BIG-IP APMの事例に学ぶ

アジェンダ

1. **リモートアクセス環境の変化**
2. **事例**

リモートアクセスの本質的な要件は変わらない

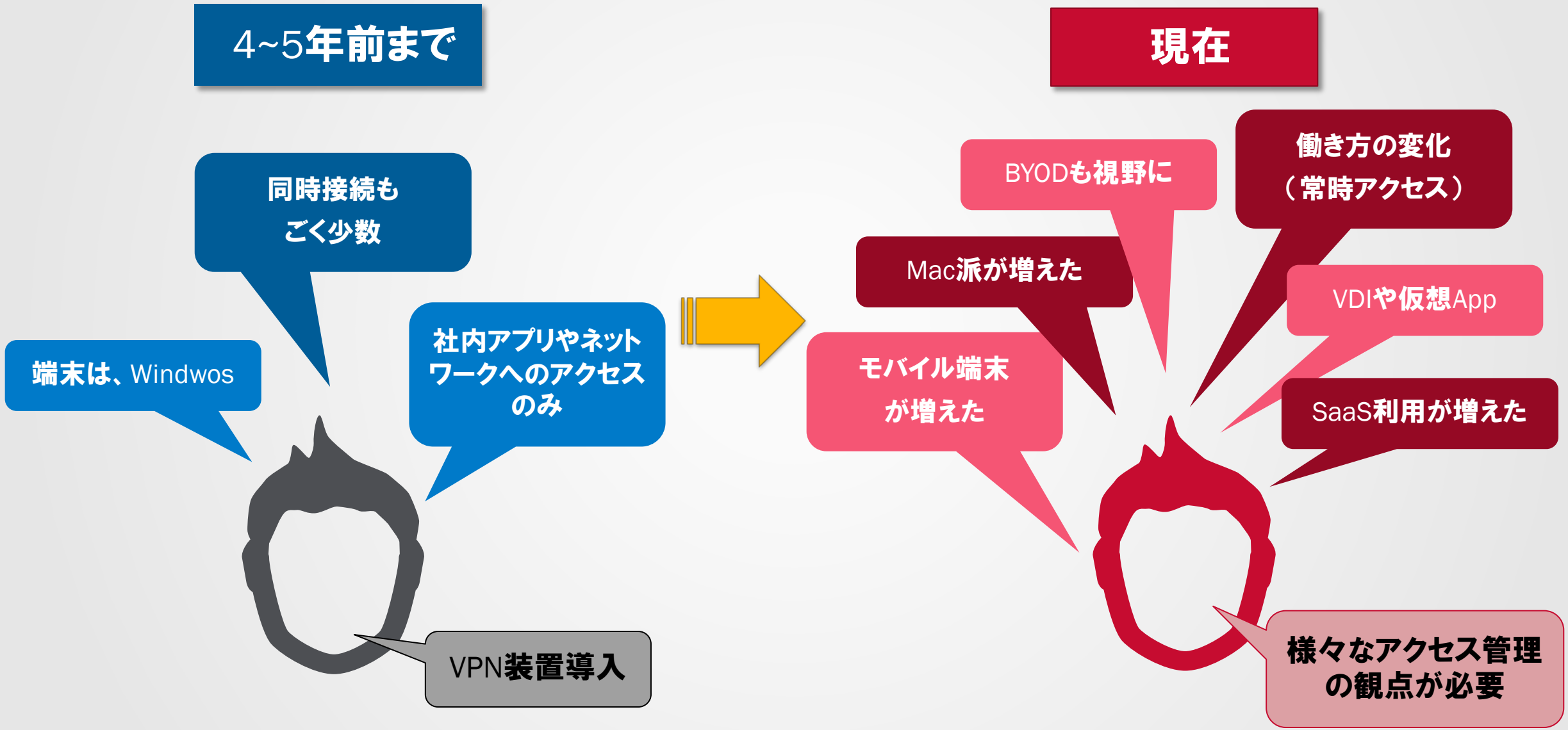
どのデバイスでも

どこからでも

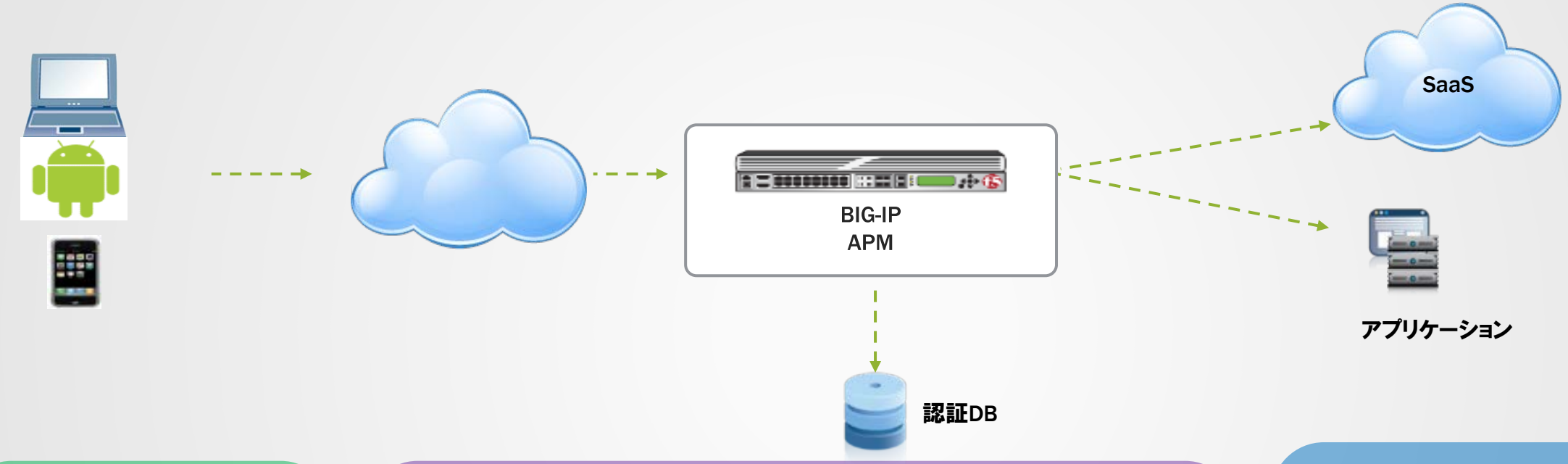
いつでも

ビジネスデータにアクセスして、仕事をしやすくしたい！
でも、「安全」かつ「手軽に」。

リモートアクセスにおける環境変化が提案のチャンス



BIG-IP APM(Access Policy Manager)とは？
様々な端末からのアプリケーションアクセスを安全かつ便利にする



クライアント
Windows
Mac
Linux
IOS
Android
WM

ログオン前チェック
Antivirus
Firewall
File info
Registry info
Process info
Window info

認証方式
Form Based
Certificate
Kerberos
Basic Auth
NTLM
SAML

認証
Radius
LDAP
Active Directory
SecurID
HTTP FORM
Kerberos
SAML
OTP

シングルサインオン(SSO)
HTTP Basic
Form Based
NTLM v1/v2
Kerberos
SAML

アプリケーション
Web Access
Web portal (webtop)
- SSL VPN
- Portal Access (web proxy)
- Application Tunnel (tcp proxy)
- VDI

GApps/Office365/Salesforce/Cybozu

事例 6つ

No	ユーザプロファイル	ソリューション タイプ	内容/ポイント
1	大手生命保険	iPad/SSL-VPN	iPadからのリモートアクセス、ユーザ属性に応じたアクセスコントロール
2	メガバンク	SSL VPN/VDI	SSL VPNとVDIを組み合わせたテレワーク環境
3	製造業	iPhone/ActiveSync	マルチデバイスによる運用負荷の軽減、コスト削減
4	IT関連サービス	SSL VPN	GW統合、Juniperからのリプレイス、コスト削減
5	ソフトバンクテレコム	SSL VPNサービス	マルチテナントサービス、コスト削減
6	大手建設業	Office365 フェデレーション	Office365へ強力なアクセスセキュリティ

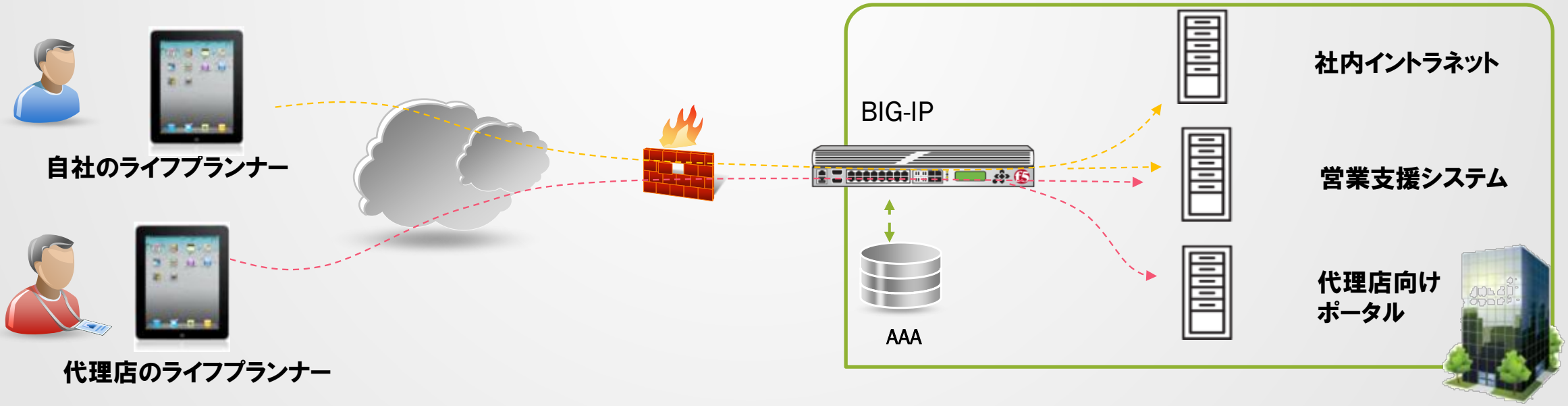
1. 大手生命保険/ライフプランナーの営業支援
iPadからの業務アプリへアクセスセキュリティ強化

■セキュリティ課題

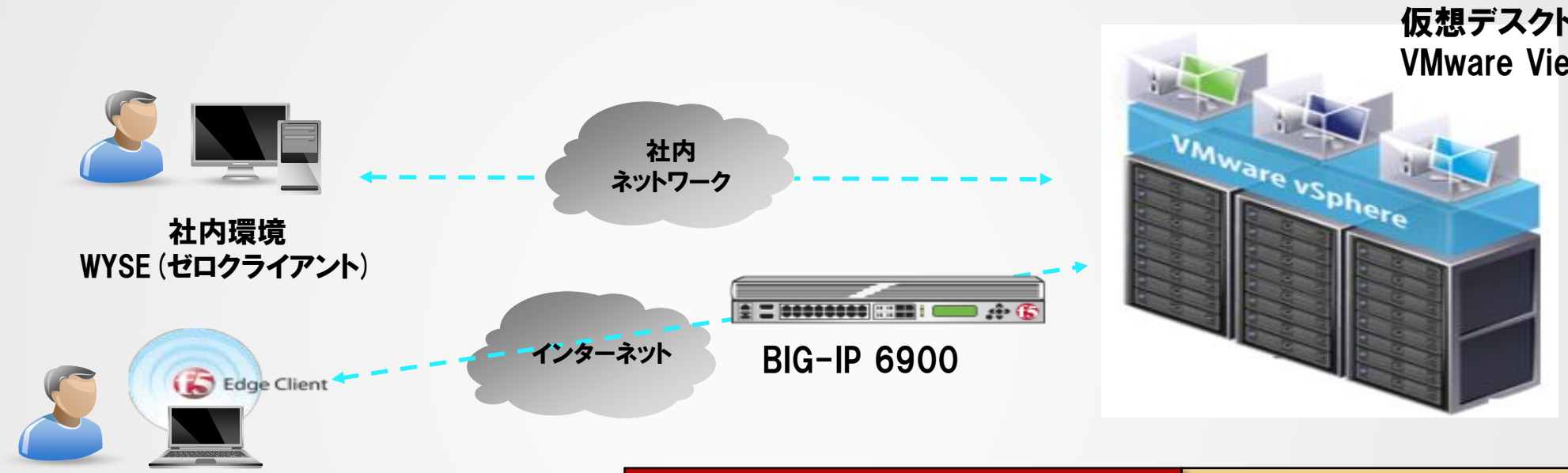
- 自社ライフプランナーおよび代理店(3000店舗) 15000ユーザのアプリへのアクセスコントロール
- スマートデバイス(iPad)のセキュリティ強化 とユーザビリティの向上
- 情報漏えい(認証強化、利用するアプリケーションの制限）

■解決策

- 認証プロキシ、シングルサインオンによる使いやすさ
- 自社と代理店のライフプランナーのアクセスコントロール
- ユーザIDとクライアント端末の紐づけを特定し、ポリシーに違反した場合はアクセス拒否
- MDM機能との連携

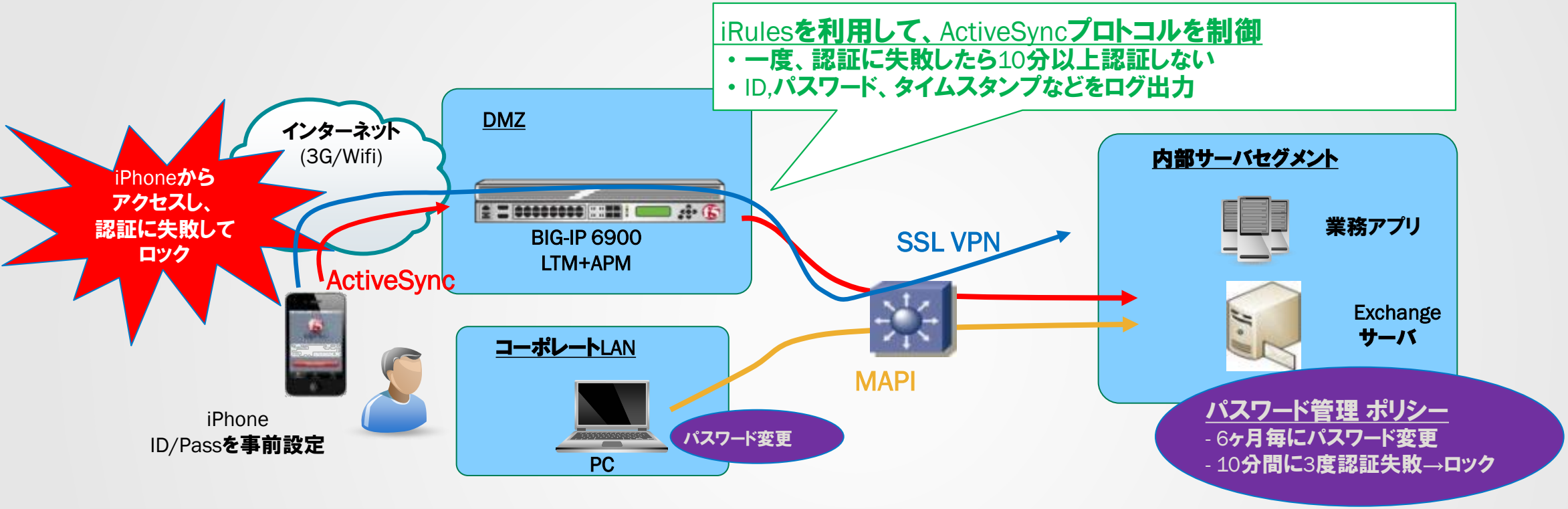


2.国内メガバンク – テレワーク導入事例
デスクトップ仮想化によるセキュリティ強化とアクセスの解放



背景/セキュリティ課題	ソリューション
•VDIによりクライアントにデータが保存されない •場所や端末に依存しない勤務環境を実現 •VDIへのアクセスを如何に安全するか	•ワンタイプパスワード •SSLクライアント認証 •ID/端末を特定 •上記のアクセス連携をBIG-IPで実現し、ポリシー違反ばアクセス拒否

3.国内大手製造業
スマートデバイス数万台の活用とiRulesによる運用負荷軽減



背景/課題	ソリューション
•iPhoneを従業員数万名に配布し、業務効率化 •ActiveSyncとSSL VPNと使ってリモートアクセス •パスワードを変更するとアカウントロック、管理者にロック解除の依頼が多発、原因はiPhoneからのActiveSyncプロトコルの認証失敗 •対応製品を探したが存在しない。	•BIG-IP APMのSSL VPN機能を使ってアプリケーションに依存なくリモートアクセス • ActiveSyncプロトコルは、認証が失敗した場合、一定時間 Exchangeサーバに認証しない様にiRulesを使ってアカウントロックの問題を解決

4.背景：IT関連サービス担当者20代の声

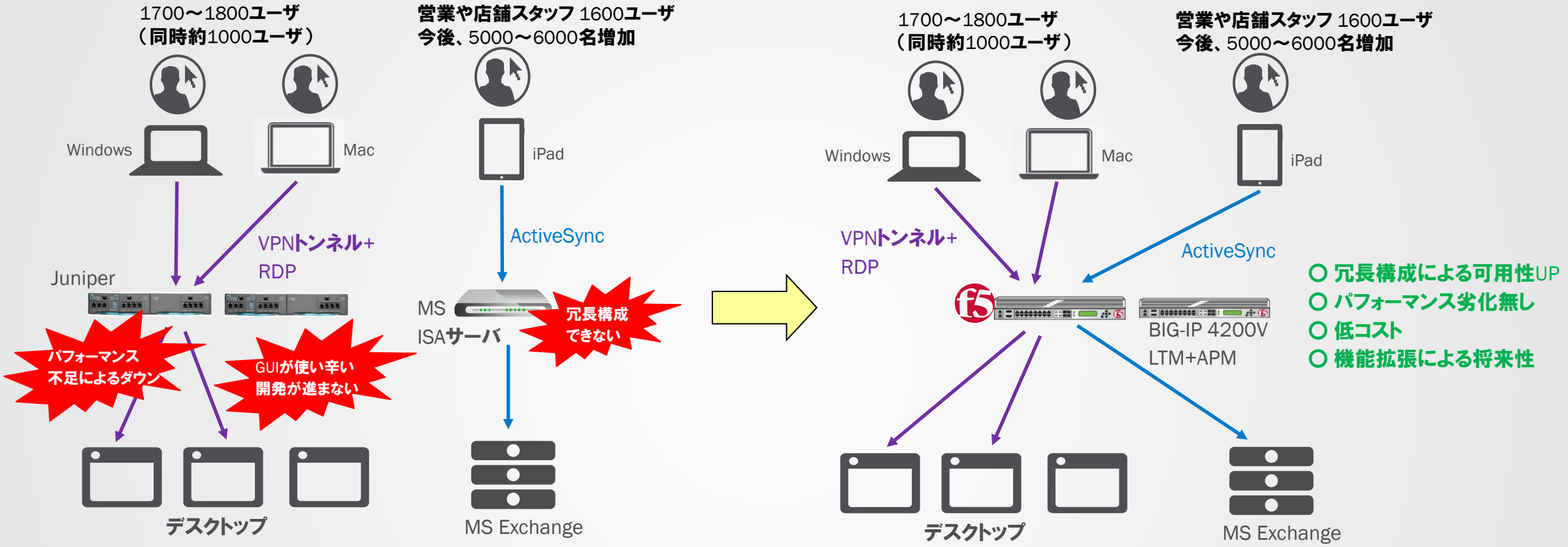
ITインフラ担当者

“マルチデバイスに対応するために、分散してしまったゲートウェイ製品を統合したい。また、ベネッセ事件が発端で、セキュリティ強化の要件が高まっている。”

“Juniper SAを7年程 運用しています。4年程前から、展開先店舗や営業スタッフのiPadの利用が増えてきました。メールやスケジュール管理をしたいという要望に対応する必要がありました。当時のJuniper SAでは、未対応だったので別途MS社製ISAサーバを経由したExchange ActiveSyncを実施。ISAは、冗長化ができない問題と販売終了の問題があり、IAサーバのハード保守が切れるタイミングで、新しいGW製品の導入を検討していました。”

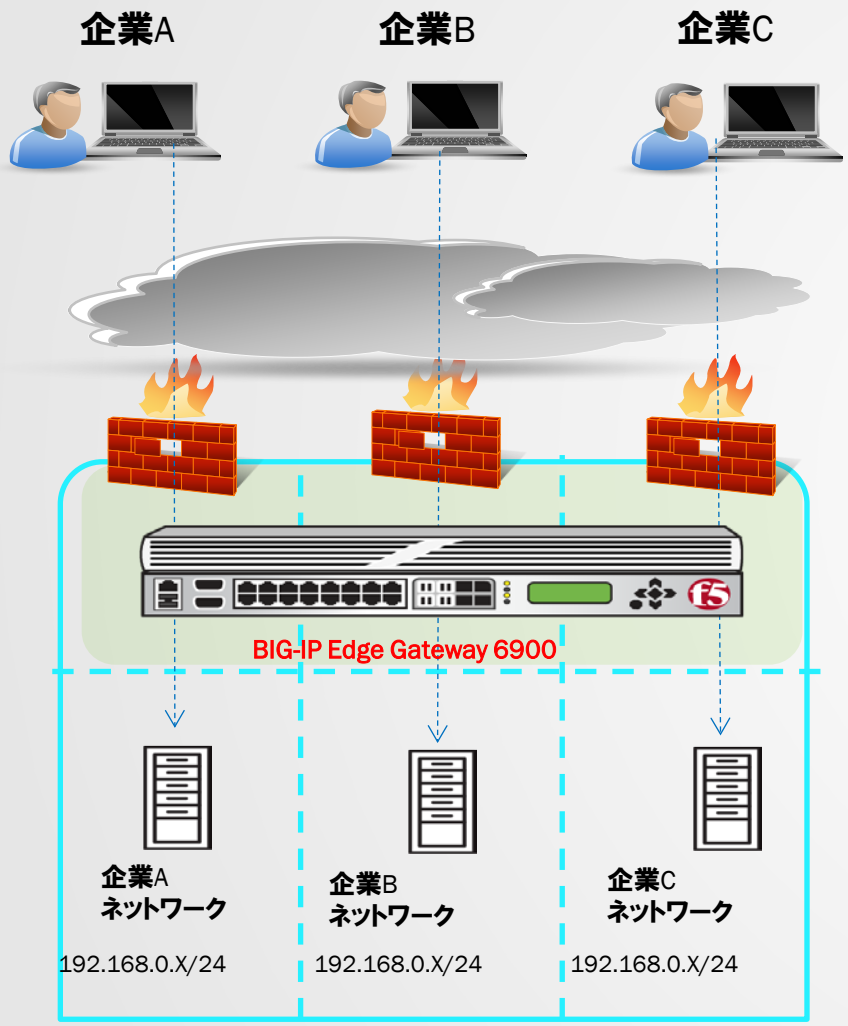
“Juniper MAGとBIG-IP APMを比較検証しました。Juniperは、最新バージョンでもGUIが使いづらいですし、機能拡張がされていない印象を受けました。F5 BIG-IP APMは、VPEによるエンドポイントセキュリティが非常にわかりやすい点が気に入りました。Juniperは、ログオン失敗原因のメッセージが出せないため、ユーザへの確認負荷が非常に重かった。BIG-IP APMであれば、失敗原因が詳細に追えるので運用負荷も下がります。また、6,000同時接続で相見積もりを取りましたが、JuniperはF5よりも1.4倍ぐらいの価格でした。”

4.JuniperとMS ISAをBIG-IPへ統合し、可用性確保と低コスト化を実現。



背景/課題	ソリューション
•iOSからメールとスケジュールを使う為に、別途 MS ISAサーバを構築したが、冗長構成が組めないので可用性に課題あり •Juniperのパフォーマンス不足、同時接続1000を超えてくるとログインできない。デスクトップアクセスができない事での業務停止の障害が2回発生し問題となる •Juniperのエンドポイントチェックが使い辛く、認証失敗の理由がわからない。 •Juniperの最新OSを検討したが、あまり変更点がなく今後の開発が不安。	•Juniper SSL VPNとMS ISAをBIG-IPへ統合し、冗長構成で可用性を確保。 •今の所、パフォーマンスダウン無し。 •Juniper MAGとBIG-IPで見積もり(条件:6000同時接続) Juniperの方が1.4倍ぐらい高かった •BIG-IP APMのエンドポイントチェックが非常にわかりやすかった。ログオン失敗原因がログ出力されるので運用が楽に。 •マルチデバイス対応やアクセス方式が複数用意されており、機能拡張が進んでいるので今後も安心して使用

5.ソフトバンクテレコム様 - ホワイトクラウドVPNサービス



※IPアドレスが重複しても問題なし

「クラウドサービスに欠かせないマルチテナント環境を高いレベルで実現できるのはBIG-IPだけでした。」

ソフトバンクテレコム株式会社
営業統括 営業開発本部 ビジネス開発統括部 セキュリティサービス開発部 第4 課
米田 章宏 氏

背景/課題

- 従来のサービスは、設備の無駄が多くコスト増
  2種類のサービス提供(占有、共有)していたが、帯域保障を検討すると、最大のキャパシティを考慮した設備投資が必要
- クラウド型サービス = 従量課金(アカウント数ベース)
- クラウド型で迅速かつ低コストなサービス提供には、ユーザ毎にIPアドレスが重複しても動作するマルチテナント機能が必須

解決策

- BIG-IPでなければマルチテナントができない(IPアドレス重複機能)
- 強力なセキュリティ機能を備える
  スプリットトンネルやPKIクライアント認証連携
- 開通までの時間を1/2、エンジニア作業量を1/10まで削減
  従来は機器の調達や設置、設定などの工程が必要だった
- iPhone/iPadなどスマートデバイスとのクロスセリング効果

6.背景：建設業 IT企画担当者の声

IT企画担当者

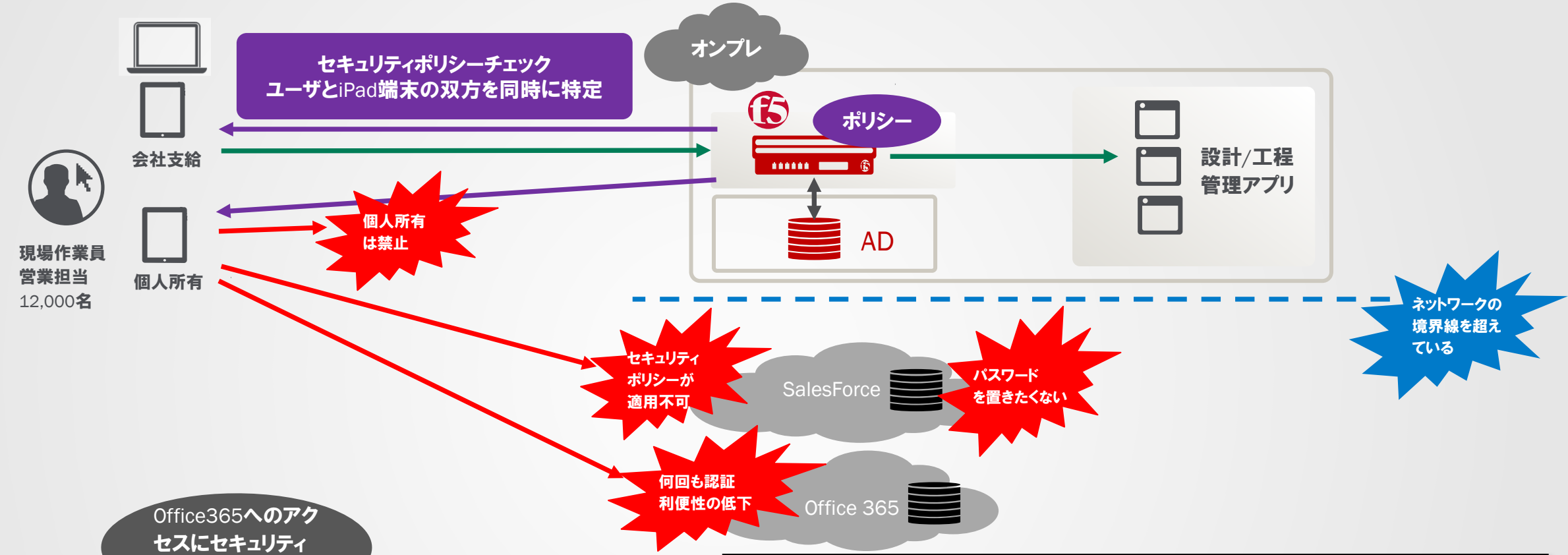
“国内拠点が300程度、12,000名のユーザがいます。10 年前にオンプレミスでコミュニケーション基盤を構築しアップデートしながら運用してきました。ストレージ容量を考えると各ユーザのメールボックス容量を2Gに制限。しかし、図面データなどメールに添付されるファイルの大容量化が進み、少ない容量での運用は辛いものでした。容量制限を超えるユーザには個別連絡して『サーバからのメール削除』をお願いしてきました。特に、ユーザが役員クラスの時は、気を使います。。。また、ハードやソフトの保守コストが負担となっていました。Office365はメールボックス容量が25G提供されており助かります。また、運用コストの軽減を考えてクラウドへの移行を決意しました。”

“現場作業や営業用に、iPadを約5,000台展開している。リモートから、設計や工程管理のアプリケーションには、VPN経由時に端末特定のアクセスポリシーをチェックしている。Office365サービスも同じアクセスセキュリティにしたいがサービス提供が無く困りました。”

ITインフラ担当者

“4年前にSalesforceを導入済み。今後もSaaSが増加が予想されるので、アカウン管理負荷やユーザの認証の手間を考えると、ID/パスワードはオンプレミスのADと同じ物でないと管理できません。”

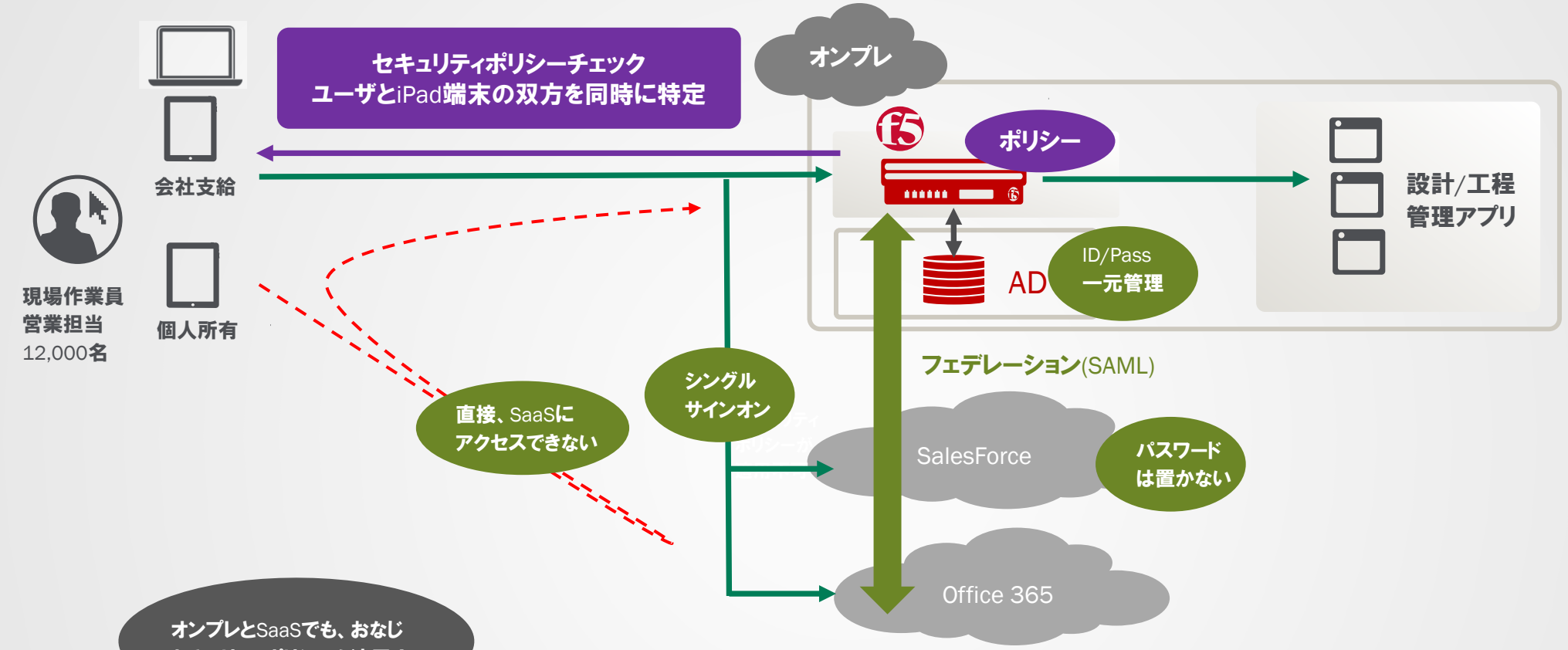
6.大手建設業 – 課題 SaaSアクセスのセキュリティチェックが不十分



背景/課題

- Salesfoce / Office365などクラウドサービスへの積極的な移行が将来に渡り続く
- オンプレのアプリには、個人と端末を識別するセキュリティポリシーを適用しているが、SaaSへ直接アクセスされるとセキュリティポリシーがかけられない
- クラウドにはパスワードを置きたくない。
- ユーザがID/パスワードを何回も入れる必要がある。
- アカントライフサイクル(追加、削除、変更)を考えると、社内のADにアカウント管理を一元化したい

6.大手建設業 – クラウドフェデレーションによりセキュリティチェックをSaaSにも適用



解決

- F5 BIG-IP とSaaSをSAML 2.0を使って信頼関係を構築（フェデレーション）
  BIG-IP (Idp)、SaaS(SP)、ネットワークの境界線を越えたアプリケーションレイヤーで
  安全性を担保
- SaaSには、オンプレのポリシーチェックをパスしないとアクセスできないので
  セキュリティ強化
- ID/パスワードは、ADを一元管理で、SaaSにはパスワードを置かないので安全
- シングルサインオン（オンプレ、Salesfoce,Office 365・・・）による利便性向上

Solutions for an application world.