JPCERT-ED-2008-0001
JPCERT/CC

技術メモ － インターネットを介したサービスにおける 適切な HTTPS の運用

初　版: 2008-03-31 (Ver. 1.0)
発行日: 2008-03-31 (Ver. 1.0)
執筆者: 中津留 勇

本文書の掲載 URL: http://www.jpcert.or.jp/ed/2008/ed080001.pdf

本文書は、サービス提供者を対象に、インターネットを介した多数の利用者に対するサービスにおける HTTPS の適切な運用について解説します。まず、HTTPS を使用したサービスの現状とその問題点を示します。次に、HTTPS の適切な運用を行うにあたり必要となる SSL/TLS についての前提知識を解説します。最後に、インターネットを介したサービスにおける HTTPS の運用で注意すべき点を具体的に述べます。

目次

1. はじめに

SSL/TLS を使用した HTTP 通信（HTTPS）は、オンラインバンキングや e コマース、その他各種会員制サービスなど、多数の利用者が個人情報を含む重要な情報をやり取りするインターネットを介したサービスにおいて、安全な通信を行うために広く使用されています。また、多くのサービス提供者は利用者に対し、「SSL を使用しているので安心してご利用ください」と知らせています。

しかし、一部の Web サイトでは HTTPS の適切な運用が行えておらず、利用者が安全な通信を行えない状態になっています。HTTPS の適切な運用が行われていない原因としては、サービス提供者が SSL/TLS を使用するだけで安全な通信が行われると誤解していることが考えられます。以下に、HTTPS の不適切な運用を行っている Web サイトの例を示します。

- アクセスしようとするとブラウザが警告を発してしまう Web サイト
- ブラウザが発する警告を無視するよう指示している Web サイト

このような Web サイトで警告を無視してアクセスを続けた場合、利用者は個人情報やアカウント情報を含む重要な通信内容を、第三者に盗聴されたり改ざんされたりする可能性があります。このような状態を放置することは利用者にとって非常に危険であり、サービス提供者は早急に運用を見直す必要があります。

本文書では、HTTPS を使用した前述のようなサービスを適切に運用するために必要となる基礎知識と、適切に運用するための具体的な注意点を解説します。

2. HTTPS と SSL/TLS の基礎知識

HTTP の通信を安全に行うため、SSL/TLS を使用して HTTP 通信を行う HTTP Over SSL や HTTP Over TLS というプロトコルがあります。[1]

これらのプロトコルを使用して通信を行う場合、Web サイトの URL は、「http://」ではなく「https://」から始まります。URL の先頭部分である HTTPS とは HyperText Transfer Protocol Secure の略であり、HTTP Over SSL や HTTP Over TLS をまとめて表現する場合にも使われています。

現在、ほとんどの Web ブラウザは HTTPS に対応しており、HTTPS を使用して Web サイトにアクセスした際には、ウインドウの右下やアドレスバーの右に南京錠のマークが表示されます。

本章では、HTTPS の適切な運用を行うために必要となる、HTTPS と SSL/TLS の基礎知識を解説し

ます。

2.1 SSL/TLS の概要

SSL (Secure Socket Layer) と TLS (Transport Layer Security) は、クライアントとサーバ間の通信を安全に行うためのプロトコルです。[4]

SSL は、Netscape Communications Corporation によって開発され、バージョン 3.0 まで更新されました。その後 IETF (The Internet Engineering Task Force) により、TLS という名称に変更され標準化が行われました。2008 年 3 月現在では TLS 1.1 が最新版となっています[2]。本文書では、SSL と TLS をまとめて SSL/TLS と記載しています。

SSL/TLS では、サーバの持つ正規の公開鍵を受け取り、その公開鍵を使用することで一時的な共通鍵を共有し、その共通鍵にて暗号化通信を行います。この手順により、SSL/TLS は以下の 3 つの機能を提供します。

- 通信するサーバの認証
  通信するサーバが、正規の秘密鍵を持つサーバであることを確認し、サーバのなりすましを検知します。
- 通信の暗号化
  通信内容を暗号化することで、通信内容の盗聴を防止します。
- 通信の改ざんの検知
  通信内容のチェックを行い、通信内容の改ざんを検知します。

2.2 SSL/TLS におけるサーバの認証方法

SSL/TLS では、クライアントはサーバの認証を行い、通信しているサーバがなりすましの行われていない正規のサーバであることを確認しなければなりません。そのために、SSL/TLS ではサーバ証明書を使用します。

サーバ証明書とは、認証局と呼ばれる発行機関が、サーバに対して発行する証明書のことであり、事前の鍵交換を行うことなく公開鍵暗号通信を行うための証明書（公開鍵証明書）の一種です。ITU-T の勧告した X.509 v3[3][5]というフォーマットに従って、以下の内容を含むデータに、認証局がデジタル署名を施したものを指します。

- 証明書の発行機関の情報
- 証明書の有効期限や、利用範囲についての情報
- サーバ及びサーバを所持している組織の情報

- サーバの公開鍵

サーバ証明書では、「公開鍵がどのサーバのものであるか」を認証局が第三者として証明しています。クライアントが信頼している第三者の証明であれば、クライアントは公開鍵が正規のものであると信用できます。

SSL/TLS での通信が行われる際、サーバはサーバ証明書をクライアントに送信します。クライアントは、受け取ったサーバ証明書の正当性を検証します。証明書が正当であることを確認した後、その公開鍵を使用して一時的な共通鍵を共有します。こうしてサーバとクライアントの SSL/TLS 接続を確立できれば、サーバの認証が成功します。

なお、HTTPS の場合には、上記の確認に加えて、接続した FQDN と証明書に記載されている FQDN が一致していることを確認します。

もし、証明書の内容が改ざんされていた場合や、証明書の正当性が検証できなかった場合、そして FQDN が一致しなかった場合など、上記の作業で一つでも失敗するとサーバの認証は失敗します。通常、サーバの認証はブラウザ等がすべて自動で行います。認証に失敗した際にはブラウザ等が警告を発します。

2.3 SSL/TLS のサーバ認証と認証局

認証局（CA: Certificate Authority）とは、様々な証明書を発行する機関を指しており、CA 証明書という認証局用の証明書を所有しています。一般的に認証局は他の認証局とツリー構造の信頼関係を形成しており、上位の認証局が下位の認証局に対して CA 証明書を発行しています。このツリー構造の最上位の認証局は、自分自身で発行した CA 証明書（自己署名証明書）を持つルート認証局となっています。認証局は誰でも構築することができ、自由に証明書を発行することができます。SSL/TLS のサーバ証明書検証時には、クライアントはサーバ証明書が信頼できる認証局によって発行されていることを確認します。

信頼される認証局は、自身の定めた運用ポリシーに基づき、証明書の申請者の身元と申請内容を審査し、合格した対象にのみ証明書を発行します。ブラウザ等には、開発者が十分に信頼できると判断したルート認証局の CA 証明書が最初からインストールされています。

ブラウザ等がサーバ証明書の検証を行う際には、サーバ証明書、サーバ証明書を発行した認証局の CA 証明書、CA 証明書を発行した認証局の CA 証明書、と順を追って確認します。このようにして、最終的にインストールされているルート認証局の CA 証明書に到達できれば、それまでのすべての認証局を信頼し、サーバ証明書の内容を信用します。また、ブラウザ等にはユーザが十分に信頼できると判断した CA 証明書、サーバ証明書を後からインストールすることができ、サーバ認証の際には、これらの証明書

に到達できた場合にも、サーバ証明書の内容を信用します。

なお、サービス提供者自身が認証局を構築し自身のサーバ証明書を発行して使用した場合、その証明書をブラウザ等が検証する際に、インストールされている証明書までの認証パスが構築できず、クライアントはサーバ証明書を信用することができません。そのため、ブラウザ等が警告を発します。このような場合には、ブラウザ等に CA 証明書又はサーバ証明書をインストールすることで警告が出ないようにすることができます。しかし、証明書をインストールする際には、証明書の内容又は発行した認証局が信頼できること、及び証明書が改ざんされていないことを、利用者が注意深く確認しなければならないことに注意してください。

また、信頼できる第三者（Trusted Third Party）を設定し、これを頂点とするツリー構造を成す認証局が発行した証明書により公開鍵の正当性を保証する仕組みを、公開鍵基盤（PKI: Public Key Infrastructure）といいます。[6]

2.4　インターネットを介したサービスと HTTPS

サービス提供者は利用者から、安心してサービスを受けられる環境の提供を求められています。
そのため、通常では、個人情報を含む重要な情報をやり取りする際には HTTPS が使用されます。

なお、SSL/TLS を用いたサーバの認証により、正規のサーバであることを確認することができますが、サービス提供者が社会的に信頼できる組織であることは確認できない点に注意してください。

また、認証局がサーバ証明書を発行する際の審査基準は必ずしも同じ水準ではないため、申請者の身元確認が十分ではない場合があります。そのため、世界的に統一された、一定水準以上の厳格な審査基準を満たさなければ発行されない EV SSL 証明書（Extended Validation SSL）が存在します。EV SSL 証明書は、より厳格な身元確認が行われているだけではなく、EV SSL 対応ブラウザで Web サイトを表示すると、アドレスバーが緑色になり、EV SSL 証明書を使用して HTTPS 通信を行っているサイトであることが認識しやすくなっています。必要に応じて導入を検討することをおすすめします。

3.　HTTPS を使用したサービスの適切な運用方法

HTTPS を使用しインターネットを介したサービスを提供する際、サービス提供者は様々なことに注意しなければなりません。本章では、前章で解説した知識を踏まえ、HTTPS に関してサービス提供者が具体的に注意すべき点を、サービスの運用前と運用時に分けて解説します。

3.1　サービス運用開始前

サービスの運用を開始するには、証明書を取得し Web サーバに格納する必要があります。具体的には、以下の順序でそれぞれの作業を行います。

1. 公開鍵のキーペアを作成する
2. 証明書の発行に必要な情報をまとめた証明書署名要求（CSR）を作成する
3. CA に CSR を提出し、証明書を発行してもらう
4. 証明書をサーバに設置し、設定を行う

サービス提供者は、上記の作業を行う中で、次の点に注意する必要があります。

① 使用する暗号の強度を高くする

SSL/TLS では公開鍵暗号方式と共通鍵暗号方式の暗号アルゴリズムを 1 つずつ使用します。それらの暗号アルゴリズムや鍵長は、サーバ側の設定とクライアントの設定に依存します。サーバ管理者が設定できるのは、以下の箇所です。

- 公開鍵のキーペアを作成する際に選択する、公開鍵暗号アルゴリズムとその鍵長
- サーバの設定時に指定する、SSL/TLS で使用できる暗号スイート

これらの設定を行う際には、暗号アルゴリズムの強度に注意しなければなりません。強度が十分ではない暗号アルゴリズムを使用して通信を行えば、通信の解読が容易になり、結果として「通信の盗聴」や「通信の改ざん」が行われてしまう可能性があります。

コンピュータ技術や暗号学の発展により、強度が十分である暗号アルゴリズムや鍵長は時代により移り変わっています。日本では、CRYPTREC（Cryptography Research and Evaluation Committees）が電子政府推奨暗号リスト[7]を公開しているので、参考にすることをおすすめします。

なお、使用している暗号アルゴリズムや鍵長が危殆化した際には、速やかに変更を行ってください。

② サーバの FQDN と証明書に記載する FQDN を一致させる

サーバの認証では、証明書に記載しているサーバの FQDN と、利用者がサーバにアクセスする際の FQDN が一致しているかどうかを調べます。そのため、証明書に記載するサーバの FQDN（通常は CSR の生成時に入力する CommonName）は、証明書を設置するサー

バの FQDN と一致させる必要があります。

FQDN が一致していない証明書を使用して通信を行った場合、通信相手のサーバが正規のサーバであるかをブラウザが確認できず警告を発します。結果として、利用者が「サーバのなりすまし」が行われているのかどうかを判断できなくなります。

③ 認証パスが構築できる証明書を発行する

HTTPS で使用する証明書は認証パスを構築できなければなりません。最も確実で簡単な発行方法は、TTP である CA から証明書を購入することです。

証明書を購入する場合、その CA の証明書、又は上位のルート CA の証明書が、サービス対象となるブラウザにインストールされていることを確認する必要があります。特に、携帯電話などのモバイル端末の利用を想定している場合には注意が必要です。

また、証明書を発行した CA の証明書がブラウザにインストールされていない場合には、ブラウザにインストールされた CA 証明書に到達するために必要なすべての CA 証明書を、サーバがクライアントに送信しなければなりません。したがってそのような場合には、必要な CA 証明書をすべてサーバにインストールしておく必要があります。

なお、サービス提供者自身で構築した認証局が発行したサーバ証明書を使用する場合は、認証パスが構築できず、証明書のインストールを行わなければなりません。しかし、多数の利用者に注意深い確認を行わせてインストールさせなければならないこと、並びにそのための環境を提供することが困難であるため、一般的に推奨されません。

認証パスが検証できない証明書を使用して通信を行った場合、サーバの認証に失敗し、ブラウザが警告を発します。結果として、利用者が「サーバのなりすまし」が行われているのかどうかを判断できなくなります。

3.2 サービス運用時

発行した証明書を使用したサービスの運用時には、以下の点に注意する必要があります。

① 証明書の有効期限に注意する

サーバ証明書には有効期限があるため、期限切れにならないよう注意する必要があります。購入したサーバ証明書であれば、多くの場合、証明書の有効期限が迫ると認証局からメール等にて連絡が来ます。

サービス提供者自身が認証局を構築し、その認証局で発行したサーバ証明書を使用している場合には、サーバ証明書だけでなくサーバ証明書を発行した認証局の CA 証明書の有効期限にも注意しなければなりません。

有効期限が切れた証明書を使用して通信を行った場合、サーバの認証に失敗しブラウザが警告を発します。結果として、利用者が「サーバのなりすまし」が行われているかどうかを判断できません。有効期限が近づいた際には、余裕を持って更新作業を行うことをおすすめします。

4. まとめ

サービス提供者は利用者の安全を確保するため、SSL/TLS を正しく理解し、HTTPS を適切に運用する必要があります。上に挙げた運用方法を実践し、適切な運用を行ってください。

なお、このメモではインターネットを介したサービスで HTTPS の適切な運用を行うための知識に限って解説しています。近年見られるフィッシングや、クロスサイトスクリプティング及び SQL インジェクションのような様々な脅威から利用者及びサービス提供者自身を守るには、HTTPS の運用方法以外にも、ドメイン名の選択から Web サイトの設計に至るまで注意すべき点が数多く存在します。[8][9][10]

利用者が安心してサービスを利用できるよう、より良い安全なサービスの提供を心掛けてください。

5. 参考文献

[1] IETF: RFC 2818 - HTTP Over TLS
http://tools.ietf.org/html/rfc2818

[2] IETF: RFC 4346 - The Transport Layer Security (TLS) Protocol Version 1.1
http://tools.ietf.org/html/rfc4346

[3] ITU-T:
X.509 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks
http://www.itu.int/rec/T-REC-X.509-200508-I/

[4] 情報処理推進機構 セキュリティセンター:
インターネットセキュリティに関する RFC の日本語訳 - 15. TLS
http://www.ipa.go.jp/security/rfc/RFC.html#15

[5] 情報処理推進機構 セキュリティセンター:
インターネットセキュリティに関する RFC の日本語訳 - 12. PKI X.509
http://www.ipa.go.jp/security/rfc/RFC.html#12

[6] 情報処理推進機構 セキュリティセンター: PKI 関連技術解説
http://www.ipa.go.jp/security/pki/index.html

[7] CRYPTREC: 電子政府推奨暗号リスト
http://www.cryptrec.jp/images/cryptrec_01.pdf

[8] 情報処理推進機構 セキュリティセンター: 安全なウェブサイトの作り方
http://www.ipa.go.jp/security/vuln/websecurity.html

[9] 産業技術総合研究所 情報セキュリティ研究センター 安全な Web サイト利用の鉄則
http://www.rcis.aist.go.jp/special/websafety2007/

[10] JPCERT Coordination Center:
フィッシングに関する FAQ - 金融機関やオンラインショッピング事業者などのオンラインサービス提供者向け
http://www.jpcert.or.jp/ir/faq.html#part3