JPRS トピックス & コラム

No.023

今改めて知っておきたい、サーバー証明書の基礎知識 ～サーバー証明書の役割とその概要～

SSL/TLS を用いた安全な通信を実現するために Web サーバーに設定される「サーバー証明書」の役割とその概要について解説します。

SSL/TLSによる通信の保護

本物のWebサイトに似せた偽サイトに利用者を誘導し、利用者がそれと気付かずに入力した機密情報の盗み取りを図る**フィッシング**の事例が、多数報告されています。最近のフィッシングでは、利用者に送りつける電子メールアドレスの差出人の詐称に留まらず、その内容の偽装についても精巧なものとなっており、誘導の手口が巧妙化しています。

フィッシングの事例が増加している背景として、電子商取引（EC）やネットバンキングなど、インターネットがさまざまな経済活動に利用されるようになったことが挙げられます。また、現在では税金の電子申告や国勢調査の回答など、国や政府の重要な手続きにもインターネットが利用されています。

こうした活動や手続きにインターネットを利用する場合、第三者に通信を盗聴されることで認証情報やクレジットカード情報が漏えいしたり、通信内容を途中で改ざんされたりすることがないようにする必要があります。

フィッシングの検知や通信の盗聴・改ざんの防止には、暗号技術を用いた**通信の保護**が有効です。通信を保護することで以下の四つの項目が実現され、より安全に情報をやりとりできるようになります。

① 通信相手の本人性確認：なりすましの防止
② 通信路の暗号化：盗聴からの保護
③ 通信内容の保護：通信内容の改ざんの検知
④ 通信相手の否認防止：通信した事実と内容の事後証明

インターネットの通信、特にTCPのようなコネクション型の通信を保護するためのプロトコルとして、TLS（Transport Layer Security）が標準化されています(*1)。TLSは当初、SSL（Secure Sockets Layer）として標準化されましたが、SSLのプロトコル仕様には致命的な脆弱性が発見されており、TLSへの移行が強く推奨されています(*2)。

SSL/TLSはインターネットをより安全に利用するために必要不可欠な技術であり、サーバー証明書はその実現のために使われています。

サーバー証明書の役割 ～ SSL/TLS による安全な通信の実現～

Webサーバーにサーバー証明書をインストールすることで、WebブラウザーとWebサーバーの間のHTTP（Hypertext Transfer Protocol）の通信をSSL/TLSで保護し、インターネットをより安全に利用できるようになります（図1）(*3)。

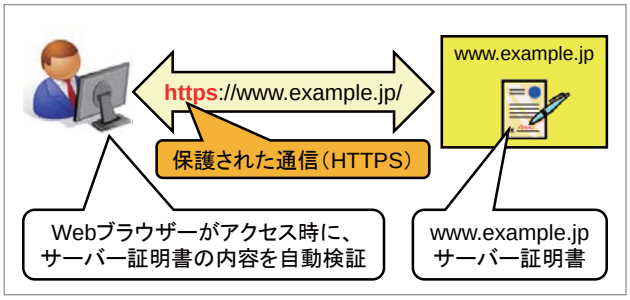

図 1 サーバー証明書による通信の保護

通信がSSL/TLS で保護されている場合、Web ブラウザーのアドレスバーの表示がhttp からhttps に変わります(*4)。HTTPS のSはSecure（安全）を表しており、安全な通信が行われていることを示します。

サーバー証明書の種類

現実世界の証明書には、社員証や学生証などのように民間の組織が発行するものから、住民票、運転免許証、パスポートなどのように公的な機関が発行するもの、それも比較的手軽に発行可能なものから、発行に際し厳密な本人確認の手続きが求められるものまでさまざまなものがあり、それに応じて証明書の信頼度も変わってきます。

(*1) 本稿執筆時点の最新版は2008年にリリースされたTLS 1.2であり、セキュリティをより強化したTLS 1.3の開発が進められています。
(*2)「常時SSL化」「SSLサーバー証明書」など、SSLという名称は現在も広く使われています。そのため、本コラムではSSL/TLSと表記しています。
(*3) サーバー証明書を用いたSSL/TLSによる通信の保護は、Webサーバー以外のサーバーでも利用できます。
(*4) Google Chromeではアドレスバーに「保護された通信」と表示されます。EV証明書（後述）の場合、組織名なども表示されます。

サーバー証明書も同様に、Domain Validation（DV）証明書、Organization Validation（OV）証明書、Extended Validation（EV）証明書の三種類があります。

DV証明書は、申請者がそのドメイン名の管理者であることを確認します。比較的手軽に発行できますが、組織を認証しているわけではないため、証明書をインストールしたWebページを表示する際、Webブラウザーに組織名が表示されません。また、そのドメイン名の管理者であることを確認できれば、既存のドメイン名に似せたドメイン名、つまり、フィッシングに悪用される恐れのあるドメイン名に対しても、発行は可能ということになります。

一方、OV証明書は、組織が確かに存在すること（実在性）を電話による調査や登記簿の確認など、いくつかの手段で認証した上で発行されます。OV証明書はその点で、DV証明書よりも信頼性が高いと言えます。

そして、金融機関など、より高い信頼性が求められる組織において、EV証明書が使われるケースが増えています。EV証明書は業界団体であるCA/Browser Forum (*5)の統一基準に基づく、厳密な認証を経て発行されます。EV証明書では、インストールされたWebサイトにアクセスするとブラウザーのアドレスバーが緑色になり、証明書に記載された組織名が表示されるようになっています。

認証局の役割 ～証明書の発行と失効～

サーバー証明書をはじめとする電子証明書は、**認証局（CA: Certificate Authority）**が発行及び失効を行います。

サーバー証明書ではそのサーバーの管理者が申請者となり、認証局に発行を申請します。申請を受けた認証局は申請者の実在性を所定の方法で確認（認証）し、確認できた相手に対し、証明書を発行します（図2）。

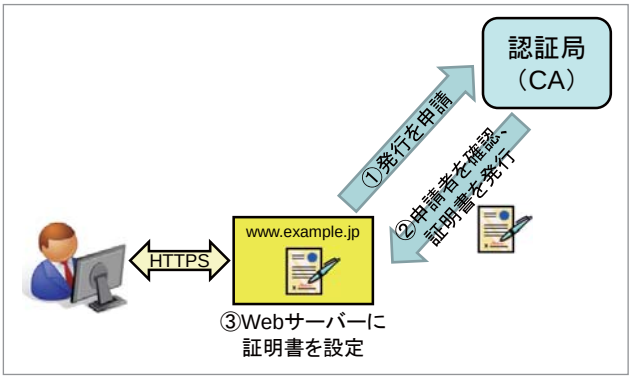

図 2 認証局によるサーバー証明書の発行

認証局は、発行した証明書が何らかの理由で信頼できなくなった場合に、その証明書を失効する役割も担います。証明書の失効が必要になる例として、記載事項の変更、事故による秘密鍵の流出、第三者による秘密鍵の盗難などが挙げられます。

認証局は、証明書の発行と失効により、暗号理論（Cryptography）における**信頼できる第三者機関（Trusted Third Party）**(*6)の役割を果たします。

認証局の信頼性

認証局の運用の不備によりセキュリティ上の問題が引き起こされたケースが、これまでにいくつか報告されています。2011年にはオランダの認証局であったDigiNotarが外部から攻撃を受け、500以上の偽のサーバー証明書が発行される事件が発生しました。

どの認証局を信頼するかは、各Webブラウザーの**信頼されたルート証明書（Trusted Root Certificates）**の設定内容に依存します。DigiNotarの事件では、主要なWebブラウザーから同社の証明書が除外されて信頼されない認証局となり、同社は2011年9月に廃業しました。

こうした事柄を踏まえ、サーバー証明書の発行を受ける際には料金だけでなく、各認証局の管理体制や運用状況なども事前に確認しておくとよいでしょう。

最近の状況

2015年に、パフォーマンスの向上やデータ転送量の効率化などを図ったHTTPの新バージョンである、HTTP/2が標準化されました（RFC 7540）。Google Chrome、Mozilla Firefox、Microsoft EdgeなどのWebブラウザーでは保護された通信路、つまり、HTTPSにおいてのみ、HTTP/2をサポートすることを表明しています。

また、Googleは2014年に検索エンジンの順位決定の要素の一つとして、HTTPSによる通信の保護、つまり「常時SSL化」の有無を検索結果のランク付けに加味すると発表しており、いわゆるSEO対策という観点からも、WebサイトのSSL/TLSへの対応が必要になっています (*7)。

こうした動きからもSSL/TLSによる通信、そしてその実現に不可欠なサーバー証明書の役割が、ますます重要になっています。

(*5) 電子証明書を使った通信の安全性やその利便性を向上させるためのガイドラインを策定している、会員制の任意団体です。主要な認証局とWebブラウザーのベンダーがメンバーとなっており、策定されるガイドラインは業界標準となっています。
(*6) 通信の当事者（送信者と受信者）双方から信頼される、通信の当事者以外の第三者機関。
(*7) HTTPSをランキングシグナルに使用します。
<https://webmaster-ja.googleblog.com/2014/08/https-as-ranking-signal.html>