

ウイルスをまん延させない!! 社内ネットワークのセキュリティ対策



DS-VG8



DS-VGX **NEW!!**



DS-VGW

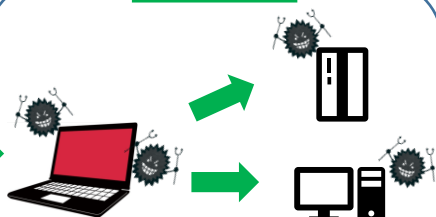
スマートフォン・タブレットの普及やノートパソコンの社外利用(持ち出し)などにより ウイルス感染の経路が多様化しております

自宅(テレワーク)



テレワーク時にSNSを利用。
ウイルスに感染・・・

社内



自宅で使用したパソコンを社内で接続
ネットワーク経由でサーバー等へ感染

2020年5月頃、大手工業メーカー社員が**在宅勤務時に社用持ち出しPCでSNSを利用した**。その際、**ウイルスを含んだファイルをダウンロードし感染**。

社内にPCを持ち帰り、**社内ネットワーク経由でウイルス感染が拡大し**
社内個人情報やサーバーログ、通信パケットが流出したという事件が発生。



宅配便業者をかたる 偽SMS

URL からアクセス
してしまうと・・・

Android

不審アプリを
インストールさせる手口

iPhone

フィッシングサイトで
「Apple IDとパスワード」や
「電話番号と認証コード」を
入力させる手口

図1：アクセスする端末種類毎の手口分類

出典:IPA 情報処理推進機構 情報セキュリティ 安心相談窓口だより

スマートフォンも普及し、仕事での活用も増えております。
パソコンとは違い、個人携帯に「**セキュリティソフト**」が入っていないことも
しばしば・・・。



スマートフォンなどの**携帯端末を狙ったウイルスや
無料アプリのダウンロードの際に、知らず知らずに
ウイルス感染していることも・・・**

スマートフォンから侵入したウイルスが**社内Wi-Fiを通じて
パソコンへまん延**してしまう可能性も十分に考えられます。

HUB

Virus Cluster Guard
8ポートモデル

DS-VG8



Wi-Fi

Virus Cluster Guard
Wi-Fiモデル

DS-VGX **NEW!!**

Wi-Fi6対応

ローミング/メッシュ対応



Wi-Fi

Virus Cluster Guard
Wi-Fiモデル

DS-VGW



HUB
option

Virus Cluster Guard
4ポートモデル(島HUB専用モデル)

DS-VG4



※4ポートモデルは8ポートまたはWi-Fiモデルのオプションであり、単体提供は行っておりません。

DS-VGシリーズ(Virus Cluster Guard)



8ポートHUBタイプ



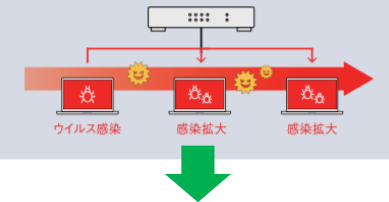
Wi-Fiタイプ **NEW!!**



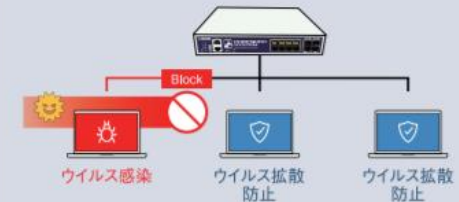
Wi-Fiタイプ

ココが
違う!!!

通常のスイッチングHUBの場合

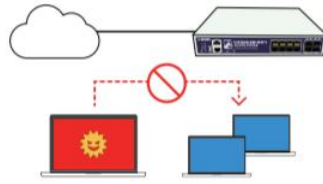


Virus Cluster Guardなら



拡散・まん延を防止する強力な4つのポイント

ウイルスやワームの拡散をブロック、ネットワークへのまん延を防止



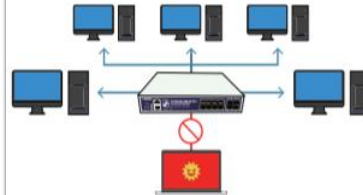
感染を他に広げない

ウイルスやワームなどのマルウェア（悪意を持ったソフトウェア）は、被害を拡大させるため次々と自身の複製を拡散しようとします。

セキュリティスイッチはワームやウイルスなどが拡散する挙動を検知・遮断します。ウイルス対策ソフトのパターンマッチングでは防げない新たな脆弱性や新種のウイルス、巧妙な手口にも対処可能です。

ワーム
自身を複製して他のシステムに拡散する性質を持ったマルウェア（悪意を持ったソフトウェア）の総称。

各種有害トラフィックによる攻撃をブロック



他の端末を攻撃させない

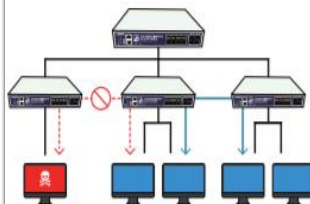
ウイルス感染した端末は、社内の特定機器を攻撃し機能を停止させたり、ネットワークに負荷をかけて業務を阻害します。被害範囲は社内に留まらず、外部に対しても無差別に攻撃を行うため「被害者が加害者になる」恐れがあります。

セキュリティスイッチは有害トラフィックを検知・遮断することにより新種のウイルスに感染しても二次被害を発生させません。

有害トラフィック

DoS 攻撃、DDoS 攻撃、ARPAttack など、ネットワークや機器に負荷をかけ正常な動作を妨げる通信のこと。

内部ハッキング・通信傍受をブロック、情報漏えいを防止



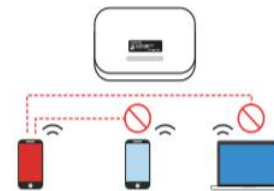
盗聴・傍受の防止

インターネットの発達により、ネットワークの盗聴ツールが誰でもかんたんに手に入る時代です。

IP 電話での通話や PC 同士の通信など、盗聴や傍受がされるとその内容は攻撃者に筒抜けになってしまいます。中間者攻撃と言われる手法により、通信が乗っ取られウイルスに感染させられる恐れもあります。

セキュリティスイッチは盗聴や傍受を検知・遮断することにより機密情報の漏えいを防止します。

セキュリティ対策が難しいスマートフォンへの対応



セキュリティWi-Fi

いまや業務端末の一部となったスマートフォンですが、セキュリティ対策は万全でしょうか？

PC に比べ、スマートフォンのセキュリティ製品は数が少なく、対策が難しいのが現状です。いつの間にかウイルスに感染してしまい、気づかないまま社内ネットワークに接続してしまったらその被害は瞬く間に広がります。

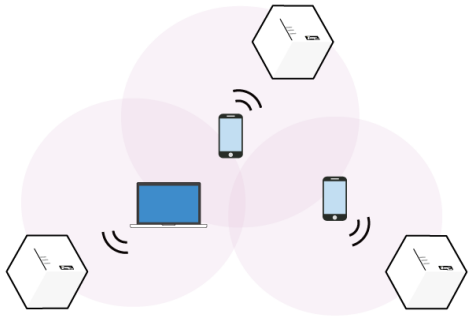
セキュリティスイッチ Wi-Fi モデルなら、スマートフォンがウイルス感染してしまっても、同じネットワークに接続された他の端末への感染拡大を防ぎます。

2025年4月発売開始 Wi-Fi6モデル

Virus Cluster Guard
Wi-Fiモデル

DS-VGX **NEW!!**

Wi-Fi6対応 ローミング/メッシュ対応



Wi-Fi6・ローミング / メッシュ対応

複数台設置する場合、同じSSID・パスワードで端末側が自動的に最適なアクセスポイントに接続します。接続先切り替えの手間なくシームレスに通信範囲を拡大し、接続しやすい環境を構築します。



		DS-VGW	DS-VGX new
無線LAN	規格	IEEE802.11a / b / g / n / ac 5GHz 2x2 867 Mbps + 2.4GHz 2x2 300 Mbps	IEEE802.11a / b / g / n / ac/ax (Wi-Fi 6) 5GHz 4x4 2402 Mbps + 2.4GHz 4x4 1147 Mbps
	認証方式	WPA/WPA2(PSK,Enterprise,Mixed Mode)	WPA/WPA2-PSK, WPA2 Enterprise, WPA3 SAE
	暗号化方式	CCMP(AES),TKIP	CCMP(AES), TKIP, WPA2, WPA3
	最大接続台数	5GHz、2.4GHzそれぞれ32台 計64台	5GHz、2.4GHzそれぞれ64台 計128台
	スループット	1200 Mbps(5GHz + 2.4GHz)	3549 Mbps(5GHz + 2.4GHz)
	アンテナ	内蔵 4本	内蔵 8本
機能	ローミング・メッシュ	—	○(3台まで)
インターフェース	ポート	10/100/1000Base-T x1	10/100/1G/2.5G/5GBase-T x2
動作環境	温度	0～45℃	-10～50℃
	湿度	15～90% ※結露がないこと	
ハードウェア	外形寸法・重量	210(W)x30(H)x210(D)mm / 500 g	225(W)x60(H)x195(D)mm / 960 g
	電源	ACアダプター(18W)、PoE(36Vdc～57Vdc)	ACアダプター(26.3W)、PoE(44Vdc～57Vdc)
製品保証	保証期間	3年(先出しセンドバック方式)	

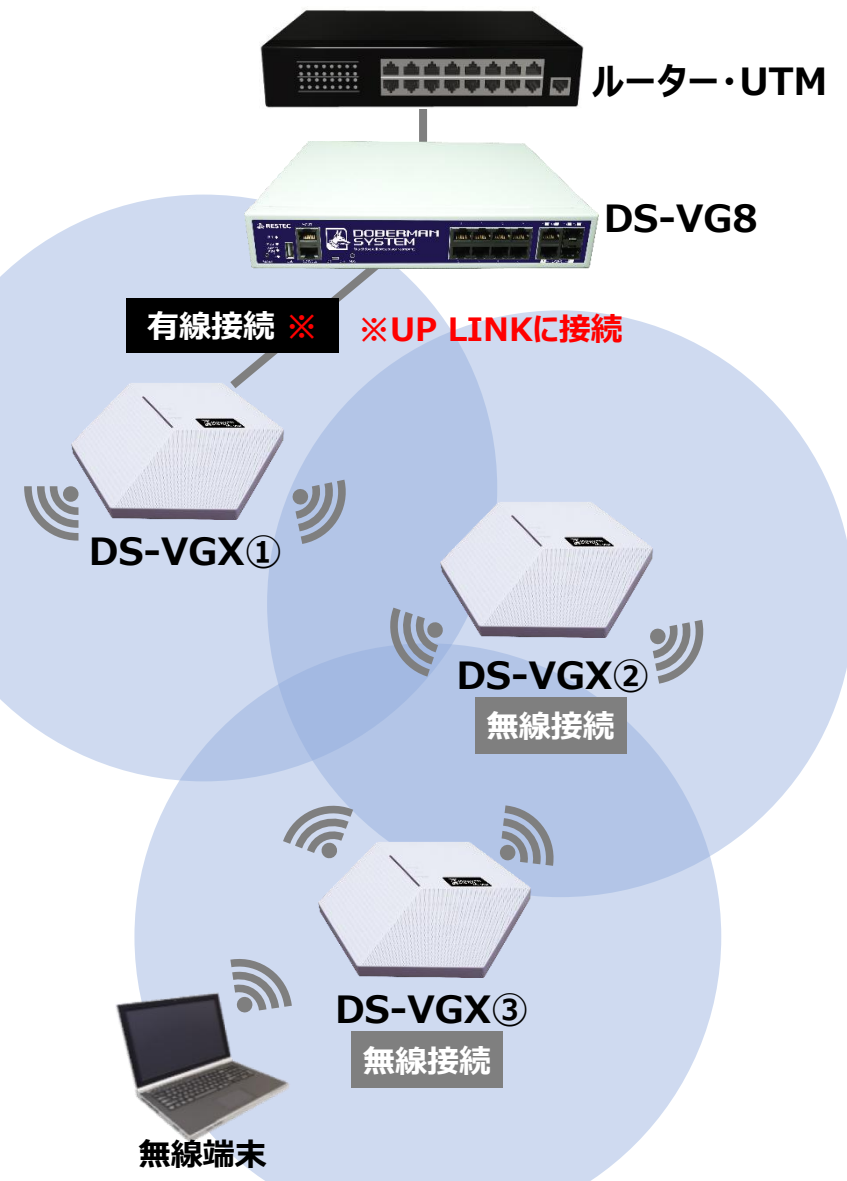
注) メッシュ環境を構築する際、同機種(DS-VGX)が複数台必要(MAX3台まで)です。

注) DS-VGXの設置間隔について、「ワンフロアで壁無し」という条件下で15mが最適です。
30m以上の間隔では電波強度が弱くなるため動作保証外です。

DS-VGX メッシュ / ローミング接続例

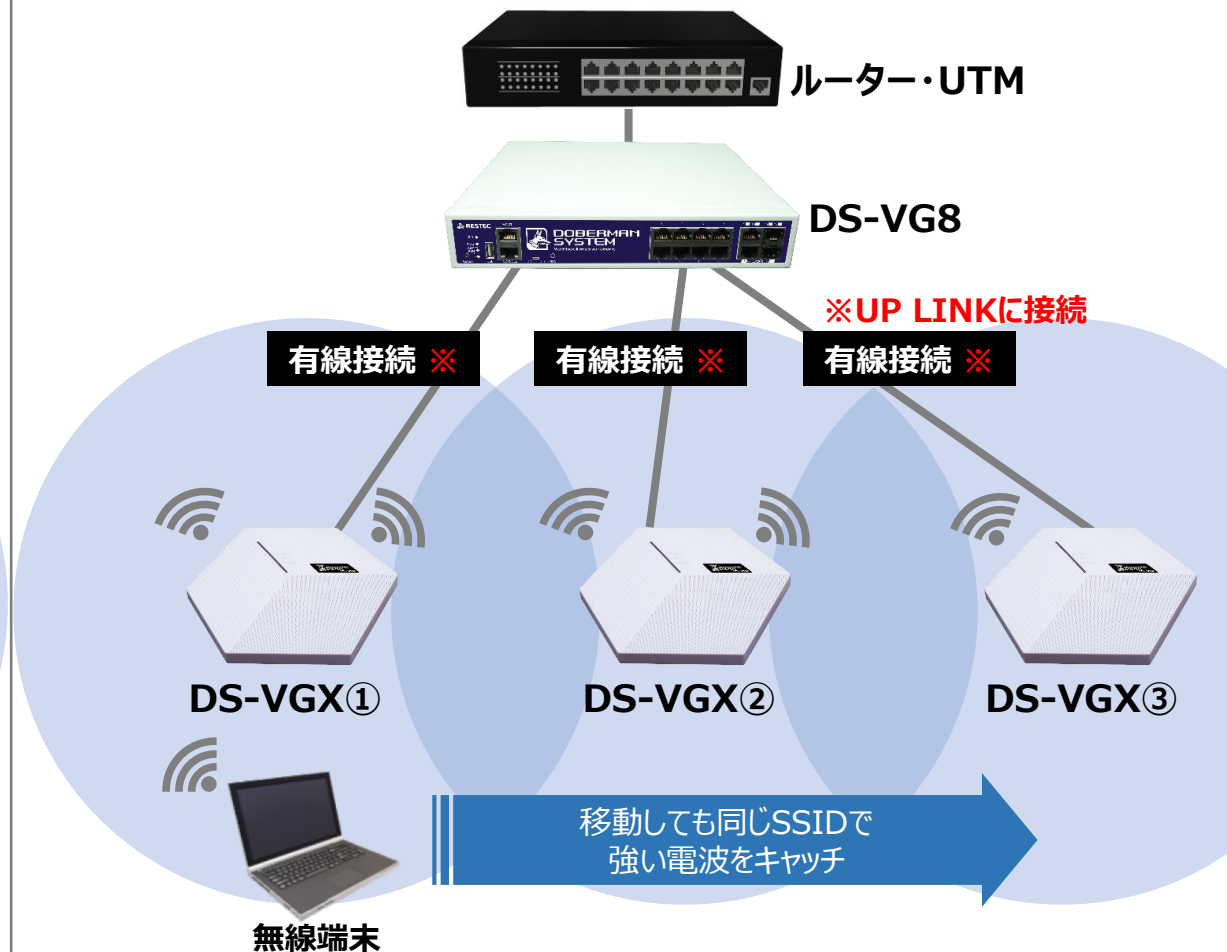
DS-VGX同士を無線接続

※同一のSSID/パスワードで設定可能



DS-VGXを有線接続

※同一のSSID/パスワードで設定可能



⚠ 注意

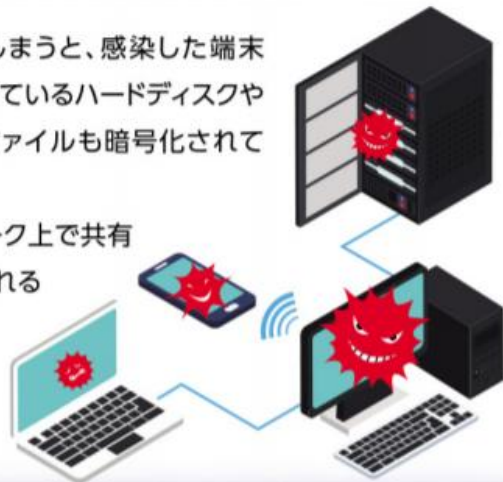
ルーター・UTM等の上流機器には端末を接続しないでください。
その端末が感染していた場合、ネットワーク全体に感染が広がります。

感染拡大のリスク

感染は会社全体に影響も…

ランサムウェアに感染してしまうと、感染した端末だけではなく、その端末に接続しているハードディスクやUSBメモリ等に保存しているファイルも暗号化されてしまいます。

また、社内LANなどネットワーク上で共有しているファイル等も暗号化されるおそれがあります。



出典:警視庁(サイバーセキュリティ対策本部) ランサムウェアに要注意 より

他の人にうつさない!!
【予防】&【まん延防止】と
ウイルス対策は**多重防御!!**



中には**重要データ**も、、、
自身の被害だけに
留まらない、、、感染リスク!!

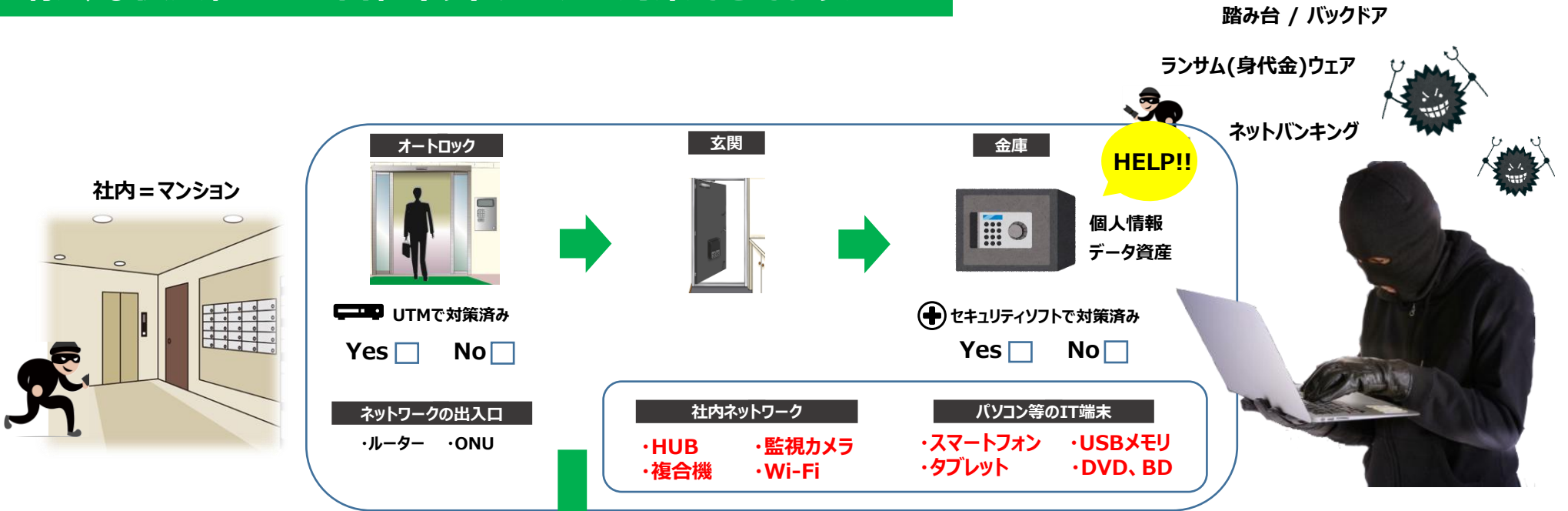


💀 社内にウイルスが拡散 💀

例) 営業の方の社外持ち出しPCが社内に。(社外でウイルス感染)
社内ネットワークを通じて、経理の方のデータまでウイルスに感染してしまった。
感染パソコンから新たな感染先を探しだし、どんどん社内ネットワークを侵食していきます。



様々な侵入経路・・・自社ネットワークは対策できていますか？



USBメモリ

お客様とのやり取りの際に
ウイルス感染・・・そのまま社内に。

**スマートフォン
タブレット**

個人端末から社内Wi-Fiへ接続。
ウイルス対策出来ておらず社内に。

新種のウイルス

セキュリティソフト等では対応
がされていないウイルスに感染。

UTM	防御項目	DS-VG
☐	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	-
-	社内でのウイルス拡散防止	☐
-	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 ※Wi-Fiモデルにはありません	☐

DS-VGシリーズができること

社内ネットワーク端末に対して、さまざまな攻撃方法があります。
特に【盗聴・搾取目的】【まん延】など以下の攻撃に有効です。



1台に感染しても【DS-VG】が社内への感染拡大をガード!! ウイルスマン延を防ぎます。
※ランサムウェア等のウイルスを検知する機器ではございませんのでご注意ください。

どの機器でもウイルス感染の可能性がありますので、**感染時のまん延リスクを最小限にとどめることが必要です。**



インターネット



UTM

個人端末

セキュリティ対策が施されていない個人端末は、ウイルス感染している可能性も・・・。



スマートフォン・タブレット

IP電話・監視カメラ

機器単体ではセキュリティ対策が施せないで、盗聴などの危険性も・・・。



8ポートHUBタイプ



8ポートHUBタイプ

CLEAR



サーバー・NAS



IP電話

古いOSのパソコン

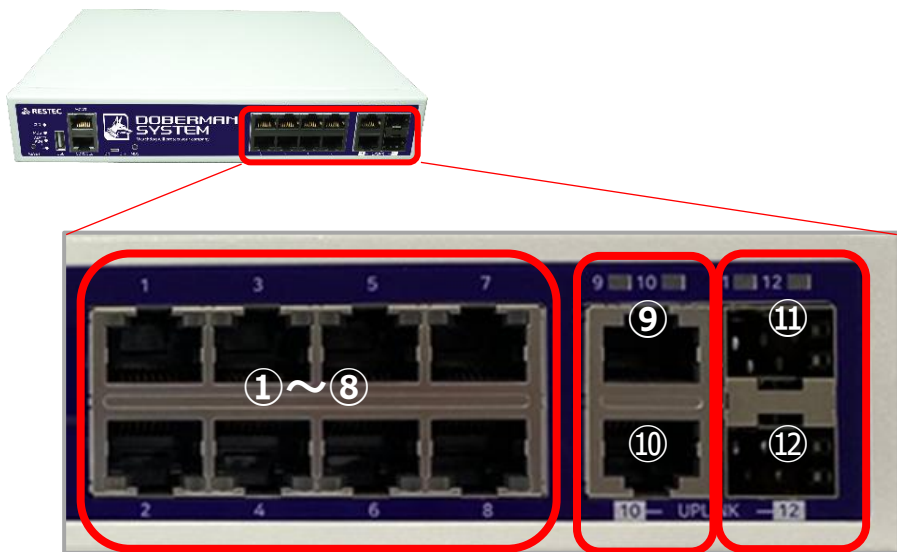
OS Verの古いPCはウイルス感染リスク大。

※Windows 7, XP, Vista

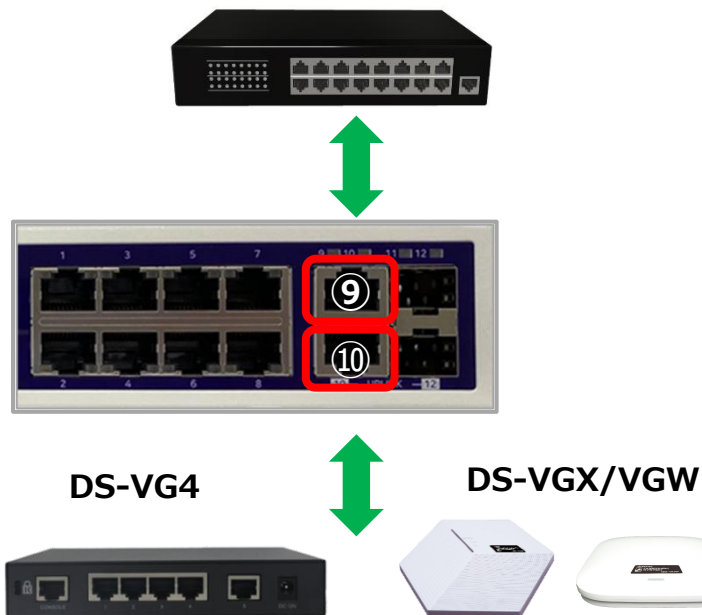
持ち出しのパソコン

テレワーク・出張・外出等
社外のネットワークに接続したPC。
感染の可能性も・・・。

DS-VG8 接続ポートについて



- **ポート①～⑧(DOWN Link)**
機器・端末接続用
(一般的なHUB / アクセスポイントを接続する)
- **ポート⑨・⑩(UP Link)**
上流機器とのカスケード接続用
(どちらに挿してもOK)
上流からの接続(UTM・HUB・ルーター等)は、
⑨・⑩をご使用ください
- **ポート⑪・⑫**
使用しません



UTM・HUB・ルーター等の上流機器からの接続は
UP Linkポート⑨をご使用ください

※⑩も接続可能ですが、説明の都合上指定しております。

【DS-VG8】・【DS-VG4】などをカスケードする場合、
【DS-VGW】を接続する場合は**UP Linkポート⑩**を
ご使用ください

※⑨も接続可能ですが、説明の都合上指定しております。

**Q1.Wi-Fiタイプ(DS-VGX / DS-VGW)は何台まで端末を接続することができますか？
Wi-Fi6には対応していますか？**

A1.カタログ背面に記載しております。

【DS-VGW】	2.4GHz 32台 / 5GHz 32台	64台まで接続可能
【DS-VGX】	2.4GHz 64台 / 5GHz 64台	128台まで接続可能・Wi-Fi6対応

Q2.ウイルスによる悪意のある通信を検知した場合、確認することができるのか？

A2.検知履歴については管理画面上でご確認いただけます。

※カタログ背面に記載のある種類のみです。

Q3.Wi-Fiタイプ(DS-VGX / DS-VGW)に有線でHUB等を接続できますか？

A3.DS-VGX / DS-VGWには上流(ルーター等)からの接続用ポートが1つのみです。下流用の接続ポートはございません。

**Q4.HUBタイプ(DS-VG8)には、5・6・7年のライセンスが記載されておりますが
どのような仕組みですか？**

A4.UTMのような検知機能の更新ライセンスではなく、当社電話サポートのライセンスを5・6・7年とご用意しております。それに伴いハードウェアについても標準3年にプラスする形で、延長保守のオプションメニューもございます。



導入(入替)の流れ



8ポートHUBタイプ

LANケーブルを挿すポートは
取扱説明書にてご確認ください。

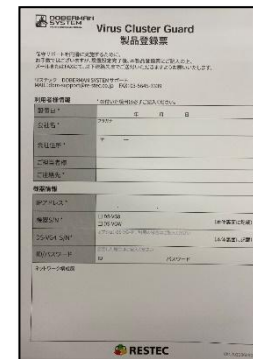
電源コネクタ形状は3 pinタイプで、
2pinへの変換コネクタも同梱。
コンセントに応じてお選びください。

既存でご利用の機器を・・・

交換いただくだけ!!



Wi-Fiタイプ



設置後に、同梱している**「製品登録票」**を
お送りください。

Wi-Fi(SSID)パスワードの設定等が
必要になります。



ウイルスまん延を防止!

新製品「Virus Cluster Guard」

「感染を広げないためのマスク」の役割
をもつ、新世代セキュリティ機器



<https://youtu.be/1tmCJAybTTQ>

Virus Cluster Guardの特長を
動画でわかりやすく解説しています。