安全なモバイルワーク・BYOD活用のご提案

～ 証明書認証を使って安全確実なBYODを実現！！～

ソリューション企画推進部　プロダクト推進１課

2015年8月

シーティーシー・エスピー株式会社

会社概要

シーティーシー・エスピーの会社概要

CTC SP

会社名	シーティーシー・エスピー株式会社　（略称 CTCSP）
英文社名	CTCSP Corporation
本社所在地	〒154-0012 東京都世田谷区駒沢1-16-7 中村ビル TEL：　03-5712-8070 URL：　http://www.ctc-g.co.jp/~ctcsp
代表者	代表取締役社長　櫻庭　愼一郎
創立	1990年4月1日
資本金	2億円
社員数	187人（2015年4月現在）
事業内容	1. ネットワーク/セキュリティ関連機器の販売 2. ストレージ関連機器・ソフトウェアの販売 3. 関連周辺機器およびサプライ品の販売 4. その他上記事業に関わるコンサルティング・導入/構築・サポート

品質マネジメントシステム
ISO9001」認証取得

駒沢オフィス内観

モバイルワークBYODについて

スマートフォンやタブレットから業務を行うモバイルワークに必ず『BYOD』というキーワードが付いてくるのが最近の定番

BYODって何？

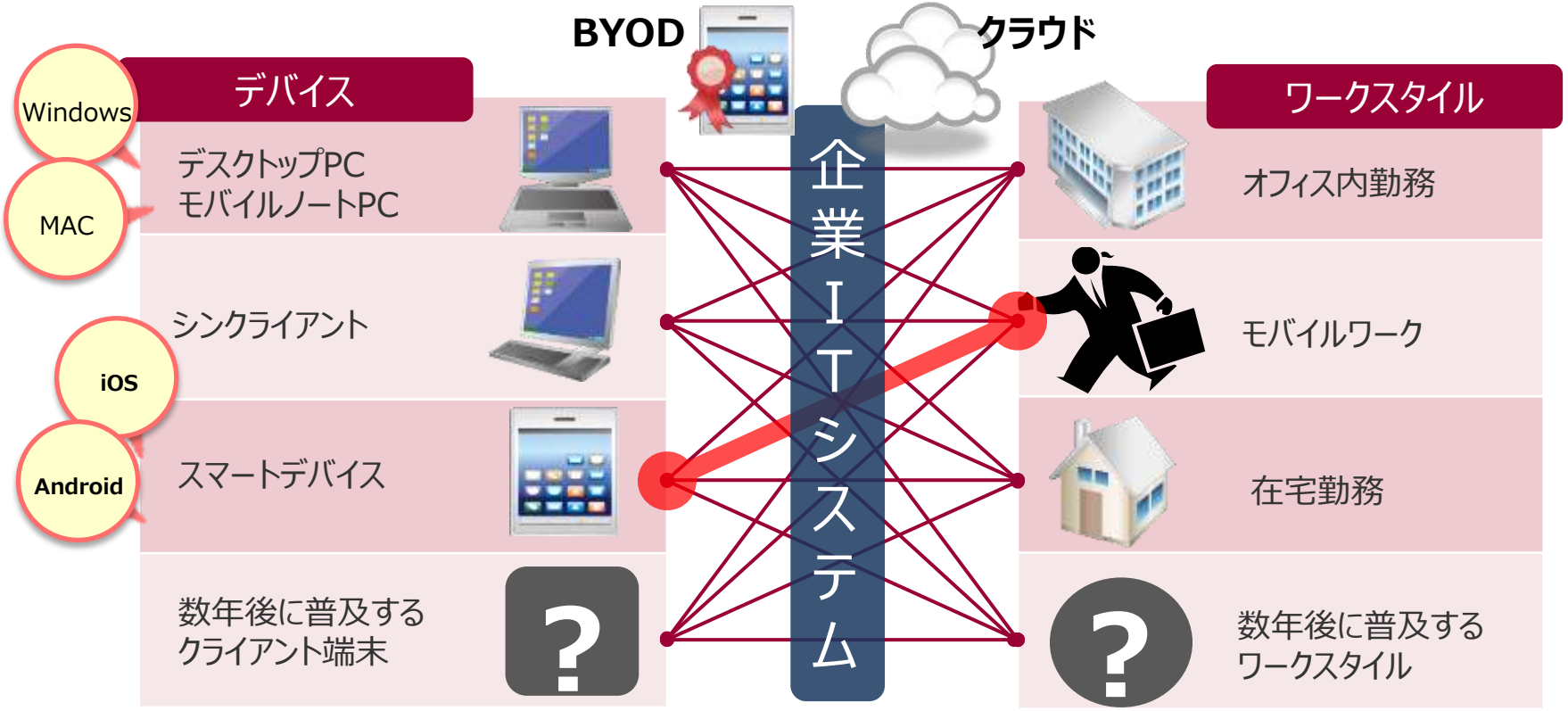
- **海外のレストランで、酒等の持ち込みを許可する。という意味のレストラン用語『BYO』から派生**

B=Bring	持っていく
Y=Your	あなたの
O=Own	自身の

※BYOFやBYOBと続く場合も。
※持ち込み料は掛かるらしい

自分の私物デバイス(主にスマホ、タブレット)を職場に持ち込み、業務に使うことをIT用語でBYODと言う。

- **多様化する時代を支える情報システム**
  - マルチデバイスによるマルチワークスタイルに対応する。
    - 短期間に激しく変化するビジネス環境では、ITシステムとしての“懐(ふところ)の深さ”が勝負を分ける。



- **BYOD(私物端末持ち込み)の良いところ**
  - 経費削減
    - コストが『ガラケー＜＜スマホ』なので。。。
  - 使い易い端末
    - 私物端末は使い易い
    - iPhone派とAndroid派
  - ２台持ちしなくてよい
    - 会社スマホと私物スマホの2台持ち最悪
      - ポケットがいっぱい
      - 2台を充電しなきゃならない

- **BYODの悪いところ**

–セキュリティ制御が出来ない

例）
会社のメールに来た仕入先からの見積もりを自分のGmailに転送して土日に家で作業しよう！

シャドウITと言います。

セキュリティの問題さえ潰せればBYODが推進できる！

- **スマホのシャドーIT化は「必然」**
  - 常に携帯する「個人電話」と、高機能な「IT機器」が同居

シャドーITとは？

システム部門の管理下にないIT機器、および、それを用いた業務活動を指す。

「管理」を旨とする情報セキュリティの考え方では、排除すべき対象。

シャドーIT の”なりやすさ”

スマートフォン

企業システムとの親和性	高
×	
オフィスへの溶け込み	高
×	
持ち歩く必要・必然性	高

ではどうやってBYODのセキュリティ向上をするか？

– MDM（モバイルデバイスマネージメント）

クライアントソフトのインストールや管理権限を使ってスマホを制御

–アプリの制限

–キャッシュクリア

–紛失時の初期化

- **社員からの意見**
  - 自分で買った端末なの何故会社に管理されなければならないのか？
  - プライベートのメールも会社に管理されるのは勘弁

- **情報システム部からの意見**
  - 私物端末なので機種、OSバージョンがバラバラで全部一元管理できるシステム/ツールが見つからない
  - コストが掛かる

という理由からあまり導入が進んでいない

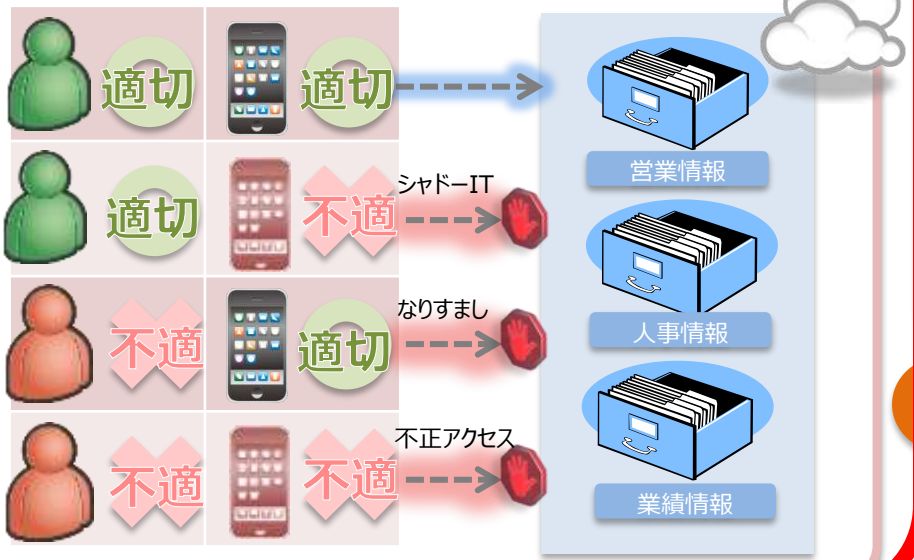
では、どうやって
モバイルワーク、BYODを
推進してゆくのが良いのでしょうか？

- **スムーズな導入を行うための「順序」**
  - 情報漏えいリスクを排除できなければ検討は進まない
    - ツール・ユーティリティを導入しても、不適切な端末の利用排除できなければ意味がない。

1 利用者と端末を「認証・識別」

認証基盤

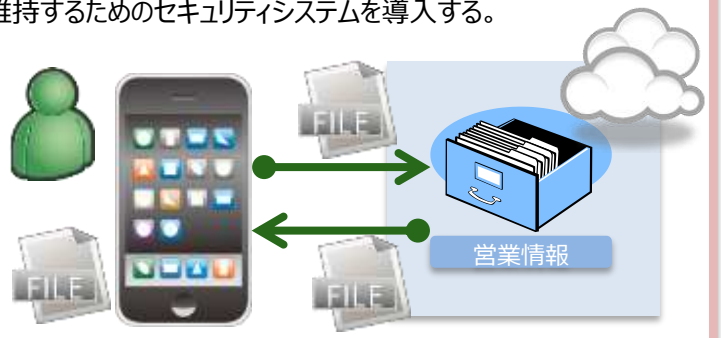
正規の「人物」が正規の「端末」を使用している場合のみアクセスを許可できる「識別・認証」基盤を整備する。



2 情報の「機密」を維持

MDM
BYOD
ツールなど

オフィス外で参照・利用される情報資産の「機密」を維持するためのセキュリティシステムを導入する。



3 「利用率」を高める施策

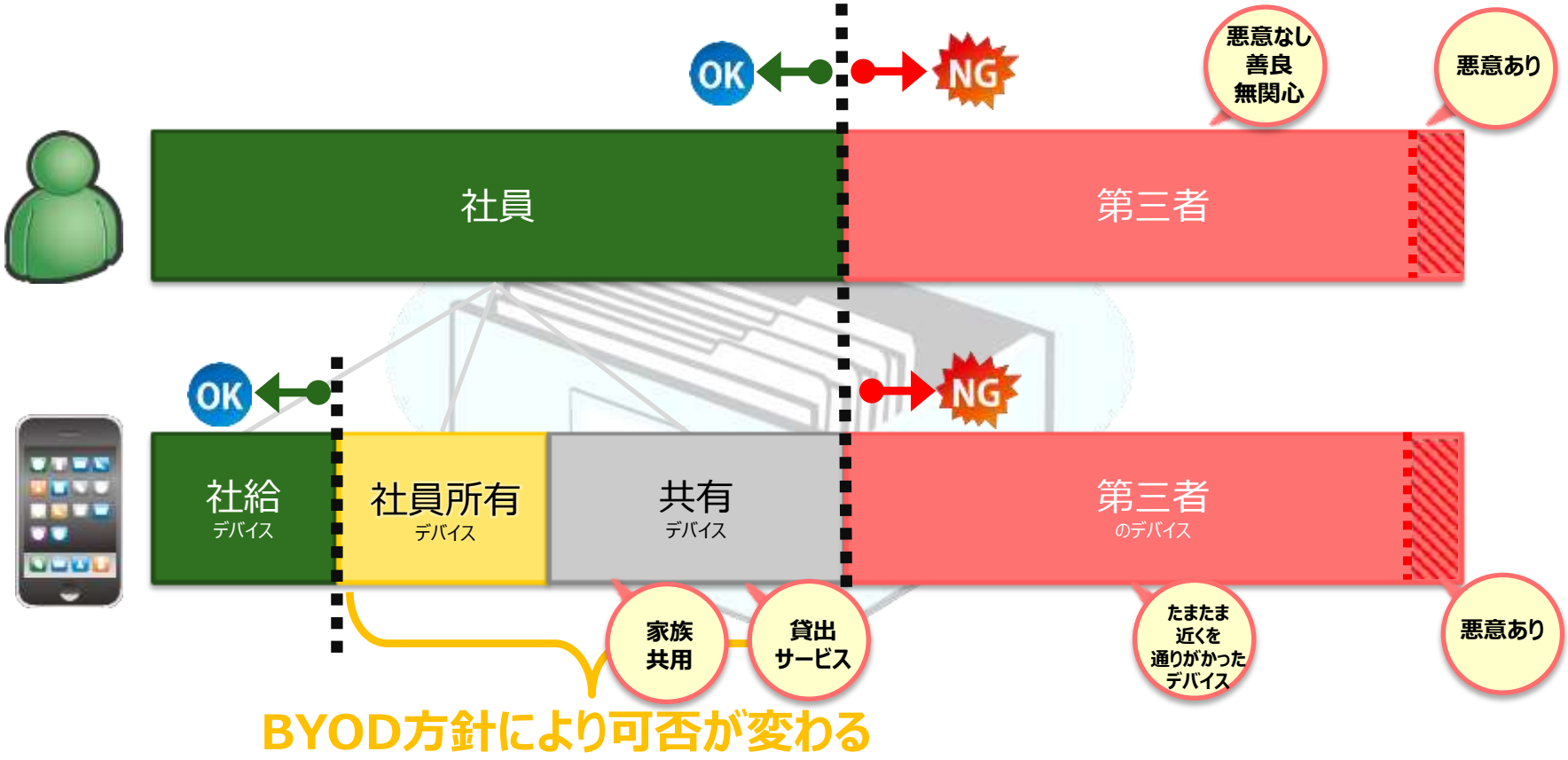
システムの快適性・利便性を向上し、利用率を高める。

シャドーITの境界線と理想の社内システム

■ 全ての私物デバイスを許可する？

– 会社方針で変わる「BYOD」と「シャドーIT」の境界線

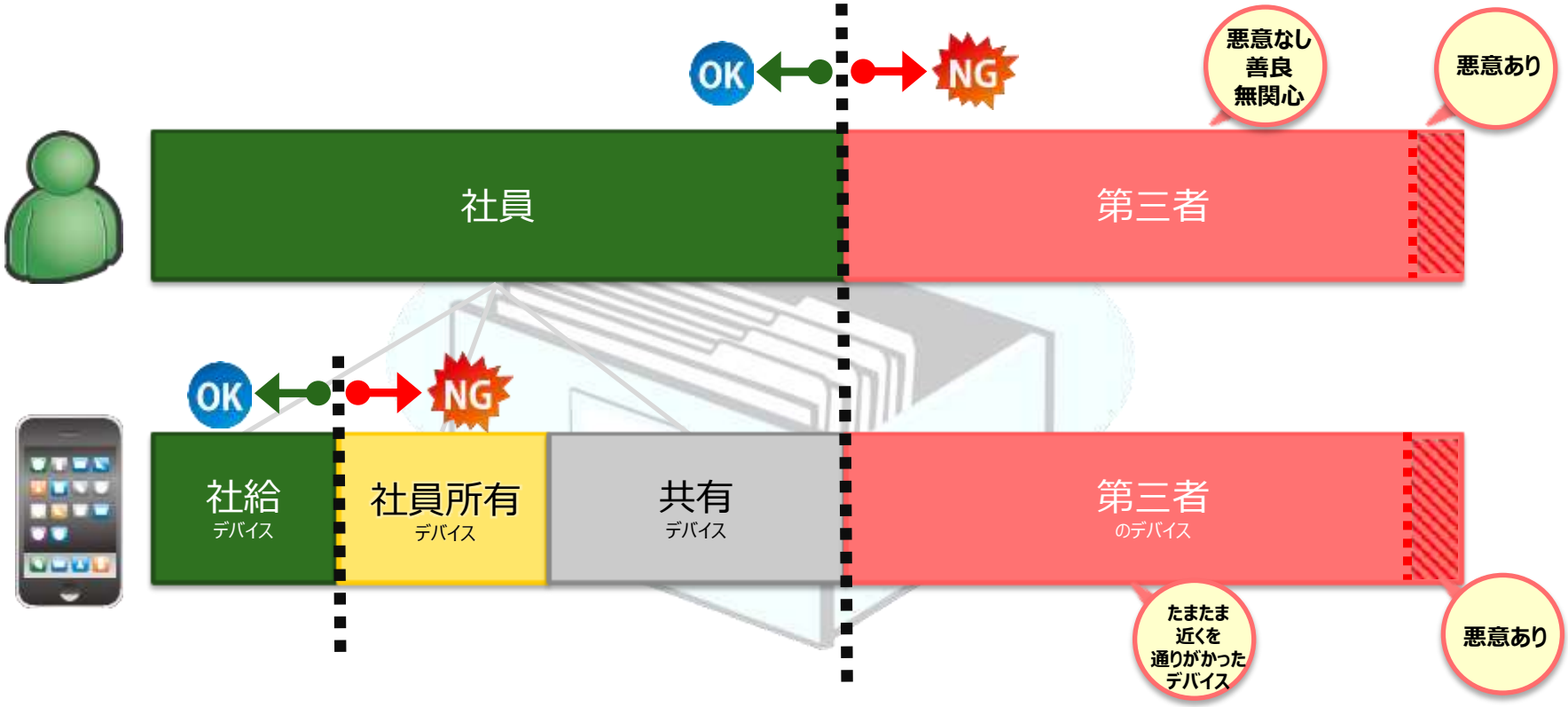
人物に対する認証は以前と変わらず、端末に対する識別は複雑になるばかり・・



■ 全ての私物デバイスを許可する？

– 会社方針で変わる「BYOD」と「シャドーIT」の境界線

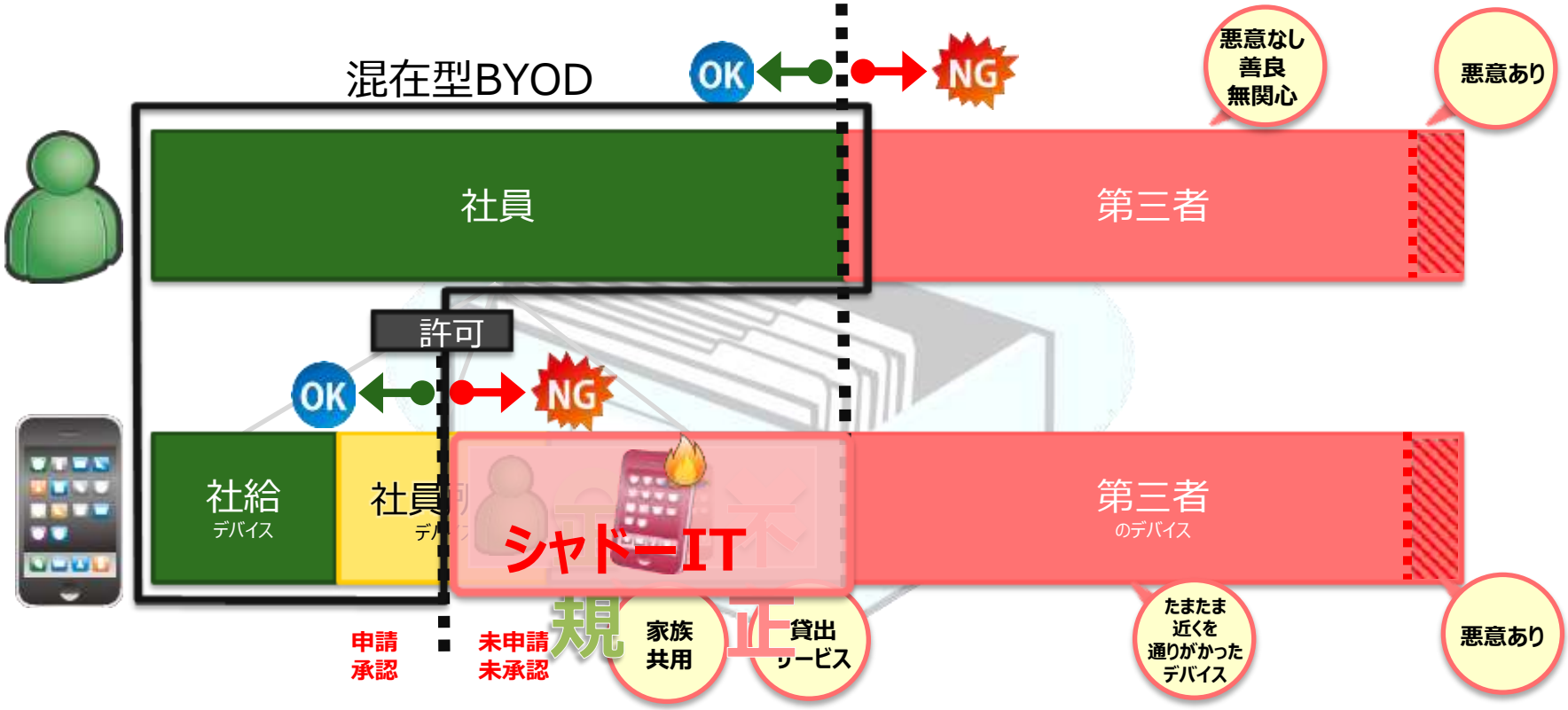
人物に対する認証は以前と変わらず、端末に対する識別は複雑になるばかり・・



■ 全ての私物デバイスを許可する？

– 会社方針で変わる「BYOD」と「シャドーIT」の境界線

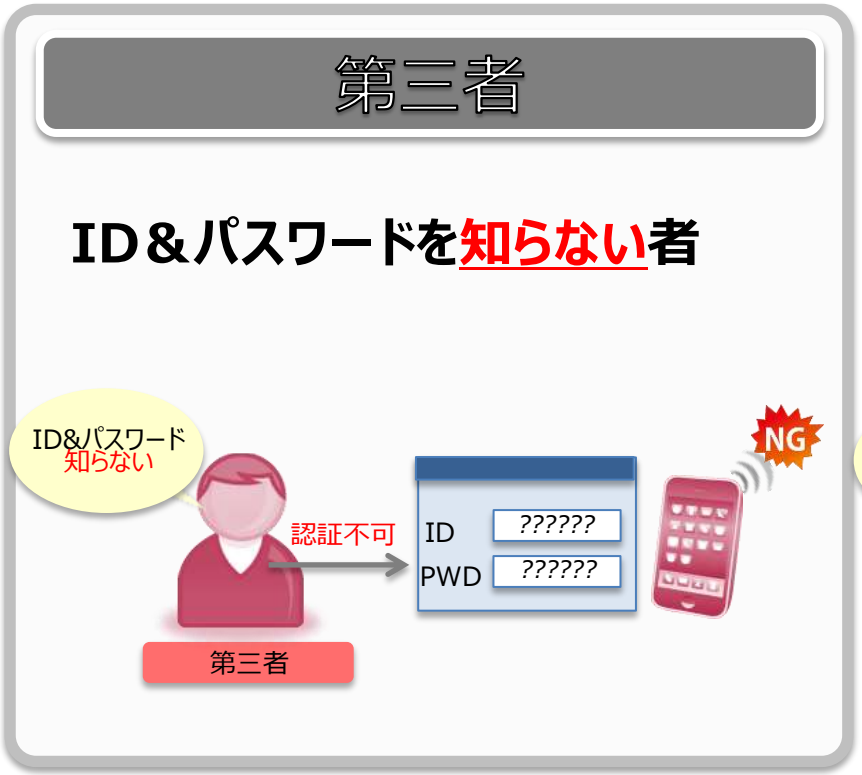
人物に対する認証は以前と変わらず、端末に対する識別は複雑になるばかり・・

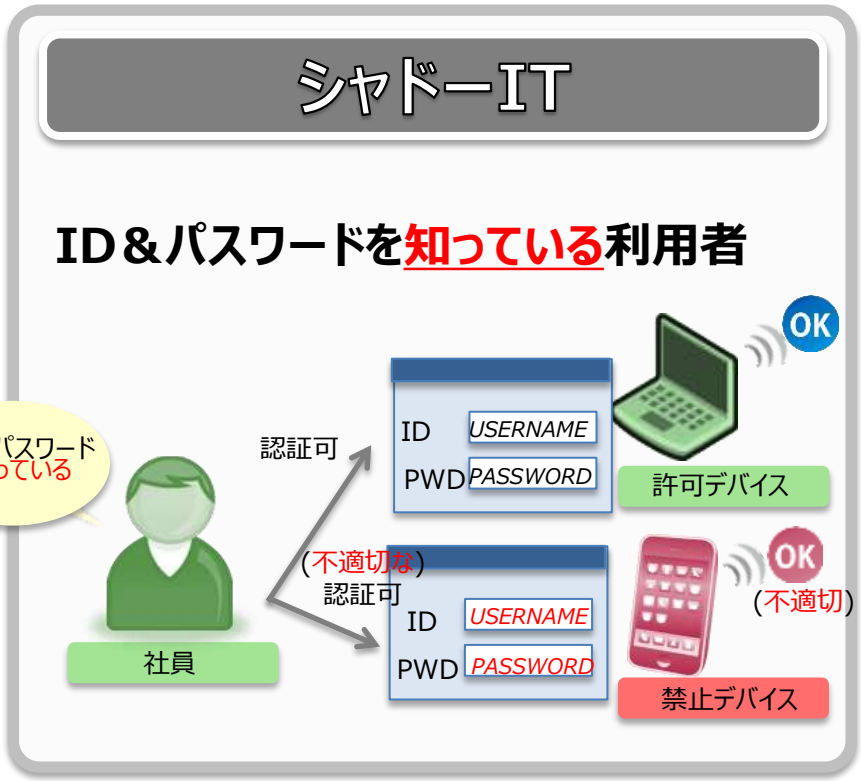


■「第三者」と「シャドーIT」の違いに注意

– 従来からのID&PASSWORD認証(のみ)では効果が薄い。

スマートデバイスの多くは、企業ネットワークにアクセス可能なクライアントを標準搭載





■ **今後のシステムでは「端末識別」が必要不可欠**

– デジタル証明書認証で不適切端末を排除する。

セキュリティ強度が弱点の「MACアドレス」、マルチデバイス環境での採用に課題の「IMEI/UDID」。

シャドーITへの対応

認証情報の複製や偽装は不可能で、
確実な端末認証を実施できる。

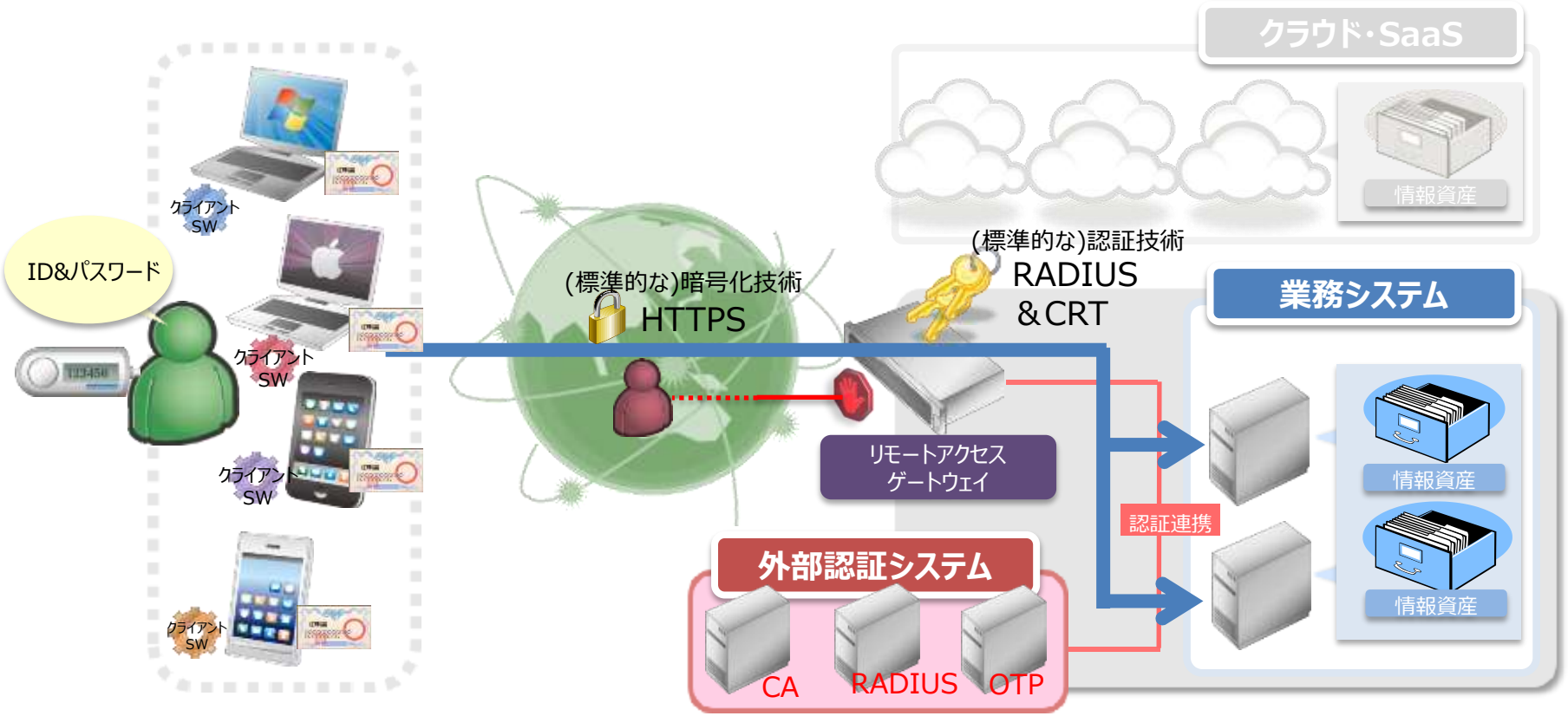
紛失盗難への対応

「**失効**」や「**再発行**」が容易で、
紛失盗難時の対応を適切に行える。

■ 内部企業システムを安全に活用する基盤

– 適切な暗号化と認証で、安全に社外から参照させる。

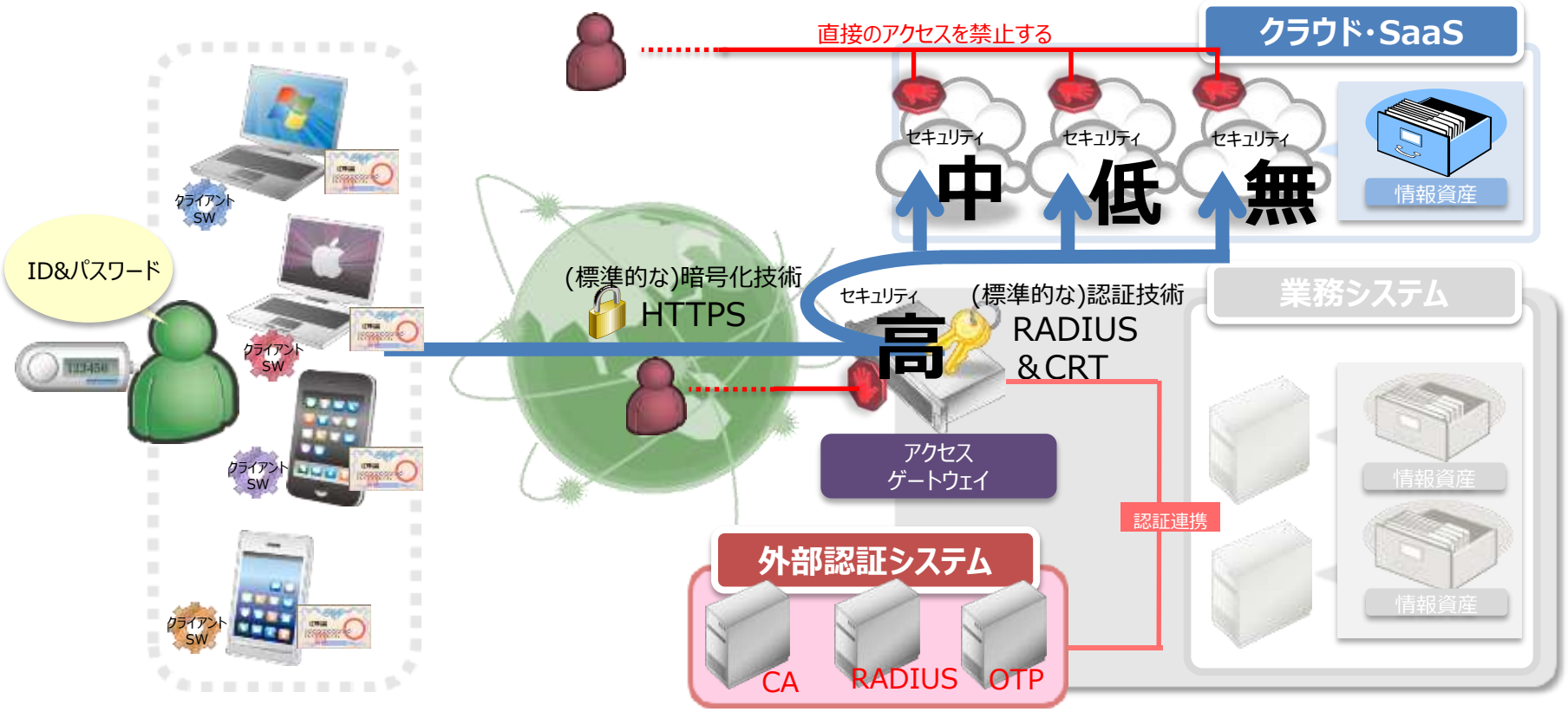
- 「外部」と「内部」をつなぐ際には、十分なセキュリティレベルの確保が必須条件に。



■ クラウドサービスを安全に活用する基盤

– アクセス経路の一本化と、セキュリティ強度を統一する。

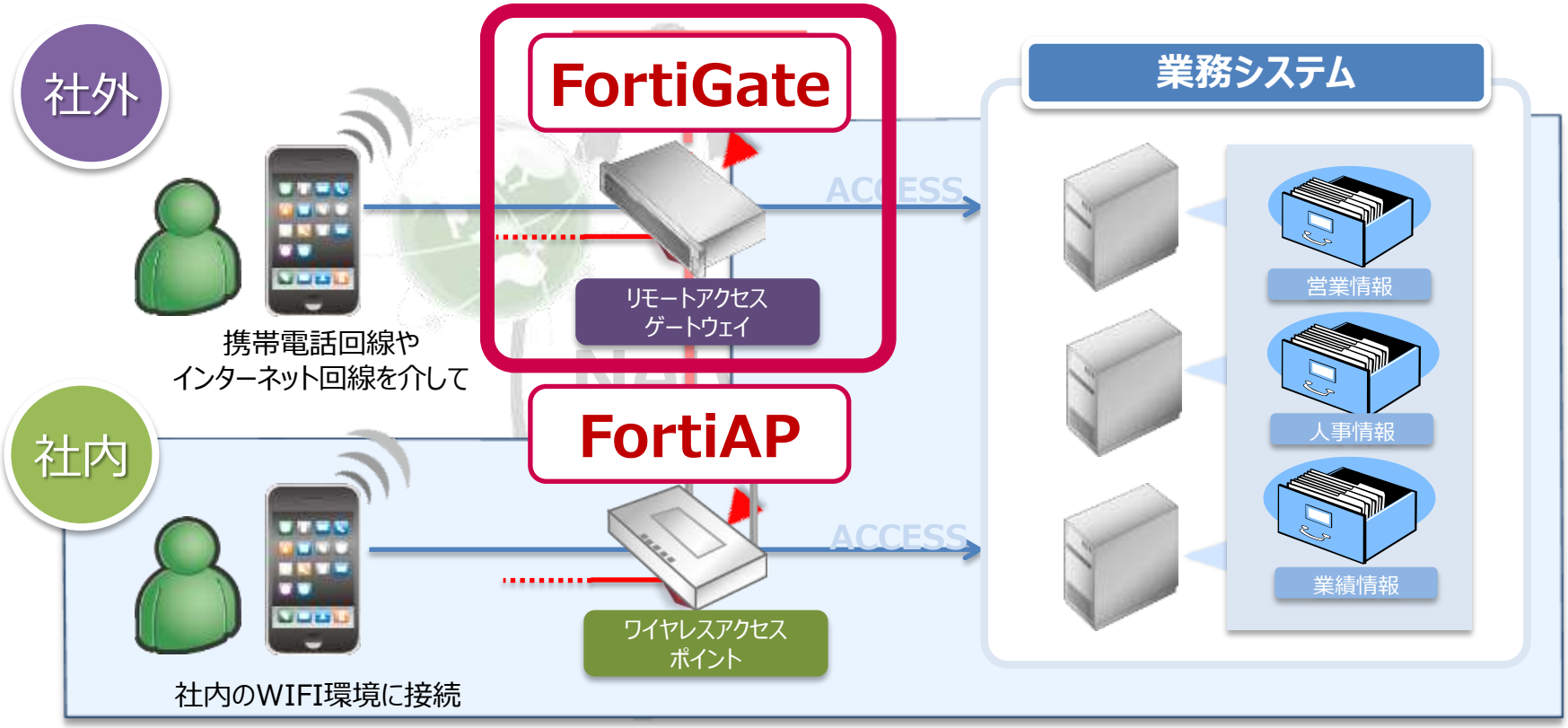
クラウドサービスへの直接アクセスは、サービス毎にセキュリティ強度の差を生じてしまう恐れが・・・



スマートフォンを活用するための基盤

－情報資産へのアクセスは社内・社外の2経路から。

社内利用であれば「ワイヤレスアクセスポイント」、社外利用であれば「アクセスゲートウェイ」が主役。



CTCSPがお勧めするリモートアクセスゲートウェイ

CTCSPがお勧めするリモートアクセスゲートウェイとは？

リモートアクセスゲートウェイ(FortiGateとは？)

CTC SP

複数のセキュリティ機能を統合し、コストを削減
運用コンソールも１つに

全てユーザー課金体系ではない

ファイアウォール

VPN

アンチウイルス

IPS

WANの最適化

アンチスパム

Webフィルタリング

アプリケーション
コントロール

情報漏洩
防止機能

L2/L3
ルーティング

FortiGateシリーズ製品ラインナップ

CTC SP

High

大規模・データセンター向け


FortiGate-3810D


FortiGate-3700D


FortiGate-3600C

中～大規模オフィス向け


FortiGate-1500D


FortiGate-1000D

小～中規模オフィス向け


FortiGate-500D


FortiGate-300D


FortiGate-200D

SOHO向け


FortiGate-100D


FortiGate-90D


FortiGate-60D

Low

FortiGateシリーズは豊富なラインナップを提供

FortiGateの優位性(1)

CTC SP

Comprehensive

FortiOS オペレーティング・システム

統合セキュリティ

High-Performance

FortiASIC ネットワーク・プロセッサ

CP:主にセキュリティ関連の処理
NP:主にネットワーク関連の処理

FortiASIC コンテンツ・プロセッサ

Real Time

FortiGuard サブスクリプション・サービス

FortiCare カスタマ・サポート

- 高速
- 省電力（汎用CPUの1/10)と発熱量の抑制

FortiGateの優位性(2)

・独自開発の「FortiASIC」により高パフォーマンスを実現：
ハードウェアレベルのアクセラレーションを実現する独自開発による2つのASICの実装しているのでオペレーティングシステム「FortiOS」と一体となり、最大のパフォーマンスと高いセキュリティを実現。

・アンチウイルス稼動でも全体性能を維持：
FortiGateは、マルチパスアーキテクチャを採用しているため、アンチウイルス機能を稼動しても全体性能が低下しません。また、定義ファイルと比較することでウイルスを検出するのではなく、プログラム・コードの動き自体を見て、ウイルスを検出するため、未知のウイルス検出スピードがNo.1です。

・クライアントライセンスは無制限：
FortiGateは、ユーザ数にかかわりなくアプライアンス単位のライセンス体系を採用しているため、イニシャルコスト、ランニングコストとも低く抑えることが可能。

・複数の仮想UTMを実現するVDOM機能：
FortiOSには、1台のFortiGateを複数の仮想FortiGateとして利用できる「バーチャルドメイン(VDOM)」という仮想UTM機能が実装されています。これにより、共通の管理方法を保ったまま、部門や部署あるいはユーザ企業ごとに独立したポリシーの設定と運用、管理者の設置が可能になります。

・第三者機関認定とファイル再構築スキャンの優れたセキュリティレベル：
フォーティネットのアンチウイルスアーキテクチャは定期的に第三者機関 (ICSA ラボ)の認定を取得。また、FortiGateは透過的に、クライアントに送信されるファイルを分析のために完全な形に復元し、圧縮ファイルは解凍して、ファイルの実行をエミュレートします。
これによりパケットのみのスキャンでは見つけられないマルウェアの検知も可能となります。

UTM導入することによるメリット

広範囲な脅威に対応

ファイヤウォール機能はもとより、複数の対策を１台で実現

ポイント①　運用効率が高い

導入負荷の軽減

導入は容易、複合的な脅威からネットワークを保護

ポイント②　導入し易い

低ランニングコスト

各検出データベースの費用がユーザ数に関わらず一定

ポイント③　導入コストが安い

一つの筐体でセキュリティ対策を実現可能

セキュリティ統合提案を実現するUTM(2)

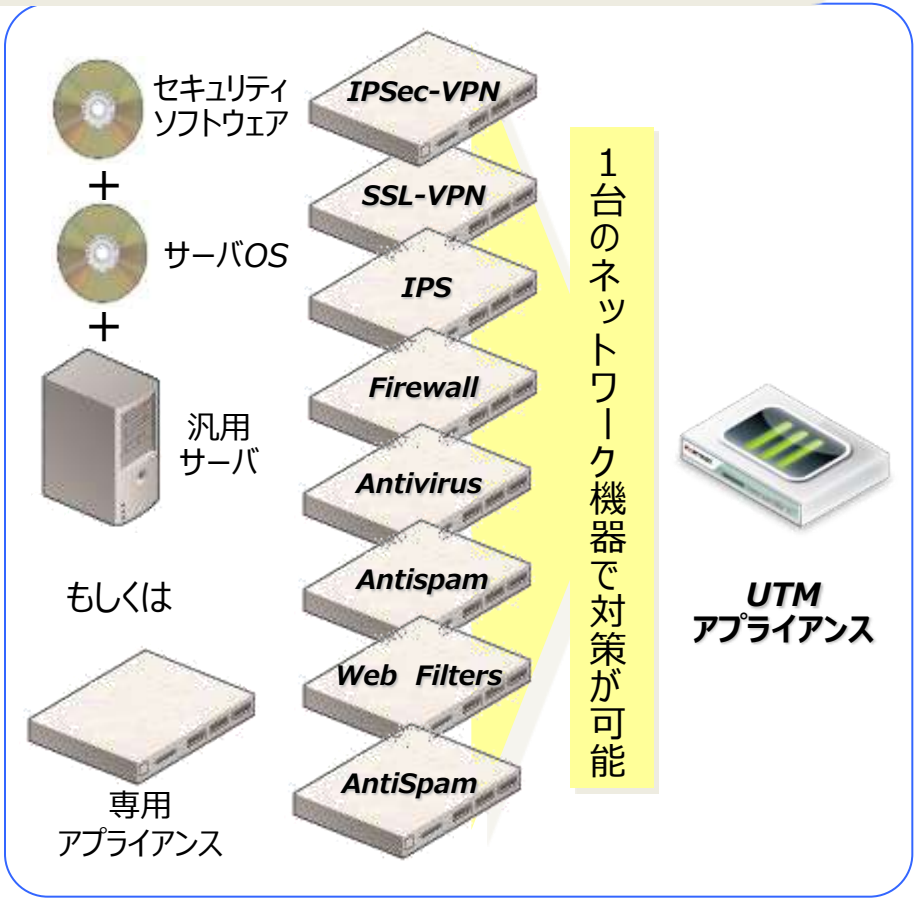
CTC SP

ポイント① 運用効率が高い

広範囲な
脅威に対応

ファイヤウォール機能はもとより、複数の対策を１台で実現

- **複数のセキュリティ対策を統合的に実現**
  - ファイヤウォール・IPS
  - IPSec-VPN、SSL-VPN
  - アンチウイルス、アンチスパム
  - Webフィルタリング
- **管理工数の削減**
  - 従来なら複数台分必要とされていたハード・ソフト等のシステムの管理が不要
  - 各サブスクリプションで検出されたログは一元的に管理
- **高いシグネチャーの信頼性**
  - 各種機能はICSA認定を取得



UTMによる対策

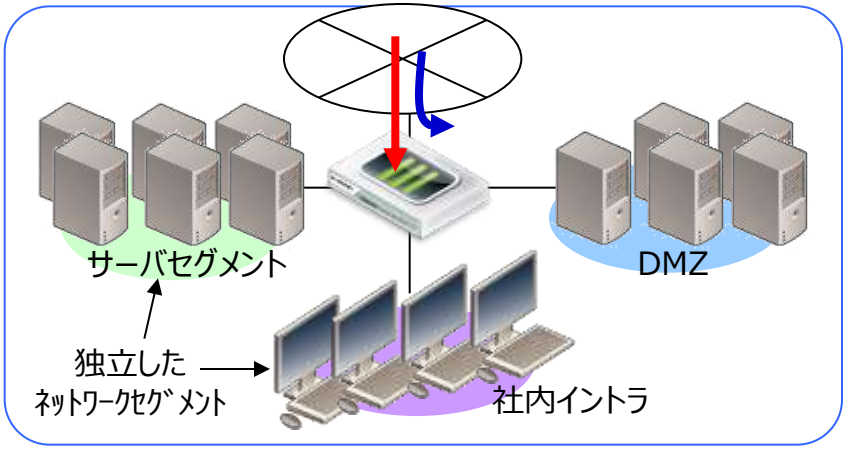
セキュリティ統合提案を実現するUTM(3)

CTC SP

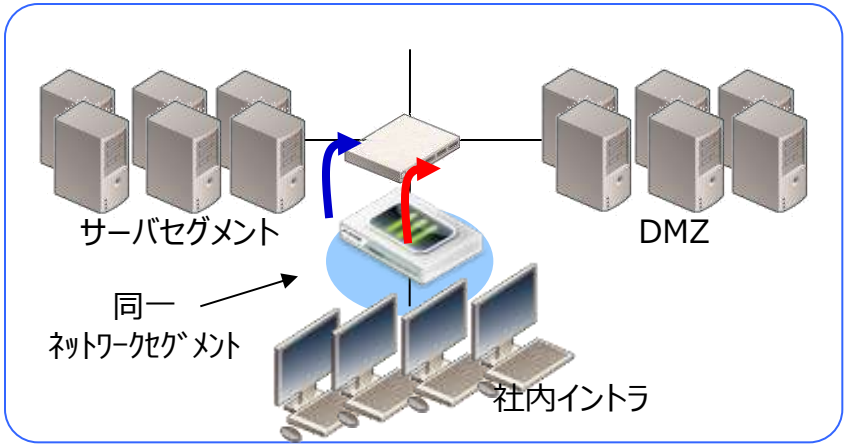
導入
負荷の軽減

ポイント② 導入し易い

導入は容易、複合的な脅威からネットワークを保護



ファイヤウォール機能も併用した例
（NAT／ルーターモード）



各種フィルタとして利用した例
（トランスペアレント／ブリッジモード）

- **用途例**
  - ファイヤウォール＋不正侵入対策
    - Firewall + IPS
  - ファイヤウォール＋ウィルス対策
    - Firewall + Antivirus
  - ファイヤウォールリプレース時にセキュリティ機能追加目的で導入

- **用途例**
  - 中小オフィスのセキュリティ対策
    - FW + AV + IPS + P2P/IM対策
  - メールセキュリティゲートウェイ
    - Antivirus + Antispam
  - ネットワーク構成の変更無しに導入可

セキュリティ統合提案を実現するUTM(4)

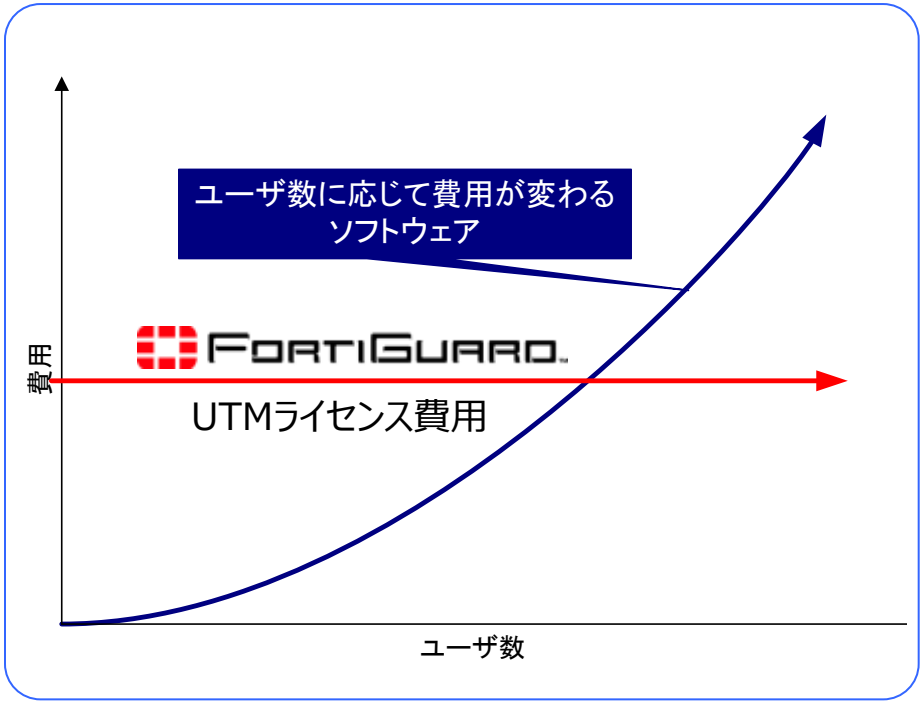
CTC SP

ポイント③　導入コストが安い

低ランニングコスト

各検出データベースの費用がユーザ数に関わらず一定

- **各種サブスクリプションサービス**
  - 各ハードに対するライセンスで、ユーザ数に関わらず一定の料金体系
  - 配下のユーザ数が多くなればなるほど、コストメリットが大きい
- **多重化ネットワークセキュリティ**
  - 既存他社セキュリティー製品に加え、２つめ、３つめのゲートウェイセキュリティを導入することで、ネットワークセキュリティの安全性を確保



ユーザ数比例型ライセンスとの料金比較イメージ

UTM市場における競合製品比較

CTC SP

FortiGateは全て自社でセキュリティー機能を開発

	パフォーマンス	ファイヤウォール	IPSec-VPN	SSL-VPN	IPS	アンチウィルス	アンチスパム	Webフィルタリング	IM/P2Pフィルタリング	集中管理製品の有無	ログ管理製品の有無
Fortinet	◎ FW/IP-SecからAV等、UTMの処理をASICで実施	○	○	○ オプションライセンス必要無	◎ 自社DB	◎ 自社DB	◎ 自社DB	◎ 自社DB	○	○ ハード＋ソフト（アプライアンス）	○
					ﾗｲｾﾝｽ更新時、機器へｷｰ投入が不要						
A社	○ ASICの処理はFW/IP-Secに限定	◎ 機能が豊富、実績多	◎ 実績が豊富	- SAシリーズでサポート 別製品	○ 自社DB	○ カスペルスキー	○ シマンテック	○ サーフコントロール	-	○ ソフトウェア	-
					ﾗｲｾﾝｽ更新時、機器へｷｰ投入が必要						
B社	○	○	◎ 元々はVPN専門機	○ 但しオプションライセンス必要	○ ﾕｰｻﾞ数ﾗｲｾﾝｽ	○ トレンドマイクロ ﾕｰｻﾞ数ﾗｲｾﾝｽ	○ トレンドマイクロ ﾕｰｻﾞ数ﾗｲｾﾝｽ	○ トレンドマイクロ ﾕｰｻﾞ数ﾗｲｾﾝｽ	-	-	-

IPSとアンチウィルスは同時に使えない

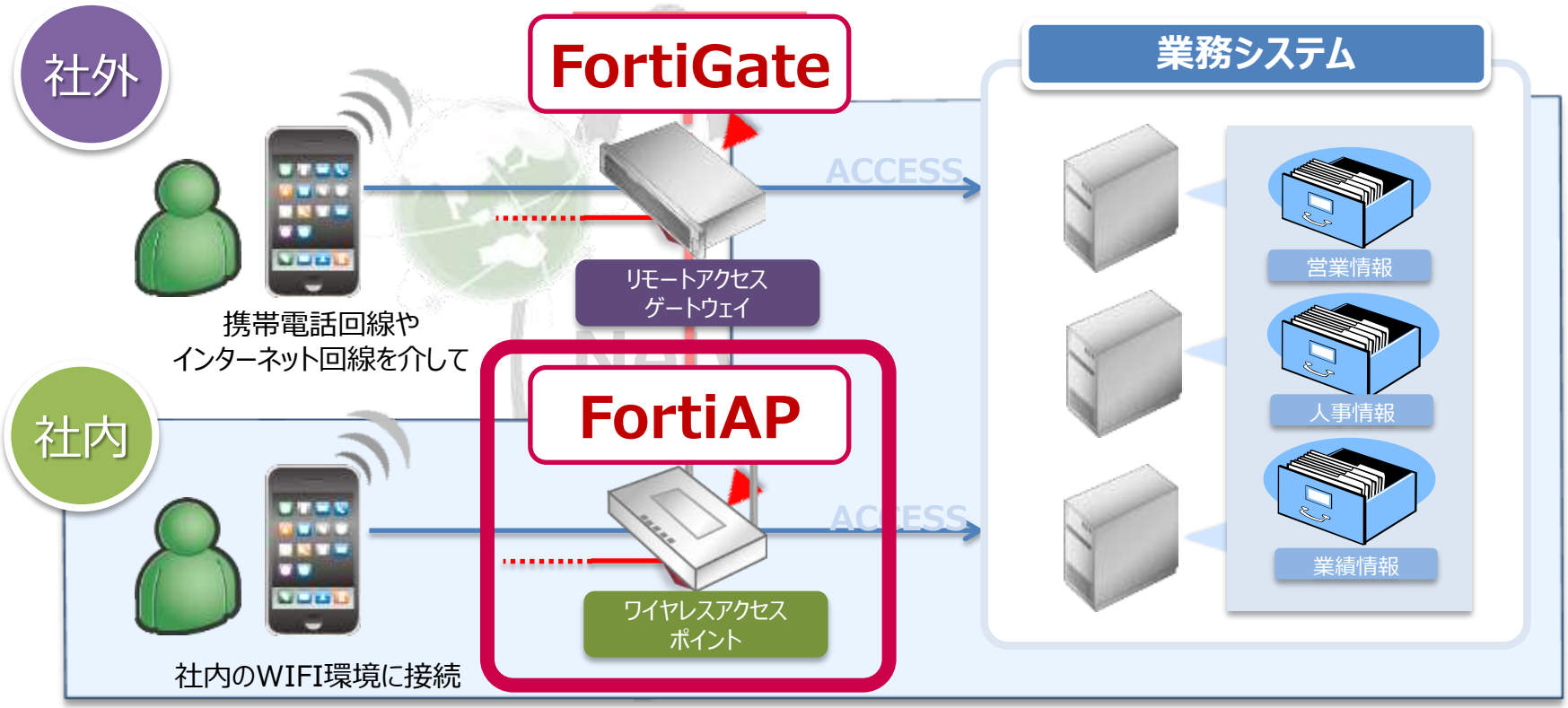
ﾓｼﾞｭｰﾙ方式で各種ｾｷｭﾘﾃｨｰｻｰﾋﾞｽを実現

Fortinetは自社で全てのセキュリティーサービスを提供。自社開発のハードウェアと合わせ高い親和性を実現し、結果として使いやすさと高いパフォーマンスを実現

スマートフォンを活用するための基盤

－情報資産へのアクセスは社内・社外の2経路から。

社内利用であれば「ワイヤレスアクセスポイント」、社外利用であれば「アクセスゲートウェイ」が主役。



CTCSPがお勧めするワイアレスアクセスポイント

CTCSPがお勧めするワイアレスアクセスポイントとは？

ワイヤレスアクセスポイント(FortiAPとは)

Fortinet社が販売しているFortiAPは、最新のIEEE802.11acやIEEE802.11n標準準拠の無線LANアクセスポイントです。リモートにある小規模の拠点／店舗の無線LAN接続を提供します。また、すべてのトラフィックをFortiGateコントローラへとトンネルする事により、FortiGateで提供可能なUTM機能を無線LAN環境で利用する事が出来るため、セキュリティの強化と容易な管理を実現します。

セキュアワイヤレス
アクセスポイント

無線コントローラ
＋UTM

セキュア
無線アクセス

■ FortiAPのターゲット

モバイル需要の拡大、コスト削減、タブレット端末普及、BYOD(私的デバイス活用)

WLANの見直し/再構築/新規採用

＋

無線環境はインフラの一部であり、ネットワーク全体として”セキュリティ”が保たれている必要ある

＝ **セキュアな無線環境**

無線コントローラはFortiGate

- **WLAN スイッチングとRF（無線電波）マネージメント**
- **SSIDやポリシーの管理**
- **自動無線リソース･プロビジョニング（ARP）**

  自動的なチャンネル選択（隣接APとのチャネル干渉を防ぐ）
- **認証**

  Wired and wireless 802.1x, Web-based captive portal, MAC address, Local user database, LDAP, RADIUS, TACACS+
- **暗号化**

  Open, Static and Dynamic WEP, WPA-TKIP, WPA-PSK-TKIP, WPA2-AES, WPA-PSK-AES, WPA Mixed mode
- **ユーザ･サービス**

  Captive portal, SSID to VLAN mapping, AAA VLAN assignment
- **ローミング**
- **不正無線APを検出してブロック**

FortiGateが無線コントローラになります！！

既にFortiGateをお使いの場合はコントローラを購入する必要はありません。
また、FortiGateのセキュリティをフルに使う事でセキュリティを高める事が容易です。

FortiAP製品ラインナップ

CTC SP

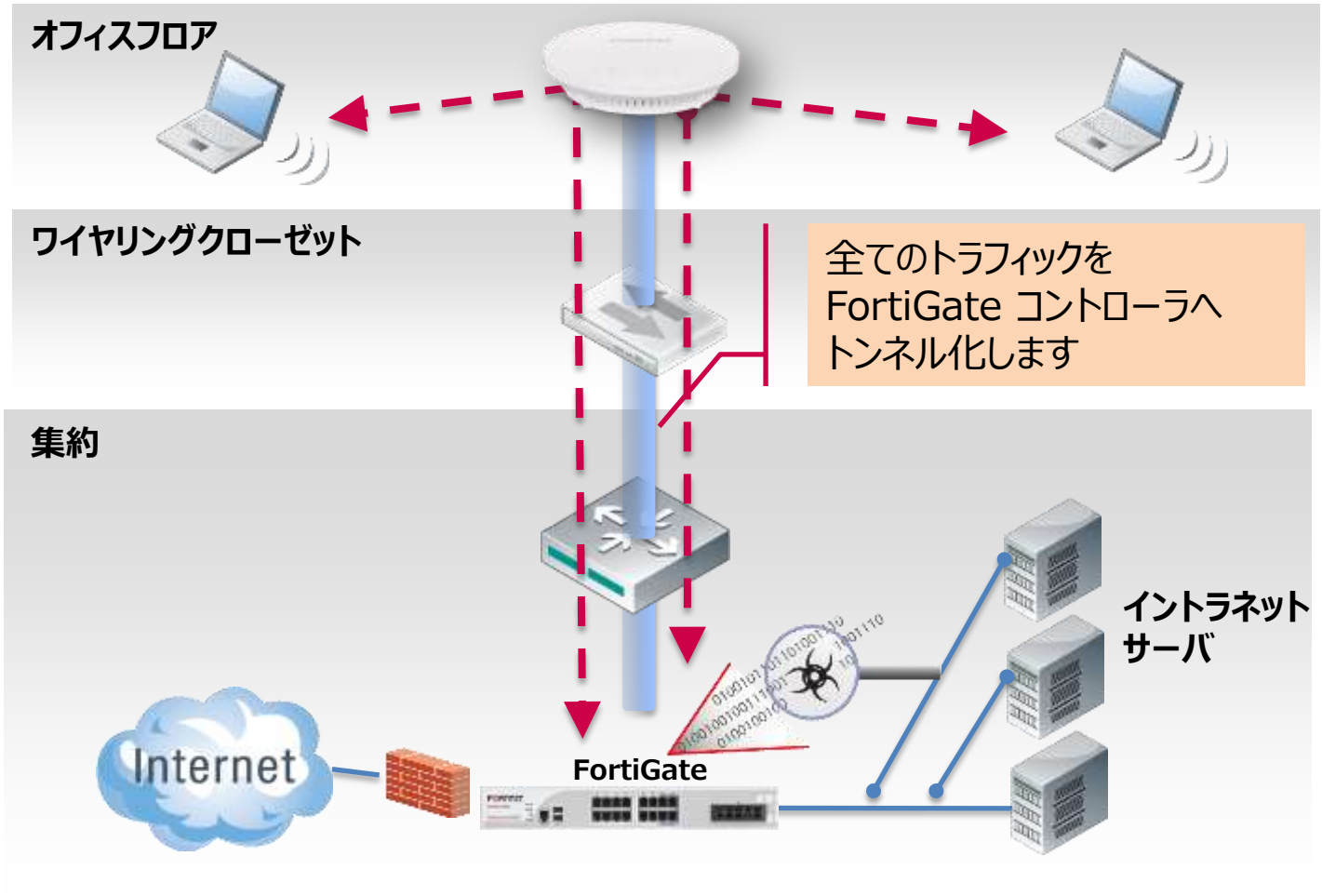
仕様	FortiAP-221B	FortiAP-221C	FortiAP-320C
設置環境	屋内	屋内	屋内・プレナム
アンテナ	4個（内蔵）	4個（内蔵）	6個（内蔵）
ラジオ１	2.4Ghz(IEEE802.11b/g/n) または5GHz （IEEE802.1a/n）	2.4Ghz(IEEE802.11b/g/n) または5GHz （IEEE802.1a/n）	2.4Ghz(IEEE802.11b/g/n)
ラジオ2	2.4Ghz(IEEE802.11b/g/n)	5GHz （IEEE802.1a/n/ac）	5GHz （IEEE802.1a/n/ac）
インターフェイス	1 x 10/100/1000	1 x 10/100/1000	2 x 10/100/1000
IEEE802.11nの機能	20 MHz / 40 MHzハイスループット（HT）モード対応 A-MPDU およびA-MSDUパケット集約をサポートし、最大伝送フレームを 拡張 Dynamic MIMO Power Saveによる消費電力低減		
サイズ	4.0 cm x 16.5 cm （高さ x 直径）	3.8 cm x 16.0 cm （高さ x 直径）	16.5 cm x 16.5 cm x 3.5 cm （奥行 x 幅 x 高さ）
重量	300g	300g	600g
消費電力（最大）	12.9W	15.7W	12.0W

FortiAP-221B

FortiAP-221C

FortiAP-320C

FortiAPの接続イメージ
　無線経由のトラフィックもUTMで検査（FortiGateコントローラへトンネル化する）



FortiGateは、ワイヤレスコントローラーとして機能する受け取ったトラフィックはUTM機能で検査されるため安心

FortiGate提案ケース（基本3ケース）

CTC SP

提案ケース①

各種セキュリティー対策の統合提案（コスト削減提案①）
（他社既存ユーザからの巻き取りの際、コストメリットが活かせる）

FW ＋ AV ＋ IPS ＋ IPSec VPN
専用機器

FW+AV+IPS+SSL-VPN

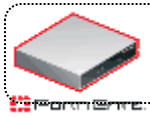
一つの機器に統合し、イニシャル
ランニング、運用コストを低減

提案ケース②

ファイヤーウォールのリプレース提案（アップグレード提案）
（FWにその他セキュリティー要件を加え、導入／運用コストを削減）

FW
専用機器

＋ FW



＋ AV + IPS + SSL-VPN + Web + AS

FWリプレースをFortinetで実現し
+αのセキュリティ要件

提案ケース③

メールセキュリティーのリプレース提案（コスト削減提案②）
（ユーザ数ライセンス不要、実績がありコストメリットの高いAV, AS）

AV ＋ AS
専用機器

＋ AV ＋ AS

トランスペアレントモードでウィルス
スパムフィルタを安価に導入

セキュリティー統合により提案／投資金額が下がることによる効果が利点

FortiGateの導入事例

FortiGate 某工場向けセキュリティ対策案件①

CTC SP

- **導入前の課題：**

  ネットワークセキュリティ製品とスパム対策を検討していたが、製品毎にシステム設計・運用が必要であり、それぞれコストが掛かることが課題であった。

- **選定した理由/採用理由：**

  UTM製品では知名度と安心感があり採用した。また、合わせてファイヤウォール製品でありながらも、スパム対策を実施できることも採用のポイントであった。

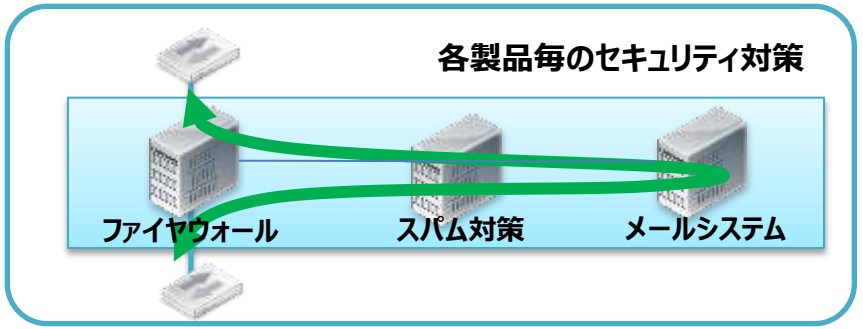
- **使用用途：**

  ファイヤウォールとアンチスパムの両方を利用し、安定稼働中。

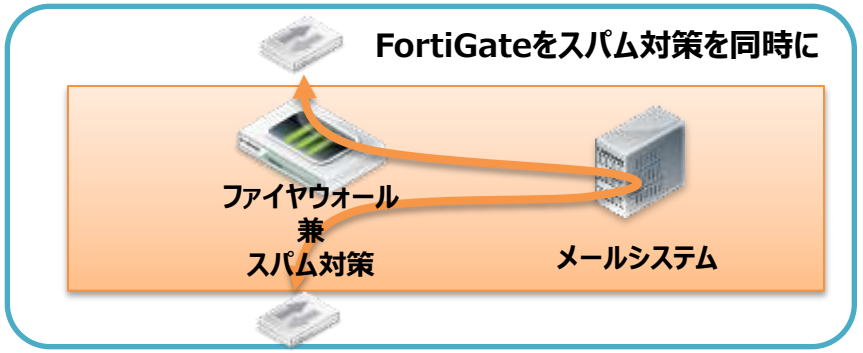
- **導入後の効果：**

  各製品毎に運用者を必要としていたが、FortiGateでは運用の効率化が可能となり、利便性も向上した。

変更前



変更後



FortiGate 某企業向けVDOM構築案件②

- **導入前の課題：**

  システム毎（4台）にファイアウォールを導入していたが、リソースに空きがあり効率的な運用が出来ていない状況であった。さらに、ファイアウォール毎の運用・保守コストが掛かるため、ランニング費用の課題もあった。

- **選定した理由/採用理由：**

  複数のファイアウォールをFortiGateの仮想ファイアウォール（VDOM機能）を利用し、1台で纏める事が可能であったことが選定理由。

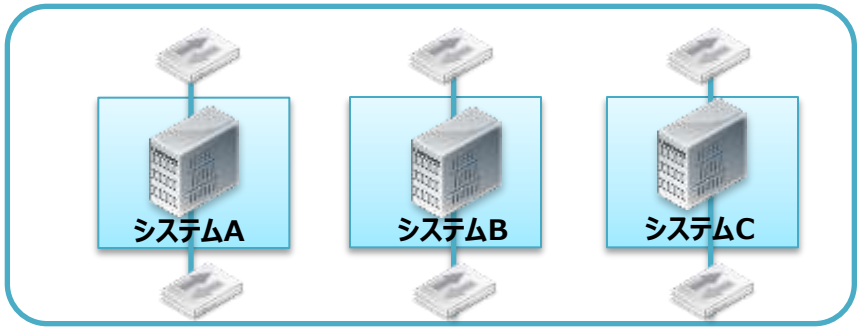
- **使用用途：**

  FortiGateのファイヤウォールとVDOM機能を利用。

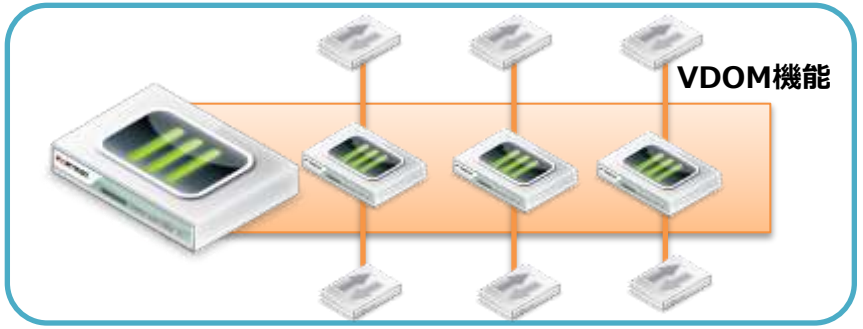
- **導入後の効果：**

  複数あったファイアウォールを1台にまとめることによって運用が簡素化できたこと、ランニングコスト（保守コストなど）も安価になった。

変更前



変更後



FortiGate 某大学向け無線アクセスポイント構築案件③

CTC SP

- **導入前の課題：**

  既設の無線アクセスポイントの保守更新のタイミングであった事、製品別にログ管理を運用していた事が課題であった。

- **選定した理由/採用理由：**

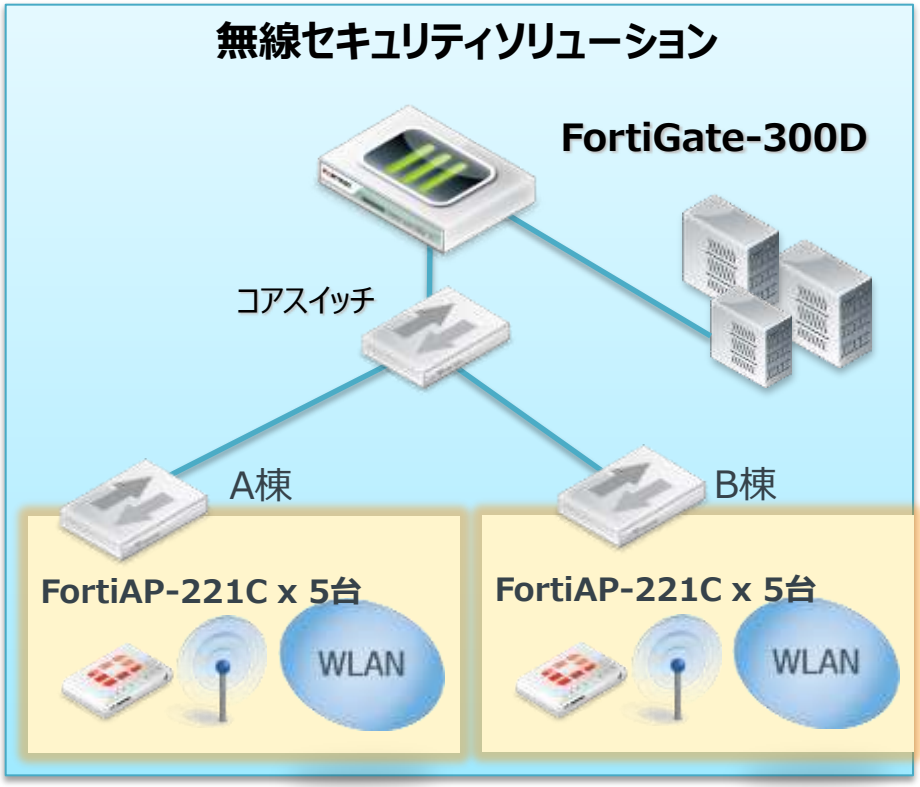
  既存導入されているFortiGateを利用して無線環境が構築できる点、無線LANの導入ログを同時に統合でき簡素化されたことが採用になった。

- **使用用途：**

  FortiGateは、ファイヤウォール、アンチウィルス、IPSを利用してネットワークの出入口でセキュリティ向上を図っている。また、教室・研究所などで無線環境を構築している。

- **導入後の効果：**

  エリア毎のセキュリティポリシーを統一、無線環境のログを統合することによって効果が向上した。



利用機能：ファイヤウォール、AV、IPS　選定機器：FG-300D、FAP-221C

認証アプライアンスであるNetAttestとは？

■ オールインワン認証アプライアンス

– 信頼性を追求し、シンプルで柔軟性のある仕組を実現

NetAttest EPS

RADIUS アプライアンス 国内シェア No.1

RADIUS　プライベートCA　ワンタイムパスワード

シリーズの歴史 10 年

シリーズ累計 12K+ 台

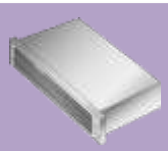
故障率 0.9 %

直感的な日本語GUI　初期設定ウィザード　堅牢な製品設計　簡便な冗長構成　障害時復旧計画　ソフトウェアメンテナンス

最適な設計　安定稼働　長期間運用

ワイヤレスアクセス

●Alcatel-Lucent ●Allied Telesis ●Avaya
●Buffalo ●Cisco Systems ●D-Link
●Fortinet ●FUJITSU ●FRUNO SYSTEMS
●Hewlett-Packard ●I・O DATA ●Meru Networks
●Proxim Wireless ●Sonic WALL



リモートアクセス

●Allied Telesis ●Array Networks ●Check Point Software Technologies ●Cisco Systems
●D-Link ●F5 Networks ●Fortinet ●FUJITSU
●Juniper Networks ●Sonic WALL ●YAMAHA

ワイヤードアクセス

●ALAXALA Networks ●Alcatel-Lucent
●Allied Telesis ●Brocade Communications
●Buffalo ●Cisco Systems ●D-Link
●Enterasys Networks ●FUJITSU ●HANDREAMNET
●Hewlett-Packard ●Hitachi Cable ●Panasonic

■管理者が証明書を発行する

高度な
PKIの知識を
要求しない
運用

NetAttest EPS Web管理画面（ユーザー一覧）

発行済

有効期限切れ

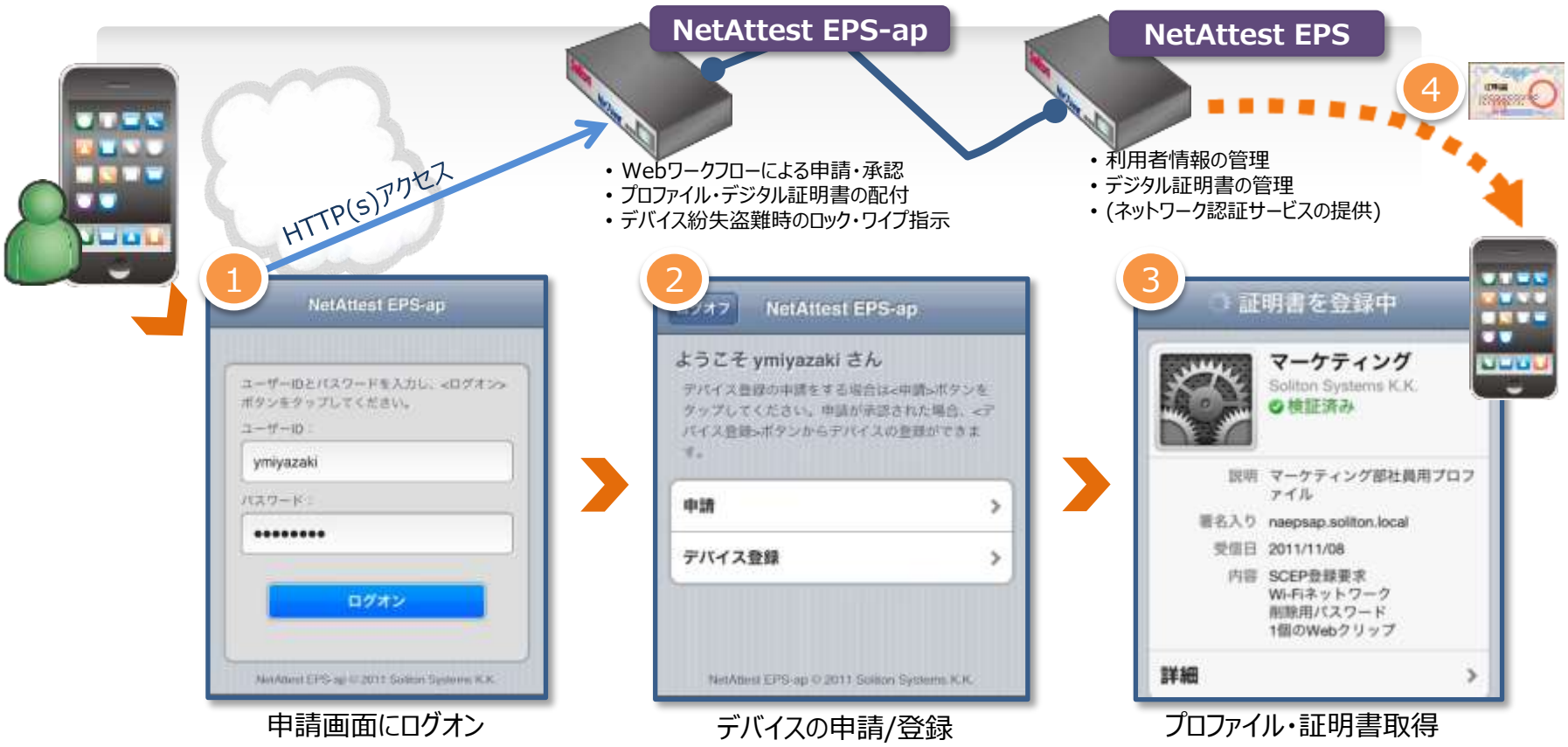
期限切れ間近

未発行

NetAttest EPS Web管理画面（ユーザー証明書発行）

■大量のスマホに証明書を展開する

申請システムで管理者の負荷を軽減
MDM機能も



申請画面にログオン　　デバイスの申請/登録　　プロファイル・証明書取得

NetAttestの導入事例

事例① スマートデバイスの利用を促進

CTC SP

PCと同様にデジタル証明書を選択。600台の iPhone/iPad への証明書配布を、わずか５日間で完了！

iPhone/iPadを600台展開
営業のメールやスケジュール利用に導入促進

×

「時間」をかけずに導入したい
証明書を簡単に配布できる仕組みが欲しい

×

「予算」なし・人海戦術も検討
携帯キャリアに依頼したら1台数万円の回答

お客様情報
・業種：製造業（水処理関連機器製造）
・従業員数：約4,700人（連結）

VPN & WirelessLAN

・VPN環境：
Cisco Systems社製
・無線LAN環境：
Cisco Systems社製
・スマートデバイス
iPhone/iPad

×

NetAttest EPS

・STモデル x2（冗長化）
- 機能拡張オプション
- 拡張CAオプション
・EPS-ap STモデル x1

証明書 | Radius | EPS-ap | VPN | iOS

<導入のポイント>

・無線LANおよびVPN環境に置いて、既に NetAttest EPS による証明書認証をPC向けに実施していた
・EPS-ap の追加により、スマートデバイスにも同様なセキュリティ基準を簡単に適用できる（実際、展開作業は1ヶ月で終了）
・日本語による管理やサポートが可能であることを含め、国産のメーカー製品である安心感があった

事例② Google Appsを社外から利用

CTC SP

Google Appsへの社外利用環境を「セキュアブラウザ+デジタル証明書」の最新ソリューションで構築！

社外からGoogle Appsの利用
会社のIPアドレスでアクセス制限している

×

会社支給端末とBYODの混在
iOS・Android端末両方に対応できること

×

端末にデータは残したくない
利用者および端末の認証強化を行いたい

お客様情報
・業種：情報通信業（情報サービス）
・従業員数：約2,200人

Soliton SecureGateway

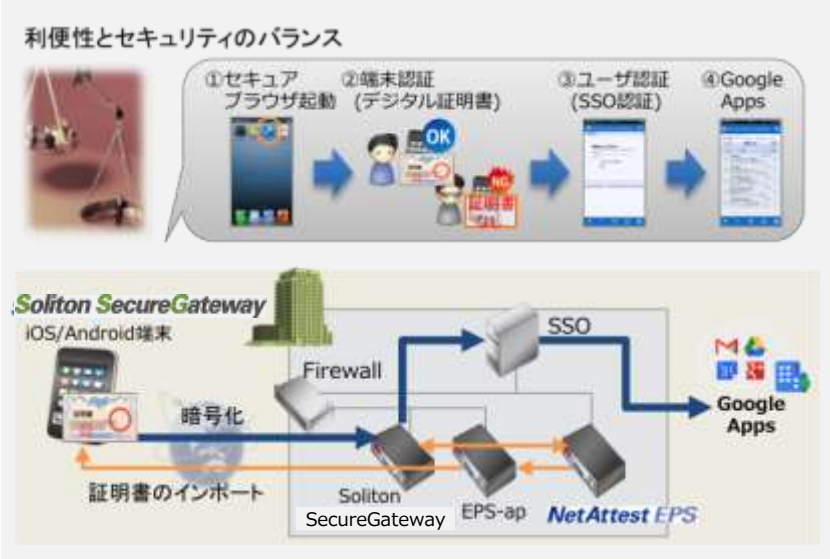
・STモデル x1
- 対象端末：iOS/Android端末
- 利用者数：500人
- 利用アプリ：Google Apps

×

NetAttest EPS

・STモデル x1
- 機能拡張オプション
- 拡張CAオプション

・EPS-ap x1



証明書 | EPS-ap | Gateway | iOS | Android | BYOD

<導入のポイント>

・Google Appsへのスムーズなアクセス、iOS/Android対応、証明書連携などから Soliton SecureGateway を選択。
・①利用者IDによる認証　②セキュアブラウザの有無　③証明書による端末認証の「3要素」認証が上層部の評価を得た。
・セキュアブラウザから証明書認証まで一貫して同一メーカーのソリューションであるためサポートが安心。

他のNetAttestの事例

CTC SP

事例

株式会社大林組
3,000台のタブレット端末で作業の効率化と建設品質の向上を実現。 ソリトンシステムズの「NetAttest EPS」と「NetAttest EPS-ap」を採用し、 無線ネットワークの導入・運用における課題を払拭。

PDF　詳細はこちら

独立行政法人 理化学研究所
研究者同士の活発な交流を支える無線ネットワーク環境を整備。 オールインワン認証アプライアンス NetAttest EPSを採用し、 無線LANローミング基盤「eduroam」への参加を短期で達成。

PDF　詳細はこちら

福井県越前市
「SmartOn職員証により、教育ネットワーク上の学校パソコンからでも、行政ネットワークにログオンできます。災害発生時に、学校を避難所として使用する時に役立つ仕組みです。」

PDF　詳細はこちら

越谷市教育委員会
小中学校の無線LANを安全に運用する「NetAttest EPS」。より分かりやすい授業を実現した埼玉県越谷市教育委員会の先進的取り組み。

PDF　詳細はこちら

まとめ

■ 情報システムにもとめられるもの

① マルチデバイスによるワークスタイルに対応する

② シャドーIT化を払拭させるためにセキュリティ制御が必要

③ システム導入の順番を守ってモバイルワークを推進

■ CTCSPからご提案するポイント

① 認証・識別を行うアクセスゲートウェイはFortiGate/FortiAP

② オールインワン認証アプライアンス（デジタル証明書を用いたセキュリティ制御）であるNetAttest

お気軽にCTCSPにご相談ください！

お気軽にご相談下さい。

CTC SP

シーティーシー・エスピー株式会社

ソリューション企画推進部　プロダクト推進１課

sp-admin@ctc-g.co.jp

TEL：03-5712-8070

http://www.ctc-g.co.jp/~ctcsp/