The Guaranteed Network

いちばん近くで、もっと先へ。

AXシリーズとSafeNetのクラウド型認証サービス およびeTokenによる認証の相互接続評価報告書

2013年1月30日

アラクサラネットワークス株式会社
ネットワークテクニカルサポート

資料No. NTS-12-R-031 Rev. 0

The Guaranteed Network

AlaxalA

はじめに

■ 注意事項

本資料に記載の内容は、弊社が特定の環境において、基本動作や接続動作を確認したものであり、すべての環境で機能・性能・信頼性を保証するものではありません。

■ 輸出時の注意

AXシリーズに関し、本製品を輸出される場合には、外国為替及び外国貿易法の規制並びに米国輸出管理規制など外国の輸出関連法規をご確認の上、必要な手続きをおとりください。なお、不明な場合は、弊社担当営業にお問い合わせ下さい。

■ 商標一覧

・アラクサラの名称及びロゴマークは，アラクサラネットワークス株式会社の商標及び登録商標です。
・SafeNet、SafeNetロゴはSafeNet, Inc.の登録商標です。
・eTokenはイスラエルAladdin Knowledge Systems社のイスラエル及びその他の国での登録商標です。
・そのほかの記載の会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

■ 関連資料

・AX2500Sシリーズ 製品マニュアル
（ http://www.alaxala.com/jp/techinfo/manual/index.html ）

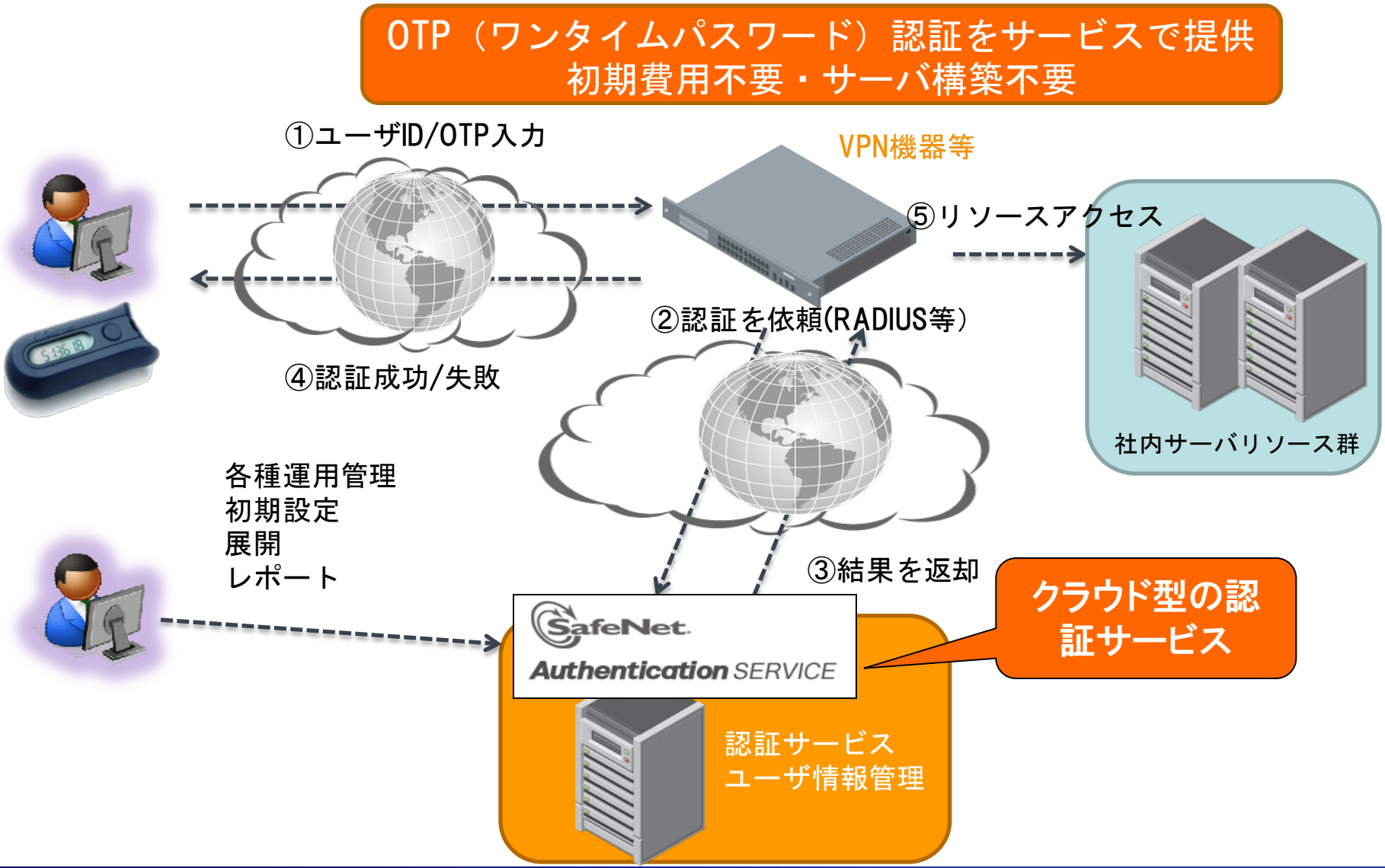
・SafeNet クラウド認証サービスについて
（https://jp-mktg.safenet-inc.com/auth-service/index.htm ）

・SafeNet eToken 製品について
（http://jp.safenet-inc.com/data-protection/multi-factor-authentication-2/ ）

目次

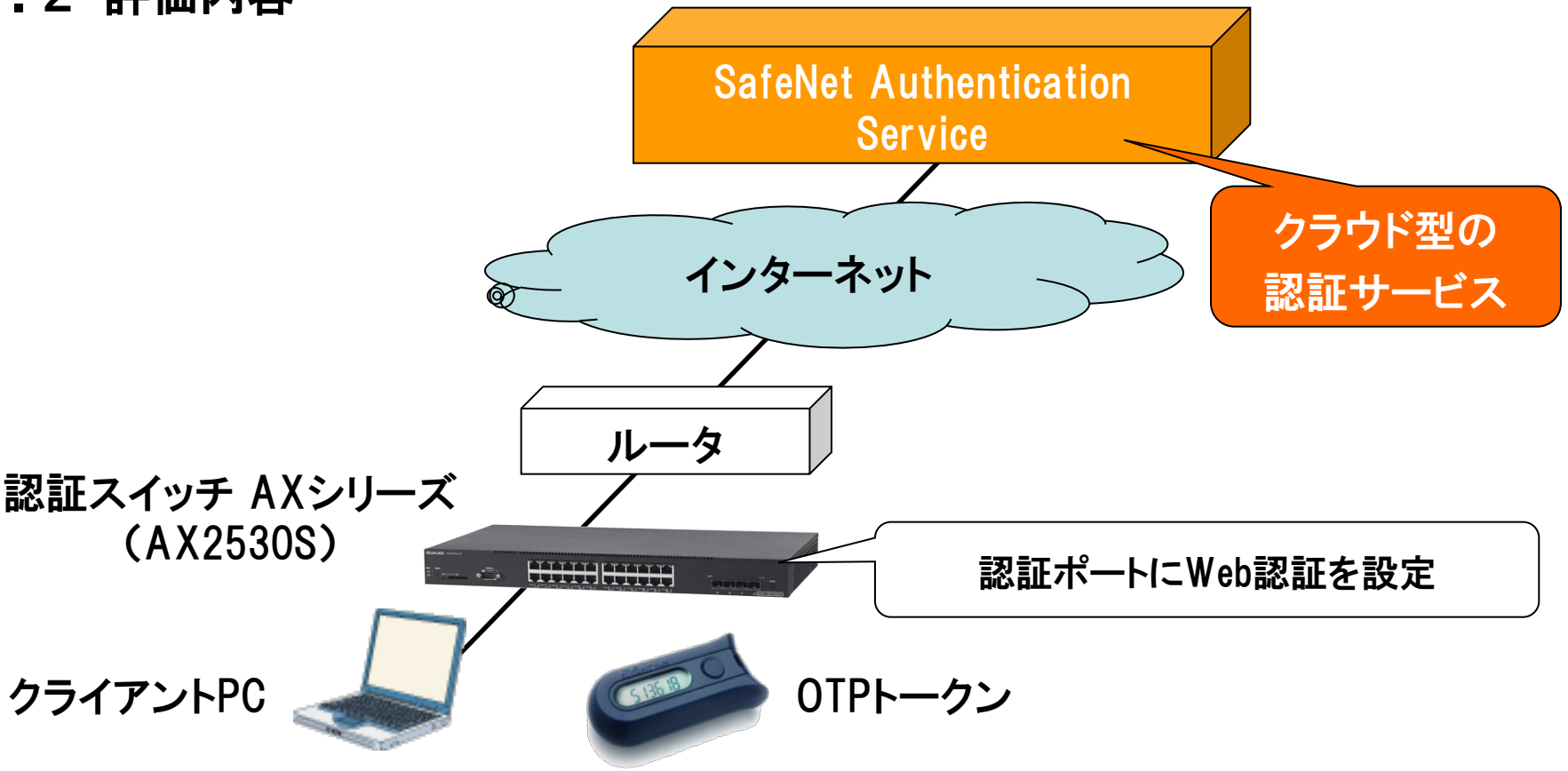
1.「SafeNet Authentication Service」との相互接続

1.1 SafeNet Authentication Service の概要



1.「SafeNet Authentication Service」との相互接続

1．2 評価内容



SafeNetクラウド型認証サービス(SafeNet Authentication Service)にインターネット経由でAXシリーズを接続し、OTPトークンを用いてクライアントPCをWeb認証できることを検証する。 また、このOTP認証のほかに、トークンを使わないパスワード認証も検証する。

1.3 評価機器および設定条件

(1)「SafeNet Authentication Service」の設定条件

- 認証ユーザの作成(OTP認証用、パスワード認証用)
- Radiusクライアントの設定として、 認証スイッチのIPアドレスと認証キーを設定する。
  (本試験構成ではインターネットに接続したルータでNATを行ったため、本試験では Radiusクライアントにはルータのグローバルアドレスを設定した。)

(2)認証スイッチ「AXシリーズ」の設定条件

- 使用機器 AX2530S (Ver3.4)
- クライアントPCを接続する認証ポートは、Web認証ポートに設定する。
- Web認証のRadiusサーバの設定として、 SafeNet Authentication Service の IPアドレスと認証キーを設定する。

1.4 評価結果

OTP認証、パスワード認証ともに、「SafeNet Authentication Service 」を認証スイッチ「AXシリーズ」のWeb認証のRadiusサーバとして設定するだけで簡単に連携がおこなえ、クライアントPCのWeb認証が正常に成功することを確認した。

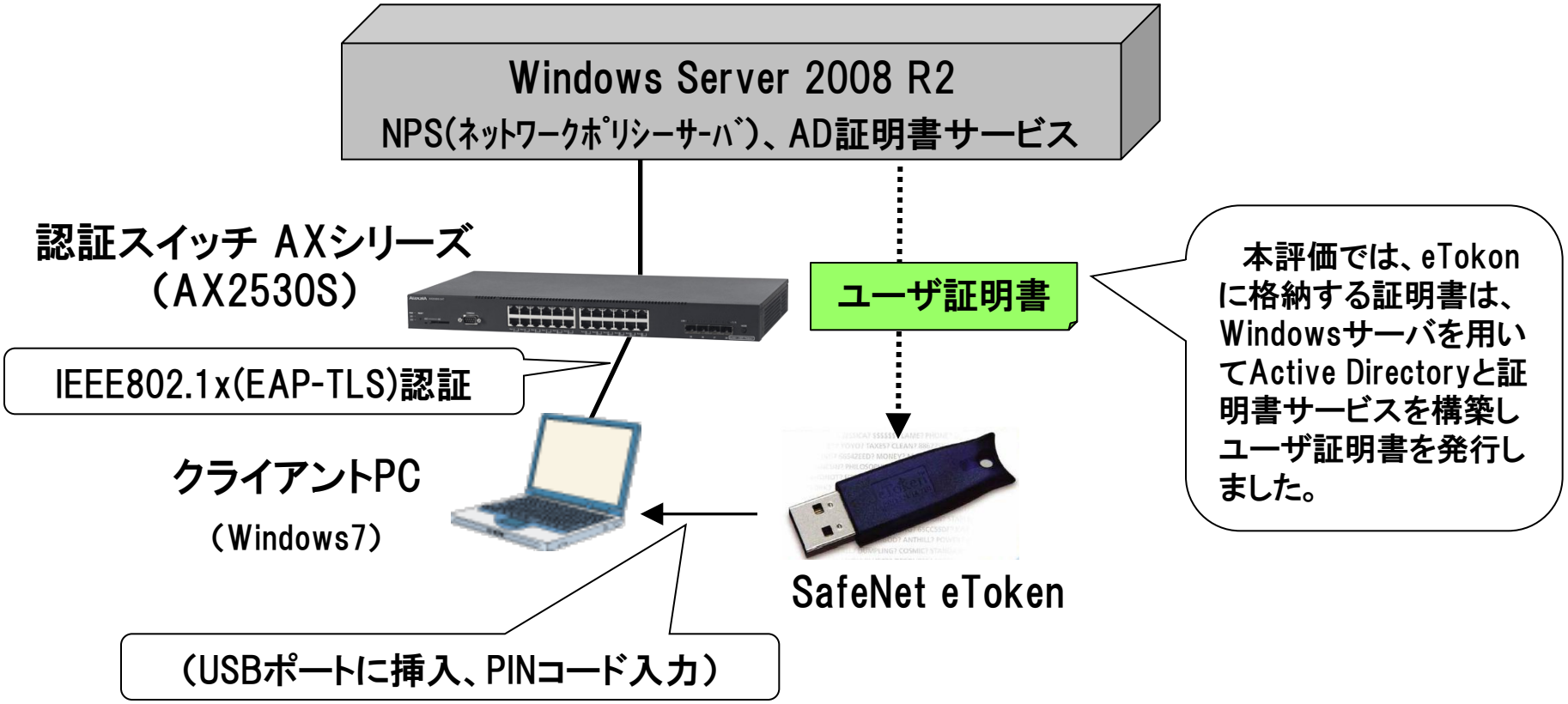
2.「SafeNet eToken」を用いたクライアント認証評価

2.1　SafeNet eToken（2要素認証製品）の概要

- フィッシング等によるID・パスワード盗用に備え、パスワード＋αの2要素認証のニーズが拡大
- クラウドへのネットワークアクセスには必須のセキュリティアイテム

2.「SafeNet eToken」を用いたクライアント認証評価

2.2 評価内容



ユーザ証明書の入ったeTokenをクライアントPCのUSBポートに挿入しPINコードを入力することでIEEE802.1x(EAP-TLS)認証が実行され、AXシリーズの通信ポートでクライアントPC認証が成功することを確認する。

2.3 評価機器および設定条件

(1)Windows Server の設定条件

- 使用バージョン　Windows Server 2008 R2　SP1
- AD(Active directory),AD証明書サービス、NPS(ネットワークポリシーサーバ)を構築し、RadiusクライアントにAX2530SのIPアドレスと認証キー設定します。

(2)「SafeNet eToken」の設定

- 使用機器　SafeNet eToken 5100
- (1)で構築したWindowsサーバの証明局からユーザ証明書を発行しeTokenに入れてPINコードを設定します。

(3)クライアントPCの設定

- 使用機器　Windows 7　SP1
- 「Wired Auto Configサービス」を有効化しLANの通信ポートのIEEE802.1xを有効化して認証方法を「スマートカードまたは証明書」を選択します。

(4)認証スイッチ「AXシリーズ」の設定条件

- 使用機器 AX2530S (Ver3.4)
- PCの接続ポートはIEEE802.1x認証ポートとし、Radiusサーバとして Windows Server 2008 R2サーバのIPアドレスと認証キーを設定する。

2.4 評価結果

認証スイッチ「AXシリーズ」と「SafeNet eToken」を用いて、クライアントPCのIEEE802.1x(EAP-TLS)認証が正常に成功することを確認しました。

The Guaranteed Network

いちばん近くで、もっと先へ。