環境活動

「ISO14001」取得

2000 年 3 月、環境マネジメントシステムに関する国際規格である「ISO14001」を取得

品質保証活動

「ISO9001」取得

1995 年 5 月、品質管理マネジメントシステムの国際規格である「ISO9001」を取得

「ISMS 適合性評価制度 ISO27001」取得

2005 年 4 月に製品保守サービスの分野にて、2007 年 3 月にアウトソーシングサービスの分野にて、
情報セキュリティマネジメントシステム(ISMS)の国際規格である「ISO27001」を取得

「プライバシーマーク認定」取得

2006 年 8 月、個人情報の取り扱いについて、適切な保護の体制を整備している事業者に対し付与する
プライバシーマーク認定である「JIS Q 15001」を取得

「ITSMS 適合評価制度 ISO20000」取得

2007 年 12 月から順次、全国 LCM サービスセンターと各種運用サービス実施部門にて、
国際規格「ISO / IEC 20000・JIS Q 20000」を取得

「事業継続マネジメント ISO22301」取得

2012 年 8 月、保守サービス事業において事業継続マネジメントシステムの国際規格「ISO22301」の第三者認証を世界で初めて取得

株式会社富士通エフサス

〒211-0012　神奈川県川崎市中原区中丸子13-2　野村不動産武蔵小杉ビルN棟
0120-860-242　http://www.fujitsu.com/jp/fsas/

●お問い合わせ

FSAS-114-1・100 HK 15.6 TS　2015年6月

FUJITSU

富士通エフサス
セキュリティソリューションカタログ

shaping tomorrow with you

社会とお客様の豊かな未来のために

セキュリティ事故被害 が多数発生しています。
危険は身近なとこ ろに潜んでいます。

被害に遭われた企業／団体は、セキュリティ対策をしていなかったわけではありません。
しかしICTシステムの多様化、サイバー攻撃の日々の巧妙化により、被害に遭ったことに気付きにくくなっています。
ようやく気付いた時には被害が拡散… ということが身近に起こっています。

標的型メールの増加

攻撃者はまずターゲットの関連会社パソコンを標的型メール攻撃で乗っ取り、次にそのパソコンを足掛かりに真のターゲットから機密情報を盗みました。間接攻撃により、**調査に多大な時間と費用がかかりました。**

不正サイト閲覧

ドメイン名登録情報の不正な書き換えによる「ドメイン名ハイジャック」が発生し、当該サイトにアクセスした利用者が**不正なサイトに誘導され、ウイルス感染**する事態が複数発生しました。

不正アクセス

Webサイト改ざんは**組織の規模、業種に関わらず**行われています。Webサイトの一時的な閉鎖などにより**被害総額が1億円**に上った企業の事例もあります。

スマートデバイス向け不正アプリ

「バッテリーを長持ちさせる」とうたう無料アプリが、実は「不正アプリ」であることも。インストールした時点で電話番号やメールアドレスなどの**個人情報**や**社内の機密情報が盗まれる**被害が急増しています。

不正利用

内部関係者の**故意による情報持ち出し**は、一回に持ち出す量が他の方法による流出量よりもはるかに多いという結果が出ています。ひとたび情報が流出すると、企業が受けるダメージは計り知れません。

進化し続けるサイバー攻撃には、 ICTシステムによる防御に加え、
導入後の最新化や異常を早期に とらえる日々の運用が重要です。

身近に潜むリスク

偽装して内部に入り込む「標的型攻撃」

攻撃パターン1:偽装メール

関係者や関連業者を装い、利用者を信用をさせ添付ファイルを開かせます。

攻撃パターン2:偽サイト

巧妙な手口で、偽サイトへのアクセスを促します。

攻撃パターン3:不正アクセス

仕掛けられたウイルスにより、攻撃者は利用者になりすまし不正アクセスを行います。

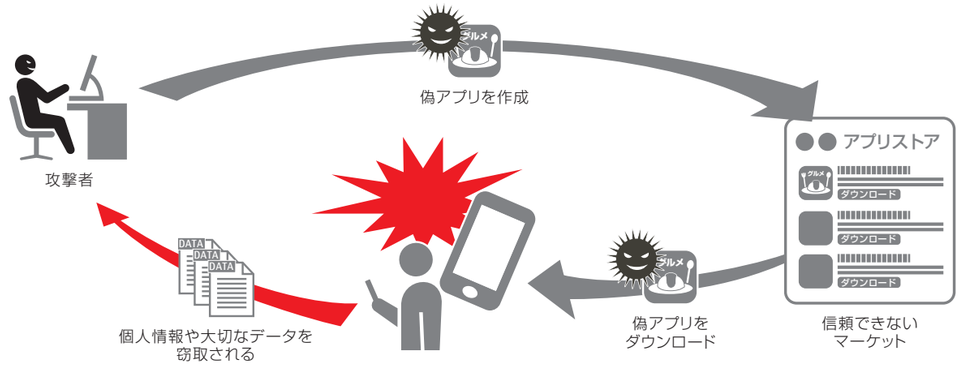
入れない(入口対策)・広めない(内部対策)・流出させない(出口対策)

⚠ 標的型攻撃対策 → P5~6

スマートデバイスからの「ウイルス感染」

スマートデバイス向け不正アプリの手口

魅力的な機能を持っていると見せかけた不正アプリで、電話帳等の情報が窃取される被害が増加しています。



情報機器は全てターゲット。不正アプリによる情報窃取を防ぐ

⚠ スマートデバイス対策 → P7~8

システムの不正利用による「情報漏えい」

不正利用の手口

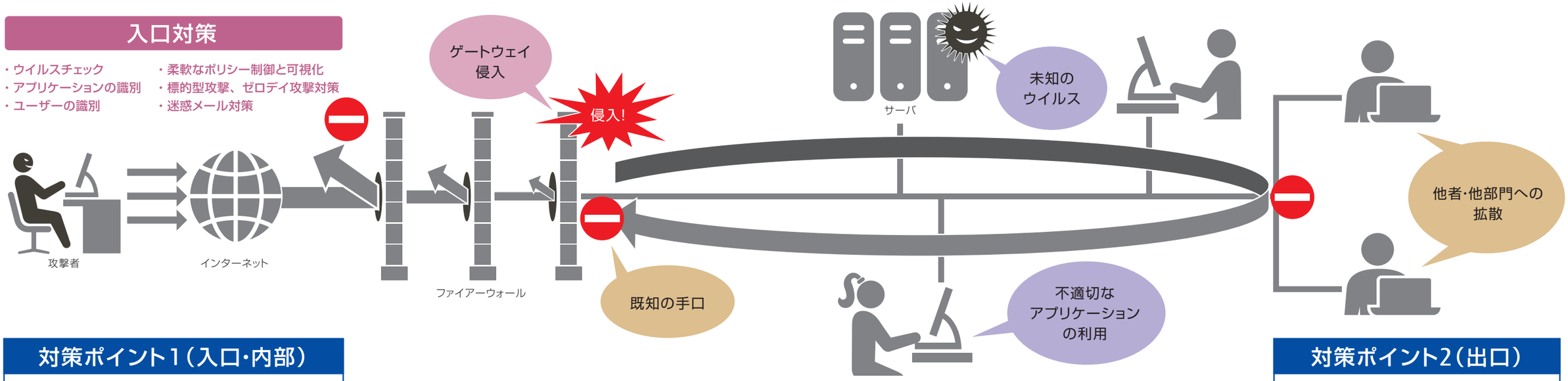
社員や職員等による個人情報や技術情報の漏えい被害が増加しています。

脅威は外部侵入者だけじゃない。社内の不正を未然に防ぐ

⚠ システムの不正利用対策 → P9~10

こんな対策があります

標的型攻撃に対する有効な対策として、外部から社内システムに「入り込む」部分についての対策（入口対策）はもちろん、社内に侵入された場合も不正な潜伏活動をいち早く見つけ、拡散を防ぐ対策（内部対策）を講じることが重要になってきました。さらに、万が一侵略した脅威が発動した場合でも、外部への情報流出などの最悪の事態を防ぐ対策（出口対策）も必要になってきています。



対策ポイント1（入口・内部）

①ゲートウェイでの侵入防止
②未知のウイルスの侵入を早期検知
③アプリケーションレベルでのアクセス制御

対策ポイント2（出口）

④脆弱性の排除
⑤侵入を前提とした蔓延防止
⑥持ち出しを前提としたデータ保護

入口・内部対策

有効な製品

次世代ファイアーウォール

・アプリケーションの識別
・柔軟なポリシー制御と可視化

PaloAlto PAシリーズ
（パロアルトネットワークス）

WatchGuard XTM
（ウォッチガード）

FortiGate UTM
（フォーティネット）

ふるまい検知

・脅威を検知/自動分析

Deep Discovery Inspector
（トレンドマイクロ）

検疫

・脆弱性チェック

iNetSec Smart Finder
（PFU）

サービス

◆次世代ファイアーウォール運用サービス　PAシリーズ　WatchGuard　FortiGate

防御の「穴」をすり抜け情報を持ち出す攻撃を検出・防御します。

参考価格 3万円/月額（WatchGuard）

◆ウイルスふるまい検知サービス　Deep Discovery Inspector

既知未知を問わずシステム内部に入り込んで潜伏する不正な活動を検出・分析します。

参考価格 50万円～/月額（スタンダード運用サービス）

◆相関ログ分析サービス

システム各所のログを収集/相関分析し、顕在化していないリスクの予兆を調査・監視します。

参考価格 40万円/月額（センサー機器2種類）

出口対策

有効な製品

情報漏えい防止

・自動暗号化

Rightspia® for Secure Documents
（富士通エフサス）

・Webフィルタリング

i-FILTER
（デジタルアーツ）

ITポリシー管理

IT Policy N@vi
（富士通システムズ・ウエスト）

ウイルス対策

・ウイルスの侵入検知、拡散防止、駆除

SubGate
（ハンドリームネット）

Trend Micro Portable Security
（トレンドマイクロ）

Trend Micro Deep Security
（トレンドマイクロ）

サービス

◆ウイルス拡散防止サービス　SubGate　TMPS

感染発覚時、セキュリティエキスパートがお客様に通報し、早期の対処を支援します。

参考価格 2万円～/月額

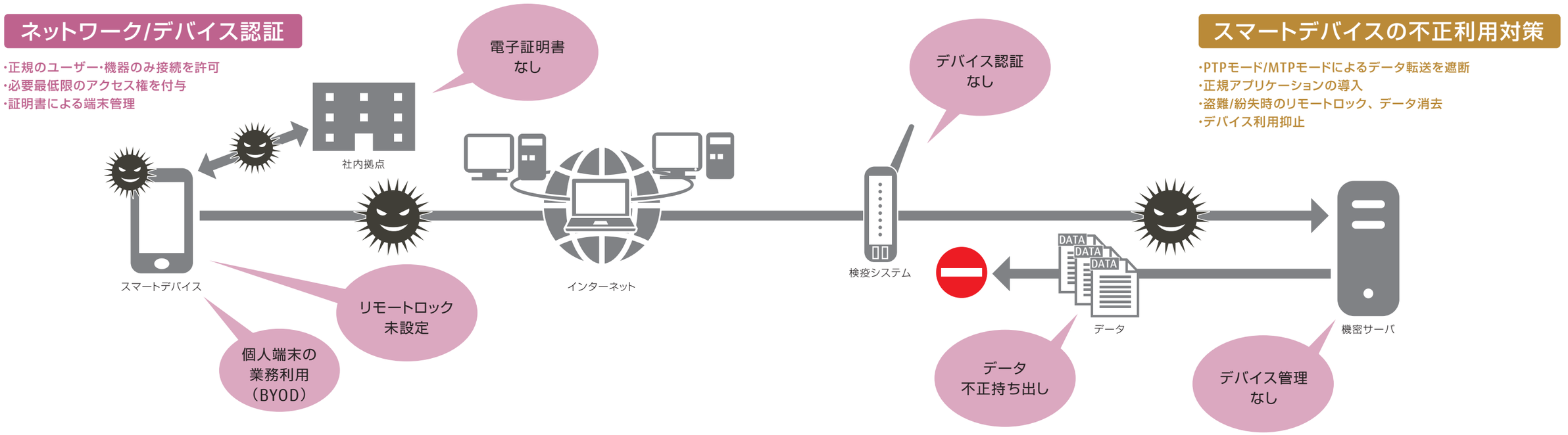
◆イントラネットゾーンスキャンサービス

イントラネットサーバの脆弱性の有無をチェックし、今後の対策をわかりやすくまとめた診断書を送付いたします。

参考価格 9万円/1IP～

こんな対策があります

近年、加速的に普及しているスマートデバイス（スマートフォンやタブレット）ユーザーをターゲットに、個人情報を収集する手口がより巧妙化しています。また、個人のスマートデバイスを業務活用（BYOD）している企業も増えてきており、セキュリティ対策の必要性が高まってきています。



対策ポイント

①正規デバイスの認証、接続許可　②デバイス紛失時の適切な対処　③不正利用の阻止

BYODがもたらす危険

BYOD（Bring your own device）とは、従業員が個人所有のスマートデバイスをオフィスに持ち込み、業務活用することです。企業にとっても業務用の端末を全従業員に用意することに比べ、機器導入コストや通信料等の経費を大幅に抑えるメリットがあります。
しかしながら、企業管理品と異なり、セキュリティ対策が個人の裁量に任されているため、紛失や盗難に対するリスクが高いこともまた特徴です。

スマートデバイスのセキュリティ対策

有効な製品

操作制限

・デバイス利用抑止
FUJITSU Software Portshutter Premium
（富士通ソフトウェアテクノロジーズ）

・資産管理
SKYSEA Client View
（スカイ）
Systemwalker Desktop Patrol
（富士通）
Systemwalker Desktop Keeper
（富士通）

検疫

・脆弱性チェック
iNetSec Smart Finder
（PFU）

SSLクライアント証明

セコム電子証明書
（セコムトラストシステムズ）

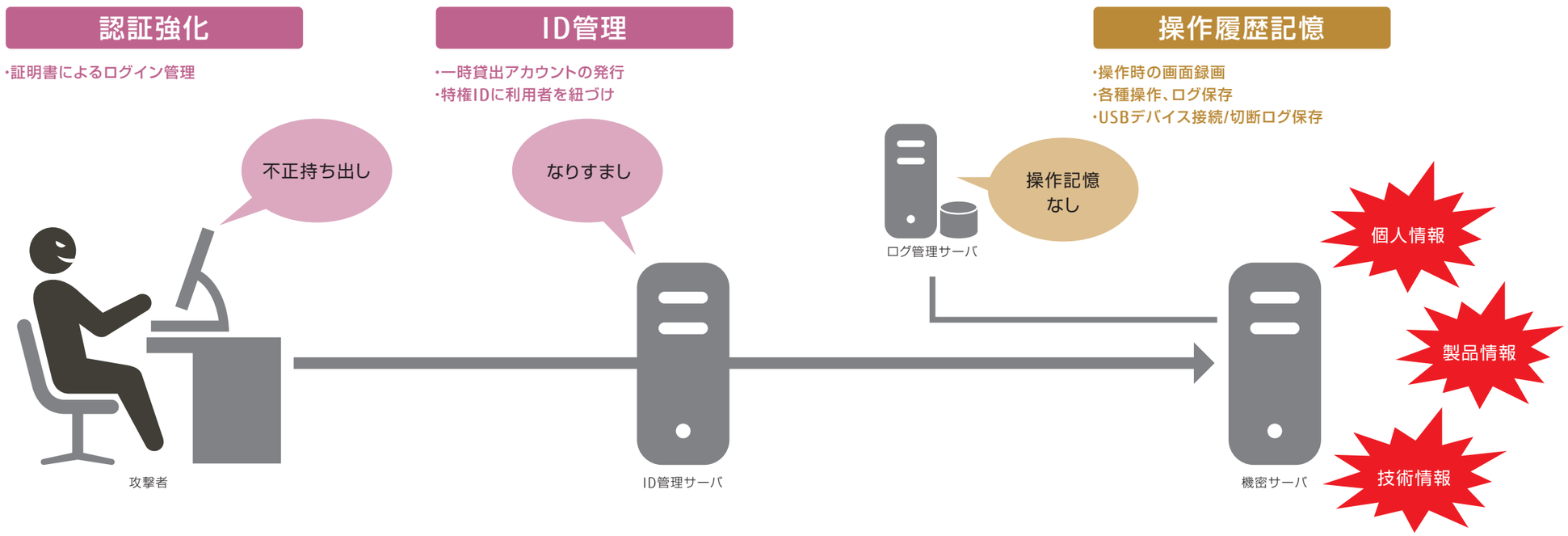
サービス

◆スマートデバイス-LCMサービス
端末・回線の月額サービス提供から、社内ネットワークへのリモートアクセス、端末のセキュリティ・コントロール、利用者サポートまで、ワンストップでご提供いたします。
参考価格 25.2万円～/月額

◆FENICSⅡユニバーサルコネクト／ビジネスWi-Fi
スマートフォン、タブレットやパソコンといった様々な端末とお客様イントラ内をセキュアに接続するネットワークサービスです。
参考価格 2万円～/月額

こんな対策があります

社員や職員等によって顧客情報が不正に売られたことによる個人情報の大量漏えいや、製品情報が退職の際に不正に持ち出されたことによる技術情報の漏えいの被害が増加しています。



対策ポイント

①認証の強化　②特権IDの管理・操作履歴の保存　③操作ログの確認

特権IDとは?

特権IDとは、アカウントの新規作成や更新、抹消などの設定が唯一行える特別な権限を持つIDをいいます。システムに対するあらゆる操作が可能な反面、少しの操作ミスが命取りになり、また悪意のある者に使われれば被害は甚大であり、情報漏えいから破壊や機能停止まで、あらゆる危険にさらされることになります。
そのような課題を解決するソリューションを「特権ID管理」といいます。特権IDと作業者を紐づけた一元管理によって、作業者の特定や証跡管理などが確実に可能となります。

不正利用対策

有効な製品

特権ID認証
・証跡管理
FUJITSU Security Solution SHieldWARE NE
（富士通ソーシアルサイエンスラボラトリ）
ESS REC
（エンカレッジ・テクノロジ）

SSLサーバ証明
セコム電子証明書
（セコムトラストシステムズ）

認証強化
Secure Login Box + SMARTACCESS
（富士通）　（富士通）

証跡強化（操作記録）
SKYSEA Client View
（スカイ）
Systemwalker Desktop Patrol
（富士通）
Systemwalker Desktop Keeper
（富士通）

サービス

◆相関ログ分析サービス
システム各所のログを収集し、顕在化していないリスクの予兆を調査・監視します。

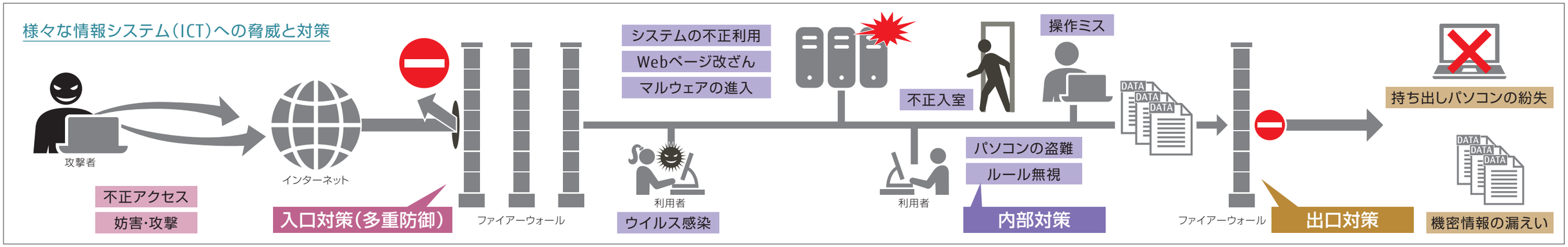
参考価格 40万円～/月額
（センサー機器2種類）

こんな調査を行います
・アンチウイルスログ、サーバログ、ファイアーウォールログを時系列で相関
　⇒マルウェア感染による情報流出の確認
・ファイアーウォールログと業務時間設定で相関
　⇒ボット感染による情報流出の確認

エフサスセキュリティMAP

安心の　可視化

現状評価　　各種認　証取得　　ポリシー策定



入口対策

不正アクセス対策

- ファイアーウォール
- 不正侵入検知
- 検疫
- Webアプリ防御
- 改ざん検知

ウイルス・スパム対策

- ウイルス侵入防止
- スパムメール防御

アクセスコントロール

- ID統合管理
- 特権ID管理
- 認証強化
- 入退室管理

内部　対策

ポリシー運用

- 各種認証維持
- 資産管理
- パッチ配布・自動適用
- 教育

ウイルス対策

- クライアントウイルス対策
- サーバウイルス対策
- ネットワークのウイルス対策
- ウイルスのふるまい検知
- 閉域網のウイルス対策

出口対策

データ保護

- デスクトップ仮想化
- 保存データ暗号化
- メールデータの保護
- データ消去
- ネットワーク暗号化

ポリシー運用

- 操作制限
- Webフィルタリング

ウイルス対策

- ウイルス漏出防止
- 不正な外部通信の検知

有効性　の確認

アタックテスト　　Webアプリケーション診断　　ログ解析　　不正アクセス監視　　個人情報探査

◆その他のソリューション

富士通エフサスは様々なセキュリティソリューションをご提供しています。

インターネットゾーンスキャンサービス　公開ゾーンへの外部からの不正アクセスに対する脆弱性を診断します。

選べる診断サービス　ネットワーク品質やセキュリティ強度を、様々な角度から健康診断いたします。

セキュリティ運用サービス　セキュリティエキスパートが、お客様システムのセキュリティ監視・運用支援などを行います。

ファイアーウォールログ解析　セキュリティエキスパートがファイアーウォールログを解析いたします。

◆セキュリティ対策診断 <無償版>

セキュリティMAPにおける各対策の推進度をグラフ化し、自社の対策に偏りがないかご確認いただけます。
実施のご要望の際には、富士通エフサス営業までお声かけください（無償：診断結果はグラフのみの提供です）。

導入事例

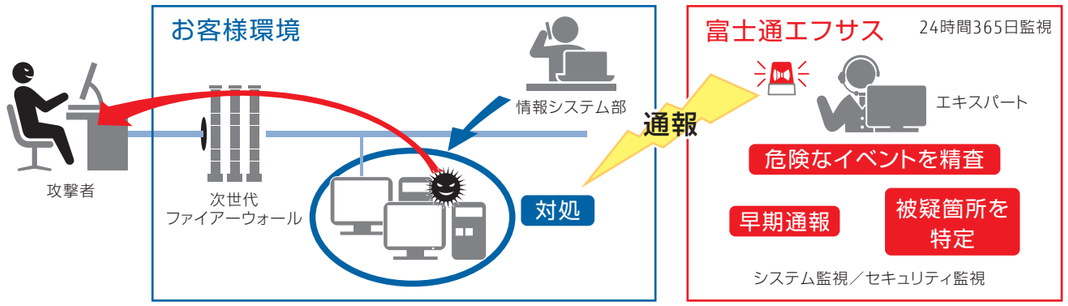
事例① A社様　比較的強固なセキュリティ対策を独自に実施しているお客様

課題　次世代ファイアーウォール装置に対し、入口対策だけではなく、出口対策も強化したい。

導入サービス

「次世代ファイアーウォール運用サービス」をご提案。

既存サービスとして、サーバおよびネットワークのシステム監視を実施しており、
次世代ファイアーウォールの“セキュリティ運用サービス”も24時間体制で対応可能。
▶システム動作異常時（ハード故障等）のサーバやネットワークに対する調査から、
不正アクセス（Dos攻撃等）の脅威に備えたセキュリティ対策までトータルでサポートします。



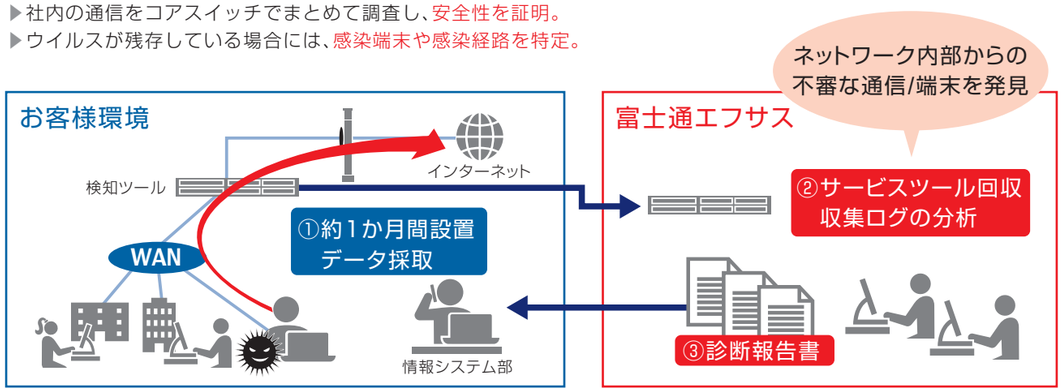
事例② B社様　過去、自社端末がサイバー攻撃の踏み台に使われてしまったことがあるお客様

課題　被害後、端末を初期化して対応したが、原因究明はできていないままで不安。

導入サービス

「ウイルスふるまい検知サービス」をご提案。

過去のインシデント経験では、外部から通報を受けるまで感染に気付けなかった。
▶社内の通信をコアスイッチでまとめて調査し、安全性を証明。
▶ウイルスが残存している場合には、感染端末や感染経路を特定。



高度なスキルの習得に向けた資格取得

業界基準となっている技術資格を取得し、最先端の技術を修得

- **富士通セキュリティマイスター**（セキュリティ）　**36名**
- **トレンドマイクロ認定資格**（セキュリティ）
  - TCSE for TMDS　**82名**
  - TCSE for ウイルスバスター コーポレートエディション　**40名**
- **CCIE**（ネットワーク）　**29名**
- **CCNP**（ネットワーク）　**223名**
- **DRII**（事業継続）　**20名**
- **BCADO認定資格**（事業計画）　**77名**
- **ITコーディネーター**（コンサルティング）　**82名**
- **情報処理技術者資格**
  （ITサービスマネージャー、プロジェクトマネージャー、システム監視技術者、情報セキュリティ、データベース、ネットワーク　他）　**99名**

2015年4月末現在 当社グループ社員(出向含む)全体

本カタログへの掲載にご協力いただいたパートナー様

- ウォッチガード・テクノロジー・ジャパン株式会社
- エンカレッジ・テクノロジ株式会社
- Sky株式会社
- セコムトラストシステムズ株式会社
- デジタルアーツ株式会社
- トレンドマイクロ株式会社
- パロアルトネットワークス合同会社
- ハンドリームネット株式会社
- フォーティネットジャパン株式会社
- 株式会社富士通システムズ・ウエスト
- 株式会社富士通ソーシアルサイエンスラボラトリ
- 株式会社富士通ソフトウェアテクノロジーズ