複数のWebサーバー運用に適したSSLサーバー証明書の選びかた

digicert® | Symantec™ Website Security

目次

1. 増加する仮想サーバーと枯渇するIPアドレス

仮想化技術の進歩によって、ソフトウェア上でWebサーバーを容易に構築できるようになりました。また、アクセスの状況に合わせてサーバーの数を自由に増減できるなど、柔軟なサーバー運用も可能になりました。仮想化環境を利用する代表的なメリットは、ひとつのグローバルIPアドレス内に異なるドメイン名を持つ複数のWebサーバーを構築できることです。これによりIPアドレス枯渇への有効な対策となります。

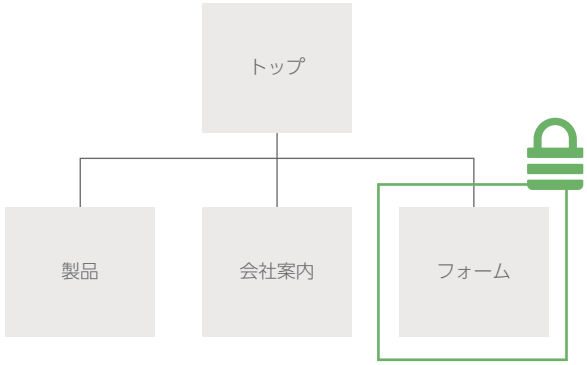
一方、昨今はSEOの改善、サイトの信頼性向上やアクセス解析の効率化、通信の安全性という観点から、常時SSL/TLS(以下、「常時SSL」)化への流れが加速しています。常時SSL化とは、これまでは決済ページや個人情報などを入力フォームページに限られていたSSL暗号を、企業や組織のWebサイトのすべてのページに適用するというものです。

この常時SSL化を仮想化環境で実現する際、注意すべきことがあります。従来の環境では、異なるドメイン名を持つ、SSL/TLS通信に対応した複数のWebサーバーをひとつのグローバルIPアドレス上で構築する場合にも、ひとつのSSL/TLSサーバー証明書(以下SSLサーバー証明書)しか配置することができませんでした。

仮想化環境を利用する目的である「コストと構築の手間の削減」を達成するには、こうした課題に対処するための技術、そのメリットやデメリットを理解しながら最適な技術を選択、実装できるようにすることが重要といえます。

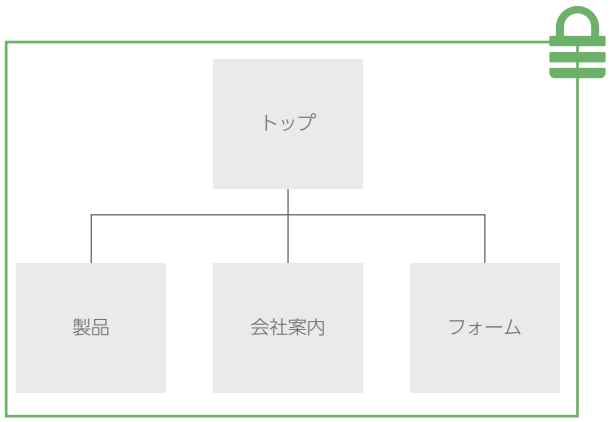
部分的なSSL利用

ログインや取引ページのみ暗号化。FiresheepやSSL Stripのような脅威に対して脆弱。顧客の信頼の損失や機密データの漏えい、マルウェア攻撃にさらされるリスクがある。



常時SSL

サイト内のすべてのページの暗号化。すべてのユーザセッションを開始から終了まで暗号化。FiresheepやSSL Stripによる攻撃に対し安全を保つことができる。SEOの改善やアクセス解析の効率化など、セキュリティ以外の利点も注目されている。



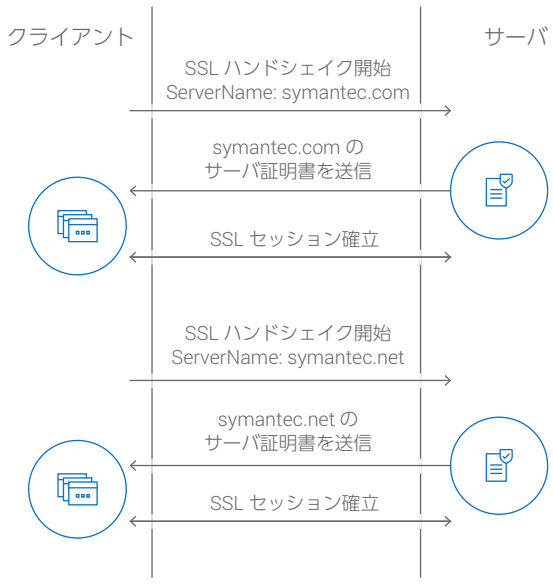
2. 複数サーバー(サイト)環境に対応する技術

こうした課題に対応するための技術として、ここではSNI、SANsならびにワイルドカード証明書という技術を紹介します。それぞれ特徴や仕組みが異なり、ポイントを理解して柔軟に組み合わせることで、グローバルIPアドレスを節約するとともに、SSLサーバー証明書の運用を効率化することができます。

複数のSSLサーバー証明書を同一IPで共有できるSNI

SNIはServer Name Indicationの略で、SSL/TLSの拡張仕様のひとつ(RFC 6066)です。SNIを導入することによって、ひとつのグローバルIPアドレスに複数のSSLサーバー証明書を設定することができるようになります。

SNIの仕組みは比較的単純で、SSLハンドシェイクの際に通信の対象となるドメイン名を通知するようにしています。これにより、Webサーバーはどのドメイン名のSSLサーバー証明書を利用すべきかを判断できます。IPアドレスを節約する方法として注目されており、クラウド事業者での利用が増えています。



このようにSNIを用いることでSSLサーバー証明書の柔軟性が拡大します。SNI上では、通常のドメイン名ごとのSSLサーバー証明書の他に、後述のSANs証明書やワイルドカードを用いることが可能です。しかしながらSNIに対応しているブラウザ、サーバーが比較的新しいものに限られているという制約があり、注意が必要です。本稿の執筆時点では、ブラウザではInternet Explorer 6 もしくはWindows XP以前での全バージョン、Windows XP上のSafari、BlackBerryブラウザ 7.1およびそれ以前、Windows Mobile 6.5、Android 2.xのブラウザ、wget 1.1.4未満(非パッチ)が非対応となっています。

また、サーバーではIBM HTTP Server、ライブラリでは、Qt 4.7、Mozilla Network Security Services server side、Java 1.6 およびそれ以前、Apache HttpComponents 4.3.1 およびそれ以前、Python 2.x (ssl, urllib[2], httplib モジュール)、PhantomJS 1.x が非対応となっています。なお、フィーチャーフォン(いわゆる携帯電話)はほぼ非対応です。

1枚で複数のドメイン名に対応するSANs証明書

SANsはSubject Alternative Namesの略で、電子証明書の代表的な規格であるRFC5280で規定され、一般には仮想サーバードメイン機能とも呼ばれています。SNIがひとつのグローバルIPアドレスに複数のSSLサーバー証明書を設定する手法であるのに対し、SANsでは1枚のSSLサーバー証明書で複数のドメイン名(FQDN)に対応することができます。つまり、まったく異なるドメイン名「www.symantec.co.jp」「www.symantecsecured.com」「www.geotrust.co.jp」などでも、ひとつのSSLサーバー証明書にまとめることができます。

具体的には、認証局からSSLサーバー証明書を取得する際に、サブジェクトコモンネームフィールドへ指定するドメイン名に加えて、SANsフィールドに設定する複数のドメイン名を指定し、所定の手続きを踏まえることで、Subject Alternative Namesフィールドにこれらの値が

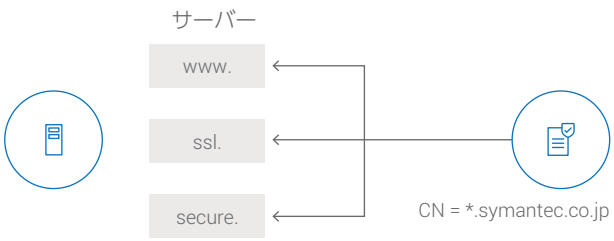
含まれる証明書が発行されます。これによりドメイン名ごとに複数回行ってきたCSR生成や申請が1回で済むようになり、運用工数を削減することができます。

ただし、SANsを用いる場合、後で新たにドメイン名を追加する際には、それまでにインストール済みのドメイン名用のSSLサーバー証明書も入れ直す必要があります。さらに、PC向け及びスマートフォン向けの最新ブラウザはほぼ対応していますが、フィーチャーフォンはSANsフィールドに対応していないため非対応となる点にも注意が必要です。

また、SSLサーバー証明書を運用する上で重要な秘密鍵の管理について、SANs証明書を用いる場合には特に注意が必要です。万一、秘密鍵が漏えいしてしまった場合、その被害がサブジェクトコモンネームに該当するWebサーバーのみならず、SANsに設定した複数のドメイン名のWebサーバーでも、影響が及ぶからです。また、新たなサイトを追加する際には鍵ペアの再作成とすべての証明書の一斉入れ替えが必要となる点を考慮に入れて運用手順を定めておくことが推奨されます。その為、一部署で新たなWebサイトを作る毎に他部署にお願いをして証明書の入れ替えを行ってもらう運用が必要な利用シーンでは避けることが推奨されます。

サブドメイン名をまとめられるワイルドカード証明書

ワイルドカード証明書は、同一のドメイン名配下の複数の異なるサブドメイン名を持つWebサーバーに対し、ひとつのライセンスで導入できるSSLサーバー証明書です。たとえば、CSRに「*.symantec.co.jp」と記載することで、「www.symantec.co.jp」「ssl.symantec.co.jp」「secure.symantec.co.jp」などのサブドメイン名を、ひとつのSSLサーバー証明書にまとめることができます。



1枚で複数のサブドメイン名をまとめることができ、新たなWebサイトの追加も既存のSSLサーバー証明書のコピーにより容易に行えるため、大幅な作業の効率化とコストの削減が見込めることがメリットとなっています。

ただし、PC向け及びスマートフォン向けの最新ブラウザはほぼ対応していますが、フィーチャーフォンは非対応です。

また、万一、秘密鍵が漏えいしてしまった場合の考慮点は、基本的にSANsの場合と同様ですが、その範囲がワイルドカードで指定し得る全てのサブドメイン名に及ぶことが課題です。つまり、ワイルドカードで指定されたWebサイトを作成や鍵ペアの管理に関してガバナンスを利かせていないと、不正なサイトが立てられたり、鍵ペア漏えいのリスクが広がることになります。Webサイトの作成や鍵の管理が非常に限られたメンバーに限られている組織では、非常に便利で安価なソリューションですが、多くのWeb・IT管理者が関わり複雑な管理が要求される組織ではリスクの管理が難しくなるでしょう。

	特徴	注意事項
SNI	ひとつのIPアドレスに複数のSSLサーバー証明書を設定できる	• ドメインごとにSSLサーバー証明書が設定可能(SANsやワイルドカードも利用可能;その際は各証明書の注意事項も確認) • SNI非対応ブラウザ、SNI非対応サーバーを確認しておくこと
SANs証明書	ひとつのSSLサーバー証明書で複数のドメイン名に対応できる	• ドメインを追加する際には、すべてのSSLサーバー証明書を入れ直す必要がある。 • フィーチャーフォン非対応 • SSLサーバー証明書の危殆化が発生した際に、複数のサイトに影響が波及する。(有限のリスク)
ワイルドカード証明書	ひとつのSSLサーバー証明書で同一のドメイン名配下の複数のサブドメイン名に対応できる	• サブドメイン名の追加が容易だが、ドメインが異なるサイトはまとめることが出来ない。 • フィーチャーフォン非対応 • SSLサーバー証明書の危殆化が発生した際に、ワイルドカードで設定し得る複数のサイトに影響が波及する。(無限大のリスク)

3. 適材適所のSSLサーバー証明書で管理の手間とコストを低減

前章で説明したように、複数のWebサーバーを運営する際に効果的なSSLサーバー証明書にもいくつかの種類や設定手法があります。それぞれに特徴があるので、使用する際にはWebサーバーの構成などに合わせた最適なSSLサーバー証明書を選ぶことが重要です。

ここでは、具体的な導入ケースを考えてみましょう。同時に、前項に挙げた技術的な側面以外の、運用上の注意点についても考えてみます。

SNIが有効なケース

ひとつのグローバルIPアドレスに複数のSSLサーバー証明書を設定できるSNIは、同一のWebサーバーを複数のユーザで共有する場合に有効です。たとえばIaaSやホスティングサービスなどでの導入に適しています。SNIを導入することで、Webサーバーサービスを利用するユーザは、それぞれ自由にSSLサーバー証明書を選んで導入することができます。

SNIは、ひとつのグローバルIPアドレスに企業名のドメイン、商品やサービス名のドメイン、キャンペーン用のドメインなど、複数のドメイン名でWebサーバーを構築する際にも有効です。

SANs証明書が有効なケース

ひとつのSSLサーバー証明書で異なるドメイン名をカバーできるSANs証明書は、企業などの組織が複数のドメイン名でWebサーバーを構築している場合に有効です。たとえば、ひとつの企業で企業名のドメイン、商品やサービス名のドメイン、キャンペーン用のドメインなど、複数の異なるドメイン名のWebサーバーを運営している場合に適しています。また、Microsoft Exchangeのように、複数ドメイン名のWebサービスを稼動させたくても、Webサーバーにインストールできる証明書がひとつに制約されている場合などに、SANs証明書が有効となります。

その一方で、たとえば企業ドメイン名のWebサーバーはIT部門が管理し、キャンペーンサイトのドメイン名はマーケティング部門が管理しているようなケースでSANs証明書によりまとめてしまうと、新たなWebサイトを作成する際に他のサイトの証明書の入れ替えまで考慮する必要が出てきて運用の柔軟性が低下したり、証明書の有効期間が満了した場合に複数サイトの作業手続きを行う担当者が不明瞭になったりするなどの運用上のデメリットが生ずる場合があるため注意が必要です。

ワイルドカード証明書が有効なケース

同一のドメイン名配下の複数の異なるサブドメイン名をひとつのSSLサーバー証明書で対応できるワイルドカード証明書は有効です。

たとえば、画像データ(image.symantec.com等)やコンテンツ(sales.symantec.com, support.symantec.com等)ごとにサブドメイン名を設定して運用している際に適しています。また、サブドメイン名の異なるWebサーバーを追加する際にも容易に対応できるため、今後も同じルールで新たなサブドメイン名の作成予定がある場合にも有効です。さらに、ワイルドカード証明書はサブドメインの数に関係なく一定コストの証明書なので、Webサーバー数の増減があっても予算の管理がしやすいという側面を持ちます。

また、複数部門でひとつのドメイン配下のWebサイトの管理を分担するような場合への考慮は、SANs証明書と同様に必要となる点に十分に注意してください。他部署に、鍵ペアなどの共有をすることになりますので、もし悪意を持って利用されると不正サイトが作られたり、アクセス権限が無い通信の内容を見られたりするリスクも発生します。その為、前述の通り、限られた管理者が一括して運用をするような場面での利用が推奨されます。

	適する用途	証明書運用上の考慮点
SNI	IaaSやホスティングサービスなどの提供事業者	普通のSSLサーバー証明書を利用する場合は、特になし。SANsやワイルドカードを利用する場合、それぞれの課題への考慮が必要
SANs証明書	異なるブランドのページを持つWebサイトで、比較的構成が安定している	Webサイトの新設、統廃合時や更新時の責任者を明確にし、すべてのサイトでの証明書の入れ替えをもれなく管理する必要あり
ワイルドカード証明書	Webサイトのドメインは決まっているが、常に新たなWebサイトを立ち上げる企業	Webサイトの新設、統廃合時や更新時の責任者複数にわたる場合、不正なサイトの作成や鍵ペアの管理で注意が必要

4. まとめ

SNI、SANs、ワイルドカードと、暗号化通信の実装技術は進化を続けています。同時に、HTTP/2によるWeb表示の高速化や、SEO改善を見据えた常時SSL化など、SSLを取り巻く環境も進化しています。

Webサーバーで推奨される暗号化技術も常に進化しており、暗号アルゴリズム、暗号化ライブラリのアップグレードが必要となる場面は少なくありません。特にWebサイトの設計・構築部門や、SSLサーバー証明書を管理している担当者は、最新動向を常に把握しつつ今後を見通すことが求められます。そしてシステム更改の際には、SSLサーバー証明書の管理も加味したシステムの構築を意識しましょう。

ひとつのグローバルIPアドレスを最大限に活用するには、SNIという選択肢がまずあります。しかし、ドメイン名ごとにSSLサーバー証明書を利用していると、証明書のコストと管理が大変になるため、SANs証明書やワイルドカード証明書を活用することで、課題を最小化することができます。その際、SANsは自由なドメイン名を後から追記できますが、その都度先に導入済みのSSLサーバー証明書を入れ直す手間が発生します。一方、ワイルドカード証明書は同じドメイン名に限定されるものの、個別のサブドメイン別にWebサイトを追加する場合の運用が容易です。

これらの特徴から、Webサイトの構成上、同一管理者配下にあるWebサイトのドメイン名が固定されていて増減することがなければSANs証明書が適しているといえます。一方、サービスの拡充やサイト統廃合の予定がある、しばしばキャンペーンを実施するなど、ドメイン名が増減する可能性があるのならWebサイトごとに証明書を1枚ずつ管理するか、ドメイン名が固定の場合はワイルドカード証明書が最適な選択肢となるでしょう。

また、SNIと、SANs証明書およびワイルドカード証明書は競合するものではないため、上記を基本に最適なSSLサーバー証明書を適材適所に選ぶことができます。自社に最適なSSLサーバー証明書を選ぶことで担当者の手間を減らせるだけでなく、コストの削減にも大いに寄与します。ただしSANs証明書やワイルドカード証明書は、認証局や証明書発行システムによって、提供の有無や制限事項に違いがあるので注意が必要です。

シマンテックやジオトラストでは、SANs証明書やワイルドカード証明書をご提供しています。また、Webサーバーのセキュリティ管理においては、SSLサーバー証明書だけではなく、Webサーバーの脆弱性の把握や設定内容の管理、SSLサーバー証明書の更新期限や設定内容の管理も必要です。

例えば、シマンテックのSSLサーバー証明書には、マルウェアスキャンや脆弱性アセスメントといった機能が標準で付属するため、より安全性の高いWebサイト運用が可能になります。また、エンタープライズ企業向けには、SSLサーバー証明書の管理および監視サービスを一元化した「Symantec Certificate Intelligence Center (CIC)」を用意しています。

CICでは、エンタープライズ企業および子会社やブランチオフィス、あるいは事業部単位などで利用するSSLサーバー証明書のライフサイクル管理を自動化し、設定されている証明書の課題を洗い出し、運用の手間を大幅に軽減します。堅牢なインフラに構築されたクラウドベースのサービスは、あらゆる認証機関のすべてのSSLサーバー証明書を検出および監視し、ビジネスの継続およびコンプライアンスを確保します。

SSLサーバー証明書とあわせて上記のような周辺サービスや機能を有効活用することで、Webサイトの安全性を保ちながら効率的な管理を実現できます。