MSIG
Mitsui Sumitomo Insurance Co., Ltd.
Thailand Branch

webサイトのセキュリティ対策

INTERRISK ASIA (THAILAND) CO., LTD.

40,000
1日に40,000以上のwebサイトがサイバー攻撃を受けています。

86%
86%のwebサイトに少なくとも1つの脆弱性があります。

1 million
毎日100万個のマルウェアが拡散されています。

$6 trillion
2021年までに6兆円の被害額が想定されています。

webサイトのセキュリティ

webサイトをマルウェアから守るにはどうすればよいのでしょうか。多くのインターネットユーザーは、普段、webサイトのセキュリティにあまり関心を持っていませんが、実は日常的にマルウェアの脅威に晒されています。
そこで本紙では、webサイトのセキュリティを知る上で基本となるSSL認証について、その種類と必要性をご紹介します。

SSL認証とは?

SSL（Secure Sockets Layer）はインターネット上でデータを暗号化して送受信する仕組みであり、SSL認証はSSLを適用する際の身分証明書です。
webサイトでは様々な情報がやり取りされていますが、データを暗号化するSSLはそれらの情報を第三者に漏えいさせないために必要不可欠な要素と言えます。

webサイトの種類

webサイトの種類によって求められる情報セキュリティのレベルは異なります。

① ブログなどの個人サイト

サイト訪問者のアクセス履歴やハンドルネームなどの情報がやり取りされます。含まれる個人情報は多くないため、一般的に情報漏えいのリスクは高くありません。

② 企業のマーケティングサイト

サイト訪問者のデータが企業のマーケティングに利用されます。サイト訪問者は入力する個人データがマーケティングに利用されることに同意する必要があります。収集される情報が多いほど漏洩した場合の影響も大きくなるため、求められるセキュリティ対策のレベルも高くなります。

（参考）アドネットワーク

アドネットワークとは、複数の広告媒体（Webサイト、SNSなど様々なソーシャルメディア）にまとめて広告を配信する仕組みであり、近年はWebサイトを用いた広告が普及しています。Webサイト上で広告を行う手法として主に広告バナーが用いられますが、バナーのリンク先が改ざんされ、悪質なWebサイトに誘導された事例もあり、セキュリティ対策を行う上では注意が必要です。

③ ショッピングサイト

住所、電話番号、クレジットカード番号などの詳細かつ重要な個人情報がやり取りされます。ユーザーネームやパスワードを含め、やり取りされる全てのデータは暗号化される必要があります。利用者もショッピングサイトのSSL認証の有無を確認することが推奨されます（SSLが適用されたWebサイトはアドレスが「http://」ではなく「https://」になります。）。

④センシティブ情報を取り扱うサイト

思想、信条や人種、社会的身分、犯罪の経歴などのセンシティブ情報を取り扱うサイトは、高いレベルでのセキュリティ対策が必要とされます。

SSL認証の必要数

SSL認証はWebサイトの名称ごとに取得する必要があります。例えば、あるWebサイトが、"www.example1.com" と "www.example2.com" の双方でアクセスできる場合、SSL認証はそれぞれの名称に対して必要になります。また、複数のWebサーバーを有している場合も複数のSSL認証が必要になるケースがあります。

SSL認証の種類

SSL認証には「Domain Validation：ドメイン認証」、「Organizational Validation： 企業実在認証」、「Extended Validation：厳格な企業実在認証」の3種類があります。これらの分類は認証を受けた企業が第三者機関によってどこまで詳細に調べられているかを示すものであり、暗号の破られにくさを示すものではありません。

① Domain Validation（DV）

SSL認証の所有者＝Webサイトの運営者がドメイン（インターネット上の住所＝Webページのアドレス）の使用権を保持していることを証明するものです。証明書にはサイト運営者の名前や所在地などの情報は掲載されないため、他の組織や企業になりすますことも可能であり、3種類のSSL認証の中ではセキュリティレベルは高くありません。

② Organizational Validation（OV）

SSL認証の所有者（組織、企業）が法的に存在することおよびその所有者がドメインの使用権を保持していることを証明するものです。OVを所有するWebサイトにアクセスするユーザーは、証明書を閲覧することでサイトを運営する企業名や所在地を確認することができます。

③ Extended Validation（EV）

世界標準のガイドラインに従って審査される最も厳格なSSL認証です。金融機関のWebサイトなどが取得しており、主要なブラウザで閲覧するとアドレスバーが緑色で表示されます。

SSL認証の必要性

自社のWebサイトで不正アクセスによる情報漏えいが生じた場合、レピュテーション（企業の評判、信用）が大きく低下します。また、マルウェアに感染して情報漏えい等が発生し、GoogleやYahooなどのポータルサイトでブラックリストに登録されると、そのWebサイトは検索できなくなります。

SSL認証を取得すると、Webサイトでやり取りされる様々な情報が暗号化されるため、情報漏洩のリスクが低減します。また、SSLの知識を持つサイト利用者に対しては、Webサイトの信頼性を向上させることができます。

Googleは2014年にSSL認証の有無をWebサイトのランキングアルゴリズムに組み込むことを表明し、SSL認証を得ているWebサイトが検索結果の上位に表示されやすくなるような設定が採用されています。このようにSSL認証の普及は全世界で進んでおり、今後、企業の情報セキュリティ対策の一環として益々重要視されていくものと考えられます。

（参考）

SSL認証に関する詳細な情報については、以下のWebサイトをご参照ください。

https://www.symantec.com/connect/blogs/typ es-ssl-certificates-choose-right-one

http://www.csoonline.com/article/3153707/sec urity/top-5-cybersecurity-facts-figures-and- statistics-for-2017.html

https://www.scmagazine.com/whitehat-security-release-website-security-statistics-report/article/536252/

https://www.techopedia.com/definition/24747/ cybersecurity

http://money.cnn.com/2015/04/14/technology/ security/cyber-attack-hacks-security/