仮想サーバを利用している場合， またその他の方法で同一計算機上で複数のサーバを運用している場合， サーバ証明書は（仮想）サーバの数だけ必要になるか

問題

VirtualHostやVMwareなどの仮想サーバを利用している場合， またその他の方法で同一計算機上で複数のサーバを運用している場合， サーバ証明書は仮想サーバの数だけ必要になるのか知りたい。

解決方法

VMwareやXenなど，同一計算機で複数の仮想環境（ゲストOS）を使用している場合

少なくとも仮想環境（ゲストOS）毎に，サーバ証明書の申請が必要です。

バーチャルホスト機能など，同一計算機・同一OSでホスト名が異なる複数のサーバを使用している場合

1枚のサーバ証明書で対応が可能です。
発行申請TSVファイルの「dNSName」の欄に，「利用管理者FQDN」に記入したホスト名以外のホスト名を
「dNSName=xxx2.example.ac.jp,dNSName=xxx3.example.ac.jp」
のように列挙して入力してください。
（各ホスト名の前に「dNSName=」を付けるのを忘れないようにしてください）
証明書上はsubjectAltName拡張にホスト名が記載されます。

その他，dNSName欄に関する制約は，発行申請TSVファイルフォーマットをご参照ください。

▶発行申請TSVファイルフォーマット

上記の通り，CSRには追加ホスト名について何ら記載する必要はありません。
また，証明書に記載できるホスト名は合計8件まで（利用管理者FQDNを除いて7件）となっておりますのでご注意ください。
記載できる文字数にも上限があります。

なお，この方法で追加されたホスト名に携帯電話・スマートフォンでアクセスした場合，一部機種では警告が表示されることが確認されております。
詳しくは情報交換ML:42以降の報告をご参照ください。

▶情報交換ML:42

同一計算機同一ホスト名ながら異なるポート番号で複数のサーバを使用している場合

（例えば80番ポートで動作するWebサーバと8000番ポートで動作するSSL-VPNサーバなど）
どちらも同じサーバ管理者の責任下で運用されていることになりますので，サーバ証明書は1つで構いません。
ただし，サーバ秘密鍵が漏洩しないよう，サーバ管理者の責任の下で厳格に管理することが前提です。
特に各サーバで異なるパスに秘密鍵を保管する場合には，秘密鍵ファイルのアクセス権の設定などに十分ご注意ください。
（例えばどちらか一方の秘密鍵ファイルだけでも管理者・サーバプロセス以外が読み取れる設定などになっていると秘密鍵が漏洩する可能性があります）

同一FQDNであっても冗長化構成などによって物理的に異なる複数のサーバを利用する場合は次のFAQも参照ください。

▶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

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