
オンプレミスの Notes/Domino と IBM Verse(SaaS)のハイブリッド環境構築のポイント

オンプレミスの Notes/Domino と IBM Verse(SaaS)のハイブリッド環境を CAMSS センターに構築しました。

ハイブリッド環境では、既存の Notes/Domino の業務アプリケーションはそのまま、1人あたりクラウド上の 50GB のメールボックスが利用でき、いつでもどこでも様々なデバイスでメールをご利用頂けます。これまで通り Notes クライアントでのご利用も可能です。

CAMSS センターでの構築・検証概要

【使用したハード/ソフト】

Supermicro/VMware ESXi6, Windows2012R2, IBM Domino9.0.1 FP7,
IBM Notes9.0.1, IBM Verse

※IBM Verse ハイブリッド環境の構築にあたって、オンプレミスには Domino の最新バージョンの 9.0.1 FP7 を適用しました。ハイブリッド環境で Verse を利用するには、クライアントは 9.0 以上が必要です。

【環境の概要】

CAMSS センターのオンプレミス環境に用意した、Notes/Domino メール環境をクラウド上の IBM Verse と連携させます。オンプレミスの DB 等は残しながら、オンプレミスとクラウドの両環境で同じメールの参照・送受信ができるようにしました。

【構築にあたってのポイント】

①サーバーの準備

オンプレミスと Verse 間のメール配信とディレクトリ同期のために、オンプレミスにメールハブサーバーとディレクトリハブサーバー、DMZ 上にパススルーサーバーを準備する必要があります。

それぞれのサーバーの役割は以下です。

メールハブサーバー：オンプレミスのメールサーバーに届いたメールを、パススルーサーバーを介して Verse に配信します。

ディレクトリハブサーバー：オンプレミスのユーザー情報等を、パススルーサーバーを介して Verse と連携します。

パススルーサーバー：DMZ 上でオンプレミスと Verse 間の通信の中継を行います。クラウドとオンプレミスでの安全な通信を行うために必要です。自社の認証者 ID から、オンプレミスの Domino ドメインとは別の Domino ドメインのサーバーとして構築します。

②選択データセンターの確認

オンプレミスと Verse 間の通信にあたって、契約時に選択したデータセンターによって、ファイアウォールの通信を許可する宛先が変わります。データセンターは契約時 US、Japan 等の選択が可能です。選択したデータセンターに合わせた宛先設定を行わないと通信が行えませんので、注意が必要です。

*本環境では、US データセンターが宛先になっております。

例:パススルーサーバーと Verse 間の通信には、Notes Remote Procedure Cord(NRPC) というプロトコルで通信が行われ、NRPC はポート番号 1352 番を使用します。ポート番号 1352 番のインバウンド、アウトバウンド通信を許可する場合は、以下の宛先に対する通信を許可します。

データセンターが US の場合→notes.**na**.collabserv.com

データセンターが Japan の場合→notes.**ap**.collabserv.com

参考 URL:データセンター毎の NRPC、SMTP、http 等のポート番号で通信する際の宛先が記載されています。

<https://www->

[10.lotus.com/ldd/bhwiki.nsf/dx/Cheat_Sheetcol_Firewall_Settings_for_IBM_Smart_Cloud_Engage_Advanced](https://www-10.lotus.com/ldd/bhwiki.nsf/dx/Cheat_Sheetcol_Firewall_Settings_for_IBM_Smart_Cloud_Engage_Advanced)

③インターネットドメインとの接続

オンプレミスと Verse の連携にあたって、Verse 側から発行される検証用のランダムで生成される固有キーを DNS の CNAME レコードへ登録します。発行される文字列は発行させる度に変わりますので、すみやかに登録する必要があります。

DNS サーバーへの CNAME レコードの登録の反映には作業画面によると、「最長 48 時間かかりますが、ほとんどの場合はそれよりも短く済む」との記載があります。本作業では 20 分程度で反映されました。

今回この作業にあたっては、作業日を IT 管理部門に事前に通知しスムーズに対応してもらえるよう、調整・依頼が必要となりました。

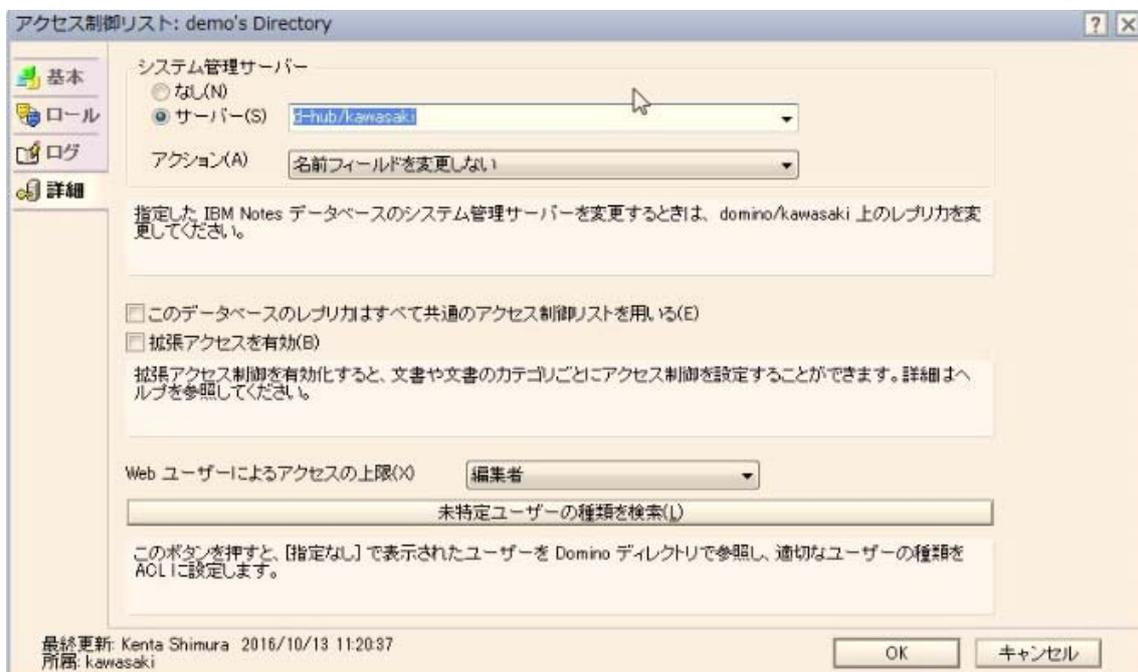
④ID ボールト信頼認証

ID ボールトとは、ユーザーID の保管庫です。ID ボールトにユーザーID をアップロードするために、ID ボールト信頼認証の発行を行います。ID ボールトを利用することによって、ユーザーがパスワードを忘れた時のパスワードの変更、ID ファイルの破損時の復旧等が簡単に行えます。ID ボールト信頼認証発行は、システム管理サーバーから実施する必要があります。

当初ディレクトリハブサーバーから信頼認証発行を行いましたが、こちらをシステム管理サーバーに指定していなかったため「エントリが索引に見つからない」というエラーが頻出してしまいました。(下図)



ディレクトリハブサーバーを設定変更しシステム管理サーバーとすることで、すぐに信頼認証の発行ができました。(以下設定画面)



構成図

