社会の安心・安全を脅かす サイバー攻撃の現状と対策

日本記者クラブ
研究会「サイバー社会」

2021年9月9日

中曽根平和研　主任研究員
大澤　淳

略歴:大澤　淳

1971年生。
1994年慶應義塾大学法学部卒
1996年同大学院修士課程修了

1995-2009年（公財）世界平和研究所研究員
2009-2014年　同主任研究員
2014年　国家安全保障局初代民間任用局員（内閣参事官補佐）
2017年-（公財）中曽根康弘世界平和研究所主任研究員

2003年明治学院大学国際学部非常勤講師
2004-2006年外務省国際情報統括官組織専門分析員
2007-2009年外務省総合外交政策局外交政策調査員
2013米国ブルッキングス研究所招聘給費客員研究員
2017-2019 国家安全保障局シニアフェロー
2018-2020 日本経済団体連合会２１世紀政策研究所研究主幹（サイバー）

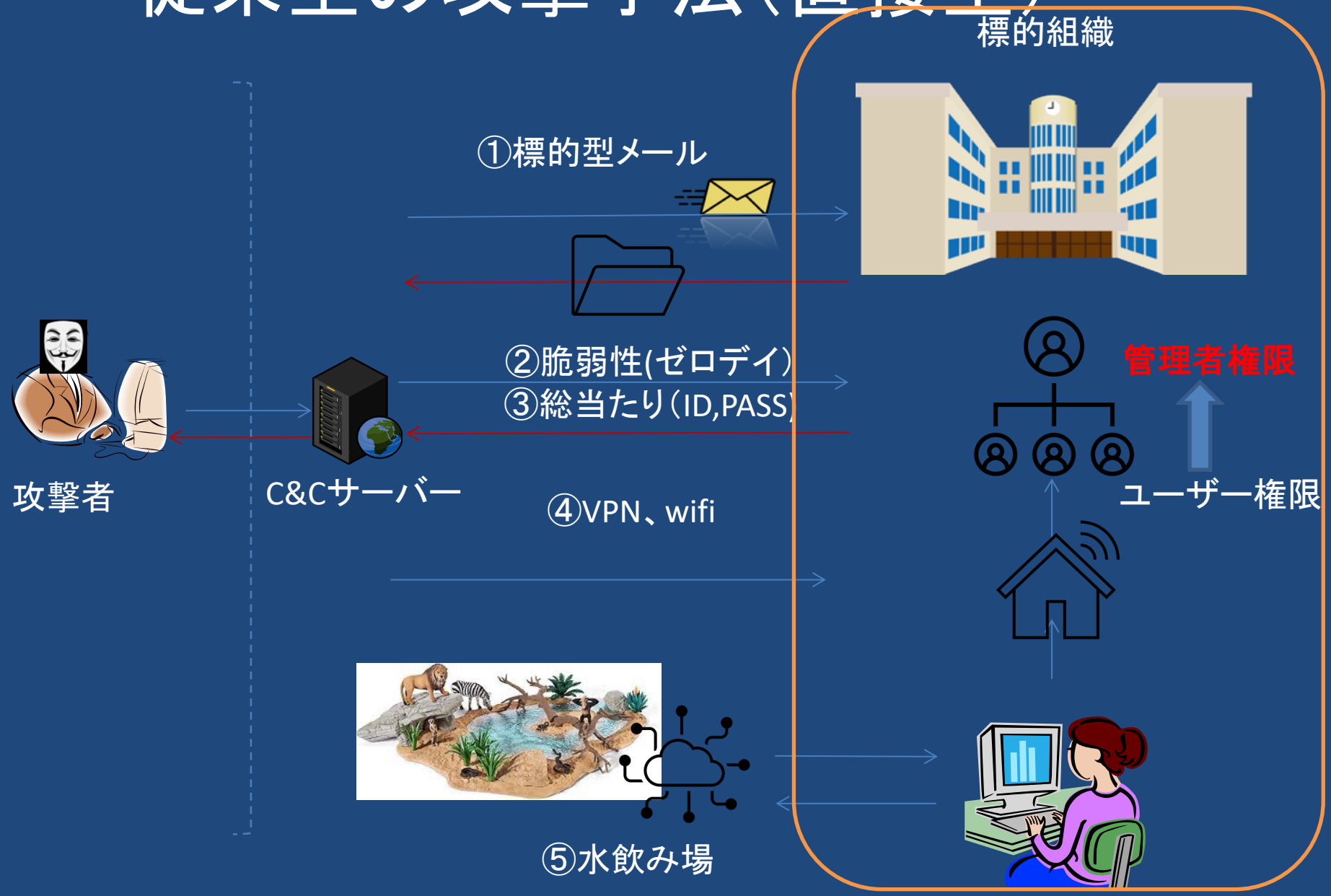
2018- 笹川平和財団プロジェクトコーディネーター（サイバー）
2018- 鹿島平和研究所理事

専門は国際政治学（安全保障、戦略評価、サイバー）

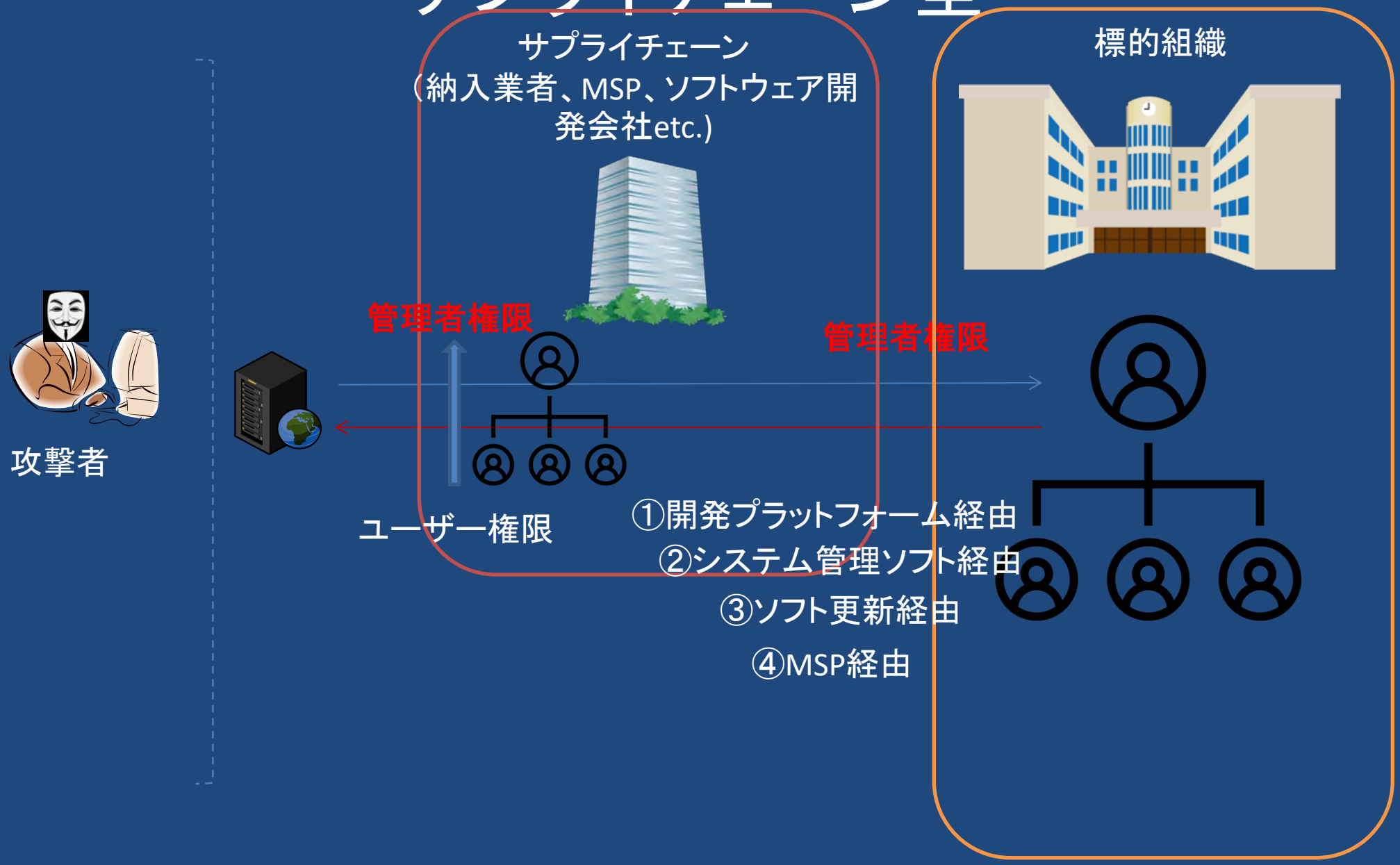
本日の内容

1. サイバー攻撃の現状
   - サイバー攻撃手法の多様化
   - 国家が関与するサイバー攻撃の増大
   - サイバー攻撃対象の広がり
2. ランサムウェアに狙われる企業・市民生活
   - ランサムウェアとは
   - ランサムウェアによる最近の攻撃例
   - 地方自治体・医療機関へのランサムウェア攻撃
   - 日本におけるランサムウェア攻撃の現状
   - 北朝鮮によるランサムウェア攻撃
   - ランサムウェアによる重要インフラへの攻撃に対する米国政府の対応
   - 国際協力によるランサムウェア摘発
3. 情報窃取型サイバー攻撃
   - 攻撃グループTickによる攻撃と警察庁による摘発
   - 中国のサイバー攻撃グループと攻撃対象
   - 産業競争力を奪う情報窃取型サイバー攻撃
   - 中国のサイバー攻撃に対する米国政府・国際社会の対応
4. 情報操作型サイバー攻撃
   - COVID-19と情報操作
   - 情報操作の概念
   - ロシアによる情報戦/影響力工作
   - 中国による認知領域の戦い
   - 各国の情報操作型攻撃への対応
5. 積極的サイバー防衛

従来型の攻撃手法（直接型）



サプライチェーン型


サプライチェーン
（納入業者、MSP、ソフトウェア開発会社etc.）
標的組織
管理者権限
管理者権限
攻撃者
ユーザー権限
①開発プラットフォーム経由
②システム管理ソフト経由
③ソフト更新経由
④MSP経由

国家が関与した主なサイバー攻撃

2007年4月　エストニアの政府・金融機関等への攻撃
2008年7月　リトアニア政府、民間企業への攻撃

2015年4月　フランスのTV5モンドへの攻撃

2015年12月，2016年12月　ウクライナ電力網へのサイバー攻撃

2013年3月　韓国の複数の放送局や金融機関等への攻撃
2016年1月　北朝鮮核実験後，韓国政府へのサイバー攻撃

2017年6月　欧州各国ランサムウェア「NotPetya」による大規模なサイバー攻撃

2017年5月　約150か国でランサムウェア「WannaCry」による大規模なサイバー攻撃

2016年2月　バングラデシュ中央銀行への攻撃、約8100万ドル不正送金

2017年　フランスの大統領選挙、ドイツの総選挙へのフェイクニュースによる情報操作

2008年8月　ジョージアの政府機関・金融機関への攻撃
2019年11月ジョージアの政府機関への攻撃

2006-12年　防衛産業他様々な産業へのサイバー窃取攻撃
2012年12月　米国メディア、シンクタンクへのサイバー攻撃
2015年6月　米国連邦人事管理局に対するサイバー攻撃

2010年8月　イラン核関連施設への「スタックスネット」による攻撃
2019年6月　無人機撃墜の報復としてサイバー攻撃
2019年9月　サウジ石油施設攻撃の報復としてサイバー攻撃

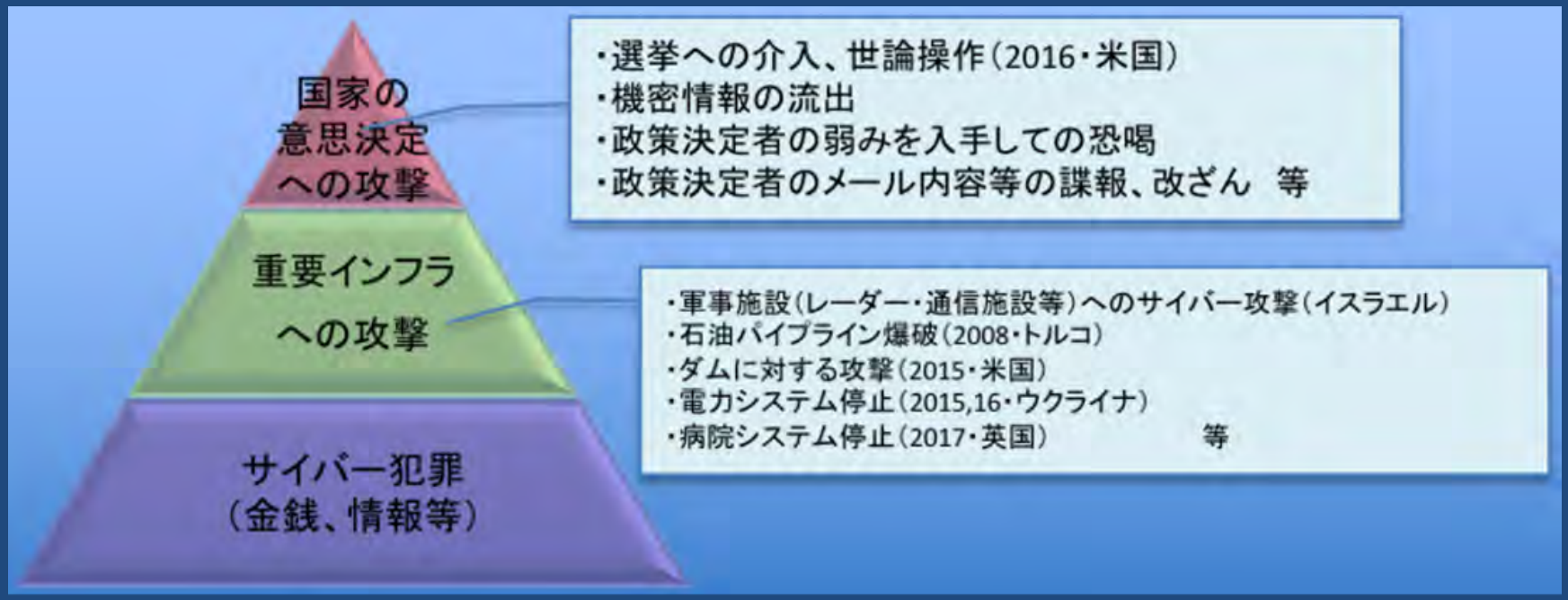
2012年8月　サウジ・カタールのエネルギー企業へ攻撃
2016年11月　空港施設等への攻撃

2014年12月　米SPE（ソニーピクチャーズエンターテインメント）に対するサイバー攻撃

2016年　米国民主党全国委員会に対するサイバー攻撃
2016年- 電力など重要インフラに対するサイバー攻撃

2006年-　米欧日・ASEAN・印等の政府機関・メディア・シンクタンク・ハイテク・防衛他様々な産業へのサイバー情報窃取攻撃

サイバー攻撃の対象の広がり



出典；笹川平和財団政策提言「日本にサイバーセキュリティ庁の創設を！」（2018年））

サイバー攻撃の類型別攻撃主体

金銭目的型：標的型攻撃、脆弱性利用などにより、特定の政府機関、銀行、企業、個人のネットワークに侵入し、不正な送金を行い、またはPC内のデータを暗号化し、解読に身代金を要求する攻撃。

情報窃取型：標的型攻撃（ウィルス付きメール、水飲み場攻撃、ゼロデイの脆弱性利用）などにより、特定の政府機関、企業、団体、個人のネットワーク、PCに侵入し、機密情報、営業情報、特許などを窃取する攻撃。

機能妨害型：DDoS攻撃等の手法により、ネットワークの許容量を超える飽和通信要求によって、サーバー、ネットワークを麻痺させる攻撃。

機能破壊型：標的型攻撃などにより、特定の政府機関、企業、団体、個人のネットワークに侵入し、システム破壊・改ざんを行う攻撃。ネットワーク内のデータ消去・改ざんを目的とするものと、制御系システムを標的として物理的破壊を目的とするものがある。

情報操作型：代理主体(Proxy)等を用いて真の発信者を隠匿たうえで、SNS等に偽ニュースを流布させることにより、対象国（主に民主主義国）における世論操作を目的とした攻撃。選挙結果に影響を与えることを企図していることも。

軍事的サイバー攻撃：軍事攻撃と一体的に行われる機能妨害・機能破壊を目的とした攻撃。電子戦の一環としてC4Iを標的とするものと、軍事行動に影響を与える死活的インフラを標的としたものがある。

ランサムウェアに狙われる市民生活

ランサムウェアとは

IT機器内にサイバー攻撃手法で侵入し、IT機器（サーバー、PC、スマホ等）のデータを暗号化し使用不能にするとともに、復号のための身代金を要求する攻撃。

初期侵入

標的型メール、水飲み場、脆弱性利用、サプライチェーン型の攻撃手法で標的のITシステムに侵入

通信

侵入したマルウェアはC&Cサーバーと交信し、暗号化ツール等をダウンロード

暗号化と外部送信

標的のITシステム内のデータを暗号化し使用不能にすると同時に、外部に送信

身代金要求

標的のPCの画面で、複合化のための暗号通貨による身代金の支払いを要求

ランサムウェアの歴史


1989年
AIDS
Trojan　共通鍵暗号を用いた暗号化
2006年
GPcoder
RSA暗号（秘密鍵と公開鍵）脅迫文
2012年
CryptLocker　2048ビットRSA暗号、ビットコインによる身代金要求
2014年
CTB-Locker　課金式プログラム（7:3）
2014年
KRSW-Locker
TorLockerの日本語版　犯人は17歳の少年（のちに逮捕）
2015年
GrandCrab　RaaS（ランサムサービスを一元提供、6:4）
2017年
WannaCry
Windows脆弱性利用　サイバーパンデミック
2019年
Maze　二重脅迫（窃取したファイルの公表）
2020年
Darkside
2021年
Kaseya
サプライチェーン型ランサム

急増するランサムウェア

FEDERAL BUREAU OF INVESTIGATION
Internet Crime Complaint Center IC3

米国におけるランサムウェアによる被害認知件数と被害額

	2015	2016	2017	2018	2019	2020
被害申立数	2453	2673	1783	1493	2047	2474
被害額mil$	1.62	2.43	2.34	3.62	8.96	29.1

出典：米国FBI-IC3年次レポートより作成

主な手口(米国2020)

1. フィッシングメール
2. リモート・デスクトップ・コントロール
3. ソフトウェアの脆弱性

日本での警察庁被害認知件数は23件
（2020.4-12）

企業のセキュリティ脅威第1位

昨年順位	個人	順位	組織	昨年順位
1位	スマホ決済の不正利用	**1位**	ランサムウェアによる被害	5位
2位	フィッシングによる個人情報等の詐取	**2位**	標的型攻撃による機密情報の窃取	1位
7位	ネット上の誹謗・中傷・デマ	**3位**	テレワーク等のニューノーマルな働き方を狙った攻撃	**NEW**
5位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	**4位**	サプライチェーンの弱点を悪用した攻撃	4位
3位	クレジットカード情報の不正利用	**5位**	ビジネスメール詐欺による金銭被害	3位
4位	インターネットバンキングの不正利用	**6位**	内部不正による情報漏えい	2位
10位	インターネット上のサービスからの個人情報の窃取	**7位**	予期せぬIT基盤の障害に伴う業務停止	6位
9位	偽警告によるインターネット詐欺	**8位**	インターネット上のサービスへの不正ログイン	16位
6位	不正アプリによるスマートフォン利用者への被害	**9位**	不注意による情報漏えい等の被害	7位
8位	インターネット上のサービスへの不正ログイン	**10位**	脆弱性対策情報の公開に伴う悪用増加	14位

出典：IPA　独立行政法人　情報処理推進機構「情報セキュリティ10大脅威2021」 https://www.ipa.go.jp/files/000088835.pdf

ダークサイドによるコロニアルパイプライン攻撃（時系列）

～5月6日

ダークサイドによる身代金要求型（二重ランサム）サイバー攻撃がコロニアル社のITシステムで発現。2時間で100G超の情報漏洩。この時点でファイルの暗号化と身代金要求があったと考えられる。

5月7日

コロニアル社がサイバー攻撃を認知。同社は、パイプライン制御のOTへの横展開（ラテラルムーブメント）はなかったものの、システム構成等が漏洩したことから、パイプライン制御のシステムを停止し、パイプラインの運用停止を発表。

5月7日夕

米国政府は、NSCを中心に、国土安全保障省、エネルギー省、運輸省、財務省、司法省、FBI、国防総省からなる対策チームを立ち上げ

5月8日

コロニアル社はダークサイド側に身代金として75ビットコイン（約5億円）を支払い。暗号化解除ツールを受け取ったが、解除速度が遅いため、バックアップからシステムをリストア。

5月9日

米運輸省は燃料輸送に関する緊急措置導入を発表（タンクローリー運転手の労働時間制限の撤廃など）

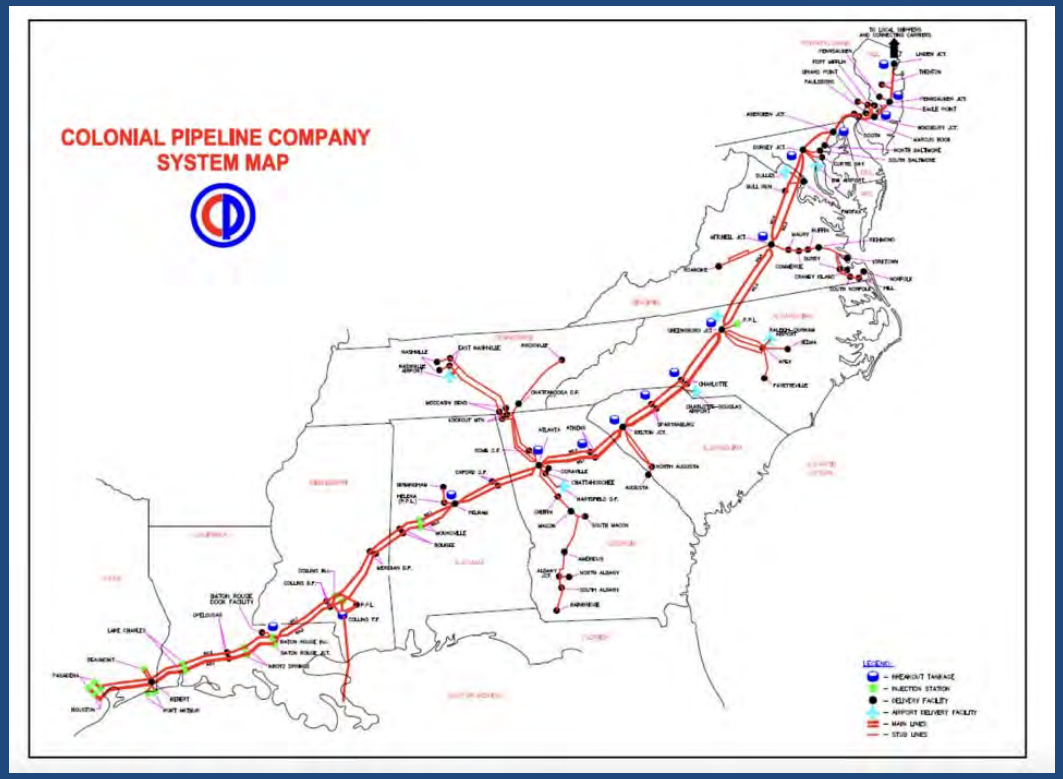
5月11日～

米国東部各州でガソリンの不足が顕在化。5月15日には、DCの80%、バージニアの35%、メリーランドの37%のガソリンスタンドがガス欠に。

Colonial Pipeline

コロニアルパイプライン社

- 南部のテキサス州ヒューストンから東部ニュージャージー州リンデンに至る8,851kmの「コロニアル・パイプライン」を運営。
- 米国最大のパイプラインで、東部から南部にかけての13州にガソリン、灯油、航空燃料などの石油製品を日量270万バレル供給。
- アトランタ、ナシュビル、ダレス、ボルチモア空港に航空燃料を直接供給。



DarkSide: サービスプラットフォームとしてランサムウェアを提供

ダークサイド（Darksupp)

- 2020年8月ごろから活動を開始したロシア系のサイバー犯罪集団。
- 開発したランサムウェアツールをサービスとして提供。
- ロシアを含むロシア語圏の諸国の企業を攻撃から外すプログラムを使用。
- 攻撃先も、医療、教育、政府機関などを除外するなどの「倫理規定」を設けている。

Let's start 10.08.2020

We are a new product on the market, but that does not mean that we have no experience and we came from nowhere.
We received millions of dollars profit by partnering with other well-known cryptolockers.
We created **DarkSide** because we didn't find the perfect product for us. Now we have it.

Based on our principles, we will not attack the following targets:

- Medicine (only: hospitals, any palliative care organization, nursing homes, companies that develop and participate (to a large extent) in the distribution of the COVID-19 vaccine).
- Funeral services (Morgues, crematoria, funeral homes).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

We only attack companies that can pay the requested amount, we do not want to kill your business.
Before any attack, we carefully analyze your accountancy and determine how much you can pay based on your net income.
You can ask all your questions in the chat before paying and our support will answer them.

We provide the following guarantees for our targets:

- We guarantee decryption of one test file.
- We guarantee to provide decryptors after payment, as well as support in case of problems.
- We guarantee deletion of all uploaded data from TOR CDNs after payment.

If you refuse to pay:

- We will publish all your data and store it on our TOR CDNs for at least 6 months.
- We will send notification of your leak to the media and your partners and customers.
- We will **NEVER** provide you decryptors.

We take our reputation very seriously, so if paid, **all guarantees will be fulfilled**.
If you don't want to pay, you will add to the list of published companies on our blog and become an example for others.

JBSへのランサム攻撃（時系列）

5月30日

世界食肉大手のJBSがRevilのランサム攻撃によりITシステムに侵害を受ける。

6月1日

JBSの米国内の食肉加工工場が停止

6月1日

ホワイトハウスの記者会見で、ロシア政府に「犯罪者を隠すべきでない」との警告を送ったことが明らかに。

6月2日

JBSのオーストラリア国内の食肉加工工場が停止。

6月2日

FBIはJBSへのランサム攻撃を、ロシア系犯罪グループREvil と Sodinokibi と発表。

6月10日

JBSは、犯行グループにビットコインで11mil$を支払い。

Kaseya サプライチェーン ランサム攻撃

政府機関・地方自治体へのランサム攻撃（米国）

地方自治体へのランサム攻撃は、2019年に106件、2020年に71件。身代金の平均額は、2019年が約100万ドル、2020年が約70万ドル。身代金要求を受けた自治体のうち、支払い（2019年6.6%、2020年12.7%）、拒否(2019年79.2%、2020年26.7%)、残りは未回答。

Date	Incidents
2019年5月	Bultimore市のITシステムがRobbinhoodの被害に遭い停止。復旧費用18mil$。
2019年6月	フロリダ州Riviera Beach市がランサムウェアの被害にあい、支払い、メール、ウェブサイトが停止。60万ドルの身代金を支払い（市議会が全会一致で決議）。
2019年7月	マサチューセッツ州New Bedford市の158台のPCがRyukの被害。身代金530万ドル。
2019年11月	米国フロリダ州ペンサコラ市（人口約5万人）がMazeの被害、ITシステムが停止。身代金1mil$。
2020年5月	テキサス州の司法管理局がランサムウェアの被害に遭い、州全域裁判所のサーバー、ウェブサイトがアクセス不能に。
2020年6月	アラバマ州Florence市がランサムウェアの被害に遭い、サーバーが停止。身代金約30万ドルを支払い。
2020年9月	ルイジアナ州第4地区裁判所がランサムウェアの被害に遭い、書類がオンライン上で公開。
2020年10月	ジョージア州Hall Countyがランサムウエアの被害に遭い、ITシステムが停止。選挙システムにも影響。
2020年11月	ペンシルベニア州Delaware County（約20万世帯）がランサムウェアの被害に遭い、ITシステムが停止。身代金50万ドルを支払い。

出典：Sungard Availability Service調べ

医療機関へのランサム攻撃（米国）

医療機関へのランサム攻撃により、2019年に764機関、2020年に560機関（80事案）が影響を受けた。身代金の平均要求額は、約460万ドル(2020)。支払われた身代金の平均額は、約91万ドル(2020)。

ランサムウェア Ryuk
東欧に拠点を置くGRIM SPIDERが攻撃主体。21年6月までに235の医療機関が攻撃を受け、2020年の1年間で100mil$の身代金を巻き上げた。

出典：BakerHostetler他調べ

Date	Incidents
2019年8月	カルフォルニア州Wood Ranch病院がランサムウェアの被害に遭い、5835名の患者のカルテがアクセス不能。外科病棟のバックアップシステムも暗号化され、データ回復不能に。病院は閉院。
2019年9月	ワイオミング州Campbell County保健機関がランサムウェアの被害に遭い、外科手術を中止。急患を別の病院に転送、新患の受付停止
2019年10月	アラバマ病院グループのDCH Health Systemがランサムウェアの被害に遭い、3病院でシステムが停止。新患の受付停止、紙と鉛筆の記録を強いられる。病院グループは身代金を支払い。
2020年9月	全米最大手の医療グループUniversal Health Serviceがランサムウエア Ryukの被害に遭い、400の病院でITシステムへのアクセスが3週間停止。被害額67mil$。
2020年10月	ニューヨーク州St. Lawrence Healthがランサムウエアの被害に遭い、3病院でITシステムが停止。
2020年10月	バーモント州バーモント大学病院がランサムウェアの被害に遭い、ITシステムが停止。5000台のPC、1300台のサーバーのデータが暗号化で使用不能に。被害総額64mil$。

出典：各種報道より取りまとめ

医療機関へのランサム攻撃（欧州他）

Date	国名	Incidents
2017年5月	**英国**	**NHS（国民保健サービス）がWannaCryの被害に遭い、ITシステムが停止。**
2020年5月	EU	ヨーロッパ最大の民間病院事業者FreseniusがSnakeランサムウェアの被害に遭い、ビジネス情報が暗号化。身代金1.5mil$支払いシステム復旧。
2020年9月	ドイツ	ロシアの犯行グループDoppelPaymerのランサムウェアにデュセルドルフ大学病院が被害に遭い、ITシステムが停止。措置の遅れから患者1名が死亡。
2021年2月	フランス	二つの病院グループ(7病院)がRyukランサムウェアの被害に遭い、ITシステムが停止。患者を他の病院に転送。フランスでは、2020年に27件の病院を狙ったランサム攻撃が発生。マクロン大統領は、10億ユーロをサイバーセキュリティに追加拠出と表明。
2021年3月	オーストラリア	首都メルボルンのEastern Healthがランサムウェアの攻撃に遭い、四つの病院のITシステムが停止。2週間システム復旧せず。
2021年5月	**アイルランド**	**Irish Health Serviceがランサムウェアの被害に遭い、同国の医療システムが停止。ドネリー保健大臣は「健康保険サービスに重大な影響」と発言。**
2021年5月	ニュージーランド	Waikato地区の医療システムがランサムウェアの被害に遭い、ITシステムが停止。

出典：各種報道より取りまとめ

北朝鮮の金銭目的型攻撃の被害

銀行への攻撃による不正送金		
日付	国名	被害額(未遂分含)
2015年12月	グアテマラ	1,600万ドル
2015年12月	ベトナム	100万ユーロ以上
2016年2月	バングラデシュ	9億5,100万ドル
2016年5月	南アフリカ、日本（ATMからの引出）	1800万ドル
2016年7月	インド	1億6,600万ドル
2016年7月	ナイジェリア	1億ドル
2017年10月	チュニジア	6,000万ドル
2017年10月	台湾	6,000万ドル
2018年1月	メキシコ	1億1,000万ドル
2018年1月	コスタリカ	1,900万ドル
2018年2月	インド	1700万ドル
2018年3月	マレーシア	3億9,000万ドル
2018年5月	チリ	1,000万ドル
2018年6月	リベリア	3,200万ドル
2018年8月	インド	1,300万ドル
2019年2月	マルタ	1,450万ドル
2019年2月	スペイン	1,080万ドル
2019年3月	ガンビア	1,220万ドル
2019年3月	ナイジェリア	930万ドル
2019年3月	クウェート	4,900万ドル

暗号通貨取引所等への攻撃		
日付	国名（取引所）	被害額(未遂分含)
2017年2月	韓国 (Bithumb)	700万ドル
2017年4月	韓国 (Youbit)	480万ドル(3618Bitcoin)
2017年5月	(Wannacry)	14万4千ドル(52Bitcoin)
2017年7月	韓国 (Bithumb)	700万ドル (Bitcoin/Ethereum)
2017年夏	韓国	2万5千ドル(70Monero)
2017年9月	韓国 (Coinis)	219万ドル(Bitcoin)
2017年12月	韓国 (Youbit)	保有する暗号通貨の17%
2017年12月	スロベニア (NiceHash)	7,000万ドル以上(Bitcoin)
2018年6月	韓国 (Bithumb)	3,100万ドル
2018年8月	インド	1,300万ドル
2018年10月	バングラデシュ	260万ドル
2019年3月	タイ、シンガポール、香港、中国（DragonEx)	900万ドル
2019年3月	韓国 (Bithub)	2,000万ドル

出典：国連専門家パネル報告書による

ダークサイドによるコロニアルパイプライン攻撃への米政府の対応（時系列）

5月8日

FBI等を中心に「コ」社の内部情報が送信されていた米国内の中継サーバーを8日にテイクダウン。「コ」社を含む他の被害企業（20数社）の窃取された情報も司法当局によって差し押さえ。

5月8日～9日

ダークサイドが身代金をためていたデジタル・ウォレット（口座）からほとんどのビットコインが引き出される。米国政府による奪還作戦が行われた模様。

5月10日

ホワイトハウスでランドール国土安全保障省顧問とニューバーガー国家安全保障担当大統領副補佐官による記者会見。ダークサイドによる犯行と断定。ロシア政府による関与は無い（バイデン大統領）

5月12日

コロニアル社はパイプラインの操業再開を発表。13日中にパイプラインの全線の運用再開。正常化までは1週間程度かかる見込み。

5月13日

米国からの圧力にさらされ、攻撃に利用していたインフラ（情報機器群）が使えなくなったとして、ダークサイドが活動停止を発表。

5月13日

バイデン大統領がホワイトハウスで記者会見、「事態は数日以内に収集の見込み」と。

White House Briefing on May 10

1. "The FBI identified the ransomware as the DarkSide variant, which they've been investigating since October of last year. It's a ransomware as a service variant, where criminal affiliates conduct attacks and then share the proceeds with the ransomware developers."
2. "In tackling ransomware, we're working to disrupt ransomware infrastructure. The FBI recently worked with international partners to disrupt two particular strains of ransomware: the Emotet and NetWalker strains."
3. "Indeed, to combat the exploitation of virtual currencies that are often used for payment in ransomware, the U.S. Treasury has also been leading international efforts, including driving development and adoption of virtual assets standards under the Financial Action Task Force. "

国際協力 ドーバー作戦 CryptLocker撲滅

Cryptolocker：2012年から2014年にかけて、世界で20万台近いシステムに感染、27mil$もの身代金を稼いだ。

米国FBIと欧州サイバー犯罪センター(EC3)は、12カ国の司法当局の協力を得て、2014年6月に、CryptolockerとGameover Zeusを拡散するために使用されていた攻撃ITインフラの差し押さえに成功。
攻撃者は自身のデータベースを安全な場所に移そうとしたが、既にネットワークの一部を押さえていた当局によって阻止された。
英米当局は、シンクホールの手法を用いて、攻撃者の通信を監視し、攻撃インフラの特定に至った。
FBIはGameover ZeusとCryptolockerの攻撃者を取りまとめていたロシア人のEvgeniy Bogachev（通称lucky12345およびslavik）を指名手配。（ロシア政府は犯罪者引き渡しを拒否）。
差し押さえられた攻撃インフラの情報を利用して、2014年8月、感染者の暗号化されたファイルを修復することができるDecrypt Cryptolockerというポータルサイトが立ち上げられた。

情報窃取型サイバー攻撃

加藤官房長官会見（2021年4月20日夕）

- 「平成28年から29年までの間、住所、氏名等の情報を偽って、日本のレンタルサーバー契約に必要な会員登録を行なった事件につき、本日、警視庁が中国籍の男を東京地方検察庁に書類送検し、その旨発表されたものと承知をしております。本件捜査を通じて、契約された日本のレンタルサーバーが、ＪＡＸＡ等に対するサイバー攻撃に悪用されたこと、またその攻撃には中国人民解放軍61419部隊を背景に持つ「Tick」と呼ばれるサイバー攻撃集団が関与した可能性が高いことが判明したことも承知をしております。この事件との直接の関係はないものの、こうした中国人民解放軍が関与している可能性が高いということであるサイバー攻撃が約200の国内企業等に対し実行されたことを警察当局において把握されているものと承知をしております。」

松本警察庁長官会見（2021年4月22日）

問　長官にお尋ねします。JAXA等に対する大規模なサイバー攻撃がありました。それに絡んで、警視庁公安部が中国籍の男を書類送検したところです。この攻撃には、中国の人民解放軍が関わっているとみているとのことですが、本事件の内容、受け止め、そして、こうした事案への警察としての対応も含めて、お考えをお願いします。

答　（長官）お尋ねの件は、平成28年から29年までの間、合計5回にわたり、住所、氏名等の情報を偽って日本のレンタルサーバの契約に必要な会員登録を行ったものですが、この事件について、4月20日、警視庁が、中国共産党員の男を被疑者として東京地方検察庁に書類送致したと承知しております。

本件事案を通じて契約された日本のレンタルサーバは、JAXA等に対するサイバー攻撃に悪用されました。

その後の捜査等を通じて、被疑者・関係者の供述をはじめ数多くの証拠を積み上げることにより、約200の国内企業等に対する一連のサイバー攻撃がTickと呼ばれるサイバー攻撃集団によって実行され、当該Tickの背景組織として、山東省青島市を拠点とする中国人民解放軍戦略支援部隊ネットワークシステム部第61419部隊が関与している可能性が高いと結論付けるに至りました。引き続き、事案の全容解明に向けて、捜査を推進してまいりたいと思います。

なお、サイバー攻撃への対応は、経済安全保障を含む国家の安全保障・危機管理上の重要な課題であると認識しており、今回の送致に当たり、攻撃の背景組織を特定するまでに至ったのは非常に意義深いものと考えております。外国の治安情報機関からも強い関心が示されているところです。

Tick による攻撃（時系列）

2006年ごろ

特定の日本の組織・企業をターゲットに、マルウェアをメールに添付して特定の人物に送りつける標的型攻撃を開始。

2013年

通信社のウェブサイトを使用した水飲み場攻撃（Webページを閲覧に来た標的にマルウェアを感染させる攻撃）が日本で初めて発覚。
官公庁等が標的。

2015年

Flashの脆弱性とMicrosoft Officeの脆弱性を利用した攻撃が発生。ハイテク、エンジニアリング、メディアが標的。

2016年

Tickの活動が公になる
日本製セキュリティ資産管理ソフトの脆弱性を利用したサイバー攻撃が発生。多数の日本企業、官公庁が犠牲に。

2018年

日本企業の海外拠点を標的とした攻撃開始。化学、ＩＴ、電機、衛星通信、重工業が標的。

2019

三菱電機に対する攻撃が発覚（2020年1月）。2019年3月に中国拠点のウィルス対策管理サーバーの脆弱性をついて侵入。国内の132台のPCが感染。

中国のサイバー攻撃グループは日本をターゲットに

攻撃グループ（別名）	攻撃対象
APT4	アジア太平洋諸国（特に日本、韓国） 航空宇宙、防衛産業
APT9 (Nightshade Panda)	日本、台湾、米国、シンガポール、インド、韓国、タイ 宇宙、農業、建設、エネルギー、医療、ハイテク、メディア、交通
APT10 (Cloud Hopper, Stone Panda, 国家安全部)	世界各地（特に2016年以降は日本） 政府機関、シンクタンク、防衛産業、宇宙、医療、メディア ＊BAE/PwCは17年4月同グループが日本をターゲットにした作戦を実行中と指摘 ＊19年2月の米国による実行犯2名の訴追、並びに米英豪加NAおよび日本医よる国際非難の後活動は低調 ＊通常のAPTと異なり、標的と取引関係にあるMSPのシステムへの侵入を足掛かりに情報を入手
APT12 (Numbered Panda、PLA)	アジア太平洋地域(-2011) 台湾・日本(2011-) メディア、軍事産業（特に衛星、暗号技術） 日本の防衛関連企業・組織を標的にした攻撃（静的解析回避型）を実行中
APT15	米国、ヨーロッパ諸国（日本） 商社、エネルギー、金融、防衛産業、外交当局、ウィグル族関連
APT16	台湾　日本 ハイテク関連、政府機関、メディア、金融関連
APT17 (Hidden Lynx)	世界各地 政府機関、防衛産業、航空産業、IT企業、法律事務所 ＊FireEyeは同グループが日本をターゲットに攻撃を活発化と指摘
Tick (PLA 61419)	**日本(2006-)、韓国 政府機関、防衛関連組織、通信、電機、重工業（造船関連）、ハイテク関連、化学、メディア**
Dragon Ok	日本：大学・学術機関（科学技術）
APT41/ Winnti	先進国全般、日本 ハイテク関連製造業、化学、電子商取引、投資ファンド、エレクトロニクス、テレコム、オンラインゲーム
Black Tech　(PLEAD)	台湾および日本(2017年末以降)：民間セクター全般
Taidoor	台湾・東南アジア中心であったが、2017年末から日本を標的に
Tonto　(PLA)	韓国のTHAAD配備に関連して攻撃を行っていたが、最近日本でも活動を開始
LODEINFO　(APT10?)	日本（2019-）　政府系機関、主要メディア、シンクタンク

攻撃グループ名はFireEye社によるもの　　出典：FireEye社資料、各種公開資料より作成

中国製造2025と10重点分野

2025

Made in China

2015年5月中国国務院は「中国製造2025」と題する10カ年の産業政策を発表

2025
- 第一段階
- 製造強国の地位確立（仲間入り）

2035
- 第二段階
- 製造強国の中位レベルの達成（イノベーション牽引国）

2049
- 第三段階
- 製造強国の指導的地位の確立（大半の分野で競争優位を確立）

10重点分野

次世代情報技術	省エネ・新エネ自動車	航空・宇宙	海洋工学 ハイテク船舶	先進鉄道
CNC工作機械 ロボット	電力設備	新素材	バイオ医薬 高性能医療機器	農業機械

産業競争力を奪うサイバー攻撃：欧米の事例

カナダの通信機器大手ノーテル社は、ベル研究所の流れを組み、いち早く光ファイバーや電話のデジタル化を模索。インターネット回線向けのコンピューター制御スイッチや通信機器製造のパイオニア的存在だった。

ノーテル社は、サイバー攻撃により、2000年から10年近く知財・ビジネス情報を窃取され、2009年に経営破綻した。中国のハッカーが2000年から、数年にわたって技術マニュアルや調査研究リポート、事業計画書、従業員の電子メールなどを含む文書をダウンロードしていたことが明らかになっている。

ノーテル社上級システムセキュリティ顧問たったBrian Shieldsは、「中国による広範なサイバー攻撃が企業崩壊の一因なった」とメディアのインタビュー で答えている。

Huaweiは、ノーテルが破綻した2009年に、同社のEthernetビジネスを400百万ドルで買い取ると持ちかけている。また、Huaweiの5Gイノベーションを支える「フェーウェイ・フェロー」の称号を与えられた童文（Tong Wen）博士はノーテルでワイヤレス技術研究に長年携わったのち、2009年にHuaweiに入社し、同社のワイヤレス・ネットワーク最高技術責任者である。また、同じ称号を与えられた朱佩英（Zhu Peiying）は、ノーテルで研究したのち2009年にHuaweiに入社し、5G研究のプログラムリーダーを務めている。

米コカコーラは、2008年9月、中国飲料メーカーの中国匯源果汁集団に買収を提案した。買収総額は24億ドルで、中国匯源果汁集団が香港市場に上場している発行済株式を12.2香港ドルで仏ダノン等の株主から買い付けるというものであった。しかし、中国の商務部は、この中国最大となる買収提案に対して、2009年3月18日に、前年施行された独占禁止法をたてに、「競争力が損なわれる」として承認しなかった。

この判断の背後には、中国政府がサイバー攻撃で得た情報が使われたと報道されている 。

一連のサイバー攻撃は、コカコーラ太平洋グループのポール・エッチェルス（Paul Etchells）副社長への2009年2月16日の標的型メール攻撃から始まったとされる。エッチェルス副社長は当時、匯源果汁集団買収の総責任者であった。サイバー攻撃により、同副社長のコンピュータが乗っ取られ、最終的にはコカコーラ内部のネットワークへの侵入を許すことになった 。一度コカコーラのネットワークに侵入したハッカーは、以後1ヶ月間に渡って、FBIが警告するまで活動を続け、企業内の機密書類のほか、企業経営陣の送受信するメールを盗み見ていたと見られている。

結局大株主であった仏ダノンは2010年7月に、中国政府系の香港投資ファンドSAIFパートナーズにコカコーラが提示した額の半値の6ドル（総額2億ユーロ）で匯源果汁集団の22.98%を売却。

米国政府は、2018年10月、民間航空機向けのジェットエンジンの知的財産を窃取するため、フランスおよび米国の複数の民間企業にサイバー攻撃を行ったとして、2名の中国情報機関員を訴追。

ウェスティング・ハウス・エレクトリックは原子力関連企業。2006年に東芝に買収された。2017年原子炉建設事業の赤字が原因でCh.11に基づく破産保護を申請し倒産。同社の主力商品の加圧水型原子炉AP!000（第3世代）は、 2008～中国に輸出され、同社と中国国家核電技術公司は技術開発協力協定を締結。2010年中国のサイバー攻撃グループAPT1がAP1000に関する技術情報を窃取したとして、2014年米国司法当局はPLAの軍人5人を起訴。AP1000の技術は中国に渡り、WHの競合製品としてCAP1400が登場。

米中首脳会談（2015年9月25日）

➢ オバマ大統領は共同記者会見で、「米中両国は経済的なサイバー情報窃取を行わず、支援しないと合意した」と発表

I raised once again our very serious concerns about growing cyber-threats to American companies and American citizens. I indicated that it has to stop. The United States government does not engage in cyber economic espionage for commercial gain. And today, I can announce that our two countries have reached a common understanding on the way forward. We've agreed that neither the U.S. or the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage. In addition, we'll work together, and with other nations, to promote international rules of the road for appropriate conduct in cyberspace.

→米中両国は営業秘密を含む知的財産に対してサイバー攻撃を行わないことに合意。

So this is progress. But I have to insist that our work is not yet done. I believe we can expand our cooperation in this area, even as the United States will continue to use all of the tools at our disposal to protect American companies, citizens and interests.

→協力が実行を伴わなければ、米国企業・国民を守るためにあらゆる手段を取り続ける、と示唆。

(出典：White House Press Release, September 25, 2015)

➢ 習主席は「サイバー犯罪に対する共同対処を強調」

China and the United States are two major cyber countries and we should strengthen dialogue and cooperation. Confrontation and friction are not made by choice for both sides. During my visit, competent authorities of both countries have reached important consensus on joint fight against cyber-crimes. Both sides agree to step up crime cases, investigation assistance and information-sharing. And both government will not be engaged in or knowingly support online theft of intellectual properties. And we will explore the formulation of appropriate state, behavior and norms of the cyberspace. And we will establish a high-level joint dialogue mechanism on the fight against cyber-crimes and related issues, and to establish hotline links.

(出典：White House Press Release, September 25, 2015)

➢ 人民日報は、双方が南シナ海、サイバー等で意見交換と短く報道

ホワイトハウスで開催された米中共同記者会見（ロイター）

司法訴追・FBIによる指名手配

情報操作型サイバー攻撃

COVID-19とフェイクニュース

ロシアによるアストラゼネカ社製ワクチンの信用を貶める情報操作。「モンキー・ワクチン」とのレッテルを貼り、欧米のメディアでの拡散を企図。中傷キャンペーンによって、自国製のワクチンの優位性確保を目指している。

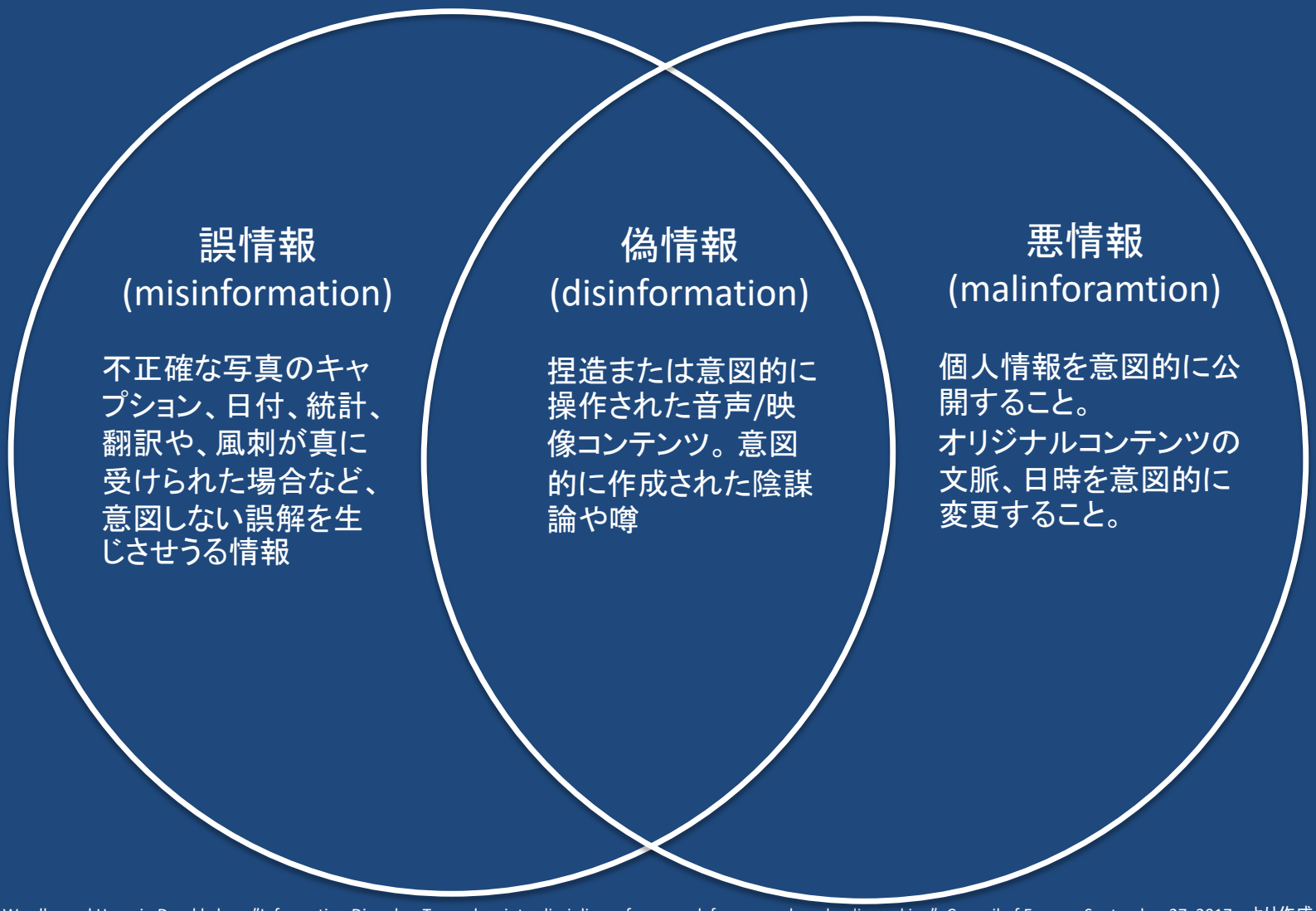
台湾193人接种阿斯利康疫苗后死亡，日本还要追加100万剂

据多家台媒消息，日本外务大臣茂木敏充6月25日宣布，将在7月中旬前追加提供100万剂阿斯利康疫苗给台湾。此前，日本捐赠的124万剂阿斯利康疫苗于本月4日抵台，而在开打该疫苗的短短数周内，台湾接种疫苗后死亡人数已接近200人。

据台媒“中央社”报道，茂木敏充25日上午在例行记者会上宣布，7月1日以后对印尼、马来西亚、泰国与菲律宾各提供100万剂阿斯利康疫苗，以及

日本が台湾に送ったアストラゼネカ社製のワクチンで、接種後多数の死者が出ていると伝える報道。台湾政府の疫病管理センターの発表では、19日現在、約145万人がアストラゼネカ社のワクチン接種を受け、接種後67件の死亡が報告されているが、ワクチンに関係する死者は確認されていない。

「information disorder/情報操作」概念整理



出典：Claire Wardle, and Hossein Derakhshan, ”Information Disorder: Toward an interdisciplinary framework for research and policymaking”, Council of Europe, September 27, 2017. より作成

ロシアの関与が疑われるフェイクニュースの事例（2016年英国）

2016年6月のEUからの独立を問う国民投票を前に、離脱を指示する組織からフェイクニュースが拡散。

英国独立党党首ナイジェル・ファラージ

EUへの拠出金が週3億5千万ポンドに達する

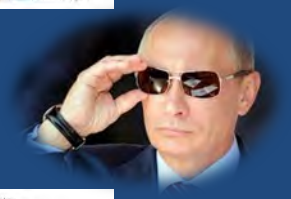
SNSで拡散

実際は、EUから英国への分配補助金などを差し引くと拠出金は週1億数千万ポンド

英国民の67%が「週3億5千万ポンド」を耳にし、42%が真実であると信じ、EU離脱はの勝利の原動力に

2016大統領選挙に影響を与えたGrizzly Step

2016年4月に侵入



DEMOCRATS
CHANGE THAT MATTERS

2015年夏に侵入

「ロシアは米国の主導する民主主義体制を弱体化させることを目的として、2016年米国大統領選挙に工作」
「2016大統領選挙キャンペーンを目標として影響工作をプーチンが指示」
「ロシアの目的は、クリントン候補を誹謗し、米国の民主主義制度への米国民の信頼を失墜させることにあった」
（米国合同情報委報告書）

WikiLeaks

2016年7月22日
・約2万件（うち8000件は添付ファイル付）のDNCのメールを公開.
サンダース候補に対する妨害を示唆するメールの公開を受け、シュルツDNC委員長が辞任。
・そのほか、オフレコ記録、献金者リストが流出。
2016年10月
・クリントン選挙対策本部長ジョン・ポデスタ氏のメールを公開

トロール部隊による情報操作

Faceook、Twitter、Instagram等のSNSに偽のニュースを投稿。
Internet Research Agency（サンクト）：従業員400名、月間予算40万ドル、12時間勤務の2交代制。
Twitter上で反ヒラリーキャンペーンを実施。移民、中絶などアメリカの矛盾を突く攻撃を実施。退役軍人のホームレス問題を指摘。

SPUTNIK
RT
RUSSIA TODAY

プロパガンダメディア

「クリントン氏、100万ドルの慈善寄付で税控除。寄付先は…自身の財団」
RT

米国司法省の発表（2020年10月19日）

- 米国司法省は10月19日、ロシア軍の情報機関であるGRUの要員6名を、世界規模の破壊的マルウェアの拡散とサイバー空間の騒乱の容疑で訴追したと発表。
- ピッツバーグ連邦大陪審は、GRUの74455部隊に所属する6ロシア国籍の要員6名が、ウクライナ、ジョージア、フランスの選挙、化学兵器関連機関、2018年平昌五輪、へのサイバー攻撃に関与したと認定し、米国企業および米国人への攻撃について訴追。
- 6名は、2015年11月から2019年10月にかけて、ロシアの戦略的利益に沿ったサイバー攻撃を実施。

FBIによって指名手配された実行犯6名

中国による認知領域の戦い

- 孫子：不戦屈敵
- 三戦：心理戦、輿論戦、法律戦（＋政治戦、宣伝戦）
  - ✓「輿論戦、心理戦、法律戦を実施 し、瓦解工作、反心理・反策反(5)工作、軍事司法および法律服務工作 を展開する」（人民解放軍政治工作条例）
- 智能化戦争：機械化戦争→情報化戦争→智能化戦争
  - ✓ AIを利用した無人機の群によるスォーム攻撃
  - ✓ 自動化されたロボットによる攻撃
  - ✓ AIを用いた認知空間の作戦
- 制脳権：物理空間から人々の認知空間の戦闘へ
  - ✓ 敵の認知域を攻撃し、我の認知域を防御
  - ✓ 認知抑制：敵の状況把握能力を弱体化、喪失させる
  - ✓ 認知形成：虚偽情報により敵の意思を挫き、誤った判断を導く
  - ✓ 認知支配：敵の意思決定メカニズムを改竄

積極的サイバー防御（ACD：Active Cyber Defense）

- ACDの定義
  「攻撃者のコストとリスクを増大させ、彼らの行動への抑止を試みること」（CrowdStrike)
  「単に脅威に対して自分のネットワークを強化するだけではなく、攻撃者の正体を暴いたり、攻撃者のシステムを無効化したりすることを目的とした対策のこと」(Glosson, 2015)

- アクティブ・ディフェンス（AD）とアクティブサイバーディフェンス（ACD）
- アクティブ・ディフェンス（AD）：
  積極的サイバー防御（ACD：Active Cyber Defense)の概念のかなり前から、米軍内では、アクティブ・ディフェンスという概念があり、この概念がサイバー領域にも適用されることとなった。軍事的には、受動的防衛と能動的防衛は数十年前から定義があり、受動的防衛とは敵の攻撃を難しくする固定陣地のような防御であるのに対して、積極的防衛とは攻撃者を消耗させるために機動的に反撃することを意味していた。

- アクティブサイバーディフェンス（ACD）：
  アクティブ・サイバー・ディフェンス（ACD）は、国防総省（DoD）の防御的サイバー作戦に対する全体的なアプローチの構成要素として提起。高度なサイバー攻撃の検出と防御を成功させるため、脅威情報や分析、サイバー活動のアラート、および対応策を迅速かつ自動的に共有して対処する能力がACDには不可欠とDoDは認識。

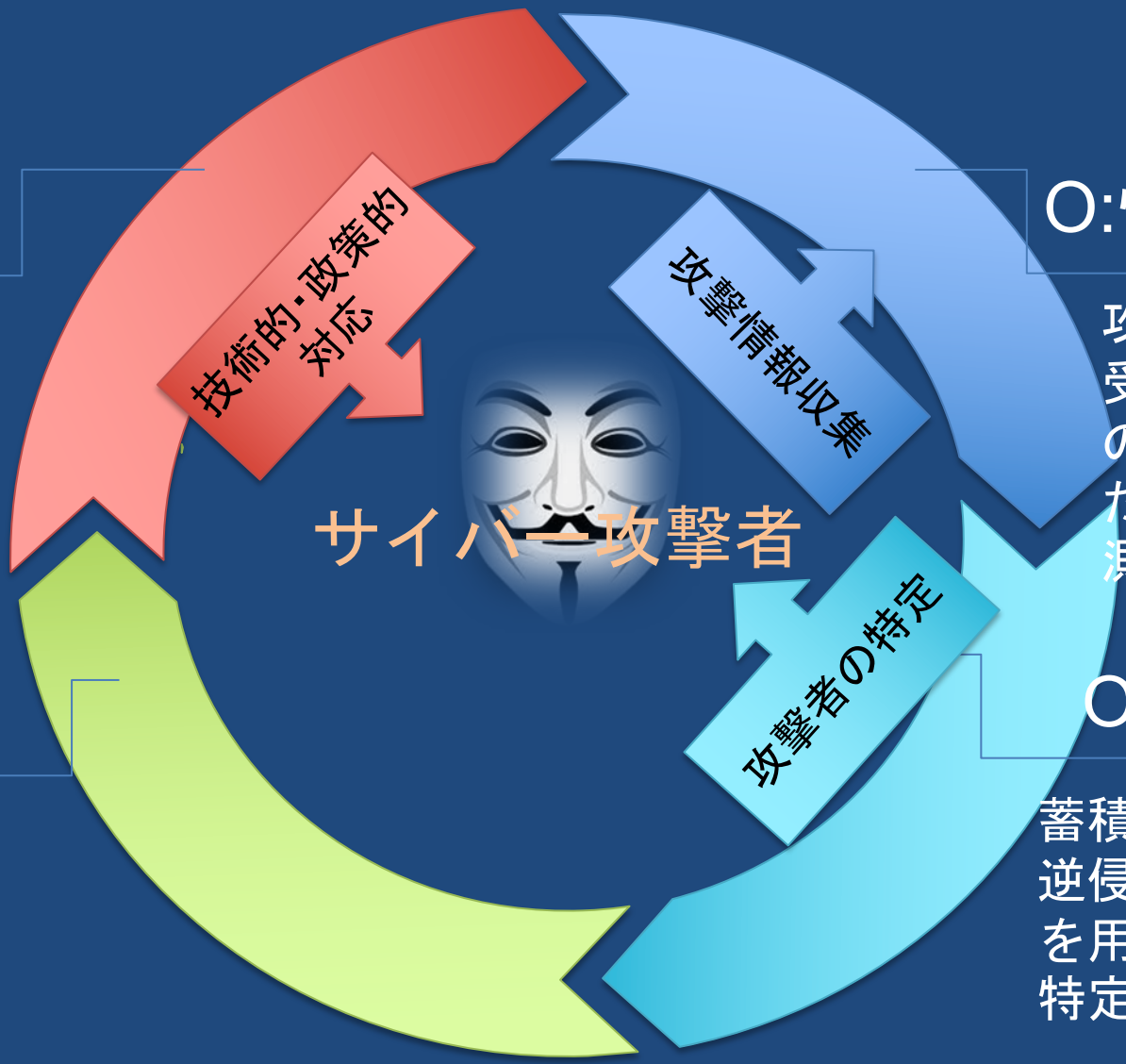
積極的サイバー防御のOODAループ

A:対応

攻撃軽減のための技術的対応や攻撃者を抑止するための政策的対応（訴追等）の実施

D:意思決定

観測データや分析から得られた状況判断をもとに対応を決定



O:情報収集

攻撃者の通信傍受、メタデータの収集等を用いた情報収集・観測

O:分析

蓄積データ分析、逆侵入やビーコンを用いた攻撃者の特定