TLS/SSL証明書 ビギナーズガイド

最適なインターネットセキュリティ ソリューションの選択

digicert®

目次

1 はじめに
1 TLS/SSL証明書の概要
1 TLS/SSLによる暗号化の仕組み
2 適正なTLS/SSL証明書が導入されているWebサイトの見分け方
3 どのようなケースでTLS/SSL証明書を使用するべきか
3 さまざまな種類があるTLS/SSL証明書
4 技術用語の簡単な解説
4 まとめ

はじめに

インターネットに関するセキュリティの確保においては、企業ユーザー、個人ユーザーを問わず、自宅や職場の物理的なセキュリティと同様のアプローチが必要です。自身の身の安全を守るだけでなく、自宅や職場、そしてWebサイトを訪れた人の安全も確保する必要があります。重要なのが、潜在的なリスクを把握し、そのようなリスクに備えてしっかりした防御体制を築くことです。急激なスピードで変化していくテクノロジーの世界では、最新の動向を常に把握しておくことは必ずしも容易ではありません。そのため、信頼をおけるインターネットセキュリティ企業をパートナーに選ぶことが最善の選択肢となります。

このガイドでは、関連する技術をわかりやすく説明するとともに、最適なインターネットのセキュリティソリューションを選択できるよう、必要な情報をご提供いたします。専門用語の説明については、巻末の「技術用語のシンプルな解説」の項を参照してください。

TLS/SSL証明書の概要

TLS（Transport Layer Security）とその前身のSSL（Secure Sockets Layer）は現在最も広く使用されているセキュリティプロトコルです。これらのプロトコルは主に、以下に示す2つの特別な役割を果たします。

1. **認証と検証：**TLS/SSL証明書にはユーザーや企業、Webサイトの素性に関する特定の詳細事項が信頼できるものであること表す情報が記載されています。Webサイトの訪問者がブラウザに表示される南京錠のアイコンやトラストマーク（例：DigiCert® Secured Seal、Norton Seal powered by DigiCert）をクリックすると、この情報が表示されます。情報はすべて、SSL証明書を発行した認証局（CA）によって検証されています。認証局の検証が得られることにはさまざまな意味がありますが、この点については後ほど説明いたします。
2. **データの暗号化：**TLS/SSL証明書を活用することで暗号化の機能を利用できるので、機密性の高い情報をWebサイトを介してやり取りするときに、情報が第三者に傍受されたり、見られたりするのを防ぐことができます。

身分証明書やパスポートは公的機関だけが発行できるように、TLS/SSL証明書の場合も、最も信頼できるのは、信用度の高い認証局（CA）が発行しているものに限られます。TLS/SSL証明書を提供する場合、CAは非常に厳しいルールやポリシーに従う必要があります。信用度の高いCAから適正なTLS/SSL証明書の発行を受けることで顧客やクライアント、パートナーから高い信頼が得られます。

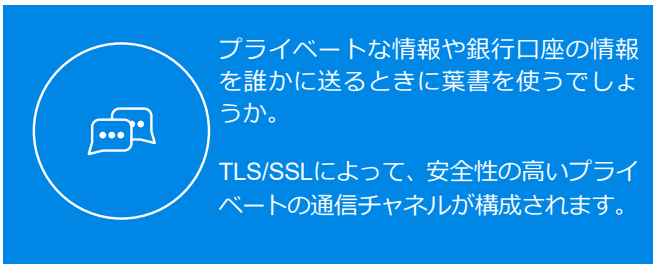
TLS/SSLによる暗号化の仕組み

鍵を使ってドアをロックしたり、ロックをはずしたりするように、暗号化でも同じ方法で情報をロックしたり、ロックを解除したりします。正しい鍵を持っていないと、情報の「ロックを解除」できません。

個々のTLS/SSLセッションは、主に以下の2つの鍵を使用して構成されます。

- 情報の暗号化（スクランブル化）には、公開鍵を使用します。
- 情報の暗号（スクランブル）を解除し、判読可能な元の形式に復元するには、秘密鍵を使用します。

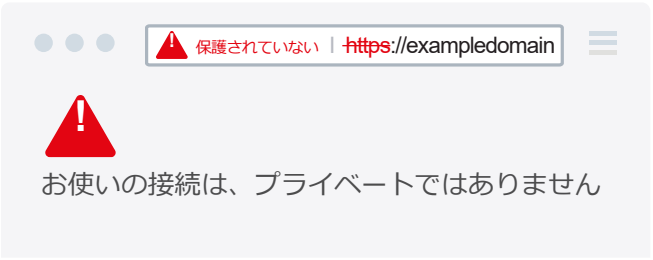
SSLは、「セキュアソケットレイヤー」を意味します。この技術では、サイトの訪問者のWebブラウザとWebサイトのあいだにセキュアなセッションリンクを確立します。これにより、このリンクを通じた通信はすべて暗号化されるため、通信のセキュリティが確保されます。



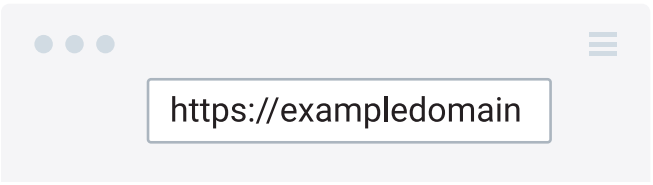
プロセス：CAが認証した企業、団体ごとに発行されるTLS/SSL証明書はどれも、特定のサーバーやWebサイトドメイン（Webサイトのアドレス）での使用を目的として発行されます。TLS/SSL証明書が導入済みのWebサイトのアドレスにユーザーがブラウザでアクセスすると、ブラウザとサーバーのあいだでTLS/SSLハンドシェイク（グリーティング）が実行されます。コンテンツ情報がサーバーにリクエストされて、ブラウザのウィンドウに表示されます。セキュアなセッションが確立されているときには、南京錠アイコンによって通信が暗号化されている事がわかります。トラストマークの表示もその1つです。トラストマークをクリックすると、TLS/SSL証明書の有効期限や、セキュリティが施されているドメイン、TLS/SSL証明書のタイプ、証明書の発行元のCAなどといった、詳細な情報が表示されます。これらはどれも、セッションのためにセキュアな接続が固有のセッション鍵で確立されていることを意味しており、安全な通信を実現します。

適正なTLS/SSL証明書が導入されているWebサイトの見分け方

1. TLS/SSLのセキュリティが施されていない標準的なWebサイトの場合、ブラウザのアドレスバーに表示されるそのサイトのアドレスの前には、「http://」が表示されます。これは、「ハイパーテキストトランスファープロトコル」を表しており、インターネット上での情報のやり取りがセキュアでない方法で行われることを意味します。近年、主なブラウザでは、TLS/SSL証明書が適切に導入されていないWebページを訪れたときに警告が表示されるので、ユーザーはこのようなサイトにアクセスするのをやめる可能性があります。



一方、TLS/SSL証明書で保護されているWebサイトでは、アドレスの前に「https://」が表示されます。これは、「セキュアなHTTP」であることを表します。



2. また、ブラウザの一番上か一番下（使用しているブラウザによって異なる）には、南京錠のアイコンも表示されます。

3. Webサイト自体にトラストマークが表示されていることも少なくありません。DigiCert™のお客様は、DigiCert® Secured SealやNorton Seal powered by DigiCertのトラストマークをWebサイトに使用しています。ページに表示されるこれらのトラストマークや南京錠のアイコンをクリックすると、CAによって検証および認証されたすべての企業情報を含め、証明書の詳細情報が表示されます。

4. ブラウザのウィンドウに表示されている閉じた南京錠をクリックするか、DigiCert® Secure Trust SealやNorton Secured Sealなどの特定のTLS/SSLトラストマークをクリックすると、認証されている組織の名前が表示されます。高いセキュリティ機能が実装されているブラウザの場合、Extended Validation（EV）TLS/SSL証明書の存在を検知すると、認証されている組織の名前をわかりやすく確認できるようになります。情報が一致しない場合は、証明書の有効期限が切れており、エラーメッセージや警告がブラウザに表示されます。

どのようなケースでTLS/SSL証明書を使用するべきか

端的に言うと情報をセキュアにやり取りしたいときにはどんなケースでもTLS/SSL証明書を使うべきです。

以下にいくつかの例を挙げます。

- Webサイトとユーザーのブラウザのあいだでセキュリティを確保する
- 企業内のイントラネットにおける内部通信のセキュリティを確保する
- 内部および外部のサーバー間を行き交う情報のセキュリティを確保する
- モバイルデバイスを介してやり取りする情報のセキュリティを確保する

まざまな種類があるTLS/SSL証明書

現在、市場には、さまざまな種類のTLS/SSL証明書が存在します。

- 1つは、自己署名証明書があります。その名が示すように、内部での用途に使用する目的で生成される証明書で、CAが発行したものではありません。Webサイトのオーナーが自分用に生成した証明書であるため、CAが発行する完全に検証および認証されたTLS/SSL証明書ほどの効力は期待できません。
- ドメイン認証の証明書はエントリーレベルのTLS/SSL証明書と見なされており、すぐに発行できます。唯一行われるチェックでは、証明書を使用する対象のドメイン（Webサイトのアドレス）をWebサイトのオーナーが所有しているかどうか確認します。ドメインのオーナーが本物の企業・団体であることを確認するものではありません
- 企業認証TLS/SSL証明書の使用は、ネットの完全なセキュリティを実現し、ユーザーの信頼を得るための第一歩と言えます。発行に多少の時間を要するこれらの証明書は、事業の存在とドメインのオーナーシップ、証明書を申請したユーザーの権限を確認するための多数の検証手続きと審査に組織が合格した時点ではじめて交付されます。

DigiCertのTLS/SSL証明書はすべて、企業認証が行われています。

- ドメイン名には、さまざまなホストのサフィックスが使用されることが少なくありません。このような場合、ワイルドカード証明書を使用すれば、host.your_domain.comなど、ドメインのどのホストにも漏れなく、TLS/SSLのセキュリティを付与できます（この例では、「host」の部分が入れ替わっても、ドメイン名は変わりません）。
- ワイルドカード証明書と似ていながらもう少し応用のきく証明書にSAN（マルチドメイン）TLS/SSL証明書があります。この証明書では、単一のTLS/SSL証明書を複数のドメインに付与することができます。
- Extended Validation（EV）TLS/SSL証明書を利用すれば、業界最高水準の認証を実現でき、最も高いレベルで顧客の信頼が得られます。EV TLS/SSL証明書で保護されたWebサイトにアクセスすると、Webサイトの正規のオーナーの名前と、EV TLS/SSL証明書を発行したセキュリティプロバイダーの名前が専用のフィールドに表示されます。また、アドレスバーには、証明書の所有者の名前や、証明書の発行元CAの名前も表示されます（一部のブラウザの場合）。このように目に見えるかたちで安心感が得られれば、eコマースに対する顧客の信頼も高まります。

技術用語の簡単な解説

暗号化：第三者が情報を利用できないよう、情報を「スクランブル化」することです。

暗号の解除：情報の「スクランブルを解除」し、元の形式に戻すことです。

鍵：情報を暗号化したりその暗号を解除したりする際に使用する数学の公式やアルゴリズムを意味します。さまざまな多くの組み合わせを持つ鍵ほど破られにくくなるように、暗号鍵の長さ（ビット数）が長くなるほど強固な暗号化が実現します。

ブラウザ：インターネットへのアクセスで使用するソフトウェアプログラムです。ブラウザには、Microsoft EdgeやMozilla Firefox、Apple Safari、Google Chromeなどがあります。

まとめ

信頼は、インターネットビジネスの世界において大きな違いを生み出します。顧客を守り、顧客の信頼を得るためのテクノロジーに投資することは、ネットビジネスやeコマースWebサイトのホスティングを手掛ける企業にとって、事業の成功に不可欠な要因の1つとなっています。効果的なかたちで導入されたTLS/SSL証明書や、適切に配置、使用されたトラストマークは、顧客の信頼を獲得するうえで、実績あるツールとして機能します。

DigiCertは現在、TLS/SSL証明書を全世界で提供する、業界のリーディングカンパニーであり、サイトの検索や閲覧、ネットショッピングやサインインをユーザー*が安心して行える環境の実現に貢献しています。DigiCertは、世界中で100万を超えるWebサーバー*のセキュリティを支えており、数多くの実績を誇る認証局です。また、eコマースや銀行業界の最大手を含め、Extended Validation TLS/SSLを使用しているWebサイトの3分の2以上*が、DigiCertのソリューションを使用しています。豊富な実績を持つDigiCertを利用することで、インターネットで最も認知されているトラストマークを掲載できます。自社のWebサイトに安心感をもたらせることでブランドイメージを強化することが可能となります。

詳細は以下のWebサイトをご覧ください。
https://www.digicert.com/jp/

*DigiCertの系列会社、関連会社、リセラーを含む

詳細については、websales_jp@digicert.comから弊社のセキュリティ営業担当者にメールでお問い合わせください。

アメリカ

ユタ州、リーハイ
2801 North Thanksgiving Way, Lehi, Utah 84043, USA

アメリカ、カリフォルニア州、マウンテンビュー
485 Clyde Ave., Mountain View, California 94043, USA

アジア太平洋、日本

インド、バンガロール
RMZ Eco World, 10th Floor, 8BCampus,
Marathalli Outer Ring Road, Bangalore - 560103, India

オーストラリア、メルボルン
437 St Kilda Road, Melbourne, 3004, Australia

日本、東京
104-0061　東京都中央区銀座6-10-1
GINZA SIX 8階

ヨーロッパ、中東、アフリカ

オランダ、ニューウェハイン
Nevelgaarde 56 Noord, 3436 ZZ Nieuwegein,
Netherlands

南アフリカ、ケープタウン
Gateway Building, Century Blvd & Century Way 1,
Century City, 7441,Cape Town, South Africa

アイルランド、ダブリン
Block 21 Beckett Way, Park West Business Park,
Dublin 12, D12 C9YE, Ireland

スイス、ガレン
Poststrasse 17, St Gallen, Switzerland, 9000

イギリス、ロンドン
7th Floor, Exchange Tower,
2 Harbour Exchange Square, London E14 9GE

ベルギー、メヘレン
Schaliënhoevedreef 20T, 2800 Mechelen, Belgium

ドイツ、ミュンヘン
Ismaninger Strasse 52, 81675 Munich, Germany

digicert®