1ZA-6

DNSを用いた公開鍵配送方式とその応用に関する研究

房野　賢一†　　中村　康弘†
防衛大学校 情報工学科

1. はじめに

近年WEBサービスをはじめとする様々なサービスにおいて，安全な通信の実現のために通信データの暗号化と通信相手の認証が求められている．これは，公開鍵暗号技術を用いて実現することができるが，なりすましを防止するために公開鍵の正当性を保証する必要がある．

この仕組みとして，サービスを提供するドメインのDNSを用いて公開鍵を配送する方式を検討する．

2. 公開鍵配送方式に関する検討

HTTPにおける暗号通信方式としては，SSL(Secure Sockets Layer)/TLS(Transport Layer Security)を用いたHTTPSが一般的であり，多くのWebサイトで利用されている．SSL/TLSは通信データを暗号化するだけでなく，通信相手を認証する手段を提供する．図1にSSL通信の動作を示す．

①：Clientは鍵生成に必要な乱数及び使用可能な暗号アルゴリズムのリストをServerに送信する．

②③④：Serverは鍵生成に必要な乱数，リストから選定した暗号アルゴリズム及びServer自身の公開鍵が含まれる証明書をClientに送信する．

⑤：Clientは Serverが提示した証明書を検証する．

⑥：Clientは pre-master-secretを作成するとともに，Client 乱数，Server 乱数及び pre-master-secret から master-secretを作成する．

⑦：Clientは③から得たServer公開鍵で pre-master-secretを暗号化し，Serverに送信する．

⑧⑨：Clientはそれ以降の通信を取り決めた暗号プロトコルで暗号化することをServerに通知するとともに，チェックサムを送信し終了する．

⑩:Serverは Client乱数，Server乱数及び pre-master-secret から master-secretを作成する．

⑪⑫：Serverは Clientに対して，⑧⑨と同じメッセージを送信する．

⑬：アプリケーションデータを送信する．

上に示す⑤証明書の検証においては，PKI(Public Key Infrastructure)の仕組みを利用することが一般的である．PKIでは，なりすましを防止するために認証局（CA）を設ける．認証局では，ある公開鍵が本人のものであるかを証明する証明書を発行する．認証局は階層構造をなし，最終的にClientが信頼する上位の認証局までたどり着くことで全体が保証される．

また，信頼の輪によって公開鍵の正当性を保証するPGP(Pritty Good Privacy)も小規模な組織等でよく使用されている．

Research of public key distribution scheme using DNS and its application

† Kenichi Fusano, Yasuhiro Nakamura, Dept. of Computer Science, National Defense Academy

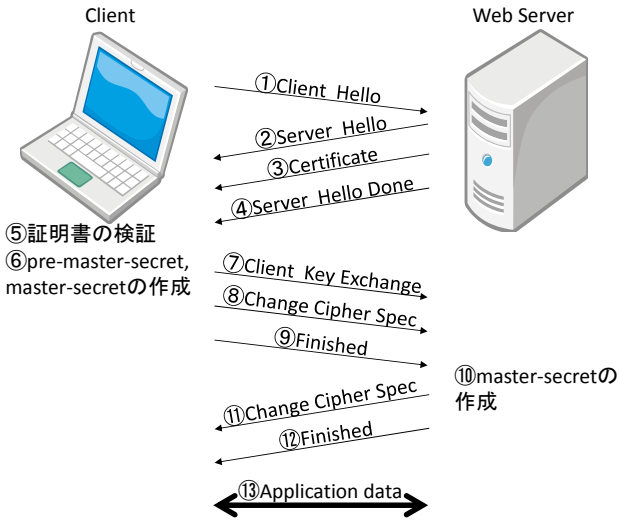

図 1　SSL通信の動作

一方で，公開鍵の保証のために認証局や信頼の輪ではなく，DNSを使う仕組みがDANE(DNS-based Authentication of Named Entities)[1][2][3]として検討されている．DANEは，DNSにそのドメイン内のホストの公開鍵をTLSAレコードとして公開する仕組みである．通常のSSLでは，Clientは Serverから証明書の提示を受けた場合，あらかじめブラウザにインポート済みの信頼できる認証局の証明書を用いて検証するが，DANEを用いた場合は，図2のようにServerと同一ドメインのDNSにTLSAを問い合わせ，そのTLSAを用いてServerが提示した証明書を検証する．DNSキャッシュポイズニング等によりDNSレコードが改竄されている可能性があるため，DNSレコードの正当性を保証する必要があるが，それはDNSSEC(DNS Security Extensions)を用いることで実現できる．DANEはPKIに比べて認証局のような第3者に頼ることなく通信相手の認証を実現できる．さらに，DNSはインターネットの根幹をなすシステムであるためDNSSECの普及も期待でき，今後の認証の基盤としてDNSを用いる方式も広く普及していくと考えられる．

しかし，DANEに関する検討はIETFにおけるドラフト段階であり，その実装に関しては検討されていない．したがって，本研究においてはDANEの実装方法を提案し，提案手法に対する比較検討を行い，長所短所を明確にすることにより導入する際の一定の基準を導き出すことを目的とする．

3. 提案手法

DANEの機能を実装する方法として，(1)Webブラウザなどの Clientに実装する方法（クライアント型）と(2)Webブラウザと Server間に Proxyを設置し，Proxyに実装する方法（Proxy型）が考えられる．

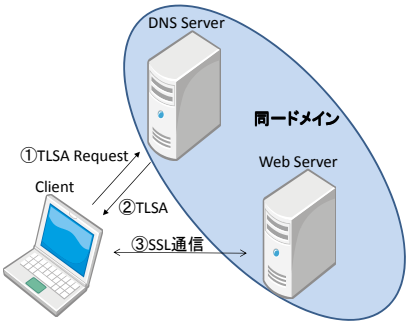

図 2　DANE における証明書の検証

3.1　クライアント型

クライアント型の動作は図 2 に同じである．

①②：Client は接続先 Server と同一ドメインの DNS から TLSA レコードを取得する．

③：Client は Server と SSL 通信を実施．以下のように場合分けしコンテンツを表示する．

PKI により証明書が検証できた場合：従来通り表示する．

DANE により証明書が検証できた場合：(a) に同じく従来通り表示する．

(b) と同様に検証したが一致しない場合：なりすましの可能性が高いため通信を切断する．

上記以外の場合：証明書の検証ができない警告を表示する．

3.2　Proxy 型

図 3 に Proxy 型の動作を示す．

①：Client は Proxy に対して Get Request を送信する．

②③：①を受けて Proxy は Server と同一ドメインの DNS から TLSA レコードを取得する．

④：Proxy は Server と SSL 通信を実施する．

⑤：Proxy は①に対する回答を Client に返信する．回答の内容はクライアント型の (2) と同様．

4.　提案手法の検討

提案手法に対して，秘匿性，ネットワーク負荷，通信遅延，導入コスト及び管理面の 5 項目について比較検討する．比較検討結果を表 1 に示す．

秘匿性については，クライアント型は，Client から Sever までの全ての通信路が暗号化されているため，秘匿性は高い．一方 Proxy 型は，Client-Proxy 間が暗号化されないため，その間において盗聴される危険性がある．したがって，この危険性を許容する又は同一 PC 内で Client と Proxy を動作させるなどの別の対策を取る必要がある．また，Proxy 自体を信頼できることが前提となる．

ネットワーク負荷については，クライアント型，Proxy 型ともに通常の SSL 通信に比べて DNS への問い合わせ分だけ増加する．

通信遅延は，ネットワーク負荷と同様，通常の SSL 通信に比べて DNS への問い合わせ分だけ，通信遅延が発生する．ただし，Proxy 型は Proxy に接続している Client の数によって遅延時間が変動する．

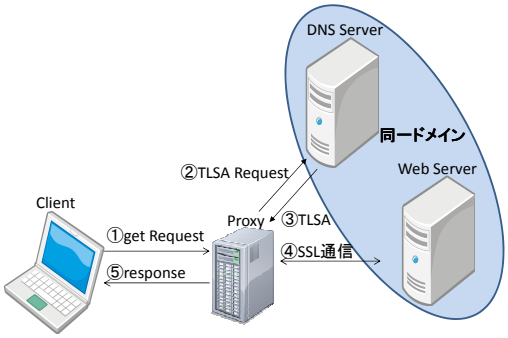

図 3　Proxy 型の動作

クライアント型は，全ての Client に導入する必要があり，導入コストが高い．一方 Proxy 型は，Proxy のみに導入するため，導入コストは比較的低い．特に 1 台の PC において複数の Client を動作させる場合，Proxy 型が有効である．

管理面については，組織内においては，ファイアーウォール等により通信の監視を行っているため，端末での通信の暗号化を許可しない場合がある．このような場合にはクライアント型は使用できないため，proxy 型が有効である．

表 1　提案手法の比較

	クライアント型	Proxy 型
秘匿性	○	△
ネットワーク負荷	△	△
通信遅延	△	△
導入コスト	×	○
管理面	△	○

5.　まとめと今後の課題

組織においては，管理面での需要や導入の容易さなどから，Proxy 型が有効であると考えられる．一方，個人で ISP と契約している場合には，不特定多数のユーザが同一の Proxy に接続するのは問題になるため，同一 PC 内に Client と Proxy を動作させるか，クライアント型にする必要がある．また，Proxy 型は Proxy の設置場所によって用途を様々に変更できるため，初期の導入に当たっては有効である．

本研究では DNS を用いた公開鍵の配送方式 DANE について調査し，実装方法の提案とその比較検討を行った．今後は，提案手法の実装及び検証・評価を行う．

参考文献

[1] R. Barnes, ”Use Cases and Requirements for DNS-based Authentication of Named Entities(DANE), ” IETF RFC 6394, October 2011.

[2] P.Hoffman, J. Schlyter, ”Using Secure DNS to Associate Certificates with Domain Names For TLS, ” Network Working Group Internet-Draft, March 2012.

[3] 木村　泰司, ”DNS を用いた公開鍵の配送技術 - DANE, ” 情報セキュリティ技術動向調査　タスクグループ報告書（２０１１年上期）.