



ID プロバイダーの SAML の要件

- [概要 \(1 ページ\)](#)
- [SAML 応答の要件 \(1 ページ\)](#)
- [SAML メタデータの要件 \(2 ページ\)](#)

概要

IdP から Security Cloud Sign On への SAML 応答は、[SAML 応答の要件 \(1 ページ\)](#) で説明されているいくつかのルールに従う必要があります。

また、[SAML メタデータの要件](#)を IdP から取得する必要があります。

SAML 応答の要件

SAML 応答の属性

IdP によって送信される SAML 応答のアサーションには、次の属性名が含まれている必要があります、IdP の対応する属性にマッピングされている必要があります。

SAML アサーション属性名	IdP ユーザー属性
firstName	ユーザーの名。
lastName	ユーザーの姓。
email	ユーザーの電子メール。これは、SAML 応答の <NameID> 要素と一致する必要があります。

たとえば、次の XML スニペットは、Security Cloud Sign On ACL URL への SAML 応答に含まれる <AttributeStatement> 要素の例です。

```
<saml2:AttributeStatement>  
  <saml2:Attribute Name="firstName"
```

```

NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml2:AttributeValue
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">John

  </saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="lastName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml2:AttributeValue
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">Doe

  </saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml2:AttributeValue
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">jdoe@example.com
  </saml2:AttributeValue>
</saml2:Attribute>
</saml2:AttributeStatement>

```

NameID 要素

IdP からの SAML 応答の **<NameID>** 要素には、その値として有効な電子メールアドレスが含まれている必要があります、電子メールは [SAML 応答の属性 \(1 ページ\)](#) の **email** 属性の値と一致する必要があります。

<NameID> の **Format** 属性は、**urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified** または **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress** に設定されている必要があります。

<NameID> 要素の例を次に示します。

```

<saml2:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">jdoe@example.com</saml2:NameID>

```

SAML メタデータの要件

Security Cloud Sign On と統合するには、IdP の SAML アプリケーションの次のメタデータが必要です。

- **シングルサインオンサービスの初期 URL** – これは「SSO URL」または「ログイン URL」と呼ばれることもあります。この URL を使用して、IdP から Security Cloud Sign On への認証を開始できます。
- **エンティティ ID URI** – IdP のグローバルな一意の名前。これは「発行元」と呼ばれることもあります。
- **X.509 署名証明書** – IdP が SAML アサーションに署名するために使用する公開キー/秘密キーのペアの公開キー。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。