HP IceWall技術レポート:

容量無制限のファイルコラボレーションサービス Box との認証連携

1. はじめに

本レポートでは伊藤忠テクノソリューションズ株式会社(以下、「CTC」)が提供するクラウド型ファイル共有サービス「Box」にIceWall SSOを利用した場合の認証連携方法についてご紹介いたします。

2. Boxとは

Box は、クラウド型ファイル共有サービスを中心とした、人と人、情報と情報をつなぐコラボレーションプラットフォームです。
ブラウザだけで様々な種類のファイルの閲覧・共有・編集ができ、高い利便性で仕事も効率的に行えます。
アクセス権限の設定や、ファイルの暗号化、バックアップ機能も充実しており、いつでも、どこからでも、安心してご利用頂けます。

3. Boxの特徴

- グローバル展開
  20地域以上の言語に対応しており、アクセスする為に必要なのはインターネット環境と接続デバイスのみなので、海外出張時、海外拠点とのコラボレーションもストレスなく実施頂けます。

- 最高クラスのセキュリティ
  データは複数のデータセンターで暗号化され、分散して保持されています。
  また、アクセスログ検索や管理機能が充実していますので自社保管以上に安心してご利用頂けます。

- 大規模導入
  保存容量無制限で、数名～数万名の企業でも導入されていますので、企業規模に関わらず、容量を気にせずにご利用頂けます。

- 便利な機能により生産性向上
  オンラインファイル編集、ファイルへのコメント記載、ファイルテキスト検索等便利な機能が充実しており、クライアント側のOSやデバイスに依存しない為いつでも、どこからでも必要なファイルを利用でき、業務効率が向上します。

4. Box で認証連携ができるメリット

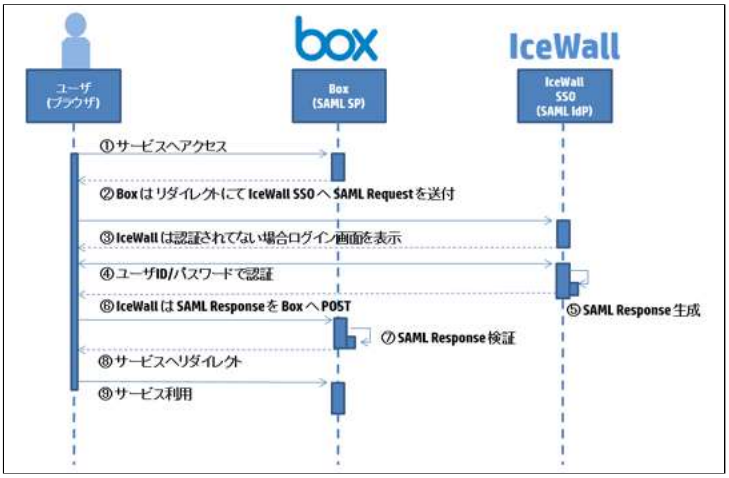
いつでも、どこからでも利用できるというのがクラウドサービスを利用する大きなメリットではありますが、IceWall SSO を用いてオンプレミスや他のクラウドサービスを含めてシングルサインオンする事で、以下のメリットが受けられます。

- 社外ネットワークからのアクセス制御
- セキュリティ対策
- 社内システムを含めたシングルサインオン
- 統一したパスワードポリシ
- 統一したアクセスログ管理
- クラウドサービス側のパスワード運用業務からの解放

5. SAML認証を使用したSSOの流れ

IceWall SSO は IceWall Federation というモジュールを利用し、SAML IdP 機能を実装する事が可能です。

Box は SAML2.0に対応しており、SAML IdP からセッションを開始する方法 (IdP Initiated) と Box ログイン画面からセッションを開始する方法 (SP Initiated) の双方に対応しています。以下ではSP Initiated のフローをご紹介します。



6. SAML IdP と SAML SP の設定に必要な情報

Box を SAML SP として設定する為に、下記の情報が必要となります。

項番	項目	必須か否か	例
1	サブドメイン	必須	ctc-g.co.jp
2	SAML IdP は何を使用するか	オプション	IceWall SSO (IceWall Federation)
3	リダイレクトするログイン画面のURL	必須	http://login.ctc-g.co.jp/fw/dfw/lt/boxidp/sso
4	認証局の発行する証明書を利用するか	オプション	いいえ
5	Box ログインに利用するユーザーのメールアドレスの属性名	必須	BoxMail
6	ユーザー姓の属性名	オプション	Lastname
7	ユーザー名の属性名	オプション	Firstname
8	ユーザーグループの属性名	オプション	BoxGroup
9	SAMLアサーションサンプル	オプション	
10	SAML IdP メタデータ	必須	

IceWall Federation を Box のSAML IdP として設定する為に、下記の情報が必要となります。

項番	項目	必須か否か	例
1	Box ログインに利用するユーザーのメールアドレスの属性名	必須	BoxMail
2	ユーザー姓の属性名	オプション	Lastname
3	ユーザー名の属性名	オプション	Firstname
4	ユーザーグループの属性名	オプション	BoxGroup
5	BoxがSAML Responseを受信する URL	必須	https://sso.services.box.net/sp/ACS.saml2
6	BoxのプロバイダID	必須	box.net

7. SAML IdP の設定手順

IceWall Federation を Box の SAML IdP として設定する手順は以下の通りです。
詳細に関しては「IceWall Federation 汎用 SAML 認証連携ガイド」をご参照ください。

事前準備：
「IceWall Federation 汎用 SAML 認証連携ガイド」に従って、IceWall Federation がインストールされているものとします。

手順：

1. IceWall Federation設定ファイルの以下の項目を変更します。

「ICEWALL_UID」にIceWall SSO のユーザーIDが格納された HTTP ヘッダ名を設定します。

```
(例) ICEWALL_UID=boxid
```

「ISSUER 」にSAML Response の ISSURE 値を設定します。

```
(例) ISSUER=http:// login.ctc-g.co.jp/fw/dfw/lt/boxidp
```

「ACS_URL 」にBox が SAML Response を受信する URL を設定します。

```
(例) ACS_URL=https://sso.services.box.net/sp/ACS.saml2
```

「SP_ENTITY_ID 」にBox のプロバイダIDを設定します。

```
(例) SP_ENTITY_ID=box.net
```

「ATTRIBUTE 」にSAML Response として Box に送る属性名を設定します。

```
(例) ATTRIBUTE= BoxMail
     ATTRIBUTE= Lastname
     ATTRIBUTE= Firstname
     ATTRIBUTE= BoxGroup
```

2. IceWall Federation SAML Response テンプレートの以下の項目を変更します。

「AttributeStatement」要素として、SAML Response にて Box に送る属性名を設定します。

```
(例)
<AttributeStatement>
   <Attribute Name=" BoxMail ">
      <AttributeValue>[BOXMAIL]</AttributeValue>
   </Attribute>
   <Attribute Name=" Lastname ">
      <AttributeValue>[LASTNAME]</AttributeValue>
   </Attribute>
   <Attribute Name=" Firstname ">
      <AttributeValue>[FIRSTNAME]</AttributeValue>
   </Attribute>
   <Attribute Name=" BoxGroup ">
      <AttributeValue>[BOXGROUP]</AttributeValue>
   </Attribute>
</AttributeStatement>
```

3. IceWall Federation メタファイルの以下の項目を変更し、Box 側に送付します。

「entityID」にSAML Response の ISSURE 値を設定します。

```
(例) entityID="http:// login.ctc-g.co.jp/fw/dfw/lt/boxidp"
```

「ds:X509Certificate」に SAML Response の署名に使用する鍵ファイルを生成した際の、公開鍵を抽出し文字列を設定します。

「Location」にシングルサインオンサービスの URL を設定します。

```
(例) Location="http:// login.ctc-g.co.jp/fw/dfw/lt/boxidp/sso"
```

8. おわりに

本レポートでは、IceWall SSO を用いて Box へ認証連携する事のメリットや設定内容をご紹介しました。オンプレミスシステムと SaaS サービスを認証連携する事で、セキュリティの確保及びユーザーの利便性の向上という双方のメリットがはかれます。Box 等の SaaS サービスの導入を検討される際には、是非とも認証部分にもご注目頂き、セットでの導入をご検討下さい。

2015.9.16　新規掲載

執筆者　伊藤忠テクノソリューションズ株式会社
http://www.ctc-g.co.jp/