FUJITSU THE POSSIBILITIES ARE INFINITE

2009年度システム技術分科会第2回会合

ネットワークセキュリティへの取り組み

2010年1月20日

富士通株式会社
ネットワークサービス事業本部
プロダクト企画事業部
天満 尚二

ネットワークセキュリティの現状

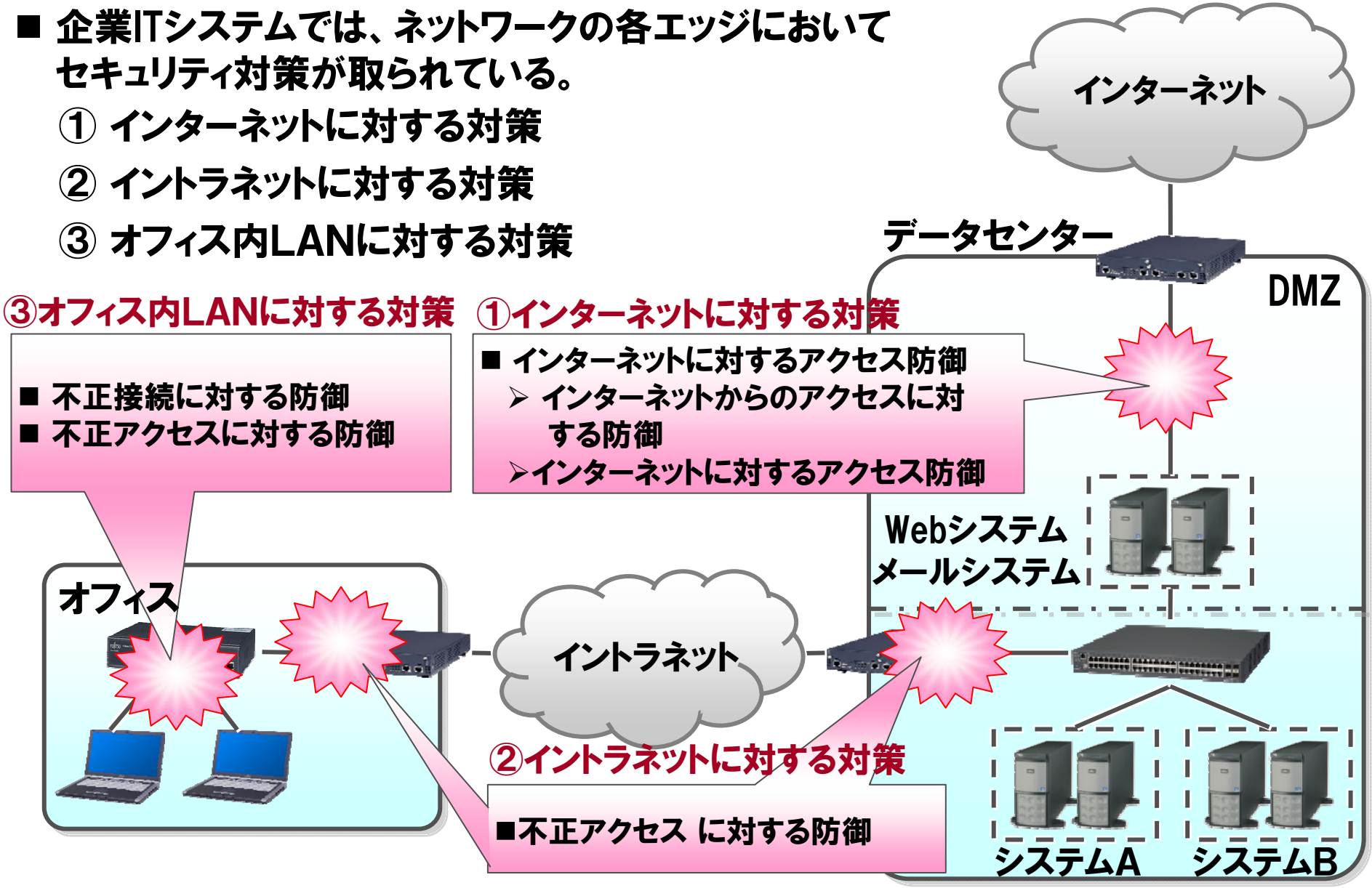
FUJITSU

■ 企業ITシステムでは、ネットワークの各エッジにおいて
セキュリティ対策が取られている。

① インターネットに対する対策

② イントラネットに対する対策

③ オフィス内LANに対する対策



① インターネットに対する対策
② イントラネットに対する対策

※イントラネットの対策の基本は、
インターネットに対する対策と同じ。

インターネットからの脅威

FUJITSU

インターネットを有効活用する場合に、さまざまな脅威が存在する

各種情報サイト・サービス

業務システム

社内システム
対する脅威

不正侵入

情報漏洩（P2P）

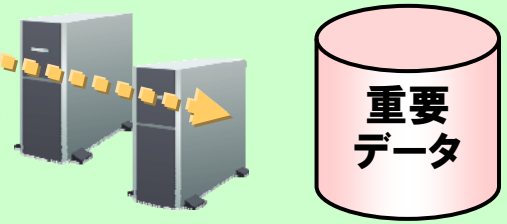
ウィルス侵入

有害なWebサイト

社内ネットワーク

利用者

顧客向けサービス



公開システムに
対する脅威

Webサイト改ざん

情報搾取

インターネット

公開サーバ

今までの対策と当社の取り組み

FUJITSU

項	機能		概要	富士通の取り組み
インターネットからの不正なアクセスを防御				
1	ファイアーウォール		外部との境界を流れるデータを監視し、不正なアクセスを検出・遮断	DoS/DDoS攻撃を防御するアノマリ型IPS機能を提供
2	IPS	アノマリ型（振る舞い検知型）	ワームやサービス拒否攻撃（DoS）などのパケットの特徴的なパターンを記憶し、該当する接続を検知、遮断し、管理者へ通知・ログ	
		シグネチャー型（パターンチェック型）		アンチウィルスの一部機能までカバー
3	アンチウィルス		予め用意されたウイルス検知パターンとファイルを比較し、検出	パターンマッチング方式とヒューリスティック方式の両方をカバー
インターネットへの不正なアクセスを防止				
4	Webコンテンツフィルタ		Webページの内容をチェックし、有害と思われるページへのアクセスを防止	プロキシモード、透過プロキシモード、完全透過モードの3方式を提供
通信データの改竄・盗み見防止				
5	VPN	IPsec	IPパケットや情報を暗号化して送受信	パスMTUディスカバリ機能でパスMTU問題を回避して確実な通信を実現
		SSL		

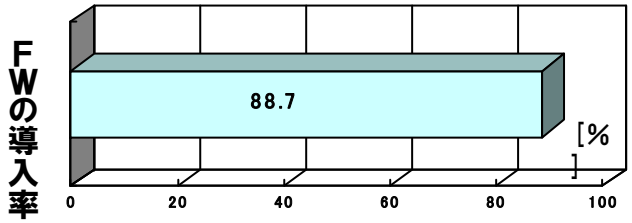
ファイアーウォールのみでは安全ではない！

FUJITSU

システム停止や情報漏洩の原因となる脅威に対する対策状況は？

9割以上の企業はファイアーウォールを導入

出展：警察庁生活安全局情報技術犯罪対策課



企業における情報セキュリティ実態調査2008
（NRIセキュアテクノロジーズ株） でも
96%の企業がファイアーウォールを導入済と回答

Webサイトを改ざん・侵入
して情報搾取する事件が急増

FWを設置しているのに、なぜ問題が発生したんだ？

インターネットに対するセキュリティ対策は、
ファイアウォールのみでは安全ではない！

更に上位レベルの対策が必要

UTMの浸透率は
30%程度
と言われています

Webアプリケーションへの脅威が増加

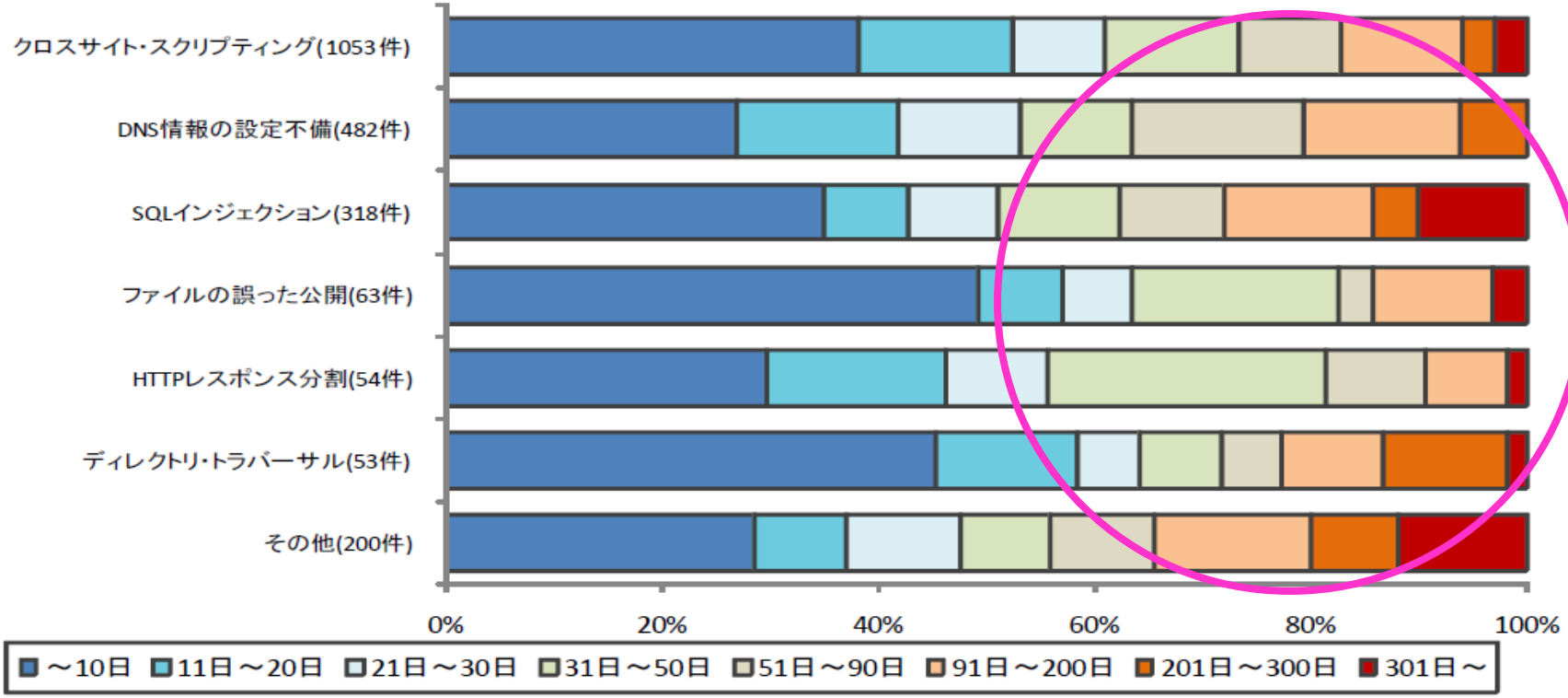
FUJITSU

■ 攻撃の増加

クロスサイトスクリプティングやSQLインジェクションなど、Webアプリケーションをねらった攻撃が増加

■修正に時間がかかる

SQLインジェクションなどWebアプリケーションの脆弱性は修正に時間がかかる



※出展:IPA 独立行政法人 情報処理推進機構

ウェブサイトの修正に要した日数の傾向

WAFで費用を抑えて大きな効果

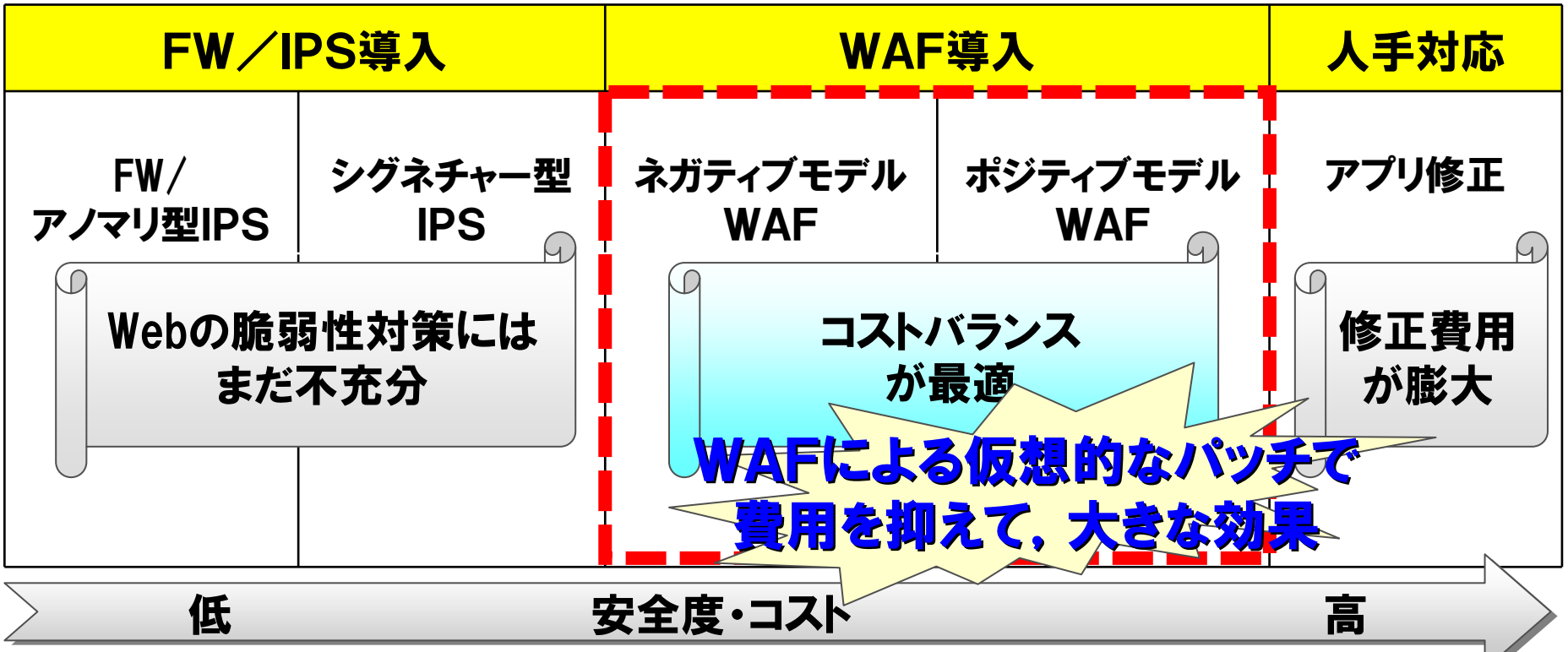
FUJITSU

Webアプリケーションの脆弱性対策

本来は、アプリケーション修正が望ましいが…

・アプリケーションの複雑化／増大化により**修正コストが莫大**

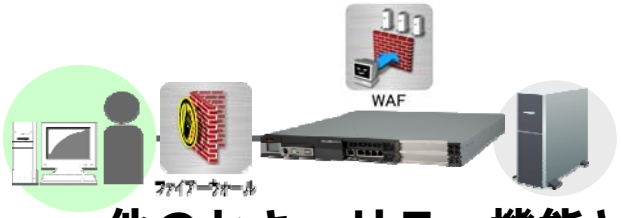
防御手段



IPCOMによるWAFに対する取り組み

FUJITSU

■ 多彩な利用形態



他のセキュリティ機能と
合わせて利用

ロードバランス機能と
合わせて利用

セキュリティ機能、
ロードバランス機能と
トータルに利用

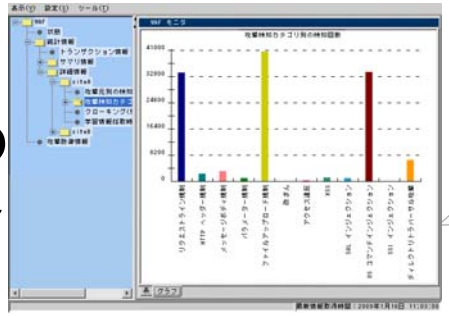
■ スケーラブルに利用

通信量など、成長に合わせ追加導入

装置追加で処理量向上

■ 容易な運用性

学習機能を利用し、
状況の解析、設定の改善などの
容易な運用サイクルをサポート

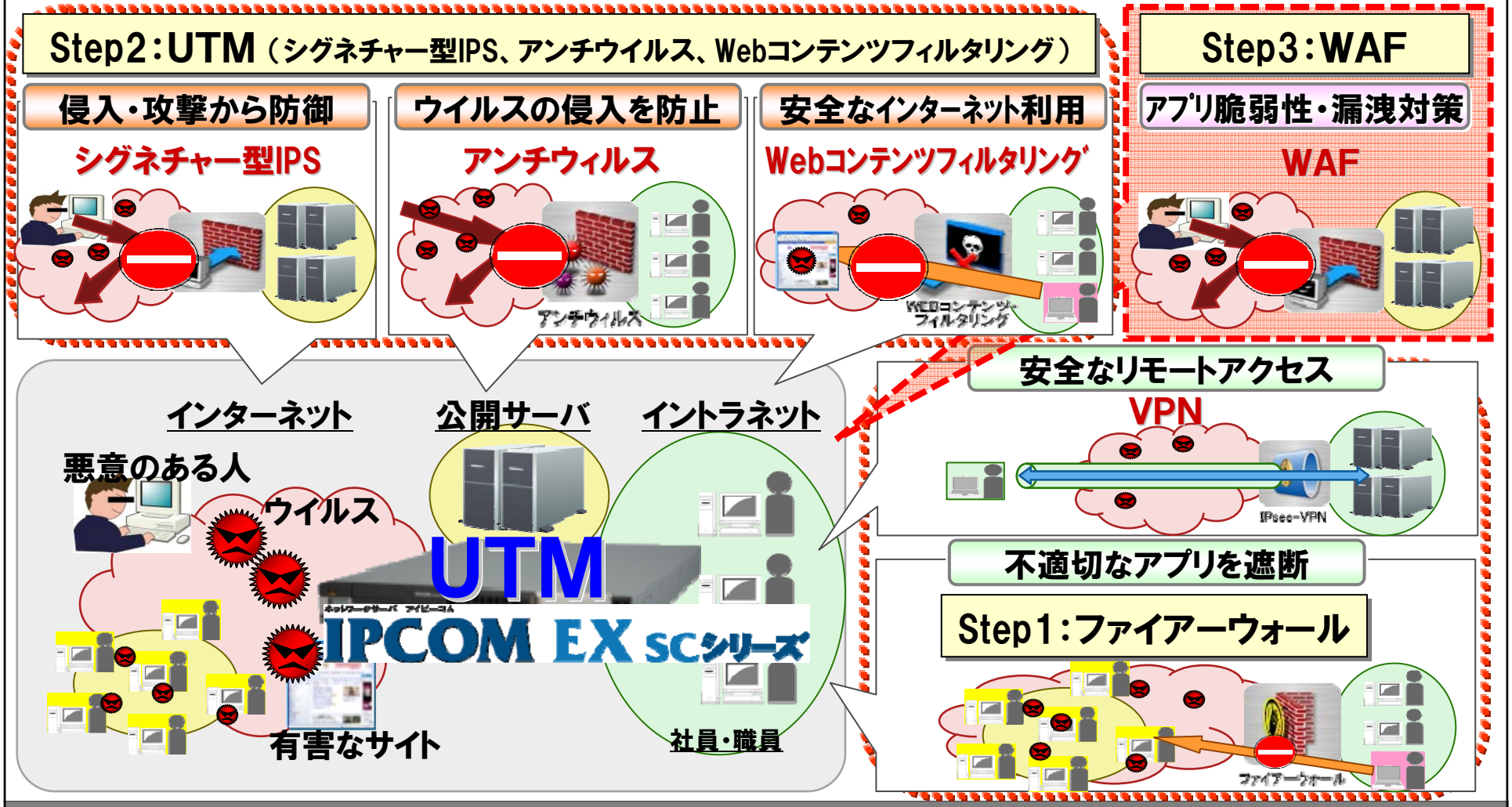


Webサイト毎の攻撃種別の
統計情報を表示可能

IPCOMで最新脅威をトータルに対策

FUJITSU

Step1：P2Pソフト対策も可能なファイアーウォール
Step2：UTM機能（シグネチャー型IPSアンチウイルス、Webコンテンツフィルタリング）を追加
Step3：WAF機能（Webアプリケーション・ファイアーウォール）を追加



IPCOMの特長：様々なセキュリテイ機能

- 既存セキュリティ機能と組合せてシステムを強固に防御
  - 5階層の防御壁でシステムを保護
  - 1台の装置で様々な攻撃に対するセキュリティを実現

IPCOMの不正アクセス防御の考え方

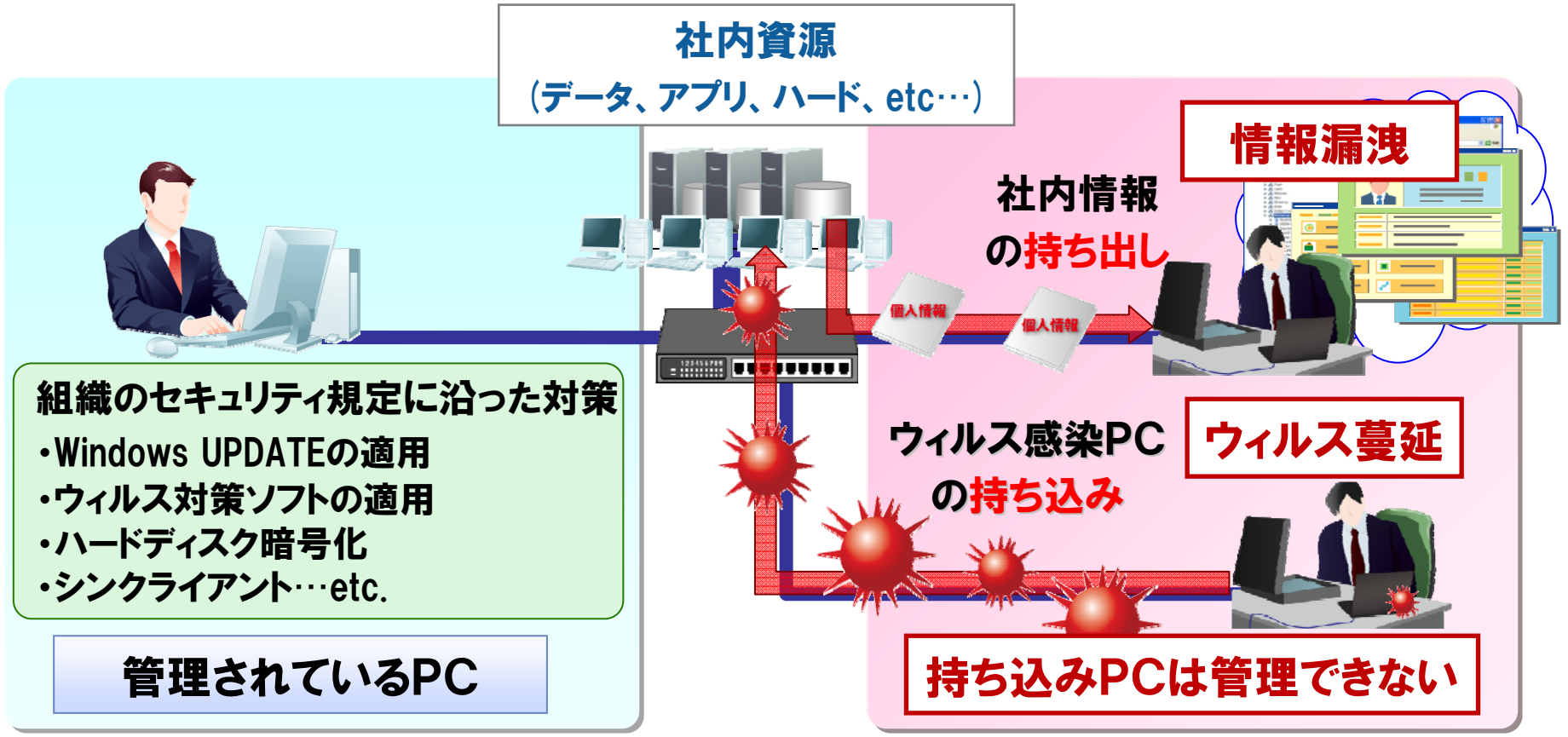
③ オフィス内LANに対する対策

無統制な持ち込みPCの利用は情報漏洩を招く

FUJITSU

セキュリティ対策の実施されていないパソコンが

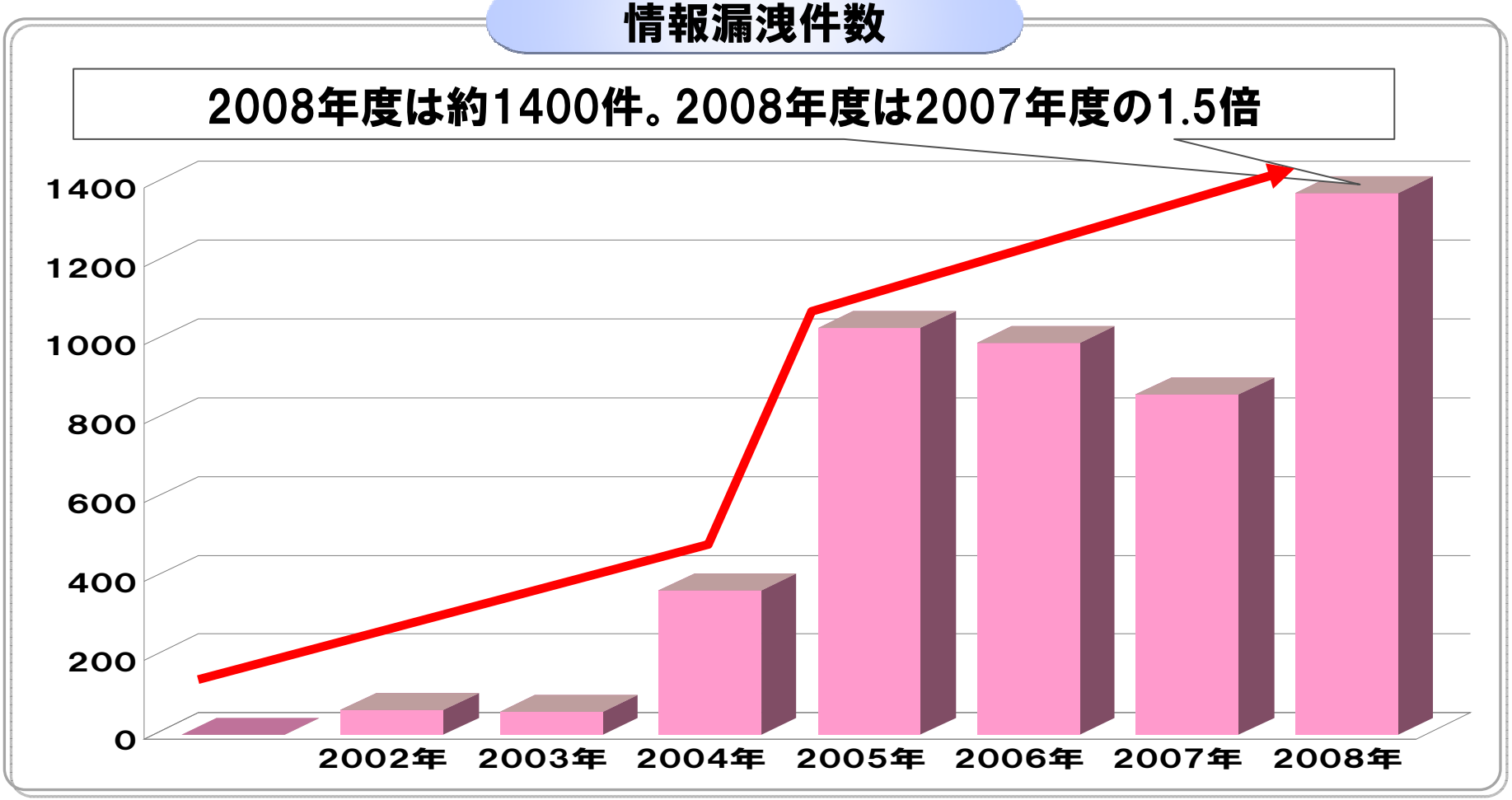
社内に持ち込まれると多くの問題が発生。



情報漏洩が激増

「内部不正行為」や「不正情報持ち出し」
発生件数の全体に占める割合は小さいが、1件当たりの漏洩した情報量は多い

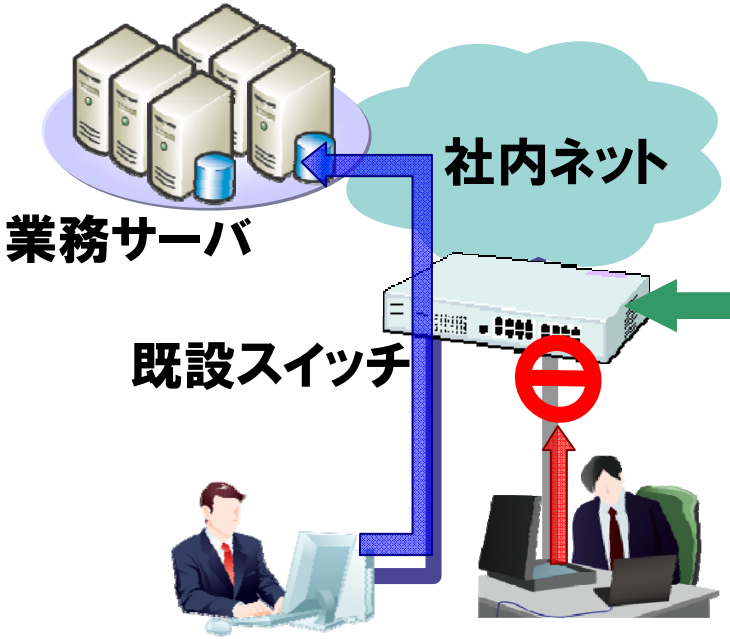
情報漏洩件数



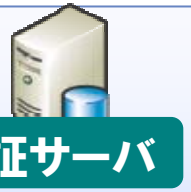
出展：日本ネットワークセキュリティ協会（JNSA）：2008年情報セキュリティインシデントに関する調査報告書 Ver.1.3）

持ち込みPC対策

「内部不正行為」や「不正情報持ち出し」に対する対策は、
PCの接続状況を監視し、持ち込みPCを排除すること。

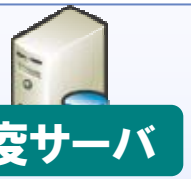


（1）持ち込みPCの遮断（不正接続防止）



■ 特長
- 現状のお客様環境にアドオン導入
- PCに、ソフトウェアをインストールする不要

（2）PCの認証・検疫



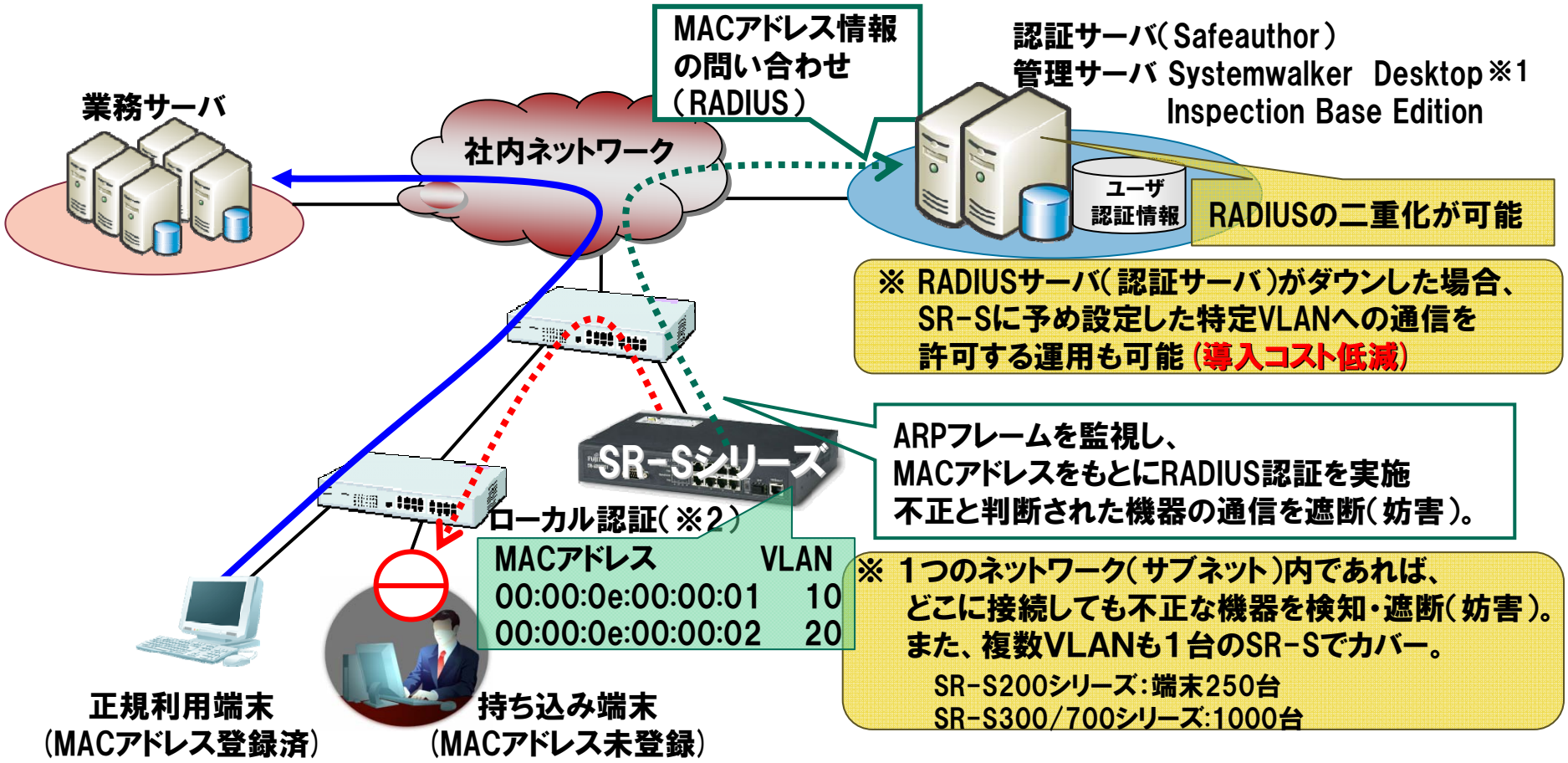
アップデート用サーバ

■ 特長
- Windowsセキュリティパッチやウイルス対策ソフトのパターンファイルの古いPCも排除
- セキュリティ対策が不十分なPCにパターンファイルを適用させることも可能

(1) 持ち込みPCの遮断(不正接続防止) -ARP認証-

FUJITSU

SR-Sを1台導入することで、
不正な機器を検出しIP通信を遮断(妨害)



※1 Systemwalker Desktop Inspection Base Edition はARP認証/MACアドレス認証のRADIUSサーバとしてご利用頂けます。
その際、クライアントライセンスは「クライアントライセンス(遮断)」を選択下さい。
※2 SR-S内に登録したMACアドレス情報を利用したローカル認証も可能です。

(2) PCの認証・検疫　-MACアドレス認証-

FUJITSU

ネットワーク機器のMACアドレスをもとに認証
IP電話等の自発的にパケットを送信してくるネットワーク機器も認証

認証サーバ(Safeauthor)
管理サーバ Systemwalker Desktop Inspection Base Edition

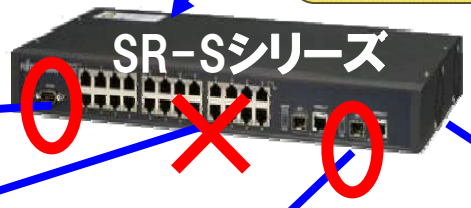
RADIUSの二重化が可能

※ RADIUSサーバ(認証サーバ)がダウンした場合、SR-Sに予め設定した特定VLANへの通信を許可する運用も可能(導入コスト低減)

ユーザ名/パスワード入力は不要。
RADIUSサーバ(もしくはSR-S)のMACアドレス情報をもとに認証。
登録していない持ち込み端末をつないだ場合は接続不可

正規利用者
(MACアドレス登録済)

持ち込みPC
(MACアドレス未登録)



IP電話
(MACアドレス登録済)

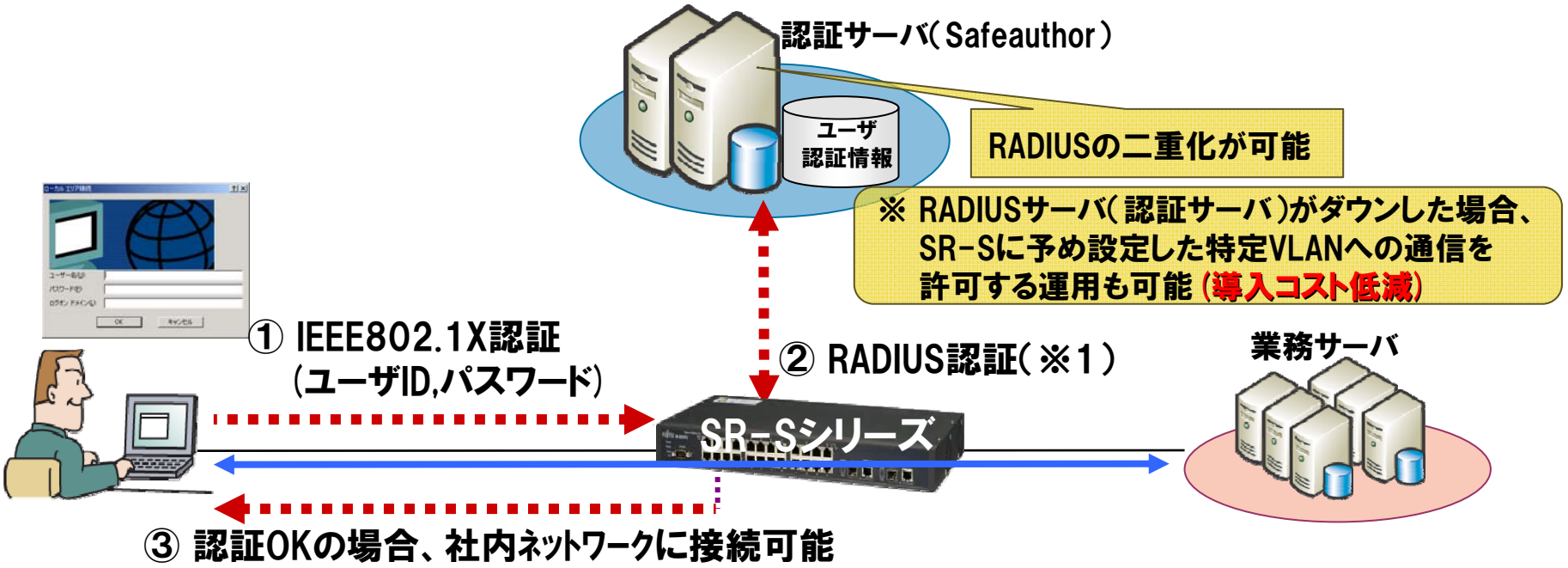
IP電話も認証可能

業務サーバ

(2) PCの認証・検疫　-IEEE802.1X認証-

FUJITSU

ユーザID／パスワード（PEAP）、または、証明書（EAP-TLS）により認証された利用者、または、コンピュータのみに通信を許可



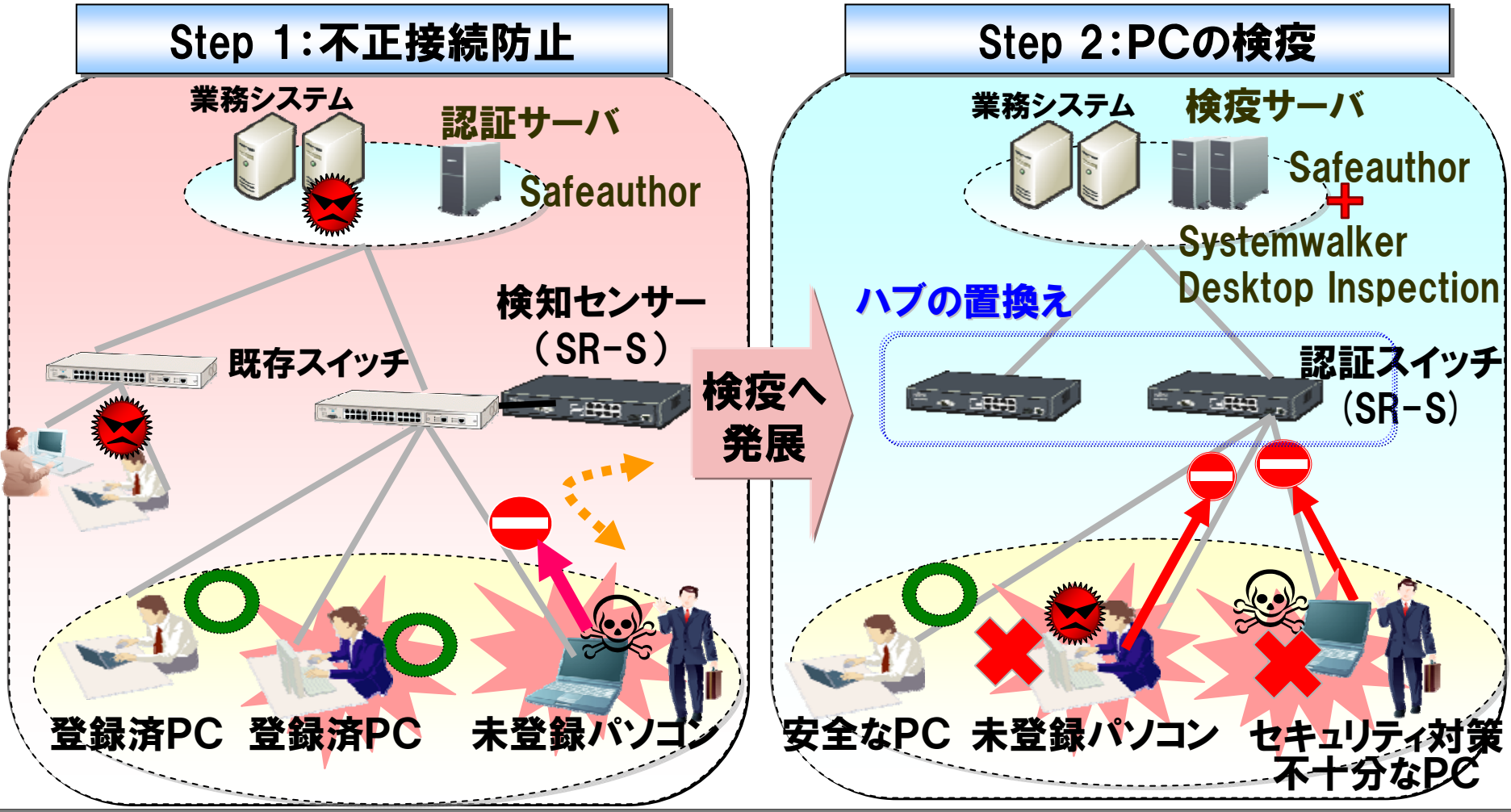
SR-SはMicrosoft社 NAP（※2）パートナーに認定されており、
ActiveDirectory環境にも対応。

※1　SR-S内に登録したユーザ情報を利用したローカル認証も可能です。（但し、利用可能な認証方式は「EAP-MD5」のみで、「PEAP」や「EAP-TLS」などは利用できません）

※2　NAP (Network Access Protection) ：Microsoft社が提供する認証・検疫ソリューションに必要なフレームワークです。

「不正接続防止」から「検疫」にステップアップ

検知センサーとして導入したSR-Sをそのまま利用。（富士通のみ）
ハブを置換え、利用者認証/パソコン認証/検疫までステップ展開。



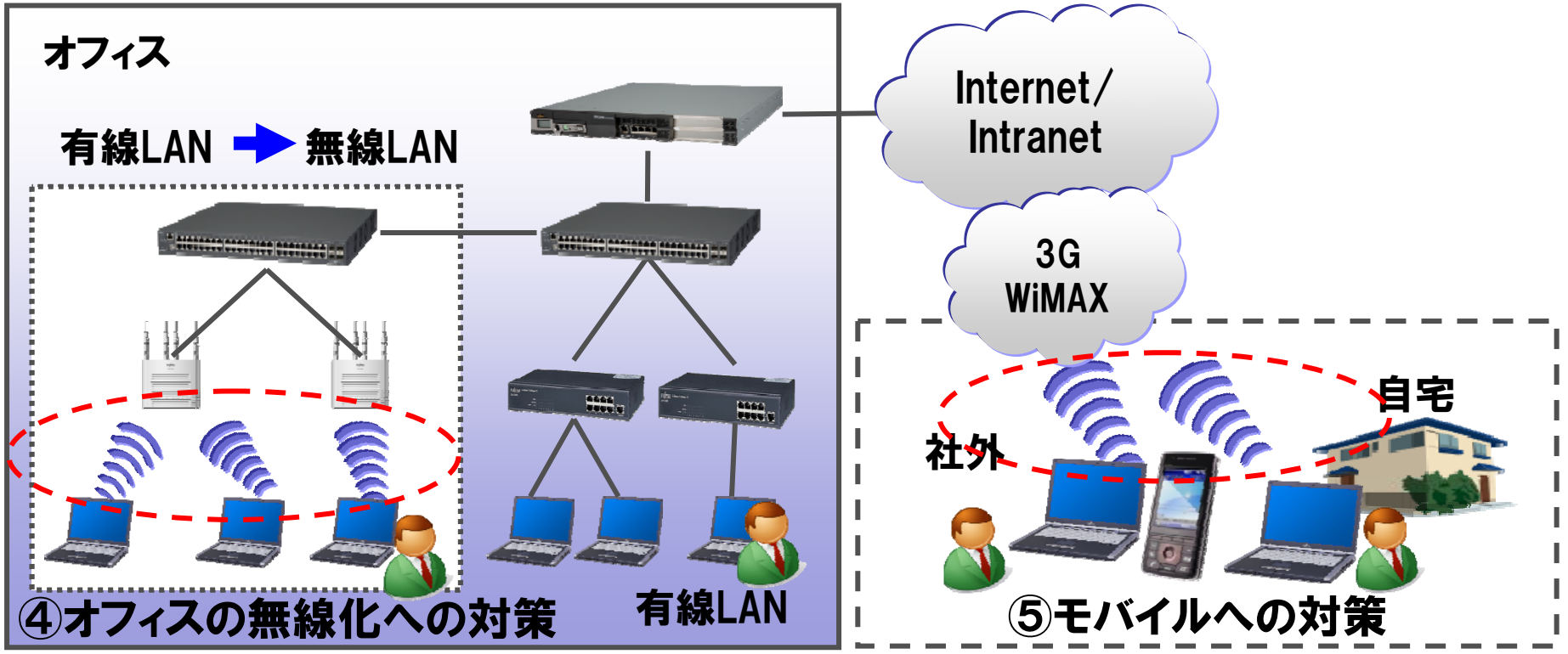
オフィス環境の変化への対応

オフィスのネットワーク セキュリティは無線へ

FUJITSU

無線環境へと変わるオフィス。
ネットワーク セキュリティはどのように変わるのか。

無線化するとセキュリティが心配と言うけれど….
基本は、「接続認証」と「データの秘匿」



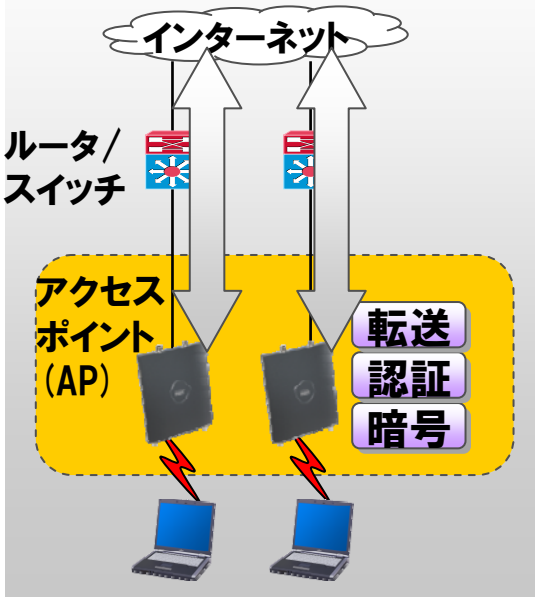
④　オフィスの無線化への対策

ハイブリッド型無線LANシステム SR－Mシリーズ

独立型とコントローラ型のそれぞれの利点を製品に反映

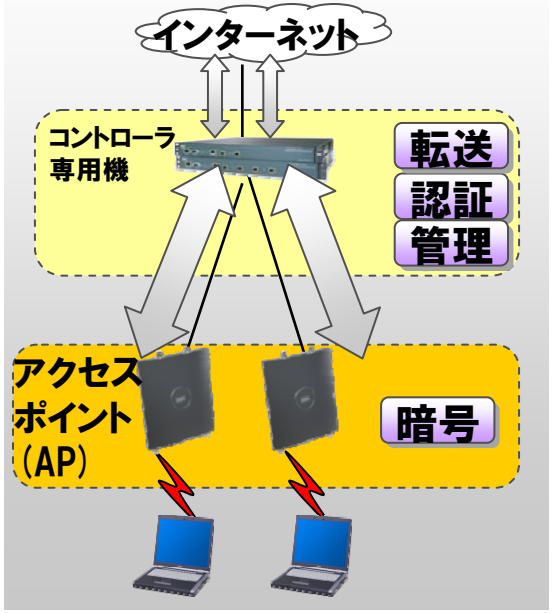
独立型

- 各APが無線LANパケット処理
- 無線LAN管理はなし



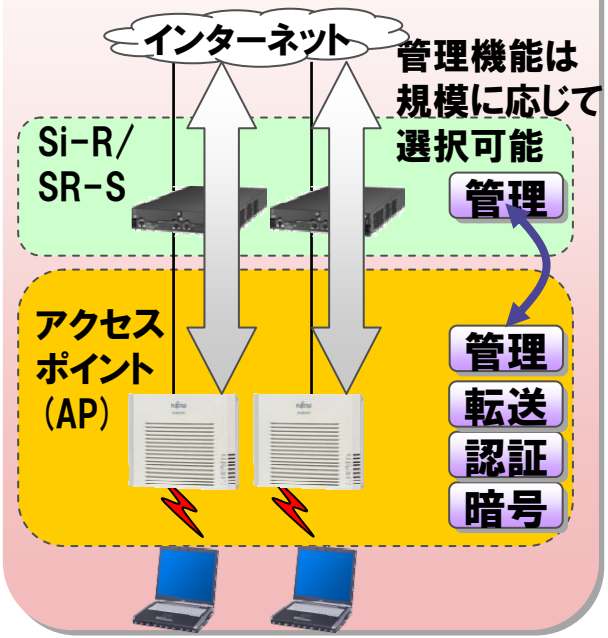
コントローラ型

- コントローラが無線LANパケット処理
（全ての通信はコントローラを経由）
- コントローラで各APを一元管理



ハイブリッド型（SR－M）

- 各APで無線LANパケット処理。
- APまたはSi-R/SR-Sで無線LAN管理



	独立型	コントローラ型	ハイブリッド型（SR－M）
管理	×個別に管理のみ	○一元管理、電波調整	○一元管理、電波調整
信頼性	○障害の局所化	×コントローラ障害で停止	○障害の局所化
性能	○アクセスポイント毎にトラフィック分散	×コントローラに全トラフィック集中	○アクセスポイント毎にトラフィック分散
コスト	○低コスト	×高コスト	○低コスト

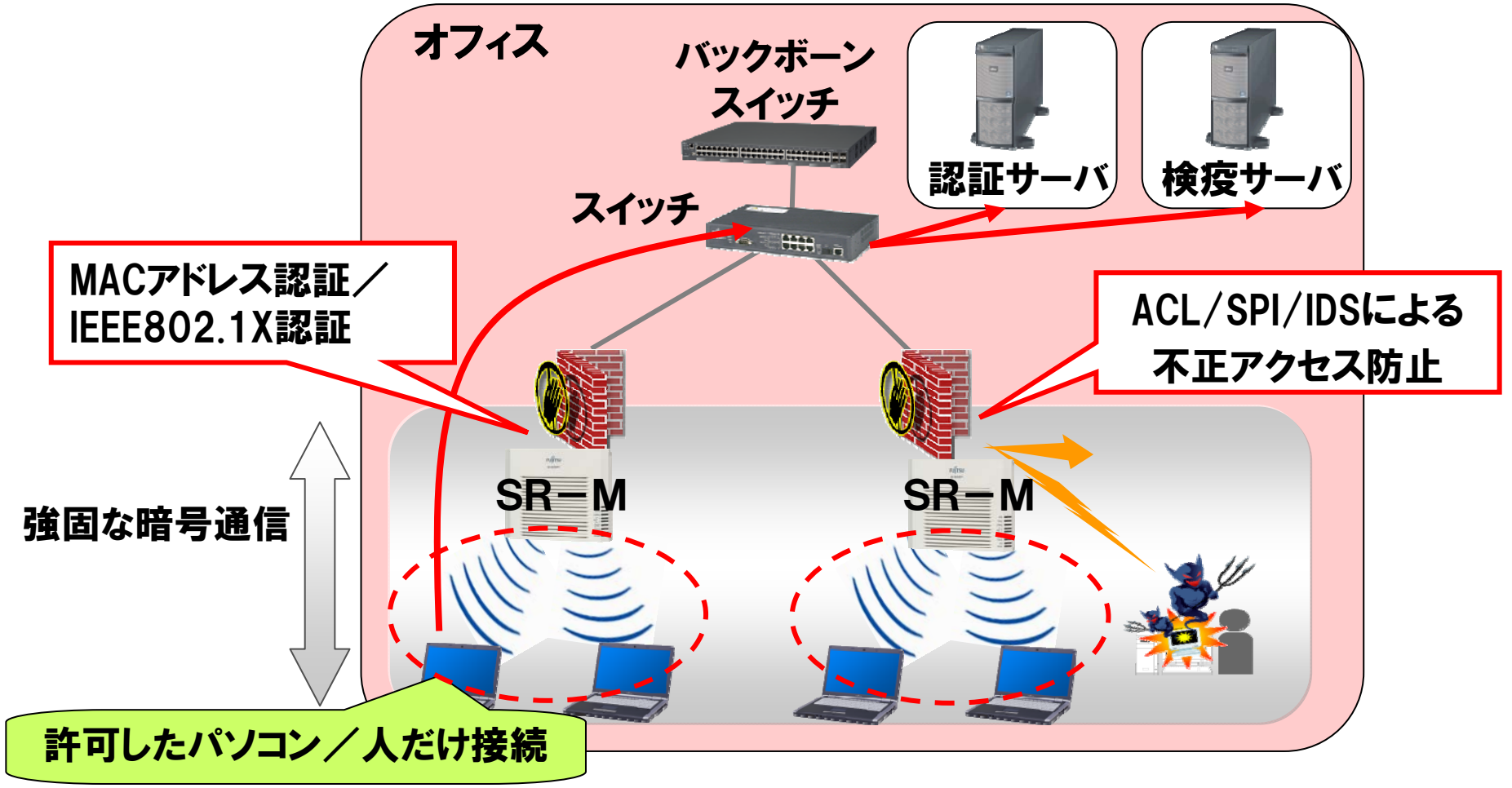
利点を反映

無線LANにおける不正接続防止

FUJITSU

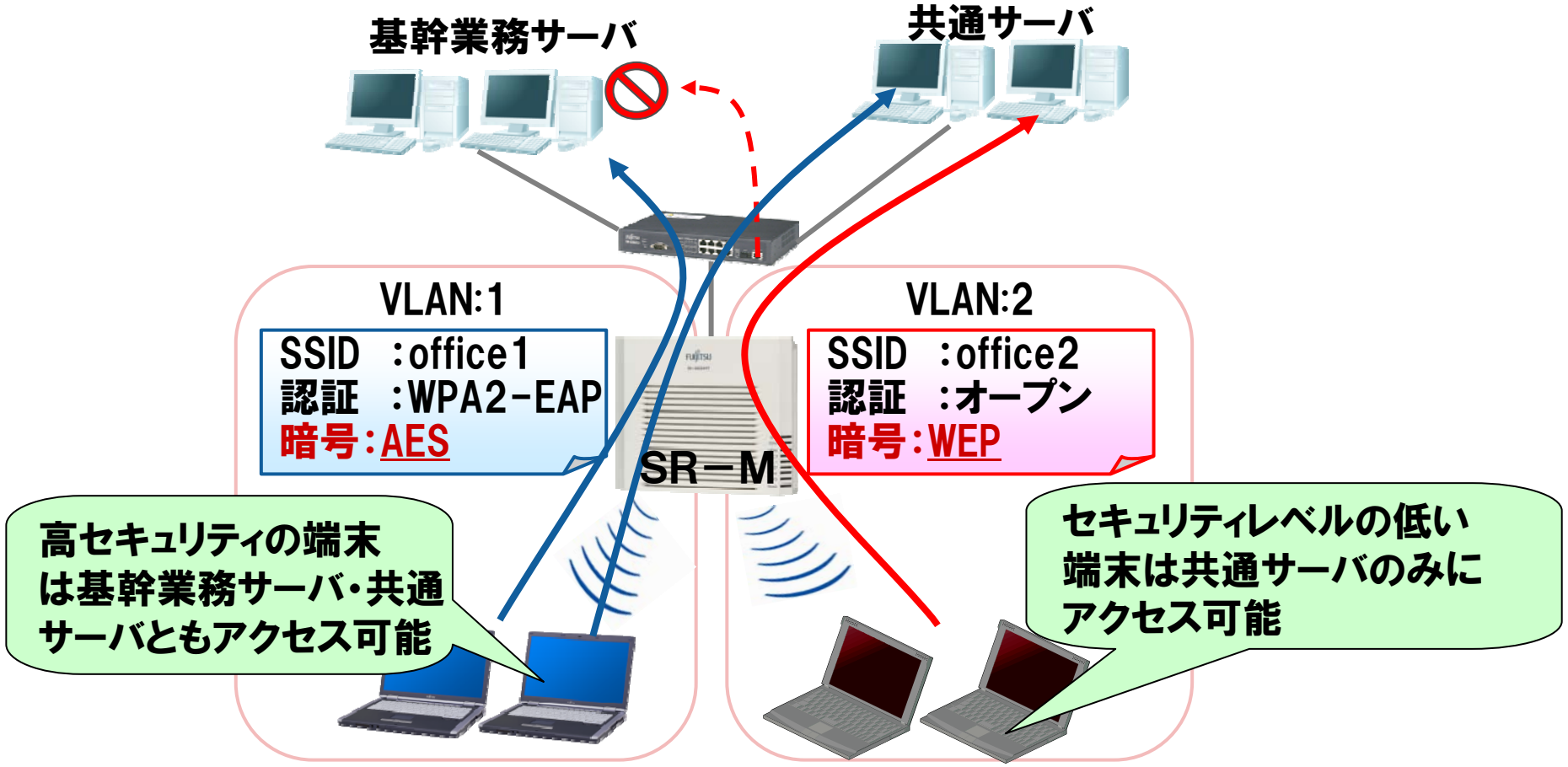
- 接続認証：SR-Sと同様、MACアドレス認証、IEEE802.1X認証に対応
- データ秘匿：業界標準WPA／WPA2 に準拠

更に、アクセス制御（ACL/SPI/IDS）により不正アクセスに対応



仮想アクセスポイント（VAP機能）

1つのアクセスポイントで、SSID毎に、マルチセキュリティ設定が可能（VAP機能）
- セキュリティレベルの異なる端末を1台のSR－Mに収容
- 端末毎にアクセス可能な領域を分離



⑤　モバイルへの対策

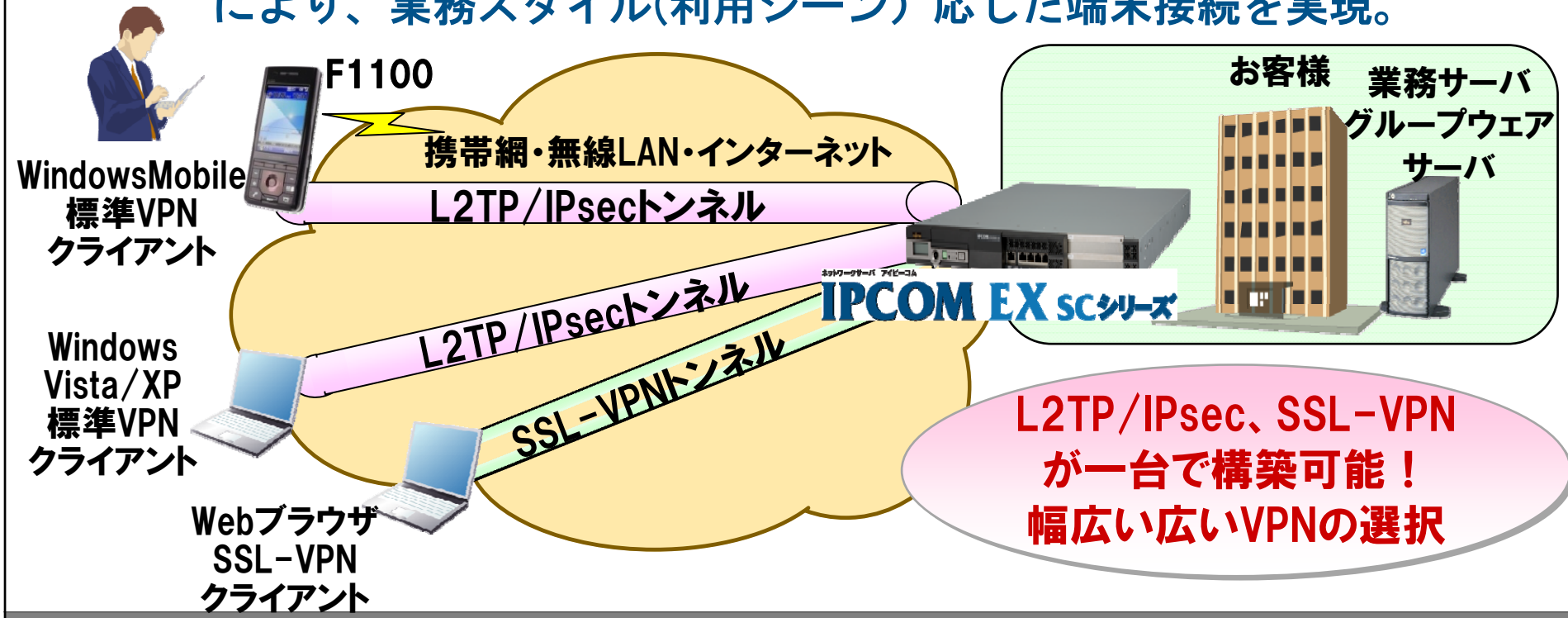
IPCOM EXシリーズのモバイルアクセス機能強化

FUJITSU

SSL-VPN/L2TP/IPsecプロトコルによるVPNゲートウェイ機能の提供

- Windows標準のVPNクライアントによる接続に対応。
  - F1100などのWindowsMobile、WindowsVista/XPからの接続に対応。
- IPsec NATトラバーサル機能
  - NAT環境からのL2TP/IPsec、IPsecの接続に対応。

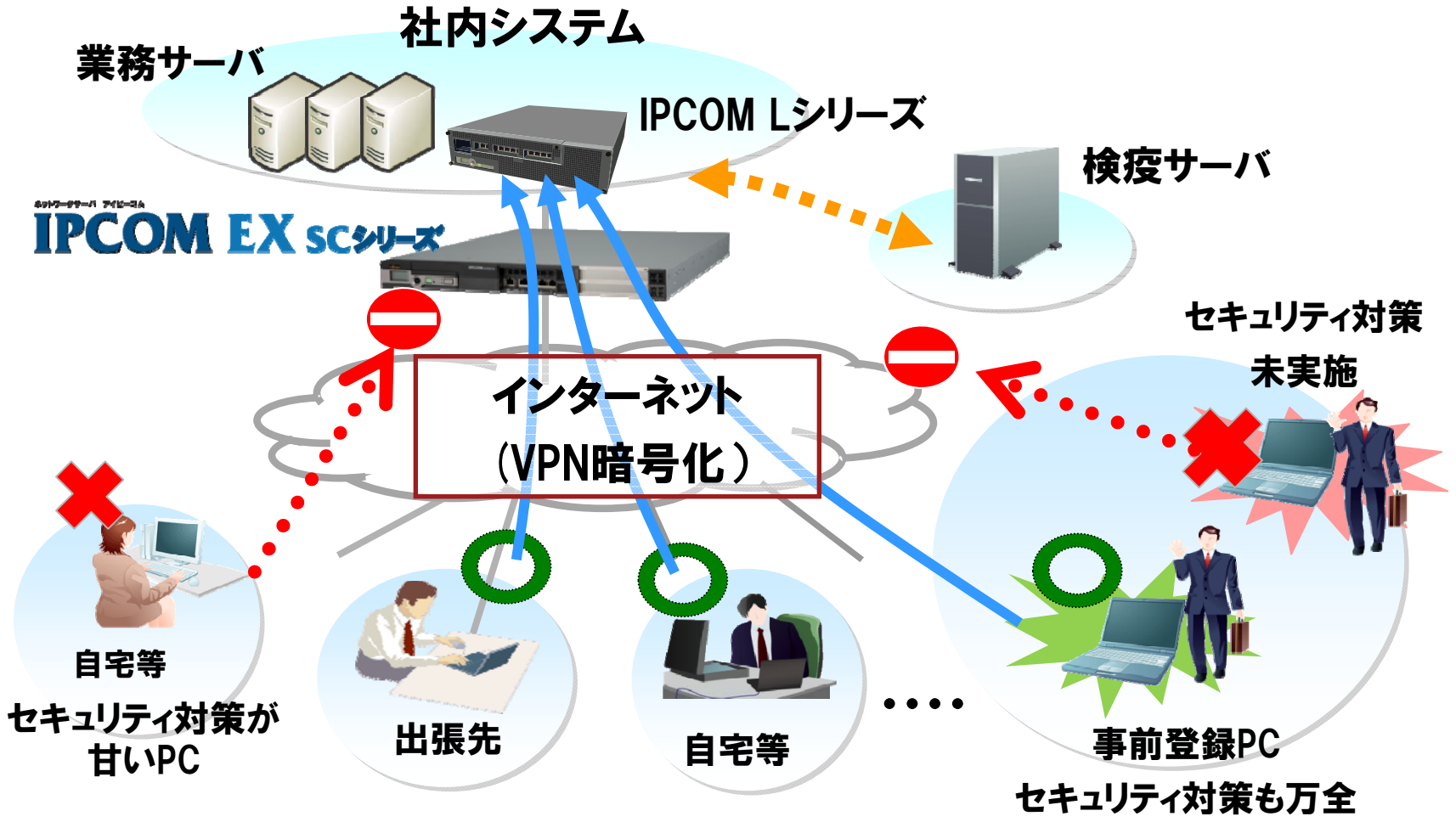
スマートフォンやWindows PCのVPN接続と、SSL-VPNによるPC接続により、業務スタイル(利用シーン）応じた端末接続を実現。



リモートアクセス検疫

FUJITSU

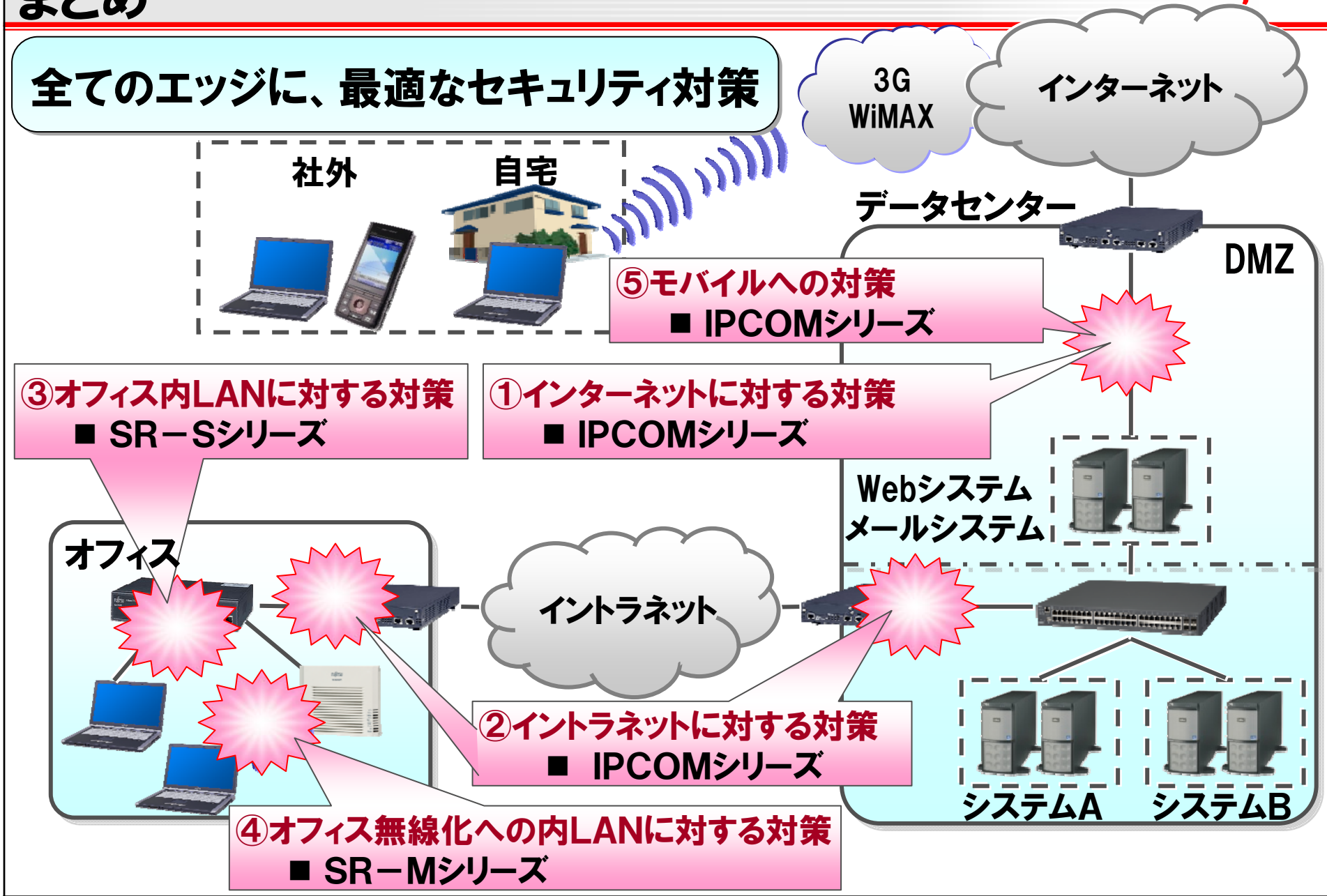
**オフィスからのイントラネット経由のアクセスと同様に、
外部からアクセスするパソコン認証・検疫**

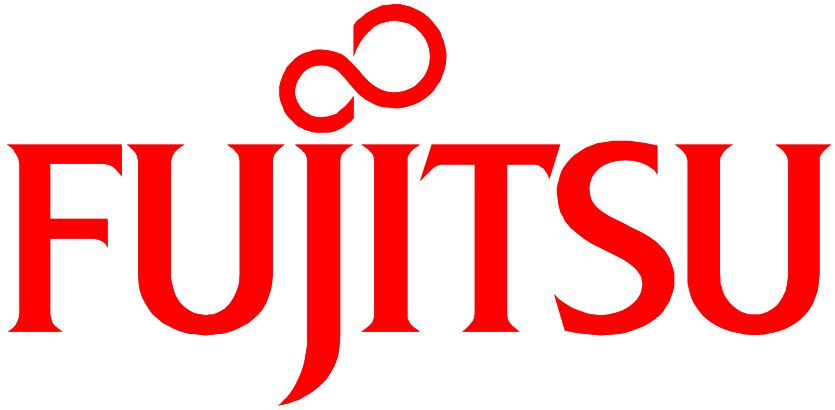


まとめ

FUJITSU

全てのエッジに、最適なセキュリティ対策





THE POSSIBILITIES ARE INFINITE