サーバの冗長化など，同一FQDNの複数サーバで証明書を利用する場合はどうすればよいですか

問題

サーバの冗長化など，同一FQDNの複数サーバで証明書を利用する場合はどうすればよいですか。

解決方法

以下の方法いずれかで可能です。
2022年7月26日にサーバ証明書のOUが廃止されるため、対応に変更点があります。

2022年7月26日までの解決方法

1. 同一FQDNであれば，発行された1枚のサーバ証明書を，必要とする複数の機器にコピーしてご利用いただくことができます。
   これは，同一FQDNのサーバを使用するケースの多くは負荷分散のためであり，負荷分散装置配下に並列設置されるサーバの鍵ペア漏洩リスクは同等とみなせるためです。
   従って，同一FQDNのサーバであるものの，設置場所が異なるなど鍵ペア漏洩リスクが異なる場合には，下記2.，3.の方法で対応いただくことを推奨します。

2. サーバ毎にCSRを作成し，各サーバに証明書を発行する方法でも対応可能です。次の点に留意して，CSRを作成してください。
   1. Common Name（コモンネーム, CN）は同一にする。
   2. Organizational Unit Name（組織部門, OU）は，最後に1，2，3等の数字をつける等，各サーバ毎に名称を変更する。
   ※これは証明書を一意にするために行っていただくものです。

3. 2と同様ですが，各サーバに個別のFQDNも割り当てられている場合，下記の方法でも対応可能です。
   次の点に留意して，CSRを作成してください。
   1. Common Name（コモンネーム, CN）は個別のFQDNにする。
   2. Organizational Unit Name（組織部門, OU）は、各サーバで同一で結構です。
   3. dNSNameに共通のFQDNを指定する。

2022年7月26日以降の解決方法（OU廃止後）

1. 同一FQDNであれば，発行された1枚のサーバ証明書を，必要とする複数の機器にコピーしてご利用いただくことができます。
   これは，同一FQDNのサーバを使用するケースの多くは負荷分散のためであり，負荷分散装置配下に並列設置されるサーバの鍵ペア漏洩リスクは同等とみなせるためです。
   従って，同一FQDNのサーバであるものの，設置場所が異なるなど鍵ペア漏洩リスクが異なる場合には，下記2. の方法で対応いただくことを推奨します。

2. 各サーバに個別のFQDNも割り当てられている場合，下記の方法でも対応可能です。
   次の点に留意して，CSRを作成してください。
   1. Common Name（コモンネーム, CN）は個別のFQDNにする。
   2. dNSNameに共通のFQDNを指定する。

   例：1枚目の主体者DN ” CN=certs1.nii.ac.jp, O=NII, L=Chiyoda-ku,ST=Tokyo,C=JP"
   2枚目の主体者DN ” CN=certs2.nii.ac.jp, O=NII, L=Chiyoda-ku,ST=Tokyo,C=JP"
   1枚目のSANsの値 "dNSName=certs1.nii.ac.jp, dNSName=certs.nii.ac.jp"
   2枚目のSANsの値 "dNSName=certs2.nii.ac.jp, dNSName=certs.nii.ac.jp"

関連記事

- IISにてOUなしのRSA用のCSR作成手順
- サーバの冗長化など，同一FQDNの複数サーバで証明書を利用する場合はどうすればよいですか
- 証明書更新発行申請時のCSRや鍵ペアの再利用について
- FQDNがIPアドレスの証明書を発行することができますか
- CSR作成時に特別な規則はありますか