2009-IOT-4 (26)
2009 / 3 / 5

PKI対応ネットワーク利用者認証システム Opengate-PKIの開発と試験運用

藤澤　優† 大谷　誠†† 渡辺　健次†††

† 佐賀大学大学院工学系研究科
〒 840-8502 佐賀市本庄町 1 番地
†† 佐賀大学理工学部
〒 840-8502 佐賀市本庄町 1 番地
††† 佐賀大学総合情報基盤センター
〒 840-8502 佐賀市本庄町 1 番地
E-mail: †fujisawa@ai.is.saga-u.ac.jp, ††otani@cc.saga-u.ac.jp, †††watanabe@is.saga-u.ac.jp

あらまし PKI(Public Key Infrastructure) は，公開鍵暗号を用い，ネットワーク上での，データの暗号化，データの完全性の保証，利用者認証といったセキュリティサービスを提供する技術基盤である．PKI は政府や大学などでネットワーク上での認証基盤として整備が進められている．Opengate は，不特定多数の利用者が多数の端末をネットワークに接続する環境のための，ネットワーク利用者認証ゲートウェイシステムである．これは 2001 年より佐賀大学全域の規模で利用されている．本研究では，将来，各大学間で連携した電子認証が行われることを想定し，Opengate に PKI を導入し，ブラウザ上から証明書による認証を可能とした Opengate-PKI を開発した．

キーワード PKI，Opengate，ネットワーク利用者認証，ディジタル証明書，EAP-TLS，RADIUS，パケット変換

Development of “Opengate-PKI” Network User Authentication System with PKI

Suguru FUJISAWA†, Makoto OTANI††, and Kenzi WATANABE†††

† Graduate Schools Science and Engineering Infomation Science, Saga University
1 Honjo,Saga City,Saga, 840-8502 Japan
†† Computer and Network Center, Saga University
1 Honjo,Saga City,Saga, 840-8502 Japan
††† Department of Information Science, Faculty of Science and Engineering, Saga University
1 Honjo,Saga City,Saga, 840-8502 Japan
E-mail: †fujisawa@ai.is.saga-u.ac.jp, ††otani@cc.saga-u.ac.jp, †††watanabe@is.saga-u.ac.jp

Abstract PKI(Public Key Infrastructure) provides security service on network, for example encryption of data, guarantee of data integrity and user certification, by public key encryption. PKI begins to be built as a certification base on a network by governments and universities. Opengate is an user authentication gateway system for networks in the open environment to public. This has been working for controlling the campus-wide open network in the Saga University since 2001. In this research, we assumed that the electronic certificate cooperated between each university is performed in the future. Based on it, we implemented Opengate-PKI, and enabled the authentication with certificates on the browser.

Key words PKI, Opengate, Network User Authentication, Digital Certificate, EAP-TLS, RADIUS, Packet Convert

1. はじめに

現在，ネットワーク上のサービス利用時には利用者 ID とパスワードを用いた個人認証が一般的に用いられている．パスワードによる認証は，入力に特別なハードウェア・ソフトウェアを必要としないため，コストの安い認証方式として広く利用されている．しかし，利用者の立場で考えると，ID とパスワードの管理など，ユーザビリティやセキュリティの面で問題も抱えている．

パスワードに代わる認証手段の一つとして，PKI に基づくディジタル証明書を利用した認証がある．PKI を利用した認証では，一つの証明書で複数のサービスの認証を行う事ができ，利用者にとっては管理が容易となり，ユーザビリティ・セキュリティの向上につながる．また，現在政府や大学間などにより，各組織の認証の基盤として PKI が整備されつつある．たとえば政府では GPKI，大学間では UPKI [2] が整備されている．

佐賀大学では，ネットワーク利用者の認証システムとして Opengate [1] を開発し，全学規模で運用している．現在，このシステムは個人の認証として利用者 ID とパスワードを用いている．本研究では，現在整備が進められている UPKI により，将来各大学間で連携した電子認証が行われる事を想定し，Opengate にディジタル証明書による認証を取り入れ，PKI に対応したシステム，Opengate-PKI を開発した．これにより，Opengate のユーザビリティ・セキュリティの向上，大学間の連携した認証への対応を目指す．

2. Opengate

本研究で開発した Opengate-PKI のベースとなっているシステムである，ネットワーク利用者認証システム Opengate について述べる．

2.1 Opengate の概要

Opengate とは，不特定多数の利用者が多様な端末を接続するネットワーク環境のためのネットワーク利用者認証ゲートウェイシステムである [1].

情報コンセント・無線 LAN と公開固定端末に適用可能で，GUI として Web ブラウザを利用する事で多様な OS の端末に対応させており，端末へ特別なソフトウェアを導入する必要はない．また，IPv4 と IPv6 の両者の全プロトコルについて，ファイアウォールと連携し，パケットの通過・拒否を制御できる．

Opengate ではユーザの最初の Web アクセスを横取りして認証ページを表示し，認証完了後は自由にネットワークを利用できる．ネットワーク利用開始時に端末に送付した JavaScript または JavaApplet により，ユーザのネットワーク利用を監視し，ユーザのネットワーク利用が終了すると即座にネットワークを閉鎖するようになっている [3].

Opengate は，佐賀大学において開発され，2001 年より佐賀大学全域の規模で利用されている．

Opengate のシステム構成を図 1 に示す．

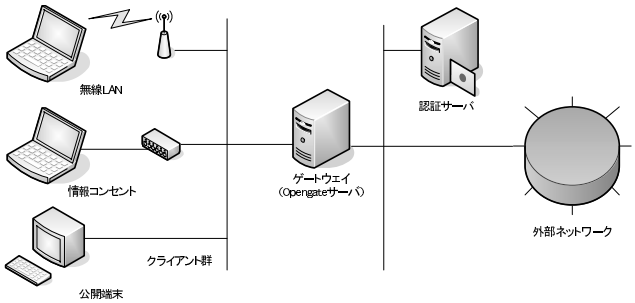

図 1　Opengate システム構成
Fig. 1　Opengate System Architecture

表 1　Opengate の動作環境
Table 1　Opengate Software Environment

サーバ	ソフトウェア	名称・バージョン
	OS	FreeBSD
	ファイアウォール	ipfw(ip6fw(注1))
	Web サーバ	Apache
クライアント	Web ブラウザ	ブラウザ (JavaScript または JavaApplet が動作すること)

2.2 動作環境

Opengate は，ゲートウェイに Web サーバとファイアウォールソフトが必要となる．現状のシステムでは，OS として FreeBSD，ファイアウォールソフトとして FreeBSD の ipfw，Web サーバとして Apache を利用している．また，ネットワーク構成によっては NAT や DHCP も合わせて利用する事ができる．

利用者端末は，Web ブラウザが利用可能である事が必要となる．また，利用者端末の利用状況監視のため JavaScript または JavaApplet を用いる．このため，JavaScript または JavaApplet が動作するブラウザが推奨される．

標準の設定ではまず，JavaScript による監視を試み，それに失敗した場合は JavaApplet による監視を試みる．JavaScript と JavaApplet のどちらで監視するか，などは設定により変更が可能である．

JavaScript，JavaApplet が両方とも動作しないブラウザの利用時には，利用者がネットワーク利用終了処理を行った場合，または，設定時間経過後に自動的に通信路が閉鎖される．

表 1 に Opengate の動作環境をまとめる

2.3 認　　証

Opengate では，ファイアフォールの閉鎖・開放により，ネットワーク利用者を制限している．

まず，Opengate 管理下にあるネットワークでは，ファイアウォールによって外部ネットワークへの接続は常に閉鎖状態にある．

ネットワーク利用者が Web ブラウザを用いて任意の Web サーバへアクセスする際，Opengate は送信される HTTP リクエストをファイアウォールの転送機能を用いて自身の Web サーバへと転送する．これにより，利用者端末に認証ページが

(注1)：FreeBSD 6.0 以前の場合．6.1 以降は ipfw に統合されている

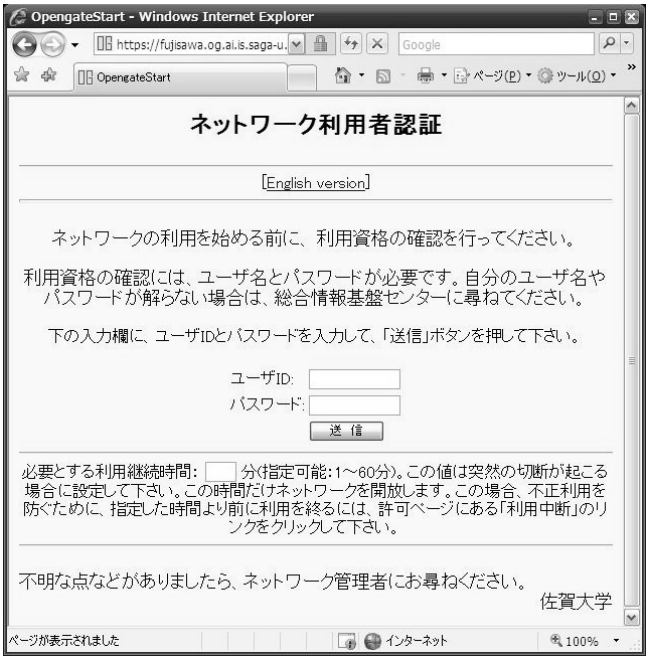

図 2　Opengate 認証ページ
Fig. 2　Opengate Authentication Page

表示される（図 2）.

ネットワーク利用者は，表示された認証ページより利用者 ID とパスワードを入力し送信する．認証に成功すると，Opengate はそのユーザに対してファイアウォールを開放し，HTTP 以外のプロトコルも含むネットワークの利用が可能となる．

Opengate サーバプログラムは Web サーバより CGI として起動され，利用者端末から送信されてきた利用者 ID とパスワードを取得し，外部の認証サーバに対して認証を行う．認証サーバには POP3，POP3S，FTP，FTPS，RADIUS，PAM を利用する事ができる．

2.4　ネットワーク利用者の監視

利用者端末では，認証後に認証完了ページが表示される（図 3）．この認証完了ページと共に，Web ブラウザに JavaScript または JavaApplet が送付される．この JavaScript または JavaApplet は，Opengate の監視プロセスと TCP コネクションを張り，利用者のネットワーク利用状況を監視する．

Web ブラウザが終了するなど，JavaScript または JavaApplet と監視プロセスとの TCP コネクションが切断された場合にファイアウォールを閉鎖する．あるいは，JavaScript または JavaApplet が監視プロセスからの定期応答メッセージに返答しない場合にもファイアウォールを閉鎖する．これにより，ネットワーク利用の終了後，即座にファイアウォールを閉鎖し，利用者の通信を終了させる事ができる．

また，利用者端末において JavaScript，JavaApplet 共に利用できない環境にある場合には，監視プロセスは任意の設定時間経過後に自動的にファイアウォールが閉鎖される仕組みになっている．

図 3　Opengate 監視ページ
Fig. 3　Opengate Watch Page

表 2　Opengate-PKI のソフトウェア構成
Table 2　Opengate-PKI Software Environment

サーバ	ソフトウェア	名称・バージョン
	OS	FreeBSD 6.3-RELEASE-p5
	ファイアウォール	ipfw
	Web サーバ	Apache 2.2.9
	認証サーバ	FreeRADIUS Version 1.1.7
	ファイアウォール	NAREGI-CA version 2.2
クライアント	Web ブラウザ	ブラウザ (クライアント認証に対応していること) IE7，Firefox2，3 など

3.　Opengate-PKI の実装

本研究で開発した Opengate-PKI について説明する．

3.1　システム構成

Opengate-PKI は従来のシステムである Opengate との互換性を保つため，従来のシステム構成とほぼ同じ構成としている．従来からの変更点は，認証時に利用する証明書を発行する認証局を準備することと，認証サーバとして RADIUS サーバを利用することである．

また，認証ページでは ID とパスワードではなく， ブラウザにインポートされている証明書を要求する．よって，クライアント側では，クライアント証明書による認証をサポートしたブラウザを利用しなければならない．

表 2 に Opengate-PKI のソフトウェア構成を示す．なお，各ソフトウェアのバージョンは開発に利用したバージョンを示している．

3.2　ディジタル証明書による認証

本研究では証明書による認証を行うため，同じく証明書による認証が可能な，無線・有線 LAN へ接続する際のユーザ認証に関するフレームワークである IEEE802.1X [4] を参考にした．IEEE802.1X では，クライアントと認証装置間で EAPOL(EAP over LAN)，認証装置と認証サーバ間で RADIUS プロトコル

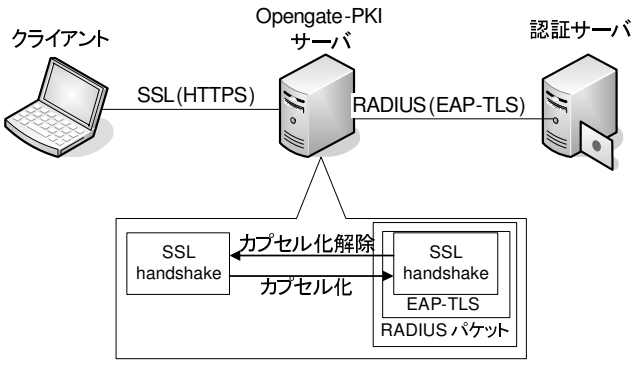

図 4　パケット変換
Fig. 4　Packet Convert

を利用する [5].

これを参考に，Opengate-PKI サーバと認証サーバ間では RADIUS EAP-TLS プロトコルを利用し，Opengate-PKI サーバとクライアント (Web ブラウザ) 間では，ブラウザのサポートが多く，証明書による認証が可能な HTTPS(SSL/TLS) を利用する．認証サーバとクライアント間でプロトコルが異なるため，Opengate-PKI は図 4 のように，クライアントとサーバ間で異なるプロトコルを相互に変換し， 認証を行う．

認証時には， まずクライアントと Opengate-PKI 間で，SSL の証明書認証を行う SSL handshake を開始する [6], [7]．この SSL handshake パケットを Opengate-PKI サーバプログラムにより取得し， RADIUS パケットへとカプセル化する．カプセル化の処理では，SSL handshake の RADIUS 属性への変換， メッセージの分割などの処理を行う．逆に，認証サーバより RADIUS パケットが送られてきた場合，パケット内より SSL メッセージを取り出し， ブラウザへと送信する．この変換処理を RAIDUS サーバでの認証が完了するまで繰り返し行うことで， Opengate-PKI はディジタル証明書による認証を実現している．

3.3　認証の詳細

図 5 に認証の流れを示す．Opengate-PKI は認証開始時に HTTPS によるアクセスを行う．クライアント側からの，SSL 接続を確立させるための SSL ハンドシェイク Client Hello メッセージから，認証は開始される．

これを受け，Opengate-PKI サーバ CGI はまず RADIUS サーバとの EAP 認証を開始する．この時はまだ EAP-TLS による認証は開始されていないため，クライアントから取得した Client Hello メッセージは RADIUS サーバへは送信しない．

この RADIUS リクエストに応えて，RADIUS サーバより EAP-TLS 認証の開始が通知される．EAP-TLS による認証が開始された後，クライアントから取得した Client Hello メッセージをカプセル化し，RADIUS サーバへと送信する．これによりクライアントと認証サーバ間の SSL ハンドシェイクが開始される．

ハンドシェイク終了まで，Opengate-PKI サーバ CGI 側でカプセル化，カプセル化解除を繰り返してハンドシェイクを行う．ハンドシェイクが終了し SSL 接続が確立されると，Web ブラウザは HTTPS(SSL により保護された HTTP パケット) パケットを送信する．Opengate-PKI サーバ CGI はこれを検知すると，SSL 接続が確立されたと判断し，RADIUS サーバへ EAP-TLS Ack を送信する．この Ack の送信は RADIUS EAP-TLS 認証での仕様である．RAIDUS サーバはこれに返答して，RADIUS Access-Accept を返し，認証完了する．

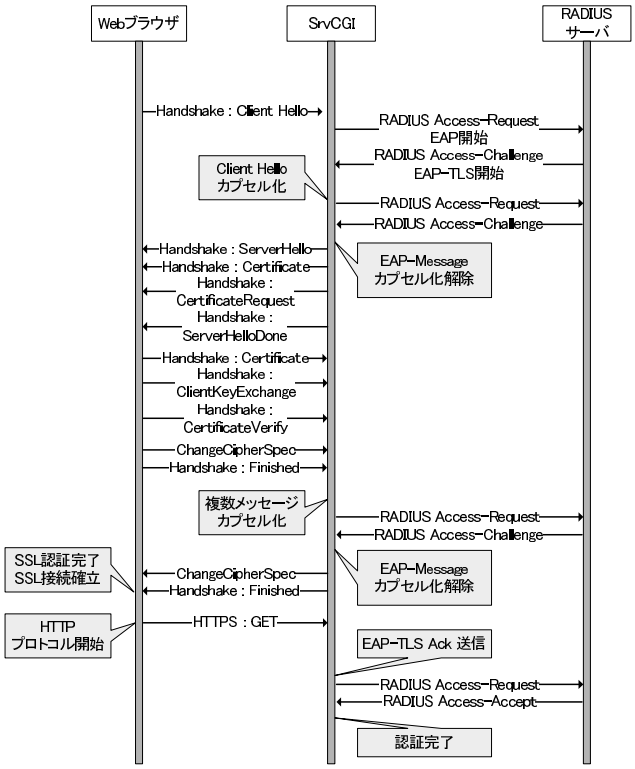

図 5　Opengate-PKI 認証シーケンス
Fig. 5　Opengate-PKI Authentication Sequence

4. 利 用 方 法

まず従来の Opengate の利用方法は次の手順である．

（1） 任意 URL へアクセスする
（2） 認証ページへ自動的に転送される
（3） 認証ページで ID とパスワードを入力し認証する
（4） 認証に成功するとネットワーク利用可能になる

次に Opengate-PKI を利用する場合について述べる．Opengate-PKI 証明書による認証を行うには，まず認証局から証明書を配付してもらう必要がある．配付された証明書を Web ブラウザにインポートする事で，証明書による認証の準備は完了である．ただし，ブラウザの設定で証明書の保護のため，パスワードを設定している場合は，その入力が必要となる．

Opengate-PKI の利用方法は次の手順である．

（1） 任意 URL へアクセスする
（2） 自動的に認証処理へ転送される
（3） 証明書認証が行われる
（4） 認証に成功するとネットワーク利用可能になる

任意の URL へとアクセスすると，認証処理へ遷移するのは

図 6　Opengate-PKI 証明書要求
Fig. 6　Opengate-PKI Certificate Request

図 7　NAREGI-CA による証明書発行ページ（認証）
Fig. 7　Certificate issue with NAREGI-CA (Authentication)

従来の Opengate と同様である．しかし，図 2 のように認証のためのページが表示されるのではなく，バックグラウンドで SSL によるアクセスが行われ，認証が開始される．

認証が開始されるとサーバ側から証明書の提出要求がブラウザへと送られる．これに対してブラウザは証明書を提出するのだが，ブラウザ毎に挙動が異なる．IE7 では図 6 のように証明書を提出するためのダイアログが表示される．このダイアログで証明書を選択することで証明書が提出される．

Firefox は，初期状態では IE と同様に証明書提出のためのダイアログが表示される．しかし，オプションで設定を変更するとブラウザが自動的に証明書提出するようになり，証明書を選択する必要はなくなる．

証明書を提出すると認証が行われ，認証に成功した場合，従来の Opengate と同様に図 3 が表示されネットワークの利用が可能となる．

5. 運 用 実 験

実験場所は，佐賀大学理工学部知能情報システム学科第 5 研究室内である．ここには無線 LAN アクセスポイントが用意されており，研究室所属ユーザが認証することで，ネットワークを利用できるようになっている．この認証には従来は Opengate を用いていた．今回はこれを Opengate-PKI と交換して実験を行った．

ネットワーク利用者は研究室の学部生，修士および研究室スタッフで，人数は 33 名である．

運用の流れを以下に示す．

（1） Opengate-PKI，認証サーバなどのインストール，設定（管理側）

（2） ユーザへの証明書発行用ライセンス ID 発行（管理側）

（3） Web 上より証明書と秘密鍵を PKCS#12 形式で取得（ユーザ側）

（4） 証明書と秘密鍵をブラウザへインポート（ユーザ側）

（5） Opengate-PKI によるネットワーク利用認証（ユーザ側）

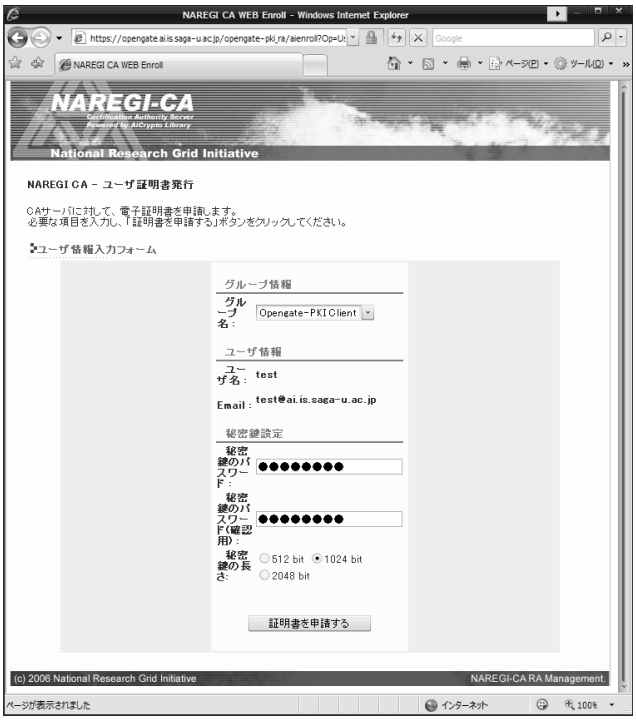

図 8　NAREGI-CA による証明書発行ページ（情報入力）
Fig. 8　Certificate issue with NAREGI-CA (input user data)

証明書の発行方法は，まず管理側からユーザへライセンス ID を発行し，ユーザは発行されたライセンス ID を使い，証明書発行ページへアクセスし（図 7），自らの証明書を発行，ダウンロードする（図 8），という方法をとった．ライセンス ID の配布にはメールを用い，証明書の発行には NAREGI-CA という CA ソフトウェアを利用した．

1 月 20 日より運用を開始し，2 月 6 日時点で証明書を発行した人数は 8 名，認証に成功している人数は 5 名であった．認証を行った環境は，Windows XP + IE6，Windows XP + IE7，Windows Vista + IE7，Mac OS X + Firefox3 という環境であった．認証完了後に関しては，特に問題も報告されず，安定して動作していると確認できた．

一方で問題も発生した．IE6 の環境では SSL2.0 を利用するため認証ができないという問題があった．SSL2.0 は認証サーバ側の RADIUS EAP-TLS プロトコルがサポートしないので，Opengate-PKI でパケット変換しても認証できない．そのため，Opengate-PKI サーバの Apache の設定で SSL 2.0 のプロトコルは利用しないようにしている．しかし，IE6 はブラウザの設定でオンになっていると，SSL 2.0 を利用しようとして認証できないようであった．今回はブラウザの設定を変更し，SSL2.0 の利用をやめることで認証できるようにした．

6. まとめと今後の課題

本研究では，ネットワーク認証システムである Opengate を PKI に対応させ，証明書による認証を可能とした Opengate-PKI を開発した．Opengate-PKI は，ネットワーク利用時に証明書を要求し，証明書が提出されれば，ネットワーク利用者を正常に認証する事を確認した．

今後の課題としては，セキュリティ向上のため，秘密鍵の保管場所を IC カードや USB トークンなどの専用デバイスへ格納し，専用デバイスを介して Opengate-PKI の利用を可能にすることが挙げられる．

文　献

[1] 大谷誠，江藤博文，渡辺健次，只木進一，渡辺義明，”HTTP コネクションの維持による利用終了検知を行うネットワーク利用者認証システムの開発とその運用，” 学術情報処理研究，No.11，pp.87-91，Sept.2007.

[2] 国立情報学研究所 学術情報ネットワーク運営・連携本部認証作業部会，”UPKI 認証連携基盤 シングルサインオン実証実験の実施について，”TOPIC 講演会資料，Sept.2008.（オンライン），入手先<https://upki-portal.nii.ac.jp/item/idata/odatao/topic20080925/>（参照 2009-2-4）

[3] 大谷誠，江藤博文，渡辺健次，只木進一，渡辺義明，”IPv4/IPv6 デュアルスタックネットワークに対応したネットワーク利用者認証システムの開発，” 情報処理学会論文誌，vol.47，No.4，pp.1146-1156，Apr.2006.

[4] M.Gast，802.11 無線ネットワーク管理 第 2 版，渡辺尚，小野良司（監訳），林秀幸（訳），株式会社オライリー・ジャパン，東京，2006.

[5] J.Hassell，RADIUS-ユーザ認証セキュリティプロトコル，株式会社アクセンス・テクノロジー（訳），株式会社オライリー・ジャパン，東京，2004.

[6] E.Rescorla，マスタリング TCP/IP SSL/TLS 編，齋藤孝道，鬼頭利之，古森貞（監訳），オーム社開発局（編），株式会社オーム社，東京，2003.

[7] J.Viega，M.Messier，P.Chandra，OpenSSL 暗号・PKI・SSL / TLS ライブラリの詳細，齋藤孝道（監訳），オーム社開発局（編），株式会社オーム社，東京，2006.