BIG-IP APM + PassLogic

リモートアクセスの
セキュリティと利便性を両立しませんか

株式会社ネットワールド

リモートアクセスの不安と不満がありませんか？

Networld

不安

ID/Password認証だけでセキュリティは大丈夫だろうか。

- パスワード流出による不正アクセス
- リスト型攻撃によるパスワードクラック

不満

忙しくてデバイス識別管理の運用業務をやってる暇がない。

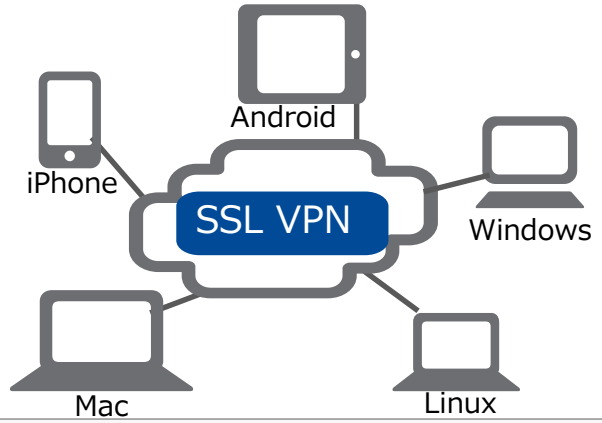
- 管理者として端末識別情報の管理が手間
- 配布済端末の情報取得に利用者から協力を得るのは無理

解決へのアプローチ

APMとPassLogicならリモートアクセスを「安全・快適」に実現できます

BIG-IP APM

デバイス認証	会社支給PCか自宅PCかスマートフォンかを識別し許可された端末のアクセスを許可
多要素認証	端末のMACアドレスや、シリアル番号などを組み合わせた多要素認証
端末チェック	アンチウィルスソフトの有無や、特定プロセスの起動チェックなど可能

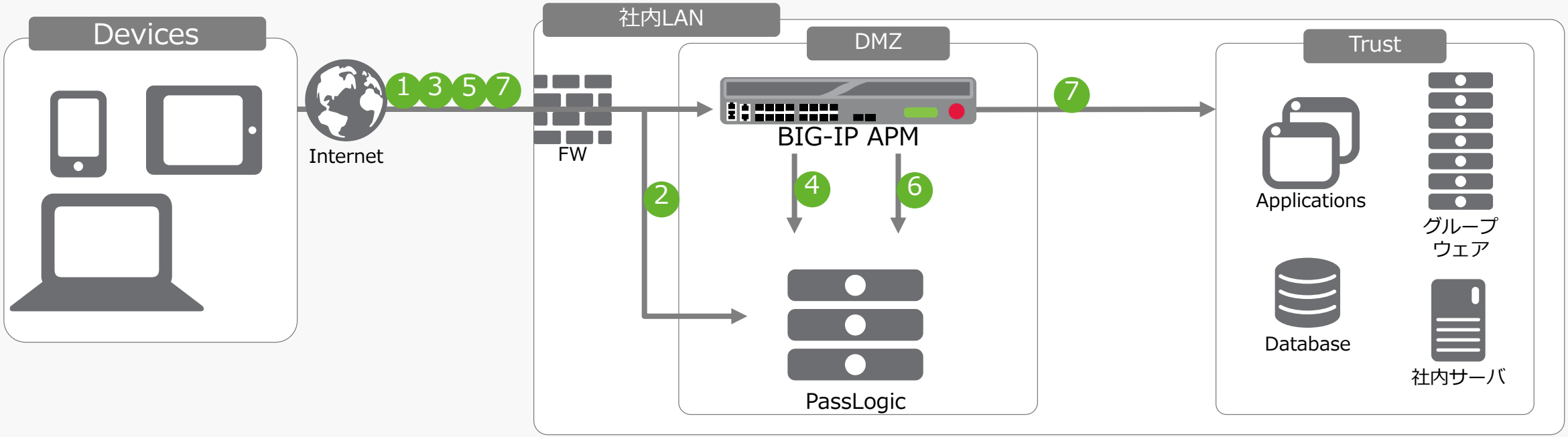


＋

PassLogic

ワンタイムパスワード	トークンやカードの所持が不要 リスト型攻撃からの防御
自動登録	BIG-IP APMで取得した端末情報を、パスロジAPIを利用して自動登録
パスロジック方式	ブラウザ上に表示される乱数表から抜出してワンタイムパスワードを生成

構成と接続フロー



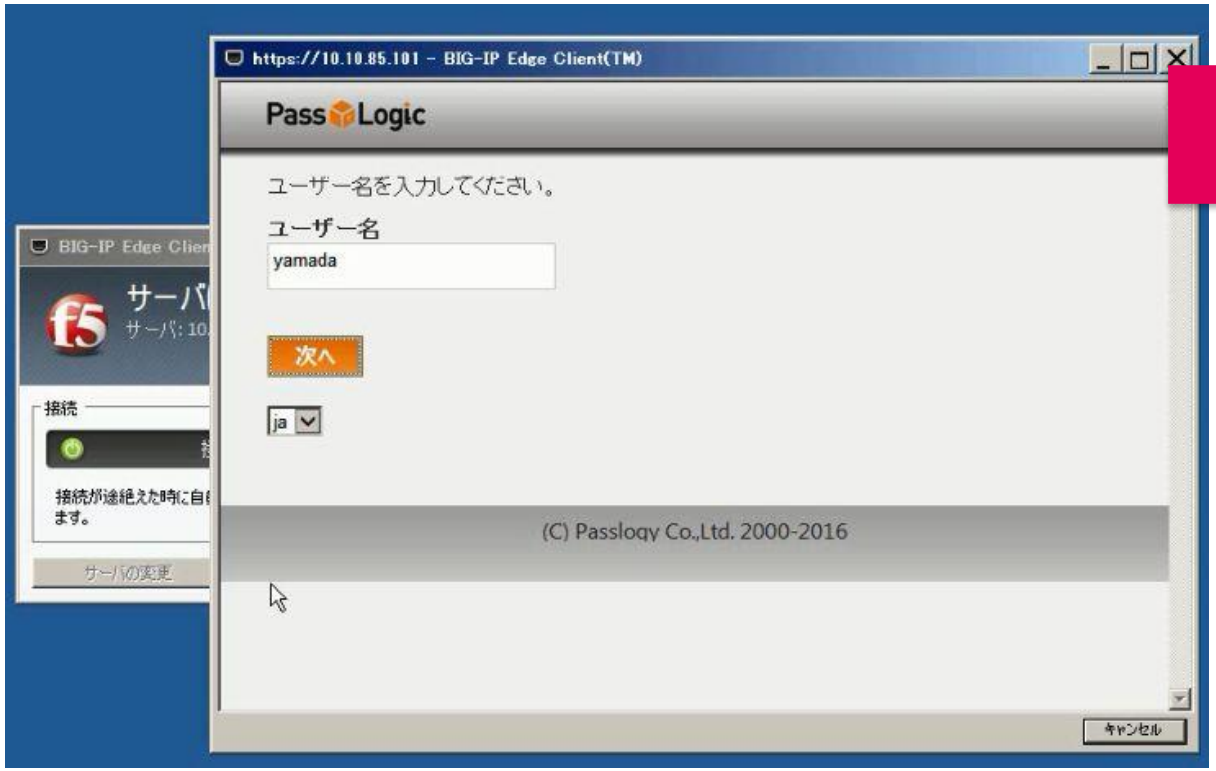
接続フロー

① SSLVPN接続のためにAPM VSのFQDNにアクセス
② PassLogic認証画面へリダイレクト
③ ユーザ名とパスワードをAPMにHTTP POST
④ APMからRADIUS認証
⑤ APMによりデバイス固有情報を取得
⑥ 新規登録が許可されている場合は、デバイス固有情報をRADIUS Attributeに登録
⑦ SSLVPN接続確立し、業務アプリケーションを利用許可

次頁に接続画面イメージ

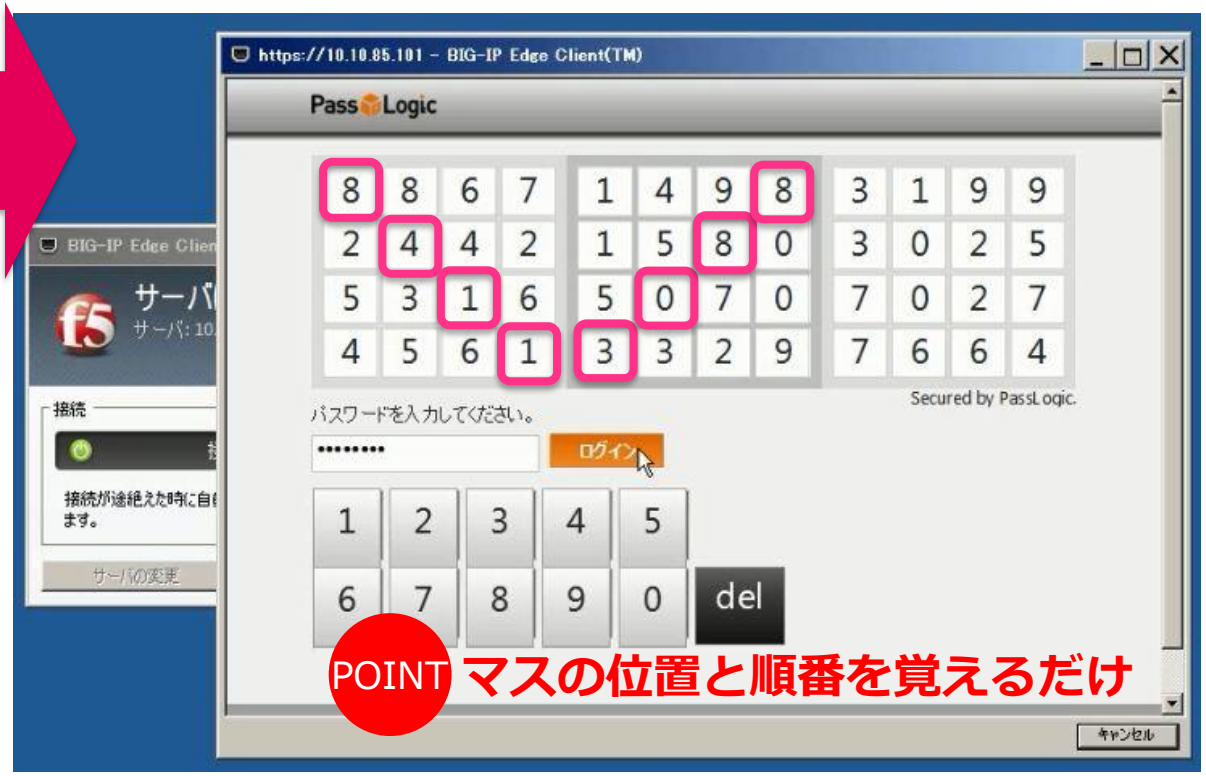
接続フロー

ユーザー名を入力



① SSLVPN接続のためにAPM VSのFQDNにアクセス
② PassLogic認証画面へリダイレクト

ワンタイムパスワードを入力



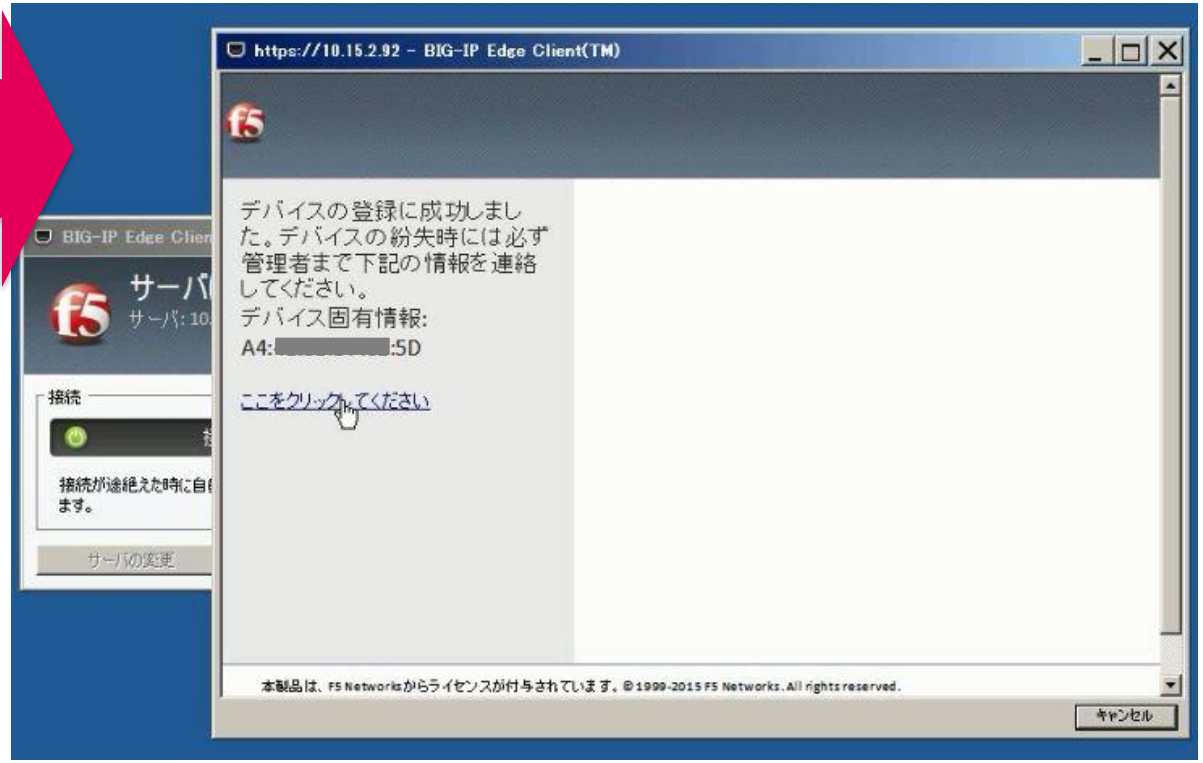
③ ユーザ名とパスワードをAPMにHTTP POST
④ APMからPassLogicへRADIUS認証

接続フロー

初回アクセス時のみ、端末登録可否を確認

⑤ APMによりデバイス固有情報を取得
⑥ 新規登録が許可されている場合は、
デバイス固有情報をRADIUS Attributeに登録

デバイス登録完了



接続フロー

SSLVPN 接続完了

⑦ SSLVPN接続確立し、業務アプリケーションを利用許可

ユーザ毎の端末情報管理

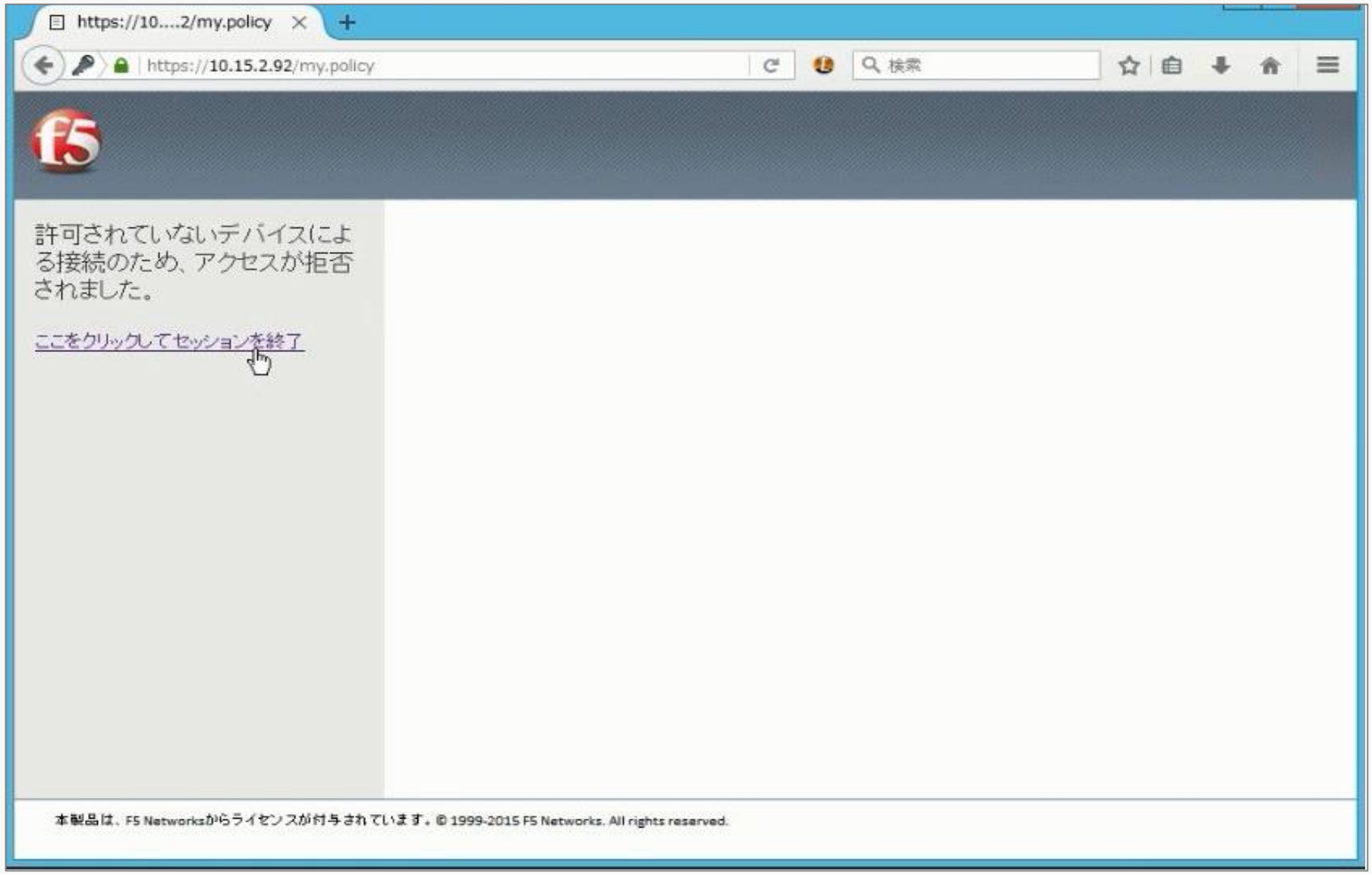
MACアドレスがPassLogicに
自動登録されている
(RADIUS Attribute で登録できる文字数は253 文字以下)

POINT **PassLogicサーバで管理者による**
ユーザ毎のデバイス識別情報管理が可能
(確認、変更、削除)

PassLogicへ端末情報が自動登録されています

【補足】未登録の端末からの接続の場合はメッセージ出力

MACアドレスが未登録の端末から接続した場合



接続フロー【Edge Client アプリ利用時】

デバイス種別毎の取得可能な識別情報

デバイス種別	識別情報	備考
Windows	NICのMACアドレス マザーボードのシリアル番号 ハードディスクドライブのシリアル番号	1つ目のNICを取得
Mac	NICのMACアドレス	1つ目のNICを取得
Linux	NICのMACアドレス	1つ目のNICを取得
iOS (iPhone,iPad)	ユニークID	※iOS6.1以降対応
Android	ユニークID	※OS初期化により値が変化

【iOS】SOL12749: Support for using the BIG-IP Edge Client to check identifying information from Apple iOS client devices

****

iOSにおけるユニークIDはUDIDを取得しております。そのためユニークIDは機器毎一意の値を取得する事が可能です。

【Android】 SOL13731: Overview of session variable support for BIG-IP Edge Client for Android devices

****

Androidにおけるユニークidは、 ANNDORID_IDを取得しております。ANDROID_IDは端末の初期化時にランダムに生成される文字列(64ビットの16進文字列)です。
複数のアプリ間で同じ値を取得できますが、異なる端末で異なる値が返ることが保証されているわけではありませんが、一般的には同じ値になる確率は天文学的な数値となります。

Q&A

- **クライアント証明書を組み合わせて利用することは可能ですか？**
  - クライアント証明書との並用可能です。

- **1ユーザで複数デバイスを登録することは可能ですか？**
  - 1ユーザ/1デバイスではなく、Mac,Windows,Linux,iOS,Androidなど複数台登録可能です。

  【例】下記の様にデバイス種別毎に登録台数を決める事ができます。
  1ユーザ ： iOS/2台　Windows/3台

  ※1ユーザの制限台数は、RADIUS Attributeで登録可能な文字数が253文字までになりますのでそれまでに限ります。

- **ユーザに紐付けるデバイスではなく、予め登録してある共有用デバイスからは無条件に許可することは可能ですか？**
  - 可能です。予め共有デバイスの端末情報を登録しておくことが可能です。

- **ジェイルブレイクされた(俗称:脱獄携帯)端末の登録を拒否することは可能ですか？**
  - 可能です。

- **本機能を利用する場合の、BIG-IPとPassLogic対応バージョンを教えてください。**
  - BIG-IP APM v12.0.0 HF1 以降
  - PassLogic2.3.0 以降

- **クライアント端末に専用のエージェントソフトをインストールする必要がありますか？**
  - はい。
    - スマートフォンの場合は無償の「Edge Client」をインストールする必要があります。
    - PCの場合はWEBブラウザプラグインのインストールでも対応可能です。

- **BIG-IPとPassLogicをまとめて構築して頂くことは可能ですか？**
  - BIG-IP/PassLogicの専任担当者がおりますので構築可能です。

導入による効果

端末情報の登録を自動化したい

2要素認証の必須要件

パスワード流出の不安

リスト型攻撃

BIG-IP APM ＋ PassLogic で解決

端末のMACアドレスやOTPを利用した２要素認証でセキュリティ強化

APIからの端末情報自動登録で管理者の負担軽減！

本資料に関するご相談・ご質問などございましたら
ご連絡お待ちしております。

お問い合わせ先：f5-info@networld.co.jp

Networld