IceWall技術レポート:

VDIをワンタイムパスワードで認証強化
– Citrix XenApp/XenDesktop

1. はじめに　～働き方改革とテレワーク～

安全なリモートアクセスを実現する手段として、VDI（Virtual Desktop Infrastructure : 仮想デスクトップ）」が使われるケースが多くあります。
本技術レポートでは、代表的なVDI製品である「Citrix XenApp /XenDesktop」と、ワンタイムパスワード製品「OneTime認証連携ツール for IceWall VDIオプション」の連携検証によって、「VDI」の認証セキュリティを効果的に強化する方法を紹介します。

2. 安全なテレワークを実現するテクノロジー　～VDI（仮想デスクトップ）～

社外からのリモートアクセスにつきまとうセキュリティの課題を、一気に解決できるテクノロジーとして注目を集めているのがVDI（仮想デスクトップ）です。VDIは、画面転送技術を使って社外の端末から社内のデスクトップ環境を遠隔操作する仕組みで、重要情報などの情報資産を端末にダウンロードする必要がない（ダウンロードを禁止できる）ので、端末の紛失・盗難時にも情報資産そのものが紛失・盗難されることはありません。この利点が評価され、VDIは社員の全面的なテレワークの手段として加速度的に導入が進んでいます。

一方で、外部インターネット経由でVDIを利用する場合、パスワードだけによる認証だけでは十分に強固だとは言えず、実際様々な多要素認証（MFA: Multi Factor Authentication）の仕組みがVDIの認証として使われています。

3. VDI（仮想デスクトップ）での多要素認証

VDIで使われる多要素認証には、ICカードや生体認証など、様々な種類があります。そのような多種類の多要素認証の中で、VDIの利点である「Any Device：あらゆるデバイスで利用できること」と強固な認証を両立し、かつコスト的にも低く抑えられる理想的な方法と言えるのが、今回紹介する「ソフトウェアベースのワンタイムパスワード」です。

多種多様な多要素認証の中で、IceWall SSOで提供されるワンタイムパスワードの優位性は、下記の技術レポートに詳しく書かれています。
» IceWall SSO ワンタイムパスワード(OTP)ソリューション

上記技術レポートの内容を要約しますと、次の通りになります。
「なりすましに対する認証強度が極めて高く、十分なユーザーの利便性を持つ」と言う旧来型のワンタイムパスワードの利点をそのまま維持しながら、旧来型ワンタイムパスワードの唯一の欠点であった「導入コスト」を低くなるように抑えたのが、「OneTime認証連携ツール for IceWall」です。

「OneTime認証連携ツール for IceWall」は、ワンタイムパスワードの標準規格であるOATHに準拠しているため、トークンとして各種ハードウェアの他にソフトウェアトークン（無償で提供されることも多い）が利用でき、導入コストを低く抑えることができます。また、ユーザー数に依存しないライセンス体系のため、特にユーザー数の多い大規模な利用においてコスト面で有利になります。まさに、VDIを使ったテレワークを広い範囲の社員に使わせるにあたって、理想的な認証強化方法と言えるでしょう。

4. OneTime認証連携ツール for IceWall VDIオプションについて

「OneTime認証連携ツール for IceWall 」は、本来 はIceWall SSOへの認証を強化するためのワンタイムパスワード製品です。それが「VDIオプション」によって、Citrix XenApp/XenDesktop などのVDI製品の認証強化も行うことができるようになりました。「VDIオプション」は、RADIUSプロトコルを使って、VDI製品との通信を行います。
OneTime認証連携ツール for IceWallに関する詳細は、開発元である株式会社エスシーシーの下記Webサイトをご覧ください。
» エスシーシー：OneTime認証連携ツール for IceWall（PDF）

5. Citrix XenApp/XenDesktop とは

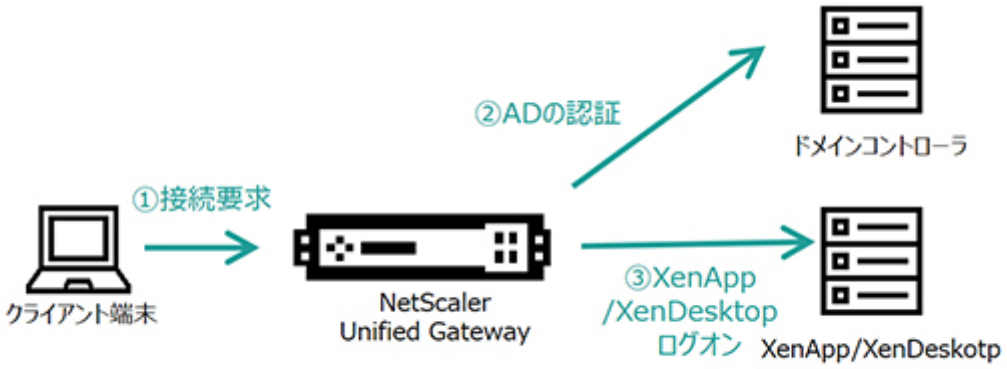
Citrix XenApp/XenDesktop は、Citrix社が提供するVDI（仮想デスクトップ）及びアプリケーション仮想化製品です。 Windowsデスクトップやアプリケーションを、集中かつ効率的に管理しながら、エンドユーザーがセキュアかつ柔軟に利用できるように 、デスクトップやアプリケーションの画面をネットワーク経由で配信します。
Citrix XenApp/XenDesktopの大きな特徴のひとつが、外部インターネット経由の通信を保護する、Citrix NetScaler Unified Gatewayです。Citrix NetScaler Unified Gatewayは、XenApp/XenDesktopと組合わせて利用する場合は、SSLリバースプロキシとして動作し、画面転送の通信をSSLで暗号化します。
Citrix XenApp/XenDesktop およびCitrix NetScaler Gatewayに関する詳しい情報は、下記のCitrix 社のサイトをご覧ください。

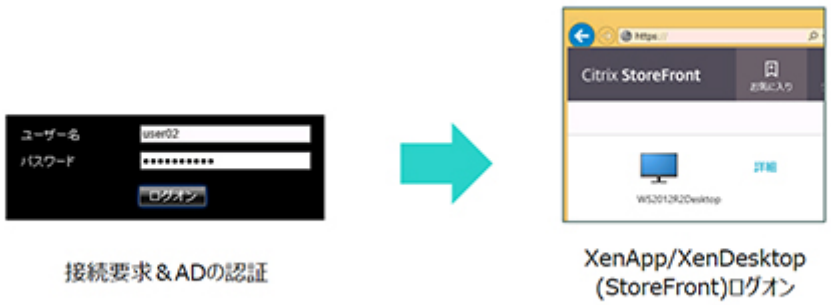
» Citrix XenApp/XenDesktop

» Citrix NetScaler Unified Gateway

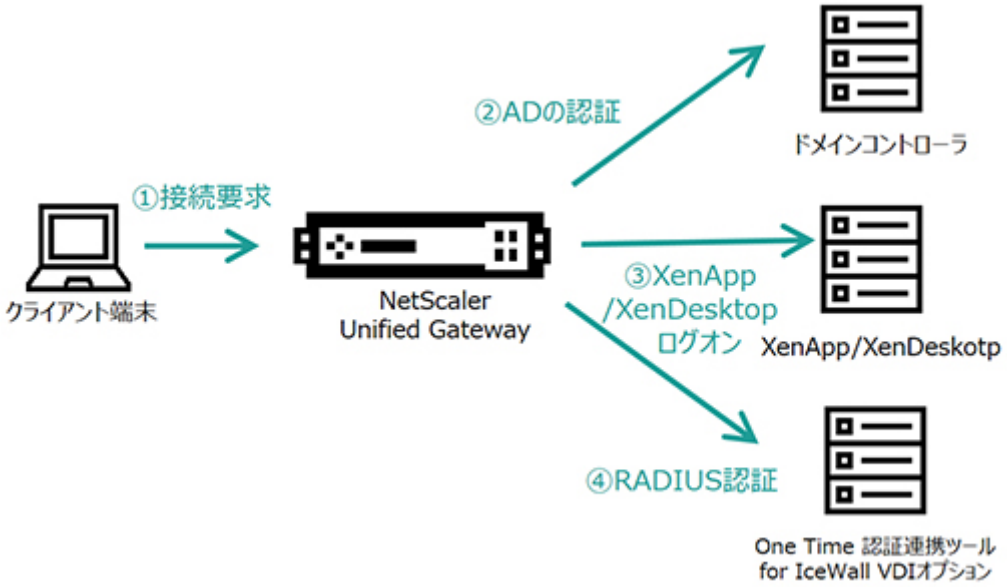
6. Citrix XenApp/XenDesktop ＋ OneTime認証連携ツール for IceWall VDIオプションの認証連携概略

通常の（多要素認証無しの）Citrix XenApp/XenDesktop では、クライアント端末からの接続要求をNetScaler Unified Gatewayが一旦受け、利用者が入力したユーザー名とパスワードをドメインコントローラに照会した上で、その認証が通れば、そのままXenApp/XenDesktopへのログオンも通るようになっています。利用者の見た目では、NetScaler Unified Gatewayにログオンすると、そのままXenApp/XenDesktop (StoreFront) までログオンが通ったように見えます。





NetScaler Unified Gateway の機能として3rd Partyの多要素認証を付加することが可能です。その場合は、NetScaler Unified Gatewayがドメインコントローラへの認証と、RADIUSサーバーに対するRADIUSプロトコルを使った認証の2つの認証を行います。OneTime認証連携ツール for IceWall VDIオプションは、RADIUSサーバーとして動作し、NetScaler Unified Gatewayからの認証要求を受ける形となります。 利用者の見た目として、NetScaler Unified Gatewayのログオン時に、「第2パスワード」を求められ、そこにワンタイムパスワードを入力する必要がありますが、それ以外の動作フローはドメイン認証だけの場合と変わりありません。



7. 連携設定と接続検証

下記の1) ～ 3) の流れで、設定と動作確認を行います。
1) 前提条件の確認
2) NetScaler Unified Gatewayの設定
3) Citrix Receiver for Webでの動作確認

以下、設定の詳細について説明します。

1) 前提条件

まず、XenApp/XenDesktop およびNetScaler Unified Gateway の各コンポーネントについては、利用者がユーザー名とドメインのパスワードを使ってNetScaler Unified Gatewayログオンし、Gateway経由で仮想デスクトップにアクセスできるように、正しく構成されていることを前提とします。

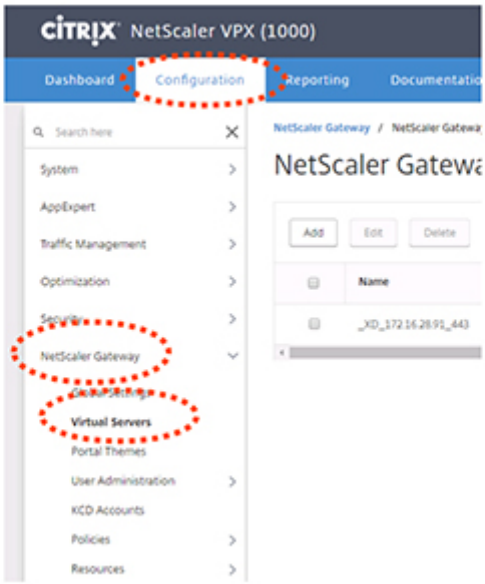
また、OneTime認証連携ツール for IceWall およびそのVDIオプションについても正しく構成され、アクティベー

トされたトークンで正しいOne Time Passwordが表示されることが検証されていることを前提とします。

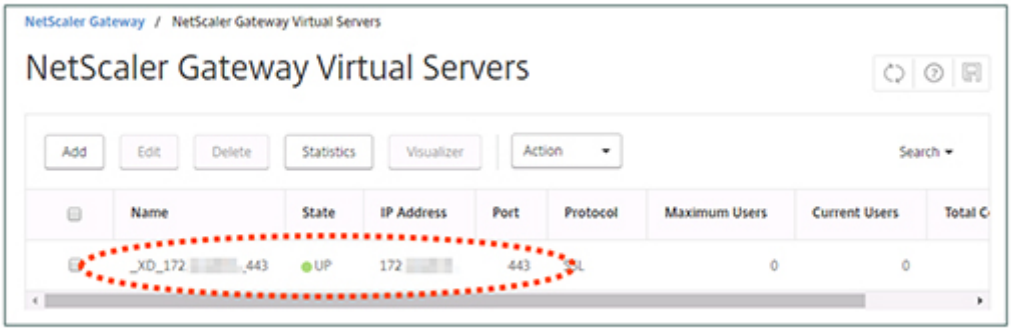
2）NetScaler Unified Gateway設定

「NetScaler Web管理コンソール」に、管理者アカウントでログオンします。

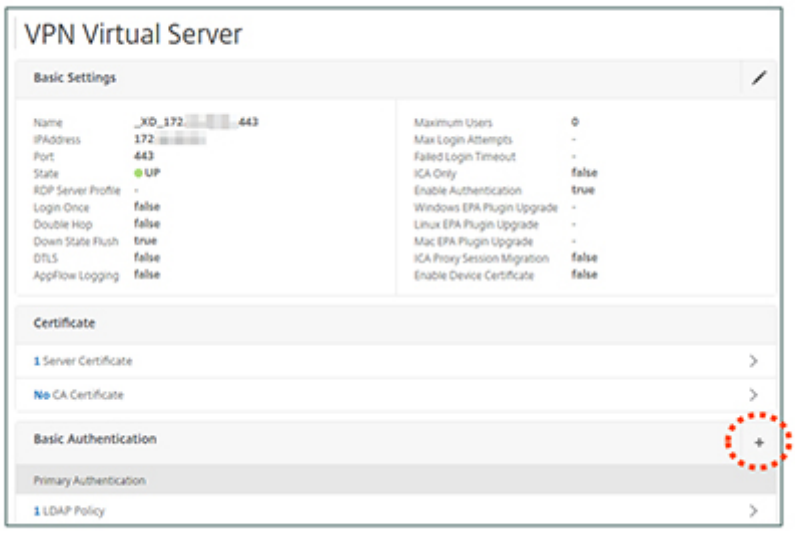
コンソール画面上部の「Configuration」タブをクリックし、左側ナビゲーションペインの「NetScaler Gateway」と、さらに「Virtual Servers」をクリックします。



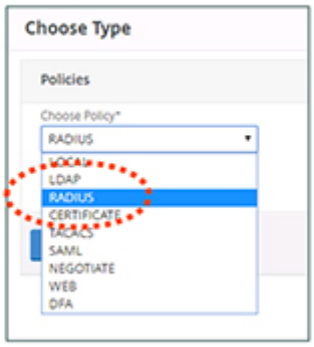
右側ペインで表示される、Gateway Virtual Serverのエントリをクリックします。



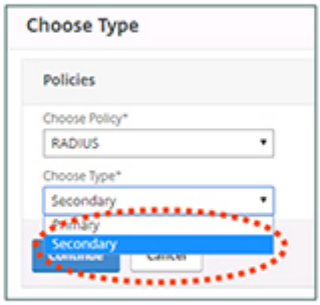
VPN Virtual Serverのページが開きますので、その中の「Basic Authentication」の右にある「＋」ボタンをクリックします。



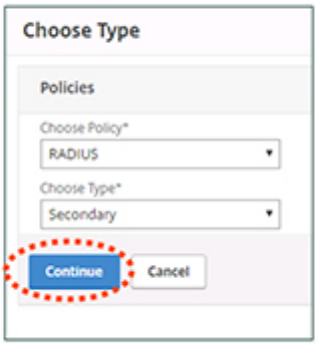
「Choose Type」の画面に遷移しますので、「Choose Policy」のプルダウンから「RADIUS」を選択します。



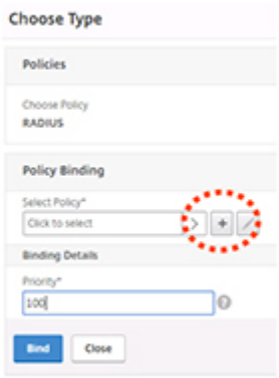
続いて、「Choose Type」から「Secondary」を選択します。



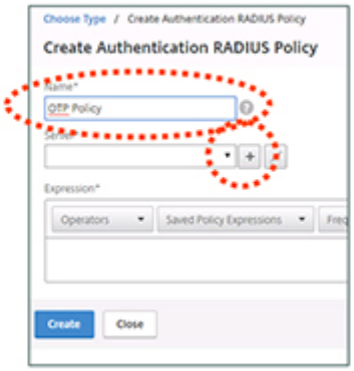
「RADIUS」および「Secondary」が選択されていることを確認して、「Continue」ボタンをクリックします。



「Choose Type」ページ内の「Policy Binding」の下にある「Select Policy」の右側の「＋」ボタンをクリックします。



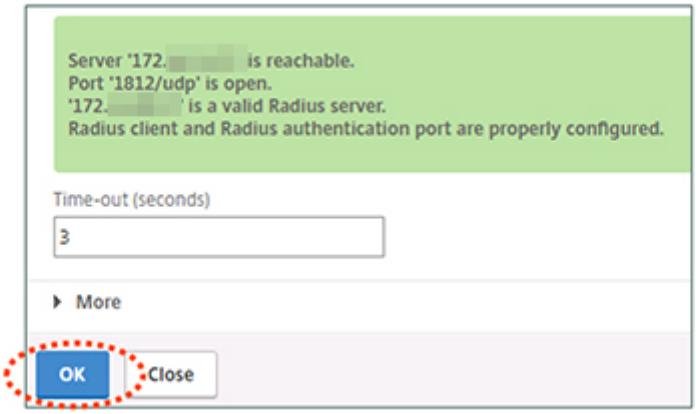
「Create Authentication RADIUS Policy」画面が現れますので、「Name」欄に、One Time Password認証を識別できる分かりやすい名前を命名し、入力します。 続いて、「Server」欄の右側にある「＋」ボタンをクリックします。



「Create Authentication RADIUS Server」画面が現れますので、次のように入力してください。

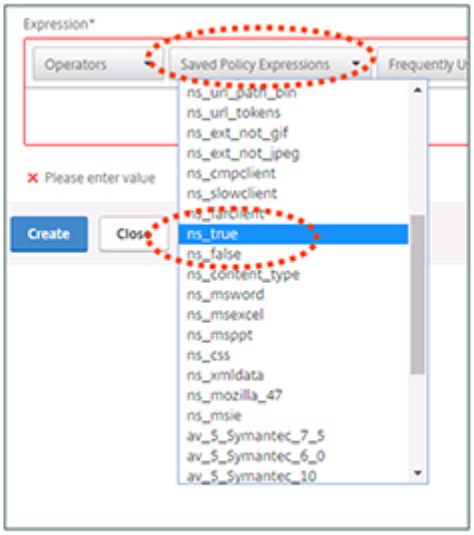
- Name:RADIUSサーバー（VDIオプションサーバー）を識別する分かりやすい名前を命名し、入力します。
- 「Server IP」をチェックします。
- IP Address：RADIUSサーバー（VDIオプションのサーバー）のIPアドレスを入力します。
- Port：デフォルトのまま（1812）にします。
- Secret Key: OneTime認証連携ツール for IceWall で設定した秘密鍵を入力します。
  さらに上記の入力が完了したら、「Test Connection」ボタンをクリックします。

「Test Conection」で、RADIUSサーバーとの通信がうまく行われた場合、下記のように「RADIUS client and RADIUS authentication port are properly configured.」と表示されます。その表示を確認後、「OK」ボタンをクリックします。
このメッセージが出ない場合は、再度上の設定を確認してください。

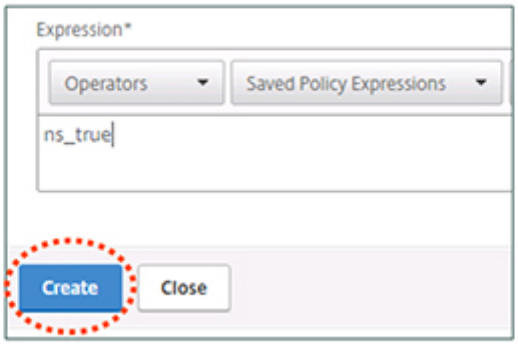


再び「Create Authentication RADIUS Policy」画面に戻ります。「Name」および「Server」欄に、上で命名した名前が表示されていることが確認できます。

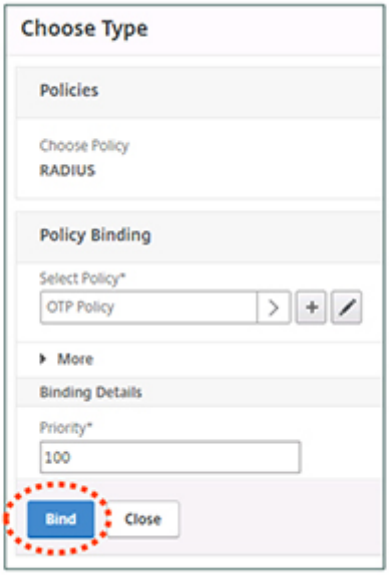
続いて、「Saved Policy Expressions」をクリックし、プルダウンから「ns_true」を選択します。



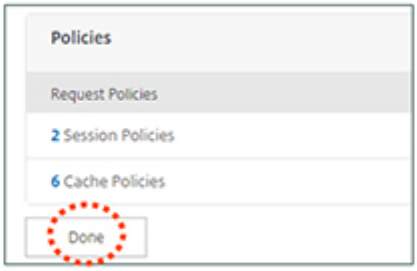
「Expression」の中に、「ns_true」と表示されていることを確認し、「Create」ボタンをクリックします。



「Choose Type」画面に戻りますので、「Bind」ボタンをクリックします。

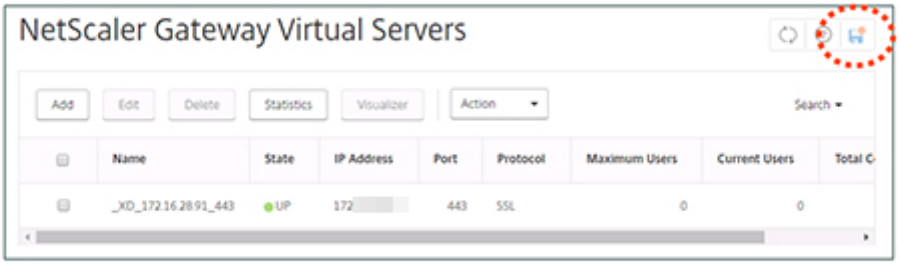


「VPN Virtual Server」画面に戻りますので、画面の最下部にある「Done」ボタンをクリックします。



「NetScaler Gateway Virtual Servers」画面に戻りますので、画面右側のフロッピーディスクアイコンのボタンをクリックして、設定を保存します。

これでNetScaler Unified Gatewayの設定は終了です。



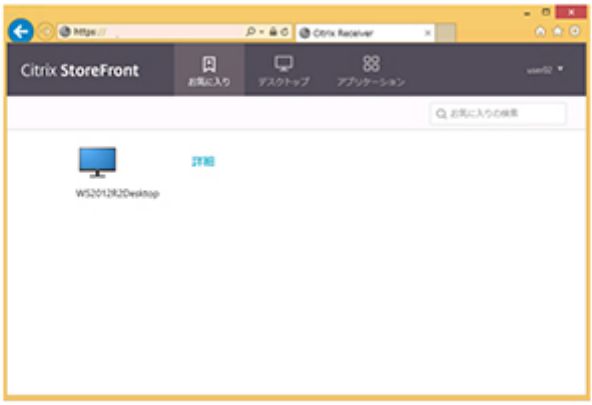
3) Citrix Receiver for Webでの動作確認

クライアント端末のWebブラウザから、NetScaler Unified GatewayのログオンURL（前提条件で動作確認したログオンURLと同じURL）にアクセスします。

従来通りのドメインのユーザー名とパスワードに加えて、「第2パスワード」の入力欄が追加されていますので、ここにトークンに表示されたワンタイムパスワードを入力し、ログオンします。

ワンタイムパスワードと、ドメインのパスワード、2つの認証を行うことで、仮想デスクトップにアクセスすることが

できるようになりました。つまり、仮想デスクトップの利用に、多要素認証が必要になったと言うことになります。



8. まとめ

上記の「連携設定と接続検証」で示した通り、NetScaler Unified Gatewayの簡単な設定のみで、Citrix XenApp/XenDesktopとOneTime認証連携ツール for IceWall VDIオプションを連携できることが確認できました。

この連携によって、仮想デスクトップ利用時の認証にワンタイムパスワードを付加した多要素認証を義務付け、認証をより強固にすることが可能です。
OneTime認証連携ツール for IceWall VDIオプション を使った仮想デスクトップの多要素認証化は、「Any Device（どんな端末からでも同じように使える）」と言う仮想デスクトップの利点を活かしながら、認証の強化を比較的低い導入コストで実現できます。

本ソリューションに関するお問い合わせ

2017/4/21　新規掲載

執筆者　　シトリックス・システムズ・ジャパン株式会社
セールスエンジニアリング本部 ネットワークSE部 大崎 克也

シトリックス・システムズ・ジャパン株式会社
セールスエンジニアリング本部 製造・流通SE部 岡部 俊城

日本ヒューレット・パッカード　テクノロジーコンサルティング事業統括 IceWallソフトウェア本部
シニアプロダクトマネージャー　山田 晃嗣

本技術レポートの内容に関するお問い合わせは[こちら]