ICT海外ボランティア会講演
無断転載禁止

連絡先
NTTデータ先端技術株式会社
〒104-0051 東京都中央区佃1-11-8
ピアウエストスクエア3階
Tel: 03-5843-6824, Fax: 03-5843-6846
E-mail: miyake@intellilink.co.jp

世界におけるサイバー攻撃の動向

2019年2月15日
NTTデータ先端技術株式会社
相談役、最高技術顧問、CISSP,PCI DSS QSA
三宅功

NTT DATA
NTTデータ先端技術株式会社

はじめに ～ 自己紹介 私と情報セキュリティマネジメントとの関わり

～研究者の時代～	
1980年～	NTT（当時電電公社）武蔵野電気通信研究所 入所 基幹交換研究部 交換方式研究室、トラヒック研究室 トラヒック理論、高速パケットNW設計法 などを研究,工学博士
～プロジェクトマネージャの時代～	
1991年～	交換システム研究所 主任研究員～研究部長 新ノード開発プロジェクトPM、ITU-T国際標準化担当 （主にATM交換機、キャリアVoIPシステム）の開発実用化
～経営者の時代～	
2003年～	NTTデータ先端技術（株）代表取締役社長
2007年～	NTTサービスインテグレーション基盤研究所 所長
2009年～	NTT情報流通基盤総合研究所 所長
2011年～	NTTデータ先端技術（株）代表取締役社長, JASA副会長
2015年	CISSP取得
2017年	PCI DSS QSA取得

始めに

情報セキュリティとサイバーセキュリティ

情報セキュリティとは？

情報及び情報システムに対する**機密性、完全性、及び可用性**を守るために、許可されていないアクセス、利用、公開、途絶、改変、破壊を防止すること。

情報資産

CIA

※NISTによる定義

情報セキュリティに対する脅威とは？

NTT DATA

- 外部からの脅威
  - サイバー攻撃
  - 物理的犯行（侵入、窃盗等）
  - 自然災害、火災等
- 内部の脅威
  - 内部犯行
  - 誤操作、意図的でないミス

実際の脅威は複合的に起こることが多い

サイバーセキュリティとは？

NTT DATA

サイバーセキュリティ

サイバー空間の利用にあたって、これをサイバー攻撃から保護あるいは防御する能力

分散コンピュータシステム

サイバー空間

グローバルな領域で、特定の情報を利用するために独立したネットワークで構成される情報システム基盤。インターネット、電気通信網、コンピュータシステム、組込型処理・制御システムなどを含む。

サイバー攻撃

企業が利用するサイバー空間を標的に、サイバー空間を介して行われる攻撃であり、コンピュータの利用環境或いは基盤に対して、利用の途絶、停止、破壊、悪意を持った制御を行うこと或いは情報の完全性の破壊、管理された情報の窃取を行うこと。

※NISTによる定義

インターネットとサイバー攻撃

インターネットの原理

Internet Society

Home | Connect Login | Become a Member | Find a Chapter | Blog | News | العربية | 简体中文 | E

Four ground rules were critical to Kahn's early thinkin

- Each distinct network would have to stand on its o
  could be required to any such network to connect i
- Communications would be on a best effort basis. I
  the final destination, it would shortly be retransmitt
- Black boxes would be used to connect the networ
  called gateways and routers. There would be no in
  gateways about the individual flows of packets pas
  keeping them simple and avoiding complicated adaptation and recovery from various failure modes.
- There would be no global control at the operations level.

Bob Kahn in Geneva, May 2013

インターネットの原理

NTT DATA

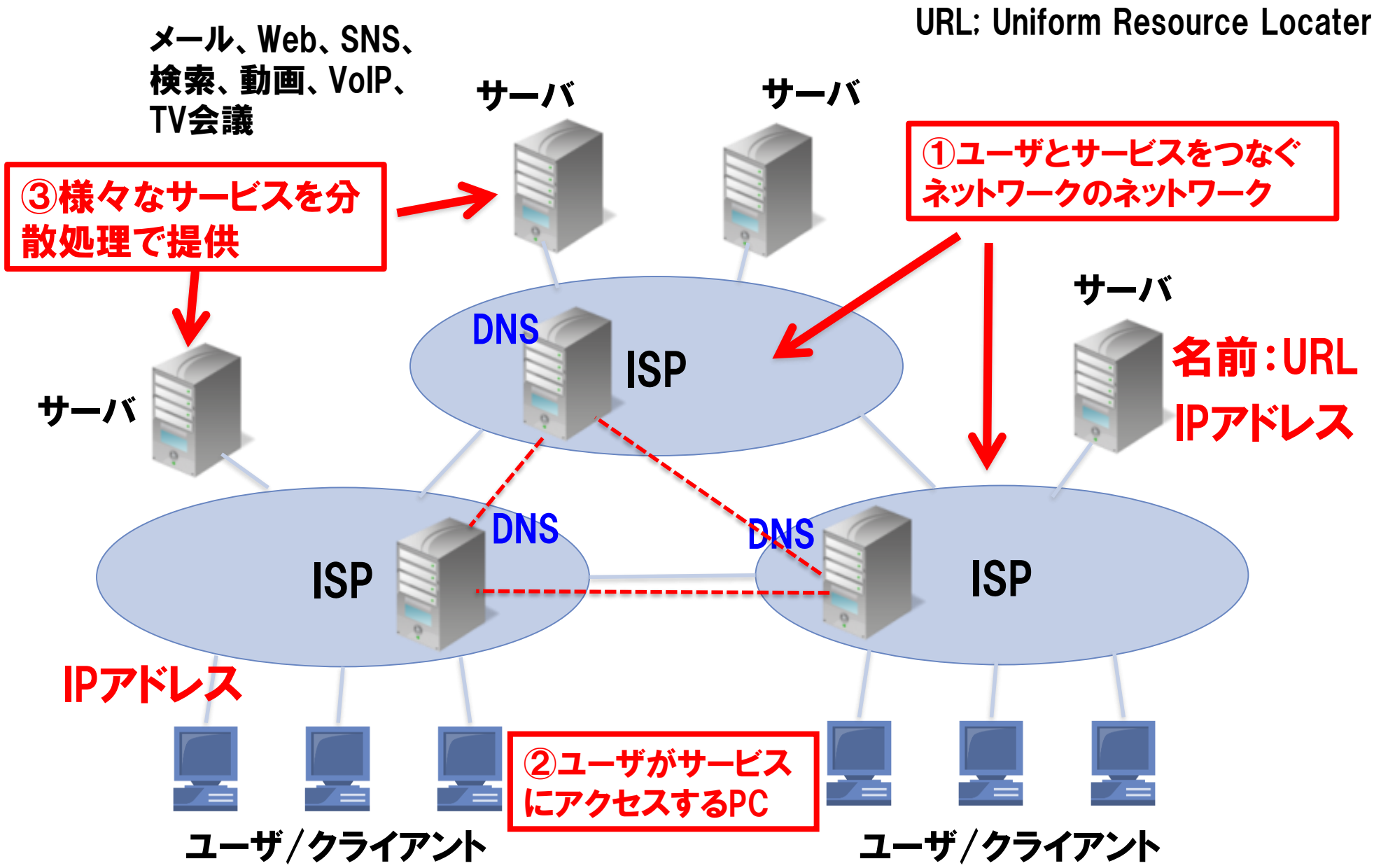
・相互に接続されるネットワークはそれぞれ独立に構成され、相互に接続される場合には、その内部の構造の変更を不要とすること。

・パケットの転送はベストエフォート型とする（すなわち、相手先に極力届ける努力はするが、保証はしない）。もし、パケットが相手先に届かない場合は、速やかに再送信を行なう。

・ネットワークを相互に接続する装置はブラックボックスである。これらは、ゲートウェイもしくはルーターと呼ばれる。ゲートウェイは個々のパケットあるいはそのフローの情報は保持しない。このことにより、できるだけ処理を単純に、エラーに対する複雑な機能はもたずに済ませることを実現する。

・全世界的な制御や運用はもたない。

インターネットの構造＝ネットワークのネットワーク



インターネット＝自律分散コンピュータネットワーク

NTT DATA

◇参入規制が低い（制度）

← IPアドレスドメインの取得のみで参加可能

誰が参加しているかわからない

◇参入コストが安い（基盤技術）

← ICT機器の大容量化とオープンソース

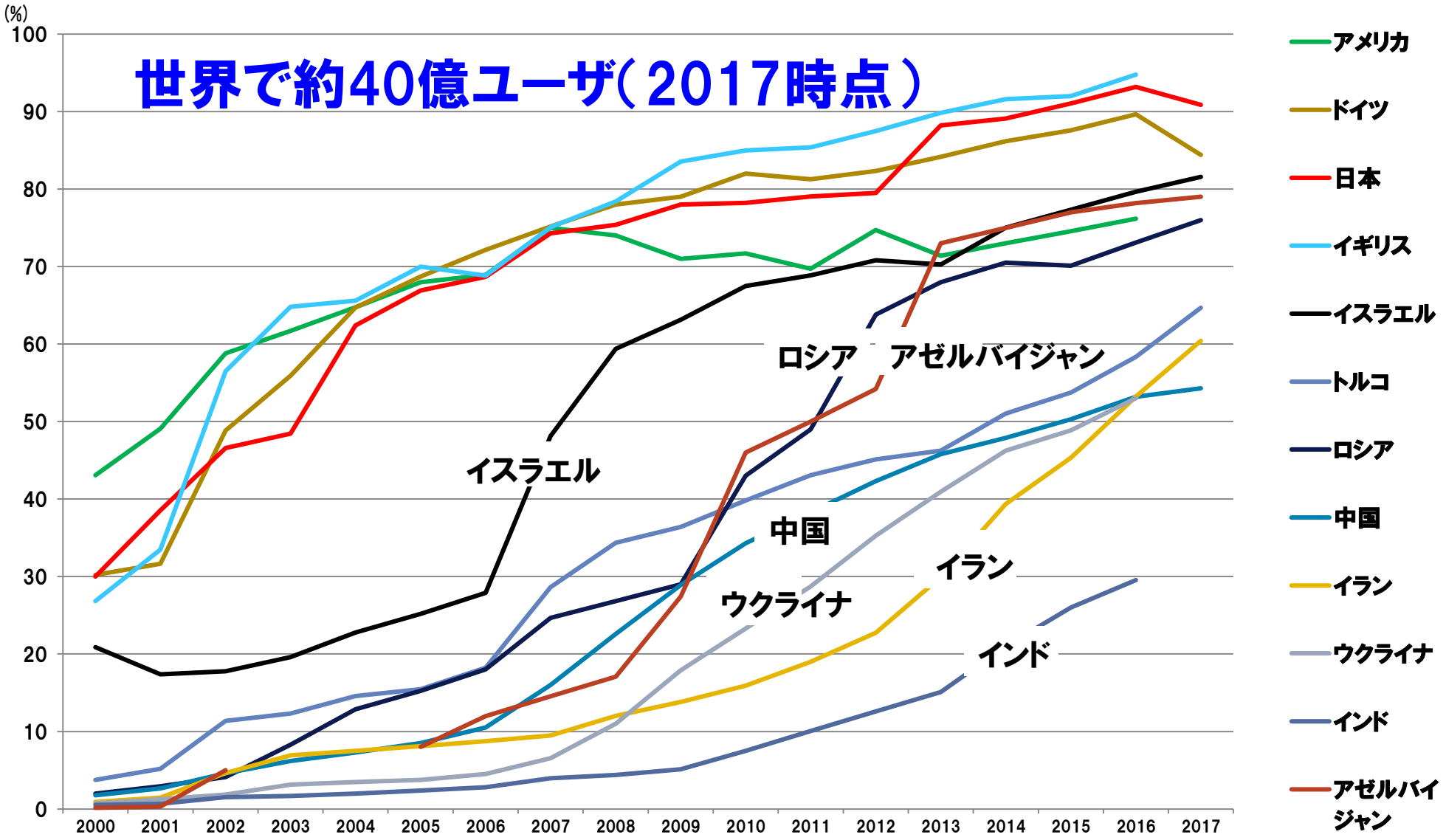
誰でも参加可能

◇IT技術のコモディティ化（利活用）

← PC,モバイルの普及による経済活動の変化

利用価値の拡大

国別のインターネット普及状況（’00～’17）



出典：ITU – ICT Statistics

サイバー攻撃のインフラにもなってしまった！！

どこからでも攻撃可能

何が行われているか？

ESET「マルウェア情報局」の情報（2019.2.1） 「Love You」キャンペーン
https://eset-info.canon-its.jp/malware_info/trend/detail/190201.html

・1月初旬より主に日本向けに行われているキャンペーン
・悪意のあるサイトにアクセスさせて、暗号通貨ツール、システム設定変更ツール、悪意のあるダウンローダー、Phorpiex（ワーム）、ランサムウェアGandCrabバージョン5.1などをダウンロードさせようと試みる。

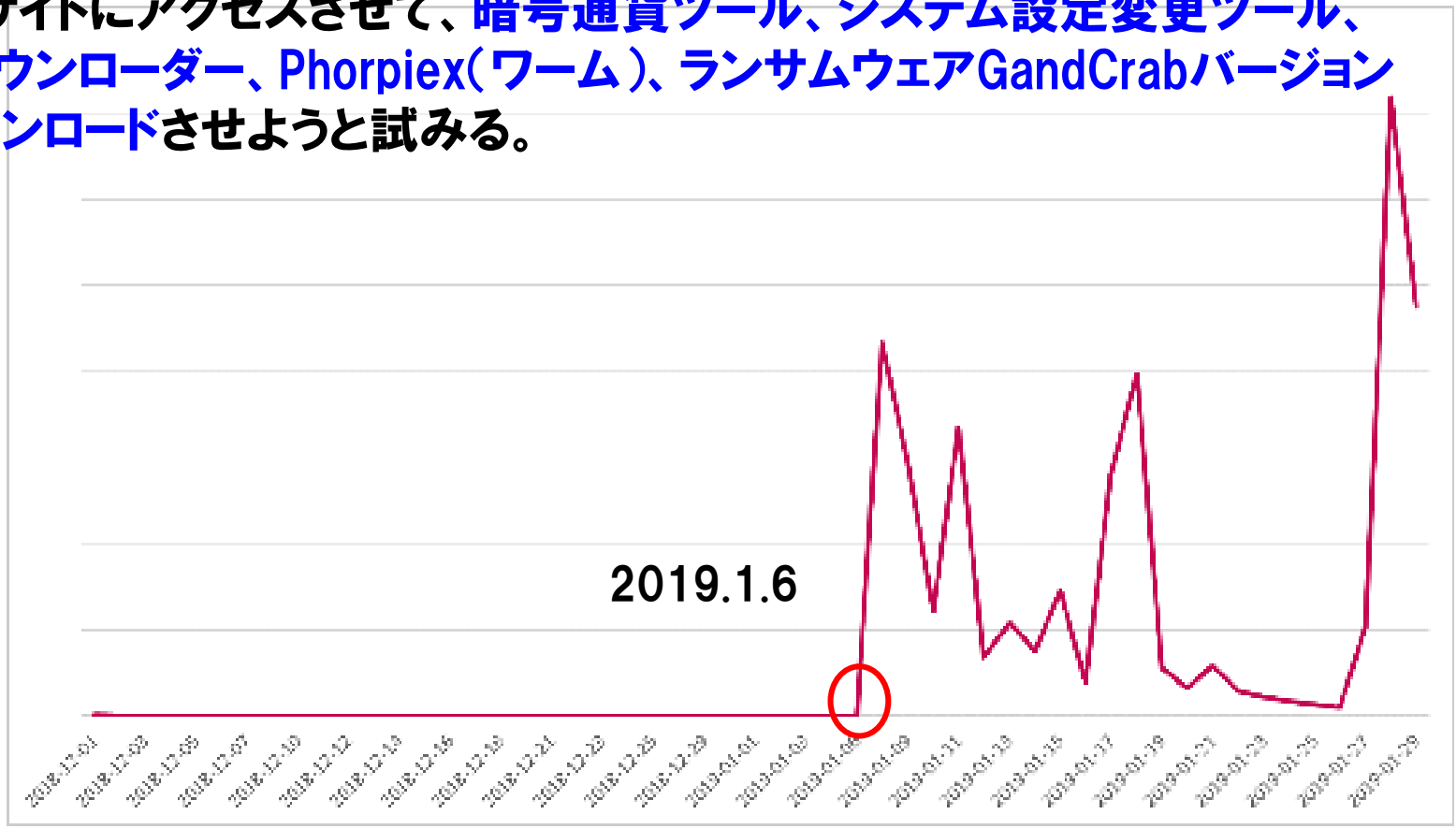


図 1 – Love you キャンペーンの最新の動向推移

攻撃者のネットワーク

ボットネットとは何か？ サイバー攻撃の自動化

NTT DATA

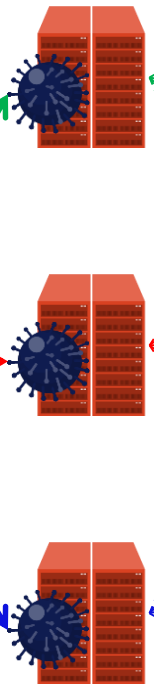
感染PCへ指令を中継する司令塔、放置されたサーバや個人PCが,知らないうちに乗っ取られ悪用される

C&Cサーバ

ボット
（感染PC/ゾンビPC）

ボットは、攻撃者からの命令通りに動作、新機能も随時追加される

攻撃者
（指令者）



・感染活動

・迷惑メール
・フィッシング詐欺

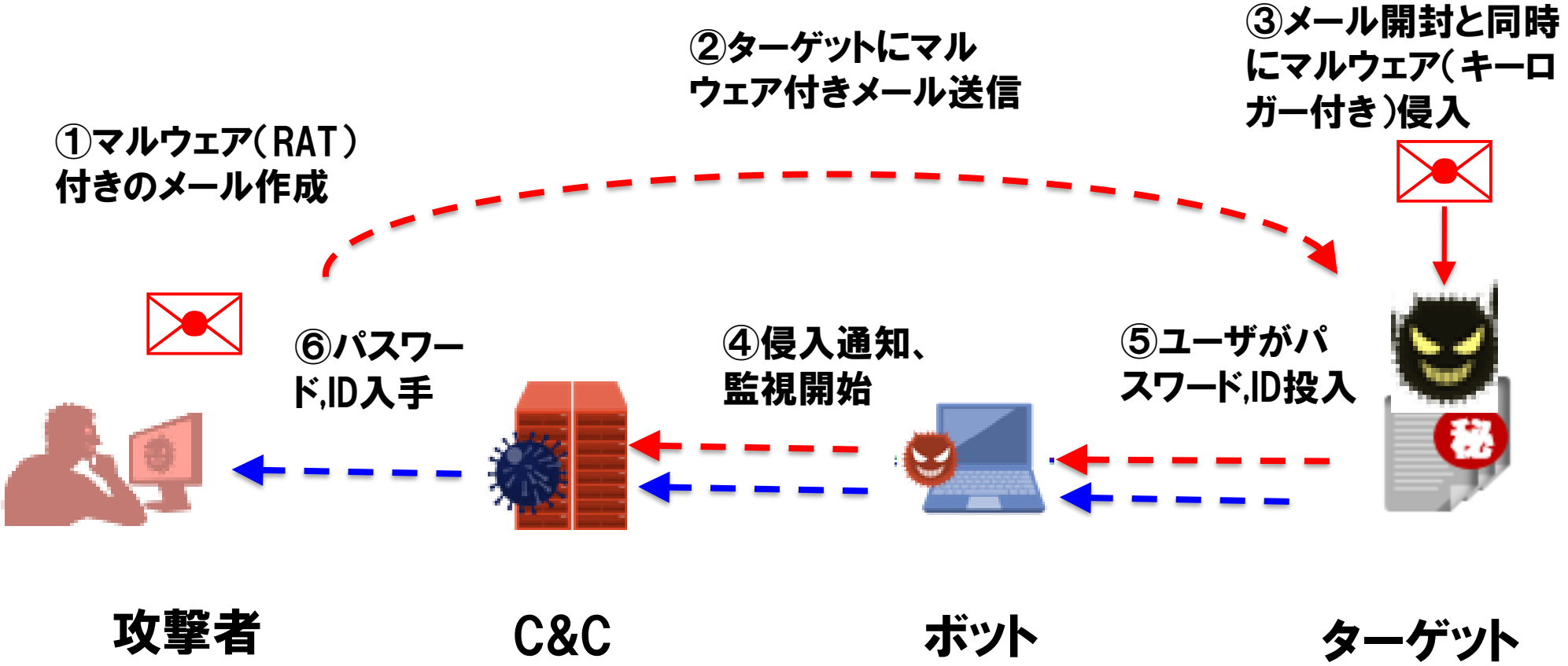
・情報漏洩/盗用
（ID/PWD、アイテム）

・第三者を攻撃
（DDOS）

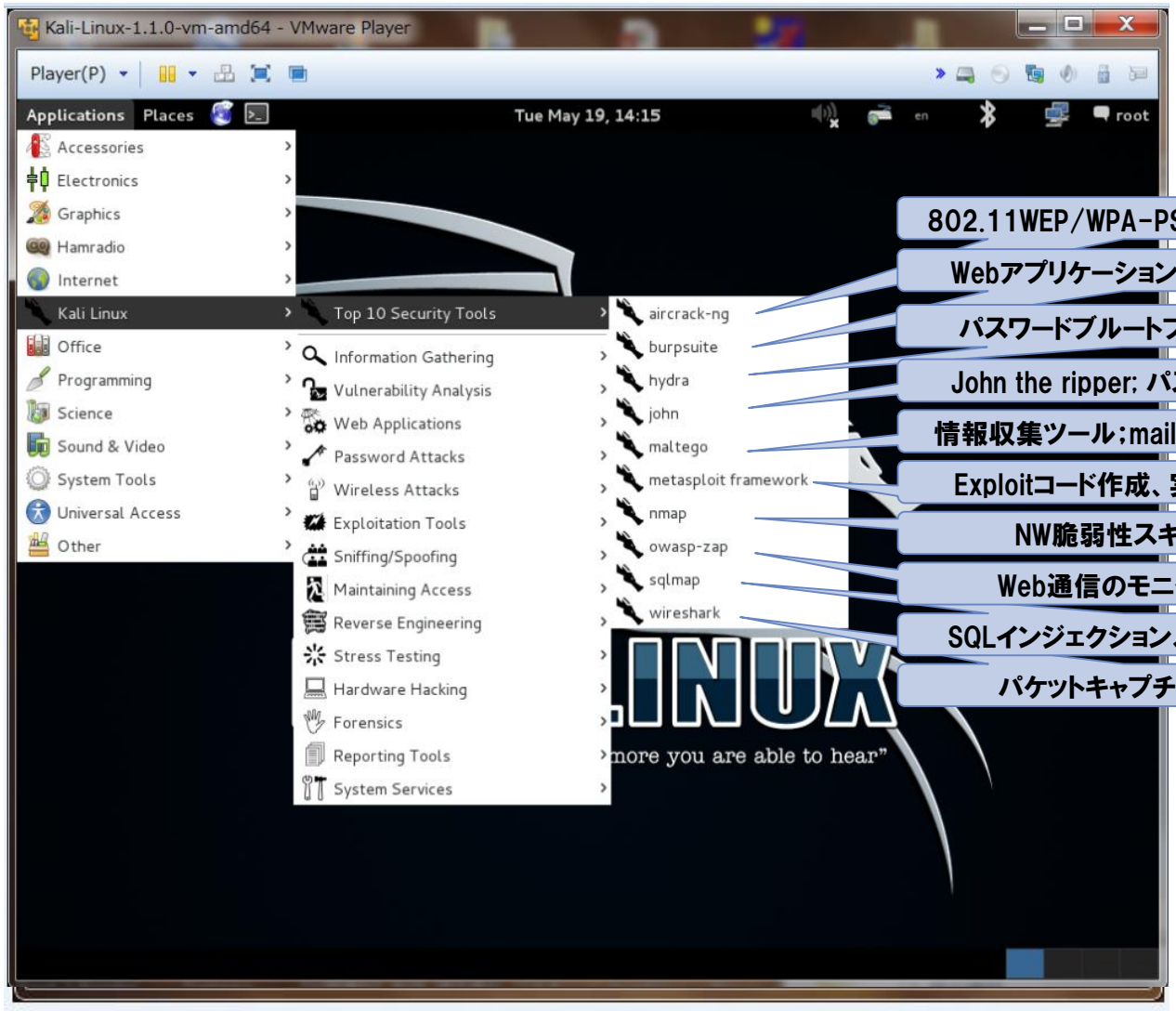
・遠隔操作
・オンラインバンキング
不正送金

出典：Bizコンパス（http://www.bizcompass.jp/）を基に編集

攻撃デモ　シナリオ



高度な統合ツール　Kali Linux



802.11WEP/WPA-PSKクラッキングツール

Webアプリケーション脆弱性検証ツール

パスワードブルートフォース攻撃ツール

John the ripper: パスワード攻撃ツール

情報収集ツール；mail, URL, IPアドレスetc.

Exploitコード作成、実行フレームワーク

NW脆弱性スキャン用ツール

Web通信のモニタ、改変ツール

SQLインジェクション、DB乗っ取りツール

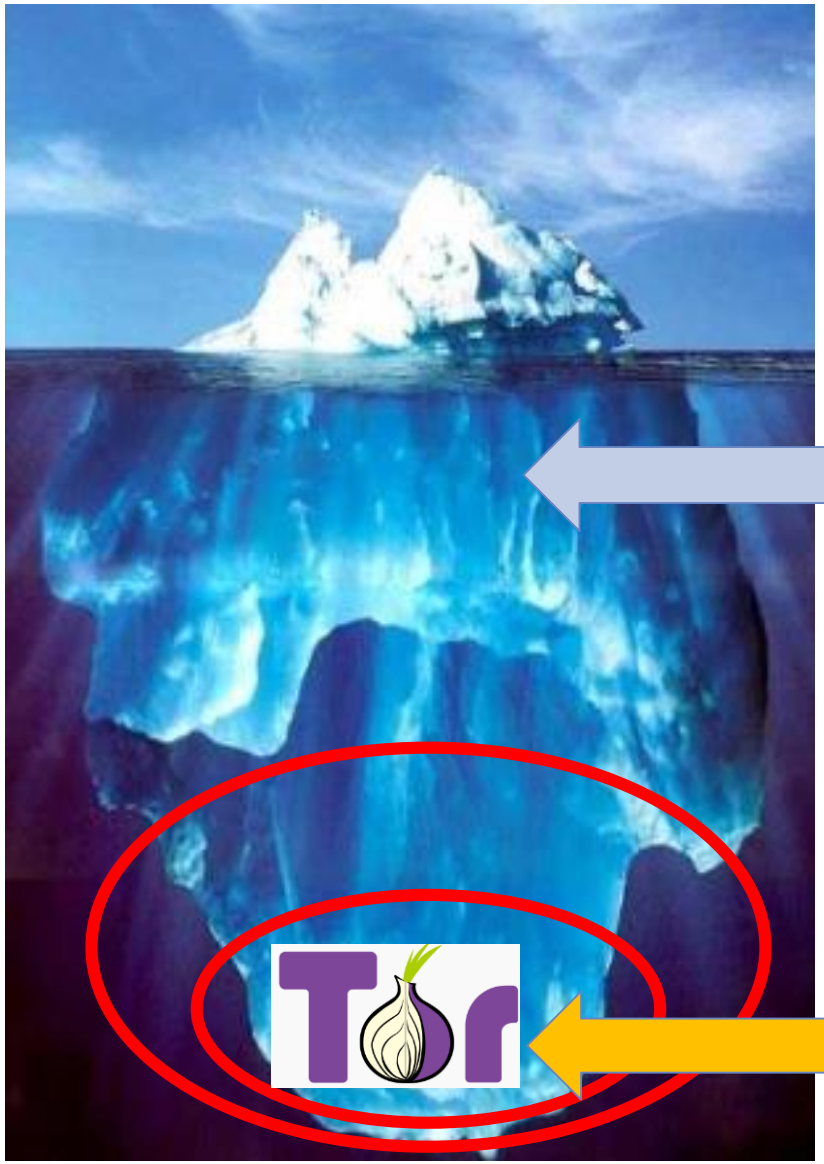
パケットキャプチャ、分析ツール

インターネットの裏世界
Dark Net/Dark Web

インターネットの世界

一般の検索エンジンで見える世界

一般の検索エンジンで見えない世界



正規の会員サイト、企業サイト、ECサイト

匿名性の高いネットワーク

Dark Net

Dark Web

闇サイトSilk Road事件

ロス・ウィリアム・ウルブリヒト容疑者
（Ross William Ulbricht）
テキサス州在住の29歳の青年

2015.1.13
裁判開始

2015.2.4
有罪判決

第二裁判　継続中
殺人容疑

争点：単なるサイトの開発者か、黒幕
Dread Pirate Robertsか

2013.10.1-10.7
主要ディーラーら7名逮捕（米・英・スウェーデン）

2013.10.1
FBIにより逮捕

2014.2
刑事告訴

2015.3.30
関連事件で当局の逮捕者

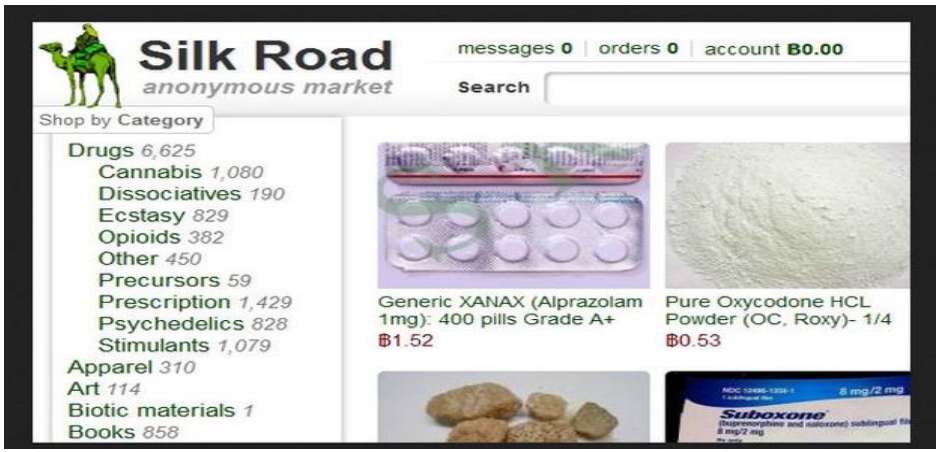
・Silk Roadウォレットから360万ドル相当のBitcoin押収
・ウルブリヒトのPCから約14万4000BTC Bitcoin
（当時のレートで約120億円相当）を押収

元麻薬取締官、元米シークレットサービス　押収したBitcoinの盗難容疑

2011 | 2012 | 2013 | 2014 | 2015

2011.2
Silk Roadサイト開設

2013.10.2
Silk Roadサイト閉鎖



Silk Road：法で規制されている薬物をオンラインで販売するためのプラットホーム（Tor)を、麻薬ディーラーたちに提供する

2011.2～2013.7
・販売者3,877アカウント・購入者146,946アカウント
・総取引数・・・1,229,465件
・総売り上げ・・・12億ドル以上
・ウルブリヒトが得た利益・・・約8千万ドル

なぜこんなことになったか？

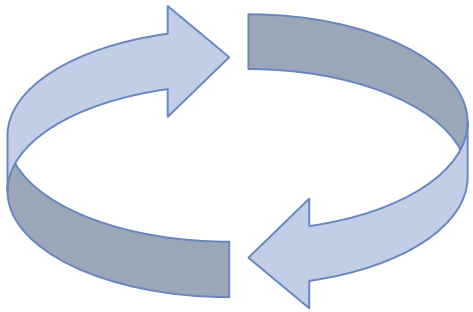
サイバーセキュリティに対する脅威の拡大

NTT DATA

増大

- 金銭
- 示威
- 知財、企業・営業秘密
- 諜報／サイバー戦争

Motivation（動機）



拡大

Opportunity（機会）

- インターネット接続の拡大
- 利用高度化

eCommerce, eBanking etc.

- 重要インフラのIT化

高度化

Measure（手段）

- マルウェア、トロイの木馬, Tor etc.
- DDoS攻撃、APT攻撃 etc.
- ブラックマーケット
- 分業と交換のインフラ

サイバー攻撃の脅威は複雑化

国家レベルのインテリジェンス、サイバー戦

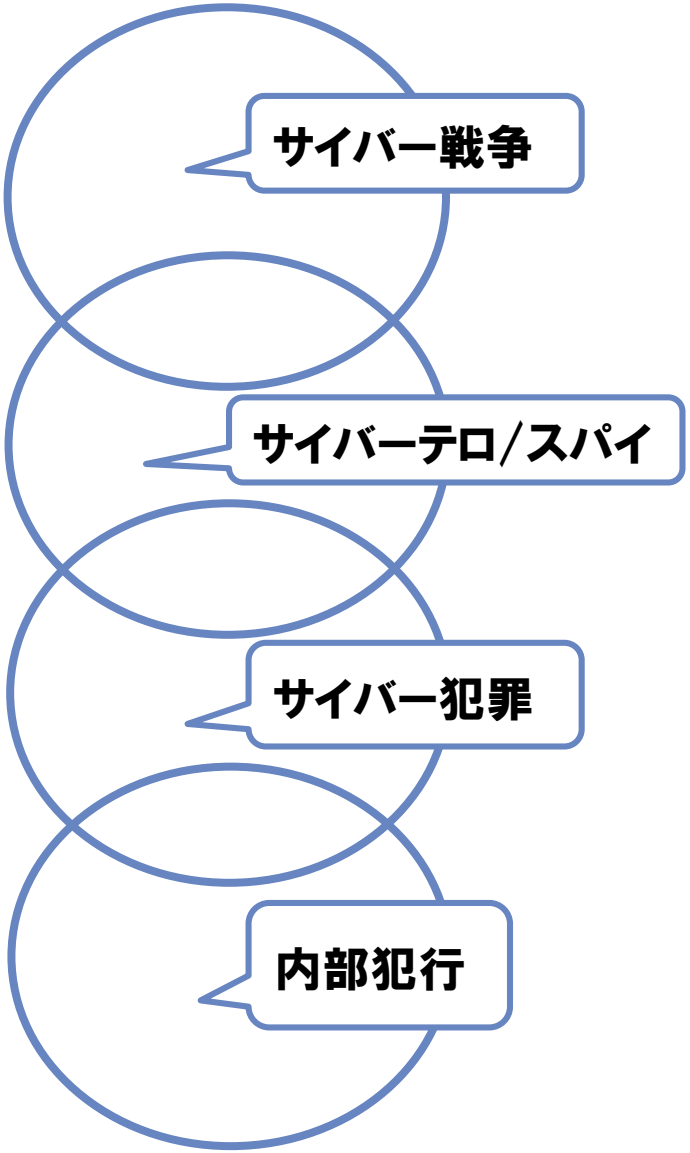
諜報型、　破壊工作型

個人・組織サイバー犯罪

換金型、　物販型

Hacktivist

内部犯行



米国vs中国

人民解放軍の２人の大佐が「超限戦」出版（Unrestricted Warfare）;米国にサイバー戦争で対抗

湾岸戦争

米軍コソボ中国大使館誤爆に対するDoS攻撃

シスコの模造品が販売；多数の政府機関等に導入

FBIが摘発;
http://www.abovetopsecret.com/forum/thread350381/pg1

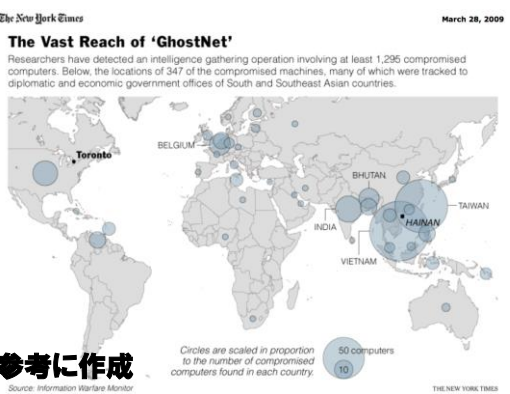
米国の主要企業に対するサイバー攻撃;Google, Lockheed Martin, Adobe, Dow Chemical, NYT

1991 | 1998 | 1999 | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012

・市民ハッカー集団の創設
・米国のソフト・ハードを標的とする幅広いサイバー諜報活動
・自国のサイバー空間防衛の段階的強化
・軍のサイバー戦闘部隊の設立
・米国のインフラ内への論理爆弾の設置

サイバー部隊の設置発表

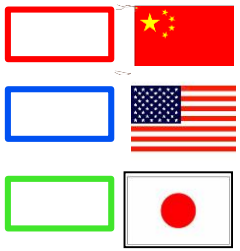
タイタン・レインに代表される侵入が繰り返される。SANSによると広東省のサーバに行き着くことが判明



ゴーストネット発見（カナダ）

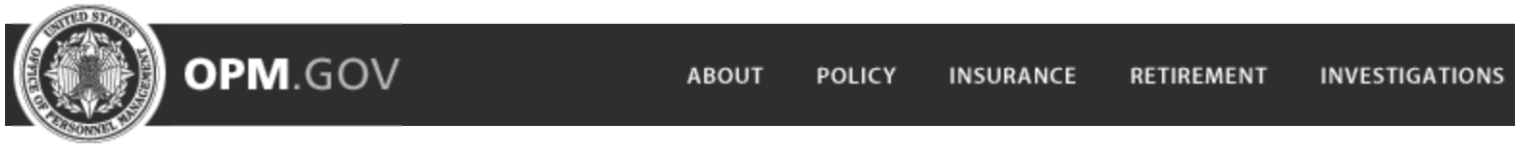
海南島にある人民解放軍陸水信号部隊が米国、日本に侵入と発表（メディアス・リサーチ社）

我が国政府、重要企業へのAPT攻撃の9割が中国（2014に判明；日経新聞）



「世界サイバー戦争」リチャード・クラーク、ロバートネイを参考に作成

OPM情報漏えい（2015.5）の概要



OPM.gov Main >

Infor

政府職員及び契約者等に関する2種類の個人情報が漏洩

What Happened

OPM recently discover
data of Federal goverr

420万の名前、生年月日、住所、社会保証番号

1. In April 2015, OPM di
   government emp
   address and Soc
   OPM in early Jur

2. While investigati
   compromised: in
   employees and
   confidence that s
   was stolen from t
   a background inv
   Some records also
   1.1 million include fingerprints. Usernames and passwords that background investigation applicants used to fill
   out their backgroun
   begun.

・過去、現在及び有望な2100万の社会保証番号に対応した政府関係職員及び契約者のセンシティブな個人情報（SF-86に対応、人事調書、教育経歴、友人、親族、病歴、犯罪歴等を含む）
・110万の指紋情報、個人情報を登録するためのパスワード

スノーデン事件よりも被害が大きい（by Washington Post）

OPM情報漏えいの顛末

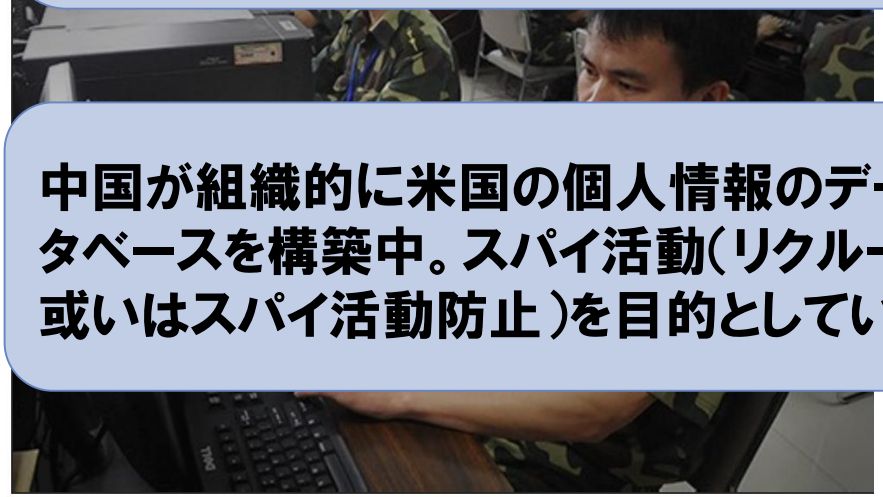
NTT DATA

Sections ≡ The Washington Post

National Security

With a series of major hacks, China builds a database on Americans

中国の”*Deep Panda*”と呼ばれるハッカー集団（政府系）による攻撃と特定。この集団は2014.4に医療保険会社Anthemも攻撃し個人情報が漏えいした。他にも、通信会社、航空会社等にも侵入



中国が組織的に米国の個人情報のデータベースを構築中。スパイ活動（リクルート或いはスパイ活動防止）を目的としている。

米中首脳が会談、サイバー対策で「相互理解」

REUTERS

2015.9.26

すでに行われているCyber Wars

NTT DATA

中東その他

東欧

1982 1989 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015

- 1982: ソビエト連邦シベリアパイプラインの破壊。アメリカ合州国による初めてのサイバー攻撃
- 1989: ソビエト連邦崩壊によりサイバー攻撃の専門家がグローバル市場へ
- 2007: エストニアへのロシアからのサイバー攻撃（5月）。DDoS攻撃から金融機関までが攻撃に晒される
- 2008: グルジアへロシアからのDDoS攻撃。南オセチアの独立問題
- 2009: NATOがサーバー防衛センタをタリンに設置
- 2010: イラク核施設への「スタクスネッツ」攻撃
- 2011: グルジアがロシアハッカーにマルウェア攻撃。写真撮影に成功

- 2012: タリンマニュアル発表。サイバー戦争の定義
- 2014–2015: ウクライナへの親ロシア派からの攻撃。NATO諸国へも波及。一方で、ウクライナからロシアへの攻撃も。

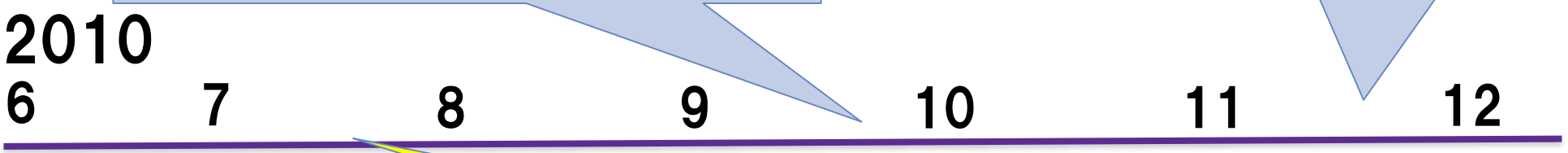
- 2004: イスラエルのシリア核施設攻撃。防空レーダがサイバー攻撃
- 2007: イスラエルvsサウジアラビア/UAE。サーバー攻撃が双方で行われる。
- 2010: インドvsバングラディシュ。ハクティビスト主体
- 2011: イスラエルvsパレスチナ アノニマスがイスラエルのサイトを攻撃
- 2012: サウジアラビアvsイラン。サウディの国営石油会社アラムコの施設が攻撃される（シャムーン）

http://matome.naver.jp/odai/2135553765085320501

Stuxnetの顛末

2010年9月28日:イラン鉱 工業省の情報技術部門幹部の話によると、イランが海 外から大規模なサイバー攻撃を受けており、産業用パ ソコン約3万台に感染が見 つかった。（トレンドマイクロ）

2010年11月16日:IAEAによりイ ラン中部ナタンツのウラン濃縮 施設で、約8400 台の遠心分 離機がすべて停止していること が確認される。（毎日.jp）

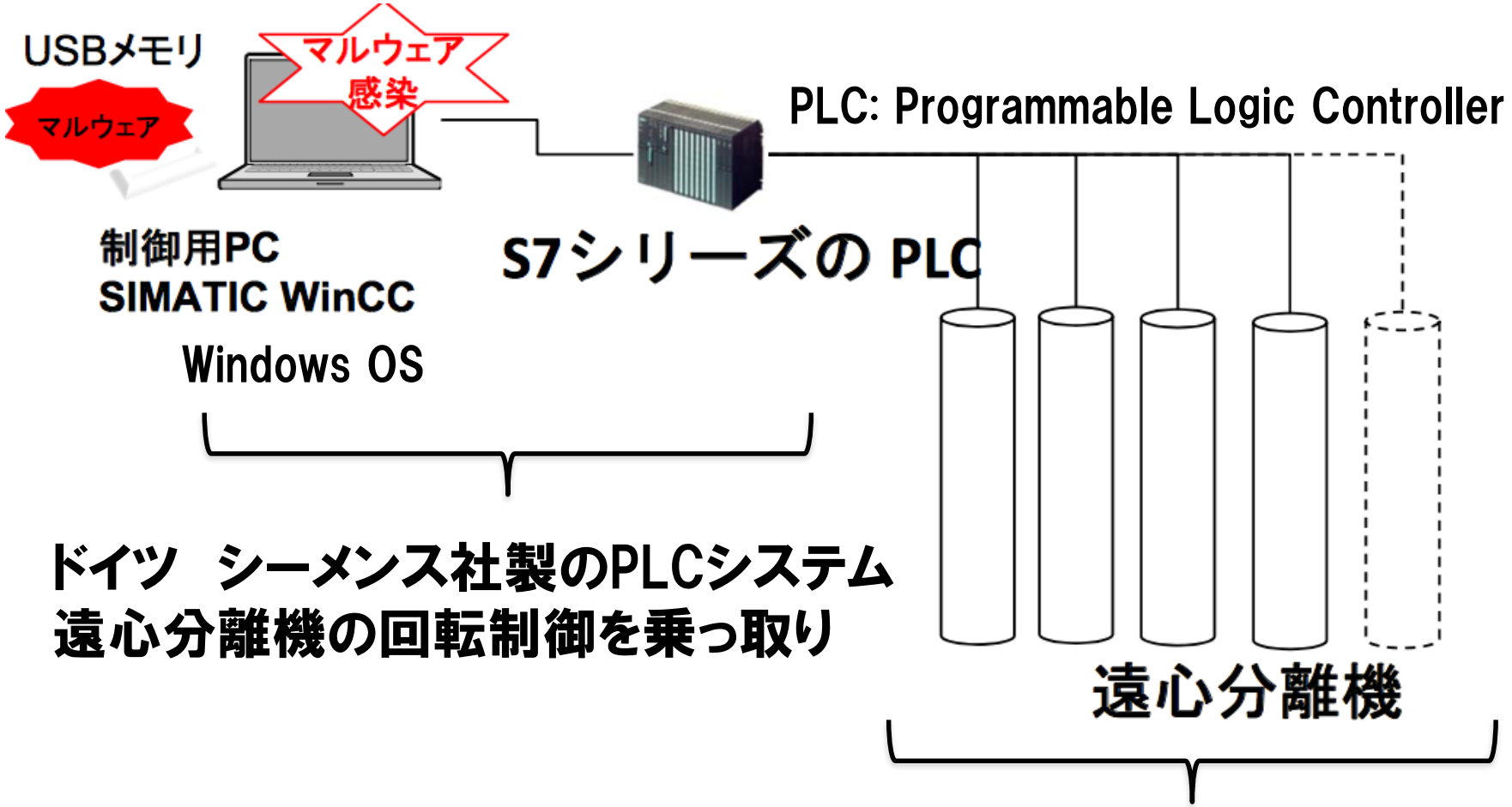


2010年6月17日:ベラ ルーシに拠点を置くアンチウイルス会社VirusBlokAda社がマルウエアのサンプルを発見（世界的にはこの時点で注目はされていなかった）

2010年7月15日:セキュリ ティブロガーBrian Krebs がVirusBlokAda社の発見を報告
2010年7月16日:VeriSignが、Stuxnetに使われたコード署名 用の証明書を無効化
2010年7月16日:Microsoftか ら、関係する最初のセキュリティ アドバイザリ（2286198）が公開（Windowsシェルの脆弱性）

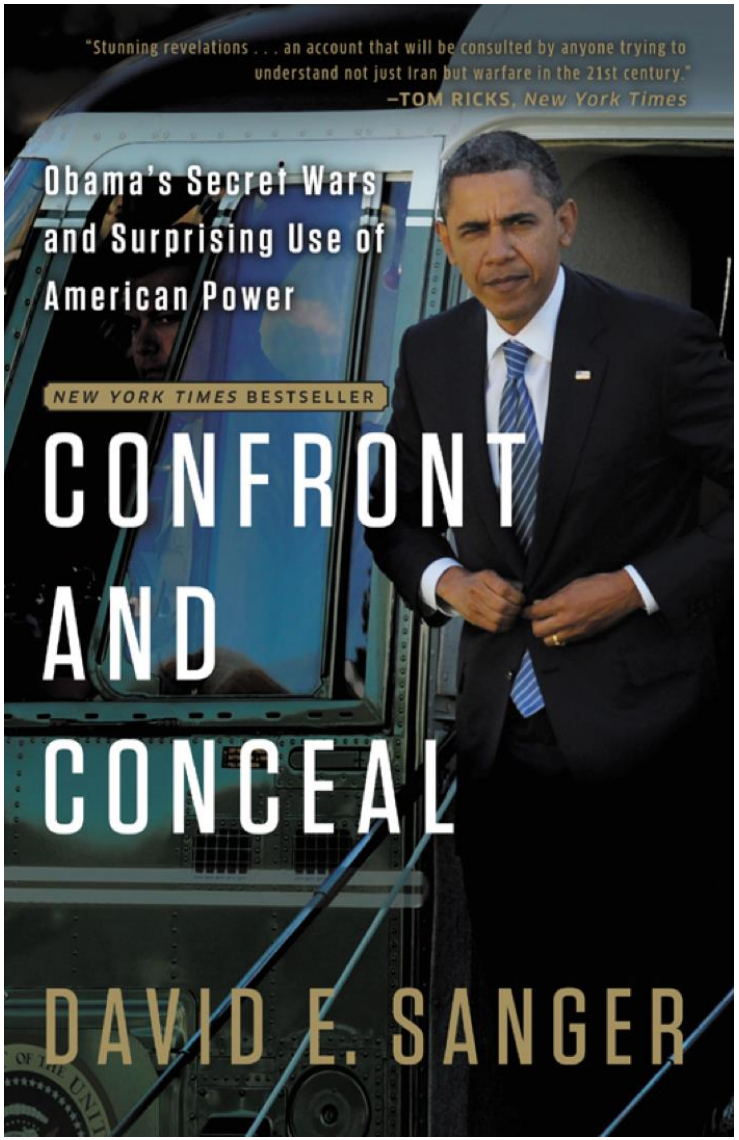
何が行われたか？

イラン中部ナタンツのウラン濃縮施設



ドイツ　シーメンス社製のPLCシステム
遠心分離機の回転制御を乗っ取り

異常回転により破壊される



・Stuxnetはブッシュ政権時代2006年から開始されたコードネーム”Olympic game”によって開発された。

・この計画は、イランの核開発を阻止するためにサイバー攻撃を仕掛けるものであり、米国及びイスラエルによって開発が実行された。

・コードの規模は通常のマルウェアの50倍。

・2010年6月オバマ大統領就任直後にプログラムミスによってStuxnetが拡散してしまう。ここで、イランへの攻撃を実施するか、中止するかの判断が行われ、最終的に実施された。

・この攻撃の後、イランにはサイバー戦部隊が設立された。

2012.6 NYタイムズ

http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=1&_r=3

原子力施設への攻撃

2015.3.17

・韓国政府は、北朝鮮がサイバー攻撃を実行し、韓国水力原子力発電株式会社から機密情報を盗んだとする報告書を発表。
・韓国のソウル中央地方検察庁が3月17日に発表した声明によると、「今回のハッキングに使用された悪意あるコードは、北朝鮮のハッカーたちが使用する、いわゆる『kimsuky』マルウェアと、構造や機能が一致。

2016.4.27

・ドイツ、グントレミゲン原子力発電所の燃料棒監視システムでマルウェアが発見された。
・コンピュータシステムだけでなく、汚染されたUSB18個も同じく発見された。
・このシステムは2008年に導入されて以降パッチが当てられていなかった。また、インターネットには接続されていなかったため実害はなかった。

AFP BB NEWS

2012.10.22

中東を舞台に「サイバー戦争」、米・湾岸諸国の石油企業が標的に

・サウジアラビアの国営石油会社サウジアラムコのコンピュータ30万台がサイバー攻撃により被害。
・マルウェアは「**シャムーン**」と名付けられている、**極めて高度なもの**。
・他に、エクソンモービル、カタール・ペトロリアムの合弁会社ラスガスも攻撃を受けた。
・イスラエルも同様の攻撃を受けていることを認める

Bloomberg

2016.12.1

サウジアラビアに大規模なサイバー攻撃、空港当局のＰＣ数千台を破壊

REUTERS

2016.12.1

サウジにサイバー攻撃、ウイルス「シャムーン」　4年ぶりに新型

FireEye

2017.9.20

Insights into Iranian Cyber Espionage:

・2013頃より活動を開始。
・現在までに米国、サウジ、韓国の「航空宇宙セクタ」及び「石油精製・化学系産業」に対する諜報活動と見られる
・活動は「土曜から水曜」

サイバー攻撃とフェイクニュースの実例

NTT DATA

BBC

サウジなど中東5カ国がカタールと断交 「テロ集団を支援」と非難

2017.6.5

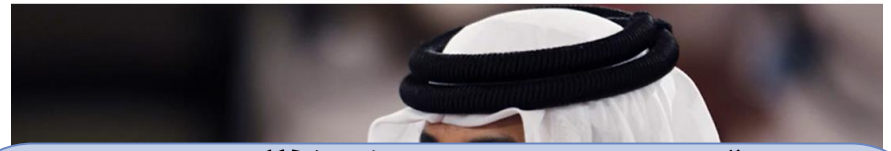
サウジアラビア、エジプト、バーレーン、アラブ首長国連邦（UAE）、イエメンの中東5カ国は5日、カタールとの国交を断絶すると発表した。5カ国はカタールがイスラム主義組織ムスリム同胞団などテロ集団を支援し、地域不安定化の原因を作っていると非難している。

The Washington Post
Democracy Dies in Darkness

2017.7.16

National Security

UAE orchestrated hacking of Qatari government sites, sparking regional upheaval, according to U.S. intelligence officials



・カタール国営通信へのハッキングで、カタールの首長が「イラン、ハマスを称賛した」と言うフェイクニュースを流す（5.25）。
・これを直接の口実としてサウジ、UAE等5か国がカタールと断交
・しかし、これはUAEによって仕組まれたものとの調査結果が出ている。

他人事ではないかも

日本経済新聞

中国、サイバー選挙介入か　カンボジアで「予行演習」

2018/8/18 2:00 | 日本経済新聞　電子版

中国が近隣国への政治介入を狙ってサイバー攻撃技術の開発に乗り出した疑いが浮上した。7月29日に総選挙があったカンボジアで大規模な「予行演習」が観測され、今後はアジアを中心に情報操作や選挙工作を広げる可能性がある。介入の主な舞台となるのが新興国でも急速に普及するＳＮＳ（交流サイト）だ。「データエコノミー」の到来は世界に便利さをもたらす一方、民主主義を揺らし始めた。

6月。米国在住のケム・モノビシャ氏に不思議な文面のメールが届いた。「裁判を傍聴しましたが、保釈が認められなかったのは残念です。状況は悪化していますね」

総選挙を控えたカンボジアに、中国がサイバー攻撃を繰り返している（ＡＰ）

出身国カンボジアの有力な人権団体からで、送り手も実在の人物だ。「最初は全く不自然とは思わなかった」。だがよく見ると無料のメールアカウントから送られている。知人を介し、米セキュリティー大手ファイア・アイに調査を依頼した。

中国が模倣するロシアのサイバー政治介入

- フェイスブックの偽アカウント、自動投稿ボットを駆使した偽情報の流布
- 選挙システムに侵入し、選挙制度への信頼を破壊
- サイバー攻撃で、ロシアと敵対する勢力の情報を盗みリーク
- フランスの右翼政党に資金支援、ドイツの反移民政党の選挙支援
- 電力網などインフラをサイバー攻撃し社会不安をあおる

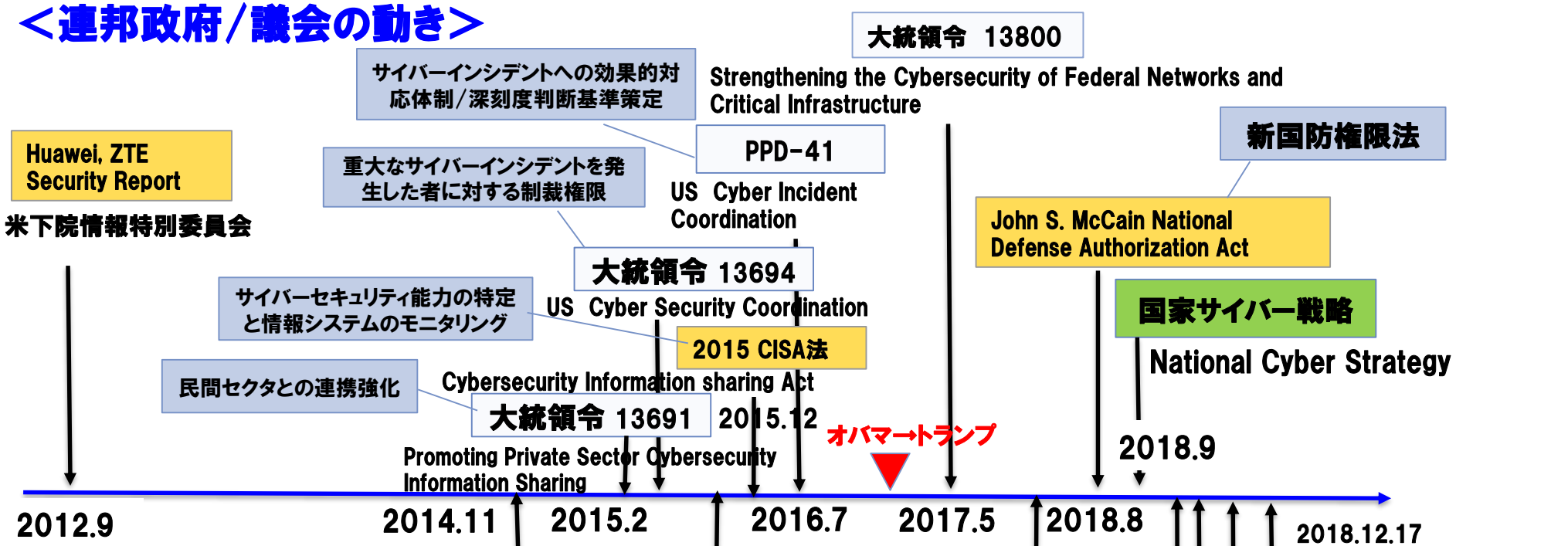
（出所）米ブルッキングス研究所の報告書

最新の米国の状況と事例

米国における最近のサイバーセキュリティ対応の経緯

NTT DATA

＜連邦政府/議会の動き＞



＜具体的事案＞

2015.6

Sony Picture 攻撃

OPM ハッキング

北朝鮮と特定　中国人民解放軍と特定

北朝鮮Park Jin Hyok(Lazarusメンバ)を以下の容疑で正式に訴追(拠点は中国大連)

- The WannaCry ransomware outbreak of 2017;
- Attempts of hacking US defense contractor Lockheed Martin in 2016;
- The 2016 Bangladesh Central Bank cyber-heist;
- The breach at Sony Pictures Entertainment in 2014;
- Breaches at US movie theatre chains AMC Theatres and Mammoth Screen in 2014;
- A long string of hacks of South Korean news media organizations, banks, and military entities across several years, and;
- Hacks of banks all over the world from 2015 through 2018.

2018.9.6

2017.11.27

中国セキュリティ企業の社員3名が米国ハイテク企業3社の企業秘密を窃取

2018.12.17

APT10グループに所属の2人の中国人を起訴(2006年より侵入を繰り替えす)

2018.10.30

5年以上にわたり米国とフランス企業協働開発のターボファンエンジンの秘密情報を窃取した江蘇省中国公安要員を起訴

2018.10.10

米国航空機関連企業から企業秘密を窃取した中国公安要員を起訴

北朝鮮要員によるサイバー攻撃

NTT DATA

FBI捜査官　Nathan P. Shield　起訴状

2018.9.6　米国司法省HPより公表

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT COPY

for the

Central District of California

FILED
CLERK, U.S. DISTRICT COURT
JUN - 8 2018
CENTRAL DISTRICT OF CALIFORNIA
BY DEPUTY

United States of America

v.

PARK JIN HYOK, also known as ("aka")
"Jin Hyok Park," aka "Pak Jin Hek,"

Defendant.

Case No. MJ 18-1479

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

Beginning no later than September 2, 2014 and continuing through at least August 3, 2017, in the county of Los Angeles in the Central District of California, the defendant violated:

Code Section	*Offense Description*
18 U.S.C. § 371	Conspiracy
18 U.S.C. § 1349	Conspiracy to Commit Wire Fraud

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

Good Job!!

/s/
Complainant's signature

Nathan P. Shields, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 06-08-18

ROZELLA A. OLIVER
Judge's signature

City and state: Los Angeles, California

Hon. Rozella A. Oliver, U.S. Magistrate Judge
Printed name and title

AUSAs: Stephanie S. Christensen, x3756; Anthony J. Lewis, x1786; & Anil J. Antony, x6579 REC: Detention

Park Jin Hyok

別名
"Jin Hyok Park,"
"Pak Jin Hek,"

- The breach at Sony Pictures Entertainment in 2014.10
- Breaches at US movie theatre chains AMC Theatres and Mammoth Screen in 2014.11

- A long string of hacks of South Korean news media organizations, banks, and military entities across several years, and: Hacks of banks all over the world from 2015 through 2018.

- Attempts of hacking US defense contractor Lockheed Martin in 2016;

- The 2016.2 Bangladesh Central Bank cyber-heist

- The WannaCry ransomware outbreak of 2017

サイバー攻撃のタイムライン

2015 2016 2017 2018

2014.11 攻撃判明

SONY PICTURES

“The Interview”公開に対する攻撃
公開予定の映画館チェーンAMCも攻撃される

2015.5 2016.2 攻撃判明 世界中の金融機関に対するハッキング

BANGLADESH BANK

バングラディシュ中央銀行

Philippine Bank

国際金融ネットワークSWIFTを
利用した金銭窃取

Southeast Asia Bank

2009~2013

韓国の金融機関、メディア、国防機関
に対する攻撃“Dark Soul”
”Operation Tory”

THAAD配備決定

2015.10

LOCKHEED MARTIN

“THAAD”配備に対する攻撃の模様

2017.5

ランサムウェア”WannaCry”拡
散。身代金取得目的？

攻撃の拠点　Chosun Expo

NTT DATA

・容疑者は北朝鮮の金策工業大学*を卒業後2002年よりChosun Expoにプログラマ（VC++）として勤務。Chosun ExpoはLab110として知られる北朝鮮のハッキンググループに関連していると推定されている。

・2011～2013年まで大連で勤務していた模様。SPE攻撃が行われた2014初頭に帰国。

・Chosun Expoは大連の北朝鮮のフロント企業。2002年よりソフトウェアの開発受託を行っていた。元々は韓国とのジョイベンでスタートするが、途中で韓国が撤退。ゲームソフト、ネットカジノ等の開発、及びフリーランスのソフト開発請負（VC++の表示あり）。

・発注先には米国企業もある模様。→　米国企業に対する攻撃のHOPとして使われていた。

＊朝鮮コンピューターセンター（1990年設置）のエンジニアを養成する大学

Chosun Expo　38 NORTH

Tweet

Site Name: Chosun Expo

Site address: http://www.chosunexpo.com

Organization: Chosun Expo

Site host: KPTC

Domain registration: Korea Lotto Joint Venture

Site Contents: Korean-language online shopping site offering various North Korea goods. The domain name is registered to the “Korea Lotto Joint Venture,” a company that previously operated an online casino based in North Korea. The server is the only website still remaining inside a group of Chinese Internet addresses assigned to the DPRK’s telecom operator.

Sony Pictures Entertainment に対するサイバー攻撃

NTT DATA

2014年11月

SONY PICTURES

- NWに侵入され機密情報を奪われ、公開される
- 数千台のコンピュータが使用不能に陥る
- 複数の経営幹部、映画出演者に映画の中止、金銭要求等の脅迫メールが届く

2014年12月

amc

“The Interview”を上映予定の映画チェーンの従業員へ脅迫メールが届く

2015年1月

- オバマ大統領がFBIの調査結果に基づき北朝鮮への追加制裁を発表
- 北朝鮮の3団体（情報機関、主要な武器取引を行っている貿易会社、軍事防衛技術の調達に従事している貿易会社）と、これらの団体や北朝鮮政府で働く個人10名を対象

*英国の劇場（Mammoth Screen）も北朝鮮関連の演劇をアナウンスした2014.8からSPEと同様の偵察活動が行われていたことが判明している。

Sony Picture Entertainment 向け サイバーキルチェイン

NTT DATA

数年間に及ぶ活動が認められる

SEP向けは2014始めから本格化？

SPEのケースでは約2カ月の活動が認められる

2014.9

2014.11

攻撃インフラ構築 → **ターゲットに対する偵察活動** → **ターゲットへの侵入** → **活動**

・マルウェアの入手/開発
・踏み台(ボットネット)構築
・偽アカウントの構築
- Gmail/hotmail等アカウント
- ワーム“Brambul”
- Proxy Service
- DDNS
- Tor

インフラ自体は他の攻撃にも利用される

- 同一のアカウントを複数のuser或いはsubjectsで利用している
- 正規のSNSからのメッセージを改竄して送信

・標的とする組織、個人情報の収集
- メールアカウント収集
- トラッキングサービスの利用
- business records search servicesの利用
- 利用しているソフトウェアとその脆弱性調査
- 個人の趣向（例えば北朝鮮に関する興味の有無）
・spear-phishing メッセージ/Social engineering
- Facebook, Googleからのメッセージを装う

・侵入により獲得したシステム情報、アカウント情報に基づくマルウェアのカスタマイズ(”Destover”)
・システムに保存されている情報の詳細な調査
・ソーシャルメディアを利用した標的型攻撃

FB, Gmail, Twitterのアカウントを利用して”The Interview”出演者にマルウェアを送る

・営業秘密情報、財務情報収集、改竄
・ITシステムの改竄、破壊
・脅迫行為
・機密情報の開示

脅迫状
We’ve got great damage by Sony Pictures. The compensation for it, monetary compensations we want. Pay the damage, or Sony Pictures will be bombarded as a whole. You know us very well. We never wait long. You’d better behave wisely.
From God’sApstls

攻撃インフラ構築

NTT DATA

AS4837 (China Unicom)
210.52.109.0/24(借りてる)

AS131279
北朝鮮のIPアドレス(2009～)
175.45.176.0/24
(このうちの7つのアドレスが使用)

攻撃インフラ
利用された攻撃インフラは、自前の"ボット"ネットワークだけでなく、フリーのメールサービス、SNSまた攻撃元を隠蔽するためのダイナミックDNS, Proxy Serviceを活用していた。

インターネット

Proxy Service

GmailやHotmailアカウントへのアクセスを隠蔽するために利用

Dynamic DNS

①アカウント作成
xxx@gmail.com
(再設定用のメルアドはhotmail)

②マルウェア侵入
(ドライブバイダウンロード等)

③情報をメールで攻撃者作成のアカウント(xxx@gmail.com)へに送信

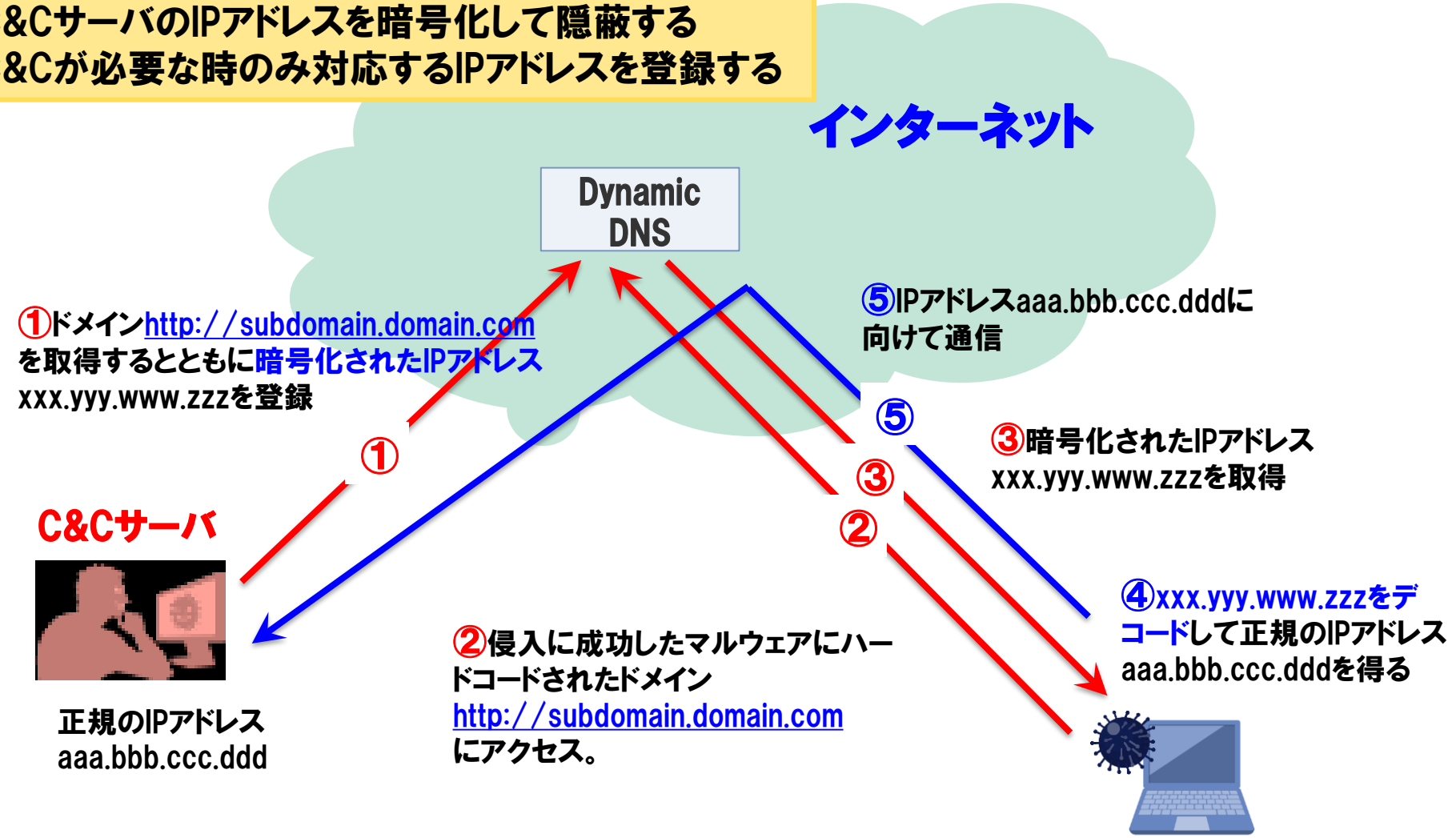
"Brambul"

Hop point
次の攻撃の拠点

Brambul
ワームの一種、2009年に報告される。侵入したPCが利用する共有サーバの脆弱性(SMB)を利用して自己増殖。侵入したPCの情報、ユーザのID/パスワードを取得してメールで攻撃者に通知。

Dynamic DNSの利用

フリーのDynamic DNSを利用して
①C&Cサーバの**IP**アドレスを暗号化して隠蔽する
②C&Cが必要な時のみ対応する**IP**アドレスを登録する



ターゲットへの侵入/フィッシングメール

NTT DATA

“Malicious activities are detected.”というGmailからの偽メッセージを利用

実在する従業員の名前

ここにFishing siteのURLを仕込む

http://www.fancug.com/link/facebook_en.html

マルウェアの侵入と活動

NTT DATA

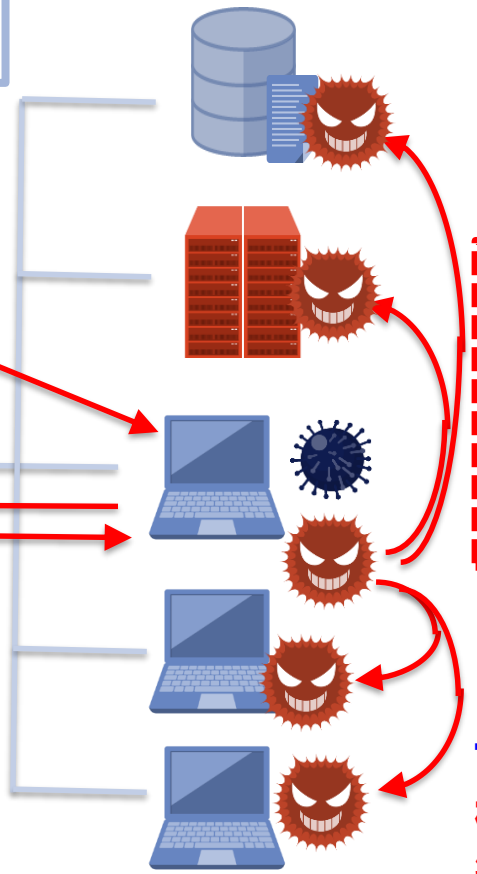
Fishing

①バックドア（C&Cサーバ のIPアドレスに紐づく DDSNのURL）付きのページをダウンロード。

C&Cサーバ

インターネット

②端末へのアクセス権を取得するとともに、様々なマルウェアをダウンロード



③様々な活動の実施
・各種クレデンシャル情報の取得
・内部ネットワークの様々なシステムに侵入
・C&Cサーバとの通信
・機密情報の取得
・データの改竄
・システムの破壊
・侵入痕跡の消去

マルウェアは目的に応じて様々な機能モジュールの組み合わせで作成される

バングラディシュ中央銀行からの不正送金

NTT DATA

消えたバングラ中銀の外貨準備、カジノで使用か

NY連銀の口座からフィリピンとスリランカの口座に113億円

記者会見で辞任を発表するバングラデシュ中銀のラーマン総裁（15日） PHOTO: A.M.

デジタルセキュリティー大手の調査関係者は、アジアの銀行に対するサイバー攻撃の背後にいる犯人を特定したと信じている。それは北朝鮮の金正恩氏だ。外貨獲得のため、紙幣偽造、麻薬密輸、奴隷労働を長年行ったあと、この独裁者は史上初めて国家支援によるデジタル上の銀行窃盗をしでかした可能性があるのだ。

【ダッカ（バングラデシュ）】ある週末、ニューヨーク連銀にあるバングラデシュ銀行（中銀）の口座から何者かが正式なパスコードを使って外貨準備約1億ドル（約113億円）を不正送金する事件が発生した。ここで何が起こったのかについては、現在も4カ国の当局が全容解明に取り組んでいる。（2016．3．17　WSJ）

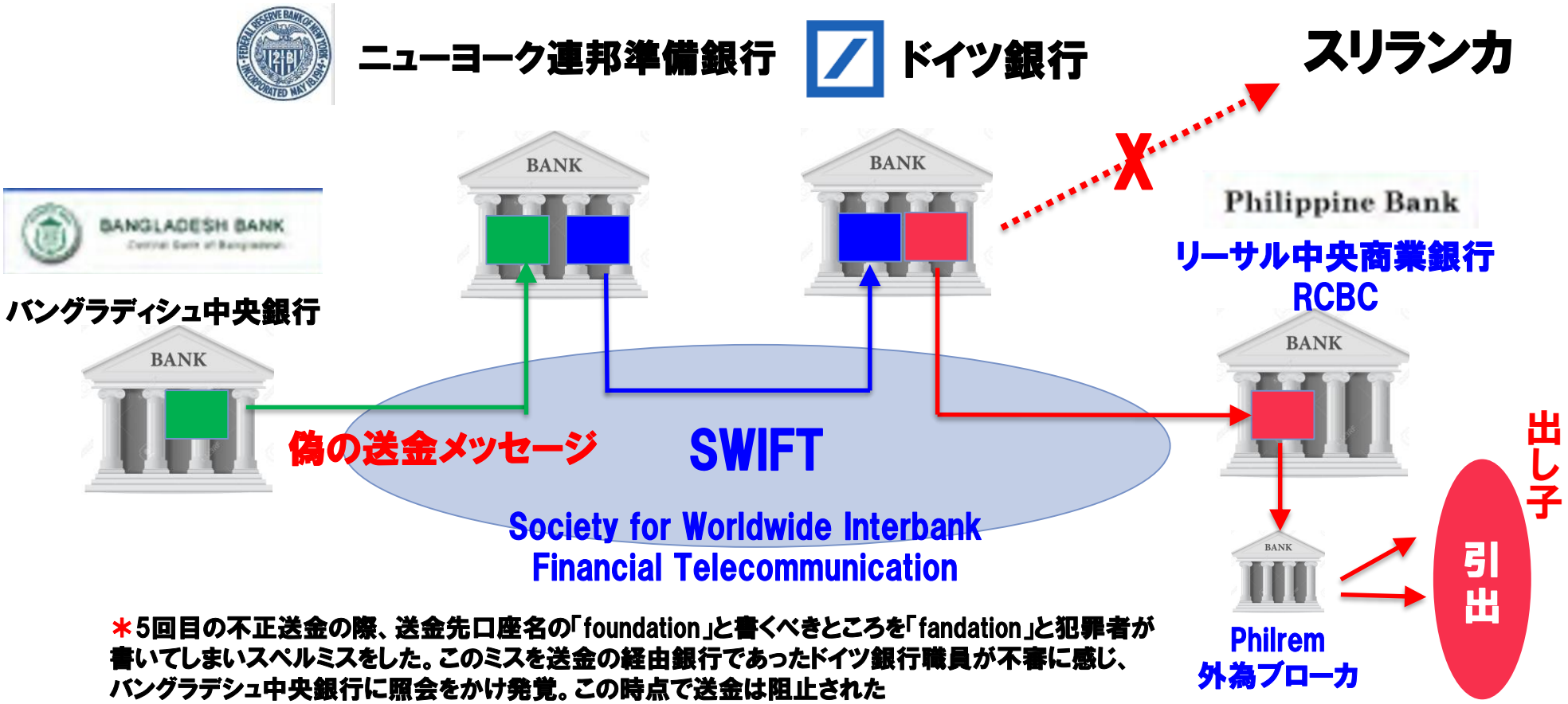
【社説】金正恩氏があなたの銀行をハッキングする時

2016．6．2 WSJ

何が行われたか？

NTT DATA

・2016.2.4バングラディシュ中央銀行より不正送金開始（この日バングラディシュは休日）
・不正送金の被害を受けた金額総額は約1億100万ドル。その内2016年3月10日時点で回収ができていないのは約8100万ドル。（約92億円）
・全部で35回の不正送金指示、最初の4回が成功、5回目のスリランカ向けで失敗・発覚＊



＊5回目の不正送金の際、送金先口座名の「foundation」と書くべきところを「fandation」と犯罪者が書いてしまいスペルミスをした。このミスを送金の経由銀行であったドイツ銀行職員が不審に感じ、バングラデシュ中央銀行に照会をかけ発覚。この時点で送金は阻止された

サイバーキルチエーン

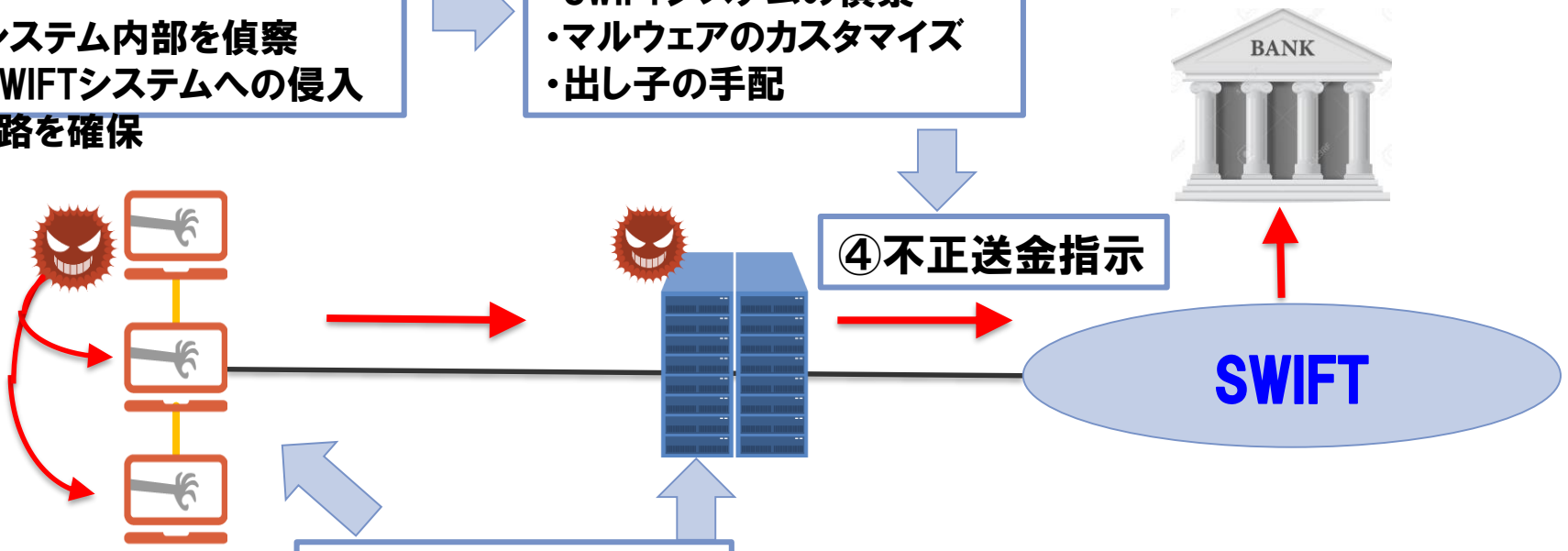
NTT DATA

①調査活動
・SWIFT関連マニュアル調査
・ターゲットの委託業者調査
・マルウェア等の情報収取

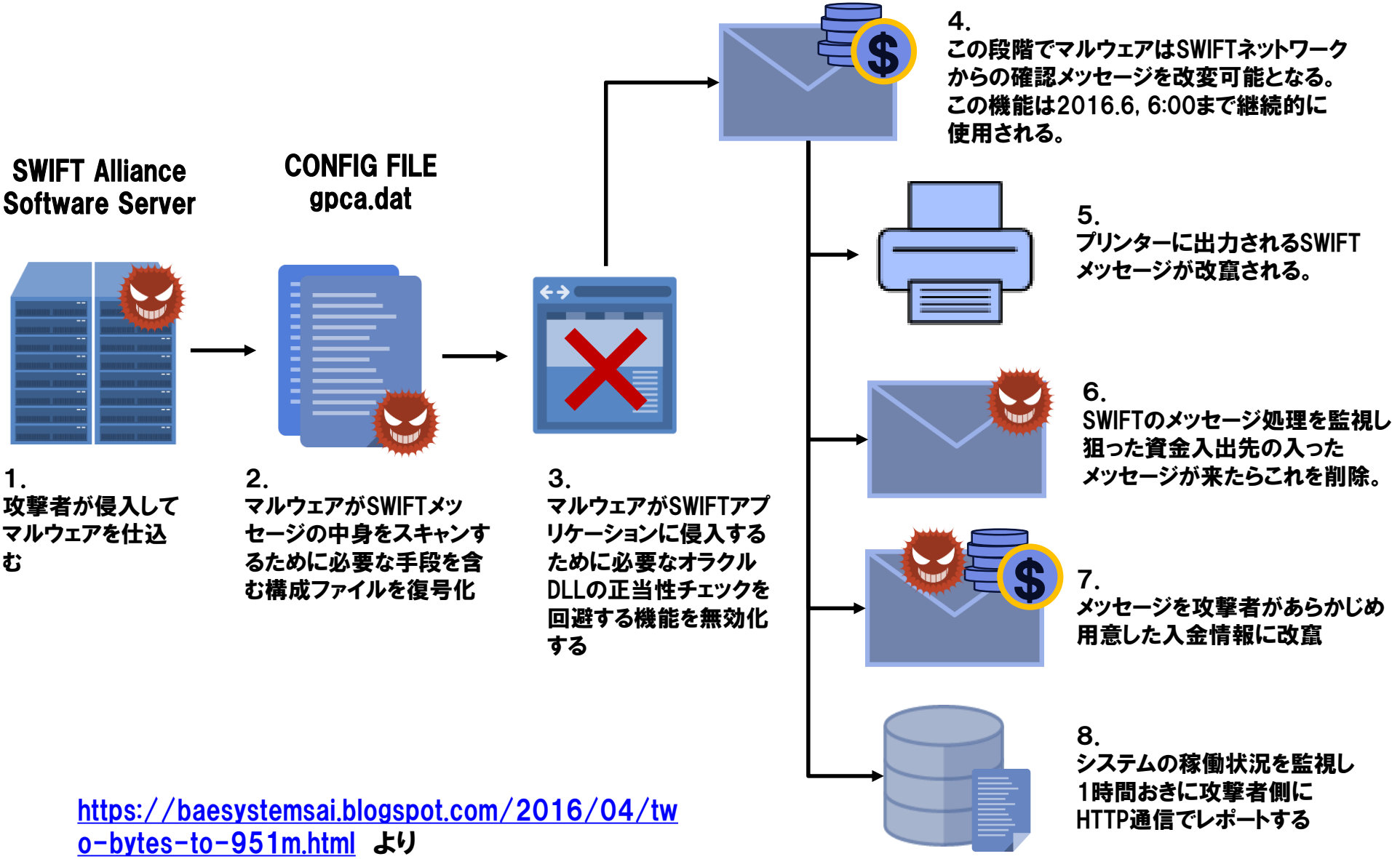
システム/プロセスの脆弱性
・バングラディシュ中央銀行のシステムはファイアウォールも無い極めて脆弱なシステムであった。
・システムの運用保守は業者に委託され、送金確認のみを行員が行っていた

②脆弱なシステムへの侵入
・システム内部を偵察
・SWIFTシステムへの侵入経路を確保

③攻撃準備
・SWIFTサーバへの侵入
・SWIFTシステムの偵察
・マルウェアのカスタマイズ
・出し子の手配



SWIFTサーバへの侵入と不正送金の仕組み

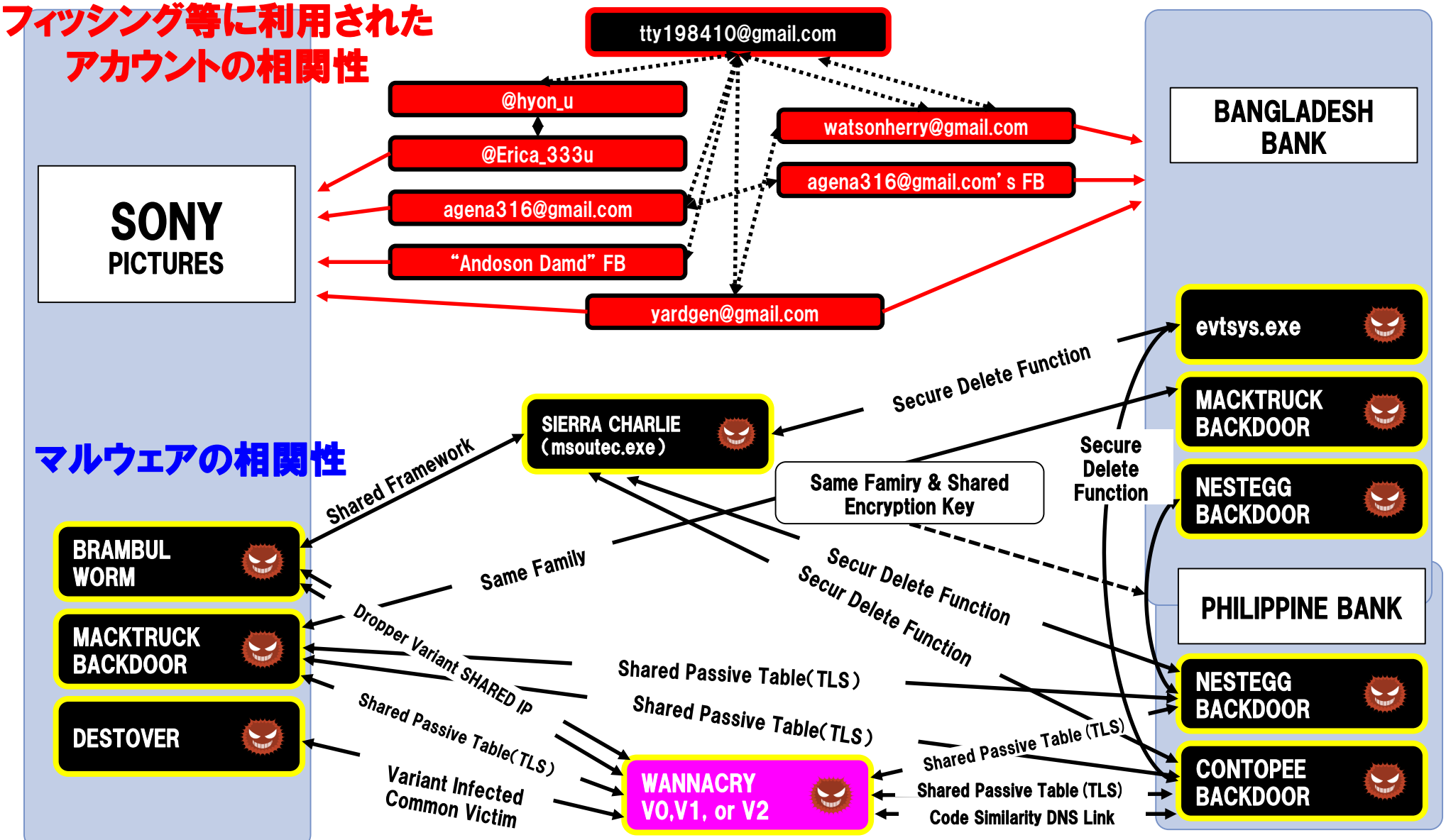


https://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html より

各攻撃の相関性

NTT DATA

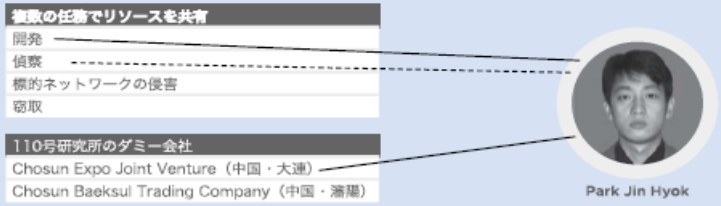
フィッシング等に利用されたアカウントの相関性



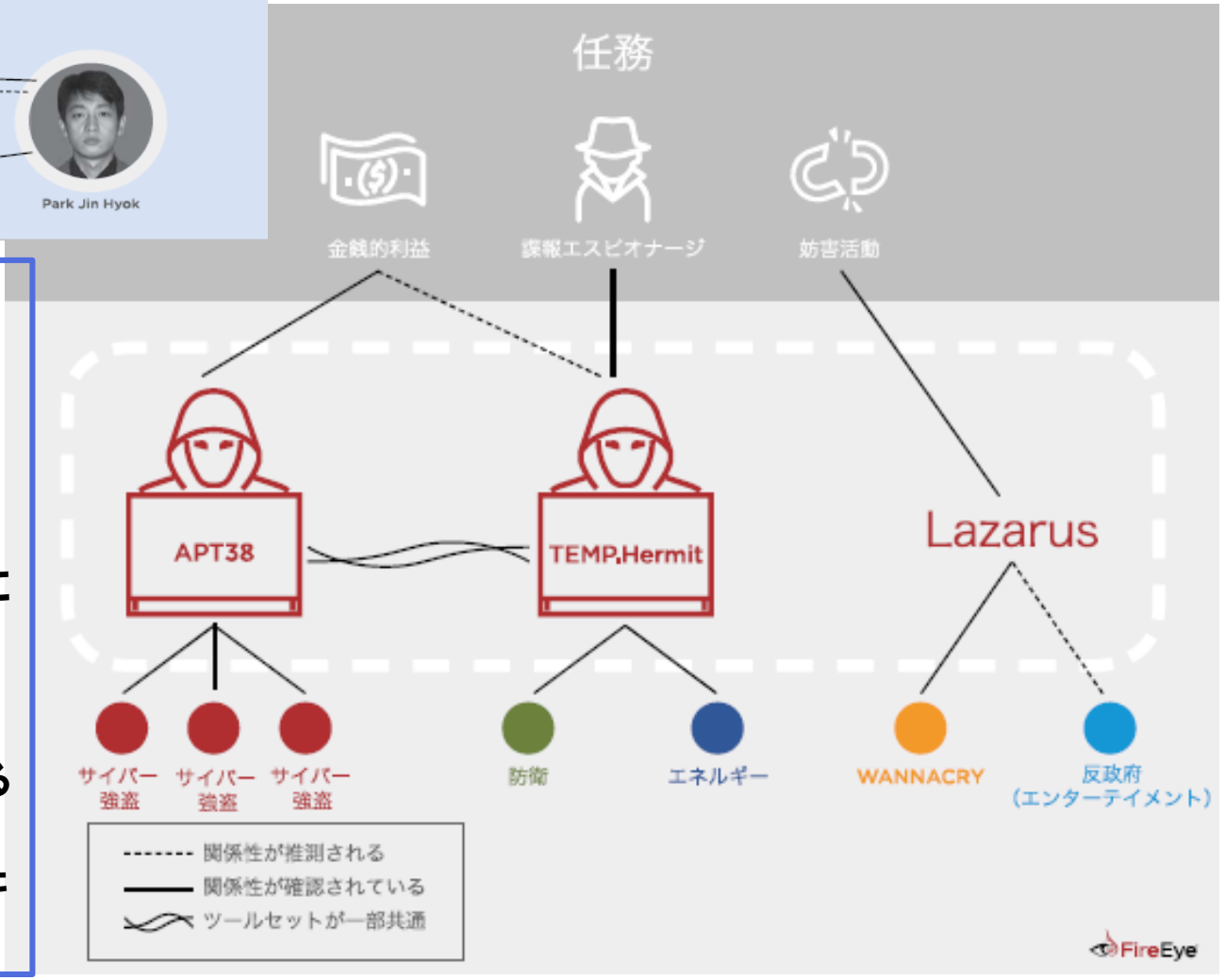
何がわかってきたか？

偵察総局（RGB）
第6技術部
110号研究所

サイバー部隊



https://www.fireeye.com/blog/jp-threat-research/2018/10/apt38-details-on-new-north-korean-regime-backed-threat-group.html



Fireeyeの調査レポート「北朝鮮国家の支援を受ける 新たな脅威グループ「APT38」の詳細」より
・一連のサイバーインシデントは北朝鮮の国家的支援を受けた組織によって実行。
・攻撃対象と目的により複数のチームに分かれて実行されているが、攻撃に用いられたインフラ、マルウェア開発フレームワークは共通点がある。
・北朝鮮に対する経済制裁が厳しくなるにつれて活動は活発化
→この調査はFBIによる訴追を補強したものになっている

雑談

世界の常識、日本の非常識

国連での議論

中国・ロシア・タジキスタン・ウズベキスタンによる共同提案（抜粋） 2011年9月

この規範は、国際的な安定と安全保障を維持する目的に沿って、･･･情報空間における各国の権利及び責務を確定し、各国の建設的及び責任ある行動を促し、情報空間における共通の脅威や課題に取り組む際の各国の協力を高めることを目的とする。

本規範への支持は任意であり、すべての国に開かれている。

○ ネットワークをはじめとするICTを利用した犯罪およびテロ活動と闘うこと、あるいは、テロリズム、分離主義、過激主義を扇動する情報（の流布）、あるいは他国の政治、経済、社会の安定並びにその精神的および文化的な環境を弱体化する**情報の流布を阻止するために協力すること**。

○ 情報を検索、取得、流布する権利及び自由を含む、情報スペースにおける権利と自由については、関連する**国内法及び規則に従うという前提で**十分に尊重すること。

○ リソースの公平な分配を確実にし、全ての人のアクセスを推進し、かつ、インターネットの安定的で安全な機能を確保するために、多国間の透明かつ民主的な**国際的インターネット管理システムの構築を促進すること**。

中华人民共和国网络安全法

第５条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

2017．6．1 施行

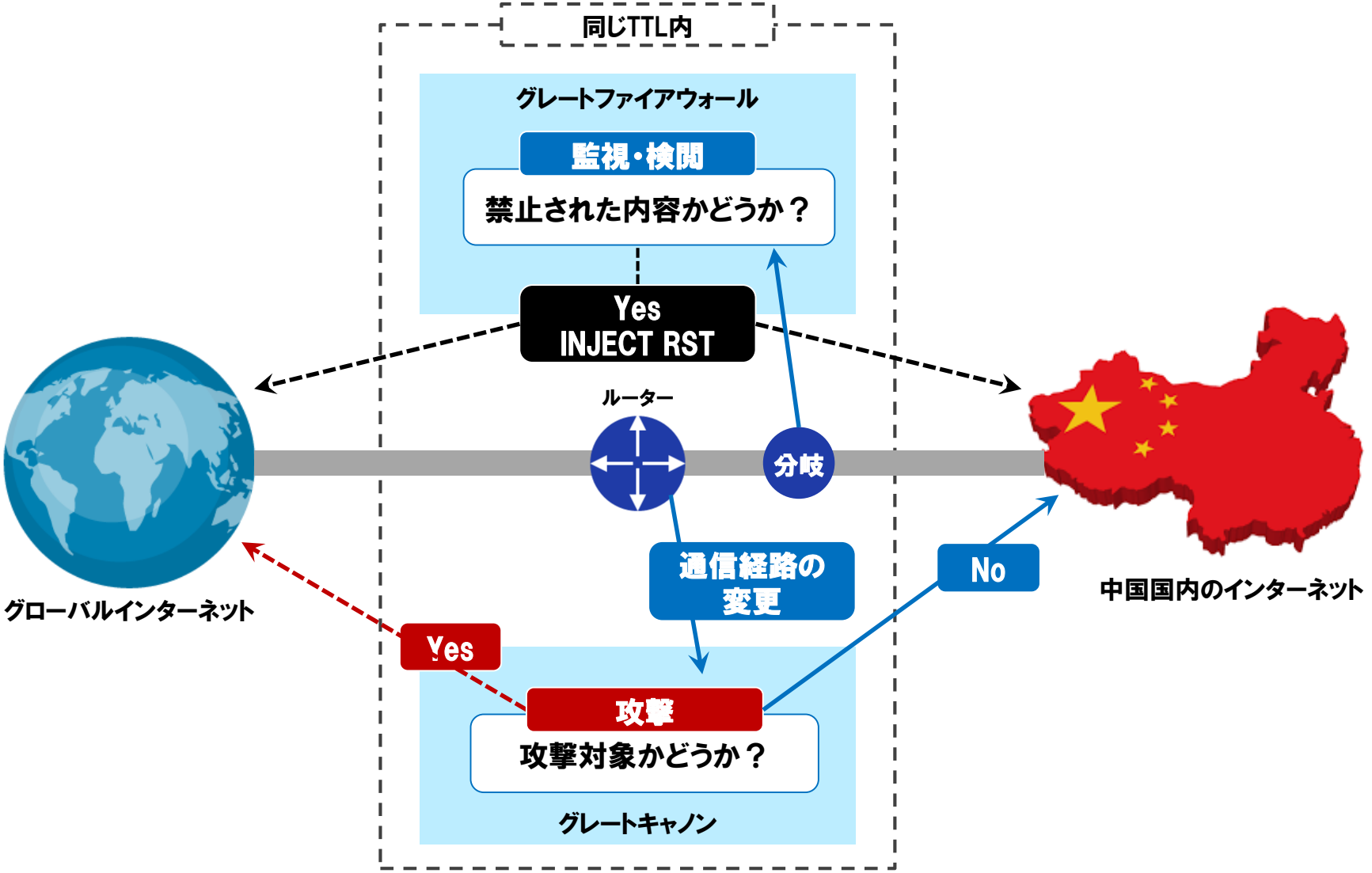
https://www.jetro.go.jp/ext_images/world/asia/cn/law/pdf/others_005.pdf

ネットワーク安全法

第５条 国は、措置を講じて、中華人民共和国の国内外からもたらされるネットワークの安全上のリスク及び脅威をモニタリング、防御、処置し、重要情報のインフラストラクチャーが攻撃、侵入、妨害、破壊を受けないよう保護し、法によりネットワークに対する違法な犯罪行為を厳しく取り締まり、ネットワーク空間の安全及び秩序を維持・保護する。

いかなる個人及び組織も、ネットワークを使用するにあたり、憲法・法律を遵守し、公の秩序を遵守し、社会道徳を尊重しなければならず、ネットワークの安全を脅かしてはならず、ネットワークを利用して国の安全、栄誉、利益を脅かし、国家政権の転覆及び社会主義制度の転覆を煽動し、国の分裂及び国家統一を破壊することを煽動し、テロリズム及び過激主義を宣揚し、民族に対する憎悪や差別を宣揚し、暴力及びわいせつな情報を流布し、虚偽情報を捏造、散布して経済の秩序及び社会秩序を撹乱し、他人の名誉、プライバシー、知的財産権その他の適法な権益を侵害する等の活動に従事してはならな

中国のグレートファイアウォールとグレートキャノン

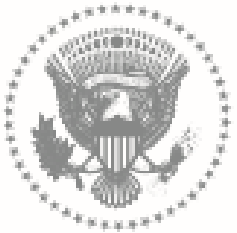


出典：「NTT技術ジャーナル」(2015 Vol27 No.10)2015年10月発行　特集「グローバルな脅威に対するセキュリティR&D」「グローバルなセキュリティ脅威の動向」：http://www.ntt.co.jp/journal/1510/files/jn201510014.pdf

NATIONAL CYBER STRATEGY

of the United States of America

SEPTEMBER 2018



THE WHITE HOUSE

WASHINGTON, DC

My fellow Americans:

Protecting America's national security and promoting the prosperity of the American people are my top priorities. Ensuring the security of cyberspace is fundamental to both endeavors. Cyberspace is an integral component of all facets of American life, including our economy and defense. Yet, our private and public entities still struggle to secure their systems, and adversaries have increased the frequency and sophistication of their malicious cyber activities. America created the Internet and shared it with the world. Now, we must make sure to secure and preserve cyberspace for future generations.

民主主義・自由主義経済

VS.

国家資本主義

アトリビュートに関する能力の欠如
インテリジェンス能力の欠如

THE SANKEI NEWS

日本年金機構情報流出　容疑者不詳のまま時効、捜査終結

2018.5.21 21:51

平成２７年５月に日本年金機構がサイバー攻撃を受け、大量の個人情報が流出した事件で、警視庁公安部は２１日、容疑者不詳のまま不正指令電磁的記録供用の疑いで書類送検し、捜査を終結した。２０日に公訴時効を迎えていた。

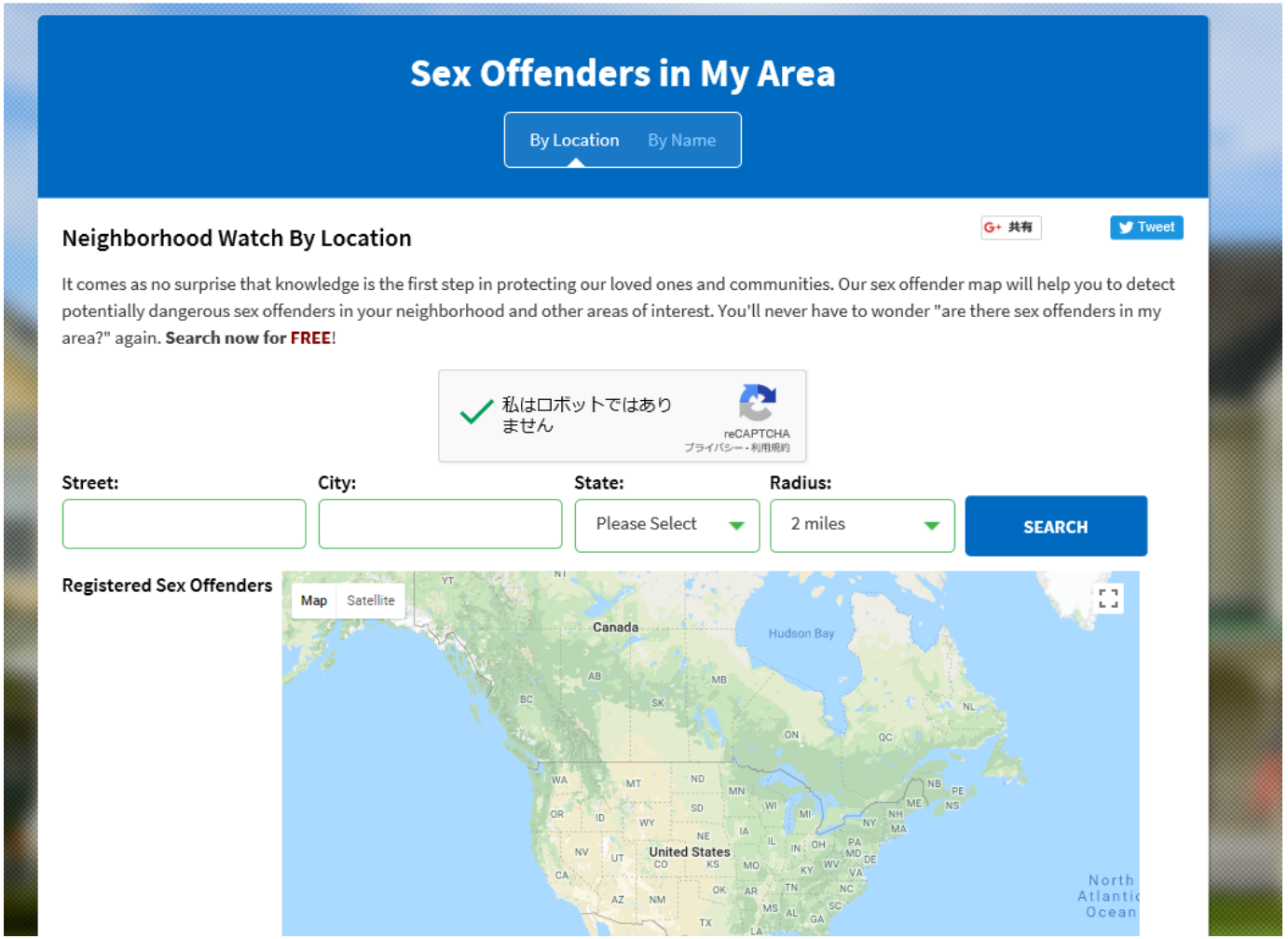
公安部などによると、業務を装った「標的型メール」が送られるサイバー攻撃を受け、機構のパソコン３１台がウイルスに感染。基礎年金番号や氏名などの個人情報約１２５万件が流出した。

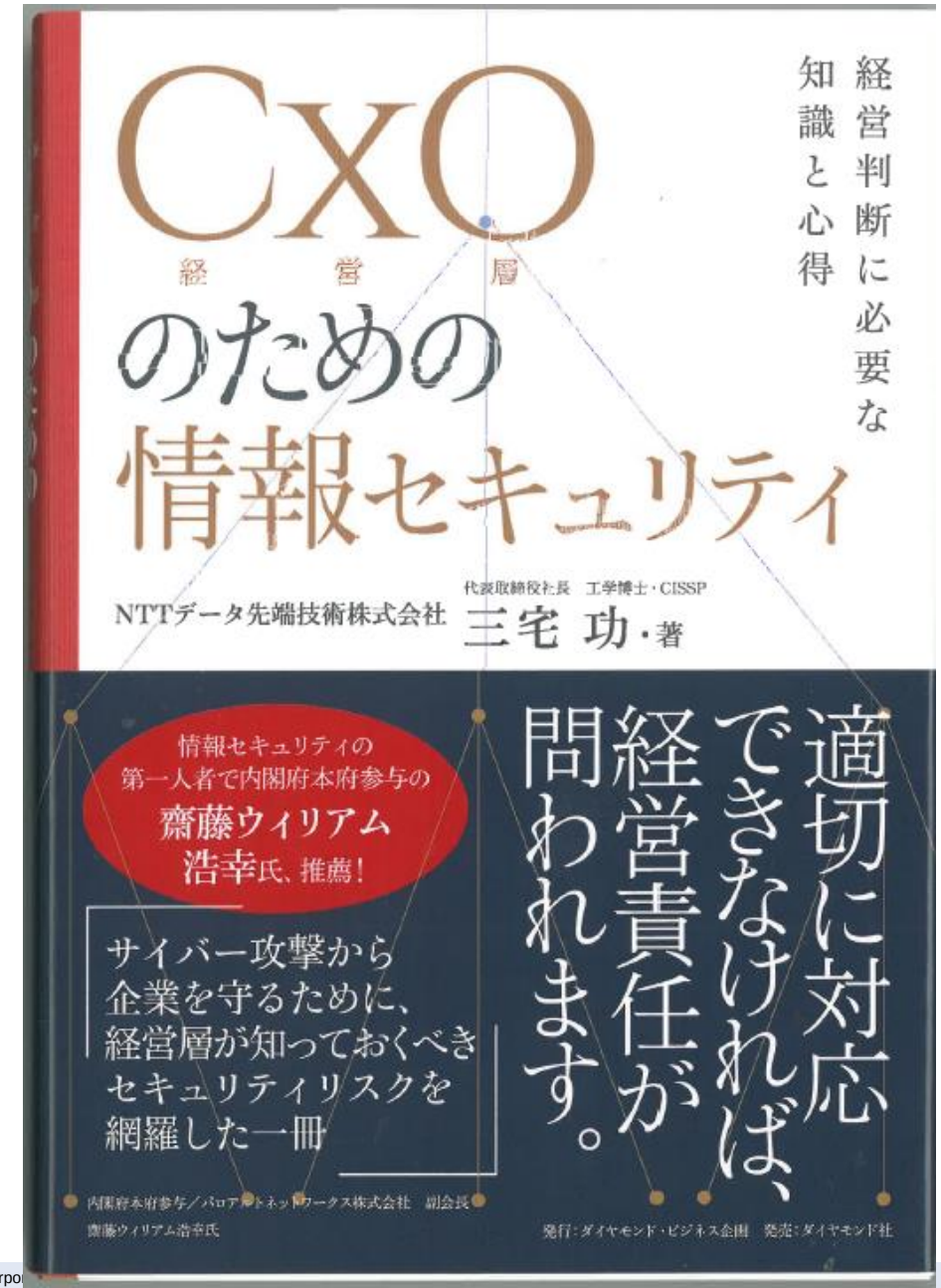
公安部はパソコンが米国や中国、シンガポールを含む国内外のサーバー２３台と不審な通信をしていたことを特定。海外の捜査当局の協力も得て捜査を進めてきたが、一部の通信記録が削除されていたり、海外のサーバーの所在地が分からないケースがあったりしたことなどから、容疑者特定に至らなかった。

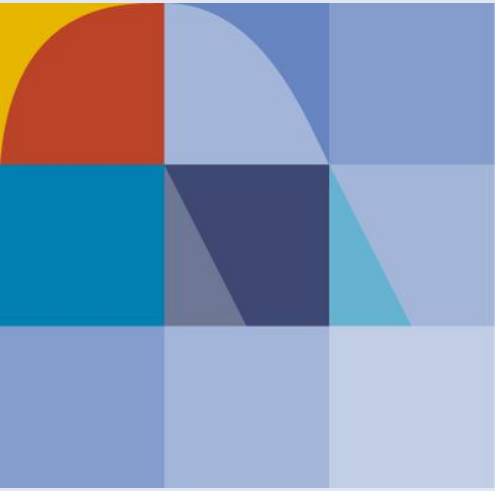
ウイルスの一部に中国語の書体（フォント）を使った形跡もあったが、作成者は特定されなかった。

バックグランドチェック

CRIMINAL® WATCH DOG







NTT DATA

変える力を、ともに生み出す。

（必要のない場合は注釈を削除してください）