Hewlett Packard Enterprise

# HPE iLO セキュア オンボーディング


## 動画タイトル

HPE iLO Secure Onboarding

## 元動画

https://www.youtube.com/watch?v=5U4tzKJZPuc

## 目的

本資料のみ参照で、あるいは動画視聴と併用していただいて、動画の内容をわかりやすくご理解いただけます。

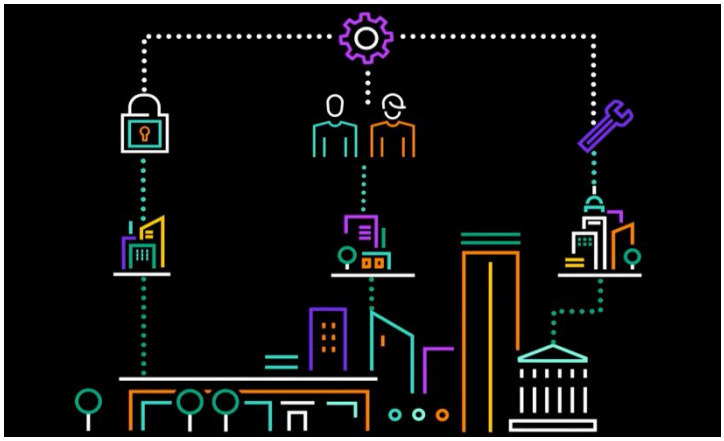
本資料には、以下のコンテンツが含まれます。

- ネットワークオンボーディングの背景
- IEEE 802.1X とは何か
- iLO と IEEE 802.1X 認証
- セキュア DevID の概要と使用時の前提条件
- IDevID の概要とオンボード方法
- LDevID の概要とオンボード方法

# ネットワークオンボーディングの背景


**背景 (1) (▶ 0:02)**

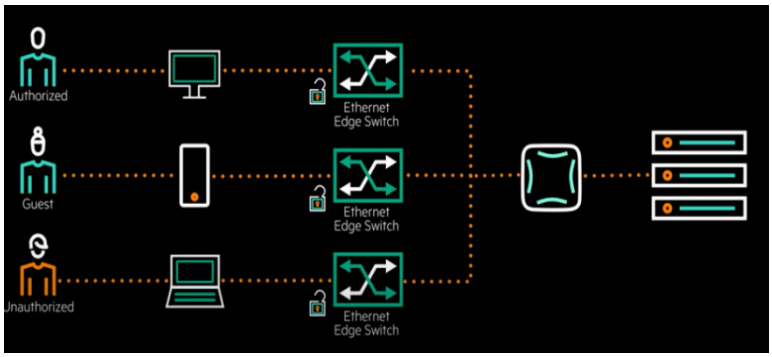
この動画では、ネットワークへセキュアにオンボーディングするための IEEE 802.1X と HPE iLO DevID の使用方法を説明しています。



**背景 (2)**
**リモート拠点にオフィスを持つ企業が抱える 3 つの課題 (▶ 0:13)**

1. データセキュリティのリスク
2. 各拠点に知識やノウハウを持つエンジニアを配置できない
3. 各拠点のサーバー管理

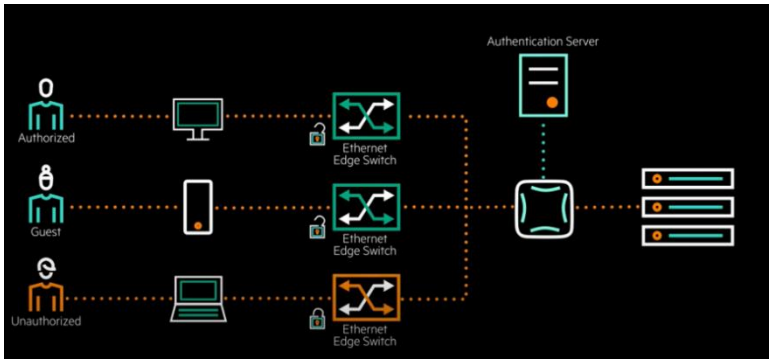
これらの課題の解決策として**「自動化」**が採用されています。




**背景 (3)**
**セキュアでないネットワークの図 (▶ 0:29)**

認証局がないため、誰がネットワークにアクセスしたかの情報が分かりません。

**問題**: 認証されていないユーザーがネットワークにアクセスし、情報を盗めてしまいます。




**背景 (4)**
**IEEE 802.1X 認証を採用したネットワークの図 (▶ 0:45)**

スイッチが認証局の役割を果たします。

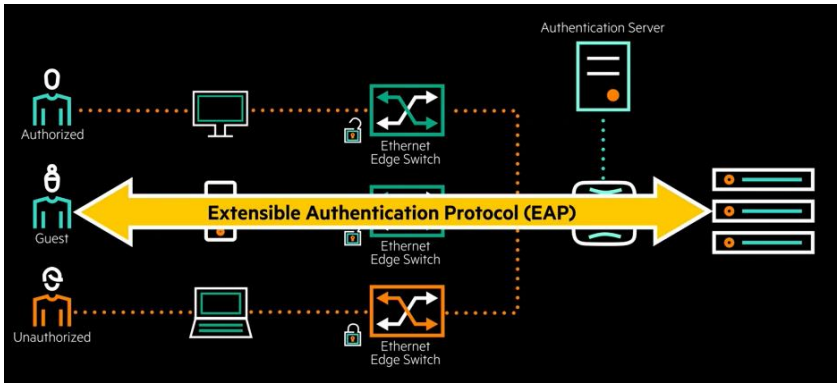
ユーザーはネットワークの認証を行い、承認されればローカルスイッチがアクセスを許可します。

# IEEE802.X とは何か？


**IEEE 802.1X とは？ (1) (▶ 1:04)**

ネットワークセキュリティでよく使用されている認証メカニズムです。

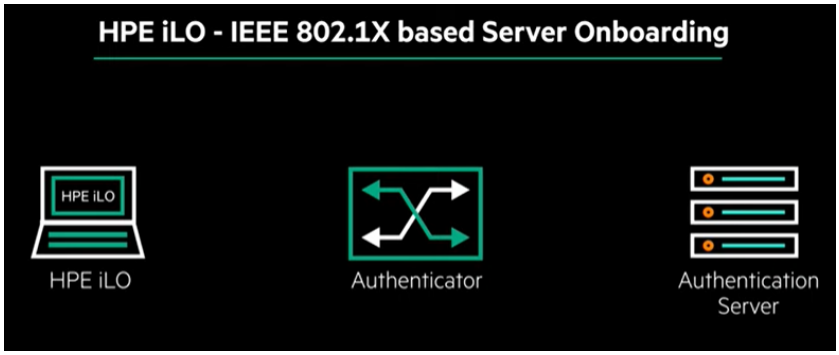
ポートベースネットワークアクセス制御のオープンスタンダードが存在し、これが NN ノードのネットワークへのアクセスを制御可能にします。




**IEEE 802.1X とは？ (2) (▶ 1:17)**

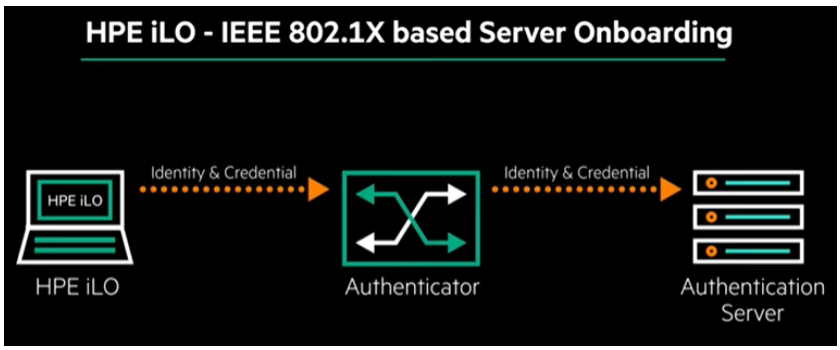
IEEE 802.1X は、認証プロセスのやりとりの際に EAP (Extensive Authentication Protocol) というプロトコルを使用します。

# iLO と IEEE 802.1X の認証




**(▶ 1:28)**

HPE iLO はネットワークアクセス認証と承認を可能にする IEEE 802.1X プロトコルに対応しました。

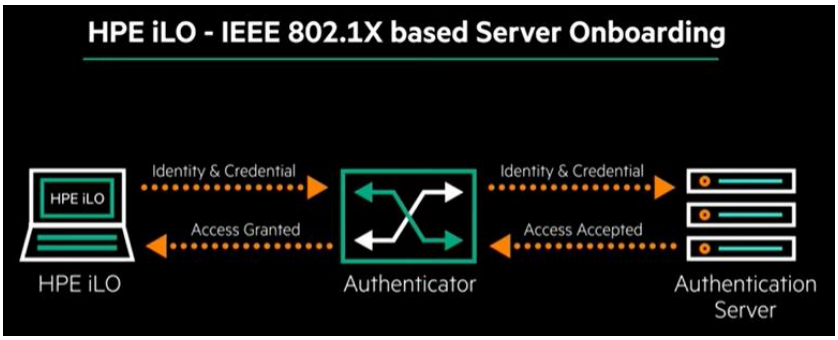



**iLO と IEEE 802.1X の認証プロセス (1)**
**(▶ 1:35)**

ローカルスイッチが iLO に対してネットワークへのアクセスを許可する前に、iLO は認証を行わなければなりません。

デバイスはスイッチと物理的にリンクされていますが、スイッチは iLO から受け取った EAP フレームのみを認証サーバーに送信します。

認証装置は iLO から受け取った EAP フレームを再パッケージ化し、認証サーバーへ送りつけます。



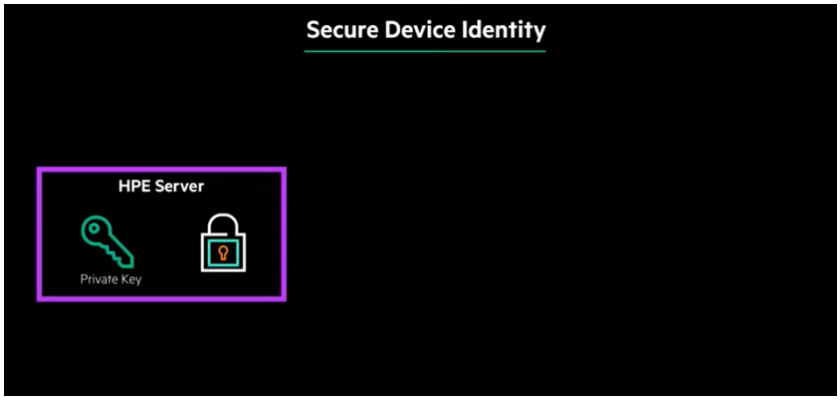

**iLO と IEEE 802.1X の認証プロセス (2)**
**(▶ 1:53)**

認証サーバーは iLO から送られたフレームを検証し、正常であればアクセスを許可します。

身元を証明するため、IEEE 802.1X プロトコルは「セキュア DevID」を使用します。

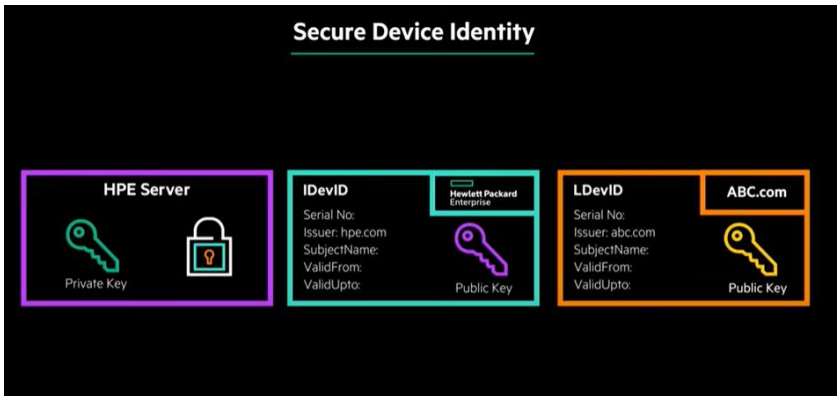
「セキュア DevID」は、相互運用可能なデバイス認証クレデンシャルとして使用されます。

# セキュア DevID の概要と使用時の前提条件




**セキュア DevID 概要 (1) (▶ 2:11)**

HPE iLO を搭載しているサーバーであれば、各サーバー固有な「セキュア DevID」を持っています。

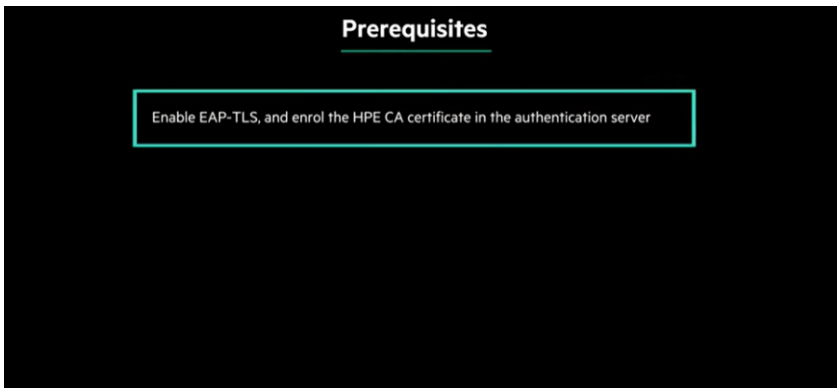



**セキュア DevID 概要 (2) (▶ 2:16)**

HPE サーバーは IDevID と LDevID もサポートしています。

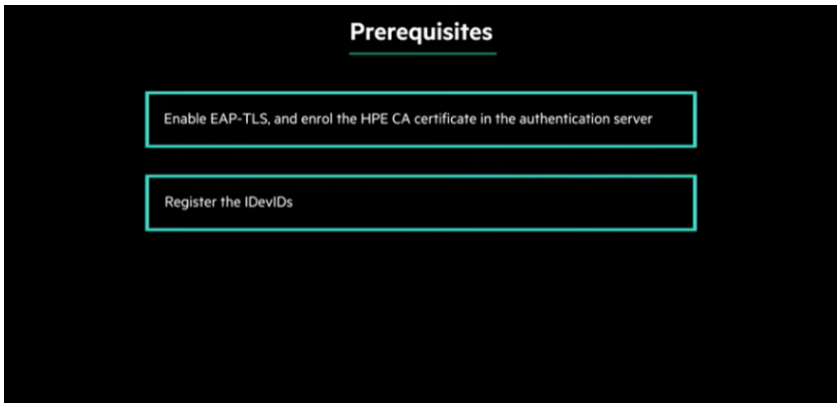
HPE iLO IDevID と HPE iLO LDevID の認証を使用するにはネットワーク上で IEEE 802.1X プロトコルを有効にしていなければなりません。

## 前提条件



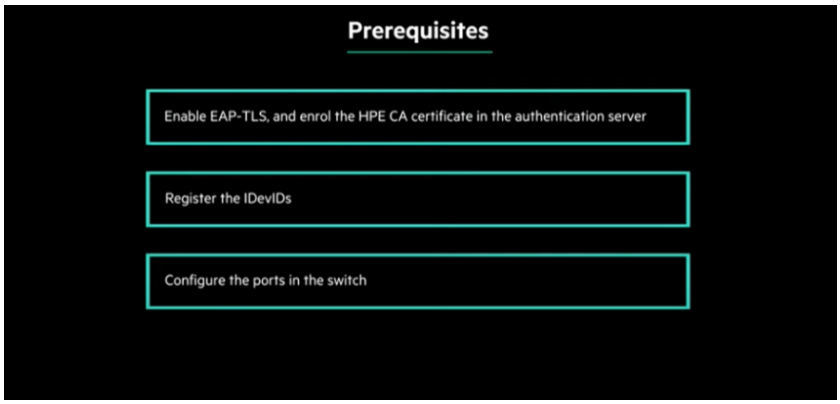

**(▶ 2:30)**

1. ネットワーク上で IEEE 802.1X が有効化されていれば、EAP-TLS も有効化
2. 認証サーバーに HPE CA 証明書を登録




**(▶ 2:39)**

3. IDevID を登録

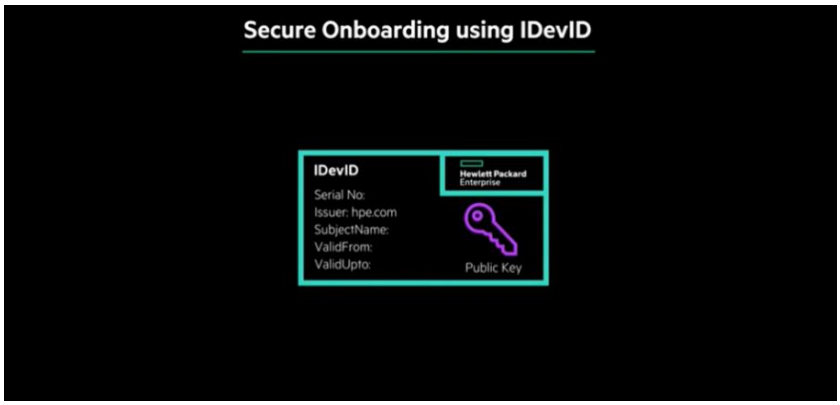



**(▶ 2:41)**

4. スイッチのポートを構成

これより、IEEE 802.1X がネットワーク上で有効化されたため、HPE iLO をセキュアにオンボードできます。

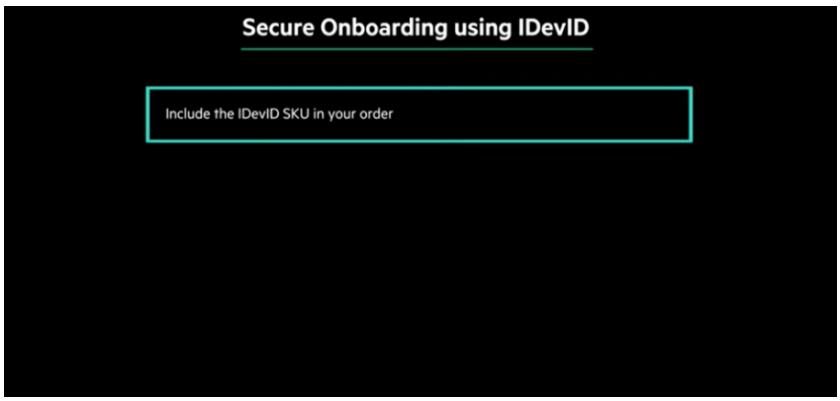
# IDevID の概要とオンボード方法




**IDevID の概要 (▶ 2:51)**

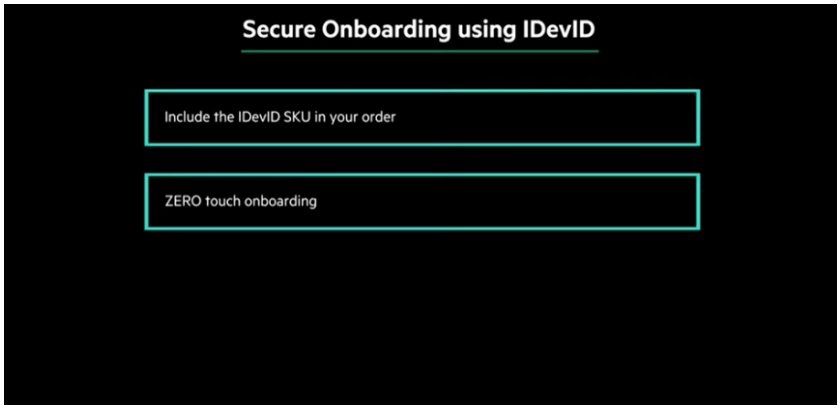
HPE iLO の IDevID は工場で組み込まれ、HPE によって正式にサインされます。

IDevID は無期限で使用でき、変更などを加えることはできません。




**IDevID のオンボード (1) (▶ 3:01)**

製品注文の際、「IDEV SKU 番号」を含める必要があります。
これを行うことにより、HPE の工場でお客様のサーバーに IDevID を組み込みます。

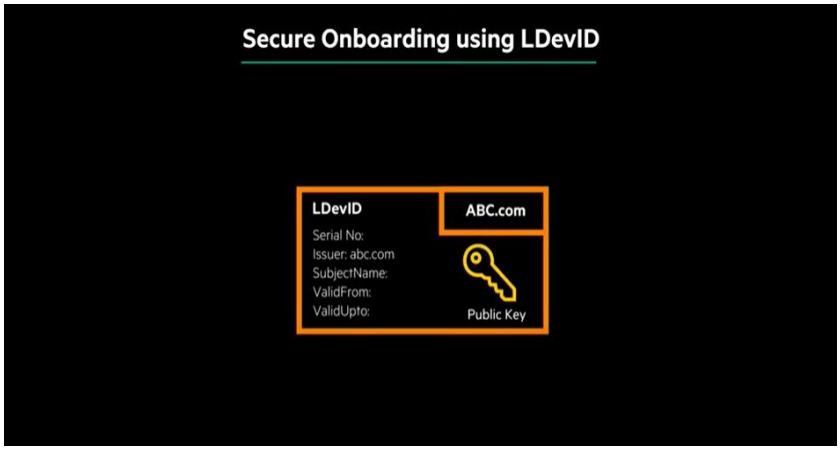



**IDevID のオンボード (2) (▶ 3:07)**

サーバーを起動する際、HPE iLO は IEEE 802.1X EAP-TLS 認証を使用し、「ゼロタッチ」でネットワークへの接続を確立します。

これで IDevID によるセキュアオンボーディングは完了です。

# LDevID の概要とオンボード方法

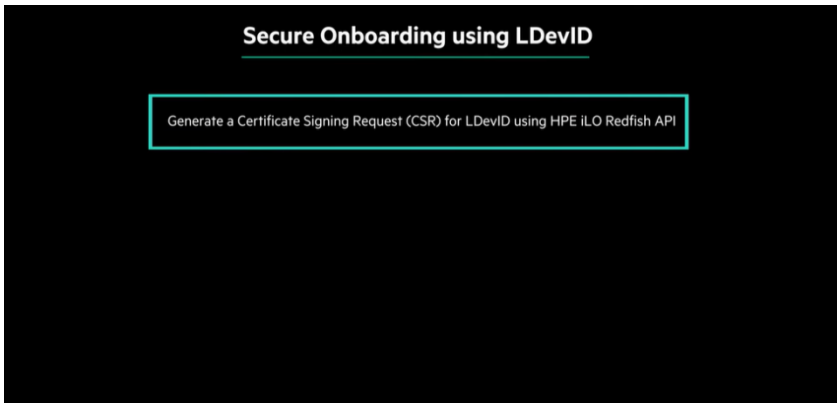



**LDevID の概要 (▶ 3:19)**

LDevID ではユーザがサーバーのアイデンティティを定義できます。

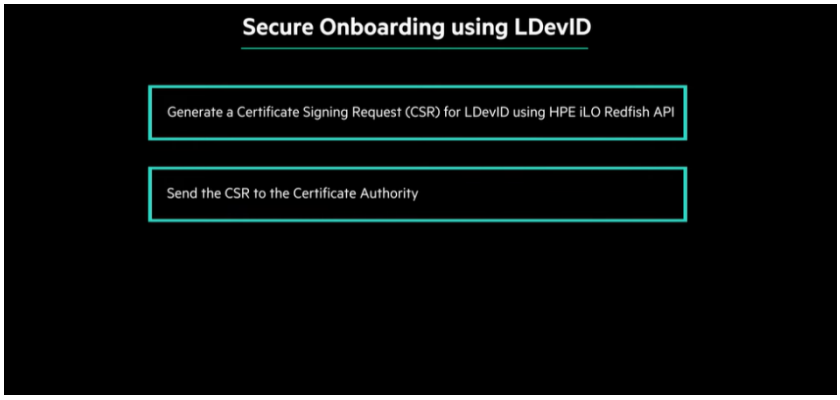
サーバーが使用されている管理ドメインごとにユニークなものを持ちます。

LDevID は認証の促進と、ローカルネットワーク管理者によるクレデンシャルの承認を補助します。



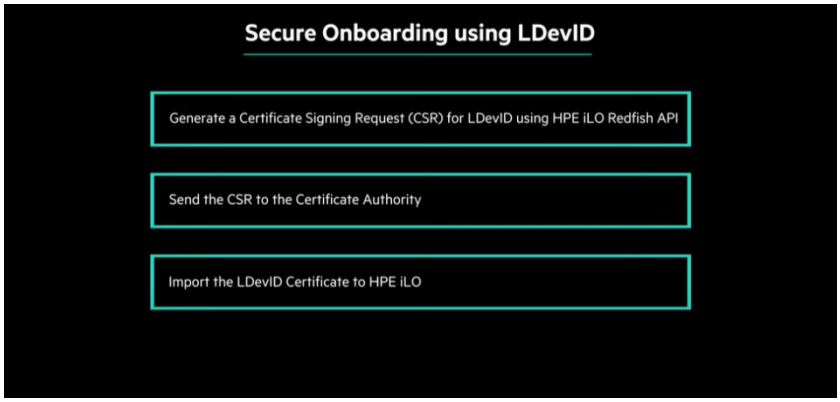

**LDevID のオンボード (1) (▶ 3:34)**

LDevID を作成、インポートするには、Redfish API を使って CSR (Certificate Signing Request) を生成します。




**LDevID のオンボード (2) (▶ 3:41)**

CSR を証明書機関に送ります。




**LDevID の**
**オンボード (3)**
**(▶ 3:44)**

LDevID の証明書を iLO にインポートします。

インポートが完了すると、IEEE 802.1X が有効なネットワーク上で iLO は LDevID 認証を使用します。

これで LDevID のオンボードは完了です。

以上