「常時 SSL 化」時代に向けた

セキュリティ対策指南書

常時 SSL 化の普及によるサイバー攻撃の現状とセキュリティ対策について

LAC 株式会社ラック

目次

1. 概要

いまや、企業にとってインターネットは必要不可欠なインフラであり、情報システムから業務システム、広告宣伝などあらゆるシーンで活用されています。インターネットには、金融システムなどライフラインと呼ばれる重要システムが接続される一方、一般消費者も、スマートフォンやタブレットなどの操作でだれでも使える手軽さと、情報検索やインターネットでの買い物などの利便性から積極的に活用され、まさに社会の基盤となっています。

インターネットには、サイバー攻撃により金銭を不当に得ようとする犯罪者も接続しています。犯罪者は、個人情報やクレジットカード情報などの盗難や、正規のサイトに似せた詐欺サイト（フィッシングサイト）を作るなど、より巧妙な手段でサイバー攻撃を行ってきました。

これらのセキュリティ対策として開発された技術が、サイトの真正性証明と暗号化通信手段を提供する、SSL/TLS（以下 SSL）です。SSL により、正規サイトの判断や通信内容の保護が可能となるなど、Web アクセスの健全化に大きく貢献しています。そして今や、Web アクセスの約 80%が SSL で通信されている状況となりました。さらに今後は、HTTP/2[1]の普及により、ほぼすべての Web サイトの通信は、SSL になると予想されます。（常時 SSL 化）

しかし、SSL による暗号化は攻撃者の通信をも同時に秘匿されてしまうため、既存のネットワークセキュリティ対策が有効に機能しない事態を招いています。SSL による暗号化通信が一般化しつつある現代においては、このネットワークセキュリティ対策が無効化されている現状に対して、何らかの方策が急務です。

この『「常時 SSL 化」時代に向けたセキュリティ対策指南書』は、常時 SSL 化が普及したこれまでの流れとそれに関わる脅威環境の変化と新しい脅威への対策方法についてとりまとめました。本書が SSL 化による現状のご理解と、セキュリティ対策を行う際の参考になれば幸いです。

[1] 2015 年に公開された HTTP プロトコルの最新バージョン

2.インターネット利用の現状と暗号化

インターネットの商用利用が進むにつれ、通信内容の盗聴や本物の Web サイトに似せたフィッシングサイトを作って誘導するなどのサイバー攻撃の頻度が増加し、Web サイトのセキュリティ対策を向上させる目的で、Web サイトと Web ブラウザのネットワーク接続を安全にする SSL が考案されました。SSL は、サーバーとクライアントの間で受け渡しを行うデータの暗号化と、暗号化に使用する証明書によるサーバーの認証、そして通信内容を改ざんするなどのサイバー攻撃を防ぐための技術です。

SSL は、電子商取引などインターネットの商用利用の拡大に伴い普及が進みました。httparchive.org が調査した情報によると、2011 年には Web 通信のわずか 2%が SSL 化されているに過ぎませんでしたが、2018 年 10 月段階では約 80%の Web 通信が SSL 化されています。

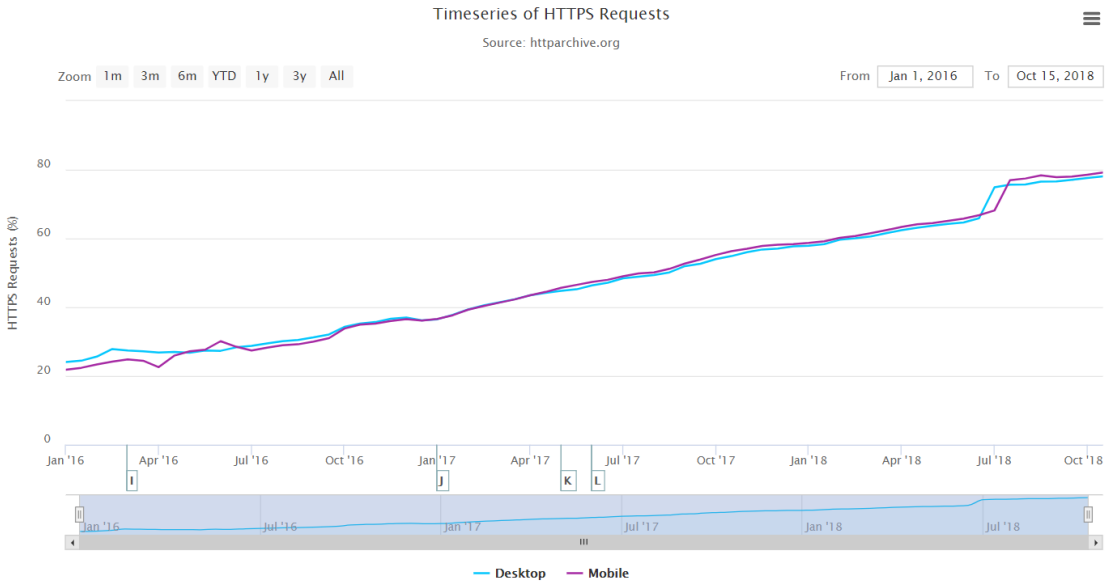

図 1　httparchive.org が公表する https リクエスト割合

急増の大きな理由は、2014 年 8 月に Google がセキュリティを考慮し SSL サイトを検索ランキングの評価要素とすることを発表[2]したことによります。Web をビジネスで活用する多くの企業では、過半数が検索エンジンからの流入である現状を考え、検索エンジンで圧倒的なシェアを誇る Google の動向に合わせて検索エンジン最適化（Search Engine Optimization：以下、SEO）の対策を行っていますが、検索ランキング評価向上の一環でもサイトコンテンツ全体を SSL 化する「常時 SSL」が当たり前になりました。

そして、この傾向をさらに加速させたのが 2018 年 7 月に Google が実施した Google Chrome で非 SSL サイトを閲覧すると警告が表示される仕様変更[3]でした。これは従来の非 SSL サイトの運用からすると、突然、不審サイトの扱いを受けてしまうものとなり、半ば強制的に常時 SSL が加速したことになります。

また、今後 HTTP/2 の普及により常時 SSL 化の流れはさらに加速されると予測でき、現在の 80%前後の常時 SSL 化の状況は、近い将来限りなく 100%に近づくと予想されます。

[2] Google ウェブマスター向け公式ブログ：HTTPS をランキング シグナルに使用します：https://webmaster-ja.googleblog.com/2014/08/https-as-ranking-signal.html

[3] サイトの接続が安全かどうかを確認する:https://support.google.com/chrome/answer/95617?hl=ja

3.SSL/TLS とは何か

SSL 暗号化がもたらした脅威環境の変化を理解する前に、SSL 暗号化の基本的な仕組みについて説明します。

インターネット接続で使用される通信プロトコルには TCP/IP が用いられますが、これは OSI の参照モデル[4]（厳密には異なりますが）のトランスポート層とネットワーク層（インターネット層）のプロトコルです。そして、HTTP や SMTP[5]などはアプリケーション層に位置しています。そして SSL についてはトランスポート層とアプリケーション層の間に存在し、HTTP などのアプリケーションよりも下層であるセッション層として実装されています。

暗号化通信までの簡単な流れを、Web アクセスのケースで図示すると次のようになります。
（SSL は、POP3 や SMTP、IMAP4 などでも利用できます。）

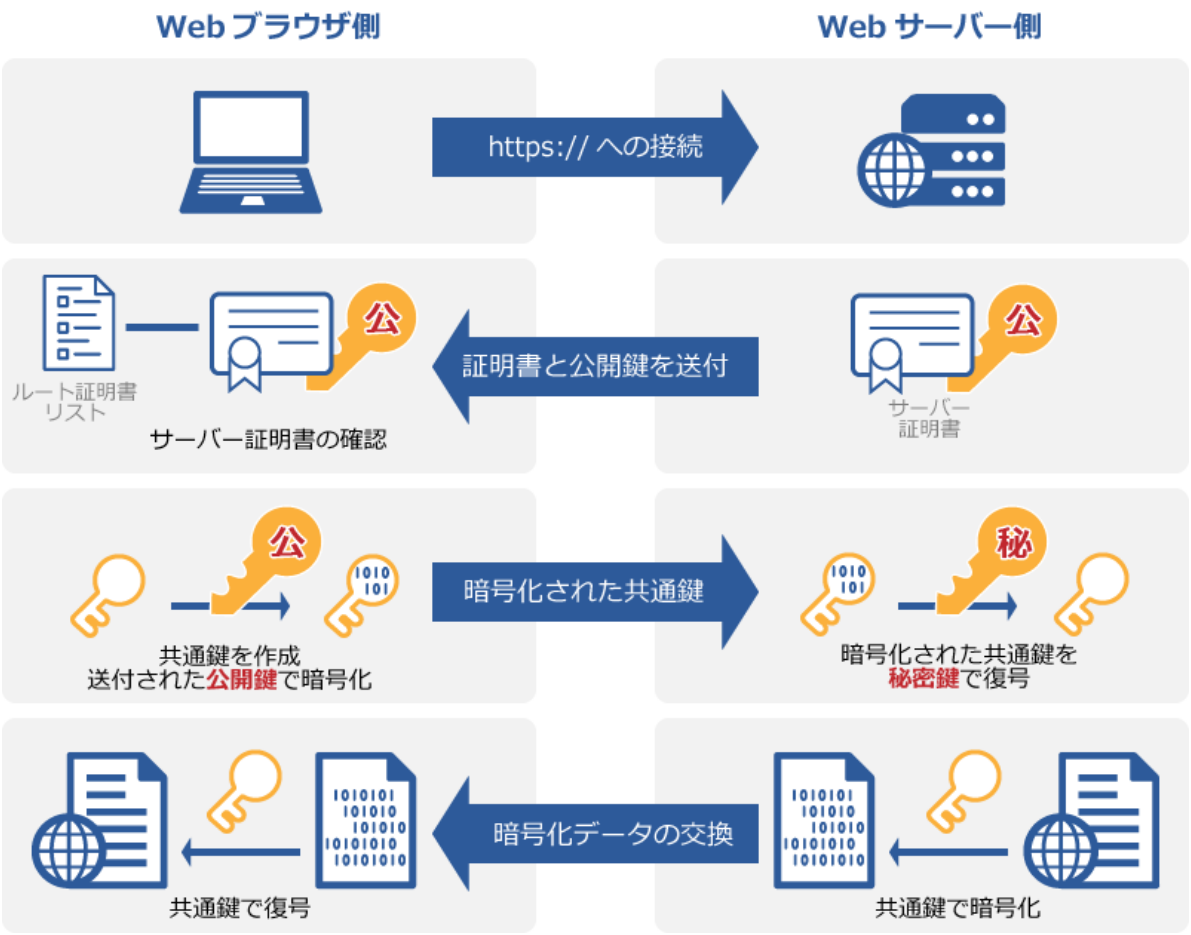

図 2　SSL 暗号化の仕組み

[4] 通信に必要な機能を階層として定義した国際標準化機構が策定した構造
[5] HTTP は Web 通信に用いられ、SMTP はメール通信に用いられるプロトコル

- ブラウザで SSL 接続が有効になっている Web サーバーに接続を開始します。
- Web サーバーは、Web サーバーに設定されているサーバー証明書と秘密鍵に対応する公開鍵を送り返します。（実際にはサーバー証明書に公開鍵は内包されています）
- ブラウザでは、受け取ったサーバー証明書が、クライアントに登録されたルート証明書リストで検証します。
- クライアントからは、暗号化接続のための一時的な共通鍵を作成し、それを Web サーバーから送られてきた公開鍵で暗号化し Web サーバー側に送ります。
- 公開鍵で暗号化された共通鍵を受けた Web サーバーでは、対応する秘密鍵で復号し共通鍵を取り出します。
- この段階で暗号化のセッションが確立し、双方が送受信する情報は、共通鍵で暗号化／復号処理を行います。

SSL 実装はトランスポート層とアプリケーション層の間、いわゆるセッション層で行われるため、一度暗号化セッションが確立すれば Web ブラウザや Web サーバー自体に特別な操作や設定を必要とせずに暗号化された通信を行うことが可能です。

SSL の導入は容易に行え、優れたセキュリティ機能を利用できます。

SSL 導入による優れたセキュリティ機能

- **発行された証明書が信頼される機関によるものかで判断ができる**

  SSL 接続で使用する鍵が、正しい中間認証局（クライアントのルート証明局に認められた認証局）で署名されたものかを確認することができます。ルート証明書で検証できない場合、その旨の警告を発し注意を促します。

- **コンピュータ間の通信セッションを暗号化し、データが盗まれても内容が判別できないようにする**

  対称鍵の共有のために、RSA2048 ビットの鍵などの公開鍵による暗号化を、通信の暗号化には AES256 ビットの鍵などの対称鍵による暗号化を用い、推測や総当たり攻撃による復号処理を現実的な時間でできないようにします。（安全性と相互接続性についての要求設定は、IPA が公開している SSL/TLS 暗号設定ガイドラインを参照）

- **通信データを通信の途中で傍受し、内容を改変して送りなおす改変行為をできないようにする**

  暗号化データを送信する場合、送信する暗号化したデータ全体のハッシュ値を生成し、中のデータが改変された場合に改変の事実がわかる仕組みを提供します。

Google は、SSL を採用し安全性の向上に取り組んでいるサイトを高評価しているため、多くの企業は SSL の導入に取り組むことになりました。

4.「常時 SSL 化」普及による新たな問題

Web サイトの信頼性を検証でき、通信データを保護し、データの改変を防ぐ SSL は、いまや 80%の Web 通信が暗号化されるまでに普及しました。しかし、SSL の普及は新たな課題を生じさせています。

以前は、Web ページからフォームなどを用いてサーバーへ情報を送信する際、入力された情報を保護する必要がある場合にのみ SSL による暗号化処理を施していました。しかし現在では、入力の有無にかかわらず Web サイト全体のアクセスに SSL を有効にする「常時 SSL 化」が進んでいます。

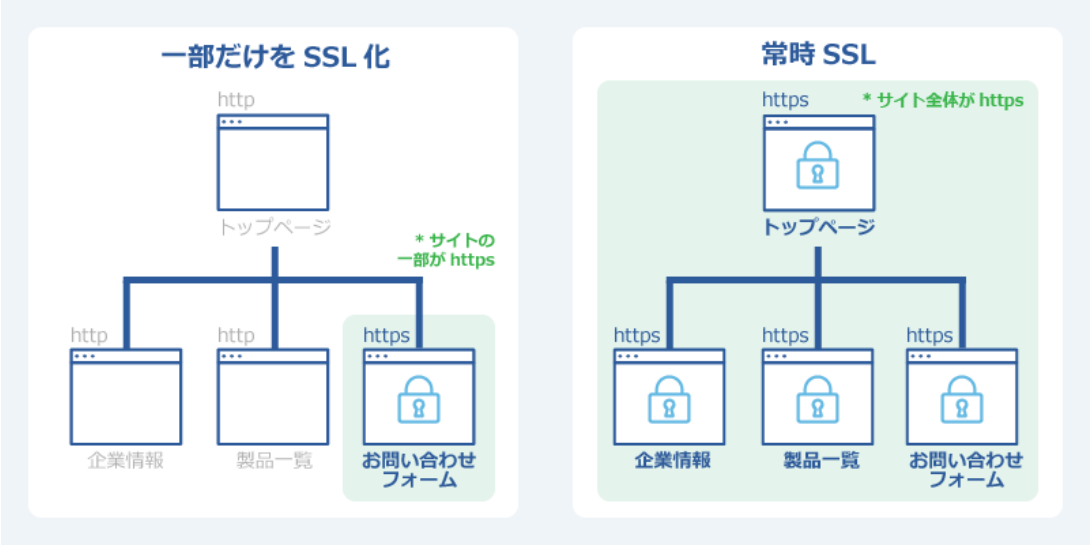

図 3　SSL 化を有効にする範囲の違い

SSL 化とセキュリティ対策製品

セキュリティ対策で活用されるソリューションの多くは、通信内容を分析することでサイバー攻撃を検知しているため、SSL により通信内容が暗号化された状況では、セキュリティ対策製品は機能しません。

セキュリティ対策製品の存在意義は、サイバー攻撃の有無について、検知・検証・軽減・防御を行うことにあります。つまり、セキュリティ対策製品は、通信の始まりから終わりまでのやり取りの内容を把握して初めて機能するものですが、常時 SSL 化が提供する情報の秘匿化は、セキュリティ対策製品に対しても情報を開示しない、諸刃の剣となります。

暗号化されていない通信の場合、次の図のように、Web ブラウザで正規 Web サイトの閲覧をしたり、Web コンテンツが送り返される内容を正確に分析することができ、不正なコンテンツがあれば防御することが可能です。

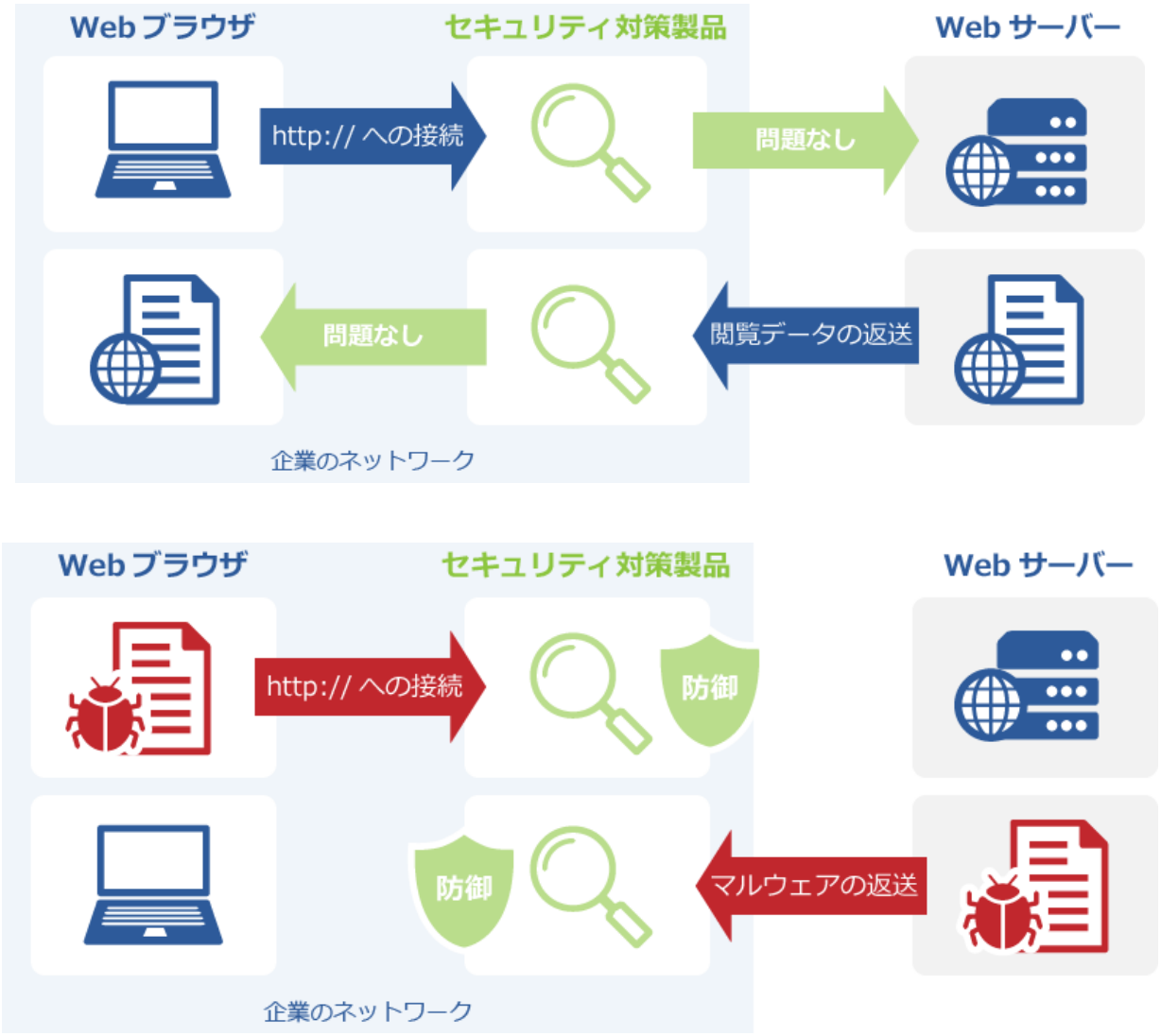

図 4　暗号化を行っていない Web アクセス時の挙動

通信暗号化状態ではマルウェアの検知が困難

常時 SSL 化が行われた Web サーバーとの通信においては、セキュリティ対策製品の防御は悪影響を受け、企業が侵入検知システムやネットワーク経路上のウイルス対策製品、情報漏えい対策製品を導入していたとしても、暗号化された Web サーバーからマルウェアが送り込まれたり、Web サーバーに機密情報が窃取されても、検知することは困難になります。

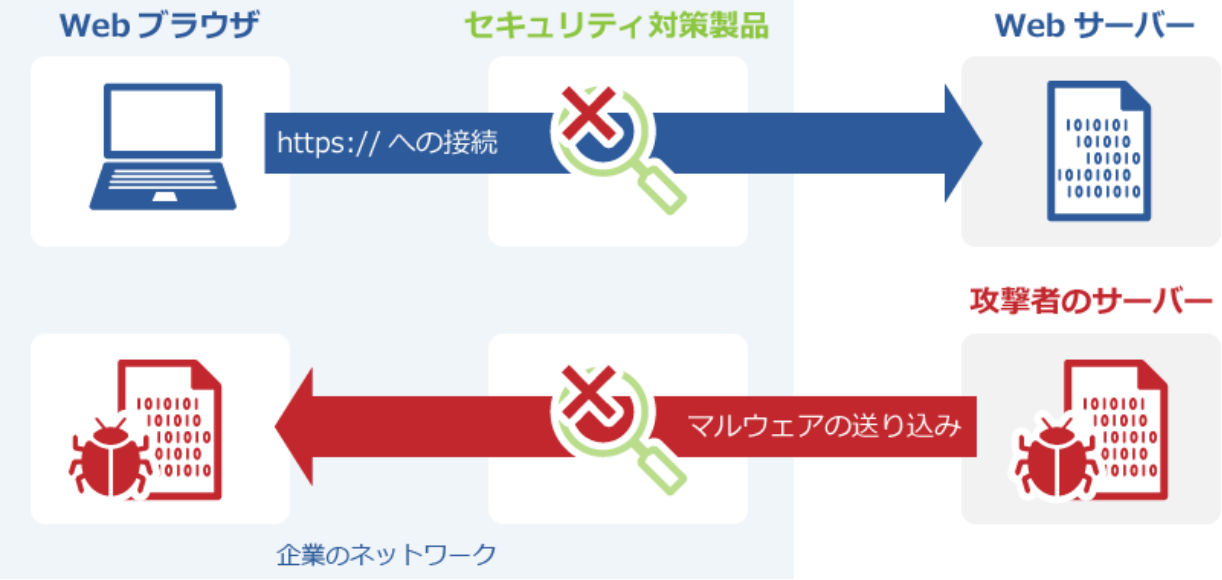

図 5 通信が暗号化された状態では Web サーバーからマルウェアが送られても検知が困難

通信暗号化状態では遠隔操作ウイルスも検知が困難

ラックが運営するサイバー救急センター®が対応した事案においては、遠隔操作されたマルウェアのコントロールに使用される「指令サーバー」は、実際に存在する企業が運営する正規の Web サーバーに不正侵入し悪用されているケースが確認されており、SSL により暗号化されていたために発見が遅れてしまったケースがあります。例えば、多くの方がコンテンツを共有するブログやデータ共有サイトが指令サーバーとして悪用された場合、常時 SSL 化の影響により通信内容の分析が機能しないことが懸念されます。

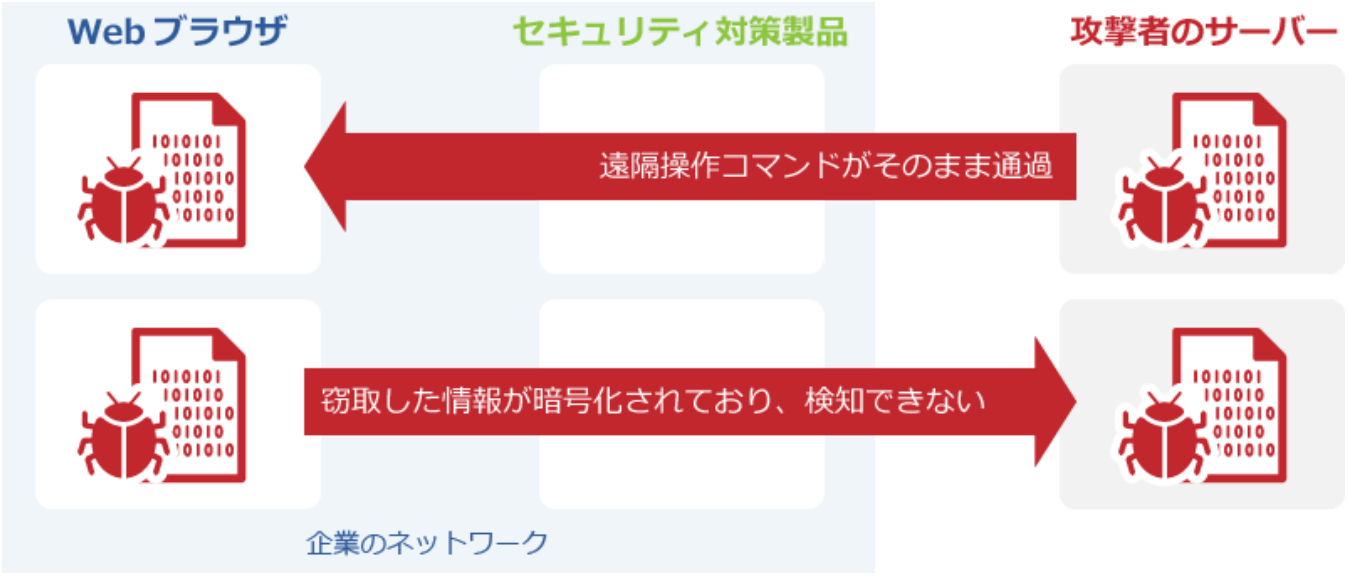

図 6 通信が暗号化された状態では遠隔操作ウイルスなどのサイバー攻撃も検知が困難

不正サイトは日々発生している

今や Web サイトを悪用したサイバー攻撃は日常的に行われており、Google 社の調査では毎日数万件の不正な Web サイトが発見されています。

図 7 では、2018 年にマルウェアを配布している Web サイトの発生件数（青いグラフ）は減少していますが、フィッシングサイトの発生件数（赤いグラフ）が増加していることが読み取れます。

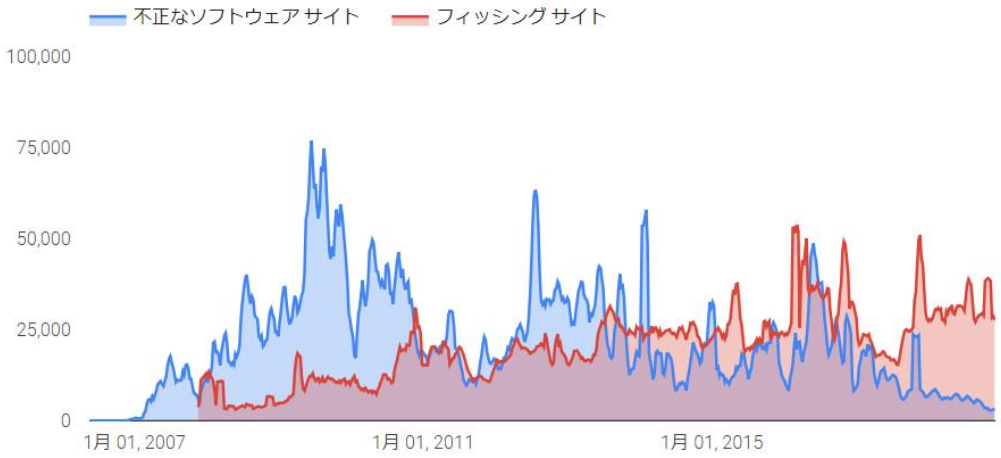

図 7 Google 社による不正サイトの発生件数の推移グラフ[6]

また、今現在動作を続けている危険な Web サイトの統計情報も公開されており、マルウェアの配布サイトの生存件数は急速に減少していますが、逆にフィッシングサイトは急増しており、Web を用いたサイバー攻撃は引き続き危険な状況にあります。

[6]セーフ ブラウジング: 不正なソフトウェアとフィッシング - Google 透明性レポート：https://transparencyreport.google.com/safe-browsing/overview?hl=ja

不正サイトも SSL を採用している

PhishLabs 社が自社のブログで 49%のフィッシングサイトが SSL を使用している[7]、と述べているように SSL はフィッシングサイトを信頼させるために悪用されている深刻な状況となっています。

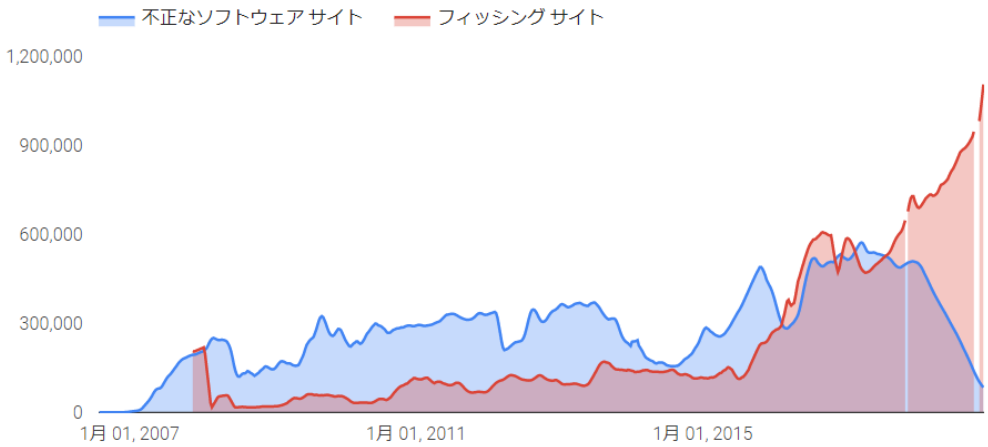

図 8 Google 社による不正サイトの生存件数の推移グラフ[6]

これらサイバー攻撃を仕掛ける危険な Web サイトは、攻撃者が用意したサイバー攻撃専用の Web サイトと、企業などが運営する正規の Web サイトを改ざんして悪用する例があり、圧倒的に正規のサイトが侵害されて、サイバー攻撃に悪用されている事例が目立ちます。

SSL が有効な Web サイトにアクセスした場合、信頼できる認証局が発行した証明書を持った Web サイトかどうかは、利用者が判断することができるという点で、フィッシングサイト対策に効果があるとも言えます。しかし、正規のサイトに寄生するフィッシングサイトに対しては、証明書の確認だけでは不正か否かの判断が困難になります。

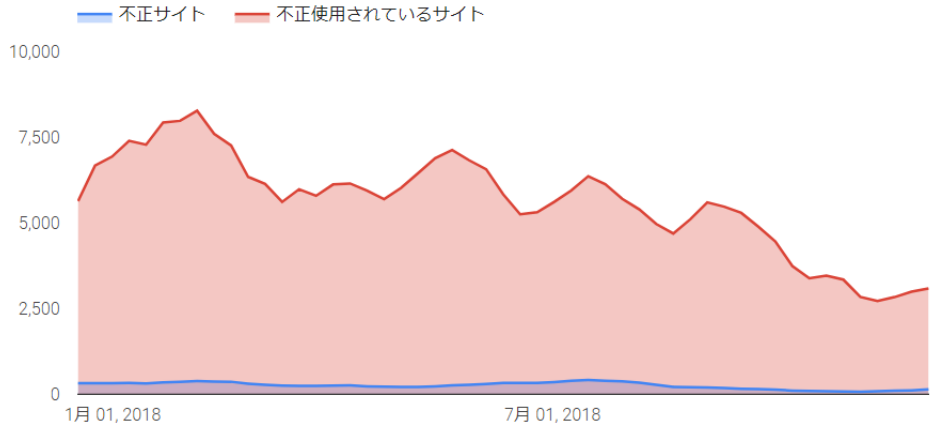

図 9　Google 社による不正使用されている正規なサイトのグラフ[6]

[6] セーフ ブラウジング: 不正なソフトウェアとフィッシング - Google 透明性レポート：https://transparencyreport.google.com/safe-browsing/overview?hl=ja
[7] 49 Percent of Phishing Sites Now Use HTTPS ：https://info.phishlabs.com/blog/49-percent-of-phishing-sites-now-use-https

不正サイトに対する Google の取り組み

Google は、フィッシングサイトや、サイバー攻撃により改ざんされた Web サーバーにユーザーを誘導しないよう、「セーフブラウジングテクノロジー（Safe Browsing）」を用いてウェブの安全性を高める取り組みをしており、コンテンツのインデックス作成のタイミングで不正と考えられるサイトも同時に発見し、検索結果に表示されたリンクをクリックする際にアクセスを思いとどまらせるメッセージを表示する機能を提供しています。もちろん、攻撃者自らが構築した Web サイトに関しては、検索エンジンに発見されないように構築することで、検出を避けるなど対策を行っていますので、この場合「セーフブラウジングテクノロジー」は効果を発揮しません。さらに特定の企業からのアクセス時のみサイバー攻撃を行う「水飲み場型攻撃」のような手法が取られた場合にも、「セーフブラウジングテクノロジー」は効果を発揮しません。

このようにサイバー攻撃を仕掛ける Web サイトは膨大な数に上り、常時 SSL 化はサイバー攻撃の事実を見えなくしてしまうリスクにつながっています。

「常時 SSL 化」時代に向けたセキュリティ対策

Web サイトの常時 SSL 化により、クライアントと Web サーバー間の情報の秘匿性が確保できる反面、セキュリティ対策機能が無効化されることが懸念されます。しかし、常時 SSL 化は確実にインターネットの常識となっていることから、インターネットを活用する企業はそれぞれが対策を施す必要があります。

『「常時 SSL 化」時代に向けたセキュリティ対策指南書』においては、現状で行える対策に関して説明します。

ロードバランサーなど通信機器を活用し「SSL インスペクションゾーン」を実装

確実な対策は、SSL で暗号化された通信データを参照可能な状況に「復号」し、既存のセキュリティ対策機能を正しく作動させることです。しかし、SSL 復号処理はネットワークの通信レスポンスに多大な負荷を与えることが懸念されています。そのため、多くの SSL 復号ソリューションはネットワーク機器ベンダーやセキュリティ対策機器ベンダーが、通信への影響を抑える工夫がされています。

SSL 復号ソリューションは、クライアントとサーバーの間に構成されたネットワーク機器が暗号化データを一時的に復号し、各セキュリティ機器にデータを通過させた後に再暗号化、そしてクライアントにデータを渡すという、いわゆるプロキシ（代理）機能を提供するものです。

基本的な考え方は、クライアントが暗号化された Web サーバーに接続する際、SSL 復号処理機器が Web サーバーに成り代わり暗号化接続を行います。また、SSL 復号処理機器はクライアントに成り代わり Web サーバーとの暗号化接続を行います。この独立した二つの暗号化接続の間で可視化された情報を、セキュリティ対策機器にデータを転送することで脅威を発見します。

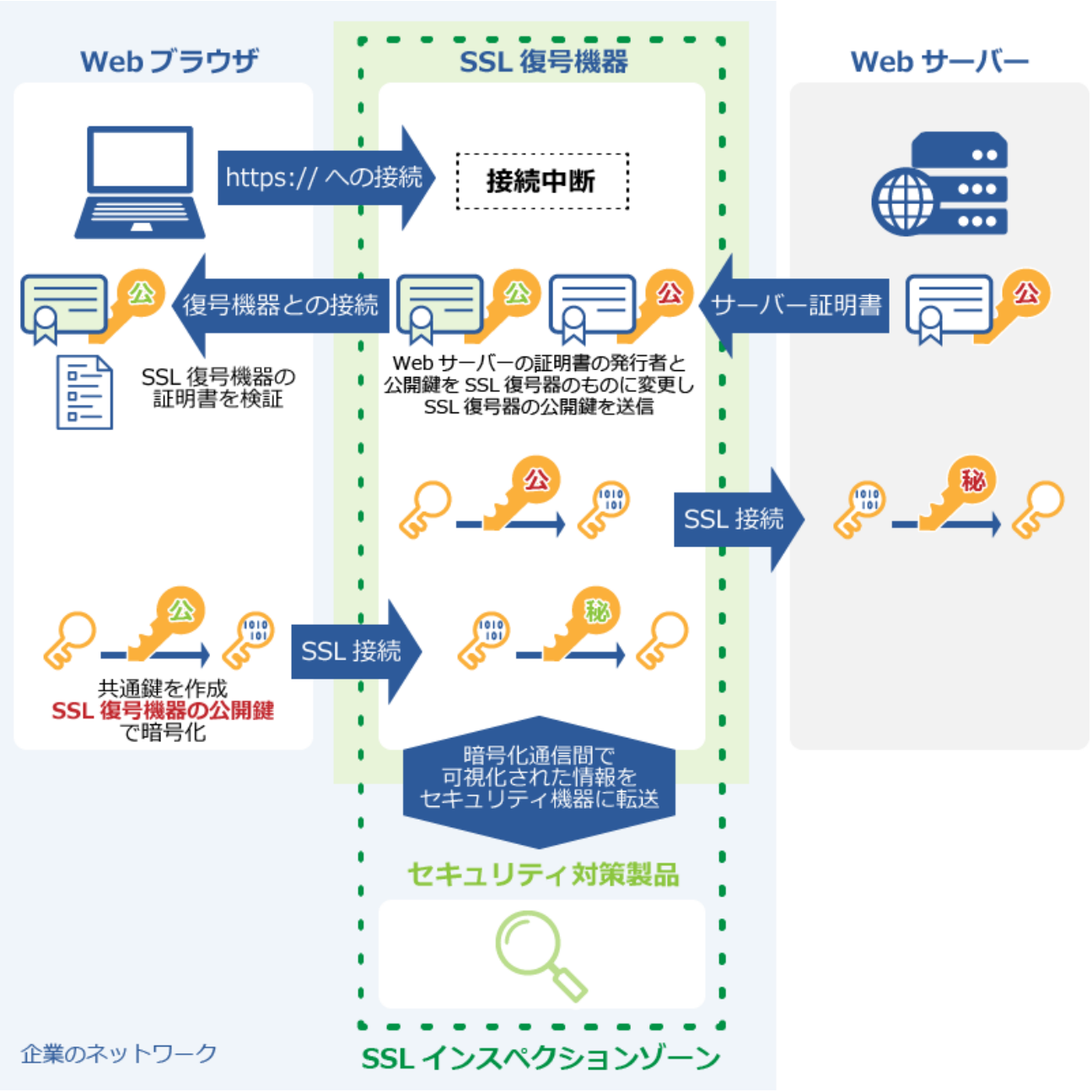

図 10　暗号通復号処理（SSL インスペクションゾーン）の仕組み

SSL インスペクションゾーン

SSL 復号機能は、複数のロードバランサ製品や UTM 製品、プロキシ製品などが実装しており、すでに侵入検知システムやウイルス対策ゲートウェイ、情報漏洩対策製品を活用している場合にはロードバランサ製品を用いることが一般的です。ラックでは、複数のセキュリティ対策機器に対して復号したデータを利用できるネットワーク領域を、「SSL インスペクションゾーン」と呼んでいます。

エンドポイントでの水際対策を実装する

Web ブラウザにより SSL 暗号化通信を行った場合、実際の通信データは暗号化されていますが、Web ブラウザなどアプリケーション側では平文（非暗号化状態）で取り扱われています。暗号化通信で不正なプログラムやスクリプトなどが送られたとしても、エンドポイントセキュリティ製品が復号されたデータを分析することで、サイバー攻撃を検知することが可能です。

しかし昨今では、従来のウイルス対策製品が実装しているシグネチャマッチング型のウイルス検知システムだけでは、対策が不十分であると言わざるを得ません。そのため、不正とみられる挙動を監視するビヘイビアブロッキング技術[8]、マルウェアの動作を安全なサンドボックス環境[9]で確認する機能などを実装していますので、最新の技術を活用したエンドポイントセキュリティ製品の導入が必要です。

また、水飲み場型攻撃のように、攻撃手法が判明しにくい標的型攻撃など、被害を受けてしまうことを見越したEDR(Endpoint Detection & Response)製品の導入も重要です。EDR 製品は、セキュリティ侵害が発生した際に被害の発生経路や被害内容を調査することを可能とするソリューションで、企業内部で発生したサイバー攻撃の痕跡などを収集し、分析と対処を可能とするものです。

Web サイトのアクセス制限を実装する

SSL による暗号化通信を行った場合であっても、通信先のサーバーの IP アドレスなどは判定が可能です。

多くの企業においては、プロキシサーバーを社内外のネットワーク境界に設置されていると考えられ、これらの機器により不正な情報を公開している Web サーバーへの接続を拒否するなどの対策が可能です。社員が使用する Web ブラウザでのアクセスはもちろん、クライアントコンピュータで動作するマルウェアが、犯罪者の公開しているサーバーに情報を送信する場合などにも検知することができる可能性があります。

これら不正なサイトの情報は、レピュテーションデータベースとして通信機器の接続拒否リスト（脅威インテリジェンス情報）として提供するサービスがあるため、これらを活用することでサイバー攻撃を抑制できる可能性はありますが、あくまでもネットワークおよびエンドポイントセキュリティ対策の補助と考えてください。

[8] ソフトウェアの行動の内容から不正なソフトウェアと判断する技術
[9] マルウェアを動かしても実際のシステムには影響を及ぼさない隔離環境のこと

効果的なセキュリティ対策の取り入れ方

SSL による暗号化通信に対して、暗号化通信データの復号による可視化、エンドポイントによるサイバー攻撃検知、不正サイトへのアクセス制限の 3 つの手段について紹介しましたが、これら対策の採用に関してはそれぞれの対策の特性を考慮した導入が必要です。

	SSL インスペクションゾーン	エンドポイントセキュリティ		Web サイトアクセス制限
		EPP	EDR	
ビジネスにインターネット利用が必須	○	○		○
ロードバランサーなど高速接続が必要	○			
ネットワークセキュリティ製品を利用中	○			
社員に Web 閲覧を許可している		○		○
事故発生時の原因調査が必須			○	
CSIRT を設置している	○	○	○	○

1．SSL インスペクションゾーンを構築し、対策をすべき企業

SSL インスペクションゾーンの構築は、ネットワーク機器の初期投資や運用負荷など、導入のハードルは低くありません。しかし、この対策が最も効果が高いことから次のような企業が対策を導入検討すべきです。

- インターネットがビジネスに密接に関係している企業
- ロードバランサーなどを用いた高速接続を必要とする企業
- 侵入検知システムやネットワーク経路上のウイルス対策製品、情報漏えい対策製品などのセキュリティ対策の運用を行っている企業
- インシデント対策の専門家チームである CSIRT を設置している企業

2．エンドポイントセキュリティ製品による水際対策をすべき企業

エンドポイント機器へのセキュリティ対策製品の導入は、ほぼすべての企業が実施していますが、最新のセキュリティ対策技術を活用したエンドポイント製品（EPP）および、セキュリティ侵害を検知および分析を行う EDR 製品の導入については、次のような企業が対策を導入検討すべきです。

- 社員にインターネットへのアクセスを許可している企業
- CSIRT を設置したり、事故発生時の原因調査を必要としている企業

3. Web サイトアクセスの制限を実装すべき企業

Web サイトへのアクセス制限は、ホワイトリスト形式や脅威インテリジェンス製品の組み込まれたネットワーク製品を導入することになりますが、この対策はあくまで補助的なものであると考えるべきで、次のような企業が対策を導入検討すべきです。

- 社員にインターネットへのアクセスを許可している企業
- CSIRT を設置していたり、事故発生時の原因調査を必要としている企業

6.まとめ

インターネットはすでに社会そのものであると言えます。世界中に膨大な数の利用者が存在し、さらに増え続けています。同時に犯罪者はあらゆる手口を行使し、金銭を窃取しようとしています。個人情報の窃取やフィッシングサイトの乱立を背景にして、その対策のひとつとして Web サイトの SSL 化が普及しましたが、犯罪者はその状況を逆手に取ろうとしています。

SSL が有効ではない Web サイトは安全ではない、という認識が広がる中、ほとんどの Web 接続は常時 SSL 化されることになります。つまり、インターネット利用者は、常時 SSL 化による Web サイトの安全策がもたらすデメリットを乗り越え、自らの力でサイバー攻撃を発見並びに防御することを求められているのです。

セキュリティ対策製品を導入したが実は脅威が見えていなかったという状況は深刻です。Web サイトの常時 SSL 化を前提としたセキュリティ対策の再構築をいますぐ検討し、実施すべきです。

なお、暗号化通信の復号については、Web アクセスの状況を把握する意味で、プライバシーの侵害と捉えられる可能性があります。就業規則やインターネット利用に関するガイドラインなど、社員との共通の認識を持つことも重要です。

まずは本資料『「常時 SSL 化」時代に向けたセキュリティ対策指南書』をお読みいただくことで、その課題を認識し、皆様の実行すべき対策を検討いただくことをお勧めいたします。

以上