目次

常時 SSL (ALWAYS-ON SSL)への移行

Google がランキング評価で常時 SSL (ALWAYS-ON SSL = AOSSL) のサイトを優遇することを発表してから、多くの企業がサイト全体の SSL 化を進めています。

Web サイトを常時 SSL 化するためには、何から手を付けるべきでしょうか？

また、常時 SSL はウェブサイトにとってどんな意味合いがあるのでしょうか？

このガイドでは「常時 SSL (ALWAYS-ON SSL) の安全性の利点、サイト全体に与える影響、実施手順」を明らかにしていきたいと思います。

常時 SSL (ALWAYS-ON SSL)で最高の検索結果ポジションを獲得

組織のセキュリティ確保は、何かをしたらすべて完成ということではなく、常に新しい何か（新しい OS、新しい脆弱性攻撃、新しいセキュリティのベストプラクティスなど）が現れ、終わりのない旅のようなものだと感じる IT 管理者もいるのではないでしょうか。

同じように、SEO も終わりのない旅のようなものといえます。Google の検索アルゴリズムは、新しい要素を加えたり、これまでの要素を廃止したり、要素のウェイトを変更したりと頻繁に変更されています。Google のアルゴリズムの要素はほとんど明らかにされておらず、あいまいで測定が困難です。

しかし、Google の HTTPS everywhere が検索エンジンのランキングアルゴリズム要素であるという発表は、常時 SSL (ALWAYS-ON SSL)がセキュリティと SEO の両面でぜひ実施すべき重要事項であることを示しています。

なぜ Google は常時 SSL(ALWAYS-ON SSL)を推進するのか？

常時 SSL(ALWAYS-ON SSL)は、セキュリティのベストプラクティスとして何年も前から推奨されています。

これまで、「Online Trust Alliance」や「CA Security Council」のような標準化団体や Microsoft が、常時 SSL こそがオンラインでユーザーのデータを安全に扱う唯一の方法だと訴えてきました。そして過去数年にわたり、Facebook、Twitter、Microsoft、Yahoo!、PayPal、Google 等のインターネット界のリーダーといえる企業が、サイトの常時 SSL 化を実施してきました。

Web サイトの常時 SSL 化を行う企業（一例）

Facebook　Twitter　Microsoft　Yahoo!　PayPal　Google

Google は、常に顧客とインターネットの利用者全体のためにセキュリティを向上させる方法を継続して探してきました。セキュリティ上の脆弱性を探求するホワイトハットハッカーの育成や、OpenSSL の独自バージョンの開発もそのために行っています。Web セキュリティの向上は、Google の体質に組み込まれたものと言ってもよいでしょう。そして現在、自らの検索エンジンとしての影響力を利用し、HTTPS everywhere (= 常時 SSL)を普及させようとしています。

Google のウェブマスタートレンドアナリスト Zineb Ait Bahajji と Gary Illyes は以下のようにコメントしています。

> セキュリティは、Google の最優先課題です。

> ....我々はまた、インターネット上の安全な領域の割合を広げるために働いています。

> ....Google の検索結果に表示されたサイトは安全であるということを確認する作業を行っています。

> ....すべての人にとって Web が安全な場所であるよう、サイトのオーナーが HTTP から HTTPS への切り替えを行うことを推奨しています。

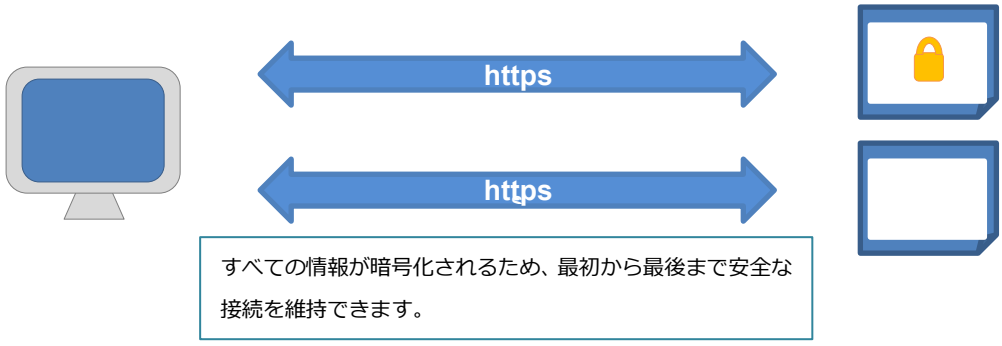
常時 SSL (ALWAYS-ON SSL) はユーザーの安全性を高めます

現状ではほとんどの Web サイトが一部のページだけで SSL を利用し、他の大部分のページは暗号化されていない平文のまま表示されています。

この場合、「hijacking」や「eavesdropping」などの新しい手法により、暗号化されていないセッションから簡単にユーザーの情報が盗まれてしまう可能性があり、今日の脅威に完璧に対抗することはできません。

対して常時 SSL (ALWAYS-ON SSL)は、ログインページやチェックアウトページのような機密性の高い情報を扱うページだけでなく、ユーザーがサイトを利用している最初から最後までのセッション全体を暗号化するため、最も安全な接続を提供しているといえます。

常時 SSL は、すべてのページ・Cookie・セッションを、ページに何が含まれているかとはかかわりなくすべて暗号化するため、情報の安全性が確保できます。



セッション Hijacking とセッション Sidejacking

ログインページを HTTPS で暗号化している場合、ログイン時には入力情報の安全が確保されます。しかし、一旦ログインが承認されると、往々にして、暗号化されていないページにリダイレクトされ以降のアクセスを続けることになります。この時点で通信が平文に戻ってしまうため、ブラウザとサーバー間の通信内容をハッカーに傍受されてしまい、セッション Cookie に含まれるセッション ID が漏えいしてしまいます。ハッカーは入手したセッション ID でユーザーに成りすますことができますので、その情報を利用しサーバーに保存されたユーザーのデータを取得したり、書き換えたりできます。

特に、対策が行われていない WiFi ホットスポットはこの攻撃が利用されやすいので注意が必要です。WiFi ホットスポットをターゲットとした使いやすい攻撃支援ツールは数多く作られており、中にはブラウザのプラグインとして利用できるものさえあります。その中のひとつ、 Firesheep というツールのダウンロード数はなんと 280 万件以上です。

SSLStrip

2009 年に Moxie Marlinspike 氏によって作成された SSLStrip は、暗号化されていないページの弱点をうまく利用した、洗練された中間者攻撃 (man-in-the-middle) です。

SSLStrip を使うと、攻撃者はネットワーク上の HTTPS リンクとリダイレクトを監視し、HTTP トラフィックをリダイレクト先にそっくりな HTTP リンクや HTTPS リンクにマッピングしてハイジャックすることができます。Web サイトに SSL 証明書がインストールされていて、HTTPS を利用していても、全アクセスを HTTPS にしていない限り、SSLStrip に対して脆弱です。

常時 SSL (ALWAYS-ON SSL) のメリット

常時 SSL (ALWAYS-ON SSL) にはマーケティングと IT の両面でビジネス上の様々なメリットがあります。

セキュリティの向上

これまでに紹介したような攻撃は、特別な装置も必要なく、簡単に行われてしまいます。悪意のある組織が求めているのはログイン ID・パスワードやクレジットカード情報だけではありません。ブラウジングの履歴や一見公開しても構わないと思われる個人情報も、彼らに取得されれば悪用される可能性があります。サイト全体を HTTPS 化すれば、こうした攻撃や次世代の脅威に対しても Web サイトとサイトの利用者双方の安全性を確保できます。

賠償金リスク回避

サイトのセキュリティが不十分で実際に個人情報が漏えいしてしまった場合、そのコストは莫大です。IBM によれば、2013 年米国におけるサイバー攻撃件数は 150 万件に及び、米国の調査会社の報告では、2014 年のデータ漏洩事故のコストは平均 350 万ドルにもなるそうです。ユーザーのデータを保護するのはお客様のためばかりではありません。Web サイト運営者自身のためでもあります。

ユーザーからの信頼の向上

テック・エドのアンケートによると、回答者の 100%が EV SSL サーバ証明書を持っている会社とのビジネスを希望するという結果がでています。HTTPS 利用時に証明書保有者の社名が入った緑のアドレスバーが表示される EV SSL サーバ証明書の利点は、ログインまたはチェックアウトページだけを SSL 化するのではなく、常時 SSL (ALWAYS-ON SSL)化することでより有効に作用します。SSL サーバ証明書を利用することでコンバージョン率が向上し、エンゲージメント指標が改善され、ブランドの評判を高めることも実証されています。

検索ランクの向上

Google の勧告に従い HTTPS everywhere（常時 SSL 化）を実施したサイトは、実施していないサイトと比べ、ランキングで高評価が得られます。このメリットは他のすべての SEO 要素と同様に、長期間にわたって保証されます。

常時 SSL (ALWAYS-ON SSL)への移行手順

常時 SSL (ALWAYS-ON SSL) への移行を成功させるために、以下のセクションをお読みください。購入したサーバ証明書をインストールするだけでは、Web サイトを正しく常時 SSL (AOSSL)化することができません。

1. 利用するホスト名をリストアップ

常時 SSL のためには、SSL サーバ証明書が必須です。

SSL サーバ証明書は、ドメイン名ではなくコモンネームと呼ばれるホスト名を証明する仕組みになっています。

例えば、【rms-digicert.ne.jp】と【www.rms-digicert.ne.jp】、【support.rms-digicert.ne.jp】はドメイン名自体は同じですが、ホスト名が異なります。仮に、rms-digicert.ne.jp の SSL サーバ証明書を持っていても、support.rms-digicert.ne.jp の証明書を持っていなければ、support.rms-digicert.ne.jp のサイトを常時 SSL にすることはできません。

常時 SSL にするためには、運営中・運営予定のすべてのホスト名を異なるドメインのものも含めてリストアップしてください。

2. 必要な証明書の種類決定

基本的な SSL サーバ証明書は 1 枚でひとつのホスト名を証明するものですが、証明書によっては 1 枚で複数のホスト名を証明できるものもあります。ホスト名ごとに証明書を取得すると枚数が多くなり管理が煩雑になり、更新漏れによる期限切れなどのトラブルになりかねません。そのため、できるだけまとめられるものはまとめ、枚数を少なくしましょう。

DigiCert の SSL サーバ証明書には複数の種類があります。リストアップしたホスト名と照らし合わせ最適な証明書を決定してください。

ケース 1

【rms-digicert.ne.jp】と【www.rms-digicert.ne.jp】のように、【ドメイン名】と【www.ドメイン名】で利用する、一番ポピュラーなケースには、SSL Plus が最適です。1 枚でドメイン名と www.ドメイン名の両方を証明します。SSL Plus には、事業者の実在を証明する組織（企業）認証タイプと、事業者の実在を厳密に検証し発行される、EV SSL Plus があります。

ケース 2

同一ドメイン名に属する複数のホスト名で利用する場合は、ワイルドカード証明書が適しています。

【www.rms-digicert.ne.jp】、【support.rms-digicert.ne.jp】、など、【***.rms-digicert.ne.jp】と

いう形のホスト名を 1 枚の証明書でカバーします。また、ドメイン名そのものもカバーされます。「***」の部分は任意です。ホスト名追加数にも制限はありません。便利なワイルドカード証明書ですが、EV タイプの証明書は提供できません。

ケース 3

利用するホスト名が複数のドメイン名にまたがる場合は、マルチドメイン証明書が適しています。所有者が同一のドメインであれば、ドメイン名の異なる複数のホスト名を 1 枚の証明書でカバーできます。マルチドメイン証明書は発行時に、利用するホスト名を証明書に登録します。EV マルチドメイン証明書もあります。

EV サーバ証明書について

EV タイプのサーバ証明書は、鍵マークだけが表示される一般の証明書とは違い、ブラウザのアドレスバーがサイト運営者の企業名入りの緑色で表示されるため、差別化が明確で、利用者からの信頼がより高まります。

3. CSR を作成

証明書を取得するためには、証明書を利用するサーバーで、CSR（証明書署名要求）を作成する必要があります。CSR にはホスト名やドメイン所有者の情報、暗号化の鍵情報などが含まれます。DigiCert をはじめとする認証局は、CSR に含まれる情報に基づいて証明書を発行します。

CSR の作成方法は利用するサーバーごとに異なります。

IIS ではサーバーに付属の CSR 作成ウイザードを使って作成できます。

Apache の場合は CSR 作成コマンドを実行する必要がありますが、Apache CSR ウイザードで必要情報を入力すれば、CSR 作成コマンドを入手できます。

4. 証明書を購入

どの認証局のどの証明書を購入するか、以下の事項について検討し決定してください。

証明の範囲

SSL サーバ証明書は、証明する範囲によってドメイン認証／組織（企業）認証※／EV 認証の 3 種類に分類されます。ドメイン認証は、証明するホスト名が実在することのみを証明します。

そのドメインの所有者が誰であるか、実在するかは証明しません。ドメイン認証の証明書は無料で発行している認証局から入手することもできます。

組織（企業）認証は、ドメインの所有者が法的に正しい住所に登録され、存在することを証明します。

EV 認証では、CA ブラウザフォーラムによって策定されたガイドラインに従い、ドメインの所有者の実在と実体をより厳密に確認し証明します。

DigiCert が発行している証明書は、組織認証と EV 認証です。

※DigiCert の組織（企業）認証 SSL は、個人でも取得が可能です。

認証局の信頼性

認証局の仕事は証明の発行だけではありません。失効管理をはじめ、一般には知られていない様々な重要業務を行っています。DigiCert のような信頼性の高い認証局を選択してください。

発行に要する時間

組織認証、EV 認証の場合、認証局から組織への認証のためのコンタクトがあります。このコンタクトが正しく完了した後、証明書の発行が可能になります。

DigiCert の証明書の認証作業は米国で行われますが、国内の他認証局と比べても、遜色ない短時間で発行しています。

サポート

株式会社アールエムエスは長年 DigiCert 証明書の正規代理店として活動しており、DigiCert の証明書についての様々な知識とノウハウを持っています。サポートはお任せください。

5. 証明書のインストール

DigiCert 証明書のインストール手順はインストール方法以下にあるサーバーごとのガイドを参照してください。

また、サポートが別途必要な場合は、電子メール info@rms-digicert.ne.jp にご連絡ください。

6. 正しく常時 SSL 化しているかの検証

証明書のインストールが完了したか、サイトが正しく設定されているかの検証を行います。常時 SSL のメリットを受けるためには、以下の確認が大切です。

インストールチェック

まず、証明書が正しくインストールされているか、プロトコルの選択が適切か、暗号化ツールの選択が適切かなどのチェックを行います。このチェックを行ってくれるのが Qualys SSL LABS の「SSL Server Test」です。これは、SSL サイトチェックの定番とも呼べるものです。

利用は簡単に始めることができます。Qualys SSL LABS SSL Server Test にアクセスし、Hostname 欄にホスト名を入力します。数分待つと判定がグラフ表示されます。総合評価で「A-」以上の評価を得られるようにしてください。

「SSL Server Test」の使い方については SSL サイト安全性評価を参照してください。

301 リダイレクト

新しく常時 SSL を開始した時点では、検索サイトや外部のディレクトリサービスなどのリンクが http になっていると思われます。http プロトコルでのアクセスを https に誘導するための設定を行ってください。Google は HTTP と HTTPS のサイトを異なったサイトであると見なします。301 リダイレクトを行っておかないと、重複コンテンツとして google の評価が下がることも考えられます。この設定は、恒久的リダイレクトあるいは 301 リダイレクトと呼ばれ、Web サーバーで設定することができます。

混在コンテンツ

リンクの記述、埋め込みコンテンツの記述などで http が使われていないかをチェックします。リンクや埋め込みコンテンツの記述で絶対リンクを使っている場合、http から https に変更します。

ページ本体は暗号化されていても、リソースのすべてが安全ではない場合（HTTP で絶対リンクが書かれている場合）には、ほとんどのブラウザが混在コンテンツに警告を表示するか、ページ表示そのものを行いません。安全でない要素はパッシブとアクティブに分類することができます。

パッシブには画像、音声、動画が含まれます。
アクティブにはスクリプト、CSS、WebSocket、フレームなどがあります。
混在コンテンツへのブラウザの対応は様々ですが、一般にはパッシブには警告して表示、アクティブは表示そのものを拒絶としているようです。利便性とセキュリティの兼ね合いからそのあたりが妥協点になっているようです。混合コンテンツはせっかくアクセスしてきた閲覧の中止を引き起こすばかりでなく、ハッカーにサイトの潜在的な脆弱性を宣伝することになります。

HSTS

HSTS と呼ばれる方法を使って、Web サイトへの 2 回目以降のアクセスでブラウザに https を強制するよう設定することができます。
例えば、ブラウザに rms-digicert.ne.jp あるいは http://rms-digicert.ne.jp と入力した場合、2 回目以降は自動的に https:// rms-digicert.ne.jp で接続します。
HSTS が設定されているサイトはサーバーが HSTS ヘッダーをブラウザに送信します。ブラウザは HSTS ヘッダーの正当性をチェックし、確認できると、そのドメインを http ではなく https でアクセスすべきドメインとして記憶します。
サーバー側の HSTS ヘッダーの設定は簡単です。apache では VirtualHost ディレクティブ内などで、IIS の場合は HTTP 応答ヘッダーで、それぞれ設定できます。

※HSTS はドメイン単位での利用が標準ですので、https を利用していないサブドメインがある場合は利用できません。