インターネット10分講座

おさえておきたい基本や、最新動向を解説するコーナーです。

Webブラウザと認証局、トラストアンカーを巡る技術動向

1 はじめに

パスワードやクレジットカード番号など、重要なデータをインターネット上でやり取りするには、セキュリティが十分確保された通信技術が必要です。現在Webブラウザでは、その役割をHTTPS通信が担っています。

HTTPSの根幹となる技術は、1990年代半ばに旧Netscape社が開発したSSL（Secure Socket Layer）がベースです。その信頼の要となる認証局の役割は、20年以上も変わっておらず、近年のサーバ証明書の誤発行や不正発行などの事件によって、その信頼にほころびが目立つようになってきました。

このような状況で、Webブラウザと認証局がインターネット通信の信頼性を維持するには、どうしたらいいのか？これまでの経緯を振り返りながら、現在導入が進んでいる、証明書の誤発行と不正発行を防ぐ最近の技術動向について紹介します。

2 進むHTTPSの導入とHTTPへの警告

エドワード・スノーデン氏が明らかにした広範囲な国家的盗聴行為により、世界のWebサイトでは全面的にHTTPSを導入する流れが加速しています。Google社の統計情報によると、2018年6月には米国で既に8割以上のページがHTTPS化されています。しかし日本では、最近急速に伸びてきているものの、まだ6割程度です※1。

HTTPS通信は、すべてが平文でやり取りされるHTTP通信と違い、TLS（Transport Layer Security）による暗号化通信を使って、Webのデータをやり取りします 図1 。

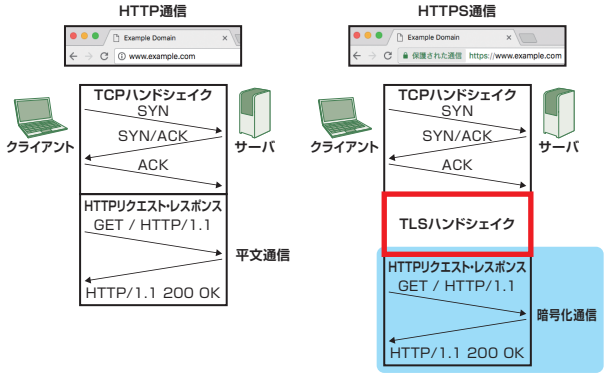

図1 HTTP通信とHTTPS通信の違い

TLSは、HTTPS通信において暗号化によるデータの盗聴や改ざんを防止するだけでなく、サーバ証明書によって接続するアドレス（URL）が、正当なものであることを認証します。Webブラウザのアドレスバーに見かける緑色の鍵マークは、TLSのハンドシェイクが無事終了したことの証です。

ただしこの証は、Webブラウザの種類によって見せ方が異なります。図1では、Google Chrome 67の場合を表しています。HTTPS通信でTLSハンドシェイクが完了すると、緑色の鍵マークと「保護された通信」の文字が表示されます。

一方、平文のHTTP通信は、丸の中にiの字のマークがアドレスバーに入り、ユーザーに対して注意を与えるように表示されています。今後は、さらに注意をうながすよう、警告付きのマークに変わる予定です 図2 。

図2 Google ChromeにおけるHTTP通信の警告

2018年9月リリース予定のChrome 69から「保護されていない通信」という記述に変わり、翌月のChrome 70からは、HTTPページでフォームの入力を行うと、赤文字の警告が表示されるようになります※2。

※1 Google透明性レポート ▶ https://transparencyreport.google.com/https/overview
※2 Evolving Chrome's security indicators ▶ https://blog.chromium.org/2018/05/evolving-chromes-security-indicators.html

このように、今後Webブラウザで平文のHTTP通信を利用する場合、さまざまな警告や制約が課せられるようになり、Webサイトの HTTPS化対応がより一層迫られることになるでしょう。これは、大手のサービスだけではなく、中小や個人が提供しているサービスに対しても、一律に求められることです。

数年前までは、Webサイトを HTTPS化することは、必要な性能を持つ機器と有料のサーバ証明書を調達しなければならないといった、手間とコストがかかる作業でした。しかしここ数年、ハードウェアの進歩により暗号処理性能が格段に向上したCPUが、比較的安価で出回るようになりました。さらに、無料の証明書発行サービス「Let's Encrypt※3」の利用が普及してきて、コスト面の課題も少なくなりました。

Let's Encryptは、サーバ証明書の申請、確認、発行といった手続きをすべて、ネットワーク上において自動化して行えることが特徴です。従来と比べると、HTTPS化へのハードルは非常に低くなっています。今後、HTTP通信に対してはさまざまな機能制限が加えられ、より一層のHTTPS化の推進が行われるでしょう。

3 HTTPS通信における信頼の要、トラストアンカー

HTTPS通信における信頼の要、その一つがトラストアンカーです。トラストアンカーは、OSやブラウザベンダが提供するソフトウェアに登録されている認証局が発行した、ルート証明書を指します。

インターネット上のやり取りは、通常不特定多数の相手と行います。その中でトラストアンカーと認証局は、顔の見えないインターネットの通信に、何かしらの信頼を与える機能を実現します。

トラストアンカーによって、どうやってHTTPS通信に信頼が与えられているのでしょうか? それを理解するため、HTTPS通信に関連する組織と役割を 図3 で表します。

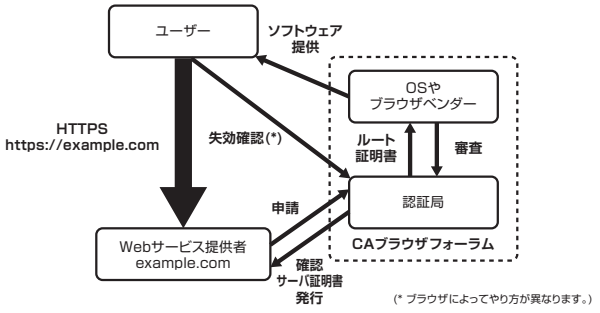

図3 HTTPS通信に関連する組織と役割

現在、認証局の多くはOSやブラウザベンダーとともに、CAブラウザフォーラム※4という団体に参加し、そこで証明書に記載する項目や発行手順などを規定・議論しています。認証局は、その規定をもとに監査会社から監査を受け、監査結果とともにOSやブラウザベンダーに、ルート証明書の登録を申請します。OSやブラウザベンダーは、時間を掛けて細かく申請内容のチェックを行い、問題がなければルート証明書をソフトウェアに組み込んで、ユーザーに提供を行います。

Webサイトの管理者は、HTTPSサービスを開始する際、認証局にサーバ証明書の申請を行います。認証局は、申請に基づき規定で決められた確認を行い、サーバ証明書を発行します。

認証局がどのような確認をするかは、発行する証明書の種類によって異なります。証明書を申請した組織が存在するか確認を行って発行するOV (Organization Validation)証明書や、登記簿など申請組織の実在をより厳密に確認するEV (Extended Validation)証明書などが、一般的な有料の認証局サービスとして提供されています。

Let's Encryptは、ドメインを所有しているかを確認するDV (Domain Validation)証明書にサービスを限定し、無料で証明書を発行しています。発行に伴う大部分の作業が自動化されているため、寄付金でまかなえるレベルにまで運用コストは下がっています。

クライアントはどうやって、HTTPS通信の信頼性を確保しているのでしょうか?その概要を 図4 に示します。

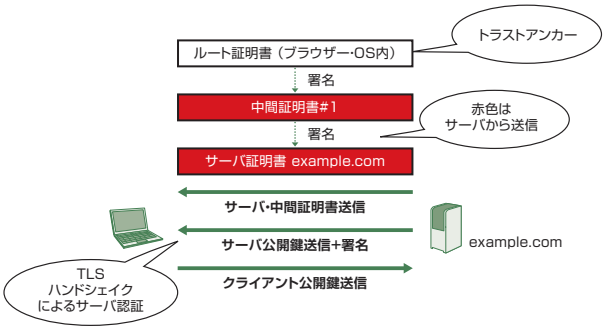

図4 HTTPS通信の信頼の要、トラストアンカー

通常、サーバ証明書は、認証局が管理している中間証明書を使って発行されます。中間証明書は、認証局のルート証明書を使って発行されます。

Webサーバは、HTTPS通信開始時のTLSハンドシェイクにおいて、サーバ証明書と中間証明書の二つをクライアントに送付します。クライアントは、証明書の内容や認証局が提供している失効情報などをチェックし、ソフトウェア内に登録されているルート証明書からサーバ証明書まで署名を検証して、その正当性を確認します。サーバ証明書から始まる一連の証明書が、電子署名によって信頼がチェーンのように繋がる、その最後のアンカーとなるのがルート証明書であるため、トラストアンカーと呼ばれるわけです。

このトラストアンカーが、事前にクライアントに登録されていることによって、ネットワークを介した顔の見えない相手に対して、認証局が代わりに信頼を与える形となり、安全な通信ができるようになっています。

※3 Let's Encrypt ▶ https://letsencrypt.org/
※4 CA/Browser Forum ▶ https://cabforum.org/

4 認証局による証明書の不正発行事件

前述のように、認証局およびトラストアンカーは、HTTPS接続の信頼を実現する重要な役割を持ちます。クライアント内のルート証明書は長期にわたり登録され、現在その数は数百以上に上ります。

多くの認証局は、インターネット上のどのドメイン名に対しても、証明書の発行が可能です。これは、どこか一つの認証局が、操作ミスで間違った証明書を発行したり、不正侵入を受けて不正証明書を発行したりすれば、その影響は全ドメインに及び、HTTPS通信全体の信頼性が土台から揺らぐような事態になりかねないことを意味します。2011年以降、ほぼ毎年のように、認証局からの不正発行事件が発生しています 表1 。

事件が発生するたびに、OSやブラウザベンダーは、ペナルティとして当該認証局が発行した証明書を条件付きで無効にしたり、トラストアンカーから削除したりするなど、事件を起こした認証局を無効化する対策を取ってきました。

根本的な解決方法が見つからないまま、認証局を登録する審査も従来より厳しくし、認証局が発行できる証明書の有効期限を短くするなどの、予防措置も取られてきました。

表1 認証局の主な不正発行事件

2011年	イギリスのComodoが不正侵入を受け、GoogleやMSのドメイン等の不正証明書が発行される。
2011年	オランダのDigiNotarが不正侵入を受け、Gmailなど大量の不正証明書が発行され、イラン国内で利用されていたことが判明。
2013年	フランスの政府系認証局ANSSI傘下の中間認証局から、不正なGoogleドメインの証明書が発行される。
2014年	トルコのTURKTRUSTが誤った中間CAの証明書を発行し、不正なGoogleドメインの証明書が発行される。
2014年	インドのNational Informatics Centre (NIC) の認証局 (CA) を経由して、不正なGoogleやYahooドメインの証明書が発行される。
2015年	中国CNNICから不正なGoogleドメインの証明書が発行される。ブラウザで無効化を行う。
2016年	中国WoSignとStartComが日付を戻して不正なSHA-1証明書を発行していたことが判明。ブラウザで無効化を行う。
2017年	Symantecが証明書の誤発行や規律違反などを繰り返していたことが明るみになった。しかしその後の改善が見られないためブラウザで無効化を決定。

そういった運用上の対策に加えて、技術的に証明書の不正発行を検知・防止する方法も取れないか、次に説明するような技術的対策が考案されてきました。

5 証明書の誤発行・不正発行を防ぐ技術

技術的にどうやって、証明書の不正発行や誤発行を検知したり防止したりできるのか、まだ完全な方法はありません。ただ、いくつかの条件の下で、より信頼性を高める技術は考案されています。その技術について、いくつか紹介します。

5.1 HPKP (HTTP Public Key Pinning)(廃止予定)

証明書に記述されている公開鍵は、更新されると通常新しい公開鍵に変わります。この正しい証明書の公開鍵の情報(ハッシュ値)を、あらかじめWebブラウザに記憶(ピニング)させ、不正発行の証明書を検知する技術です 図5 。

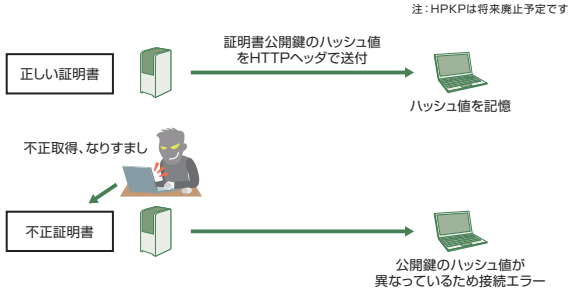

図5 HPKP (HTTP Public Key Pinning)

このピニング方式は、当初Google社が、2011年にオランダDigiNotar社による不正発行の直後に導入を行いました。

Google社やFacebook社等の大手は、Webブラウザのソースコードに直接公開鍵情報を書き込むことによって対策をしていますが、一般のWebサイトまで広げることができないため、HTTPヘッダでWebブラウザに通知する仕様が、2015年にRFC7469として規定されました。しかし実際には、それほどHPKPの利用が広がりませんでした。その理由は、

- 証明書の入れ替えや認証局の変更など運用が大変で、ミスをしたら大事故になる。
- 不正発行された証明書の方がピニング登録されてしまい、長期間にわたり接続不能状態が引き起こされる可能性がある。

といったことが挙げられています。

これらの状況を受け、Chrome 69でHPKPを廃止する予定になりました。

5.2 CAA (Certification Authority Authorization)

多くのWebサイトの管理者は、サーバ証明書の認証局を頻繁に変更することはあまりないでしょう。手続きなどを考えると、多くても数社の認証局だと思われます。

証明書が誤発行される認証局は、これまでまったく付き合いのない認証局の場合が多く、サイト管理者が事前に証明書を発行する認証局を指定して公開していれば、誤発行を防ぐことができるでしょう 図6 。

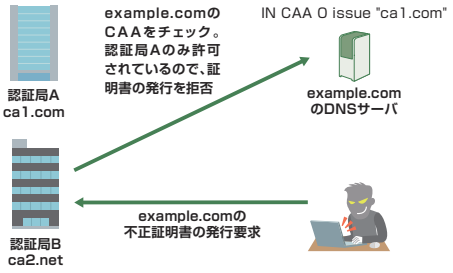

図6 DNS CAA (Certification Authority Authorization)

2013年にRFC6844で規定された、DNS CAA (Certification Authority Authorization)は、DNSのレコードを使ってWebサイトの管理者が、証明書を発行できる認証局の指定をする機能です。

認証局は、サーバ証明書を発行する際に、該当ドメイン名のCAAレコードをチェックします。CAAが設定されており、自社が許可されていることを認証局が確認すれば、証明書を発行する仕組みです。

CAブラウザフォーラムは、2017年9月8日以降、認証局の証明書発行業務で、CAAに対応することを必須としました。DNS CAAレコードは新しいレコードであるため、古いDNSソフトウェアやDNSサービスだとまだ対応していない可能性がありますが、今後徐々に普及していくでしょう。

5.3 CT (Certificate Transparency)

認証局による誤発行や不正発行を防ぐ方法の一つとして、認証局の証明書発行業務を、衆人環視の下でガラス張りにするということが挙げられます。それを実現するのが、CT (Certificate Transparency)の仕組みです 図7 ※5。CTは、2013年にRFC6962として仕様化されました。

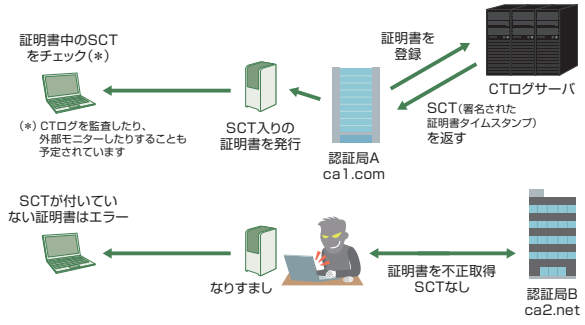

図7 CT (Certificate Transparency)

一般的に発行される証明書は、インターネット上で利用されるものであるため、証明書の内容は公開されても問題ないものが大部分です。一部、社内向けでドメイン名などを隠したい証明書もありますが、現在のCTでは考慮されていません。

2013年、Google社を中心として、証明書のCTログサーバを用意して、証明書の発行時に、ログサーバに証明書のログを残す仕組みを開発しました。登録する際に、CTログサーバからは、証明書データにタイムスタンプを付与したSCT(署名付き証明書タイムスタンプ)を返します。認証局は、SCTを埋め込んだ証明書を作成して、Webサイト管理者に発行します。こうして発行された証明書は、ログサーバに登録されたというタイムスタンプの入った、透かし入りの証明書となります。

Webブラウザは、証明書を受け取ると中のSCTをチェックし、Webブラウザで登録されたログサーバから発行された、署名の検証を行います。SCTが付与されていなかったり、不正なタイムスタンプや署名が入っていたりするような場合には、不正な証明書としてエラーにします。

2015年2月に、ChromeはEV証明書に対してCT対応を必須とし、認証局が対応を行いました。2016年6月には、誤発行が行われたSymantec社に対するペナルティとして、全証明書をCT対応にするように要請しました。

CT導入の効果はありました。これまで発行されてきたサーバ証明書のほとんどがログに蓄積されるため、問題のあるような認証局の運用状態が、次第に明らかになってきたのです。

さらに、Chrome 68(2018年7月リリース予定)からは、2018年4月30日以降に発行される全証明書に対して、CTチェック開始を行う予定です。Apple社のSafariも追随し、2018年10月15日以降に発行される全証明書に対してCTチェックを開始します。

今後は、受け取ったSCTが本当にログに保管されているのか監査を行ったり、ログを常時モニターしたりして、自身のWebサイトの証明書が不正発行されていないか検知するような仕組みの導入も追加で予定されています。

CTはログに証明書の発行を記録するだけなので、証明書の誤発行、不正発行を未然に防ぐことはできませんが、認証局の証明書発行作業を透明化することで、抑止力になるものと期待されています。

6 まとめ

このように、ブラウザベンダーと認証局の間で、HTTPS通信の信頼性を維持していく仕組みが導入されていますが、やはりまだ完全なものではありません。認証局には、さらなる信頼性向上が求められる一方で、無料証明書を発行する認証局の台頭など、コスト的に厳しいビジネスになりつつあります。

従来通りの枠組みのまま、いくつかの認証局が脱落し淘汰が行われていくのか、それとも新しく信頼性を確保するモデルを模索し根本的な解決を探るのか、今後大きな課題として直面するかもしれません。

(ヤフー株式会社 大津繁樹)

※5 Certificate Transparency ▶ https://www.certificate-transparency.org/