WHITE PAPER:

White Paper

偽 SSL サーバ証明書発行事件から見る認証局の役割

Symantec

Norton SECURED
powered by Symantec

CONTENTS

1. はじめに

サーバを SSL 通信対応にするには、SSL サーバ証明書が必要です。証明書は認証局と呼ばれる証明書発行機関が独自の審査基準に基づいて作成します。認証局から発行を受けた証明書をサーバにインストールし、PC 等のクライアントがその証明書の情報を参照することでサーバ間の安全な通信が実現できます。

ではもし認証局が発行した証明書が実は信頼に値しないものであったとしたらどうなるでしょうか。どんなに高度な暗号技術を利用しても、信頼性の基盤自体が揺らいでは、安全な通信を実現することはできません。

2011 年には、証明書の信頼性に関わる事件が連続して発生しました。本ホワイトペーパーでは、なぜこのようなことが起こったのか、証明書の危殆化によるリスクとその対策について考察します。

2. 事件は認証局でおきていた

2011 年に信頼性の低い証明書、安全性の低い証明書が発見され、その認証局が発行した証明書が無効にされるという事件が連続して発生しました。認証局から発行される SSL サーバ証明書は、必ずしもすべてが信頼性の高い証明書とはえいないことが改めて浮き彫りにされました。まずはこの事件について、簡単に振り返ってみることにします。

(1) 連続して発生した認証局が舞台の事件

2011年、偽造証明書に関連した事件が連続して発覚しました。

- 2011 年 3 月、アメリカの認証局から Gmail、Skype、Mozilla、Microsoft アップデートなどの偽造証明書が発行されるという事件が発生。
- 2011 年 8 月、オランダの認証局 DigiNotar から 531 件の偽造証明書が発行されていたことが判明。
- 2011 年 11 月、東南アジアの中間認証局から強度の低い秘密鍵を使用しているなどの深刻な欠陥のある 22 件の証明書が発行されたことが判明。

事件の共通点は、正当な証明書と区別の付かない、「信頼してはいけない」証明書が発行されたということです。

DigiNotar と東南アジアの事件の舞台となった認証局からは、当地政府関連サイトへの証明書も発行されていたため、大きな混乱を招くことになりました。

偽造された証明書の発覚に伴って、Microsoft や Google、Mozilla などの代表的なウェブブラウザベンダは緊急のアップデートを行い、舞台となった認証局自体を信頼される認証局のリストから削除し、その認証局発行の証明書を失効させるという対応をとることになりました。

(2) 原因は認証局のインフラの脆弱性

偽の証明書はどうして発行されてしまったのでしょうか。DigiNotar に関しては、「ComodoHacker」と名乗る人物が不正侵入したという犯行声明を発表しています。インフラの脆弱性を突いて、システムへのパスを不正に入手して侵入し、証明書を発行するための情報を盗み出すことで、偽造証明書の発行が可能になったということです。事件の原因は、不正侵入を許した認証局の脆弱性にあったようです。また侵入後、善後策の実施が遅れたことで被害を拡大させたことも不信に繋がり、やがて DigiNotar は倒産することになりました。

3. 事件の背景 — 信頼できる証明書とは

証明書が信頼できないようでは、通信の安全性を保証する基盤が崩れてしまいます。信頼できない証明書が氾濫してしまうと、通信相手が保証されず、暗号強度を高めても通信の安全性が崩れる結果となります。

通信の安全性を確保するためには、証明書が通信相手を保証してくれるような信頼できるものであることが必須です。それでは、信頼できる証明書とはどのようなものなのでしょうか。

（1）誰でも発行可能な証明書、何故それを購入するのか

SSL 関連のモジュールがインストールされている UNIX 系の OS や Windows サーバならば、簡単な操作で、SSL サーバ証明書を発行することが技術的には可能です。

では、何故証明書を認証局から購入するのでしょうか。それは、「信頼できる第三者に証明書の信頼性を客観的に保証してもらう」ためです。

例えば、免許証やパスポートは認定された機関が発行したものだけが有効です。自分で印刷したものでは免許を取得したことや国籍を客観的に保証することはできません。

インターネットでも同様のことが言えます。インターネットを安全に利用できるようにするためには誰かがそのサーバ、サイトの存在を確認したことを客観的に保証する必要があります。その役割を担っているのが「第三者認証局」という組織です。

（2）証明書の信頼性とは

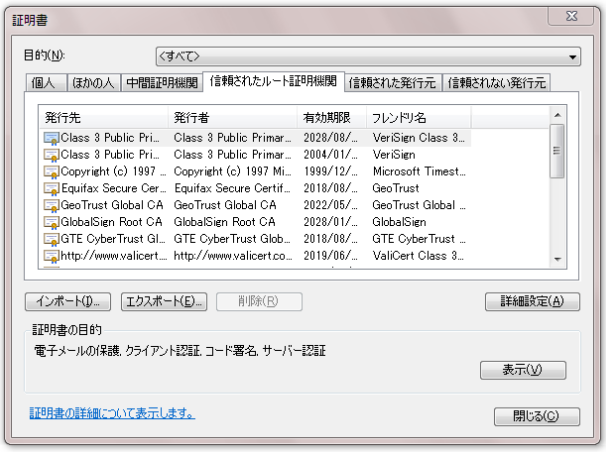
発生した一連の事件は、SSL 通信の仕組みや暗号アルゴリズムに問題があった訳ではありません。認証局が不正な証明書の発行を許してしまったことに起因しています。

信頼できる証明書とは、厳格な審査と徹底管理された工程のもとで発行されたものでなければなりません。

（3）証明書の信頼性は認証局に依存 — 認証局の階層構造 —

それでは、証明書の信頼性は誰によって保証されているのでしょうか。SSL サーバ証明書として一般的に利用される証明書は、上位の認証局が下位の認証局の証明書を保証するという階層的な構造になっています。認証局は、さらに上位の認証局によって保証されているという構造です。

階層の一番上位にあたる認証局は「ルート認証局」と呼ばれていて、ウェブブラウザなどで認証局が発行したルート証明書を表示して、確認することが可能です。



ルート認証局は、ルート認証局自身による保証以外に、第三者の監査によって信頼性を保証しています。ウェブブラウザやアプリケーションに標準的に組み込まれているルート認証局証明書は、信頼に値する証明書を発行する認証局として認められていることを示しています。シマンテックも信頼されたルート認証局の代表的なひとつです。

（4）信頼できる認証局とは

認証局自体の信頼性はどのように判断すればいいのでしょうか。

認証局の信頼性については、各認証局が設けている CPS（Certification Practice Statement：認証実施規程）で確認することができます。CPS とは認証局が証明書の発行、管理、失効及び更新を含む一連のサービスを提供する際に採用する手続きを記載したもので、その他にも設備や技術的要件なども反映されています。

また、認証局は、Web Trust for CA という第三者による監査基準に準拠することも求められています。この監査によって、運用が適正に行われているかどうかが判断されます。Web Trust for CA では次のような基準が監査の対象となっています。

- 認証局業務の開示
- サービスインテグリティ（サービスの完全性）
- 認証局環境の統制（コントロール）

シマンテックでは上記の基準に加えて、物理ファシリティの堅牢性、ネットワークファシリティの堅牢性、バックグラウンドチェックをした人材による認証作業など、その他の重要な要素を基準として追加して、認証局としての信頼性を保つ努力をしています。認証局として認められているということは、こういった作業手続きや情報の保管などが、一定の安全基準を満たしているということなのです。

4. 想定されるリスクとその影響

証明書が偽造された時のリスクと影響について考えてみましょう。

（1）利用者へのリスク

証明書が偽造されると、フィッシング詐欺の被害が発生する可能性が高くなってしまいます。偽のサイトが信頼できるサイトであると証明されてしまうためです。フィッシング詐欺によって、各種の個人情報が漏洩してしまう可能性も大きくなります。

（2）サイト運用上のリスク

証明書が信頼できないものだと発覚した場合、一般的に発行元の認証局によって、その証明書だけの失効処理が行われます。しかし、DigiNotar のケースに見られるように認証局自体が信頼できないと判断されると、ブラウザや OS、その他のアプリケーションで、ルート証明書が無効となり、その認証局が発行した証明書はすべて失効扱いにされてしまいます。そうなった場合、その認証局から発行された証明書を使用しているサイトは、一旦サービスを停止して、信頼できる別の認証局から証明書を再度取得する、といった対応が必要になります。その費用や対応にあたる人件費、サービス停止による売上げ減少など大きな損害を被ることになります。

利用者にとっては、証明書の問題ではなく、サイトを運用する組織の問題に見えてしまう可能性もあるので、サイトを管理する組織自体の信頼性にも影響を与えかねません。

5. リスクへの対処 —サイト管理者が検討すべきこと—

証明書の危殆化のリスクにはどのように対処したらいいのでしょうか。リスクへの対処方法について考察していきます。

（1）認証局の安全性の確認と信頼できる認証局の選択

まず、大切なことは、信頼できる認証局によって発行された SSL サーバ証明書を導入するということです。認証局の信頼性は、CPS などで確認できます。認証局の運用方針に関する情報は認証局のウェブサイトで公開されていることが一般的です。

（2）セキュリティアップデートの実行

OS やブラウザのベンダが発行するセキュリティアップデートには、信頼性の低い認証局の証明書の失効などの処理も含まれています。アップデータの安全性・信頼性・影響範囲などを確認した上で、迅速にアップデートすることで安全な環境を保つ手助けとなります。

6. シマンテックの取り組み

シマンテックが、信頼される認証局として取り組んでいる各対応は、CPS（Certification Practice Statement：認証業務運用規程）に記載して公開しています。

CPS には、認証業務に関する規約が詳細に定められています。シマンテックでは、この規約に厳密に従って認証業務が執行されています。

インフラの強化など自社内で信頼性の向上に努力するだけでなく、ISAE3402「第三者のサービス受託会社の統制活動に関する保証報告」に基づき、外部機関による監査も受けています。第三者による客観的な評価を受け入れることで、より高い信頼性を得られるように努めています。

7. まとめ

2011 年に連続して発生した証明書の信頼性にかかわる事件。その共通点は、正当な証明書と区別の付かない「信頼してはいけない」証明書が発行されたというところにありました。

利用者の安全性を確保するためには、信頼できる認証局が発行する信頼できる証明書を利用することが重要です。つまり証明書は、認証局による厳格な審査と徹底管理された工程のもとで発行されたものでなければなりません。

証明書導入時には、CPS や過去の運用実績などの情報を確認して、認証局の信頼性を評価することが大切です。あわせて認証ファシリティそのものの堅牢性の確認をお勧めします。シマンテックでは、CPS に定められた規約に厳密に従って、認証業務が執行されています。外部機関の監査も受け、第三者による客観的な表を受け入れることで、より高い信頼性を得られるように努めています。

合同会社シマンテック・ウェブサイトセキュリティ
https://www.jp.websecurity.symantec.com/
〒104-0028　東京都港区赤坂1-11-44赤坂インターシティ
Tel : 0120-707-637
E-mail : websales_jp@symantec.com