外出先でタブレットからオフィスのPCを遠隔操作

FUJITSU Thin Client Solution
モバらくだ Desktop Access

「モバらくだ Desktop Access」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。

モバイル端末から「Desktop Accessクライアント」を活用することで、時間や場所を選ぶことなく、使いたい時に自席PCをセキュアに操作できます。

特 長

- モバイル端末を活用して安心・安全なシンクライアント環境を実現
- 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は不要な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

想定される利用シーン

受発注業務での利用

既存のPC向け受発注システムをモバイル端末から利用

ペーパーレス会議での利用

会議資料はモバイル端末で各自が取得し、ﾍﾟｰﾊﾟﾚｽ会議が実現

ＢＣ（事業継続性）の実現を支援

大地震発生時や新型インフルエンザ発生時の在宅勤務に利用

営業活動の強化、効率化

モバイルワークを可能とすることで、営業の顧客訪問活動の強化、営業活動時間の有効活用を実現

在宅勤務・人材の有効活用

週１回の在宅勤務による社員のワークライフバランスの向上
育児・介護支援制度、団塊世代のスキル活用

その他の利用シーン

①建設現場や展示場など期間限定の事務所での業務
②出張が多い役員や管理職の承認・決済業務
③社内システムのトラブル等での迅速な対応など様々な利用シーンが考えられます。

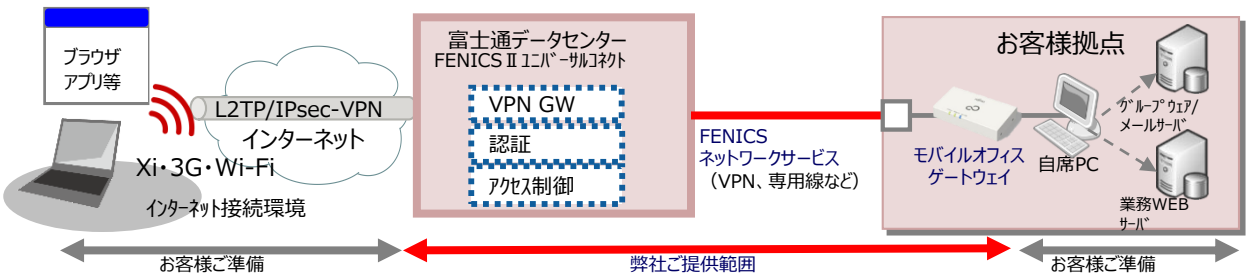
http://www.fujitsu.com/jp/group/fnets/products/mogw/index.html

shaping tomorrow with you
社会とお客様の豊かな未来のために

■ モバイル端末による『**安心**』『**便利**』なシンクライアント環境を『**簡単**』に実現し、自席のPC電源投入や、リモートデスクトップ接続により、いつでも、どこでも業務が行えます。

価格例（消費税抜き）

構成Ⅰ： ＶＰＮサービス利用型（ＦＥＮＩＣＳⅡユニバーサルコネクトをご利用の場合） 50名利用時



①FENICSをご利用中のお客様
（ユニバーサルコネクト＋モバイルオフィスゲートウェイの価格）

FENICS	Desktop Access
初期費：100,000円 月額費：1,000円／1アカウント	初期費：298,000円 保守費：24,000円／年額

*1：月額費には、FENICSビジネスVPNのオプションインフラ接続利用料（月額10,000円）は含まれておりません。

②新規にFENICSをご導入のお客様
（ユニバーサルコネクト＋モバイルオフィスゲートウェイ＋ビジネスVPNの価格）

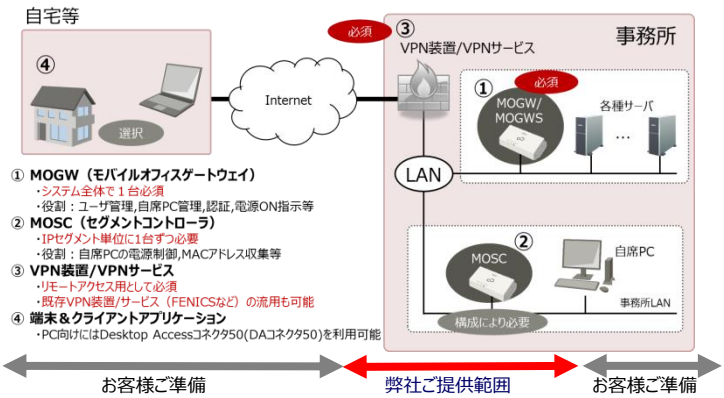
FENICS	Desktop Access
初期費：173,400円 月額費：1,600円／1アカウント	初期費：298,000円 保守費：24,000円／年額

*2：ネットワークサービスはFENICSビジネスVPNをご利用の場合になります。
（フレッツ光ネクスト ファミリータイプ：回線・レンタルルータSi-R80brin含む）

*3 *4 *5 *6 *7

*3：初期費にはレンタルルータ、モバイルオフィスゲートウェイの設定/構築費は含まれておりません。
*4：モバイルオフィスゲートウェイの保守料（年額：24,000円/台）が別途必要になります。
*5：お客様のネットワークセグメントが複数ある場合には、別途セグメントコントローラー（118,000円/台）がセグメント毎に必要となります。
*6：モバイルオフィスゲートウェイ用クライアントソフトはAppStoreから無償でダウンロードできます。
*7：リモートデスクトップ用ソフトはGoogle Playよりお客様にてご購入下さい。

構成Ⅱ： ＶＰＮ自営構築型（Ｃｉｓｃｏ ＡＳＡの場合） 50名利用時



① **MOGW（モバイルオフィスゲートウェイ）**
・システム全体で１台必須
・役割：ユーザ管理,自席PC管理,認証,電源ON指示等
② **MOSC（セグメントコントローラ）**
・IPセグメント単位に1台ずつ必要
・役割：自席PCの電源制御,MACアドレス収集等
③ **VPN装置/VPNサービス**
・リモートアクセス用として必須
・既存VPN装置/サービス（FENICSなど）の流用も可能
④ **端末＆クライアントアプリケーション**
・PC向けにはDesktop Accessコネクタ50(DAコネクタ50)を利用可能

モバイルオフィスゲートウェイ

標準価格 ￥298,000（税別）／台
■１システムに最低１台必須
■ユーザ認証やRDP接続ファイル管理 など

ご参考 ： VPN装置 Cisco ASA 5510

標準価格 ASA5510 本体A11 ￥568,000～（税別）／台
■IPSec 暗号化通信
■同時接続ユーザ数 ：50～
■ユーザ登録数 ：50～

*8：接続先が1セグメントの環境となります。２セグメント以上の場合、別途モバイルオフィスセグメントコントローラ（MOSC）¥118,000(税別)/台が必要となります。
*9：導入費用が別途必要となります。また、回線費用は含まれておりません。
*10：モバイルオフィスゲートウェイの保守料およびASA5510の保守料が別途必要になります。

お問い合わせ先

富士通コンタクトライン（総合窓口）TEL：**0120-933-200**
受付時間：9：00-17：30（土、日、祝日、当社指定の休業日を除く）
http://jp.fujitsu.com/telecom

富士通株式会社
〒105-7123 東京都港区東新橋1-5-2 汐留シティセンター

2015.09

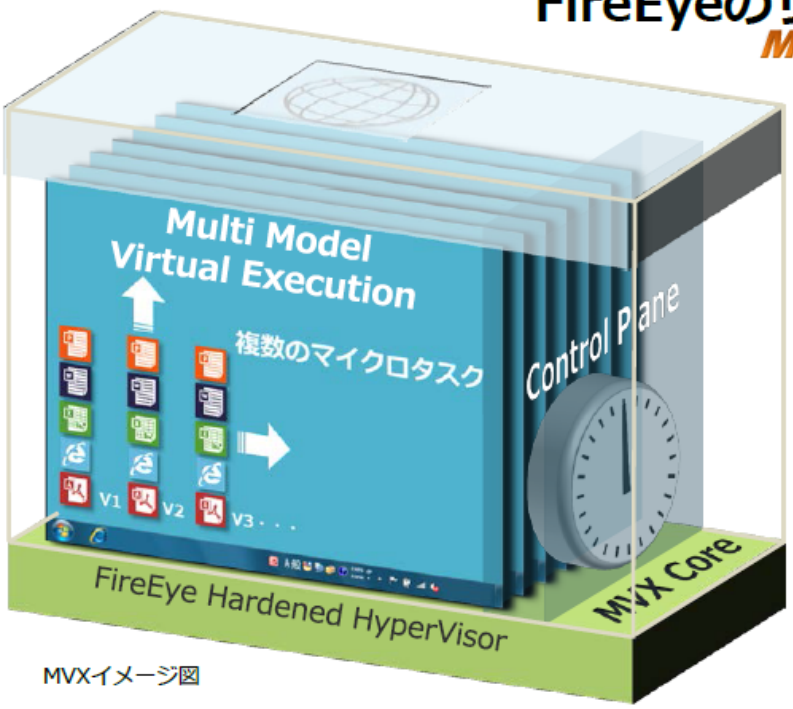
FUJITSU

ファイア・アイ
FireEye 脅威対策プラットフォーム

ファイア・アイ エヌエックス
FireEye NXシリーズ（Webトラフィック用脅威対策プラットフォーム）
ファイア・アイ イーエックス
FireEye EXシリーズ（E-mail用脅威対策プラットフォーム）

攻撃が複雑化・巧妙化する中、既存の対策手法では限界！

FireEyeのサイバー攻撃検知技術/MVX
Multi-Vector Virtual Execution



MVXイメージ図

創業時より標的型攻撃、ゼロディ攻撃対策に特化したソリューションを提供するFireEyeは、一般的なセキュリティ対策製品を回避するマルウェア、それを利用して行われるサイバー攻撃のわずかな痕跡も見逃しません。

FireEye™
なら
検知できます

独自の仮想技術
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。

2000パターンの実行環境
攻撃者が狙う特定のOS／アプリのバージョンに依存する脆弱性、その組み合わせを網羅。

ネットワーク、メモリ環境も再現
コールバック通信、メモリへの直接ロード等、複雑なマルウェアの脅威化プロセスを忠実に再現。

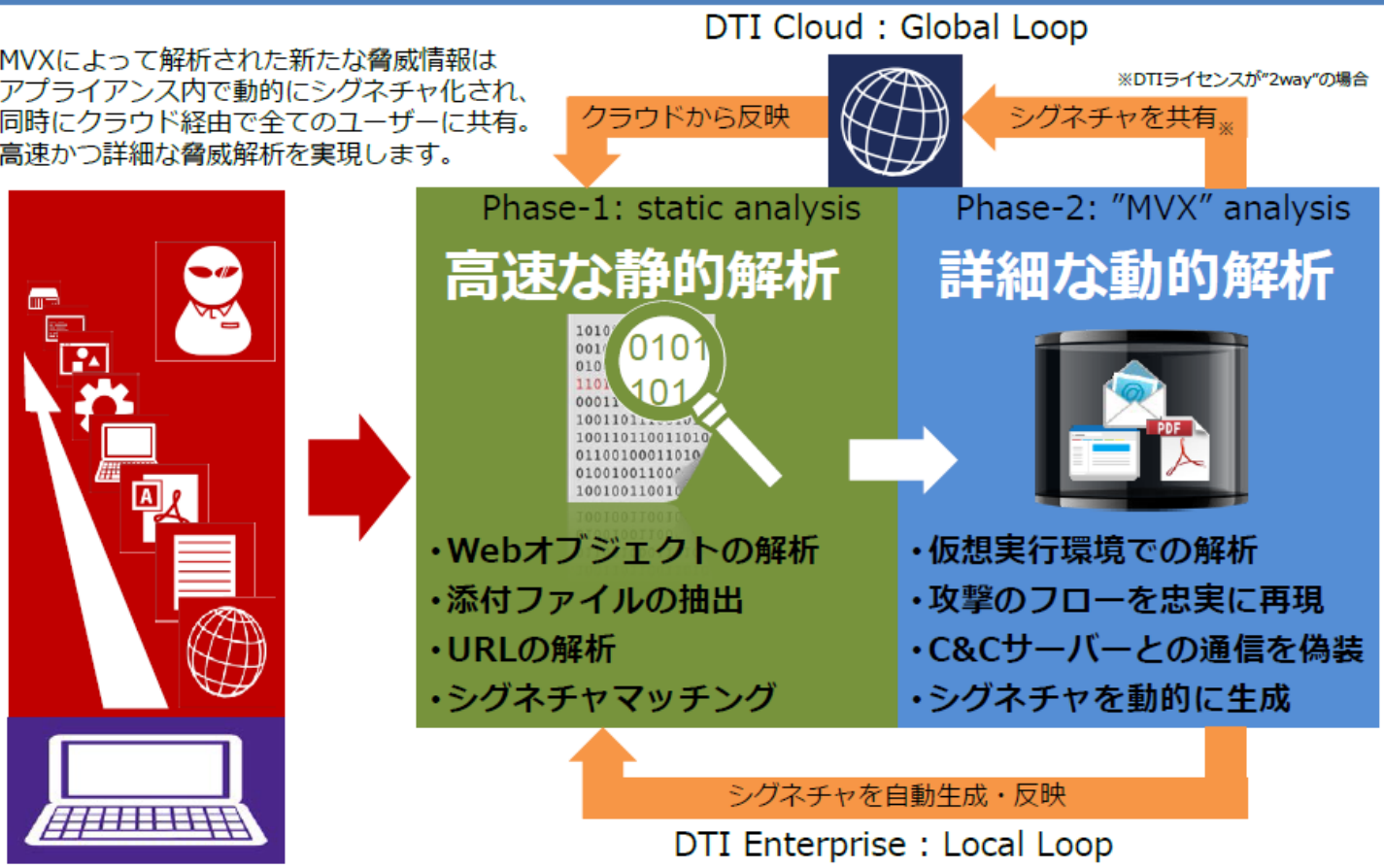
サンドボックス回避技術に対抗
発症遅延や多弾頭（ペイロード）方式等、マルウェアのサンドボックス回避技術を無効にします。

- **2012年8月以降、世界で発見された27のゼロディ攻撃のうち、18を発見**
- **リスク可視化サービスを利用した企業の95%で感染を確認**

shaping tomorrow with you

DTI(Dynamic Threat Intelligence)による脅威情報の共有・反映

MVXによって解析された新たな脅威情報は
アプライアンス内で動的にシグネチャ化され、
同時にクラウド経由で全てのユーザーに共有。
高速かつ詳細な脅威解析を実現します。



FireEye製品ポートフォリオ

NXシリーズ：Web

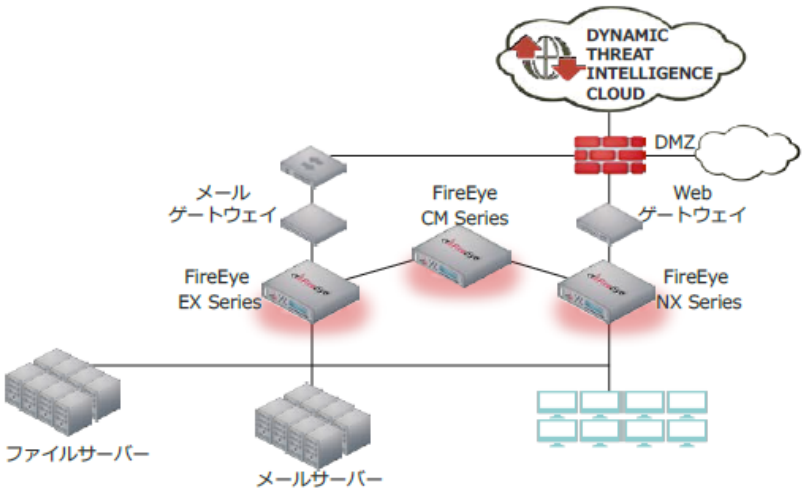
- Webトラフィック(HTTP)の入口対策
- すべての通信 (ポート不問) の出口対策

EXシリーズ：Mail

- E-mail (SMTP)の入口対策
- E-mailの添付ファイルを検査

CMシリーズ：Management

- NX/EX等各種装置の集中管理



製品・サービスについてのお問い合わせは
富士通コンタクトライン　0120-933-200　受付時間 9:00～17:30(土・日・祝日・当社指定の休業日を除く)
富士通公開サイト　http://jp.fujitsu.com　詳細はこちら http://fenics.fujitsu.com/products/ipcom/

FUJITSU

アプリケーションの可視化と制御を実現する次世代ファイアーウォール

Palo Alto Networks PAシリーズ

パロアルトネットワークスの次世代ファイアーウォールソリューション『PAシリーズ』は、これまでのポート番号やプロトコルベースのファイアーウォールでは不可能であった、「アプリケーション」、「ユーザ」、「コンテンツ」といったポリシーベースによる制御を実現します。

従来型ファイアーウォールの課題

ポート番号ベースでの制御を行う従来型のファイアーウォールでは、高度化したアプリケーションの制御と可視化が不可能である。また昨今の標的型攻撃への対策もなされていない

①アプリケーションの高度化
- アプリケーション開発者はファイアーウォールがポート番号ベースで制御することを前提に開発しているため簡単にファイアウォール越えが可能
- 動的なポートスキャン、80/443ポートの活用、暗号化を利用し簡単にファイアウォールを通過

②標的型攻撃
- 新たな脅威（未知のマルウェア）に対する対策がなされてない
- ボットネットに感染した端末を特定できない

従来型ファイアーウォールでは対応できない

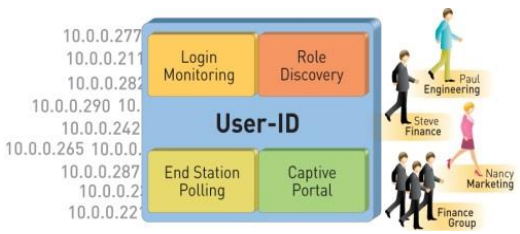
PAシリーズで解決

アプリケーション識別し制御（APP-ID™）

ポート番号、プロトコル、SSL暗号化に関わらず1800種類以上のアプリケーションを識別し制御と可視化を実現

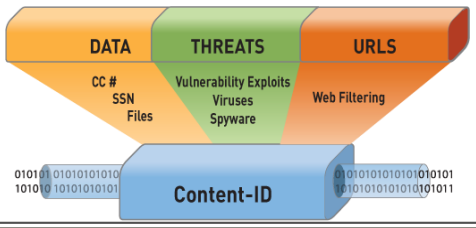
ユーザ識別し制御（User-ID™）

IPアドレスに関わらず、Active Directory 等と連携することによりユーザーの可視化と制御を実現



高度なコンテンツセキュリティを実現（Content-ID™）

アプリケーションに埋もれた脆弱性攻撃、情報漏えい、マルウェアやスパイウェア等の脅威、悪意あるサイトへの遮断などリアルタイムで防御



標的型攻撃への対策

昨今のサイバー攻撃の主流となっている標的型攻撃対策として活用可能

- WildFireによる標的型対策
  未知のウィルスの進入を防ぐ
- ボットネット対策
  ボットネットに感染している端末を早期に発見、防御

http://fenics.fujitsu.com/products/paloalto/

shaping tomorrow with you

社会とお客様の豊かな未来のために

PAシリーズは、昨今のサイバー攻撃の主流となっている**標的型攻撃**対策としても活用できます。

■ **WildFire による標的型攻撃対策**

仮想実行(サンドボックス)環境でプログラムを実行することにより振る舞いベースでマルウェアを検知。
迅速にシグネチャを生成、すべてのお客様のデバイスにシグネチャを配信し標的型攻撃へ対応。

■ **ボット感染端末を早期発見、防御**

振る舞いベースで未知のバックドア通信を検出し、毎日レポート。
不明なプロトコルやIRCなどの通信が多い端末をリストアップ。

※ 配信されるシグネチャはWildFire用のシグネチャとして配信されますが、翌日、脅威防御やURLフィルタリングのシグネチャやDBとして更新され、WildFire用のシグネチャからは削除されます。WildFireを利用する際は、脅威防御とURLフィルタリング(PAN-DB)と一緒にご利用下さい。

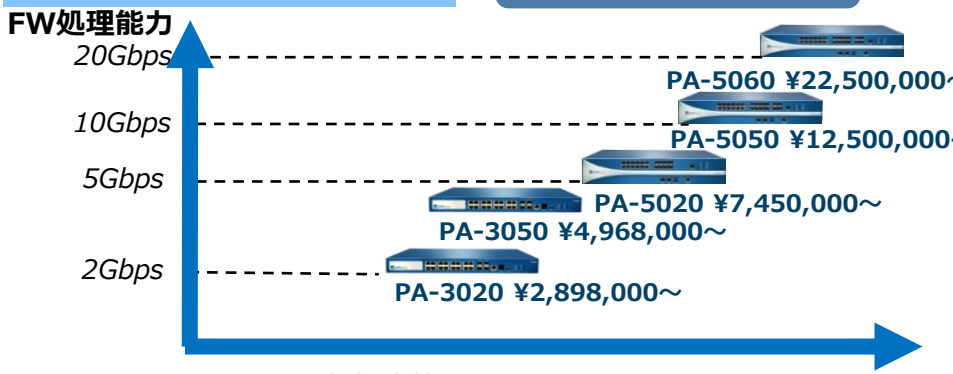
ボットネットレポート例

同じサイトから 48回
実行ファイルをダウンロード

Source address	Source User	Description
10.55.15.18	fujitsu/taro.fuji	Repeatedly (48) download excutables from the same unknown URL esysprotor.com/omni.gif
10.155.5.36	fujitsu/jiro.fuji	Repeatedly Visited (271) the same URL "72.246.170.26/."

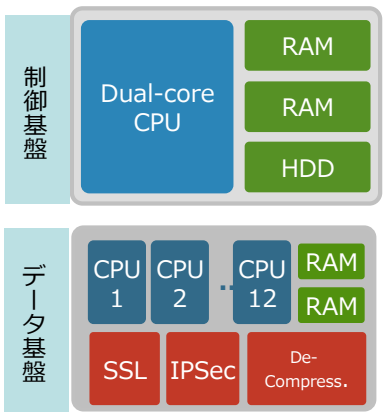
同じサイトに 271回ホスト名
ではなく、IPアドレスでアクセス

PAシリーズ　ラインナップ



専用設計されたハードウェア

次世代ファイアーウォールを 1から専用設計。制御基盤とデータ基盤を分離したアーキテクチャにより高速処理を実現



［価格例］

分類	製品名	標準単価	数量	標準合計	備考
PAシリーズ	PA-3020	¥2,898,000	2	¥5,796,000	FW処理能力　2Gbps、脅威防御　1Gbps、冗長（HA）構成
サブスクリプションライセンス	脅威防御	¥405,000	2	¥810,000	PA-3020用脅威防御ライセンス 1年・HA構成用（2台分）
	脅威防御	¥405,000	8	¥3,240,000	PA-3020用脅威防御ライセンス 1年・HA構成・更新用（4年×2台分）
	URLフィルタリング	¥405,000	2	¥810,000	PA-3020用URLフィルタリング（PAN-DB）ライセンス 1年・HA構成用（2台分）
	URLフィルタリング	¥405,000	8	¥3,240,000	PA-3020用URLフィルタリング（PAN-DB）ライセンス 1年・HA構成・更新用（4年×2台分）
	WildFire	¥405,000	2	¥810,000	PA-3020用WildFireライセンス　1年・HA構成用（2台分）
	WildFire	¥405,000	8	¥3,240,000	PA-3020用WildFireライセンス　1年・HA構成・更新用（4年×2台分）
合計				¥30,726,000	

お問い合わせ先

富士通コンタクトライン　0120-933-200

受付時間 9:00～17:30（土・日・祝日・当社指定の休業日を除く）

富士通公開サイト　http://jp.fujitsu.com

[PAシリーズ]の詳細はこちら http://fenics.fujitsu.com/products/paloalto/