IMPERVA®

Imperva Incapsula DDoS Protection

データシート

大規模で高度なDDoS攻撃も自動的に緩和

Imperva Incapsulaは、ビジネスへの影響を最小限に抑えながら、ネットワークやプロトコル、そしてアプリケーションレベルの攻撃など、大規模で高度なDDoS攻撃からWebサイトを保護します。オンラインサービス企業は、Impervaが提供するクラウドベースのサービスによって、仮に攻撃を受けた場合でも、高いパフォーマンスでサービスの提供を継続し、経済的な損失を受けることなく、企業の評判における深刻なダメージも排除することができます。

DDoS Protectionサービスは、SYNフラッド攻撃やDNSアンプ攻撃など、大規模な攻撃に対応できるだけでなく、高度で先進的な対応メカニズムによって、複雑なアプリケーションレイヤ攻撃についても緩和することが可能です。このサービスでは、誤検出を最小限に抑えながら、DDoS攻撃を自動的かつ透過的に緩和できるため、サイト訪問者にサイトが攻撃を受けていることを気付かれることもありません。

DDoS Protectionは、攻撃をモニターして分析するための包括的なダッシュボードに加え、お客様のサイトが攻撃を受けた場合でもサイトが稼動を続けられるよう、経験豊富な専門家で構成された24時間365日対応の専門NOC（ネットワークオペレーションセンター）サービスを提供します。

提供サービス

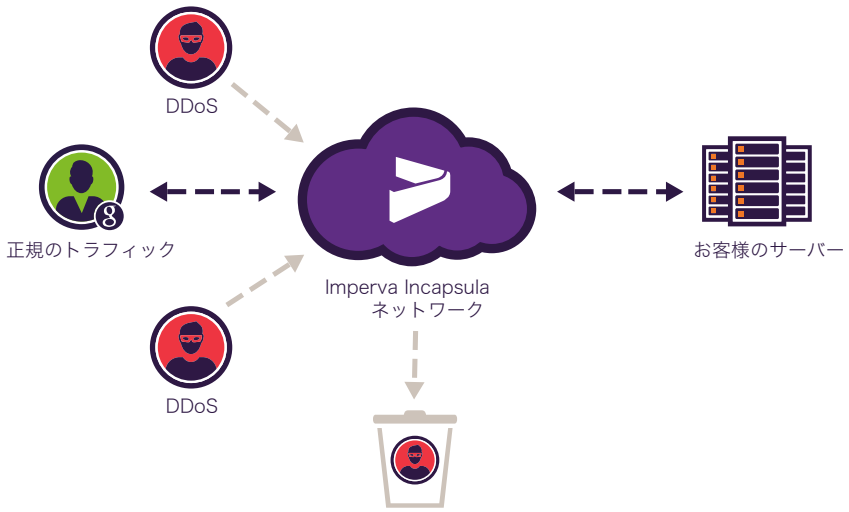
- 世界各地に配置されたデーターセンターをベースとする強力なサービス基盤
- SYNフラッド攻撃、DNS攻撃、DNSアンプ攻撃に対する特別なサポート
- 複雑なアプリケーションレイヤ攻撃を緩和する高度なアルゴリズム
- 攻撃をモニターして分析するための包括的なダッシュボード
- エンタープライズグレードで対応する24時間365日稼動のNOC
- エニーキャスト、ユニキャスト、ハイブリッド型ルーティングをサポートし、DDoS攻撃を効果的に緩和
- Infrastructure Protectionがネットワークレイヤ攻撃からサブネット全体を防御

Incapsulaが選ばれる理由

- 攻撃を常時自動で検知し、「攻撃中」モードを起動できる
- 誤検出を抑えた透過的な影響緩和対応により、ビジネスへの影響を最小化
- 大規模なDDoS攻撃から小規模なDDoS攻撃まで一貫した防御を実現
- ハードウェアの導入もしくはソフトウェアのインストール、Incapsulaのサービスとの統合、またはWebサイトの変更を行わなくても、DNSの設定を変えるだけで使える

あらゆるタイプのDDoS攻撃を包括的に防御

Incapsulaは、SlowlorisやICMP、TCP&UDPフラッドなどのネットワークレベルの攻撃や、サーバーのリソースをパンクさせてしまうGETフラッドなどのアプリケーションレベルの攻撃など、あらゆるタイプのWebサイト攻撃を防御します。本サービスは、アプリケーション、Webサーバー、DNSサーバーの脆弱性を悪用したり、奇襲攻撃や大規模なボットネット脅威を仕掛ける高度な攻撃を検知し、その影響を緩和します。



大規模な攻撃にも対応できる拡張性の高い大容量ネットワーク

SYNフラッド攻撃やDNSアンプ攻撃のような大規模DDoS攻撃のバンド幅は、通常100Gbpsを上回るため、ネットワークキャパシティをパンクさせないための対策を講じる必要があります。Impervaが提供するグローバルネットワークのキャパシティは1Tbps(terabits per second)を超え、どんな規模の攻撃にも耐えられるようになっています。Incapsulaのオールウェイズ・オンなクラウドサービスは、お客様の外部のネットワークで攻撃を緩和することで、正常なトラフィックだけがお客様のホストサーバーに届くようにします。

インテリジェントなマルチレイヤ防御

IncapsulaのISPグレードのエッジルーターは、DNSアンプ攻撃やMartianパケットなど、不正なパケットをフィルタリングして即座に隔離するようになっています。残りのトラフィックは、パケットのサービスクラスに応じて優先順位付けされ、それぞれが10Gbsのアップリンクを持つ、各スクラビングセンターの間で分散されます。Incapsulaの各スクラビングセンターには、相互接続された複数の高性能のスクラビングクラスターが配置されています。このクラスターを使って、DDoSトラフィックのプロファイリングとブロッキングを実施します。もし攻撃を受けた場合には、インバウンドパケットとHTTPセッションを処理します。Incapsulaでは、優れたインテリジェントのトラフィックプロファイリングとボット検知テクノロジーを使用して、正規の利用者に影響を与えることなく、不審なトラフィックだけを確実に除去します。

Incapsulaはあらゆるタイプの DDoS攻撃からWebサイトを 防御します：

- TCP SYN+ACK
- TCP FIN
- TCP RESET
- TCP ACK
- TCP ACK + PSH
- TCP Fragment
- UDP
- ICMP
- IGMP
- HTTP Flood
- Brute Force
- Connection Flood
- Slowloris
- Spoofing
- DNS flood
- Mixed SYN + UDP or ICMP + UDP flood
- Ping of Death
- Smurf
- Reflected ICMP 及び UDP
- Teardrop
- ゼロデイDDoS攻撃
- Apache、Windows または OpenBSDの脆弱性を標的にした攻撃
- DNSサーバーを標的にした攻撃
- その他多数

アプリケーションレベルの攻撃に対する高度な緩和対策

訪問者識別テクノロジーによって、正規なWebサイトの訪問者（人間や検索エンジンなど）と、自動化されたあるいは悪意あるクライアントを識別します。この機能は、DDoS攻撃があたかも正規な訪問者がリクエストを出しているように見せかける、アプリケーションレベルの攻撃に対して特に有効です。簡単に回避されたり、誤検出しやすいテクニック（例えばレート制限やスプラッシュ/ディレイスクリーンなど）をベースにしたDDoS防御サービスとは異なり、Incapsulaでは、人間とボットトラフィック、「正規な」ボットと「不正な」ボットの違いを区別し、AJAXとAPIを特定することができます。GoogleやBingのような正規なボットは、たとえ攻撃を受けている最中でもお客様のWebサイトにアクセスすることができます。

DNS DDoS攻撃の防御

IncapsulaのDNS DDoS攻撃阻止機能は、サイトの可用性にとって重要なDNSサーバーを標的型攻撃から防御します。NSレコードの定義をIncapsulaに変更するだけで、保護ドメインに対する全てのDNSクエリを検査し、Incapsulaクラウド内の不審なトラフィックをフィルターできるようになり、「安全なクエリ」だけがお客様のDNSサーバーに到達します。この機能によってサーバーをDDoS攻撃から守り、他のサーバーに対するDNS amp攻撃するための踏み台としてお客様のサーバーが利用されることを阻止します。攻撃を受けた場合、お客様は、Eメールによるアラートと GUIによる通知を受けます。

トランスペアレントな緩和

Incapsulaでは、あらゆるDoS攻撃やDDoS攻撃からの防御だけでなく、誤検出の発生も抑えることができます。Incapsulaは、0.01％未満の誤検出率でトランスペアレントな攻撃緩和対策を実施するため、通常のユーザーエクスペリエンスが損なわれることがありません。つまり、業務効率を落とすことなく、長期に渡るDDoS攻撃から身を守ることができるのです。お客様の正規なサイト訪問者の99.99%は、攻撃の影響を受けたり、スプラッシュスクリーンや遅延にいら立つこともなく、いつもと同様にサイトを利用できます。

自動検知とトリガー

Incapsulaのオールウェイズ・オンなDDoS緩和機能は、長期に渡り短時間の攻撃を不規則な間隔で繰り返す「奇襲」攻撃に対しても対処できるよう対策が施されています。手動で機能をオン・オフする必要のあるDDoS緩和ソリューションの場合には、このようなタイプの攻撃が厄介な問題となります。自動検知と起動が可能なIncapsulaの場合には、攻撃の検知と緩和に完全に対応することが可能です。

現状のDNSベースの迅速で容易なルーティング

DDoS Protectionは、新たなハードウェアやソフトウェア、Webアプリケーションとの連携やコード変更を行う必要無しに、容易に展開することが可能です。サービスを利用する際には、お客様のWebサイトのDNS設定を変更するだけの対応で済みます。導入の手間が不要なことで、既存のホスティングプロバイダーやアプリケーションインフラストラクチャーを変更することなく、ほんの数分で防御を開始することができます。

“Incapsulaによって、大規模なDDoS攻撃にも耐え、標的となったWebサイトを稼動させ続けることができました”

eWEEK

2013年10月1日 “LATEST 100 GIGABIT ATTACK IS ONE OF INTERNET’S LARGEST”

サブネット向けのインフラ保護

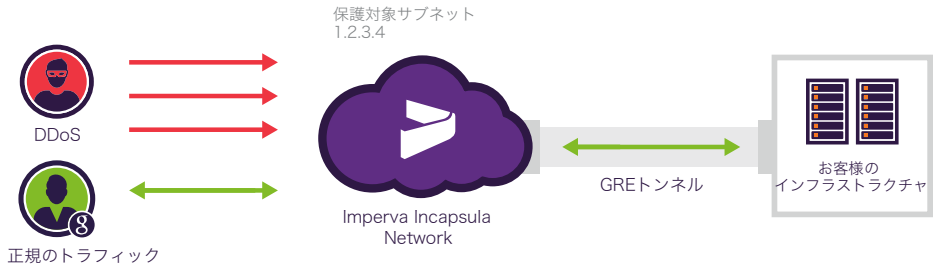
Incapsulaでは、複数の種類のサービスや宛先IPアドレスのサブネット全体のプロトコルを防御する必要がある企業向けに、オンデマンドの形でBGPルーティングベースのDDoS防御機能を提供しています。攻撃を受けた場合、トラフィックは、IncapsulaのBGPアナウンスメントを使用するスクラビングセンター経由でリルートされます。ここから先、Incapsulaは「ISP」として機能し、全ての防御IPレンジのアナウンスメントをアドバタイズします。全ての着信ネットワークトラフィックは、検査及びフィルタリングされ、GREトンネル経由のセキュアな状態で正規のトラフィックだけが企業のネットワークに転送されます。

DDoS攻撃を受けている間、トラフィックはIncapsula経由で流れます。BGPアナウンスメントは、保護対象サブネットをIncapsula経由でルーティングし攻撃を緩和するために使用されます。

IPアドレス向けのインフラ保護

お客様は、Incapsulaから保護IPアドレスを受け取り、その後はIncapsulaが全ての着信トラフィックを調査、フィルタリングします。さらに、冗長構成でセキュアな双方向GREトンネルを使ってクリーンなトラフィックを元のIPに転送し、お客様のアプリケーションからのアウトバンドトラフィックをお客様のエンドユーザーに返します。

IPアドレス単位での保護は、高トラフィックやIPカウントが低いHTTP以外を使用しているアセット（ゲームサーバーやSaaSアプリケーションなど）だけでなく、IP直接の攻撃に対する防御にも最適なものと言えます。



DDoS攻撃を受けている間、トラフィックはIncapsula経由で流れます。お客様のトラフィックは、IncapsulaのIPアドレスにルーティングされ、Incapsulaネットワークでクレンジングされた後、セキュアなGREトンネルを経由してお客様に転送されます。

協調セキュリティ

Incapsulaは、新しい攻撃方法を含め、DDoS攻撃に関する集団的な知識を活用し、Webサイトを保護します。数千のWebサイトから構成されるサービスネットワーク全体の情報を、クラウド

IMPERVA INCAPSULA

ソーシング技術を駆使して集約し、新しい攻撃を見極め、既知の悪意のあるユーザーを特定。この情報を基に保護対象Webサイト全体に対して緩和対策ルールをリアルタイムで適用します。

コスト効果の高いクラウドベースのDDoS攻撃防御

Incapsulaは、数Gbitのインターネット接続を実現し、ハードウェアの追加や運用にコストをかけることなく24時間365日DDoS攻撃からお客様を保護するクラウドベースのサービスです。従って、バンド幅をオバープロビジョニングしたり、追加のサーバーやロードバランシングのアプライアンスをオンプレミスで用意する必要もありません。さらにIncapsulaでは、エンタープライズプランのお客様に対して、DDoS攻撃のセキュリティに関するお客様のあらゆるニーズに対応できるよう専任のアカウントマネージャーをアサインします。

DDoS攻撃とセキュリティのスペシャリストによる、エキスパートサポート

DDoS Protectionは、Incapsulaの実戦経験豊富なセキュリティオペレーションセンター (SOC) のエンジニアよる継続的なモニタリングと緩和対策を提供します。本サービスには、予防的なイベント管理や対応、継続的なリアルタイムモニタリング、ポリシーのチューニングの実施、攻撃概要レポートの提供、そして24時間365日のテクニカルサポートが含まれています。

株式会社 Imperva Japan

www.imperva.jp
Mail：FM-Japan@imperva.com
TEL：03-6263-0671