CLOUDFLARE

ホワイトペーパー

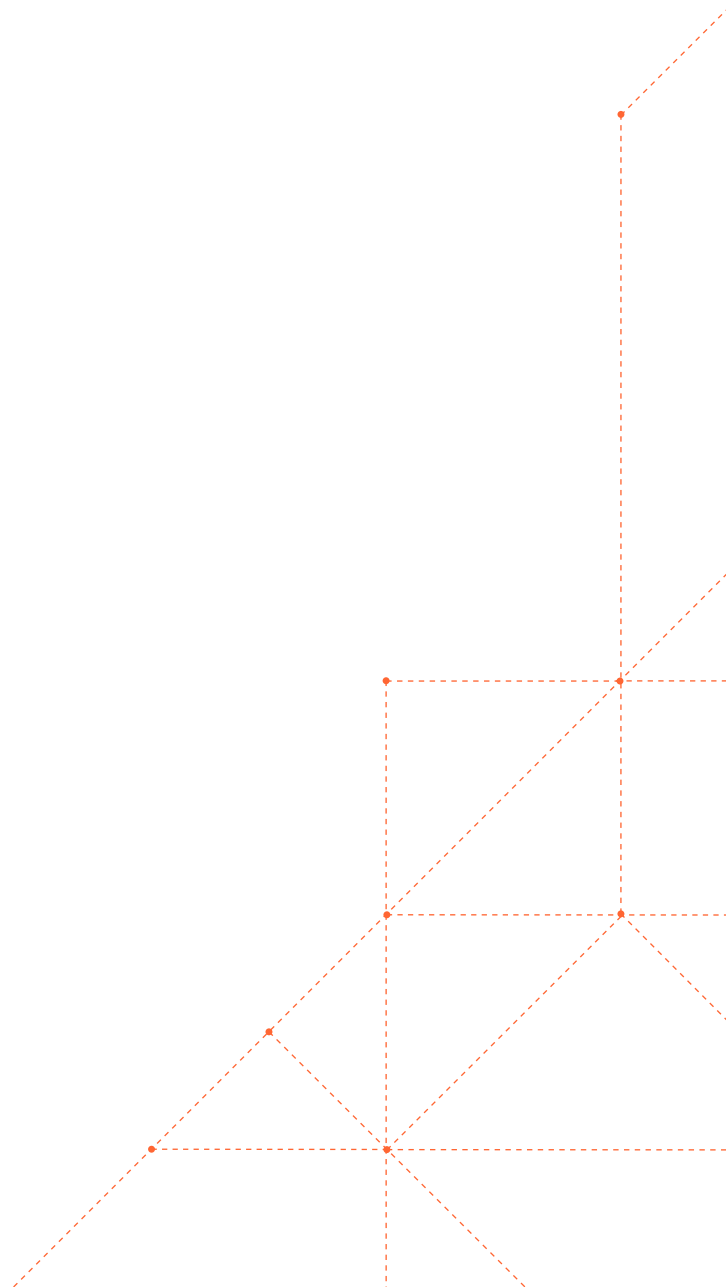
最小で最大を成す

費用対効果の高いアプリケーション セキュリティとパフォーマンスの 戦略 - 7社の実例

概要

悪性ボット、DDoS攻撃、コードインジェクション、その他の脆弱性からWebアプリケーションとAPIを保護することは、企業にとって重要な任務です。しかし、堅牢なセキュリティ戦略の実装が難しい場合があります。予算の制約やチームメンバー増員の限界がある場合は特にそうです。

本書では、アプリケーションセキュリティ戦略の効率化とコスト削減に成功した企業の実例をご紹介します。それらのサクセスストーリーから学ぶことによって、企業はアプリケーションセキュリティの実践による経費効率化について貴重な知見を得ることができます。



セキュリティ・ITチームが限られたリソースで多くをなしとげなければならない時

企業の予算に制約がある時は、どのチームもその影響を受けないわけにはいきません。経済全般の不確実性、売上減少、組織改編、その他のさまざまな理由で、セキュリティチームとITチームは予算増額の希望は叶えられずに業務改善を強いられることがよくあります。それどころか、コスト削減を同時に実現せよと言われることさえあります。

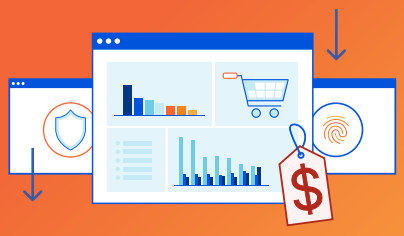
しかし、アプリケーションのセキュリティとパフォーマンスは、成果の妥協が許されない分野です。セキュリティに関しては、アプリケーションの保護が年々複雑化する一方です。攻撃は大型化と複雑化がこれまで以上に進んでいますし、組織の成長に伴って攻撃対象領域が拡大しています。ある推定（共通脆弱性識別子（CVE）プログラム）では、2022年に新たに確認された脆弱性が前年比25%増の総数2万5059件であったと報告しています。

一方、パフォーマンスに関しては、消費者があらゆるデジタル体験に速さ、信頼性、パーソナライゼーションを期待しています。少しでも遅くなるとユーザーエンゲージメントとコンバージョンに多大な影響をもたらし、顧客の期待に応えられない企業は見放されてしまいます。

予算の制約と期待の高まりという2つの圧力に挟まれたセキュリティチームとITチームは、少ないリソースで多くの成果を出す方法を見つける必要があります。本書では、成果を犠牲にすることなく費用対効果の高いセキュリティとパフォーマンスを効率よく確立した企業の実例をご紹介します。

アプリケーションセキュリティの実践におけるコスト削減の方法

WebアプリケーションとAPIを最新の脅威から守る上で最善の防御策とは、多層セキュリティサービスを提供するだけでなく、無駄な経費をカットできるものです。それを実現するため、企業はベンダーの統合、証明書管理の合理化、トラフィックコストの増大につながる攻撃に絞った保護、転送料金の削減など、いくつかの重要戦略を用いることができます。



セキュリティベンダーの統合によるコスト削減

証明書管理の自動化により人件費とインフラ費用を合理化

トラフィックコスト増大につながる攻撃をブロック

帯域幅やクラウドの使用料、転送料金など予想外の料金やコストを排除

セキュリティベンダーの統合によるコスト削減

Gartnerの最近の調査によれば、企業の75%がセキュリティ対策のベンダー統合を検討しているといいます。依存するベンダーの数を絞ることによって、企業はサプライチェーンプロセスを最適化して効率化を達成でき、それがコスト削減につながります。

高級時計のオンラインマーケットプレイスChrono24は、Cloudflareとの統合により複数ベンダーへの依存を減らしました。

Chrono24は、以前はEdgeCastのCDNソリューションと他の複数ベンダーのDDoS軽減とWAFを利用していました。そうしたソリューションの寄せ集めはパフォーマンスが悪く、大幅な遅延、セキュリティパフォーマンスの低さ、ベンダー費用の無駄につながっていました。

Cloudflareのソリューション（CDN、WAF、DDoS軽減など）と統合した後は、Webサイトのセキュリティとパフォーマンスの費用が67%削減されました。

「パフォーマンスとセキュリティをプロバイダー1社の元に統合したことで、基準コストの大幅削減が実現しました」と、技術ディレクターのSven Ferber氏は述べています。「今は以前の約3分の1になっていると思います。」

ベンダー統合は、企業が購買と管理の費用を合理化するための極めて効果的な戦略になり得ます。以下は、ベンダー統合を検討する際に使える3つの簡単な質問です：

1. 現行ベンダーは脅威に対する保護を提供し、アプリケーションのパフォーマンスを改善しているか？
2. アプリケーションとAPIを単一のコンソールで管理できるか？
3. 社内の複数チームが同じベンダーを使い予算を効率化できているか？

企業は上記の統合のヒントに従って、コストの削減、サプライチェーン管理の簡便化、主要ベンダーとの関係強化を実現できます。

chrono24 The World's Watch Market

要点

企業の**75%**がベンダー統合を検討

Chrono24ではCloudflareとの統合後、WebサイトセキュリティおよびITのコストが**67%**減

企業は、ベンダーの数を絞りサービスを統合することによって、**コスト削減**とサプライチェーン管理の簡便化が可能

証明書管理の自動化により人件費とインフラ費用を合理化

複数のドメインと地域にわたるセキュリティ設定の展開は、ITチームにとって高コストで時間もかかるプロセスになる可能性があります。隠れたコストはサポート対象組織にとってさらなる悩みの種となり、予算の制約がある場合は特に頭の痛い問題です。

それらの隠れコストは証明書管理の費用という形をとるのが一般的です。SSL/TLS証明書はネットワークのデジタルIDになります。平均的企業のWebプレゼンスには、数千とは言わないまでも数百の証明書が必要になるかもしれません。それらの証明書の管理に人件費とインフラ費用が嵩み、コスト高になる可能性があります。予期せぬ証明書の期限切れによる逸失収益は言うまでもありません。

eコマースのプラットフォームSHOPYYは、プライベートキーの作成、保護、ドメイン検証、発行、更新、再発行など、SSL証明書の管理をCloudflareで自動化しています。

SHOPYYは当初、無料の証明書管理ツールを使っていましたが、提供される証明書は信頼性が低く、有効期限が短いものでした。そのため、SHOPYYは証明書の管理と更新プロセスを監督する人材を追加採用しなければなりませんでした。

今はCloudflare SSL for SaaSで証明書管理のプロセスをCloudflareに任せられ、SHOPYY社内で必要なのは全プロセスの保守要員1人だけになりました。

「Cloudflareの製品を使ったら、運用と保守の費用だけで60%のコスト削減になりました」と、創業者兼CTOのYuanming Chen氏は述べています。

また、証明書管理に不備があると、証明書の失効により収益にも影響を及ぼしかねません。オンライン融資マーケットプレイスのLendingTreeは、CloudflareのTLS証明書を使って費用を節約し、期限切れを予防しています。

「当社には何千ものプロパティがあります。その規模を考えれば、証明書を更新し損なうのは時間の問題でした」と、アプリケーションセキュリティのリードJohn Turner氏は述べています。「CloudflareのTLS証明書なら自動的に更新されますし、**管理コストと証明書期限切れによる逸失収益を合わせて年間約5万ドルの節約になっています。**」

効果的な証明書管理システムを確立すれば、リソースの適切な再配分にも役立ちます。ドイツで設立され、クラウドベースのアプリケーションを展開する自動プラットフォームmogeniusは、Cloudflareで証明書管理を自動化しています。そのおかげで、コアビジネスの開発により多くの時間をかけられるようになりました。

「Cloudflareがやってくれることすべてを社内でやろうとすると、業務時間の少なくとも20%をとられます」と、共同創業者でCPOのJan Lepsky氏は述べています。「**Cloudflareのおかげで、クラウド開発と顧客へのパイプライン展開の最適化に集中できます。**」

隠れたコストを避け、事業運営を円滑に行いたい企業にとって、証明書管理を肩代わりしてもらうことは極めて重要です。証明書関連業務を手作業でバラバラに行う非効率なやり方は、人件費とインフラ費用が高くつき、証明書失効による中断で収益が失われたり、無駄の多いリソース配分につながったりします。

企業は、SSL for SaaSやTLS証明書などの機能を備えた証明書管理を実装することにより、大幅なコスト節約と収益の改善を実現できます。

SHOPYY

lendingtree

mogenius®

要点

SHOPYYはCloudflare SSL for SaaSを使い、運営と保守のコストを60%削減

LendingTreeはCloudflare TLSを使って管理費と逸失収益を年間5万ドル節約

mogeniusはCloudflareで証明書管理業務を自動化し、時間を20%節約してコアビジネスに集中

トラフィックコスト増大につながる攻撃をブロック

APIの利用が増えるにつれて、攻撃対象領域が拡大します。悪性ボット、DDoS攻撃、その他の脅威がアプリケーションやAPIを侵害する可能性があり、経営幹部や技術部門のリーダーはそれぞれ、そうした攻撃がビジネスに大きな影響を及ぼしかねないことを認識しています。

ある推定によれば、これまでAPIのセキュリティが不十分なために企業が被ったコストは年間750億ドルに上ると言われています。

APIへの攻撃はクレデンシャルスタッフィングやDDoS攻撃につながり、正当なユーザーに対するサービスが滞るだけでなく、攻撃によって膨れ上がったトラフィックのコストを企業が負担せざるを得ない状況になりかねません。

LendingTreeでは、以前のセキュリティベンダーがDDoS攻撃中は上乗せ料金を請求したため、多額の支払いをしていました。この課金モデルでは膨大な超過コストが発生しただけでなく、正当なトラフィックがブロックされました。

「テレビで新しいスポットCMを打ったり、新たなソーシャルメディアキャンペーンを実施したりするたびに、リクエスト数がベンダーに言われて指定した任意の上限を超え、その急増がDDoS攻撃と解釈されて、正当なトラフィックがブロックされました」と、アプリケーションセキュリティリーダーのJohn Turner氏は振り返ります。「**当社は潜在顧客を失っただけでなく、サイトを訪問してもらうために費やしたお金も無駄になりました。それでも『DDoS攻撃対策』**の料金を請求されたのです。」

この非効率を是正するため、LendingTreeはCloudflareのボット管理機能とレート制限機能を導入しました。その結果、**48時間以内に特定APIエンドポイントへの攻撃が70%減り、同社はAPIエンドポイントの不正利用を阻止することによって5か月も経たないうちに25万ドルを節約できたのです。**

オンラインゲーミングの持ち株会社Flutter Entertainmentでは、トラフィックの70～90%が悪性であることが判明し、悪性ボットをフィルタリングしてブロックするソリューションを必要としていました。Cloudflare Bot Managementの実装後、**Flutterへの悪性トラフィックは90%減少し、年間200万ポンド以上の節約ができました。**

ボット管理とDDoS攻撃対策を利用することで、企業は攻撃やAPIの不正利用を防止し、攻撃関連の支出を抑えることができます。企業がセキュリティベンダーを選考する際は、以下の条件に注目する必要があります：

- 機械学習を用い、トラフィックの観察データに基づいてレート制限を設定している
- 最新の攻撃はIP制限を簡単に掻い潜ることができるため、地理的位置やIPロケーションに基づくレート制限以上の対策を講じている
- 開発者が、Webアプリケーションとパブリックapiのトラフィックをすべてwafとapiゲートウェイ経由でルーティングしている
- DDoS攻撃対策、WAF、APIゲートウェイのツールを統合し、多層の脅威防御を実現している
- 企業がトラフィックを処理する場所で保護が行われるようにすることにより、遅延を低減している
- 定額制のDDoS軽減を提供し、超過料金を廃止している

適切なベンダー・セキュリティ戦略を実装することで、年間数百万ドルとは言わないまでも、数千ドルの節約ができます。

Flutter™

要点

不十分なAPI保護のため、企業に**年間750億ドル**ものコストが発生していることが判明

適切なアプリケーションセキュリティツールを実装すれば、**年間数百万ドルとは言わないまでも、数千ドルの節約が可能**

LendingTreeでは、DDoS攻撃対策によって特定APIへの攻撃が48時間以内に70%減少し、攻撃を阻止したことにより5か月も経たないうちに25万ドルを節約

Cloudflare Bot Managementのおかげで、Flutterでは悪性トラフィックが90%減少し、年間200万ポンド以上の節約を達成

帯域幅やクラウドの使用料、転送料金など予想外の料金やコストを排除

多くのセキュリティサービスはクラウドに依存し、多くのクラウドプロバイダーはストレージやコンピューティングの料金を企業に請求します。加えて、データ転送料金も請求するのが一般的です。転送料金は、ストレージからのデータ転送に関連する費用です。

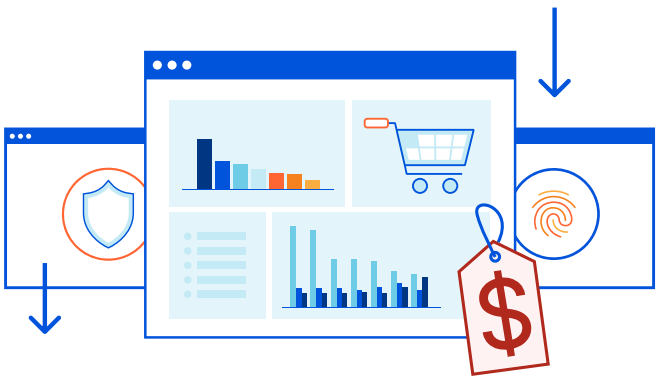
転送料金は、顧客階層、サブスクリプションのタイプ、転送データ量など複数の要因に基づいて計算されます。そのため予測が難しく、料金が嵩んでくると企業にとっては打撃です。実際、IDCの推定では、クラウドストレージのコストに占める転送料金の割合は6%以上に上ります。

このことを踏まえ、欧州のデジタルディレクトリー・ローカル検索サービスPagesJaunesはCloudflare CDNの実装を決め、帯域幅使用料の節約とキャッシュとDNSの管理の改善に役立てました。

「Cloudflare CDNにトラフィックが吸収される分、当社のインフラストラクチャにかかる負担が減り、耐障害性が高まるのがすぐわかりました」と、アーキテクチャ、パフォーマンス、セキュリティの責任者Loïc Troquet氏は断言します。「**帯域幅の70%は、Solocalのインフラで支えなくてもよくなりました。**」

帯域幅を節約すればコストを削減できます。オンライン学習ツール**Quizlet は、CloudflareのCDN、DNS、WAF、DDoS軽減サービスを導入してから日々の総帯域幅消費を10TB以上節約し、Google Cloud Servicesのネットワーク転送料金を50%以上削減しています。**

アプリケーションセキュリティの戦略と実践の実装により、予測不能な転送料金をなくすことができます。



PagesJaunes

Quizlet

要点

適切なCDNベンダーの選択など、アプリケーションセキュリティ戦略の実装によって、予測不能な転送料金を排除可能

Cloudflare CDNを導入したPagesJaunesは、帯域幅を70%節約

QuizletはCloudflareを使って**日々の総帯域幅消費を10TB以上節約**し、Google Cloud Servicesのネットワーク転送料金を50%以上削減して、毎月数千ドルを節約

Cloudflareでアプリケーションセキュリティを合理化し、コストを削減

Cloudflareを使えば、企業は効率改善と経費合理化のためのアプリケーションセキュリティ戦略を策定することができます。Cloudflareの統合アプリケーションセキュリティポートフォリオは、クラス最高の定額制DDoS攻撃対策、たいていの高度攻撃を阻止するWebアプリケーションファイアウォール、事前防止的なAPIセキュリティ、脅威インテリジェンスに基づくボット管理、高度なクライアントサイド攻撃の検出をまとめたものです。

ご関心がおありですか？

Cloudflareへ今すぐご連絡ください

CLOUDFLARE

enterprise@cloudflare.com | www.cloudflare.com

REV:BDES/4588.2023JUN05