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

富士通では、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」と、ファイアーウォール、アンチウイルス、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。豊富なラインナップでさまざまな状況に対応し、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

ネットワーク・セキュリティ 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）	ファイアーウォール、IPS、アンチウイルス、WAF※2、Webコンテンツ・フィルタリング、IPsec-VPN、SSL-VPN、L2TP／IPsecによりさまざまな脅威に対応。
高速VPN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。

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 ASA5500シリーズ

セキュリティを高める機能を統合	シスコシステムズ社の「ASA5500シリーズ」は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させることで、高信頼なセキュリティソリューションを提供。

Palo Alto Networks社製 次世代ファイアーウォール PA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、コンテンツや脅威の種類によるファイアーウォールポリシーにより、アプリケーションの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・観察し、防御策を提供するWildFireにより、未知の攻撃からもシステムを防御可能。

FireEye社製 脅威対策プラットフォーム 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。

富士通ネットワークソリューションズ社製 リモートアクセス製品 モバらくだシリーズ

モバらくだ Desktop Access	遠隔地から、簡単操作でセキュアに自席PCを操作できる環境を実現。
モバらくだ Virtual Browser	遠隔地から、簡単操作でセキュアに社内Webシステムやクラウドサービスへアクセスできる環境を実現。

PFU社製 セキュリティ製品 iNetSecシリーズ

サイバー攻撃検知 セキュリティ運用効率化	未知の脅威を検知すると共に、攻撃プロセスを時系列で見える化することで攻撃の全容を把握してセキュリティ運用の効率化を実現。
IT機器リスク対処アプライアンス・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。

※1 UTM（Unified Threat Management）：ファイアーウォール、アンチウイルス、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

FUJITSU Network IPCOM

CHECK ! http://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

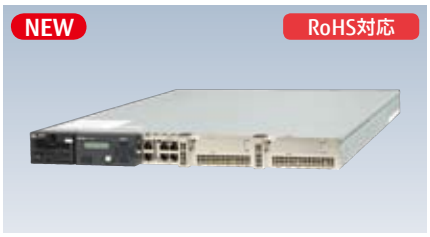
ネットワークのあらゆる脅威に対応したり、効率的なネットワークを実現するネットワークアプライアンスプラットフォーム「FUJITSU Network IPCOM EX2シリーズ」

IPCOM EX2-3500

標準価格（税別）：¥3,380,000

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）：
¥3,583,500～

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）：
¥3,660,500～



IPCOM EX2-3200

標準価格（税別）：¥1,980,000

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）：
¥2,183,500～

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）：
¥2,260,500～

IPCOM EX2-1100

標準価格（税別）：¥580,000

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）：
¥643,500～

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）：
¥720,500～

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。
http://www.ipv6ready.org/

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】

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

※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 アンチウイルス　サポートサービスの契約が必要
※3 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　※4 IPCOM EX2 シグネチャー型IPSサポートサービスの契約が必要

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】

アンチウイルス※2 | Webコンテンツ・フィルタリング※3 | IPsec-VPN | FNAルーティング
シグネチャー型IPS※4 | L2TP／IPsec | 認証・検疫ゲートウェイ | 標的型攻撃対策連携

※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 アンチウイルス　サポートサービスの契約が必要
※3 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　※4 IPCOM EX2シグネチャー型IPSサポートサービスの契約が必要

【アイコンの説明】 RoHS対応　RoHS指令（EU〈欧州連合〉が2006年7月1日に施行した有害物質規制）に適合した製品です。

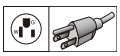
IPCOM EX2シリーズ ハードウェア

シリーズ名		IPCOM EX2シリーズ		
モデル名		EX2-3500	EX2-3200	EX2-1100
インターフェース※1	10／100／1000BASE-T	0[20]	4[12]	4[8]
	1000BASE-SX	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	○		
	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	○		
	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	○		–
	暗号カードB	○		–
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		
	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		
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		21 kg（本体+添付レール+オプションフル搭載）	15 kg（本体+添付レール+オプションフル搭載）	9 kg（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→P110

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Bは最大1枚搭載可能。なお、暗号カードA／B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

●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。 http://www.fujitsu.com/jp/documents/products/network/security-bandwidth-control-load-balancer/ipcom/material/option-ipcom-ex2.pdf

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	EX2-1100
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			○	
Webコンテンツ・フィルタリンク※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B×1 利用時：7.0Gbps	0.6Gbps
L2TP／IPsec※7			○	
SSL-VPN※9			○	–
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			○	–
	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B×1 利用時：14,000tps	–
HTTP／HTTPS圧縮※11			●	–
リンク負荷分散※1			○※12	
認証・検疫ゲートウェイ			○	
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／v2／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→P111

※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または暗号カードBが使用可能。EX2-1100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または暗号カードBが必要。また、暗号カードAは最大2枚、暗号カードBは最大1枚搭載可能。
※10　128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または暗号カードBが必要。
※12　NW機能拡張ライセンスが必要。

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	EX2-1100
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			○	
	Webコンテンツ・フィルタリンク※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B×1利用時：7.0Gbps	0.6Gbps
	L2TP／IPsec※7			○	
	SSL-VPN			–	
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				–	
	最大性能（RSA 2,048bit）			–	
HTTP／HTTPS圧縮				–	
リンク負荷分散※1				●	
認証・検疫ゲートウェイ				○	
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／v2／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→P111

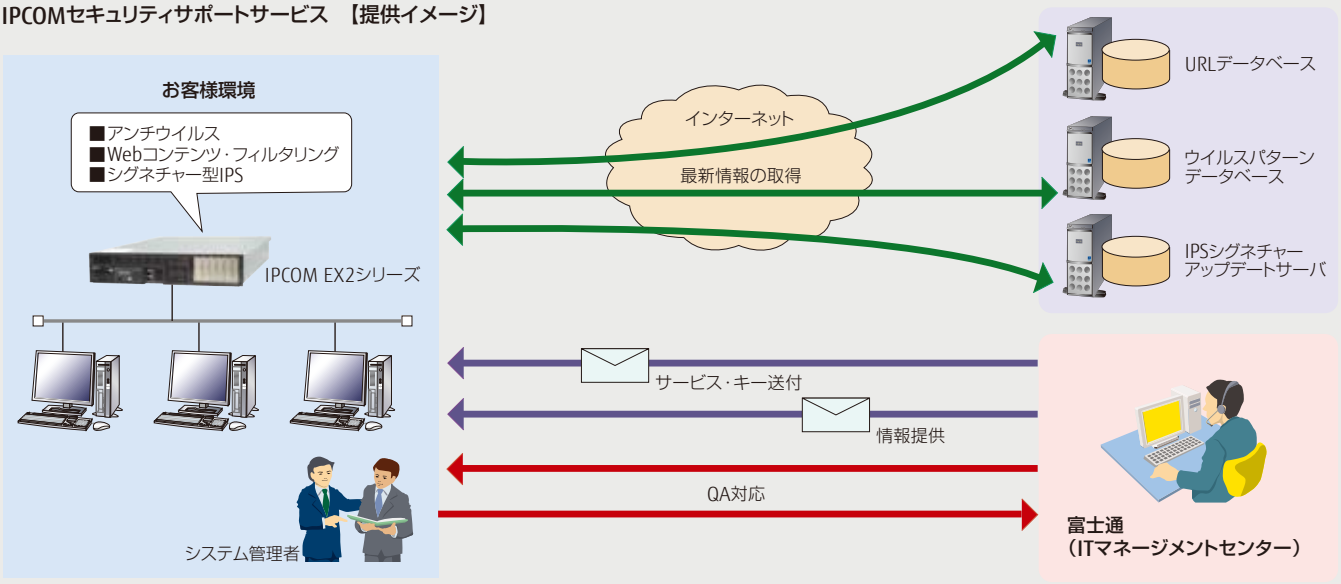
※1　IPv6サポート。
※2　1518バイト長のデータをUDP 通信で測定した値。
※3　128バイト長のファイルをHTTP通信で1秒間にダウンロードする値。
　　セッション数／秒は、TCPコネクションの確立、ファイルのダウンロード、TCPコネクションの切断を行う一連の処理を1セッションとした1秒間の処理数。
※4　128Kバイト長のファイルをHTTP通信で測定した値。
※5　IPCOMセキュリティサポートサービスが必要。
※6　ハードディスクオプションが必要。
※7　EX2-3500／EX2-3200はソフトウェア暗号に加え、暗号カードAまたは暗号カードBが使用可能。EX2-1100はソフ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

IPCOM セキュリティサポートサービス

CHECK ! http://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 アンチウイルスサポートサービス

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 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フィルターリスト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 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、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。

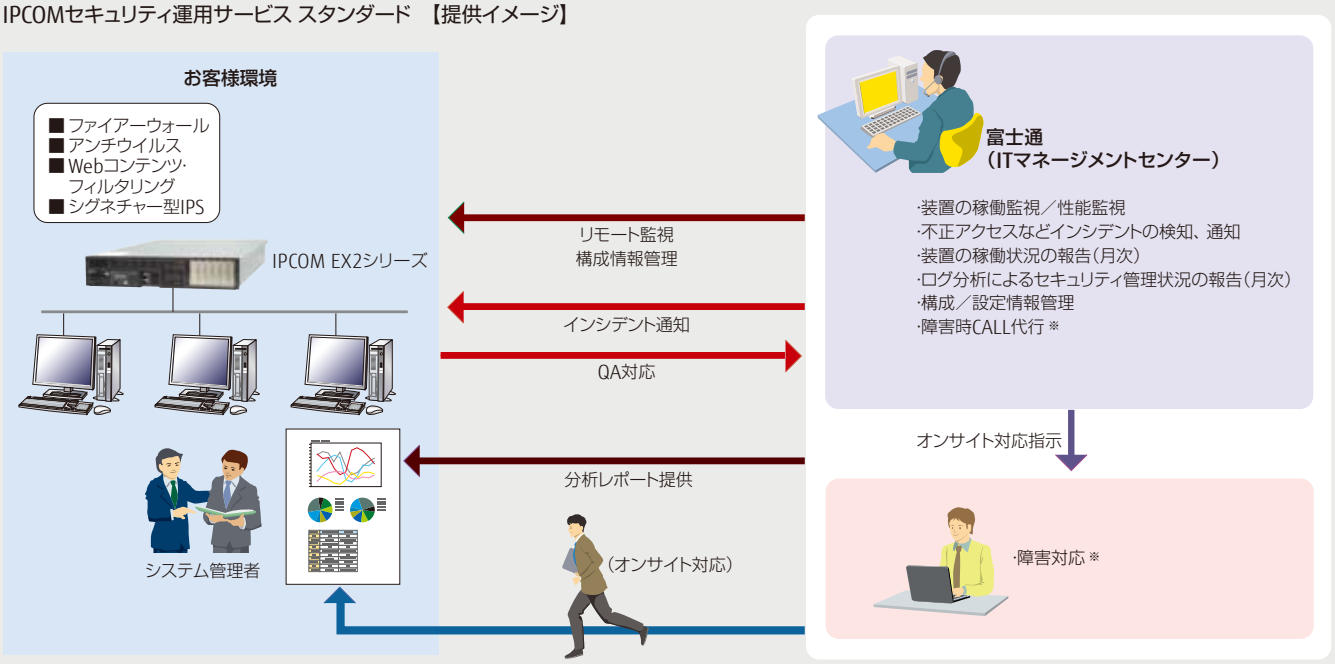
IPCOM セキュリティサポートサービス 型名／価格一覧→P112

IPCOM セキュリティ運用サービス スタンダード

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

不正アクセスやウイルスなどのインターネットのさまざまな脅威からICTシステムを守るために必要なIPCOMの運用を、お客様に代わって行います。

IPCOMセキュリティ運用サービス スタンダード　【提供イメージ】

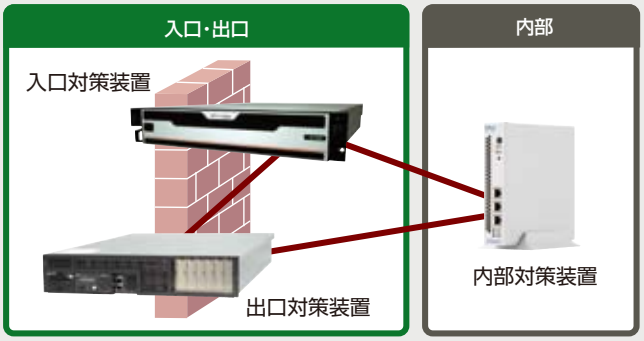


※別途、SupportDesk契約が必要です。

IPCOM セキュリティ運用サービス スタンダード 製品／価格一覧→P112

IPCOM セキュリティ連携ソリューション

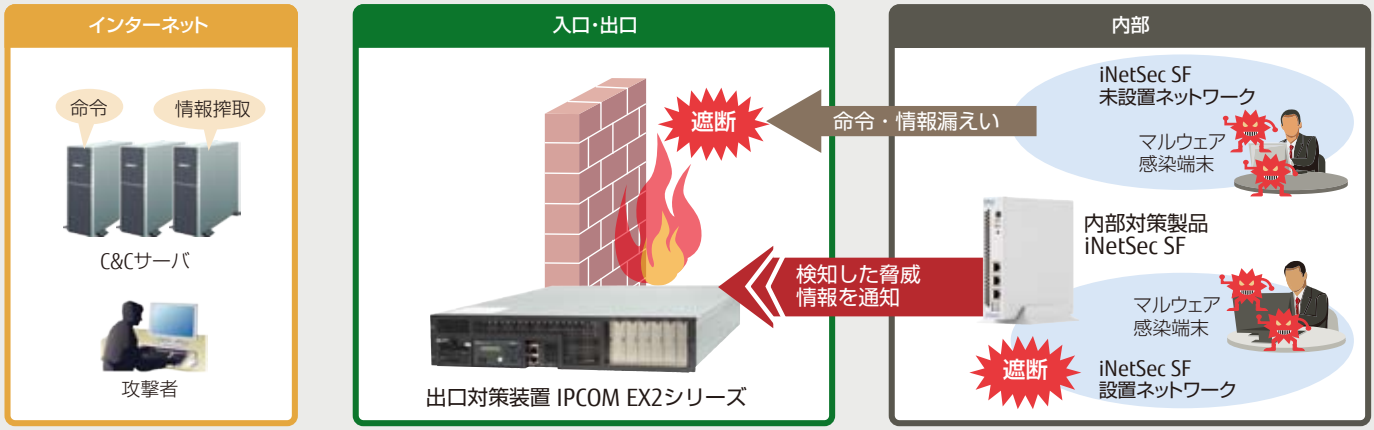
標的型サイバー攻撃対策ソリューションとして、各対策装置（入口、内部、出口対策装置）を連携させる富士通独自の機能を提供します。各対策装置を直接、連携することでシンプルな構成で実現が可能で、検知から遮断まで人手の介入なしで対策でき運用負荷を低減し、自動連携することで迅速に情報漏えい対策が可能です。



内部・出口対策装置（iNetSec）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！ http://www.fujitsu.com/jp/documents/products/network/security/inetsec/sf/



入口・出口対策装置（FireEye）連携

標的型サイバー攻撃対策の入口対策装置FireEye NXシリーズのサンドボックス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！ http://www.fujitsu.com/jp/nwps/ipcom/material/#ipcomfireeye

CHECK ! http://www.fujitsu.com/jp/nwps/mobarakuda/

FUJITSU Thin Client Solution モバらくだ Desktop Access

「モバらくだ Desktop Access（旧:モバらくだ for PC）」は、セキュアにいつでもどこでもオフィスになる環境を実現するソリューションです。遠隔地から簡単操作でセキュアに自席PCを操作でき、「どこからでも」「いつもの自席PC」で作業することが可能です。

■特長

・既存のオフィス環境にアドオンする簡単さ
・モバイルPCには、Microsoft Officeやセキュリティ対策ソフトなどのアプリケーションのインストールが必要ないため二重投資が不要
・持ち出し端末へのデータ保存抑制や一元管理が可能
・自席PCに保存されている資料もモバイルPCから編集可能
・自席PCの電源操作をモバイルPCから自在に操作可能

モバイルオフィスゲートウェイ

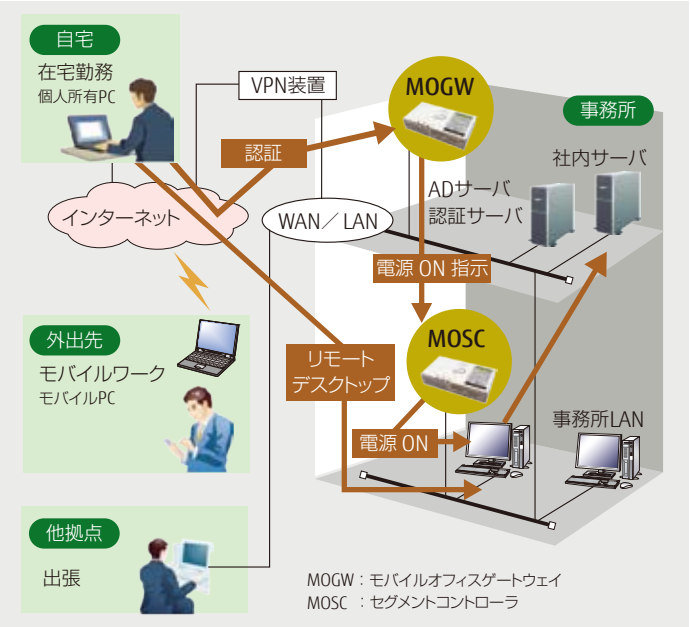
標準価格（税別）：¥298,000

セグメントコントローラ

標準価格（税別）：¥118,000

Desktop Accessコネクタ50（DAコネクタ50）

標準価格（税別）：¥50,000



FUJITSU Thin Client Solutionモバらくだ Virtual Browser

「モバらくだ Virtual Browser（旧:モバらくだ for スマートデバイス）」は、ネットワーク上に強固なセキュリティのしくみを構築することで、既存のWebベースの社内システムやクラウドサービスに手を加えることなく、スマートデバイスから「安全かつ快適」に業務ができる環境を実現します。

■画面転送技術により社内Webシステムの改修不要

画面転送技術によりPC用サイトをスマートデバイスで、そのまま閲覧可能であるため既存の社内Webシステムをスマートデバイス用に改修する必要はありません。

■高速表示技術（RVEC）※搭載

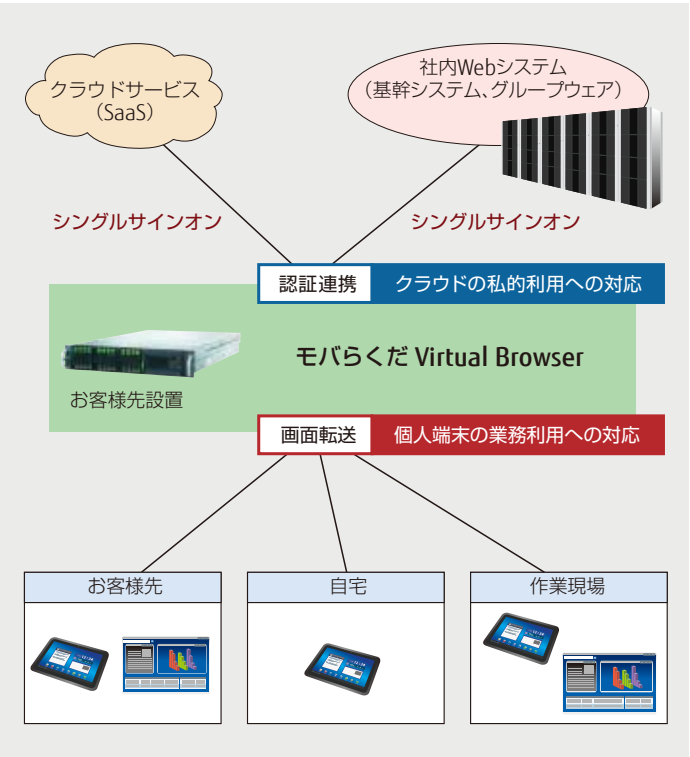
モバらくだ Virtual Browser上で動作するWebブラウザの画面を独自の高速表示技術（RVEC）によりモバイル環境利用時でも安定した操作が可能になります。これにより、データ転送容量が大きなコンテンツやFLASHなどのリッチクライアントを組み込んだ複雑な業務システムも、操作に遅延がなくレスポンスが早くなるので、ストレスがない滑らかな画面表示で操作できます。また、タブレットで快適に操作できるように独自のユーザーインターフェースを採用しています。

■SSOによるクラウドサービスにおけるセキュリティを強化

シングルサインオン（SSO）によりシステムごとのID／パスワード入力が不要であるため入力の煩わしさを解消します。またActiveDirectory／LDAPとも連携可能で、使い慣れたID／パスワードでログインが可能です。さらに、クラウドサービスとの認証連携により利用者へパスワードを通知する必要がないためクラウドサービスの私的（不正）利用や退職者による情報漏えいを抑制できます。

■運用形態に合わせた細やかなアクセス制御

接続メニューは、場所、時間帯によって利用者グループごとにWebポータルメニューとして動的に作成・表示します。



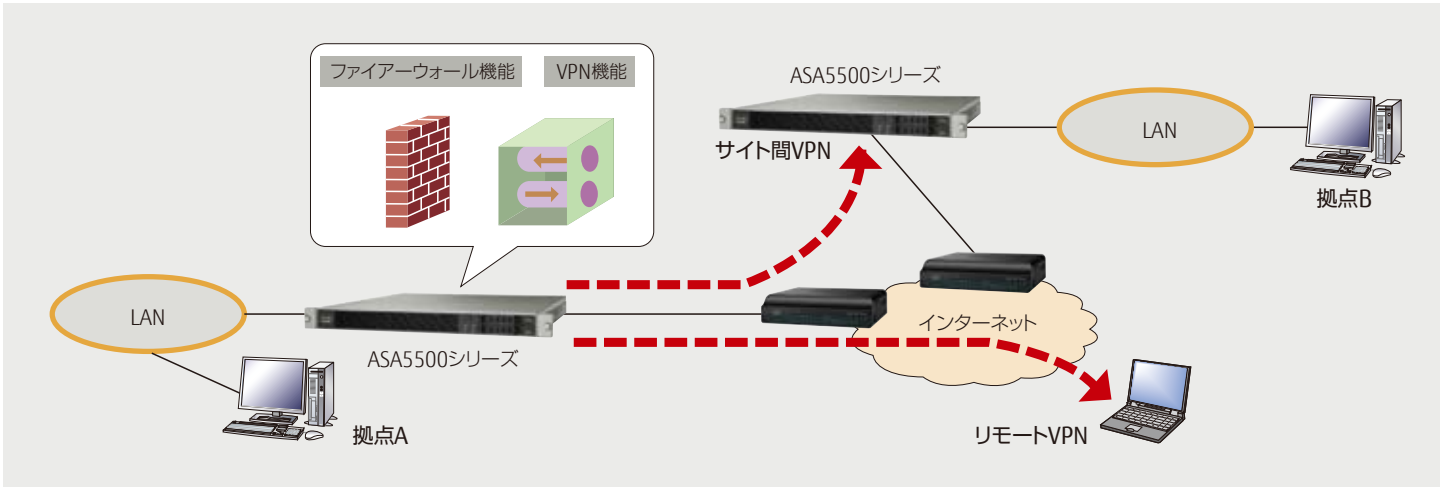
※ Remote Virtual Environment Computing
（株）富士通研究所が開発した画面転送の操作応答性能を向上させる高速表示技術

CHECK ! http://www.fujitsu.com/jp/nwps/cisco-asa5500/

シスコシステムズ社製 セキュリティアプライアンス

ASA5500シリーズ

「ASA5500シリーズ」は、ネットワークセキュリティ、およびVPNサービスを可能とする適応型セキュリティアプライアンスです。複数のテクノロジーを集約させることで、高信頼なセキュリティソリューションを提供します。
また、各種セキュリティサービスを統合することにより、運用コストの削減を実現します。



高信頼なセキュリティソリューションを提供し、大〜小規模拠点への設置に最適なセキュリティアプライアンス

ASA5585-X

●大規模向けセキュリティアプライアンス
●ファイアーウォール性能:40Gbps
●3DES／AES VPN性能:5Gbps

■ ファイアーウォール機能

プロトコル異常検出、アプリケーション／プロトコル状態の追跡などを行うことで、アプリケーションレイヤーに対する攻撃からネットワークを防御するとともに、企業環境におけるアプリケーションやプロトコルの使用方法を制御します。

■ VPN機能

IPSecとSSLベース両方のVPNサービスに対応しています。これにより、接続要件に合わせたVPNソリューションが提供可能です。また、VPNサービスの統合化により、運用コストの削減を実現します。

ASA5525-X〜5555-X

●小規模〜中規模向けセキュリティアプライアンス
●ファイアーウォール性能:1Gbps〜4Gbps
●3DES／AES VPN性能:200Mbps〜700Mbps

■ インテリジェントなネットワーク統合機能

仮想ファイアーウォール
単一のアプライアンス装置を複数の仮想ファイアーウォールに論理的に分割することで、それぞれ独自のポリシーと管理が可能です。

802.1qベースのVLAN機能
複数のスイッチが稼働しているネットワーク環境への導入を可能にします。

シスコシステムズ社製　セキュリティアプライアンス

ASA with FirePOWER／Firepower Management Center(FMC)

「ASA with FirePOWER」は、従来のASAシリーズのファイアーウォール機能に加えて、高度な侵入防御システム(Intrusion Preventions System)やマルウェア防御(Advanced Malware Protection)をサポートします。
また、「Firepower Management Center(FMC)」では、それらの機能の設定情報を統合管理することができます。

ASA5506-X～5555-X with FirePOWER

■ 高度なセキュリティ機能をサポート

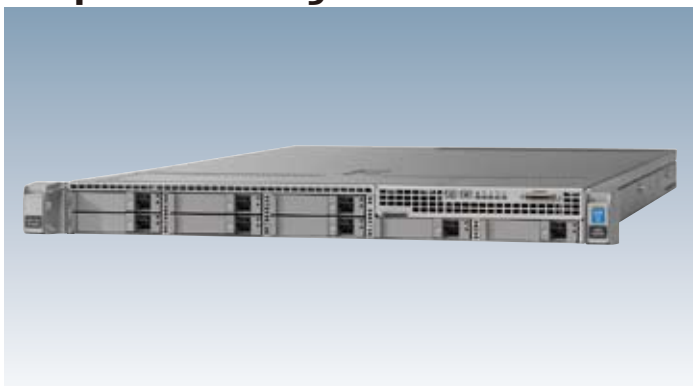
侵入防御システム (Intrusion Preventions System)
ネットワーク上の通信を記録し、侵入を検知した場合、通信の遮断を即実行します。

マルウェア防御(Advanced Malware Protection)
既にマルウェアと判明しているファイルのダウンロードを防止することができます。
また、侵入時にマルウェアと判断されないファイルをダウンロードした端末を記録しているため、後にそのファイルがマルウェアと発覚した場合には、そのファイルをダウンロードした端末に通知することが可能です。

■ 既存環境に容易に導入可能

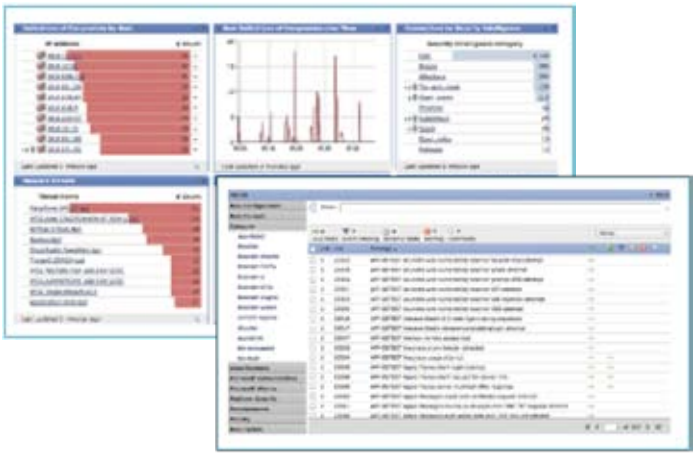
既に導入済みのASAシリーズにFirePOWERのモジュールを追加するだけで、ASA with FirePOWERの利用が可能です。

Firepower Management Center(FMC)



■ 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ASA with FirePOWER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。

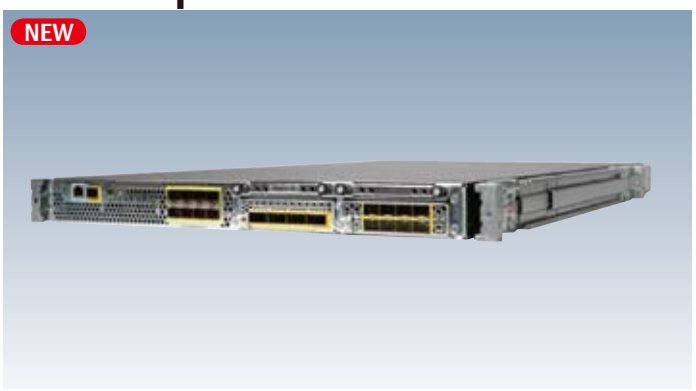


シスコシステムズ社製　セキュリティアプライアンス

Cisco Firepowerシリーズ

「Cisco Firepowerシリーズ」アプライアンスは、シスコの長年実績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、下記の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シリーズと同様のOSで動作し、ファイアーウォールやVPN機能を提供

Cisco Firepower 4100シリーズ



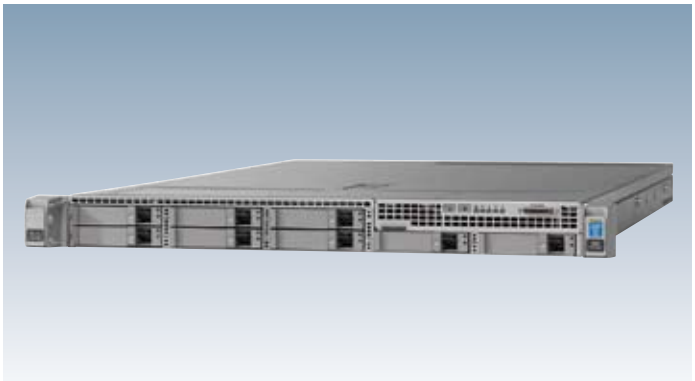
■ 脅威に重点を置いた世代ファイアーウォール（NGFW）
アプリケーションのきめ細かいアクセス制御、マルウェアからの保護、外部からの侵入脅威分析と防御、脅威検出から修復までの初動短縮が可能です。さらに、Firepower Management Center（FMC）を活用することで、単一インターフェイスによる管理性向上が可能になります。

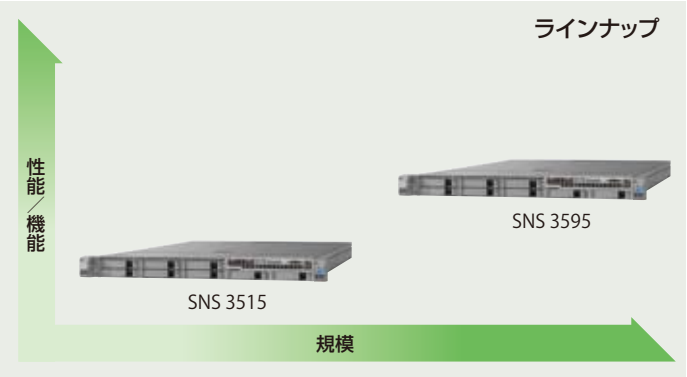
■ ハイパフォーマンスおよび高いインターフェース密度
最大60Gbps のステートフル ファイアーウォール スループットを実現可能で、1／10／40ギガビット イーサネット インターフェースをサポートします。10ギガビット イーサネットを最大24ポート、同一筐体で収容することが可能です。全てのモデルが1RUのフォーム ファクタとなっているため、省スペースを求められる環境にも適しています。

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。





■ 高度なアクセス制御機能をサポート

AAA機能

●Authentication：認証

クライアントに対し、ユーザーアカウント／パスワードを確認することで、ネットワークにアクセス権限を持つか判断します。
認証を利用することで、不正なクライアントの侵入を防止することができます。

●Authorization：認可

認証されたクライアントに対して、アクセスポリシーを付与します。それぞれのクライアントに適切なアクセスレベルを認定することで、ユーザーが利用できるネットワーク・サービスを柔軟に制御することができます。

●Accounting：アカウンティング

それぞれのクライアントのアクセス時間などをログで記録することができます。
また、Webベースのユーザーインターフェースを採用しており、利便性の高いモニタリングが可能です。

Client Profiling機能

アクセスしているクライアント端末のOSを識別することができます。

WebAuth機能

クライアントのアクセスについて、ブラウザベースの認証が可能です。

Guest Access Server機能

一時的に使用可能なゲストアカウントをクライアントに払い出すことができます。

onboarding機能

認証されたクライアントに対し、次回以降のネットワーク接続時に使用するプロファイル（SSID、認証方式など）を通知することで、クライアントの接続ポリシーの制御が可能です。

■ 多様なプロトコルをサポート

標準的な認証プロトコルであるRADIUSをサポートします。IEEE802.1Xに対応しており、多様なEAPプロトコル（EAP-TLS、EAP-PEAPMS-CHAPv2、EAP-FASTなど）もサポートします。

■ 複数台構成による信頼性向上

複数台構成により、大規模システムでの認証・制御が可能となります。
また、認証システムの信頼性が向上します。
複数台を一括で設定・管理できる機能を有しており、管理性の面で優れています。

CHECK ! http://www.fujitsu.com/jp/nwps/paloalto/

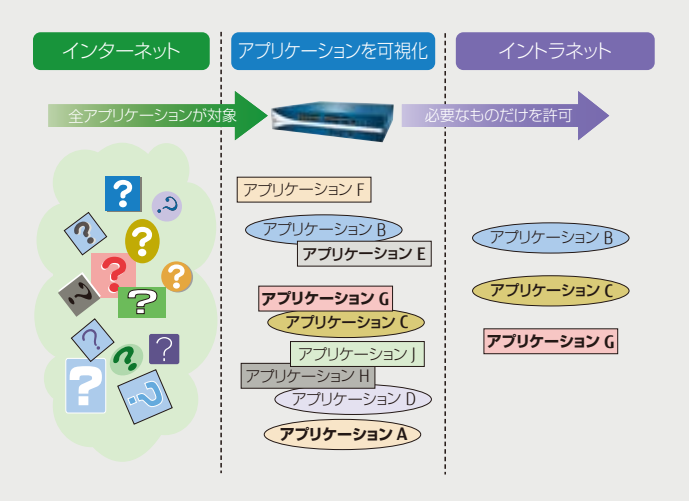
Palo Alto Networks社製 次世代ファイアーウォール

PAシリーズ

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。

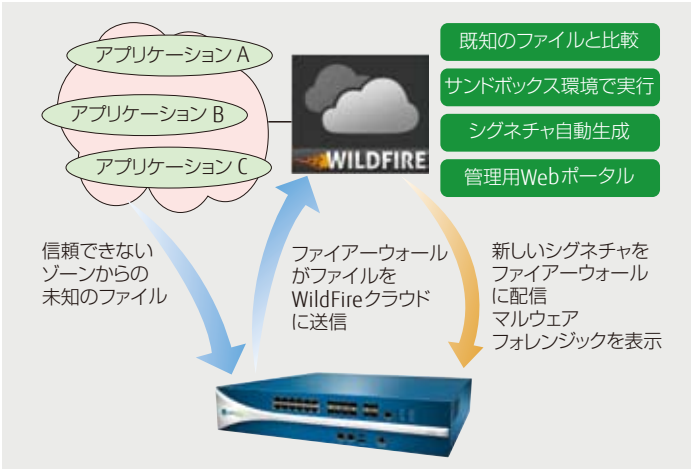
■ すべてのアプリケーションを可視化

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-7050

●ファイアーウォール性能：20G～120Gbps
●脅威防御性能：10G～60Gbps

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-5000シリーズ

●ファイアーウォール性能：5G～20Gbps
●脅威防御性能：2G～10Gbps

PAシリーズ

PA-3000シリーズ

●ファイアーウォール性能：2G～4Gbps
●脅威防御性能：1G～2Gbps

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

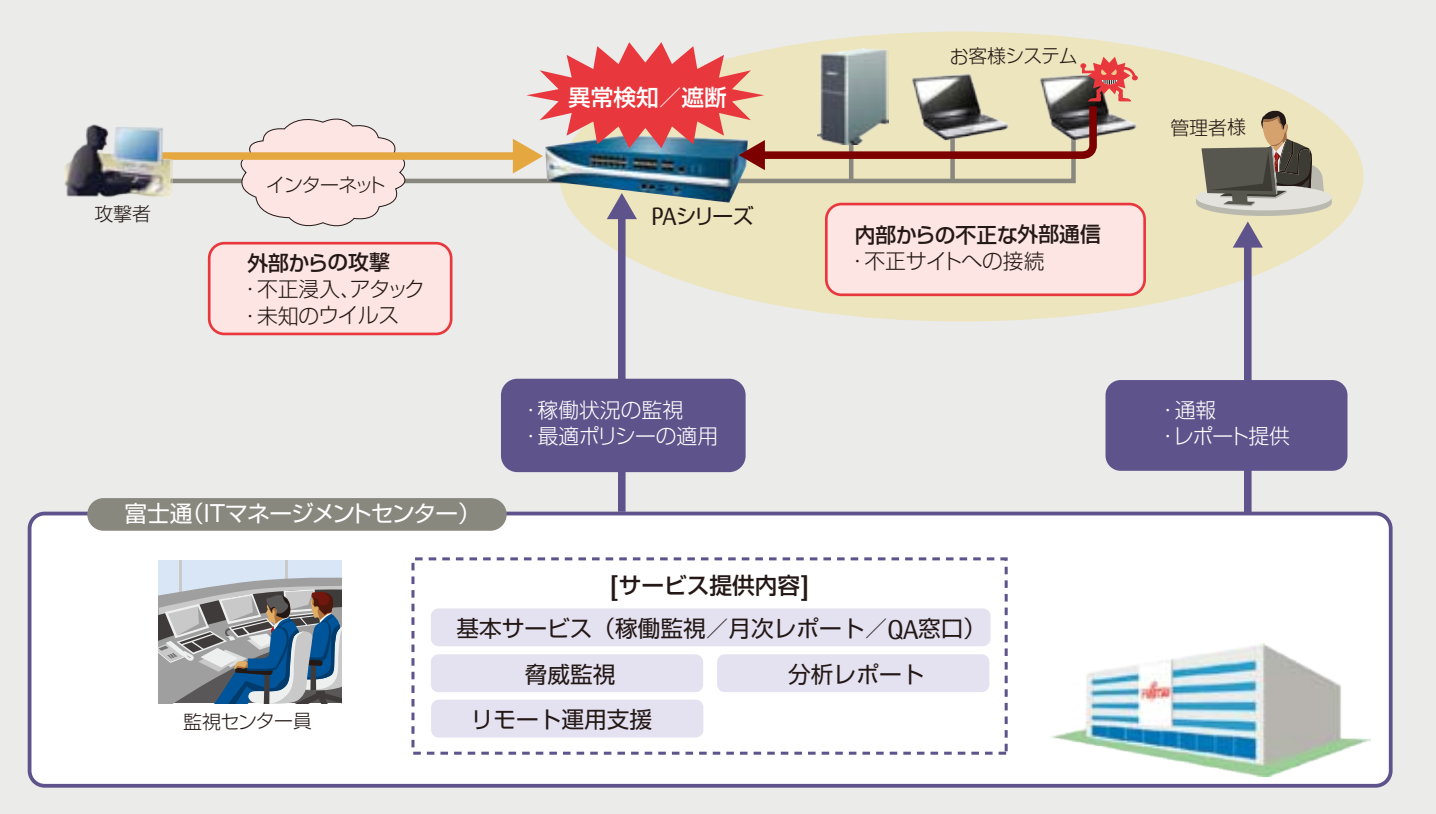
Panoramaシリーズ

M-100

●PAシリーズを一元的に管理
●管理デバイス数：最大1000デバイス
●ディスク容量：1TB～4TB

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。



マルウェア感染端末自動隔離パック(MS)

■ SDNを利用した内部対策

PAシリーズで検知した脅威情報を元に、感染端末が接続しているポートをマルウェア感染端末自動隔離パック(MS)で遮断。インターネット入口／出口での脅威検知・遮断に加え、ネットワーク内部のマルウェア感染拡大を防止します。

※マルウェア感染端末自動隔離パック（MS）には、FUJITSU Network VELCOUN-X Security Connectorが含まれています。
Security Connector はVELCOUN-Xのオプションソフトウェア製品です。VELCOUN-Xの詳細についてはP9を参照ください。
※マルウェア感染端末自動隔離パック（MS）は、PCサーバ FUJITSU Server PRIMERGYにVELCOUN-Xソフトウェアをインストール済みの形で提供します。

CHECK ! http://www.fujitsu.com/jp/nwps/fireeye/

FireEye社製 脅威対策プラットフォーム

FireEyeシリーズ

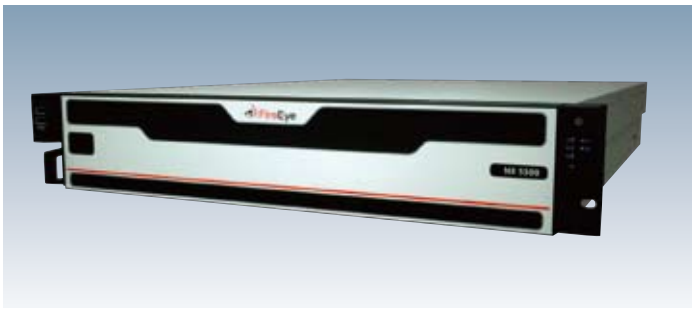
FireEye社製脅威対策プラットフォーム「FireEyeシリーズ」は、実行形式ファイルやPDFファイルなど、さまざまな形式の不審なファイルをアプライアンス上の仮想環境で動作させ、そのふるまいを観察し、悪意のあるファイルかどうかを判別し、未知のマルウェアを見える化します。

■ 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。

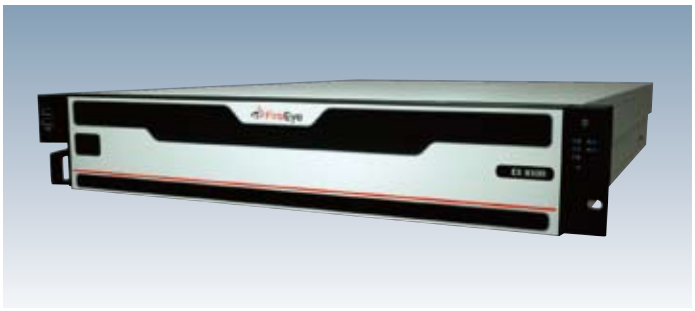
FireEyeシリーズラインナップ

FireEye NXシリーズ



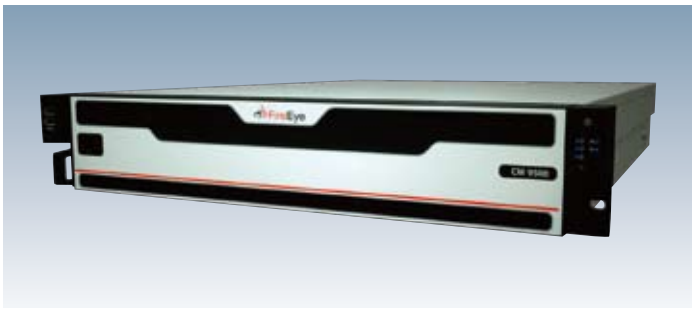
ファイアーウォール、IPS、アンチウイルス、Webゲートウェイでは検知できず、すり抜けてしまうWebベースの攻撃を防御するための脅威対策プラットフォームです。
ゼロデイのWeb攻撃や複数のプロトコルを使用したコールバックを検知し、機密データやシステムを確実に保護します。

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、P36を参照ください。）

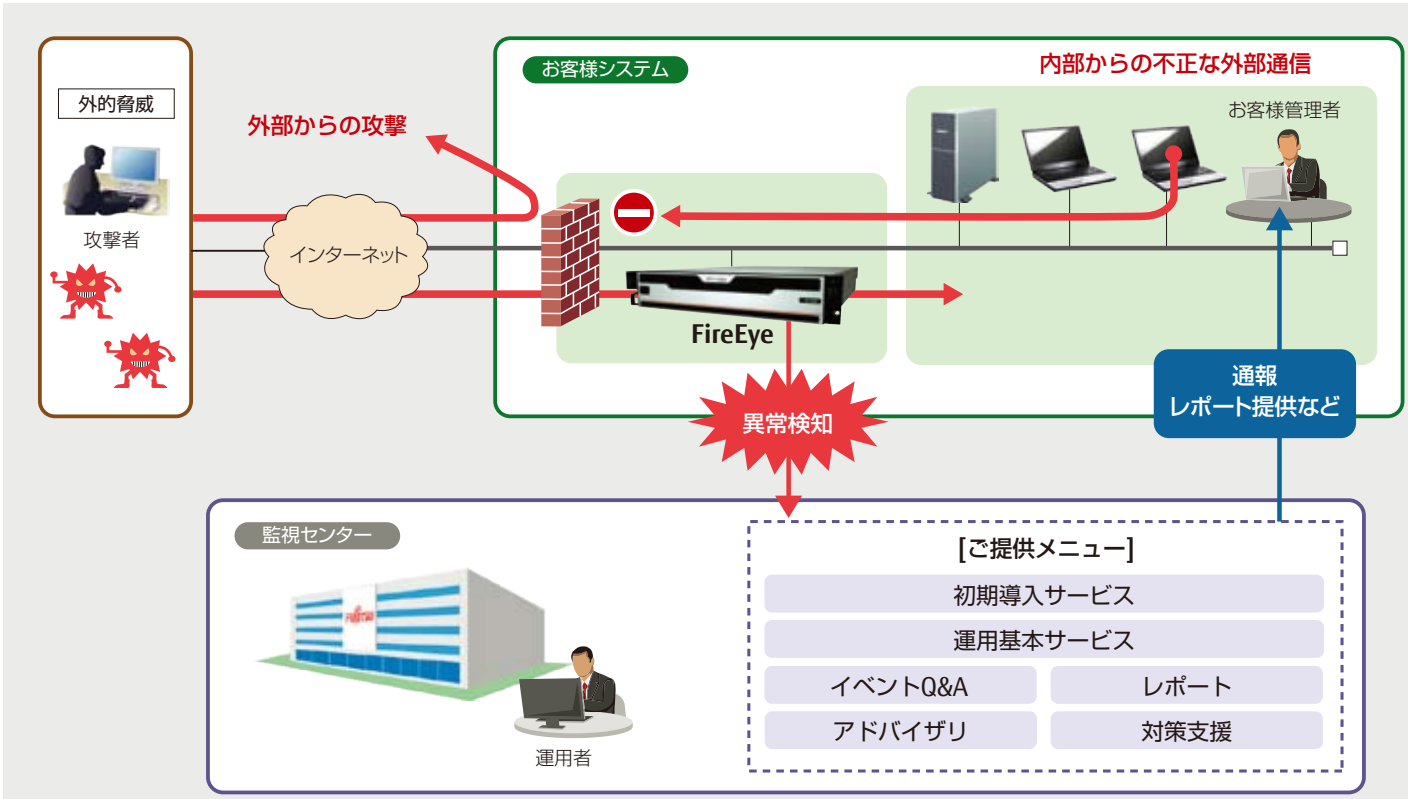
■ 入口対策－内部対策連携

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 Intra Wall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 Intra Wall連携:詳細は、P49を参照ください。）

FireEyeセキュリティ運用サービス

CHECK ! http://www.fujitsu.com/jp/nwps/fireeye/

お客様環境のFireEyeシリーズを24時間365日監視し、攻撃検知時の通知や対処支援などを提供するサービスです。



FireEye セキュリティ運用サービス（月額）：30 万円～

■ 24時間365日の常時監視

・セキュリティに精通した選任技術者が常時監視します。
・攻撃を検知した場合は、選任技術者が早急に連絡します。
・検知したアラート情報をまとめた月次レポートを提供します。社内での報告などの活用の他、攻撃の傾向に関する情報から、今後のセキュリティ対策検討にもご活用いただけます。

■ 適切な分析・対処支援を実現

・検知したアラートについて、選任技術者が分析し、レポートで報告いたします。（オプション）
・検知したアラート内容に対して、お客様がご不明な内容のQ&A対応を行います。FireEye製品のアラートに不慣れなお客様も安心してご利用いただけます。（オプション）

PFU社製　セキュリティ製品

iNetSecシリーズ

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

サイバー攻撃検知・セキュリティ運用効率化アプライアンス

iNetSec MP

iNetSec MP 2040は、未知の脅威を検知すると共に、攻撃プロセスを時系列で見える化することで攻撃の全容を把握できるネットワークセキュリティ製品です。
対処の際に必要となる情報を的確に把握することにより、検知後のセキュリティ運用の効率化を実現します。

iNetSec MP 2040

■「見つからないを見つける」検知技術

PFU社独自の標的型サイバー攻撃検知技術「Malicious Intrusion Process Scan」を搭載。内部侵入における攻撃者の行動プロセスに着目した「攻撃者行動遷移モデル」を活用し、侵入直後からの攻撃行動の流れを照合することで、高い検知精度を実現しています。

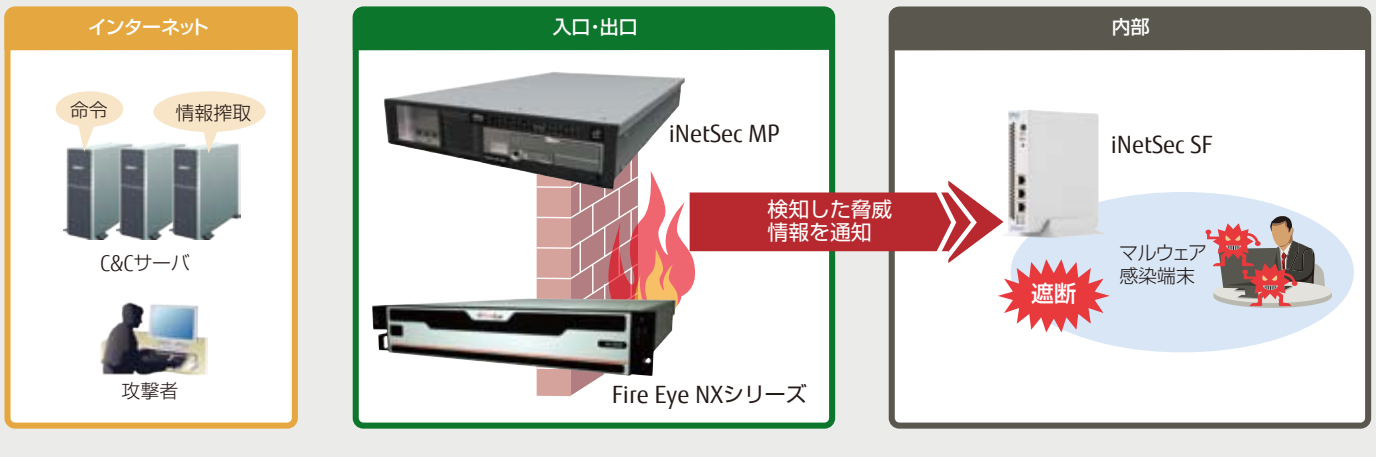
■「見つけた後が違う」攻撃プロセスの見える化

対処の優先度付けやログの収集・分析などの調査に必要な作業が自動化されており、容易に「攻撃プロセスの見える化」が可能です。これにより、対処の際に必要となる情報を的確に把握することができ、セキュリティ運用の効率化を実現します。

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iNetSec MPや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。

CHECK ! http://www.fujitsu.com/jp/products/network/security/inetsec/mp/



IT機器リスク対処アプライアンス

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、順序など）から、マルウェアによる不正な意図を持った通信を検知したり、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; RAT）を検知し、自動遮断機能で被害を未然に防止します。

■ 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。

※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。
※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。

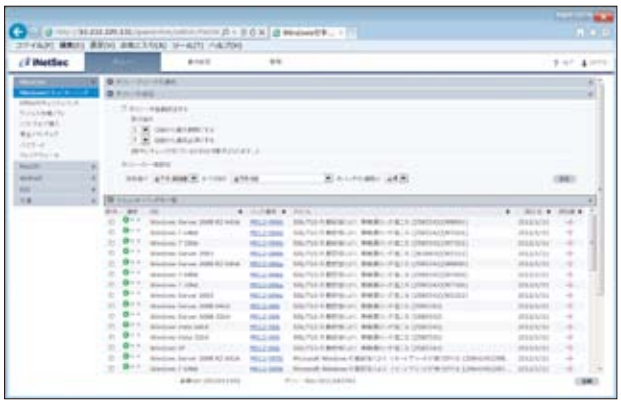
PC検疫ソフトウェア

iNetSec Inspection Center

「iNetSec Inspection Center」は、不正利用者や危険なパソコンやスマートデバイス（Android／iOS）をネットワークから排除するために必要なポリシーを定義するための検疫ポリシーサーバ※2です。iNetSecシリーズとIPCOM EX2シリーズ（ゲートウェイ型認証検疫装置）と合わせて検疫ネットワークシステムを構成できます。

■ 不正利用者をネットワークから排除

事前に登録されたMACアドレス以外のパソコンやスマートデバイスのネットワーク利用を防止します。ネットワークアクセス時にユーザー認証（ユーザーID／パスワード、証明書）を行い、不審者のネットワーク利用を防御します。導入を義務付けた任意のソフトウェアを検査し、未導入端末（iOS除く）の接続を排除します。



iNetSec Inspection Center 検疫ポリシー設定画面例

■ 危険なパソコン／スマートデバイスを隔離

ネットワーク接続時にパソコンやスマートデバイスのセキュリティ監査を自動実行します。最新のセキュリティパッチ／ウイルスパターン／アプリケーションパッチ※3 に更新されていないパソコン／スマートデバイスを隔離できます。

■ セキュアなパソコン／スマートデバイスへの容易な誘導

隔離された危険なパソコンやスマートデバイスに対して、任意の URL／コマンド（パソコンのみ）を起動するためのボタンが付いた警告メッセージを表示可能です。この警告メッセージの指示に従ってボタンをクリックし、セキュリティパッチを適用することで、パソコンをセキュアな状態にできます。

※2 サポート商品（検疫辞書パック）の契約が必須です。
本商品がないと検疫システムは構成できません。
※3 アプリケーションパッチは、Adobe Reader、Adobe Flash Player および Java が対象。

隔離パソコンに対して表示される警告メッセージ表示例