

## HPE iLO セキュア オンボーディング

IEEE 802.1X and DevID based Server Onboarding

HPE ILO SECURE ONBOARDING

## 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



IEEE 802.1X and DevID based Server Onboardin

### 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。





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。



# HPE Server Virvate Key

## 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。

	Secure Devi	ce Identity		
HDE Server	IDevID			APC com
Private Key	Serial No: Issuer: hpe.com SubjectName: ValidFrom: ValidUpto:	Hewlett Packard Enterprise	Serial No: Issuer: abc.com SubjectName: ValidFrom: ValidUpto:	Public Key

## 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

Prerequisites
Enable EAP-TLS, and enrol the HPE CA certificate in the authentication server

### (▶ 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

Enable EAP-TLS, and enrol the HPE CA certificate in the authentication server Register the IDevIDs	Enable EAP-TLS, and enrol the HPE CA certificate in the authentication server Register the IDevIDs	Prerequisites
Register the IDevIDs	Register the IDevIDs	Enable EAP-TLS, and enrol the HPE CA certificate in the authentication server
Register the IDevIDs	Register the IDevIDs	
		Register the IDevIDs

# (▶ 2:39)

3. IDevID を登録

	Prerequisites	
	Enable EAP-TLS, and enrol the HPE CA certificate in the authentication server	
	Register the IDevIDs	
Γ	Configure the ports in the switch	

#### (▶ 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 はエ 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。

Secure Onboarding using IDevID	
Include the IDevID SKU in your order	

#### 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。

Secure Onboarding using IDevID	
Include the IDevID SKU in your order	
ZERO touch onboarding	
	•

#### 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 ABC.com	ABC.com	LDevID
Serial No:		Serial No:
SubjectName:	<u>ور</u>	SubjectName:
ValidFrom:	<u>v</u>	ValidFrom:
ValidOpic. Public Key	Public Key	validopio.

### 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。

Secure Onboarding using LDevID	LDevID のオンボード (1) (► 3:34)
Generate a Certificate Signing Request (CSR) for LDevID using HPE iLO Redfish API	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。

Generate a Certificate Signing Request (CSR) for LDevID using HPE iLO Redfish API いたいのでのようには、そのことのでは、そのことのいいいいいいいいいいいいいいいいいいいいいいいい	Generate a Certificate Signing Request (CSR) for LDevID using HPE iLO Redfish API いたいのでは、 Send the CSR to the Certificate Authority	Generate a Certificate Signing Request (CSR) for LDevID using HPE iLO Redfish API CSS しま	Generate a Certificate Signing Request (CSR) for LDevID using HPE iLO Redfish API いたいのでは Send the CSR to the Certificate Authority	Generate a Certificate Signing Request (CSR) for LDevID using HPE iLO Redfish API Send the CSR to the Certificate Authority	Secure Onboarding using LDevID	LDe (► 3:
らしていていていていていていていていていていていていていていていていていていてい	りま	りま	りま	りま	Generate a Certificate Signing Request (CSR) for LDevID using HPE iLO Redfish API	CSF
Send the CSR to the Certificate Authority	Send the CSR to the Certificate Authority	Send the CSR to the Certificate Authority	Send the CSR to the Certificate Authority	Send the CSR to the Certificate Authority		りま
					Send the CSR to the Certificate Authority	

**.DevID のオンボード (2)** ▶ 3:41) CSR を証明書機関に送 Jます。



Secure Onboarding using LDevID	LDevID の オンボード (3) (► 3:44)
Send the CSR to the Certificate Authority	LDevID の証明書を iLO にインポートします。
Import the LDevID Certificate to HPE iLO	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

