

IceWall技術レポート：

Active Directory環境でのIceWallへのアクセス（信頼関係を結んでいない複数ドメイン編）



1. はじめに

IceWallでMicrosoftのActive Directory（以下、AD）と連携する事で統合Windows認証を使用したアクセスができます。統合Windows認証を使用することでADドメインに参加したWindows端末から非Windowsアプリケーションへシングルサインオンでのアクセスが可能になります。

今回紹介する方法によって、従来のWindows環境ではあきらめざるを得なかった、ドメイン信頼がない複数ADドメイン環境でのシングルサインオンを実現することができます。

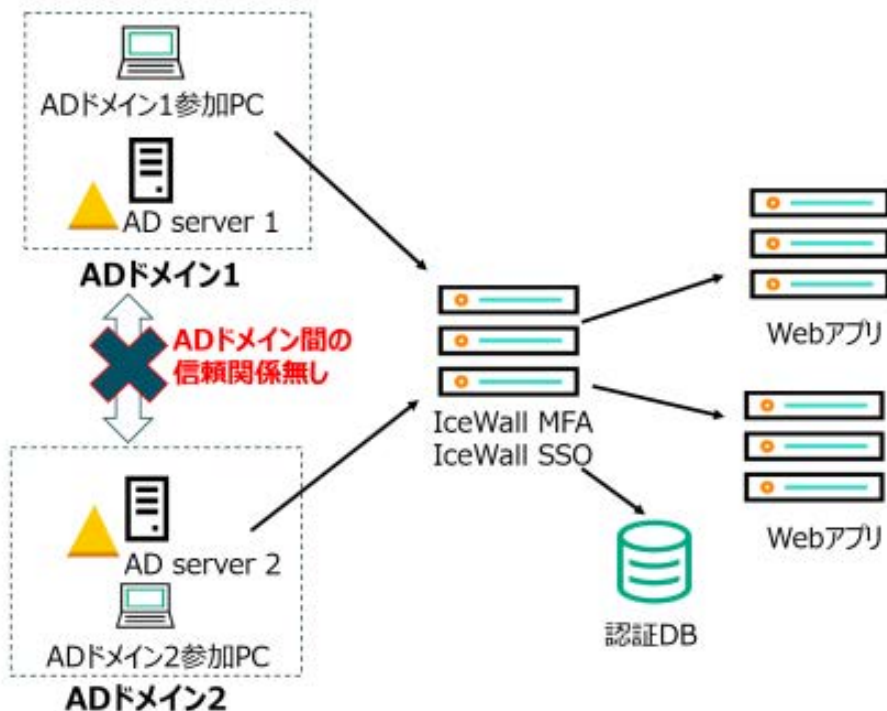
本レポートでは、「信頼関係を結んでいない複数ドメイン」の環境下でIceWall MFAおよびIceWall SSOに統合Windows認証を使用したアクセスを可能にするシステムの構築手順を説明します。

なお「信頼関係を結んでいる複数ドメイン」の場合については以下のレポートを参照してください。

技術レポート：[IceWall SSO Domain Gateway Optionが連携可能な複数ドメイン構成](#)

1.1. 信頼関係を結んでいない複数ADドメインとIceWallの連携概要

以下が概要図です。



ADドメイン1とADドメイン2は信頼関係を結んでいない、外部の信頼もしくはフォレストの信頼の関係が存在しない、独立したADドメインです。

「ADドメイン1に参加しているPC」と「ADドメイン2に参加しているPC」のどちらからアクセスしているユーザーからも統合Windows認証でIceWallにアクセスする事ができます。

認証DBには、ADドメイン1とADドメイン2に登録されている両方のユーザー情報が登録されている必要があります。

各ADドメインのADサーバー上で作成した鍵情報をIceWallのサーバー内の一つkeytabファイルに保存する事で両方のドメインからアクセスが可能になります。

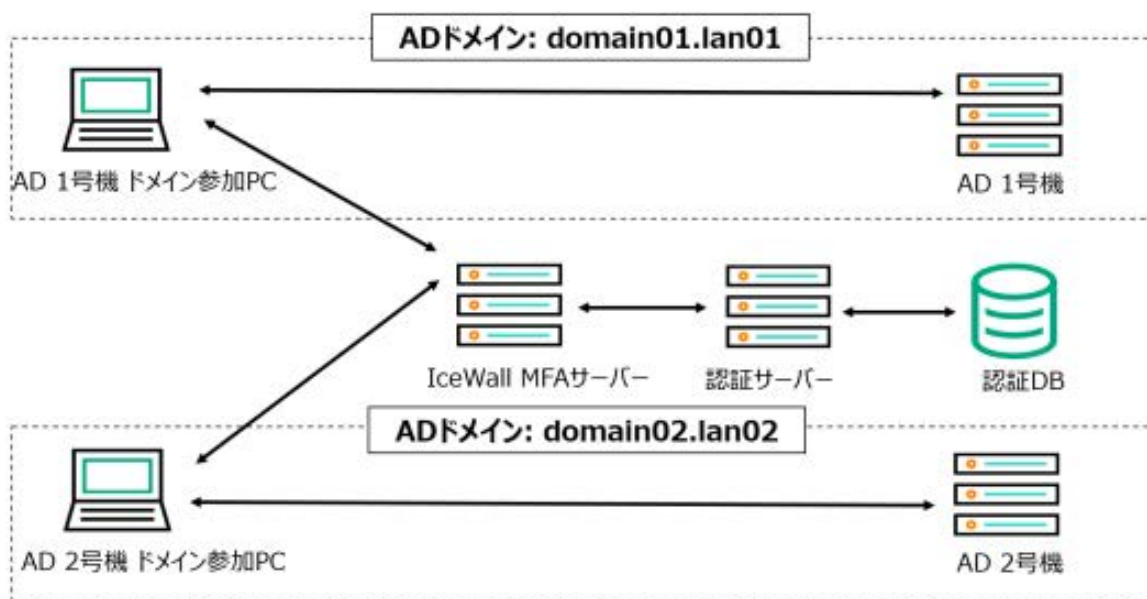
以降の章では、IceWall MFAとIceWall SSOのそれぞれで環境を構築する例を記載します。

2. IceWall MFAでの構築手順

IceWall MFAが動作するOS環境がLinuxとWindowsの場合の2つのケースでシステムを構築し、検証を行っています。

2.1. 構成

IceWall MFAでの構成図は以下の通りです。



2.1.2. Linux環境 詳細情報

IceWall MFAサーバーのOSがLinuxの場合の各サーバーの詳細は以下の通りです。

サーバー役割	ホスト名	OS	備考
IceWall MFA	mfa01.domain01.lan01	Red Hat Enterprise Linux Server release 7.6	IceWall MFA Controllerバージョン : 04.00.03.180827A IWA Pluginバージョン : 04.00.01.180827A Apache Tomcatバージョン : 7.0.76-7 OpenJDKバージョン : 1.8.0.181-7.b13
AD 1号機	ad01.domain01.lan01	Windows Server 2019	インストール済みサービス <ul style="list-style-type: none"> DNSサーバー Active Directoryドメイン サービス
AD 2号機	ad02.domain02.lan02	Windows Server 2019	(Active Directory機能レベル : Windows Server 2016)
IceWall 認証サーバー	certd01.domain01.lan01	Red Hat Enterprise Linux Server release 7.6	認証モジュールからFederation認証するためのユーザーが認証DBに存在する必要があります。

2.1.3. Windows環境 詳細情報

IceWall MFAサーバーのOSがWindows Serverの場合の各サーバーの詳細は以下の通りです。

サーバー役割	ホスト名	OS	備考
IceWall MFA	mfa01.domain 01.lan01	Windows Server 2016	IceWall MFA Controllerバージョン : 04.00.03.180827A IWA Pluginバージョン : 04.00.01.180827A Apache Tomcatバージョン : 9.0.34 Oracle JDKバージョン : 11.0.7
AD 1号機	ad01.domain0 1.lan01	Windows Server 2019	インストール済みサービス ■ DNSサーバー ■ Active Directoryドメイン サービス
AD 2号機	ad02.domain0 2.lan02	Windows Server 2019	(Active Directory機能レベル : Windows Server 2016)
IceWall 認証サーバー	certd01.domai n01.lan01	Windows Server 2016	認証モジュールからFederation認証するためのユーザーが認証DBに存在する必要があります。

2.2. 構築手順

IceWall MFAサーバーのOSがWindows Serverの場合の各サーバーの詳細は以下の通りです。

2.2.1. AD 1号機での手順

1. IceWall MFAのサービス・プリンシパル・ネーム (以下、SPN) を登録するためのユーザーを作成します。

ユーザー名は例として「mfa01_ad01」で説明します。

2. 作成したユーザー「mfa01_ad01」のプロパティのアカウントタブを表示して「このアカウントでKerberos AES 256ビット暗号化をサポートする」にチェックを入れます。

手順3のktpassコマンドの -crypto オプションで指定する暗号化方式に合わせて設定する必要があります。

3. コマンドプロンプトで ktpassコマンドを実行し、Keytabファイルを作成します。

```
ktpass -crypto [Kerberosチケットの暗号化方式] -princ [プリンシパル名(HTTP/FQDN@REALMS)] -mapuser [SPNを登録するユーザー名] -pass [パスワード] -ptype [プリンシパルの種類] -out [出力ファイル名]
```

※FQDNが大文字の場合でも、小文字で指定する必要があります。

※REALMSは大文字で記述する必要があります。

コマンド例：

```
ktpass -crypto AES256-SHA1 -princ HTTP/mfa01.domain01.lan01@DOMAIN01.LAN01 -mapuser mfa01_ad01 -pass password -ptype KRB5_NT_PRINCIPAL -out C:\mfa01_ad01.keytab
```

```
Targeting domain controller: ad01.domain01.lan01
```

```
Successfully mapped HTTP/mfa01.domain01.lan01 to mfa01_ad01.
```

```
Password successfully set!
```

```
Key created.
```

```
Output keytab to C:\mfa01_ad01.keytab:
```

```
Keytab version: 0x502
```

```
keysize 92 HTTP/mfa01.domain01.lan01@DOMAIN01.LAN01 ptype 1 (KRB5_NT_PRINCIPAL)
```

```
vno 3 etype 0x12 (AES256-SHA1) keylength 32
```

```
(0x70bb23da12c7a5c4aafe3106972a9b18a931d35d8a37392725c6f3596b8e166e)
```

4. ユーザーアカウントに関連付けされているSPNを確認する為にsetspnコマンドを実行します。

```
setspn -L [ユーザー名]
```

コマンド例：

```
setspn -L mfa01_ad01
```

次の項目に登録されている CN=mfa01_ad01,OU=icewall,DC=domain01,DC=lan01:

```
HTTP/mfa01.domain01.lan01
```

2.2.2. AD 2号機での手順

作成するkeytabファイルは、1つのファイル内に複数の鍵情報を格納する必要があります。

1つのkeytabファイル内に複数の鍵情報を格納する手順として、以下の2通りの方法があります。

- AD 2号機でktpassコマンドを実行する際に、追加で「-in」オプションの指定をする。
- Linuxサーバー上のktutilコマンドで、複数のkeytabファイルを1つにまとめる。

■AD 2号機でktpassコマンドを実行する際に、追加で「-in」オプションの指定をする手順

1.AD 1号機で作成したkeytabファイルをAD 2号機に転送します。

2.「2.2.1. AD 1号機での手順」を参照し、同様の手順でkeytabファイルを作成します。

手順3のktpassコマンドを実行する際に、「-in」オプションでAD 1号機のkeytabファイルを指定します。

以下のコマンド例は、SPNを登録するユーザー名を「mfa01_ad02」、及び作成するkeytabファイル名を「krb5.keytab」として説明します。

コマンド例：

```
ktpass -crypto AES256-SHA1 -princ HTTP/mfa01.domain01.lan01@DOMAIN02.LAN02 -  
mapuser mfa01_ad02 -pass password -ptype KRB5_NT_PRINCIPAL -in C:\mfa01_ad01.keytab  
-out C:\krb5.keytab
```

Existing keytab:

```
Keytab version: 0x502  
keysize 92 HTTP/mfa01.domain01.lan01@DOMAIN01.LAN01 ptype 1 (KRB5_NT_PRINCIPAL)  
vno 3 etype 0x12 (AES256-SHA1) keylength 32  
(0x70bb23da12c7a5c4aafe3106972a9b18a931d35d8a37392725c6f3596b8e166e)  
Targeting domain controller: ad02.domain02.lan02  
Successfully mapped HTTP/mfa01.domain01.lan01 to mfa01_ad02.  
Password successfully set!  
Key created.
```

Output keytab to C:\krb5.keytab:

```
Keytab version: 0x502  
keysize 92 HTTP/mfa01.domain01.lan01@DOMAIN01.LAN01 ptype 1 (KRB5_NT_PRINCIPAL)  
vno 3 etype 0x12 (AES256-SHA1) keylength 32  
(0x70bb23da12c7a5c4aafe3106972a9b18a931d35d8a37392725c6f3596b8e166e)  
keysize 92 HTTP/mfa01.domain01.lan01@DOMAIN02.LAN02 ptype 1 (KRB5_NT_PRINCIPAL)  
vno 3 etype 0x12 (AES256-SHA1) keylength 32  
(0xff9a3c54f5a2fb1d3d599a37bd85d9edf32563055b032a388e3c989bc8b066cd)
```

■Linuxサーバー上のktutilコマンドで複数のkeytabファイルを1つにまとめる手順

1. 「2.2.1. AD 1号機での手順」を参照しkeytabファイルを作成します。
手順3のktpassコマンドを実行する際は、「-in」オプションの指定は行いません。
2. LinuxサーバーにAD 1号機、及びAD 2号機で作成したkeytabファイルを転送します。
3. 「krb5-workstation」をインストールして、ktutilコマンドを使用できるようにします。
4. ktutilコマンドで複数のkeytabファイルを1つにまとめます。

```
# ktutil  
ktutil: read_kt [AD 1号機で作成したkeytabファイル]  
ktutil: read_kt [AD 2号機で作成したkeytabファイル]  
ktutil: list  
slot KVNO Principal  
-----  
1 3 [AD 1号機で作成した鍵のSPN]  
2 3 [AD 2号機で作成した鍵のSPN]  
ktutil: write_kt [出力先のファイル名]  
ktutil: quit
```

コマンド例：

```
# ktutil  
ktutil: read_kt /tmp/mfa01_ad01.keytab  
ktutil: read_kt /tmp/mfa01_ad02.keytab  
ktutil: list  
slot KVNO Principal  
-----
```

```
1 3 HTTP/mfa01.domain01.lan01@DOMAIN01.LAN01
2 3 HTTP/mfa01.domain01.lan01@DOMAIN02.LAN02
ktutil: write_kt /etc/krb5.keytab
ktutil: quit
```

2.2.3. IceWall MFAサーバーでの手順

1. IceWall MFAの製品マニュアル「導入ガイド for 統合 Windows 認証オプション」を参照し、インストールと設定を行います。

2. 作成したkeytabファイルをIceWall MFAサーバーに転送します。
OSがLinuxの場合は「/opt/icewall-mfa/mfa/config/plugin/iwa/krb5.keytab」に配置します。
OSがWindows Serverの場合は「C:\Program Files\icewall-mfa\mfa\config\plugin\iwa\krb5.keytab」に配置します。

3. Tomcatを実行するユーザーに、keytabファイルの読み込み権限を設定します。

OSがLinuxの場合のコマンド例：

```
# chown tomcat:tomcat /opt/icewall-mfa/mfa/config/plugin/iwa/krb5.keytab
# chmod 600 /opt/icewall-mfa/mfa/config/plugin/iwa/krb5.keytab
# ll /opt/icewall-mfa/mfa/config/plugin/iwa/krb5.keytab
-rw----- 1 tomcat tomcat 97 5月 11 16:59 /opt/icewall-
mfa/mfa/config/plugin/iwa/krb5.keytab
```

OSがWindowsの場合は、keytabファイルのプロパティからTomcatの起動ユーザーの読み込み権限を確認します。

4. IceWall MFAの設定ファイルjaas.confの「principal」を設定します。

jaas.conf設定例：

```
principal=*
```

5. 設定ファイルkrb5.confの「default_realm」を設定します。
krb5.confの配置する場所は、JavaのバージョンとOSの組み合わせによって異なります。
「default_realm」に設定する値は存在しないREALMでも動作可能ですが、例として「DOMAIN01.LAN01」で説明します。

◎OpenJDK 1.8.0 と Linux の組み合わせの場合
/etc/krb5.conf

```
[libdefaults]
default_realm = DOMAIN01.LAN01
```

◎Oracle JDK.11 と Windows Server の組み合わせの場合
C:\Program Files\Java\jdk-\conf\security\krb5.conf

```
[libdefaults]
default_realm = DOMAIN01.LAN01
```

6. DNSの名前解決の設定を行います。

hosts設定例：

```
127.0.0.1 mfa01.domain01.lan01 localhost.localdomain localhost
```

※名前解決の候補を複数記述する場合は、FQDNを先に記述する必要があります。

2.2.4. クライアント端末での手順

1. IceWall MFAサーバー、およびADサーバーの名前解決ができるようにDNS設定を行います。
2. クライアント端末をADドメインサーバーにドメイン参加させます。
3. Microsoft Internet Explorerを起動し、画面右上の歯車のアイコンをクリックして「インターネットオプション(O)」を表示します。
4. 以下の順序で「ローカルイントラネット」の設定画面を表示します。
[セキュリティ タブをクリック] - [ローカルイントラネットを選択] - [サイトををクリック] - [詳細設定をクリック]
5. ローカルイントラネットにIceWall MFAサーバーを追加します。

設定例：

```
http://mfa01.domain01.lan01
```

6. 以下の順序で「セキュリティ設定」の設定画面を表示します。
[セキュリティ タブをクリック] - [ローカルイントラネットをクリック] - [レベルのカスタマイズをクリック]
7. 以下の順序でユーザー認証の設定をします。
[ユーザー認証] - [ログオン] - [イントラネットゾーンでのみ自動的にログオンする]
8. IceWallログインページにアクセスし、統合Windows認証を行います。
アドレス欄に指定するURLはIPアドレス形式での指定ではなく、FQDNで指定する必要があります。

IceWall MFAのOSがLinuxの場合のURL例：

```
http://mfa01.domain01.lan01/iwproxy/bk01/index.html
```

IceWall MFAのOSがWindows Serverの場合のURL例：

```
http://mfa01.domain01.lan01/fw/dfw/bk01/index.html
```

3. IceWall SSOでの構築手順

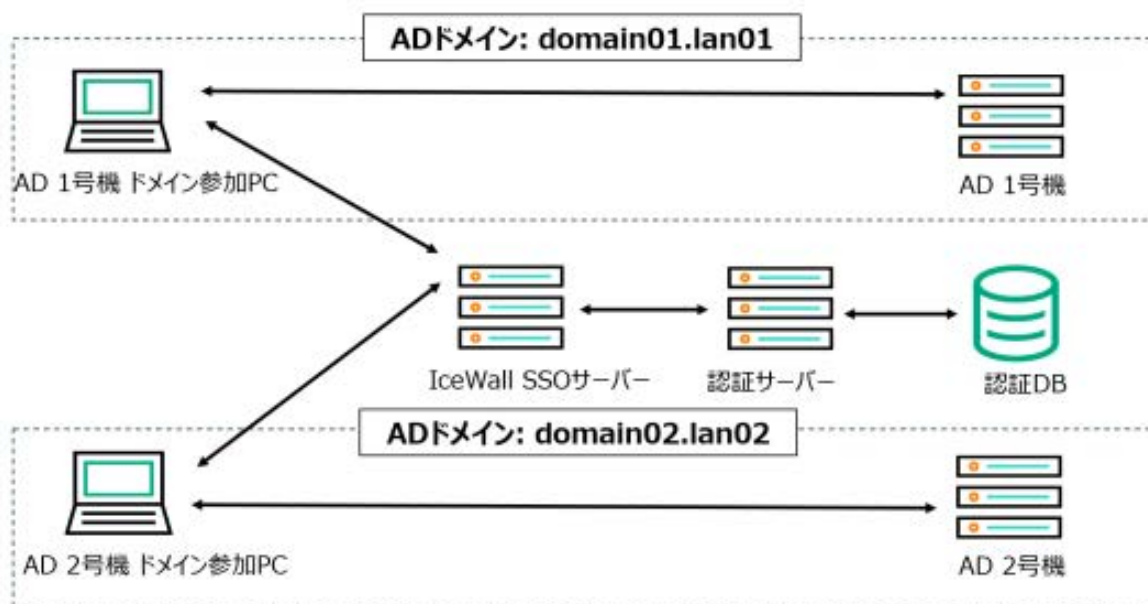
IceWall SSOでは、信頼関係を結んでいない複数ドメイン構成に対してLinux環境でのみ統合Windows認証が可能です。

そのためIceWall SSOサーバーのOSがLinuxの場合のみ説明します。

(Windows環境ではkeytabファイルを使用しないため、信頼関係を結んでいない複数ドメイン構成での統合Windows認証は行えません)

3.1.構成

IceWall SSOでの構成図は以下の通りです。



3.2.環境詳細

各サーバーの詳細は以下の通りです。

サーバー役割	ホスト名	OS	備考
IceWall SSOサーバー	dgfw01.domain01.lan01	Red Hat Enterprise Linux Server release 7.6	Domain Gateway Optionバージョン: 11.00.00.170804Ahttpdバージョン: 2.4.6-88

AD 1号機	ad01.domain 01.lan01	Windows Server 2019	インストール済みサービス <ul style="list-style-type: none"> ■ DNSサーバー ■ Active Directoryドメイン サービス (Active Directory機能レベル : Windows Server 2016)
AD 2号機	ad02.domain 02.lan02	Windows Server 2019	
IceWall 認証サーバー	certd01.domain 01.lan01	Red Hat Enterprise Linux Server release 7.6	認証モジュールからFederation認証するためのユーザーが認証DBに存在する必要があります。

3.2.1. 構築手順

ここではすでにIceWall SSOでユーザーIDとパスワードによる認証ができる状態が構築されている前提で、それ以降に必要な手順を説明します。

3.2.2. AD 1号機での手順

前述の「2.2.1. AD 1号機での手順」を参照し、同様の手順でkeytabファイルを作成します。

3.2.3. AD 2号機での手順

前述の「2.2.2. AD 2号機での手順」を参照し、同様の手順でkeytabファイルを作成します。作成するkeytabファイル名は、「krb5.keytab」とします。

3.2.4. IceWall SSOサーバーでの手順

1. 「導入ガイド Domain Gateway Option for UNIX」を参照し、インストールと設定を行います。
2. keytabファイルをIceWall SSOサーバーの「/etc/krb5.keytab」に配置します。
3. httpdを実行するユーザーに、keytabファイルの読み込み権限を設定します。

```
# chown apache:apache /etc/krb5.keytab
# chmod 600 /etc/krb5.keytab
# ll /etc/krb5.keytab
-rw----- 1 apache apache 194 5月 11 15:59 /etc/krb5.keytab
```

4. 設定ファイルdgfw.confの「SERVICE_NAME」に「HTTP@FQDN」の形式で設定します。

dgfw.conf設定例 :

```
SERVICE_NAME=HTTP@dgfw01.domain01.lan01
```

5. DNSの名前解決の設定を行います。

hosts設定例：

```
127.0.0.1 dgfw01.domain01.lan01 localhost.localdomain localhost
```

3.2.5. クライアント端末での手順

前述の「2.2.4. クライアント端末での手順」を参照し、統合Windows認証の設定を行います。

URL例：

```
http://dgfw01.domain01.lan01/fw/dfw/LOCALHOST/index.html
```

4. トラブルシューティング

IceWall上での統合Windows認証でエラーとなる場合の確認ポイントを記載します。

4.1. クライアント端末でのKerberosチケットの取得確認

クライアント端末でKerberosチケットの取得が成功しているか確認する場合は、「klist」コマンドを実行します。

klistコマンド例：

```
klist
```

```
現在のログオン ID: 0:0x14b3e3d
```

```
キャッシュされたチケット: (2)
```

```
#0> クライアント: user01 @ DOMAIN01.LAN01
```

```
  サーバー: krbtgt/DOMAIN01.LAN01 @ DOMAIN01.LAN01
```

```
  Kerberos チケットの暗号化の種類: AES-256-CTS-HMAC-SHA1-96
```

```
  チケットのフラグ 0x40e10000 -> forwardable renewable initial pre_authent
```

```
name_canonicalize
```

```
  開始時刻: 4/28/2020 11:12:40 (ローカル)
```

```
  終了時刻: 4/28/2020 21:12:40 (ローカル)
```

```
  更新期限: 5/5/2020 11:12:40 (ローカル)
```

```
セッション キーの種類: AES-256-CTS-HMAC-SHA1-96  
キャッシュ フラグ: 0x1 -> PRIMARY  
呼び出された Kdc: ad01.domain01.lan01
```

```
#1> クライアント: user01 @ DOMAIN01.LAN01  
サーバー: HTTP/mfa01.domain01.lan01 @ DOMAIN01.LAN01  
Kerberos チケットの暗号化の種類: AES-256-CTS-HMAC-SHA1-96  
チケットのフラグ 0x40a10000 -> forwardable renewable pre_authent name_canonicalize  
開始時刻: 4/28/2020 11:12:40 (ローカル)  
終了時刻: 4/28/2020 21:12:40 (ローカル)  
更新期限: 5/5/2020 11:12:40 (ローカル)  
セッション キーの種類: AES-256-CTS-HMAC-SHA1-96  
キャッシュ フラグ: 0  
呼び出された Kdc: ad01.domain01.lan01
```

4.2. keytabファイル内の鍵情報の確認

keytabファイル内の鍵情報を確認する方法を説明します。
以下の手順はLinuxサーバー上での確認手順です。

1. 「krb5-workstation」をインストールして、ktutilコマンドを使用できるようにします。
2. ktutilコマンドでkeytabファイルの内容を表示します。

```
# ktutil  
ktutil: read_kt /etc/krb5.keytab  
ktutil: list  
slot KVNO Principal  
-----  
1 3 HTTP/mfa01.domain01.lan01@DOMAIN01.LAN01  
2 3 HTTP/mfa01.domain01.lan01@DOMAIN02.LAN02  
ktutil: quit
```

4.3. その他の確認点

その他のエラーの原因として、以下の項目が考えられます。

- REALMを大文字で統一して設定していない
- ADサーバー、IceWallサーバー、クライアントの時刻が大きくずれている

5. まとめ

IceWall SSOのWindows版以外なら信頼関係を結んでいない複数ADドメインの環境下でも、単一のkeytabファイル内に複数の鍵情報を保管することで、IceWallでの統合Windows認証が可能となります。

ここで述べた内容は、技術的観点に基づいて検証した結果を示したもので特定の環境での動作や性能を保証するものではありません。

実際の構築に関しては、HPEまたはIceWallパートナーへご相談ください。

関連技術レポート

[Domain Gateway オプションの環境構築における考慮点](#) →

[Active Directory環境でのIceWallへのアクセス（信頼関係を結んでいる複数ドメイン編）](#) →

2020/6/1

執筆者 社名：日本ヒューレット・パッカー株式会社

所属：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

名前：神原健太

[技術レポート一覧へ](#) →

お探しの情報は見つかりましたか？





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)

© Copyright 2024 Hewlett Packard Enterprise Development LP

[個人情報保護方針](#) | [ご利用条件・免責事項](#) | [AdChoices & クッキー](#) | [サイトマップ](#)

