IceWall技術レポート:

IceWall SSO＋Aruba ClearPassの連携
－ 無線LANとWebサービスの提供で集客力・顧客満足度向上

1. はじめに ～無線LAN提供による集客と顧客満足向上～

昨今では、店舗・スタジアム・劇場と言った公共の場所で高速な無線LANサービスが提供されることが多くなっています。このような公共の場所での無線LANサービスは、利用者にとって便利でありがたいものであるのと同時に、提供する事業者側にとっては、集客を促進するための手段として、あるいは顧客満足度を高めるための手段にもなりえます。
さらには、単にインターネットに接続可能な無線LANを提供するだけでなく、事前にWebなどで個人情報を登録した会員向けに特別なWebサービスを提供することで、より一層ビジネスの可能性を高めることも考えられるようになってきました。

このような無線LANと種々のWebサービスの提供において、IceWall SSOとAruba ClearPassとの認証連携が、顧客満足度を最大化するサービス提供を可能にします。本技術レポートでは、IceWall SSOとAruba ClearPassとの連携させる方法について紹介いたします。

2. 適用ソリューションの例

＜適用例1＞
あるショッピングモールは、個人情報を登録した会員向けに、お買い得情報やクーポンなどの情報をWeb経由で提供していました。
顧客満足度向上を狙って、新たに実際の店舗内で無線LANサービスを提供することになりましたが、Webサービスの会員のみがそのログオンアカウントで店舗内の無線LANにアクセスできるようにしました。こうすることで、Webサービスの登録率を上げる効果も期待できます。
一旦無線LANのための認証を行えば、その店舗のサイトにはシングルサインオンでログオンできますので、顧客は気軽に会員向けのポイントやクーポン情報を利用できます。これによって、店舗での顧客の購買意欲を促すことも期待できます。

＜適用例2＞
あるスポーツチームは、ファンクラブ会員限定でチームの状況をWebサイトで提供していました。
さらにファンクラブ会員向けに、ホームスタジアムでの無線LANサービスを提供し始めました。スタジアム内無線LANにアクセスすれば、ファンクラブ向けのサイトにもシングルサインオンでログオン可能です。
ファンクラブサイトでは、出場選手の情報など、スタジアム観戦をより楽しくするための情報が提供されます。
さらには、サイト内で提供されるゲームやくじによって、チームグッズをプレゼントしたり、スタジアム内でのゲームに参加出来たりします。
ファンクラブへの入会者を増やすためにも、ファンクラブ会員をスタジアムに足を向かせるためにも、これらの仕組みは役立ちます。

3. Aruba ClearPassとは

Aruba ClearPassは、モバイルデバイスやIoTデバイスなどの無線LAN対応デバイスに、セキュアなネットワークアクセスを提供する製品です。
RADIUSによる拡張性の高いAAA(Authentication Authorization Accounting: 認証, 認可, 課金)をベースにユーザー、デバイスなどの様々なコンテキスト・データを活用し、各デバイスやユーザーに応じたポリシーを無線、有線、VPNのネットワークアクセスを制御する製品です。
標準で様々な3rdパーティITシステム(NGFW, MDM/EMM, DIEM, IdentityStoreなど)との連携機能を持ち、認証

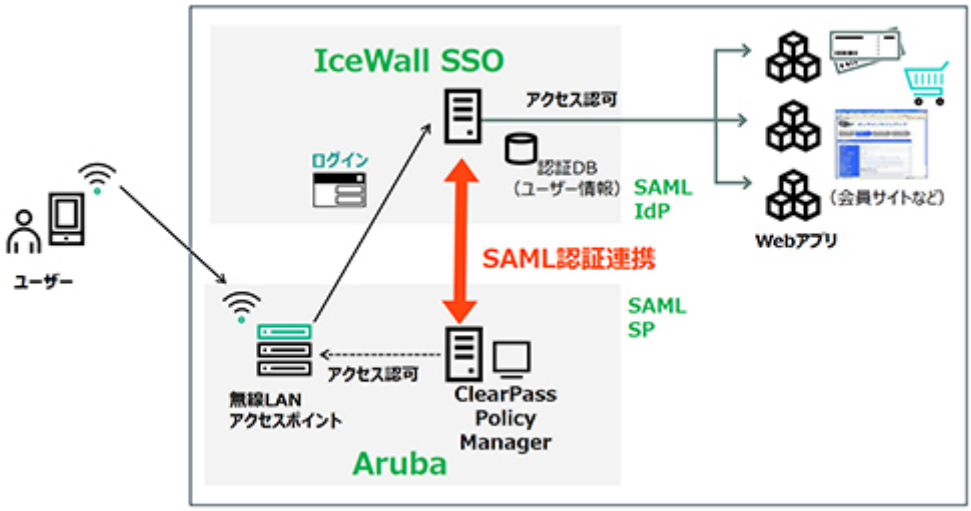
情報、コンテキスト情報などの様々な情報を共有することで、ネットワークセキュリテイを維持する協調的な適応型防御機能を構築することができます。
またマルチベンダーの環境で、あらゆる種類のモバイルデバイスのユーザーに、セキュアで自動化されたゲストアクセスを提供するClearPass Guestを備えています。

4. IceWall SSO＋Aruba ClearPassの認証連携概略

ClearPass Policy Managerは、SAMLによる 3rd Party 製品(例えば、Shibboleth, simpleSAMLphp, Google Apps など)との認証連携の機能を有しています。
SAML Service Provider (SP)と SAML Identity Provider (IdP)の双方に対応しており、Single Sign-On の機能として下記のA) B) C)の3つの動作をサポートしています。

A) Automatic Sign On (ASO)
HPE Aruba Wi-FiコントローラとClearPassの環境における802.1xによるネットワークアクセス認証の結果を、他のSAML製品のログイン認証システムへ提供します。
(Aruba ClearPassは、IdPとして動作します)
B) Access Network SSO
他IdPの認証システムを利用し、ネットワークへのゲストアクセス(ゲストログイン)を提供します。
(Aruba ClearPassはSPとして動作します)
C) ClearPass Admin SSO
Aruba ClearPassシステムにログインする際に、他のIdPの認証システムを利用します。
(Aruba ClearPassはSPとして動作します)

本技術レポートでは、上記B)の機能を用いて、IceWall SSO (Federation) をSAML IdP, ClearPass Guest User Access をSAML SP として構成する方法を解説します。
(下図参照)



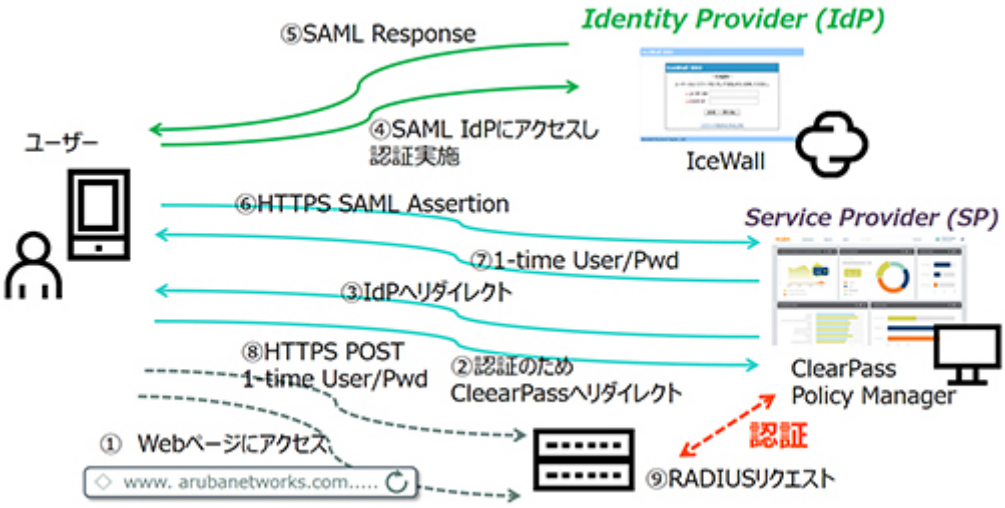
IceWall SSO＋Aruba ClearPassの連認証携概略
-無線LANアクセスとWebアプリの認証を連携

(注意事項)
SAML SP、SAML IdPのいずれも、NTPを使用した時間の同期とDNSでの名前解決が必要です。

5. Access Network SSO動作概略

無線LAN対応デバイスから、提供されているSSIDにWi-Fi接続をし、Webブラウザーから任意のサイトにアクセスすると、Wi-Fiサービスは入力された任意のサイトからIceWall SSOが提供するログイン画面へリダイレクトされます。(ユーザーから見ると、強制的にIceWall SSOのログイン画面に誘導されたように見えます。)

ユーザーがIceWall SSOのログイン画面にて認証を行うと、Aruba ClearPassはSAML連携によってIceWall SSO (Federation)から認証情報を入手し、その認証情報に基づいてWi-Fiネットワークへの接続を許可します。これによりユーザーは、Wi-Fiネットワークから任意のインターネットサイトにアクセスが可能になります。
Wi-Fiネットワークの利用が許可されただけでなく、IceWall SSOが提供するSingle Sign-On機能も提供されますので、IceWall SSOと連携した様々なWebサービスへ、追加の認証手続き無しにアクセスすることが可能になります。



Access Network SSO
– ClearPassはSAML SPとして動作

0. ユーザーが、提供されているWi-FiのSSIDを選択。
1. Webブラウザーより任意のWebページにアクセス。
   (フロー図では、www.arubanetworks.com)
   1.1 無線LANコントローラは、Webブラウザーに対してClearPassの認証用Webページへリダイレクト指示。
2. Webブラウザーは、1.1で指示されたClearPassの認証用Webページへ接続。
3. ClearPassの認証用Webページは、SSOの認証設定により、IdPの認証用Webページへリダイレクト指示。
4. Webブラウザーは、3で指示されたIdPの認証用Webページへ接続。
   4.1. IdP認証画面においてusername/passwordを入力し、IdPでユーザー認証を行う。
5. IdPは、認証応答 SAML Responseを返信。
6. Webブラウザーは、ClearPassにSAML Assertionを送信。
7. ClearPassは、SMAL Assertionを受けたことにより、one-time(一時的な) usernameとpasswordをWebブラウザーに送信。
   (このone-time usernameとpasswordを使ってRADIUS認証を行いWi-Fiサービスを提供)
8. Webブラウザーは、HTTP POSTで one-time usernameとpasswordを無線LANコントローラに送信。
9. 無線LANコントローラは、one-time usernameとpasswordを使用してWi-FiサービスのためのRADIUS認証をClearPassへ送信。
10. ClearPassは、RADIUS認証を実施し、Wi-Fiサービスを許可。
11. Webブラウザーは、Wi-Fiサービスを許可されたことで、最初にアクセスしたページ(上の図ではwww.arubanetworks.com)を表示。

6. ClearPassの設定手順

Aruba ClearPassでは、ClearPass GuestにおけるWebログインページでSAML Single Sign-Onを有効にすることができます。
構成には、ClearPass GuestにおけるWeb ログインページでの設定と、ClearPass Policy ManagerにおいてSAML SPとしてゲストユーザーに適用する認証サービスの構成が必要になります。それぞれ下記のようなステップになります。

1) ゲストアクセスのための Web Login ページの作成
2) サービステンプレートを使ってゲストアクセスサービスを追加
   (下記のサービステンプレートを使用)
   2.1) ClearPass Admin SSO Login (SAML SP Service)
   2.2) Guest Access
3) ゲストユーザーのrole構成のためのエンフォースメント追加
4) SSO コンフィグレーションへの IdP URLの追加
5) IdP側(IceWall SSO)の設定
6) 接続テスト

以降で手順の詳細を記述します。

1）ゲストアクセスのためのWeb Login ページの作成

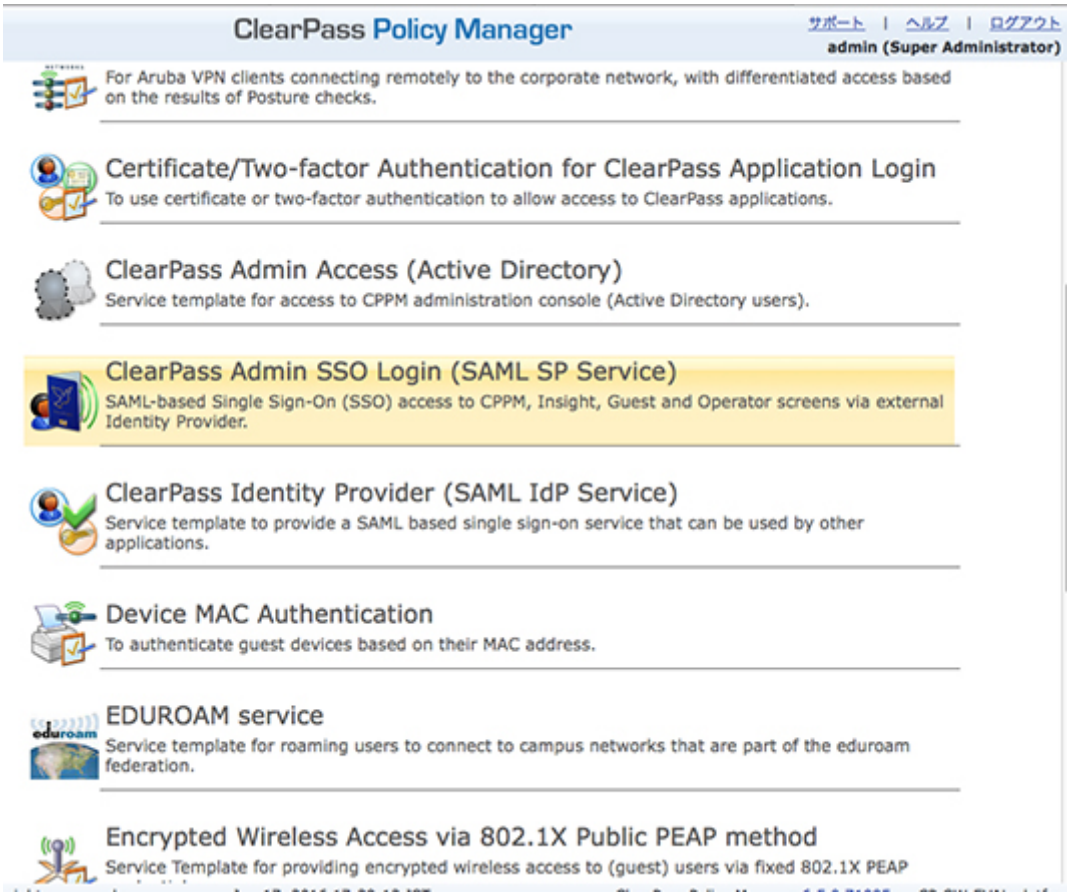
ClearPass Guestにアクセスし”ホーム >> 構成 >> Pages >> Webログイン”へ移動します。
“Webログイン ページの新規作成”をクリックし、Web Login Editorで“名前”および“ページ名”を入力します。
“事前認証チェック”では、リストから”Single Sign-On - enable SSO for this web login”を選択します。
他の部分は、デフォルトで問題ありませんが、必要に応じて設定願います。
最後に、“変更を保存”します。

[拡大画像を表示]

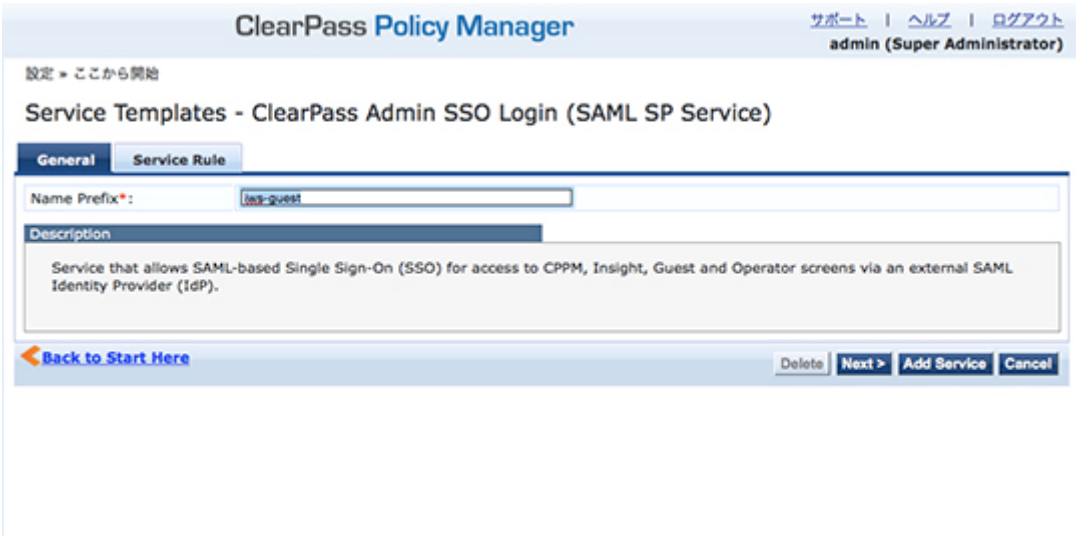
2）サービステンプレートを使ってSSOサービスを追加

2.1）ClearPass Admin SSO Login（SAML SP Service）

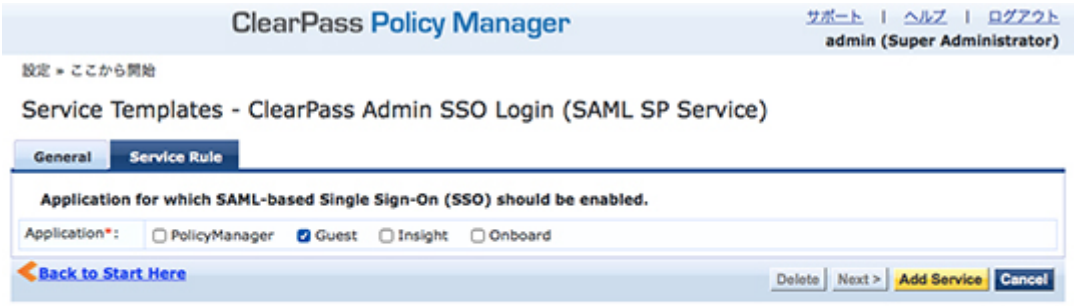
ClearPass Policy Managerにアクセスし、“設定 >> ここから開始”へ移動します。次に“ClearPass Admin SSO Login (SAML SP Service)”を選択します。



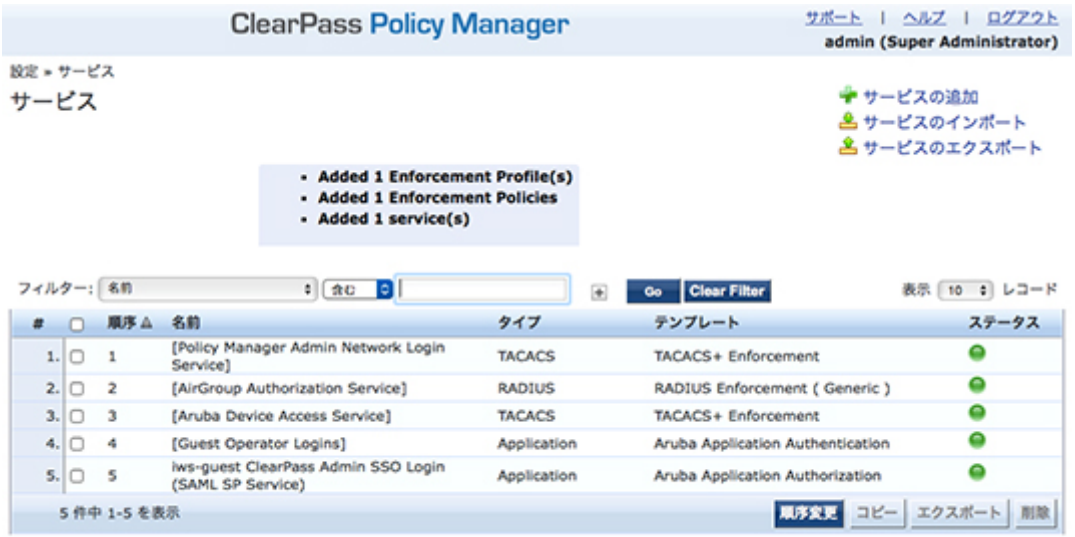
構成wizardが始まり、指示にしたがって必要項目を入力していきます。
General タブではName Prefixを入力します。このName Prefixは、サービス、エンフォースメントポリシー・プロファイルなどのwizardで作成する名前のprefixに使用されます。Nextをクリックして、構成を進めてください。



Service Ruleタブでは、ApplicationとしてGuestを選択し、Add Serviceをクリックします。



1つのエンフォースメント・プロファイル、1つのエンフォースメントポリシー、1つのサービスが追加されます。
このページでは、iws-guest ClearPass Admin SSO Login (SAML SP Service)という名前のサービスが作成されたことが確認できます。



サービスのサマリーページは、下図のようになっています。
ClearPass Admin SSO Loginサービスと共通のwizardを使用しているため、ClearPass Guestに使用できるよう、エンフォースメント・プロファイルの変更を続いて行います。

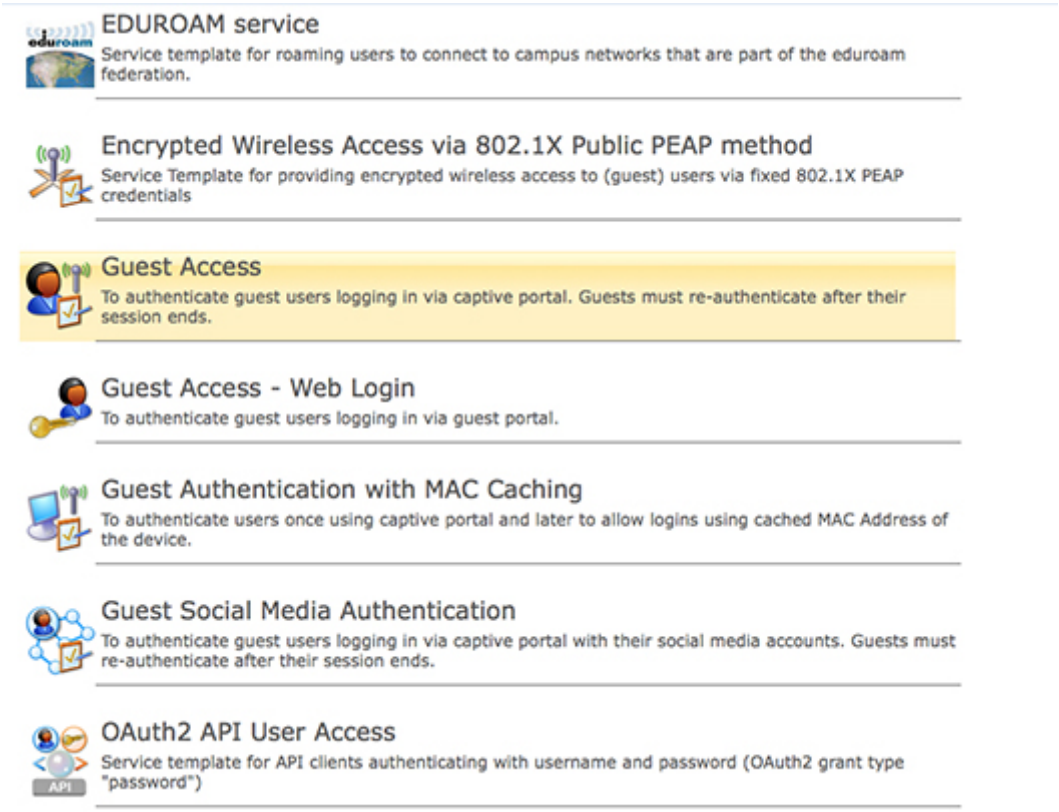
“設定 >> エンフォースメント >> プロファイル”へ移動し、“Admin SSO Login プロファイル”をクリック後、“プロファイル”タブを表示します。“名前”を適切な名称に変更します。(“Admin SSO” を Guest SSO” 等)

“属性”タブを選択し、SSO-Roleの属性値を [User Authenticated]に変更し、保存します。

2.2) Guest Access

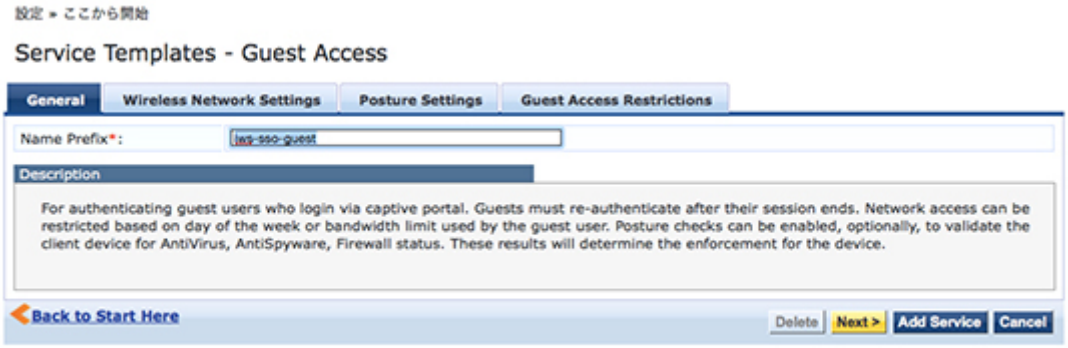
サービステンプレートを使ってゲストアクセスサービスを追加します。

ClearPass Policy Managerにアクセスし、“設定 >> ここから開始”へ移動した後、“Guest Access”を選択します。

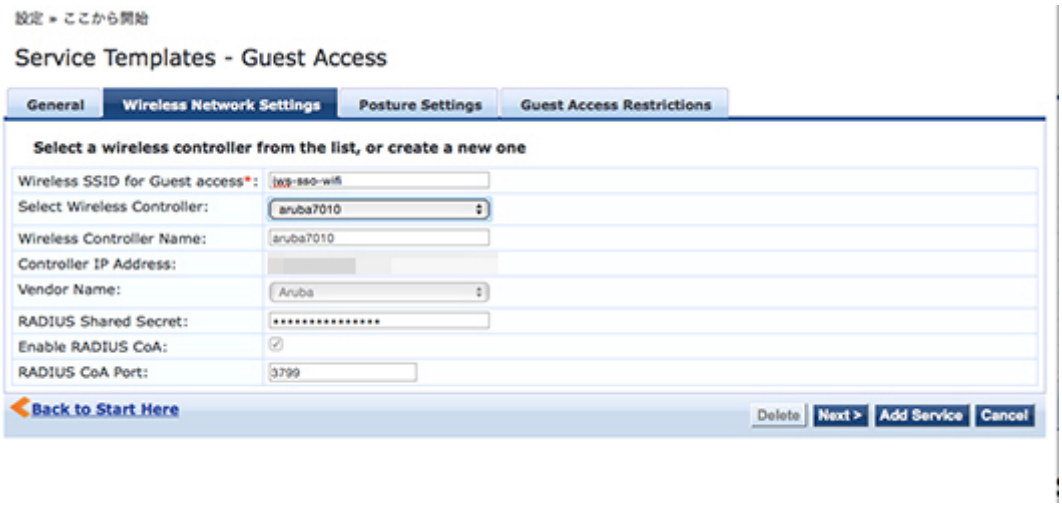


構成wizardが始まり、指示にしたがって必要項目を入力していきます。

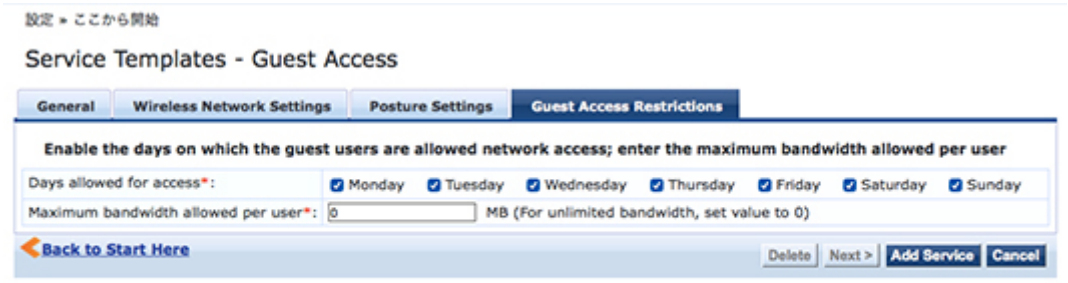
General タブではName Prefixを入力します。このName Prefixは、サービス、エンフォースメントポリシー・プロファイルなどのwizardで作成する名前のprefixに使用されます。Nextをクリックして、構成を進めてください。



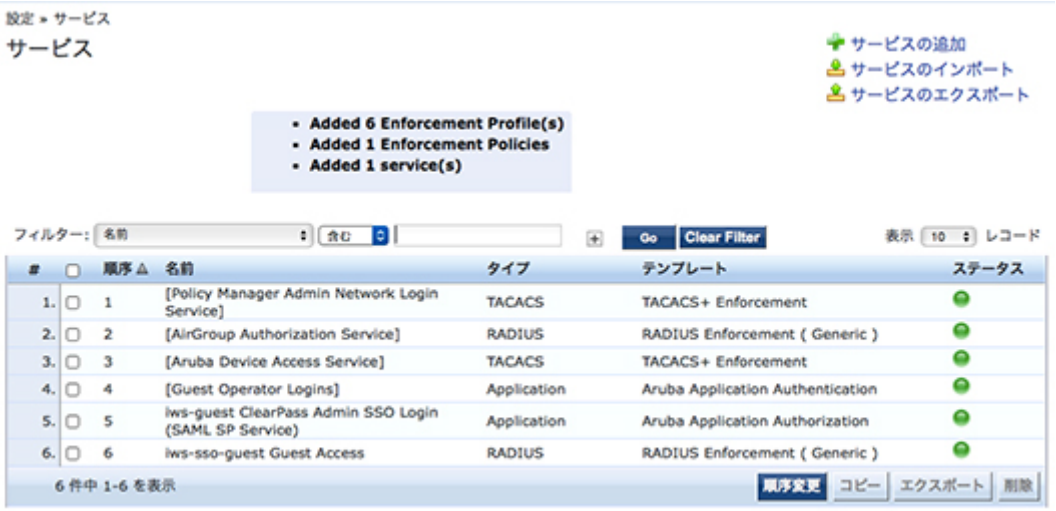
“Wireless Network Settings”タブでは、Wi-Fiのゲストアクセスサービスで使用するSSIDの名前を入力し、Wireless Controllerを選択した後、RADIUSのShared Secretを入力しNext>>をクリックします。
(Wireless Controllerのリストは、すでに登録済みのNetwork Access Deviceが表示されます。なにも表示されない場合は、ネットワークデバイスを追加してください)



“Guest Access Restrictions”タブでは、ゲストユーザーのネットワークアクセス制限について設定が可能です。
例えば曜日などに応じたアクセス制限や、最大バンド幅を設定することができます。



6つのエンフォースメント・プロファイル、1つのエンフォースメントポリシー、1つのサービスが追加されます。
このページでは、iws-sso-guest Guest Accessという名前のサービスが作成されたことが確認できます。



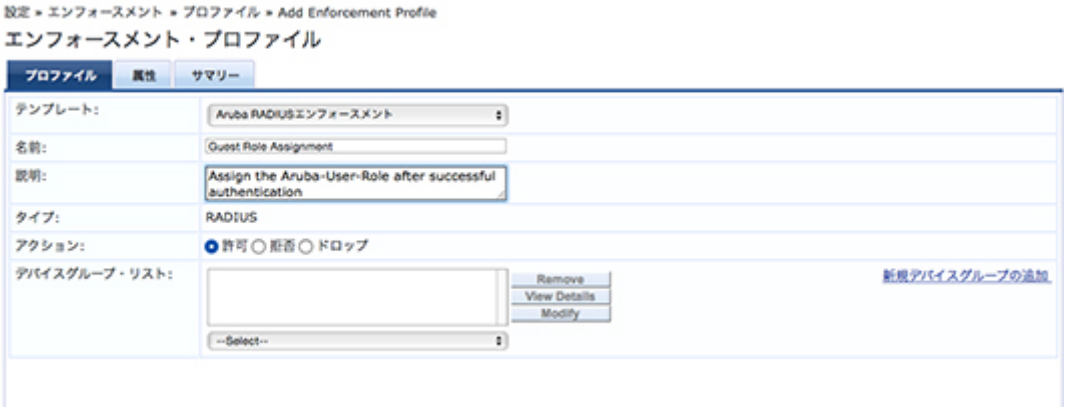
RADIUSサービスの認証方式を変更する必要があるため、“設定>>サービス”へ移動し、iws-sso-guest Guest Accessサービスを編集します。
編集画面の“認証”タブで、あらかじめ登録されている認証方式をすべて、“Remove”（削除）した、--Select to Add から[SSO]を選択し、認証方式に登録後、保存します。

3）ゲストユーザーのrole構成のためのエンフォースメント追加

wireless controllerで設定しているGuest user roleのRADIUSエンフォースメントを追加します。
このエンフォースメントは、認証が成功した際に使用されます。
ClearPass Policy Managerの“設定 >> エンフォースメント >>プロファイル”へ移動し、Add Enforcement Profile をクリックします。

以下の構成プロファイルを作成しセーブします。

1. テンプレート : Aruba RADIUSエンフォースメント
2. 名前 : プロファイルの名前を入力
3. 説明 : オプション

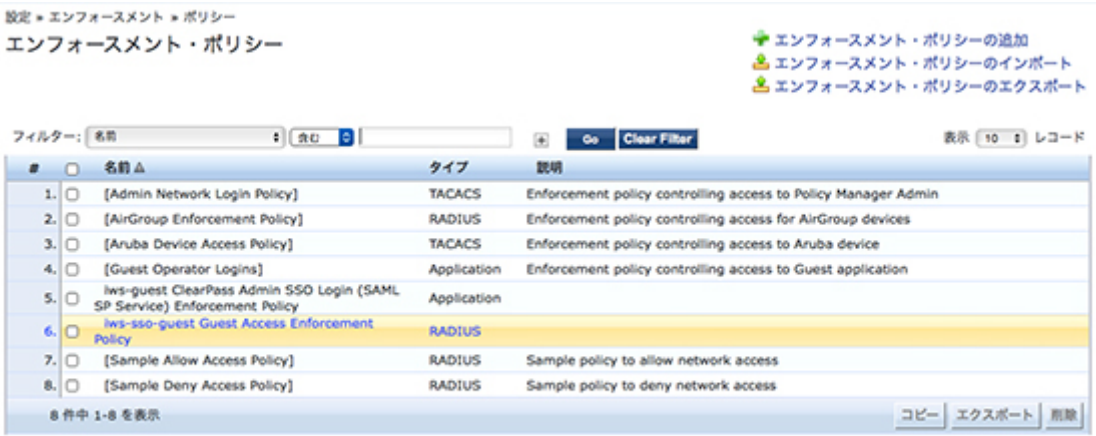


[拡大画像を表示]

“属性”タブでは、”Aruba-User-Role”の属性値を入力し保存します。
この値は、Wireless controllerで設定してあるrole名と一致させる必要があります。本技術レポートでは、guestという値であり、Wireless controller上で、guestという名前のroleが存在することを前提にしています。

[拡大画像を表示]

すでに作成済みのエンフォースメントポリシーに、上記で作成したエンフォースメント・プロファイルを追加します。
“設定 >> エンフォースメント >> ポリシー”へ移動し、該当ポリシー(＜Name Prefix＞ Guest Access Enforcement Policy ～ 本技術レポートでは“iws-sso-guest Guest Access Enforcement Policy”)をクリックします。



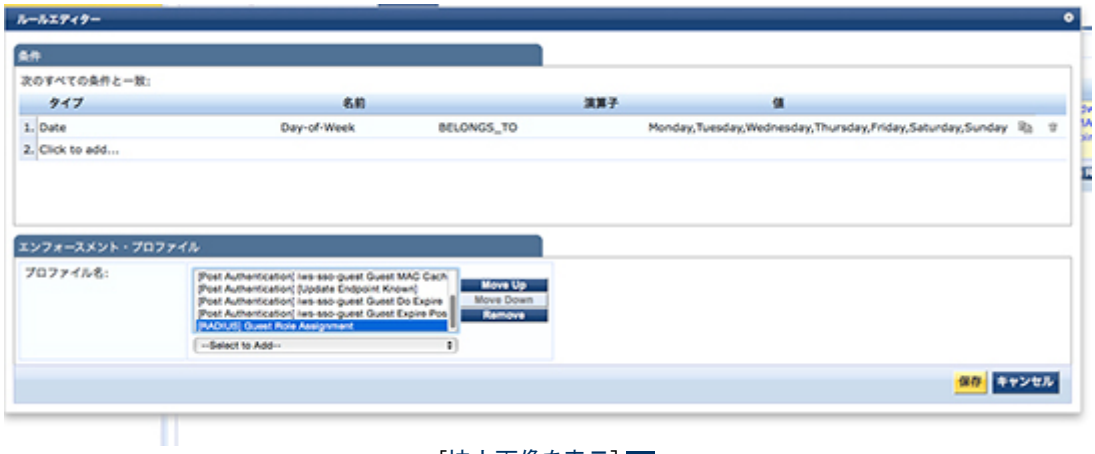
[拡大画像を表示]

“ルール”タブを選択し、すでに作成済みのルールを編集します。

ルールを選択し[Edit Rule]をクリックします。

[拡大画像を表示]

“ルールエディター”がポップアップし、ここで編集を行います。
上記で作成したエンフォースメント・プロファイル(本技術レポートでは[RADIUS] Guest Role Assignment)を追加します。

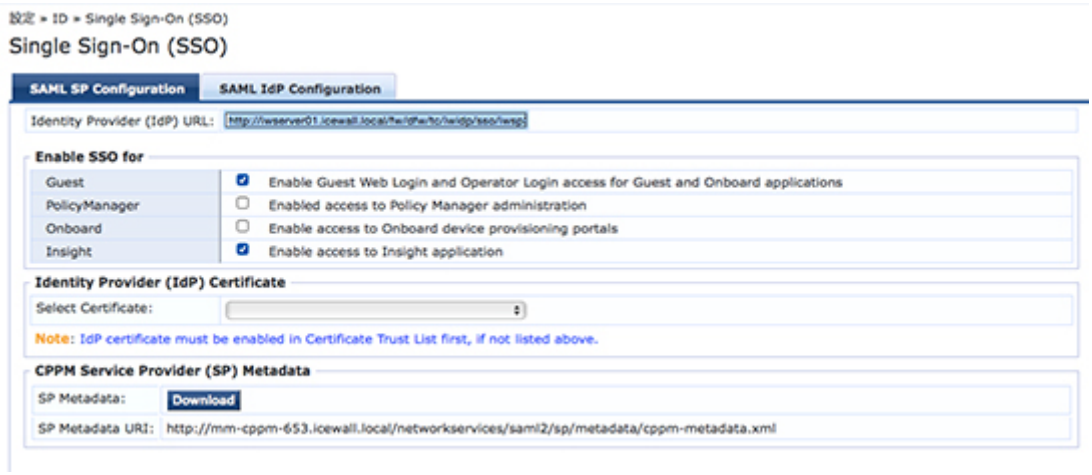


[拡大画像を表示]

4) SSOコンフィグレーションへのIdP URLの追加

ClearPass Policy Managerで、SSOの設定を行います。
“設定 >> ID >> Single Sign-On(SSO)”へ移動し、SAML SP Configuration タブにて、Identity Provider (IdP) URL を入力します。
IceWall SSO (Federation)の場合、“http://<IceWall SSOのFederationサーバー名>/fw/dfw/tc/iwidp/sso/config”になります。本技術レポートでは、IceWall SSOのFederationサーバーをホスト名 iwserver01、ドメイン名icewall.local、iwsp3.confと設定しているため、URLは、“http://iwserver01.icewall.local/fw/dfw/tc/iwidp/sso/iwsp3”と入力します。

次にSSOサービスを有効にするアプリケーションを選択します。



[拡大画像を表示]

Aruba Controller (もしくはInstant)では、guest用SSID (本技術レポートでは、iws-sso-wifi)と、captive portalとしてweb login pageのURLを登録し、必要に応じて認証前のIdPサーバーへのアクセス許可の firewall 設定を行います。

5) IdP側(IceWall SSO)の設定

IceWall SSOのFederationサーバー にClearPassへのサービスのためのconfig fileを作成します。

```
/opt/icewall-federation/config/iwidp/iwidp3.conf
```

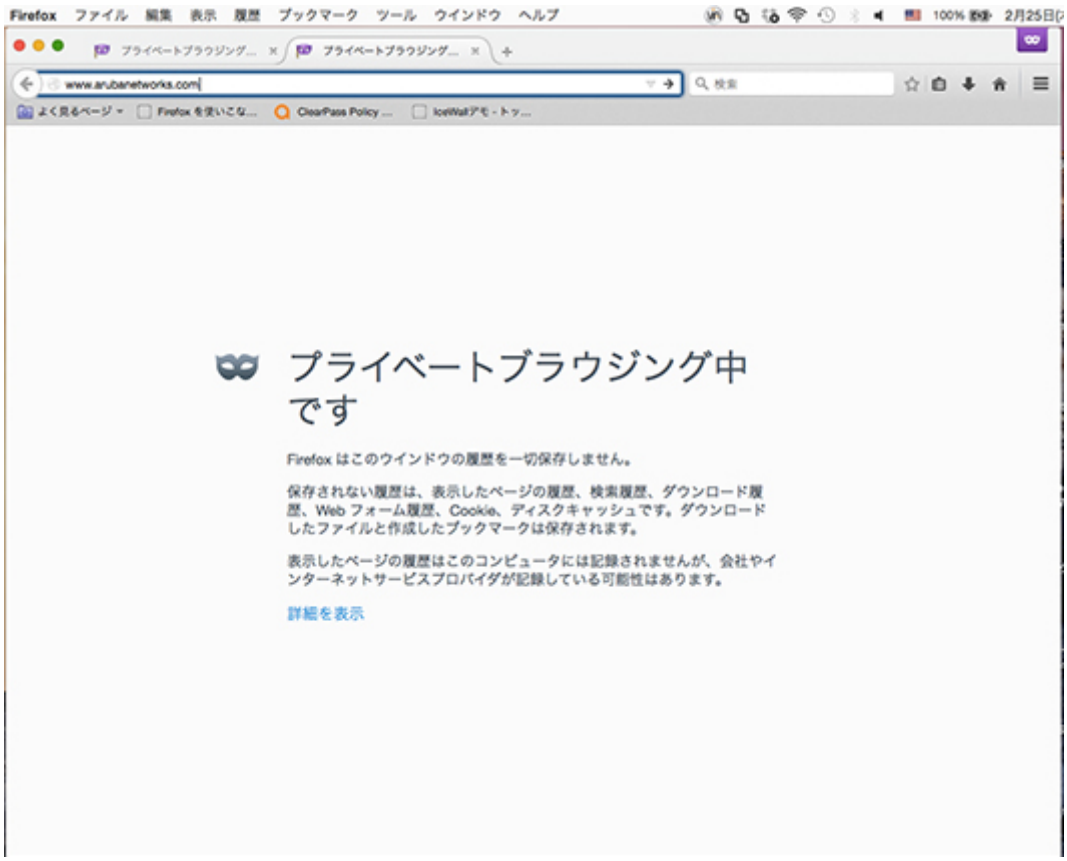
上記config fileに、Assertion Consumer Service (ACS)URL, Service Provider Entity IDとして各々下記を設定します。

```
#-------------------------------------------------------------------------------
# ACS_URL : Assertion consumer service's URL of Service Provider
# SP_ENTITY_ID : ID of Service Provider
#-------------------------------------------------------------------------------
ACS_URL=https://<ClearPass hostname>/networkservices/saml2/sp/acs
SP_ENTITY_ID=https:///<ClearPass hostname>/networkservices/saml2/sp
```

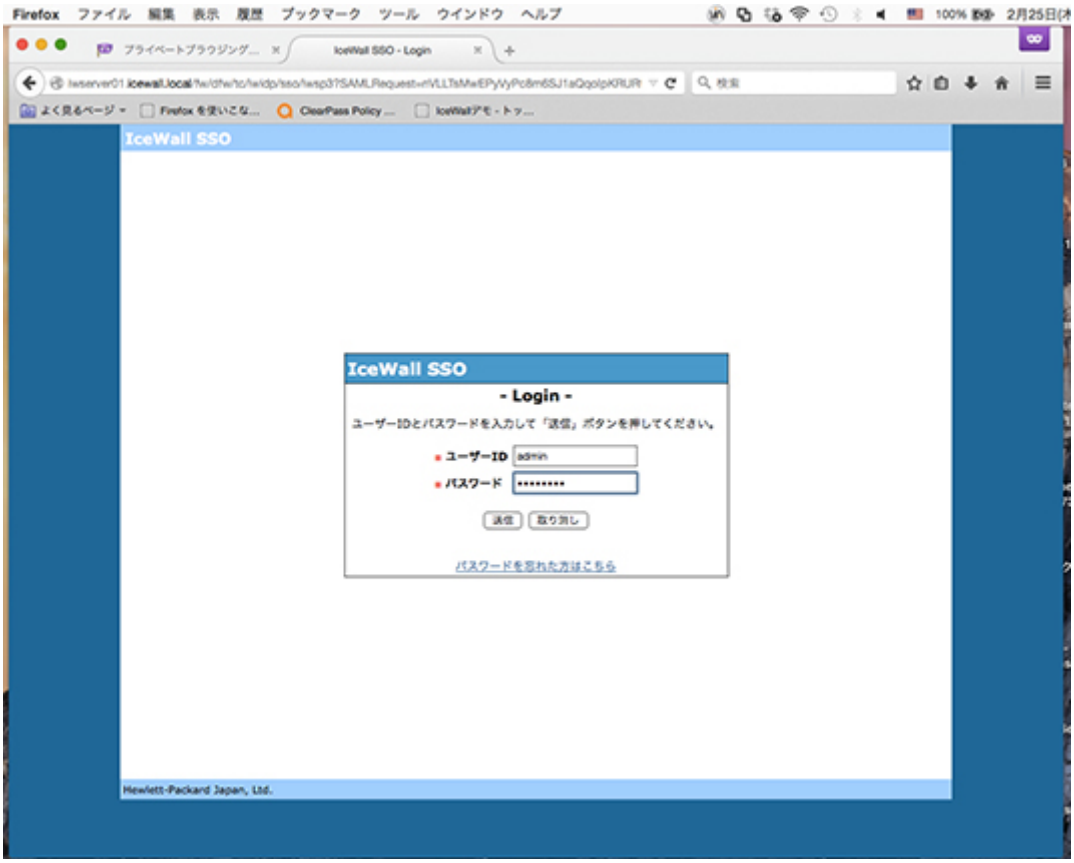
6) 接続テスト

端末をguest用SSIDに接続。Webブラウザーで任意のインターネットサイトにアクセスすると、IceWall SSOへリダイレクトされて、IceWall SSOのログイン画面が表示されます。登録済みのユーザーアカウントを使用して認証が成功すると、指定したインターネットサイトが表示されます。
IceWall SSOのポータルサイトにアクセスした場合は、追加の認証をすることなく、Wi-Fi接続時に認証を行ったユーザーの権限でポータルサイトにアクセスできます。

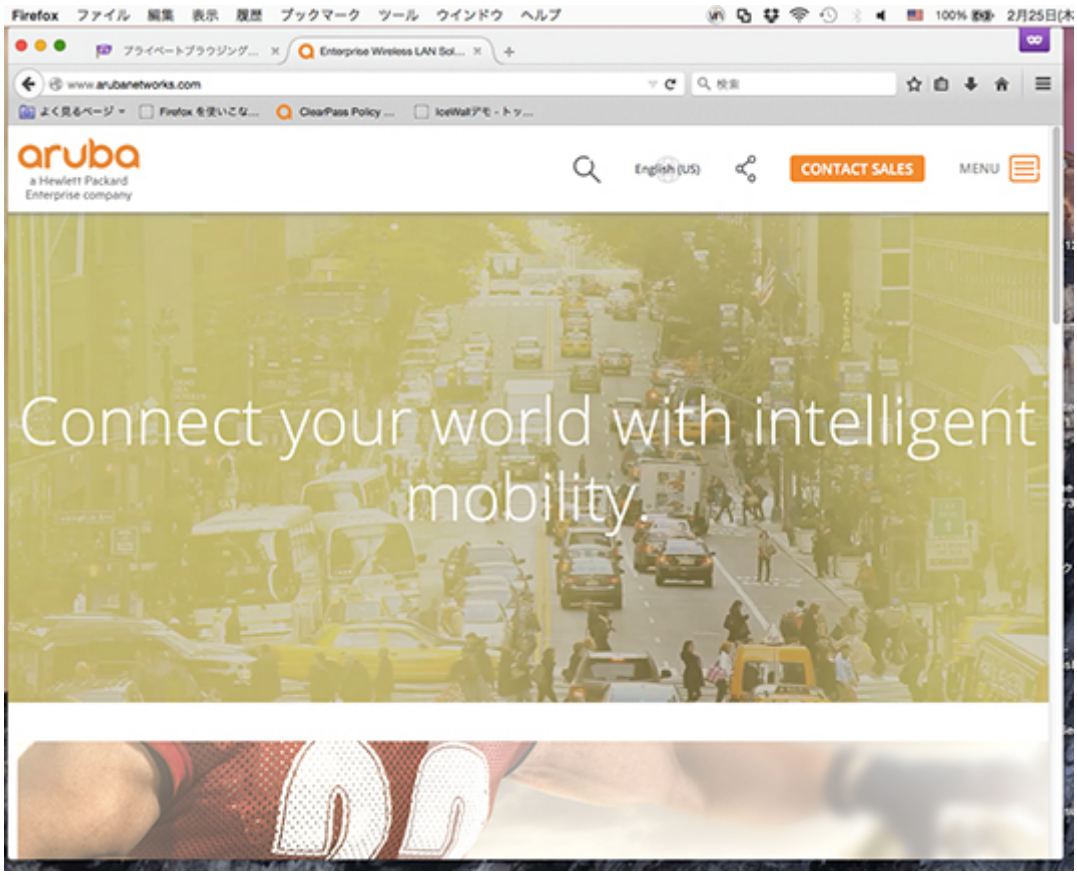
・永続的なCookieの影響を排除するため、Webブラウザのプライベートブラウジングモードで検証します。



・ユーザー指定したサイトのアドレスに関わらず、必ずIceWall SSOのログオン画面に誘導されます。



・IceWall SSOのログオンが完了すれば、当初ユーザーが指定したサイトが表示されます。



・ユーザーがIceWall SSOのポータルサイトにアクセスした場合は、追加の認証の必要なくポータルにアクセスできます。

7. まとめ

IceWall SSOとAruba ClearPassの連携により、提供されたSSIDにアクセスするとIceWall SSOの認証に誘導され、そこでの認証によって無線LANサービス及び各WebサービスがSingle Sign-Onで利用できることが確認できました。
冒頭に記述したように、様々な用途に応用が期待されます。

本ソリューションに関するお問い合わせ

2016.7.13　新規掲載

執筆者　日本ヒューレット・パッカード　ネットワーク事業統括本部　コンサルティング技術部
水谷 雅洋