CLOUDFLARE®

SaaSプロバイダーサバイバルガイド

パフォーマンス、セキュリティ、暗号化 -- オンラインアプリケーションの最重要課題

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

概要

2020年のSaaS市場は、2016年比で196%増加すると予想されています。[1] SaaS市場が拡大し続け、企業の経営基盤における重要な構成要素となっている中、セキュリティやパフォーマンスはSaaSプロバイダーとその顧客の両者にとっての最重要課題であり続けます。市場の成長が続く限り、最高の安全性とパフォーマンスでアプリケーションを顧客に提供するSaaSプロバイダーの競争は激化する一方です。効率の低いアプリケーションや攻撃に対する脆弱性があると、収益性、エンドユーザーのエンゲージメント、ブランドの評判などへの悪影響は避けられず、顧客離れを引き起こします。SaaSプロバイダーの重要な部分を占める企業は、ブランド名を含む個人名のドメイン（バニティドメイン）を暗号化する必要がありますが、それにはSSLのライフサイクルを通じて手動管理しなければならず、展開の所要時間が長くなり間接費も必要になります。その代わりに複雑な自動ソリューションを社内で構築する場合は、その業務にエンジニアの労力が必要となり、中核技術に注力できなくなります。

Cloudflareが提供するSaaSプロバイダー向けのパフォーマンスとセキュリティソリューションは、SaaSプロバイダー、エンドカスタマー、エンドビジターの利用体験を保護・促進します。Cloudflareがグローバルに10 Tbpsで配信するコンテンツデリバリーネットワーク（CDN）をArgoのスマートルーティング、負荷分散、パフォーマンスの最適化と組み合わせることで、サイト訪問者のレイテンシーが最大で2倍軽減します。Cloudflareの高度なDDoS攻撃対策は、Rate LimitngとWebアプリケーションファイアウォール（WAF）とを組み合わせて、ネットワーク層、トランスポート層、アプリケーション層をターゲットとする大規模な帯域幅消費型攻撃と複雑な攻撃の両方を軽減します。さらに、SaaSプロバイダーは、カスタムバニティドメインに簡単に実装できて完全に管理されるSSLソリューションによって顧客データの転送を保護できます。

レイテンシーと不適切なセキュリティによるビジネスの悪影響

SaaSアプリケーションのレイテンシーや不適切なセキュリティは、どのような形であっても、カスタマー利用体験、コンバージョン率、検索エンジンランキングが低下する結果となり、減収や顧客離れを引き起こします。

パフォーマンスと可用性はSaaSアプリケーションのエンゲージメントにも影響

Webサイト、アプリケーション、APIを利用する顧客にとっては高速でしかも高可用であることが重要です。オンライン資産の利用時にレイテンシーが発生したり利用できない状況になるとSaaSアプリケーションのエンゲージメントやコンバージョン率は目に見えて低下します。

たとえば、Googleの報告では、サイトのレイテンシーが100～400ミリ秒増えるだけで顧客行動で目に見えた影響があるとされています[1]。また、Walmartではサイトの読み込み時間がほんの数秒長くなっただけでコンバージョン率が大きく減少したことが分かっています[2]。Amazonでもサイトでのレイテンシーが100ミリ秒短縮されるたびに1%の増収につながることが明らかになっています。[3]

SaaSアプリケーションが抱えるパフォーマンス上の一般的な問題は内的な要因に関するものです。これはSaaSプロバイダーが共用ホスティングするインフラストラクチャまたはアプリケーションの設定にマイナスに働きます。このような要因の1つがサイト訪問者と元のSaaSアプリケーションの場所との地理的な距離です。距離が100マイル増えるたびに0.82ミリ秒のレイテンシーが推定されます[4]。大量の最適化されていない静的コンテンツを遠距離から利用する訪問者のレイテンシーはさらに長くなります。

ただし、サーバー、ネットワーク、アプリケーションだけでパフォーマンスが決まるわけではありません。トラフィックの急増や季節的な影響が共用インフラストラクチャの負担となってアプリケーションのレイテンシーを発生させたり、まったく利用できなくなる場合もあります。

読み込み時間が遅かったり利用できなくなると、収益性、コンバージョン率、直帰率、検索エンジン（SEO）ランキング、ブランドの評判、顧客満足度、サービルレベルアグリーメント（SLA）でSaaSアプリケーションへの悪影響が非常に大きくなります。

[1] http://www.sfgate.com/business/article/Google-s-speed-need-instantaneous-Internet-3251049.php
[2] https://www.slideshare.net/devonauerswald/walmart-pagespeedslide
[3] https://blog.gigaspaces.com/amazon-found-every-100ms-of-latency-cost-them-1-in-sales/
[4] http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/

SaaSアプリケーションをターゲットにした攻撃の影響

常時オンラインのアプリケーションにおけるセキュリティ上の影響は、それが市場参入を試みる新興のSaaSプロバイダーであれ、以前はローカルのアプリケーションをクラウドに移行しようとしている定評あるソフトウェア企業であれ、見過ごすことはできません。

SaaSアプリケーションやサービスにとって、攻撃の対象となり得る領域は公開のインターネットに接する部分が増えるほど拡大し、多くの場合で共用インフラストラクチャを通じてワークロードにも広がります。SaaSプロバイダーにとっての攻撃ベクトル（攻撃元区分）には、ログインポータル、共用DNS/ホスティング、複雑なアプリケーションの脆弱性などがあります。多くのSaaSプロバイダーは複数のクライアントアプリケーションを共用インフラストラクチャでホスティングするため、この共用インフラストラクチャでデータ漏洩、信頼性インシデント、攻撃があれば他の顧客にも悪影響が及ぶおそれがあります。

上記のターゲットがベクトルとなる特定の攻撃には、帯域幅消費型攻撃、複雑なDDoS攻撃、ブルートフォースログイン試行、アプリケーションの脆弱性の悪用、および、暗号化されていない顧客データの傍受などがあり、これらはすべて、さまざまなデバイスを通じてWebサイト、アプリケーション、APIをターゲットにします。継続的な攻撃の成功によって被るビジネス上の影響は、サービスの提供不能から、ブランド力の低下、顧客離れ、大幅な減収、ダメージ修復による犠牲までさまざまです。

2013年にAdobeに侵入したハッカー集団は、290万人の顧客のクレジットカード情報や他の個人情報を盗み出しました。[5] Adobeの情報セキュリティ最高責任者のBrad Arkinは「今日の企業にとってサイバー攻撃は不運な現実」と言及してオンラインビジネスのリスクを認めています。

2016年10月16日、Airbnb、Amazon.com、Netflix、The New York Times、Paypal、Pinterest、Reddit、Tumblr、Twitter、 Verizon、Visa、The Wall Street Journal、Yelp、Zillowと他の多くの企業はすべて悪名高いMiraiボットネット攻撃により長時間にわたり業務が停止しました。直接のターゲットにアプリケーション自体は含まれていませんでしたが、これらのWebサイトやアプリケーションを共用するDNSサービスプロバイダーのDynは攻撃されました。Dynがこのインシデントを解決して影響を受けたすべてのWebサイトのサービスを復旧させることができたのは11時間後でした。[6]

暗号化か、カスタムバニティドメインかの選択

オンライン事業者にとって、SSL／TLS暗号化を採用することは従来セキュリティ上のベストプラクティスでしたが、より安全なインターネットの構築を目指す大手テクノロジー企業からの圧力によって、これが必須要件となりつつあります。たとえばGoogle Chrome Webブラウザーでは、2016年末より、HTTPSを使用しないWebサイトをユーザーにとって「安全でない」と明示するようになりました。[7] また、現在 Appleでは、すべてのiOSアプリケーションに対して、アプリストアに送信する前にHTTPS接続の利用を求めています。[8]

SSLの初期、オンライン事業者は、HTTPS経由のトラフィックを暗号化するか、パフォーマンス上の期待に応える訪問者エクスペリエンスを提供するかを選ぶ必要がありました。数年前までは、SSLプロトコルが原因でレイテンシーが増え、Webサイトとアプリケーションのパフォーマンスが損なわれていました。また、事業者がセキュリティの向上よりもパフォーマンスを優先したとしても、当時存在していたSSL実装の運用上の課題によって汎用が妨げられていました。HTTP/2（HTTP 1.1の後継）の開発など、近年のSSLの改良により、SSLを使ったHTTPS経由のトラフィック保護が、非暗号化HTTPのパフォーマンスを上回るようになっています。

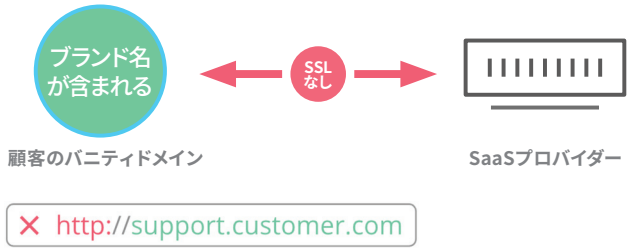
過去に事業者が暗号化とパフォーマンスのどちらかを選ぶ必要があったように、今日のSaaSプロバイダーの主要サブセット企業にも、顧客のトラフィックを暗号化するか、独自のブランド名を持つバニティドメインを顧客が使用できるようにするか、という選択が求められます。適切なブランドの提示、セキュリティ、検索エンジンのランキング、可用性の最大化などの利点を組み合わせるためには、どちらも欠かせません。

[5] http://www.nytimes.com/2013/10/04/technology/adobe-announces-security-breach.html
[6] http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
[7] https://techcrunch.com/2016/06/14/apple-will-require-https-connections-for-ios-apps-by-the-end-of-2016/
[8] https://techcrunch.com/2016/06/14/apple-will-require-https-connections-for-ios-apps-by-the-end-of-2016/

このようなSaaSプロバイダーの多くは、通常、ランディングページ、Webサイト、サポートポータルなど、一般に公開されるオンライン資産の作成を顧客に許可しています。一般に、SaaSプロバイダーは、自社のプライマリドメインのサブドメインで新しく作成されたこれらの顧客の資産をホスティングします。たとえば、SaaSプロバイダーの顧客が作成する資産のURLは**customercompany.com**や**support.customercompany.com**などのブランド名を含むバニティURLではなく、**customercompany.saasprovider.com**のようになる場合があります。ブランド名を含むバニティドメインがないとSEOランキングが低下し、ブランドの認識度や訪問者の信頼を失うため、顧客にとってこれは問題です。

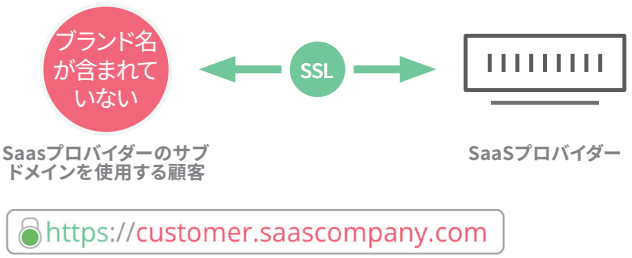
SaaSプロバイダーと顧客は、customercompany.comまたはsupport.customercompany.comなどのURLにCNAMEを設定してcustomercompany.saasprovider.comとすることでドメインのブランディング問題を解決しています。顧客はこのようにしてブランド名が含まれた独自のバニティドメインを使用できますが、SaaSプロバイダーは簡単にはSSLを有効化できなくなり、SSLのライフサイクル全体のプロセス管理が困難になります。SSLのライフサイクルプロセスを手動で管理したり、社内でエンドカスタマー向けのソリューション構築を試みると、所要時間や手作業が増えてコストもかかります。

SaaSプロバイダーが上記の課題に取り組む場合のシナリオには次の3つがあります。



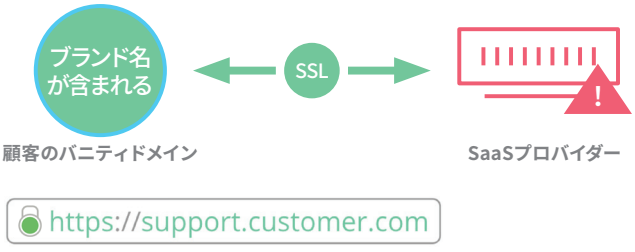
暗号化未対応でブランド名が含まれるバニティドメイン

SSLを使用しないカスタムバニティドメインは、SSLによるパフォーマンスの利点がなく安全にデータを転送できません。のぞき見に対して脆弱なために訪問者が閲覧する前にコンテンツが編集されたりインジェクション攻撃を受けるおそれがあります。



暗号化に対応済みでブランド名が含まれないドメイン

SaaSプロバイダーを通じてSSLに対応済みでカスタムバニティドメインでないドメインは結果的にブランド力やSEOランキングが低くなります。

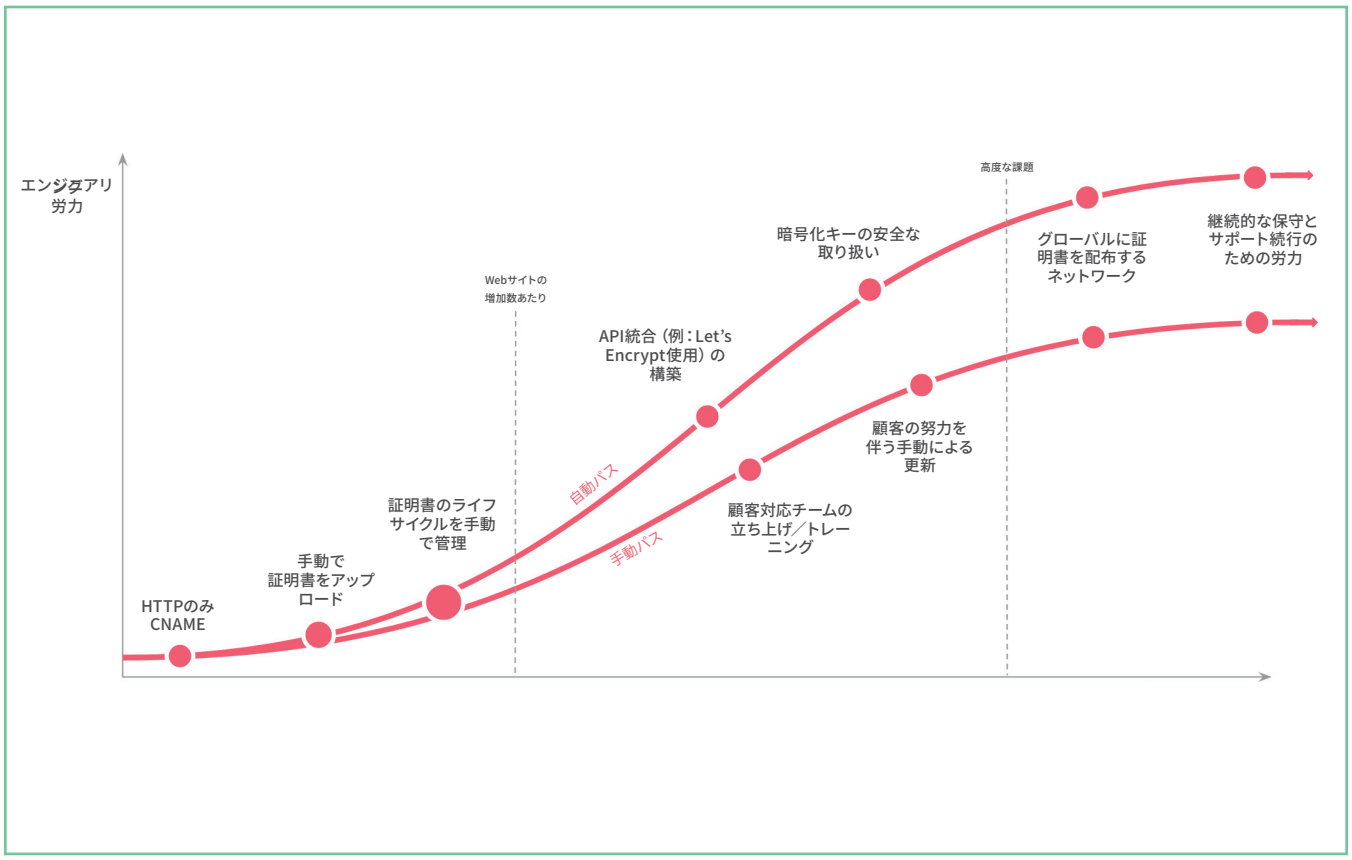


困難な社内での対応

暗号化したうででブランド名を含むドメインを希望するSaaSプロバイダーはSSLのライフサイクルを手動で管理することができますが、展開期間が長期に及んで間接費がかかるか、複雑な自動ソリューションを社内で構築する結果になります。

重要な点は、SaaSプロバイダーが顧客のドメインをSSLで管理するために自社でソリューションを構築するときに直面する技術的な課題です。以下の図は、SSLの自動ソリューションを社内で構築しようとしたSaaSプロバイダーがたどる典型的なロードマップを示したものです。

社内でのソリューション構築で採用可能な2通りのパスがありますが、どちらも理想的ではありません。最初（上部）のパスはSSLプロセスを自動化しますが、大規模なエンジニアリングが必要で、数々の複雑な課題も伴います。2番目のパスは、SaaSプロバイダーと顧客の両方が相応の作業を手動で行う必要があります。



SaaSアプリケーションのセキュリティ、パフォーマンス、可用性のためのCloudflare

Cloudflareは、レイテンシーを減らしてコンテンツ配信を最適化するだけでなく、これらのメリットをエンドカスタマーのインターネット資産にまで拡大することで、SaaSプロバイダーのWebサイト、アプリケーション、APIを使用するエンドユーザーの体験を改善します。

可用性がグルーバルに拡大

Cloudflareの中核的なソリューションは、グローバルなエニーキャストを利用したコンテンツデリバリーネットワーク（CDN）です。世界57か国117+5か所を拠点とするデータセンターから配信され、すべての地域でサイト訪問者の最寄りの場所にSaaSアプリケーションのコンテンツを誘導します。また、Cloudflareがサービスを提供するマネージドDNSドメインの38%で世界で最も信頼性の高いDNSネットワークが稼働しています。平均クエリ速度が数ミリ秒のCloudflareは、すべてのマネージドDNSプロバイダーで最速のグローバルパフォーマンスを誇ります。

アプリケーションの可用性が大幅に拡大

Cloudflareの可用性の高いDNSインフラストラクチャーとグローバルなAnycast™ネットワークをさらに強化したCloudflareのLoad Balancingは、複数のサーバーにトラフィックを振り分けて地理的に最も近い場所にトラフィックをルーティングすることによってレイテンシーを軽減します。Load Balancingには、高速フェイルオーバーを備えた正常性チェックが含まれており、訪問者に障害が発生しないように迅速にルーティングします。加えて、Load Balancingは複数のクラウドプロバイダーやオンプレミスのインフラストラクチャで使用できるため、単一のプロバイダーやサーバーによる障害の影響を軽減でき、クラウドのベンダーロックインも回避できます。

訪問者の体験を高速化

CloudflareのCDNは、HTML、CSS、JavaScriptの自動縮小やGzip圧縮などの高度な最適化技術に基づいて構築され、ファイルやリソースのサイズが20%以上縮小されます。これに加えて専用の画像やモバイルの最適化でSaaSアプリケーションのパフォーマンスがさらに向上します。

Cloudflareは世界中のインターネットトラフィックの10%以上を配信しながらネットワークパスの実際の使用状況と信頼性をリアルタイムで分析します。CloudflareのスマートなルーティングアルゴリズムであるArgoは、収集された情報を基に利用可能な最速のパスでトラフィックをルーティングします。同時にオープンで安全な接続を維持することで接続設定時のレイテンシーを軽減します。Argoのスマートルーティングにより、インターネットの平均レイテンシーはさらに35%軽減し、接続エラーは27%少なくなります。

「Cloudflareの提供により、Crispのサービス品質は非常に高く、サービス応答時間は非常に短くなりました。この提供は、高価なネットワークインフラストラクチャを大衆向けにコモディティ化したものです。これがなくては私たちのビジネスは立ち行かないでしょう」

crisp™

Valérian Saliou氏
Crisp最高技術責任者

SaaSアプリケーションと顧客データの保護

Cloudflareのクラウドベースのセキュリティソリューションは、SaaSプロバイダーのWebサイト、アプリケーション、APIを保護し、エンドカスタマーのインターネット資産にまでそのメリットをもたらします。

117か所を超えるCloudflareデータセンターのエニーキャストネットワークは、史上最大のDDoS攻撃の10倍に相当する10 Tbpsのスループットを備え、OSIモデルの3、4、7層をターゲットにした攻撃から保護します。Rate LimitingとWebアプリケーションファイアウォール（WAF）を組み合わせれば、Cloudflareのセキュリティソリューションで、アプリケーション層をターゲットにした複雑な攻撃も軽減できます。また、CloudflareのSSL for SaaSを利用すれば、Saasプロバイダーとエンドカスタマーは、通信の暗号化によってデータ傍受と悪意のあるコンテンツのインジェクションを防ぎながら、カスタムバニティドメインの使用を続けることができます。

顧客の機密データの保護と安全を確保

SaaSアプリケーションに保存される個人／企業の機密データ増加に伴い、総当たりログイン試行、データ漏洩、中間者攻撃に対する保護が非常に重要になります。

こうした種類の攻撃に対する保護としてまずCloudflareのWebアプリケーションファイアウォール（WAF）を使用すれば、アプリケーション層をターゲットとした複雑な攻撃を軽減できます。CloudflareのWAFは、OWASPの上位10種類の脆弱性に対する保護、一般的な統合と言語（PHP、Magento、WordPress、Drupal、Atlassianなど）をターゲットとしたアプリケーション固有の脆弱性に対する保護をデフォルトで提供します。CloudflareのWAFにより、SaaSプロバイダーは、新たに検出された攻撃ベクトルと脆弱性に対処するためのカスタムルールセットをすばやく作成し、30秒以内にCloudflareネットワーク全体にルールを適用できます。

Rate LimitingをCloudflareのDDoS攻撃対策と併用することで、不審なリクエストレートの訪問者をブロックするための微細なコントロールが可能になります。Rate Limitingには、アプリケーションやWebサイト内の権限のない領域にアクセスを試みる総当たりログイン試行の軽減機能が装備されており、一定時間内に特定のIPアドレスから特定のエンドポイントに送信されるリクエスト数を制限します。

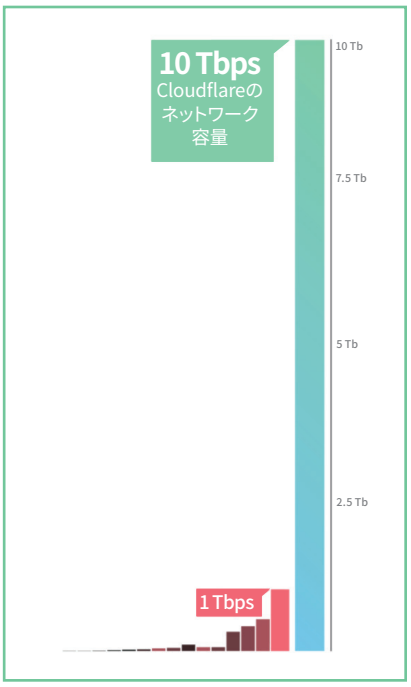
「Cloudflareのソリューションはとにかく効果的です。担当チームはこちらの要求をすべてかなえてくれただけでなく、カスタマイズをほぼ瞬時に適用してくれました」

zendesk | **Amanda Kleha氏**
Zedeskオンライン事業部長

CloudflareのSSL for SaaSは、中間者攻撃によるデータの傍受や、暗号化されていない接続でのトラフィックののぞき見などから確実に保護しながら、カスタムCNAMEを設定したバニティドメインのSSL／TLS証明書を自動管理する最も効率的な方法を提供します。

悪意あるトラフィックをブロックして可用性を確保

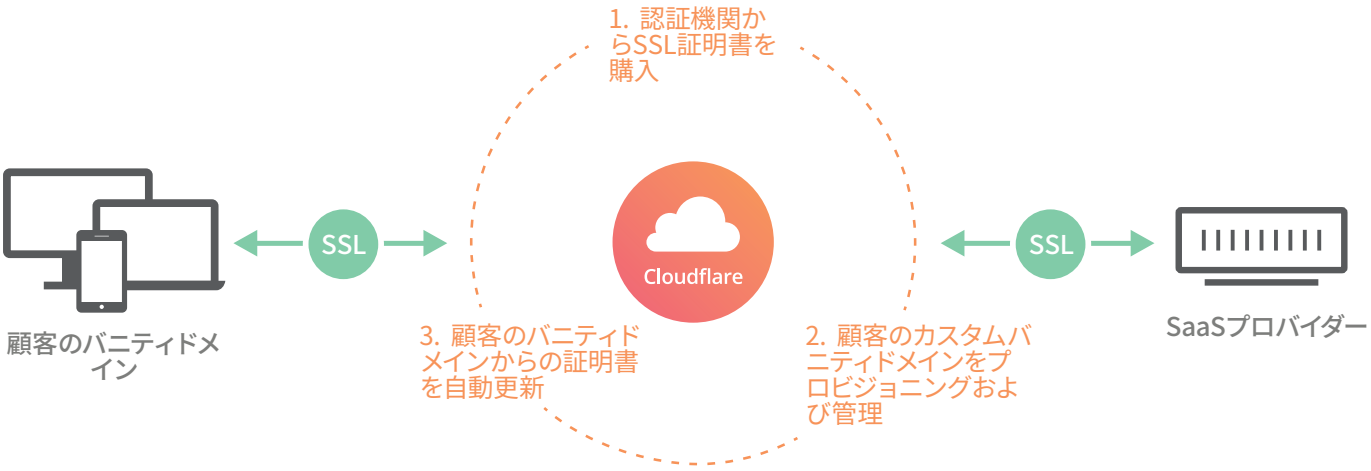
顧客の機密データの盗難や損失は多大な損害を引き起こすだけでなく、攻撃が成功して妨害されたサービス提供の被害者になった場合、影響は深刻です。Cloudflareの主軸とも言えるサービスは、世界57か国117か所以上のデータセンターが拠点のグローバルなコンテンツデリバリーネットワーク（CDN）です。Cloudflareのネットワークスループットを合計すると10 Tbpsを超えます。これは、歴代最大のDDoS攻撃のおよそ10倍に相当します。3、4、7層をターゲットに試行されるあらゆる大量のDDoS攻撃は、吸収されてCloudflareのネットワークに均等に分散されます。このためSaaSの顧客にダウンタイムが発生することはなく最大限の可用性が確保されます。CloudflareのRate Limitingソリューションを DDoS攻撃対策と組み合わせると微細な制御が可能になり、疑わしい要求をする訪問者をブロックします。特定のIPが定義済みのしきい値を超過するとブロックされ、割り当てられた一定期間は特定のエンドポイントに対する要求を送信できなくなります。



SaaSプロバイダー向けの自動SSLソリューション

SaaSプロバイダーは、Cloudflareネットワークのセキュリティやパフォーマンス上のメリットをSSL for SaaSで拡大してエンドカスタマーに提供することでエンドカスタマーは独自のカスタムバニティドメインを使用できます。CloudflareのSSL for SaaSソリューションにより、 顧客はSaaSプロバイダーのサブドメインに自身のバニティドメインのCNAMEを

引き続き設定できます。これで顧客はブランド名が含まれるURLのメリットが得られ、CloudflareはSaaSプロバイダーとその顧客のSSLライフサイクル全体を有効化して管理できます。顧客ドメインではSSLが有効になって訪問者の信頼性が高まり、SEOの検索ランキングが上昇します。さらに最新のHTTP/2プロトコル対応となることから結果的に通信速度が大きく改善します。



ブランド名の含まれる訪問者の体験

自身のカスタムブランド化したバニティドメインを使用できるSaaSプロバイダーの顧客は引き続きこのドメインを利用できるだけでなく、完全に管理されるSSL証明書のメリットも追加されます。カスタムのCNAMEを設定したバニティドメインを使用するSaaSの顧客は、ブランド認知が高まるためSEOランキングが上昇し、Webサイト訪問者やアプリケーション利用者からの高い信頼も維持できます。

顧客資産の安全性とパフォーマンスを確保

SSL for SaaSは、CNAMEを設定したカスタムバニティドメインに専用のSSL／TLS証明書をシームレスに追加する機能を提供します。HTTPSによるデータ通信では、中間者攻撃やネットワークののぞき見を防ぐことができるため顧客の機密データを安全に転送できます。SSLの有効化により、通信速度がさらに高速化されるHTTP/2プロトコルの普及が進んでいます。

ライフサイクルの自動管理とSSLの迅速な展開

Cloudflareは、SaaSプロバイダーが提供するCNAMEを設定した顧客のバニティドメインのSSLについて、プライベートキーの発行や保護から、ドメインの検証／発行／再発行にいたるまで、そのライフサイクル全体を通じて管理します。SaaSプロバイダーとエンドカスタマーの両者ともSSLのライフサイクルを管理する負担が不要になります。SSL発行のプロセス中にCloudflareから新しい認証要求が転送され、数分以内にHTTPSが使用可能になります。

「Cloudflareとのビジネスには、エンジニアとしてこれ以上ないほど満足しています」

UDACITY

Paul Bauer氏
Udacity社プラットフォームエンジニア

要点

Cloudflareにご登録いただくと、SaaSアプリケーションのパフォーマンスとセキュリティが改善されるだけでなく、CNAME設定済みのエンドカスタマーのバニティURLで簡単にSSLが利用できるようになります。設定は簡単で、実装にかかる時間は通常5分以内です。www.cloudflare.com/plans/ではFreeプランからEnterpriseプランまで各種プランをご用意しています。SaaSプロバイダー様向けCloudflareの詳細については、www.cloudflare.com/saas/をご覧ください。

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com