



DoS攻撃

reimei



DoS (Denial of Service) 攻撃とは？

- 情報セキュリティにおける可用性を侵害する攻撃手法
- サービス不能攻撃
- 妨害が目的で情報の窃盗や破壊が目的ではない

DoS (Denial of Service) 攻撃とは？

1. CPUやメモリなどのシステムリソースを過負荷状態、又はオーバーフロー状態にする
2. 大量のパケットを送りつけネットワークの帯域を溢れさせる
3. ホストのセキュリティホールについてOSや特定のアプリケーションを異常終了させる

DoS攻撃の歴史

1. 発見の世代 (1996年 ~ 1998年)
 - DoS攻撃を可能とする手法や脆弱性が発見
 - 攻撃者が一人
2. ツールの世代 (1999年 ~ 2000年)
 - DoS攻撃からDDoS攻撃へと進化 (攻撃指令管理技術の確立が背景)
3. ワーム世代 (2001年 ~ 2000年代中盤)
 - 自己複製しながら伝搬するワームが登場 (攻撃エージェント配備技術の確立が背景)
 - 時刻で制御しながら攻撃
4. ボット世代 (2000年代中盤 ~ 現代)
 - ツールとワームが融合したボットネットが登場
 - 分身を制御する技術と増やす技術を兼ね備えたシステム
 - 配備したエージェントを自在に制御しながら攻撃

<https://andmem.blogspot.com/2014/02/dosattack.html#chapter-13>

いろいろな DoS攻撃

- DDoS攻撃
- SYN(FIN) Flood 攻撃
- ACK Flood攻撃
- UDP Flood 攻撃
- ICMP Flood 攻撃(Ping Flood 攻撃)
- EDoS攻撃
- Connection Flood 攻撃
- 反射・増幅型DDoS攻撃
- smurf攻撃
- DNS Amp 攻撃
- IoT機器を悪用したDDoS攻撃
- HTTP GET/POST Flood 攻撃
- Slow HTTP DoS 攻撃
- Stream Flood 攻撃
- DNS Flood 攻撃
- Ping of Death
- Land

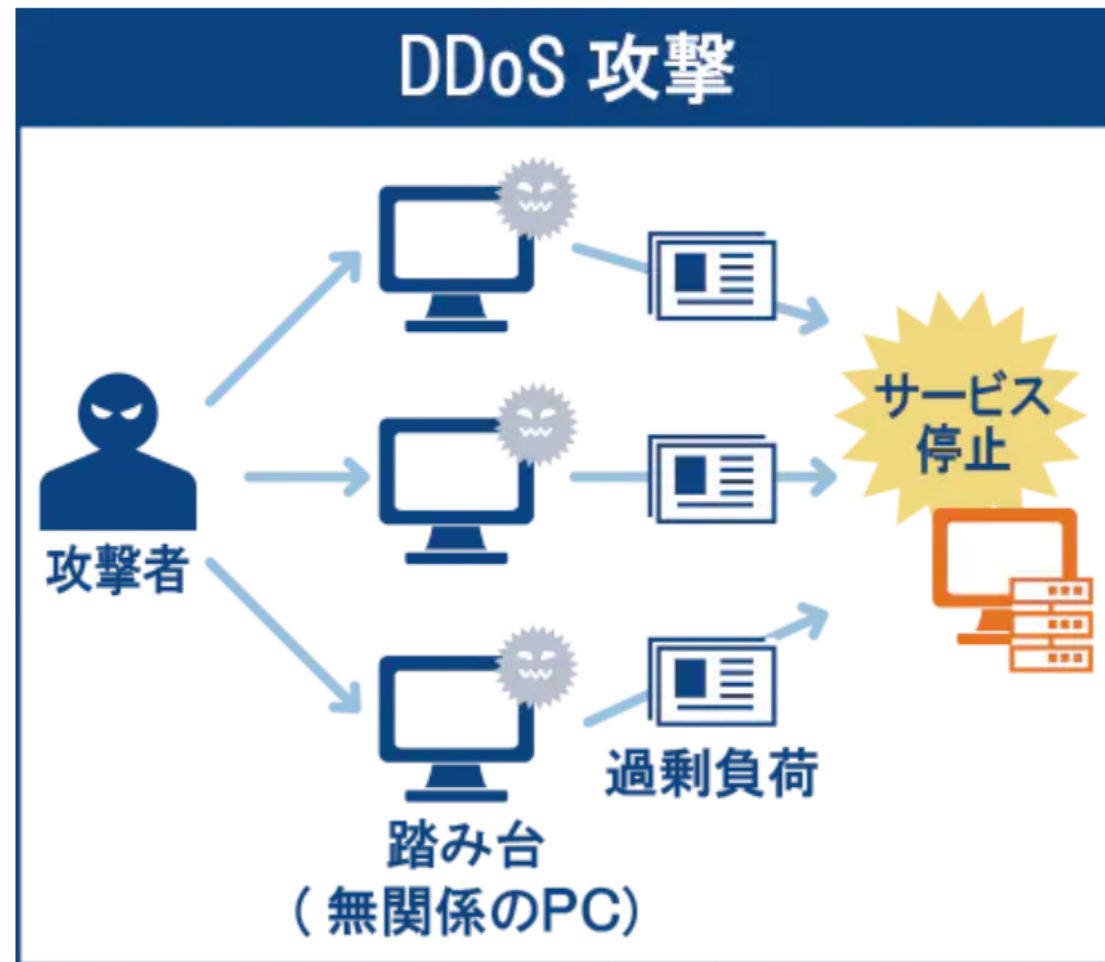
DDoS攻撃

- Distributed Denial of Service attack
分散型サービス不能攻撃
- 多数の踏み台に予め仕掛けておいた攻撃プログラムから一斉にDoS攻撃を仕掛ける攻撃手法
- 近年はボットネットによって実行されるケースが大半
- 分類 2 に該当

https://www.ntt.com/business/services/network/internet-connect/ocn-business/bocn/knowledge/archive_18.html

DoS
(Denial of Service)
攻撃とは？

1. CPUやメモリなどのシステムリソースを過負荷状態、又はオーバーフロー状態にする
2. 大量の packets を送りつけネットワークの帯域を溢れさせる
3. ホストのセキュリティホールについてOSや特定のアプリケーションを異常終了させる



DDoS攻撃 対策

- 十分な帯域を持つネットワークを使用
- 公開サーバーおよび経路上のネットワーク機器の処理能力を増強
- 発信元アドレスが明らかに偽装されているパケットやブロードキャスト宛パケットをファイアーウォールで遮断
- 不要なICMPパケット、UDPパケットの遮断、もしくは帯域制限
- CDNを利用
- CDNプロバイダ等が提供するDDoS攻撃対策サービスを利用
- Firewall/IPSの導入

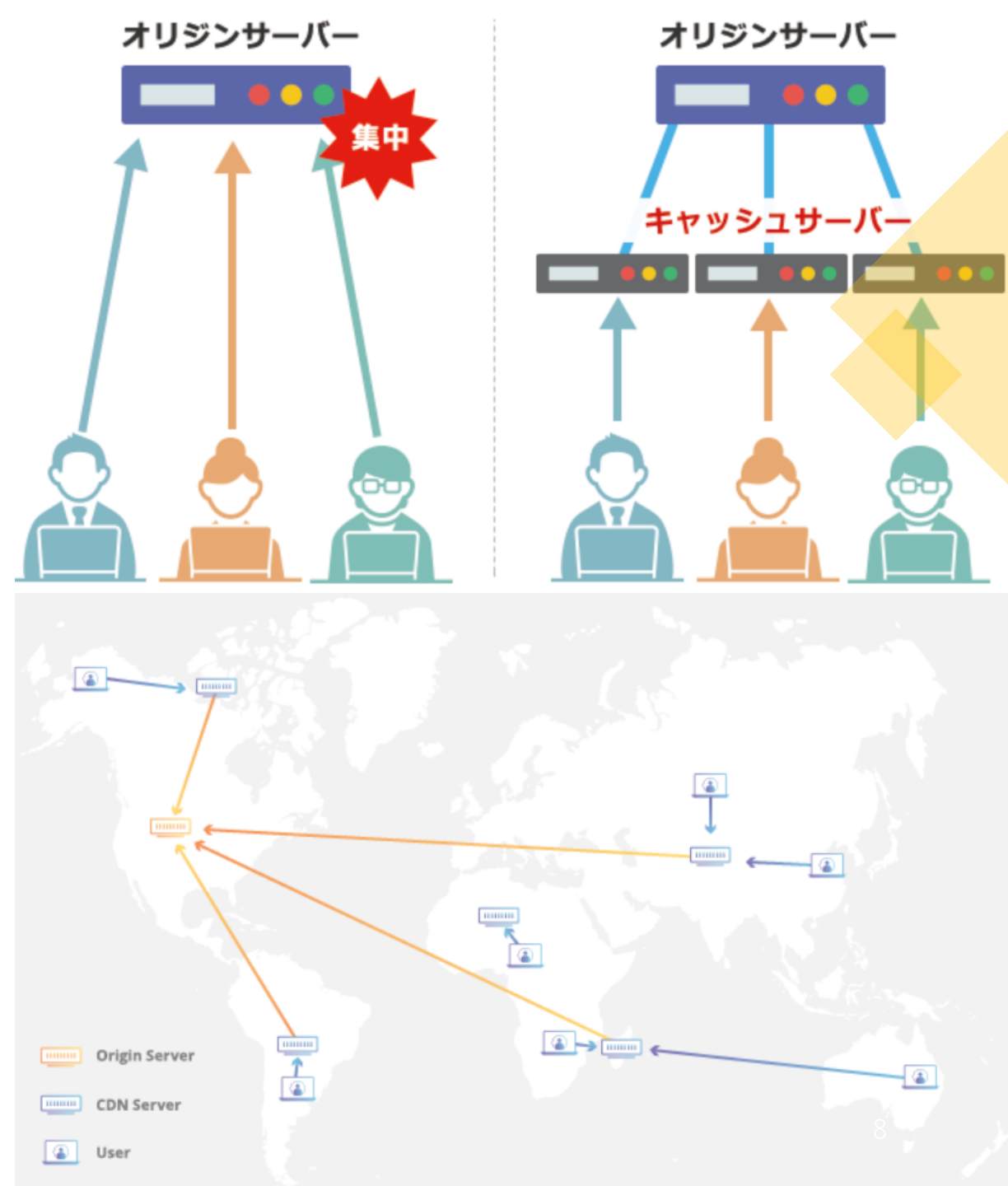
CDN

- Content Delivery Network
- インターネットコンテンツを高速配信するために連携する地理的に分散されたサーバーのグループ
- ウェブコンテンツを効率的かつスピーディーに配信できるように工夫されたネットワーク
- キャッシュサーバーは負荷を肩代わりしてくれるレンタルサーバーのようなもの

<https://www.cloudflare.com/ja-jp/learning/cdn/what-is-a-cdn/>

<https://knowledge.sakura.ad.jp/19191/>

<https://www.kagoya.jp/howto/network/cdn/>



SYN(FIN) Flood 攻撃

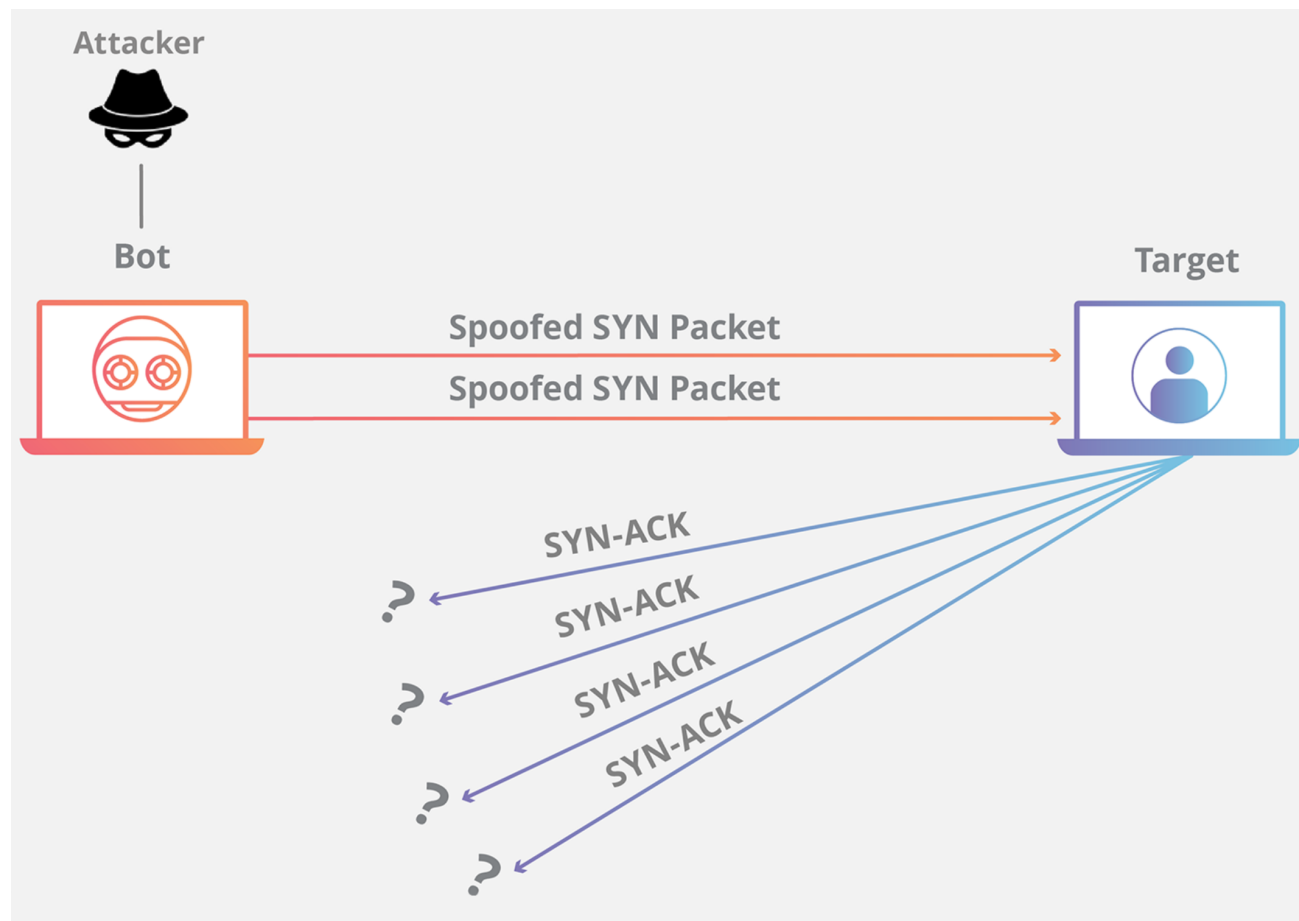
DoS
(Denial of Service)
攻撃とは？

1. CPUやメモリなどのシステムリソースを過負荷状態、又はオーバーフロー状態にする
2. 大量の packets を送りつけネットワークの帯域を溢れさせる
3. ホストのセキュリティホールについてOSや特定のアプリケーションを異常終了させる

- SYNパケットを大量に送りつけて、正常なサービスの提供を妨害する攻撃
- 発信元が偽装されているため攻撃者の特定が困難
- 分類 1or 2 (規模による) に該当

1. 攻撃者は発信元を偽装したSYNパケットを送信
2. ホストはSYN/ACKパケットを返すがACKパケットが返らない
(その間もSYNパケットが送られ続けられる)
3. ホストは情報をテーブルにセットしてタイムアウトを待つが、やがてリソースを使い果たして接続要求を受信不可

[https://www.cloudflare.com/ja-
jp/learning/ddos/syn-flood-ddos-attack/](https://www.cloudflare.com/ja-
jp/learning/ddos/syn-flood-ddos-attack/)



SYN Flood 攻撃 対策

- SYN CookieやSYN Floodプロテクション機能を持つOSやファイアウォールを使用
- コネクション確立時のウェイトタイムを短縮
- ルータやスイッチによるSYNパケットの帯域制限
- Firewall/IPSの導入

SYN Cookie

- SYN/ACKパケットのシーケンス番号に埋め込まれるデータ
- 通常はTCPヘッダをハッシュ化した値

1. SYNパケットを受け取った段階ではTCPソケットは閉じたまま
2. SYN CookieをセットしたSYN/ACKパケットをクライアントに返信
3. ACKパケットを確認して正当な通信ならソケットをオープンにしてTCPコネクションを確立

→ 攻撃者は送信元のアドレスは適当なので正しいシーケンス番号を持つACKをホストに渡すことができないので正当な通信か判断可能

ACK Flood 攻撃

DoS
(Denial of Service)
攻撃とは？

1. CPUやメモリなどのシステムリソースを過負荷状態、又はオーバーフロー状態にする
2. 大量のパケットを送りつけネットワークの帯域を溢れさせる
3. ホストのセキュリティホールについてOSや特定のアプリケーションを異常終了させる

- ACKを大量に送信することで接続のためのリソースを使用させる攻撃
- ACKを連続して送信すると通信ログがACKパケットでいっぱいになるので、別の攻撃のカモフラージュとして使用されることも
- ターゲットはパケット破棄を大量に行わなければならない、リソースが枯渇
- 分類 1 に該当

<https://www.cloudflare.com/ja-jp/learning/ddos/what-is-an-ack-flood/>

ACK Flood 攻撃 対策

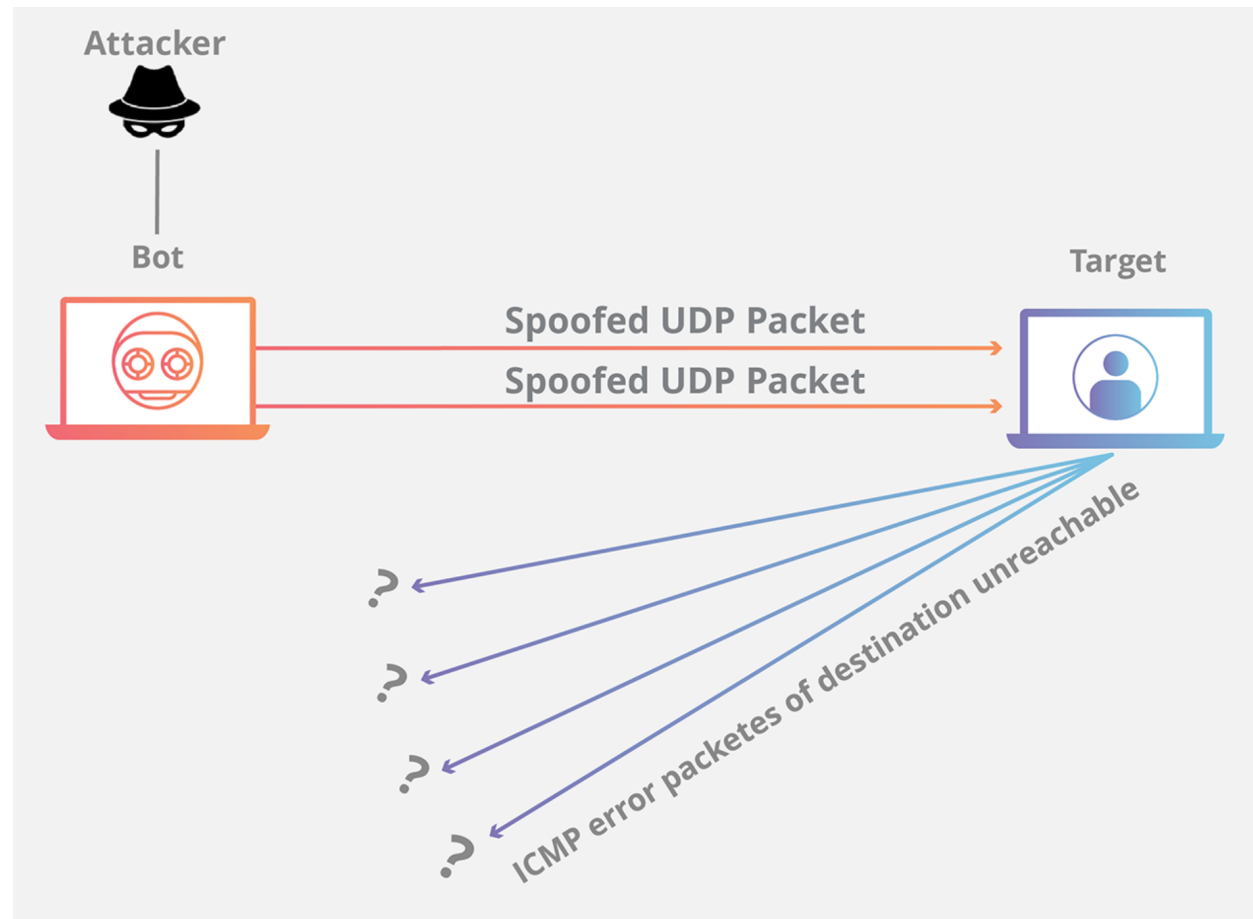
- CDN(Content Delivery Network) を使用して不要な ACK パケットを選別
- Firewall/IPS の導入

UDP Flood 攻撃

- ターゲットのUDPポートにサイズの大きなパケットを大量に送り続ける攻撃
- 分類 1 or 2 (規模による) に該当
- 非常に小さいパケットを送る攻撃もあり、これはファイアウォールなどのネットワーク機器に負荷をかけることが目的
- UDPはコネクションレスなので発信元アドレスの偽装は容易であり、攻撃者の特定は困難

DoS
(Denial of Service)
攻撃とは？

1. CPUやメモリなどのシステムリソースを過負荷状態、又はオーバーフロー状態にする
2. 大量のパケットを送りつけネットワークの帯域を溢れさせる
3. ホストのセキュリティホールについてOSや特定のアプリケーションを異常終了させる



UDP Flood 攻撃 対策


- 不要なUDPサービスを停止
- 不要なUDPサービスへのアクセスをファイアウォールでフィルタリング
- ルータやスイッチによるUDPパケットの帯域制限
- Firewall/IPSの導入

ICMP Flood 攻撃 (Ping Flood 攻撃)

- ターゲットにサイズの大きなICMP echo request (ping)を大量に送り続ける攻撃
- 分類 1 or 2(規模による) に該当
- ICMPはUDP同様コネクションレスなので発信元アドレスの偽装は容易であり、攻撃者の特定は困難

DoS (Denial of Service) 攻撃とは？

1. CPUやメモリなどのシステムリソースを過負荷状態、又はオーバーフロー状態にする
2. 大量のパケットを送りつけネットワークの帯域を溢れさせる
3. ホストのセキュリティホールについてOSや特定のアプリケーションを異常終了させる



ICMP Flood 攻撃 (Ping Flood 攻撃) 対策

- ルータやファイアーウォールでICMPパケットを遮断
- ルータやスイッチによるICMPパケットの帯域制限
- Firewall/IPSの導入

EDoS攻撃

- Economic Denial of Service attack
- ストレージ容量やトラフィック量に応じて課金されるクラウドの特性を悪用し、クラウド利用企業の経済的な損失を狙ってリソースを大量消費させる攻撃
- 有効な対策がない

Connection Flood 攻撃

DoS
(Denial of Service)
攻撃とは？

1. CPUやメモリなどのシステムリソースを過負荷状態、又はオーバーフロー状態にする
2. 大量のパケットを送りつけネットワークの帯域を溢れさせる
3. ホストのセキュリティホールについてOSや特定のアプリケーションを異常終了させる

- ターゲットのTCPポートにコネクションを確立し続けることで大量のプロセスを起動してソケットを確立する攻撃
- コネクション数に制限がない場合はシステムリソースを使い尽くすまでコネクションを確立
- コネクションを確立するため発信元アドレスを偽装することはほぼ不可能だが、ターゲットに対して確実に影響を与える
- 分類 1 に該当

Connection Flood 攻撃 対策

- ホストのソケットオープン数やTCPキューの割り当て数を増加
- ホストの設定によって同じIPアドレスからの同時接続数を制限
- ホストを冗長構成にするとともにロードバランサを用いた負荷分散
- ルータやファイアウォールで攻撃元アドレスからのパケットを遮断
- Firewall/IPSの導入

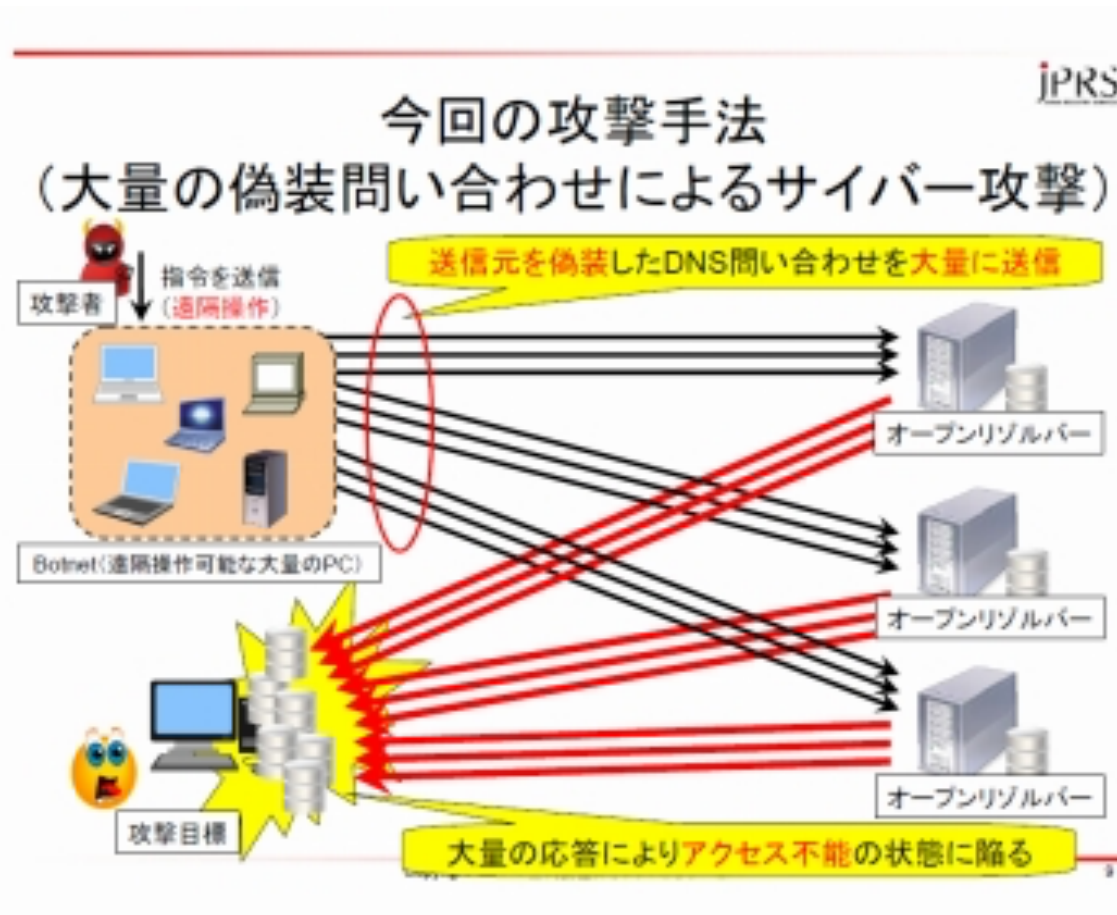
反射・増幅型DDoS攻撃

DoS
(Denial of Service)
攻撃とは？

1. CPUやメモリなどのシステムリソースを過負荷状態、又はオーバーフロー状態にする
2. 大量の packets を送りつけネットワークの帯域を溢れさせる
3. ホストのセキュリティホールについてOSや特定のアプリケーションを異常終了させる

- 応答パケットを大量に発生させてDoS攻撃を行う反射型のDDoS攻撃
- 分類 2 に該当
 1. 攻撃者はC&Cサーバを通じてゾンビPC(botに感染したPC)に攻撃命令
 2. ゾンビPCはターゲットのIPアドレスを発信元アドレスにセットして、攻撃に利用するリフレクタ(NTPサーバーやオープンリゾルバ等)にリクエストを送信
 3. リフレクタは偽装された発信元アドレスに増幅した応答パケットを大量に送信
 4. ターゲットのインターネット接続回線が輻輳状態に陥り、正常なリクエストを受信不可

<https://internet.watch.impress.co.jp/docs/interview/597628.html>



反射・増幅型 DDoS攻撃 対策

- 攻撃対象となる可能性のあるサーバーを外部に公開する必要がない場合は適切なアクセス制限を施してインターネットからのアクセスを遮断
- 攻撃に悪用されやすいコマンドなどを無効
(NTPサーバが過去にやりとりした最大600件のアドレスを回答する「monlist」コマンドなど)
- 十分な回線帯域を確保するとともにネットワーク機器、サーバーの負荷分散などを含めたサイト全体の再構成やパフォーマンスチューニング
- Firewall/IPSの導入

smurf攻撃

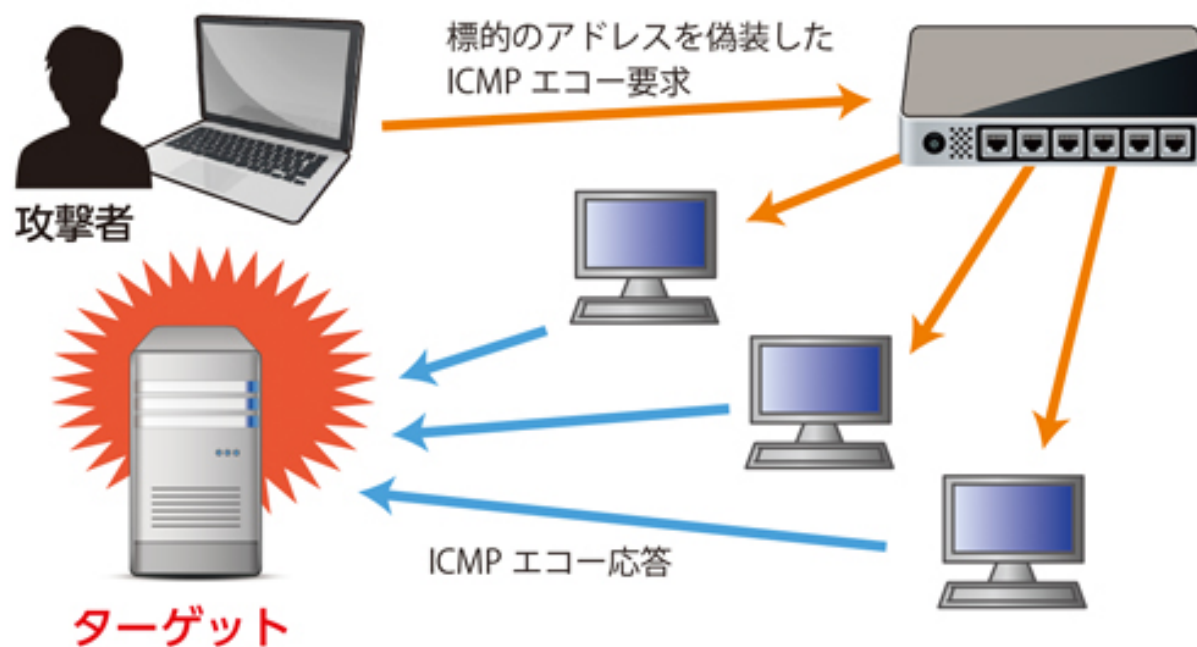
DoS
(Denial of Service)
攻撃とは？

1. CPUやメモリなどのシステムリソースを過負荷状態、又はオーバーフロー状態にする
2. 大量の packets を送りつけネットワークの帯域を溢れさせる
3. ホストのセキュリティホールについてOSや特定のアプリケーションを異常終了させる

- 反射・増幅型DDoS攻撃の一種
- 発信元を偽装したICMP echo requestによってホストが接続されたネットワーク帯域を溢れさせる攻撃
- 分類 2 に該当

1. IPアドレスの送信元を標的のアドレスに偽装
2. ICMP echo requestを送信
3. echo requestパケットに反応して各端末が応答パケットを送信

https://eset-info.canon-its.jp/malware_info/term/detail/00001.html



smurf攻撃 対策

- ルータやファイアーウォールでICMPパケットを遮断
- ルータやスイッチによるICMPパケットの帯域制限
- ブロードキャストアドレス宛のパケットを遮断
- Firewall/IPSの導入

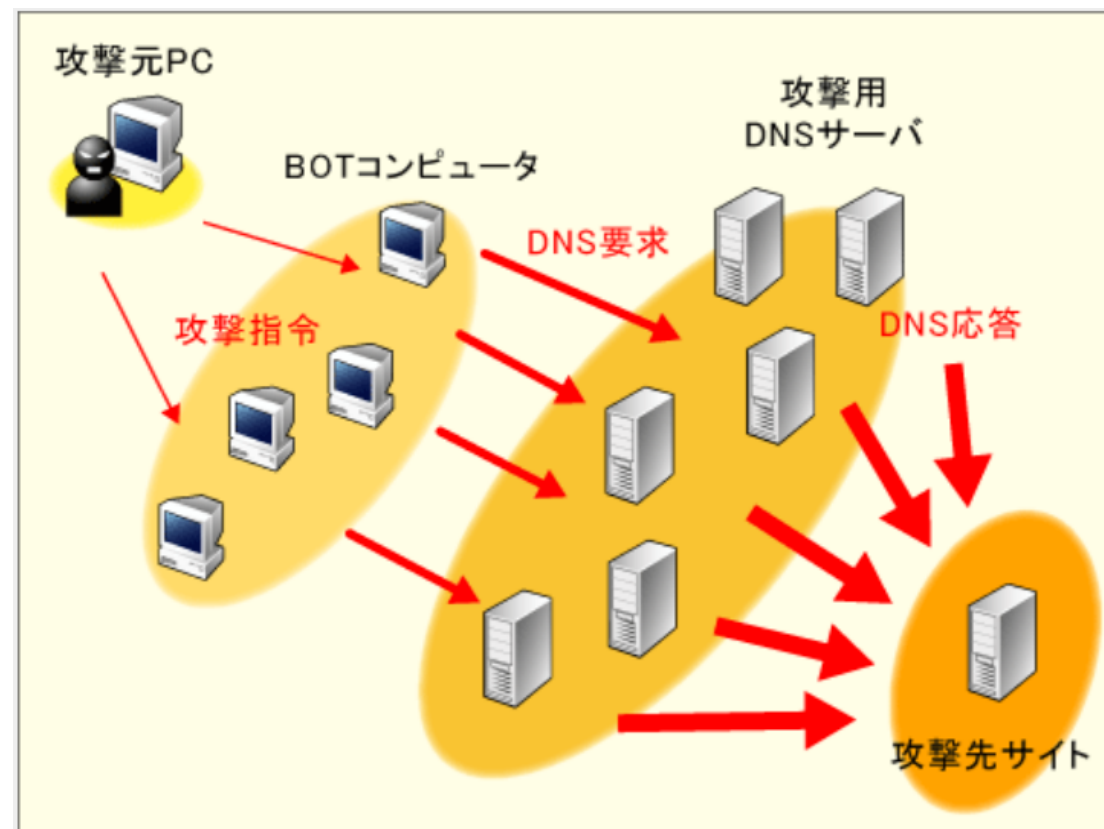
DNS Amp 攻撃

DoS
(Denial of Service)
攻撃とは？

1. CPUやメモリなどのシステムリソースを過負荷状態、又はオーバーフロー状態にする
2. 大量の packets を送りつけネットワークの帯域を溢れさせる
3. ホストのセキュリティホールについてOSや特定のアプリケーションを異常終了させる

- 反射・増幅型DDoS攻撃の一種
 - 分類 2 に該当
 - DNSサーバーを攻撃パケットの踏み台として悪用する手法
 - 踏み台となったDNSサーバー自体の負荷が高まり、サービス不能状態になる場合も
1. 攻撃者は発信元アドレスを最終的なターゲットとなるホストのIPアドレスに詐称した上で攻撃に加担させるDNSサーバー宛にクエリを送信
(応答メッセージのサイズが大きくなるようにする)
 2. クエリを受け取ったDNSサーバーは偽装されたアドレスに応答を返信

<https://www.atmarkit.co.jp/ait/articles/0608/26/news015.html>



DNS Amp 攻撃 対策

- コンテンツサーバーとキャッシュサーバーを完全に分離
- キャッシュサーバーの機能をインターネット側からの利用を禁止
- 自分が送信していないDNSパケットに対するDNS応答は無視・ブロック
- Firewall/IPSの導入

※ コンテンツサーバー
DNSゾーン情報を外部に対して提供
キャッシュサーバー
クライアントからの名前解決要求を処理

<https://www.atmarkit.co.jp/ait/articles/0608/26/news015.html>

IoT機器を悪用したDDoS攻撃

DoS
(Denial of Service)
攻撃とは？

1. CPUやメモリなどのシステムリソースを過負荷状態、又はオーバーフロー状態にする
2. 大量の packets を送りつけネットワークの帯域を溢れさせる
3. ホストのセキュリティホールについてOSや特定のアプリケーションを異常終了させる

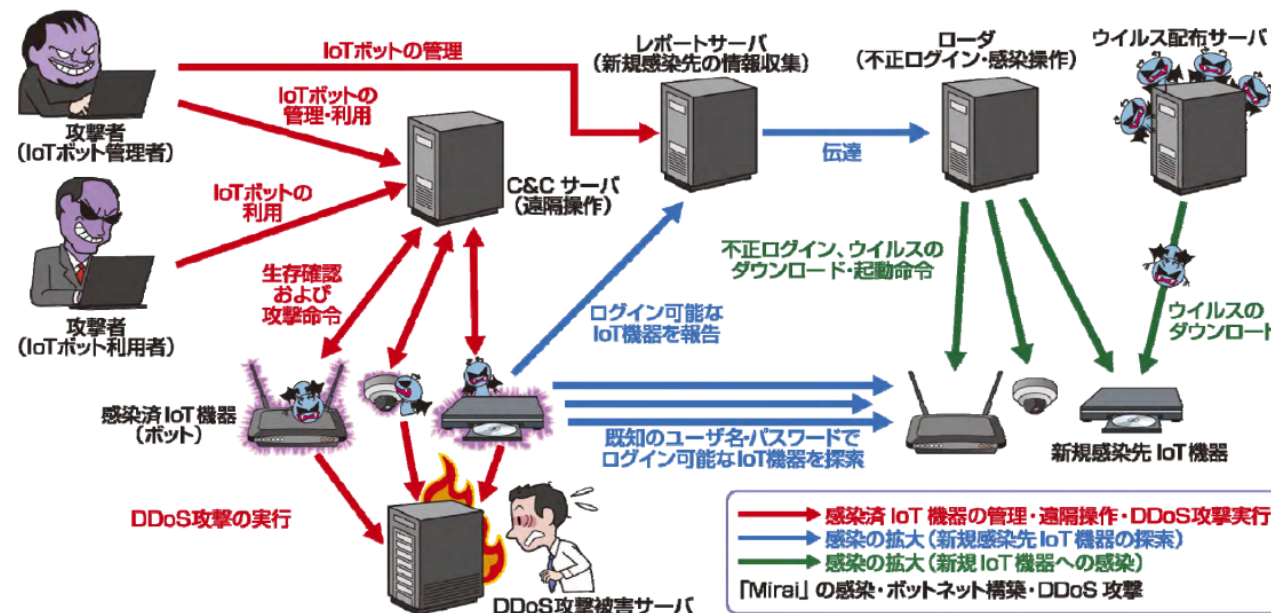
- IoT機器の脆弱性を悪用して感染を広げ、C&Cサーバーからの指令を受けて攻撃する手法
- 分類 2 に該当
- 2016年に確認された「Mirai」というマルウェアは、工場出荷時の脆弱なパスワードが設定されたIPカメラなどのIoT機器にログインを施工して感染を拡大したのち、C&Cサーバーからの指令を受けて攻撃

<https://www.ipa.go.jp/files/000059579.pdf>

IoTにおける脅威の事例

「Mirai」の主な挙動(感染・ボットネット構築・DDoS攻撃)とは？

IPA



IoT機器を悪用したDDoS攻撃 対策

- 製品出荷後に不要となる管理機能は無効化した上で出荷
- 製品出荷後も一部必要となる管理機能は無効化手段を提供し、説明書等に明記して利用者に周知徹底
- 初期パスワードを変更可能としセキュアなパスワードに変更すべきであると説明書等に明記して利用者に周知徹底
- 動作上問題無ければルータ経由でネットワークに接続し、ルータにて不正通知をブロック
- ネットワーク接続前、初期パスワードをセキュアなものに変更
- Firewall/IPSの導入

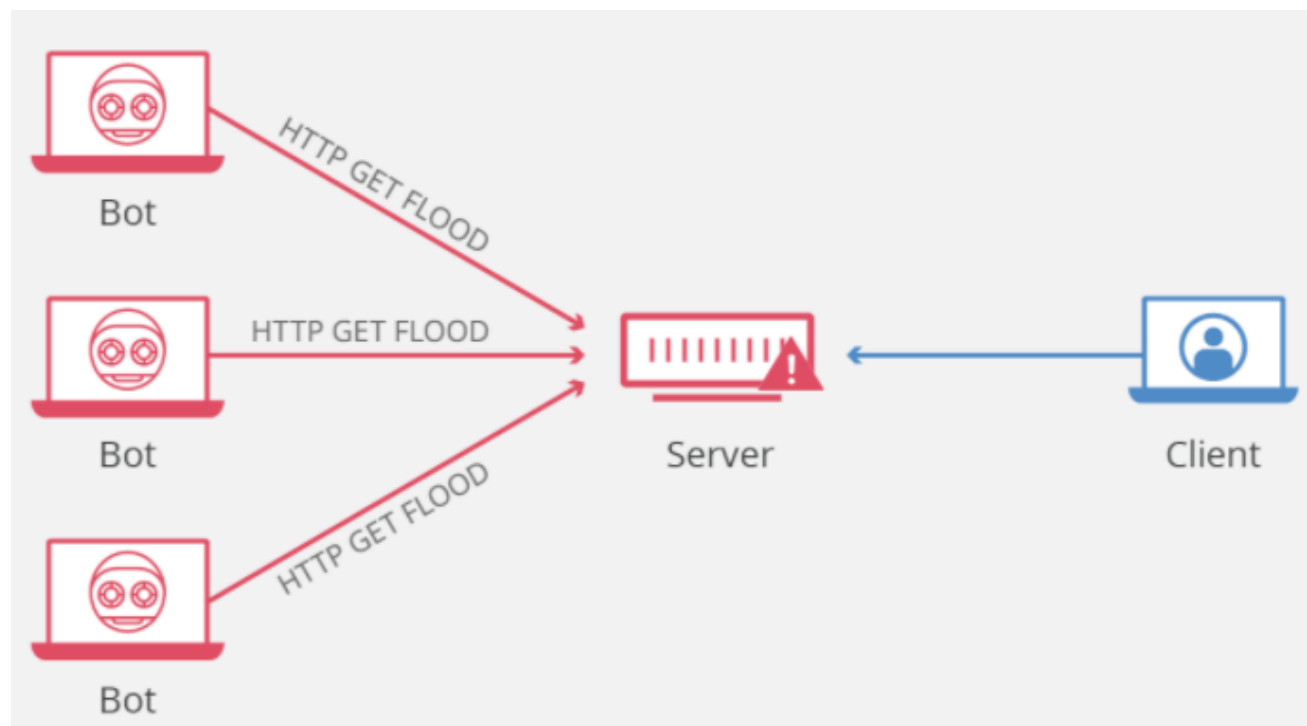
HTTP GET/POST Flood 攻撃

DoS
(Denial of Service)
攻撃とは？

1. CPUやメモリなどのシステムリソースを過負荷状態、又はオーバーフロー状態にする
2. 大量のパケットを送りつけネットワークの帯域を溢れさせる
3. ホストのセキュリティホールをついてOSや特定のアプリケーションを異常終了させる

- 分類 1 or 2 に該当
- GET
 - 複数のコンピュータが連携して、ターゲットから画像、ファイル、またはその他の資産に対する複数のリクエストを送信
 - ターゲットに着信リクエストと応答が殺到すると正当なトラフィック送信元からの追加リクエストに対してサービス拒否が発生
- POST
 - フォーム(POST)を受け取った際、多くの場合はデータベースに保存
 - フォームデータを処理し、必要なデータベースコマンドを実行するプロセスはPOSTリクエストを送信するために必要な処理能力と帯域幅の量に対して処理が多い
 - これを利用してサービス拒否をするまで多くのPOSTリクエストをターゲットに直接送信して、リソースを消費

<https://www.cloudflare.com/ja-jp/learning/ddos/http-flood-ddos-attack/>



HTTP GET/POST Flood 攻撃 対策

- Captchaテストのようにリクエストをするコンピューターがbotかどうかをテスト
- WAFの導入
- 悪意あるトラフィックを追跡して選択的にブロックするためのIP評価データベースの管理
- エンジニアによるオンザフライ分析
- ホストを冗長構成にするとともにロードバランサを用いた負荷分散
- Firewall/IPSの導入

Slow HTTP DoS 攻撃

DoS
(Denial of Service)
攻撃とは？

1. CPUやメモリなどのシステムリソースを過負荷状態、又はオーバーフロー状態にする
2. 大量のパケットを送りつけネットワークの帯域を溢れさせる
3. ホストのセキュリティホールについてOSや特定のアプリケーションを異常終了させる

- 攻撃者はターゲットに対してHTTPのコネクションを切断されないように維持しながらウェブサーバーに断片的なリクエストを連続的に送信
- これにより要求を完了することができず、コネクションが閉じられない上リソースが消費
- 結果、ウェブサーバーのリソースを攻撃者が消費し続けることで、ウェブサーバーはサービスの提供不可
- 分類 1 or 2

<https://siteguard.jp-secure.com/blog/what-is-slowloris-attack>

Slow HTTP DoS 攻撃 対策

- 接続に対するタイムアウトの設定
- 攻撃に対する対策モジュールの追加
- リバースプロキシの設置
- WAFの導入
- Firewall/IPSの導入

Stream Flood 攻撃

DoS
(Denial of Service)
攻撃とは？

1. CPUやメモリなどのシステムリソースを過負荷状態、又はオーバーフロー状態にする
2. 大量のパケットを送りつけネットワークの帯域を溢れさせる
3. ホストのセキュリティホールをついてOSや特定のアプリケーションを異常終了させる

- スマホなどのデータ通信として利用されているパケット通信を利用した攻撃手法
- 偽のIPアドレスやポート、RST(強制切断)フラグが設定されたパケットを大量に送りつけることでネットワークやサーバーに大きな負担
- 分類 1 or 2 に該当

https://www.amiya.co.jp/column/denial_of_service_attack_20200511.html

Stream Flood 攻撃 対策

- 十分な帯域を持つネットワークを使用
- 公開サーバーおよび経路上のネットワーク機器の処理能力を増強
- 発信元アドレスが明らかに偽装されているパケットやブロードキャスト宛パケットをファイアーウォールで遮断
- Firewall/IPSの導入

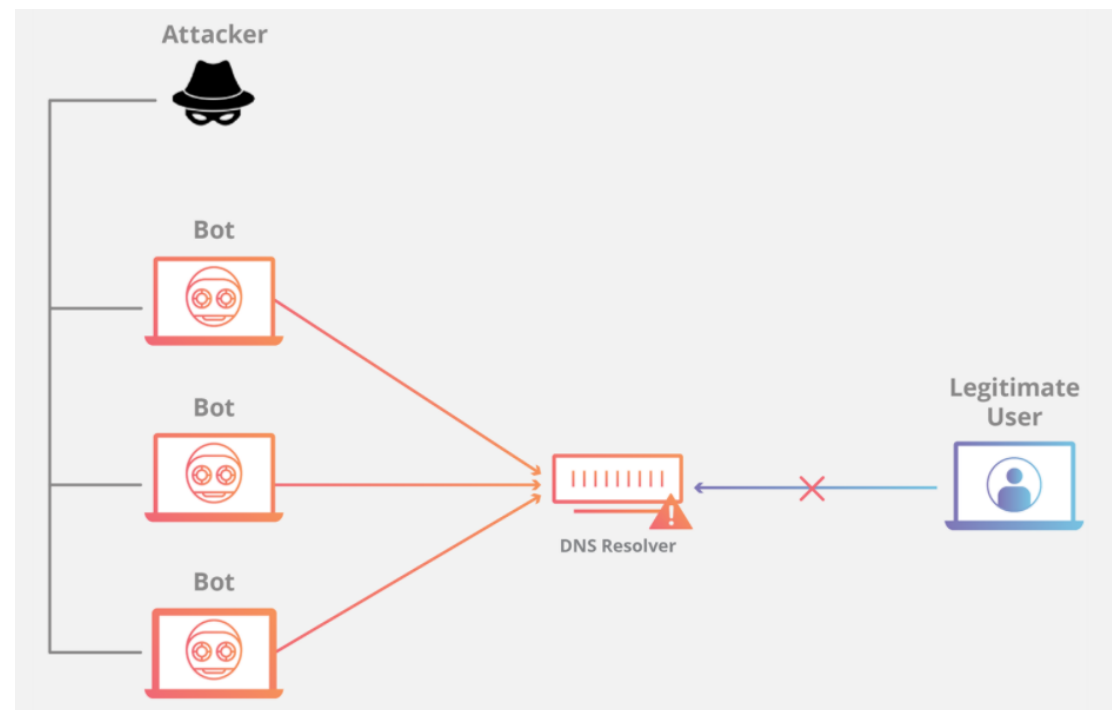
DNS Flood 攻撃

- 攻撃者がターゲットのDNSサーバーをフラッディングして、そのDNSサーバーが行う名前解決を妨害する攻撃
- これにより正当なトラフィックに 응답するwebサイト、API、webアプリケーションの機能を侵害
- 分類 2

<https://www.cloudflare.com/ja-jp/learning/ddos/dns-flood-ddos-attack/>

DoS
(Denial of Service)
攻撃とは？

1. CPUやメモリなどのシステムリソースを過負荷状態、又はオーバーフロー状態にする
2. 大量のパケットを送りつけネットワークの帯域を溢れさせる
3. ホストのセキュリティホールについてOSや特定のアプリケーションを異常終了させる



DNS Flood 攻撃 対策

- リアルタイムで攻撃トラフィックを監視、吸収、およびブロックできる非常に大規模で高度に分散したDNSシステムの使用
- Firewall/IPSの導入

<https://www.cloudflare.com/ja-jp/learning/ddos/dns-flood-ddos-attack/>

Ping of Death

DoS (Denial of Service) 攻撃とは？

1. CPUやメモリなどのシステムリソースを過負荷状態、又はオーバーフロー状態にする
2. 大量のパケットを送りつけネットワークの帯域を溢れさせる
3. ホストのセキュリティホールについてOSや特定のアプリケーションを異常終了させる

- イーサネット技術を悪用した攻撃
- イーサネットにおいて5バイト未満のパケットに分割されて通信を行なっているところに対し、規格外もしくは悪意あるパケットを送りつけることで例外処理を行わせてサーバーをダウン
- 分類3に該当
- オリジナルのPing of Deathはほぼ絶滅している
- 1998年以降に製造されたデバイスは概ね保護
- Microsoft WindowのIPv6パケットに対する攻撃が発見されたが、2013年半ばにパッチが発行済み

https://www.amiya.co.jp/column/denial_of_service_attack_20200511.html

<https://www.cloudflare.com/ja-jp/learning/ddos/ping-of-death-ddos-attack/>

Ping of Death 対策

- ターゲットに到達する前に不正なパケットを破棄
- Firewall/IPSの導入

Land

- 送信元と攻撃対象の宛先のIPアドレスと同じにすることで接続要求のパケットを双方で送受信し合う状態になることで無限ループが発生し、負荷がかかることでシステムは応答不可
- 分類 3 に該当

DoS
(Denial of Service)
攻撃とは？

1. CPUやメモリなどのシステムリソースを過負荷状態、又はオーバーフロー状態にする
2. 大量のパケットを送りつけネットワークの帯域を溢れさせる
3. ホストのセキュリティホールをついてOSや特定のアプリケーションを異常終了させる

https://www.amiya.co.jp/column/denial_of_service_attack_20200511.html

Land 対策

- IPパケットフィルタの設定
- Firewall/IPSの導入

<http://www.rtpro.yamaha.co.jp/RT/FAQ/IP-Filter/land-attack-filter.html>

まとめ

- インフラの設計をするときは
DoS攻撃への対策を意識しよう！

参考文献

- SYNフラッド攻撃 | CLOUDFLARE
<https://www.cloudflare.com/ja-jp/learning/ddos/syn-flood-ddos-attack/>
- SYN cookies | weblio辞書
<https://www.weblio.jp/wkpja/content/SYN+cookies SYN+cookies%E3%81%AE%E6%A6%82%E8%A6%81>
- UDPフラッド攻撃 | CLOUDFLARE
<https://www.cloudflare.com/ja-jp/learning/ddos/udp-flood-ddos-attack/>
- Ping – 概要 | Wikipedia
<https://ja.wikipedia.org/wiki/Ping>
- ICMP攻撃 | マルウェア情報局
https://eset-info.canon-its.jp/malware_info/term/detail/00001.html
- smurf攻撃とping flood攻撃の違い | yahoo知恵袋
https://detail.chiebukuro.yahoo.co.jp/qa/question_detail/q12115076242
- DDoS攻撃の主な攻撃手法8つの特徴をまとめてみた | CyberSecurityTIMES
<https://www.shadan-kun.com/blog/measure/1426/#07>
- DoS/DDoS攻撃について | AndMem
<https://andmem.blogspot.com/2014/02/dosattack.html>
- DDoS攻撃とは？ | CLOUDFLARE
<https://www.cloudflare.com/ja-jp/learning/ddos/what-is-a-ddos-attack/>
- DDoS攻撃とは？意味と読み方、対策方法 | NTT Communications
https://www.ntt.com/business/services/network/internet-connect/ocn-business/bocn/knowledge/archive_18.html
- 分散サービス拒否(DDoS)攻撃を仕掛けるDNS amp とは？ | atmarkit
<https://www.atmarkit.co.jp/ait/articles/0608/26/news015.html>

参考文献

- ACKフラッドDDoS攻撃とは？ | DDoS攻撃の種類 | CLOUDFLARE
<https://www.cloudflare.com/ja-jp/learning/ddos/what-is-an-ack-flood/>
- CDNとは？ | CLOUDFLARE
<https://www.cloudflare.com/ja-jp/learning/cdn/what-is-a-cdn/>
- CDNってそもそも何？なんかサーバの負荷が下がるって聞いたんだけど！～Web制作/運営の幅が広がるCDNを知ろう第1回～ | さくらのナレッジ
<https://knowledge.sakura.ad.jp/19191/>
- 過去最大の300Gbps超のDDoS攻撃に悪用されたDNSの「オープンリゾルバー」とは | INTERNETWatch
<https://internet.watch.impress.co.jp/docs/interview/597628.html>
- 顕在化したIoTのセキュリティ脅威とその対策～脅威分析と対策検討、脆弱性対策の重要性～ | 独立行政法人情報処理推進機構
<https://www.ipa.go.jp/files/000059579.pdf>
- HTTPフラッド攻撃 | CLOUDFLARE
<https://www.cloudflare.com/ja-jp/learning/ddos/http-flood-ddos-attack/>
- Slowloris攻撃とはウェブサーバーの脆弱性対策に有効な実践的対策 | SITEGUARD
<https://siteguard.jp-secure.com/blog/what-is-slowloris-attack>
- DoS・DDoS攻撃とは？攻撃を防ぐ対策について解説。最新の動向についても | AMIYA
https://www.amiya.co.jp/column/denial_of_service_attack_20200511.html
- Land攻撃に対処するフィルタを教えてください。 | RTシリーズのIPパケット・フィルタに関するFAQ
<http://www.rtpro.yamaha.co.jp/RT/FAQ/IP-Filter/land-attack-filter.html>
- Ping of Death DDoS攻撃 | CLOUDFLARE
<https://www.cloudflare.com/ja-jp/learning/ddos/ping-of-death-ddos-attack/>
- DNSフラッドとは？ | DNSフラッドDDoS攻撃 | CLOUDFLARE
<https://www.cloudflare.com/ja-jp/learning/ddos/dns-flood-ddos-attack/>
- 【図解】CDNとは？仕組みと技術の基礎知識 | カゴヤのサーバー研究室
<https://www.kagoya.jp/howto/network/cdn/>
- うかる！情報処理安全確保支援士2021