FUJITSU

狙われる企業データを守る！
多層的なサーバセキュリティのご提案

セキュリティ事故や被害は増大しています

2014年標的型サイバー攻撃事例

時期	業種	従業員数	漏洩情報
2014年2月	大学(米国)	約9,000名	約29万件の学生、職員の個人情報
2014年2月	出版・通販(日本)	約270名	約1160件の顧客情報
2014年5月	オークション(米国)	約18,000名	約1億4500万人分の顧客情報
2014年7月	製造(日本)	約430名	約6万2,000件の顧客情報
2014年8月	小売(日本)	約170名	約900件の顧客情報
2014年8月	医療(医療)	約90,000名	約450万人分の患者情報
2014年9月	大学(米国)	約3,000名	約4,000名の学生の個人情報
2014年9月	航空(日本)	約10,000名	約19万件の顧客情報
2014年10月	金融(米国)	約260,000名	約8,300万人分の顧客情報
2014年11月	郵便(米国)	約800,000名	職員・顧客情報

2014年公表情報をもとにトレンドマイクロが調査

情報流出時の被害は甚大です

セキュリティ事故が発生した場合の平均想定損害賠償額・・・
1億926万円！*

*:日本ネットワークセキュリティ協会
「2013年 情報セキュリティインシデントに関する調査報告書」より引用

近年の脅威と対処例は？

IPAの「セキュリティ10大脅威2015」で報告された上位3位と対処例

攻撃者は愉快犯ではなく、金銭取得を目的として、クレジットカード情報や個人情報、企業の重要な機密情報をターゲットにしています。

1 「インターネットバンキングやクレジット情報の不正利用」
クレジットカード情報の窃取や、POS端末感染の増加
⇒対処例：ソフトウェア更新、ウイルス対策ソフト導入など

2 「内部不正による情報漏えい」
正規アクセス権限を持つ職員が、情報持ち出し
⇒対処例：システム操作の記録と監視など

3 「標的型攻撃」
標的企業・組織のウイルス感染したパソコンを遠隔操作、情報を外部に送信
⇒対処例：機密情報を内部で「多層防御」

	情報セキュリティ10大脅威2015
1	インターネットバンキングやクレジットカード情報の不正利用
2	内部不正による情報漏えい
3	標的型攻撃による諜報活動
4	ウェブサービスへの不正ログイン
5	ウェブサービスからの顧客情報の窃取
6	ハッカー集団によるサイバーテロ
7	ウェブサイトの改ざん
8	インターネット基盤技術を悪用した攻撃
9	脆弱性公表に伴う攻撃
10	悪意のあるスマートフォンアプリ

「情報セキュリティ10大脅威 2015」
独立行政法人　情報処理推進機構(IPA) 2015年3月

最終的には、サーバにある重要な企業データが狙われます。
標的の環境を入念に事前調査し、従来型のウイルス対策だけでは検出できない
標的毎にカスタマイズされた攻撃が増える中、新しい対策も求められています。

サーバに必要な対策

パターンマッチングだけでない、多層的なサーバ防御

➢ 入口の対策
ネットワーク経由で脆弱性を狙う攻撃に対処

➢ 内部の対策
従来のウイルス対策に加えて、変更監視/セキュリティログ監視により、攻撃予兆や不正の証跡を把握

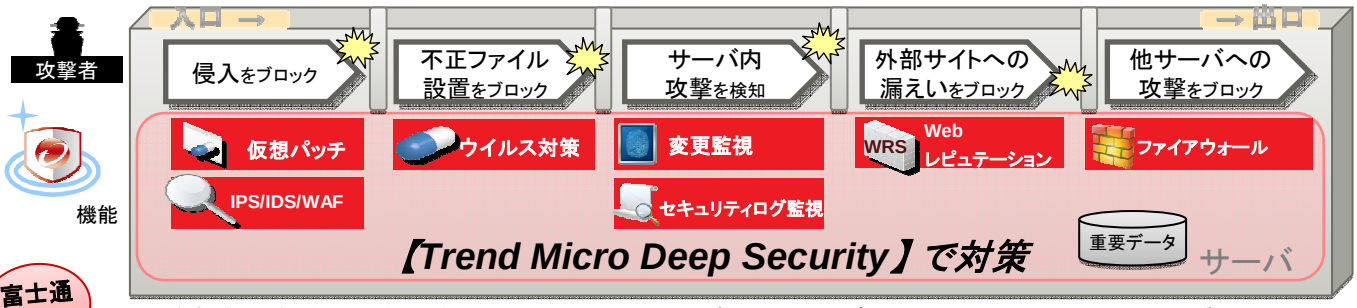
➢ 出口の対策
機密情報の送信や別サーバへの攻撃拡大に対処

多層の防御

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

概要

サーバ攻撃の入口から出口までの各レイヤで、防御機能を提供



富士通なら

仮想パッチ：脆弱性への攻撃コードをネットワークのパケットレベルでブロック　**Webレピュテーション**：不正な外部サイトへの通信をブロック

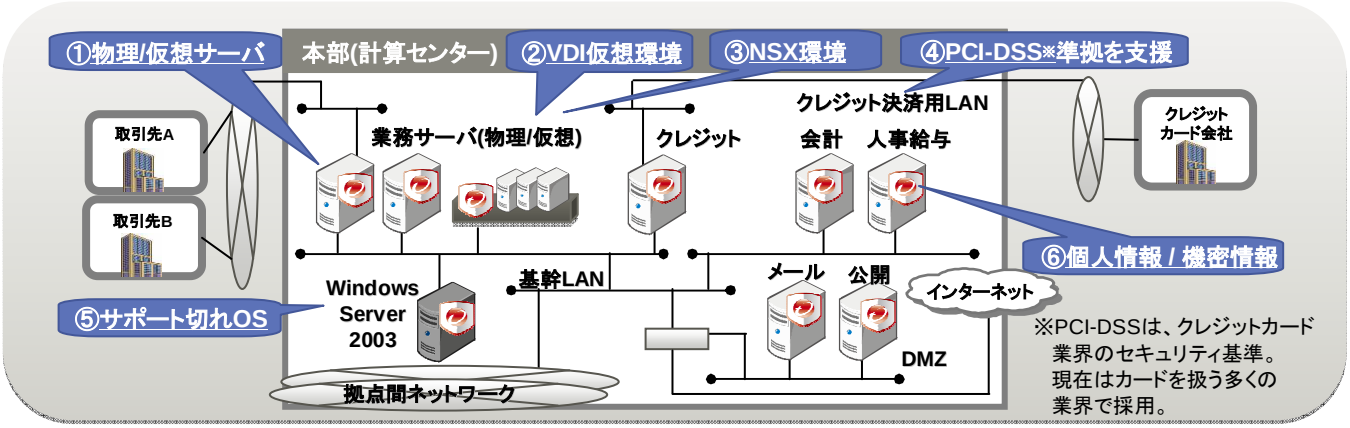
サポート：**富士通 SupportDesk**に対応、ハード、OSからアプリケーションまで、ワンストップのサポート対応
クラウド：**FUJITSU Cloud IaaS Trusetd Public S5/FUJITSU Cloud IaaS Private Hosted A5+**のオプションでも提供
実　　績：金融、製造、流通、自治体、保険、医療をはじめとした**各種業種のお客様に採用実績**あり

活用シーン

Deep Security 6つの「できる」で、さまざまなシーンに適用が可能

できる

①**物理/仮想**をまとめて共通ポリシーで対策 できる！
②**VDI**含めた**仮想環境**をエージェントレスで対策 できる！
③**VMware NSX**と連携、感染した仮想マシンを自動隔離 できる！
④**PCI-DSS**要件に多数対応、認定取得の負担を軽減 できる！
⑤**サポート切れOS**に、仮想パッチで脆弱性対策を実現 できる！
⑥FW/IDS/WAFにより**個人情報 / 機密情報**を保護 できる！



価格例

Deep Security Advance　導入ケース　(物理サーバ5台への対策を想定)

製品名	単価	数量	金額
Deep Security Advance	¥213,500	5	¥1,067,500
Deep Security SupportDesk	-	-	¥106,200
PRIMERGY RX2520 M1[Deep Security 管理サーバ用]※1	¥972,680	1	¥972,680
Microsoft SQL Server 2014 Standard	オープン価格	1	オープン価格
Deep Security 導入サービス※2	個別見積	-	-
合計			¥2,146,380

※1 管理サーバはPRIMERGY RX2520M1 [型名PYR2521R3N](CPU：インテル® Xeon®プロセッサーE5-2403v2 [1.80GHz] 、メモリ：20GB、HDD：300GB)を想定しています。
　価格にOS価格、CAL価格は含まれておりません。
※2（参考）Deep Security導入サービスのサービスメニュー例（作業内容等）については、次のURLからご確認いただけます。http://jp.fujitsu.com/group/fst/services/deepsecurity/

補足

・サポート切れOSの延命選択はお客様責任となります。また、Windows Server 2003用仮想パッチの配信は2017年12月末までとなります。
・価格例に記載の価格は標準価格となります。管理対象のサーバ本体価格は含んでおりません。
・Deep Security製品およびSDKの価格は初年度価格であり、次年度以降は更新費用が必要となります。
・今後、価格の変更、仕様の変更、バージョンアップ等により、内容の全部もしくは一部に変更が生じる可能性があります。
・各社の社名、製品名、およびサービス名は、各社の商標または登録商標です。

お問い合わせ先

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
http://jp.fujitsu.com/