常時SSL（Always On SSL）による Web サイトの保護

オンラインサービス、官公庁、企業、ユーザに対するプライバシー、個人情報、セキュリティの新たな脅威を緩和するためのベストプラクティスを策定、推進することにより、インターネットの信頼性と安全性を高めます。

2012 年 3 月 7 日更新

目次

概要

インターネットは、信頼とユーザの安全を基盤として構築されてきました。商取引サービスや金融サービスを提供する世界中の大手企業は、長年にわたり、Secure Socket Layer（SSL）および Transport Layer Security（TLS）技術を使用して顧客の通信と取引を保護してきました。このセキュリティモデルは、Web ブラウザ、モバイルデバイス、電子メールクライアント、その他のインターネットアプリケーションの信頼性を確保するために 10 年以上にわたって使用されてきました。これは、現在も基本的に有効です。Web サイトやその利用者では通常、パスワードやクレジットカード番号などの機密情報を保護するために SSL/TLS を採用しています。2005 年以降、SSL/TLS を使用する Web サイトの数は 2 倍以上に増加し、今日では 450 万以上のサイトで認証局が発行した SSL 証明書が使用されていると推定されます[1]。

しかし、Web 2.0 とソーシャルネットワーキングの出現により、ユーザのオンライン接続時間とログイン時間は増加し、クレジットカード番号以外の通信も行われています。多くのユーザは、主な通信手段として Facebook、Gmail、Twitter を使用しています。また、ボットネット、マルウェア、情報漏えい、電子メールの偽造、オンライン詐欺、その他のセキュリティやプライバシー上の課題が急増するのに伴い、セキュリティ脅威の情勢も変化しています。しかし、Web のセキュリティの実装は、これらの変化に常に対応してきたわけではありません。多くの企業は、ユーザが Web サイトにログインする際の認証プロセスを SSL/TLS プロトコルによって暗号化していますが、その後のユーザセッションでは、ページを暗号化していません。この実装では、Web サイトの利用者が悪質なオンライン攻撃を受けやすくなる危険があり、信頼度の高い Web サイトを利用する場合でも、膨大な数のユーザが知らぬ間に脅威にさらされることになります。

オンライントラストアライアンス（OTA）は、セキュリティ、ビジネス、およびインタラクティブ広告のコミュニティに呼びかけ、協力してユーザを危険から保護しています。すべての関係者は、ベンダーに依存せず、簡単に実装でき、グローバルに利用できるセキュリティのベストプラクティスを採用して、信頼とユーザの安全を確保するために適切な手段を講じる義務があります。このようなベストプラクティスの 1 つが 常時SSL（「Always On SSL」あるいは「AOSSL」）です。これは、Web サイト全体で SSL/TLS を使用してユーザを保護し、ログインからログアウトまで持続的にセキュリティを確保するというアプローチです。常時SSL は、実績のある実用的なセキュリティ対策であり、ユーザが機密情報を共有したり表示でき るすべての Web サイトで実装する必要があります。

このホワイトペーパーでは、常時SSL の緊急の必要性と、ユーザにエンドツーエンドの保護を提供するための対策について説明しています。また、インターネットの安全性を高めるために協調して取り組み、常時SSL を他社に先駆けて使用している Facebook、Google、PayPal、Twitter の 4 社について詳細に説明しています。

[1] Netcraft 社の SSL に関する調査（2012 年 2 月）

OTA は、OTA 運営委員会のメンバーである AllClear、DigiCert、Epsilon、IID、Intersections、LashBack、MarkMonitor、Message Systems、Microsoft、PayPal、Pitney Bowes、Publishers Clearing House、Return Path、Secunia、Star Marketing Group、Symantec、TrustSphere および VeriSign の各社のご協力に感謝します。

また、このホワイトペーパーの作成にご協力いただいた Facebook 社の Alex Rice 氏、Google 社の Adam Langley 氏、PayPal 社の Andy Steingruebl 氏、Microsoft 社の John Scarrow 氏、Symantec 社の Quentin Lui 氏および Rick Andrews 氏、Twitter 社の Bob Lord 氏、および OTA の Craig Spiezle 氏に深く感謝します。

このレポートの最新情報は、https://otalliance.org/aossl.htm に掲載されます。コメントがある場合は、staff@otalliance.org 宛てに電子メールでお送りください。

オンラインでの持続的な保護の必要性

今日のユーザは、成長を続けるさまざまな大規模の Web 2.0 のサービスにアクセスし、オンラインで検索、共有、ショッピングを行い、充実したインタラクティブかつパーソナライズされた体験をしています。多くのサービスは、ブラウザの Cookie に依存し、ステートフルかつ 持続的なユーザセッションを作成して、このような体験を実現しています。一般的に、ユーザがサイトにログインするときは、ID 認証のためにユーザ名とパスワードを送信する必要があります。Web サーバがユーザごとに生成した一意のセッショントークン ID を Web ブラウザに送ると、その ID は Cookie にキャッシュされます。Web ブラウザは、ログインしたユーザがサイトとインタラクティブなやりとりを行うたびに、キャッシュされた Cookie の内容を Web サーバに送り返します。この Cookie は、期限が切れるか削除されるまで有効となります。

HTTP 上での保護されていない Cookie により、ユーザは攻撃を受けやすい状態に

多くの Web サイトは、HTTPS プロトコルを使用し、暗号化された SSL チャネルを通じてログイン情報を送信していますが、セッション Cookie を設定した後は、ユーザを HTTP に格下げします。この場合、ユーザのパスワードは保護されますが、その後、Web ブラウザがドメインにリクエスト送信をするときに、セッション ID を含む Cookie が平文で送信されるため、ユーザはセッションを乗っ取られやすい状態になります。また、暗号化されているのはログイン時のみであるにもかかわらず、すべてのセッションが安全であるとユーザに誤解させ、間違った安心感を生み出しかねません。

企業によっては、サイト全体で HTTPS を使用していても、セッション Cookie に secure フラグを立てていないことがあります。ユーザは URL を部分的に入力する（たとえば、「https://」を URL の前に付けずに入力する）ことが多く、ブラウザが最初にリクエスト送信する際、HTTPS ページにリダイレクトされる前に Cookie が公開されてしまうため、これも危険です。オープンネットワークを監視している攻撃者は、暗号化されていない HTTP リクエスト送信を 1 つ入手するだけで、ユーザの Cookie を盗み、アカウントを乗っ取ることができます。

これらの問題は新しいものではなく、セッション Cookie を使用しているすべての Web サイトに影響します。ユーザが入力したキーワードを送り返す検索エンジンも、このような攻撃を受けやすいと言えます。今後、これらの問題に対して企業は無関心でいられません。また、ユーザを教育するだけでは十分ではありません。業界におけるオンラインセキュリティの全体的な状況は転換点を迎えています。エンドツーエンドで信頼とユーザの安全を守るため、Web サイトは変わる必要があります。

セッションの乗っ取りは驚くほど容易に

セッションの乗っ取りは新しい問題ではありませんが、最近リリースされた「Firesheep」と呼ばれる Firefox ブラウザのプラグインは、保護されていない HTTP 接続（およびオープン WiFi ネットワーク）特有の脆弱性に関して、ユーザと攻撃者双方の関心を集めています。Firesheep は、Eric Butler 氏と Ian Gallagher 氏によって開発されたもので、このプラグインを使用すると、プログラミングスキルを持たない攻撃者でも、人気のある多数の Web サイトでユーザカウントを驚くほど容易に「サイドジャック」できるようになります。Firesheep は、カフェ、図書館、インターネットカフェなどで、暗号化されていない WiFi 接続のようなオープンネットワークを検出して接続し、パケット盗聴プログラムを使用して保護されていない Cookie を入手します。Firesheep が認識している保護されていない Web サイトをネットワーク上のユーザが利用すると、そのユーザ名と、接続しているサービスが即座に取得され、表示されます。攻撃者は、ユーザ名をダブルクリックして、そのアカウントにすぐにアクセスすることができます。

Firesheep は、機能の統合と使いやすさの点で革新的です。しかし、Butler 氏と Gallagher 氏によれば、セキュリティの専門家が数年にわたって警告を発してきた問題のおよぶ範囲とその重大性が、Firesheep によって明らかになったとのことです。また、攻撃者は、Firesheep の何年も前に作成された「Hamster」「Ferret」「CookieMonster」などのソフトウェアツールを使用して比較的容易にオープンネットワークを盗聴し、Cookie を盗み、HTTP セッションを乗っ取ることができます。

図 1：Firesheep 操作時のスクリーンショット

これらのツールを手にした攻撃者は、この脆弱性を悪用して、完全または部分的にユーザカウントにアクセスできるようになります。完全なサイドジャックを避けるために、ユーザがパスワードを変更するときに古いパスワードを確認するなどの予防策を講じている Web サイトもありますが、多くの場合、攻撃者はユーザカウントを完全に乗っ取ってパスワードを変更することができ、そのアカウントが接続している他のサービスを乗っ取る可能性もあります。

カフェだけの問題ではない

セッションの乗っ取りは、カフェなどに限定された問題にすぎず、暗号化されていない WiFi ネットワークの利用を避けることが解決策になると考えるユーザがいます。しかし、このような想定は現実的ではありません。実際には、Firesheep などのツールを使用することで、有線か無線かを問わず、暗号化されていない HTTP セッションで送信される Cookie を含むあらゆるネットワークトラフィックを傍受することができます。見過ごされているもう 1 つの点として、ソーシャルネットワークサイト、Web メール、Web 2.0 アプリケーションを利用している大規模企業と政府機関が挙げられます。従業員が保護されていないサイトにアクセスしてセッションが乗っ取られると、攻撃者はそのアカウントを媒介としてマルウェアを蔓延させることができるほか、権限の必要な資産へアクセスし、データセキュリティ侵害を引き起こす可能性があります。このような侵害によって生じる損害を歓迎する Web サイト運営者はいないでしょう。

ユーザを教育するだけでは不十分

ユーザの意識を向上させ、サイドジャックの危険に対抗するために、米国電子フロンティア財団（EFF）は、独自の Firefox 拡張機能である HTTPS-Everywhere を開発しました。これにより、Firefox では、一部の Web サイトに接続するときに HTTPS 接続のみが使用されます。さらに、EFF とインターネット関連の非営利の権利擁護団体である Access は、Web 閲覧の「最低限のセキュリティ」として 常時 SSL の認知度を高めて導入を促進させるため、「HTTPS Now」と呼ばれる国際的な啓蒙キャンペーンを開始しました。このキャンペーンの Web サイトでは、各サイトでの HTTPS の使用状況に関する情報をユーザが検索したり、提供したりすることができます[2]。HTTPS-Everywhere は、特定の Web サイトでは正しく機能するツールと考えられますが、対応していないサイトではユーザを保護することができません。また、HTTPS-Everywhere は、Chrome、Safari、Internet Explorer には対応していないため、主要なブラウザがこの機能に対応するか、デフォルトでこの機能を組み込むまでは、その利用価値は限定的です。

EFF の取り組みは称賛されるべきですが、ユーザの教育とクライアントサイドのツールだけでは、Web サイトにおけるセッション管理の脆弱性を解消することはできません。また、インターネットにアクセスするためにユーザがカフェ、図書館、空港、その他の公共の場所でオープンネットワークを利用しなくなるという状況は非現実的です。Web サイト運営者は、ユーザが使用するブラウザやネットワークの種類にかかわらず、データのプライバシーを保護する必要があります。サイドジャック攻撃を受ける前に予防策を講じることで、企業は、顧客の流失、および訴訟や評判の失墜に伴う深刻な経費の負担も避けることができます。

ユーザエクスペリエンスのすべてを保護する 常時 SSL

常時 SSL は、Web サイト利用者をエンドツーエンドで保護する、基本的かつ費用対効果の高いセキュリティ対策です。これは製品やサービスではなく、既存の SSL 証明書の代わりとなるものでもありません。むしろこれは、ログイン画面だけでなく、ユーザセッション全体を保護する必要性を認識した、セキュリティに対するアプローチの 1 つです。常時 SSL は、サイト全体で HTTPS を使用することに始まり、すべてのセッション Cookie に secure フラグを設定し、暗号化されていない HTTP 接続によってその Cookie の内容が送信されるのを防ぐことにもなります。また、EV（Extended Validation）SSL 証明書や HSTS などの手段を追加すると、中間者攻撃（Man-in-the-Middle Attack）に対してインフラをさらに強化することができます。

> 「常時 SSL は、最も一般的なネットワーク脅威の多くを防ぐ、比較的簡単で非常に費用対効果の高い方法であるとシマンテックでは考えています。このホワイトペーパーに記述されている、インターネット業界をリードする企業の経験によって、その導入の実現性とそれがもたらすメリットも証明されました。すべての Web サイト運営者が常時 SSL を早期に採用することが望まれます。」
>
> – Symantec 社の Quentin Liu 氏

他社が実施しており、あなたが実施すべきこと

オンライン攻撃がますます頻繁になり、実行が容易になるにしたがい、世界中の企業は、機密データを伴うすべてのオンライン取引の安全を確保するため、これまで以上に厳しく監視されます。政府機関やプライバシー団体は、企業に 常時 SSL の利用を求めています。

[2] https://www.eff.org/press/archives/2011/04/19-0

2011 年 1 月、Charles Schumer 上院議員（民主党、ニューヨーク州）は、SSL ハックの報告を受けて Yahoo! 社、Twitter 社、および Amazon 社 に文書を送付し[3]、「ハッカー志望者を歓迎している」ような HTTP の状況を非難し、常時 SSL の実装の促進を求めました。

現在、Facebook、Google、PayPal、Twitter など、世界有数の大規模で信頼度の高い Web サイトで 常時 SSL が実装されており、販促データや非機密データも含め、Web サイト上でやりとりされるすべての通信の暗号化に HTTPS が使用されています。これらの企業は、持続的な保護の重要性が高まっていることを認識し、Web 全体を通じてオンラインユーザに安全な環境を提供できるよう努めています。

Facebook

Web 上で最も利用者数の多いサイトである[4] Facebook の月間アクティブユーザ数は、2011 年 12 月末時点で 8 億 4,500 万人、同月の 1 日あたりの平均アクティブユーザ数は 4 億 8,300 万人でした[5]。Facebook 社は、ユーザの情報の保護に熱心に取り組んでおり、同社のセキュリティ担当チームは、スパム、フィッシング、マルウェア、その他のセキュリティ脅威から Web サイトを保護するため、高度なシステムを開発しました[6]。2011 年 1 月、より安全なプラットフォームをユーザに提供するための主要な取り組みの一環として、Facebook 社は 常時 SSL の実装を開始し、ユーザは HTTPS によって Web サイトを閲覧できるようになりました。この変化に対するユーザの反応は驚くべきもので、Facebook のアクティブユーザの 19 パーセント以上が、安全な Web 閲覧の有効化を選択しました。

膨大なアプリケーション移行の調整

Facebook 社は、100 万人を超える開発者によるシステムを HTTPS と OAuth 2.0（Yahoo 社、Twitter 社、Google 社などが共同で策定したオープンスタンダード）[7]に移行する際、さらに困難な課題に直面しました。HTTPS に対応していないサードパーティのアプリケーションでは、ユーザが安全な Web 閲覧を行っているときに、コンテンツの混在に関するセキュリティ警告がブラウザで表示され、多くのアプリケーションがブロックされます。そのため、この点に関して多大な努力を要しました。Facebook 社は、開発者の移行を支援するため、サイトとアプリケーションを HTTPS に移行するための開発者向けロードマップを作成し、6 カ月間にわたる計画の概要を明らかにしました[8]。

安全な接続に対応したアプリケーションを作成していた開発者の場合、移行は速やかに行われましたが、複数のアプリケーションを持つ一部の大規模な開発者の場合は、必要なコードを探して書き換えたり、必要なインフラの改良をするためにより多くの時間とリソースが費やされました。

> 「ネットワーク上でお客様のプライバシーが危険にさらされないため、安全で信頼できるサービスを提供する自信が高まりました。」
>
> – Facebook 社の Alex Rice 氏

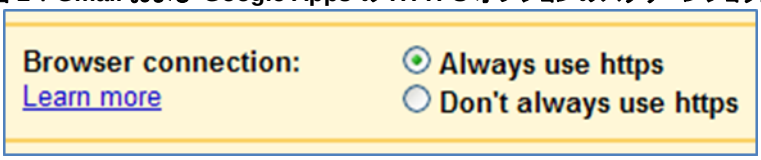
[3] http://www.infosecurity-magazine.com/view/16328/senator-schumer-current-internet-security-welcome-mat-for-wouldbe-hackers/
[4] http://www.google.com/adplanner/static/top1000/
[5] http://newsroom.fb.com/content/default.aspx?NewsAreaId=22
[6] https://www.facebook.com/blog/blog.php?post=486790652130
[7] http://oauth.net/2/
[8] https://developers.facebook.com/blog/post/497/

常時 SSL を導入するアプローチへの移行は、Facebook 社にとってその努力に値するものでした。現在、同社は単一の認証規格を使用し、HTTPS を通じてアプリケーションを提供することで、よりシンプルで安全性が高く、信頼できるプラットフォームを提供しています。このように第一歩を踏み出した Facebook 社は、現在、国際的なインフラを拡大して遅延を許容レベルまで抑える取り組みを進めています。Facebook のアクティブユーザの約 80 パーセントは北米以外に在住しているため、これは Facebook 社にとって重要な要素です。

Google

Google 社は、主に公共情報を扱う検索エンジンとして登場しましたが、同社の成長とともに、よりカスタマイズされたユーザエクスペリエンスを提供するようになりました。そのため、同社は個人情報のプライバシーを保護する重要性を以前から理解しています。Google 社は、Gmail と Google Apps を作成した際、自社で利用できるほど信頼性のある世界規模の製品を構築しようとしていたため、最初からこれらのアプリケーションを HTTPS に対応するよう設計していました。当初、HTTPS はユーザのログイン情報を保護するために使用されていましたが、その後、Google 社が 2008 年 7 月に公開した機能により、Gmail と Google Apps のすべてのユーザが「常に https を使用する」オプションが追加されました。

図 2：Gmail および Google Apps の HTTPS オプションのスクリーンショット



2010 年 1 月、Google 社は HTTPS を Gmail および Google Apps のデフォルト設定にすることを決めました[9]。これにより、ユーザはブラウザと Google 間で電子メールを常に保護することが容易になりました。この移行はコンピュータの追加や特殊なハードウェアを必要とせず、パフォーマンスへの影響はごくわずかでした。Google 社の研究者によると、SSL/TLS の影響は、同社のフロントエンドコンピュータにおける CPU 負荷の 1 パーセント未満でした（1 回の接続あたりのメモリ使用は 10 KB 未満で、ネットワークオーバーヘッドの 2 パーセント未満）。

安全な検索

安全な検索環境を提供することは、より複雑な課題でした。2010 年 5 月、Google 社は検索の暗号化オプションを導入し、ユーザは他のユーザによる傍受に対して、より保護された状態で検索ができるようになりました。また、Google 社は最近、サインインしているユーザのデフォルトの検索環境として HTTPS を使用し始めました。この変更により、ユーザの検索クエリーと Google の検索結果ページが暗号化されるようになりました[10]。このアプローチのセキュリティ上のメリットは明らかです。ユーザは、コンピュータと Google 間でエンドツーエンドの暗号化を使用することにより、より安全でプライベートな検索ができるようになりました。しかし、検索に関連するシステム、特に Web 解析と SEO（検索エンジンの最適化）は、より複雑でした。

[9] http://gmailblog.blogspot.com/2010/01/default-https-access-for-gmail.html
[10] http://googleblog.blogspot.com/2011/10/making-search-more-secure.html

ユーザが Google の検索結果をクリックして Web サイトにアクセスするときは、そのリクエストが Google からのリンクによるものかどうかを示す「リファラ」フラグがブラウザによって設定されます。SEO および Web 解析の専門家の多くは、この情報をもとに Web サイトの利用状況の統計データを収集したり、オンラインマーケティングの取り組みの効果を測定しています。しかし、ユーザが安全に検索をしている場合、検索キーワードは保護されています。つまり、Google の検索結果においてクリック先となるサイトは、ユーザが Google から来ていることはわかっても、個別のクエリーについては情報を受け取ることができません。

しかし、Google 社が指摘しているとおり、Google ウェブマスター ツールを使用すれば、サイトは過去 30 日間に自社サイトへのトラフィックを生み出した上位 1,000 個の検索クエリーをまとめたリストを受け取ることができます。この情報により、Web マスターは、HTTPS を有効にしている各ユーザの機密を保護しながら、ユーザトラフィックに関するより正確な統計データを保持することができます。さらに、ユーザが Google の検索結果ページに表示されている広告をクリックした場合は、ブラウザは継続してネットワーク経由で関連するクエリーを送信するので、広告主はキャンペーンの有効性を測定して広告やサービスを改善することができます。

Google 社は、将来的に自社製品の 常時 SSL 対応を強化することを計画しており、同社の研究者は、SSL/TLS に関する情報を引き続き公開しています。また、Google 社は、SSL をより広範囲かつ効果的に実装するための業界でのさらなる取り組みを強く支持しており、Web 全体にわたってすべての正当なコンテンツを保護し、すべてのユーザにシームレスで安全なユーザエクスペリエンスを提供するというビジョンを持っています[11]。

PayPal

1998 年以来、オンライン決済ソリューション分野での世界的リーダーである Pay Pal 社は、SSL/TLS を早期に採用しました。同社は、2000 年にはすでにユーザのログイン画面以降の全ページを HTTPS 経由で提供しており、2006 年には ログイン画面も HTTPS によって保護し始めていました。また、PayPal 社は、EV SSL 証明書を導入した最初の企業の 1 つであり、早くも 2007 年にはすべてのログインページにこの証明書を実装し始めていました[12]。

PayPal のサービスは多くのトランザクションを処理するものであるため、PayPal 社はパフォーマンスに関して独自の課題に直面しました。ユーザが 1 回のセッションで比較的長い時間を費やすサイトとは異なり、PayPal のサービスでは、その多くが短時間のセッションです。また、SSL/TLS ハンドシェイクはこのプロセスの中で最も時間を消費するため、Pay Pal 社は、ユーザエクスペリエンスに影響を与えかねないパフォーマンスを注意深く監視し、管理しなければならないことを認識していました。しかし、PayPal 社はブラウザへの接続によってすべてのコンテンツを同じサーバから提供できたため、実際には、HTTPS への転換によってサイトが高速化されたケースもありました。

PayPal 社のセキュリティ担当チームは、同社のサイトがフィッシャー、ハッカー、その他のサイバー犯罪者にとって特に魅力的な標的となっていることを十分認識しており、顧客と評判を守るために特別手段を講じました。その目的は、フィッシング詐欺や、SSLStrip（ネットワークパケットの傍受はするが、再ルーティングや改ざんは行わない受動的な Firesheep とは対照的なツール）などの活発な攻撃ツールを阻止することでした[13]。

[11] http://googleblog.blogspot.com/2011/10/making-search-more-secure.html
[12] https://otalliance.org/resources/EV/index.html
[13] http://www.thoughtcrime.org/software/sslstrip/

これらの取り組みは、PayPal 社のセキュリティエンジニアである Jeff Hodges 氏が共同開発した HTTP Strict Transport Security（HSTS）仕様のリリースとして結実しました[14]。HSTS では、Web サイトが SSL 接続の場合のみアクセスできることを明示したり、ユーザが SSL 接続の場合のみ特定のサイト上でやりとりできるようにする方法が規定されています。現在、HSTS には Google Chrome と Mozilla Firefox が対応しています。HSTS を使用する PayPal.com などのサイトは、そのサイトでは暗号化された情報のみが送受信されることをブラウザに明示し、ユーザが誤って HTTP のページにアクセスしたり、フィッシング攻撃や SSLStrip 攻撃によって HTTP ページに誘導されないよう保護します。

Twitter

リアルタイムの情報ネットワークである Twitter は、表現の自由が制限されている地域ではとりわけ、多くの話題の中心となっています。Twitter は話題性のあるいくつかのセキュリティインシデントにおいて標的となりましたが、Twitter 社は、サイトをより安全にする取り組みを急速に進めてきました。

Twitter の PC サイト、スマートフォンクライアント、モバイル サイトは、[ツイート]ボタンなどの機能も含め、すでに HTTPS に対応していましたが、Twitter 社はすぐに、常時 SSL の実装というより野心的な目標を掲げました[15]。2011 年 5 月、Twitter 社は、ユーザが決めた設定に基づき、常に HTTPS を使用できるオプションを提供すると発表しました。ユーザの非常に肯定的な反応に後押しされ、Twitter 社はこのオプションの実装を早めて 2012 年 1 月にすべてのユーザに提供し、HTTPS はすべてのユーザのデフォルトオプションとなりました。

Twitter 社は、常時 SSL の採用にあたり、いくつかの独自の課題を克服しました。同社がトラフィックの一部をコンテンツデリバリネットワーク（CDN）にアウトソーシングした際、その CDN が増加する SSL の負荷を確実に処理することが優先事項となりました。Twitter 社とそのパートナー企業にとっては、サイトの参照元や解析結果を追跡する能力を維持することも重要事項であり、Twitter 社のエンジニアはコードを書き換え、コンテンツの混在に関連する固有の問題に対処しました。

得られた教訓

Facebook、Google、PayPal、Twitter 各社のセキュリティ専門家が貴重な見識を提供し、公共サービスとしての OTA と共有することによって、Web サイト運営者およびサイトのユーザがサイドジャックやその他の攻撃から保護されました。Web サイトに 常時 SSL を実装する前に、これらの見識を重要なポイントとして考慮する必要があります。

SSL は高価ではない

一部の企業は、常時 SSL によって Web サイト運営のオーバーヘッドとコストが増加すると考えているため、実装には消極的です。認証局が発行する SSL/TLS 証明書は無料ではありませんが、その費用は固定されており、既存の SSL 証明書と差し替える必要はありません。複数のドメイン名を保護する必要がある場合は、証明書を購入するときにドメイン名を SAN（サブジェクトの別名）に追加することで保護できます。

SSL 証明書の費用とは別に、CPU 負荷の増加に対処するため、コンピュータの要件の問題と、ハードウェアを追加で購入する必要性を考慮しなければなりません。

[14] http://tools.ietf.org/html/draft-hodges-strict-transport-sec-02
[15] https://dev.twitter.com/docs/tweet-button/faq

人気のある大規模な Web サイトでは、ネットワークパケットの暗号化と復号のために必要となる付加的なコンピュータ処理によって、ハードウェア要件が大幅に増加することを予想すべきかもしれません。しかし、多くの企業は必ずしもこれに該当するわけではありません。

たとえば、Google 社の研究者が 常時 SSL に関連するコンピュータの負荷について行った広範な研究では、同社の IT 環境にハードウェアを追加で実装する必要はないことがわかりました。大半のデータによると、SSL/TLS のコンピュータへの影響は、技術の進歩によって最小限に留まりますが、自社の Web サーバのパフォーマンスをプロファイリングして、自社環境でのパフォーマンス上の不利益を確認しておくことを推奨します[16]。

「ここで読むのをやめられる方も、1 つだけ覚えておいてください。SSL/TLS の費用はもはや高くありません。10 年前はそうだったかもしれませんが、今は違います。どの企業でも、ユーザのために HTTPS を導入することができるでしょう。」

– Google 社の Adam Langley 氏

ネットワークの遅延によるパフォーマンスの課題

エンドツーエンドで HTTPS を使用することにより、多少のネットワークの遅延が発生します。この主な原因は、SSL/TLS ハンドシェイクを確立するために、クライアントとサーバ間でラウンドトリップが必然的に増加することです[17]。これは、海外にまたがるような長距離通信を、とりわけネットワーク帯域幅が限られている地域と行う場合や、ユーザが比較的短い SSL/TLS セッションを何度も開始するサイトの場合、特に厄介な問題となります。遅延は簡単に解決できる問題ではありません。しかし、適切な計画によってパフォーマンス上の不利益に対処することはできます。金融サービス企業では、デフォルトで強力な暗号化が実装されていながら、遅延の少ない充実した閲覧環境が提供されています[18]。また、Google 社の研究者が実験している「False Start」などの新技術によって、SSL/TLS ハンドシェイクに関連する遅延が 30 パーセント軽減されることが確認されています[19]。

安全な Web 開発は移行を容易にする

安全な開発プラクティスが初期の段階から守られていると、結果として、ほぼ同じ開発コストでも長期的に費用対効果の高い安全な Web サイトや Web アプリケーションを開発することができます[20]。特に多くの製品を持つ大規模企業の場合、コードを発見し、書き換えるにはコストも時間もかかります。現在構築されているすべてのサイトは、デフォルトで HTTPS を使用し、特にオンラインフォームでは、常に HTTP 接続を HTTPS に速やかにリダイレクトする必要があります。考慮すべき点は他にも多くあります。たとえば、MozillaWiki などのリソースや、Open Web Application Security Project（OWASP）などのグループによって、安全な Web アプリケーションおよび Web サービスを構築するための包括的なガイドラインが提供されています[21]。

[16] http://www.imperialviolet.org/2010/06/25/overclocking-ssl.html
[17] http://www.semicomplete.com/blog/geekery/ssl-latency.html
[18] http://www.wired.com/images_blogs/threatlevel/2009/06/google-letter-final2.pdf
[19] http://googleonlinesecurity.blogspot.com/2010/05/extending-ssl-to-google-search.html
[20] https://www.owasp.org/index.php/OWASP_Guide_Project
[21] https://wiki.mozilla.org/WebAppSec/Secure_Coding_Guidelines

コンテンツの混在による複雑さ

コンテンツの混在は、ハイパーリンクを使用するインターネットの特性によって生じる複雑な問題です。多くの Web サイトでは、複数のソースからコンテンツが表示され、それがサードパーティのものであることもよくあります。このコンテンツがハイパーリンクでリンクされていると、通常は安全なサイトでも、積極的な攻撃者がカスケーディングスタイルシート（CSS）や JavaScript コードの読み込みを悪用できるため、セキュリティが侵害される可能性があります[22]。同様に、HTTPS ページが HTTP 経由で画像、インラインフレーム、またはフォントを読み込む際、中間者攻撃によって HTTP のリソースが傍受されることがあります。また、Facebook などのサイトでは、コンテンツの混在を防ぐために SSL/TLS の使用を要求し始めており、今後、HTTPS を使用しないアプリケーションやコンテンツはブロックされるようになります[23]。これらの問題を回避するには、Web サイトのコードによって HTTP 経由でファイルを呼び出さないようにする必要があります。これには以下を含め、さまざまな要素が含まれます。

- <img> タグ内の画像ファイルやそれらのファイルへのリンク
- 外部の CSS（.css）ファイル
- JavaScript（.js）ファイル
- 埋め込みのメディアおよびインラインフレームのコンテンツ（Flash など）
- DOCTYPE 宣言で指定された URL または <html> タグ内の URL
- 外部の API および SDK の呼び出し（Facebok SDK など）

HTTP か HTTPS かの指定がないために安全なコンテンツと安全でないコンテンツが混在する問題を避ける方法として、相対リンクがあります。ただし、相対リンクは、検索エンジンスパムや「302 ハイジャック」攻撃によって悪用されることがあるため、使用する必要性があるかどうかを慎重に検討した上で、使用する場所や方法を決定する必要があります[24]。

Web サイトに 常時 SSL を実装するには

自社の顧客や評判を長期的に保護することを真剣に考える企業は、常時 SSL を実装しています。OTA は、常時 SSL を実装してユーザを保護する手順の概要を明らかにしています。表 1 に要約されているとおり、提供できる保護と保証のレベルは、どのようなセキュリティ機能の実装を選択するかによって異なります。

表 1：常時 SSL によるセキュリティ対策の概要

セキュリティ機能	可	良	優
HTTPS の持続的接続	✓	✓	✓
secure フラグの付いた Cookie	✓	✓	✓
EV SSL 証明書による HTTPS の持続的接続		✓	✓
HTTP Strict Transport Security（HSTS）			✓

[22] https://www.eff.org/https-everywhere/deploying-https
[23] http://googleonlinesecurity.blogspot.com/2011/06/trying-to-end-mixed-scripting.html
[24] http://www.dummies.com/how-to/content/prevent-someone-from-hijacking-your-web-sites-sear.html

HTTPS の持続的接続をすべての Web ページで実行する

常時 SSL は、Web サイトにアクセスしたユーザが、どのページにいてもできる限り簡単に「常に HTTPS を使用」できるようにすることを目的としています。HTTPS プロトコルは、HTTP と同じくテキストベースのプロトコルですが、暗号化された SSL/TSL セッション中に動作するという点で異なります。HTTPS を実施するために必要な手順は、以下のとおりです。

- サードパーティの認証局から取得した SSL/TLS 証明書をインストールする
- Web サーバへの接続をすべてポート 80 からポート 443 に切り替える
- 暗号強度を指定する（128 ビットなど）

初めは、ユーザが任意で HTTPS を有効にできるようにしてもかまいません。しかし、長期的には、HTTPS をデフォルト設定にし、必要に応じてユーザが HTTPS を無効にできるオプションを提供することが推奨されます。サイト全体で HTTPS を使用することで、ユーザにセキュリティやプライバシー上の重要な保証をするのに必要となる最低限のセキュリティを提供することができます。

SSL 証明書を正しく実装する

HTTPS を有効にするには、サードパーティの認証局から取得した有効な SSL/TLS 証明書を使用する必要があります。自己署名証明書でもユーザと Web サイト間の通信を暗号化することはできますが、信頼される機関によってドメインの身元が検証されていることをユーザに知らせることができるのは、認証局が発行した証明書のみです。接続に自己署名証明書が使用されていると、Web ブラウザはこれを潜在的なリスクと見なし、サイトが安全でない可能性があるという警告メッセージを表示することがあります。そのため、適切な認証局を選択することが非常に重要です。

また認証局は、SSL 証明書を用いた厳格なセキュリティプラクティスを維持し、Web サイトが SSL で保護されている場合、その Web サイトとユーザが通信した時に起こりうる何らかの詐欺行為への適切な補償となりうるものであることを認識してください。

また、あなたのインストールした SSL 証明書に、必要となるすべての中間証明書が含まれていることを確認してください。証明書に問題があると、多くの Web ブラウザは、サイトにアクセスしようとするユーザをブロックしたり、セキュリティの警告メッセージを表示します。厳格な検証を実施している Facebook などのサイトでは、証明書チェーンに問題がある場合、そのコンテンツを自社のユーザからブロックすることがあります。SSL/TLS の実装をチェックし、エラーや警告を修正するのに利用できるサードパーティ製の SSL 分析ツールもいくつか提供されています。

すべてのセッション Cookie に secure フラグを設定する

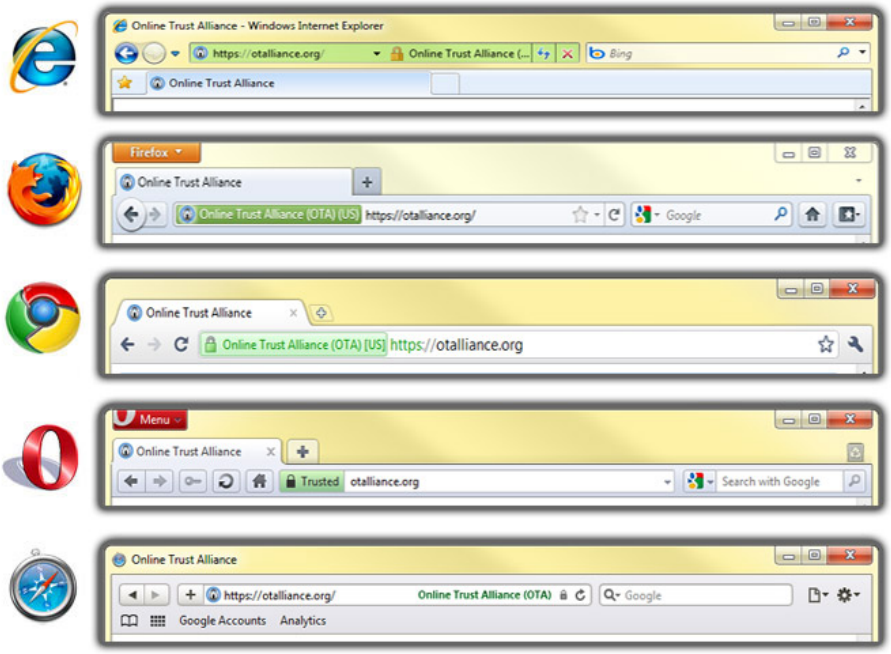
セッション Cookie には、オプションで secure フラグを設定できます。このフラグにより、ブラウザは、送信元サーバが HTTPS を使用して Cookie を返送する場合のみ、そのサーバにアクセスするようになります。secure 属性は、サーバからユーザエージェントに送られるセッション Cookie のコンテンツが保護されていることを示す、セキュリティ上のアドバイスと考えることができます。これにより、ユーザが誤って（またはだまされて）HTTP 経由で Web サーバにブラウザリクエストを送信した場合でも、Cookie が HTTP 経由で送信されるのを防ぐことができます。

EV 証明書による信頼性の向上

SSLStrip などの悪用に対する保護を強化するため、OTA は、Extended Validation SSL 証明書（EV SSL 証明書）の Web サイトへの実装を検討することを推奨しています。EV SSL 証明書で保護されたサイトは、CA ブラウザフォーラムによって確立された厳密な検証を受けます。このフォーラムには、30 以上もの大手の認証局やブラウザソフトウェアのベンダーが共同で参加しています。

この検証プロセスでは、信頼できるサードパーティのソースを使用して Web サイト運営者の身元と存在を確認します。EV SSL 証明書で保護された Web サイトにアクセスすると、アドレスバーが緑色になり、組織名が表示されるので、Web サイト運営者の身元を視覚的に確認することができます。

図 3：EV SSL 証明書が使用されているときの Web ブラウザの表示



OTA では、企業が責任を持ち、安全な接続が要求されるすべてのサイトに EV SSL 証明書を導入することを推奨しています。IT 部門は、EV SSL 証明書によってユーザのセキュリティが保護され、攻撃に対する企業の脆弱性が軽減されることを、経営幹部とエンドユーザが理解できるよう支援する必要があります。すべてのユーザは、EV SSL 証明書に対応しているブラウザにアップグレードすべきです。また、オンライン取引を行っているすべての Web サイトは、セキュリティおよびブランド保護戦略の一環として EV SSL 証明書を評価する必要があります。

HSTS の実装により、活発な攻撃を防止

多くの場合、HTTP ページからユーザがリダイレクトされるときや、HTTPS サイトに誘導するリンク（ログインボタンなど）をユーザがクリックしたときに、HTTPS 接続は開始されます。しかし、保護されていないページから保護されたページへ移行する間に、受動的に、またはユーザをだまして（たとえば、フィッシングメールを使用して）正当な Web サイトへの HTTP リンクをクリックさせることによって、中間者攻撃が行われる可能性があります。

これらのタイプの攻撃に対する最も強力な対策は、Web サイトに HTTP Strict Transport Security（HSTS）を実装することです。HSTS では、Web サイトが SSL 接続の場合のみアクセスできることを宣言し、ユーザが SSL 接続の場合のみ特定のサイト上でやりとりできるようにする方法が規定されています。HSTS には Google Chrome と Mozilla Firefox が対応しています。HSTS を使用する PayPal.com などのサイトは、そのサイトでは暗号化された情報のみが送受信されることをブラウザに示します[25]。HSTS を使用すると、ユーザが HTTP から HTTPS にリダイレクトされるときにセッション Cookie が盗まれるのを防ぐことができます。HSTS は現在、フィッシングや中間者攻撃に対する最も強力な対策です。

まとめ

これまでに多くの専門家が Web サイト開発者や運営者に、SSL/TLS を使用してユーザ認証、金融取引、その他の重要な活動を保護するよう勧告してきました。しかし、多くの企業はコスト、パフォーマンス、その他の問題に対する懸念から、サイト全体の暗号化をためらっていました。現在、インターネットは転換点を迎えており、今日のモバイル環境や、オンラインに常時接続しているユーザを保護するには、部分的な HTTPS の使用では明らかに不十分です。SSL/TLS 自体は今でも基本的に有効ですが、Firesheep の登場は、Web サイト運営者がログインページやショッピングカートだけでなく、ユーザエクスペリエンスのすべてを保護するきっかけとなりました。端的に言えば、SSL は自動車のシートベルトのようなものです。移動中は常に締めておく必要があります。

常時 SSL は、乗っ取りを企てる攻撃者を阻止する確実な方法ではなく、Web サイト上でやりとりを行うユーザを保護するために、全体的なセキュリティ戦略の一環として実装する必要があります。とはいえ、常時 SSL は、サイドジャックやその他の中間者攻撃を阻止できる実績のあるアプローチであり、大半の企業にとっては、導入費用もかつてほど高くはありません。Facebook 社、Google 社、PayPal 社、Twitter 社およびその他の企業が示すとおり、非常に大規模で複雑な Web サイトでさえ、HTTPS を使用して充実したユーザエクスペリエンスを提供することができます。遅延やコンテンツの混在などの問題によって課題が生じることもありますが、このホワイトペーパーで概説したガイドラインおよびベストプラクティスを利用することで、これらの問題に対処し、パフォーマンスを最適化することができます。

さらに重要な点として、常時 SSL を使用すると、Web サイトに対するユーザの信頼を守ることができます。信頼とユーザの安全を守ることは、非常に難しい問題であり、技術的な方法だけでは解決できません。たしかに、システムを単純に信頼しなければならない側面がユーザにはありますが、UNIX の主要な開発者の 1 人である Ken Thompson 氏の言葉を借りれば、「ソフトウェアを作った人を信頼することのほうが、おそらくもっと重要である」[26]と言えるかもしれません。セキュリティに対して 常時 SSL を導入するアプローチをとることによって、企業がユーザのセキュリティやプライバシーについて真剣に考え、ユーザを保護するために適切な手段を講じていることがユーザに伝わり、これがユーザを守る第一歩となるのです。

オンライントラストアライアンス（OTA）について

[25] http://hacks.mozilla.org/2010/08/firefox-4-http-strict-transport-security-force-https/
[26] http://www.ece.cmu.edu/~ganger/712.fall02/papers/p761-thompson.pdf

独立した非営利団体である OTA は、オンラインサービス、企業、ユーザに対するプライバシー、個人情報、セキュリティの新たな脅威を緩和するベストプラクティスおよびパブリックポリシーを策定、推進することによってインターネットの信頼性と安全性を高めることを使命としています。OTA は、業界、企業、政府機関と協力するためにオープンな対話を促進することで、インターネットの信頼性を弱め、規制への要求を増大させる各種のインターネットの乱用、脅威、プラクティスへの対処を進めています。

https://www.otalliance.org/

本書に含まれる資料は教育および情報提供のみを目的としています。発行者、オンライントラストアライアンス（OTA）、OTA のメンバー、および執筆者は、本書の誤りまたは不備について一切の責任を負いません。また、本書またはその内容の用途や解釈、および本書の使用によって直接的または間接的に引き起こされたすべての結果に対して、一切の責任を負いません。OTA は、本書に記載された推奨事項の採用を選択する企業のセキュリティプラクティスまたはビジネスプラクティスに関して、一切の判定や支持を行いません。法的助言またはその他の助言については、各社の弁護士またはその他の適切な専門家とご相談ください。本書で表明されている見解は、必ずしも OTA のメンバー企業または関連企業の見解を反映するものではありません。