

FirePass[®]

Remote Access Controller

安全で利便性の高いリモートアクセス環境を実現する
SSL VPN



IT agility. Your way.

「情報の活用」と「情報の保護」を同時に実現し、 ビジネスの効率アップ！

FirePassは、企業データへのリモートアクセスに高い利便性と強固なセキュリティを提供するSSL VPNです。

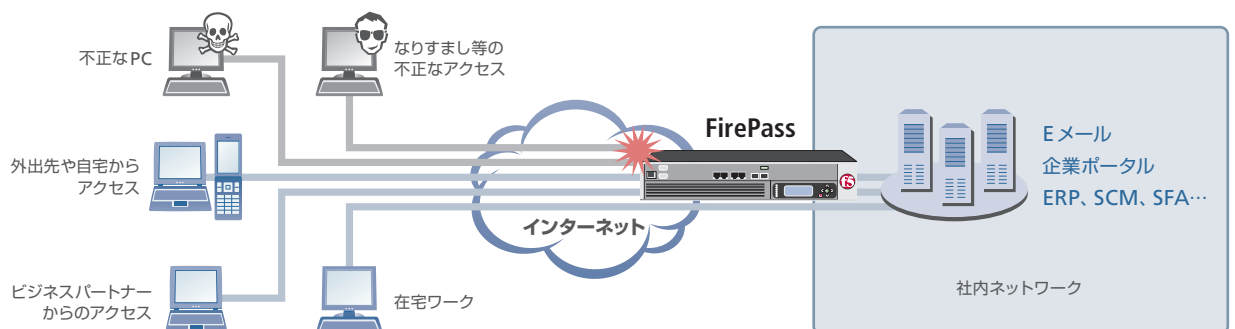
パソコンや携帯電話、スマートフォンなどのあらゆる端末から場所や時間に制限されないアクセスをユーザに提供し、業務効率の向上、意思決定スピードの向上、柔軟なワークスタイルを実現します。同時に、強固なセキュリティポリシーの簡単な作成を実現するフローチャート式のツールや、利用アプリケーション・外部デバイスの利用を制限するグループポリシー機能などにより、情報漏えいリスクの大幅な軽減を実現します。さらに、日本語化された簡単な管理者画面やオンラインヘルプ・マニュアルにより、運用管理に伴うコストや負担を削減します。

課題

- スマートフォンなどを含む最新のクライアント端末を使って企業データへアクセスしたい
- ノートPCは社外持ち出し禁止、外出先からのリモートアクセス禁止では仕事の効率が上がらない
- 現在のリモートアクセスシステムでは、ホテルや海外の出張先からだと企業データにアクセスできないので仕事にならない
- セキュリティに対する意識が向上し、経営者から情報管理の徹底・強化が求められている
- 会社のPCが外出先で紛失や盗難にあうと、会社情報の漏えいにつながりかねない
- 自宅やネットカフェからのアクセスを認めると、情報漏えいやウイルス感染が心配だ
- 現在のリモートアクセスシステムでは、VPN専用のクライアントソフトを、利用者ひとりひとりの端末にインストールするのが大変だ

解決策

- 利用者はWebブラウザを搭載するPC、スマートフォン、携帯電話さえあれば、いつでも社内ネットワークにアクセスでき、ビジネスの効率がアップ
- セキュリティレベルの低いクライアントからのアクセスを制限することで、情報の漏えいや社内ネットワークへのウイルス感染を防止
- アクセスを会社が認めたPCだけに限定したり、ユーザが使えるアプリケーションを限定したりなど、セキュリティレベルの柔軟な設定を実現
- 管理者は利用者端末に専用ソフトをインストールする必要がないことから、導入の手間がかからず即座にSSL VPN環境を構築すると同時に、管理コストを削減



FirePassの主な特長

最強の「エンドポイントセキュリティ」

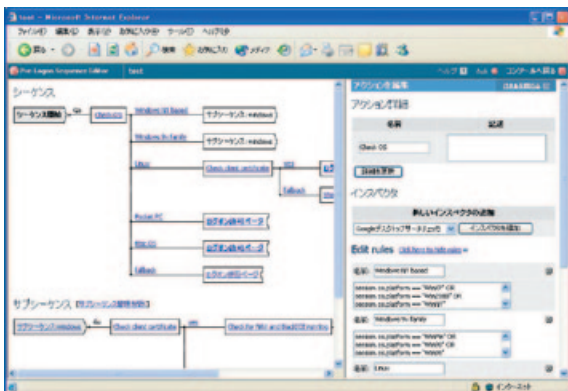
利用者がログオン前にセキュリティ状態をチェックする「ログオン前シーケンス」。クライアントOSの種類やIEのバージョン、パッチの適用状況だけでなく、ウイルス対策ソフトが最新の状態で稼働しているかなどのチェックを行います。リモートアクセス終了時にデバイスにデータや履歴を残さない「プロテクトドワークスペース」。ログアウト時にキャッシュに蓄えられたデータを消去する「キャッシュクリーンアップ」など、アクセスポイントをセキュリティリスクにしない、包括的なエンドポイントセキュリティを備えています。この優れた機能はリモートアクセスはもとより、社内LANやワイヤレスLANにおいても有効です。

コンプライアンス対応強化を実現する「グループポリシー機能」

ネットワークドメイン外のクライアントにも、エンドポイントセキュリティチェックとグループポリシー遵守の強制を実現。さらに、HIPAA、PCI、GLBAのようなコンプライアンス対応の強化を図るポリシーテンプレートを搭載。簡単ですばやい適用を実現するだけでなく、集中管理することによりポリシーの劣化を防ぎます。

フローチャート式の「ビジュアルポリシーエディタ」

アクセスポリシーは見やすいフローチャート式で作成。グループ、ユーザ、デバイスごとの容易な管理を実現します。



強固なセキュリティポリシーの簡単な作成を実現するビジュアルポリシーエディタ

誰にでもわかりやすい日本語画面

ユーザ画面および管理者画面は、機能名を含めすべて日本語表記。さらに、オンラインヘルプも充実し、手間やコストのかからない運用管理を提供します。

デバイスや場所を選ばない、さまざまなアクセス方法

【ネットワークアクセス】

クライアント端末に入っているアプリケーションがすべて使える「ネットワークアクセス」は、Outlook、Notesなど、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、普段使い慣れた環境から社内サーバへのアクセスを提供。クライアント端末に専用ソフトウェアをインストールする必要がなく、導入の手間と管理コストを削減します。

【ポータルアクセス】

SSLに対応したWebブラウザを搭載したクライアント端末から、社内イントラネットやメール、共有ファイルなどにアクセスする「ポータルアクセス」は、Windows、Linux、Macintoshなどの各種PCはもちろん、スマートフォンやネットカフェなどからでもセキュアなアクセスを実現します。

【モバイルアクセス】

携帯電話やPDAなどのデバイスから、メールサーバに接続する「モバイルアクセス」では、携帯電話のメールアドレスに会社のメールを転送する場合と異なり、会社のメールアドレスから返信するためビジネスユースに適しています。Webブラウザでメールを送受信し、端末のメールボックスにはデータが残らないため、万一デバイスを紛失しても情報漏えいの心配がありません。



認証ソリューション

セキュリティをさらに強化するには、アクセスしてきたユーザが本人かどうかのチェックが不可欠です。FirePassでは、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認証を強化する各種認証ソリューションを多数用意しています。

(次ページ参照)

FirePass®

連携可能な認証ソリューション

★：株式会社シー・エス・イーはTechnology Alliance Partnerです。

ソリューション提供各社	製品/サービス
ワンタイムパスワード	
株式会社シー・エス・イー★ ファルコンシステムコンサルティング株式会社 NECソフト株式会社 RSAセキュリティ株式会社 エントラストジャパン株式会社 日本ベリサイン株式会社 株式会社アイディーエス	SECUREMATRIX® WisePoint Authenticator UBIQPASS® RSA SecurID®, RSA Keon® IdentityGuard™ ベリサイン ユニファイドオーセンティケーション (UA) MITS OTP
デジタル証明書	
日本ベリサイン株式会社 株式会社NTTドコモ ペンティオ株式会社 サイバートラスト株式会社 株式会社ソリトンシステムズ 日本ジオトラスト株式会社	マネージドPKIサービス FirstPass® PKIプライベートCA Cybertrust Shared PKI for SSL VPN Net'Attest® CA トゥルークレデンシャル エクスプレス (TCX) / トゥルークレデンシャル (TC)

ソリューション提供各社	製品/サービス
デバイス特定認証	
株式会社エヌ・エス・アイ フェニックステクノロジー株式会社 沖電気ネットワークインテグレーション株式会社	RegistGate® Phoenix TrustConnector™ ROUD™ (RegistGate)
2要素認証	
サードネットワークス株式会社	Secure Call
生体認証	
株式会社ディー・ディー・エス ソニー株式会社 株式会社ユーエスシー	UBF PUPPY FKEY
検索ネットワーク	
NTTデータ先端技術株式会社 株式会社PFU 日本電気株式会社	NOSiDE® Inventory Sub System iNetSec® Inspection Center InfoCage PC 検疫

ハードウェア仕様

	FirePass 1200シリーズ				FirePass 4100シリーズ			FirePass 4300シリーズ				
モデル名	1205	1210	1220	1230	4110	4120	4130	4305	4310	4320	4330	4340
標準同時接続数 (利用ユーザ数目安)	10 (100)	25 (250)	50 (500)	100 (1000)	100 (1000)	250 (2500)	500 (5000)	100 (1000)	250 (2500)	500 (5000)	1000 (10000)	2000 (20000)
最大同時接続数	100				1000 (10000*)			2000 (20000*)				
メモリ搭載	●				●			●				
CPU	シングルCPU				デュアルCPU			デュアルCPU (デュアルコア)				
ハードドライブ	●				●			●				
ギガビットCUポート	2×10/100Mbpsイーサネット				4×10/100/1000Mbpsイーサネット			4×10/100/1000Mbps イーサネット				
ギガビットファイバーポート (SFP-GBIC Mini)	●				●			2 (オプション)				
外形寸法 (cm)	H4.3, W42.4, D27.9				H8.9, W44.5, D59.7			H8.9, W44.5, D59.7				
重量	4.53kg				18.1kg			19.5kg				
動作時温度	5 ~ 40℃				5 ~ 40℃			5 ~ 40℃				
動作時湿度	20 ~ 90% (湿度40℃にて、結露のないこと)				20 ~ 90% (湿度40℃にて、結露のないこと)			20 ~ 90% (湿度40℃にて、結露のないこと)				
定格入力電流 (A)	100 ~ 240VAC 4/2A 50/60Hz				90 ~ 240VAC 9/4A 50/60Hz			90 ~ 240VAC 9/4A 50/60Hz				
最大消費電力	250W				400W			460W				
最大発熱量	785BTUs				939BTUs			939BTUs				
適合規格	UL 60950 (UL 1950-3), CSA-C22.2 No 60950-00 (Bi-national standard with UL 60950) CB test certification to IEC 950, EN 60950				UL 60950 (UL 1950-3), CSA-C22.2 No 60950-00 (Bi-national standard with UL 60950) CB test certification to IEC 950, EN 60950			UL 60950 (UL 1950-3), CSA-C22.2 No 60950-00 (Bi-national standard with UL 60950) CB test certification to IEC 950, EN 60950				
電磁波認定	EN55022 1998 Class A FCC Part 15B Class A VCCI Class A				EN55022 1998 Class A FCC Part 15B Class A VCCI Class A			EN55022 1998 Class A FCC Part 15B Class A VCCI Class A				
冗長電源 (AC)	-				○			●				

●=標準搭載/○=オプションにより提供 ※1=クラスターリング構成時

機能一覧

接続機能	FirePass 1200	FirePass 4100	FirePass 4300	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
Webアプリケーション	●	●	●	イントラネット (HTTP, HTTPS), OWA, SharePoint, iNotes, Oracle 10g Portal, SAP ERP Portal
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)
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 Presentation Server, 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)
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
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	●	●	●	ユーザのグループ属性の自動判別 (Active Directory, LDAP, RADIUS, クライアント証明書)
エンドポイント・セキュリティチェック	●	●	●	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
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イルオーバー機能
クラスターリング*2	-	●	●	複数台のFirePassユニットを同時に稼働し、負荷分散
グループポリシー	○	○	○	クライアントPC上の操作をコントロールしセキュリティを強化

●=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=クラスター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 等
ログ・レポート	ログイン、セッション、HTTPログ、アプリケーションログ、システムログ、サマリレポート、グループレポート
ロードモニタ	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、プロセス生成率、NICの統計

2009年04月現在。最新情報はF5ネットワークスのWebサイトをご確認ください。



F5ネットワークスジャパン株式会社

東京本社
〒107-0052 東京都港区赤坂4-15-1 赤坂ガーデンシティ19階
TEL 03-5114-3210 FAX 03-5114-3201

西日本本社
〒530-0001 大阪市北区梅田2-2-2 ヒルトンプラザウエスト オフィスタワー19階
TEL 06-6225-1250 FAX 06-6225-1111

お問い合わせはF5 First Contactまで: www.f5networks.co.jp/fc/

●お問い合わせ先

株式会社富士通ソーシアルサイエンスラボラトリ
マーケティング本部 ソリューション推進部
〒211-0063 川崎市中原小杉町1-403
武蔵小杉タワープレイス
TEL 044-739-1251
E-mail: ssl-info@cs.jp.fujitsu.com
URL: <http://www.ssl.fujitsu.com/>