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、WANで必要な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「FUJITSU Network IPCOM EX SCシリーズ」、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機能を持つ「FUJITSU Network IPCOM EX NWシリーズ」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 EX SCシリーズ

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 EX NWシリーズ

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

未知のマルウェアと禁止アプリケーションを検知・遮断	ネットワークに侵入したマルウェアの活動や、業務で利用を禁止している禁止アプリケーションを検知・遮断が可能。
ICT機器を見える化して不正接続を防止	ネットワーク上に存在するパソコンやプリンターなど、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・セキュリティ

IPCOM EX SCシリーズ

現在のICTシステムは、DoS攻撃、不正アクセス、Webの改ざん、情報漏えい、ウイルスなどのさまざまな脅威にさらされています。
IPCOM EX SCシリーズは、UTM機能によりこれらの脅威に対応し、ICTシステムを強固に守ります。

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。

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 EX2700 SC
標準価格(税別)：¥6,798,000

IPCOM EX2500 SC
標準価格(税別)：¥3,718,000

IPCOM EX2300 SC
標準価格(税別)：¥2,178,000

IPCOM EX2-1100
IPCOM EX2-1000 SC
ソフトウェア V01
標準価格(税別)：¥643,500＊
＊本体、ソフトウェア、必須ハードウェアオプションを含む

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

IPCOM EX2シリーズ諸元

ハードウェア名		IPCOM EX2-1100
インターフェース※1	10／100／1000BASE-T	4[8]
	1000BASE-SX	0[2]
拡張スロット数		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)	○
	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	○
ストレージ		
	IPCOM EX2-1100用HDD	○
保守・運用管理	運用管理LAN	10／100／1000BASE-T×1
	RS232-C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※2	10／100／1000BASE-T×1
諸元	形態	19インチラック搭載 (1U) ※3／卓上設置
	外形寸法 (W.D.H) 突起物を除く	422mm×437mm×43.7mm
	質量	約9kg (本体+ラックレール+オプションフル搭載)
	電源ケーブル※4	◎
	AC100V用	○ (平行2極接地極付プラグ)
	AC200V用	○ (NEMA L6-15P)
	消費電力／皮相電力※5	82W／85VA
	発熱量※5	296kj／h
	騒音	6.5 B (A) 以下／47db以下

IPCOM EX2シリーズ 型名／価格一覧→P112

○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)
※1 [ ] 内はオプション使用時の最大値　※2 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　※3 ラック搭載時はラックマウントキット (別売) が必要　※4 電源ケーブルはオプションのため、AC100V／AC200V用いづれかのケーブルが必須　※5 AC100V使用時の値

●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

ソフトウェア名		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		●
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	5Gbps
	サイジング用性能※3	3.5 Gbps
	セッション処理性能※4	78,000セッション／秒
	最大同時セッション数	200,000
	アノマリ型IPS	●
	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・フィルタリング※5 ※6	○
VPN		○
	IPsec-VPN※1 ※7	○
	L2TP/Ipsec※7	○
帯域制御※1		○※8
	最大制御可能帯域幅※2	4.5Gbps
	最大同時セッション数	200,000
リンク負荷分散※1		○※8
認証・検疫ゲートウェイ※9		○
標的型攻撃対策連携※6 ※10		○
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	●

●標準機能　○オプション機能(ライセンスが必要)
※1 IPv6サポート　※2 IPv4環境で1518バイト長のデータをUDP通信で測定した値　※3 IPv4環境でインターネット通信で利用される平均的なデータの128Kバイト長のファイルをHTTP通信で測定した値　※4 IPv4環境で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　※5 IPCOMセキュリティサポートサービスが必要　※6 ストレージオプションが必要　※7 IPsec-VPNライセンスまたはL2TP／IPsec-VPNライセンス必要。EX2-1100はソフトウェア暗号のみ　※8 NW機能拡張ライセンスが必要　※9 認証・検疫GW 500クライアントライセンスが必要　※10 標的型攻撃対策連携ライセンスが必要

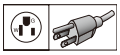
IPCOM EX SCシリーズ諸元

モデル名			IPCOM EX2700 SC	IPCOM EX2500 SC	IPCOM EX2300 SC
インターフェース※1		10/100/1000BASE-T	[20]		4[12]
		1000BASE-SX	[10]		[4]
		10GBASE※2	[10]		—
拡張スロット数			5		2
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※3			○		
UTM			○		
	ファイアーウォール※3		○		
		性能（全二重）※4	15Gbps	6.0Gbps [9Gbps]※5	3.6Gbps [5Gbps]※5
		最大同時セッション数	2,000,000	1,000,000 [2,000,000]※6	1,000,000
		アノマリ型IPS	○		
	シグネチャー型IPS※3		オプション※7※8		
	WAF		オプション※8		
	アンチウイルス		オプション※7※8		
	Webコンテンツ・フィルタリング		オプション※7※8		
VPN			オプション		
	IPsec-VPN※3	性能（AES）	暗号カードA2：1.2Gbps 暗号カードB：2.0Gbps※10 暗号カードB×2：3.0Gbps※9 暗号カードC：6.0Gbps※15※16		
	L2TP/IPsec		オプション		
	SSL-VPN		オプション		
帯域制御（L7）※3			オプション		
		制御可能帯域幅（全二重）※4	15Gbps	6.0Gbps [9Gbps]※5	3.6Gbps [5Gbps]※5
		最大同時セッション数	2,000,000	1,000,000 [2,000,000]※6	1,000,000
サーバ負荷分散（L7）※3			—		
SSLアクセラレーター※3			オプション		
		性能（2,048bit）	暗号カードA2：1,000tps 暗号カードB：2,000tps 暗号カードB×2：4,000tps※9 暗号カードC：14,000tps※13※15		
HTTP／HTTPS 圧縮			○※11		
リンク負荷分散※3			オプション		
認証・検疫ゲートウェイ			オプション		
標的型攻撃対策連携			オプション		
信頼性※3		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、CLI（telnet、SSHv2）、SNMP（v1/v2c/v3）、NTP、syslog、メール通知、RS-232C、ビジュアライザ機能※8		
ハードディスクユニット			オプション		
諸元		形態	19インチラック搭載（2U）		19インチラック搭載（1U）
		外形寸法（W.D.H）突起物を除く	439×700×86.9mm		422×578×43.7mm
		質量	24kg	22kg	14kg
		電源/電源形状※14	AC100V/平行2極接地極付プラグ（125V15A NEMA 5-15P）×1（冗長時：2） AC200V/2極接地極付引掛形プラグ（250V10A NEMA L6-15P）×1（冗長時：2）※12		
		消費電力/皮相電力※17	315W/318VA（電源非冗長時） 343W/352VA（電源冗長時）	252W/260VA（電源非冗長時） 288W/300VA（電源冗長時）	120W/130VA（電源非冗長時） 131W/140VA（電源冗長時）
		発熱量※17	1134kJ/h（電源非冗長時） 1234.8kJ/h（電源冗長時）	907kJ/h（電源非冗長時） 1036.8kJ/h（電源冗長時）	432kJ/h（電源非冗長時） 471.6kJ/h（電源冗長時）
		騒音	55dB以下		47dB以下

※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 IPv6サポート　※4 IPv4での性能値　※5 [ ]内はアップグレードオプション使用時　※6 諸元拡大オプション使用時
※7 IPCOMセキュリティサポートサービスが必要　※8 ハードディスクユニットが必要
※9 EX2500/2700は、2枚搭載可能。性能値はEX2700またはEX2500でアップグレードオプション使用時
※10 EX2500/2700への搭載時の性能。EX2300へ搭載時の性能は1.5Gbps
※11 HTTPS圧縮を行なうには、SSLアクセラレーターオプションおよび暗号カードが必要
※12 オプションの200V用電源ケーブル（SJ-PWCBL2）にて対応
※13 EX2700への搭載時の性能。EX2500（アップグレードオプション使用時）へ搭載時の性能は11,000TPS
※14 サポートUPS　ネットワーク接続：PY-UPAR122、PY-UPAR152、PY-UPAC3K2
※15 EX2500/2700のみ搭載可能　※16 EX2700への搭載時の性能。EX2500へ搭載時の性能は3Gbps　※17 100V時の値

IPCOM EX SCシリーズ 型名/価格一覧→P108

注：平行2極接地極付プラグ



●IPCOM EX SC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-sc.pdf

ネットワーク最適化

IPCOM EX NWシリーズ

アプリケーションレベルの帯域制御により、重要なトラフィックを保護し安定したレスポンスを実現します。
また、ネットワークの高信頼化により、ネットワークに異常が発生した場合でもサービスを継続できます。

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。

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 EX2700 NW
標準価格(税別)：¥6,875,000

IPCOM EX2500 NW
標準価格(税別)：¥3,795,000

IPCOM EX2300 NW
標準価格(税別)：¥2,255,000

IPCOM EX2-1100
IPCOM EX2-1000 NW
ソフトウェア V01
標準価格(税別)：¥720,500＊
＊本体、ソフトウェア、必須ハードウェアオプションを含む

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※4
シグネチャー型IPS※5　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 アンチウイルス サポートサービスの契約が必要　※3 IPCOM 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 FNA:Fujitsu Network Architecture　※5 IPCOMシグネチャー型IPSサポートサービスの契約が必要

IPCOM EX2シリーズ諸元

ハードウェア名		IPCOM EX2-1100
インターフェース※1	10／100／1000BASE-T	4[8]
	1000BASE-SX	0[2]
拡張スロット数		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)	○
	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	○
ストレージ		
	IPCOM EX2-1100用HDD	○
保守・運用管理	運用管理LAN	10／100／1000BASE-T×1
	RS232-C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※2	10／100／1000BASE-T×1
諸元	形態	19インチラック搭載 (1U)※3／卓上設置
	外形寸法 (W.D.H) 突起物を除く	422mm×437mm×43.7mm
	質量	約9kg (本体+ラックレール+オプションフル搭載)
	電源ケーブル※4	◎
	AC100V用	○ (平行2極接地極付プラグ)
	AC200V用	○ (NEMA L6-15P)
	消費電力／皮相電力※5	82W／85VA
	発熱量※5	296kj／h
	騒音	6.5B (A) 以下／47db以下

IPCOM EX2シリーズ 型名／価格一覧→P112

ソフトウェア名		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		●
VLAN		●
アドレス変換機能※1		●
UTM		●
UTM ファイアーウォール※1		●
UTM ファイアーウォール※1	最大性能※2	5Gbps
UTM ファイアーウォール※1	サイジング用性能※3	3.5 Gbps
UTM ファイアーウォール※1	セッション処理性能※4	78,000セッション／秒
UTM ファイアーウォール※1	最大同時セッション数	200,000
UTM アノマリ型IPS		●
UTM シグネチャー型IPS※1※5※6		○
UTM アンチウイルス※5※6		○
UTM Webコンテンツ・フィルタリング*※5※6		○
VPN		○
VPN	IPsec-VPN※1※7	○
VPN	L2TP/IPsec※7	○
帯域制御※1		●
帯域制御※1	最大制御可能帯域幅※2	4.5Gbps
帯域制御※1	最大同時セッション数	200,000
リンク負荷分散※1		●
認証・検疫ゲートウェイ※8		○
標的型攻撃対策連携※6※9		○
信頼性※1	ホットスタンバイ	●
信頼性※1	LAN二重化	●
信頼性※1	ゲートウェイ・フェールセーフ	●

○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)
※1 [ ] 内はオプション使用時の最大値　※2 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　※3 ラック搭載時はラックマウントキット (別売) が必要　※4 電源ケーブルはオプションのため、AC100V／AC200V用いづれかのケーブルが必須　※5 AC100V使用時の値

●標準機能　○オプション機能(ライセンスが必要)
※1 IPv6サポート　※2 IPv4環境で1518バイト長のデータをUDP通信で測定した値　※3 IPv4環境でインターネット通信で利用される平均的なデータの128Kバイト長のファイルをHTTP通信で測定した値　※4 IPv4環境で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　※5 IPCOMセキュリティサポートサービスが必要
※6 ストレージオプションが必要　※7 IPsec-VPNライセンスまたはL2TP／IPsec-VPNライセンスが必要。EX2-1100はソフトウェア暗号のみ　※8 認証・検疫GW 500クライアントライセンスが必要
※9 標的型攻撃対策連携ライセンスが必要

●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

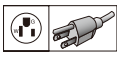
IPCOM EX NWシリーズ諸元

モデル名			IPCOM EX2700 NW	IPCOM EX2500 NW	IPCOM EX2300 NW
インターフェース※1		10/100/1000BASE-T	[20]		4[12]
		1000BASE-SX	[10]		[4]
		10GBASE※2	[10]		–
拡張スロット数			5		2
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※3			○		
UTM			○		
	ファイアーウォール※3		○		
		性能（全二重）※4	15Gbps	6.0Gbps [9.0Gbps]※5	3.6Gbps [5Gbps]※5
		最大同時セッション数	2,000,000	1,000,000 [2,000,000]※6	1,000,000
		アノマリ型IPS	○		
	シグネチャー型IPS※3		オプション※7※8		
	WAF		–		
	アンチウイルス		オプション※7※8		
	Webコンテンツ・フィルタリング		オプション※7※8		
VPN			オプション		
	IPsec-VPN※3	性能（AES）	暗号カードA2：1.2Gbps 暗号カードB：2.0Gbps※10 暗号カードB×2：3.0Gbps※9 暗号カードC：6.0Gbps※13※14		
	L2TP/IPsec		オプション		
	SSL-VPN		–		
帯域制御（L7）※3			○		
		制御可能帯域幅（全二重）※4	15Gbps	6.0Gbps [9.0Gbps]※5	3.6Gbps [5.0Gbps]※5
		最大同時セッション数	2,000,000	1,000,000 [2,000,000]※6	1,000,000
サーバ負荷分散（L7）※3			–		
SSLアクセラレーター※3			–		
		性能（2,048bit）	–		
HTTP／HTTPS圧縮			–		
リンク負荷分散※3			○		
認証・検疫ゲートウェイ			オプション		
標的型攻撃対策連携			オプション		
信頼性※3		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、CLI（telnet、SSHv2）、SNMP（v1／v2c／v3）、NTP、syslog、メール通知、RS-232C、ビジュアライザ機能※8		
ハードディスクユニット			オプション		
諸元	形態		19インチラック搭載（2U）		19インチラック搭載（1U）
	外形寸法（W.D.H）突起物を除く		439×700×86.9mm		422×578×43.7mm
	質量		24kg	22kg	14kg
	電源／電源形状※12		AC100V／平行2極接地極付プラグ（125V15A NEMA 5-15P）×1（冗長時：2） AC200V／2極接地極付引掛形プラグ（250V10A NEMA L6-15P）×1（冗長時：2）※11		
	消費電力／皮相電力※15		315W／318VA（電源非冗長時） 343W／352VA（電源冗長時）	252W／260VA（電源非冗長時） 288W／300VA（電源冗長時）	120W／130VA（電源非冗長時） 131W／140VA（電源冗長時）
	発熱量※15		1134kJ／h（電源非冗長時） 1234.8kJ／h（電源冗長時）	907kJ／h（電源非冗長時） 1036.8kJ／h（電源冗長時）	432kJ／h（電源非冗長時） 471.6kJ／h（電源冗長時）
	騒音		55dB以下		47dB以下

※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 IPv6サポート　※4 IPv4での性能値
※5 [ ]内はアップグレードオプション使用時　※6 諸元拡大オプション使用時　※7 IPCOMセキュリティサポートサービスが必要
※8 ハードディスクユニットが必要　※9 EX2500／2700は、2枚搭載可能。性能値はEX2700またはEX2500でアップグレードオプション使用時
※10 EX2500／2700への搭載時の性能。EX2300へ搭載時の性能は1.5Gbps
※11 オプションの200V用電源ケーブル（SJ-PWCBL2）にて対応
※12 サポートUPS　ネットワーク接続：PY-UPAR122、PY-UPAR152、PY-UPAC3K2
※13 EX2500／2700のみ搭載可能　※14 EX2700への搭載時の性能。EX2500へ搭載時の性能は3Gbps　※15 100V時の値

IPCOM EX NWシリーズ 型名／価格一覧→P109

注：平行2極接地極付プラグ



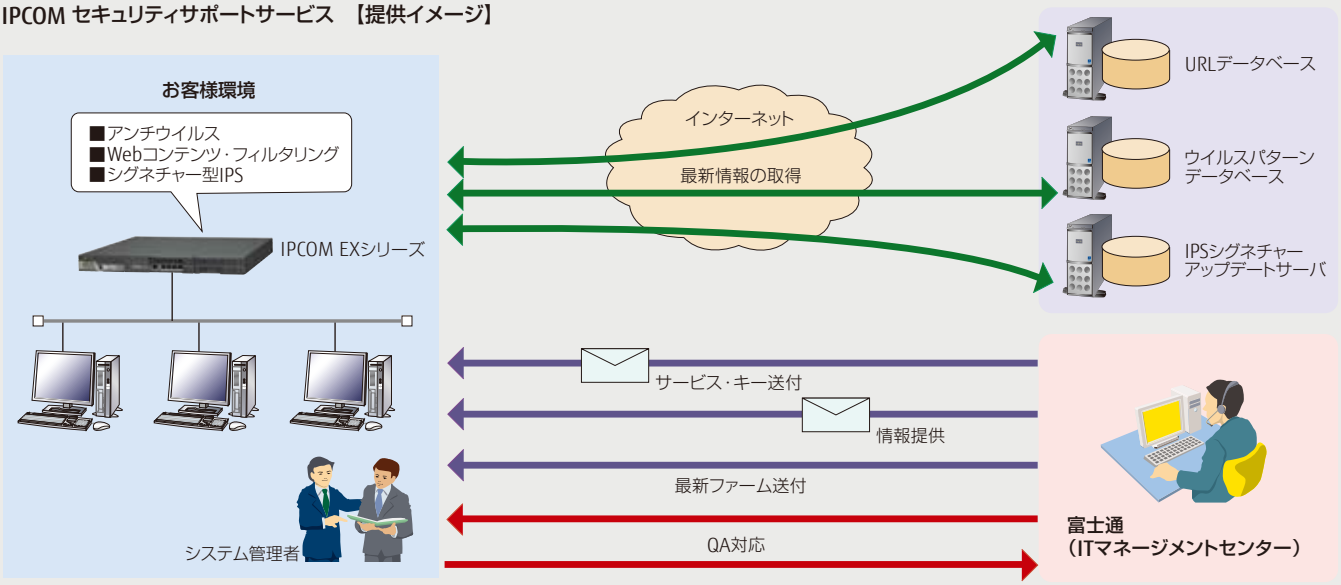
●IPCOM EX NWシリーズのハードウェアオプションについてはこちらをご参照ください。
http://www.fujitsu.com/jp/documents/products/network/security-bandwidth-control-load-balancer/ipcom/material/option-ipcom-nw.pdf

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。
最新版アップデートファームウェアの提供	本サービスの利用に必要なIPCOMの最新アップデートファームウェアを提供します。
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。
最新版アップデートファームウェアの提供	本サービスの利用に必要なIPCOMの最新アップデートファームウェアを提供します。
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。
最新版アップデートファームウェアの提供	本サービスの利用に必要なIPCOMの最新アップデートファームウェアを提供します。
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。

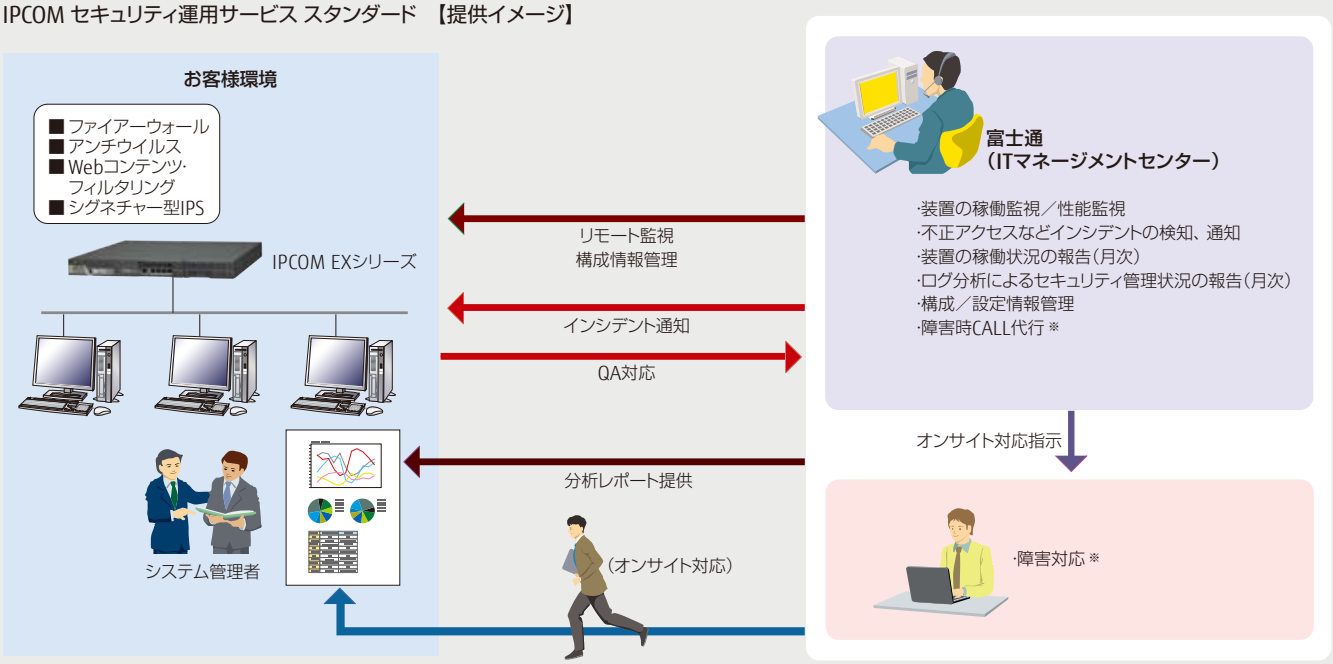
IPCOMセキュリティサポートサービス 型名／価格一覧→P113

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】

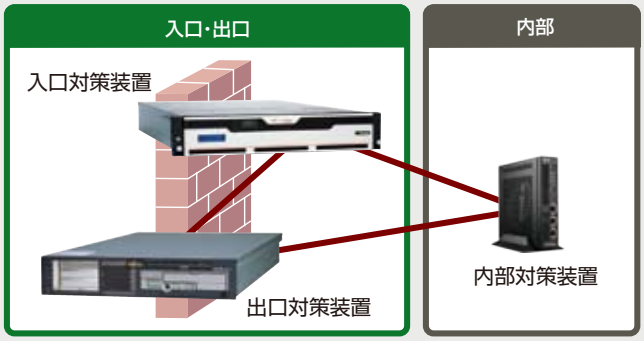


※別途、SupportDesk契約が必要です。

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→P114

IPCOMセキュリティ連携ソリューション

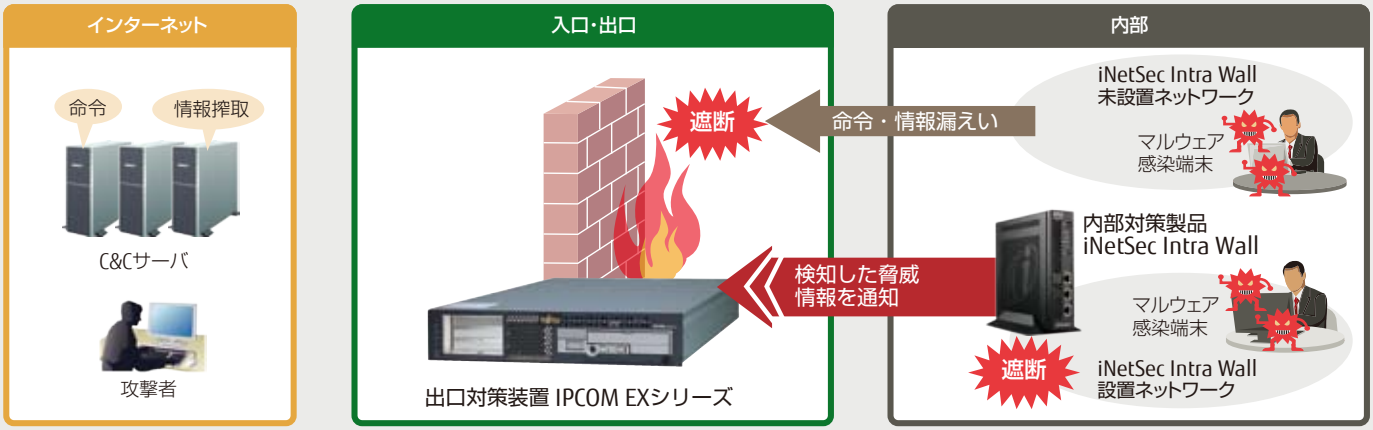
標的型サイバー攻撃対策ソリューションとして、各対策装置（入口、内部、出口対策装置）を連携させる富士通独自の機能を提供します。各対策装置を直接、連携することでシンプルな構成で実現が可能で、検知から遮断まで人手の介入なしで対策でき運用負荷を低減し、自動連携することで迅速に情報漏えい対策が可能です。



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 Intra Wallで検知した脅威情報をもとに、出口対策装置のIPCOM EXシリーズで該当通信を遮断し、iNetSec Intra Wall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/nwps/ipcom/material/#ipcominetseciw



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 EX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/

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

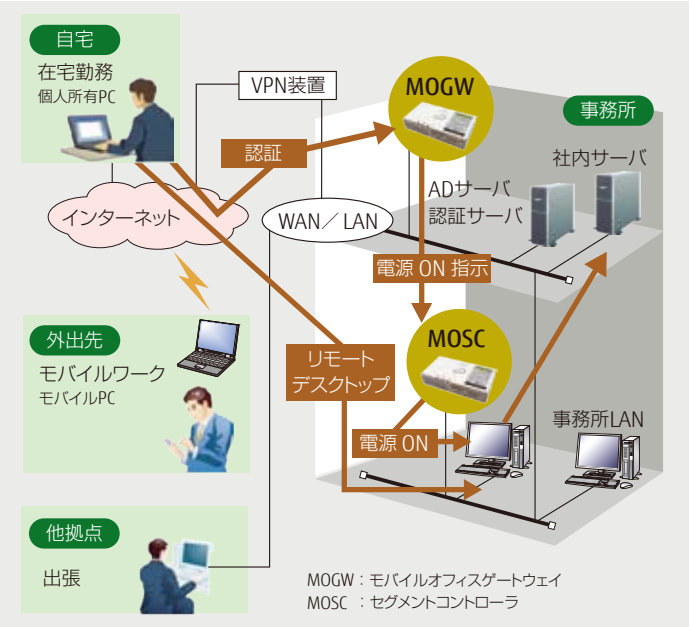
標準価格（税別）：¥298,000

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

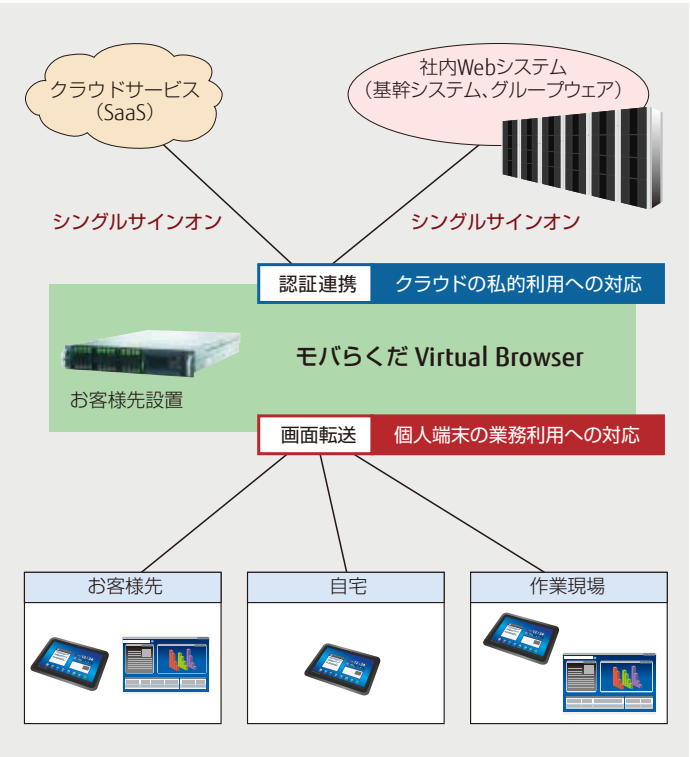
モバらくだ Virtual Browser上で動作するWebブラウザの画面を独自の高速表示技術（RVEC）によりモバイル環境利用時でも安定した操作が可能になります。これにより、データ転送容量が大きなコンテンツやFLASHなどのリッチクライアントを組み込んだ複雑な業務システムも、操作に遅延がなくレスポンスが早くなるので、ストレスがない滑らかな画面表示で操作できます。また、タブレットで快適に操作できるように独自のユーザーインターフェースを採用しています。

■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。



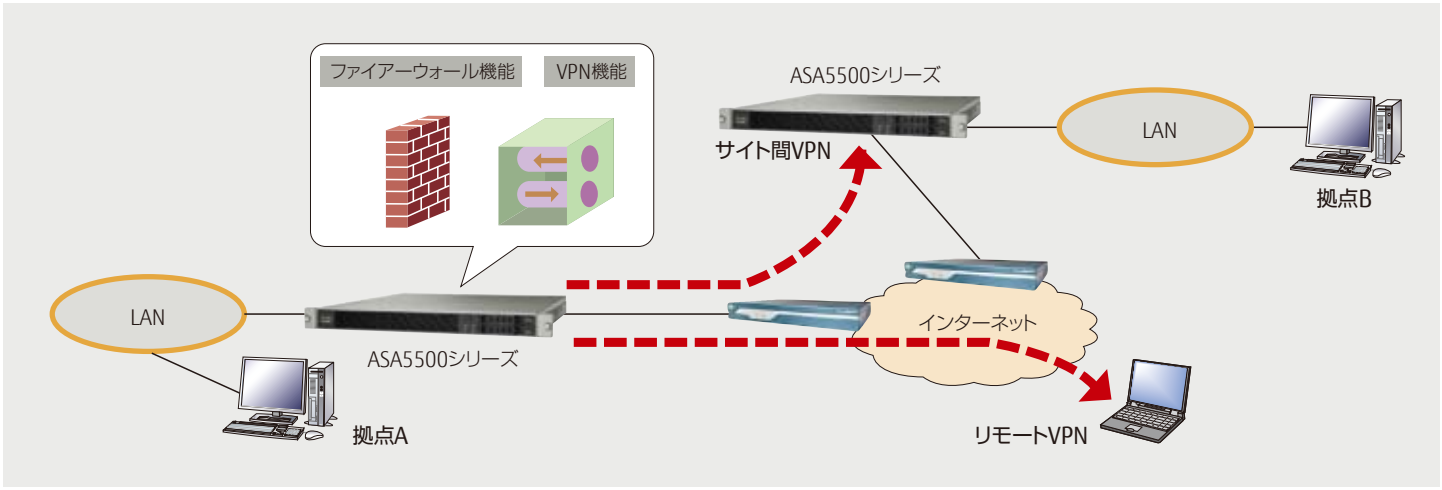
※ Remote Virtual Environment Computing
（株）富士通研究所が開発した画面転送の操作応答性能を向上させる高速表示技術

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

ASA5512-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

ASA5505

●小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:150Mbps
●3DES／AES VPN性能:100Mbps

■ 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。

■ 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。

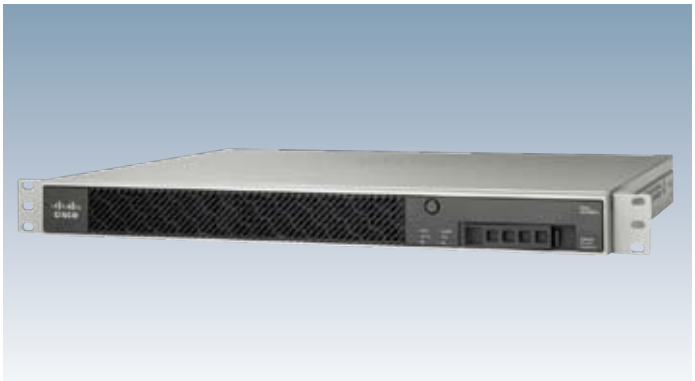
802.1qベースのVLAN機能
複数のスイッチが稼働しているネットワーク環境への導入を可能にします。

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(Anti 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。

ASA with FirePOWER



■ 高度なセキュリティ機能をサポート

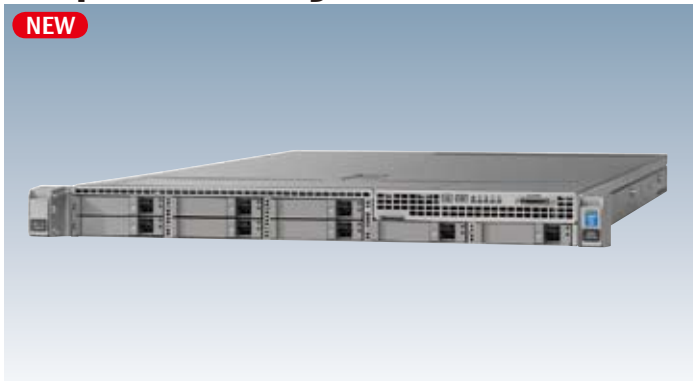
侵入防御システム (Intrusion Preventions System)
ネットワーク上の通信を記録し、侵入を検知した場合、通信の遮断を即実行します。

マルウェア防御 (Anti 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)



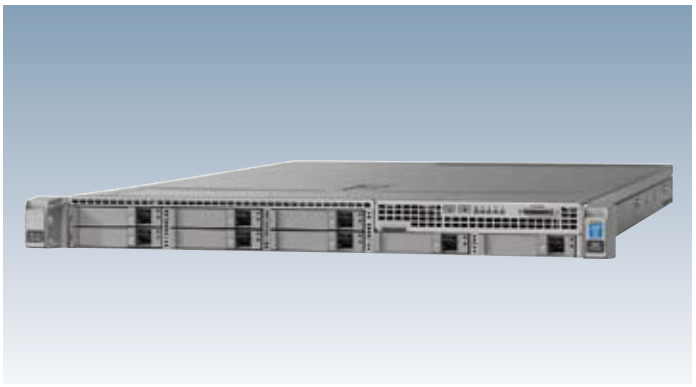
■ Firepower Management Center (FMC) による効率的な運用・管理が可能

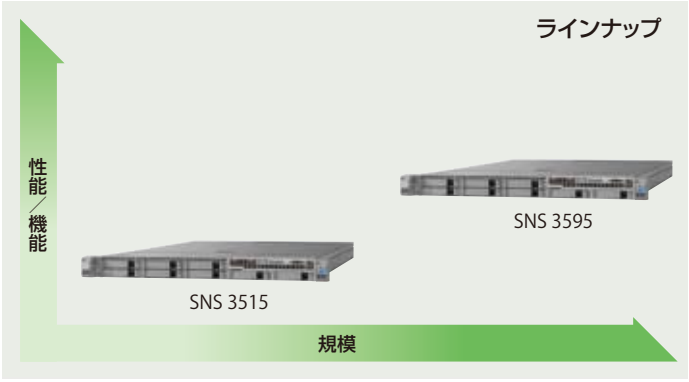
Firepower Management Center (FMC) により、複数台のASA with FirePOWERを統合管理することで、一括設定やネットワーク上の攻撃の可視化などができます。

シスコシステムズ社製 セキュリティアプライアンス

Cisco 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。

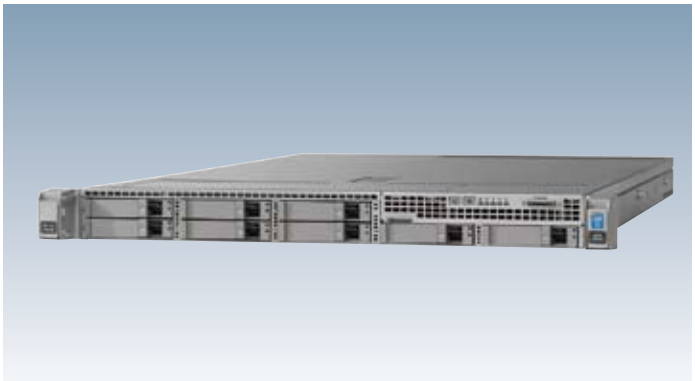
■ 複数台構成による信頼性向上

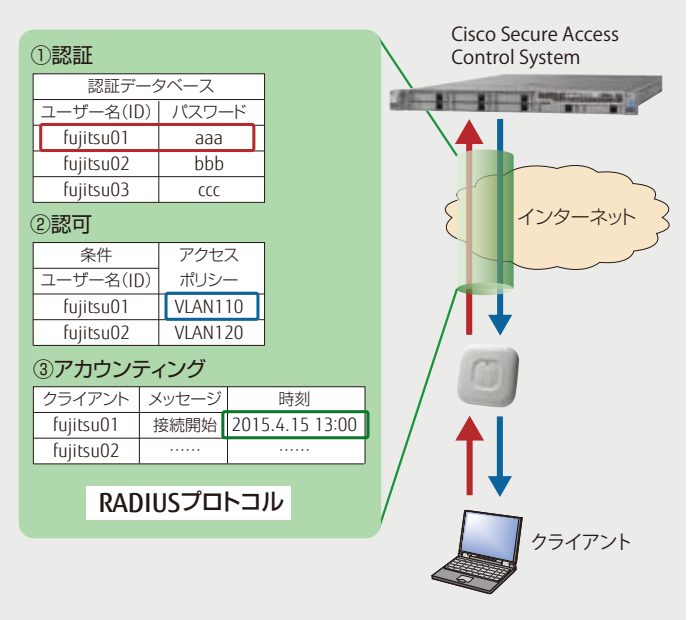
複数台構成により、大規模システムでの認証・制御が可能となります。
また、認証システムの信頼性が向上します。
複数台を一括で設定・管理できる機能を有しており、管理性の面で優れています。

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 Access Control System

「Cisco Secure Access Control System」は、企業ネットワーク内におけるクライアントからのアクセスを認証・管理し、セキュリティ違反や不正なユーザーを制御することでセキュリティ強化を実現します。





■ 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。

■ 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/

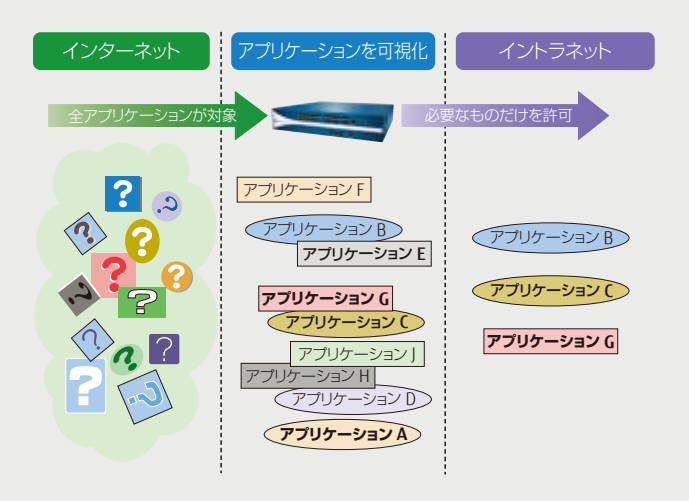
Palo Alto Networks社製 次世代ファイアーウォール

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。

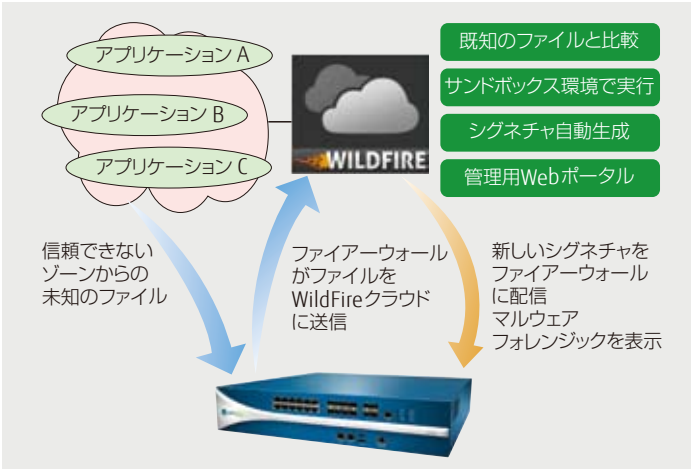
■ すべてのアプリケーションを可視化

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

NEW

●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

NEW

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

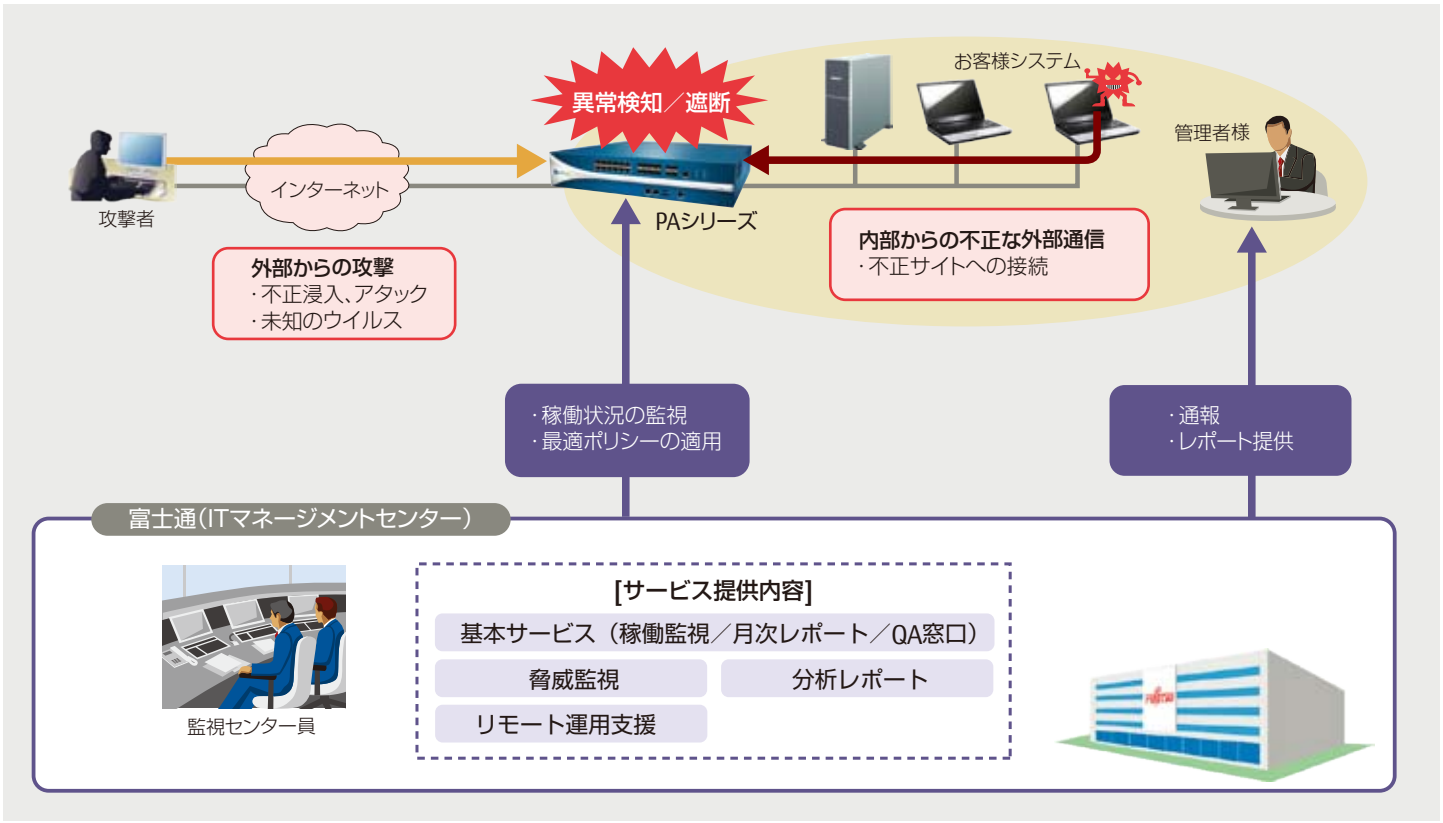
Panoramaシリーズ

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。

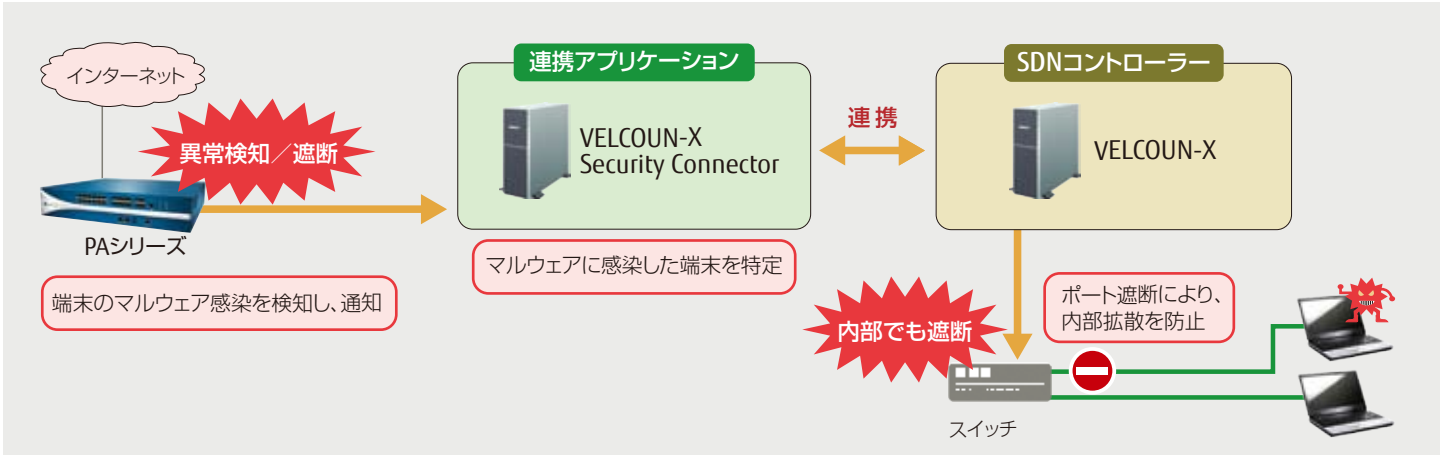


SDNコントローラー／PAシリーズ連携製品

FUJITSU Network VELCOUN-X Security Connector

■ 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VELCOUN-X（SDNコントローラー）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。



※FUJITSU Network VELCOUN-X 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。

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、P34を参照ください。）

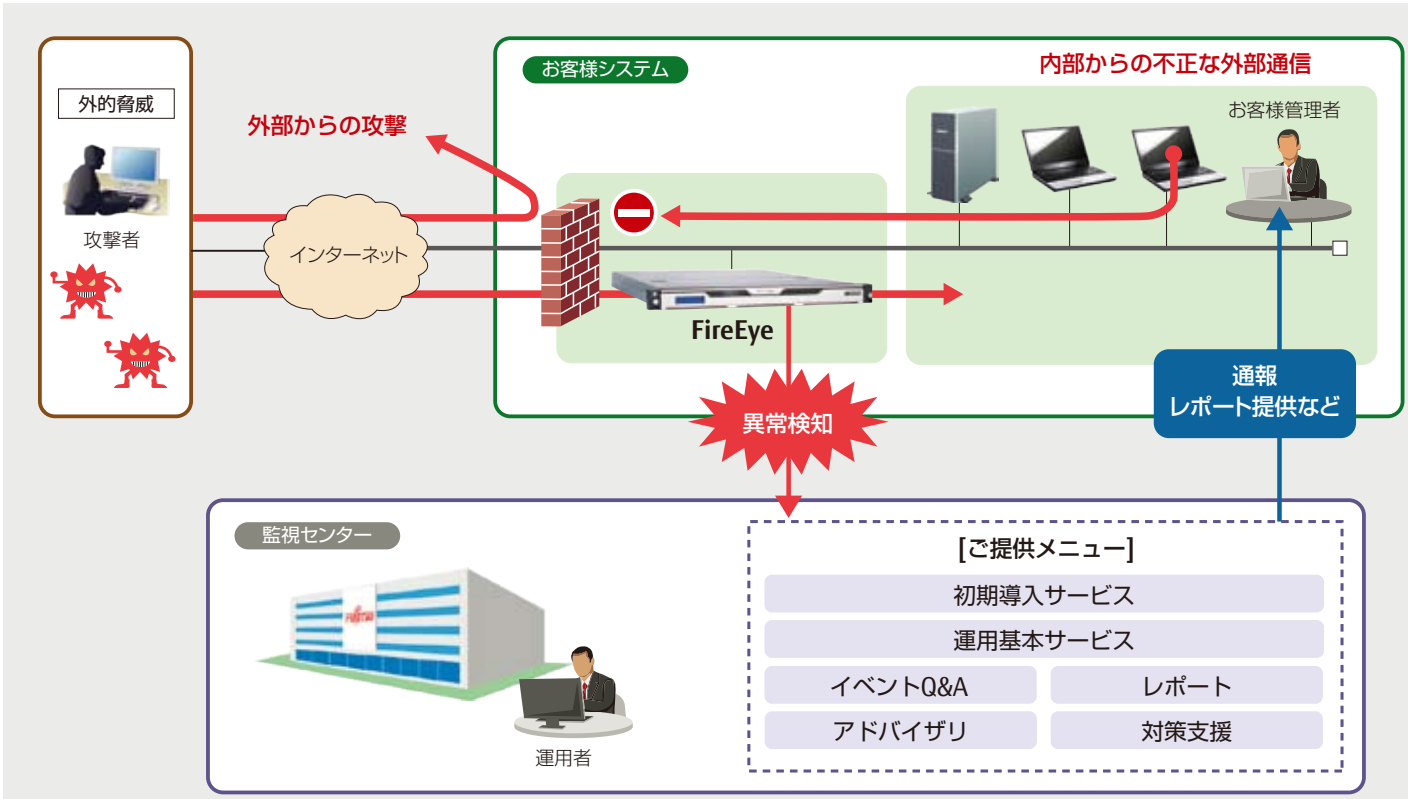
■ 入口対策－内部対策連携

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、P47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

富士通ネットワークプロダクト製品と組み合わせて販売・保守可能な製品として、PFU社製セキュリティ製品を提供します。

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

内部対策アプライアンス

iNetSec Intra Wall

「iNetSec Intra Wall」は、ネットワークに侵入したマルウェアの活動を検知、防御することができる内部対策アプライアンス製品です。センサーハードウェア(iNetSec Intra Wall センサー)とマネージャーソフトウェア(iNetSec Intra Wall マネージャー)により構成されます。

iNetSec Intra Wall センサー

■ 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

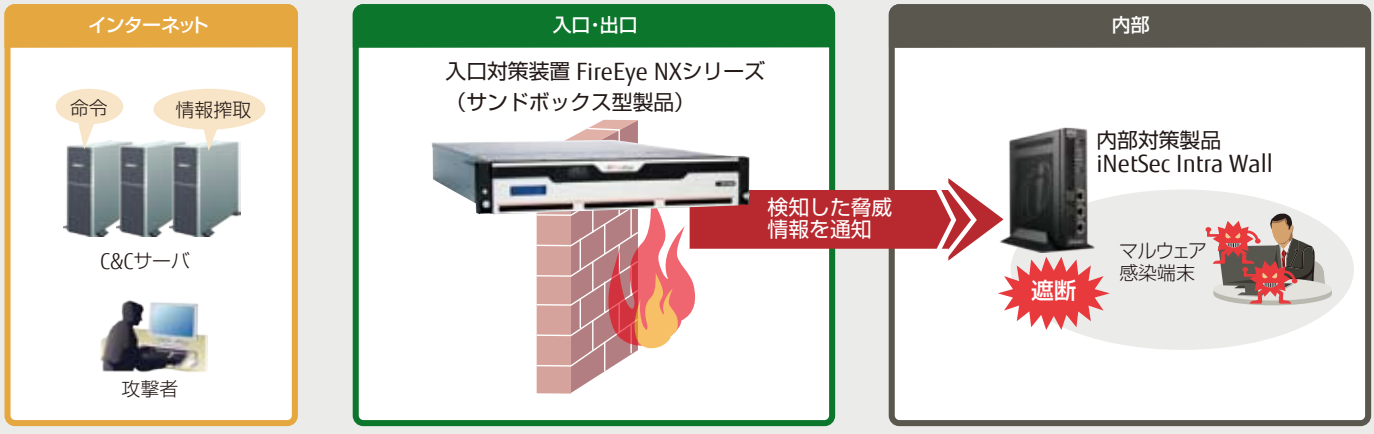
ファイル共有ソフトやSNSなど、業務で利用を禁止しているアプリケーションの利用を検知し、端末をネットワークから隔離します。ネットワークのセキュリティーポリシーの統制と情報漏えい対策の強化を実現します。

※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。
※本製品は、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。

内部・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シリーズのサンドボックスで検知した脅威情報をもとに、内部対策装置のiNetSec Intra Wall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/nwps/intrawall/#inetseciwfireeye



ICT機器管理アプライアンス

iNetSec Smart Finder

「iNetSec Smart Finder」は、ネットワーク上に存在するパソコンやプリンターなど、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 Smart Finderセンサー）とマネージャーソフトウェア（iNetSec Smart Finderマネージャー）により構成されます。

iNetSec Smart Finder 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〉、プリンター、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。

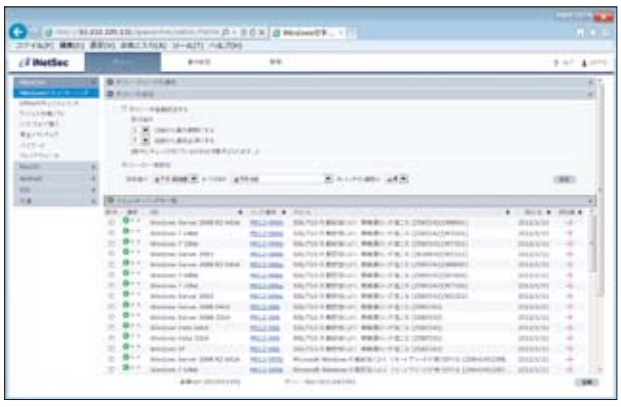
PC検疫ソフトウェア

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 EX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