ネットワークのあらゆる脅威に対応、効率的なネットワークを実現

ネットワークアプライアンスプラットフォーム「Fujitsu Network IPCOM EX2シリーズ」と、ファイアーウォール、アンチウイルス、クラウドサンドボックス、IPS、Webコンテンツ・フィルタリング、VPNなどネットワークセキュリティ機能を持つ「EX2 SCソフトウェア」、帯域制御、リンク負荷分散などネットワークの信頼性向上に必要な「EX2 NWソフトウェア」を用意しており、安全で高信頼なネットワークを実現します。また、セキュリティ対策に必要な他社製品に関しても取り扱っています。

Fujitsu Network IPCOM

CHECK ! https://www.fujitsu.com/jp/nwps/ipcom/

ネットワークアプライアンスプラットフォーム
IPCOM EX2 シリーズ

ネットワークセキュリティ　IPCOM EX2 SC ソフトウェア	
次世代ファイアーウォール	アプリケーション通信の可視化と制御で、幅広い脅威に対するネットワークセキュリティの強化を実現。
統合セキュリティ対策（UTM※1）、高速 VPN 対応	ファイアーウォール、アンチウイルス、クラウドサンドボックス、IPS、WAF※2、Web コンテンツ・フィルタリング、IPsec-VPN、L2TP／ IPsec によりさまざまな脅威に対応。暗号化処理専用アクセラレーター（ASIC）の搭載。
認証・検疫	不正利用者や危険な端末の接続を遮断し、セキュアな社内ネットワークを実現。

ネットワーク最適化　IPCOM EX2 NW ソフトウェア	
次世代帯域制御	アプリケーション通信の可視化と帯域制御で、重要なアプリケーショントラフィックを保護し、安定したレスポンスを実現。
リンク負荷分散	複数の回線を束ねて、一本の広帯域回線として利用可能。
認証・検疫	不正利用者や危険な端末の接続を遮断し、セキュアな社内ネットワークを実現。

※1 UTM（Unified Threat Management）：ファイアーウォール、アンチウイルス、クラウドサンドボックス、VPN などを統合した機能。統合脅威管理。
※2 WAF：Web アプリケーションファイアーウォール

■ 他社セキュリティ対策製品

シスコシステムズ社製 セキュリティアプライアンス

CHECK ! https://www.fujitsu.com/jp/products/network/cisco/

Identity Services Engine、Secure Network Analytics

アクセス権限管理	アクセス情報を識別し、アクセス権限を設定・管理。ネットワークの可視性とセキュリティ分析。

Firepowerシリーズ

セキュリティ／帯域制御	ファイアーウォール／ VPN 機能を提供するのに加え多様な脅威に対して包括的な防御。

Firepower Management Center

セキュリティ機能を統合	ネットワークセキュリティ、および VPN サービスを単一のプラットフォームに集約。高度な侵入防御システムやマルウェア防御をサポート。

FireEye 社製 脅威対策プラットフォーム

CHECK ! https://www.fujitsu.com/jp/products/network/security/fireeye/

FireEyeシリーズ

標的型攻撃対策	不審なファイルをアプライアンス上の仮想環境で実行・観察し、未知の攻撃の見える化を実現。

Palo Alto Networks社製 次世代ファイアーウォール

CHECK ! https://www.fujitsu.com/jp/products/network/security/paloalto/

PAシリーズ、VMシリーズ、Panoramaシリーズ

次世代ファイアーウォール	アプリケーションの身元やその利用者への脅威の種類によるファイアーウォールポリシーで安全な使用許可を実現。
標的型攻撃対策	不審なファイルをクラウド上の仮想環境で実行・観察、WildFire により、未知の攻撃からもシステムを防御可能。

PFU社製 セキュリティ製品

CHECK ! https://www.fujitsu.com/jp/nwps/inetsec/

iNetSecシリーズ

セキュリティ対策アプライアンス・脆弱性検査	ネットワーク上に存在するパソコンやプリンタなど、さまざまな ICT 機器を自動的に検出し、管理外の不正なネットワーク接続を排除可能。また脆弱性検査サーバと連携し、パソコンの脆弱性の検査が可能。

タニウム社製 端末向けセキュリティプラットフォーム

CHECK ! https://www.fujitsu.com/jp/products/network/security/tanium/

Tanium Endpoint Platform

リアルタイムな端末管理	高速に PC・サーバなどの端末の状態を一元的に可視化し、端末の管理・制御を実現。

Fujitsu Network IPCOM

CHECK ! https://www.fujitsu.com/jp/nwps/ipcom/

IPCOM EX2 シリーズ

ネットワークのあらゆる脅威に対応したり、効率的なネットワークを実現するネットワークアプライアンスプラットフォーム「Fujitsu Network IPCOM EX2 シリーズ」

RoHS 対応

IPCOM EX2-3500

標準価格（税別）：¥3,887,000

IPCOM EX2-3000 SC ソフトウェア V01 利用時の最小構成の標準価格（税別）：¥4,090,500 ～

IPCOM EX2-3000 NW ソフトウェア V01 利用時の最小構成の標準価格（税別）：¥4,167,500 ～

RoHS 対応

IPCOM EX2-3200

標準価格（税別）：¥2,277,000

IPCOM EX2-3000 SC ソフトウェア V01 利用時の最小構成の標準価格（税別）：¥2,480,500 ～

IPCOM EX2-3000 NW ソフトウェア V01 利用時の最小構成の標準価格（税別）：¥2,557,500 ～

NEW　RoHS 対応

IPCOM EX2-1100B

標準価格（税別）：¥667,000

IPCOM EX2-1000 SC ソフトウェア V01 利用時の最小構成の標準価格（税別）：¥730,500 ～

IPCOM EX2-1000 NW ソフトウェア V01 利用時の最小構成の標準価格（税別）：¥807,500 ～

IPCOM EX2 SC ソフトウェア機能

• 標準搭載機能

ルータ / ファイアーウォール※1 / アノマリ型 IPS

必要に応じて機能を追加

• オプション機能

シグネチャー型 IPS※2	アンチウイルス※3	クラウドサンドボックス※4	Web コンテンツ・フィルタリング※5	WAF
L2TP／IPsec	帯域制御※1	SSL アクセラレーター	リンク負荷分散	IPsec-VPN
認証・検疫ゲートウェイ	標的型攻撃対策連携	クラウドサービス制御※6		

IPCOM EX2 NW ソフトウェア機能

• 標準搭載機能

ルータ / ファイアーウォール※1 / アノマリ型 IPS / 帯域制御※1 / リンク負荷分散

必要に応じて機能を追加

• オプション機能

FNA ルーティング	シグネチャー型 IPS※2	アンチウイルス※3	クラウドサンドボックス※4	Web コンテンツ・フィルタリング※5
IPsec-VPN	L2TP／IPsec	認証・検疫ゲートウェイ	標的型攻撃対策連携	クラウドサービス制御※6

※1　アプリケーション辞書・国／地域別 IP アドレスリストに対応
※2　IPCOM EX2 シグネチャー型 IPS サポートサービスの契約が必要です。
※3　IPCOM EX2 アンチウイルス サポートサービス 2 または IPCOM EX2 アンチウイルス サポートサービス 2（クラウドサンドボックス付）の契約が必要です。
※4　IPCOM EX2 アンチウイルス サポートサービス 2（クラウドサンドボックス付）の契約が必要です。
※5　IPCOM EX2 Web コンテンツ・フィルタリング サポートサービスの契約が必要です。
※6　クラウドプロキシ機能とドメインリスト管理を提供。

【 アイコンの説明 】

RoHS対応　RoHS指令（EU〈欧州連合〉）が2019年7月22日に施行した有害物質規制）に適合した製品です。

● IPCOM EX2 シリーズのハードウェアオプションについてはこちらをご参照ください。
https://www.fujitsu.com/jp/products/network/material/#option-load-balancer

IPv6 Ready Logo Phase-2：
IPv6 対応機器同士の高度な相互通信についての認定プログラム。
詳細はホームページをご覧ください。
https://www.ipv6ready.org/

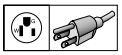
■ IPCOM EX2シリーズ ハードウェア

シリーズ名		IPCOM EX2シリーズ		
モデル名		EX2-3500	EX2-3200	EX2-1100B
インターフェース ※1	10／100／1000BASE-T	0[20]	4[12]	4[8]
	1000BASE-SX ※12	0[10]	0[4]	0[2]
	10GBASE ※2	0[10]	0[4]	–
拡張スロット数		5	2	1
拡張インターフェースカードオプション	1000BASE-Tインターフェースカード2（バイパス機能付き）※3 ※12	○		
	1000BASE-Tインターフェースカード4	○		
	1000BASE-SXインターフェースカード2 ※12	○		
	10Gbase-SFP+インターフェースカード2	○		–
暗号カード ※4	暗号カードA ※13	○		–
	暗号カードA2H ※13	○		–
	暗号カードB2	○		–
ストレージ				
	IPCOM EX2-1100用HDD ※5	–		○
	IPCOM EX2-3500／3200用HDD ※6	○		–
電源二重化				
	EX2-3500電源二重化オプション	○	–	
	EX2-3200電源二重化オプション	–	○	–
保守・運用管理	運用管理LAN	10／100／1000BASE-T × 1		1000BASE-T × 1
	RS-232Cシリアルインターフェース	コンソール接続用（D-SUB9 ピン）×1		
	UPS-LAN ※7	10／100／1000BASE-T × 1		100／1000BASE-T × 1
諸元	形態	19インチラック搭載（2U）	19インチラック搭載（1U）	19インチラック搭載（1U）／卓上設置
	外形寸法（W.D.H）突起物を除く	439mm×698.5mm×87mm	422mm×689mm×44mm	422mm×437mm×43.7mm
	ラックマウントキット	標準添付	標準添付	○
	最大重量	21kg（本体＋添付レール＋オプションフル搭載）	15kg（本体＋添付レール＋オプションフル搭載）	9kg（本体＋ラックレール＋オプションフル搭載）
	入力電圧	AC100-120V／AC200-240V	AC100-240V	AC100-240V
	電源ケーブル ※8	◎		
	AC100V用	○（平行2極接地極付プラグ）		
	AC200V用	○（NEMA L6-15P）		
	定格電流	AC100V 9.5A／電源ユニット AC240V 4.8A／電源ユニット	AC100V 3.5A／電源ユニット AC240V 1.5A／電源ユニット	AC100V 2.5A AC240V 1.1A
	消費電力／皮相電力 ※9	210W／215VA ※10 256W／262VA ※11	167W／171VA ※10 180W／186VA ※11	82W／85VA
	発熱量 ※9	756kJ／h ※10 922kJ／h ※11	602kJ／h ※10 648kJ／h ※11	296kJ／h
	騒音	7.5B（A）以下		6.5B（A）以下

○ オプション（必要に応じて選択）
◎ 必須オプション（いづれかのオプションを必ず選択）

IPCOM EX2シリーズ 型名／価格一覧→P13-9

注：平行2極接地極付プラグ



※1　[ ]内はオプション使用時の最大値。
※2　10GBASE-SR用、LR用SFP+モジュールまたは10GBASE-CRケーブルを搭載可能。
※3　1000BASE-Tインターフェースカード2（バイパス機能付き）は最大1枚搭載可能。
※4　暗号カードAは最大2枚、暗号カードA2H／B2は最大1枚搭載可能。なお、暗号カードA／A2H／B2の混在搭載は不可。
※5　EX2-1000 LB ソフトウェア V01使用時は必須。
※6　EX2-3000 IN ソフトウェア V01およびEX2-3000 LB ソフトウェア V01使用時は必須。
※7　サポートUPSは、PY-UPAR122、PY-UPAR152、PY-UPAC3K2で、LANケーブル（ストレート）接続。なお、各UPS装置にはネットワークマネージメントカード（PY-UPC01）が必要。
※8　電源ケーブルはオプションのため、AC100V（IX2HPCNA）／AC200V（SJ-PWCBL2）用いづれかのケーブルが必須。なお、電源二重化利用時は2本必要。
※9　AC100V使用時の値
※10　標準電源構成時
※11　電源二重化オプション搭載時
※12　EX2-3000 DC ソフトウェア V02との組み合わせでは未サポート。
※13　EX2-3000 DC ソフトウェア V02との組み合わせでは未サポート。 暗号カードB2を使用してください。

■ IPCOM EX2 SCシリーズ ソフトウェア

ハードウェア装置名			EX2-3500／EX2-3200	EX2-1100B
ソフトウェア名			EX2-3000 SC ソフトウェア V01	EX2-1000 SC ソフトウェア V01
IPルーティング	IPv4		Static、RIPv1／v2、OSPFv2、BGPv4	
	IPv6		Static、RIPng	
PPPoEクライアント			●	
FNAルーティング			–	
Link Aggregation			●	–
VLAN			●	
アドレス変換機能 ※1			●	
UTM				
ファイアーウォール ※1			●	
	最大	性能 ※2	15Gbps	5Gbps
		セッション処理性能 ※3	120,000 セッション／秒	78,000 セッション／秒
	サイジング用性能 ※4		7Gbps	3.5Gbps
	最大同時セッション数		2,000,000	200,000
アノマリ型IPS ※1			●	
シグネチャー型IPS ※1 ※5 ※6			○	
アンチウイルス ※5 ※6			○	○
クラウドサンドボックス ※5 ※6			○	○
Webコンテンツ・フィルタリング ※5 ※6			○	
WAF ※6			○	–
VPN				
IPsec-VPN ※1 ※7			○	
	最大性能 ※8		暗号カードA×1 利用時：2.0Gbps 暗号カードA×2 利用時：3.5Gbps 暗号カードA2H×1 利用時：5.5Gbps 暗号カードB2×1 利用時：7.0Gbps	0.6Gbps
L2TP／IPsec ※7			○	
帯域制御 ※1			○ ※12	
	最大	制御可能帯域幅 ※2	13Gbps	4.5Gbps
		セッション処理性能 ※3	100,000 セッション／秒	74,000 セッション／秒
	サイジング用性能 ※4		6.0Gbps	3.5Gbps
	最大同時セッション数		2,000,000	200,000
サーバ負荷分散			–	
SSLアクセラレーター ※1 ※9			○ (TLS1.0／1.1／1.2／1.3)	–
	最大性能 (RSA 2,048bit) ※10		暗号カードA×1 利用時：2,000tps 暗号カードA×2 利用時：4,000tps 暗号カードA2H×1 利用時：8,000tps 暗号カードB2×1 利用時：20,000tps	–
	最大性能 (ECDSA secp256r1) ※10		暗号カードA×1 利用時：1,000tps 暗号カードA×2 利用時：2,000tps 暗号カードA2H×1 利用時：6,000tps 暗号カードB2×1 利用時：15,000tps	–
HTTP／HTTPS圧縮 ※11			●	–
リンク負荷分散 ※1			○ ※12	
認証・検疫ゲートウェイ			○	
クラウドプロキシ ※13			○	
ドメインリスト管理 ※13			○	
標的型攻撃対策連携 ※6			○	
信頼性 ※1	ホットスタンバイ		●	
	LAN二重化		●	
	ゲートウェイ・フェールセーフ		●	
保守・運用管理			日本語WebUI (https)、CLI (telnet,SSHv2)、SNMP (v1／v2c／v3)、NTP、syslog、メール通知、ビジュアライザ機能 ※6	

● 標準機能
○ オプション機能 (ライセンスが必要)

IPCOM EX2シリーズ 型名／価格一覧→P13-9

※1 IPv6サポート。
※2 1518バイト長のデータをUDP 通信で測定した値。
※3 128バイト長のファイルをHTTP通信で1秒間にダウンロードする値。
セッション数／秒は、TCPコネクションの確立、ファイルのダウンロード、TCPコネクションの切断を行う一連の処理を1セッションとした1秒間の処理数。
※4 128Kバイト長のファイルをHTTP通信で測定した値。
※5 IPCOMセキュリティサポートサービスが必要。
※6 ハードディスクオプションが必要。
※7 EX2-3500／EX2-3200はソフトウェア暗号に加え、暗号カードA／A2Hまたは暗号カードB2が使用可能。EX2-1100Bはソフトウェア暗号のみ。
※8 1400バイト長のデータをUDP通信で測定した値。
※9 暗号カードA／A2Hまたは暗号カードB2が必要。また、暗号カードAは最大2枚、暗号カードA2H／B2は最大1枚搭載可能。
※10 TLS1.2で128バイト長のファイルをHTTPS通信で1秒間にダウンロードする数。
トランザクション／秒 (TPS) は、TCPコネクションの確立、SSLハンドシェイク、ファイルのダウンロード、TCPコネクションの切断と行う一連の処理を1トランザクションとした1秒間の処理数。
※11 HTTPS圧縮を行うには、SSLアクセラレータライセンスと暗号カードA／A2Hまたは暗号カードB2が必要。
※12 NW機能拡張ライセンスが必要。
※13 クラウドサービス制御ライセンスが必要。

■ IPCOM EX2 NWシリーズ ソフトウェア

ハードウェア装置名			EX2-3500／EX2-3200	EX2-1100B
ソフトウェア名			EX2-3000 NW ソフトウェア V01	EX2-1000 NW ソフトウェア V01
IPルーティング	IPv4		Static、RIPv1／v2、OSPFv2、BGPv4	
	IPv6		Static、RIPng	
PPPoEクライアント			●	
FNAルーティング			–	○
Link Aggregation			●	–
VLAN			●	
アドレス変換機能 ※1			●	
UTM				
ファイアーウォール ※1			●	
	最大	性能 ※2	15Gbps	5Gbps
		セッション処理性能 ※3	120,000 セッション／秒	78,000 セッション／秒
	サイジング用性能 ※4		7Gbps	3.5Gbps
	最大同時セッション数		2,000,000	200,000
アノマリ型IPS ※1			●	
シグネチャー型IPS ※1 ※5 ※6			○	
アンチウイルス ※5 ※6			○	○
クラウドサンドボックス ※5 ※6			○	○
Webコンテンツ・フィルタリング ※5 ※6			○	
WAF			–	
VPN				
IPsec-VPN ※1 ※7			○	
	最大性能 ※8		暗号カードA×1 利用時：2.0Gbps 暗号カードA×2 利用時：3.5Gbps 暗号カードA2H×1 利用時：5.5Gbps 暗号カードB2×1 利用時：7.0Gbps	0.6Gbps
L2TP／IPsec ※7			○	
帯域制御 ※1			●	
	最大	制御可能帯域幅 ※2	13Gbps	4.5Gbps
		セッション処理性能 ※3	100,000 セッション／秒	74,000 セッション／秒
	サイジング用性能 ※4		6.0Gbps	3.5Gbps
	最大同時セッション数		2,000,000	200,000
サーバ負荷分散			–	
SSLアクセラレーター			–	
HTTP／HTTPS圧縮			–	
リンク負荷分散 ※1			●	
認証・検疫ゲートウェイ			○	
クラウドプロキシ ※9			○	
ドメインリスト管理 ※9			○	
標的型攻撃対策連携 ※6			○	
信頼性 ※1	ホットスタンバイ		●	
	LAN二重化		●	
	ゲートウェイ・フェールセーフ		●	
保守・運用管理			日本語WebUI (https)、CLI (telnet,SSHv2)、SNMP (v1／v2c／v3)、NTP、syslog、メール通知、ビジュアライザ機能 ※6	

● 標準機能
○ オプション機能 (ライセンスが必要)

IPCOM EX2シリーズ 型名／価格一覧→P13-9

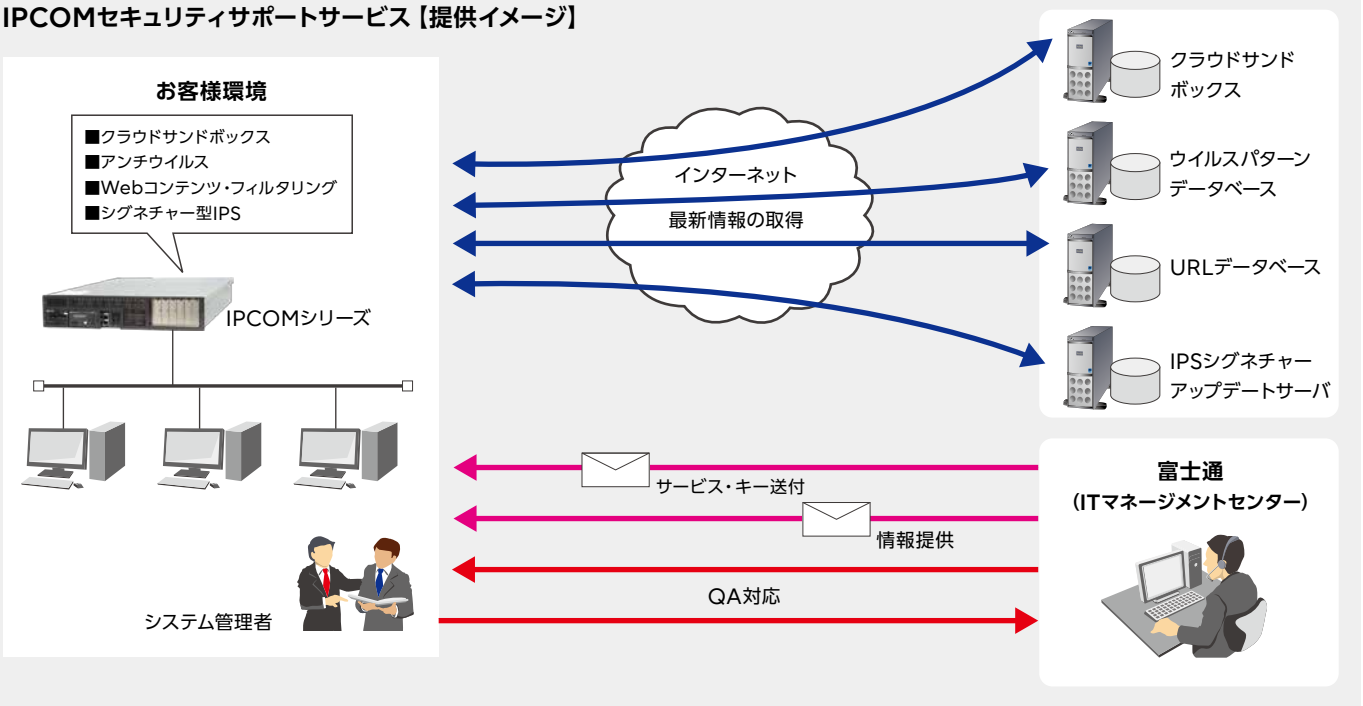
※1　IPv6サポート。
※2　1518バイト長のデータをUDP 通信で測定した値。
※3　128バイト長のファイルをHTTP通信で1秒間にダウンロードする値。
　　セッション数／秒は、TCPコネクションの確立、ファイルのダウンロード、TCPコネクションの切断を行う一連の処理を1セッションとした1秒間の処理数。
※4　128Kバイト長のファイルをHTTP通信で測定した値。
※5　IPCOMセキュリティサポートサービスが必要。
※6　ハードディスクオプションが必要。
※7　EX2-3500／EX2-3200はソフトウェア暗号に加え、暗号カードA／A2Hまたは暗号カードB2が使用可能。EX2-1100Bはソフトウェア暗号のみ。
※8　1400バイト長のデータをUDP通信で測定した値。
※9　クラウドサービス制御ライセンスが必要。

IPCOM セキュリティサポートサービス

CHECK ! https://www.fujitsu.com/jp/solutions/business-technology/security/secure/hacker-frustration/ipcom/index.html

ネットワークサーバ IPCOM のアンチウイルス機能、Web コンテンツ・フィルタリング機能、シグネチャー型 IPS 機能を実現するサービスです。常に、ウイルス定義ファイルや不正アクセスシグネチャーファイルなどの該当セキュリティ環境を、最新の状態に維持することができます。

IPCOMセキュリティサポートサービス【提供イメージ】



IPCOM EX2/VE2 アンチウイルスサポートサービス 2

IPCOM で、常に最新のウイルス定義ファイルの情報に基づいた、ウイルスの検出・駆除を行う環境を提供します。

サービス内容	**アンチウイルス機能の提供**	本サービスの利用のため、お客様に「サービス・キー」を提供します。このサービス・キーを装置に入力することにより、IPCOMでアンチウイルス機能が利用可能になります（サービス・キーの有効期間は1年間になります。翌年以降のサービス継続には、毎年サービス・キーの更新が必要になります）。
	ウイルス定義ファイルの自動アップデート／自動更新	IPCOMのウイルス定義ファイルの自動アップデート／自動更新を可能にします。
	情報提供	最新のウイルス関連情報をお客様に通知します。また、サービス・キーの有効期間満了の事前通知、更新用のサービス・キーの送付をします。
	お問い合わせ対応	本サービスに関するお問い合わせを、お客様から受付し、回答を行います。 ●受付：24時間365日 ●回答：月曜日～金曜日（祝日、富士通の指定の休業日を除く）、9：00 ～ 17：00

IPCOM EX2/VE2 アンチウイルスサポートサービス 2（クラウドサンドボックス付）

IPCOM で、常に最新のウイルス定義ファイルの情報に基づいた、ウイルスの検出・駆除を行う環境を提供します。
また、ゼロデイ攻撃対策として、クラウドサンドボックスによって、未知のウィルスを検知できる機能を提供します。

サービス内容	**アンチウイルス機能およびクラウドサンドボックス機能の提供**	本サービスの利用のため、お客様に「サービス・キー」を提供します。このサービス・キーを装置に入力することにより、IPCOMでアンチウイルス機能およびクラウドサンドボックス機能が利用可能になります（サービス・キーの有効期間は1年間になります。翌年以降のサービス継続には、毎年サービス・キーの更新が必要になります）。
	ウイルス定義ファイルの自動アップデート／自動更新	IPCOMのウイルス定義ファイルの自動アップデート／自動更新を可能にします。
	情報提供	最新のウイルス関連情報をお客様に通知します。 また、サービス・キーの有効期間満了の事前通知、更新用のサービス・キーの送付をします。
	お問い合わせ対応	本サービスに関するお問い合わせを、お客様から受付し、回答を行います。 ●受付：24時間365日 ●回答：月曜日～金曜日（祝日、富士通の指定の休業日を除く）、9：00 ～ 17：00

IPCOM EX2 Webコンテンツ・フィルタリングサポートサービス

IPCOM で、常に最新の URL フィルターリストに基づいた、お客様ネットワーク内から不正サイトへのアクセスを規制する環境を提供します。

サービス内容	**Webコンテンツ・フィルタリング機能の提供**	本サービスの利用のため、お客様に「サービス・キー」を提供します。このサービス・キーを装置に入力することにより、IPCOMでWebコンテンツ・フィルタリング機能が利用可能になります（サービス・キーの有効期間は1年間になります。翌年以降のサービス継続には、毎年サービス・キーの更新が必要になります）。
	URLフィルターリストの自動取得	IPCOMのURLフィルターの自動取得を可能にします。
	情報提供	サービス・キーの有効期間満了の事前通知、更新用のサービス・キーの送付をします。
	お問い合わせ対応	本サービスに関するお問い合わせを、お客様から受付し、回答を行います。 ●受付：24時間365日 ●回答：月曜日～金曜日（祝日、富士通の指定の休業日を除く）、9：00 ～ 17：00

IPCOM EX2/VE2 シグネチャー型IPSサポートサービス

IPCOM で、常に最新の IPS シグネチャーに基づいた、不正アクセス防御機能を提供します。

サービス内容	**不正アクセス防御（IPS）の機能提供**	本サービスの利用のため、お客様に「サービス・キー」を提供します。このサービス・キーを装置に入力することにより、IPCOMでシグネチャー型IPS機能が利用可能になります。（サービス・キーの有効期間は1年間になります。サービスの解約がない限り、1年間ごとに自動更新になります。）
	シグネチャーファイルのダウンロード／自動更新	シグネチャーアップデートサーバにネットワーク接続することにより、シグネチャーファイルのダウンロード／自動更新を行うことができます。
	情報提供	最新シグネチャー情報、シグネチャーアップデートサーバの運用情報などをお客様に連絡します。
	お問い合わせ対応	本サービスに関するお問い合わせを、お客様から受付し、回答を行います。 ●受付：24時間365日 ●回答：月曜日～金曜日（祝日、富士通の指定の休業日を除く）9：00 ～ 17：00

＊IPCOMでアンチウイルス機能、クラウドサンドボックス機能、Webコンテンツ・フィルタリング機能、シグネチャー型IPS機能をご利用の場合、本サービスの契約が必須になります。　＊本サービスは年間拘束のサービスです。

IPCOM セキュリティサポートサービス 型名／価格一覧→P13-11

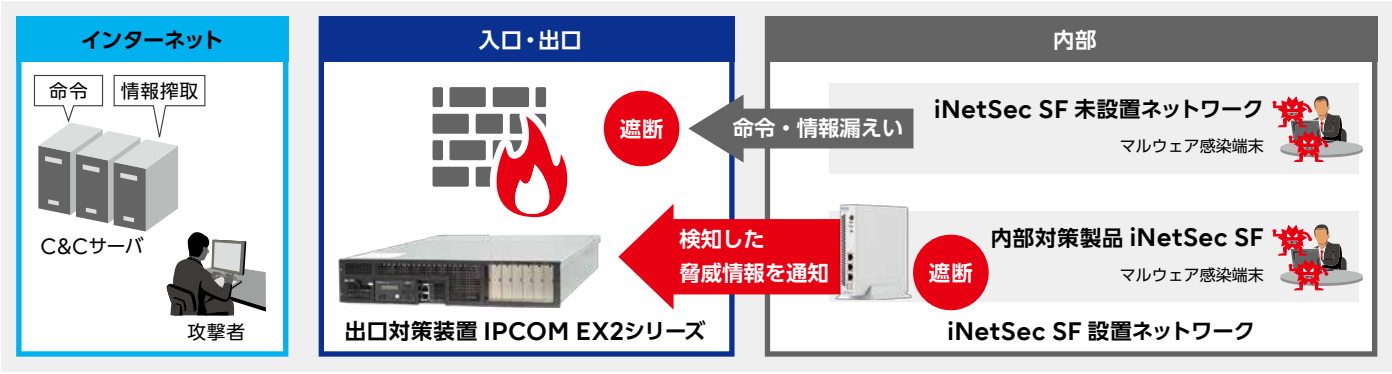
IPCOM セキュリティ連携ソリューション

標的型サイバー攻撃対策ソリューションとして、各対策装置（入口、内部、出口対策装置）を連携させる富士通独自の機能を提供します。各対策装置を直接、連携することでシンプルな構成で実現が可能で、検知から遮断まで人手の介入なしで対策でき運用負荷を低減し、自動連携することで迅速に情報漏えい対策が可能です。

内部・出口対策装置（iNetSec SF）連携

標的型サイバー攻撃対策の内部対策装置 iNetSec SF で検知した脅威情報をもとに、出口対策装置の IPCOM EX2 シリーズで該当通信を遮断し、iNetSec SF を設置していないネットワークからの情報漏えいを防ぎます。

CHECK！ https://www.fujitsu.com/jp/nwps/ipcom/material/#ipcominetsecsf



入口・出口対策装置連携

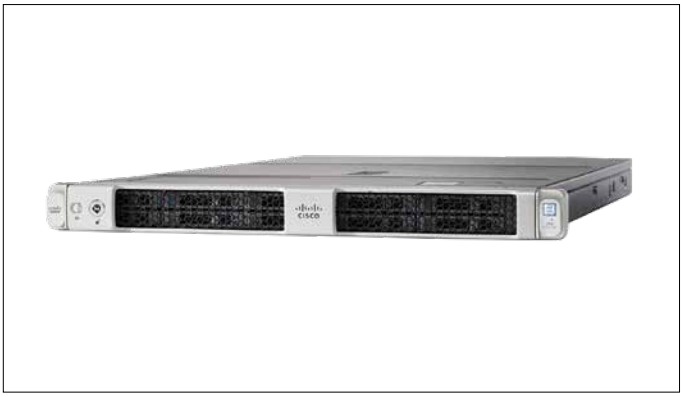
標的型サイバー攻撃対策の入口対策装置 FireEye NX シリーズで検知した脅威情報をもとに、出口対策装置の IPCOM EX2 シリーズで該当通信を遮断し、情報漏えいを防ぎます。

CHECK！ https://www.fujitsu.com/jp/nwps/ipcom/material/#ipcomfireeye

シスコシステムズ社製 セキュリティアプライアンス

Cisco Identity Services Engine

「Cisco Identity Services Engine」は、個人のアクセス認証、個人のアクセス権限割り当てだけでなく、「何時」、「何処から」、「どの情報端末で」のアクセス情報を識別し、アクセス権限を設定・管理します。ゲストアクセス環境を実現すると共に、不正なクライアントの進入を防止することができます。



■ 主な機能と特長

Identity Services Engine (ISE) は、企業のモビリティの課題を克服し、進化するネットワークを連続する攻撃から保護するITプロフェッショナルの頼れるツールとなります。さまざまな機能が用意されていますが、その一部を紹介します。

●ゲスト エクスペリエンスを簡素化
ゲストのオンボーディングと管理を容易にします。カスタマイズが簡単でブランド化されたISEのモバイルおよびデスクトップのゲストポータルを使用すると、わずか数分でアクセスを作成できます。
ISEのダイナミックビジュアルワークフローでは、ゲストアクセスのあらゆる面をすべて管理できます。

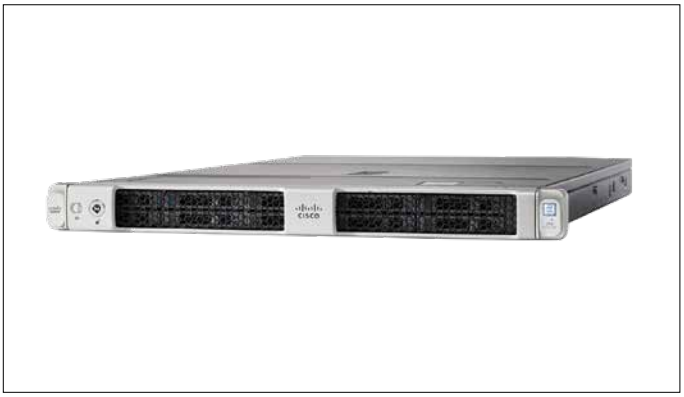
●BYODと企業モビリティを合理化
そのままで簡単に使える設定を利用して、セルフサービスのデバイスのオンボーディングと管理が可能です。Identity Services Engineには、内部の認証局、マルチフォレストActive Directoryサポート、統合型企業モビリティ管理 (EMM) パートナー ソフトウェアが含まれています。

●高度に安全なアクセスを提供
ネットワーク アクセス ポリシー管理の一元化と統合によって、一貫した高度に安全なアクセスをエンド ユーザに提供します。有線、無線、VPNのいずれでネットワークに接続しているかは関係しません。

シスコシステムズ社製 セキュリティアプライアンス

Cisco Secure Network Analytics

「Cisco Secure Network Analytics」は、ビジネス全体にわたるネットワークの可視性とセキュリティ分析をします。



■ 特長

業界トップクラスの機械学習と動作モデリングによりデジタルビジネスにおける新たな脅威を回避できます。テレメトリを使用してネットワークインフラストラクチャから情報を収集することで、ネットワーク上に誰がいて何をしようとしているのかを把握し、高度な脅威を検出して迅速に対応します。効果的なネットワーク セグメンテーションで重要なデータを保護し、1つのソリューションにこれらの機能を搭載したSecure Network Analyticsが、ビジネスの成長を後押しします。

Cisco Firepowerシリーズ

「Cisco Firepwer シリーズ」アプライアンスは、シスコの長年実績のあるファイアーウォール／ VPN 機能を提供するのに加え、次世代 IPS 機能／マルウェア防御機能も組み込むことができます。多様な脅威に対して包括的な防御が可能となります。また、Firepower Management Center（FMC）からの管理により、脅威の可視性を高め、インシデントレスポンスを速めることが可能になります。

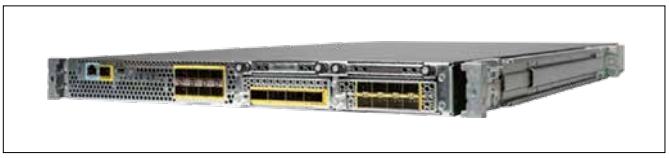
Cisco Firepower シリーズでは、下記動作モードをサポートしています。

ASA モード：長年実績のある ASA5500 シリースと同様の OS で動作し、ファイアーウォールや VPN 機能を提供

FTD モード：ASA OS と FirePower OS を統合し、ファイアーウォールや VPN に加え、侵入防御システム（Intrusion Preventions System）やマルウェア防御（Advanced Malware Protection）などのセキュリティ機能をサポート

※ FTD(Firepower Threat Defense)

Cisco Firepower 4100シリーズ



■ 強化されたセキュリティ、高速化、さらなる省スペース

完全一体型のシスコの次世代ファイアーウォール（NGFW）プラットフォームを利用することで、さらに多くの脅威を防御できます。1ラックユニット サイズである4100シリーズは、インターネットエッジや高パフォーマンス環境に最適です。この製品は、ネットワークの現状を示し、攻撃を素早く検出するため、さらに迅速に対応を行うことができます。同時に、管理における複雑性を緩和します。

■ 脅威に重点を置いた世代ファイアーウォール（NGFW）

アプリケーションのきめ細かい制御、マルウェアからの保護、脅威および脆弱性の分析と制御、検出から修復までの期間の短縮、単一の管理インターフェースによる複雑性の緩和が可能です。

■ 最適化されたパフォーマンスおよび密度

主要な機能には、1／10／40ギガビットイーサネット インターフェースのサポート、最大60Gbpsのステートフルファイアーウォール スループット、低遅延、および1RUのフォームファクタなどがあります。

Cisco Firepower 2100シリーズ

■ 卓越したビジネスの復元力および保護の実現

優れたセキュリティによってビジネスの復元力を確保し、パフォーマンスを維持します。このFirepower 2100シリーズには革新的なデュアルマルチコアCPUアーキテクチャが搭載されています。このアーキテクチャはファイアーウォール、暗号化、および脅威の検出機能を同時に最適化します。

■ 脅威に重点を置いた NGFW

脅威に対する卓越した防御により、ビジネスの復元力を高め、パフォーマンスを維持します。アプリケーションに対してきめ細かい制御を適用できます。マルウェアからの保護、検出から修復までの期間の短縮、デバイス上の管理インターフェースによる複雑性の緩和が可能です。

■ パフォーマンスとポート密度の最適化

ファイアーウォールのスループットは2Gbps～8.5Gbpsです。ローエンドモデルでは16個の1GEポートがサポートされます。ハイエンドモデルでは最大24個の1GEポートまたは最大16個の10GEポートがサポートされます。すべてが1RUフォームファクタに収まっています。

Cisco Firepower 1000シリーズ

■ 高度な脅威からの保護

Application Visibility and Control（AVC）、次世代侵入防御システム、AMP（高度なマルウェア制御）、URL フィルタリングが連携し、エンタープライズレベルの保護を実現しています。

■ 優れた暗号化トラフィック検査機能

現在のインターネットトラフィックの70%は暗号化されています。隠れた脅威からトラフィックを保護し、セキュリティを向上させます。

■ パフォーマンスと信頼性

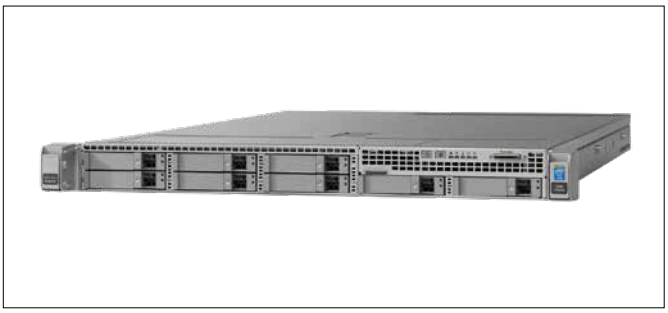
前世代の製品よりも検査スループットが最大で3倍向上しています。お客様は、スループットを一切犠牲にすることなくセキュリティサービスを利用できます。

■ 幅広いポートフォリオ

Cisco Threat Response などのツールと連携して、お客様の環境全体で脅威を検出して阻止します。

Firepower Management Center (FMC)

「Firepower Management Center（FMC）」では、Firepower シリーズを統合管理することができます。



■ Firepower Management Center（FMC）による効率的な運用・管理が可能

Firepower Management Center（FMC）により、複数台のFirepowerシリーズを統合管理することで、一括設定やネットワーク上の攻撃の可視化などができます。

FireEyeシリーズ

CHECK ! https://www.fujitsu.com/jp/products/network/security/fireeye/

FireEye社製脅威対策プラットフォーム「FireEyeシリーズ」は、実行形式ファイルやPDFファイルなど、さまざまな形式の不審なファイルをアプライアンス上の仮想環境で動作させ、そのふるまいを観察し、悪意のあるファイルかどうかを判別し、未知のマルウェアを見える化します。

■ 特長

●独自の仮想技術を使用しており、一般的なサンドボックス製品と違い、マルウェアに仮想環境であることを気づかせません。
●コールバック通信、メモリへの直接ロードなど、複雑なマルウェアの脅威化プロセスを忠実に再現し、マルウェアのふるまいを可視化。
●発症遅延や多弾頭（ペイロード）方式などのマルウェアのサンドボックス回避技術に対抗します。

FireEyeシリーズラインナップ

FireEye NXシリーズ

ファイアーウォール、IPS、アンチウイルス、Webゲートウェイでは検知できず、すり抜けてしまうWebベースの攻撃を防御するための脅威対策プラットフォームです。
ゼロデイのWeb攻撃や複数のプロトコルを使用したコールバックを検知し、機密データやシステムを確実に保護します。

FireEye EXシリーズ

アンチスパムやレピュテーションベースのセキュリティ対策では検知不可能なスピア・フィッシング・メールをブロックするための脅威対策プラットフォームです。
すべての添付ファイルを解析し、高度な標的型攻撃のスピア・フィッシング・メールを検知、隔離します。

FireEye CMシリーズ

FireEye NX、EXシリーズの管理、レポート作成、データ共有を統合する集中管理プラットフォームです。
容易に導入可能なネットワークベースのプラットフォームであり、使用することで、FireEye環境で自動生成された脅威情報をローカル環境にリアルタイムで配信し、ネットワーク全体で標的型攻撃を防御できます。
また、FireEyeの各脅威対策プラットフォームの構成、管理、レポート作成を一元化できます。

FireEye ETP

電子メールを利用した高度な攻撃からネットワークを保護するクラウド型のソリューションです。普及が進むクラウド型メールサービスに欠けている、高度なメール・セキュリティとして、EXシリーズ相当の機能を提供し、メール経由の脅威をリアルタイムで検知し、APT攻撃から防御します。

FireEye NXシリーズ連携製品

■ 入口対策－出口対策連携

入口のFireEye NXシリーズで検知した脅威情報を元に、出口のIPCOMで該当する通信を遮断し、情報漏えいを防止します。
（FireEye-IPCOM連携：詳細は、P6-8を参照ください。）

■ 入口対策－内部対策連携

入口のFireEye NXシリーズで検知した脅威情報を元に、内部のiNetSec SFで該当する通信を遮断することで、内部での感染拡大を防止します。
（FireEye-iNetSec SF連携：詳細は、P6-15を参照ください。）

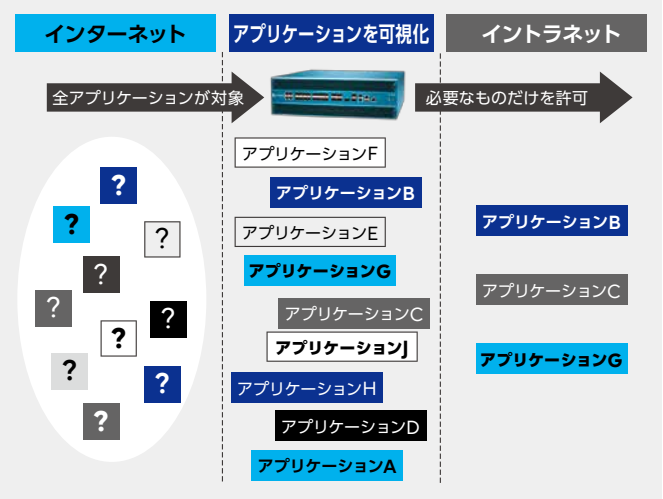
PAシリーズ、VMシリーズ、Panoramaシリーズ

CHECK ! https://www.fujitsu.com/jp/products/network/security/paloalto/

Palo Alto Networks 社製「PA シリーズ」は、アプリケーション、ユーザー、およびコンテンツの情報を元にトラフィックを分類し、アクセス制御を行う次世代ファイアーウォール製品です。トラフィックの可視化／分析／レポートの各ツールが提供する機能を活用することで、管理者は、ネットワークの状況を迅速に把握し、適切な対応をとることができます。

■すべてのアプリケーションを可視化

インターネット上には、有益なアプリケーションだけではなく、情報漏えいの要因となるアプリケーションが混在しています。
PAシリーズでは、特別な設定なしで、これらすべてのアプリケーションを可視化することが可能です。可視化したアプリケーションを取捨選択することにより、イントラネットへ必要なものを通過させ、不要なものを遮断できます。
PAシリーズは、アプリケーションの可視化のために最適化された、専用設計のハードウェア／ソフトウェアを使用しています。



■WildFireによる未知のマルウェア検知と多層防御による標的型攻撃対策

WildFireでは、未知のファイルをクラウド上のサンドボックス（仮想環境）で動作させ、振る舞いを観察します。その結果、解析したファイルが悪意のあるプログラム（マルウェア）であるかを判別します。マルウェアと判断された場合は、パターンファイルを生成し、世界中のPAシリーズに配信します。複数の攻撃手段を用いて段階的に行われる標的型攻撃に対しては、複数の防御手段を利用する多層防御が有効です。
PAシリーズでは、IPS、アンチウイルス、アンチスパイウェア、URLフィルタリングなどの多層防御を1台で実現できます。また、WildFireで検知された世界中のマルウェア解析情報は、自動的に各機能に反映されるため、最新の情報をもとにしたセキュリティ対策が可能です。

PAシリーズ

PA-5200シリーズ

●ファイアーウォール性能：18.5G～72.2Gbps
●脅威防御性能：9.2G～30Gbps

PA-3200シリーズ

●イアーウォール性能：5G～8.8Gbps
●脅威防御性能：2.2G～4.7Gbps

PA-800シリーズ

●ファイアーウォール性能：940M～1.9Gbps
●脅威防御性能：610M～780Mbps

VMシリーズ

VMシリーズ

PAシリーズ相当の機能を仮想環境上で提供します。

●製品種別：VM-50、VM-100、VM-300、VM-500、VM-700
●ファイアーウォール性能：200M～16Gbps
●脅威防御性能：100M～8Gbps

注）インスタンスのサイズやクラウドの仕様により性能が制限される場合があります。

Panoramaシリーズ

M-200

●Palo Alto Networks社製品を一元的に管理
●管理デバイス数：最大1000デバイス
●ディスク容量：16TB

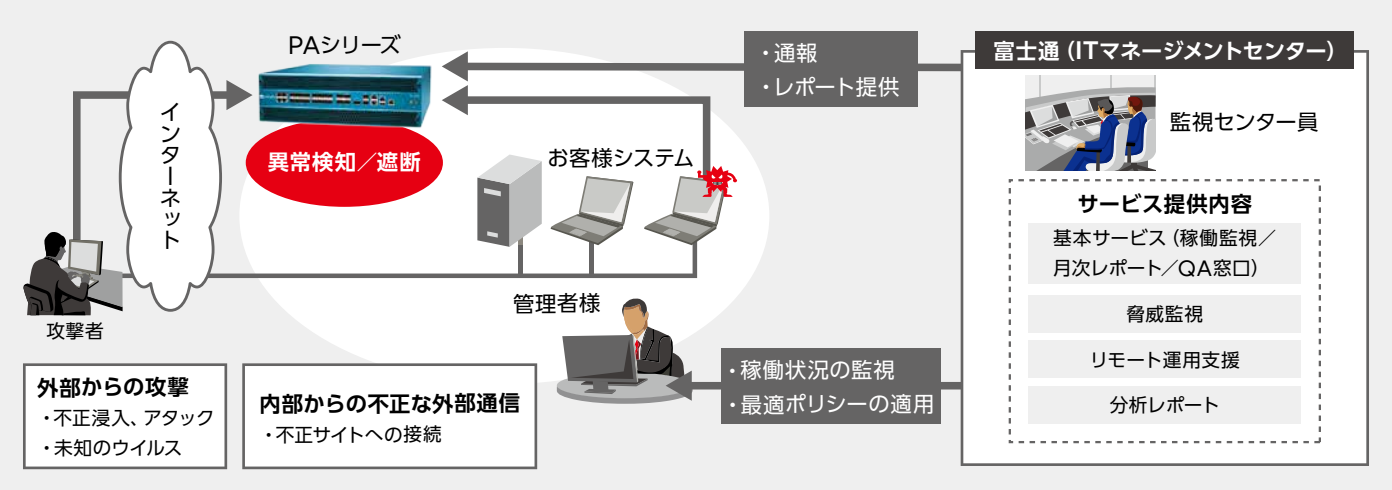
仮想版Panorama

Panoramaシリーズ相当の機能を仮想環境上で提供します。

●管理デバイス数：最大1000デバイス

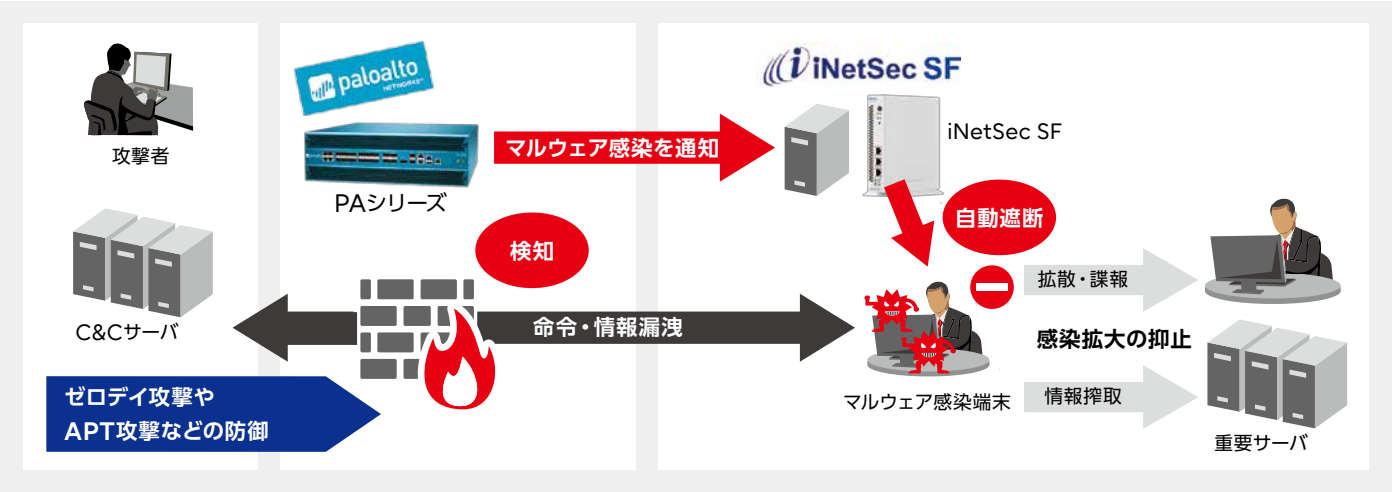
パロアルトネットワークス運用サービス

24 時間監視や分析レポート、リモートによる運用支援により次世代ファイアーウォール PA シリーズの状態を常に最適に保ち、お客様システムを保護します。



iNetSec SF 連携機能

PA シリーズで検知したマルウェア感染端末を iNetSec SF が自動遮断します。攻撃検知から感染端末の特定、遮断までを自動化します。エージェントレスで動作するため、端末の設定変更などは不要であり、簡単に導入可能です。



iNetSecシリーズ

CHECK ! https://www.fujitsu.com/jp/nwps/inetsec/

セキュリティ対策アプライアンス

iNetSec SF

「iNetSec SF」は、ネットワーク上に存在するパソコンやプリンタなど、さまざまなICT機器を自動的に検出し、管理外の不正な機器のネットワーク接続を排除するための専用アプライアンス製品です。センサーハードウェア（iNetSec SF 510センサー）とマネージャソフトウェア（iNetSec SF マネージャー）により構成されます。

iNetSec SF 510センサー

■ 持ち込みパソコンの不正接続を防止

社内に接続された持ち込みパソコンを検知し、排除を行います。排除された持ち込みパソコンからWebブラウザを使った利用申請も可能です。

■ ICT機器の「見える化」

接続されたICT機器の固有情報を自動収集します。MACアドレス／IPアドレス以外にも、ホスト名やベンダー名、機器種別（PC〈Windows／Mac／Linux〉、プリンタ、ルータ／スイッチなど）※1の自動取得が可能です。

※1 自動識別機能は、すべての機器の識別を保証するものではありません。サポートサービスに含まれる機器自動識別辞書の更新により、識別機器が拡充されます。

■ 未知のマルウェア活動をリアルタイムに検知・遮断

端末間の通信を監視し、その振る舞い（種別、方向、通信頻度など）から、自己拡散型マルウェアによる拡散行為や、標的型サイバー攻撃に共通するリモートアクセス型のマルウェア（Remote Access Trojan）を検知し、自動遮断する機能で被害の局所化が可能です。
また、今まで対策の難しかったクローズドネットワークにも適応可能です。※2 ※3

■ 禁止アプリケーションを検知・遮断

ファイル共有ソフトやSNSなど、業務で利用を禁止しているアプリケーションの利用を検知し、端末をネットワークから隔離します。ネットワークのセキュリティーポリシーの統制と情報漏えい対策の強化を実現します。※2 ※4

※2 マルウェアの検知、禁止アプリケーションの検知を行う場合、センサーは監視するスイッチのアクセスポート（またはトランクポート）と、ミラーポートに接続します。
※3 マルウェアの検知機能は、総務省委託研究「サイバー攻撃・検知に関する研究開発」の成果を使用しています。
※4 全ての禁止アプリケーションの検出を保証するものではありません。

標的型サイバー攻撃対策（入口・内部対策連携）

標的型サイバー攻撃を検知するFireEye NXシリーズからの脅威情報をもとに、内部対策装置のiNetSec SFで感染端末の通信を遮断し、マルウェアの拡散や情報漏えいを防ぎます。

Tanium Endpoint Platform

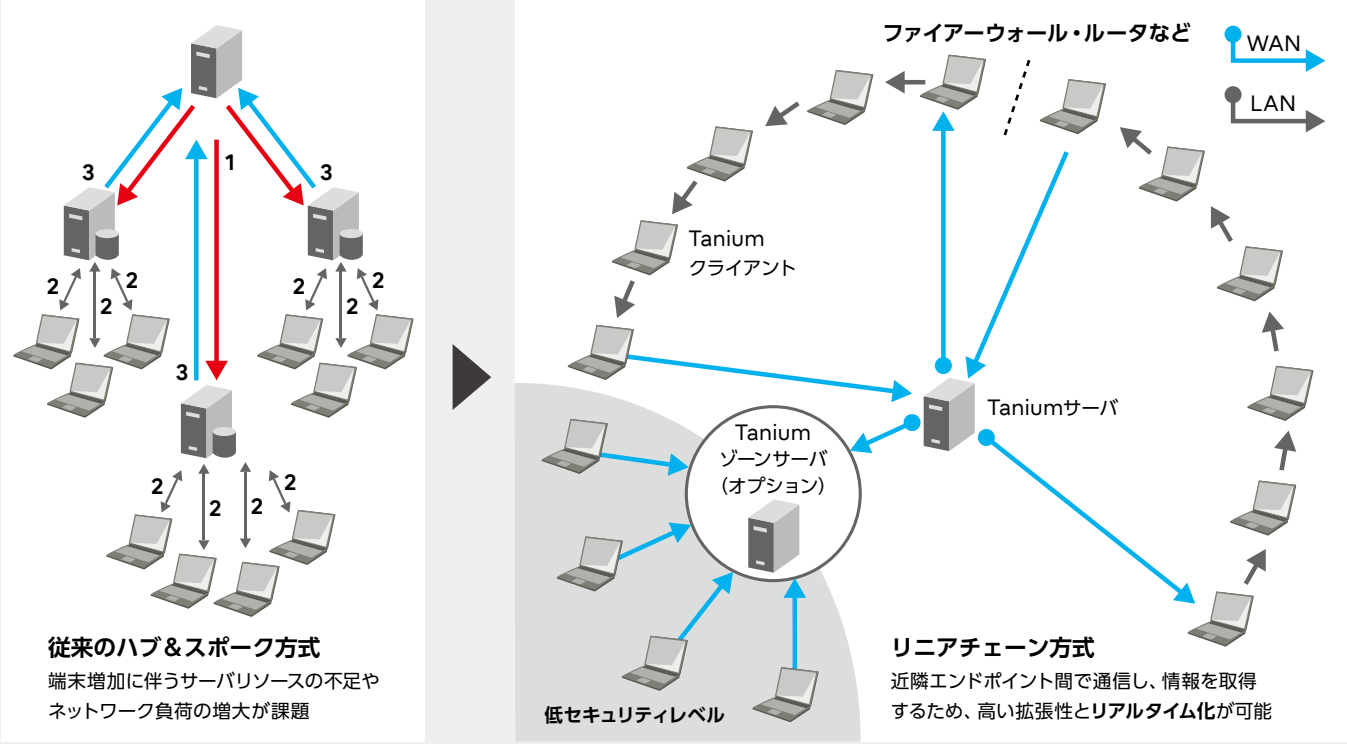
CHECK ! https://www.fujitsu.com/jp/products/network/security/tanium/

Tanium Endpoint Platform は、タニウム社の独自技術により大規模な環境においても高速に PC・サーバなどの端末の状態を一元的に可視化し、管理機能と端末を制御する対処機能を提供するプラットフォームです。モジュールを追加することで、セキュリティ脆弱性への攻撃のステップに合わせた対策が可能です。

1万台でも10万台でも数十秒以内で全数の現状を可視化

■Tanium独自のリニアチェーン方式

従来のIT資産管理システムは、情報収集に全ての端末とサーバ間の通信が発生するため、システムの拡大に伴いサーバを増設する必要やネットワーク負荷が大きくなるなどの課題があります。
タニウム社が開発し特許を取得しているリニアチェーン方式は、複数の端末が1つのグループを形成し、グループ内で情報を伝達します。サーバの要求もグループの最初と最後の端末が受信と応答を行うため、端末が増加してもサーバの増設は不要、かつ数十万台でもネットワークに大きな負荷を与えずに管理することが可能です。

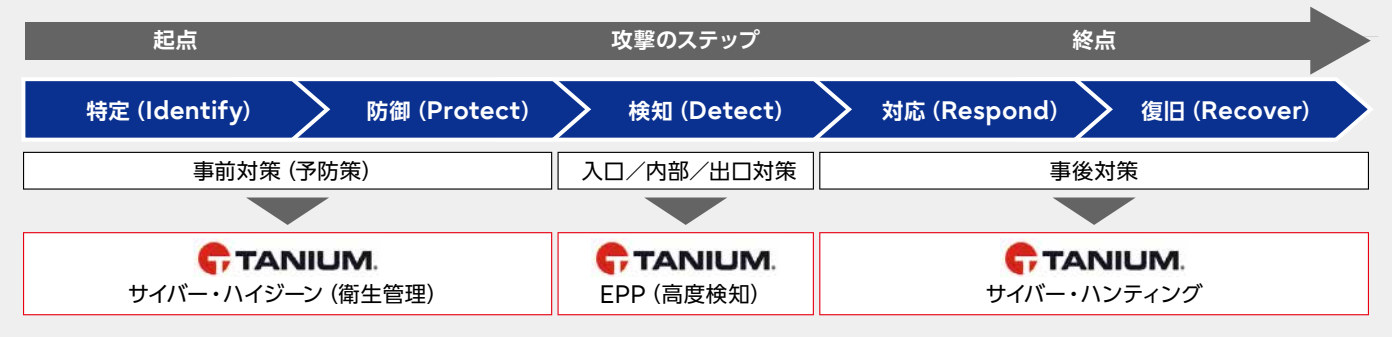


攻撃のステップに合わせたセキュリティを選択

■衛生管理（サイバー・ハイジーン）

情報セキュリティは、攻撃のステップに合わせサイバーフレームワーク*における5つの分野（「特定」「防御」「検知」「対応」「復旧」）で対策を講じることが重要です。特に「特定」「防御」にあたる事前対策（非管理端末を含めOSなどを最新状態に保つこと）、つまり「セキュリティハイジーン（衛生管理）」の重要性が再認識されています。

Tanium Endpoint Platformは、事前対策やそれぞれのステップに対しモジュールを追加することで対応することが可能です。また必要なモジュールだけを追加することが可能で、既存システムと併用することができます。



* 米国の国立標準技術研究所（NIST）が2014年2月に公開

刻々と変わる端末の状況をリアルタイムに把握

■ IT端末の情報収集

IT資産管理は、刻々と変化する状況をリアルタイムで管理・対応する必要があります。Tanium Endpoint Platformなら、非管理端末の可視化も含め、数十万台でも数十秒以内で非管理端末を含めた全ての現状をリアルタイムに可視化しセキュリティポリシーに違反する端末の隔離を可能とします。

・個人PCなど非管理端末、プリンターや計測器などの可視化
・OSや禁止されたアプリケーションのインストール状況の把握
・管理サーバへのアクセス機能だけを残し違反する端末を隔離することが可能

効果例①

数十万台の衛生管理の徹底が可能
2週間間～数か月 ➡ 数十秒

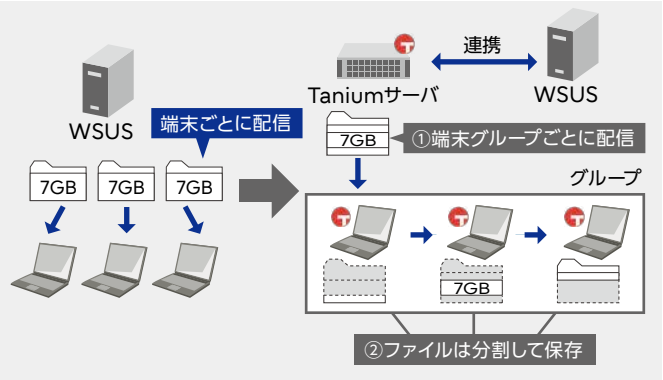
効果例②

インシデント対処に費やされる時間の短縮
数日～数か月 ➡ 瞬時

ネットワークに負荷をかけず、確実にWindows Updateを行う

■ IT運用管理

Windows10はパッチサイズが数GBにもおよび、社内ネットワークの帯域を圧迫します。またWSUSやSCCMを利用していても、管理できない端末が非常に多く未適用はセキュリティの脆弱性となります。



Tanium Endpoint Platformなら、リニアチェーン方式によりネットワークに大きな負荷をかけず数GBのパッチを配信が行え、非管理端末の可視化によりパッチの適用漏れを無くすことが可能です。またWSUSと併せて利用し、パッチ管理と配信を分けた最適化も可能です。

効果例①

パッチの配信はグループ単位
➡ ネットワーク負荷を軽減

効果例②

大容量のファイルもグループで分散保持し、必要なときに再構築する。
➡ 端末のストレージ消費を軽減

働き方改革への利用

■ 在宅勤務管理

在宅勤務者の稼働状況を管理することも可能です。

・PCの起動時間やシャットダウン時間の管理　・特定アプリケーションの起動時間やシャットダウン時間の管理

Taniumライセンスラインナップ

Tanium Core Platform（基本機能）

Core Platform	リアルタイムの可視化と制御を実現する基盤を確立・維持・管理する基本機能
Interact	Ask-Know-Actを実施するための検索画面など、Webインターフェースモジュール
Connect	Taniumで得た情報を他製品と連携・ファイル／メールなどで出力したり、情報を入力するためのモジュール
Trends	Taniumで得た情報の可視化（グラフ化）やデータ蓄積（傾向表示）などを行うモジュール

拡張モジュール（オプション機能）

Threat Response	リアルタイムの検知、過去情報の探索、対応を一括で行えるEDR用モジュール（IR、Trace、Detect）
Comply	セキュリティ監査と脆弱性診断を実行するモジュール
Discover	非管理端末を発見し、表示するモジュール
Integrity Monitor	ファイル・フォルダ・レジストリの変更を監視・検知するモジュール
Patch	Microsoft／Linuxのパッチを確認・配信するモジュール
Asset	オフライン端末を含めた端末情報を保存するモジュール
Enforce	エンドポイントのポリシー・防御機能を管理するモジュール
Deploy	ソフトウェアのインストール、更新、削除を行うモジュール