レポート２

複数のルートCAを持つことの利点を（思いつく限り）挙げてください。

1. ユーザー（サーバー）数の増加に伴う処理量の増加を効果的に抑えることができる。

2.ハッキング攻撃によるルートCA漏洩の被害を軽減する。

クライアントが偽造された証明書を受け入れた場合に発生する可能性のある脅威を（思いつく限り）リストアップしてください。

1. サーバからクライアントへの送信過程で、機密性の高い証明書やファイルなど、含まれている可能性のあるものが漏えいする可能性があること。 ニュース（2011年3月、ハッカーが Comodo に侵入し、mail.google.com, addons.mozilla.org, login.yahoo.com など7つのWebドメインから計9枚の電子証明書を盗み出しました。）

2.悪意のあるルート証明書が発行した偽造証明書が信頼リストに紛れ込んでいると、コンピュータのすべての安全な通信が危険にさらされ、機密情報が解析され盗聴され、有効なデジタル署名と安全なHTTPSに見える接続も実際には信頼されなくなる。

3.未承認の危険なサイトに接続する可能性がある。

ルートCAから公開鍵証明書を失効させる方法を説明する。

使用されなくなった証明書は、CRLに記載される。失効した証明書の関連項目は、証明書の有効期限が切れてCAがリストから削除できるようになるまでCRLに残ります。OCSPバインド方式は､SSL証明書の有効性を迅速かつ安全に確認するのに役立ちます。OCSP バインディング技術を用いた検証のための検証シーケンスは、以下のステップで構成される。

ステップ1.SSLで保護されたWebサイトをホストするWebサーバーは、CAにリクエストを送信します。 CAからの応答として、証明書のステータスが署名のタイムスタンプ（timestamp）と共に表示される。 タグに署名することで、ウェブサーバーがタグを一切変更しないことが保証される。

ステップ2. 閲覧者のブラウザがサーバーに接続する。 このとき、サーバはCAから受け取ったタイムスタンプをSSL証明書にバインドする。

ステップ3.Webブラウザがタイムスタンプを確認する。 証明書の提供者によって署名されているため、信頼できる。

ステップ4. 証明書が信頼できるものであれば、ブラウザでページが開かれる。 そうでない場合は、エラーメッセージが表示される。

この場合の証明書失効情報での運用の問題点を記述する。

その結果、SSLの信頼の連鎖が崩れ、多くのユーザーが攻撃される危険性があります証明書の失効情報をすぐに公開することはできません。 証明書の失効による潜在的な損失を軽減することができる 逆に､CRLの更新頻度が低いと､失効した証明書がタイムリーに発行されず、紛失のリスクが高まります。