DPF研究会講演
無断転載禁止

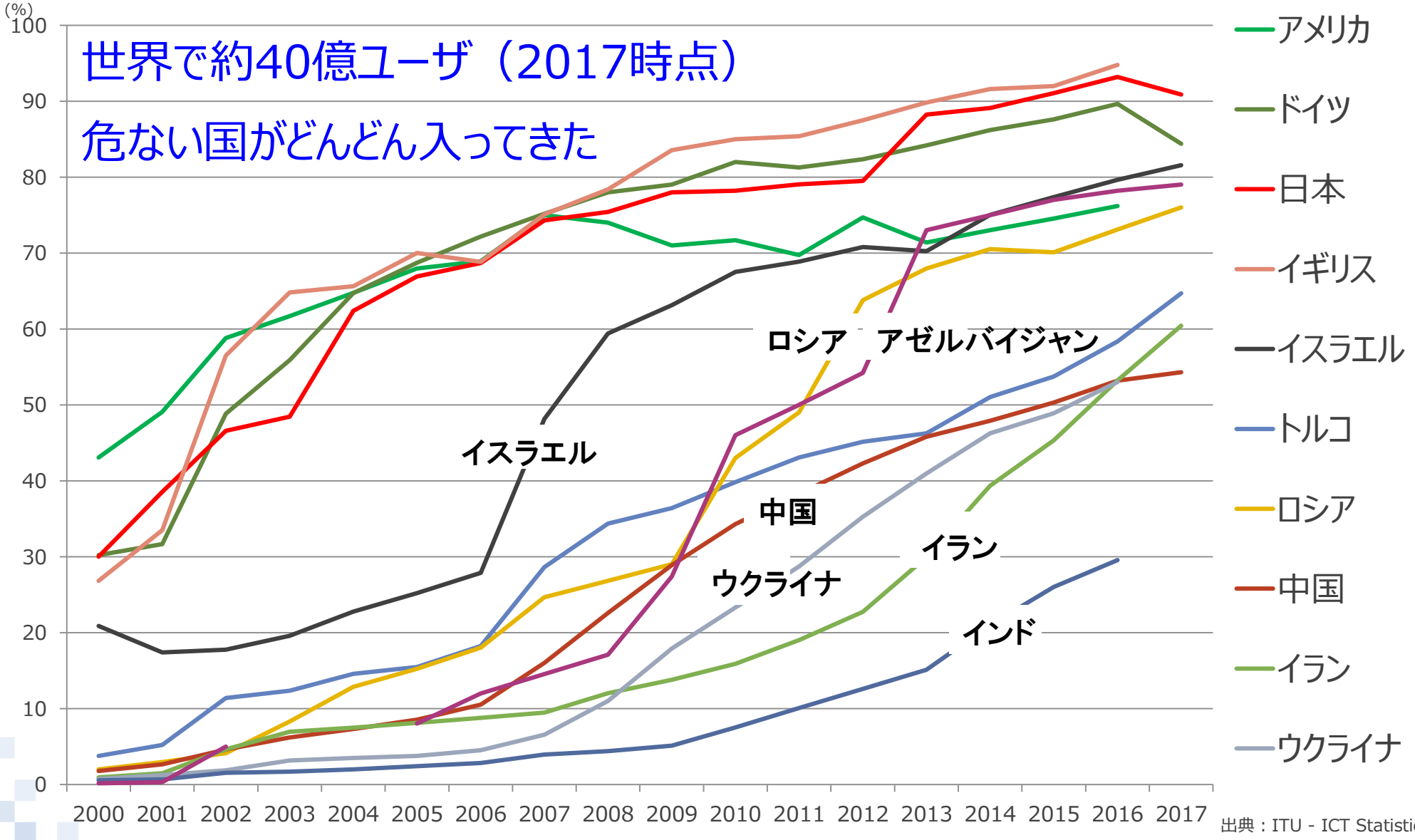
NTT DATA
Trusted Global Innovator

ディジタル時代の CybersecurityとCyberethics

2019年6月28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、　miyake@intellilink.co.jp

インターネットの拡大とサイバー攻撃

国別のインターネット普及状況(’00～’17)



出典：ITU - ICT Statistics

ブロックチェインへの攻撃

国連北朝鮮専門家パネル報告書(2019.2)より

https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports　全文：378page

北朝鮮の核・弾道ミサイル開発に対する国連決議に基づく制裁の実施状況をレポート。
制裁は石油・石炭等の輸出入、金融取引、武器取引等の制限。多くの違反が継続して行われていることを報告。違反の中にはサイバー攻撃も含まれている。

Figure I
Yuk Tung and Ocean Explorer on 28 October 2018

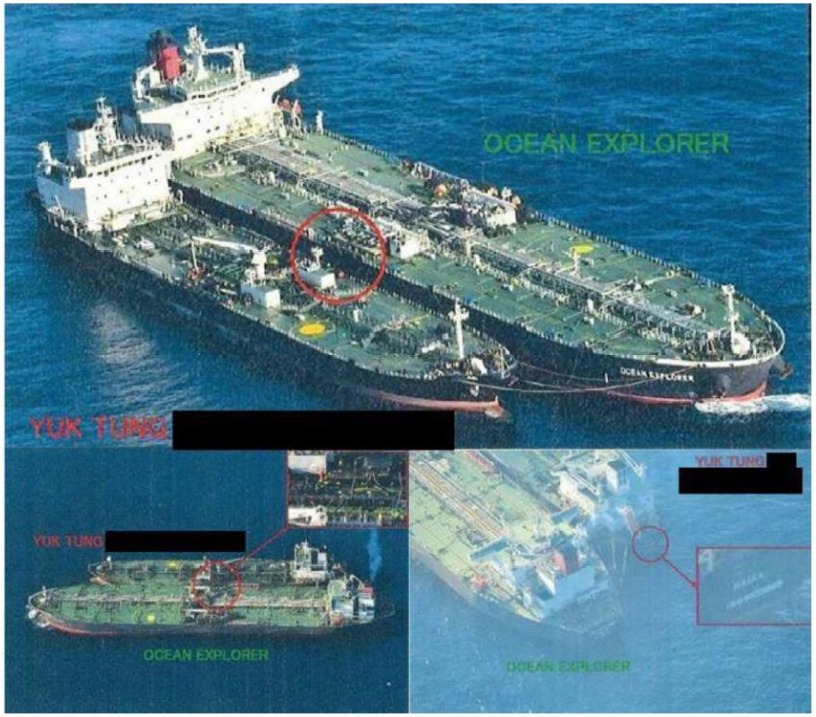
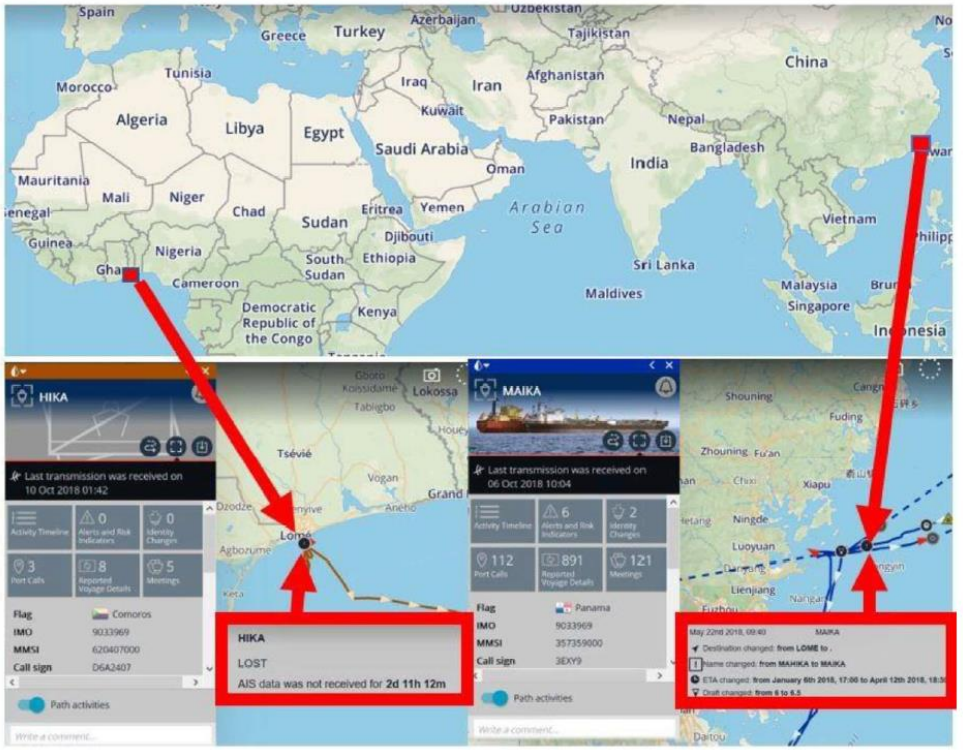


Figure II
Yuk Tung*, a.k.a. *Maika*, begins spoofing *Hika*, a.k.a. *Mahika



NTT DATA
NTTデータ 先端技術株式会社

国連北朝鮮専門家パネル報告書より　サイバー攻撃関連

■　Blockchain platform for vessel transactions, Paragraph 28～30

・香港をベースとしたブロックチェーン”Marine Chain”を利用した形跡。CEOはシンガポール国籍、Etheriumを利用して船の売買に利用。少なくとも1名の北朝鮮国籍の人物がボードメンバ。資金源及び船籍偽装に利用される可能性が指摘される。Marine Chainは2018.4設立、2018.9に閉鎖される。

■　Cyberattacks, Paragraph 109～115

FBIにより訴追された件に加え、以下の攻撃をリストアップ。

①バングラディシュ中央銀行に対する攻撃に引き続いて、2018.5、Banco de Chiliに対しSWIFT経由の香港の口座への不正送金を実施。被害額＄10million

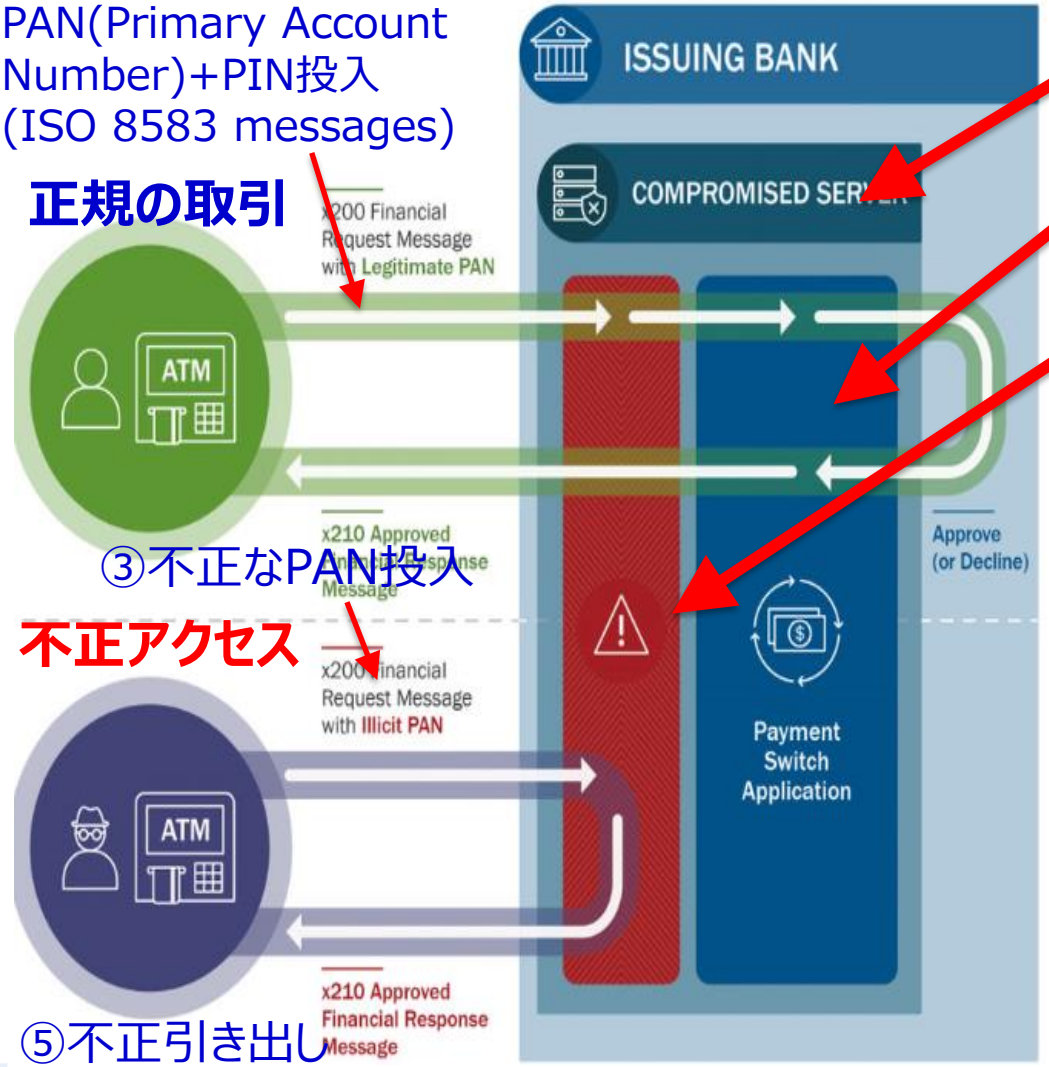
②2018.10.2, インドCosmos Bank口座より世界28か国、14000のATMより引出が行われ、SWIFTを経由して香港の口座に不正送金。米国は“FASTCash Campaign”として警戒を呼び掛ける。この攻撃は、INTERPOLが金融機関向けに出したガイドラインを突破。

③2017.1から2018.9までに仮想通貨取引所への攻撃を実施し、少なくとも5回成功。被害額571milion＄　→　うち534milion＄がコインチェック（Japan）

FASTCash Campaign

銀行のオンラインバンキングシステム

PAN(Primary Account Number)+PIN投入 (ISO 8583 messages)



PSS:Payment Switch Server

正常な取引（トランザクション）の場合、PANをチェックして、対応する口座残高を確認の上、支払い許可通知をATMに送る

①マルウェアを侵入させ外部からのアクセスを確保。その後、PSSのアプリを改変。

②改変されたPSSアプリはトランザクションをモニタし、正規のPANの場合はそのまま正規処理。

④事前に仕込まれた不正なPANが来た場合は、残高証明のプロセスには回さず、そのまま支払いメッセージを作成して送信。

・ターゲットは、アジア・アフリカのセキュリティの甘い銀行。スピアフィッシングメールによるAPT攻撃と見られる。
・FBI/US-CERTは発見された10種類のマルウェアの特徴より北朝鮮と断定

https://thehackernews.com/2018/10/bank-atm-hacking.html

仮想通貨交換所への攻撃

SUCCESSFUL ATTACKS ON CRYPTO EXCHANGES 2017-2018

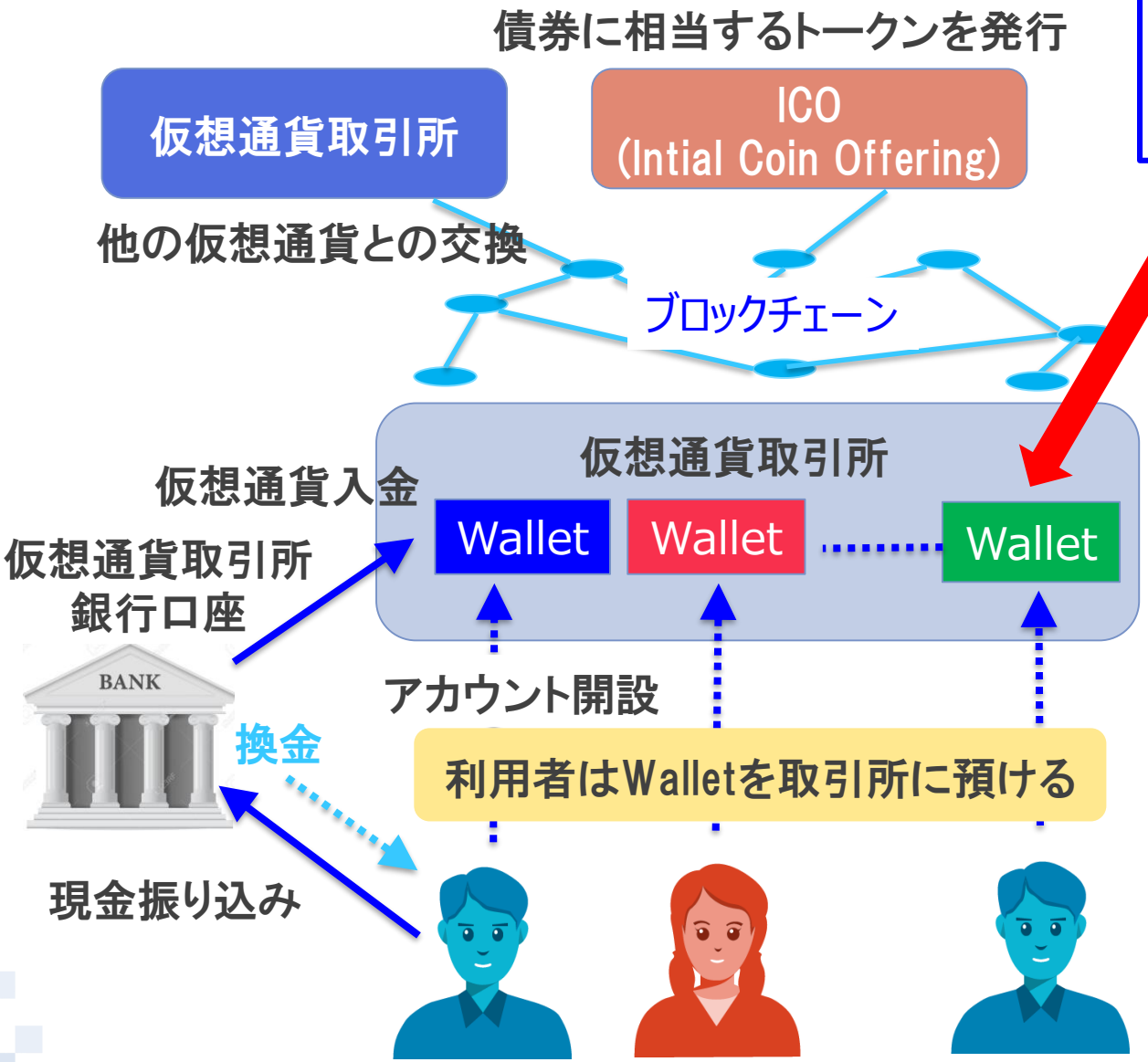
GROUP IB

Date	Name of Project	Country	Criminal group	Stolen in cryptocurrency	Stolen in USD
Feb 2017	Bithumb	South Korea	Unknown	-	$7 mln
Apr 2017	YouBit	South Korea	Unknown	-	$5,6 mln
Apr 2017	Yapizon	South Korea	Lazarus	3,816 BTC	$5,3 mln
Apr 2017	Ether Delta	-	Unknown	-	$266 k
Aug 2017	OKEx	Hong Kong	Unknown	-	$3 mln
Sept 2017	Coinis	South Korea	Lazarus	-	-
Dec 2017	YouBit	South Korea	Lazarus	17% of assets	-
Jan 2018	Bitstamp	Luxemburg	Unknown	18,000 BTC	$5 mln
Jan 2018	Coincheck	Japan	Lazarus	523,000,000 NEM	$534 mln
Feb 2018	Bitgrail	Italy	Unknown	17,000,000 NANO	$170 mln
Jun 2018	Bithumb	South Korea	Lazarus	-	$32 mln
Jun 2018	Coinrail	South Korea	Unknown	-	$37 mln
Jun 2018	Bancor	-	Unknown	-	$23 mln
Sept 2018	Zaif	Japan	Unknown	-	$60 mln ?
				TOTAL	$882 mln

＄571 million

https://www.group-ib.com/media/gib-crypto-summary/

仮想通貨取引所とCoinCheck事件



仮想通貨取引所であるCoinCheckの情報システムに侵入されて顧客のWalletの秘密鍵が盗まれる

2018.1.26, 2:57
XEM(CoinCheckが使っている仮想通貨)流出開始
11:25
CoinCheckが流出確認
12:7
XEMの入金を制限
14:6
Twitter上で大量送金が報告

原因
・社員がマルウェア付きのメールを開封することで侵入される。
・Walletがインターネットに晒されていた。
・秘密鍵にマルチシグ対応がされていなかった。

最近の動向　国際的な取り組みより

■金融活動作業部会(FATA:Financial Action Task Force on Money Laundering)
1989年設立された政府間機関。マネーロンダリング対策及びテロ資金対策に関する国際基準（FATF勧告）の策定及び見直し、監視、導入支援。

■我が国もこの勧告に基づいて法制度等の整備を実施。「犯罪収益移転防止法」を整備（最新は2016年改訂*）。本人確認、資金移動の透明性確保、多国間連携（テロ組織等の疑いのある個人・組織情報共有）等

＊本人確認の身分証明書に証明写真のないもの（健康保険証など）を使用する場合は、証明する書類を2点以上提示することが義務づけられた。

■FATA４次勧告(最新版が2018.10に改定)
仮想通貨交換業者、仮想通貨管理業者、ICO関連サービス業者におけるマネロン・テロ資金供与規制が課された。

■上記勧告に従ったガイドライン「マネー・ローンダリング及びテロ資金供与対策に関する規則・ガイドライン」を金融庁で策定（９月発効）。これを業界自主基準とする。
口座開設時の本人確認厳格化・格付け、仮想化通貨交換事業者のセキュリティ対策強化、流通のトレーサビリティ向上等が盛り込まれている。

インターネットの攻撃インフラ化の事例（北朝鮮の事例）

北朝鮮要員によるサイバー攻撃

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,"

Case No. MJ 18-1479

Defendant.

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.

/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

北朝鮮による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

BANGLADESH BANK

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

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
India Cosmos 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”

LOCKHEED MARTIN

THAAD配備決定

2015.10

“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？

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

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　サイバーキルチェーン

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

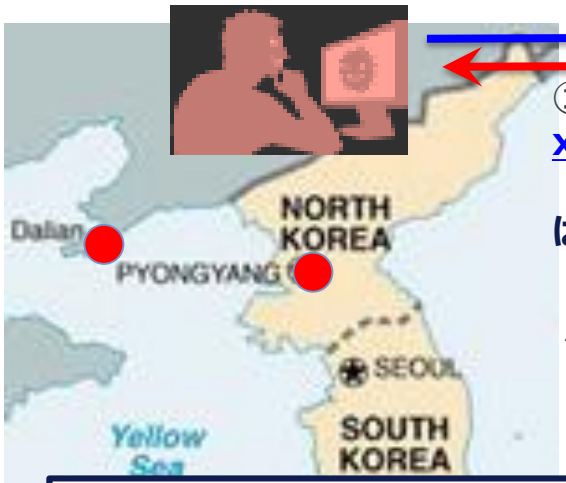
脅迫状
We’ve got great damage by Sony Pictures. The compensation for it, monetary compensations we want. Pay the damage, or Sony Pictures will be bombarded as a whole. You know us very well. We never wait long. You’d better behave wisely.
From God’sApstls

攻撃インフラ構築

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。

ターゲットへの侵入/フィッシングメール

“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

Fishing

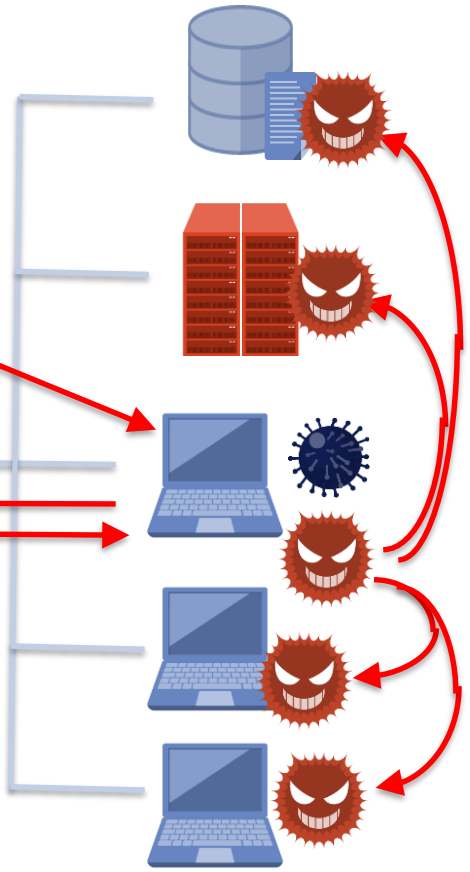
①バックドア（C&Cサーバ のIPアドレスに紐づく DDSNのURL）付きの ページをダウンロード。

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感染範囲の拡大
Lateral Movement



④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

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

https://jp.wsj.com/articles/SB12798596211232484180504581604150882421590?mod=article_inline

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。

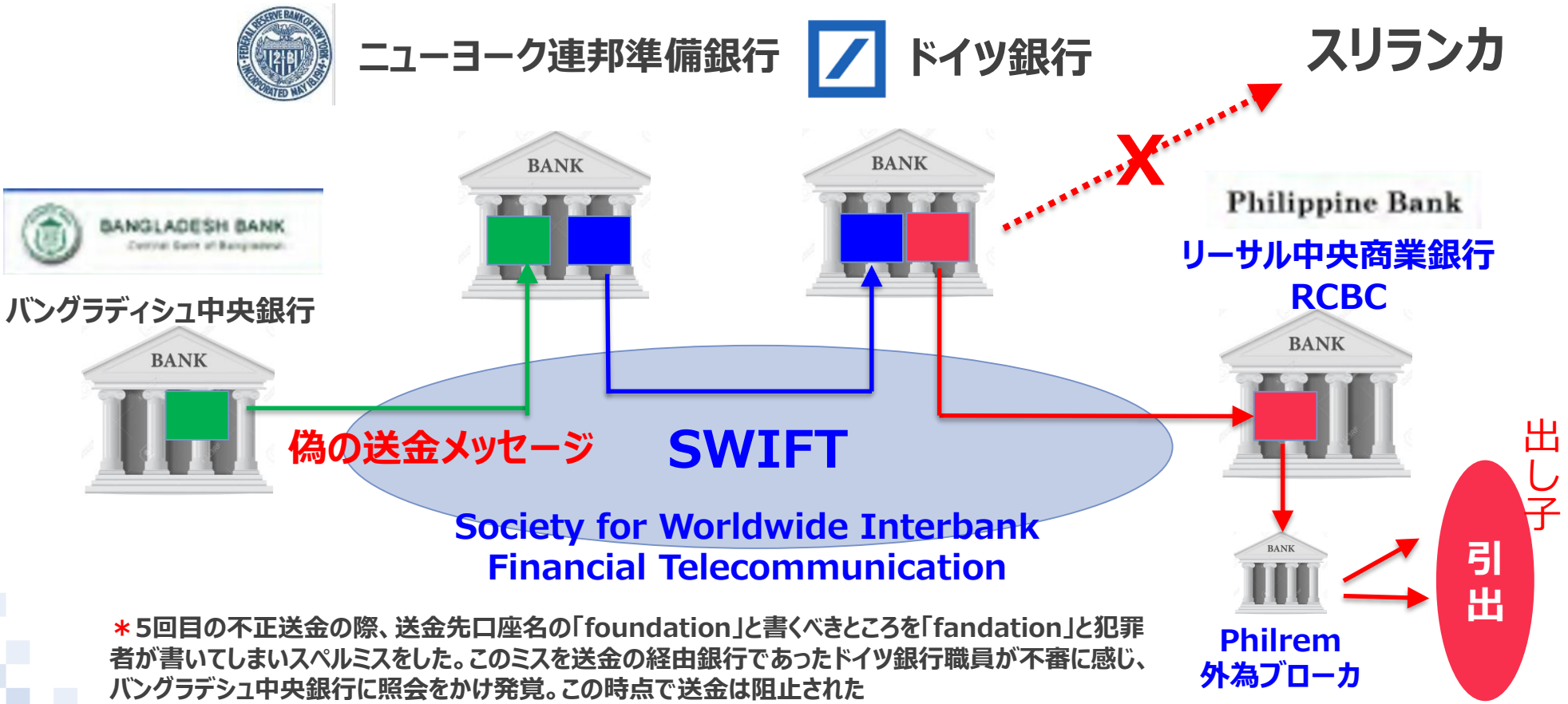
【ダッカ（バングラデシュ）】ある週末、ニューヨーク連銀にあるバングラデシュ銀行（中銀）の口座から何者かが正式なパスコードを使って外貨準備約1億ドル（約113億円）を不正送金する事件が発生した。ここで何が起こったのかについては、現在も4カ国の当局が全容解明に取り組んでいる。（２０１６．３．１７ WSJ）

【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

https://jp.wsj.com/articles/SB10513819889225894892604582103393364153580

何が行われたか？

・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

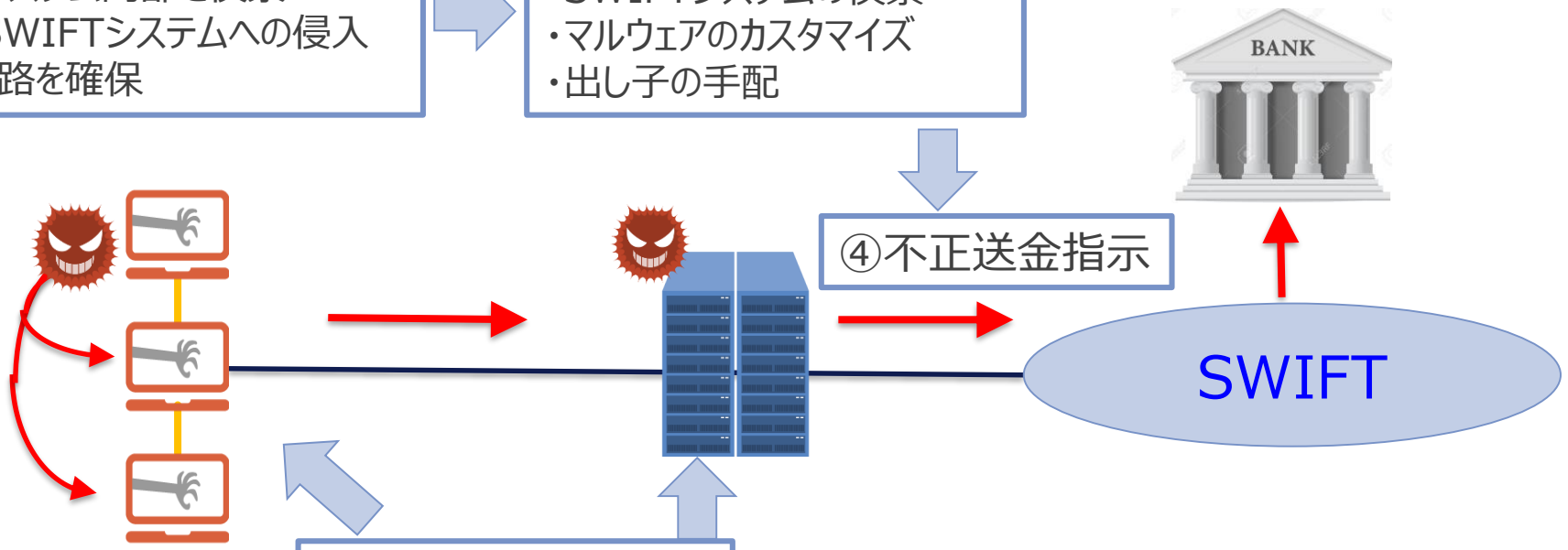
サイバーキルチェーン

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

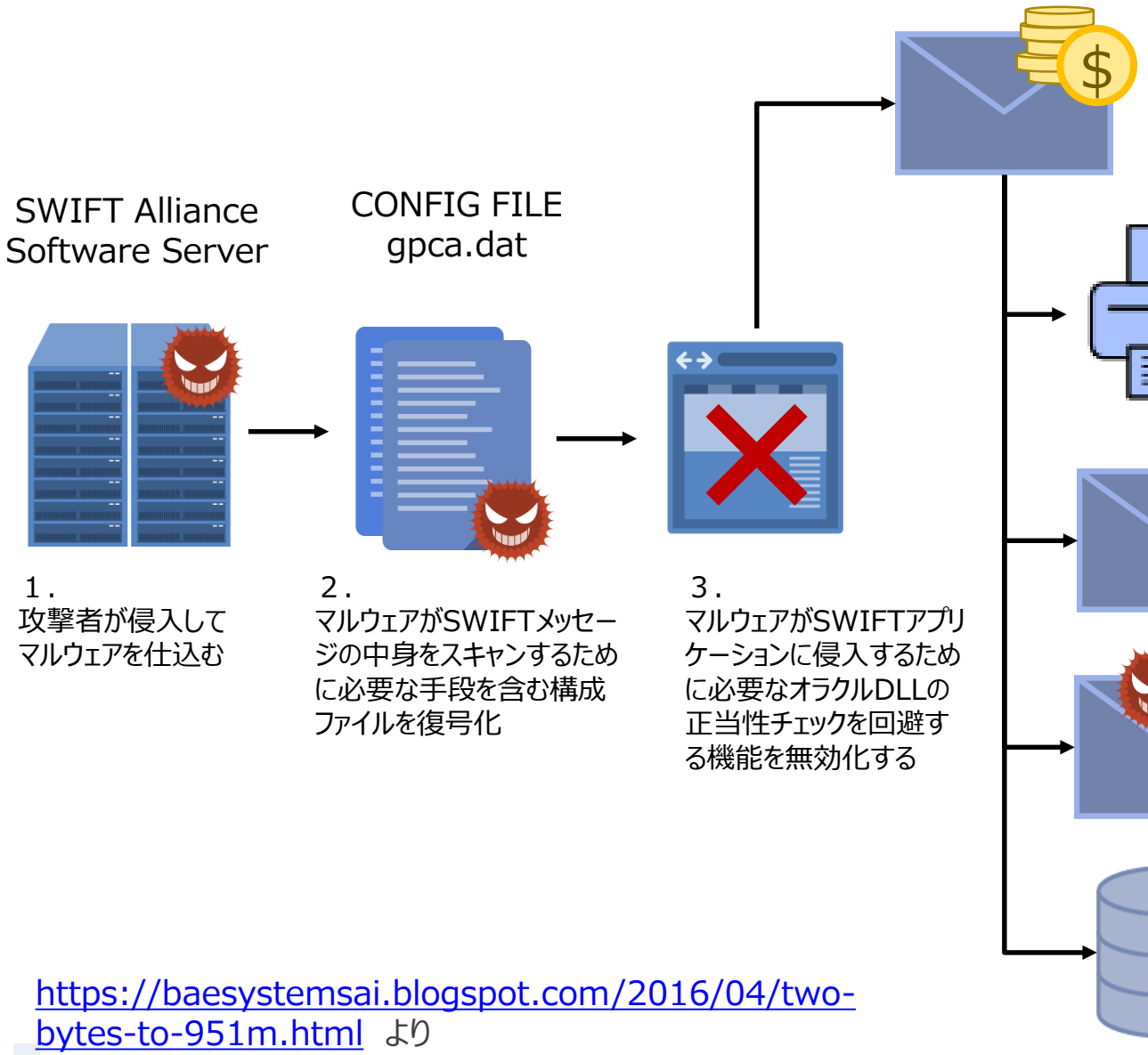
②脆弱なシステムへの侵入
・システム内部を偵察
・SWIFTシステムへの侵入経路を確保

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



NTT DATA
NTTデータ 先端技術株式会社

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

ランサムウェア　WannaCry　2.0

Major Cyberattack Sweeps Globe
FedEx, U.K. Hospitals, Spanish C

Experts say hackers targeted a software vulnerability that hac
earlier by the NSA

HITACHI
Inspire the Next

ランサムウ

株式会社日立製作所は、日立グループ
よび対策の状況についてお知らせしま

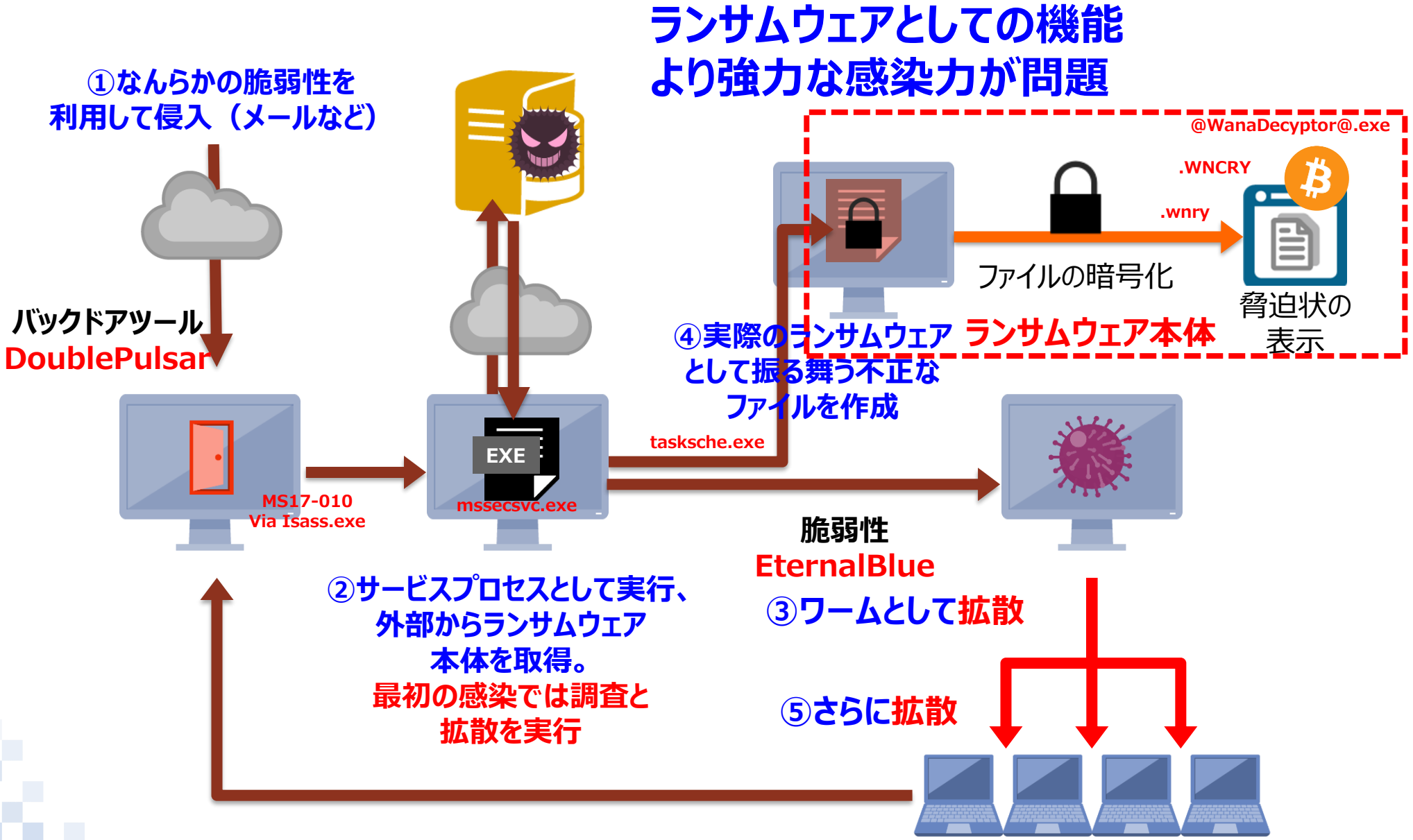
5月12日(金)深夜、社内システムの一部で異常を検知しました。その後、5月13日(土)未明に対策チームを立ち上げ、状況の把握や対策の検討を開始しました。一部の社内システムにおいて不具合が生じ、5月15日(月)以降、メールの送受信等に影響が発生しました。日立グループでは、対策本部を編成し、国内外のグループの総力を挙げ、パートナーやベンダー企業の協力も得ながら復旧に取り組んでいます。不具合が発生したメールシステムについては、本日時点で概ね復旧が完了し、今週中の全面復旧を見込んでいます。

今回のランサムウェアの影響を受けた一部の社内システム不具合により、お客様をはじめ取引先関係の皆様にご迷惑、ご心配をおかけしていることをお詫び申し上げます。

なお、今回のランサムウェアによる被害に関して、情報漏えいは確認されておらず、また、日立グループから送信するメールによりお客様や社外の皆様へ被害が拡大することはありません。

以上

WannaCry 2.0の侵入と拡散プロセス



タイムラインで見てみると

2016年8月　NSAより情報
漏洩した機密文書を
Shadow Brokers公開
2017年４月５回目の公開
未公開の脆弱性をつくコード
(Eternal Blue)が含まれていた

2017年3月14日
マイクロソフト
脆弱性情報公開

2017年5月9日
RiskSenceがテスト
コード公開
自己複製機能

2017年5月12日未明
WannaCry
キャンペーン開始
国内でも被害

5月13日
マイクロソフト
サポート切れOS
にも緊急パッチ供給

5月14日
IPA記者会見

5月15日
首相官邸に
危機対策室

5月16日
150ヵ国30万件
の被害（ホワイトハウス）

5月23日
北朝鮮関与？
Symantec

Ver.0
2017年2月検出

Ver.1
2017年3月検出

Ver.2
自己複製型

・北朝鮮が他の攻撃に使用したツール群と著しい類似性があった
・表示画面、BitCoinの送付先が類似
・タイムゾーンが朝鮮時間、ハングル版Windows利用 etc. by FBI

国家によるサイバー攻撃

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

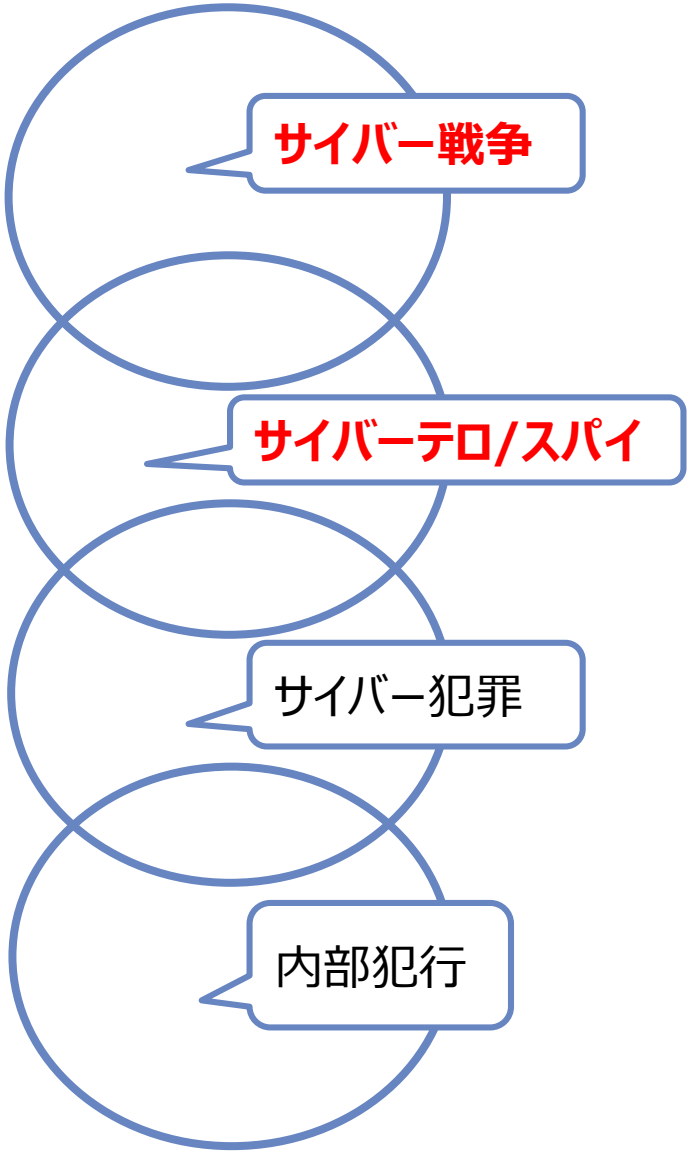
諜報型、 破壊工作型

個人・組織サイバー犯罪

換金型、 物販型

Hacktivist

内部犯行



国家によるサイバー攻撃の類型　1/2

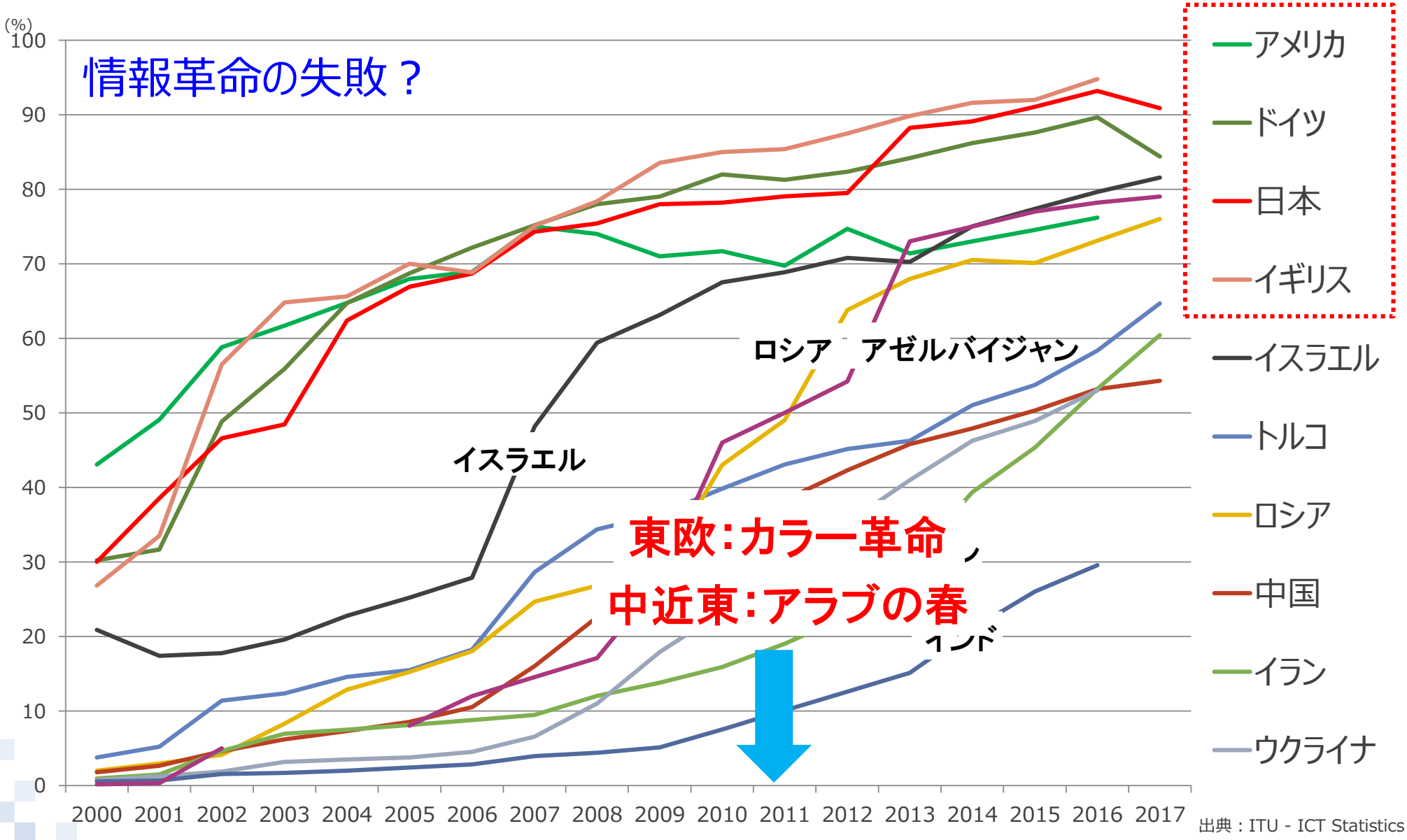
類型	特徴	意図
機密情報窃取 (Espionage)	政府機関、重要インフラ関連企業等の機密情報を扱うネットワークに対してサイバー攻撃(APT攻撃)を仕掛け、これを窃取する。	自国に利する軍事上の機密、企業秘密、特定個人情報等を獲得
インターネット接続の妨害	公開されたWebサイトに対してするDDoS攻撃、DNS/BGP等のインターネット接続基盤に対する攻撃	政治的意図の強要、経済的利益の獲得
妨害活動 (Vandalism)	特定の政治的意図をもって、Webサイト改竄、ネットワークへの侵入による機微な情報の開示。	敵対する相手に対する政治的圧力の行使
破壊活動 (Sabotage)	重要インフラ、機微なシステムそのものを使用不能とする破壊活動。	経済的なダメージ、或いはクリティカルな政治的意図の強要

国家によるサイバー攻撃の類型　2/2

類型	特徴	意図
ランサムウェア (Ransomware)	重要情報の暗号化による脅迫	経済的利益の獲得 破壊活動
金融取引ネットワークへの攻撃	金融取引ネットワークインフラ(オンライン取引、SWIFT, 仮想通貨等)への侵入と不正送金	経済的な利益の獲得 金融インフラの破壊による経済的ダメージ
情報操作 (Information operations)	フェイクニュース、マスメディアへの侵入と欺瞞情報の流布	世論操作、政治的圧力のための口実
不正な情報開示 (Forced transparency)	機微あるいは個人情報の窃取と流布	敵対する相手に対する信用、評判の失墜
Hack Back	サイバー攻撃者に対抗した、攻撃側ネットワークへの侵入、威示活動、破壊活動	サイバー攻撃に対する反撃

Turning Point
民主主義への新たな脅威

サイバー攻撃の変化　そもそもの始まり



出典：ITU - ICT Statistics

「世界最優秀のテクノロジー専門家たちは何年もの間、自分たちが世界をつなぎさえすれば、より純粋な、世界規模の民主主義が現れると思い込んでいた。ツイッターとワッツアップによって「アラブの春」が実現したとき、彼らは喜んだ。そして、独裁者を打ち破り、新たな、より透明性のある民主主義を生み出す武器を作り上げたのだと確信した。しかし、厳しい現実が姿を現した。」

「The Perfect Weapon」 N.Y.タイムズ Daivd Sanger

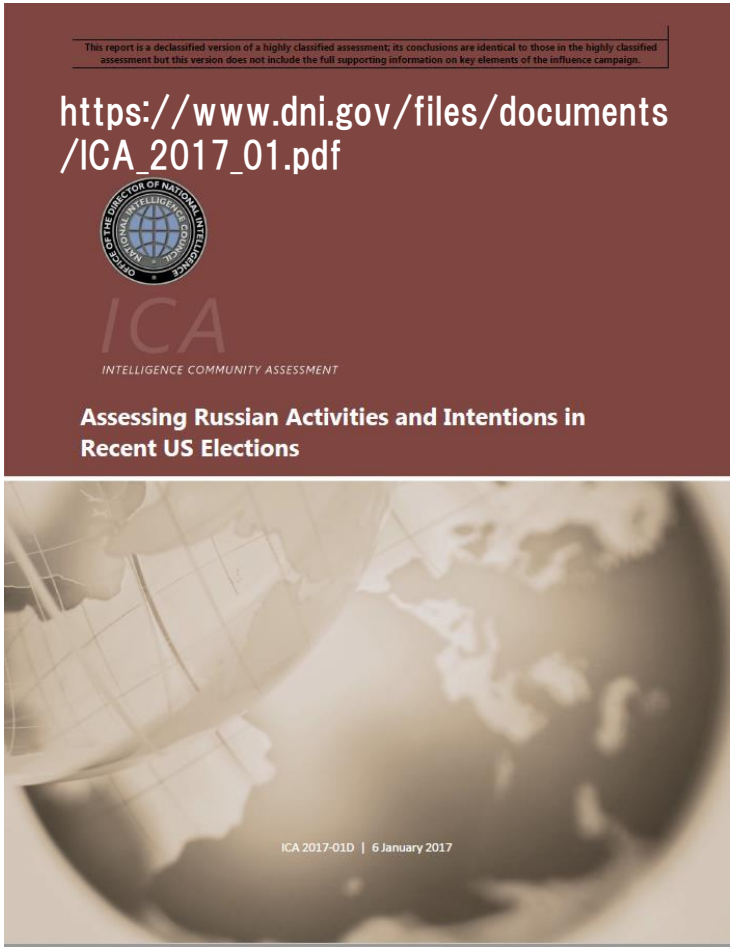
プーチンの反撃

中国のディジタル文化大革命

ロシアによる選挙介入

2016　米国大統領選挙へのロシアの介入

米国家情報長官室(ODNI),中央情報局(CIA)，連邦捜査局(FBI), 国家安全保障局(NSA)評価報告書、2017.1.6



■選挙介入とは、①選挙・国民投票等の政治制度/システムに対する工作、②有権者の意思決定に対する影響工作

■2016.3~4 米民主党本部(DNC)に侵入、内部情報（メール等）窃取が発覚。
「グシファー2.0」という架空のハッカーを登場させ、クリントン候補に関する不都合な情報をリークさせるとともに、DNC侵入は自分がやったとの欺瞞工作を実施。
情報はさらにウィッキリークスでも流される。
いずれもロシア情報部局GRUと繋がりがあることが判明

■2016春ごろ　IRAによりインターネット上に反イスラム団体「ハート・オブ・テキサス」及び親イスラム団体「アメリカ・ムスリム連合」を作り両者の対立を扇動。

■クリントン候補の健康状態に関わるフェイクニュースがロシアのTV番組、米国Webサイトで度々流される。

■複数の州の有権者登録システムに対する侵入の試みが確認される

IRA(Internet Research Agency)の活動

https://www.newsweekjapan.jp/tsuchiya/2019/03/post-34.php

■プーチンの盟友プリゴジンにより設立
■2013年頃サンクトペテルブルグに拠点設置。2014初めごろから2016米大統領選挙への介入準備開始。
■画像編集、Web検索最適化の専門家を雇うとともに、米大統領選挙の対立軸や選挙民特性を分析し効果的なプロパガンダ、フェイクニュースを発信。
■2016年時点では数百名規模で活動していた模様。
■2018米中間選挙ではハックバックを受けたため、活動休止に追い込まれる。

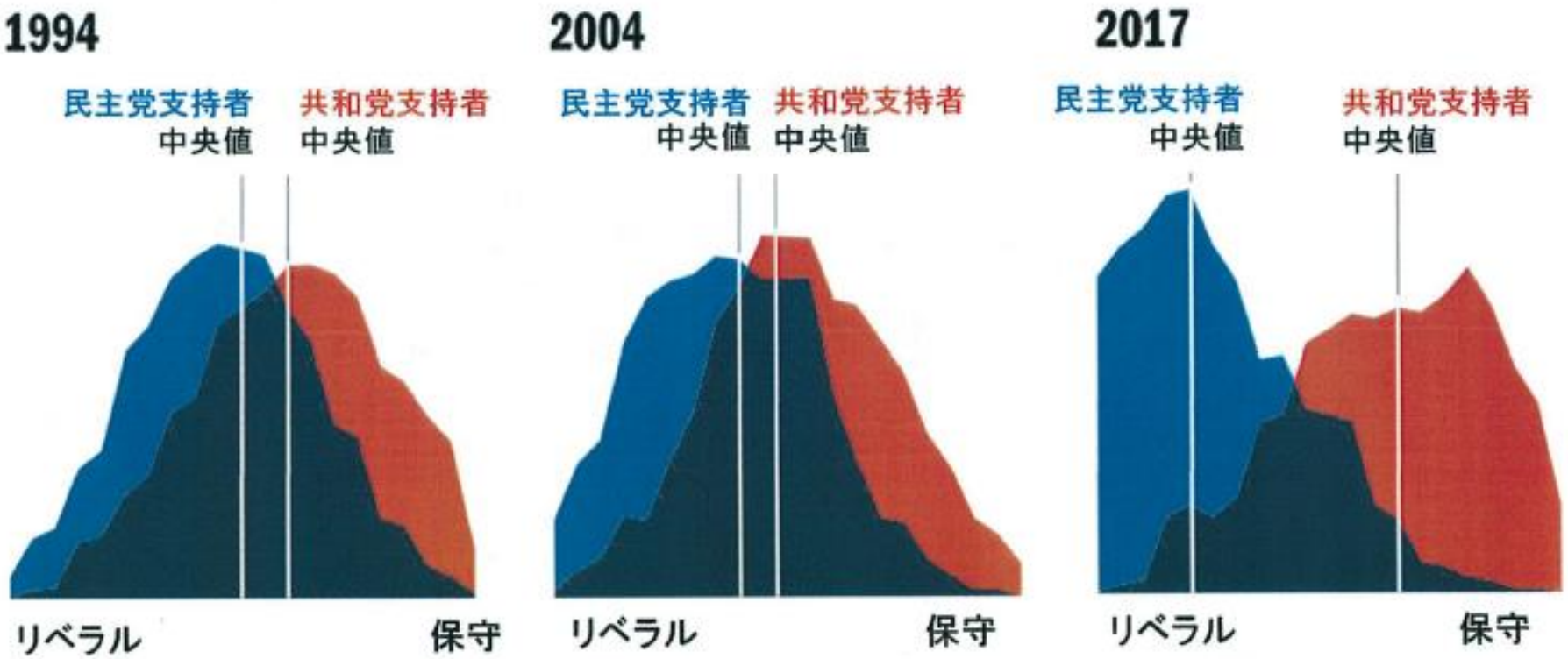
■2018.5.10に米下院情報問題常設特別調査委員会はIRA社による政治広告約3500点を公開。
https://intelligence.house.gov/social-media-content/social-media-advertisements.htm
■政治広告はターゲットが絞り込まれていた（地域、年齢等）

https://www.bustle.com/p/what-do-the-russian-facebook-election-ads-look-like-youll-recognize-some-of-these-3205398

米下院情報委員会資料
https://intelligence.house.gov/social-media-content/social-media-advertisements.htm

https://www.bustle.com/p/what-do-the-russian-facebook-election-ads-look-like-youll-recognize-some-of-these-3205398

何が起こったか　米国の分断



Source; U.S. Adults conducted June 8-18, 2017

Code of Practice on Disinformation

https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

2018年9月～10月に、最初の署名者として、Facebook、Google、Twitter、Mozillaの4事業者と、広告関係8団体が署名

広告配置の監視	1. 関連する行為に対する広告とマネタイズインセンティブを阻止するための方針・プロセスを設ける
政治的広告及び	2. すべての広告は、編集されたコンテンツと明確に区別されることができなければならない
	12. 偽情報の追跡及びその影響の理解に関する、誠意ある独立した取組を支援する
	13. 自社プラットフォームにおける偽情報及び政治広告に関する誠意ある研究を禁止又は抑制しない
	14. 偽情報及び政治広告に関する研究を促進する
	15. 学術機関、ファクトチェッキングコミュニティ、関係事業者による議論を促進するイベントを毎年開催する
のエンパワー	13. 自社プラットフォームにおける偽情報及び政治広告に関する誠意ある研究を禁止又は抑制しない
	14. 偽情報及び政治広告に関する研究を促進する
	15. 学術機関、ファクトチェッキングコミュニティ、関係事業者による議論を促進するイベントを毎年開催する

中国の脅威

中国の超監視社会

中国のネット検閲

法律に従って60以上の条例が中国政府によって作られ、地方の国有インターネットサービスプロバイダの一部や、中国政府、商社、団体などが検閲を実施している(Wikipedia)

金盾(Great Fire Wall)

中国本で実施されているインターネット情報検閲、ブロッキング (インターネット)システム

https://ja.wikipedia.org/wiki/%E9%87%91%E7%9B%BE

中国政府は2014年に初めて「社会信用システム」を提案、市民の行動を監視し、ランク付けし、スコアが高いものに恩恵を、低いものに罰を与えると発表した。この制度の下で、エリートはより恵まれた社会的特権を獲得し、ランクの底辺層は実質的に二流市民となる。この制度は2020年までに、中国の人口14億人すべてに適用されることになっている。
(News Week 2018.5.2)

https://www.newsweekjapan.jp/stories/world/2018/05/14-8_1.php

中国の超監視社会　ディジタル文化大革命

上海・外灘。赤信号を突っ切るなどした歩行者は即座に捕捉され、電信柱に備え付けた液晶モニターに掲示される。カメラを供給する杭州海康威視数字技術（ハイクビジョン）は当局の大量発注で監視カメラの世界最大手に上り詰め、米国は国防権限法で名指しで取引を禁じた。(2019.4.15日経新聞)

https://www.nikkei.com/article/DGXMZO43565550Q9A410C1000000/

上海・臨港新城が導入した「城市大脳」は張り巡らせたカメラ網で街全体を監視する(2019.4.15日経新聞)

https://www.nikkei.com/article/DGXMZO43565550Q9A410C1000000/

グローバル化する中国の脅威

Four Million Current, Former Federal Employees Affected by Cyber Attack

BY **REUTERS** 6/4/15 AT 5:41 PM

2015.6.4

https://www.newsweek.com/four-million-current-former-federal-employees-affected-cyber-attack-339694

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。過去、現在及び関連する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

中国の”Deep Panda”と呼ばれるハッカー集団（PLA所属）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

Technical forensics of OPM hack reveal PLA links to cyber attacks targeting Americans

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。

https://flashcritic.com/technical-forensics-of-opm-hack-reveal-pla-links-to-cyber-attacks-targeting-americans/

グローバル化する中国の脅威

Le Monde 2018.1.28

2012年に中国により建設されアフリカ連合に寄贈された建物（アジズアベバ）から監視カメラ・盗聴装置が発見された。ルモンド（仏）は、「寄贈したビルは中国がアフリカ連合本部を自国の監視下に置くための陰謀だった」と告発。

https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html

CBC （カナダ 2019.2.27）

国連（UN）の専門機関「国際民間航空機関（ICAO）」がサイバー攻撃を受けた事実を数か月にわたって隠蔽（いんぺい）し、航空業界全体にマルウエア（悪意のあるソフトウエア）を拡散させていたことが明らかになった。侵入は2016年頃から行われ、攻撃元は中国と特定されている。

https://www.cbc.ca/news/canada/montreal/montreal-based-un-aviation-agency-tried-to-cover-up-2016-cyberattack-documents-show-1.5033733
https://www.cbc.ca/news/canada/montreal/emissary-panda-chinese-hackers-cyberattack-icao-1.5034177

グローバル化する中国の脅威

THE WALL STREET JOURNAL. 2019.6.25

中国ハッカー、世界の通信大手にサイバー攻撃か

https://jp.wsj.com/articles/SB12120469692213223839204585386420879216614?mod=WSJ_article_EditorsPicks_5

中国政府の支援を受けたとみられる複数のハッカーが、世界の通信事業大手少なくとも10社の携帯電話ネットワークに侵入し、ユーザーの位置情報やテキストメッセージ記録、電話履歴を盗み出していたことが分かった。米サイバーセキュリティー会社サイバーリーズンの最新の報告書で明らかになった。

報告書によると、数年間にわたるサイバー攻撃は、軍当局者や反体制活動家、スパイ、法執行当局者ら計20人を対象にしていた。全員が中国と関係があるとみられ、対象地域はアジアや欧州、アフリカ、中東に及ぶ。ハッキングは現在も続いているという。

インターネットガバナンスの議論

インターネットガバナンスの議論（2012　WCIT-12）

■ITUを中心に国連において主に発展途上国から、インターネットのガバナンスに対しITUや主権国家の権限を強めることを求める働きかけが継続（⇒アラブの春の影響？）。
2012年WCIT-12での国際電気通信規則(ITRs)の改定に盛り込まれる方向となったが結局、多数決での採択に持ち込まれたものの以下の論点が噛み合わず先進国を中心に、4割近い加盟国が署名拒否。

主な争点	ロシア、アラブ、アフリカのスタンス	米国、欧州、日本のスタンス
インターネット資源（IPアドレスやドメイン）に関する国やITUによる管理（インターネットガバナンス）	現行の民間主導のインターネット資源管理体制(ICANN)ではなく、**国際機関等により割り当てられるべき**	企業やユーザーの市民も参画する形によるマルチステークホルダーアプローチを支持（ITUでインターネット資源を割り当てる必要はない）
インターネット上の表現の自由	**政府によるインターネット上の表現（コンテンツ）に対する検閲、遮断等に関する規定を追加すべき**	ITRに、コンテンツ規制、検閲、遮断等につながるおそれのある規定を追加すべきでない
セキュリティ対策	**国際的に拘束力のあるITRにて「セキュリティ」を扱うべき**	ITRではコンテンツ規制、検閲、遮断等につながるおそれのある「セキュリティ」を扱うべきでない。広範な意味を持つ「セキュリティ」ではなく、ネットワークの「堅牢性」に限定すべき

https://www.ituaj.jp/wp-content/uploads/2013/05/WCIT12.pdf

インターネットガバナンスの議論（2018　IGFパリ会合）

2018.11.12~14パリで開催

冒頭のマクロン大統領演説が話題を呼ぶ

⇒インターネットは社会インフラ化、しかし悪意の攻撃に利用されている

⇒実効性のある対応が必要”Internet of Trust”

⇒インターネットには正しい規制が必要

⇒GAFAでも中国型でもない

サイバー空間の信頼性と安全性のためのパリ･コール

- 悪意あるオンライン活動の予防と強靭性を向上
- インターネットのアクセシビリティと完全性を保護
- 選挙プロセスへの干渉を防ぐために協力
- サイバー空間を通した知的財産権侵害に協力して対抗
- 悪意あるプログラムやオンライン技術の拡散を防止
- デジタル製品やデジタルサービスの安全性ならびにすべての人の「サイバー衛生」を向上
- サイバー傭兵や非国家主体の攻撃に対する対抗措置を実施
- 適切な国際規範の強化に協力して取り組む

https://jp.ambafrance.org/article13835

インターネットガバナンス　中国の動向

http://j.people.com.cn/n3/2018/0929/c95952-9504941.html

・2018.11.7~9,浙江省烏鎮で開催
・テーマは「相互信頼・共同ガバナンスのデジタル世界を構築ーオンライン空間の運命共同体を共同で建設」
・中国と世界が相互接続する国際プラットホームや国際インターネットシェア共同ガバナンスをめぐる中国のプラットホームを構築

中华人民共和国网络安全法

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

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「国家情報法」　2017年6月28日より施行

＜立法趣旨＞国の情報活動の強化・保障及び人権の尊重・保障に留意し、国の情報活動に対し基本となる法的原則と法的根拠を他の規定（国家安全法、反スパイ法、反テロリズム法等）と整合性を図りつつ提供する。そのための国の情報活動の実施体制等を規定

中央国家安全委員会　中央軍事委員会（人民解放軍）　国家安全省

＜第7条＞

いかなる組織及び国民も、法に基づき**国家情報活動に対する支持、援助及び協力を行い**、知り得た国家情報活動についての秘密を守らなければならない。

国は、国家情報活動に対し支持、援助及び協力を行う個人及び組織を保護する。

「中国の国家情報法」国立国会図書館
http://dl.ndl.go.jp/view/download/digidepo_11000634_po_02740005.pdf?itemId=info%3Andljp%2Fpid%2F11000634&contentNo=1&_lang=en

米国のスタンス　国家サイバー戦略　2018.9

中国、ロシア、北朝鮮、イランを脅威として名指し

https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

How Did We Get Here?

Russia, Iran, and North Korea conducted reckless cyber attacks that harmed American and international businesses and our allies and partners without paying costs likely to deter future cyber aggression. China engaged in cyber-enabled economic espionage and trillions of dollars of intellectual property theft. Non-state actors

Pillar IV: *Advance American Influence*

Promote an Open, Interoperable, Reliable, and Secure Internet

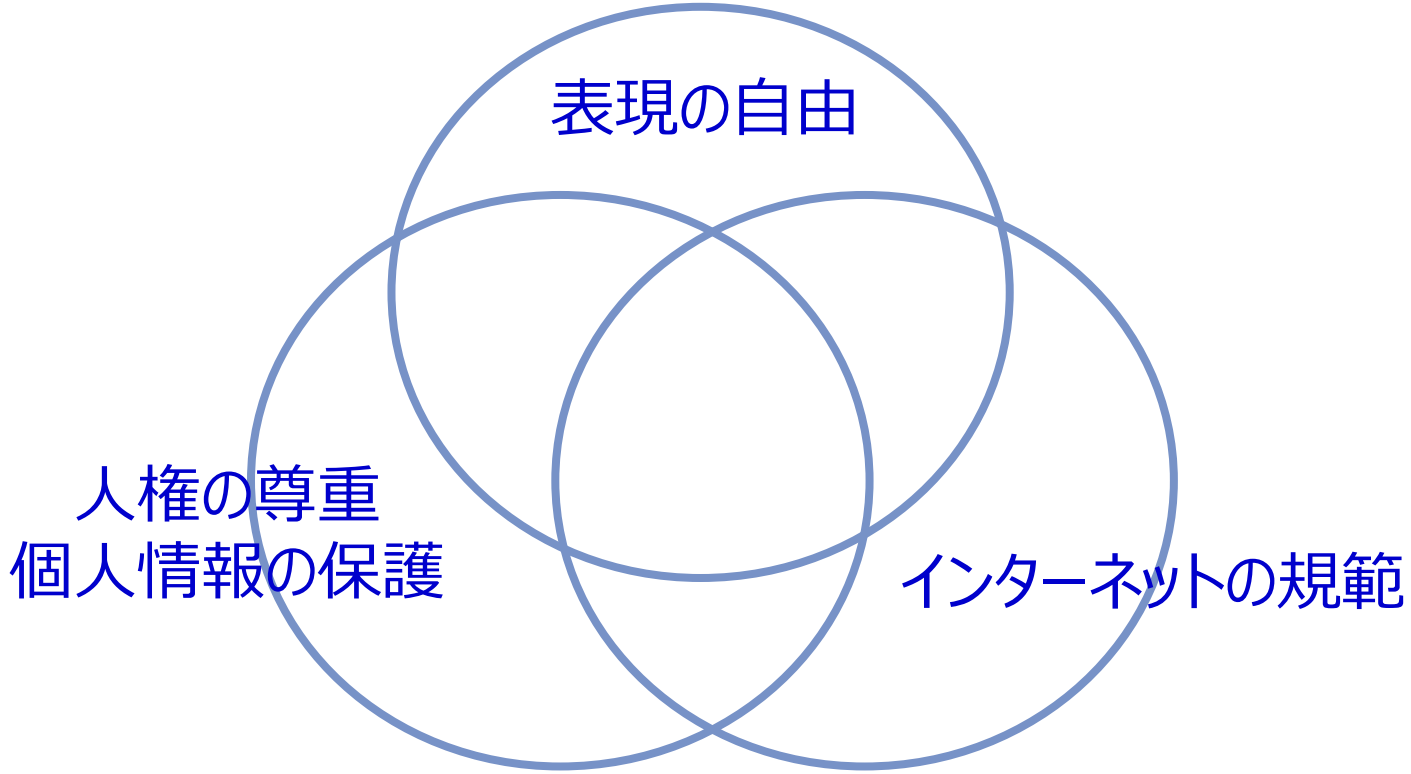
- *Protect and Promote Internet Freedom*
- *Work with Like-Minded Countries, Industry, Academia, and Civil Society*
- *Promote a Multi-Stakeholder Model of Internet Governance*
- *Promote Interoperable and Reliable Communications Infrastructure and Internet Connectivity*
- *Promote and Maintain Markets for United States Ingenuity Worldwide*

Build International Cyber Capacity

- *Enhance Cyber Capacity Building Efforts*

何が問題か？

- 民主主義 vs. 覇権主義
- マルチステークホルダ vs. 国家主権



様々な試み

ディジタル・ジュネーブ条約の提案（2017 マイクロソフト）

戦時における文民の保護を定めたもの

https://cybertechaccord.org/

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

https://cyberstability.org/

インターネットの規範(Norm)の作成を議論中

1. 製品・サービスの改ざん禁止
2. ICT機器のボット化禁止
3. 国家による脆弱性開示プロセス(VEP) の作成
4. プロダクトに対する重大な脆弱性の抑止
5. 防御の基本となる衛生状態の維持
6. 犯罪者によるサイバー攻撃への対抗

これからどうなるのか？

ディジタル時代の新たな課題　とりあえず思いつくままに

- マルチクラウド、マイクロサービス、IoT等のCybersecurity
  →境界防御の破綻、Zero Trust?
  →サプライチェーンのセキュリティ保障は？
- AIのセキュリティ
  → Deep Fakeにどう立ち向かう
  → GAN（Generative Adversarial Networks：敵対的生成ネットワーク）は敵か味方か？
  → データ、アルゴリズムに対する攻撃
  → AIの武器化への対抗は可能か？
- Democratizing AIの行方？
- Private vs. Public
- Trust　？

ディジタル時代でも変わらない原則？

経済発展の基本原則

需要と供給

分業と交換

労働力、資本、全要素生産性（制度と情報流通）

自己組織化と共進化

社会の可視化とネットワーク化

基本的な規範としての民主主義

NTT DATA

Trusted Global Innovator