コンピュータセキュリティ 7－4
（2000. 1. 21）

サーバ証明書の有効性を確認する SSL/TLS 通信プロトコルの改良とその評価

藤永卓人† 木村成伴‡ 海老原義彦‡

†筑波大学工学研究科 ‡筑波大学電子・情報工学系

概要:
代表的な暗号化通信である SSL/TLS 通信では，認証局による署名が施されたサーバの証明書を用いてコネクションが設立される．しかし，このとき廃棄証明書リストが参照されないため，サーバの秘密鍵が漏洩した場合，廃棄された証明書による不正利用を早急に防ぐことができなかった．これを改善するため，本稿では SSL/TLS 通信におけるハンドシェイク時にサーバの証明書の廃棄情報を確認するための二つの PKI モデルを提案する．一つはクライアントがディレクトリサーバから SSL/TLS サーバの証明書の廃棄情報である認証辞書を取り寄せ，当該の証明書が廃棄されていないか検証する方式である．もう一つはサーバが証明書とともにその認証辞書を用いてクライアントに送信する方式である．最後に，ネットワークシミュレーション実験を行い，両方式を比較評価する．

Improvement and Evaluation of SSL/TLS Communication Protocol by Confirm Validation of Server Certificate

Takuto Fujihaga† Shigetomo Kimura‡ Yoshihiko Ebihara‡

†Doctoral Program in Engineering, University of Tsukuba
‡Institute of Information Sciences and Electronics, University of Tsukuba

Abstract:
SSL (Secure Socket Layer) and TLS (Transport Layer Security) are famous coded communications. To establish the SSL connection, the server's certificate, which is signed by its certificate agency, is needed. At this connection establishment, however, the CRL (Certificate Revocation List) is not referred. Thus, the misuse of the revoked certificate is not quickly prevented, when the secret key of the server is stolen. This paper proposes two kinds of PKI models to valid certification revocation information in SSL/TLS communication handshake. For the first model, a SSL/TLS client obtains revocation information from Authenticated Dictionary to check validation of the server. For the second one, the server sends the both of its certificate and Authenticated Dictionary to client. From the network simulations, the performance of both methods are evaluated.

1 背景

近年の急速なインターネットの普及に伴い，利用者が持つ情報の漏洩を防止することが重要な課題となっている．これを実現するために通信データの暗号化は不可欠な技術であり，現在，PGP や SSH, SSL[1]/TLS[2] 等の暗号化通信が利用されている．この内，SSL (Secure Socket Layer) / TLS (Transport Layer Security) はソケットを使う全てのアプリケーションに適用可能な暗号化通信方式である．特に，HTTP では，ほとんどの WWW ブラウザに SSL の機能が組み込まれているため，幅広く利用されている．

SSL/TLS では安全な公開鍵の受渡しのために認証局 (CA: Certification Authority) 方式を採用している．この方式では，信頼のおける第三者機関である認証局が事前にサーバの正当性を調査しておいて，サーバの公開鍵や所有者の情報に認証局の秘密鍵で署名を行う．この署名付き情報を電子証明書 [3] (または単に証明書) と呼び，その具体的な形式は ITU-T 勧告の X.509 に定義されている．

各クライアントは信頼できる認証局の公開鍵を保持することで，サーバが提示した証明書にある認証局の署名を認識することができる．その結果，認証局の信頼の下で安全にサーバの公開鍵が取得できる．

この証明書は容易に入手できるため，サーバの秘密鍵が何らかの問題により漏洩した場合，サーバのなりすましや通信内容の盗聴，改ざんなどが可能となる．これに対して現状の認証局方式では，鍵の所有者が公開鍵を廃棄する旨を認証局に通知することで対処している．認証局は廃棄された証明書のリストに署名を行った廃棄証明書リスト (CRL: Certificate Revocation List) を公開している．これを参照することで証明書の廃棄情報が確認できるようになっている．

しかし，SSL/TLS プロトコルでは，通信確立時に CRL またはディレクトリを参照していない．また，証明書の有効期限は十分長くとられている (年単位など) ことが多く，その期限が切れるまでの間，秘密鍵を取得した第三者によって，廃棄されたはずの証明書を利用した不正使用を許すことになる．

このため，SSL/TLS 通信においてサーバの秘密鍵が漏洩した場合の被害を軽減することを考えた場合，クライアントがサーバの証明書を入手した直後にその証明書の廃棄情報を確認することが有効と考えられる．

本稿ではクライアントがサーバ証明書の廃棄情報の確認を行うための PKI (Public Key Infrastructure) を提案する．さらにそれぞれの PKI の方式における SSL/TLS 通信の確立回数とディレクトリ，および認証局の負荷についてのネットワークシミュレーションを行い，比較評価を行う．

2 提案方式

2.1 SSL/TLS 通信の概要

SSL/TLS 通信では伝送されるデータを暗号化するために，共通鍵暗号が使用される．これは公開鍵暗号よりも共通鍵暗号の方が暗号化に要する計算時間が少なくて済むためである．SSL/TLS 通信では複数の種類の共通鍵暗号方式が用意され，通信開始のネゴシエーションの際にサーバおよびクライアントで使用できる暗号方式の内から 1 つが選択される．例えば，SSLv3 で利用できる共通鍵暗号方式として DES や 3DES，RC2，RC4 がある．

ただし，共通鍵をサーバとクライアントで共用するためには公開鍵暗号が用いられる．公開鍵暗号方式では，公開鍵の安全な受渡し方法が問題となるが，SSL/TLS 通信ではネゴシエーション開始時に公開鍵が記入されている証明書をサーバがクライアントに通知することになっている．例えば，SSLv3 で利用できる公開鍵暗号方式として RSA，Diffie&Hellman などがある．

以下にハンドシェイクの終了までの動作を示す．

1. サーバが認証局の署名付き証明書を送信する．クライアントは証明書の正当性を認証局の公開鍵で確認する．
2. 証明書の確認後，クライアントは通信データの暗号化に使用可能な暗号の種類などの共通鍵作成に必要な情報をサーバの公開鍵で暗号化してサーバに通知する．
3. サーバはクライアントに共通鍵作成に必要な情報をクライアントに通知する．
4. サーバとクライアントはお互いに入手した情報から共通鍵を作成し，暗号化通信を行う．

しかし，上述の手順では CRL またはディレクトリが参照されていないため，サーバの秘密鍵が漏洩した場合，廃棄された証明書を用いた不正使用が可能となる恐れがある．

これを改善するために，以下では SSL/TLS 通信においてサーバ証明書の廃棄情報の確認を行うための PKI システムを以下で提案する．

2.2 クライアントがディレクトリサーバから廃棄情報を入手する方式

クライアントは SSL/TLS サーバから証明書を受け取り，署名を確認する．最初の方式では，SSL/TLS コネクション設立時に，この証明書が信頼できるものかどうかを確認するため，クライアントがディレクトリにその証明書に関する Authenticated Dictionary[4] の取り寄せ依頼を行う．取り寄

せた Authenticated Dictionary を検証した結果，サーバ証明書が廃棄されている場合，クライアントは SSL/TLS サーバに対してエラーメッセージを返す．なお，ディレクトリは証明書を発行した認証局から発行証明書全体の Authenticated Dictionary を定期的に取り寄せるものとする．

Authenticated Dictionary は Naor らによって考案された証明書の廃棄状況を示す方式で，CRL と等価な廃棄情報を持ちながら，ディレクトリの持つ証明書の廃棄情報の更新とクライアントに対しての証明書の廃棄情報の通知に必要とされる通信量を大幅に減少させる利点を持っている．Authenticated Dictionary の構成を述べる．まず，認証局が廃棄証明書をそのシリアル番号でソートし，これらの値を葉とする 2-3 分木を作る．上位ノードの値は下位ノードの値を一方向性ハッシュ関数にかけることによって作成する．認証局はルートノードの値，木の高さ，および，更新日時に署名を行ったものと廃棄証明書のシリアル番号のリストをディレクトリに送信する．ディレクトリは認証局の署名を確認し，廃棄証明書のシリアル番号のリストから 2-3 分木を作成する．ディレクトリはクライアントからの廃棄情報の取り寄せ依頼に対して，該当する証明書が廃棄されている場合は証明書の失効情報とルートノードから該当する証明書のシリアル番号を持つ葉までのパス上の各ノードの兄弟の値と認証局の署名付のルートノードの値，木の高さ，および，更新日時を送信する．廃棄されていない場合は廃棄証明書のシリアル番号のリストの中で取り寄せ依頼のあった証明書のシリアル番号に最も近いシリアル番号を持つ両隣の 2 つの廃棄された証明書のシリアル番号 (取り寄せ依頼のあった証明書のシリアル番号を s，リスト上のシリアル番号を l_1，l_2 とすると，$l_1 < s < l_2$ となる，リスト上の最大の l_1 と最小の l_2) を持つ葉までのパス上のノードの兄弟の値と認証局の署名付のルートノードの値，木の高さ，および，更新日時を送信する．なお，ディレクトリが持つ証明書の廃棄情報の更新は，追加する廃棄証明書と期限切れのため削除する廃棄証明書の情報を認証局から取り寄せることによって行う．

本稿における Authenticated Dictionary 方式で使用するパケットの形式を表 1~4 に示す．

廃棄情報の取り寄せ依頼メッセージ (表 1) はクライアントがディレクトリに対して送信し，それに対してディレクトリは廃棄情報の応答メッセージ (表 2) を送信する．更新依頼メッセージ (表 3) はディレクトリが認証局に対して Authenticated Dictionary

データ項目	データ長
メッセージの種類	1 バイト
問い合わせ証明書の数	4 バイト
問い合わせ証明書の シリアル 番号列	4 バイト × 列数

表 1: 廃棄情報の取り寄せ依頼メッセージ

データ項目	データ長
メッセージの種類	1 バイト
署名アルゴリズム	1 バイト
2-3 木の高さ	1 バイト
ルートノードの値	16 バイト
今回の更新日時	4 バイト
次回の更新日時	4 バイト
以上の項目への署名	16 バイト
証明書のシリアル番号	4 バイト
廃棄の有無	1 ビット
以下の情報を 2-3 分木の高さだけ繰り返す.	
兄弟の中での位置	2 ビット
兄弟の数	1 ビット
兄弟の値	16 バイト

表 2: 廃棄情報の応答メッセージ

データ項目	データ長
メッセージの種類	1 バイト

表 3: Authenticated Dictionary の 更新依頼メッセージ

データ項目	データ長
メッセージの種類	1 バイト
署名アルゴリズム	1 バイト
2-3 木の高さ	1 バイト
ルートノードの値	16 バイト
今回の更新日時	4 バイト
次回の更新日時	4 バイト
以上の項目への署名	16 バイト
削除する廃棄証明書数	4 バイト
削除する廃棄証明書のシリアル番号列	4 バイト × 列数
追加する廃棄証明書数	4 バイト
追加する廃棄証明書のシリアル番号列	4 バイト × 列数

表 4: Authenticated Dictionary の更新応答メッセージ

の更新情報を要求する際に用いられ，その応答として認証局は更新応答メッセージ (表 4) を送信する．

本方式の場合，ディレクトリに証明書の廃棄情報が通知されていれば被害を受けずに済むが，認証局とディレクトリ間，ディレクトリとクライアント間の通信負荷と通信量が増加することが考えられる．

2.3 クライアントが SSL/TLS サーバから廃棄情報を入手する方式

2 番目の方式では通信接続時に SSL/TLS サーバが証明書とともに証明書の廃棄情報をクライアントに送信する．ここで SSL/TLS サーバから送られる廃棄状況を信頼できるものとするため，廃棄情報の送信には Authenticated Dictionary を使用する．これは SSL/TLS サーバがディレクトリから取り寄せていたものを使用し，認証局はディレクトリに Authenticated Dictionary を配布する．本方式の場合もディレクトリに証明書の廃棄情報が通知されていれば被害を受けずに済むが，認証局とディレクトリ間，ディレクトリと SSL サーバ間の通信負荷と通信量が増加することが考えられる．

本稿において SSL/TLS サーバがディレクトリへ送信する Authenticated Dictionary を用いた自分自身の証明書の廃棄情報の取り寄せ依頼メッセージは表 1と同様とし，それに対するディレクトリの応答メッセージも表 2 と同様とする．また，ディレクトリサーバが認証局に対して行う Authenticated Dictionary の更新依頼メッセージとそれに対する認証局の応答メッセージも表 3，4 と同様とする．また，SSL/TLS サーバは表 2 のメッセージからメッセージの種類を削除したものをサーバ証明書とともにクライアントに送信するものとする．

次節では 2 つの提案方式についてネットワークシミュレーション実験を行い，両者の性能の評価を行う．

3 シミュレーション実験と評価

3.1 シミュレーションモデル

2.2 節および 2.3 節の PKI におけるシミュレーションモデルを図 1，2に示す．前者では SSL/TLS クライアントが SSL/TLS サーバとのハンドシェイク時にディレクトリサーバから Authenticated Dictionary の部分木 を取り寄せる．後者では，SSL/TLS サーバが証明書の廃棄状況を示す Authenticated Dictionary の部分木を更新するためにディレクトリサーバに対して部分木の更新依頼を行う．また，どちらの場合も Authenticated Dictionary の更新をディレクトリサーバ，認証局サーバ間で行う．

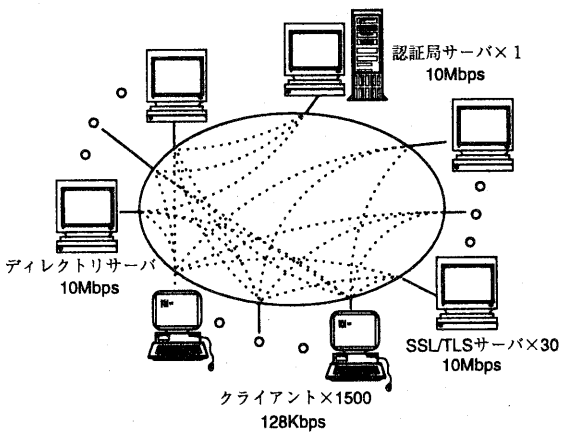

図 1: 2.2 節の方式のシミュレーションモデル

このときの，シミュレーション条件は以下の通りである．

- 認証局サーバは 1 台，SSL/TLS サーバは 30 台，クライアントは1,500 台とし，ディレクトリサーバは 1 ～ 30 台 まで変化させる．

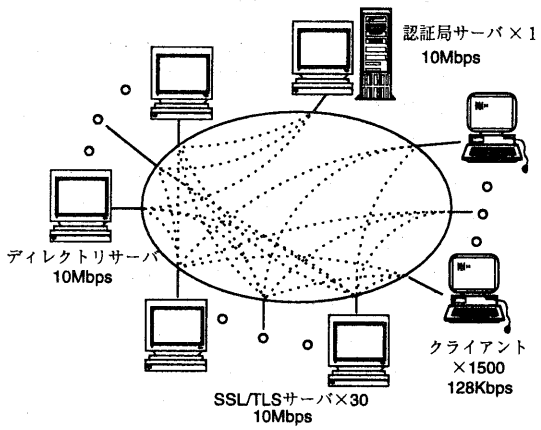

図 2: 2.3 節の方式のシミュレーションモデル

- SSL/TLS サーバ，ディレクトリサーバ，認証局サーバの伝送速度は 10Mbps とし，クライアントの伝送速度は 128Kbps とする．
- クライアントと SSL/TLS サーバ，ディレクトリサーバ間，SSL/TLS サーバとディレクトリサーバ間，ディレクトリサーバと認証局間の伝搬遅延はそれぞれ 82m 秒とする．
- クライアントの接続先の SSL/TLS サーバ，ディレクトリサーバ，SSL/TLS サーバの接続先のディレクトリサーバはランダムに決定されるものとする．
- 認証局サーバへの同時接続可能数を 2，ディレクトリサーバ，SSL/TLS サーバへの同時接続可能数を 20 とする．
- クライアントの接続要求発生の間隔は指数分布に従うものとし，そのときの平均要求間隔を 3600 秒とする．
- ディレクトリサーバの Authenticated Dictionary の更新を 150 秒毎にディレクトリサーバ，認証局サーバ間で行う．
- SSL/TLS サーバの持つ証明書廃棄情報の更新は 150 秒毎に SSL/TLS サーバ，ディレクトリサーバ間で行う．
- 現在の時刻が SSL/TLS サーバからクライアントへ送信する Authenticated Dictionary の次回の更新日時を過ぎていたら，SSL クライアントはエラーメッセージを送信し，通信を切断する．
- ディレクトリは Authenticated Dictionary の更新時は接続不能とする．
- それぞれのノードが署名を行うために必要な時間と署名の検証に必要な時間を 150m 秒とする．
- ディレクトリサーバが Authenticated Dictionary の更新時に 2-3 分木を作成するために必要な時間を 100m 秒とする．
- シミュレーション時間は 3600 秒とする．
- 認証局からディレクトリサーバへ送信する Authenticated Dictionary の内容は全て同一である．
- SSL サーバは Authencticated Dictionary の更新依頼を期限切れから 300m 秒後にディレクトリサーバに行うものとする．

本シミュレーションで得られた値はバッチ平均法により 90% の信頼係数で 10% の精度を満たすことを確認した．

3.2 SSL/TLS クライアントと SSL/TLS サーバ間で確立された SSL/TLS 通信確立数の比較

ディレクトリサーバ数を変化させたとき，従来の SSL/TLS 通信の方式と各提案方式おいてシミュレーション時間内に確立された SSL/TLS 通信の数を図 3に示す．

2.2 節の PKI モデルの場合，SSL/TLS クライアントがディレクトリサーバから Authenticated Dictionary を取り寄せて証明書の信頼性の検証を行うが，従来の方式と比較しておよそ 70% の SSL/TLS 通信確立回数しか達成されていない．2.3 節の PKI モデルの場合，従来の方式とほぼ同程度の SSL/TLS 通信確立回数を達成できることが示された．

3.3 ディレクトリサーバに対する接続要求の比較

ディレクトリサーバ数を変化させたとき，2.2 節と 2.3 節 それぞれの PKI モデルにおいて，ディ

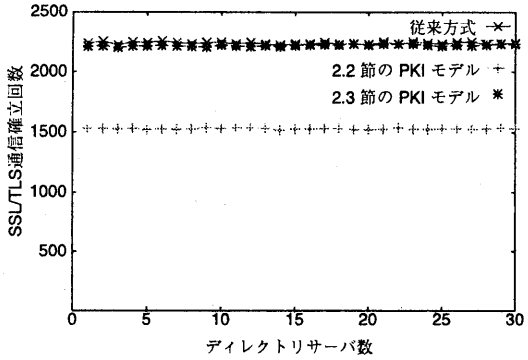

図 3: SSL 通信確立回数の比較

レクトリサーバに対して接続要求を行うノード (2.2 節のモデルではクライアント，2.3 節のモデルでは SSL/TLS サーバ) が 1 回あたりの接続要求に対して何度接続を行っているかを図 4に示す．

図 4から 2.2 節においてはディレクトリサーバの個数が 15 個前後，2.3 節においてはディレクトリサーバの個数が 7 個前後になると，ディレクトリサーバ数の増加にともなう 1 回あたりの接続要求に対する接続回数の減少が停止し，ディレクトリサーバに対する負荷が軽減されたことがわかる．この結果から 2.3 節の PKI モデルの場合の方が，ディレクトリサーバに対してより少ない負荷でモデルを実現できることが分かった．

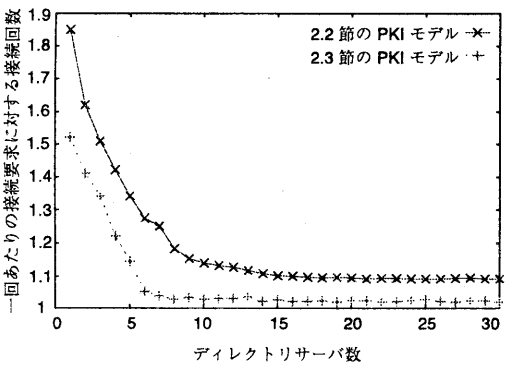

図 4:

4 結論と今後の課題

本稿では SSL/TLS 通信おけるサーバ証明書の不正利用を防止するために証明書の有効性を確認するための PKI モデルを 2 つ提案し，それぞれにおいて計算機シミュレーションによって SSL/TLS 通信の確立回数と，ディレクトリサーバの負荷について比較評価を行った．その結果，2.3 節の PKI モデルの方が SSL/TLS 通信確立回数，ディレクトリサーバの負荷に関して 2.2 節の PKI モデルよりも従来モデルに近い結果を得ることができた．これは 2.3 節の PKI モデルが SSL/TLS 通信のハンドシェイク時に Authenticated Dictionary を SSL/TLS サーバがクライアントに渡すためだと考えられる．

本稿ではディレクトリを信頼できないものとして考えたが，OCSP (Online Certificate Status Protocol) や SVCG (Simple Certificate Validation Protocol) で利用されるディレクトリは信頼のおけるものとしてクライアントからの廃棄情報確認依頼に対して直接応答を行っている．これらを利用した PKI モデルに関する考察や比較も今後の課題としたい．

参考文献

[1] Alan O. Freier, Philip Karlton and Paul C. Kocher, "The SSL Protocol Version 3.0," Netscape Communications, INTERNET-DRAFT, draft-freier-ssl-version3-02.txt, 1996.

[2] Tim Dierks, Philip L. Karlton, Alan O. Freier and Paul C. Kocher, "The TLS Protocol Version 1.0," Request for Comments: 2246, 1999.

[3] Russell Housley, Warwick Ford, Tomi Polk and David Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," Request for Comments: 2459, 1999.

[4] Moni Naor and Kobbi Nissim "Certificate Revocation and Certificate Update," Faculty of Mathematics and Computer Science The Weizmann Institute of Science, Technical Reports CS99-05, 1999.