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。

ー旦無線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。





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。
- 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
- 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

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。

	Web Login Editor
* 名前:	cewall-sso-guest このWebログイン ページの名前を入力します。
ページ名:	cewall-sso-guest このWebログインのページ名を入力します。 Webログインには"page_name.php"からアクセスできます
說明:	lceWall SSO Guest Login (IceWall SSO IdP - ClearPass SP) Webログインに関するコメントまたは説明。
* ペンダー設定:	Aruba Networks 標準のネットワーク機成に適した定義済みの設定グループを連択します。
Login Method:	Controller-initiated — Guest browser performs HTTP form submit S Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.
* アドレス:	securelogin.arubanetworks.com ペンダーの製品のIPアドレスまたはホスト名を入力します。
セキュアなログイン:	 ペンダーのデフォルト設定を使用する Webログイン プロセスに適用するセキュリティ オブションを選択します。
ダイナミック アドレス:	資格情報の送信のためにコントローラがIPを送信する 多くのマルチコントローラ環境では、元のリダイレクトの一部として提供される別のアドレスに資格情報を送信する必要があります。 上のアドレスは、パラメータが存在しない、または次の要件を満たしていない場合に常に使用されます。
Security Hash:	Do not check – login will always be permitted Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the user, for example their MAC address.
ログイン フォーム ログイン フォームの動作と	内容を指定するオプション。
Prevent CNA:	Enable bypassing the Apple Captive Network Assistant The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not work with all vendors, depending on how the captive portal is implemented.
* 事前認証チェック:	Single Sign-On — enable SSO for this web login SNAS認証に進む前にユーザー名とバスワードをどのようにチェックするかを選択します。
デフォルトの宛先 ログイン後の充先クライア:	ントのリダイレクト先を制算するオブション。 [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。

ClearPass Policy Manager	サポート I ヘルプ I ログアウト admin (Super Administrator)
設定 > ここから開始	
Service Templates - ClearPass Admin SSO Login (SAML SP Service)	
General Service Rule	
Name Prefix*: (agr-guest	
Description	
Service that allows SAML-based Single Sign-On (SSO) for access to CPPM, Insight, Guest and Operato Identity Provider (IdP).	r screens via an external SAML
Sack to Start Here	elote Next > Add Service Cancel

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。

ClearPass Policy Manager	サポート ヘルブ ログアウト admin (Super Administrator)
設定 » ここから開始	
Service Templates - ClearPass Admin SSO Login (SAML SP Service)	
General Service Rule	
Application for which SAML-based Single Sign-On (SSO) should be enabled.	

Delete Next > Add Service Cancel

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。

			ClearPass Polic	cy Manager		<u>サポート</u> admi	in (Super Administrator)
18定 » サー	サービ ビス	z				÷ & &	サービスの追加 サービスのインポート サービスのエクスポート
			 Added 1 Enfo Added 1 Enfo Added 1 Serv 	vrcement Profile(s) vrcement Policies vice(s)			
フィル	9-:	80	\$ (AC)		•	Go Clear Filter	表示 10 🔹 レコード
	0	順序△	名前	タイプ		テンプレート	ステータス
1.	0	1	[Policy Manager Admin Network Lo Service]	gin TACACS		TACACS+ Enforcement	Θ
2.	0	2	[AirGroup Authorization Service]	RADIUS		RADIUS Enforcement (Gene	ric) \Theta
3.	0	3	[Aruba Device Access Service]	TACACS		TACACS+ Enforcement	•
4.	0	4	[Guest Operator Logins]	Application		Aruba Application Authentica	ition \varTheta
5.	0	5	iws-guest ClearPass Admin SSO Lo (SAML SP Service)	gin Application		Aruba Application Authorizati	ion \Theta
	5 194	1-5 をき	示			東市文王	コピー エクスポート 削除

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。

Application*:

PolicyManager
Guest
Insight
Onboard

Back to Start Here

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。

	ClearPass Policy M	lanager	<u> サポート</u> <u>ヘルプ</u> <u>ログアウト</u> admin (Super Administrator)
^{定。サービス > 編集 - Iws-gu} トーピス - iws-guest	est ClearPass Admin SSO Login (S t ClearPass Admin SSO Note: This Service	AML SP Service) Login (SAML SP Service ce is created by Service Temple	ice) ate
サマリー サービス ロ	コール エンフォースメント		
<u>サービス:</u>	hus quast ClassDass Admin CCO I	colo (CAMI CD Convice)	
說明:	SAML-based Single Sign-On (SSC Provider.)) access to CPPM, Insight, Guest	and Operator screens via external Identity
タイプ:	Aruba Application Authorization		
ステータス:	Enabled		
監視モード:	Disabled		
その他のオプション:	•1		
サービスルール			
次のすべての条件と一致:			
タイプ	名前	演算子	
1. Authentication	Туре	EQUALS	SSO
2. Application	Name	BELONGS_TO	Guest
a— <i>I</i> II:			
ロール・マッピング・ポリシー	: •		
エンフォースメント:			
キャッシュされた結果の使用:	Disabled		
エンフォースメント・ポリシー	: Iws-guest ClearPass Admin SSO	Login (SAML SP Service) Enforcer	ment Policy
く サービスに戻る			無効化 コピー 保存 Cancel

"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)

設定 * エンフォースメント * プロファイル * Edit Enforcement Profile - iws-guest ClearPass Admin SSO Login (SAML SP Service) Enforcement Profile エンフォースメント・プロファイル - iws-guest ClearPass Admin SSO Login (SAML SP Service) Enforcement Profile

名前:	Iws-guest ClearPass Guest SSO Login (SAML SP Servic	
說明:		
タイプ:	Application	
アクション:	 許可〇 拒否〇 ドロップ 	
デバイスグループ・ リスト:	Remove View Details Modify	新規デバイスグループの追加

"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。

ClearPass Policy Manager

サポート | ヘルブ | ログアウト admin (Super Administrator)

設定 * エンフォースメント * プロファイル * Edit Enforcement Profile - Iws-guest ClearPass Guest SSO Login (SAML SP Service) Enforcement Profile エンフォースメント・プロファイル - Iws-guest ClearPass Guest SSO Login (SAML SP Service) Enforcement Profile

サマリー プロファイル	- 単独			
属性名		属性值		3
1. SSO-Role	×	 [User Authenticated]	•	2 3
2. Click to add				

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。
```



EDUROAM service

Service template for roaming users to connect to campus networks that are part of the eduroam federation.

((@))	
1.1.4	
N	
200	
<14	~

Encrypted Wireless Access via 802.1X Public PEAP method

Service Template for providing encrypted wireless access to (guest) users via fixed 802.1X PEAP redentials



To authenticate guest users logging in via captive portal. Guests must re-authenticate after their session ends.



Guest Access - Web Login To authenticate guest users logging in via guest portal.

	(9)	(
5	7	1

Guest Authentication with MAC Caching

To authenticate users once using captive portal and later to allow logins using cached MAC Address of the device.

	R.
a	17-

Guest Social Media Authentication

To authenticate guest users logging in via captive portal with their social media accounts. Guests must re-authenticate after their session ends.

۲	6	Э
<(D	>
A	91	

OAuth2 API User Access

Service template for API clients authenticating with username and password (OAuth2 grant type "password")

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。

設定 × ここから開始

Service Templates - Guest Access

General	Wireless Network Se	ettings Posture Settings	Guest Access Restrictions	
Name Prefit	x*: (<u>ins-ssc</u>	o-guest		
Description				
For auth restricte client de	enticating guest users w d based on day of the w vice for AntiVirus, AntiS	vho login via captive portal. (reek or bandwidth limit used ipyware, Firewall status. The	Guests must re-authenticate after by the guest user. Posture checks se results will determine the enfor	their session ends. Network access can be can be enabled, optionally, to validate the reement for the device.
<back 5<="" th="" to=""><th>Start Here</th><th></th><th></th><th>Delete Next > Add Service Cancel</th></back>	Start Here			Delete Next > Add Service Cancel

"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)

General Wireless Network	Settings Posture Settings	Guest Access Restrictions	
Select a wireless controller f	rom the list, or create a new o	one	
Wireless SSID for Guest access*:	two-sec-wifi		
Select Wireless Controller:	(aruba7010 0)		
Wireless Controller Name:	aruba7010		
Controller IP Address:			
Vendor Name:	(Aruba 1)		
RADIUS Shared Secret:			
Enable RADIUS CoA:	0		
RADIUS CoA Port:	3799		

"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。

設定 » ここれ Service	-6開始 Templates - Guest	Access						
General	Wireless Network Setting	s Postu	re Settings	Guest Access	Restrictions			
Enable t	he days on which the gues	t users are	allowed net	work access; en	ter the maxin	num bandw	vidth allowed	per user
Days allowe	d for access*:	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Maximum b	andwidth allowed per user*:	0	MB	(For unlimited ba	ndwidth, set va	alue to 0)		

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。

-1	ビス				을 サ- 오 サ- 오 サ-	ーピスの追加 ーピスのインポート ーピスのエクスポート
7-16	9-:	名前	Added 6 Enforceme Added 1 Enforceme Added 1 Enforceme Added 1 service(s)	ent Profile(s) ent Policies	Clear Filter	表示 10 1 レコード
	-		6 m	6.17		
			41	21/	テンプレート	ステータス
# 1.	0	1	(Policy Manager Admin Network Login Service)	TACACS	テンプレート TACACS+ Enforcement	27-92
# 1. 2.		1 2	(Policy Manager Admin Network Login Service) (AirGroup Authorization Service)	TACACS RADIUS	テンプレート TACACS+ Enforcement RADIUS Enforcement (Generic)
# 1. 2. 3.		1 2 3	Policy Manager Admin Network Login Service] [AirGroup Authorization Service] [Aruba Device Access Service]	TACACS RADIUS TACACS	テンプレート TACACS+ Enforcement RADIUS Enforcement (Generic TACACS+ Enforcement) 0 0 0 0 0
# 1. 2. 3. 4.		1 2 3 4	Policy Manager Admin Network Login Service] [AirGroup Authorization Service] [Aruba Device Access Service] [Guest Operator Logins]	TACACS RADIUS TACACS Application	デンプレート TACACS+ Enforcement RADIUS Enforcement (Generic TACACS+ Enforcement Aruba Application Authentication	27-92) 0
# 1. 2. 3. 4. 5.		1 2 3 4 5	Policy Manager Admin Network Login Service] [AirGroup Authorization Service] [Aruba Device Access Service] [Guest Operator Logins] iws-guest ClearPass Admin SSO Login (SAML SP Service)	TACACS RADIUS TACACS Application Application	TACACS+ Enforcement RADIUS Enforcement (Generic TACACS+ Enforcement Aruba Application Authentication Aruba Application Authorization	27-92 0 0 0 0 0 0 0 0 0

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。

锈証方式:	[\$50] Move Up Move Dow Remove View Detail	新しい認証方式の違か 8
	-Select to Add +	-
勝証ソース:	[Guest User Repository] [Local SQL DB] Move Up Move Dow Remove View Detail Modify	n 新しい認証ソースの追加 s
	-Select to Add E	
ユーザー名除去ルール:	□ ユーザー名プレフィックス/サフィックスを除去するためのコン	マ区切りのルールリストを指定できるようにする

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。

10.05 AL 12.05 ALL 1.00 ALL 1.

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

7077476 Rtt	449-	
テンプレート:	Aruba RADIUSIIV7 x - XXVN \$	
名前:	Quest Role Assignment	
說明:	Assign the Aruba-User-Role after successful authentication	
タイプ:	RADIUS	
アクション:	●許可○ 拒否○ ドロップ	
デバイスグループ・リスト :	Compared to the second	新規デバイスグループの追

"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。

設定。エンフォースメント。プロファイル。Edit Enforcement Profile - Guest Role Assignment エンフォースメント・プロファイル - Guest Role Assignment

サマリー プロファイル	#1					
タイプ		名前		1		9
1. Radius:Aruba	*	Aruba-User-Role (1)		= guest	2	9
2. Click to add						
		[<u>拡</u>]	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。

100 I	ショエンフ	7	ォースメント * ポリシー ースメント・ポリシー		⊕ エンフォースメント ▲ エンフォースメント ▲ エンフォースメント タースメント ・	 ポリシーの追加 ポリシーのインポート ポリシーのアクスポート
2	11.9	-:(88 • (<u>AC</u>)	817	Go Clear Filter	表示 10 1 レコード
E		0	tini a	717		den la
	1.	9	[Admin Network Login Policy]	TACACS	Enforcement policy controlling access to Policy Manager Ac	pmin
	2.	0	[AirGroup Enforcement Policy]	RADIUS	Enforcement policy controlling access for AirGroup devices	
	3.	0	[Aruba Device Access Policy]	TACACS	Enforcement policy controlling access to Aruba device	
	4.	0	(Guest Operator Logins)	Application	Enforcement policy controlling access to Guest application	
	5.	0	Iws-guest ClearPass Admin SSO Login (SAML SP Service) Enforcement Policy	Application		
	6.	0	iws-sso-guest Guest Access Enforcement Policy	RADIUS		
	7.	0	[Sample Allow Access Policy]	RADIUS	Sample policy to allow network access	
	8.	0	[Sample Deny Access Policy]	RADIUS	Sample policy to deny network access	
	8	件中	1-8 を表示		2	ビー エクスポート 刑除

[<u>拡大画像を表示</u>] i

"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。

設定 > エンフォースメント > ボリシー > 編集 - iws-eso-guest Guest Access Enforcement Policy エンフォースメント・ポリシー - iws-sso-guest Guest Access Enforcement Policy



"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。

LA C					
えのすべての条件と一致:					
タイプ	6.0		演算子	9	
1. Date	Day-of-Week	BELONGS_TO		Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday	a 1
2. Click to add					
・ンフォースメント・プロ: プロファイル名:	Pres Autoencesor, Intereo guest Guest M	AC CAXA			
ンフォースメント・プロ) プロファイル名:	Post Authentication (ins-see quest Guest M Post Authentication) (see see quest Guest M Post Authentication) (see see quest Guest De Post Authentication (ins-see quest Guest De	AC Cath Move Up Nove Down Kenove			
: ンフォースメント・70) ブロファイル名:	P > 4/A Post Automatication Instance quest Guest M Post Automatication Voltante Desponse Knee Post Automatication Voltante Desponse Automatication Instance quest Dans De Automatication Instance Automatication De Automatication Automatication De Collector In Addr-	AC CatA n) brie Ros grie Ros 1			

[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。

SP Configuration	SAML	IdP Configuration
entity Provider (IdP) URL:	http://	wserver01.icewall.iccal/fwitdfwito/widp/sso/wsp
hable SSO for		
Guest	0	Enable Guest Web Login and Operator Login access for Guest and Onboard applications
PolicyManager	0	Enabled access to Policy Manager administration
Onboard	0	Enable access to Onboard device provisioning portals
Insight	•	Enable access to Insight application
fentity Provider (IdP) (ertific	ate
elect Certificate:		¢)
ote: IdP certificate must I	be enab	led in Certificate Trust List first, if not listed above.
PPM Service Provider (SP) Me	tadata

[拡大画像を表示]	i
-----------	---

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ヘリ 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。

fox ファイル 編集 表示 蔵屋 プックマーク ツール ウインドウ ヘルプ	0 9 6 9 0	 100% 858	2月25日(
●			80
🛞 Inserver01 icenalUccal/hv/d/w/c/w/dp/sso/hssp31SAMLRequest-r/MLTsMixEPyWyPc8m6SJ1sQqolpKRUR 🖤 🦿	9、秋泉	\$ 0 +	* ≡
よく見るページ = □ Firefox を使いこな Q ClearPlans Policy □ koethatアモ・トッ			
IceWall SSO			
	_		
IceWall SSO			
- Login -			
ユーザーIDとパスワードを入力して「送信」ボタンを押してくだ	av.		
- 1-7-ID astin			
.729-8			
「通信」総合のと			
パスワードを言れた方はこちら			
Hewlett-Packard Japan, Ltd.			

・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。



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