communications 株式会社デジタル・コミュニケーションズ

本社 〒103-0014
東京都中央区日本橋蛎殻町1-29-9 ネオテック水天宮ビルM1階
TEL 03-6231-1855 FAX 03-6231-1880
www.dcoms.co.jp