インターネット上の「なりすまし」を防ぐために ～SSL/TLS サーバー証明書の最新動向～

サイバートラスト株式会社
技術本部　プロダクトマネジメント部
エグゼクティブプロダクトマネージャー
林　達郎　氏

サイバートラスト株式会社
技術本部　プロダクトマネジメント部
エグゼクティブプロダクトマネージャー
岡本　敦　氏

■サーバー証明書の機能

電子商取引を行う上で代表的な脅威である盗聴、改ざん、なりすましといったリスクを回避し、安全な取引を行うために標準的に利用されているのが、SSL/TLS サーバー証明書である。

サーバー証明書の機能は、1990 年代の誕生当初から「通信の暗号化」と「Web サイトの認証」の 2 つである。通信の暗号化という機能によって盗聴と改ざんを、Web サイトの認証という機能によってなりすましを防ぐことができる。

サーバー証明書には、Domain Validation（DV）証明書、Organization Validation（OV）証明書、Extended Validation（EV）証明書の 3 種類がある。DV 証明書はドメインの使用権の有無さえ確認できれば発行されるが、OV、EV 証明書は「申請組織の実在性の有無」、「申請責任者のその組織への所属の有無」までも審査の中で確認される。DV 証明書、OV 証明書、EV 証明書はいずれも暗号の強度に違いはなく、認証レベルに差異がある。

■サーバー証明書の認証レベル

サーバー証明書取得の際に必須となる審査には、1.ドメインの使用権があるか、2.申請組織が実在しているか、3.証明書の申請責任者が本当にその組織に属しているか、の 3 段階あるが、DV 証明書発行の際にはドメインの使用権の有無のみを審査する。他方、OV 証明書と EV 証明書の審査項目は上記の 3 項目すべてであると言う意味で同じであるが、EV 証明書の審査の方がより厳格に行われる（図 1）。

（図 1）

申請組織の実在性の有無の審査では、OV 証明書は「登記がされているか」、または「帝国データバンクのような信用調査会社による、実在性に関する調査を受けているか」、のいずれか一方の条件を満たせば認められるが、EV 証明書は登記とともに信用調査会社の調査を受けていることの両方を条件とする。なお、ベンチャー企業のように設立されてまだ歴史が浅い場合には、銀行口座が開設されているかどうかも併せて確認することもある。

申請責任者が本当にその組織に属しているかを確認する際には、OV 証明書の場合、証明書申請者の連絡先情報を認証事業者の方で調べ、申請責任者本人に対して電話等で申し込みの有無および内容を確認する。他方、EV 証明書の場合は、人事部相当部署に電話をして申請責任者の在籍確認をするとともに、申請責任者の上司に、申込権限を申請責任者に与えているかを確認し、最後に申請責任者本人に申し込んだ事実を確認する。

このように、より厳格な審査を経るからこそ、EV 証明書の場合は、その Web サイトの安全性を閲覧者に視覚的にアピールするための工夫～①PC ブラウザのアドレスバーを緑色で表示、②Web サイトの運営組織の名称を表示～が為されている。

証明書であれば DV 証明書、OV 証明書、EV 証明書のいずれでも良いのかというとそうではなく、現に、某インターネットセキュリティ会社は DV 証明書に対して警鐘を鳴らしており、また IPA（独立行政法人情報処理推進機構）も EV 証明書を推奨している。

■証明書大量使用の時代へ

近時、Google、Microsoft、Mozilla、Apple といった大手ブラウザベンダーは、常時 SSL 化（Web サイトのすべてのページにサーバー証明書を実装すること）を推進しており、特に強力に推進しているのが Google である。Google は「HTTPS Everywhere」とのタグラインのもと、SHA-1 を使用している Web サイトに対して Chrome 上でアラートを出すことで SHA-2 へのアップグレードを間接的に推奨したり、認証事業者の信頼性担保の仕組みである Certificate Transparency（CT）の義務化によってインターネット上から不正な証明書を排除している。また、機密情報を入力するページにサーバー証明書を実装していない場合には、Not secure（安全ではない）という警告を出す「HTTPS by Default」という新たな取り組みも 2017 年 1 月（Chrome 56）から導入する。

これら大手ブラウザベンダーは Web サイト運営事業者に恩恵を与えることによってもサーバー証明書の実装化を推進している。HTTP のバージョンを HTTP/2 に上げると Web サイトの表示速度が 2 倍、3 倍に改善され、快適な Web ブラウジング環境を閲覧者に提供することができるが、HTTP/2 を使うためにはサーバー証明書が必要となる。さらに Google は、Web サイトがサーバー証明書を実装していることを検索結果のランキング決定の条件の 1 つとしている。この SEO 上の優遇措置は全クエリの 1%未満というスモール・スタートで既に開始しており、将来的にはそのウェイトを上げる予定である。このように、サーバー証明書を実装した信頼できるサイトであることは、Web マーケティングの観点からも重要である。

■常時 SSL 時代の課題

常時 SSL 化に踏み切る際には、いくつかの考えるべきポイントがある。サーバー証明書の 1 枚 1 枚につき申請、審査、実装、動作確認、失効（証明書に問題が生じたことでの使用停止）が必要となり、大量のサーバー証明書のライフサイクルに応じた各対応をいかに効率よく行うかが TCO（Total Cost of Ownership）削減の観点より課題となる。

また、ブラウザベンダーはより安全な Web 環境の実現という観点より暗号に対する規制を頻繁に変えるため、サーバー証明書を実装している企業はその都度対応の必要に迫られる。

また、2014 年からはハッカーの攻撃対象が SSL/TLS にフォーカスされてきており、同年に発見された Heartbleed や POODLE から、今年発見された DROWN まで深刻な脆弱性が見つかっている。こうした脆弱性への対応には高度な知識と迅速な対応が求められるため、手厚いカスタマーサポートを提供するベンダーから証明書を取得することが望ましい。

当社は、サーバー証明書の管理をお客様に効率よく行っていただくためのツールと手厚いカスタマーサポートを無償で提供している。なお、脆弱性が発見されると、特設 Web ページを迅速に設け必要な情報を公開するとともに、お客様にメールにより脆弱性の概要と

対応方法をお伝えし、担当営業、カスタマーサポートによるサポートも万全に行っている。

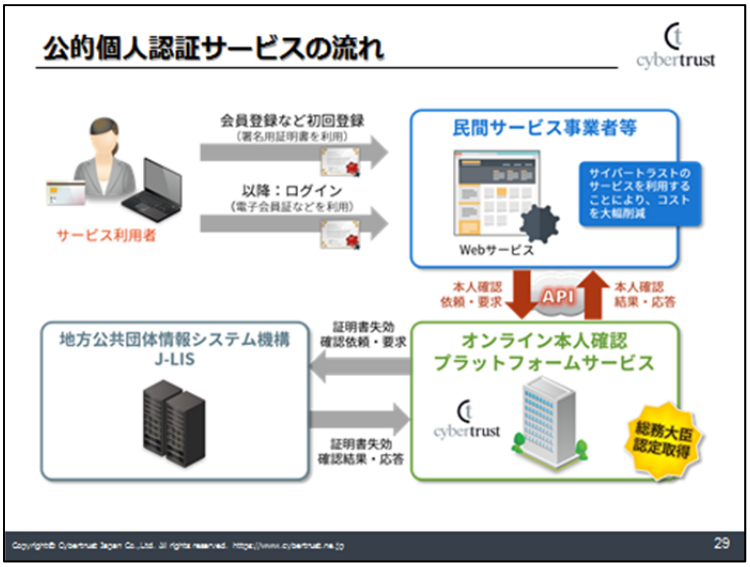
■公的個人認証サービス

平成 28 年 1 月に施行された改正公的個人認証法の主なポイントは 1. 民間事業者が公的個人認証サービスを利用可能に（民間事業者がマイナンバーカードを使って本人確認することが可能に）、2. マイナンバーカードの無料配布、3. 2 種類の電子証明書（署名用電子証明書、利用者証明用電子証明書）を（初回発行に限り）無料インストール、という点である。

署名用電子証明書は旧来の JPKI 同様、署名する目的で使われる。他方、利用者証明用電子証明書には個人を特定する情報は入っておらず、主に、Web サービス等にログインする際に使われる。たとえば銀行の Web サービスを利用するような場面であれば、署名用電子証明書でアカウント登録を行った後、利用者証明用電子証明書を利用してアカウントページへログインする、というような流れになる。

これらの電子証明書を利用した本人確認サービスでは、従来は窓口に赴いたり、顔写真、免許証のコピーの送付などが求められた銀行口座の開設や保険申込みが、マイナンバーカードで署名することによって、オンラインで遠隔地から行えるようになる。また、当社のように総務大臣の認定を受けた事業者が提供する本人確認サービスでは、電子証明書の失効情報を取得できるため、本人確認に加えて、電子証明書の状態が変わった場合に利用者の住所変更、死亡、海外転居などを利用者からの申請を待たずに検知することができる。

Web サービスを提供する事業者は、サービス利用者の会員登録や、登録後のログインの仕組みにこうした本人確認サービスを利用することによって、本人確認の際のコストを大幅に削減できる（図 2）。



（図 2）