SailPoint IdentityNowによるHPE IceWallのアクセス権限管理

IceWall技術レポート

1. はじめに →
2. IceWall のアクセス権限 →
3. IdentityNowでの権限管理 →
4. IdentityNowとIceWallの接続 →
5. アクセス権限管理の方式と設定 →
6. さいごに →

1. はじめに

ゼロトラストセキュリティの導入では、誰に対しても必要最小限の権限のみが与えられることが求められます。

ユーザーのアクセス権限が適切に管理されていなければ、最小権限の原則を満たせずセキュリティの低下につながります。

本レポートではSailPoint IdentityNow※1で管理された適切なアクセス権限を、IceWall※2のアクセス制御に活用する方法をご紹介します。

※1 SailPoint IdentityNowはアイデンティティガバナンス・管理（IGA）サービスです。

※2本レポートでは認証DBにLDAPを利用しています。

※　本レポートの内容は2022年9月時点のIdentityNowサービス、およびIceWall 認証モジュール（certd） Ver 11.0 patch 6 (ICP3モード)に基づきます。

2. IceWall のアクセス権限

IceWallでのアクセス制御は、２つの設定に従って行われます。一つ目は「ユーザーがどのグループに所属するか」を判定する設定です。二つ目は「対象システムへのアクセスが許可されるグループ」を定義する設定です。ここで使用されるグループはIceWallに設定する独自のグループであり、必ずしも認証DBにてグループとして管理されているわけでは無いことに注意する必要があります。

ユーザーがどのグループに所属するかは、ユーザーの属性の値が、グループ所属判定の設定に記述された正規表現にマッチするかどうかで判定されます。グループ所属判定の設定は、グループ設定ファイル（cert.grp）に下記の書式で記述します。

```
グループ名,属性名="判定正規表現"
```

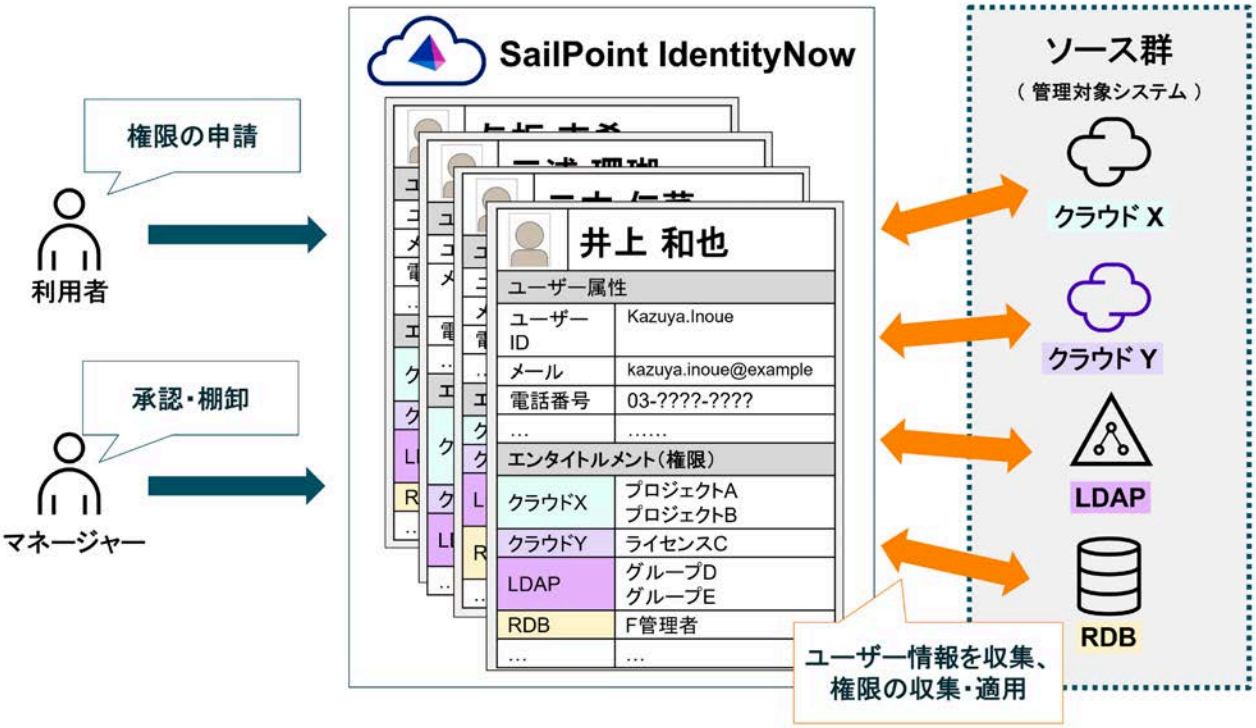
- **複数値属性**
  認証DBがLDAPであった場合、IceWallは複数値属性を扱うことが出来ます。グループ所属判定の属性が複数値だった場合、いずれかの値が判定正規表現にマッチすればそのグループに所属していると判定されます。この動作を利用すると、複数のグループで判定に用いる属性を同一、判定正規表現を異なるものとし、認証DBの単一属性に値を追加・削除することで、そのユーザーのアクセス権限を制御することが可能となります。
  認証DBがRDBであった場合には、複数値属性を扱うことは出来ないため、このような方式での制御は出来ません。

3. IdentityNowでの権限管理

3.1 SailPoint IdentityNow とは

SailPoint IdentityNow は、IGAを提供するSaaSサービスです。組織が利用する様々なシステム（クラウドサービスやオンプレミスアプリケーション）において、各ユーザーアカウントがどのような権限（エンタイトルメント）を保有しているかを収集し、監査し、棚卸し、是正する事が出来ます。また、ポリシーに従って自動で権限を付与・剥奪することや、申請と承認によって一時的に権限を付与することも出来ます。

3.2 エンタイトルメント管理



IdentityNowでは、管理対象のシステムをソースと呼びます。ソースでのユーザー権限はソース毎にグループであったり、ライセンス割り当てであったり、あるいは単なる属性値であったりと様々ですが、IdentityNowではそれらを抽象化してエンタイトルメントとして扱います。IdentityNowは、定期的にソースからユーザーのエンタイトルメントを収集し、棚卸しを行い、結果をソースに反映することで、ソースのユーザー権限を適正に保つことが出来ます。また、ワークフローを利用した申請と承認を行うことで、ソースのユーザーに権限の割り当てを行うことも出来ます。

3.3 LDAPソースのエンタイトルメント

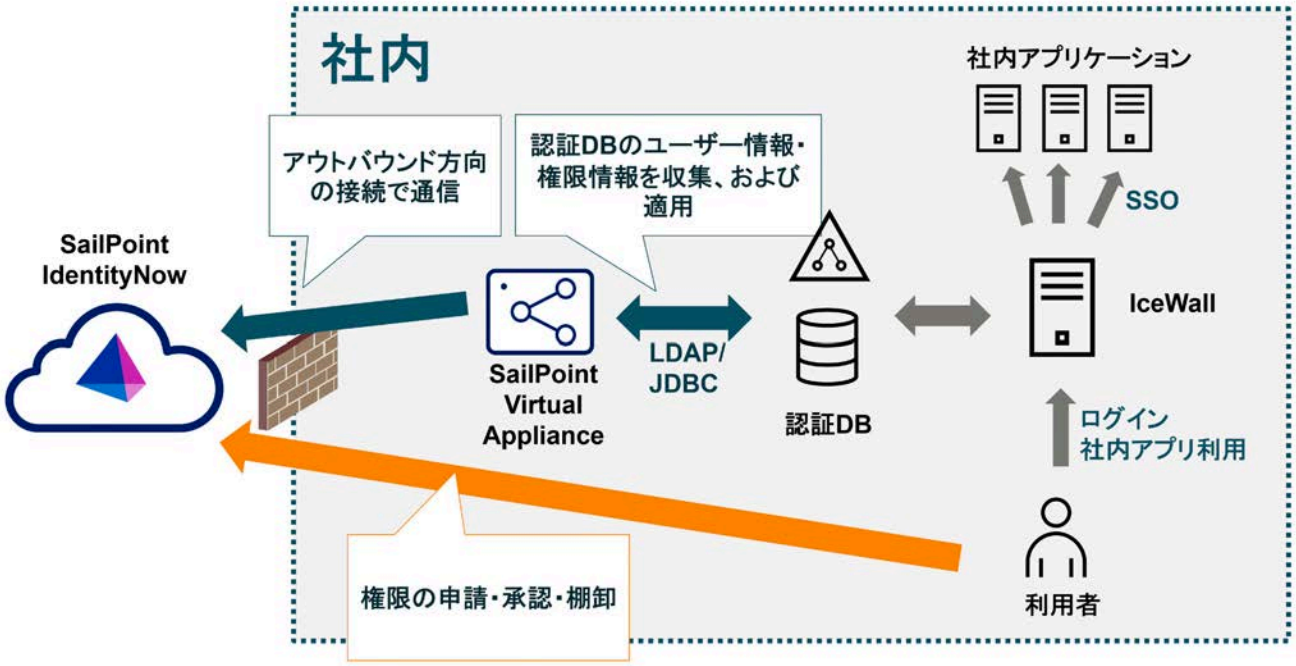
IdentityNowは、LDAPソースについては、『LDAPグループにメンバーとして所属』しているかどうか、と『ユーザーエントリがエンタイトルメントを表す属性を保有』しているかどうか、の、二つ状態をエンタイトルメントとして扱うことが出来ます。

- **LDAPグループにメンバーとして所属**
  groupOfNames, groupOfUniqueNames などのLDAPのグループエントリに、ユーザーがメン

バーとして登録されていることを、エンタイトルメントを保有していると扱う方式。

- **ユーザーエントリがエンタイトルメントを表す属性を保有**
  ユーザーエントリの特定の属性が特定の属性値を持つ場合に、エンタイトルメントを保有していると扱う方式。一つの複数値属性のそれぞれの値がそれぞれエンタイトルメントであると扱うことも出来ます。

4. IdentityNowとIceWallの接続



SaaSであるIdentityNowから、社内（オンプレミス）のソースを管理するために、SailPoint Virtual Appliance というシステムを、IdentityNowとソースの両方に対して通信が可能なネットワークに配備します。

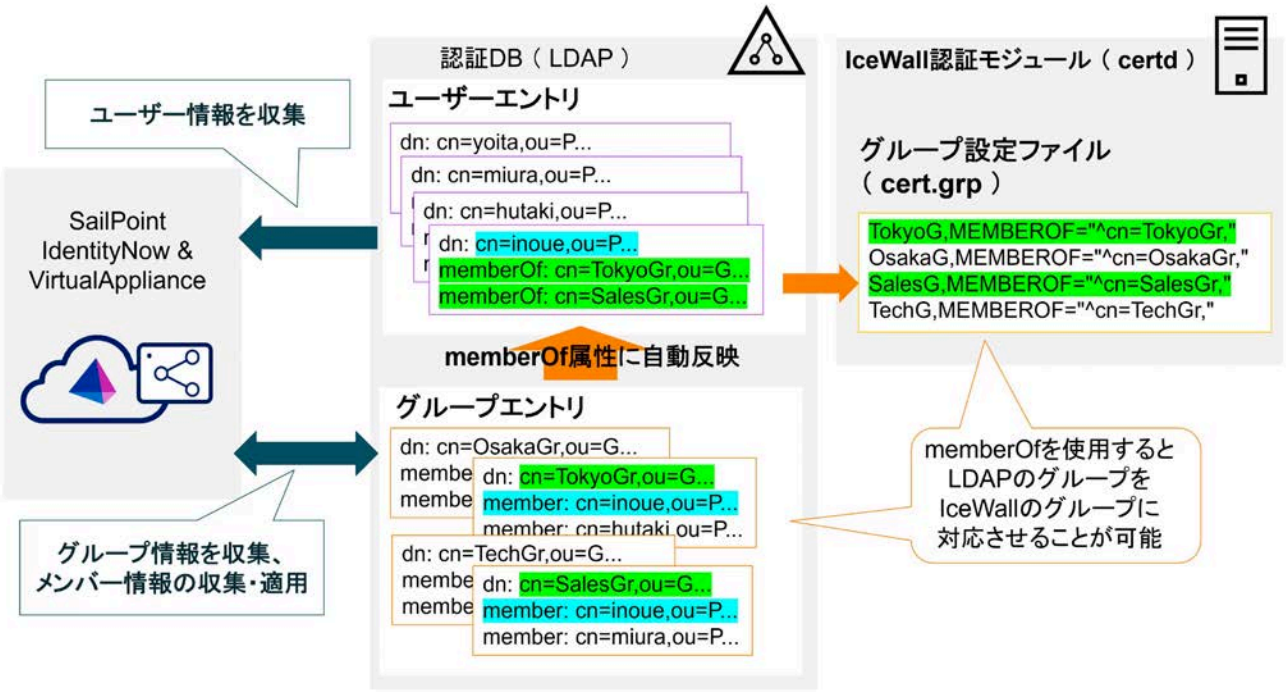
Virtual Appliance は、LDAPやJDBCを通じてソースに直接アクセスし、ユーザー情報や権限情報の収集および適用を行います。またIdentityNowにHTTPSで通信し、そのVirtual Applianceで実施するタスク（ユーザー情報やグループ情報の収集・適用）を取得し、それを実行し、結果をIdentityNow に送付します。

5. アクセス権限管理の方式と設定

IceWallの認証DBがLDAPの場合、IdentityNowでのアクセス権限管理は３つの方式が考えられます。

5.1 memberOf属性を利用してグループエントリをIceWallグループに対応させる方式

- **方式概要**
  LDAPサーバーでmemberOf属性機能を有効にすると、LDAPグループに所属したユーザーのエントリには、グループのDNを値とするmemmberOf 属性が自動的に追加されるようになります。
  memberOf属性は複数値属性であり、複数グループに所属すると、その全てのグループのDNが値に追加されます。
  IceWallのグループ所属判定にグループDNにマッチする正規表現を用いることで、LDAPグループとIceWallグループとを１対１に対応させることが出来ます。
  IdentityNowではLDAPグループへの所属状態をそのままエンタイトルメントとして扱います。



- **設定方法**
  IceWallでは、認証DBカラム情報ファイル（ dbattr.conf ）にて memberOf属性を読み込むよう設定し、グループ設定ファイル（ cert.grp ）にて、それぞれのグループDNだけにマッチするよう判定正規表現を記述します。

- dbattr.conf の設定例

```
MEMBEROF=memberOf
```

- cert.grp の設定例

```
TokyoG,MEMBEROF="^cn=TokyoGr,"
OsakaG,MEMBEROF="^cn=OsakaGr,"
SalesG,MEMBEROF="^cn=SalesGr,"
TechG,MEMBEROF="^cn=TechGr,"
```

IdentityNowでは、LDAPグループへの所属をエンタイトルメントとして扱うようソースを構成します。

1. ソースタイプに「OpenLDAP」を選択して新規ソースを作成し、環境に合わせて接続設定を行う。

2. 「アカウントおよびグループ設定」にて、以下の通り設定する。

設定項目	説明
アカウント設定	
検索識別名	ユーザーエントリを検索する際のベースDN。
LDAP検索フィルター	ユーザーエントリを検索する際のフィルター。 例：(objectclass=inetOrgPerson)
グループメンバー検索識別名	ユーザーが所属しているグループエントリを検索する際のベースDN。 通常はグループ設定の検索識別名と同じになる。
グループメンバー検索フィルター	ユーザーが所属しているグループエントリを検索する際の追加フィルター。
グループ設定	
検索識別名	グループ一覧を検索する際のベースDN。
LDAP検索フィルター	グループ一覧を検索する際のフィルター。 例：(objectclass=groupOfNames)

3. 接続をテストする。

4. 「アカウントスキーマ」と「関連付け」を環境に合わせて適切に設定する。この時、アカウントスキーマの groups 属性は変更しないこと。

5. グループエントリが groupOfUniqueNames ではなく groupOfNames の場合、グループ用スキーマを変更する必要がある。Web画面からはこの設定を行えず、APIを用いて設定する必要がある。

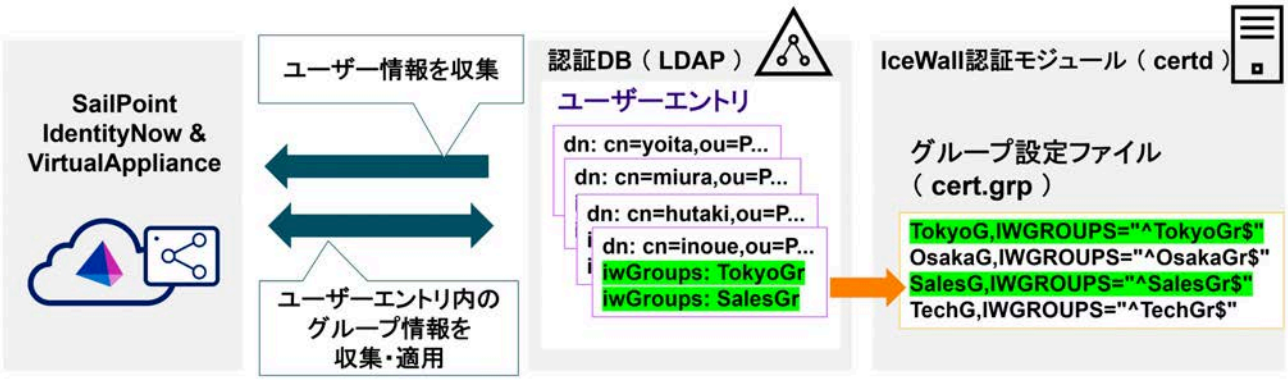
```
$ curl -X PATCH \
 https://{tenant}.api.identitynow.com/v3/sources/{source-id}/schemas/{schema-id} \
 -H 'Authorization: Bearer {Access-Token}' \
 -H 'Content-Type: application/json-patch+json' \
 -d '[ { "op": "replace",
        "path": "/nativeObjectType",
        "value": "groupOfNames" },
      { "op": "replace",
        "path": "/configuration/groupMemberAttribute",
        "value": "member"  } ]'
```

6. エンタイトルメントのアグリゲーションを行う。グループがエンタイトルメントとして収集される。

7. アカウントのアグリゲーションを行う。アカウントとエンタイトルメント保有状況が収集される。

5.2 ユーザーエントリの複数値属性の値をIceWallグループに対応させる方式

- **方式概要**
  ユーザーエントリの一つの属性が持つ複数の値がそれぞれIceWallのグループと対応するようにします。
  IdentityNowでは、値がそれぞれエンタイトルメントであると扱います



- **設定方法**
  IceWallでは、認証DBカラム情報ファイル（dbattr.conf）にてグループ標示の複数値属性を読み込むよう設定し、グループ設定ファイル（cert.grp）にて、それぞれの値だけにマッチするよう判定正規表現を記述します。

- dbattr.conf の設定例

```
IWGROUPS=iwGroups
```

- cert.grp の設定例

```
TokyoG,IWGROUPS="^TokyoGr$"
OsakaG,IWGROUPS="^OsakaGr$"
SalesG,IWGROUPS="^SalesGr$"
TechG,IWGROUPS="^TechGr$"
```

IdentityNowでは、ユーザーエントリのグループ標示属性の値をエンタイトルメントとして扱うようソースを構成します。

1. ソースタイプに「OpenLDAP」を選択して新規ソースを作成し、環境に合わせて接続設定を行う。
2. 「アカウントおよびグループ設定」にて、以下の通り設定する。

設定項目	説明

設定項目	説明
アカウント設定	
検索識別名	ユーザーエントリを検索する際のベースDN。
LDAP検索フィルター	ユーザーエントリを検索する際のフィルター。 例：(objectclass=inetOrgPerson)

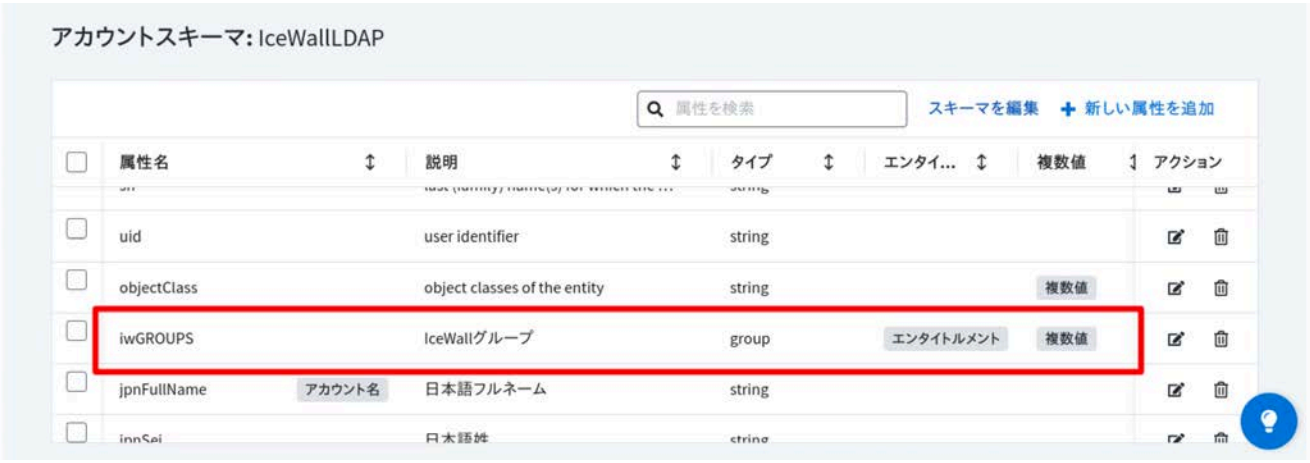
グループ関連の項目は設定しない。

3. 接続をテストする。

4. 「アカウントスキーマ」と「関連付け」を環境に合わせて適切に設定する。アカウントスキーマには、グループ標示属性を以下の通り追加する。

設定項目	説明
名前	グループ標示属性名
タイプ	「group」を選択
エンタイトルメント	チェックする
複数値	チェックする

設定すると、次のようにアカウントスキーマ画面に表示される。

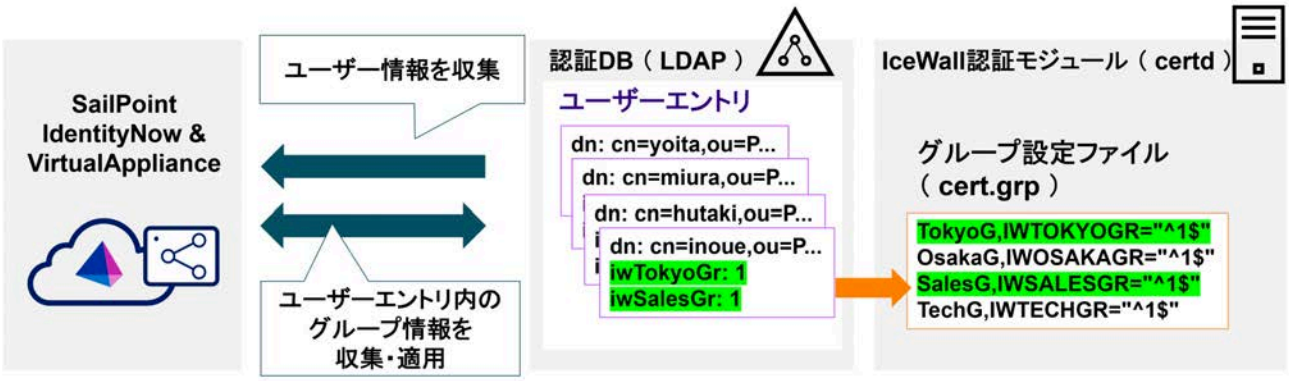


5. アカウントのアグリゲーションを行う。アカウント情報とエンタイトルメント保有情報が同時に収集される。

- エンタイトルメント情報

- アカウントのエンタイトルメント保有状況

5.3 ユーザーエントリにIceWallグループに個別に対応する複数の属性を持たせる方式



- **方式概要**
  IceWallのグループそれぞれに対応する単数値属性をユーザーエントリに持たせます。各属性は真偽を

表す値を採り、値が真の場合にグループに所属すると判定します。IdentityNow では、それぞれの属性で値が真の場合をエンタイトルメントとして扱います。

- **設定方法**
  IceWallでは、認証DBカラム情報ファイル（ dbattr.conf ）にて全てのグループ標示の属性を読み込むよう設定し、グループ設定ファイル（ cert.grp ）にて、各属性の真値にマッチするよう判定正規表現を記述します。

- dbattr.conf の設定例

```
IWTOKYOGR=iwTokyoGr
IWOSAKAGR=iwOsakaGr
IWSALSEGR=iwSalesGr
IWTECHGR=iwTechGr
```

- cert.grp の設定例

```
TokyoG,IWTOKYOGR="^1$"
OsakaG,IWOSAKAGR="^1$"
SalesG,IWSALESGR="^1$"
TechG,IWTECHGR="^1$"
```

IdentityNowでは、ユーザーエントリの全てのグループ標示属性をエンタイトルメントとして扱うようソースを構成します。

1. ソースタイプに「OpenLDAP」を選択して新規ソースを作成し、環境に合わせて接続設定を行う。
2. 「アカウントおよびグループ設定」にて、以下の通り設定する。

設定項目	説明
アカウント設定	
検索識別名	ユーザーエントリを検索する際のベースDN。
LDAP検索フィルター	ユーザーエントリを検索する際のフィルター。 例：(objectclass=inetOrgPerson)

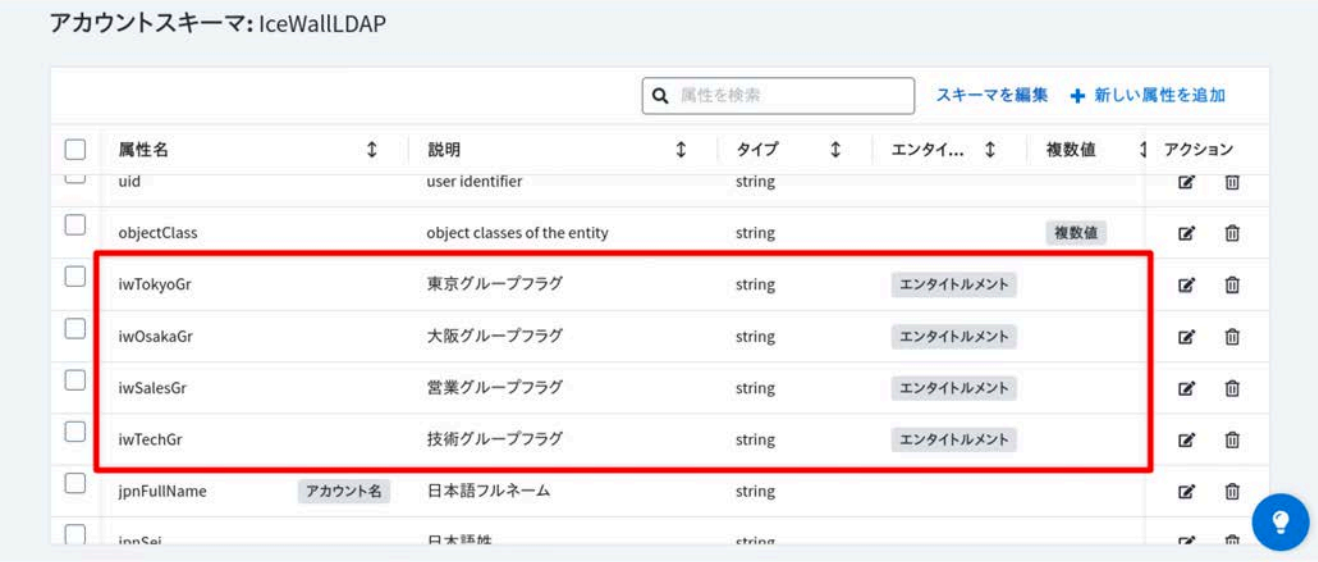
グループ関連の項目は設定しない。

3. 接続をテストする

4. 「アカウントスキーマ」と「関連付け」を環境に合わせて適切に設定する。アカウントスキーマには、全てのグループ標示属性を以下の通り追加する。

設定項目	説明
名前	グループ標示属性名
タイプ	「string」を選択
エンタイトルメント	チェックする
複数値	チェックしない

設定すると、次のようにアカウントスキーマ画面に表示される。



- 5. アカウントのアグリゲーションを行う。アカウント情報とエンタイトルメント保有情報が同時に収集される。ただし、エンタイトルメント一覧画面では、属性値で表示されるため次のような表示になる

6. 各エンタイトルメントに分かりやすい名前と説明文を設定する。これは管理画面で直接設定することは出来ず、CSVに記述してアップロードする必要がある。
まず、エンタイトルメント一覧画面のCSVダウンロードボタンを押してテンプレートCSVをダウンロードする。

7. テンプレートCSVのdisplayNameおよびdescriptionに表示名と説明を記述する。

- エンタイトルメントCSVの設定例

```
attributeName,attributeValue,displayName,description,privileged,schema
iwOsakaGr,1,OsakaGr,大阪グループ,false,Entitlement
iwTokyoGr,1,TokyoGr,東京グループ,false,Entitlement
iwTechGr,1,TechGr,技術グループ,false,Entitlement
iwSalesGr,1,SalesGr,営業グループ,false,Entitlement
```

8. エンタイトルメント一覧画面のCSVアップロードボタンを押して変更したCSVをアップロードする。
数秒待ってから画面をリロードすると表示に反映される。

- エンタイトルメント情報

- アカウントのエンタイトルメント保有状況

6. さいごに

昨今、セキュリティの脅威はますます増大しており、ゼロトラストや最小権限の原則の実現が強く求められています。
一方で情報システムの多様さ複雑さは増すばかりであり、少数の担当者が情報システムの適切な権限を手動で維持することはもはや不可能です。

今回ご紹介しました SailPoint IdentityNow は、多数のクラウド・オンプレミスシステムのユーザー権限を集中管理し、それらを適切な状態に保つための多くの作業を自動化します。ゼロトラスト実現の一歩として検討されてみてはいかがでしょうか。

2022.10.31　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

技術レポート一覧へ →

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)