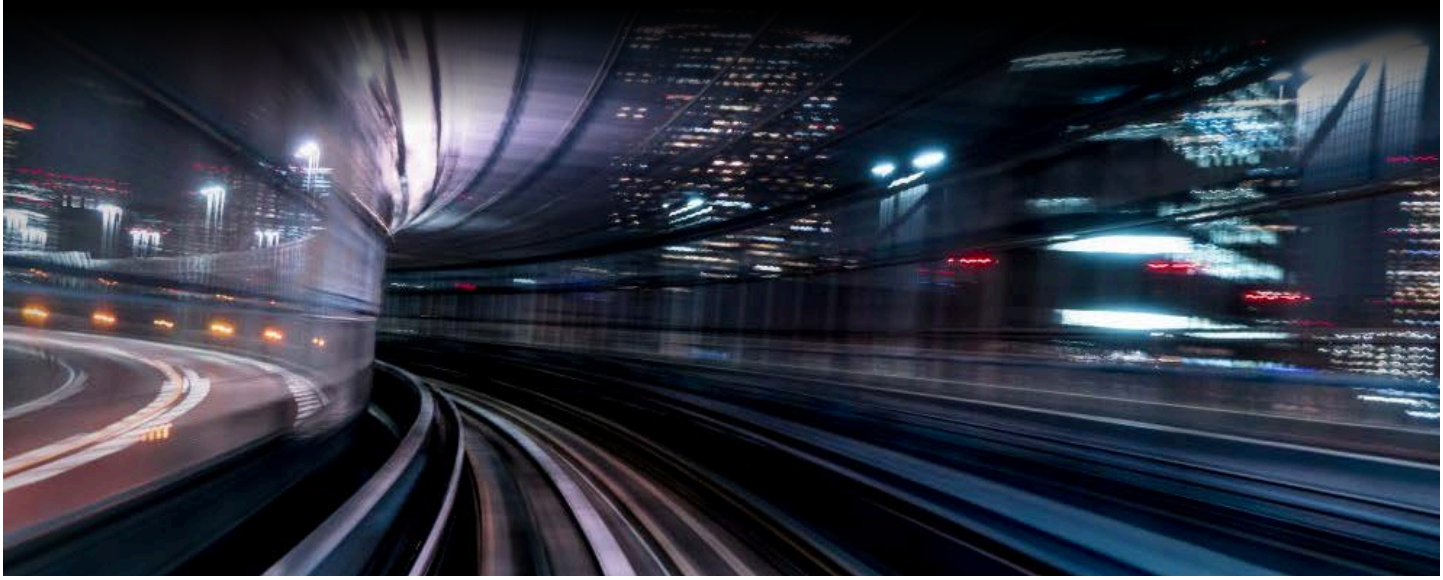
オリジナルURL対応機能特集5：オリジナルPATH方式

IceWall技術レポート



1. はじめに

IceWall技術レポート「ここが知りたい！8.0 の新機能特集（1）- オリジナルURL対応機能特集1： 基本編」において、リバースプロキシサーバーでのURL変換を不要とするソリューションである「オリジナルURL方式」についてご説明しました。
本技術レポートでは、その応用編として、さらに別のニーズに対応が可能な「オリジナルPATH方式」について、その特長や設定方法をご紹介します。

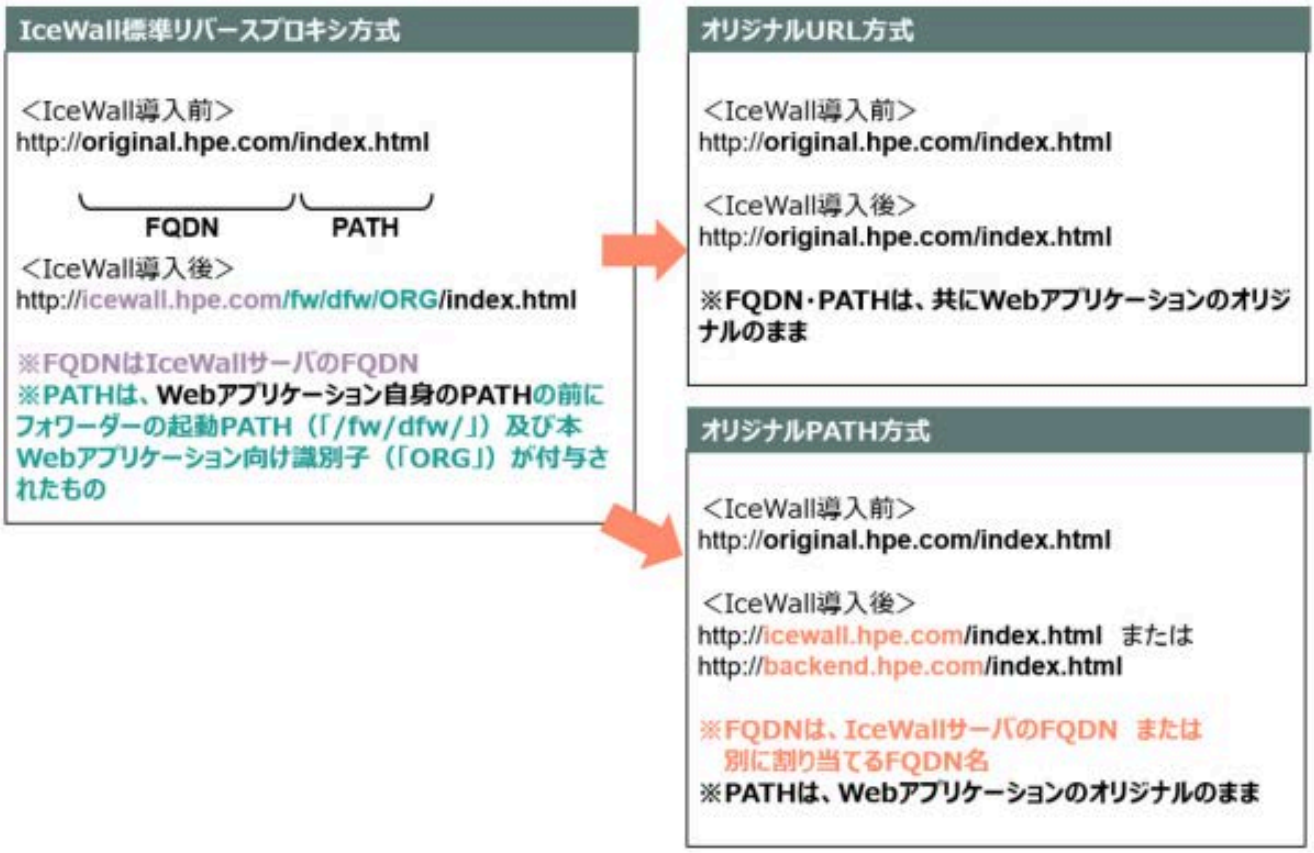
---

2. オリジナルPATH方式とは

以前にご説明しました「オリジナルURL方式」は、Webアプリケーションのオリジナルのアクセスそのままでリバースプロキシ経由のアクセスができるようにすることで、従来のリバースプロキシ接続時に課題となるケースがあったコンテンツ内のURLの変換処理を不要とする方式でした。

それに対して、「オリジナルPATH方式」は、Webアプリケーションのオリジナルのアクセスの内、PATH部分についてはWebアプリケーションのオリジナルのPATHそのままを使用し、アクセスURLのFQDN部分にはIceWallサーバーのFQDNまたは別のFQDNを割り当てる方式です。

「オリジナルURL方式」と「オリジナルPATH方式」のイメージは次の通りです。



オリジナルPATH方式は、オリジナルURL方式と違って、アクセスURLのFQDN部分は、Webアプリケーションのオリジナルとは異なりますので、Webアプリケーションのコンテンツ内にオリジナルのFQDNが含まれている場合には、IceWallサーバーにてFQDNを変換した上でクライアントに引き渡す必要がある点は注意点になります。(Java AppletやActiveX等のバイナリモジュール内にオリジナルのFQDNを含むURLが組み込まれている場合には、IceWallサーバーにて変換ができないため、オリジナルPATH方式は使用できません。オリジナルURL方式の利用をご検討ください。)

オリジナルPATH方式で複数のWebアプリケーションを接続する際の留意点

オリジナルPATH方式でFQDN部分にIceWallサーバーのFQDNを使用する場合、複数のWebアプリケーションをオリジナルPATH方式で接続するためには、次の例のように、(1)アプリケーション自身のPATHによってアプリケーションの区別ができる、(2)アプリケーションの区別のため、FQDNにポート番号を割り当てることができる、のいずれかの条件/対応が必要となります。

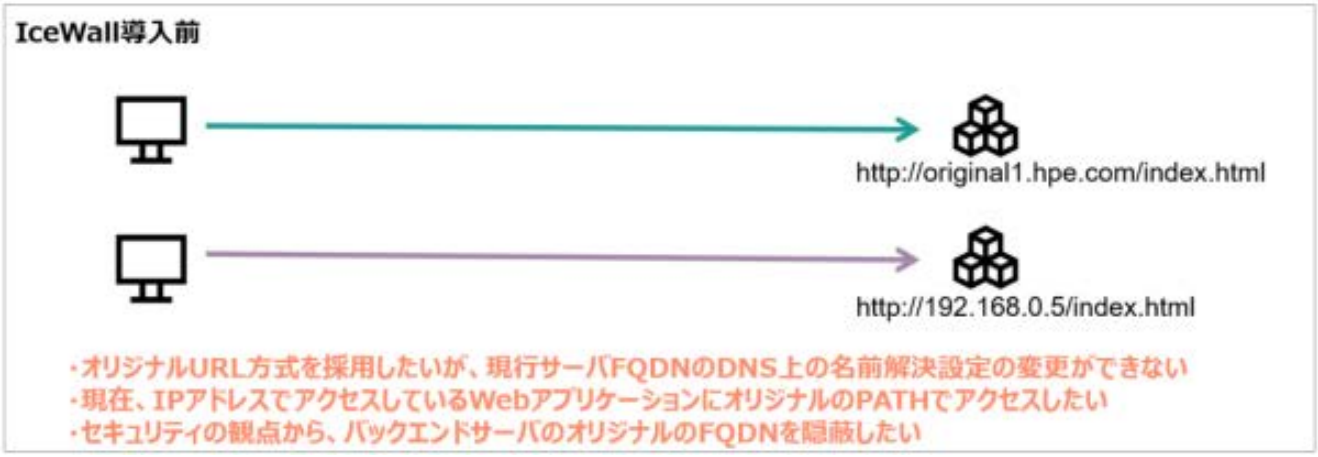
なお、オリジナルPATH方式でFQDN部分に別のFQDN名を割り当てる場合には、次の例のように、複数のWebアプリケーションのぞれぞれに別のFQDN名を割り当てることでアプリケーションの区別が可能となります。

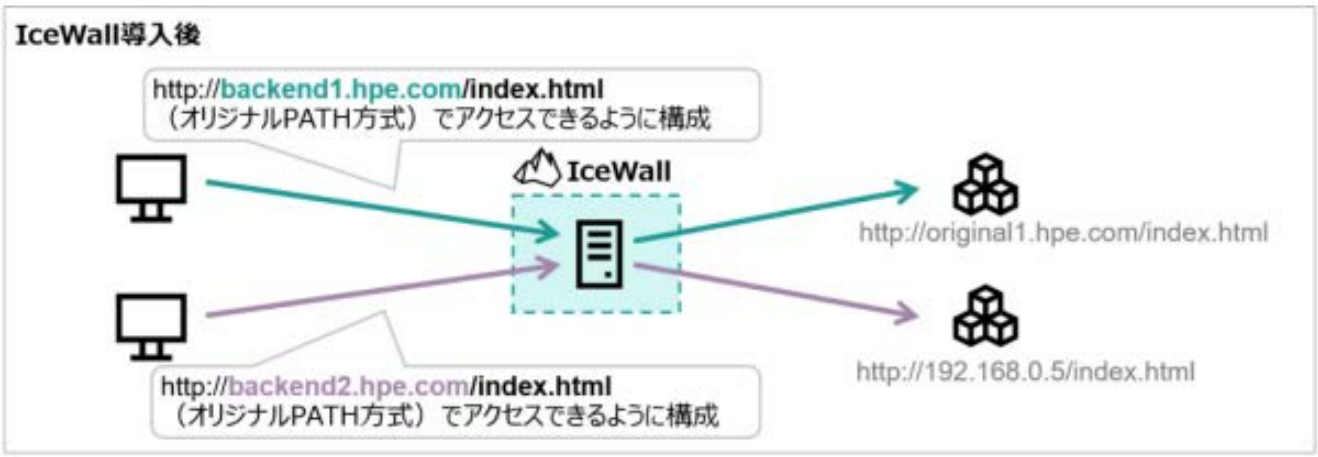
---

3. オリジナルPATH方式が有用なケース

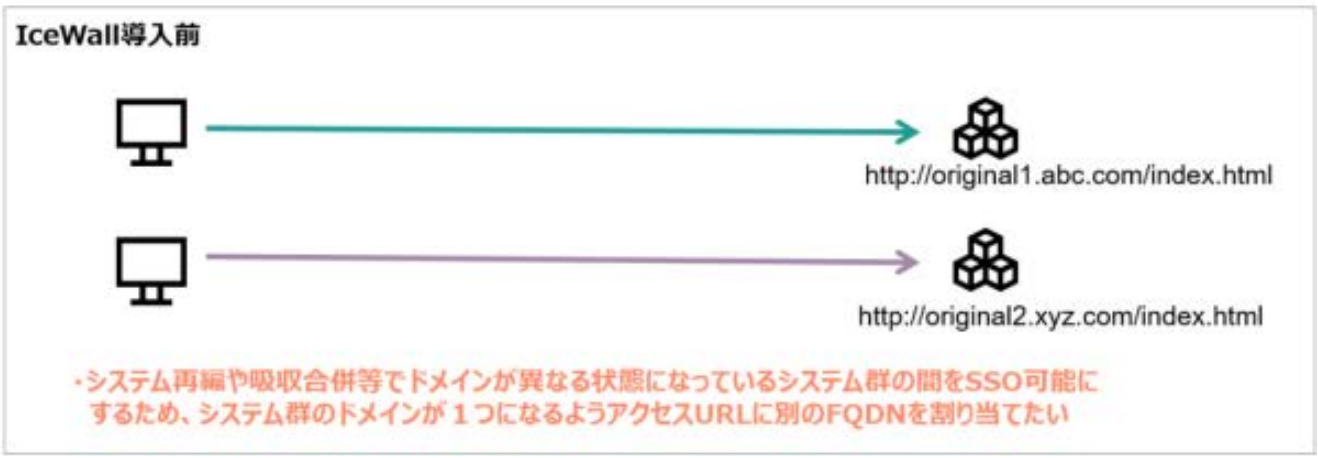
「オリジナルPATH方式」が有用なケースとしては次のような場合が挙げられます。

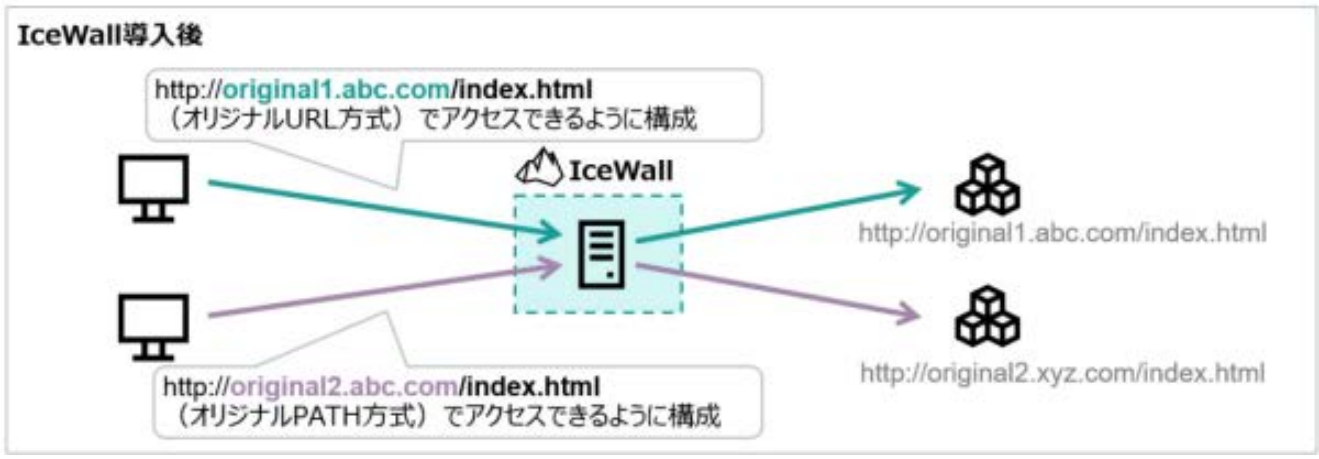
- ケース１（システムや環境上の制約への対応）



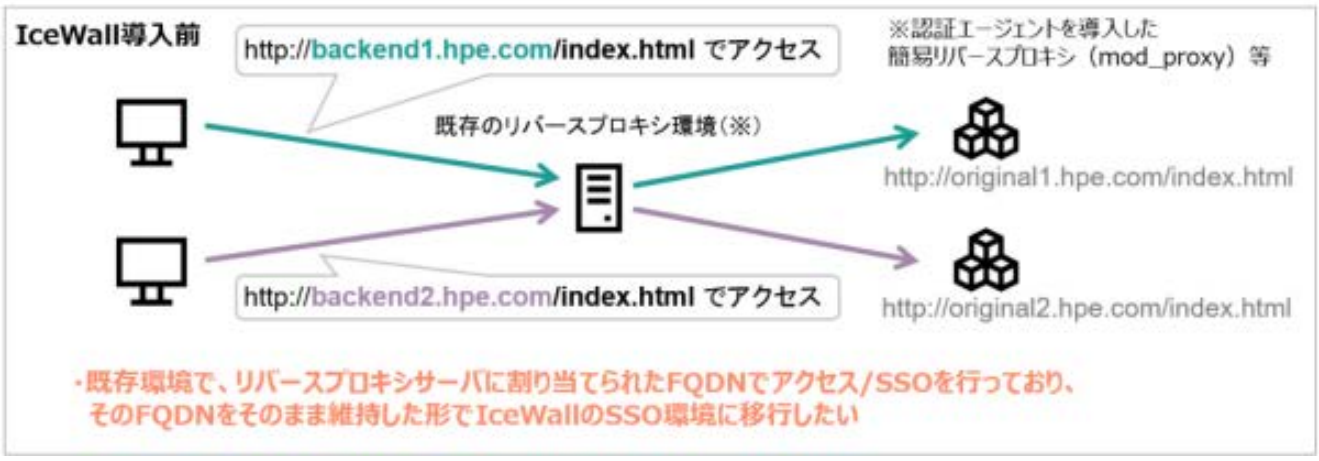


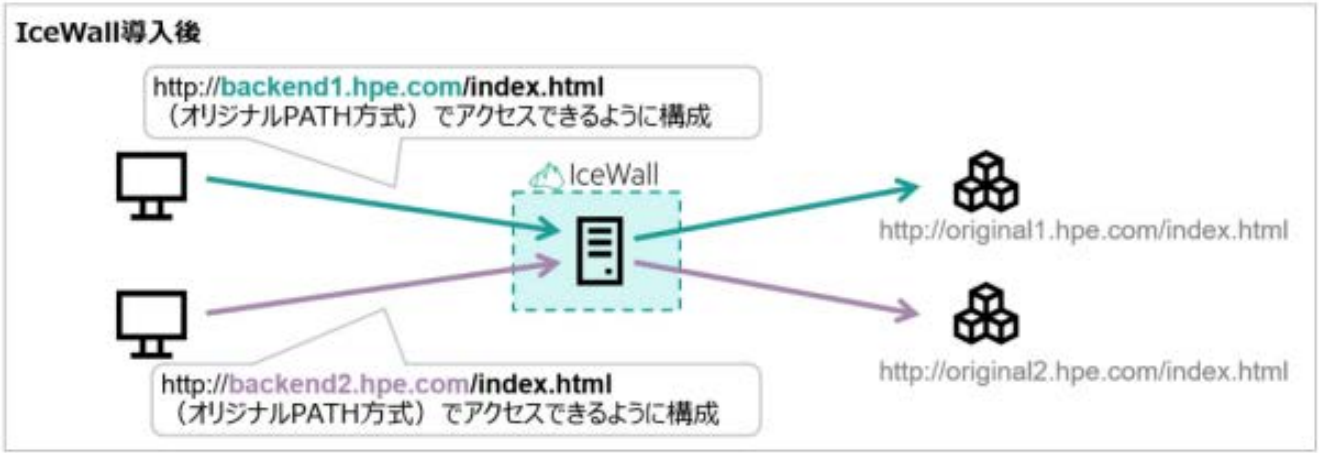
- ケース２（システム再編等によるアクセスURLのFQDNドメインの統合）





- ケース 3 （移行前環境との互換性維持）

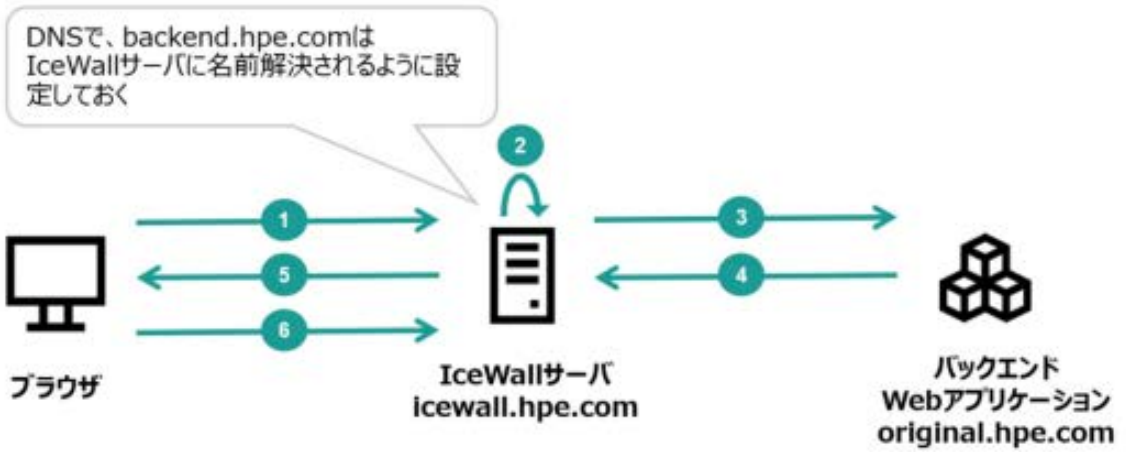




---

4. 処理の流れ

オリジナルPATH方式（FQDN部分に別のFQDN名を割り当て）の例で、オリジナルPATH方式の処理の流れをご説明します。



① ブラウザは、http://backend.hpe.com/index.htmlにアクセスします。この際、DNSにより、backend.hpe.comはIceWallサーバー（icewall.hpe.com）のIPアドレスに名前解決されるため、IceWallサーバーにアクセスします。

② IceWallサーバーのApache HTTP Serverは、環境変数（例：IW_PATH）に/fw/dfw/ORG をセットし、フォワーダーモジュールにアクセスを引渡します。

③ IceWallサーバーのフォワーダーモジュールは、環境変数よりアクセス先となるバックエンドサーバーを認識し、バックエンドWebアプリケーションの/index.htmlにアクセスします。

④ バックエンドWebアプリケーションは、コンテンツを返送します。

⑤ IceWallサーバーのフォワーダーモジュールは、コンテンツをブラウザに返送します。その際、コンテンツ内に絶対パスのURLとしてhttp://original.hpe.comが含まれていた場合、http://backend.hpe.comにキーワード変換した上で返送します。（※1）

⑥ ブラウザは、その後もhttp://backend.hpe.com配下のアクセスURLでアクセスを続けます。（※2）

※1：

・コンテンツがLocationヘッダーによる30xリダイレクトであり、かつアプリケーションの実装によりContent-Typeが未設定であった場合、フォワーダーはキーワード変換を行わない（※IceWall SSO 10.0までの制限となります。IceWall SSO 11.0では、本制限はありません。）ため、そのままではIceWallの標準アクセスURLにリダイレクトしようとしてしまい、オリジナルPATHのURLにリダイレクトされません。その場合には、Apache　HTTP Serverにおいて、オリジナルPATHのURLにリダイレクトさせる処理の追加が必要になります。　（設定例は後述）

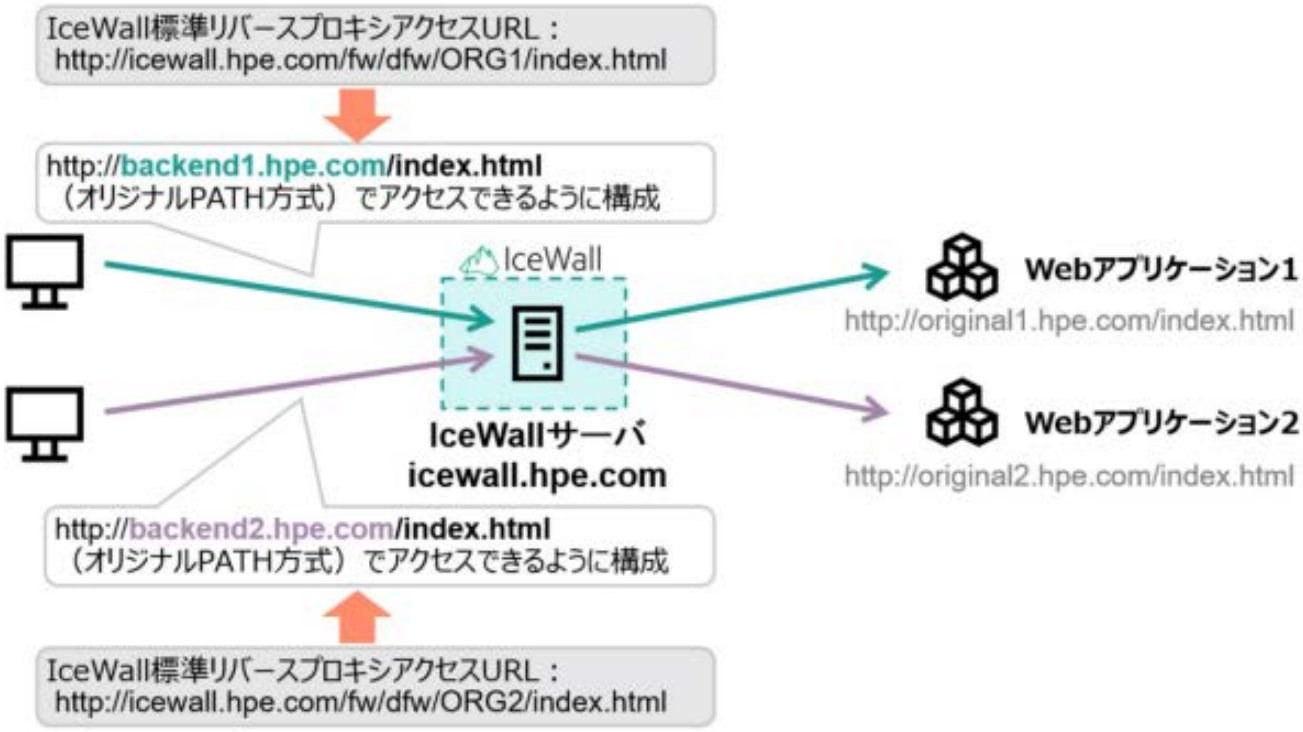
・Java AppletやActiveX等のバイナリモジュール内にオリジナルのFQDNを含むURLが組み込まれている場合には、キーワード変換ができないため、オリジナルPATH方式は使用できません。オリジナルURL方式の利用をご検討ください。

※2：

・リクエストのRefererヘッダーにhttp://backend.hpe.comのURLが入っている場合、バックエンドサーバーまでそのURLが通知されてしまうため、Apache　HTTP Serverにおいて、Refererヘッダーを変換した上でバックエンドサーバーにアクセスするようにします。（設定例は後述）

5. 設定例

本節では、実際の設定方法について、以下の具体例を使用してご説明します。



オリジナルPATH方式の設定は、以下の3つの手順により構成されます。

1) クライアントの名前解決設定

2) Apache HTTP Serverの設定

3) IceWall SSOの設定

1）クライアントの名前解決設定

オリジナルPATH方式でアクセスFQDNとして別に割り当てるFQDN名は、DNSでIceWallサーバーに名前解決されるように設定します。（オリジナルPATH方式のFQDN部分にIceWallサーバーのFQDNを使用する場合には、DNSへの追加設定は必要ありません。）

DNSへの設定例

icewall.hpe.com	IN	A	192.168.0.1
backend1.hpe.com	IN	CNAME	icewall.hpe.com
backend2.hpe.com	IN	CNAME	icewall.hpe.com

2）Apache HTTP Serverの設定

IceWallサーバーのApache HTTP Serverの設定ファイル（httpd.conf）のフォワーダーの設定の前に以下の設定を追加します。

httpd.conf　設定例

```
LoadModule rewrite_module /usr/lib64/httpd/modules/mod_rewrite.so

RewriteEngine on

RewriteCond %{HTTP_HOST} ^backend1\.hpe\.com
RewriteCond %{REQUEST_URI} !^/fw/dfw.*
RewriteCond %{REQUEST_URI} !^/img/.*
RewriteRule ^/(.*) /fw/dfw/ORG1/$1 [E=IW_PATH:/fw/dfw/ORG1,PT,NS,L]　・・・①

RewriteCond %{HTTP_HOST} ^backend1\.hpe\.com
RewriteCond %{REQUEST_URI} ^/fw/dfw/ORG1/.*
RewriteRule ^/fw/dfw/ORG1/(.*) /$1 [R=302,NE,L]　・・・②
SetEnvIf Referer http://backend1.hpe.com/(.*)$ backend1=$1　・・・③
RequestHeader set Referer http://original1.hpe.com/%{backend1}e
env=backend1　・・・④

RewriteCond %{HTTP_HOST} ^backend2\.hpe\.com　・・・⑤
RewriteCond %{REQUEST_URI} !^/fw/dfw.*
RewriteCond %{REQUEST_URI} !^/img/.*
RewriteRule ^/(.*) /fw/dfw/ORG2/$1 [E=IW_PATH:/fw/dfw/ORG2,PT,NS,L]

RewriteCond %{HTTP_HOST} ^backend2\.hpe\.com
RewriteCond %{REQUEST_URI} ^/fw/dfw/ORG2/.*
RewriteRule ^/fw/dfw/ORG2/(.*) /$1 [R=302,NE,L]
SetEnvIf Referer http://backend2.hpe.com/(.*)$ backend2=$1
RequestHeader set Referer http://original2.hpe.com/%{backend2}e env=backend2
```

（説明）

① アクセスURLがフォワーダー経由のURL、IceWallの画像ディレクトリ、以外の場合、フォワーダー経由のURLに変換し、環境変数IW_PATHに/fw/dfw/ORG1をセットします。

② リクエストがIceWallの標準アクセスURLで送られてきた場合（＝Locationヘッダーによるリダイレクト時）は、改めてオリジナルPATHへリダイレクトします。

③ RefererヘッダーのURLがオリジナルPATH方式のURLの場合、環境変数backend1にアクセスURLのPATH情報をセットします。該当しない場合backend1は値なしとなります。

④ backend1にPATH情報がある場合、RefererヘッダーのURLをoriginal1.hpe.comのFQDNのURLに変換します。

⑤ backend1の設定と同様の形で、以降backend2の設定も追加します。

3）IceWall SSOの設定

- フォワーダー設定ファイル（dfw.conf)

以下に従い設定します。

設定値	説明
REQUEST_URI=1	パス情報をREQUEST_URIから取得する設定
VIRTUALPATH_ENV=IW_PATH	フォワーダー経由のパス情報を格納する環境変数名を設定（httpd.confのRewriteRuleで使用した変数名と合わせる）
COOKIEATTR=domain=hpe.com; path=/	フォワーダーが付与するCOOKIE情報（この例ではdomain属性とpath属性）を設定
HOST=ORG1=original1.hpe.com:80 HOST=ORG2=original2.hpe.com:80 SVRFILE=ORG1,./sample.conf SVRFILE=ORG2,./sample.conf	オリジナルPATH方式の対象となるバックエンドシステムを設定（この例ではエイリアス名はORG1,ORG2）
REPKEY=Location: http://original1.hpe.com/fw/dfw/ORG1,Location: http://original1.hpe.com REPKEY=Location: http://original2.hpe.com/fw/dfw/ORG2,Location: http://original2.hpe.com	ログイン直後のリダイレクト時など、フォワーダー自身が出すLocationヘッダーを変換

- ホスト設定ファイル（sample.conf)

以下に従い設定します。

設定値	説明
#URLKEY=A,HREF #URLKEY=BASE,HREF （省略） #URLKEY=INPUT,SRC #URLKEY=LINK,HREF	URL変換が行われないようにするためにコメントアウトします
REPKEY=original1.hpe.com,backend1.hpe.com	バックエンドサーバーから送られてきたコンテンツに含まれるオリジナルのFQDNはアクセスURLに割り当てるFQDNにキーワード変換します
UNCONV_HEADER=SET-COOKIE	バックエンドサーバーから送られてきたset-cookieのパスはURL変換の必要がないため、本項目を設定します。 ※なお、バックエンドサーバーからの30xリダイレクト時のLocationヘッダーのURLはバックエンドサーバー自身のFQDNであるため、アクセスURLに割り当てるFQDNに変換する必要があることから、本項目には「LOCATION」は設定しません。（Locationヘッダーは一旦IceWallの標準アクセスURLに変換して送られ、リダイレクトアクセス時にApache HTTP Serverによってオリジナルパスのパスに再リダイレクトされます。）

6. まとめ

本技術レポートでは、「オリジナルURL方式」の応用編として、さらに多様なニーズ・環境に対しても、リバースプロキシ型SSOの適用を可能にする「オリジナルPATH方式」をご紹介しました。

バックエンドシステムのシングルサインオン対応の１つのパターンとして、本実装方法を是非ご検討ください。

2018/2/13 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)