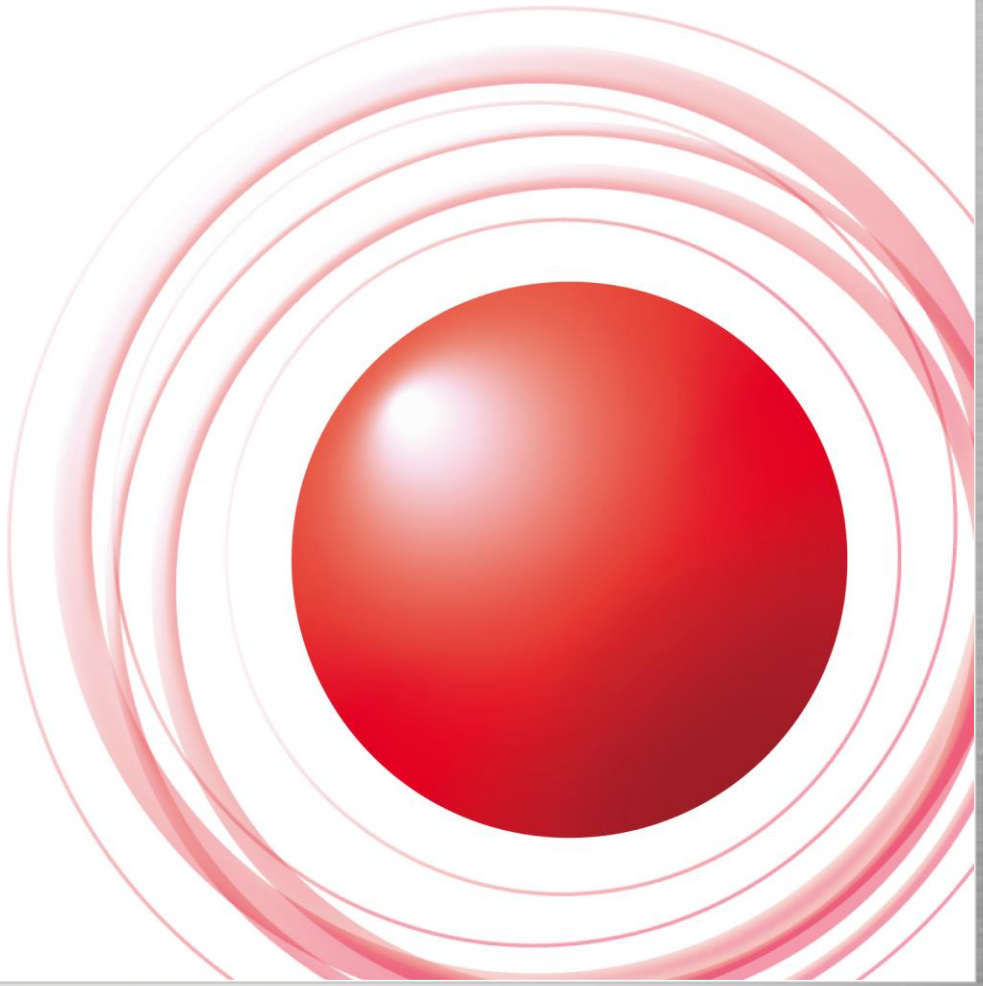
IIJ Technical WEEK 2015

セキュリティ動向2015

IIJ
Internet Initiative Japan



2015年11月12日
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

DDoS攻撃

PUA

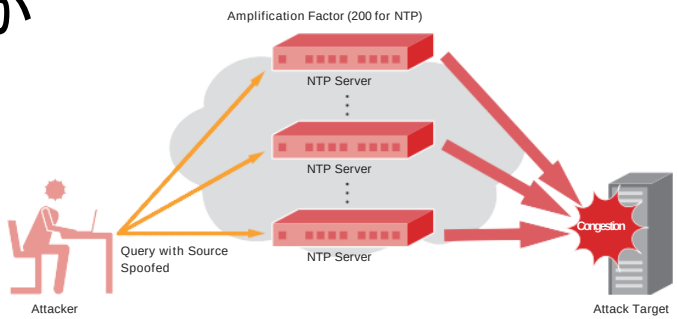
標的型攻撃

新しい対策技術の検討

DDoS攻撃

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。

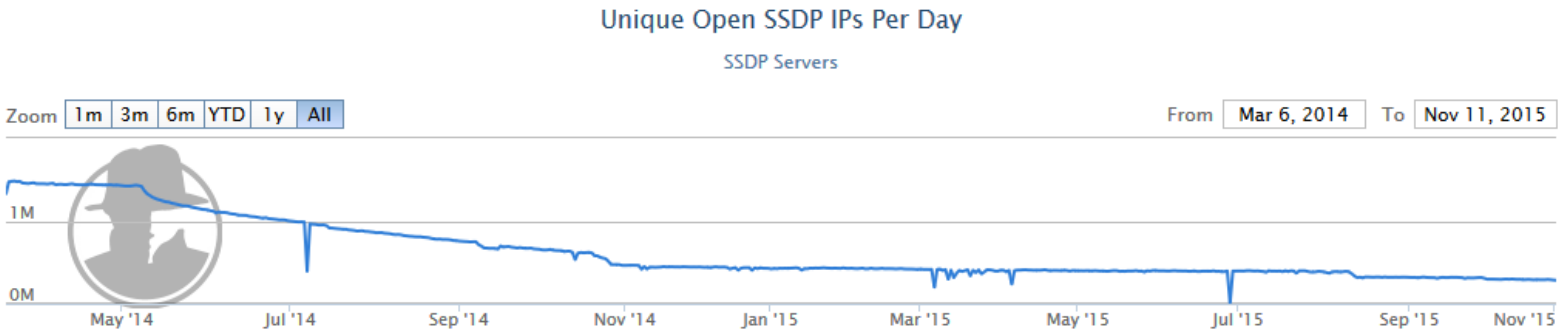


Internet Initiative Japan Inc., Internet Infrastructure Review (IIR) Vol.23, 1.4.2 DrDoS Attacks and Countermeasures (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol23_EN.pdf)

DDoS攻撃

DrDoSに加担するホームルータの状況

- ホームルータの問題による脅威
  - ホームルータの設定が変更され、通信を操作される。
  - ホームルータの接続情報（ISPのIDとパスワード）が盗まれて悪用される。
  - DrDoSなどの踏み台として悪用される。
- ホームルータの脆弱性は認知され、国内メーカやISPによる対策の努力が行われている。
- 結果として国内ではDrDoSの踏み台となるホームルータの数は減少傾向にある。
- しかし、国外においてはまだまだ対策が進んでいない（本年発生したある攻撃では99%が国外の踏み台を利用）。



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

DDoS攻撃

DD4BC(DDoS for Bitcoin)

- 匿名の何者かによる恐喝事件
  - DDoS攻撃を実施
  - 脅迫状で100Bitcoin支払え
- Twitter等での予告（凍結済）
- 昨年から他国活動
- 2015年5～7月に国内被害
  - 最初の攻撃で10Gbps-40Gbpsの規模
  - 1時間程度継続
  - 国内では金融機関以外での被害も

http://cointelegraph.com/news/113499/notorious-hacker-group-involved-in-excoin-theft-owner-accuses-ccedk-of-withholding-info

Or just google “DD4BC” and you will find more info.

So, it’s your turn!

All <redacted> sites are going under attack unless you pay 100 Bitcoin.

Pay to 1NbhLM43duL2J2tBX2qQWBojEm5fNSoMEp

Please note that it will not be easy to mitigate our attack, because
our current UDP flood power is 400-500 Gbps, so don't even bother.

Right now we are running small demonstrative attack just on your
<redacted>
Don't worry it will stop in 1 hour.
It's just to prove that we are serious.

We are aware that you probably don't have 100 BTC at the moment, so we
are giving you 24 hours to get it and pay us.

It's easy to get BTC from Webmoney. Just exchange WMZ to WMX and make
withdrawal request to our BTC address at
https://wmx.wmtransfer.com/en-US/Home/Withdraw#

Or check this for best exchanger: http://howtobuybitcoins.info/

Current price of 1 BTC is about 220 USD.

IMPORTANT: You don’t even have to reply. Just pay 100 BTC to
1NbhLM43duL2J2tBX2qQWBojEm5fNSoMEp – we will know it’s you and you

DD4BCによる脅迫状（抜粋）
https://community.akamai.com/docs/DOC-1894より

- おそらく素人の個人もしくは集団による行為で、400Gbpsなどの破壊的な攻撃能力はない模様。しかし10Gbps～40Gbpsでも十分な迷惑行為となる。

DDoS攻撃

Armada Collective

- DD4BCのようにDDoS攻撃に伴って恐喝を行う事件
  - 10月に国内事案があった（とされる：未確認）。
  - 11月に入り、複数のメールサービス事業者、ホスティング事業者などを攻撃
- protonMail事件
  - 100Gbpsにも及ぶ攻撃が発生
  - 20BTC(6,000USD)支払うも、攻撃は継続（6日間）。

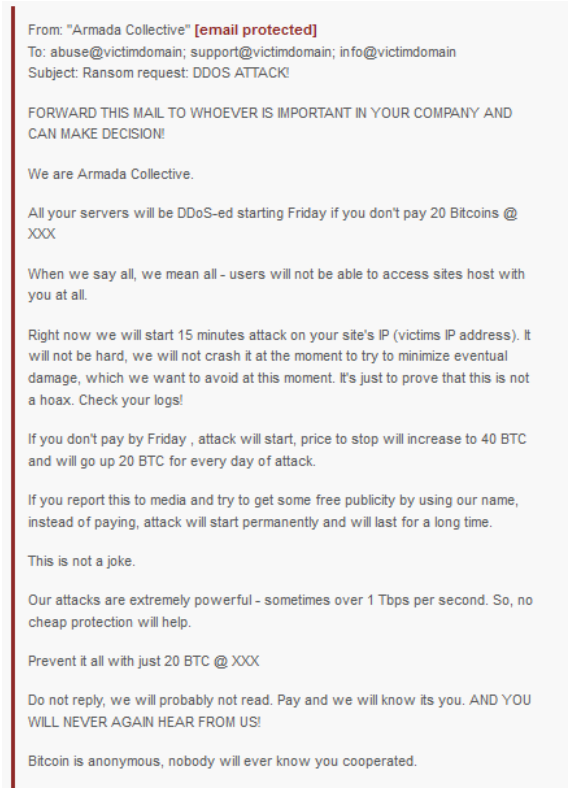

ProtonMail

ProtonMail Statement about the DDOS Attack

As many of you know, ProtonMail came under sustained DDOS attack starting on November 3rd, 2015. At the current moment, we are not under attack and have been able to restore services, but we may come under attack again.

We are currently working with solution providers to find a way to mitigate this attack, however, it is quite unprecedented in size and scope so unfortunately finding a working solution is not easy. Because of the sophistication of this attack, we will also need to resort to quite expensive solutions which will burden our finances. It is for this reason that we are also collecting donations for a ProtonMail defense fund.

https://protonmaildotcom.wordpress.com/2015/11/05/protonmail-statement-about-the-ddos-attack/


From: "Armada Collective"
To: abuse@victimdomain; support@victimdomain; info@victimdomain
Subject: Ransom request: DDOS ATTACK!

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

All your servers will be DDoS-ed starting Friday if you don't pay 20 Bitcoins @ XXX

When we say all, we mean all - users will not be able to access sites host with you at all.

Right now we will start 15 minutes attack on your site's IP (victims IP address). It will not be hard, we will not crash it at the moment to try to minimize eventual damage, which we want to avoid at this moment. It's just to prove that this is not a hoax. Check your logs!

If you don't pay by Friday , attack will start, price to stop will increase to 40 BTC and will go up 20 BTC for every day of attack.

If you report this to media and try to get some free publicity by using our name, instead of paying, attack will start permanently and will last for a long time.

This is not a joke.

Our attacks are extremely powerful - sometimes over 1 Tbps per second. So, no cheap protection will help.

Prevent it all with just 20 BTC @ XXX

Do not reply, we will probably not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.

https://grahamcluley.com/2015/11/armada-collective-ddos/

DDoS攻撃

Anonymous　#OpKillingBay

- 2013年11月から和歌山県の太地町のイルカ漁への抗議活動
- Anonymousを自称する@_**RektFaggot_**が10月5日の太地町を皮切りに複数のHPへの攻撃を行う。

  The JapanNews(読売新聞英語版)、成田国際空港、中部国際空港、日本政府観光局、ぷらら、太地漁協、捕鯨協会、高野町、九度山町、運輸労連、ASCII、東洋経済新報社、南知多ビーチランド、環境水族館アクアマリンふくしま、あわしまマリンパーク、南海電鉄、毎日新聞、北海道マリンパーク、しながわ水族館、くじらの博物館、鳥羽水族館、アイスランドのISP(siminn)、、日本経済新聞社
- 特定の企業からの情報漏えい
- 観測された最大級の攻撃
  - 5GbpsUDPリフレクション攻撃10時間

DDoS攻撃

PUA

標的型攻撃

新しい対策技術の検討

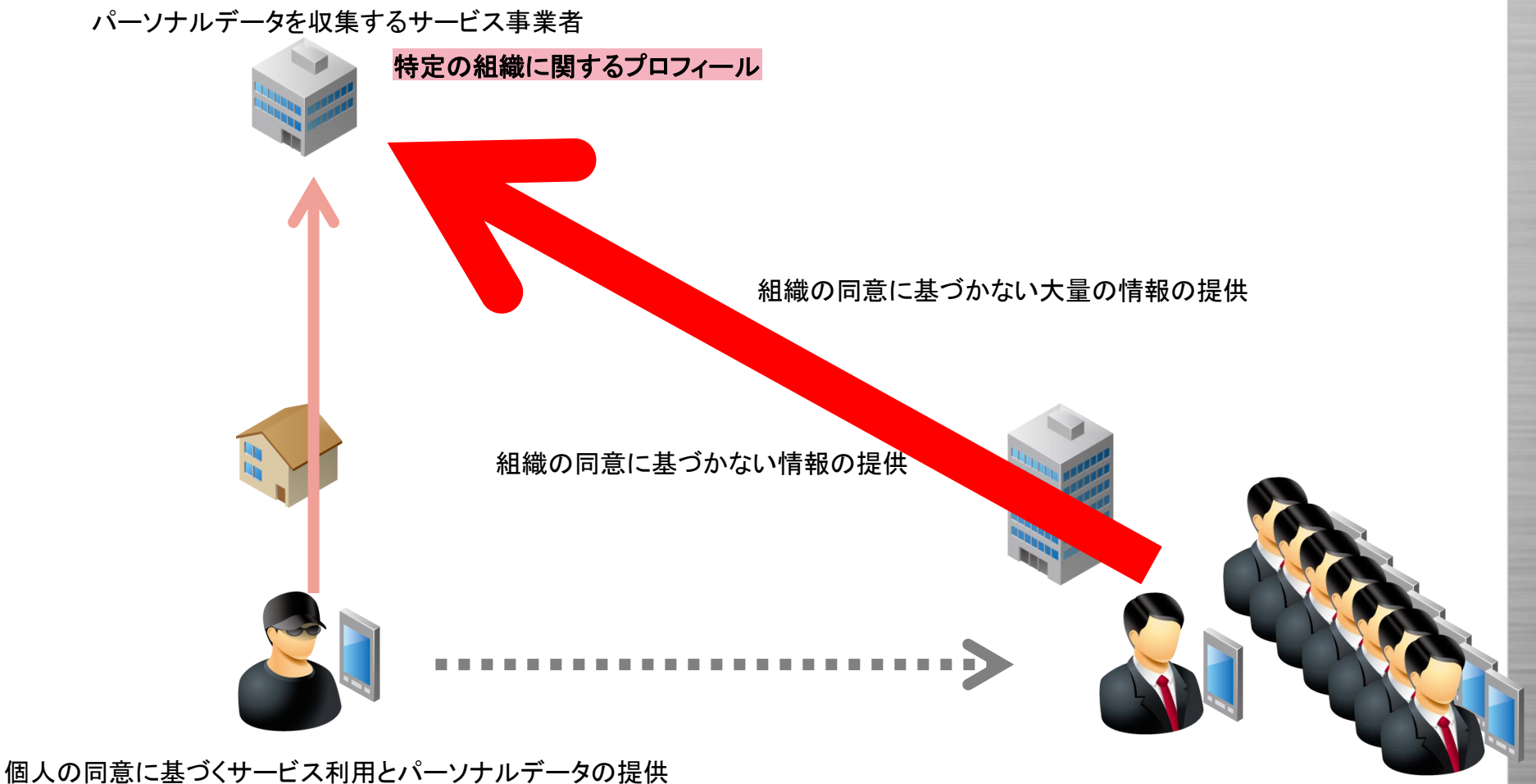
PUA

背景：個人情報保護法改正

- 2015年8月28日可決(2016年1月第三者委員会「個人情報保護委員会」発足、2017年全面施行)。
- 目的：主に、海外勢のビジネスを阻害しつつ国内のビジネスを醸成することが(と読める)。
- 改正のポイント
  - 5,000件条項の削除(小規模事業者が対象に)
  - 慎重な取り扱いが求められるパーソナルデータ
    - スマートフォンやタブレット端末など移動体端末に蓄積される以下のようなパーソナルデータ
      - 電話帳情報、GPSなどの位置情報、通信内容・履歴、メール内容・送受信履歴等の通信履歴、アプリケーションの利用履歴、写真・動画、契約者・端末固有ID
    - 継続的に収集される購買・貸出履歴、視聴履歴、位置情報等
  - 取り扱い概要
    - 目的を説明したうえで利用者の同意を得る。
    - 実質的な個人の識別性でデータの種類を分類、取扱範囲を規定(第三者への提供含む)。
      - 個人の識別性を減らすための匿名化措置。
    - 第三者機関による検証。

PUA

背景：パーソナルデータと企業のセキュリティの親和性の悪さについて



PUAとは？

- Potentially Unwanted Application(PUA)
  - PUP (Potentially Unwanted Program)とも呼ばれる。
  - ユーザにとって不要である可能性がある機能をもったソフトウェア群の総称。
  - ウイルス対策ソフトで検出、駆除されない。
- なぜPUAが組織の中に導入されてしまうのか
  - 他の正当なアプリケーションと抱き合わせで導入されるもの
  - 正当なアプリケーションに余計な機能がついているもの
  - PCなどにプレインストールされているもの
  - ユーザをだましてインストールされるもの

PUA 導入の例

- 抱き合わせでインストールされるもの
  - 著名なソフトウェアであってもいくつかのソフトウェアを同時にインストールしようとする。
  - 例：Java
    - Ask toolbar
      - スタートページと検索エンジンをAsk.comへ変更
      - 検索キーワードすべてを送信
- 正当なアプリケーションに別の（余計な）機能がついているもの
    - Awesome screenshot
      - Google Chrome のスクリーンショット拡張
      - 入力したURLすべてを特定のサーバに送信（最新版はこの機能を取りやめ）
    - Horbor Zoom
      - ブラウザの画像部分を拡大する拡張
      - 入力したURLすべてを特定のサーバに送信

PUA 導入の例(2)

- PCなどにプレインストールされているもの
  - Superfish : メーカ製ではなく、第三者製のソフトウェア
  - 主な機能:ブラウザに広告を表示
    - 通信の間に介在し(端末内でproxyとして動作し)インターネット側から到着したコンテンツに広告のURLを挿入してブラウザに渡す。
  - SSL/TLSなどの暗号化通信にも対応
    - オレオレ証明書の導入。
    - インターネット側から到着したコンテンツに広告を挿入後、全体を署名しなおす。
  - 深刻な副作用
    - 広告配信元にURL情報が洩れる(Referer:フィールド)。
    - 証明書の秘密鍵がばれている(マルウェアへの署名などに悪用される可能性)。

PUA 導入の例(3)

- ユーザをだましてインストールするもの
  - 著名なダウンロードサイトからPUAを配布してた事例
  - CNET
    - CNETのダウンロードサイトであるdownload.com経由でnmapをダウンロードした場合、ツールバー系のPUAが混入していた事例。
    - http://insecure.org/news/download-com-fiasco.html
  - Source Forge
    - Source ForgeからFilezillaなどをダウンロードした場合にAsk.comツールバーが混入していた事例。Filezillaの作者もこれは意図した挙動であることを認めていることから、個別同意がなされていたことがわかる。
    - https://blog.malwarebytes.org/online-security/2013/11/sourceforge-drives-off-downloads-ask-why/
    - https://forum.filezilla-project.org/viewtopic.php?t=30240
  - Softonic
    - Softonicからソフトウェアをダウンロードする場合、ソフトニックダウンローダというダウンローダを経由してダウンロードするが、ソフトニックダウンローダにPUAがバンドルされていたことを伝える事例。
    - http://www.forest.impress.co.jp/docs/news/20110302_430339.html
- 広告枠からのマルウェア感染(マルバタイジング)などもたびたび報告されている。
  - 「不正広告に日本から900万アクセス、金銭狙う攻撃への誘導が日本でも顕著に」
    http://blog.trendmicro.co.jp/archives/12174

クイズ
どれが本物のダウンロードボタンでしょう？

ウイルス対策ソフトとPUA

- ウイルス対策ソフトで削除されないPUAが存在する理由
  - 法的問題
    - インストール時にユーザ同意をとっているため、完全に黒とは言えない。
    - 一方的に妨害した場合、機会損失などで訴えられるかもしれない（ユーザにとっては不必要かもしれないが、ベンダーにとっては必要なので削除されたら困る）。
  - 解析妨害によってウイルス対策ソフトが単純に検知できていない。
    - マルウェアと同様の技術を利用しているものが存在する。
  - 優先順位の問題
    - 表面上深刻な被害を引き起こす機能がないマルウェアはなかなか対策されない。
  - 単なるデータによるもの
    - ブラウザのプラグインなどはJavascriptとhtmlで実現されたものがあり、データとしてユーザ環境にダウンロードされ、ブラウザ上でとして実行される。
    - 企業などで実施されているソフトウェアのアセット管理の仕組みで発見しにくい。

PUA

PUAにより収集される情報

- PUAにより外部に送信された情報は、悪用を試みる第三者の手にわたる（販売される）可能性が否定できない。
- パーソナルデータとしてのURLの取り扱いについて
  - URLは一般にはパーソナルデータには含まれないが、名前やID、メールアドレスなどの特定情報が含まれた時にはパーソナルデータとなる。
  - 組織内でユーザがブラウザで日常的に表示しているコンテンツの位置（URL）が漏えいしている場合、どのようなリスクが考えられるか。URLには、サーバのホスト名、サーバに渡す情報の一部（状況によっては認証情報、セッションID、ファイル名など)が含まれる。顧客名をファイル名やフォルダ名にするような場合。
  - 仕事で使うサーバのURLを日常的に収集されることにより、本来秘匿すべきその組織の内部システムの情報が第三者に知られていることになり、悪用された結果、標的型攻撃などが短時間行われる可能性があ

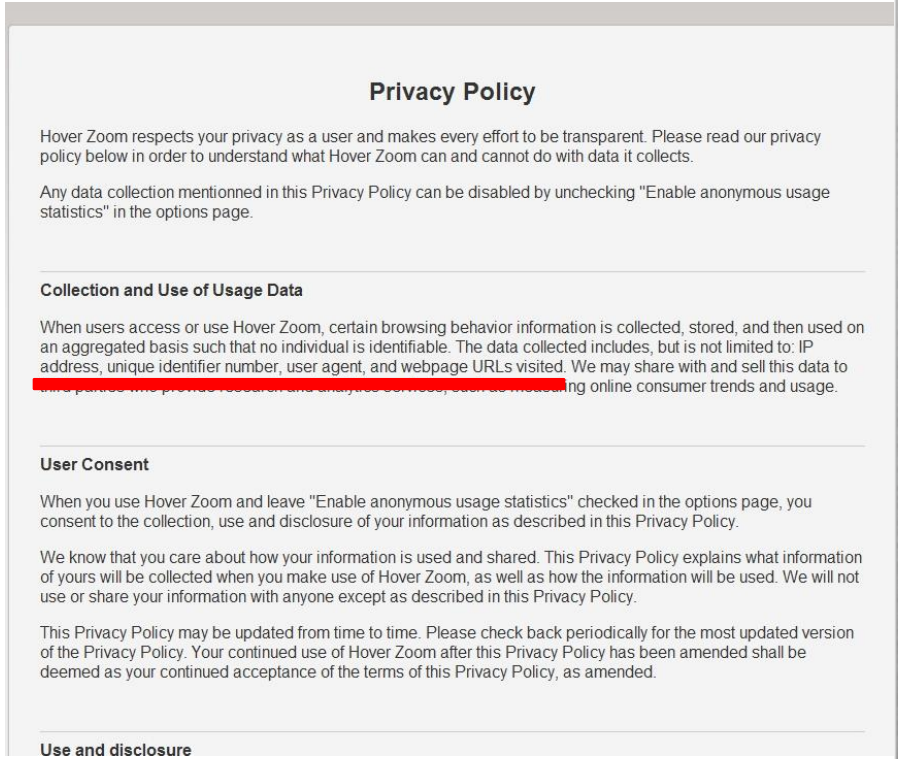
図 2.2.1-1 高度標的型攻撃 攻撃シナリオ

IPA,『高度標的型攻撃』対策に向けたシステム設計ガイド」より
http://www.ipa.go.jp/files/000042039.pdf

PUA

悪質なPUAの例

- Hover Zoom
  - 利用者の望まない動作をするWebブラウザ拡張。
  - Webページ内の画像を拡大するだけのWebブラウザ拡張のはずだが、実際にはユーザがアクセスしたURLを盗み出す機能が付いている。



Privacy Policy

Hover Zoom respects your privacy as a user and makes every effort to be transparent. Please read our privacy policy below in order to understand what Hover Zoom can and cannot do with data it collects.

Any data collection mentionned in this Privacy Policy can be disabled by unchecking "Enable anonymous usage statistics" in the options page.

Collection and Use of Usage Data

When users access or use Hover Zoom, certain browsing behavior information is collected, stored, and then used on an aggregated basis such that no individual is identifiable. The data collected includes, but is not limited to: IP address, unique identifier number, user agent, and webpage URLs visited. We may share with and sell this data to [redacted] online consumer trends and usage.

User Consent

When you use Hover Zoom and leave "Enable anonymous usage statistics" checked in the options page, you consent to the collection, use and disclosure of your information as described in this Privacy Policy.

We know that you care about how your information is used and shared. This Privacy Policy explains what information of yours will be collected when you make use of Hover Zoom, as well as how the information will be used. We will not use or share your information with anyone except as described in this Privacy Policy.

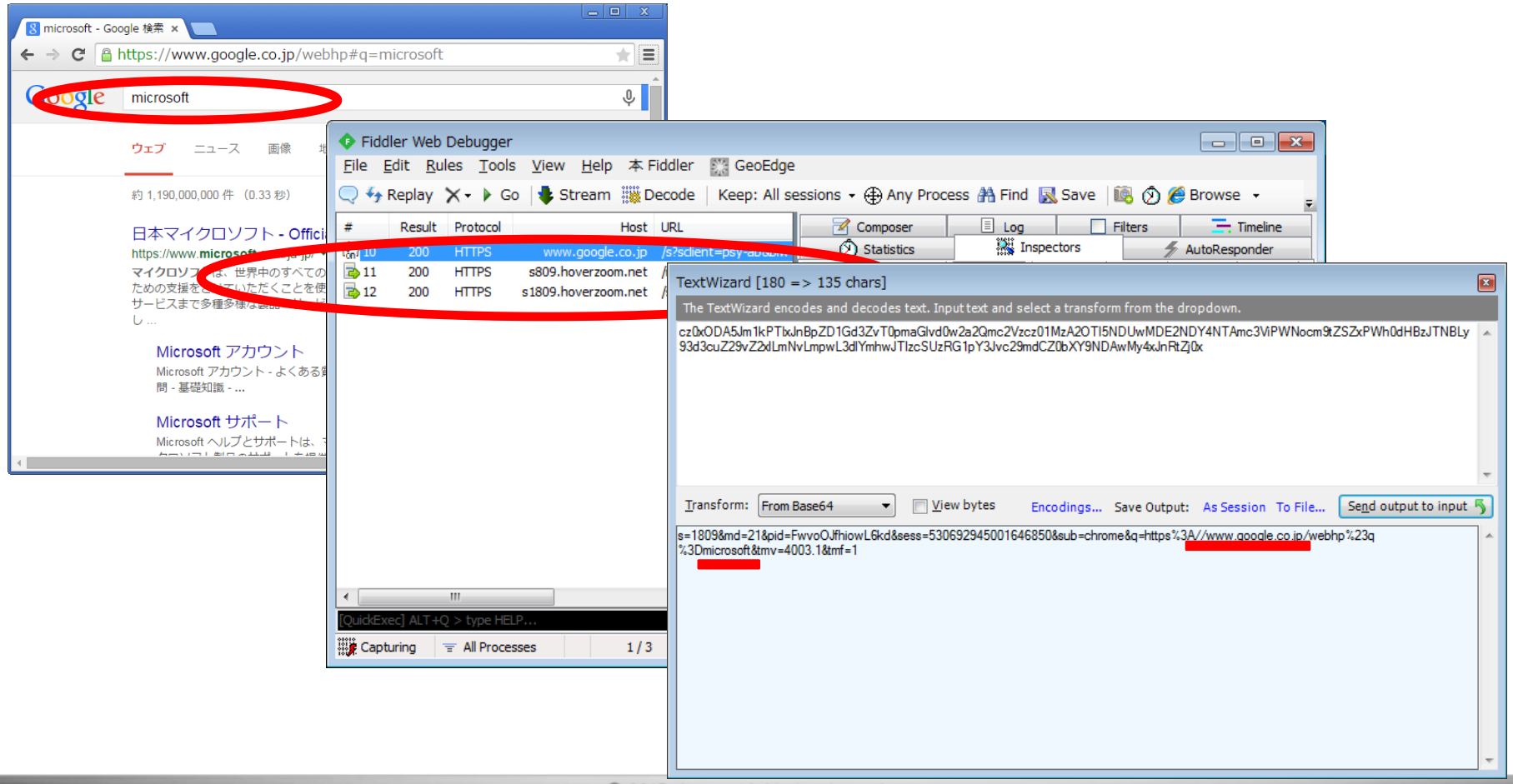
This Privacy Policy may be updated from time to time. Please check back periodically for the most updated version of the Privacy Policy. Your continued use of Hover Zoom after this Privacy Policy has been amended shall be deemed as your continued acceptance of the terms of this Privacy Policy, as amended.

Use and disclosure

PUA

悪質なPUAの例

- Hover Zoom (2)



PUA

外部にURL情報を送信するブラウザの拡張機能の組織内での利用に関する注意喚起

セキュリティ啓発情報
意図せず導入されるソフトウェア　～その存在と動き。把握していますか？～
http://www.lac.co.jp/security/alert/2014/02/05_edu_01.html

【スパイウェア】【アドウェア】入れてはいけない拡張まとめ2014（Chrome、Firefox）
http://matome.naver.jp/odai/2139104770956843701

外部にURL情報を送信するブラウザの拡張機能の組織内での利用に関する注意喚起
https://sect.iij.ad.jp/

悪質化するPUA
http://www.iij.ad.jp/company/development/report/iir/027.html

PUA

ブラウザの拡張機能

- ブラウザの拡張機能の特長
  - 利用者権限でインストール可能
  - プロセステーブル上はブラウザとしてしか現れない
  - ブラウザの機能（情報の表示やアフィリエイトにかかわる拡張機能が多い）
    - 広報部門、IT部門に利用者が（ユーザマニュアル作成など）
  - 発見、制御の難しさ
    - ソフトウェア資産管理ツールなどでは検出が難しい
    - ウイルス対策ソフトでは検出できない（できなかった）
  - ブラウザベンダによる削除の努力
    - いたちごっこが実施されている

PUA

URLを送信するブラウザ拡張の状況

- URLを送信する（余分な）機能を持つブラウザ拡張機能 6種(2015/05時点)
- URLを送信する本来機能を持つブラウザ拡張機能3種
- 過去にはIEのBHOとしても存在した（現在は入手不能）

- いくつかの組織が、行動情報把握の目的で、拡張機能作成者にURL送信するモジュールを組み込むようにビジネスを行っている様子がうかがえる。

現時点でURL送信機能が削除されているブラウザ拡張であっても、古いバージョンを使い続けていればURLが送信され続けている点に注意。

PUA

ブラウザ拡張導入の制御

- 既知のURL情報送信拡張機能をどう制御するか
  - ◎ブラウザ拡張機能の制限ポリシーの導入（google chromeなど、ブラウザ依存）
  - ○一部ウイルス対策ソフトの機能で検出
  - ○インターネット境界で送信先への通信をFQDNで規制
  - △インターネット境界で送信先への通信をIPアドレスで規制(IPアドレス空間が広大で副作用が考えられる)
- 未知のURL情報送信拡張機能をどう制御するか
  - 一般情報入手、個別確認
  - インターネット境界で通信のアノマリの検出

PUAに対峙するために

- PUAと呼ばれるアプリケーションの存在の広報、周知。
- 組織においては（現状）
  - ユーザ同意と組織のセキュリティの関係の整理。
  - PCの受け入れ時の検査（プレインストールされているソフトウェアの安全性を検証）。
  - ソフトウェアのアセットの管理（ユーザに自由にアプリケーションをインストールさせない）。
  - アプリケーションの入手先は正規の発行元に限定する（都度検索して入手先を探さない）。
  - ウイルス対策ソフトでマルウェアが検知されたら、他の（検知できない）マルウェアの存在を疑う。
  - PCから発せられる通信のアノマリ（必ず特定のURLにアクセスするなど）を検出する。できれば暗号化通信に関するアノマリ検知も行う。
  - 情報漏えいに該当する通信の規制。
  - PUAの扱いについてはウイルス対策ソフトなど社内セキュリティに供するシステムを信用しない。

DDoS攻撃

PUA

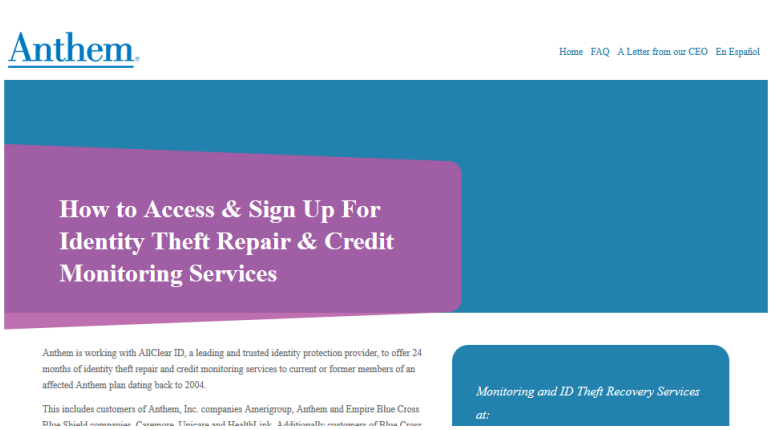
標的型攻撃

新しい対策技術の検討

標的型攻撃

米国の最近の事件

- アンセム情報漏えい事件
  - 20151/27に AnthemのDB管理者が不審な挙動を発見した。
  - 少なくとも昨年12月から 1/27まで、攻撃者による活動があったことを確認した。
  - 約8,000万件の顧客情報が漏洩した可能性がある。DBに保存されたデータは暗号化されていなかった。ただし、医療情報は含まれていない.
  - Anthemは 1/29に FBIや HITRUST C3 (Cyber Threat Intelligence and Incident Coordination Center)に連絡している。
  - FBIは調査の結果、Deep Panda (CrowdStrikeが命名した、中国が関与していると見られる攻撃グループの一つ) による攻撃と結論づけて、関係各所に注意喚起。
  - Deep Pandaの過去の活動などから、Anthemは昨年 4月から攻撃されていた可能性がある。



https://www.anthemfacts.com/

https://hitrustalliance.net/

標的型攻撃

日本国内の最近の状況

- 日本国内においても2014年より大規模なキャンペーンが実施されている。
  - キャンペーンcloud-omega, blue-termiteなどと呼ばれる。
  - 大きな組織や企業の保険組合などが対象。
  - 共通の特徴
    - 文面「医療費通知」など。
    - マルウェアEmdiviの利用。
    - 国内にサーバ。
  - 2014/09から2015年も継続中。
  - 攻撃対象総計100組織以上。

piyolog RSS

<[インシデントまとめ] 複数の国... | [脆弱性まとめ] 一太郎の脆弱性 ... >

2014-11-07

医療費通知の偽装メールについてまとめてみた

インシデントまとめ | 23:34 | 21 users

2014年9月、10月頃より、健康保険組合等から医療費通知を偽装したメールが出回っており、添付ファイルを開くとマルウェアに感染する恐れがあると注意喚起が出されています。ここではその関連情報をまとめます。

医療費通知の偽装メールに関係する注意喚起

発信日時	喚起元	被害報告	注意喚起
2014年9月30日	富士重工業健康保険組合	あり(グループ会社社員)	健保名の不審メールにご注意下さい
2014年10月3日	荒川区	あり?(国民健康保険加入者宛)	医療費通知を装った不審なメールにご注意下さい。
2014年10月29日	UBS	–	健保組合からのお知らせを装ったウィルスメールにご注意下さい
2014年10月29日	HOYA健康保険組合	無し	医療費通知を装ったウィルスメールにご注意ください
2014年10月30日	インフォコム	–	当社を騙る電子メールにご注意ください「インフォコム"の名称を不正に使用した医療費通知に関する注意喚起」
2014年10月31日	住商連合健康保険組合	あり (某大手商社)	「医療費のお知らせ」を装ったウィルスメールにご注意ください！
	住友商事健康保険組合	–	「医療費のおしらせ」を装ったウィルスメールにご注意ください。(認証あり)
2014年11月5日	人材派遣健康保険組合	無し	健保組合からのお知らせを装ったウィルスメールにご注意ください
2014年11月6日	三菱レイヨン健康保険組合	–	医療費通知不審メールに対する注意喚起について(認証あり)
2014年11月7日	三菱化学健康保険組合	あり (三菱系企業)	健康保険組合を騙る不審メールにご注意下さい！
2014年11月10日	石油製品販売健康保険組合	無し	医療費通知に偽装した不審メールについて
	日本ケミコン健康保険組合	無し	医療費通知の偽装メールについて
	東京実業健康保険組合	無し	医療費通知を装ったウイルスメールにご注意ください【注意喚起】

http://d.hatena.ne.jp/Kango/20141107/1415370890

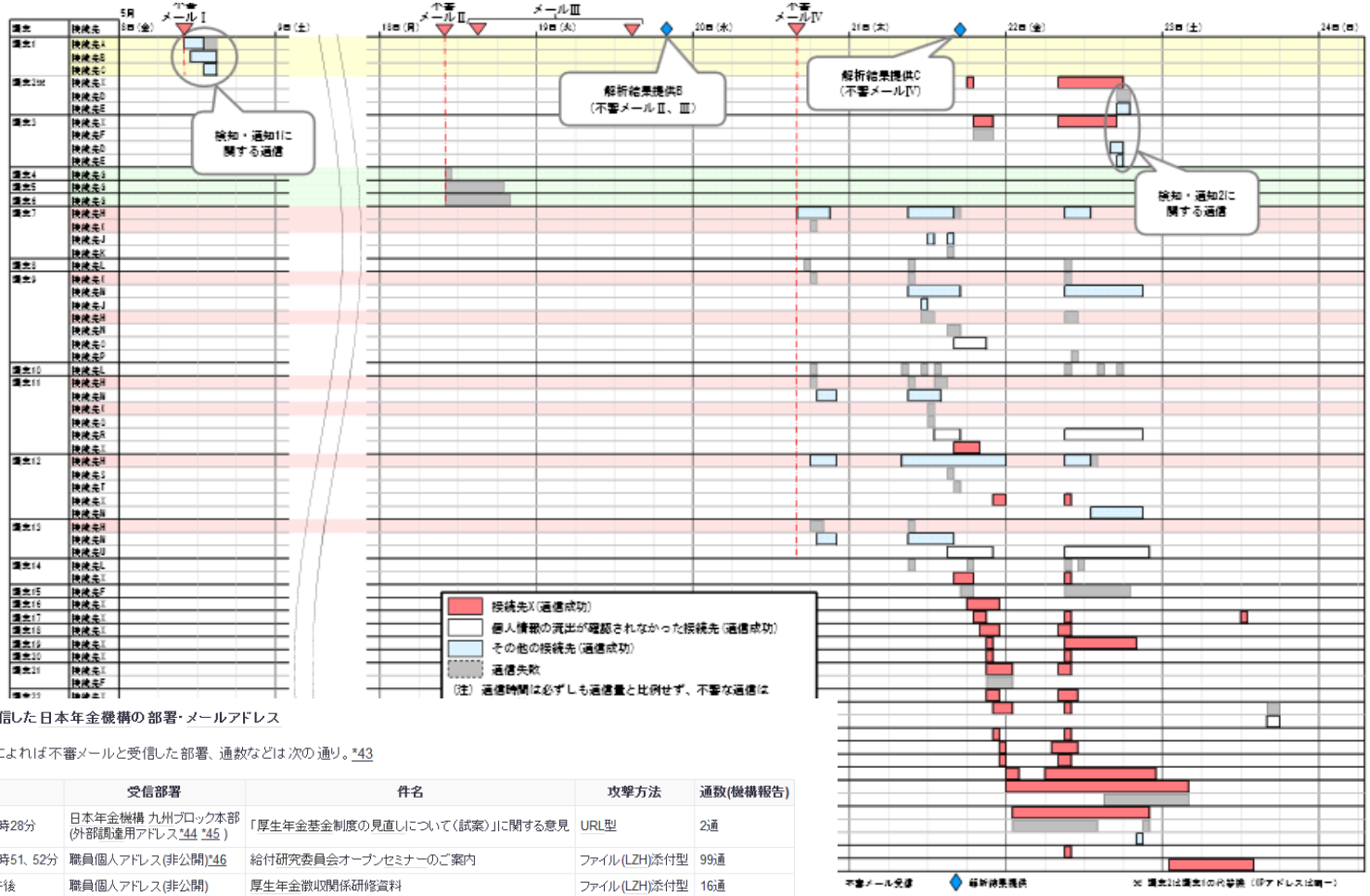
標的型攻撃

日本国内の最近の状況（2）

- 年金機構の事件に関する3報告書
  - 内閣官房サイバーセキュリティセンター報告書
    サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査結果」
    http://www.nisc.go.jp/conference/cs/
  - 厚生労働省検証委員会報告書
    日本年金機構における不正アクセスによる情報流出事案検証委員会
    http://www.mhlw.go.jp/stf/shingi2/0000095311.html
  - 年金機構調査報告書
    「不正アクセスによる情報流出事案に関する調査結果報告」
    https://www.nenkin.go.jp/oshirase/press/2015/201508/20150820-02.html

標的型攻撃

日本国内の最近の状況（3）



不審メールを受信した日本年金機構の部署・メールアドレス

- 調査報告によれば不審メールと受信した部署、通数などは次の通り。*43

受信日	受信部署	件名	攻撃方法	通数(機構報告)
2015年5月8日 10時28分	日本年金機構 九州ブロック本部 (外部調達用アドレス*44 *45)	「厚生年金基金制度の見直しについて（試案）」に関する意見	URL型	2通
2015年5月18日 9時51、52分	職員個人アドレス(非公開)*46	給付研究委員会オープンセミナーのご案内	ファイル(LZH)添付型	99通
2015年5月18日 午後	職員個人アドレス(非公開)	厚生年金徴収関係研修資料	ファイル(LZH)添付型	16通
〃	職員個人アドレス(非公開)	厚生年金徴収関係研修資料	URL型	3通
2015年5月19日 午前	職員個人アドレス(非公開)	厚生年金徴収関係研修資料	URL型	1通
2015年5月20日 午後	公開アドレス	【医療費通知】	ファイル(LZH)添付型	3通

以下は日本年金機構が注意喚起を行った際に取り上げられていた不審メールの4つの例。*47 *48

内閣官房サイバーセキュリティセンター報告書より

http://d.hatena.ne.jp/Kango/20150601/1433166675

標的型攻撃

IPA(独立行政法人 情報処理推進機構)脅威と対策研究会による各ガイド

- 各ガイドと発出コンセプト
  - 「新しいタイプの攻撃」の対策に向けた設計・運用ガイド 2011/8 , 2011/10
    - 出口対策

  - 「標的型メール攻撃」対策に向けたシステム設計ガイド 2013/8
    - 内部対策
    - 標的型攻撃メールに特化した内容

  - 「高度標的型攻撃」対策に向けたシステム設計ガイド 2014/8
    - NISC政府政策「リスク評価手法」に連動
    - 高度標的型攻撃対策を対象とした内部(攻撃段階)対策に特化:
      通常のセキュリティ対策で検出・対処できないマルウェアによる標的型攻撃(=高度標的型攻撃)を対象に、監視や遮断など、内部における対策を、対策セットとして提案。

標的型攻撃

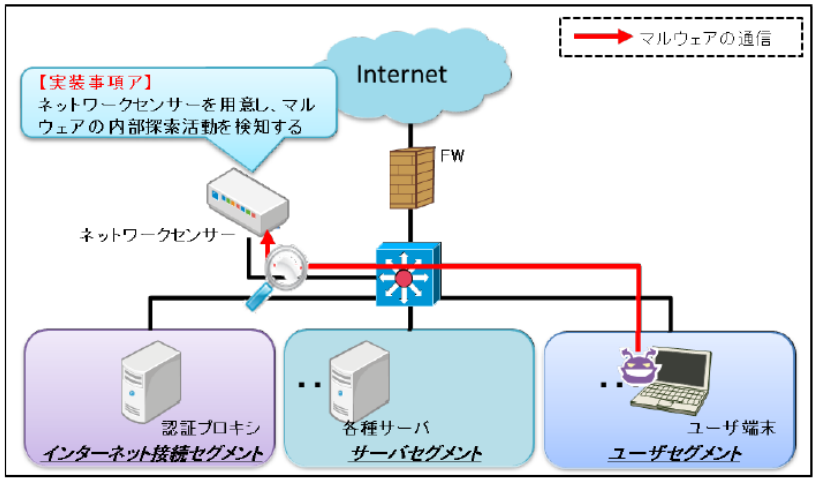
「高度標的型攻撃」対策に向けたシステム設計ガイド

- 攻撃シナリオと対策セット
  - 高度標的型攻撃の各段階で実際にネットワーク内で実施される攻撃について検討
  - 検出遮断に向けたポイントを対策セットとして抽出

表 2.2.4-1 攻撃シナリオ一覧

	想定脅威	攻撃手口	攻撃が成功する要因／運用側の問題点
初期潜入	マルウェア感染	メール型マルウェア	・ソフトウェア脆弱性の放置 ・ユーザの心理的・行動的な隙
		ウェブ感染型マルウェア	
基盤構築	バックドア開設	直接外部通信タイプ	・FW のフィルタリングルールの形骸化
		プロキシ通信対応タイプ	・素通しに近いプロキシサーバの運用
		★認証プロキシ突破タイプ	・OS の標準仕様を悪用した通信のため、検知が困難
	ユーザ端末での諜報	ツールダウンロード・実行	・ツールやコマンド実行結果がログに残らず検知が困難
		コマンドの実行	
		認証情報の窃取	
	ネットワーク環境の調査・探索	IP アドレスの探索	・正常通信のため、機器やセンサー装置による攻撃か否かの判別が困難
		サービスポート探索	
内部侵入・調査	端末間での侵害拡大	近隣端末へ攻撃ツールのコピー	・ユーザ端末におけるファイル共有サービスの開放
		Pass the Hash 攻撃	・PC キッティング作業時の共通アカウントの設定 ・Domain Admins を使用した PC のリモートメンテナンス作業
	端末からサーバへの侵入	管理者端末の乗っ取り	・ユーザ端末と管理端末を共用したサーバ運用
		ユーザ端末からのサーバへのリモート操作	・フラットなネットワーク構造 ・サーバにおけるアクセス権限の不備
目的遂行	データ窃取・外部送信	ファイル分割して外部に送信	システム全体が乗っ取られているため、対策が困難
	データの破壊・業務妨害	業務データ削除	
		破壊プログラムの設置と実行	

★:新たな攻撃手口



対策セットの例
「高度標的型攻撃」対策に向けたシステム設計ガイドP93監視強化策（新規）より引用

攻撃シナリオ一覧
「高度標的型攻撃」対策に向けたシステム設計ガイドP42 攻撃手法の変化より引用

DDoS攻撃

PUA

標的型攻撃

新しい対策技術の検討

新しい対策技術の検討

- VDI(Virtual Desktop Infrastructur)の応用
- SDN(Software Designed Network)の応用
- AI(Artificial Intelligence)の応用

新しい対策技術の検討

クラウド環境とVDI

- クラウド環境

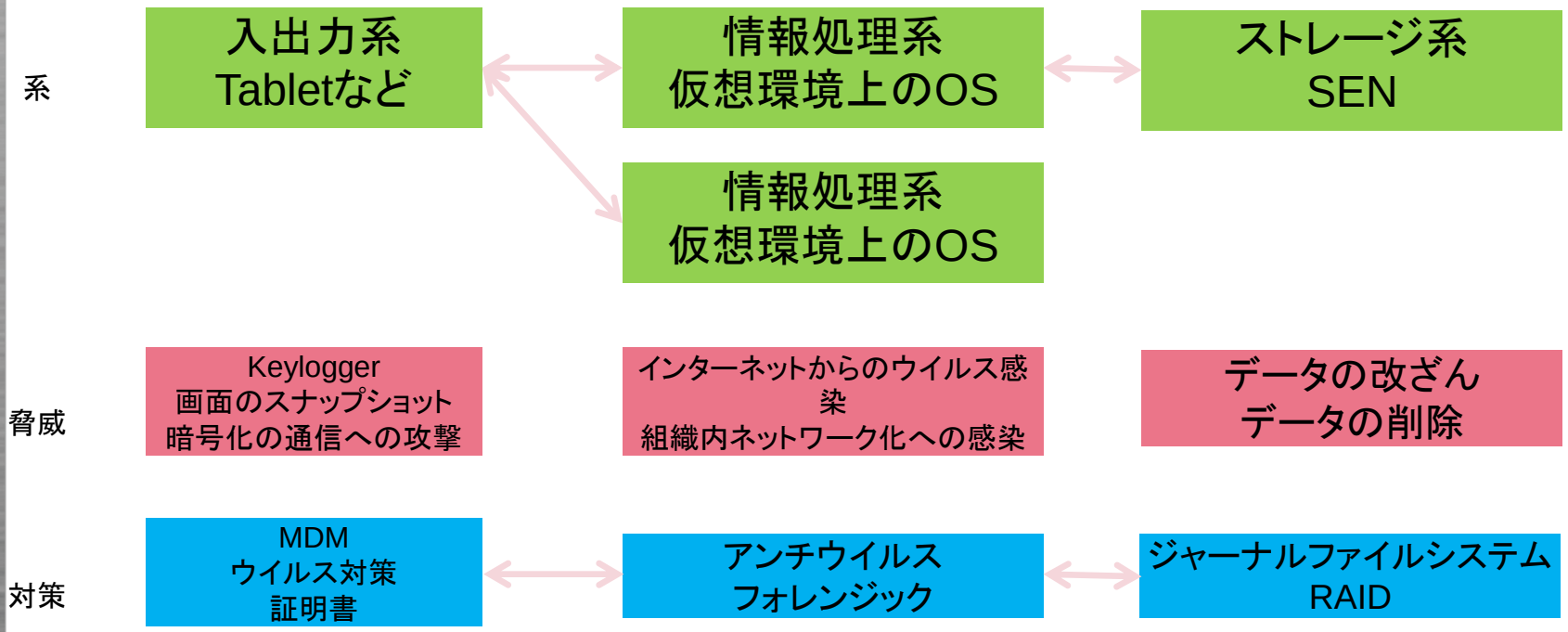
- VDI(Virtual Desktop Infrastructure)環境

⇒利用者の環境がネットワーク越しの複数のサービスで構成される

新しい対策技術の検討

VDI技術のセキュリティへの応用

- クラウド、VDI環境のセキュリティ上の利点
  - 脅威の分割統治：影響範囲の局所化、対策時の事業継続

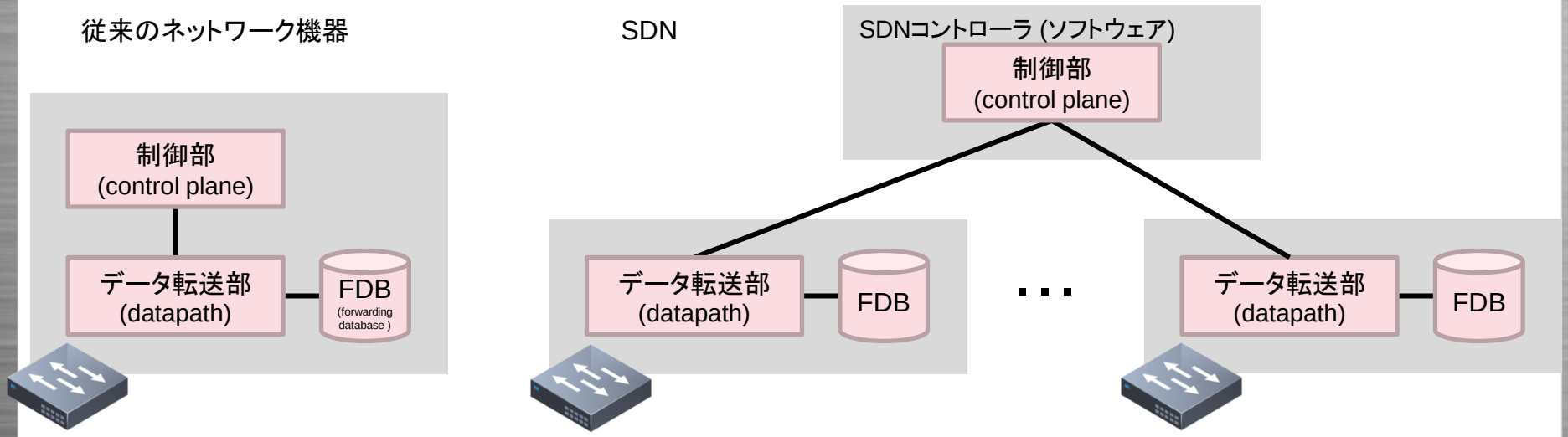


  - 各機能の事案にそれぞれ代替設備を投入しながら、対応することが可能となる。

新しい対策技術の検討

SDNとは

- Software Defined Networking
- “The physical separation of the network control plane from the forwarding plane, and where a control plane controls several devices.” (https://www.opennetworking.org/ja/sdn-resources-ja/sdn-definition)
- ネットワーク機器のパケット転送機能をソフトウェアで集中制御



新しい対策技術の検討

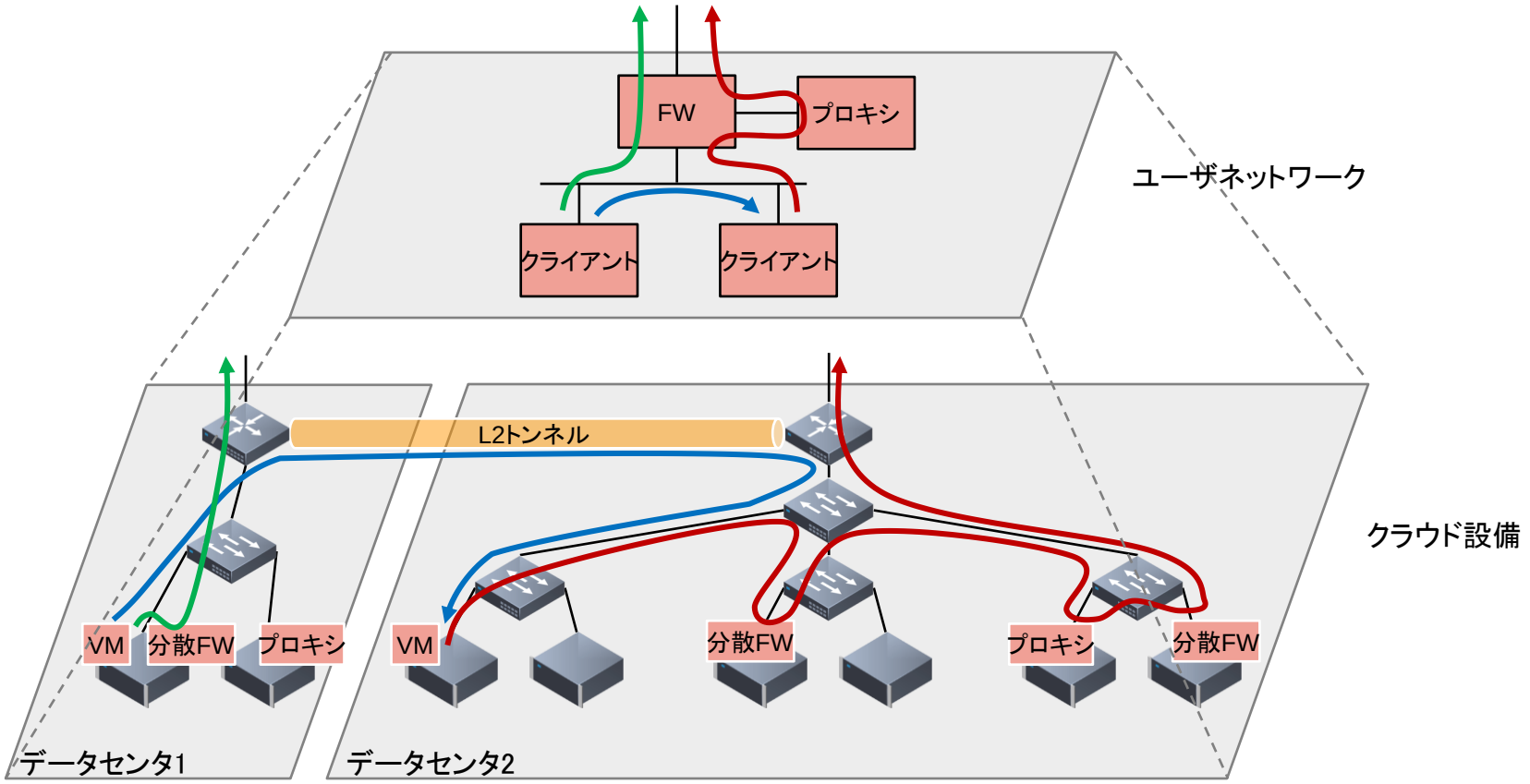
SDNとは(Cont.)

- 柔軟かつ迅速、動的にネットワーク構成を変更できる
  例)
  - 論理ネットワークの作成、変更 (VLAN)
  - フロー毎の経路や優先度の割り当て、変更
    - ACL、ロードバランス、QoS
- ネットワークの設計哲学：所与の機能から実現可能なアプリケーションを考えた時代から、実現したいアプリケーションから機能を実装する。
- 2つの重要な概念
  - NFV (Network Function Virtualization)
    - パケット転送機能の柔軟な設定変更だけではなく、他のネットワーク機能。ACL、認証、accounting、VPN、proxy や、セキュリティの機能を提供するファイアウォール、IPS、WAFなどもネットワーク機能だと考え、仮想化(仮想アプライアンス)して迅速に構成できるようにすること。
  - マイクロセグメンテーション(Micro Segmentation)
    - 各仮想/物理サーバ上のサービス/アプリに応じて、ネットワークレベルでもサーバ個別に最適な通信要件を自動で強制することでネットワークの性能を最適化したり、セキュリティの境界を最小にすることで侵犯の影響を最小にしようとすること。

新しい対策技術の検討

SDNとは(Cont.)

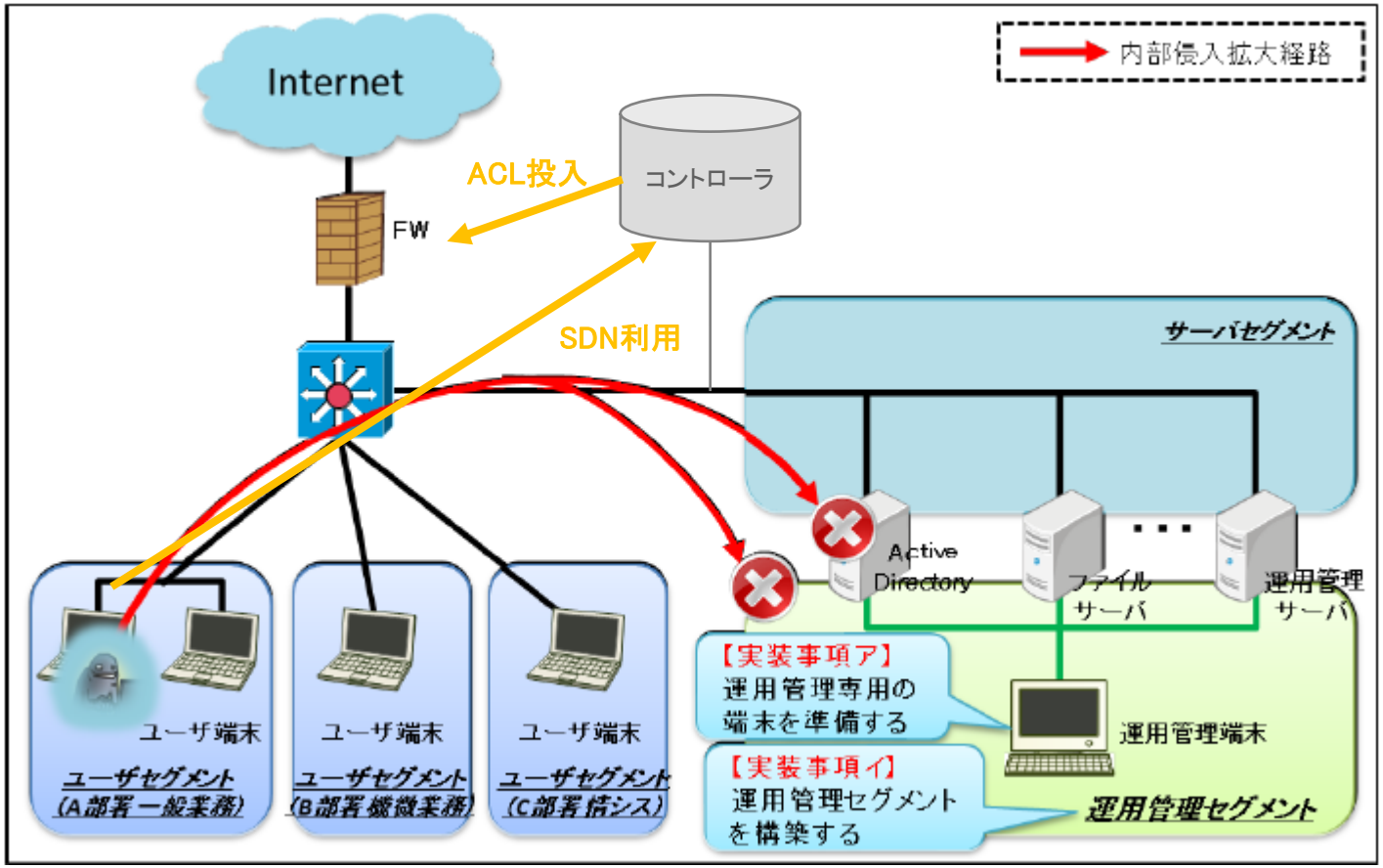
- 一つの機能が、実際には同一アドレスで複数の場所に分散配置されている可能性も（下図：分散ファイアウォール）



新しい対策技術の検討

SDN技術を用いた対策セットの実現

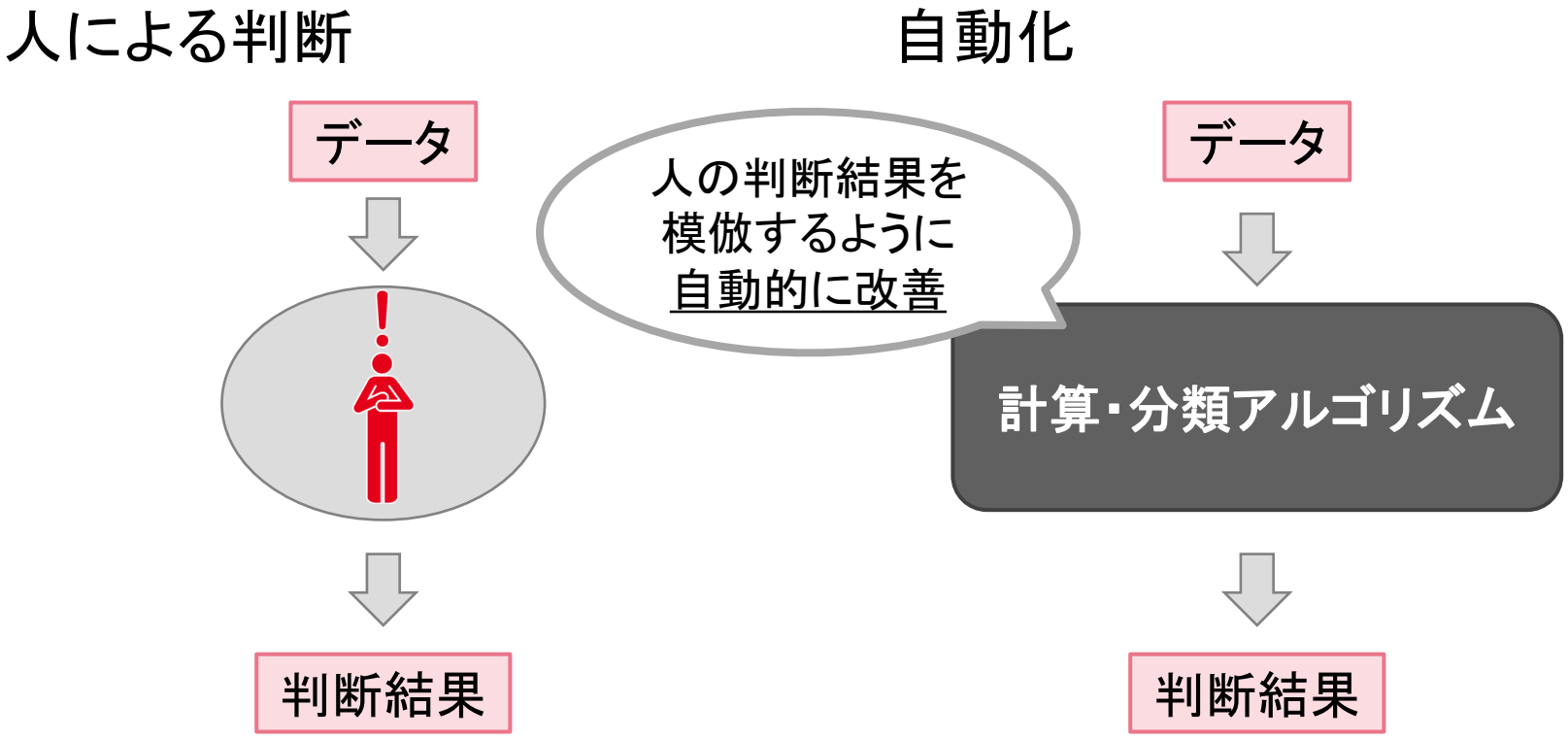
- 高度標的型攻撃対策ガイドの対策セット実現への応用（対策セットD）
  - ユーザセグメントで検出された疑わしい通信を特定するため検出装置に通信を捻じ曲げる
  - 内部侵入拡大通信と判明した場合にACLを自動投入し遮断



「高度標的型攻撃」対策に向けたシステム設計ガイドP70防御遮断策（断④）より引用

新しい対策技術の検討

機械学習で人による判断を模倣

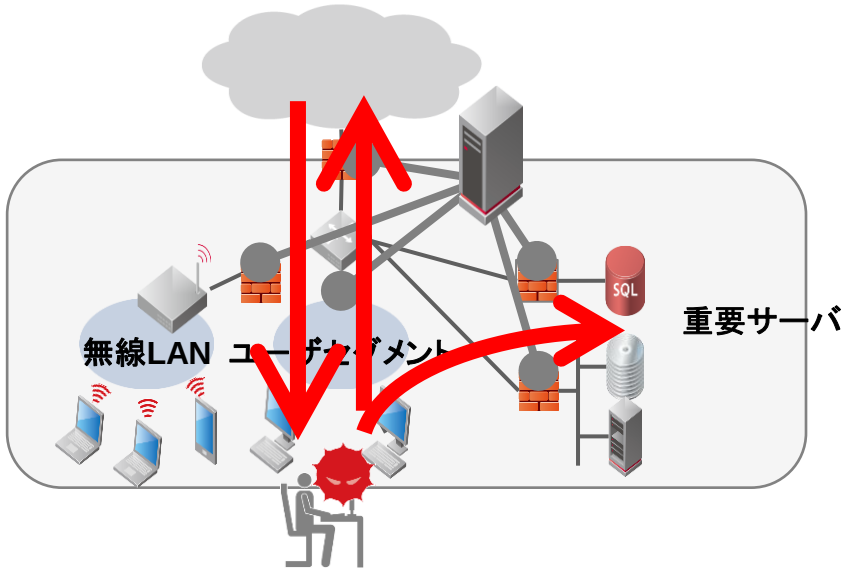


人による判断の基準が明確であれば今までも自動化できていた。
機械学習は、判断基準が明確化できない場合にも応用できる
可能性がある。

新しい対策技術の検討

標的型攻撃の検知

- 機械学習の利用
  - 標的型攻撃マルウェアのバイナリ的特徴を学習
  - ユーザ毎の通信プロファイルを学習
- 標的型攻撃マルウェアの侵入を検知
  - メール、Webなどの外部との通信にマルウェアが含まれていないか検査
- マルウェア感染後の通信を検知
  - 正常なプロファイルから外れる社内の通信
    - 感染拡大、サーバへの侵入、機密データ収集
  - 正常なプロファイルから外れる社外との通信
    - C&Cサーバとの通信、データ持ち出しの通信



まとめ

- DDoS攻撃
- PUA
- 標的型攻撃
- 新しい対策技術の検討

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