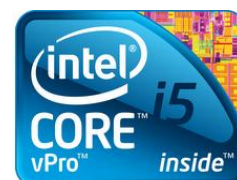


(参考資料としての利用に限る)

Intel vPro テクノロジー対応 SSL 証明書インストールについて



1. はじめに

vPro クライアントと Setup and Configuration Service (SCS) との間において以下のような手順で、vPro の設定情報を行うまえに**セキュアな通信路を確立**します。その際にスターフィールドなどの Intel 社が認めた商用認証局 (CA) が発行した SSL 証明書が使用されています。

- (ア) vPro クライアントの管理エンジン (Management Engine: ME) は DNS サーバーに Provisionserver に Lookup を行います。
- (イ) その結果に従って vPro クライアントの ME が Provisionserver の IP アドレスに IP ポート 9971 を使用してリモート構成の Hello メッセージを送信します。
- (ウ) Provisionserver はスターフィールド CA から発行されたルート証明書を含んだリモート構成用 SSL 証明書を vPro クライアントの ME に送信します。
- (エ) vPro クライアントの ME は SSL 証明書の妥当性をチェックします。SSL 証明書からルート証明書を抽出しそのハッシュ値を計算します。それが自分の持つ証明書のハッシュ値のリストと照合します。
- (オ) 証明書が OID(1.3.6.1.5.5.7.3.1,2.16.840.1.113741.1.2.3:SSL サーバー証明書とインテルリモート構成を示す OID)あるいは OU(Intel(R) Client Setup Certificate) が指定されたもので、ハッシュ値があえば、vPro クライアントの ME は非対称鍵のペアを生成し、その公開鍵を自己署名証明書にに入れて送り返します。
- (カ) サーバーは TLS セッションキーを受け取った公開鍵で暗号化し、vPro クライアントの ME に送ります。
- (キ) これで TLS 接続が確立されます。

その後、vPro の構成情報を Provisionserver から vPro クライアントの ME に送信します。

2. シングルドメイン証明書を使用した場合

(ア) 仮想サーバー1:

jcert.info ドメインコントローラー、DNS、DHCP:

- Windows Server 2003 R2

(イ) 仮想サーバー2:

vPro 構成サーバー (Intel Setup and Configuration Service):

- Windows Server 2003 R2
- FQDN: scs.jcert.info
- DNS alias: provisionserver.jcert.info
- スターフィールド SSL 証明書:

CN=scs.jcert.info

OU=Intel(R) Client Setup Certificate

(ウ) L3 イーサネット・スイッチ:

192.168.90.0/24 を VLAN 90 に割り当て外部ネットワークとルーティング

(エ) vPro クライアント: HP2530p AMT 4.1.1 クライアント

以上の環境で vPro クライアントが jcert.info ドメインで正常に構成されたことを確認されております。

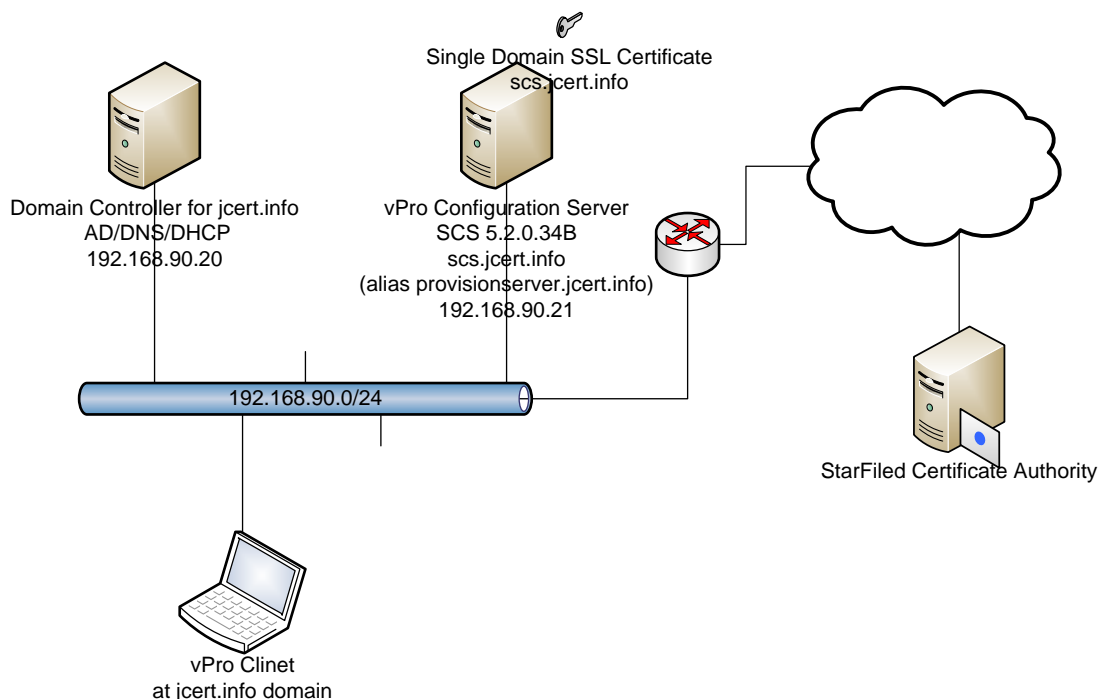


図 1 シングルドメイン環境

3. マルチドメイン証明書を使用した場合

(ア) 仮想サーバー1:

jcet.info ドメインコントローラー、DNS、DHCP:

- Windows Server 2003 R2

(イ) 仮想サーバー2:

vPro 構成サーバー (Intel Setup and Configuration Service):

- Windows Server 2003 R2
- FQDN: scs.jcet.info
- DNS alias: provisionserver.jcet.info
- スターフィールド SSL 証明書:
CN=scs.jcet.info
OU=Intel(R) Client Setup Certificate
DNS alias: eng.jcet.info, mktg.jcet.info

(ウ) 仮想サーバー3:

mktg.jcet.info ドメインコントローラー、DHCP リレー (仮想サーバー1へ
DHCP 要求をリレー):

- Windows Server 2003 R2

(エ) L3 イーサネット・スイッチ: 192.168.90.0/24 を VLAN 90 に 192.168.91.0/24 を VLAN 91 に割り当て外部ネットワークとルーティング

(オ) vPro クライアント: HP2530p AMT 4.1.1 クライアント

vPro クライアントがドメイン jcet.info (サブネット 192.168.90.0) 及び
mktg.jcet.info (サブネット 192.168.91.0) のそれぞれで正常に構成されたことが確
認されました。

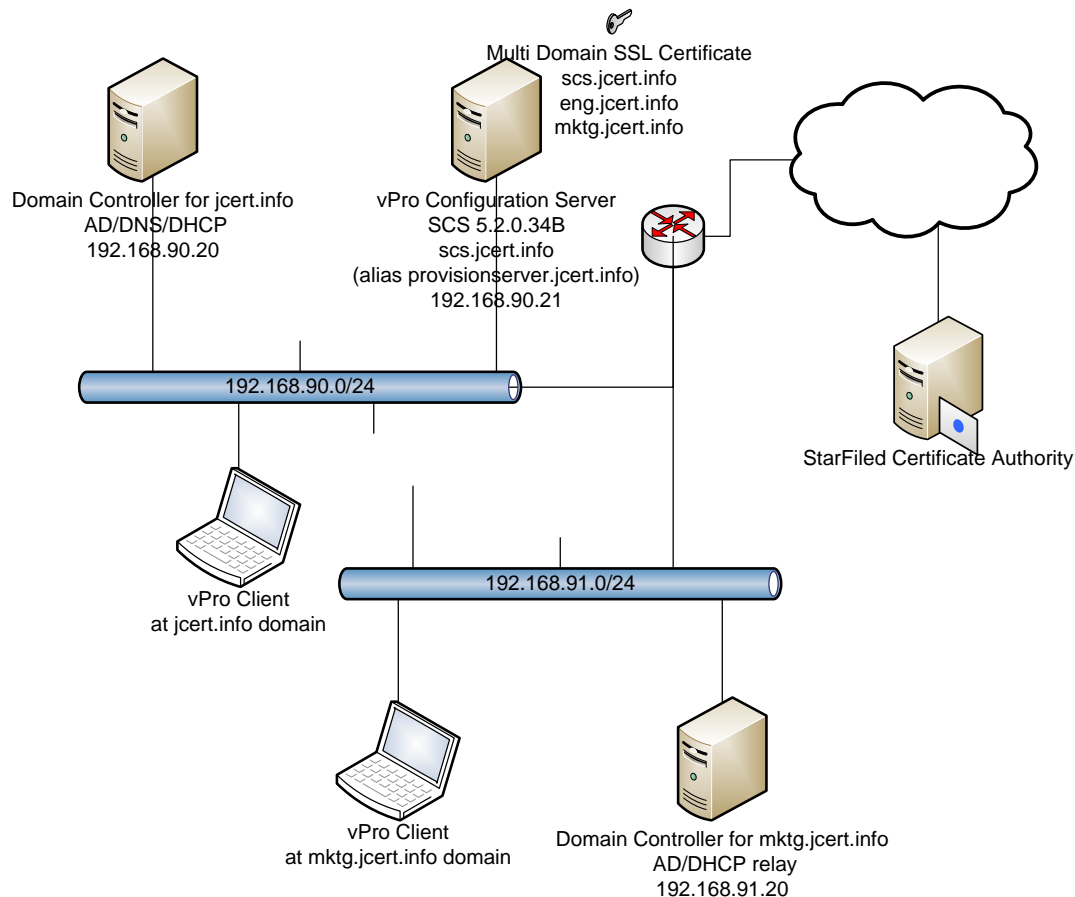


図 2 サブドメインを含んだ環境(マルチドメイン証明書)

4. ワイルドカードドメイン証明書を使用した場合

(ア) 仮想サーバー1:

jcert.info ドメインコントローラー、DNS、DHCP:

- Windows Server 2003 R2

(イ) 仮想サーバー2:

vPro 構成サーバー (Intel Setup and Configuration Service):

- Windows Server 2003 R2
- FQDN: scs.jcert.info
- DNS alias: provisionserver.jcert.info
- スターフィールド SSL 証明書:

CN= *.jcert.info

OU=Intel(R) Client Setup Certificate

(ウ)仮想サーバー3:

mtkg.jcert.info ドメインコントローラー、DHCP リレー(仮想サーバー1へ
DHCP 要求をリレー):

- Windows Server 2003 R2

(エ)L3 イーサネット・スイッチ:192.168.90.0/24 を VLAN 90 に 192.168.91.0/24
を VLAN 91 に割り当てて外部ネットワークとルーティング

(オ)vPro クライアント:HP2530p AMT 4.1.1 クライアント

vPro クライアントがドメイン jcert.info(サブネット 192.168.90.0)及び
mtkg.jcert.info(サブネット 192.168.91.0)のそれぞれで正常に構成されたことが確
認されました。

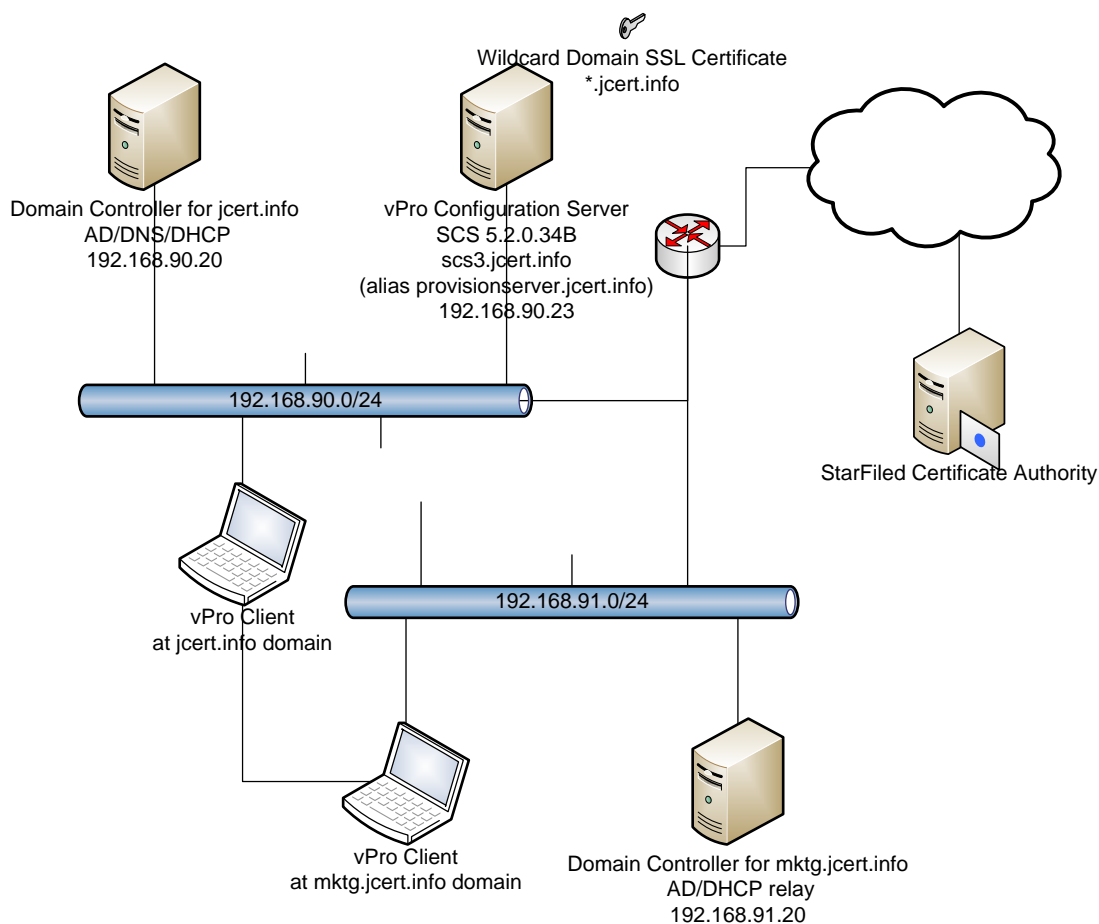


図 3 サブドメインを含んだ環境(ワイルドカード証明書)