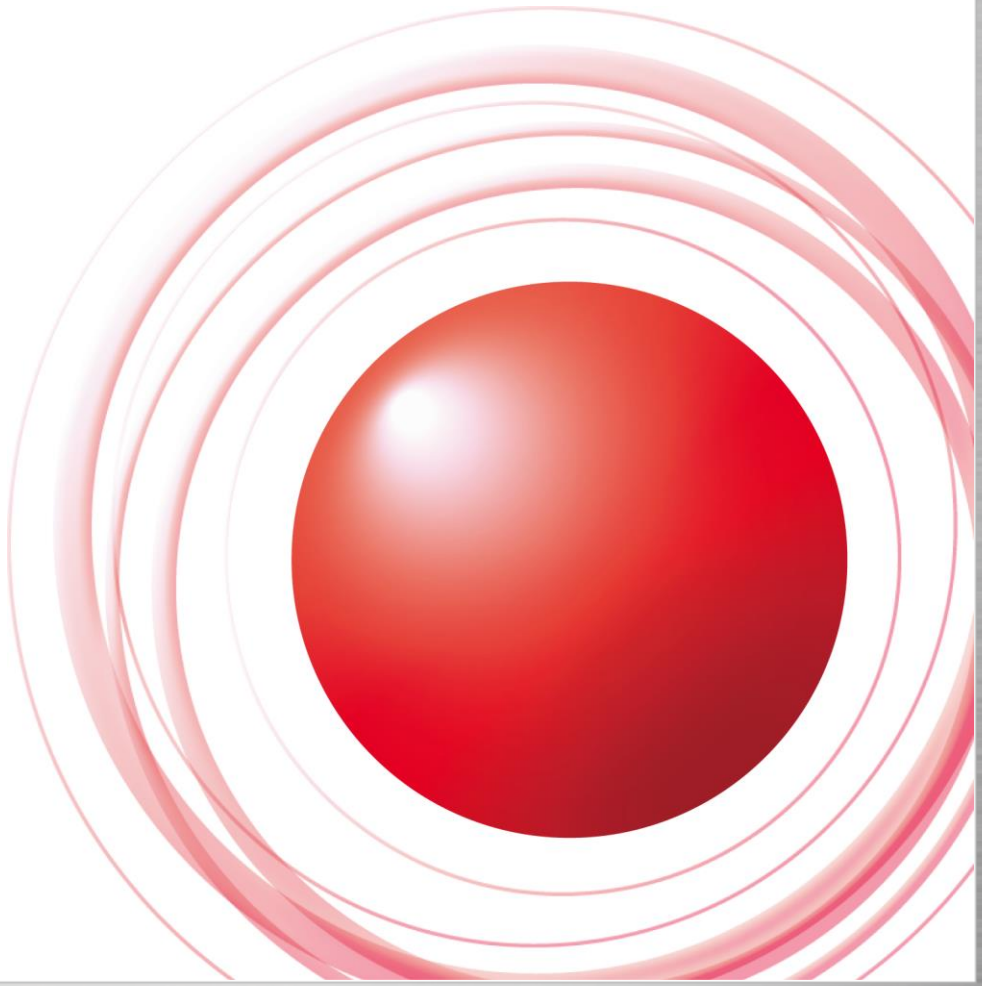
InternetWeek2014 S8: DDoS2014

DDoS攻撃の過去、現在、そして未来への提言

IIJ
Internet Initiative Japan



2014/11/19
株式会社インターネットイニシアティブ
サービスオペレーション本部　セキュリティ情報統括室
齋藤 衛

Ongoing Innovation

はじめに

このマークがついた資料はEyes Only です。

この資料には門外不出の秘密と、それなりの秘密が含まれいています。
状況を把握してもらうために見てもらいますが、このマークが掲示されたら以下を遵守してください。:

- 事前に許可した者以外の写真撮影禁止
- 事前に許可した者以外の録音録画禁止
- 他言無用、Tweet禁止
- この部屋を出たら忘れる
  (印象だけ記憶にとどめるのは可。数字などは忘れること)

DDoS攻撃の過去

DDoS攻撃の現在

未来への提言

DDoS攻撃年表

2000年前後　米国でのDDoS攻撃発生事例(Yahoo!, amazon,eBayなど)
(世界規模で発生するネットワークワームによる輻輳)
2003年　国内(IIJ顧客)初のDDoS攻撃事例
2004年　Antinnyウイルスにより ACCSに対して定期的に発生するDDoS攻撃状大量通信
2004年　サッカーAsiaCup2004。日本サッカー協会、スポンサー企業、官公庁、報道機関　などに対するDDoS攻撃。
2005年　中国や韓国からの、官公庁関連サイトや大手企業に対する同時多発的攻撃
DDoS攻撃の規模：国内1Gbps以下、国外6Gbps
2006年　DNS Open Resolverを悪用したDrDoSの発生（国内）
竹島の日に関連する攻撃
2007年　エストニアでのサイバー攻撃
企業に対する攻撃恐喝事件（国内）
2008年　韓国から2ちゃんねるに対する攻撃
グルジア紛争にともなう攻撃
北京オリンピックに関連する攻撃
2009年　韓国でマルウェアを使った米国および韓国国内に対する大規模DDoS攻撃

DDoS攻撃の過去

DDoS攻撃年表

2010年　中国からの9月18日前後の同時多発的攻撃
中東ジャスミン革命に関連してAnonymous台頭。以後頻繁にDDoS攻撃を起こす。
DDoS攻撃の規模：国内10Gbps以下、国外60Gbps

2011年　韓国3.3大乱
中国からの9月18日前後の同時多発的攻撃

2012年　中国からの9月18日前後の同時多発的攻撃
Anonymousによる#OpJapan
DDoS攻撃の規模：国内14Gbps以下、国外100Gbps

2013年　DNS DrDoS(国内)
迷惑メール対策団体Spamhauseに対してDNSによる大規模DrDoS攻撃
DDoS攻撃の規模：国内20Gbps以下、国外300Gbps

2014年　NTP DrDoS(国内)
ブラジルワールドカップ 2014。開催前に反対運動によるDDoS攻撃、改ざんなど。
SSDP DrDoS(国内)
DDoS攻撃の規模：国内100Gbps、国外400Gbps

DDoS攻撃の過去

DoS攻撃：大量の通信の発生方法

- 人海戦術
- DDoS攻撃ツール(多くホストに埋め込み、同時に動かすもの)
- DDoS攻撃機能を持つマルウェア
- ボットネット(指令に従い同時に多数が動作するマルウェア)
- DDoS攻撃ツール(1台で大量通信発生、IPアドレスの詐称)
- DDoS攻撃代行サイト
- ルータなどを踏み台にする手法(DrDoS)

DDoS攻撃代行サイトの例

DDoS攻撃ツールの例

DDoS攻撃の過去

DDoS攻撃への対策

2004年　AntinnyウイルスによりACCSに対して定期的に発生するDDoS攻撃状大量通信に対する国内ISPによる対策実験、共同対処実験(TelecomISAC Japan)

2005年　中国からの同時多発的攻撃を受け、大量通信等のガイドラインの内容検討開始

（日本流のDDoS対策兵器　さあや）

DDoS対策サービス開始(IIJ)

2006年　電気通信事業におけるサイバー攻撃対応演習(総務省)

ボットネット対策事業 Cyber Clean Center(CCC) (総務省、経産省)

2007年　電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン第一版

（「DDoS攻撃はもう脅威ではない」という風評）

2009年　通信分野横断演習(TelecomISAC Japan)

2011年　電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン第二版

DoS即応WG 発足(TelecomISAC Japan)

2012年　ルータ脆弱性問題WG発足(TelecomISAC Japan)

2013年　マルウェア対策プロジェクトACTIVE開始(総務省)

脆弱性保有ネットワークデバイス調査WG発足(TelecomISAC Japan)

電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会

2014年　電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン第三版

実践的サイバー攻撃防御演習(CYDER)(総務省)

DDoS攻撃の過去

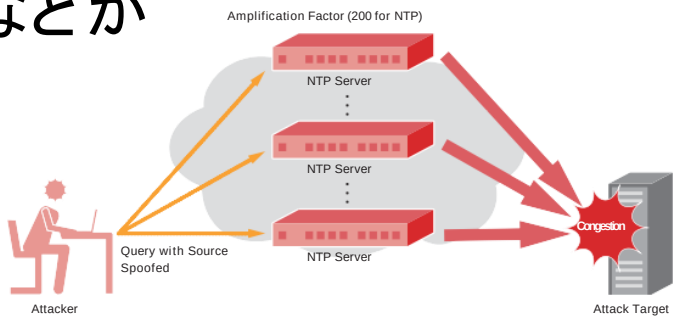
DDoS攻撃の現在

未来への提言

DDoS攻撃の現在

DrDoS(Distributed reflection Denial of Service)攻撃

- ホームルータなどの装置を踏み台にして、少量のデータ(命令)を送付し、多量の応答を得ることにより増幅された通信を、IPアドレスの詐称を用いて被害者に送付する。
- 通信プロトコルとしてDNS、NTP、SNMP、SSDPなどが悪用された実績があり、他のプロトコルも悪用の可能性が指摘されている。
- 背景として、脆弱性やデフォルト設定の問題、ユーザによる設定ミスなどを抱えるホームルータなどがインターネット上に多数存在する。



Internet Initiative Japan Inc., Internet Infrastructure Review (IIR) Vol.23, 1.4.2 DrDoS Attacks and Countermeasures (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol23_EN.pdf)

DDoS攻撃の現在

NTPによるDrDoSの特異性（NTPをぶっ放し続けている輩はだれか）

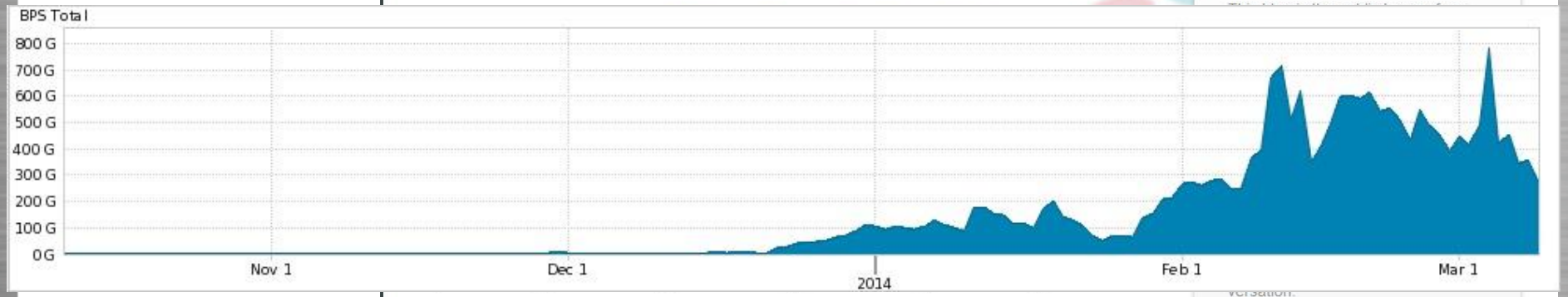
- AroborNetworks 800Gbps

NTP attacks continue – a quick look at traffic over the past few months

BY: CHRIS G. SELLERS - 03/10/2014

FEATURING

ARBORSERT
Security Engineering & Response Team



You can see that the observed traffic increase started at the end of 2013 and increased to nearly 800Gb/s in early March across the participants of Arbor Network's ATLAS system. Let us dive in a little closer.

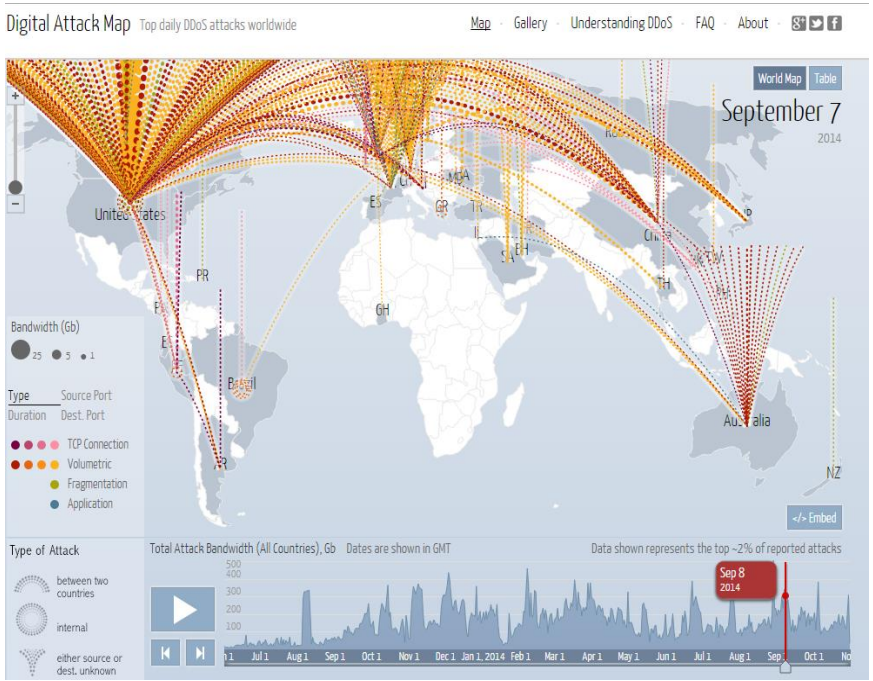
Arbor is a company with a history rooted in groundbreaking research at the University of Michigan a decade ago, and we remain researchers at heart. We hope you find our perspective interesting and we welcome your comments and feedback.

LIVE DATA FEED

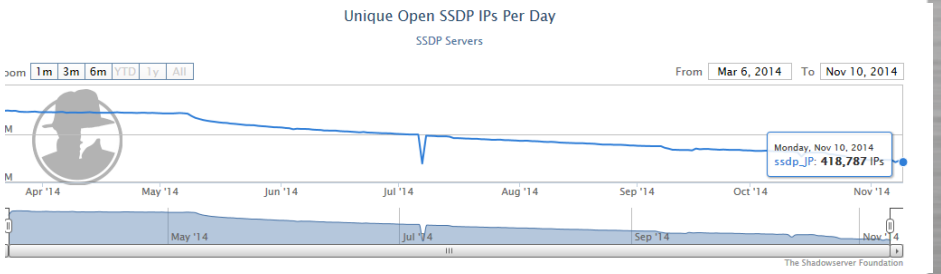
DDoS攻撃の現在

SSDPによるDrDoS

- 8/25-9/初旬　UPnP , SSDP (1900/udp)を踏み台とした攻撃が発生
  - Google の digital attack map で日本から米国に向け50Gbpsと表示された。が、実際にはそれほど深刻ではなかった。



http://www.digitalattackmap.com/



https://ssdpscan.shadowserver.org/stats/ssdp_jp.html

DDoS攻撃の現在

2014年のDDoS攻撃

- 2013年以後DNSやNTP、SSDPなどのDrDoSが多発している。
- 100Gbps+, 300Gbps,400Gbpsの規模が毎月のように発生

DDoS攻撃の現在

なぜ脆弱なホームルータが多いのか

- 機器の問題:
  - デフォルト設定がいいかげん。
  - 管理者認証がデフォルトでadmin/admin。
  - パスワードをplain textで保存。
  - 設定確認手法や通信記録の機能が未熟。

- 利用者の問題:
  - 利用者は家電のように扱い、情報通信機器として「運用」していない。
  - 利用状況を把握しない、設定を見直さない。対策ファームウェアをリリースしても使わない。

- この現状に、家庭内ネットワークに新しい装置がどんどんどんどん追加されている(状況を放置すれば悪化するのみ)。

DDoS攻撃の現在

電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会

- 2013年11月から2014年3月に実施された総務省研究会
  - 構成員は法律の研究家、法曹界、各通信業界団体(ガイドライン4団体＋データ通信協会/TelecomISAC Japan)
  - 技術内容を検討する技術WG
  - 各通信業界団体における検討WG

- 主目的は総務省マルウェア対策施策　ACTIVE の普及活動に阻害要因となる通信の秘密の取り扱いに関する検討。DDoS攻撃など他の事案についても一緒に検討。
- 5つの課題
  - ・ACTIVE 普及啓発(マルウェア配布サイトへのアクセス防止)
  - ・C&Cサーバで入手した情報を元にしたマルウェア感染駆除の拡大
  - ・新たなDDoS攻撃であるDNSAmp攻撃の防止
  - ・SMTP認証の情報を悪用した迷惑メールへの対処
  - ・攻撃の未然の防止と被害拡大の防止

DDoS攻撃の現在

電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会

- 「動的IPアドレス空間にある DNS open resolver を踏み台にするDNS amp攻撃については、攻撃を誘発する通信を止めてよいか。」
- 問題：通信の宛先ポートで破棄する行為は通信の秘密の窃用にあたる。
- 動的IPアドレスの空間に対するDNSのクエリの通信をブロックすることについて、宛先のIPアドレス及びポート番号を確認した結果がDNSAmp攻撃の防止以外の用途で利用しない場合に、正当業務行為として違法性が阻却される

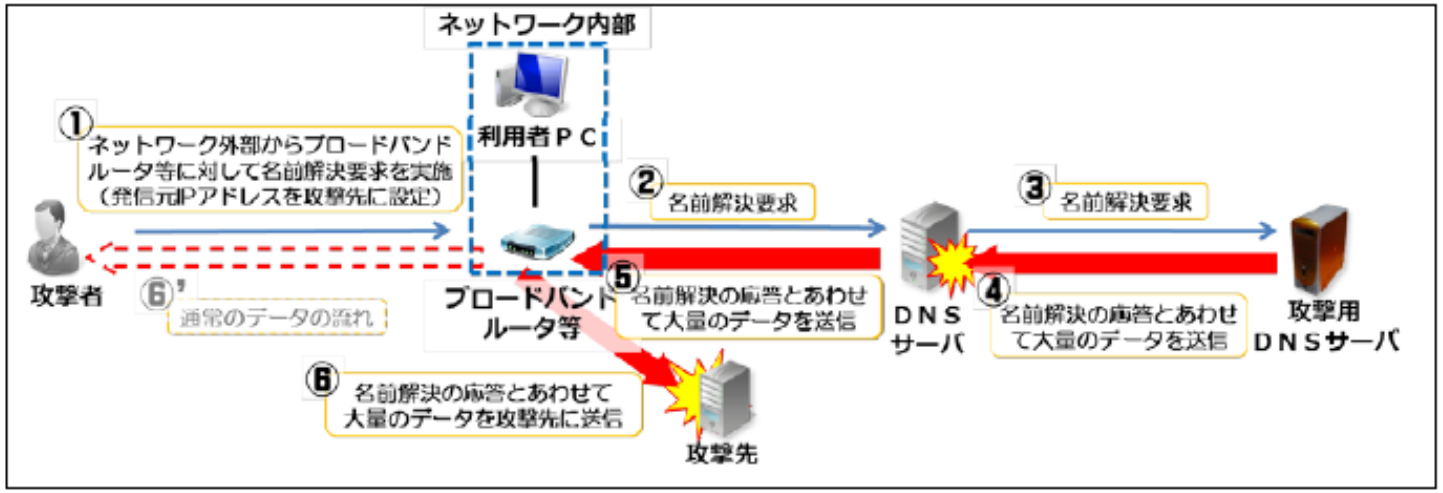


図６　DNSAmp 攻撃

DDoS攻撃の過去

DDoS攻撃の現在

未来への提言

未来への提言

未来への提言

スポーツイベントに関連して発生したテロ事件

1972年	ミュンヘンオリンピック開催中パレスチナ武装組織によりイスラエル選手団の2人を殺害、9人を人質に取った。
1987年	大韓航空機爆破事件。乗員乗客115人全員死亡。北朝鮮工作員金賢姫、金勝一による犯行。翌年開催のソウルオリンピック妨害のため。
1996年	アトランタオリンピック　爆弾テロ。元米兵による犯行。
1996年	イギリスのマンチェスターの中心街でトラックが爆発し約200人が負傷。サッカーUEFA欧州選手権ドイツ対ロシアの試合の直前。
2002年	マドリード・サッカースタジアム爆発事件。サッカースタジアム近辺車に仕掛けられた爆弾が2発爆発。17名負傷。レアル・マドリード対バルセロナの欧州チャンピオンズリーグ準決勝の数時間前。バスク地方独立主義者の犯行。
2008年	スリランカ、マラソン開始時に自爆テロ。15人が死亡、約100人が負傷。反政府勢力による犯行。
2009年	スリランカ、クリケットチームと審判員が移動中に武装集団に襲撃され、警察官6人と市民2人の計8人が死亡し、少なくとも選手6人が負傷。
2010年	ワールドカップ南アフリカ大会関連。ウガンダの首都カンパラにある飲食店で少なくとも3回の爆発。死者は50人以上。アルカイダとの関連報道も。
2013年	ボストンマラソン爆弾テロ。ゴール付近で2つの爆弾が爆発し、4名死亡、300人以上が負傷。チェチェン系の兄弟二人の犯行で宗教的背景。
2013年	ソチ冬季オリンピック。ソチから600キロ離れたヴォルゴグラードで、バスや駅舎が爆破される事件が続き、合わせて41名が死亡、120名が負傷。オリンピックとの関連が疑われ、厳重な警戒態勢が敷かれた。

近年のスポーツイベント・テロ事件、ナショナルジオグラフィック
http://www.nationalgeographic.co.jp/news/news_article.php?file_id=20130417004
オリンピックとテロ、防衛省防衛研究所
http://www.nids.go.jp/publication/briefing/pdf/2014/briefing_188.pdf

未来への提言

スポーツイベントに関連して発生したサイバー攻撃

2004年　サッカーAsiaCup2004。日本サッカー協会、スポンサー企業、官公庁、報道機関　などに対するDDoS攻撃。

2008年　北京オリンピック。オリンピック史上初、サイバー攻撃を想定した対策を実施。

2008年　スイス＋オーストリア、UEFA Euro 2008。公式サイトに対するDDoS攻撃など(通信インフラDeutche Telekom：数Gbps)。

2010年　南アフリカワールドカップ2010。Symantecが関連偽サイト詐欺メールなどのサイバー攻撃に対して警告。

2012年　ロンドンオリンピック。開会式直前に電力網を対象としたサイバーテロにより会場を停電させると予告（実際には発生せず）。

2012年　ポーランド＋ウクライナ、UEFA Euro 2012。国内Anonymousによる攻撃(通信インフラOrange + Ukrainian Telecom：120Gbps~240Gbps)。

2014年　ブラジルワールドカップ 2014。開催前に反対運動によるDDoS攻撃、改ざんなど。

未来への提言

AFC AsiaCup 2004

- 試合の応援としてのDDoS攻撃
- 日本チームの試合時にDDoS攻撃が発生
  - 政府関連サイト
  - 日本サッカー協会
  - スポンサー（スポーツ用品メーカ、清涼飲料水企業など）
  - 試合開始と同時に攻撃開始、試合終了と同時に攻撃も終了。
- 最終戦　2004年8月7日@北京 中国vs日本
- 他国の試合については攻撃の事実は表面化しておらず、サッカー試合における攻撃の意味よりも、日中間関係により発生したと考えるべき。

未来への提言

今日のスポーツイベントとサイバー攻撃

- 開催そのものへの反対、妨害行為
- 開催国、参加国への威力行為
- 試合の応援としての攻撃
- 賭けに関連するサイバー攻撃
- ニュース性の悪用
  - 便乗のお祭り的攻撃
  - サイバー犯罪への応用
    - 、ID窃取など目的として偽サイトにとるSEO poisoning、フィッシング、SMSやメール、SNSなどを悪用
    - チケット売買に関連する犯罪
  - 標的型攻撃などへの応用

未来への提言

未来予測（2014年9月における2020年予測）

2020年に想定すべき社会的影響の大きい変化

- パーソナルデータ、個人情報保護法改正
- 通信環境の変化（SIMロックフリー、通信契約時の本人確認の簡略化）
- ウエアラブル〇〇の流行と、個人活動にかかわる情報の常時電子化
- 個人もしくは企業にかかわる情報保存と処理の分散化（より広範なクラウド利用）
- BMI/BCI
- **IoT全盛時代**
- シンギュラリティ

未来への提言

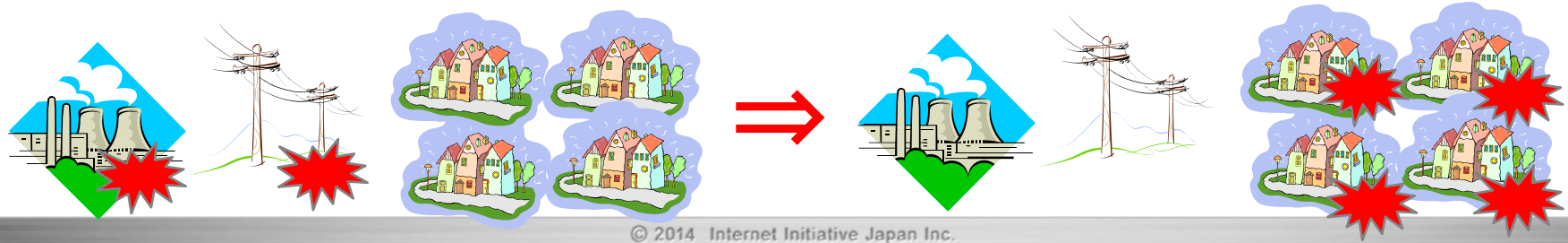
IoT全盛時代

- IoTの利用分野
  - オフィスビル、エネルギー産業、家庭、健康、工業全般、小売、治安、ICT分野など
  - その一部は重要インフラ事業
- 2014年のIoT装置
  - 個人を取り巻くもの
    - スマートフォン、タブレット、ヘルスメータ、眼鏡、時計、車など
  - 家庭に存在するもの
    - スマート家電、スマートメータ、HEMS、スマートトイレなど
  - オフィスに存在するもの
    - 照明、空調、入退室管理、監視カメラなど
  - 公共の場所に存在するもの
    - デジタルサイネージ、自動販売機、監視カメラなど

未来への提言

新しいサイバーテロ

- 重要インフラ分野で利用するIoT装置の誤動作、乗っ取り、動作停止
  - 家電の誤動作から火災など。
  - 電気ガス水道など生活インフラに対する影響。
    ⇒ IoT装置はサイバーテロを引き起こす可能性がある。
- IoT全盛時代のサイバーテロ
  - 発電所や送電網を機能させなくするのが従来のテロの想定。
  - 受電する家庭や企業の機器を機能不全にすることでも同じ被害を与えることができる。
  - 機能不全（電気は来ているが電圧が不安定）も想定。



未来への提言

IoT全盛時代への提言（通信事業者向け）

- IoT全盛時代は重要インフラのサービスが個人利用者に届く最後の切片が、通信に乗っかってくることに他ならない。

- IoT全盛時代を迎えるならば、通信はより頑健に、より高機能になっていなければ、社会全体が脆弱となる。

- 一方で我々はホームルータのセキュリティも確保できていない。

- 通信はもっと頑健にならなきゃ！

未来への提言

将来の大規模DDoS攻撃の抑制のためにISPがやるべきこと

- 研究会、ガイドライン
  - DNS以外のプロトコルに関するDrDoS対策の検討
  - 国内犯（自社網の中からの攻撃）に関する検出、対処の仕組み
- より詳細な実態調査
  - 法人環境やモバイル環境に関する調査
  - モバイル機器の脆弱性調査
  - IoT機器の脆弱性調査
- ユーザ環境の正常化
  - 脆弱なユーザ環境の把握
  - 本人特定と対処
- ISP間の連携、協調の強化

まとめ

- DDoS攻撃の過去
- DDoS攻撃の現在
- 未来への提言

IIJ Internet Initiative Japan

ご清聴ありがとうございました

お問い合わせ先　IIJインフォメーションセンター
TEL：03-5205-4466（9：30～17：30 土/日/祝日除く）
info@iij.ad.jp
http://www.iij.ad.jp/

Ongoing Innovation