WHITE PAPER

自己署名のSSLサーバ証明書の隠れたコスト

信頼されたセキュリティベンダーの証明書と比べて、自己署名証明書が高コストで高リスクとなる理由

From Symantec™

VeriSign
Authentication Services

VeriSign®
A SYMANTEC AFFILIATED COMPANY

WHITE PAPER

WHITE PAPER

CONTENTS

はじめに

企業は、業績が急成長しているときも常に最終収益を注視しています。通常、企業にとってセキュリティは、費用削減の第一の対象とはしないものですが、一部の IT プロフェッショナルは、予算からサードパーティの SSL 認証局 (CA) から発行される SSL サーバ証明書を排除することで、簡単にコスト削減できると考えます。

企業のホームページや電子商取引のページなど対外的なサイトに対しては、SSL セキュリティに費用をかけることが必要であると見なされますが、対内的なサイトについては、自己署名の SSL サーバ証明書が代替手段になると、一部の IT プロフェッショナルは考えます。イントラネットのポータルや wiki のような対内的なサイトをホストするサーバーには、内部の従業員のみがアクセスするため、自己署名証明書を利用すれば、事実上費用をまったくかけずに十分な保護が得られる、と信じています。

しかしこの種の方法は、リスクがあります。

SSL サーバ証明書の総所有コスト（TCO）は、証明書の価格そのものよりもはるかに大きくなります。セキュリティ用のハードウェアにはじまり、管理ソフトウェアや、データセンター施設などに至るまで、安全な自己署名アーキテクチャの確立にかかるコストは、みるみるうちに膨らみます。それだけでなく、自作式による SSL セキュリティへの取り組みでは、組織がさまざまな形で危険にさらされる（技術的な観点でもビジネス的な観点でも）可能性があります。

本ホワイトペーパーでは、自己署名式アーキテクチャの場合と、サードパーティの SSL 提供ベンダーと連携した場合の比較も含め、自己署名の SSL サーバ証明書の真の TCO について解説します。本書で解説する問題点は、企業が自己署名証明書の利用を決定する前に、十分考慮するに値するものです。

サードパーティによる認証と自己署名証明書の違い

1995 年に SSL プロトコルがデビューしたとき、世界にようやく、ウェブ上で安全な取引を行うための基礎ができました。以来 SSL は、ウェブベースの取引で使用される、最も重要な認証プロトコルとして進化してきました。

なぜ SSL が必要なのでしょうか。インターネット上でのほとんどのウェブトラフィックは、暗号化されていない形式でやりとりされます。これは、技術的に十分な専門知識とツールがあれば誰でも簡単に、二者間の会話を「盗聴」できることを意味します。SSL セキュリティは、ウェブサーバーとブラウザ間を移動するデータを暗号化することで、情報の傍受とデコードを極めて困難にします。

ただし SSL セキュリティは、単に暗号化のみを行うためのものではありません。純粋に技術的な観点では、公開鍵基盤 (PKI) はデータ転送を安全に守るという優れた仕事をしますが、トランザクションのセキュリティはそれだけでは十分ではありません。取引の当事者は、コミュニケーションの相手が正当な参加者であると、どうすれば確信できるでしょうか。例えば、顧客が高価なカメラを購入しようとしている場合、企業はその顧客に対して ID 情報の裏付けを示せることが必要です。さもなければ、顧客のクレジットカード情報は送信中に暗号化されるものの、もしリテールのウェブサイトが詐称されたものであれば、暗号化されたデータがすべてネット犯罪者に送信され、簡単に解読されてしまう可能性があります。

サードパーティによる検証が重要なのは、この点です。信頼された、独立した認証局によって署名された証明書は、その証明書を所有する組織が確かに実在することを、保証します。

とはいえ、技術的な観点では、SSL セキュリティが機能する際に、サードパーティによる検証は必須ではありません。企業は証明書に自己署名することができます。自己署名証明書を使用した場合、実際にはその企業は、「自分は本人です。信頼してください。」と言っていることになります。

しかし、Internet Explorer や Firefox のような標準的なウェブブラウザには、この自己署名は有効ではありません。自己署名証明書で「保護された」サイトにアクセスしようとすると、通常は、署名した組織が不明であり信頼できない、というエラーメッセージが表示されます。当然のことながら、この種のメッセージは、見込み客やパートナー企業、および他の関係者に、不安を与えます。このため、対外的なウェブサイトに自己署名する企業は多くありません。ユーザーの信頼を維持することは、とても重要です。

一方、対内的なサイトやサーバーは、SSL サーバ証明書のユースケースとして、異なるシナリオを提起します。企業の電子メールサーバー、人的資源（HR）ポータル、個別プロジェクト管理用 wiki、ソフトウェア開発におけるサンドボックスなど、SSL セキュリティで保護することの多い内部サイトやサーバーの種類は数多くあります。こうした領域にアクセスするのが従業員のみである場合、組織にとって本当にサードパーティが署名した証明書が必要でしょうか。やはりこの場合も、自己署名証明書を使用した場合は、安全なシステムであると信頼するよう、従業員に乞うことになります。従業員は、その意思はあったとしても、そうすべきでしょうか。

SSL セキュリティ基盤のコスト

データセンターと物理的セキュリティ

自己署名証明書は本質的に、主要な認証局が署名した証明書に比べ、信頼性に劣ります。信頼できるサードパーティの認証局には、暗号化キー、特にセキュリティ上重要なルート証明書の秘密鍵が安全に保管されていることを保証できるようにするための、堅ろうなプロセスがあります。こうした認証局にとって、セキュリティは常に最優先であり、担当者は入念な審査を経たのち、高度な訓練を受けます。また、こうした認証局には、秘密鍵の保管場所について厳格なポリシーがあります。実際、主流のウェブブラウザで認証局が承認されるためには、こうした鍵がスマートカード上の抽出不可能なストレージに保管されていなければなりません。

また、強力な SSL セキュリティを提供するには、認証局はシステムエラーを防ぐための高可用性とフェールオーバーのメカニズムも提供する必要があります。こうすることで、必要なときにいつでもオンデマンドで適切な認証を提供できることを保証できるようになります。

主要な認証局に整っている高いセキュリティ標準を満たせるよう、こうしたインフラストラクチャを複製するには、コストのかかるコンポーネントが数多く必要です。第 1 に、組織には高可用性（HA）を実現できる証明書発行システムとデータの複製が必要です。第 2 に、関連する要件として、この複製は、2か所にある2つの異なるデータセンター内の 2 つの異なるセキュアルームを使用して、実施されなければなりません。これにより、停電などの予期せぬ要因により一方のデータセンターがダウンした場合にも、もう一方のデータセンターで確実に認証を行うことができるようになります。データセンター間での複製がなされないと、サーバーやブラウザが認証プロセスを完了できず、SSL で保護された重要なトランザクション（電子商取引サイトでのクレジットカードによる購入、HR ポータルへの新入社員情報のアップロードなど）が停滞することになります。

さらに、証明書発行システムのあるデータセンターとデータそのものも、保全する必要があります。つまり、物理的に厳格なセキュリティ対策を確立することが必要です。また、データルームに物理的にアクセスできる従業員の選抜や、施錠されたエリアへの入室を許すためのカードキーリーダーの設置、ビデオ監視カメラの取り付け、定期的な見回りを行うための監視員の雇用といった、追加の予防措置も必要です。権限のない人がこうした制限された部屋に入ることができるとすれば、鍵を入手して暗号化データをクラックすることが可能であり、トランザクションは危険にさらされます。

コロケーションによるラック 1 台の安全なデータセンタールーム（接続設備とユーティリティ一式含む）の基本コストは、月額千ドルから 1 万ドル超までさまざまです※1。ラックの追加、帯域幅の増加、技術サポートの利用などにより、多くの場合、コストはさらに何百ドルも膨らみます。さらに、2か所のデータセンターでデータを複製するため、これらのコストはすべて倍になります。明らかに、SSL の暗号化プロセスと認証プロセスに必要な物理的インフラとセキュリティの維持コストは、多くの企業が許容できる額を超えています。

※ 1 ： ソース : http://www.hostventures.com/colocationprices.html, http://www.creativedata.net/index.cfm?webid=168, http://www.datacenterknowledge.com/archives/2011/02/11/analysis-colocation-pricing-trends/

ハードウェアコンポーネント

自己署名の SSL サーバ証明書を生成できるソフトウェアは簡単に無料あるいは非常に安価で入手できますが、秘密鍵を管理するには、やはり各データセンターにハードウェアセキュリティモジュール（HSM）が必要です。また、事業継続性を確保するため、各 HSM についてサポート契約を結ぶ必要があります。

SSL HSM は、PKI SSL プロトコルシステムにおいてデジタルキーの管理と秘密鍵の認証を専門に行う、安全な暗号化プロセッサ（物理的な 1 台のハードウェア）です。HSM には 3 つの目的があります。第 1 に、ウェブ上のトランザクションを暗号化するための公開鍵と秘密鍵を安全に生成します。第 2 に、取り出しを防止できるように、鍵を安全に保管します。第 3 に、重要な暗号データの管理を企業が行えるようにします。

HSM は非常に特殊なハードウェアで、通常は極めて高価であり、廉価版で 1 台 13,000 ドル（約 130 万円）、上位機種で 30,000 ドル（約 300 万円）です。やはり、複製と高可用性の実現のためには、いかなる SSL インフラでも最低 2 台（各データセンターに 1 台）は HSM が必要です。

最後に、現在ではあまり意味がありませんが、企業では HSM を使用して非対称暗号と対称暗号の両方のアプリケーションサーバーをオフロードします。米国標準技術局（NIST）では企業で 2048-bit の RSA キーを使用するよう勧告しています。

管理と担当者

純粋なハードウェアコストに加え、自己署名による SSL セキュリティを管理するためのスキルある専門家を教育するための時間とコストや、SSL サーバ証明書の使用を管理するためのポリシーの確立も、重要な考慮事項です。

SSL サーバ証明書への自己署名を可能にするツール（Microsoft Certificate Authority など）には、証明書管理の機能は含まれていません。この前提においては、SSL プロトコルに厳格に従っていることを保証できるようにするための堅ろうなプロセスを、企業が計画、実装する必要があります。そうした実装なしでは、誰もが SSL サーバ証明書を要求、受領できることになり、ひいては、誰もが自由自在にあるサイトを詐称できることになります。

第 1 に SSL サーバ証明書を発行する企業に必要なのは、ドメインの証明書を作成、署名する権限があるのは誰であるかを慎重にコントロールし、確立されたポリシーに従って作成や署名が実行されるようにするためのプロセスを確立することです。十分な在職期間のある信頼できる担当者のみが証明書を作成、署名する権限を持ち、かつ、担当者はベストプラクティスや標準や技術に沿う形で十分な教育を受けることを、ポリシーに定めます。この権限は軽率に与えるべきものではなく、万一、調査が必要になった場合に備えて、明確な監査証跡が必要です。

第 2 に、主要なサードパーティ認証局は一般に、多くのプロセス（証明書を作成する権限を委譲する、CA による証明書への署名を許可する、といったプロセス）を自動化、迅速化するための使いやすい管理インターフェースを備えた、ウェブベースのアプリケーションを提供します。証明書署名要求（CSR）は、当該ドメインに対する権限を付与された人が、最終的に許可します。信頼された CA には、これらすべての流れが規定どおりに行われることを保証できるようにするための、堅ろうな自動化された手続きがあります。

第 3 に、自己署名証明書を利用することを決めた組織には、上記と同様のプロセスが必要になります。一部の企業はカスタムソフトウェアを書くことで SSL セキュリティのワークフローを自動化しようとしますが、多くの企業は単に手動でプロセスを管理しようとします。これには膨大な時間と、高度なスキルのある信頼できるスタッフ（場合によっては、高賃金のベテラン社員）の労力が必要です。

第 4 に、管理ツールや警告機能（信頼された CA の証明書であれば、証明書とセットで提供されることが多い）がなければ、証

明書の期限切れの通知を受け取ることもできません。自己署名証明書の期限切れや更新を手動で追跡する必要が生じ、膨大な時間を要する作業が必要となるため、その間、スキルの高い担当者が他のミッションクリティカルな作業から離れることになります。期限切れのSSLサーバ証明書のコストは容認できないほど大きくなります。例えば、自己署名証明書はつぎはぎだらけのセキュリティを生じさせ、顧客のみならず社内関係者にさえマイナスの影響を与え得る警告メッセージを引き起こします。

最後に、ソフトウェアのみによる暗号化では、鍵の状態の可視性が極めて制限されます。鍵をハードウェアに保管しないと、存在する鍵の数と、それらの鍵にアクセスし得た人物を特定できると保証することが極めて困難になります。ネットワークが危殆化すれば、サイト外で複製された鍵がないか、また同様に危殆化されていないか、知るすべがありません。

結局、秘密鍵は基本的には単なるファイルです。ファイルサーバー、仮想ファイルシステムや仮想サーバー、ストレージエリアネットワーク（SAN）あるいはネットワーク接続ストレージ（NAS）といったシステムは、バックアップし、コピーし、複製することが可能です。つまり、鍵の複製がいくつ存在し、どこに配置されているのか、把握するのは困難です。

鍵が HSM のようなハードウェアに保管されている場合、一般に鍵はそうしたデバイス上で生成されるため、鍵そのものが本質的に強固であり、さらに鍵がデバイスの外に持ち出されることが決してありません。つまり企業は、鍵がどこに存在し、複製がいくつ存在するのかを、常に正確に把握することができます。多くの HSM では、ポリシーベースのアクセスを実現するための強固な二要素認証を利用できるため、より適切な鍵管理ポリシーを実施できます。例えば、証明書への署名を、権限のある人物が 2 名いる場合にのみ可能にするといった制限を実行することが可能です。

こうした管理タスクをすべて実行するための適切な素質と経験を持つ人物を確保することは、コストがかかります。ComputerWorld が実施した IT 給与調査（2011 年）※2 によれば、中堅セキュリティプロフェッショナルの年収は約 10 万ドルです。企業の規模によっては、熟練スタッフをひとり雇うコストでさえ、特に信頼されたサードパーティの SSL 提供ベンダーを利用する場合のコストに比べ、自己署名 SSL セキュリティのコストを妥当なしきい値以上に押し上げることになりかねません。

企業にはインフラ管理を外注するという選択肢も常にありますが、この戦術は追加コストを生むだけでなく、別の問題を提起します。つまり、外注先を誰が管理するのか、外注先が大きな損害につながる過ちを犯したらどうなるのか、といった問題です。これらの懸念に加え、インフラの外注先は、アウトソースしているという依存関係があるため、取り替えるのが困難です。

自作式 SSL セキュリティ戦略の技術上、ビジネス上のリスク

自己署名のSSLサーバ証明書に伴って生じ得る、あらゆるハード面でのコストに加え、企業は運用上のリスクの増大にも直面します。定量化することは困難ですが、これらの危険が及ぼすコストは、緩和しない限り、相当な額に及びます。

リスクの一例としては、環境がセキュアになっていない場合に暗号化 / 復号プロセスの両端で発生し得るセキュリティ侵害の可能性など、技術的なものが挙げられます。加えて、セルフサービスの自己署名証明書方式では、証明書を失効させることは極めて困難です。

ビジネス上のリスクは、ほぼ間違いなく、技術上のリスクよりもさらに深刻です。ビジネス上のリスクのほとんどは、顧客やエンドユーザーとの信頼の構築に関わるものです。オンラインバンキングであろうと、個人を特定し得る情報の従業員用ポータルへのアップロードであろうと、あらゆるウェブベースの取引で信頼は重要です。

信頼の真の価値を定量化することは困難ですが、見込み客の信頼を勝ち得なければ、収益への大打撃はまぬがれません。HR ポータルのような内部サイトの場合は、従業員間の信頼が欠如し、給与履歴や個人データの安全性を危惧するような状況があれば、従業員の士気や生産性に影響を与えることも考えられます。

※ 2：April, 2011. http://www.computerworld.com/s/article/9214739/Salary_Survey_2011.

考慮すべきもう 1 つの要素は、サードパーティの SSL ベンダーが提供できる保証制度 です。こうした保証は、1 万ドル（約 100 万円）から 25 万ドル（約 2,500 万円）近辺までさまざまですが、データ侵害が発生した場合に取引高を補うことを意図しています。自己署名証明書には保証制度がありません。

さらに、内部で自己署名証明書を使用することのリスクとして、いずれ従業員が、ブラウザが発するセキュリティ警告を無視し始め、ブラウザの証明書ストアに信頼できない証明書を追加するようになる可能性があることが挙げられます。そうなれば、内部のネットワークやシステムが潜在的に危殆化するばかりでなく、組織全体のセキュリティに対する姿勢が緩み、内部システムの保全を意図して作られたポリシー全体が弱体化します。

最後に、サードパーティの認証局であれば適切に配備されるセキュリティプロセスと対策が、内部の認証局では欠如しがちであるため、自己署名証明書を利用する組織は、標的型攻撃（APT）、つまり複数の攻撃ベクトルを持つ攻撃に見舞われるリスクも高くなります。例えば、認証局を格納し実行しているサーバーが、物理的なセキュリティ境界を設けないまま、他のシステムと同じネットワークに接続されているような場合があります。また、証明書の生成に使用するルート鍵の利用に際して、生体認証によるアクセスコントロールが備わっていない、ということも内部の認証局にはよくあることです。こうしたことすべてが、証明書発行の過程におけるセキュリティや適正評価の低下につながります。要するに、セキュリティという名の錯覚のもとに、組織が運営されることになります。

総合的な総所有コスト（TCO）の増加

強固で信頼性の高い SSL セキュリティインフラを構成する要素は多数あります。自己署名の SSL サーバ証明書と、SSL セキュリティのリーディングカンパニーであるシマンテックが提供する SSL サーバ証明書のコストの比較を、次の表にまとめます。

	自己署名証明書（年額）	シマンテックの SSL サーバ証明書※3
SSL サーバ証明書	追加コストなし	証明書あたり 800 ドル （約 8 万円）
RDC ファシリティ	24,000 ドルから 240,000 ドル （約 240 万円から 2400 万円）	含まれる
ハードウェアセキュリティモジュール（HSM）と、関連ソフトウェアおよび保守料金	26,000 ドルから 60,000 ドル （約 260 万円から 600 万円）	含まれる
管理 / 人件費	正社員 1 名あたり 100,000 ドル※4 （約 1 千万円）	含まれる
合計	**年間 150,000 ドルから 400,000 ドル （約 1500 万円から 4000 万円）**	**年間 80,000 ドル （約 800 万円） （証明書 100 枚と仮定）**

すべてのコストを合計すると、自己署名証明書は、高コストなセキュリティオプションです。シマンテックのような信頼できる認証局と連携するということは、コストを節約できるだけでなく、世界で最も信頼されたセキュリティ企業の専門技術とリソースによって会社の SSL セキュリティが支えられていることで、安心を得られることでもあります。

※ 3：シマンテック SSL サーバ証明書を 100 枚、2013 年 9 月現在の価格で購入した場合の年間コスト。価格は予告なく変更される場合があります。
※ 4：最低限想定される人数。人数は証明書の枚数に比例して増加。

結論

自己署名の SSL サーバ証明書を使用することが組織のセキュリティコストの削減につながると、多くの IT プロフェッショナルが信じていますが、実際の数字は、そうでないことを示しています。データセンターのインフラや物理的なセキュリティから、PKI SSL システムに必要なハードウェアやソフトウェア、証明書のライフサイクル管理に必要な人員まで、自己署名による SSL セキュリティの実際のコストは、みるみるうちに膨らみます。

対外的なサイトにも、対内的なサイトにも、強固な SSL 保護が必要です。シマンテックのような信頼できるサードパーティ認証局を利用することが、クラス最高の SSL セキュリティで顧客その他の関係者を保護するための、最も簡単で、最もコスト効率の良い方法です。シマンテック SSL サーバ証明書を使用すれば、企業規模に関係なく、最終的な収益にインパクトを与えずに、サイトを保全し、サイトの信頼を維持することができます。

WPSelf-SignedSSL_2013_1309

日本ベリサイン株式会社
https://www.VeriSign.co.jp/
〒 107-0052　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@verisign.co.jp