論文

サイバー空間におけるルート認証局と EV SSL 証明書

福　井　幸　男

1　はじめに

筆者は 2010 年 12 月に『情報システム論入門－社会を守る暗号セキュリティ編』（日科技連）を刊行した。本稿では、世界を震撼させたトルコのルート認証局「TURKTRUST」事件をとりあげて、フィッシングサイトの具体例を検証する。これは、同書第 6 章 8 節「公開鍵の証明書」および 9 節「Web サーバの認証」についての補録的な説明でもある。

2　PKI と EV SSL 証明書

2-1　PKI

サイバー空間において最大の問題は匿名性にある。そもそも、ユーザー（太郎とする）は、インターネット上の取引においては、取引相手（花子とする）の顔が見えない以上、相手をにわかに信用することはできない。そこで、取引相手が絶対的に信頼できる人物であるとの確証が欲しい。それが認証局（Certification Authority：CA）の役割である。そのお墨付きがあれば、信頼できる取引相手と考えて、太郎は安心して取引を進めることができよう。ルート認証局は世界にごく僅かしかない大元の認証局で、自らの正当性を自ら証明する絶対的な存在である。中間認証局はルート認証局以外の認証局であり、ルート認証局が発行したデジタル証明書によって、自らの正当性を保持する認証局である。いずれの認証局も、花子が正当な人物（*you are who you claim to be,*（Ducklin, p.3））であることを、SSL（secure sockets layer）サーバ証明書発行で保証する。これにより、太郎は二つの情報、つまり、①相手の花子の身元を示す情報と、②認証局の情報を確認できる。

一部重複を恐れず、公開鍵暗号による秘密通信の流れを説明する。その基本原則は、一組の公開鍵と秘密鍵のペアからなる。その公開鍵が偽物であるならば、どうなるだろうか。花子からの署名を偽の公開鍵で解読しても花子の署名とは一致しない。そこで太郎は認証できないと判定するしかない。こうした事態を避けるために、公開鍵が花子の真正のものであることを証明する仕組みが不可欠となる。これが電子証明書による本人確認の仕組み、PKI（Public Key Infrastructure; 公開鍵基盤）である。この場合、公開鍵を厳重に保管し管理するセンターが必要で、これを KDC（=Key Distribution Centre）と呼ぶ。もしも、α（太郎）がβ（花子）と通信したい場合は、αは、KDC からβの公開鍵を取得して通信するわけである。αに限らず誰でもβの公開鍵を取得できる（図 1 参照）。

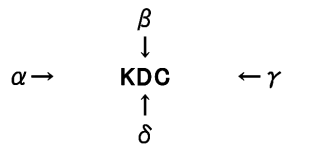

図 1　KDC の構図

しかし、悪意の第三者が KDC の管理の甘さを突いて、特定機関の公開鍵を勝手に登録したり、あるいは変更する可能性が考えられる。公開鍵の単なる管理機関の存在だけでは KDC は社会の要請には応えられない。そこで、こうした事態を避けるために、KDC の機能を強化した第三者機関が認証局である。認証局は、「この公開鍵は花子のものだ」と認証するデジタル証明書を発行する。認証局を使った公開鍵の流れを見るとつぎのようにまとめることができる。

(1)　まず、花子は秘密鍵と公開鍵のペアを作成する。

(2)　花子は秘密鍵を秘匿し、公開鍵を認証局に登録する。認証局の本人確認の手続きは様々である。メールが申し込み本人に届くことで本人確認とする簡単なレベルのものから、直接本人と面談するレベルまで、確認の程度は異なる。ここに、申込み者の確認がやや甘い SSL サーバ証明書と、厳格な EV SSL 証明書の違いを見出すことができる（2-2 節参照）。

(3)　認証局は花子の公開鍵を収めたデジタル証明書を発行する。

(4)　認証局はこのデジタル証明書に対して、自局の秘密鍵でデジタル署名する。

(5)　太郎は花子のメッセージを本物と確認したい。そこで認証局から花子の公開鍵を入手する。

(6)　太郎はこの公開鍵が真正と信じたいのだが、ニセモノという万が一の場合に備えて、この鍵を検証する手続きを踏む。

(7)　デジタル証明書には認証局のデジタル署名がついている。太郎はこの証明書の発行元の認証局が詐称されていないかを調べる必要がある。そこで、認証局自身の公開鍵を使ってデジタル署名を検証する。検証に成功すれば、認証局自体の信頼性に間違いはないと確認できる。太郎は公開鍵が花子のものと判断する。

(8)　花子は自分の秘密鍵で暗号化したメッセージを太郎に送信。

(9)　太郎は花子からの暗号文を花子の公開鍵で解読。

なお、(1) から (7) の作業までは、公開鍵の登録と検証の際に花子、太郎そして認証局が絶対欠かしてはならない作業手順である。一旦、検証が終われば太郎は花子の公開鍵を手元に保存しておけばよい。

2-2　SSL サーバ証明書による Web サーバの認証

PKI の代表例が SSL を使った Web サーバの認証の仕組みである。そもそも、サイバー空間におけるセキュリティの三要素たる「CIA」、すなわち機密性（confidentiality）、完全性（integrity）、そして可用性（availability）において、SSL は機密性維持の要になっている（福井 2011、p.120）。

フィッシングやファーミングの被害をなくすために、Web ブラウザは URL アドレスを「http」から「https」に変えている。これは、認証局からのお墨付きがあってこそ可能であり、サイトの先頭画面の上部に南京錠マークもつく。これをクリックすれば、「SSL サーバ証明書」が確認できる。要するに、SSL サーバ証明書の機能（福井 2010、pp.149-150）は、①本物のサイトであることの検証と、② Web サイトとの送受信の暗号化にある。とくに、①に関しては証明書を発行する認証局の信頼性に依存する。また、②に関しては、Web ユーザーが独自に情報を暗号化できない。Web 運営者もしかりである。彼らにできるのは SSL サーバ証明書を導入することだけである。

SSL なるプロトコルの機能を、インターネット・ショッピングの場合を例に説明する。SSL の機能は二つある。①相手の Web サーバがなりすましではなく本物のサイトのサーバであることを確かめるために、クライアントサーバ（Web ブラウザ）は Web サーバから「SSL サーバ証明書」を受け取ってこれを検証する。②クライアントサーバが、カード情報や買い物情報を暗号化して送信すると、暗号化データを受け取った Web サーバがこれを復号化して元に戻す。①と②の機能は、SSL 通信ソフトが自動処理している。それぞれ以下の (1) と (2) の役割を果たす。

(1)　カード会社の Web サーバの認証

Web ブラウザ（クライアントサーバ）はカード会社側の Web サーバに、SSL 通信の要求を行う。これにこたえて、Web サーバは自分の公開鍵を入れた SSL サーバ証明書を送る。SSL サーバ証明書にはこの証明書の発行元である認証局のお墨付きがあるので、クライアントは公開鍵を信頼できる。

(2)　データの暗号化と復号化

公開鍵を受け取ったクライアントは自分の秘密鍵自体をこの公開鍵で暗号化して送る。この秘密鍵が盗聴されたとしてもこの秘密鍵を正しく元に戻せるのは、公開鍵を送信した Web サーバしかないから安全である。これで両者は秘密鍵を共有することになる。次に、クライアントの Web ブラウザはこの秘密鍵を使って、カード情報と買い物情

報を送信する。最後に、Web サーバはこれらの情報を同じ秘密鍵で解読する。なお、この秘密鍵はランダムに生成されたセッション鍵（今回の取引セッションでのみ使う）である。

2-3　CA/Browser Forum

この動きを推進したのが、アメリカの業界団体として、ボランティア的に創設された CA/Browser Forum である。2016 年現在 50 機関が参加しており、その国別の参加機関数は次の表 1 の通りである。アメリカ 12 機関、中国 5 機関、スイスとトルコが 4 機関、オランダ 3 機関と続き、日本（グローバルサインとセコムトラスト・システム）、英国、台湾、チェコ、スイスが 2 機関で続く。主要な世界各国を網羅しており、情報ネットワークのセキュリティにかける各国の積極的な態度を示している。さらに、ソフトウェアベンダーズとして、アップル、グーグル、マイクロソフト、モジラ（旧ネットスケープコミュニケーションズ）、オペラソフトウェア（ノルウェー）、奇虎 360 が参加している。

しかし、通信経路が暗号化されているシグナルとして南京錠マークがつくからといって、当該 Web サーバが絶対安心といえるかと言うとこれは断言できない。過去に申請元の組織の実在性を確認せずに SSL サーバ証明書を発行した認証局が存在したからである（松本・宇根、p.7）。

2-4　日本におけるフィッシングサイトの現状

JPCERT コーディネーションセンターの 2016 年 7 月から 9 月の報告レポートの結果を示す（表 2 参照）。フィッシングサイトに関連するインシデントは相変わらず多く、467 件にのぼる（1 行目）。

3　ルート認証局

3-1　ルート認証局「TURKTRUST」事件

事の発端は次の通り。2012 年 12 月 24 日に、グーグルのソフトウェアの技術者であるラングレイ氏が同社のインターネット閲覧ソフト「クローム」で、Google.com のドメインを詐称したなりすましのサイト（クローンサイト）を発見し、このフィッシ

表 1　認証機関数

順位	国名	加盟機関数	順位	国名	加盟機関数
1	アメリカ	12	11	イタリア	1
2	中国	5	11	エストニア	1
3	スイス	4	11	フランス	1
3	トルコ	4	11	ブラジル	1
5	オランダ	3	11	ポーランド	1
6	日本	2	11	ドイツ	1
6	英国	2	11	ギリシャ	1
6	チェコ	2	11	サウジアラビア	1
6	台湾	2	11	バミューダ	1
6	スイス	2	11	リトアニア	1
			11	バミューダ	1
			11	イスラエル	1
					50

出所）https://cabforum.org/members/、2016.10.25 閲覧

表 2　2016 年 7 月～ 9 月のインシデント報告

インシデント	7月	8月	9月	合計
フィッシングサイト	166	147	154	467
Web サイト改ざん	236	158	160	554
マルウェアサイト	157	49	131	337
スキャン	371	412	315	1098
Dos/DDoS	5	9	40	54
制御システム関連	2	2	1	5
標的型攻撃	1	6	3	10
その他	74	90	112	276

出所）JPCERT コーディネーションセンター報告レポート

ングサイトには不正なデジタル証明書が付与されていることを確認したのである。第三者に真正なグーグルのサイトと誤認させる恐れがあり、もしもユーザーが誤認した場合、フィッシングによって、ID、パスワード、クレジットカード番号、氏名、住所などの個人情報が詐称される攻撃となりかねない。事態の重要性に気付いたグーグル本社は直ちに調査を開始し、この認証証明書の最終発行元を追跡・確認した結果、トルコのルート認証局 TURKTRUST と判明した。さらなる調査の結果、同局が 2 組織に本来は SSL サーバ証明書を発行するべきところ、2011 年 8 月のある限られた期間にのみ、「誤って」中間認証局証明書を発行したことが判明した（Daly, pp.1-2）。グーグル社は直ちにマイクロソフト社およびモジラ社に連絡し、両社は直ちにインターネットエクスプローラおよびファイアーフォックスでの EGO（アンカラの公共運輸局）による認証のサイトを閉鎖した。ワシントンのトルコ大使館およびニューヨークならびにロサンゼルスの領事館はこの件のコメントを出していない（Menn）。

他の組織は中間認証局証明書を要求したものではないとして自ら TURKTRUST に連絡し、TURKTRUST は中間認証局証明書を無効化した。もう一方の組織、EGO はこれに気付かず、また、TURKTRUST も気付かず、EGO は事実上、中間認証局発行の権限を保持することになった。その結果として、EGO は SSL サーバ証明書を申請するいかなる組織に対して、その申請するいかなるドメイン名にも SSL サーバ証明書を発行したのである。つまり、TURKTRUST をルート認証局とする証明書を発行したのである。その結果、EGO が発行した証明書を持つサイトは世界中のありとあらゆるブラウザーに受け入れられることになった（Ducklin, pp.2-5）。結果として、グーグルのなりすましのドメインに対しても真正性を認証したのである。

さて、2012 年に入って、BYOD のユーザーがおそらくトルコ国内のホテルで、グーグルにアクセスするために、ホテルの EGO ネットワークに切り替えをしたところ、Google.com のウェブ表示画面に対して予想もしない警告画面が表示されたことに驚いて、ヘルプデスクに問い合わせた可能性が強い。

2012 年 12 月 21 日、EGO は、おそらく政治的な理由から、従業員に対する検閲のために、G メール通信の盗聴を試みたとのアメリカ自由人権協会のスタッフのコメントがある（Ducklin）。実際、また、グーグルは偽の認証書を実装するサイトがイラン国内で発覚し同社は同国の G メール利用者にパスワードの変更を求めた（Menn）。EGO は、ネットワーク外部からの HTTPS によるデータのセキュリティ解析を開始した。しかし、これは容易ならざる試みである、なぜなら HTTPS による通信は暗号化されているからである。

HTTP による通信であれば、たとえば、市販のパケットキャプチャソフト「Wireshark」を使えば、ネットワークを流れた通信の中身が見えて、やり取りされたデータの内容がわかる（『日経ネットワーク』、pp.68-70）。しかし、HTTP に security の S がついた HTTPS の通信ではこんな芸当はできない。同じ通信プロトコルであっても大違いである。HTTP ができなくて、HTTPS ができるのは、通信の秘匿性の確保である。同社は MITM 攻撃（福井、pp.105-106）を試みた。つまり、Web ブラウザーから Web サーバまでの SSL 通信を中継局とも言えるプロキシーの段階で盗聴して、暗号化されたデータを復号化して解読し、さらに再度暗号化して元に戻して流すという操作である。このとき、何も知らない閲覧者はブラウザーからの警告画面を受信することになる。プロキシーで一時的に SSL 通信の流れが復号化と暗号化の作業で停止する場合に自動的に警告画面を表示する仕組みとなっている。そこで、一つの回避対策として、プロキシー内部自体にプライベートなルート認証局の証明書を実装すれば問題は回避できることになる。ルート認証局ならば情報の解読が本来の業務であるので、ブラウザーはプロキシーを真正な認証局と誤認するからである。（Ducklin, pp.6-7）。

ところが、こうした煩雑な処理対策を回避するために、現代のルート認証局は、誤ってか偶然かを問わず、中間認証証明書を出した場合も想定して、「Public Key Pinning」を埋め込んで、これを阻止している。これは、MITM 攻撃を回避するた

めに、予め、特定の公開鍵と特定の Web サーバをピン止め（pinning）してつなぐもので、この対応関係をユーザーが知ることができれば、MITM 攻撃を見抜くことができるわけである。このために、Web サーバは紐付けした公開鍵一覧リストを記憶しており、相手側 Web サーバから送信された公開鍵がリストにあるかどうかを確認することで、HTTPS への脅威を回避できるのである。相手側が勝手に実装した証明書と確認できれば、認証を無効化する（https://developer.mozilla.org/ja/docs/Web/Security/Public_Key_Pinning, 2016.10.28 閲覧）。

その後、TURKTRUST が本格的な調査に入っているとの噂が表面化し、この事件は世界中の認証の信頼性を危機に陥れたことになった。

再発を防止するために、グーグル社のローリー氏は、認証の透明性を確保する重要性を強調して、「今後、認証局は、ドメインの運営者に知らせずに当該ドメインを認証することを差し控えて、そのためには、認証局はドメイン認証のためのデジタル証明書を運営者に事前に見える形で発行すべきである」との見解を示した。さらに、「誤って発行した証明書によって、ユーザーが受ける被害をできるだけ食い止めるために、たとえ手間や時間や費用がかかったとしても、ドメインの運営者や関係者がログの解析に協力が欠かせない」とした（Daly）。

TURKTRUST 事件の政治的背景を簡単に述べたい。トルコは 2002 年以来、与党公正発展党（AKP）が単独政権でエルドアン大統領が率いており、クルド人との対立やイスラム勢力の台頭など政治的な撹乱要因が多く、厳しい治安統制を維持している。事件の背景に反政府運動への監視強化の側面があったのかなかったのかは闇の中に封じ込められている。事件の真相は不明である。

3-2　EV SSL 証明書と CA ブラウザーフォーラム

2007 年 1 月 30 日に、日本電子認証協議会（JCAF）が創設された。同会の企業概要には、「インターネット上での商取引や本人確認に不可欠である、PKI（公開鍵認証基盤）をはじめとした、各種電子認証方式の標準化と普及促進を目的として、日本国内の電子認証関連事業者及インターネットブラウザ・ベンダーによって設立された団体です。現在は主に、次世代の世界標準である EV SSL 証明書に関する標準化と普及促進活動を行っています」とある。

我が国はアメリカにならい、SSL サーバ証明書を厳しくした EV（extended Validation）SSL 証明書を導入した。従来の認証局が電話確認などの非常に簡単な確認作業だけで実在性の確認がとれたとして、簡単に SSL サーバ証明書を発行してしまうケースがあった。これでは、「https:// ～」や「南京錠マーク」が表示されたとしても、信頼のおけないサイトがあったことになる。一部の認証局は、TURKTRUST のように、SSL サーバ証明書自体の信頼性を失いかねない事態を招いていた。世界各国の認証局においては、証明書の認証プロセスが厳格性を欠く場合でも、通信データの暗号化は同一の技術基準で実施されるので、鍵マークは表示される。Web ユーザーは企業名を知っていても、その URL は知らないかあやふやに記憶していることが少なくない。フィッシング詐欺のリスクが高まることになりかねない。

この事態を解決するために、日本電子認証協議会の前身である CA ブラウザフォーラムが策定したのが、EV SSL 証明書の発行と管理のためのガイドラインである。このガイドラインによって、証明書発行に関する厳格な認証プロセスが明確化され、EV SSL 証明書を申請する企業や団体は、この厳格な認証プロセスを経て EV SSL 証明書を取得できることになった。EV SSL 証明書を導入したサイトはその証しとして、アドレスバーが緑色に変化するなどのユーザーインターフェイスで、誰もが分かりやすい形で安心感を与えている。しかも、Web サイトの運営組織と EV SSL 証明書を発行した認証局を表示するので、Web 運営組織の実在性が確認できる（表 3 参照）。

表 3　SSL 証明書と EV SSL 証明書の比較

SSL証明書	EV SSL証明書
HTTPS: 鍵マーク	HTTPS: 鍵マーク アドレスバーを緑色表示 Webサイト運営組織表示 EV SSL証明書を発行した認証局表示

これは、アクセスした Web サイトが暗号化通信により盗聴・改竄のリスクから守られること、さらに、その Web サイトを運営する組織の実在性確認ができ、同時にフィッシング等の身元詐称犯罪を防止する効果が期待されている。EV SSL 証明書の発行対象を法人に限定し、登記事項証明書等の提出をもって実在性が確認できる資料とした。EV サーバの名前の通り、従来の SSL サーバ証明書を拡張（Extended Validation）したのである。

4　インターネットショッピングの流れ

Web ブラウザ画面上で商品を買い物かごに入れて支払いを行おうとすると、次の画面がアドレスバーに緑色で表示される。SSL によるので、http が https に切り替わり、右に南京錠マーク🔒がつく。取引先 Rakuten をマウスで示すと、認証実行の主体が Verisign と表示される。

図 2　HTTPS の画面

クリックすると、下記の画面が表示される。

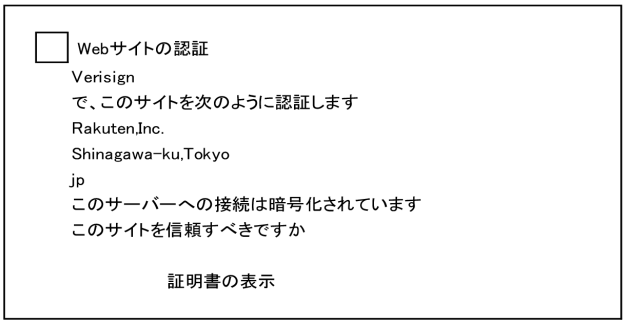

図 3　Verisign の認証画面（1）

［証明書の表示］をクリックすれば、つぎの画面となる。発行者が明示されている。Symantec Class EV SSL CA がルート証明認証局である。

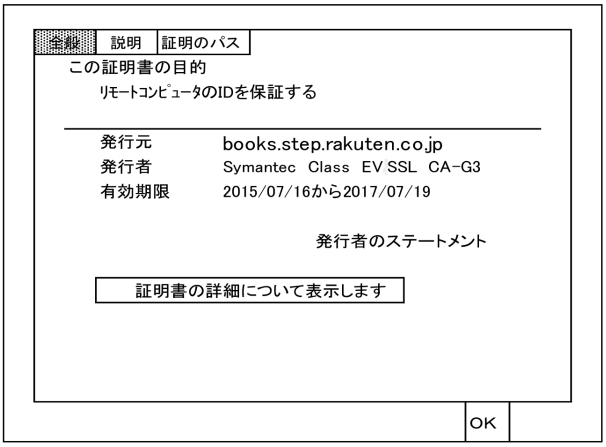

図 4　Verisign の認証画面（2）

さらに、説明タブをクリックすると、下記の図 5 が表示される。公開鍵は 2048bits の RSA 公開鍵暗号方式である。ハッシュアルゴリズムを使用している。

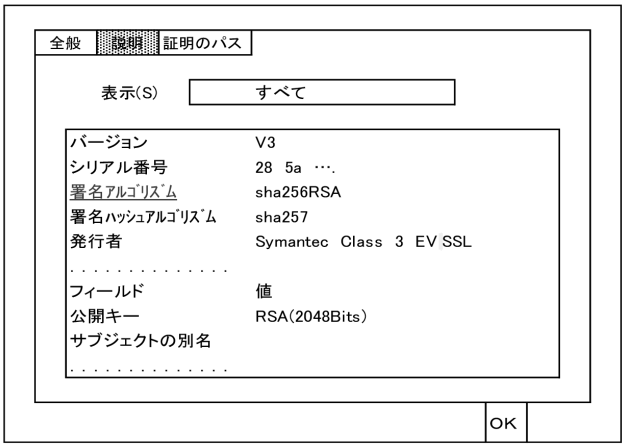

図 5　Verisign の認証画面（3）

最後に、この公開鍵は、一行 25 個（16 進法表示の 2 桁が 25 個）が 10 行と最終行 20 個の計 270 個のデータである。16 進法 2 桁は、8 ビットを示すから、8 × 270 ＝ 2160 ビットを示す。公開鍵の前後にヘッダーとフッターが計 112 ビットついているので、正味の公開鍵の長さは 2048 ビットとなる。

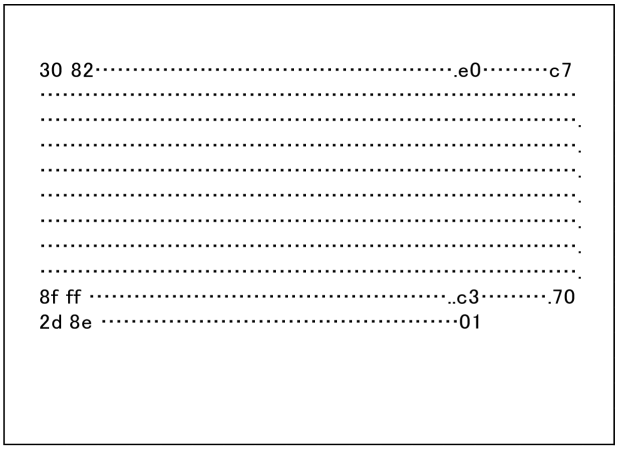

図 6　Verisign の認証画面（3）

5　おわりに

2012 年末に表面化した TURKTRUST 事件を紹介した。サイバー空間の通信の秘匿性は SSL サーバ証明書で守られるとしても、Web サイト自体の実在性を 100％保証しているわけではない。これを証明する EV SSL 証明書の重要性を示した。さらに、ヒューマンファクターの重要性も示した。“Every chain is as strong as its weakest link”（鎖全体の強さは、その中の最も弱い環によって決まる）。ケズゼリイ（Keszthely）が警告するように、サイバー空間のセキュリティを脅かす最大の弱点は、インターネットの管理者やユーザーのケアレスミスなのである（Keszthely, p.8）。

偶発的なヒューマンエラーの他に、意図的なヒューマンエラーがある。認証局が慎重に素性を調べることなく、中間認証局証明書を発行する場合が過去にあった。セキュリティの著名な専門家であるソグホアン（Soghoian）氏の警鐘を紹介して（Menn）本稿を終りたい。「サイバー空間全体のセキュリティは、真正で安全であるべき認証局に全面的に依存しており、（極めてまれであるとしても）証明書を誤って発行してしまった事例が過去にあったという現実は、サイバー空間がいつ破滅するかも知れない時限爆弾を抱えているようなものである」。

（参考文献）

福井幸男（2010）:『情報システム入門－社会を守る暗号セキュリティ編－』、日科技連

福井幸男（2011）:「サイバー空間におけるセキュリティとは何か－ CIA の三要素－」、『商学論究』第 59 巻第 2 号、関西学院大学商学研究会

Daly Kyle (2013): Turkish agency mistakenly allows for spoofing of Google sites, *SNL Media & Communications Report (Jan 7)*

Ducklin, P. (2013): The TURKTRUST SSL certificate fiasco-what really happened, and what happens next?,（https://nakedsecurity.sophos.com/2013/01/08/the-turktrust-ssl-certificate-fiasco-what-happened-and-what-happens-next/、2016.10.23 閲覧）

Keszthely, A. (2015): IT-Security Management: SSL/TLS Certificates, *Management Challenges of the Contemporary Society, Proccedings* 8-2, pp.39-45, Cluj-Napoca:Babes Bolyai University

Menn, Joseph (2013): Corrected－Turkish agency blamed by US companies for intercepted Web pages, *Reuters News*

松本泰・宇根正志（2010）「SSL 証明書における暗号アルゴリズム移行の現状と今後の対応」、ディスカッションペーパー No.2010-J-11, 日本銀行金融研究所

次世代型の SSL 証明書「EV SSL 証明書」の認証プロセスの要件定義と標準化をする業界団体「米国 CA（Certification Authorithy）ブラウザフォーラム（http://www.secu354.co.jp/contents/cyumoku/cyumoku-100525-5-15.

htm、2016.10.20 閲覧）
日本ベリサイン㈱ SSL 製品本部ダイレクトマーケティング部（2011）「ルート証明書を正しく理解する」、10 月 14 日、大阪市北区梅田ビジネスセンター
日本ベリサイン㈱ SSL 製品本部ダイレクトマーケティング部（2012）「ルート証明書を正しく理解する」、4 月 20 日、大阪市北区淀屋橋カンファレンスセンター
日本ベリサイン㈱ SSL 製品本部ダイレクトマーケティング部（2012）「ウェブサイトを取り巻く脅威とその対策について」、10 月 11 日、大阪市福島区 TKP 淀屋橋センター