暗号化、プライバシー、データ保護：バランスのとれたアプローチ

包括的なSSL/TLSインスペクションのための
ビジネス、プライバシー、およびセキュリティ

zscaler™

要点

SSL/TLS公開鍵暗号化は、データ保護の業界標準であり、Webトランザクションを保護する目的で、インターネットの多くで利用されています。そのセキュアな暗号化によって、転送中の特権付きデータは保護され、信頼と匿名性がユーザに提供されます。しかしながら、攻撃者もまた SSL/TLS を利用し、その信頼と匿名性を悪用して活動を隠蔽する場合があります。

企業の IT 管理者は、包括的な SSL/TLS インスペクション方法を採用することで、暗号化されたトラフィックに隠されたリスクを軽減する必要があります。本書では、暗号化された脅威がもたらすリスクを検証し、そのリスク管理が持つ、ビジネス、プライバシー、セキュリティにとっての意味を検討し、セキュリティニーズと従業員のプライバシー権をうまく両立させるための対策も提示します。最終的な目標は、個々の従業員の権利を保証し、脅威や攻撃から組織を保護する最善の方法を IT 管理者が確認できることです。

かつてのインターネットは、テクノロジに精通した一部の人に開かれた空間でしたが、

複雑な新しいビジネスや日常生活が行われる場所へと変貌を遂げました。「ユビキタス」によって新たなリスクが生まれ、「すべての人のためのインターネット」となったことから、ビジネスを遂行し、日常生活を送る目的でインターネットを利用する我々を騙そうとする犯罪者の活動場所にもなっています。

特に送受信中の場合は、特権付きデータを保護する必要があり、暗号化は、その最も実用的な方法を提供します。業界標準の SSL/TLS 暗号化プロトコルでデータをエンコードすることで、それを傍受する犯罪者が実用的な方法で（すなわち、多くのコストをかけることなく）復号化することはできません（図 1 の「トランスポート層セキュリティ [TLS] と Secure Sockets Layer [SSL]」のサイドバーを参照）。暗号化は、信頼の確立と匿名性の確保にも役立ちます。このような機能の組み合わせにより、SSL/TLS 暗号化は、簡単な Web ブラウズから e コマースでの購入までのインターネット上の通信を保護する最適の手段となっています。

今日のビジネス環境では、個人のプライバシーを保護するために、企業のリソースを保護し、個人のプライバシーも守ることが不可欠です。SSL/TLS は、どちらも正反対とも思える役割を果たすものですが、犯罪者に悪用されると、SSL/TLS テクノロジは非常に危険なものになります。マルウェアを暗号化して隠す目的で犯罪者に利用されたとすると、どうなるでしょうか？企業は今日、このような脅威にどうやって対抗できるのでしょうか？

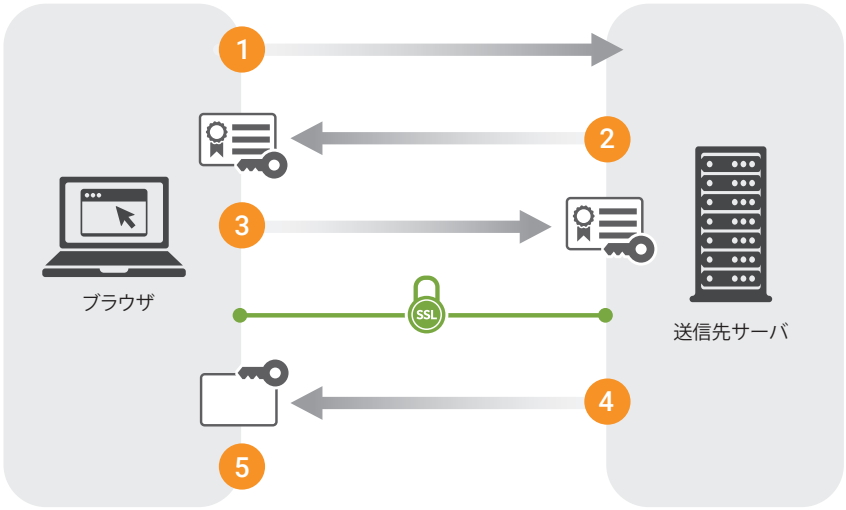
オープンからセキュアへ：SSL/TLSによってオンライン保護がどのように可能になるのか

インターネットは進化を遂げました。かつては、Yahoo、Google、Microsoft、あるいは近くの大学の Web サイトなどをブラウザで参照する場合でも、プライバシーや保護は必要ありませんでした。ブラウザのアドレスバーに URL を入力すると、Cookie が使われたり迂回したりすることもなく、途中で悪用される可能性のあるデータがほとんどない状態で、そのサイトに直接アクセスできました。ところが、現在は、同じネットワークを使って、当たり前のように個人情報や機密情報を共有し、ビジネスも行うようになりました。インターネットが生活空間になり、ブラウズという行為そのものも、貴重なデータになりました。このような変化によって、Web サービスを利用する、よりプライベートで安全な方法が必要とされるようになりました。

こういった背景から生まれたのが、暗号化テクノロジです。SSL（Secure Sockets Layer）暗号化（およびその後継である TLS（Transport Layer Security）は、サードパーティの検証済み「公開鍵」証明書を使って、ブラウザと送信先サイトの間にセキュアトンネルを確立します。これらの証明書とそれによって確立される関係によって、一連の相互にリンクされた信頼のチェーンが作成されます。信頼のチェーンとは、「信頼できる誰かがあなたを信頼しているので、私もあなたを信頼する」ということです。ある会社が、ブラウザが認識する認証機関（ベリサインや Thawte など）の証明書を購入した場合、その会社は、そのチェーンの信頼できる

メンバーになります。SSL/TLS で保護されたサイトを参照すると、ブラウザと Web サイトが認証情報（証明書）とパラメータを交換し、後続の通信が暗号化されるようになります。その通信がキャプチャされたとしても、ブラウザと Web サイトのサーバ以外がそれを理解することはできません。SSL と TLS プロトコルは数十年にわたり、このような暗号化機能を提供してきました。

ブラウザ/サーバ間接続におけるSSL/TLSの仕組み



1. ユーザがブラウザを開いて、HTTPS要求を送信します。
2. 送信先サーバが、暗号化された公開鍵とSSL/TLS証明書を返します。
3. ブラウザクライアントが証明書を検証し、暗号化された鍵を作成して送信先サーバに送り返します。（サーバ証明書が有効であると確認されないと、通信が終了します。）
4. 送信先サーバが受信した鍵を復号化し、暗号化されたコンテンツ（および鍵）をクライアントに配信します。
5. クライアントがコンテンツを復号化します。

図1.ブラウザから送信先サーバへの接続でのSSL/TLSの仕組み。

SSL/TLSは、3つの重要な機能をWebブラウズに提供します。

Privacy

セキュアトンネルに含まれるデータが表示されたり、他者と共有されたりすることはありません。

信頼

ブラウザが会話する相手が目的とするサーバ/Webサイトであることを確認します。

匿名性

ユーザのブラウズ動作は、ユーザとサーバの間のいかなる当事者からも隠されます。

TLS（Transport Layer Security）および SSL（Secure Sockets Layer）[1] は、暗号化を使用して2つのデバイス間にセキュアトンネルを作成することを目的としたネットワークプロトコルです。これにより、パブリックコンピュータネットワーク経由のセキュア通信が提供されます。SSLとTLSは、暗号化と復号化に公開鍵と秘密鍵の両方を使用する暗号化方式によってデータを保護し、証明書を利用することで、通信する当事者を認証します。

[1] https://en.wikipedia.org/wiki/Transport_Layer_Security

匿名性によって、ブラウザとその背後にいる人物に関する情報が保護されますが、ブラウザとサーバのIPアドレスが保護されるわけではありません。このギャップは、匿名化プロキシー[2]やTORなどの匿名ネットワークの存在によって解決されます。[3]

暗号化のリスク1：犯罪者に信頼を悪用される

SSL/TLS 暗号化は、プライバシーを保証するためのものです。ブラウザと送信先の間にいる誰にも、自分が参照していたり共有したりするデータを知られることはありません。しかし、信頼のチェーンを思い出す必要があります。すなわち、犯罪者もまた信頼を悪用しようとすることがあり（図 1 参照）、トンネルのプライバシーや匿名性の機能より、SSL/TLS 固有の信頼の方が重要になっているということです。

図2. 犯罪者がSSL/TLSで暗号化された配信を使って信頼を悪用する例。

たとえば、単純なインターネット検索には暗号化のメリットがないように思えますが、Google によって暗号化されます。データに機密性がない可能性はありますが、そのページを処理する Google によって信頼に不可欠な要素が提供されるという安心感が得られます。これと同じ暗号化の信頼のチェーンによって、検証が提供されます。最近のほとんどの Web サイトがそうであるように、Google は、すべてのページを SSL/TLS 経由で「HTTPS」URL を使って提供します。平文で文字がやり取りされる時代は終わりを告げました（Zscaler は、インターネットトラ

https://en.wikipedia.org/wiki/Anonymizer

https://en.wikipedia.org/wiki/Tor_(anonymity_network)

フィックのトレンドを観察できる立場にいますが、実際に、Zscaler 経由でやり取りされるデータトラフィックの83%以上が SSL/TLS で暗号化されるようになったことが確認されています)。[4])

セキュアトンネルモデルは、セキュリティを考慮して設計されたものですが、ユーザの信頼に関して言えば、悪用可能であることに変わりありません。すべての組織（および個人）が SSL/TLS 証明書を購入でき、組織はその証明書を使用して、正規のインターネット送信先（または正規の Web ページのコンポーネント）を取得あるいは模倣し、正当な証明書でサイトを侵害します。犯罪者は、このような方法でコンピュータの背後にいる人を騙し、貴重なユーザデータにアクセスして、転送中の暗号化されているデータであっても復号化できます。犯罪者は信頼できる当事者を装います。トラフィックは暗号化されているため、データ収集は検知されず、そのような行為をブロックする目的で導入されているコントロールやツールを回避します。

暗号化リスク2：攻撃者がマルウェアを隠す

フィッシング、スプーフィング、ランサムウェア攻撃の増加によって、インターネットに対する信頼が失われました。どうすれば、正規のサイトを閲覧していることを確認できるのでしょうか？どうすれば、サイトのコンテンツ（広告、記事、要素）が侵害されていないことを知ることが出来るのでしょうか？どうすれば、明らかに正規に見えるサイトに暗号化されたマルウェアが潜んでいないことを確認できるのでしょうか？

攻撃者は多くの場合に、正規のサイトへのコンテンツのフィードに利用される、CDN（Content Delivery Network）などのサードパーティプロバイダを侵害（または偽装）し、そうすることで、意図や目的は違うとしても、HTTPS で保護された正規のサイトでマルウェアを拡散することができます。

犯罪者は、SSL/TLS 暗号化を使って脅威を隠すようになっており、その脅威の高度化も進んでいます。これは新しい脅威ではありません。攻撃者は常に、安全なコードにマルウェアを隠してきましたが、そのために必要なコストが大きく変わりました。数年前から、無料の SSL/TLS 証明書を簡単に利用できるようになり、破壊的なマルウェアを暗号化するコスト（と労力）が大幅に低下しました。

Zscaler が確認した、暗号化されたトンネルで発見される脅威の数が、この数年で指数関数的に増加しました。現在、検知される高度な脅威の 54%以上が、SSL/TLS 暗号化チャネルを経由するものです。[5] さらに問題なのは、SSL/TLS で暗号化されたフィッシング攻撃が 2018 年に 300%も増加したことです。[6]

攻撃者は、同じ SSL/TLS プロトコルを使用して、マルウェアのソース（「ドライブバイ」などの、マルウェアが置かれた専用の暗号化サイトなど）やマルウェアのアウトバウンド通信を暗号化します。その暗号化は、「信頼できる」データという幻想を生み出し、犯罪者が企業に侵入して資産にアクセスし、データの外部への持ち出しをわかりにくくするフリーパスを提供することになります。

---

https://www.zscaler.com/threatlabz/encrypted-traffic-dashboard

https://www.zscaler.com/resources/solution-briefs/add-advanced-threat-protection-to-close-your-security-gaps.pdf

https://www.zscaler.com/blogs/research/february-2018-zscaler-ssl-threat-report

暗号化のリスク3：悪意ある人物がデータの外部への持ち出しを隠す

社外の犯罪者がデジタル資産を盗む目的で企業ネットワークに侵入する場合、その犯罪者は、企業のセキュリティ境界の外部にデータを持ち出すという課題に直面することになります。社内の犯罪者も、同じ課題に直面します。社内の独自情報をどのように外部に持ち出せばよいのでしょうか？

犯罪者は、インバウンドの暗号化されたデータにマルウェアを隠します。場合によっては、そのマルウェアが組織で活動を開始して内部システムに感染し、外部の C&C（コマンド & コントロール）サーバに接続して、重要な情報を外部に持ち出すこともあります。

暗号化は、悪意の（時には偶発的な）情報漏洩を隠すことができます。アウトバウンド SSL/TLS をインスペクションすることなく、管理者がデータの機密性が確保されていることをどのように判断できるのでしょうか？ SSL/TLS インスペクションは、インバウンド（犯罪者を排除するため）とアウトバウンド（機密情報が持ち出されないようにするため）の両方のデータトラフィックに対応する必要があります。アウトバウンドの例としては、データの損失の防止や、ゼロデイ攻撃のデータ持ち出しの脆弱性の特定と修復には、SSL インスペクションが不可欠です。[7]

プライバシーの新時代におけるアクセスとセキュリティのバランス

インターネット接続の進化によって、平文から暗号化されたデータの送受信へ、暗黙的な信頼から明示的な信頼へと変化し、プライバシーの新時代を迎えました。このことは、個人データ管理に対する消費者からの声だけでなく、ヨーロッパの GDPR（一般データ保護規則）[8]、カナダの Personal Information Protection and Electronic Documents Act（個人情報保護および電子文書法）[9]、米国のユーザのプライバシー件を規定するいくつかの既存の（カリフォルニア州、メイン州、ネバダ州）あるいは提案された（ハワイ州、イリノイ州、マサチューセッツ州、ミシシッピ州、ニューメキシコ州、ニューヨーク州、ロードアイランド州、テキサス州、ワシントン州）法規制ガイドラインにも反映されています。

ブラウズやインターネットのすべてのトラフィックが同じわけではありません。ほとんどの場合、プライバシーをどのように捉えるかは、個人によって異なります。民主的で自由な考え方をするユーザによるブラウズは個人的なものである可能性が高いのに対し、権威主義の強い Web ユーザは、Tor などの匿名ネットワークを使って、海外の家族との通信が検閲されないようにします。いずれの場合も、データはユーザ自身のものであり、権威主義の政府機関を除けば、各ユーザのプライバシー権の保護に反対する人はほとんどいません。どちらのユーザは、データの損失または傍受のリスクを負っており、そのリスクは、自分の家とデバイスに限定されます。

---

https://searchsecurity.techtarget.com/definition/zero-day-vulnerability

https://eugdpr.org/

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

企業や政府が提供するインターネットアクセスとなると、話は変わってきます。ほとんどの人が、インターネットである程度のプライバシー権が企業ユーザに保証されるようにする必要があることに同意します。ユーザの買物の習慣、休暇先の選択、趣味、またはブラウズしたサイトを仲間の従業員に知らせるようにする理由はほとんどありません。多くの場合、プライバシーを管理するさまざまな法律がその目的を支援しています。SSL/TLS は長年にわたり、そういったプライバシー、さらにはブラウズの匿名性を可能にしてきました。

しかしながら、期待されるプライバシーにはコストとリスクが伴います。犯罪者が自らの利益のためにその特権を悪用できるのであれば、それでもプライバシーを保護できるのでしょうか？エンタープライズ環境では、リスクは、一人の従業員だけではなく、組織全体に関係します。暗号化テクノロジの機能という点から言うと、今日の企業の IT 管理者は、侵入しようとする脅威のリスクとプライバシーの保証を比較し、その重要性を検討し、個人である従業員の権利と企業を保護するための要件をうまく両立させる必要があります。

組織では、絶対的なプライバシーに対する権利の見解はあまり明確ではありません。インターネットを使用するすべての企業、つまりは、あらゆる企業が、従業員、株主、顧客に対し、自らを保護し、法律および法規制のガイドラインを遵守する責任を負っています。IT 管理者は、技術的および手続き上のコントロールを使用することで、攻撃や危険な行動を防止し、検知します。リスクを軽減して「家」を保護するには、内部、インバウンド、およびアウトバウンドのすべてのデータトラフィックにこれらのコントロールを適用する必要があります。

法規制の状況によって、企業のデータ管理が複雑になる可能性があります。ヨーロッパの一部の地域では、個人の Web 閲覧のプライバシーと場合によっては匿名性を確保するために、従業員の個人情報を保護することが、企業に求められています。たとえば、ドイツの Telekommunikationsgesetz[10]（「Telecommunications Act」または TKG）は、従業員による個人的な使用のためのインターネットへのアクセスを提供する企業に適用されるものと一般的に考えられており、TKG はユーザを「電気通信の秘密」の対象とするよう、明確に要求しています。また、サービスを損害や傍受から適切に保護し、かつ、ユーザが閲覧するデータを適切に保護することを組織に義務付けています。TKG のコンプライアンスが必要とされる企業は、ユーザの「電気通信の秘密」と資産保護をうまく両立させる必要があります。

最近の Google 透明性レポートによると、[11]Chrome ブラウザのトラフィックの最大 93%が暗号化されています。悪意のある人物が暗号化されたチャネル経由で高度な脅威を送り込み、企業のセキュリティコントロールを回避する今、企業が自らとそのデータの両方を保護し、データ保護の法規制に準拠した形で従業員のプライバシー権も守るには、どうすれば良いのでしょうか？

トンネルを開く — SSL/TLSの復号化とインスペクション

企業環境におけるマルウェア攻撃は、1 人の個人に限定されるものではありません。攻撃者が従業員のマシンへのアクセスを手に入れると、多くの場合は、その従業員に許可されている範囲の別の場所（「東西、すな

---

https://germanlawarchive.iuscomp.org/?p=692

https://transparencyreport.google.com/https/overview?hl=en

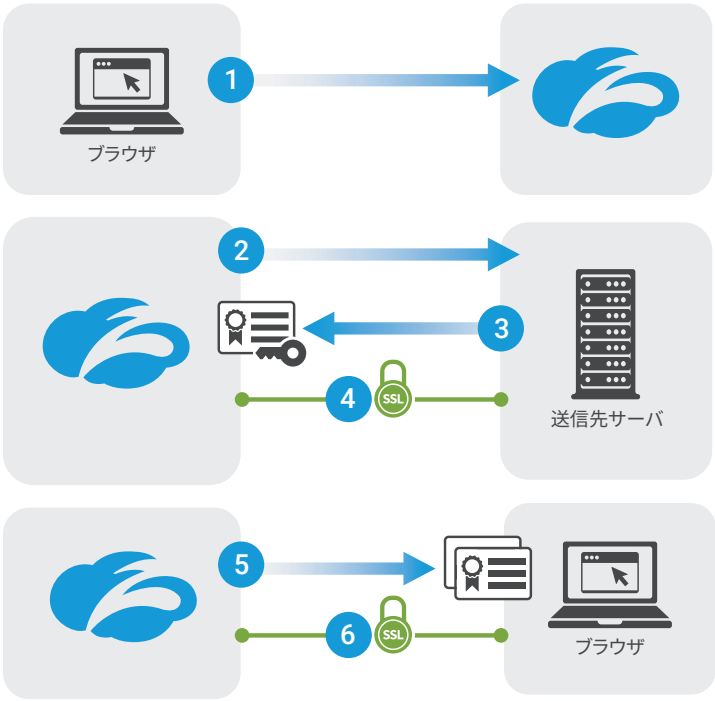
わち水平方向[12]）に移動できるようになるため、企業ネットワークの他のシステムやコンピュータに感染が拡大する恐れがあります。

サイバーセキュリティコントロールは、組織に出入りするオープンテキスト通信を簡単にインスペクションできますが、インバウンドやアウトバウンドデータの SSL/TLS 暗号化によって、インスペクションが複雑になります。暗号化された脅威が個々のユーザとより広範な企業の両方にこのような危険をもたらす現状で、セキュアトンネルのプライバシーを保護する手段はあるのでしょうか？

もちろん、その手段はあります。壊滅的な被害をもたらす、暗号化された脅威のリスクとの戦いは、SSL/TLS データのインスペクションから始まります。企業には、資産を保護するための制度上や法律上の義務があり、それには従業員のコミュニケーションの保護が含まれます。

SSL/TLS データをインスペクションするには、その信頼のコミュニケーションチェーンの行き先を変えて、ブラウザとインスペクションデバイスの間のトンネルと、さらには、インスペクションデバイスと送信先の間の後続のトンネルで、割り込みを発生させる必要があります。

ZscalerによるSSL/TLSで暗号化されたデータのインスペクションの方法 — ワークフロー



1. ユーザがブラウザを開いて、HTTPS要求を送信します。
2. Zscalerサービスが、HTTPS要求をインターセプトします。Zscalerサービスが、別のSSLトンネル経由で自らのHTTPS要求を送信先サーバに送信し、SSLネゴシエーションを実行します。
3. 送信先サーバが、証明書とその公開鍵をZscalerサービスに送信します。
4. Zscalerサービスと送信先サーバが、SSLハンドシェイクを完了します。アプリケーションデータと以降のメッセージは、SSLトンネル経由で送信されます。
5. Zscalerサービスが、ユーザのブラウザとSSLネゴシエーションを実行します。Zscalerサービスがブラウザに、Zscaler中間証明書または組織のカスタム中間ルートとZscaler中間CAによって署名されたサーバ証明書を送信します。ブラウザが、ブラウザの証明書ストア内の証明書チェーンを検証します。
6. Zscalerサービスとブラウザが、SSLハンドシェイクを完了します。アプリケーションデータと以降のメッセージは、SSLトンネル経由で送信されます。

ハンドシェイクが完了すると、*Zscaler*ポリシーエンジンが*SSL/TLS*ポリシールールを評価し、グローバルブロック/バイパスを適用し、信頼されていない発行元の証明書を検証し、通知を表示します（必要な場合）。

---

https://searchnetworking.techtarget.com/definition/east-west-traffic

図3. ZscalerによるSSL/TLSで暗号化されたデータのインスペクションのワークフロー。[13]

この例では、インスペクションによって個人とソースの間の信頼関係は失われません。従業員は、データソースではなく、ブラウズするデバイスを提供する組織を信頼し、インスペクションデバイスは、送信先とデータの内容を「参照」します。

ここで、暗号化、匿名性、プライバシーの中で、他の 2 つを尊重しつつ、この重要な保護機能を組織が実行できるのだろうかという疑問が生じます。 もちろん、適切かつ確実に実行する方法があります。暗号化されたマルウェアによってもたらされる脅威によって、SSL/TLS インスペクションが企業のサイバーセキュリティ管理に不可欠の要素となった今、組織は、セキュリティ要件と従業員のプライバシーをうまく両立させる必要があります。SSL/TLS トラフィックのインスペクションを実施しない組織は、PII の紛失、知的財産の盗難、産業スパイ、あるいはランサムウェア感染などの不要なリスクにさらされることになります（暗号化されたデータをインスペクションする組織の割合が増加し、約半数がヨーロッパに拠点を置く、Zscaler の企業顧客の 72%が、SSL/TLS トラフィックをインスペクションしています）。

個人の匿名性がオンラインで、ある程度は保証されます

SSL/TLS インスペクションモデルの評価にあたっては、最初に、匿名性に注目する必要があります。一部の組織では、従業員の職場での行動が規定によって管理されるのと同様、インターネットアクセスの提供が、従業員契約によって付与、管理され、規定によって確立され、管理される権利となっています。

規定の適用には、監視が必要です。SSL/TLS トンネルによって、ブラウザとサーバの間のあらゆるもの、あらゆる人に、その送信元と送信先が公開されることになり、これらのトランザクションのログは、挙動の分析とインシデントの検知に不可欠です。ログを検証することで、規定が順守されていることを確認し、規定の有効性を継続的に改善できます（ログ遡及分析は、犯罪捜査でもよく使われます）。

SSL/TLS インスペクションプロトコルが導入されている場合、インターネットアクセスは組織によって従業員に提供され、各従業員の雇用契約によって管理される特権であるため、従業員がオンラインでブラウズする際に完全な匿名性が保証されると期待するべきではありません。企業の資産を保護するため、ユーザがアクセスする URL、ブラウズ行動、およびデバイスアクセスを追跡することを組織が選択する可能性があります。会社規定によって、そのインターネット使用のガードレールが確立され、規定に違反した場合にどうなるかも明記されます。

SSL/TLS インスペクションは、オンラインでの個人の匿名性の終焉を意味するものではありません。企業は、プライバシーに対する従業員の要求と最新のサイバーセキュリティ対策を両立させることができます。有効な SSL/TLS インスペクションには包括的データ監視が必要ですが、そのインスペクションによって生じるデータへのアクセスは制限される可能性があります。必要になるまでの間は、調査や裁定（たとえば、潜在的なポリシー違反に対する検証と対応）の期間中であっても、ログ分析において従業員の匿名性を維持することができます。この匿名性は一般的に、ログのインデックス化または難読化と呼ばれるものです。

13 https://help.zscaler.com/zia/about-ssl-inspection

IT 管理者が、ログ全体にインスペクションし、分析する必要がある場合があります。たとえば、サイバーセキュリティの責任者は、定期的にログを確認することで、SSL/TLS トンネル経由のマルウェアコールバックを特定し、見つかった場合は、IT セキュリティ担当者がマシンクリーンアップのワークフローを開始し、従業員と協力して特定の感染デバイスからマルウェアを削除する（またはデバイスを初期化あるいは破壊する）必要があります。このプロセスは、「4 つの目[14]」アプローチと呼ばれるもので、セキュリティ管理者と従業員の代表者（たとえば、労働組合のリーダー、あるいはおそらくは外部の弁護士）の両方がコンソールログを一緒に検証するというものです。

ログによって感染が特定された場合は、個人である企業ユーザの匿名性を維持することはできず、「難読化を解除」してアイデンティティを明らかにする必要があります。

データの持ち出し — 組織からの望ましくないデータの「漏洩」も、難読化の解除が必要とされる可能性がある別の状況です。通常、ログレビュープロセスによって、以前のフィルタリングされていない SSL/TLS トラフィックが実際に犯罪者や未承認の送信先 Web サイトを送信先とするものである可能性があると判断できます。その場合は、法執行機関の関与と、捜査に協力するためのデータの難読化の解除が必要になることがあります。

従業員は、組織に対するリスクまたは脅威によってその匿名性の解除が必要になるまでの間、会社の同僚、上司、さらには企業のセキュリティチームに対して、自らのブラウズの匿名性が維持されると考えるべきでしょう。上記の状況では、多くの場合に従業員の雇用契約に組み込まれているはずである AUP（Acceptable Use Policy）により、難読化の解除について組織が文書化している必要あります。会社のデバイスまたはネットワークを利用したインターネットの使用は、従業員がこのことに（通常は雇用開始時に）同意した場合にのみ許可されます。

データの保護：GDPRが適用される環境でのSSL/TLS復号化

SSL/TLS 暗号化通信トンネルをデータインスペクションとポリシー適用のために「開く」と、表面上は、データがプライベートとは言えない状態になるように思えるため、企業の法務部やプライバシーを重視する多くの人が、その点を懸念事項として訴えます。GDPR をその拠り所として持ち出し、GDPR は組織に対し、SSL/TLS で暗号化された個人データの復号化やインスペクションを禁止していると指摘する人もいますが、我々はこれを正しくない意見だと考えます。

通常の暗号化されていないセッションでも、ブラウザとサーバの間のすべての当事者（ISP、ネットワークプロバイダ、キャッシュプロキシ）に対して、まったく同じ義務を適用しなければならなくなります。GDPR のガイドラインはそのような状況でも、各当事者が同じレベルの機密性で個人データを処理するよう求めています。暗号化によって、データコントローラ、さらにはデータプロセッサに課せられる義務が変わるわけではありません。誤った議論をさらに沈静化させるのであれば、個人データは、たとえば暗号化されたトンネルを利用する場合であっても、その従業員の会社が提供したデバイスで、暗号化されていない方法で処理されるのであって、その会社の論理で言えば、プライバシーの絶対的な確保というものは存在しないのです。

---

https://whatis.techtarget.com/definition/four-eyes-principle

SSL/TLS インスペクションを使用することで、ポリシーが適用され、暗号化されたデータトラフィックに潜む潜在的な脅威が特定されます。脅威を特定するため、インスペクションデバイスがデータを復号化し、一連の「既知の有害な」シグネチャと照合して検証し、データストリームをインスペクションすることで、マルウェアの侵入や企業データの不適切な持ち出しなどの脅威リスクを判断します。脅威がないと判断されたデータは、再パッケージ化されて送信されます。この方法で実行される SSL/TLS インスペクションによって、従業員のプライバシーが侵害されることはありません。データは誰にも共有されず、データの主体者の権利を侵害するような方法で使用されることもありません。この SSL/TLS インスペクションプロセスは、個々のプライバシー権を侵害することなく、組織の資産を攻撃の脅威から保護します。

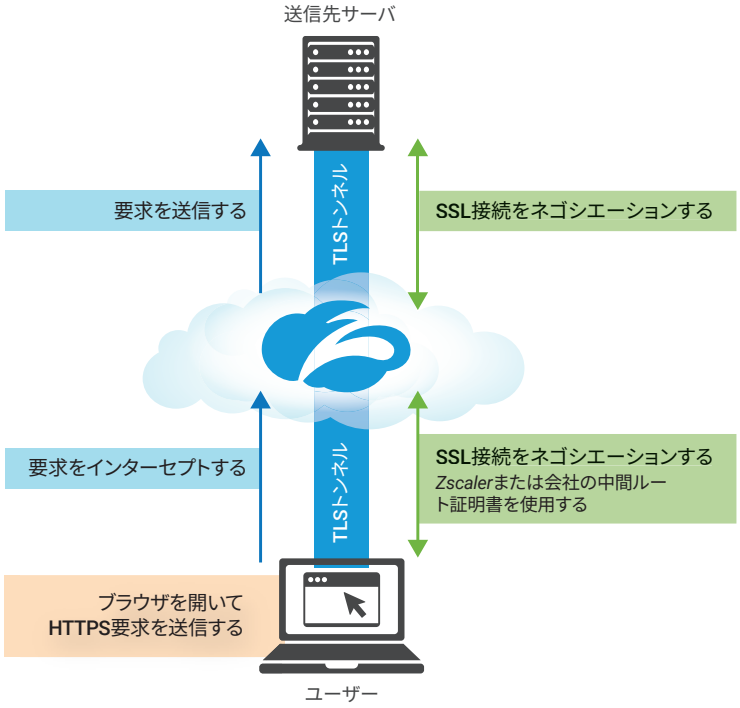
Zscaler は、包括的 SSL/TLS インスペクション機能を提供することで、お客様のデータトラフィックを保護し、PFS（Perfect Forward Secrecy）を提供します。[15]Zscaler がデータをディスクに保存することはありません：データインスペクションが完了すると、データフローはいかなる妨害を受けることもなく続行し、トランザクションそのもののログ以外の何らかのソースデータのレコードが保存されることはありません。Zscaler は、転送中のデータを保護するだけでなく、インスペクション時にすべての SSL/TLS キーを保護します（Zscaler による、SSL/TLS で暗号化されたデータのインスペクションの方法については、図 3 と 4 を、Zscaler による、SSL/TLS で暗号化されたすべてのデータとすべての暗号鍵の詳細については、こちらを参照してください）。[16])

---

https://www.zscaler.com/blogs/corporate/tls-13-busting-myths-and-debunking-fear-uncertainty-doubt

https://help.zscaler.com/zia/safeguarding-ssl-keys-and-data-collected-during-ssl-inspection

ZscalerによるSSL/TLSで暗号化されたデータのインスペクションの方法 — ワークフロー



Zscalerは、インラインSSLプロキシとして動作します。クライアントによって確立されたSSL接続を終了して、サーバへの新しいSSL接続を確立します。クライアントから見ると、Zscalerはサーバになり、元のSSLサーバから見ると、Zscalerはクライアントになります。

クラウドベースのZscaler SSL/TLSインスペクション:

- 優れたスケーラビリティにより、すべてのトラフィックのインスペクションが可能
- 証明書管理を簡素化
- ネットワーク管理を簡素化
- **AES/GCM/ECDHE**暗号化で**PFS**のトラフィックを保護
- 有効なポリシーコントロールを適用
- ユーザデータの安全性を保証(一時的に保存され、クラウドに保存されることはない)

図4. ZscalerによるSSL/TLSで暗号化されたデータのインスペクションのインラインプロキシモデルの方法。[17]

重要なのは、結果としてのプライバシーの権利に注目し、その結果が達成される方法を検証することであり、その結果に影響を与えると思える個々の手順の明確化が重要なわけではありません。トラフィックのインスペクションと、ブロックするか否かの二者択一の結果は、暗号化されたデータへのアクセス、監視、または保存と同じではありません。

包括的 SSL/TLS インスペクションは、組織、組織の従業員、および組織の資産のプライバシー保護に役立つため、GDPR や全体的なプライバシーのコンプライアンスが強化されます。SSL/TLS インスペクションがなければ、内部の個人データ /PII が外部に公開されてしまうリスクが高くなり、コンプライアンス違反の重大なリスクにさらされることになります。

https://help.zscaler.com/zia/about-ssl-inspection

データ保護の法規制によるプライバシーとセキュリティのサポート

データプライバシーの法規制、その中でも、EU の GDPR、[18] イギリスの NIS（Network and Information Systems Regulation 2018）[19]、TKG[20] などが、個人データを組織が保護し、それと同時にインターネットへの自由かつ公正なアクセスを保証する目的で制定されました。これらの法規制は、個人の権利を守ると同時に、システムやデータを保護するために企業にセキュリティ対策の実施を課すものであり、たとえば、TKG は組織に対し、「技術的な保護対策[21]」によって、データの損失と外部からの攻撃を防ぐよう義務付けています。また、NIS には、システム（およびシステム内のデータ）の侵害を防ぐための適切なセキュリティ対策を組織は実施する必要があると明記されています。そして、GDPR の第 5 条[22] には、これらの組織は、

> 個人データの適切なセキュリティが保証される方法でデータを処理する必要があると明記されており、これには、技術的または組織的に適切な手段による、無許可または違法な処理や偶発的な損失、破壊、または損傷からの保護が含まれます。

さらには、GDPR 32 条（処理のセキュリティ）は組織に対し、個人データの処理にあたっては、「リスクに適したレベルのセキュリティを確保できる」セキュリティ対策を実装するよう義務付けています。軽減を目的とするセキュリティリスクの重要性を考慮すると、SSL/TLS インスペクションは非常に「適した」方法です。

脅威は、暗号化されたトラフィックにも潜んでいます。インスペクションなしでは、SSL/TLS で暗号化されたデータが「無害」あるいは「有害」のどちらであるかを判断する方法がありません。暗号化されたデータトラフィックを包括的なインスペクションがなければ、TKG、NIS、GDPR のプライバシーとセキュリティの両方の要件を満足することはできず、従業員と会社の利益を守ることはできません。

要点：SSL/TLSインスペクションの実装方法

セキュリティとデータ保護において SSL/TLS インスペクションが有効であることについては、議論の余地がありません。IT リーダーは、SSL/TLS インスペクションを導入して、組織のデータ、従業員、資産を保護する必要があり、導入しないと、取り返しのつかない損害が発生する可能性があり、職務怠慢と判断される恐れもあります。

---

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-gdpr/

http://www.legislation.gov.uk/uksi/2018/506/contents

https://germanlawarchive.iuscomp.org/?p=692

https://germanlawarchive.iuscomp.org/?p=692#87

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e1807-1-1

SSL/TLSインスペクションを組織に導入するIT管理者は、いくつかの重要事項を考慮する必要があります。

1. 従業員に通知します。

- 有効な AUP が存在し、そのポリシーがプロキシ / コンテンツフィルタで適用されていることを確認します。
- 一般的には、雇用契約を通じて、全従業員が AUP に明示的に同意していることを確認します。
- 何が個人データに相当するのか、また、組織がそれらのデータをどれ位の期間保存するのかを、従業員が理解しておくようにします。
- 従業員に対し、インスペクションの対象となるのがどのデータであるかを正しく伝えることで、会社のリソースを使用する際に、正しい情報に基づいて判断できるようにします。
- 労働者評議会や労働組合からの合意と支援を得て、SSL/TLS インスペクションが従業員の利益にもなることを実証します。
- 具体的に何をどのように行うのかを周知します。

2. 法的根拠に基づき、GDPR の下にデータを処理します。ここでの法規制は敵ではありません。企業が NIS などの対象となる場合、その法的根拠は「法的義務」となります。また、前述のように、企業には、組織とその資産の保護にあたって「正当な利益」があります。

3 社内のチームまたは外部の専門家から、法律およびプライバシーに関する助言を求めますが、論点を整理しておく必要があります。 たとえば、弁護士やプライバシーの専門家が、ベンダが提供するサービスを完全に理解していないなかったり、セキュリティ対策がリスクに適しているかどうかを判断するための技術的観点を持ち合わせていなかったりする場合があります。

4. プロセスとコントロールが有効かつ適切であることを確認します。

- データを難読化するか、一般ユーザに表示されないようにし、「知る必要がある」場合にのみ利用できるようにします。
- 個人データをレビューするための厳密で文書化されたプロセスがあることを確認します。
- このワークフローを定期的に見直し、適用します。
- データを決められた期間保存し、その期間が過ぎたら削除します。
- データの保存期間中は、データの安全性が確保されるようにします。

SSL/TLSインスペクション：法規制のコンプライアンスを保証する正しい方法

SSL/TLS インスペクションは、企業、企業の従業員、および企業の資産のプライバシーを保護するための「適切なセキュリティ対策」となります。SSL/TLS インスペクションは、組織を攻撃の脅威から保護すると同時に、個人のプライバシー権とうまく両立させ、結果として、組織の法規制のコンプライアンスを強化することにもなります。

暗号化された脅威は、現実のものであり、破壊力と有害性があり、（指数関数的に）増加し続けています。トラフィックを復号化しないことを選択した企業の IT リーダーは、ユーザのプライバシーと企業の資産の両方を危険にさらすだけでなく、データ保護のさまざまな法規制へのコンプライアンス違反のリスクを犯すことにもなります。現代社会においては、IT リーダーが SSL/TLS インスペクションを導入することで、企業のセキュリティリスクと戦い、従業員とユーザのプライバシーを保護する必要があります。

ゼットスケーラーについて

ゼットスケーラーは2008年に、「アプリケーションがクラウドに移行されるなら、セキュリティもクラウドに移行する必要がある」という、シンプルではあるものの力強い概念に基づき、設立されました。Zscalerは現在、世界中の数千の組織のクラウド対応の運用への移行を支援しています。