WHITE PAPER

ウェブサイトの信頼性を高める EV SSL 証明書

VeriSign®
A SYMANTEC AFFILIATED COMPANY

注：
本書は VeriSign, Inc. のホワイトペーパーの翻訳版であり、記載されている全てのサービス・製品を日本ベリサインが提供していない場合があります。また、記載されている価格についても米国内での価格になっておりますことをご了承ください。詳細は担当営業までご連絡ください。

WHITE PAPER

CONTENTS

オンラインビジネスは、信頼性欠如の危機に直面しています。ウェブサイトのセキュリティに対する信頼が低下し、オンラインショッピングの回数を減らしたり、完全に止めたりする消費者が増加しています。米国 Forrester Research 社が実施したアンケート調査によると、インターネットユーザの 24% が、ウェブサイトの安全対策に不安を感じているためにオンラインショッピングを躊躇しており、同様の理由で 61% のインターネットユーザが、オンラインショッピングの回数を減らしたと報告されています。

主要なブラウザベンダやベリサインをはじめとする認証ベンダによって設立された業界団体である CA/ ブラウザフォーラムは、オンラインビジネスを展開する企業と消費者のために、Extended Validation SSL 証明書（EV SSL 証明書）と呼ばれる SSL サーバ証明書の実用化に努めてきました。この証明書は、正当なウェブサイトに対する消費者の安心感を増大させ、フィッシング攻撃の実効性を低下させることによって、オンラインビジネスを活性化します。

この EV SSL 証明書は、2007 年から導入され、オンラインビジネスを展開する企業は、消費者に対して本物のウェブサイトであることを明示できるようになり、消費者は本物のウェブサイトであるかどうかを確認できるようになります。

SSL のアイデンティティ立証能力の低下

実世界にある企業を模倣することは非常に困難ですが、インターネット上では簡単に模倣することができるため、消費者はフィッシング詐欺と呼ばれる被害に遭う可能性があります。SSL サーバ証明書は、そのような模倣を防ぎ、消費者を保護することを目的として開発されました。

当初、SSL サーバ証明書はウェブサイトのアイデンティティを立証するのに十分な役割を果たしていました。しかし、SSL サーバ証明書の認証基準には業界標準が存在せず、それぞれの認証局が独自の基準を採用してきたため、消費者は目的のウェブサイトが本当に信頼できるウェブサイトであるかどうかを確認するために、非常に多くの手間と時間を費やさなければなりませんでした。また、現在はインターネットの操作に不慣れな利用者層が急増したことに加えて、一般的なブラウザでの鍵アイコンの視認性が低いこともあり、従来の SSL サーバ証明書だけでは、フィッシング詐欺の対策としては十分とは言えなくなってきました。

消費者に信頼されるアイデンティティの確立

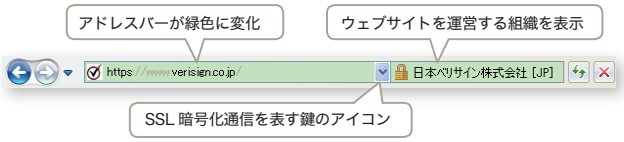
SSL サーバ証明書が、本当に信頼されるようになるためには、2 つの弱点を補強する必要がありました。最初に、ウェブサイトを運営する組織の実在性をより高い精度で立証する新しい SSL サーバ証明書が必要でした。次に、消費者がそのウェブサイトの認証情報を容易に識別できるブラウザのインタフェースが必要でした。このような過程を経て開発された新しい証明書が、EV SSL 証明書です。

主要なブラウザベンダ、認証ベンダなどによって構成される CA/ ブラウザフォーラムは、EV SSL 証明書を発行するすべての認証局が順守すべきガイドラインを策定しました。EV SSL 認証のガイドラインは、組織の実在性認証の手順を基に作成されています。認証局は、ガイドラインに則った認証を完了すると、EV SSL 証明書を発行することができるようになります。

EV SSL 証明書は、従来の SSL サーバ証明書と同様に機能します。実際、EV SSL 証明書を認識するように設計されていないブラウザは、従来の SSL サーバ証明書と同様の動作をします。しかし、EV SSL 証明書に対応した新しいブラウザでは、証明書の視認性を高め、より多くの情報を表示するようになっています。

信頼されたウェブサイトであることを示す緑色のアドレスバー

主要なブラウザには、ウェブサイトを運営する組織の実在性確認をより強化した機能が追加されています。最も顕著なのは「緑色のアドレスバー」です。Internet Explorer 7 以降、FireFox3 以降、Chrome 等のブラウザで EV SSL 証明書が発行されたウェブサイトにアクセスすると、ブラウザのアドレスバーが緑色に変わり、サイト運営組織名が表示されます。この視覚的な変化は、そのウェブサイトを運営する組織の実在性がより高い精度で検証されているということを表します。アドレスバーの緑色は「そのウェブサイトは信頼されており、安心して利用できる」ということを意味します。



※ 上記の表示は Internet Explorer 8 の場合です。

2006 年秋、米国ベリサインはオンラインショッピングの経験者を対象としたアンケート調査を実施しました。その結果、これらのインターフェイスはかなり効果的であることが確認されました。

- 回答者の 100% が、緑色のアドレスバーを表示した EV SSL 証明書を導入したウェブサイトとそうでないウェブサイトを識別しています。
- 回答者の 100% が、クレジットカード情報を入力する場合に、緑色のアドレスバーを表示したウェブサイトの方を選択する傾向にあります。
- 回答者の 98% が、EV SSL 証明書を導入したオンラインショップとそうでないオンラインショップがあった場合、緑色のアドレスバーを表示したオンラインショップの方を好意的に感じます。
- 回答者の 80% が、以前は緑色のアドレスバーを表示していたが、現在はそうでないウェブサイトでの購入を躊躇します。

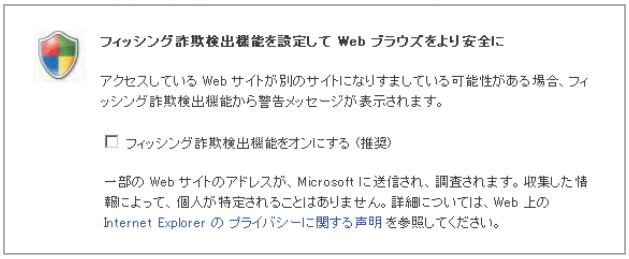
Internet Explorer 7 以降には、アドレスバーの右にセキュリティステータスバーというフィールドが追加されています。このフィールドは、ブラウザがユーザに対して、ウェブサイトの信頼性を確認するための有効な情報を提供できるときに表示されます。EV SSL 証明書を持つページでは、セキュリティステータスバーにウェブサイトを運営する組織名が表示されます。この文字列は認証局がその組織名を検証して証明書の中に記載したもので、消費者はこの文字列の正確性を信頼することができます。

セキュリティステータスバーには、そのウェブサイトに証明書を発行した認証局名も表示されます。これにより、消費者は取引を始める前に、ウェブサイトに採用されている証明書のブランドを確認できるようになります。

SSL サーバ証明書のブランドによって、消費者の取引傾向に影響があることが調査によって分かっています。たとえば、ヨーロッパの大手旅行サイト Opodo は、同社の注文ページでベリサインのマーク※1 を掲出した場合と掲出しなかった場合を比較するテストを行い、マークを掲出したページの売り上げが掲出しなかったページの売り上げより 10% 高いことを確認しました。Opodo のサービスマネージメント責任者の Warren Jonas 氏は、「信頼という要因が、オンラインショッピングに及ぼす影響を実感しました。以来、当社では、ヨーロッパ各拠点のすべての決済画面には必ずベリサインのマークを掲出しています」と話しています。さらに、有名なマーケットリサーチ会社である米国 TNS 社は、2006 年夏にオンラインショッピング経験者を対象として、セキュリティを意味するオンラインのマークについて調査を行い、オンライン取引で信頼を表すマークとして、ベリサインのマークの認知度は他のマークをはるかに凌いで最も高かったと報告しています。同調査は、世界のオンラインショッピング経験者の 56%がベリサインのマークを認識していることも示しており、これは第 2 位の SSL サーバ証明書ブランドの 8 倍に相当します。これらの結果から、ユーザはウェブサイトに導入する SSL サーバ証明書のブランドを重視していることがよくわかります。よって、インターネットユーザに最も認知されているブランドを選択すれば、売り上げを 10% 以上増大させることが可能になります。

EV SSL 証明書対応ブラウザは、EV SSL 証明書の高い信頼性を保証するために、緑色のアドレスバーやその他のインターフェイスを表示する OCSP（Online Certificate Status Protocol）を有効にすることを要求しています。OCSP を有効にすると、ブラウザは SSL サーバ証明書が取り消されていないことをリアルタイムで確認します。最新のブラウザは、OCSP をサポートしていると同時に、インターフェイスに OCSP を無効化するコントロールを搭載しています。OCSP を有効にすることによって、ユーザは、そのウェブサイトが EV SSL 認証のガイドラインに則った厳格な基準に基づいて認証されていることだけでなく、証明書の取り消しが要求されるような事態が発生していないことも確認できます。

Internet Explorer 7 以降のブラウザでは、OCSP を直接有効にするだけでなく、OCSP を必要とする他の機能をユーザが有効にしたときも、自動的に OCSP を有効にします。この機能は、フィッシングフィルター (Phishing Filter) と呼ばれ、正当性が疑わしいと分類されたウェブサイトにアクセスしようとすると、赤色や黄色のアドレスバーを表示します。フィッシングフィルター機能を有効にすると、EV SSL 証明書のインターフェイスも有効になります。



フィッシングフィルターを有効にすると、EV SSL も自動的に有効になります。

※1：現「ノートン™ セキュアドシール」

EV の動作

EV SSL 証明書のアーキテクチャは、消費者がウェブサイトの存在性を確認するために信頼できる情報が提供されるように設計されています。EV SSL 証明書の信頼性は、新しく、分かり易いインターフェイスとともに、1) 認証手順の修正、および 2) リアルタイムな証明書の確認に依存しています。

1) 最初は認証手順を見直しました。CA/ ブラウザフォーラムは、信頼できる認証結果を保証するために、慎重に EV SSL 認証のガイドラインを策定しました。同ガイドラインでは、資格のある認証局は、証明書の申請者から申告された情報をそのまま使用するのではなく、認証局が独自に確認した一次情報を使用しなければならないと要求しています。同ガイドラインは、何百万ものウェブサイトを 10 年以上にわたり認証してきた実績のある技術を採用しています。また、認証局は、EV SSL 認証のガイドラインを順守していることを立証するために、年に一度 WebTrust による監査を受ける必要があります。この手順によって、証明書に記載されているすべての情報が正確であることや、証明書の申請者が、その組織の証明書を取得する権限を有することが保証されます。

2) 次は、認証局が認証した内容が証明書に正確に反映されていることと、証明書が EV SSL の認証基準に正しく適合していることを確認するようにしました。すべての SSL サーバ証明書にはセキュアなハッシュ関数を含んでおり、万が一、何らかの改ざんが行われた場合には正しく機能しないので、証明書の完全性は保証されています。さらに、EV の機能が、リアルタイムに証明書の有効性を確認することによって、証明書が良好な状態であることを保証しています。これらを確認する方法は、2 つの機能として備わっています。一つめの機能は前述の OCSP です。OCSP が各証明書の取り消し状況をリアルタイムに確認するので、EV SSL 証明書に、危殆が発生した場合や他の何かの理由で証明書の取り消しが必要である場合は、EV に対応したブラウザでは、その証明書が有効であるという表示はされません。二つめの機能は Microsoft® ルートストアです。Internet Explorer 7 以降のブラウザは、不正な EV SSL 証明書に対処するために、Microsoft® ルートストアをリアルタイムに参照して、そのルート証明書が EV SSL 証明書として承認されていることを確認します。ルート証明書が Microsoft® ルートストアに登録されていない場合、その EV SSL 証明書では緑色のアドレスバーやその他の EV のインターフェイスは機能しません。同様に、年に一度実施される監査に合格しなかった場合や、不適切な EV 証明書を繰り返し発行した場合、Microsoft は Microsoft® ルートストア内の承認された EV ルート証明書リストからそのルート証明書を削除することができます。この処置によって、疑わしいルートが発行したすべての証明書は、緑色のアドレスバーや EV SSL 証明書独自のインターフェイスが無効化されます。

WPEVSSL2009_1204

日本ベリサイン株式会社
https://www.VeriSign.co.jp/
〒104-0028　東京都中央区八重洲 2-8-1
Tel : 03-3271-7017
E-mail : websales@verisign.co.jp