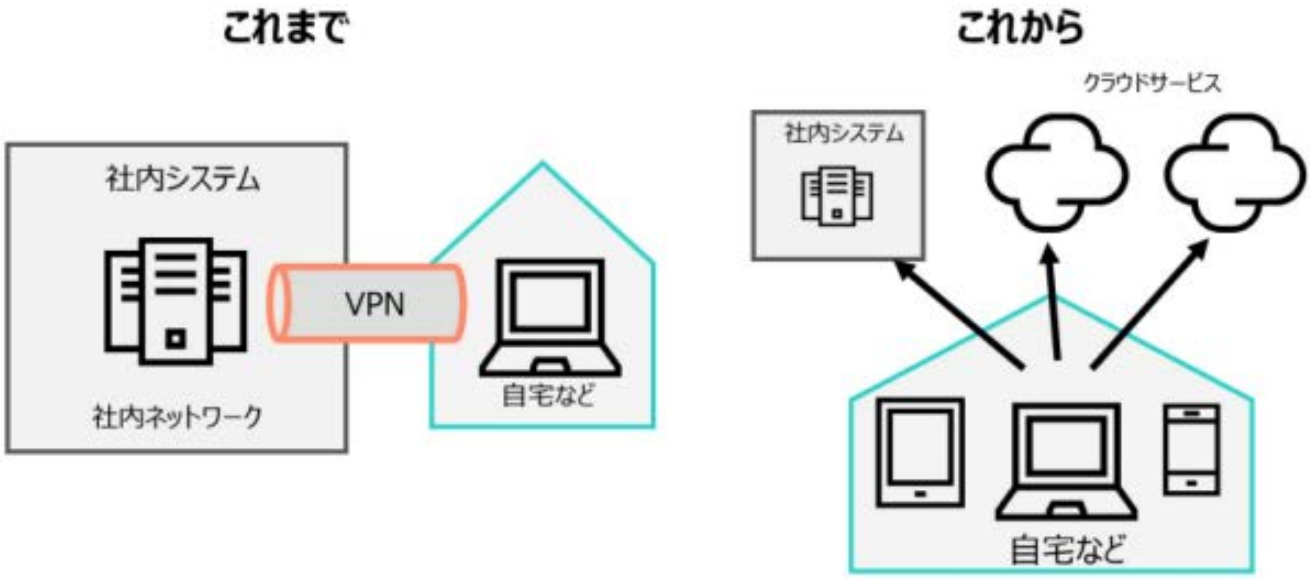
サイバートラスト デバイスIDとの連携による「端末の認証」

IceWall技術レポート

1. はじめに

社外からのリモートアクセス方法の変化

多くの企業が「働き方改革」に取り組む中、自宅や外出先など、社外から企業情報システムにアクセスして仕事をする機会が増えています。このような場合、従来はVPNなどを使って企業内ネットワークに接続するやり方が主流でした。昨今では、Office 365などのクラウドサービスの普及により、企業ネットワークにアクセスしなくても社外から直接クラウドサービスにアクセスする運用もできるようになっています。また、PCだけでなくスマートフォンやタブレットと言ったスマートデバイスが利用されるケースも増えてきています。



求められるクラウドサービス利用時の「端末の認証」

一方で、社外の端末からクラウドサービスに直接アクセスするような運用の場合、私物の端末やネットカフェの端末からの利用によって、それら端末経由での情報漏洩が起きるリスクも指摘されています。このようなリスクを排除するために、**利用するユーザーの認証に加えて「端末の認証」を行い、許可された端末からしか利用を許さないような制限をかけることも求められるようになっています。**
従来型のVPNによるリモートアクセスなら、「端末の認証」はVPNクライアントの機能によって一元的に行うことができました。しかしながら、クラウドサービスへの直接アクセスの場合は、そのようなVPNクライアントの機能は利用できません。どのような仕組みでクラウドサービスにアクセス可能な端末を制限すれば良いのでしょうか？

IceWall SSO とサイバートラスト デバイスID の組合せによる広範囲な端末認証

IceWall SSOとサイバートラスト デバイスIDの組合せにより、広範囲なクラウドサービスに対する「端末の認証」を行うことができます。例えば、Office 365、Salesforceなど複数のクラウドサービスを利用している場合に、下記の例のような制限が可能です。

例1） 会社から支給された特定のPCだけ許す

例2） 私物のPCやネットカフェ端末からの利用は、正規のユーザーであっても許さない

まさに、働き方改革が求められ、クラウド利用が普及する中で求められるセキュリティ対策と言えるでしょう。

本技術レポートでは、厳格な端末認証を提供するソリューションであるサイバートラスト デバイスIDとIceWall SSOとの連携方法をご紹介します。

---

2. サイバートラスト デバイスIDとは

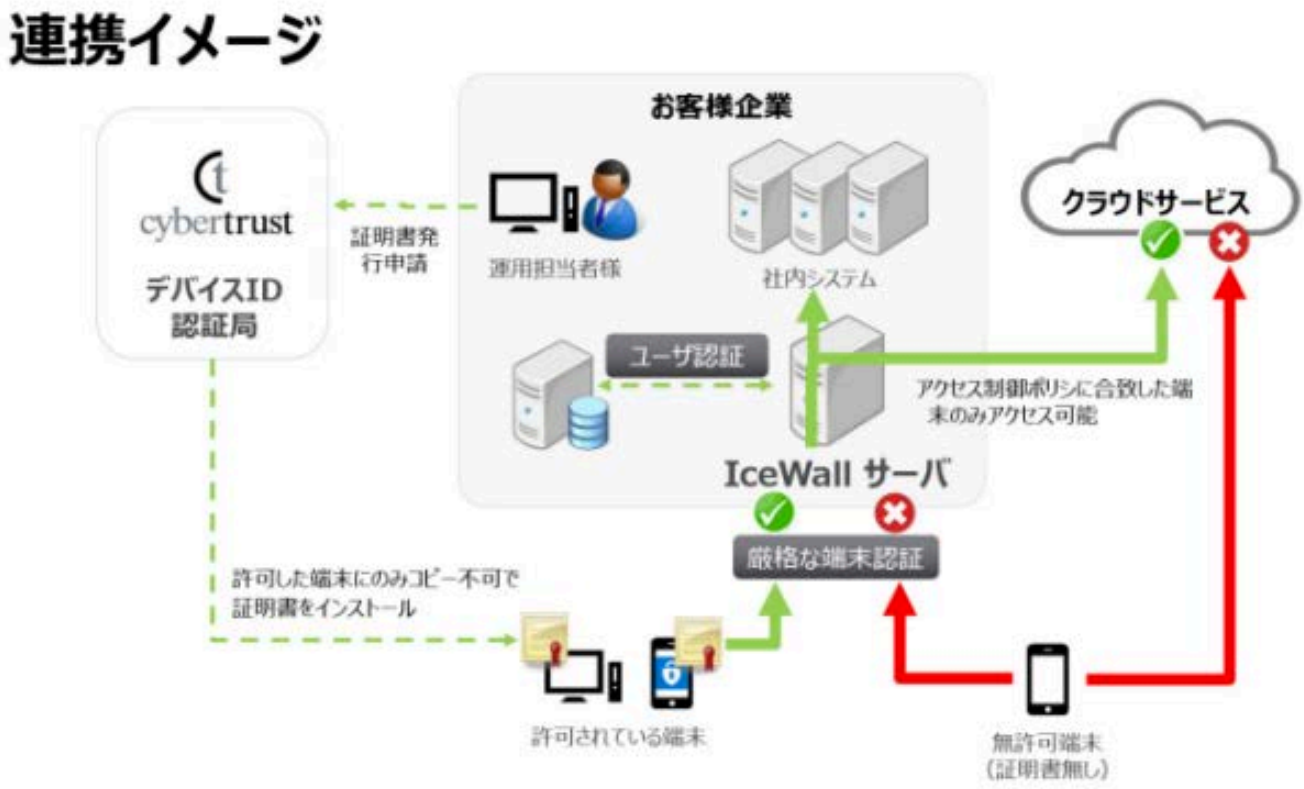
サイバートラスト デバイスIDは、管理者が端末に対して発行する証明書により、許可した端末だけをネットワークやシステムにアクセスできるようにするデバイス証明書発行管理サービスです。
デバイス IDでは、厳格な端末認証として、管理者が指定した端末にのみデバイス証明書を登録、かつ一

度登録されたデバイス証明書の複製や取り出しができない仕組みをWindows、macOS、iOS、Android で実現しています。
また、デバイスID UPNオプションにより、厳格な端末認証に加えて、デバイス証明書内に登録されるユーザー情報（UPN）によるデバイス証明書配布時の配布対象ユーザーの本人確認を行うことも可能です。

---

3. 連携イメージ

サイバートラスト デバイスIDとIceWall SSOを組み合わせることで、クラウドサービスや社内システムの利用に際して、厳格な端末認証の上でユーザー認証・認可制御を行う統合認証基盤を実現できます。

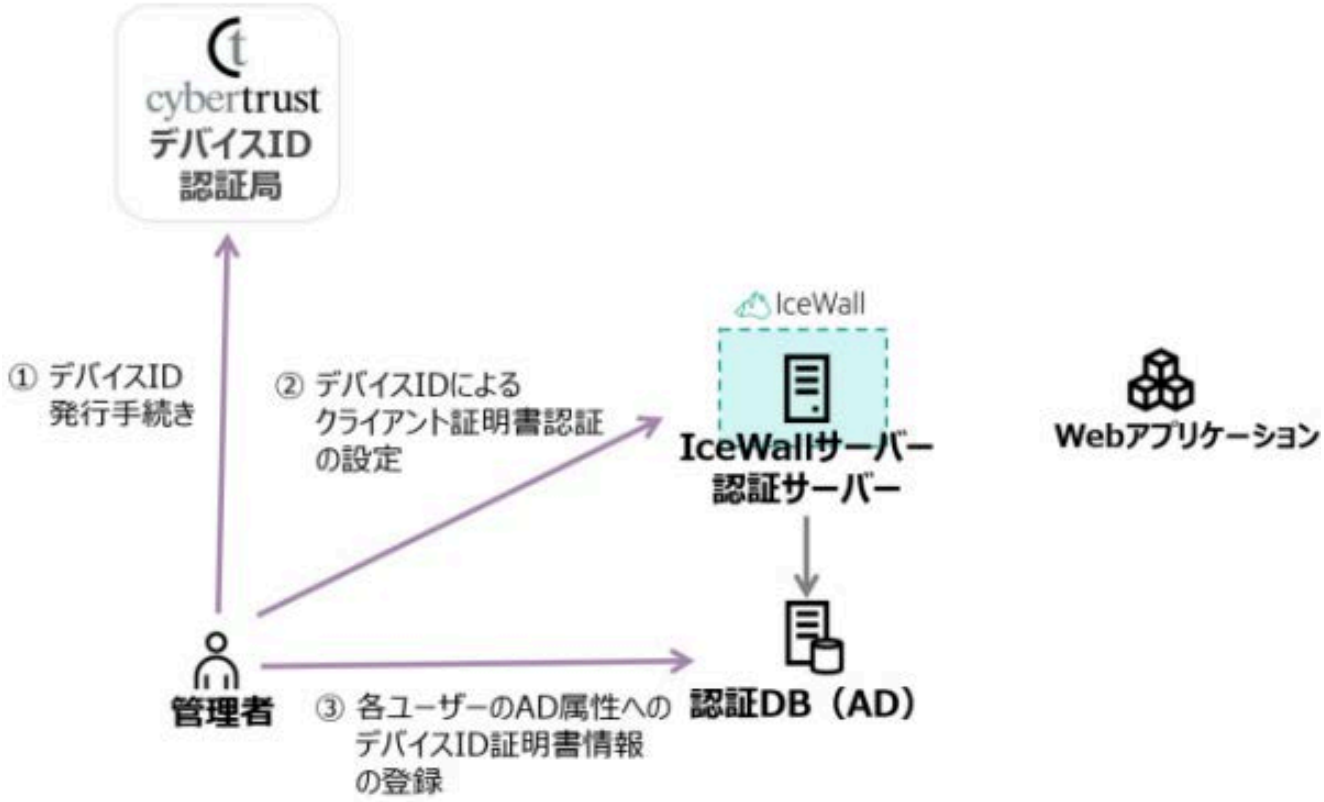


さらに、デバイスID UPNオプションとIceWall SSOクライアント証明書認証オプションを連携することで、デバイス証明書内に登録されているユーザー情報（UPN）でのみシステム利用時のユーザー認証ができるよう制限することが可能です。これにより、端末に紐づけられたユーザーにのみシステム利用を許可するという、より厳密な認証のニーズにも対応できます。

---

4. 設定作業の流れとポイント

本章では、サイバートラスト デバイスIDで発行されるデバイス証明書（UPN入り）とIceWall SSOを連携する場合の設定作業の流れとポイントをご説明します。概要は以下の図の通りです。



① デバイス証明書発行手続き

サイバートラスト デバイスID RAオペレータ画面にアクセスし、ユーザー向けのデバイス証明書（UPN入り）の発行申請を行います。あわせて、ルート認証局証明書（PEM形式）をダウンロードします。
※詳細は、サイバートラスト デバイスIDのマニュアルをご参照ください。

② デバイス証明書によるIceWall SSOクライアント証明書認証オプションの認証設定

IceWallサーバー内のApache HTTP Serverに対して、SSLサーバー証明書及びルート認証局証明書、CRLを設定します。
次に、IceWallサーバー及び認証サーバーにおいて、IceWall SSOクライアント証明書オプションの認証設定を行います。
その際、デバイス証明書内のUPNをIceWall SSOのユーザーIDとして取得するため、以下の設定を行います。

/opt/icewall-sso/fw/dfw/cgi-bin/dfw.conf

```
#CC_UID=CN
#CC_UIDKEYS=
#CC_UIDKEYE=
#CC_ENVNAME=CLIENT_CERT
CC_DECODE_FLG=0
CC_ENVUID=SSL_CLIENT_SAN_OTHER_msUPN_0
CC_ENVSERIAL=SSL_CLIENT_M_SERIAL
CC_ENVEXPIRE=SSL_CLIENT_V_END
CC_ENVISSUER=SSL_CLIENT_I_DN
```

また、自社向けに発行されたデバイス証明書のみアクセスを受け付けるように次の設定も行います。

Apache HTTP Server設定ファイル（/etc/httpd/conf.d/ssl.conf 等）

```
＜Directory "/opt/icewall-sso/dfw/cgi-bin"＞
SSLRequire (%{SSL_CLIENT_S_DN_O} eq "XXX") ・・・※
:
:
＜/Directory＞
```

※「XXX」の部分には、デバイス証明書の「O」の値（契約時にシステムにより自動的に付与される固定値。法人名と組織識別子）が入ります。

※各設定方法の詳細は、Apache HTTP Server及びIceWall SSOのマニュアルをご参照ください。

③ 各ユーザーのAD属性へのデバイス証明書情報の登録

各ユーザーのAD属性（IceWall SSOクライアント証明書オプションで発行時シリアルNoの参照先として設定した属性）に、各ユーザー向けに発行されたデバイス証明書のシリアルNoおよび発行者名称を登録します。

＜登録データの例（第三世代のデバイス証明書の場合）＞

```
XXXXXXXX:CN=Cybertrust DeviceiD Public CA G3,O=Cybertrust Japan Co.\,Ltd.,C=JP
```

＜登録データの例（第二世代のデバイス証明書の場合）＞

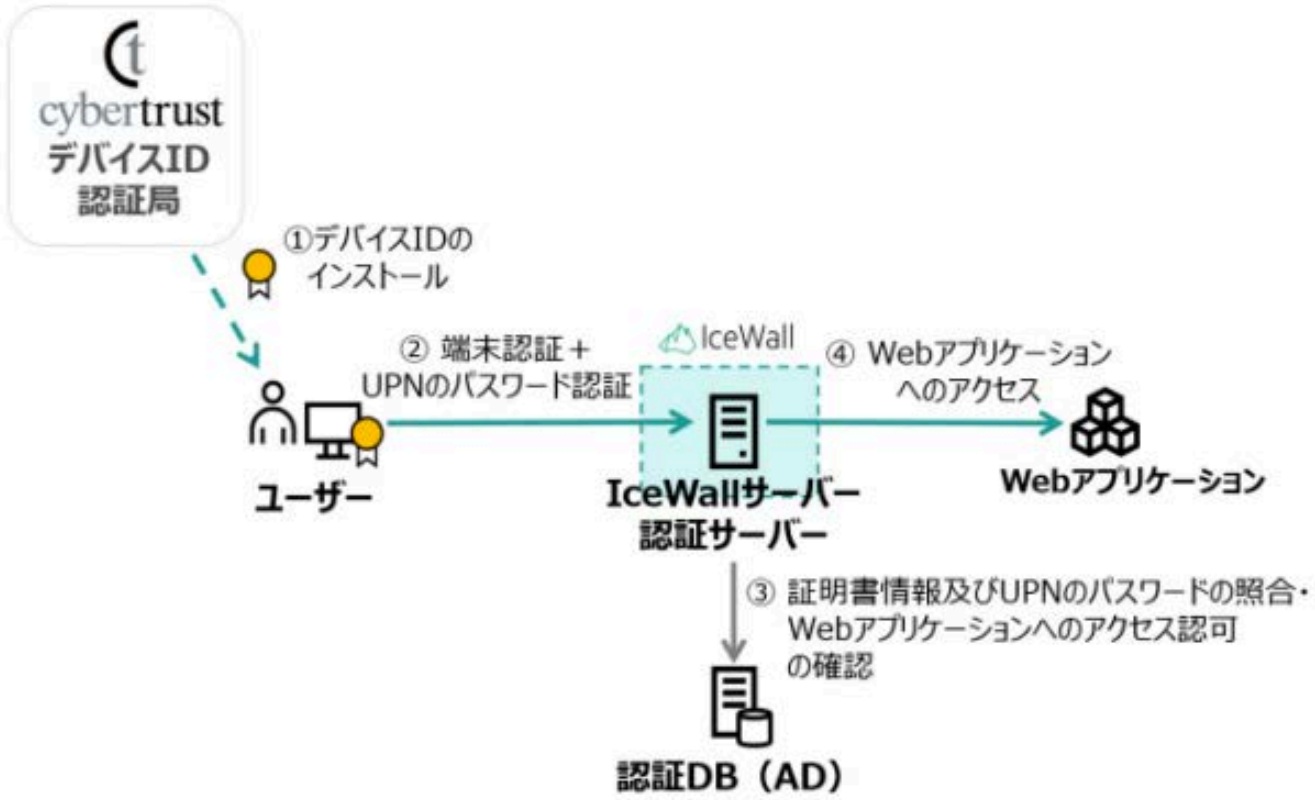
```
XXXXXXXX:CN=Cybertrust DeviceiD Public CA G2,O=Cybertrust Japan Co.\,Ltd.,C=JP
```

※デバイス証明書のシリアルNO（上記例のXXXXXXXX）は、サイバートラスト デバイスID RAオペレータ画面の「発行済み証明書のレポート」等で確認します。
※シリアルNOと発行者名称の間には、「:」（半角コロン）が入ります。

---

5. 認証・アクセスの流れ

本章では、ユーザーの認証・アクセスの流れをご説明します。概要は以下の図の通りです。



① デバイス証明書のインストール

管理者により発行されたデバイス証明書を指示に従い、クライアント端末にインストールします。
※管理者により、あらかじめデバイス証明書がインストールされた端末が配布される場合もあります。詳細はサイバートラスト デバイスID マニュアルをご参照ください。

② 端末認証＋UPNのパスワード認証

クライアント端末のブラウザからIceWall配下のWebアプリケーションのURL（https）にアクセスすると、証明書の確認ダイアログが表示されますので、デバイス証明書の証明書情報を確認の上、OKを押します。デバイス証明書を未インストールの端末の場合はエラー画面が表示されます。（端末認証）

端末認証が成功した場合は、引き続きIceWall SSOのログイン画面（ユーザーIDにはデバイス証明書内のUPNが自動表示）が表示されますので、認証DB（AD）上のパスワードを入力してログインします。（UPNのパスワード認証）

③ 証明書情報及びUPNのパスワードの照合・Webアプリケーションへのアクセス認可の確認

認証サーバーは認証DB（AD）にアクセスして、クライアントから提示されたデバイス証明書の証明書情報と認証DB（AD）上の証明書情報、および入力されたパスワードと当該UPNのパスワードがそれぞれ合致していることを確認し、IceWall SSOの認証セッションを発行します。また、Webアプリケーショ

ンへのアクセス認可の有無を確認します。

④ Webアプリケーションへのアクセス

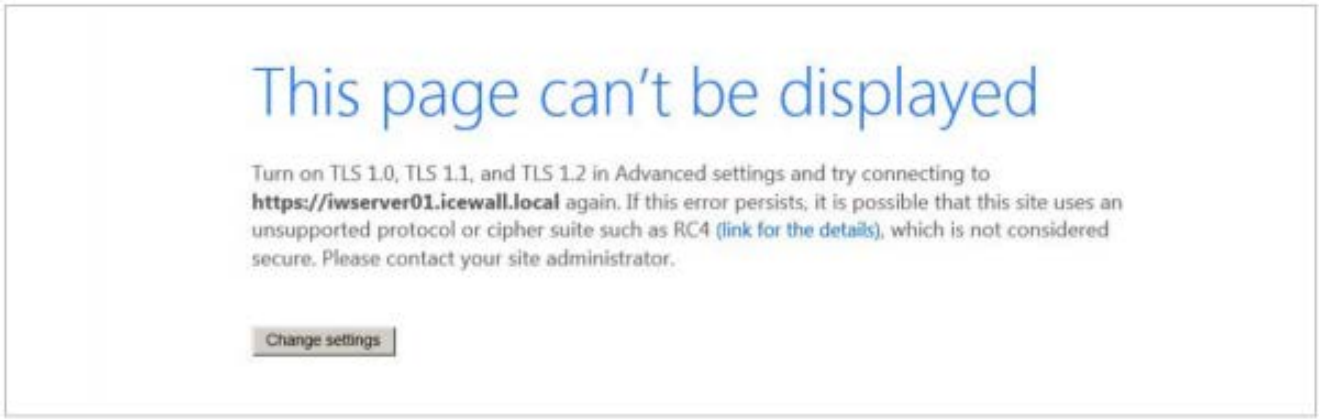
Webアプリケーションへのアクセス認可がある場合には、Webアプリケーションにアクセスします。

以降は、IceWall SSO配下のWebアプリケーション群やクラウドサービスに対して、アクセスが可能となります。(シングルサインオン)

---

6. デバイス証明書の無い端末からのアクセス

上で説明した認証・アクセスの流れは、デバイス証明書がインストールされた「許可された端末」からアクセスした場合のものです。デバイス証明書の無い「無許可の端末」からアクセスした場合は、IceWall SSOのログイン画面にはアクセスできず、Webブラウザには下記のようなTLSのエラーメッセージが表示されます。



つまり、例え正当なユーザーによる利用であっても無許可の端末からのサービス利用（クラウドサービスや社内イントラWebアプリ）は（本来の狙い通り）できないと言うことになります。

7. まとめ

本技術レポートでは、サイバートラスト デバイスIDとIceWall SSOの連携により、厳格な端末認証の上でユーザー認証・認可制御を行う統合認証基盤を実装する方法をご紹介しました。

企業の情報資産やクラウドサービスへの安全なアクセスを実現するための方法として、本実装方法を是非ご検討ください。

サイバートラスト デバイスID お問い合わせ先：

製品・サービス総合受付
電話　：0120 - 957 – 975
e-mail：servicedesk@cybertrust.co.jp

2018/4/18 新規掲載

執筆者　：日本ヒューレット・パッカード株式会社
Pointnext事業統括　IceWallソフトウェア本部 認証コンサルティング部
谷垣 敦

技術レポート一覧へ →

お探しの情報は見つかりましたか？

検索のサポート


ご購入方法


製品サポート


営業へのお問い合わせ


お問い合わせ先一覧




企業情報

会社情報

アクセス

お問い合わせ

採用情報

HPEについて

インクルージョン & ダイバーシティ

サステナビリティと企業責任

経営幹部

お知らせ

ニュースルーム

イベント・セミナー

新着情報

重要なお知らせ

パートナー

パートナープログラム

認定資格制度

OEMソリューション

サポート

製品サポート

ソフトウェア & ドライバー

標準保証確認

オペレーショナルサポート

教育とトレーニング

製品リサイクル

機器部品の妥当性確認

コミュニティ

HPE Japan ブログ

リソース

お客様事例

ご購入方法

オンラインストア

HPE Customer Center

Eメール登録

ドキュメントライブラリ

Resource Library

ビデオギャラリー

金融サービス

日本 (ja)