IIJ Internet Initiative Japan

資料2－4

サイバーセキュリティタスクフォース分科会

ISPにおけるDDoS攻撃対策の現状

安全をあたりまえに
wizSafe

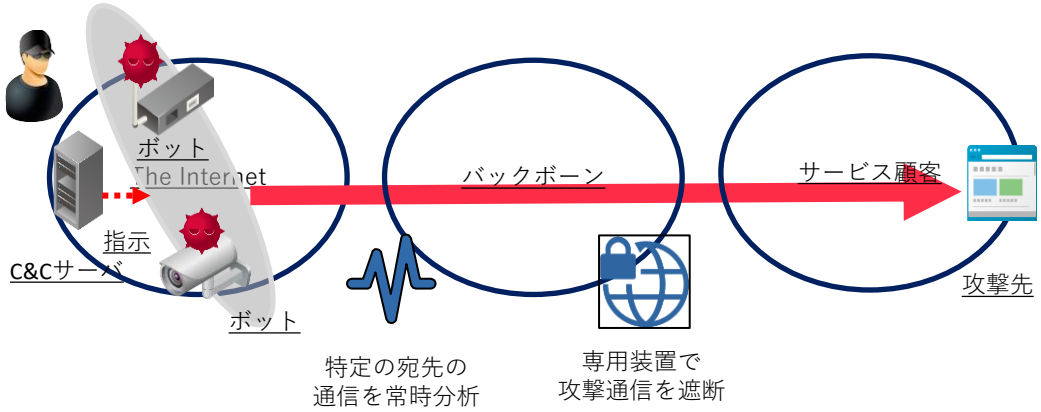
2023/02/16

株式会社インターネットイニシアティブ
セキュリティ本部
齋藤　衛

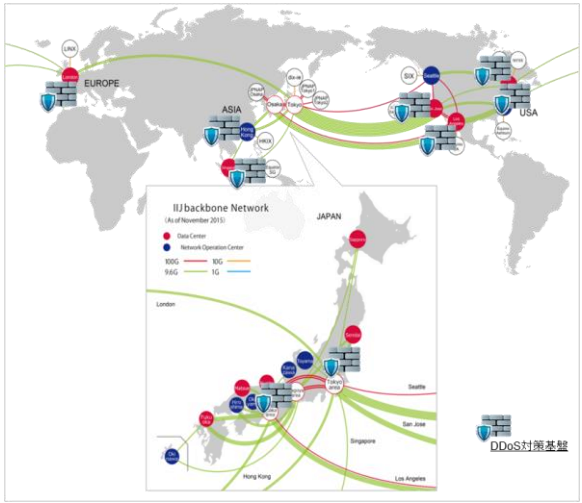
Copyright Internet Initiative Japan Inc.

情報通信ネットワークに対するサイバー攻撃について

- 大量通信が外部から到着する（inboundの）サイバー攻撃への対策については、約20年間の対応実績があるが、その期間において、攻撃は回数、規模ともに増加傾向が続いている。このため、通信設備もしくは顧客設備に対する攻撃については、その検知の仕組みと対策装置の導入を積極的に実施し、現在では他のISPとの接続点すべてにおいて異常検知と対策が実施できるようになっている。



ISPにおけるInboundのDDoS対策の実施

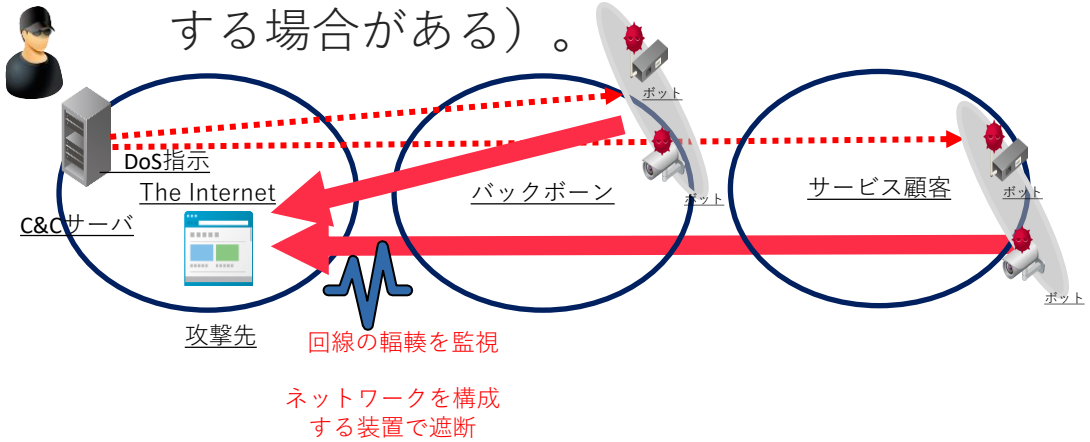


IIJにおけるDDoS対策装置の設置状況

Copyright Internet Initiative Japan Inc.

情報通信ネットワークに対するサイバー攻撃について

- 一方で、自社網内や顧客から他のネットワークを攻撃するような(outboundの)大量性を伴う通信についても、頻度や規模が増している。今日では、自社網を安定的に運用するために、このような攻撃に積極的に対応することが必要である。特に一昨年末より一部の監視カメラなどがボット化することが頻発し、100Gbpsを越える規模の攻撃が日常的に発生している（ボットが自社網内、顧客の設備、もしくはその両方に存在する場合がある）。



ISPにおけるOutboundのDDoS対策の実施

IIJにおけるOutbound攻撃対策の実施状況
（画面表示のみ）

Copyright Internet Initiative Japan Inc.

IIJでの対策

- **Inboundの攻撃の検出と対策**
  - 事前に保護すべき対象IPアドレス、ネットワークを決め常時通信を分析することで異常を検知、専用装置により攻撃の種類によって適切な対応を選び攻撃通信のみを止める。
- **Outboundの攻撃の検出と対策**
  - 攻撃は回線などの輻輳を検出するシステムで検出を行い、攻撃かどうかの判定および対応は自動化できておらず、人が介在して判断、実施している。
  - 攻撃通信への対策については、DDoS攻撃対策の専用装置ではなく、網を構成する装置で実施している（現状、機能的に専用装置は使えない）。
  - 攻撃元アドレスは多岐にわたり詐称されている場合もあるため、攻撃先アドレスで制御する場合が多い。この時、正常な通信を阻害する副作用が起こる可能性がある。また、攻撃先は時間により変化するので、この対策は一時対策となる場合も多い。
  - 攻撃元への対策
    - 攻撃元アドレスを利用する顧客に連絡し、対策を依頼することもあるが、大量性のある通信のみの情報だけでは状況の説明と対策の方法を伝えることが難しく、また、自社における通信にはあまり影響がみられないことなどを理由に対応してもらえない場合がある。
    - 攻撃元アドレスが顧客の顧客（顧客がISPなどの場合）である場合、顧客に対応を依頼することになるが、その際にも同様に対策に関する技術情報を必要とする場合がある。
  - 攻撃の通信量が特にひどい場合にはICT-ISAC Japanなどを通じて情報共有と他社の状況の確認を行う場合がある。

Copyright Internet Initiative Japan Inc.

その他の状況

- IIJではセキュリティ事業において、おとりホスト（honeypot）を運用しており、網内のボットネットの感染活動についてある程度把握している。しかしすべての検体を取得、解析できてはおらず、すべてのC&Cサーバを特定できてはいない。
- 他のISPで活動しているボットネットと自社網の中で活動しているボットネットは異なる可能性がある。
  - 外部組織から購入しているインテリジェンス情報やIoC情報などにボットネットのC&Cサーバと分類されているIPアドレスの情報が含まれていることがあるが、観測点が国外であることが多く、網内で活動しているボットネットとの適合率は低い。
- DNSフィルタリングでの対策
  - 網内で活動していることが明らかなボットネットのC&Cサーバについて、DNSフィルタリングでの通信抑止を試みたことがあるが、プログラム内にサーバ情報を内包していたり、外部DNSサーバの参照などにより迂回されてしまった。

C&Cサーバへの通信の阻害による対策への期待

- 一方でC&Cサーバへの通信を阻害することにより、比較的副作用の少ないDDoS攻撃対策となる可能性がある点に期待をしている。

Copyright Internet Initiative Japan Inc.

対策を進めるにあたっての課題

- **攻撃通信を破棄することでの対策について**
  - Outboundの大量通信を検出するための技術が十分でなく、攻撃かどうかの判定と対策に人手が介在しており、運用負荷が高い。
  - また対策技術もこなれておらず、攻撃先に関する通信の破棄だけでは副作用が発生するため、実際には輻輳が発生してから緊急避難または正当業務行為として対策を行うことになる。
- **攻撃元への対策について**
  - 端末での対策については、ISPではユーザが利用する端末に関する技術情報を持っていないことが多く、その場合適切な助言や指摘を実施できない。
- **C&Cサーバへの通信の遮断について**
  - C&Cサーバの情報があったとして、すぐに遮断できるとは限らない。最低限、他の通信を巻き込まないかといった副作用の有無などは確認すべきではないか。
  - 遮断期間はどのくらいと取るべきか検討が必要。
  - 対策に関する情報提供（影響を受けた顧客への開示）について検討が必要。
  - 予防的対策の是非については検討する必要がある。可能性は低いにしろ副作用がゼロではないためC&Cサーバの遮断は、大量通信を発生させたとわかっている場合のみ可能なのではないか。

Copyright Internet Initiative Japan Inc.

対策を進めるにあたっての課題(2)

- **攻撃の通信やC&Cサーバへの通信の遮断は恒久対策とはならない**
  - 大量通信そのものの遮断、C&Cサーバへの通信の遮断が実現できたとしてその効果は一時的なものであると予想できる。
    - PCのボットにおいても古くからC&Cサーバを動的に変更する仕組みを持っていることがわかっており、C&Cサーバへの通信の阻害は、他のC&Cサーバを割り当てられるまでの間有効である。
    - 脆弱性を持つIoTを放置することで、容易に他のボットネットの構築に悪用されてしまう可能性が高い。
  - IoTを勝手に悪用されてしまわないようにすることが恒久対策となる。
  - 一時対策から恒久対策につなげるための活動が必要で、このためにはマルウェアの情報、感染に用いられる脆弱性などの情報、感染してしまう機種などの特定と共有が必要である。

Copyright Internet Initiative Japan Inc.

課題の解決に向けて

- **攻撃元への対策の強化**
  - 対応の現場にて、機器や脆弱性、IoTボットに関する技術情報を参照できるようにできないか。ISP一社でそれを実施するのは困難であり、複数の組織でそれらの情報を積極的に集めて共有もしくは、公開するような仕組みを構築できるのではないか。
  - 特に顧客対応においては、状況を伝えるための第三者情報があった方が顧客を納得させやすい。IoTの脆弱性情報やIoTボットの種類、対策についてまとめて提示するような活動を、中立的な業界団体などで実施してほしい。
- **現状の大量通信を遮断による対策の強化**
  - 通信事業上の輻輳の検出や対策の技術について、他の事業者と共有や一緒に検討することができないか。
  - ICT-ISACに、個別攻撃の発生状況や攻撃規模の相場感、攻撃手法などの共有の仕組みはあるが、もっと活性化すべきである。
- **C&Cサーバへの通信の遮断に向けて**
  - 遮断の副作用を検討し、それを減らすために、遮断をしてよい状況について詳細に検討すべきである。遮断の前に対象C＆Cサーバの状況、自社網の中でのボットの活動状況、当該ボットネットによるDDoS攻撃の発生の有無などを確認し、遮断に直接的な効果があることを前提にした方がよいのではないか。
- **恒久対策に向けて**
  - 機器の情報、感染方法の情報、マルウェア（ボット）の情報、ボットネットのC&Cサーバの情報、攻撃の大量通信の発生の情報、すべてがそろわないと恒久対はならず、こうした情報を積極的に調査、共有する仕組みが必要である。特に装置の情報収集や、マルウェアの解析など負荷の高い作業について、個々のISPでは追い付いておらず、何らかの公的なサポートご検討いただけないか。またその共有の場としてNICTやICT-ISACなど協力を仰ぐのが適切なのではないか。

Copyright Internet Initiative Japan Inc.

wizSafe

安全をあたりまえに

http://www.iij.ad.jp/wizsafe/

Copyright Internet Initiative Japan Inc.