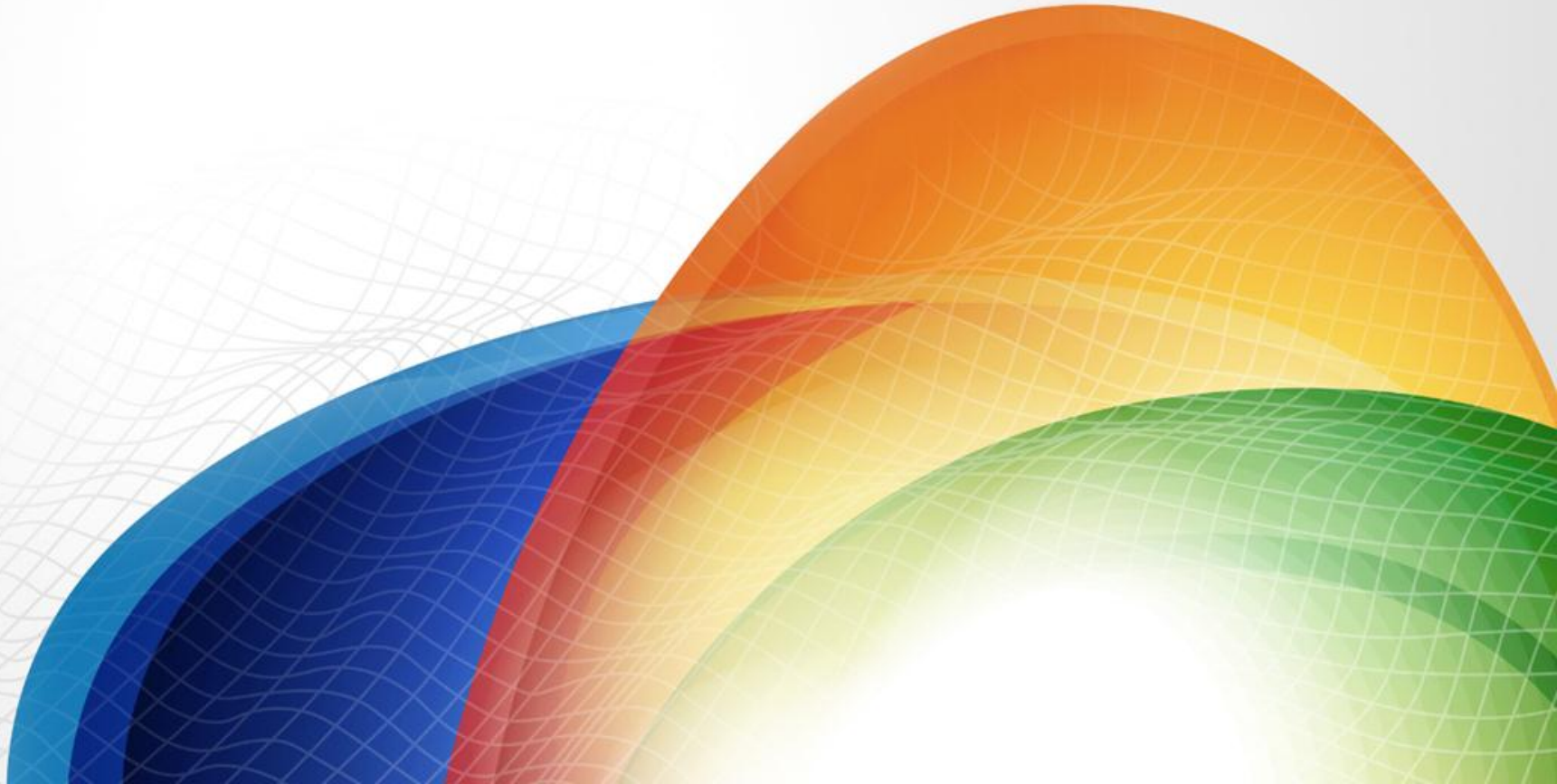
BIG-IP Access Policy manager (APM)

SSL VPNリモートアクセス・アクセス管理・認証基盤統合ソリューション

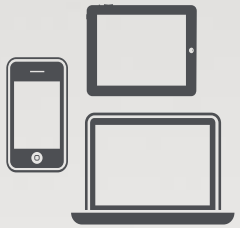


激変するユーザー環境に
最適なソリューションを提供するF5

アプリケーションのWeb化

71% の情報通信業界有識者が2020年までにほぼ全てのビジネスパーソンがweb/モバイル経由で業務に従事すると予測

スマートデバイスの爆発的増加



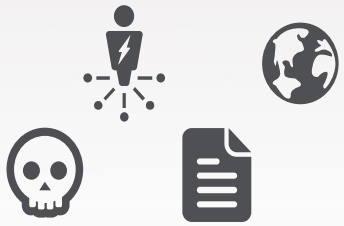
95% のビジネスパーソンが1台以上のモバイル機器を利用

1.3億の企業が2014年までにモバイル・アプリケーションを利用するようになる

進化し続ける外部脅威

58% のインターネット犯罪が思想・活動家の関与するもの

81% インターネット被害がハッカーに関連するもの

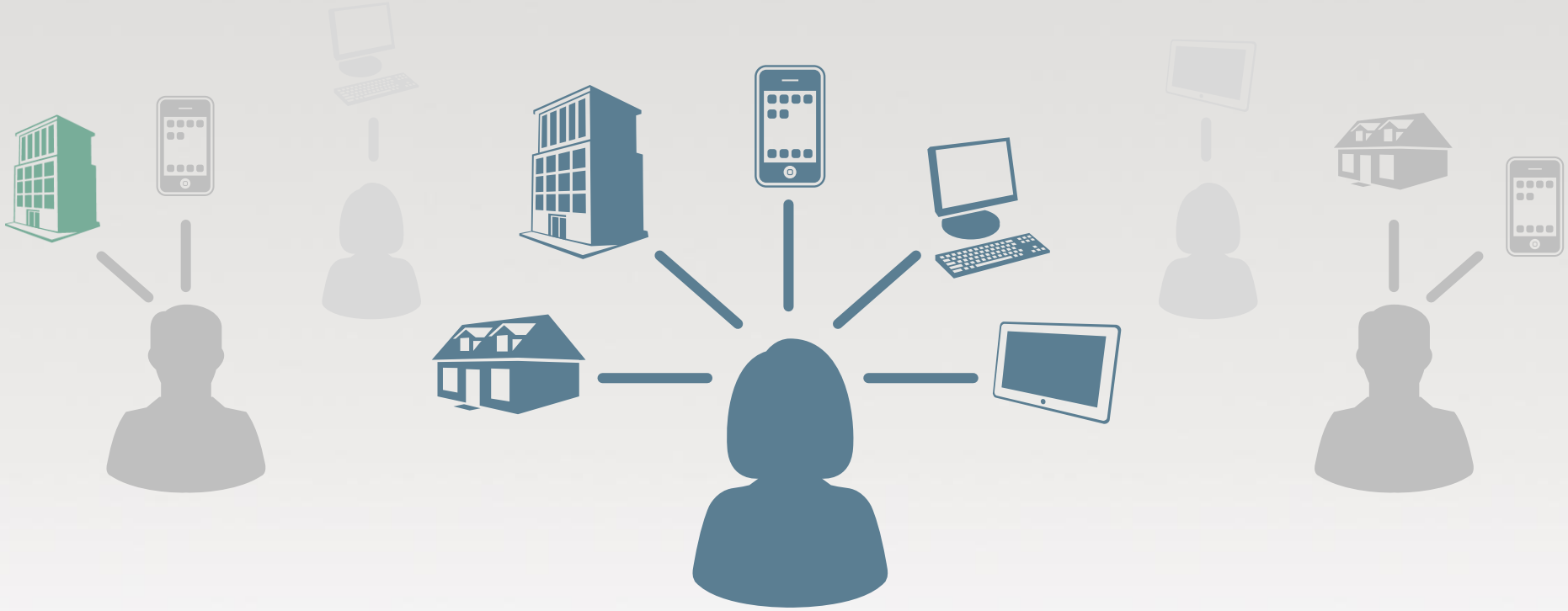


クラウドへの移行が加速

80% の新しいアプリケーションはクラウドベース

72% のCIOはアプリケーションをクラウドに移行・移行予定

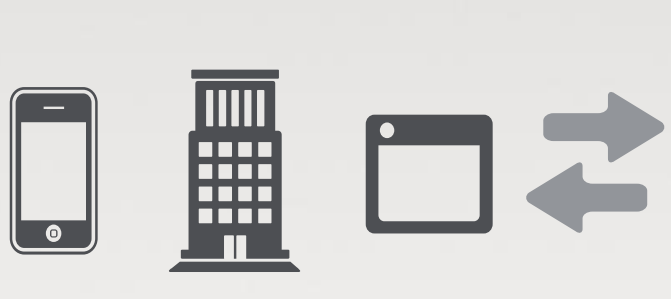
ユーザが求めている事とは



エンドユーザは、どのようなアプリケーションに対しても、
いつでも、どこでも、自由にアクセスできる事を求めている…

F5はアプリケーション、ユーザー・アクセス端末情報への高度な可視化と管理性をご提供します

Users

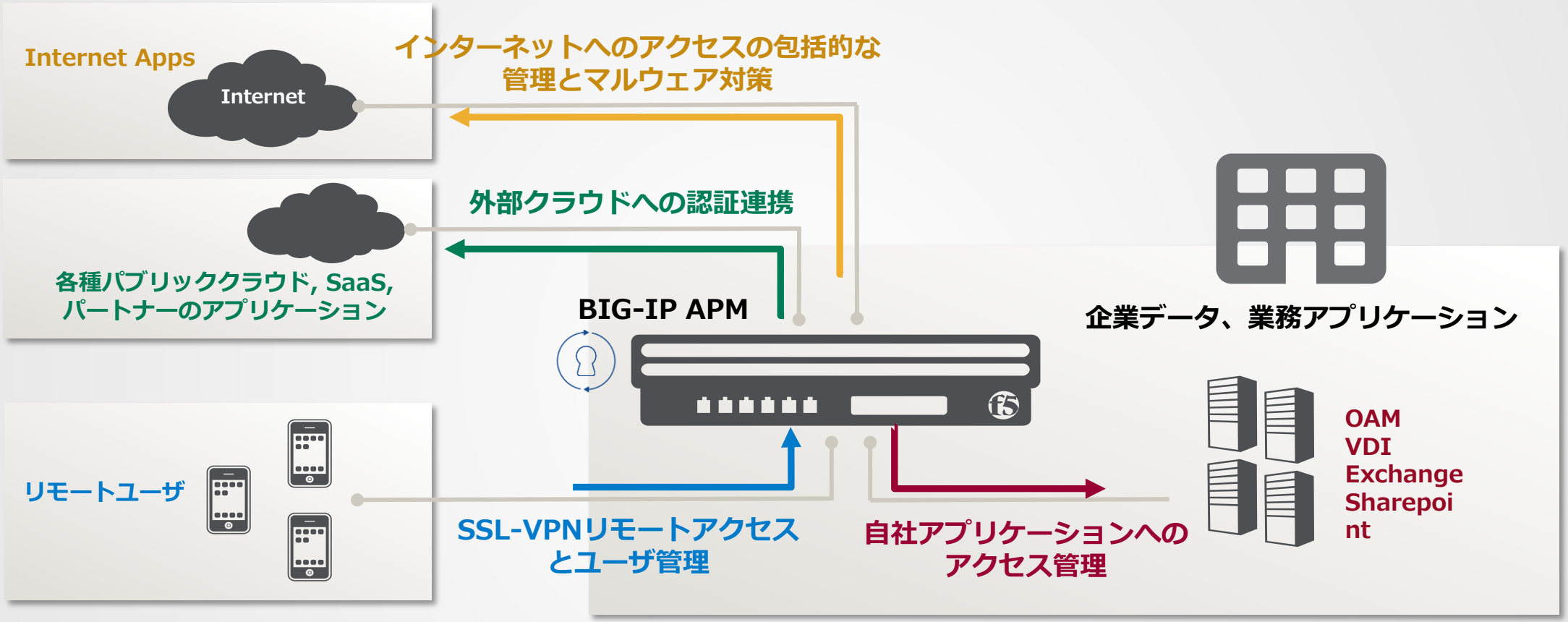


どこからのアクセスに対しても
セキュアな環境をご提供

Resources

ユーザーのアプリケーションを、
ロケーションを問わず守る

F5のアクセスセキュリティ、認証基盤連携



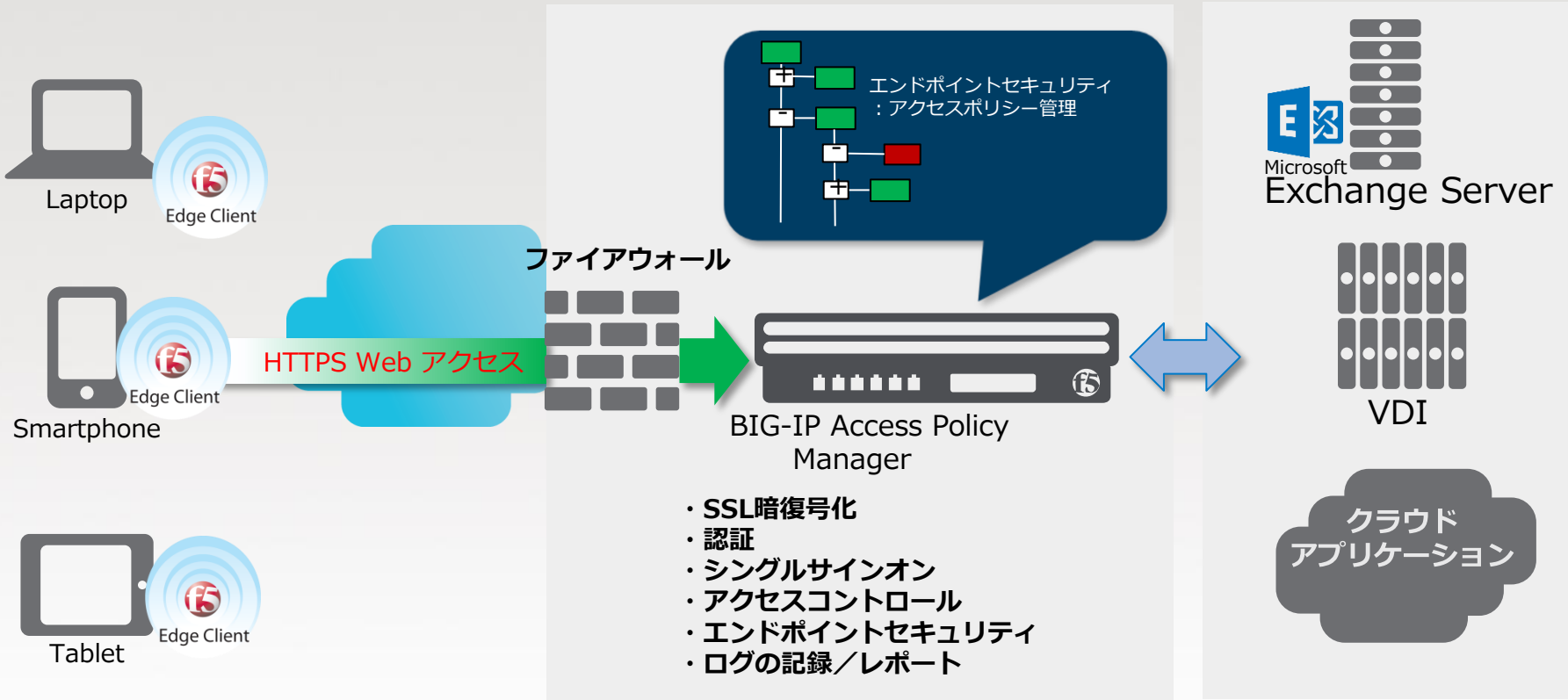
リモートアクセス、ユーザアクセス管理、シングルサインオン、フェデレーション。
そして、ユーザデバイスからウェブアクセスまで全て一元管理。

主要機能紹介

SSL-VPNによるセキュアなリモートアクセス

BIG-IP Access Policy Manager (APM)

- ✓ セキュリティポリシーは強制するが、ユーザビリティを損なわない
- ✓ 運用管理の負荷を低減

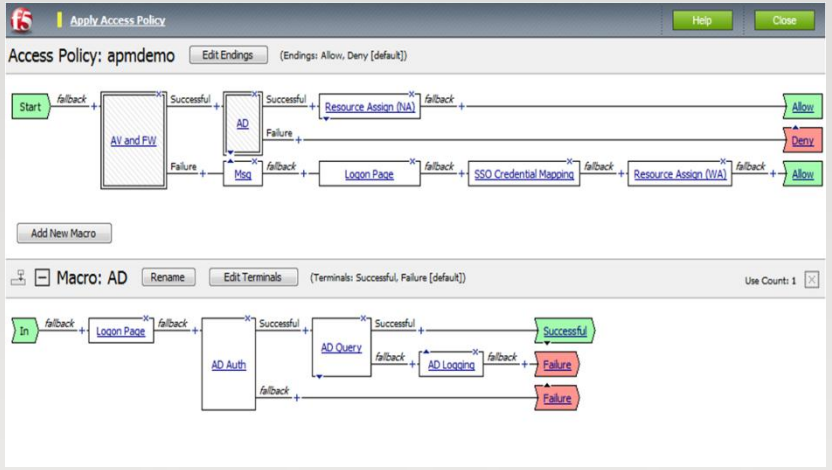


高いユーザビリティ/セキュリティ/運用管理性を実現

アクセス管理の統合
BIG-IP Access Policy Manager (APM)

BIG-IP® APM によるメリット:

- 最大10万ユーザという大規模環境にもアプライアンス一台で対応
- 認証基盤の統合、リモートアクセス、ウェブアクセス、アプリケーションへのアクセスを効率化



BIG-IP® APMの特徴:

- Webシングルサインオンおよび認証・アクセスコントロールサービスを中央で集中管理
- BIG-IPのスピードでのフルプロキシL4 – L7アクセス制御
- アクセスポリシーにエンドポイントチェックを追加
- ビジュアルポリシーエディタ (VPE)により、ポリシーベースのアクセスコントロールを提供
- VPEルール – カスタムのアクセスポリシーのためのプログラムインターフェース

*AAA = Authentication, authorization and accounting (or auditing)

エンドポイントのアクセスを制御

BIG-IP Access Policy Manager (APM)

許可、拒否、もしくは下記のようなエンドポイントの属性に基づいた制御を実施

- アンチウィルスソフトウエアのバージョンやアップデート状況
- ファイアウォールソフトウエアのステータス
- 特定アプリケーションのインストール
- 証明書の有無

非管理デバイスのために保護された仮想デスクトップ（Protected　Work Space）を提供

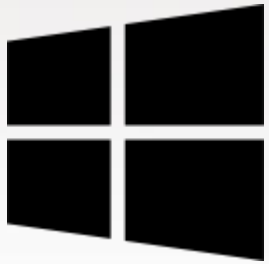
- USBへアクセスを制限
- キャッシュクリーナーによる情報の消去
- マルウエアの進入を防御

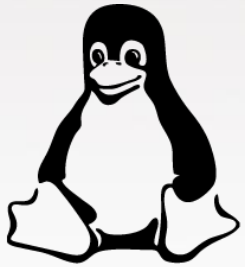
幅広い対応プラットフォーム

F5は、モバイルデバイスにおいてセキュアかつ高速にリモートアクセスを提供する唯一のADCベンダ

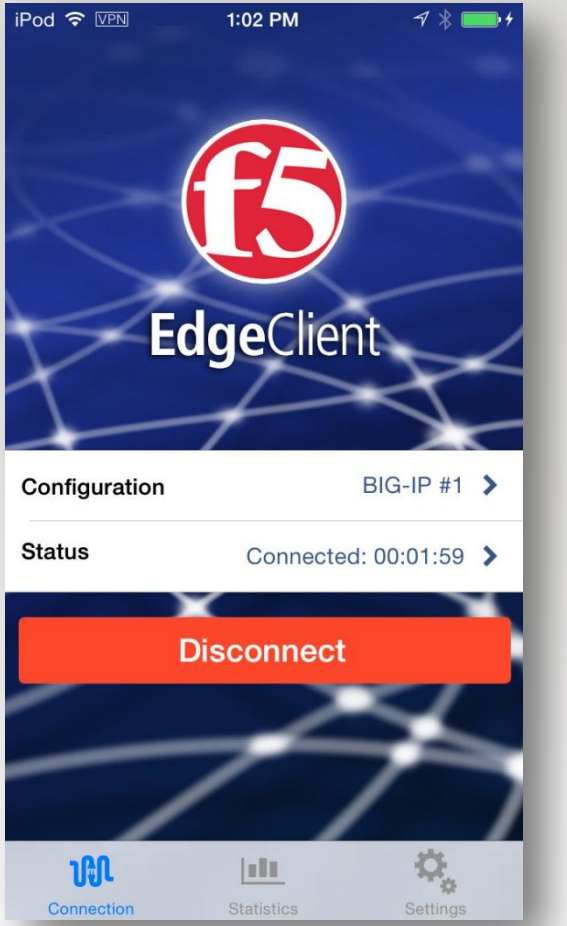
- モバイルデバイス

- Desktop/Laptop



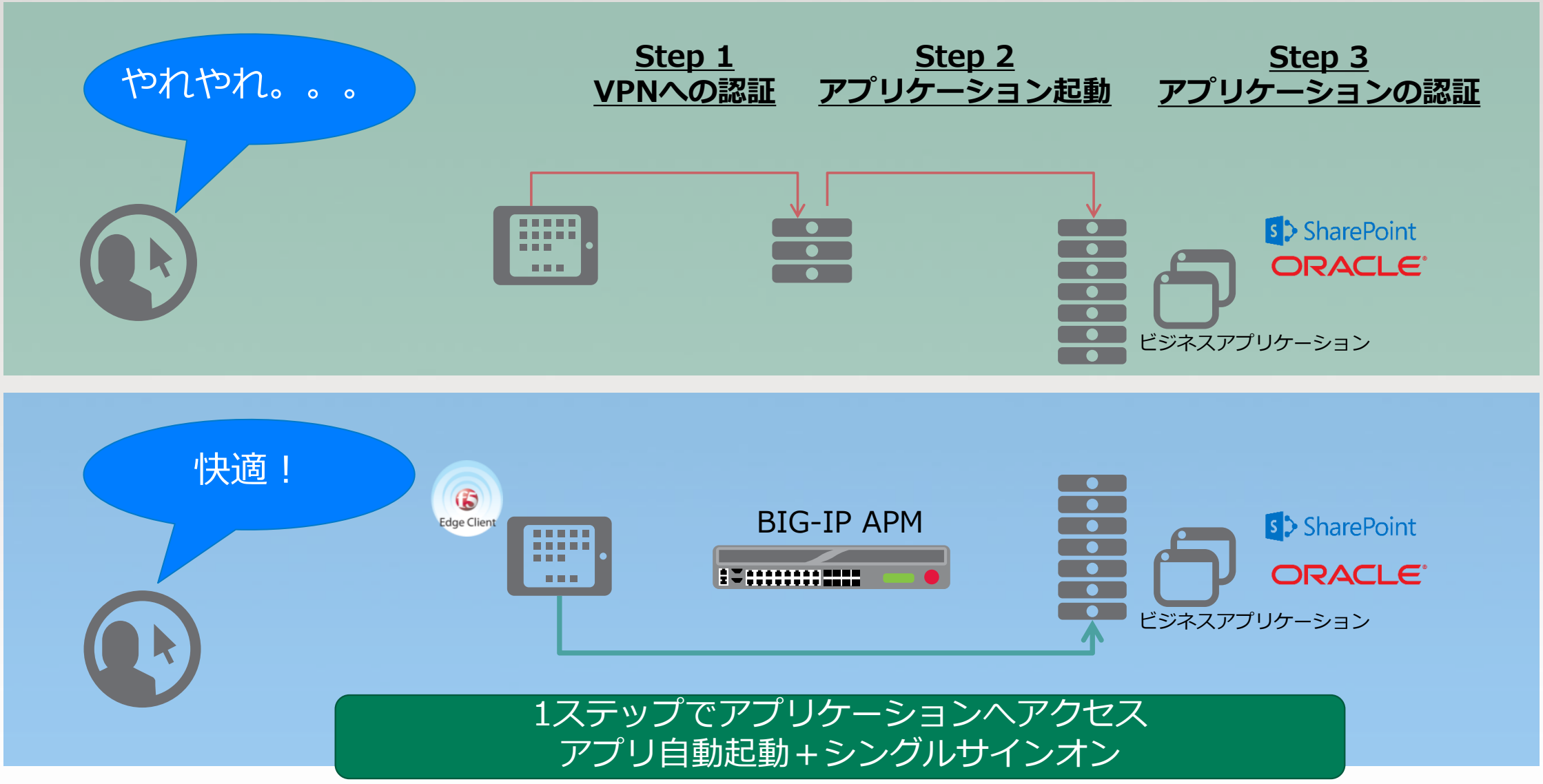


専用クライアントアプリケーション



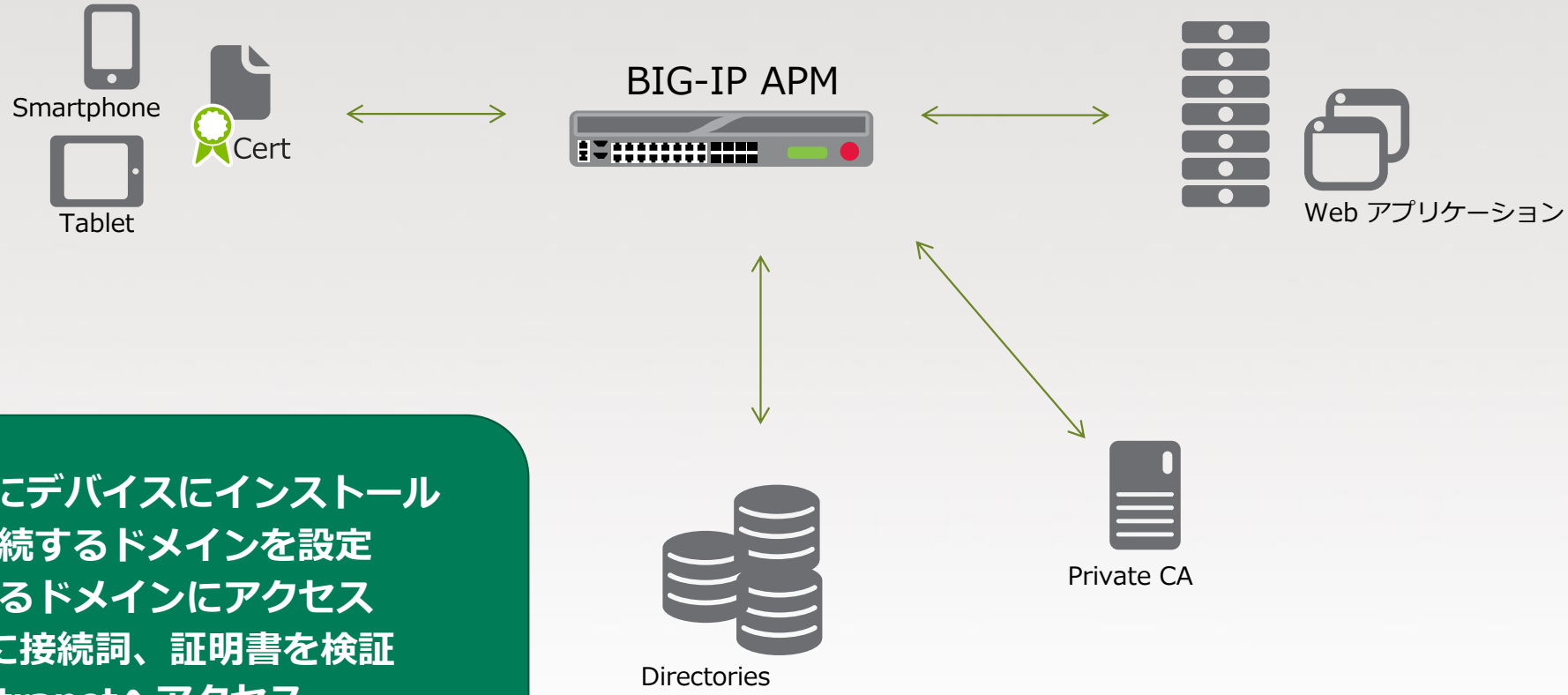
各種アプリケーションストア・マーケットプレイスよりダウンロード可能

アプリケーションに簡単にアクセス
シングルサインオン (SSO)



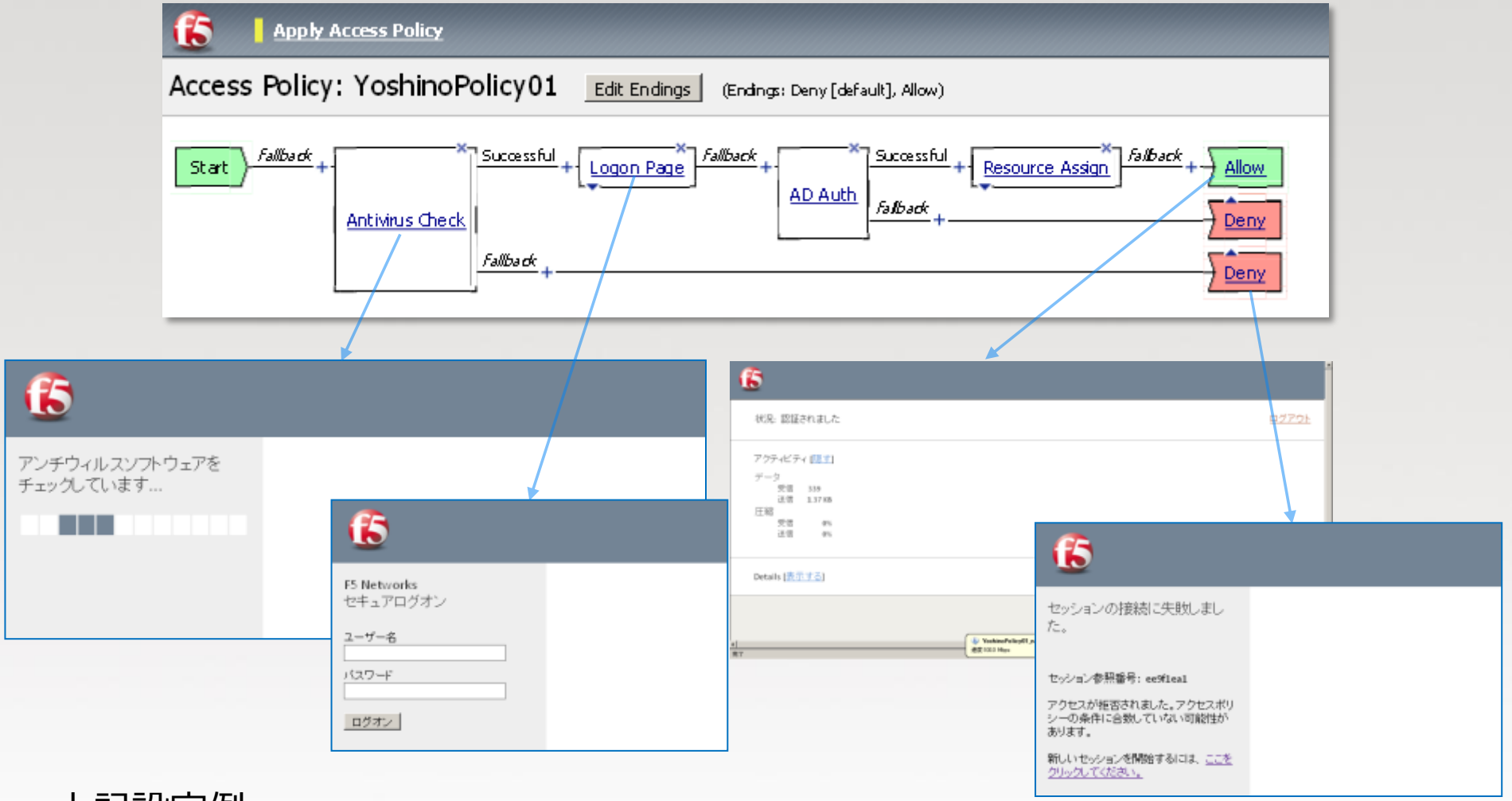
オンデマンド VPN

モバイルデバイスにクライアント証明書をインストールし、特定のドメインへのアクセスの場合自動的にVPN接続が可能。（iOSのみ）



1. ユーザは証明書を事前にデバイスにインストール
2. Edge ClientにVPN接続するドメインを設定
3. ユーザはVPN接続をするドメインにアクセス
4. 自動的にAPM/EDGEに接続詞、証明書を検証
5. 検証された場合のみIntranetへアクセス

強力かつ柔軟なセキュリティポリシー

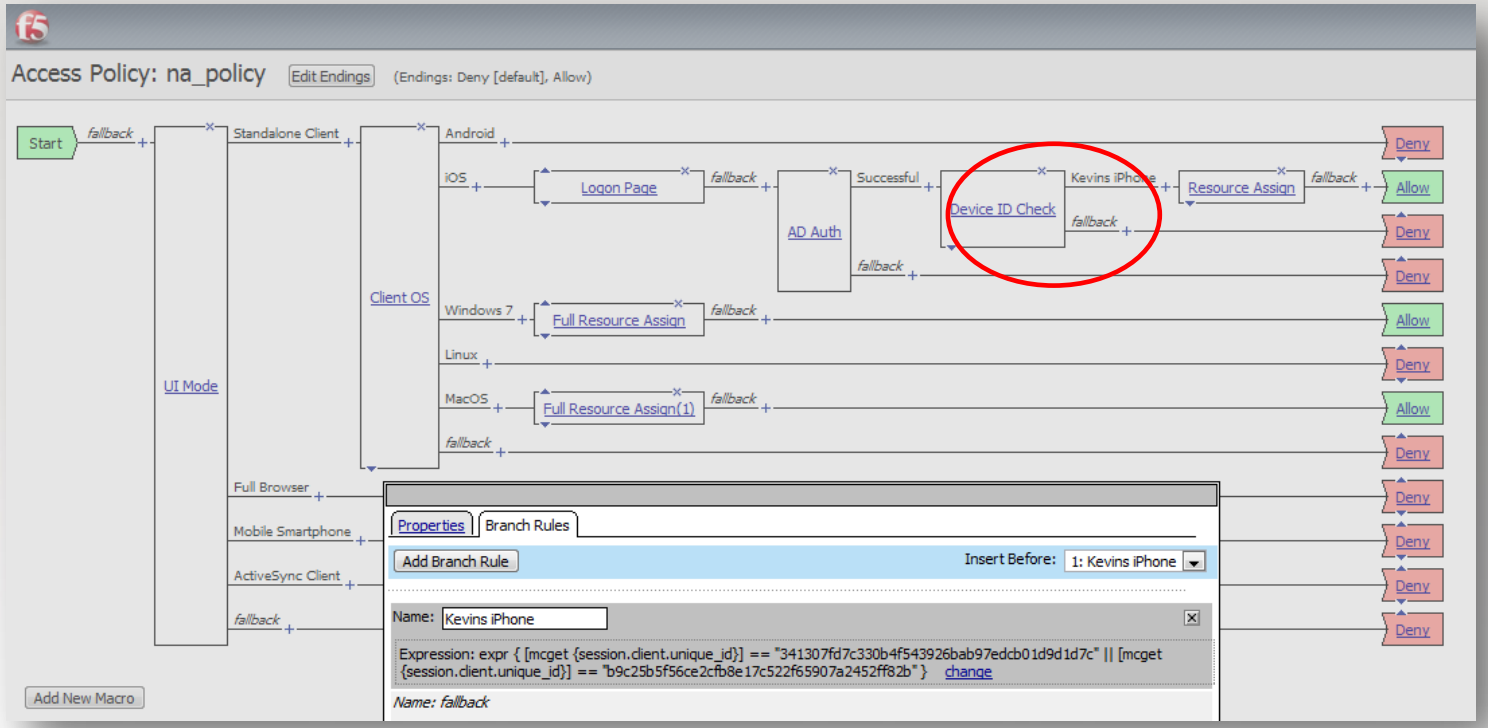


上記設定例：

接続➔ クライアントのチェック➔ ログオン画面が現れ➔ AD認証➔ SSL-VPN

IDと端末の紐付きを特定

- 誰が、いつ、どこから、どんな端末からアクセスしたのかを判定可能なポリシーエディタ
  - 利用者の状況に合わせたアクセスコントロールを柔軟に実現



例： Yamadaというアカウント名で、iPad利用時に、
XXXXXというデバイスIDというアクセスでなければ拒否する

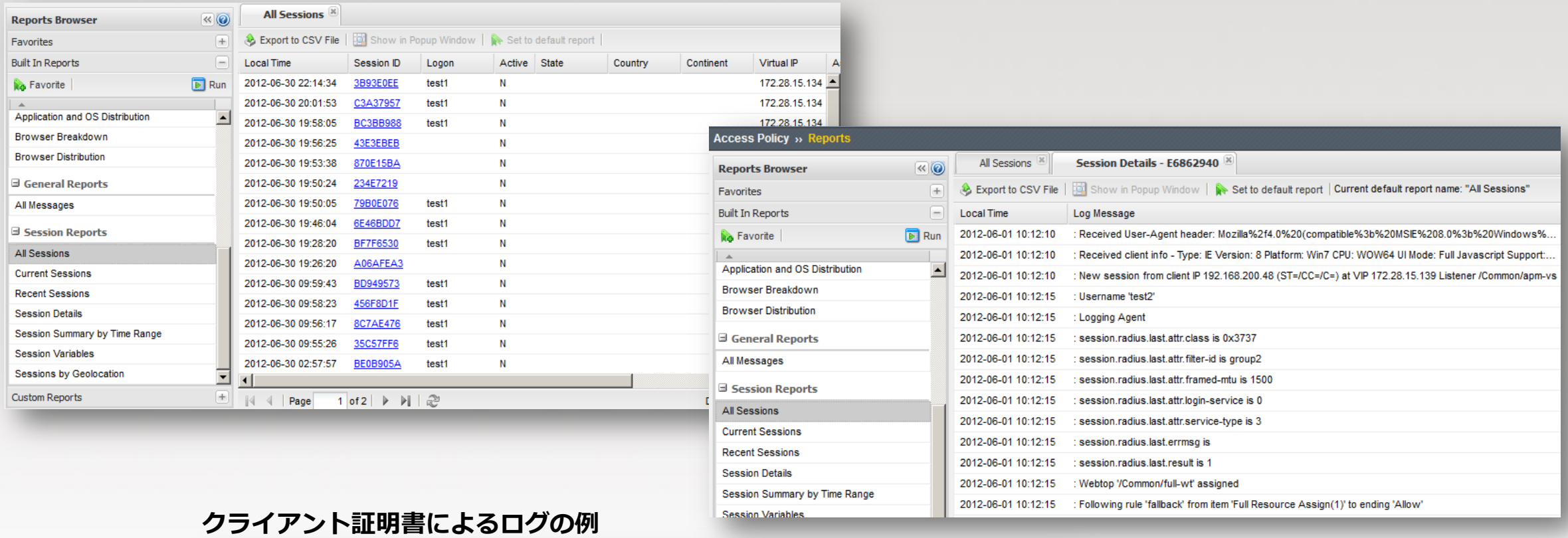
モバイルデバイスの識別

モバイルデバイスでは、デバイスのインスペクションができないため
クライアントソフトから取得できる情報が重要となる。

	例
• iOS	
• プラットフォーム情報	iOS
• MACアドレス(WiFi)	90:21:55:07:4A:32
• モデル名	iPhone 4
• バージョン情報	4.3
• ユニークID(UUID)	8ccaf965e51e3077
• Android	
• プラットフォーム情報	Android
• MACアドレス(WiFi)	90:21:55:07:4A:32
• モデル名	Galaxy Nexus
• バージョン情報	4.0.2
• ユニークID	8ccaf965e51e3077
• シリアルナンバ	016BEB2097AF1456
• IMEI番号	354569041052233

アクセスレポート機能による運用管理

充実で柔軟なレポート機能（認証失敗理由、ライセンス使用率など）



クライアント証明書によるログの例

```
2012-06-26 04:28:09 : Following rule 'fallback' from item 'Logon Page' to item 'Client Cert Inspection(1)'
2012-06-26 04:28:09 : Following rule 'fallback' from item 'Client Cert Inspection(1)' to ending 'Deny'
2012-06-26 04:28:09 : Access policy result: Logon_Deny
```

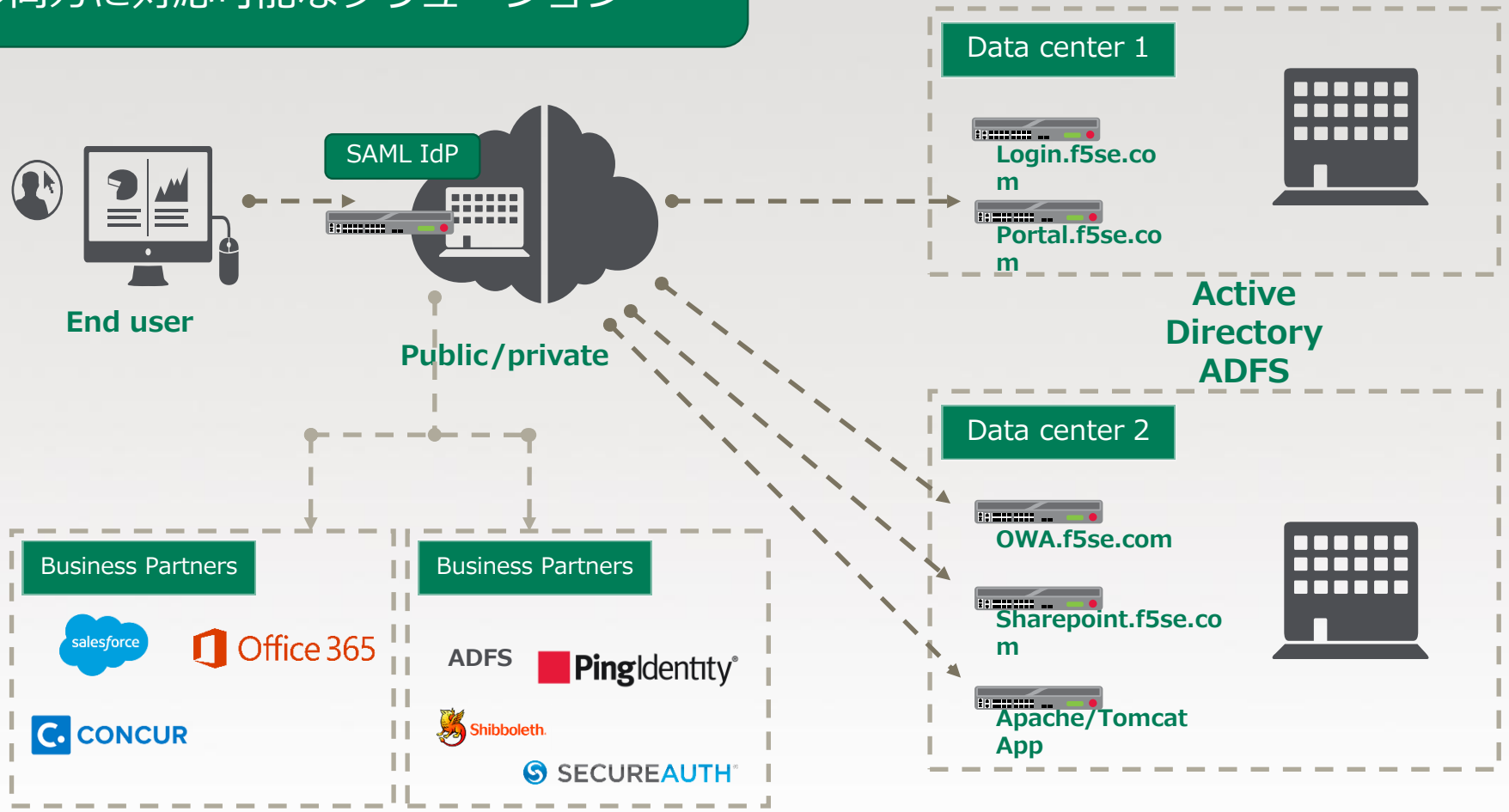
ハイブリッドクラウド・アプリケーション利用における課題

- ✓ SalesForceなどクラウドアプリケーションへのアカウント/アクセス管理の問題
- ✓ 企業買収やグループ企業などビジネス活動では統合されているが認証管理システムが追い付いていけない
- ✓ アプリ毎の認証機能開発のコスト

SAML対応によるクラウド相互認証連携

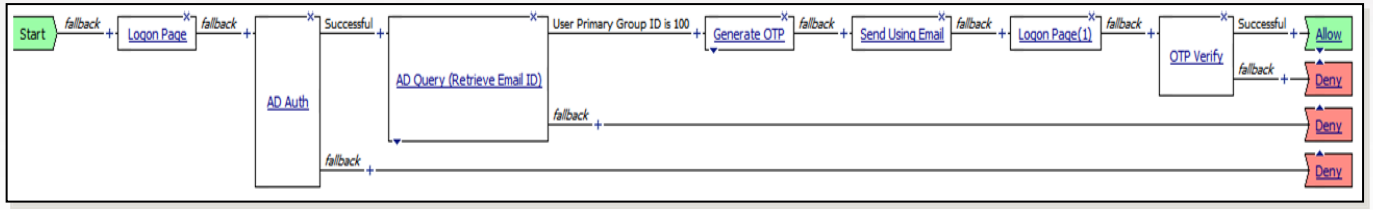
クラウドや複数データセンター間連携を実現

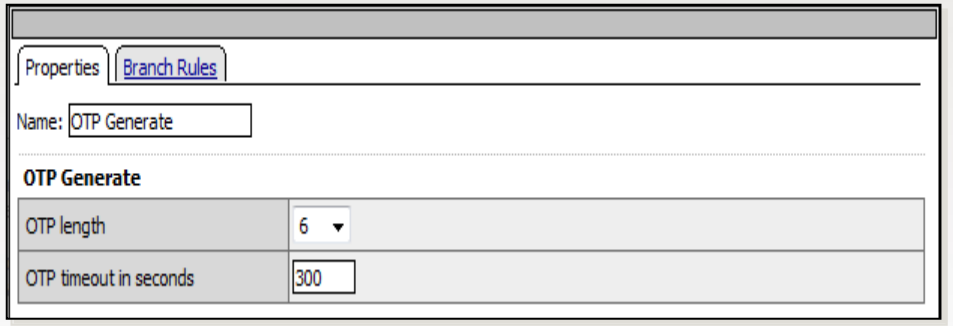
SAML 2.0に対応し、且つSPプロファイル及びIdPプロファイル両方に対応可能なソリューション



APM ワンタイムパスワード

- ワンタイムパスワードの精製・解読をサポート
  - パスワード長、タイムアウト値などは柔軟に設定可能
- OTPをEメール / SMSで送信
  - ユーザーEメール情報をAD queryから抽出
  - Eメール、SMS GatewayまたはHTTP認証と統合
- 認証失敗後の追加認証などの使用用途も有用





Solutions for an application world.