

FirePass®

FirePass® Remote Access Controller リモートアクセスコントローラ

- 運用コストがかかるIPSecの悩みを解消
- 充実のクライアントセキュリティ機能
- 柔軟なポリシー設定でアクセスを制御



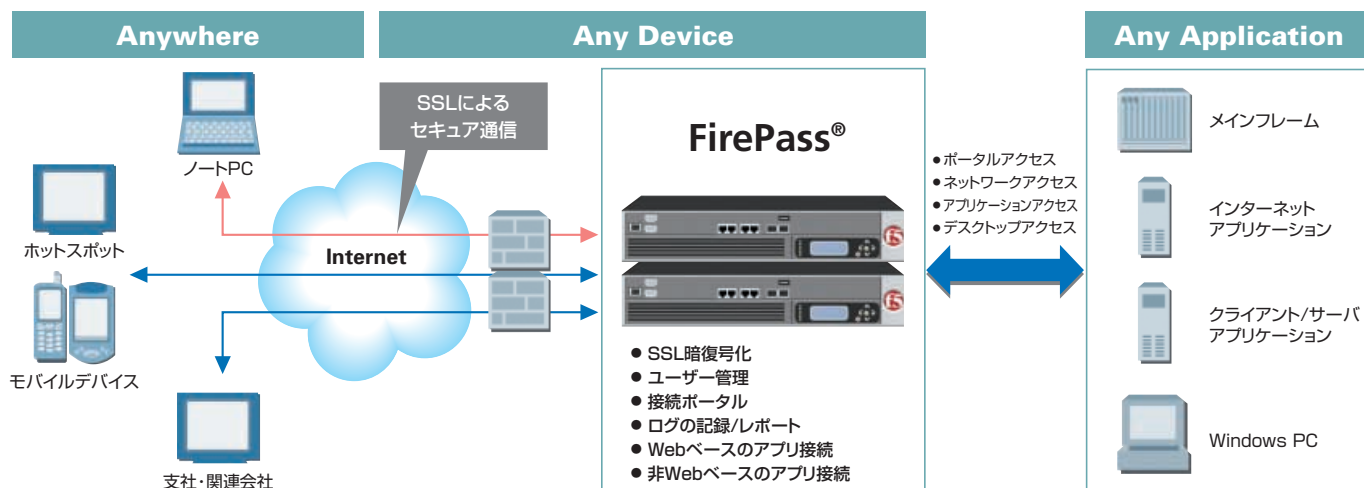
FirePass 4100 シリーズ



FirePass 1000 シリーズ

強力なエンドポイントセキュリティを搭載し、 きわめて安全で運用コストの少ないSSL VPN環境を実現

アプリケーションを選ばず	IPSecのようなVPN専用ソフトなしで、どんなアプリケーションにも対応する「ネットワークアクセス」機能を標準搭載しています。
デバイスを選ばず	Webブラウザを搭載するデバイスなら、PCだけでなくPDAや携帯電話でもメールを読んだり共有ファイルにアクセスできます。
場所を選ばず	インターネットに接続できる環境さえあれば、どんなところからでも社内ネットワークへ安全にアクセスできます。



Webベースアクセスを可能にする「ポータルアクセス」、アプリケーションへの柔軟なアクセスを実現する「ネットワークアクセス」と「アプリケーションアクセス」

F5ネットワークスのFirePassは、接続する際のデバイスや場所を選ばず(Any Device/Anywhere)、社内システムで稼動するどのようなアプリケーションにも接続可能な(Any Application)、SSL VPNアプライアンス製品です。

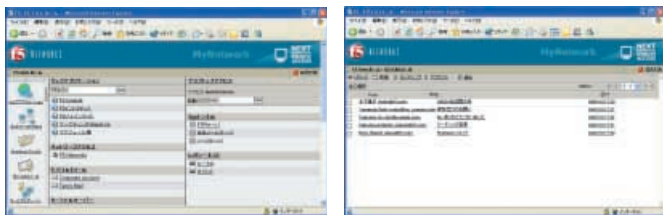
Portal Access

標準Webブラウザを使ってアプリケーションに接続「ポータルアクセス」

FirePassでは、Webブラウザを使って各種アプリケーションを利用する場合、「ポータルアクセス」を使います。SSLに対応したWebブラウザを使えるデバイス環境さえあれば、どこからでも社内イントラネットやメール、共有ファイル等への極めてセキュアなアクセスを可能にします。Windows、Linux、Unix、Macintoshといった各種PCはもちろん、PocketPCやPalmといったPDA端末からでも社内の情報に手軽にアクセス、また、ネットカフェの端末やキオスク端末などからもセキュアなアクセスが可能です。

Webベースのアプリケーションはもちろん、社内ネットワーク上のEメール、ファイルサーバ上の共有ファイルなどへもアクセスできます。また、ファイルサーバアクセス機能を利用して、SMBで共有されたWindowsファイル、NFS上のUnixファイルを開覧、アップロード、ダウンロード、コピー、移動、削除できます。メール送受信も、モバイルEメール機能を利用してWebブラウザだけで行なえます。

- ウェブアプリケーション
- モバイルEメール
- Windowsファイル
- Unixファイル



FirePassのポータルとモバイルEメール

Mobile Access

携帯電話やPDAから社内へアクセス「モバイルアクセス」

ユーザーが携帯電話やPDAといったモバイルデバイスを使ってリモートアクセスするのなら、「モバイルアクセス」が便利です。モバイルアクセスは、SSL通信が可能なミニブラウザからメールの送受信/共有ファイルの開覧/イントラネットへの接続ができるように、ポータル画面の変換やメール本文を自動的にフォーマットします。共有ファイルの開覧時には、DOCファイルを開覧でき、社外での情報共有に活躍します。



携帯電話で社内へアクセス

Network Access

IPベースですべてのアプリケーションにアクセス「ネットワークアクセス」

FirePassには、クライアント環境からサーバへそのまま接続できる「ネットワークアクセス」が標準で搭載。Outlook、Notesといったクライアント/サーバ系のアプリケーションから業務アプリケーションまで、ユーザーが普段使い慣れたクライアント環境を使って、社内サーバへSSL VPN接続できます。

業界で唯一のマルチプラットフォーム対応、そしてクライアントにはWindowsだけでなく、MacintoshやLinux、さらにはPocketPCもサポート。クライアントへの専用ソフトウェアのインストールは一切なく、完全なクライアントレスで運用でき、管理コストが削減できます。



Application Access

アプリケーションごとの柔軟な接続を提供「アプリケーションアクセス」

Webベースのアクセスとして、アクセスする「ターミナルサーバ」、TelnetやIBM 3270/5250などのホストサービス用の「レガシーホスト」、X Window Systemに接続する「Xウィンドウアクセス」の各機能を提供。また、クライアント環境からのアクセスとして、特定のTCPアプリケーションにアクセスする「Appトンネル」が提供されます。

- Appトンネル
- ターミナルサーバ
- レガシーホスト
- Xウィンドウアクセス

Desktop Access

自宅や出先から、社内にある自分のPCにアクセス「デスクトップアクセス」

FirePassのデスクトップアクセスは、社内のPCをリモートで操作するユニークな機能です。離れた場所から会社のPCに保存したユーザー自身の各種データに直接アクセスできます。アクセスはWebブラウザからマイドキュメントやOutlook、Internet Explorerなどを操作する方法と、直接WindowsデスクトップのGUIを開いて各種アプリを操作する方法の2通りがあります。

Client Security

セキュリティと情報活用を両立させる 「クライアントセキュリティ機能」

リモートアクセスしてくるクライアントPCが社内のセキュリティリスクとならず、管理者が安心してSSL VPNを運用できるようにする仕組みが「クライアントセキュリティ機能（エンドポイントセキュリティ）」です。

FirePassでは、ログオン前とログオン時に2段階でポリシーチェックを実行し、ログオン自体と、ログオン後のリソースアクセスの許可を別々のポリシーで制御できます。これにより、ログオンを許可したクライアントに対してより厳密なチェックを実行し、安全性に応じてアクセス可能なリソースを制御できます。たとえばクライアント証明書を持つデバイスにはフルアクセスを許可、その他のデバイスに対してはWeb経由での情報アクセスのみを許可といった制御が可能です。

ポリシーチェックには、クライアントOSの種類やバージョン、IEのバージョン、パッチの適用状況、指定のプロセスの稼働有無だけでなく、ウイルス対策ソフトが最新の状態で稼働しているかのチェックも含まれます。対応のウイルス対策ソフトはSymantecやTrendmicroなど、国内外の主要な製品15種類以上（2005年5月現在）に及びます。



危険度が高いと判断されたクライアントに対しては、警告メッセージを表示し（フォールバックポリシー）、ポリシー違反をして接続できないユーザーを混乱させることなく適切な対処を促し、管理コストの低減を図れます。

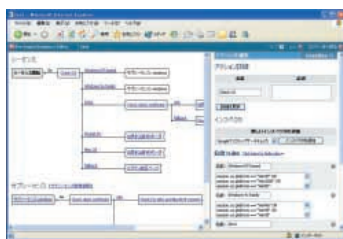
キャッシュクリーンナップや、ユーザーがリモートで行なう作業を仮想のデスクトップ内に制限してしまうプロテクトドワークスペース機能により、情報漏えいへの対策も万全。パスワード盗聴を防止するバーチャルキーボード、さらにネットワークアクセス時にリモートPCが踏み台となることを防ぐセーフスプリットトンネルといった機能もあり、クライアントPCの危険性を徹底的に排除します。

Visual Policy Editor

アクセスポリシーをわかりやすく簡単に設定できる 「ビジュアルポリシーエディタ」

ポリシーチェックの基準となるアクセスポリシーは、簡単に定義・設定できることが必須。FirePassでは、視覚的にわかりやすい方法でアクセスポリシーを設定できるツール「ビジュアルポリシーエディタ」を標準搭載。フローチャートを描く要領で簡単にポリシーを定義できます。

ビジュアルポリシーエディタでは、ポリシーチェックの一連の手順となる「シーケンス」を定義。シーケンスは必要にあわせていくつでも作成でき、再利用可能なサブシーケンス（例：クライアント証明書の有無など）を組み合わせて、段階的に構成できるので、あらゆる可能性を想定した柔軟で強力なポリシーチェックが可能です。



Authentication

より安全なSSL VPNの運用に不可欠 「認証ソリューション」

ワンタイムパスワードやSSLクライアント証明書を使って、ログオン時のユーザー認証を強化する各種認証ソリューションとの導入実績が多数あります。F5 ネットワークスでは以下の代表的な認証ベンダー等と協業しており、さまざまな認証製品、サービスとFirePassの連携がすでに実証されています。

製品/サービス	ソリューション提供各社
RSA SecurID®	RSA セキュリティ
RSA Keon®	RSA セキュリティ
SECUREMATRIX	シー・エス・イー
WisePoint Authenticator	ファルコンシステムコンサルティング
マネージドPKIサービス	日本ベリサイン
UBIQPASS	NECソフト
FirstPass®	NTTドコモ

SSL Accelerator

高負荷なSSL処理をオフロードする 「SSLアクセラレータ」を搭載可能

FirePass 4100シリーズには、高性能SSLアクセラレータが標準搭載。このSSLアクセラレータはセッションの新規接続処理だけでなく、実データの暗復号化処理（バルク暗号化）もハードウェア処理できることが特長で、CPUからSSLの負荷を完全にオフロードします。また、DESに代わる次世代の標準暗号化方式として米国政府により選定された「AES（Advanced Encryption Standard）」にも対応。さらに金融、医療、政府機関など、きわめてセキュアな秘密鍵の管理ソリューションが求められる組織には「FIPS 140-2 Level 2 Certified」として認定されているSSLアクセラレータをオプションで提供します。



Reverse Proxy

あらゆる企業のWeb環境に対応する 「リバースプロキシ機能」

企業のインフォメーションポータルなどダイナミックコンテンツが多用されている複雑なWebアプリケーションに対応できる先進のリバースプロキシを搭載。HTMLで記述された単純なWebページだけではなく、Javascript、VBscript、Javaアプレット、ActiveX、Flashを活用したコンテンツにも対応し、あらゆる企業のWeb環境へスムーズな導入が可能です。FirePassはVPNC認定を取得しており、WebポータルやExchangeとの相互運用性が第三者機関により実証されています。



■ ハードウェア仕様

	FirePass 1000シリーズ			FirePass 4100シリーズ				
								
モデル名	1010	1020	1030	4110	4120	4130	4140	4150
標準同時接続数	25	50	100	100	250	500	1000	2000
最大同時接続数	100			2000 (20000*1)				
CPU	Pentium III×1			Xeon×2				
メモリ	512MB			4GB				
HDD	40GB			80GB				
ネットワークインターフェイス	10/100Mbps イーサネット×3			10/100/1000Mbps イーサネット×4				
外形寸法	425 (W) × 44 (H) × 280 (D) 1U			445 (W) × 89 (H) × 622 (D) 2U				
重量	4.5kg			16.3kg				
電源	100-240V ~ 4/2A 50/60Hz			90-240VAC 9/4A 50/60Hz				
最大消費電力	180W			400W				
動作時温度	0 ~ 40℃			5 ~ 40℃				
動作時湿度	5 ~ 85% (温度40℃にて。結露のないこと)			5 ~ 85% (温度40℃にて。結露のないこと)				
適合規格	US/Canada - UL - UL 1950 European Union - Low Voltage Directive - EN 60950 European Union - EMC Directive EN50081-2 & EN61000-6-2 CE			US/Canada - UL - UL 1950 European Union - Low Voltage Directive - EN 60950 EMC Directive - EN 50081-2 & EN 61000-6-2 CE				

*1 クラスタリング構成時

■ 機能一覧

接続機能	FirePass 1000	FirePass 4100	対応アプリケーション/機能
ネットワークアクセス	●	●	TCP/UDP アプリケーション (すべてのIP アプリケーション)。IPsec と同等の接続
ウェブアプリケーション	●	●	イントラネット (HTTP, HTTPS)、OWA2000、iNotes
モバイルEメール	●	●	Web ブラウザによるメールの読み書き (POP3, IMAP, SMTP, LDAP)
Windows ファイル	●	●	共有ファイル (SMB, Windows Workgroup, Windows ドメイン, Novell 5.1/6.0)
Unix ファイル	○	●	共有ファイル (NFS ファイル)
App トンネル	○	●	固定ポートのTCP アプリケーション (Exchange, Lotus Notes, FTP, Oracle, SAP など)
ターミナルサーバ	○	○	ターミナルサービス (Citrix MetaFrame, Microsoft WTS, VNC)
レガシーホスト	○	○	ホスト系サービス (VT100, VT320, Telnet, X-Term, IBM 3270/5250)
Xウィンドウアクセス	○	●	X Window System 上のアプリケーション
モバイルアクセス	○	●	モバイル端末 (Palm などの PDA, iモード, WAP, PocketPC) から接続
デスクトップアクセス	○	○	社内に設置されたユーザーのPC (Windows デスクトップ) 上のアプリケーション
SSL アクセラレーション機能			
SSL アクセラレーション	—	●	SSL のセッション処理、およびデータ暗復号化処理を高速化するハードウェアアクセラレータ
FIPS SSL アクセラレーション	—	○	FIPS 140 に対応した SSL ハードウェアアクセラレータ
その他の機能			
ダイナミックポリシーエンジン	●	●	グループごとの動的なユーザー管理 (認証、アクセス制御) 機能
ダイナミックグループマッピング	●	●	ユーザーのグループ属性の自動割当 (Active Directory, LDAP, Radius, クライアント証明書)
クライアント完全性チェック	●	●	安全性が確認されないリモート PC を接続させない
プロテクトドワークスペース	●	●	リモート PC で読み込まれたデータの痕跡を残さない
Web アプリケーションセキュリティ	●	●	コンテンツ解析による HTTP 攻撃防御、およびファイルのウイルススキャン (ブラウザアクセス時)
クライアント API	●	●	オープンな API および SDK により、自動接続する Win32 アプリケーションの開発
冗長化*1	●	●	アクティブ/スタンバイ構成によるフェールオーバー機能
クラスタリング*2	—	●	複数台の FirePass ユニットの同時に稼働し、負荷分散

●=標準搭載 ○=オプションにより提供 *1 スタンバイ用のユニットは別売 *2 クラスタリング用のユニットおよびオプションライセンスは別売

■ 管理機能

認証方法・対応システム	内部データベース、LDAP、RADIUS、Windows Active Directory、NT Domain、X.509 デジタル証明書 (PKI)、HTTP ベーシック認証、Web フォーム認証、RSA SecurID、Vasco DigiPass (オプション)、SiteMinder 等
ログ・レポート	ログオン、セッション、HTTP ログ、アプリケーションログ、システムログ、デスクトップアクティベーション、サマリーレポート、グループレポート
ロードモニター	現在の同時接続数、CPU 使用率、メモリ使用率、メモリページング、ディスク I/O、ロードアベラージュ、プロセス生成率、NIC の統計



<http://www.f5networks.co.jp/>

F5 ネットワークスジャパン株式会社
F5 Networks Japan K.K.

〒150-6018 東京都渋谷区恵比寿4-20-3 恵比寿ガーデンプレイスタワー18F
TEL. 03-5447-3360 FAX. 03-5447-3351

お問い合わせ先
株式会社富士通ソーシャルサイエンスラボ
ソリューションコーディネーター統括部マーケティング推進部
〒211-0063 川崎市中原区小杉町1-403
武蔵小杉タワープレイス

TEL 044-739-1251
E-mail : sa-info@ssl.fujitsu.com
URL: <http://www.ssl.fujitsu.com/>

©2004 F5 Networks, Inc. 全著作権所有。F5、F5 Networks および FirePass は、F5 Networks, Inc. の商標、または登録商標です。
●本文中に記載されている製品名、および社名はそれぞれ各社の商標、または登録商標です。