SubGate

SubGate

新しい「セキュリティ対策」のカタチ

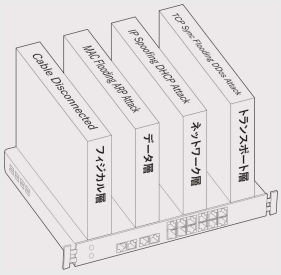
対策が困難だった「拡散防止」「二次被害防止」に
最適な「Network Security Appliance」

ウイルスの拡散を防ぎ、
二次被害からネットワークを守る

SubGate の導入効果

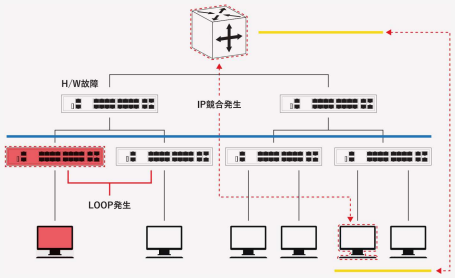
防御し切れない巧妙な攻撃、感染後の二次被害対策は必須!!

年々進化しているサイバー攻撃、もはや感染を100%阻止することは不可能です。SubGateは新種のコンピュータウイルスに感染しても被害範囲を最小限化し、内部の二次被害拡大を防ぎます。



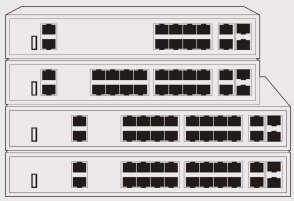
・ウイルス感染後の二次被害対策は必須

・ワームなど、ウイルスの拡散防止
・各種有害トラフィックによる内部攻撃遮断
・通信傍受(ARP-Spoofing)攻撃遮断で情報漏えい防止



・ネットワーク管理・運用が大変

・ネットワーク端末の状況確認・管理
・有害トラフィック発生時のリアルタイムモニタリング
・有害トラフィックを遮断するので安定したネットワークサービスが可能
・ループ発生時、即時検知・遮断及び発生個所(論理ポート番号)特定可能



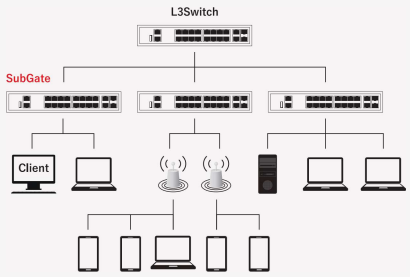
高性能 L2 インテリジェント スイッチ

独自の セキュリティ 機能

専用管理 システム

・コストが高くて導入できない

・高性能L2インテリジェンススイッチと内部ネットワークセキュリティ機能を統合、導入・運用コストの大幅削減が可能
・専用の統合管理システムを無償提供



・機能が良くても導入・運用が大変

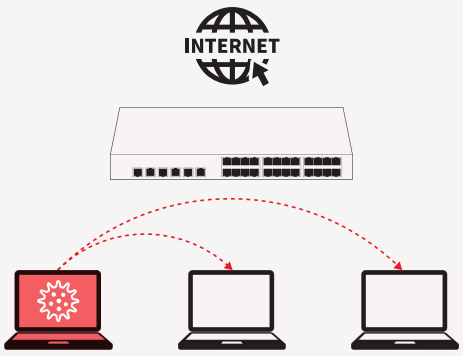
・現在利用しているL2スイッチ(HUB)と入れ替えるだけで導入が完了
・既存ネットワーク機器との干渉・依存無し(共存可能)
・簡単操作(コマンド体系)

SubGate 導入の必要性

過去発生した大きなサイバーセキュリティ事故から得た教訓は、様々セキュリティ脅威に対抗するために、既存の入り口対策だけではなく、今までなかった「出口・裏口」のセキュリティを強化する必要があります。

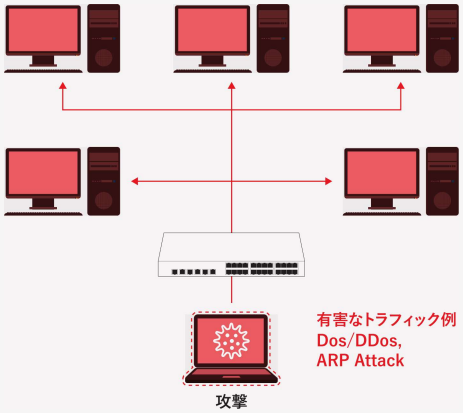
SubGate が提供する3つのセキュリティ機能

SubGate が安全で快適なネットワーク環境を提供



ワーム・ウィルスなどの拡散をリアルタイムで検知・防止

昨今のネットワークセキュリティは、入り口や端末側のセキュリティソフトにより、一定の防御を行っていますが、新しい脆弱性や巧妙な手法には歯が立たず、被害が後を絶ちません。特に、ウイルス対策が困難なモバイルデバイスやBYOD機器、USBメモリやCDなど媒体を経由したデータが、ネットワークに流れる場合、現状の対策は十分とは言えません。そこで、SubGateは、振舞検知方式で、新しいワームやウィルスなどの拡散の挙動をリアルタイムで検知・遮断することができますので、既存のパターンマッチング製品では対応できない2次感染や拡散の被害を最小に抑えることができます。

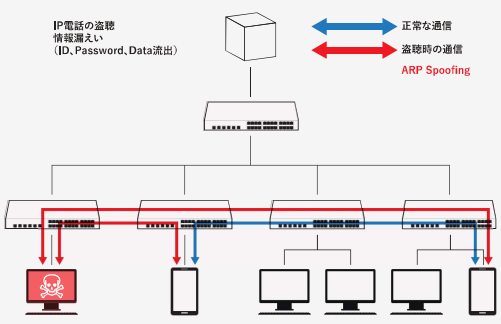


有害トラフィックによる各種攻撃を遮断

ウイルスは目的によって社内の特定マシンを攻撃し、サービスができないようにしたり、ネットワークの運用を妨害するために必要のないトラフィックを出すことでネットワークの負荷を上げるような攻撃を行います。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ので知らないうちに「加害者」になる恐れもあります。SubGateは広範囲の有害トラフィックを検知・遮断することによって、新種ウイルスに感染しても二次被害を発生させません。

※有害トラフィックの事例

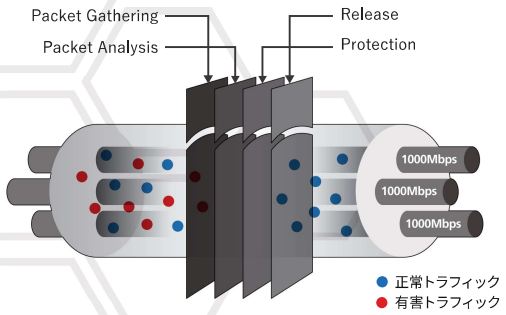
攻撃の狙い	動 作	種 類
特定マシンを定め、 機能できないようにする	特定のIPに大量のパケットを 送信し、CPUの負荷を上げる	DoS、DDoS Attack IP Spoofingなど
ネットワークに不要な負荷を掛ける	不特定多数のIPに大量の パケットを送信	Broadcast Attack DHCP Floodingなど



ハッキングによる盗難・盗聴・情報漏えい防止

インターネットで入手できてしまうフリーのツールなどを使えば、ID/パスワードのハッキングやIP電話の盗聴、エクセル、ワード、パワーポイントなどの各種資料が簡単に不正取得される時代です。実際のウイルスにはこのような内部ハッキングするウイルスが数多く存在し、自分も知らいないうちに踏み台にされ、加害者になってしまいます。このような通信傍受系マルウェアに感染されるとマイナンバーを含む機密情報が盗まれたり、IP電話での重要な会話の盗聴、メールアカウント情報盗用、テレビ会議や監視カメラデータの改ざんなど、被害範囲は計り知れません。ウイルスの感染によって、企業内のPCがこれらの脅威の踏み台として利用される事件、事故も増加しています。SubGateはこのような通信傍受の代表的な攻撃であるARP-Spoofing攻撃をアクセスネットワーク層で検知・遮断できるように搭載した新しい製品です。

SubGate の特長



有害トラフィックの選別遮断

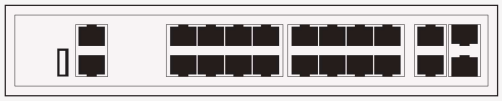
有害トラフィックのみ選別遮断するSmart遮断方式

・ネットワークに問題を及ぼす有害トラフィックのみを選別検知/遮断
・正常トラフィックは遮断しないため通常業務の継続が可能

MDSセキュリティエンジン

MDS Security Engine

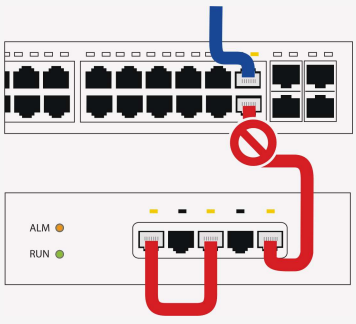
・特許技術によるロジックでリアルタイムPacket分析
・行動基盤方式(振る舞い検知型)で新種ウイルスによる攻撃も検知・遮断可能
・パターンファイルの更新不要



強力な認証機能

認証されていない端末のアクセスを防止

・Embedded RADIUSサーバ標準装備
・最大512ユーザーまで認証可能
・802.1X/MAC/Multi-User認証サポート



リアルタイムループ遮断

ユーザPort間に発生する様々なループ遮断

・ユーザミスによるLoop遮断
・ネットワークサービスDOWN防止
・ループ発生箇所を瞬時で特定、迅速な対応が可能

統合ネットワーク管理SW

03 Management

管理：簡単な管理体系
装置形状/自動Configuration保存/グループ別ポリシー及びリモート設定機能

02 Visibility

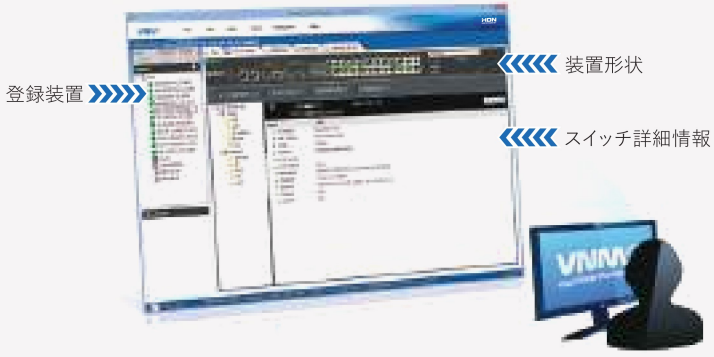
可視性：ネットワーク状況の可視性確保
ネットワーク全体の状況/有害トラフィックの発生状況/ネットワーク構成図

01 Analysis

分析：リアルタイム有害トラフィック分析
有害トラフィック分析/過去Event分析ユーザ追跡分析

Visual Node Managerは複数の
SubGateを簡単に統合管理できます

VNM導入時のメリット



- ネットワークの専門知識がなくてもネットワーク管理及び分析が可能
- 統合管理による運用者の業務軽減
- ネットワーク管理のための追加NMS 導入のコスト不要

VNMの機能

ネットワーク図作成

リアルタイム有害トラフィック監視

SubGate設定

ネットワークトラフィック確認

SG2400シリーズ

		Non PoE SG2400 Series						PoE SG2400 Series		
		SG2412GW	SG2420G	SG2428G	SG2452G	SG2430GX	SG2456GX	SG2412GPoE	SG2420GPoE	SG2452GPoE
H/W	Mac capacity (K)	16K	16K	16K	16K	16K	16K	16K	16K	16K
	Power Supply	1	1	1	1	1+1(option)	1+1(option)	1	1	1
	Power Redudancy	-	-	-	-	Support	Support	-	-	-
	Power Hot-Swap	-	-	-	-	Support	Support	-	-	-
インターフェース	10/100 Base-TX	-	-	-	-	-	-	-	-	-
	10/100/1000 Base-T	10	18	24	48	24	48	10	18	48
	1000 Base SX/LX/ZX	2	2	4	4	-	-	2	2	4
	10G Base-R	-	-	-	-	4 + 2(option)	4 + 4(option)	-	-	-
	最大使用ポート	12	20	28	52	30	56	12	20	52
PoE	PoE/PoE+	-	-	-	-	-	-	af/at/bt	af/at/bt	af/at
寸法/重量	消費電力 (W)(Dual)	16.8W	22.4W	25.3W	44.3W	30.1W(33.8W)	50.7W(54.5W)	25.1W	30.6W	53.2W
	Width (mm)	250	250	440	440	440	440	280	280	440
	Height (mm)	44	44	44	44	44	44	44	44	44
	Depth (mm)	200	200	330	330	400	400	280	280	330
	Weight (kg) (Single/Dual)	1.9kg	2.0kg	3.8kg	4.4kg	6.6kg	7.2kg	3.2kg	3.3kg	5.3kg

※SG2412G、SG2420Gモデルはファンレス(FAN LESS)タイプです。

SubGate AP

H/W	Model	WSG-1200C
	Antennas	Built-In
	Power Supply	1+1(PD)
Interface	Console Port	1
	10/100/1000 Base-T	1
Wireless	protocol	802.11a/b/g/n/ac
	Security	WPA/WPA2(PSK, Enterprise, Mixed Mode)
	encryption	CCMP(AES) , TKIP
PoE	only PowerDevice	802.3at(PD)
寸法/重量	消費電力	18W
	Width(mm)	210
	Height(mm)	30
	Depth(mm)	210
	Weight(kg)	0.5

SG1005G

H/W	Mac capacity (K)	8K
	Power Supply	1
インターフェース	10/100 Base-TX	N/A
	10/100/1000 Base-T	5
	1000 Base SX/LX/ZX	N/A
	10G	N/A
	最大使用ポート	5
PoE	PoE/PoE+	N/A
寸法/重量	消費電力 (W)	12
	Width (mm)	158
	Height (mm)	27
	Depth (mm)	105
	Weight (kg) (Single/Dual)	0.37

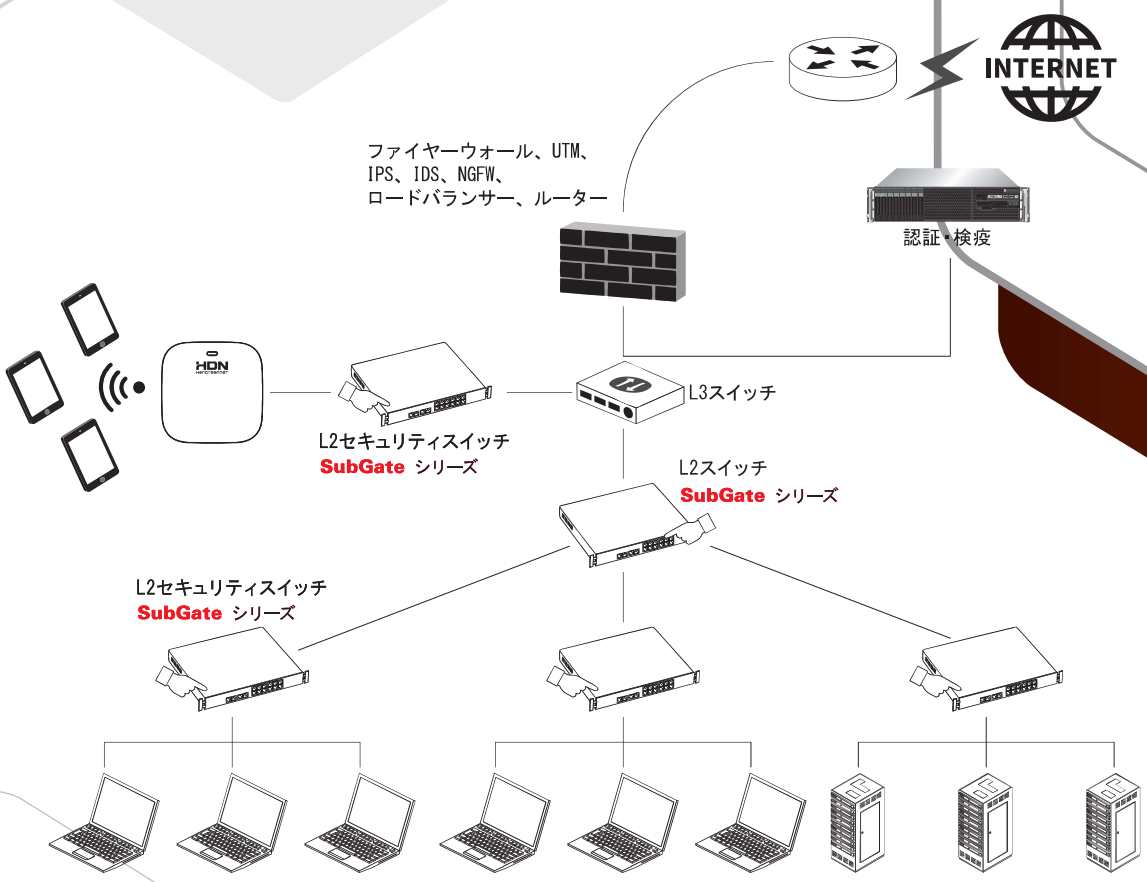
仕様詳細

特徴	仕様
VLAN	• 4K VLAN ID Range(Active VLAN 512) • 802.1Q Port based VLAN • Protocol/IP Subnet/MAC based VLAN • Shared VLAN • Hybrid VLAN • Voice VLAN • 802.1ad VLAN stacking (QinQ)
Resiliency	• STP/RSTP/MSTP • PVSTP • ERP (Ethernet Ring Protection) • Self Loop Protection • SPR (Smart Port Redundancy) • SSR (Smart Switch Redundancy) • UDLD
Link Aggregation	• IEEE 802.3ad LACP, Static-channel-group • Trunk groups – 5,12,20,28,30 Model(max 12 group) – 52, 56 (max 24 group)
Monitoring	• Port Mirroring • 1:1, N:1, N:N TFM (Traffic Flow Monitoring)
L2 Multicast	• IPv4 IGMP Snooping (v1/v2/v3) • IPv6 MLD Snooping (v1/v2)
QoS	• 8 queue per port • Rate Limit (Ingress/Egress) • Diffserv • Auto QoS • SP, WRR, DRR
Management	• LLDP, LLDP-MED • RMON (Group 1,2,3,9) • Local/Remote Syslog • USB インターフェースサポート • Auto Config 機能サポート • Multi OS • 統合管理 S/W (VNM) • IPv4/IPv6 Telnet / SSH • IP SLA • Software Download: FTP, SFTP, TFTP, USB • DHCP Server/Relay • SNMP v1/v2c/v3, Trap 対応 • sFlow • NTP/SNTP • SIM(Single IP Management): • 802.3az EEE

特徴	仕様
Security	• セキュリティ専用 Engine • DHCP Snooping • Port Security • IP Source Guard • ACL – L2/L3/L4 ACL – Time Base ACL – VLAN ACL – Ingress/Egress ACL – CPU-ACL • IPv4/IPv6 DHCP/NetBIOS Filtering • Storm Control • Embedded RADIUS 認証 • IP, MAC, IP+MAC 組合せ認証(VIPM) • AAA 認証 – Local, RADIUS, TACACS+ 認証 • Multi 認証 • 802.1x – Multi-user, MAC bypass Guest-VLAN, Dynamic-VLAN • 有害トラフィック選別遮断 – Attack 遮断 : DoS/DDoS Attack, DHCP Attack, ICMP Attack, ARP Attack – Flooding 遮断 : TCP Syn Flooding, UDP Flooding, MAC Flooding – Spoofing 遮断 : ARP Spoofing, IP Spoofing – Scanning 遮断 : Host Scanning, Port Scanning – IPv6 DAD Attack 遮断 : • 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
PoE	• 802.3af / 802.3at • ポート別 PoE 電源遮断機能

＊ 一部モデルでは仕様が異なる場合があります。
＊ 802.3btはSG2412GPoE/SG2420GPoEモデルのみサポート

SubGate の導入環境例



株式会社サブゲート
〒101-0021 東京都千代田区外神田2-5-15外神田Kビル4階
TEL: 03-5207-2744 / FAX: 03-5207-2743
www.subgate.co.jp
sales@subgate.co.jp
tech@subgate.co.jp

スイッチリプレースなら
「SubGate」

ネットワーク脅威からの
被害を最小化！