財務総合政策研究所 ランチミーティング
2021年9月21日

# サイバー空間と国際政治
## ― サプライチェーン脅威を中心に ―

一般社団法人 先端技術安全保障研究所
所長 小沢 知裕

# サイバー空間は新しいワイルドウェスト？

開拓時代の西部アメリカに
例えられるサイバー空間

参考）リチャード・ハースの記事

By Ramon Boersbroek on VisualHunt

# 攻撃者が有利？

ワイルドウェスト
開拓時代の西部
- 粗暴、無法
- 武装した人（多い）・保安官（少ない）

現代のサイバー空間
- 攻撃が防御に比べて容易
- 犯罪者による攻撃
- 国家による攻撃

国家の関与も

# サイバー空間における攻撃手法

システムを使えなくする

破壊　妨害

- イラン、ウラン濃縮施設破壊（2010）

システムを不正に使用する

窃用　改竄

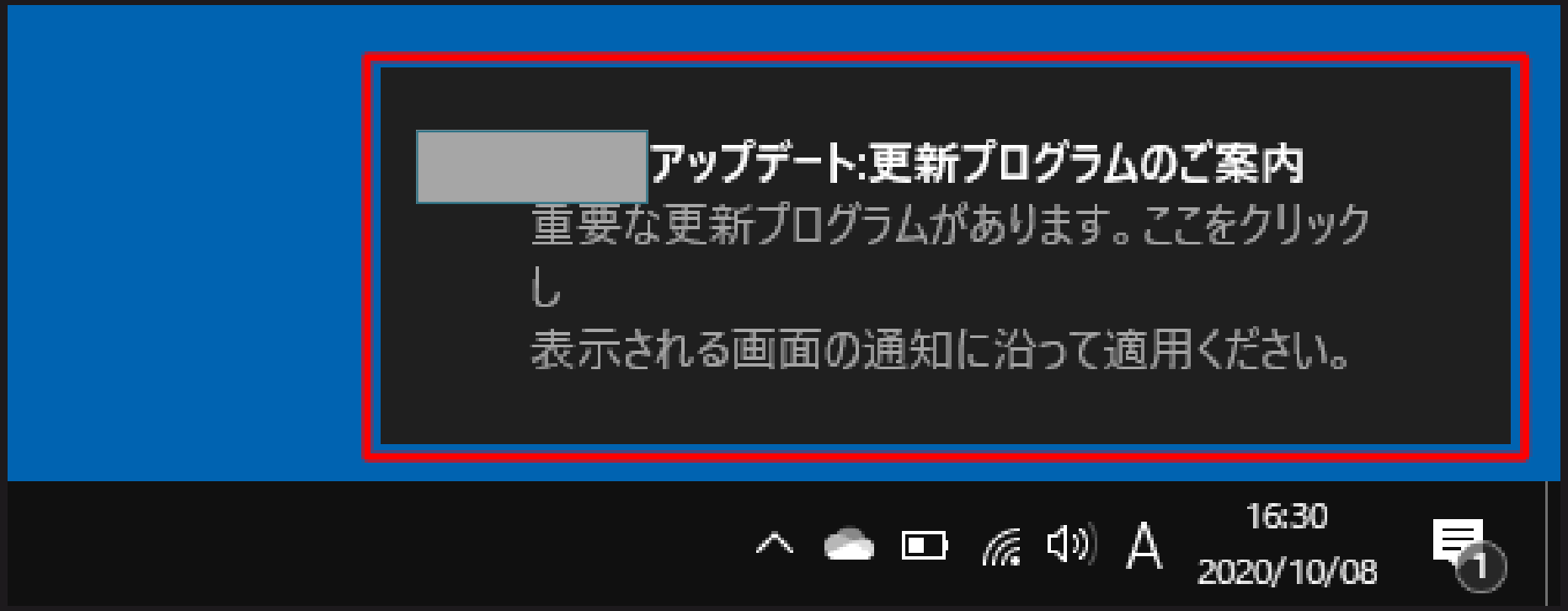
- ソニー・ピクチャーズエンタテインメントへの攻撃（2014）

スパイ　暴露　脅迫

ディスインフォメーション

- ロシア疑惑（2016）
- コロニアルパイプライン停止（2021）

# アップデートしてますか？



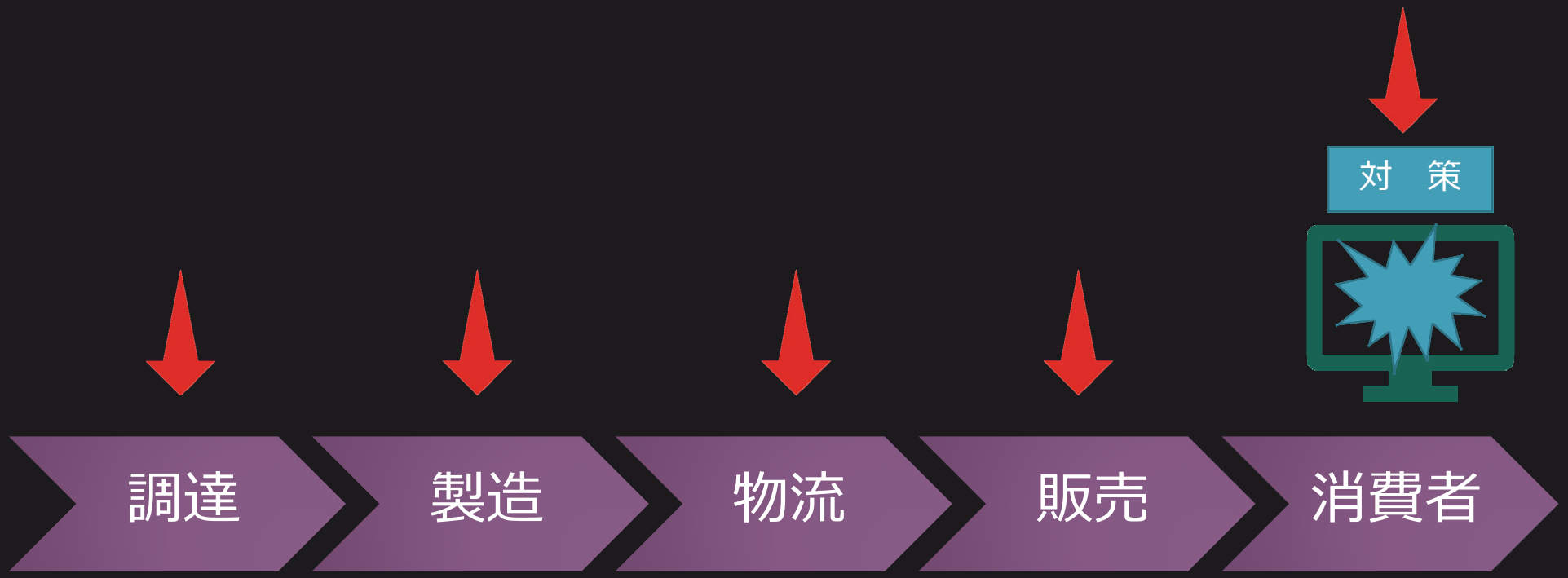
# 攻撃される
# アメリカ

- 米複数省庁のシステムに長期にわたる侵入（～2020年12月）

9つの省庁（司法省、国務省、財務省、エネルギー省、商務省など）
約100の企業（シスコ、SAP、インテル、ファイア・アイ、富士通、楽天など）

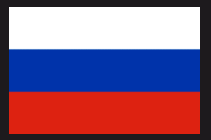
- 米企業ソーラーウィンズ社のネット監視ソフト「オリオン」の更新プログラムを介して感染
- 英米当局がロシア情報機関（SVR）を攻撃者と断定
- 米国および英国がロシアに対し制裁

# サプライチェーン脅威



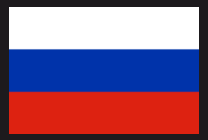
# 4年前に始まったトレンド
## ― ソフトウェアサプライチェーン攻撃 ―

| 発見時期 | 概要 |
|---|---|
| 2017年 | ウクライナ製税務会計ソフト・ミードック |
| 2017年 | 韓国製遠隔管理ツール・ネットサラン |
| 2017年 | PC最適化無料ツール・シークリーナー |
| 2019年 | 台湾ASUS社製品 |
| 2019年 | ゲーム会社3社のゲームソフト |
| 2020年 | モンゴル製チャットソフト・イージーデスクトップ |
| 2020年 | 米ソーラーウインズ社のネット監視ソフト |



ロシア軍情報機関
（サンドワーム）

？



ロシア対外情報庁
（コージーベア）

# その目的は？

| 発見時期 | 概要 | |
|---|---|---|
| 2017年 | 税務会計ソフト・ミードックが感染（NotPetya） | ⇒ ランサムウェアだが利益を殆ど得ず |
| 2017年 | 韓国製遠隔管理ツール・ネットサランが感染 | ⇒ バックドアを設置。スパイ活動？ |
| 2017年 | PC最適化無料ツール・シークリーナーが感染 | ⇒ 2,000,000台に感染も、標的は40台 |
| 2019年 | ASUS製品が感染 | ⇒ 600,000台に感染も、標的は600台 |
| 2019年 | ゲーム会社3社のゲームソフトが感染 | ⇒ 700,000台に感染も、標的は40台 |
| 2020年 | ソーラーウインズ社のネット監視ソフトが感染 | ⇒ 米省庁のシステムなどへ侵入 |

国家によるスパイ活動が疑われる

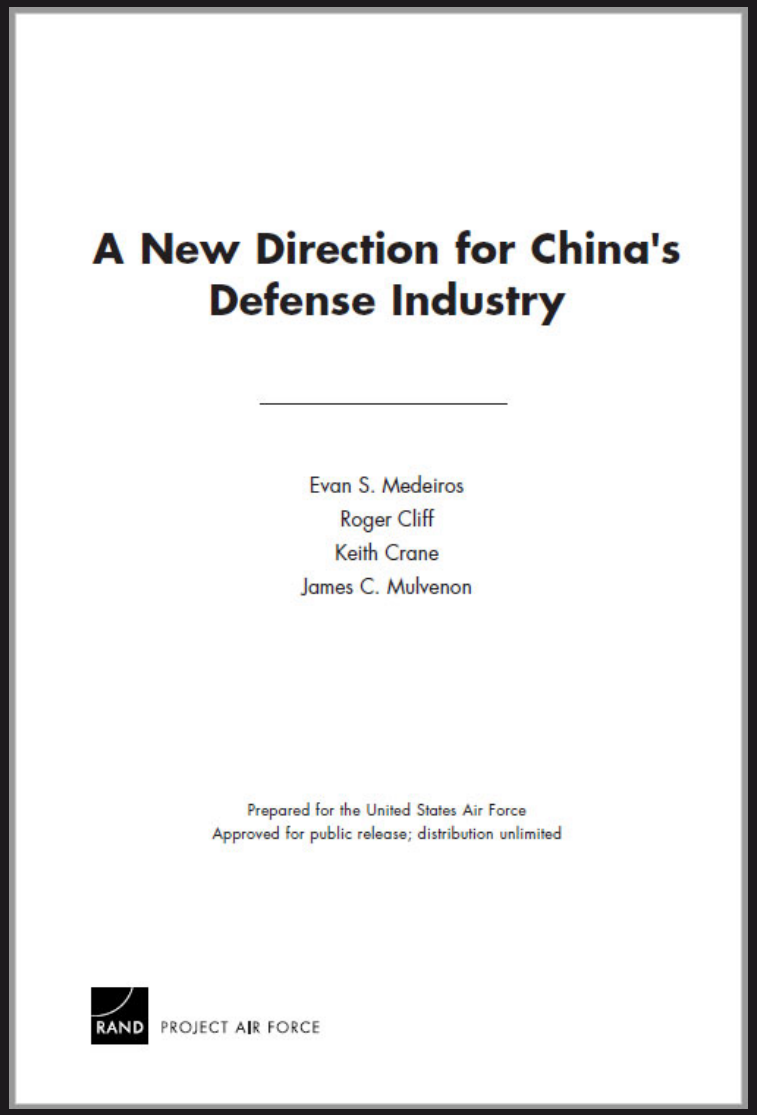
# サプライチェーン脅威のタイムライン

ソフトウェアサプライチェーン脅威

2017

2005　サプライチェーン脅威

もともとはハードウェアの問題




# ハードウェアのサプライチェーン脅威

2005年 米研究所がレポート
『**中国の防衛産業の新しい方向性**』
を発表

中国資本の米国内通信システム
への進出に懸念を表明

スパイツール？

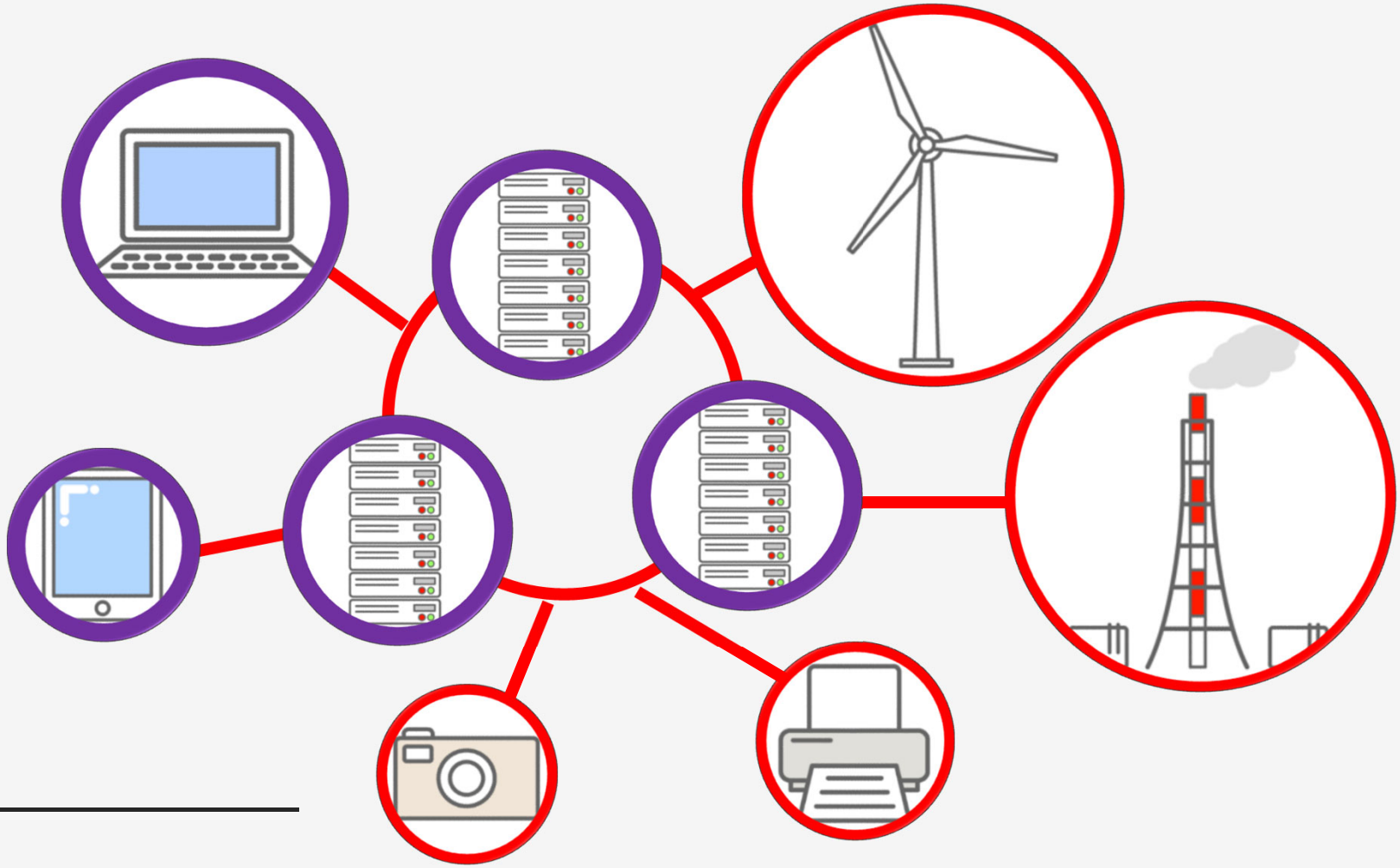
# 2012年
# 米下院情報委員会

Public Domain by
U.S. Federal Government


ZTE

- 中国企業２社の現地法人幹部が証言。
- スパイ行為を行う仕組みの疑いを否定。
- 翌月、同委員会はレポートを発行。

# 通信機器メーカーが売っているもの

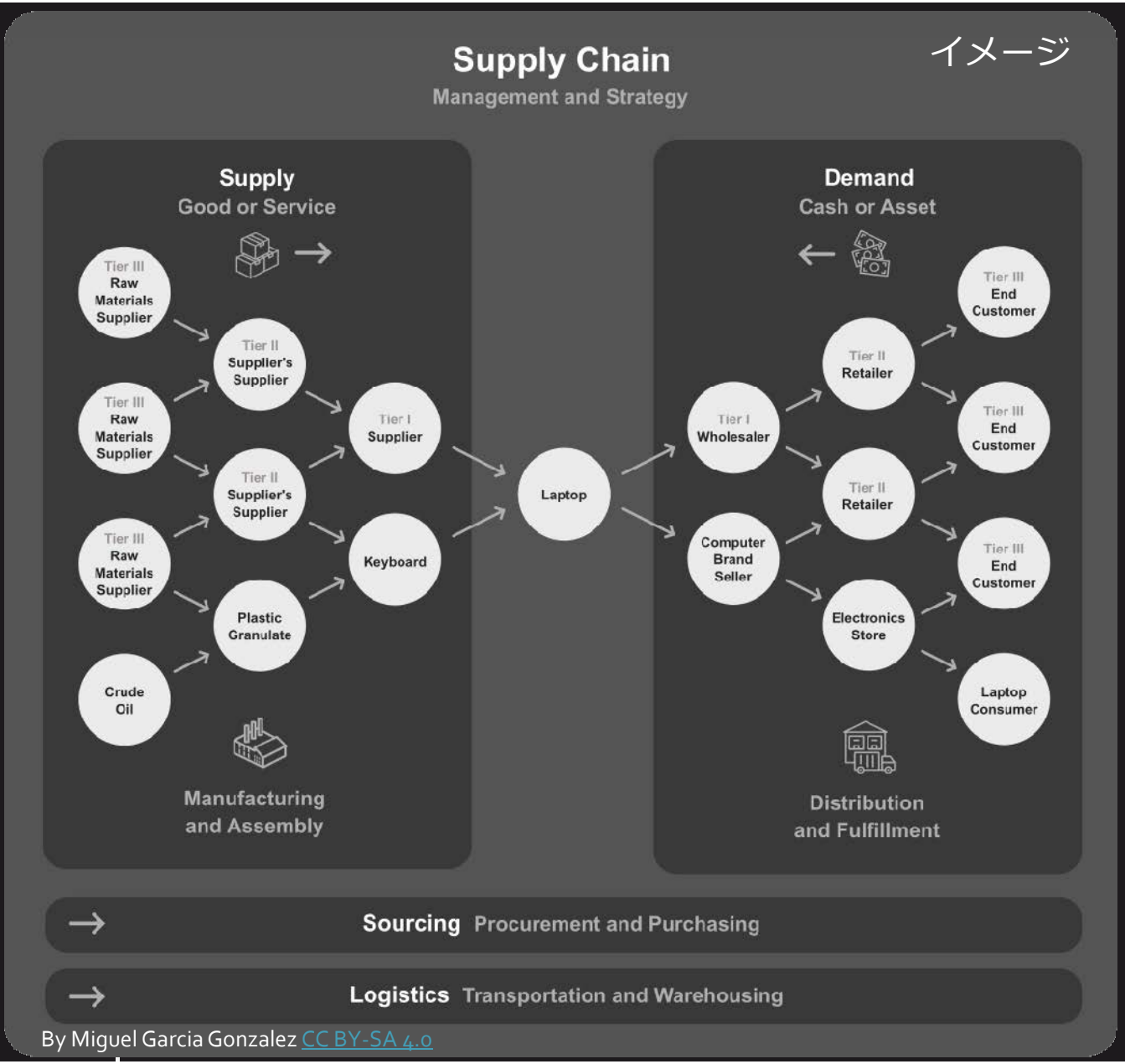


# 中国メーカーへの米国の対応

対象 ： 通信機器メーカー（基地局、スマホ）2社
監視カメラメーカー 3社

（および上記の関連企業）

- 米政府機関における当該企業製品、サービスの購入禁止（2019年8月）
- 米政府機関における当該企業製品、サービス使用者との契約禁止（2020年8月）



By Miguel Garcia Gonzalez CC BY-SA 4.0

# サプライチェーン脅威とは？

例えばiPhoneは...

43カ国からの部品によって構成

外部だけじゃない攻撃者

スパイウェア（ハードウェア）が見つからない？

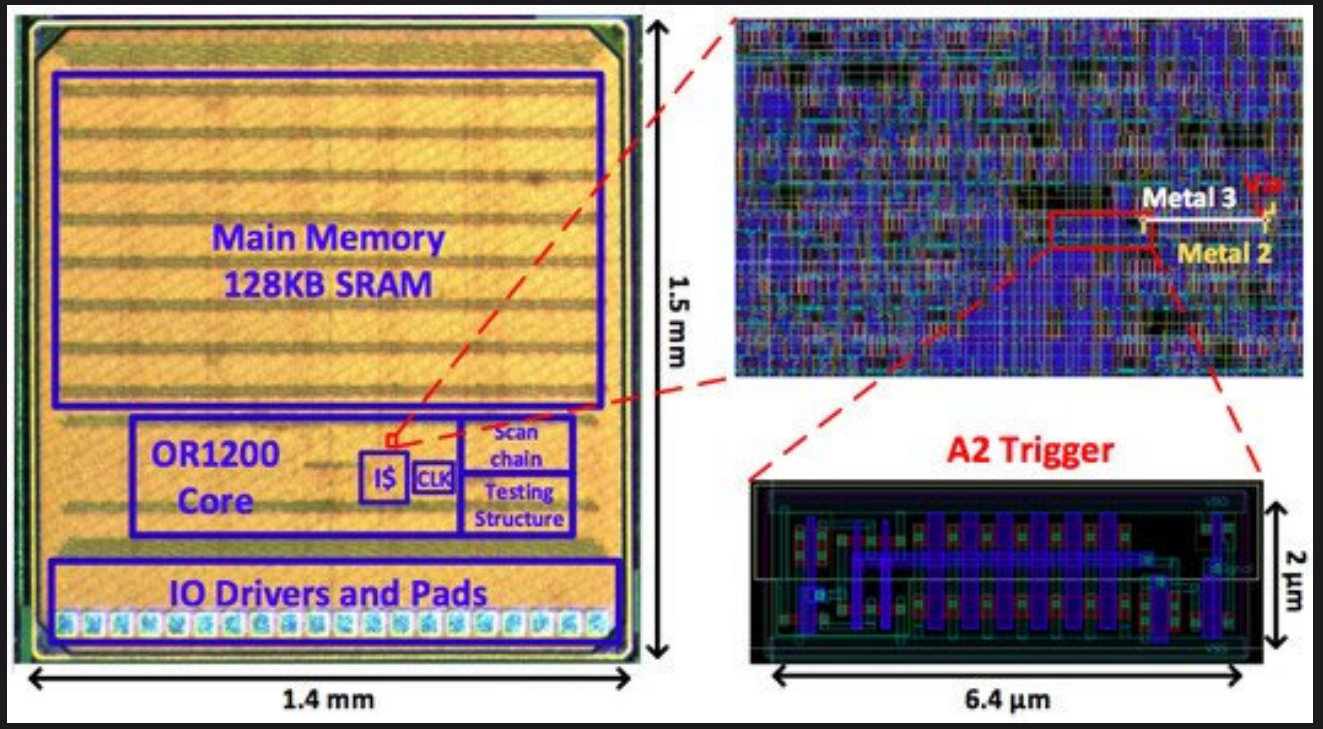
# 実質的に検知不能?

ミシガン大学の研究者が実験に成功

髪の毛の幅の1,000分の1サイズ

システムへの完全なアクセスを実現

通常の手段では検知不能




Kaiyuan Yang, Matthew Hicks, Qing Dong, Todd Austin, Dennis Sylvester, "A2: Analog Malicious Hardware", 2016 IEEE Symposium on Circuits and System (ISCAS)

# 対策

- 自社だけ守ってもダメ。
- 自国だけ守ってもダメ。
  - 関係会社、ビジネスパートナー、委託先
  - 米政府機関は、セキュリティーガイドライン NIST SP800-171を設定
  - 経産省はサイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）を策定

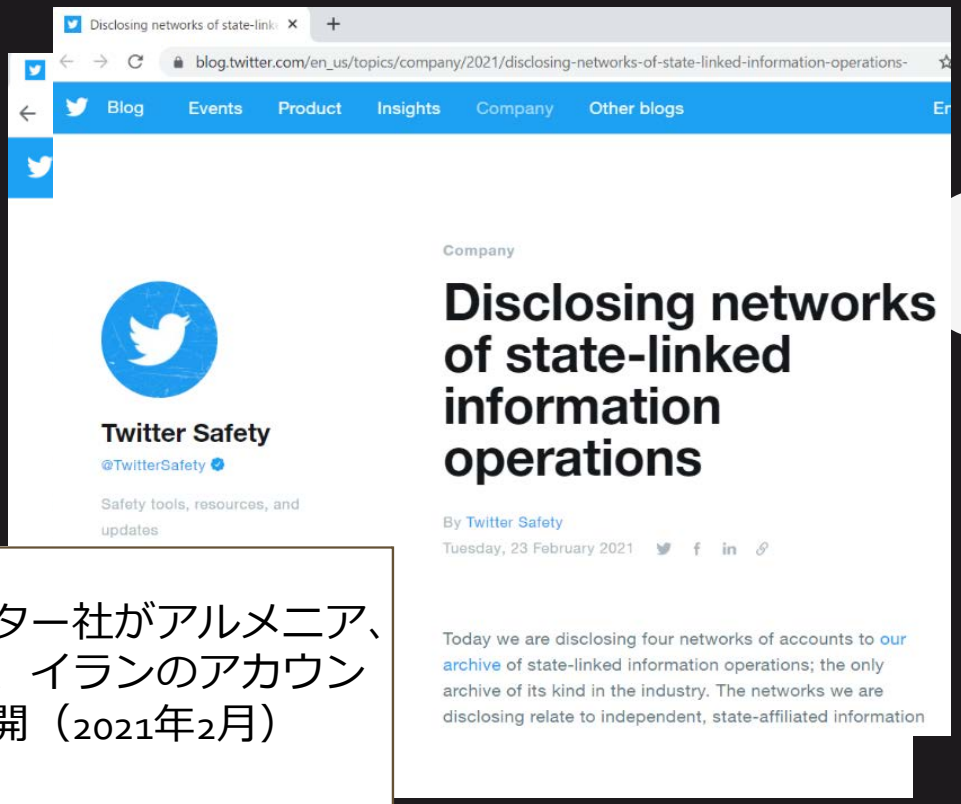
# サプライチェーンから
# 少し離れます

# ソーシャルメディアの操作

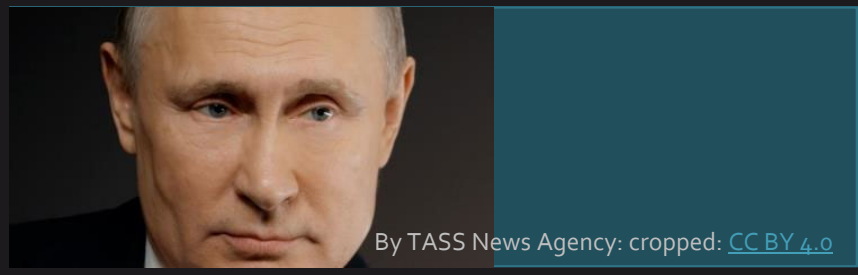
2016年 米大統領選挙（ロシア疑惑）

2018年 米中間選挙

2020年 米大統領選挙




ツイッター社がアルメニア、ロシア、イランのアカウントを公開（2021年2月）




2016年 米大統領選挙（ロシア）

# 対立の構図

| | |
|---|---|
| 1位グループ | 米国 |
| 2位グループ | 豪州、カナダ、中国、フランス、イスラエル、ロシア、英国、 |
| 3位グループ | インド、インドネシア、イラン、日本、マレーシア、北朝鮮、ベトナム |

IISSによるランキング（2021年6月）

# 狙われた東京オリンピック

英政府機関がロシア軍情報機関によるサイバー偵察があったと発表


By Ftaaffe CC BY-SA 4.0

# 対立の構図

| | |
|---|---|
| 1位グループ | 米国 |
| 2位グループ | 豪州、カナダ、中国、フランス、イスラエル、ロシア、英国、 |
| 3位グループ | インド、インドネシア、イラン、日本、マレーシア、北朝鮮、ベトナム |

IISSによるランキング（2021年6月）

# WANTED

WANTED
BY THE FBI

CONSPIRACY TO COMMIT COMPUTER FRAUD; CONSPIRACY TO COMMIT WIRE FRAUD; WIRE FRAUD; AGGRAVATED IDENTITY THEFT; CONSPIRACY TO COMMIT MONEY LAUNDERING

GRU HACKING TO UNDERMINE ANTI-DOPING EFFORTS

Dmitriy Sergeyevich Badin
Artem Andreyevich Malyshev
Alexey Valerevich Minin
Aleksei Sergeyevich Morenets
Evgenii Mikhaylovich Serebriakov
Oleg Mikhaylovich Sotnikov
Ivan Sergeyevich Yermakov

DETAILS

On October 3, 2018, a federal grand jury sitting in the Western District of Pennsylvania returned an indictment against 7 Russian individuals for their alleged roles in hacking and related influence and disinformation operations targeting, among others, international anti-doping agencies, sporting federations, and anti-doping officials. The indictment charges Dmitriy Sergeyevich Badin, Artem Andreyevich Malyshev, Alexey Valerevich Minin, Aleksei Sergeyevich Morenets, Evgenii Mikhaylovich Serebriakov, Oleg Mikhaylovich Sotnikov, and Ivan Sergeyevich Yermakov, with computer hacking activity spanning from 2014 through May of 2018, including the computer intrusions of the United States Anti-Doping Agency (USADA), the World Anti-Doping Agency (WADA), and other victim entities during the 2016 Summer Olympics and Paralympics and afterwards. The indictment charges these defendants with conspiracy to commit computer fraud, conspiracy to commit wire fraud, wire fraud, aggravated identity theft, and conspiracy to commit money laundering. The United States District Court for the Western District of Pennsylvania in Pittsburgh, Pennsylvania, issued a federal arrest warrant for each of these defendants upon the grand jury's return of the indictment.

THESE INDIVIDUALS SHOULD BE CONSIDERED ARMED AND DANGEROUS, AN INTERNATIONAL FLIGHT RISK, AND AN ESCAPE RISK

If you have any information concerning this case, please contact your local FBI office, or the nearest American Embassy or Consulate.

WANTED
BY THE FBI

CONSPIRACY TO COMMIT COMPUTER INTRUSION

Ahmad Fathi
Hamid Firoozi
Amin Shokohi
Mohammad Sagogh Ahmadzadegan
Omid Ghaffarinia
Nader Saedi

ndividuals are wanted by the FBI for cyber crimes, incl
which affected entities in both the United States and o
living in Iran.

ny information concerning this case, please contact
Consulate.

WANTED
BY THE FBI

iring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of
ercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code
mmands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

WANG DONG
es: Jack Wang, "UglyGorilla"

SUN KAILIANG
Aliases: Sun Kai Liang, Jack Sun

WEN XINYU
Aliases: Wen Xin Yu, "WinXYHappy", "Win_XY", Lao Wen

HUANG ZHENYU
Aliases: Huang Zhen Yu, "hzy_lhx"

GU CHUNHUI
Aliases: Gu Chun Hui, "KandyGoo"

HACKERS WANTED BY THE FBI

Gholamreza Rafatnejad
Ehsan Mohammadi
Seyed Ali Mirkarimi
Abdollah Karima
Mostafa Sadeghi
Sajjad Tahmasebi
Mohammed Reza Sabahi
Roozbeh Sabahi
Abuzar Gohari Moqadam

米国は訴追と制裁で対応

# ソーシャルメディアの操作

2011年 米中央軍テロ対策

2012年 中南米大統領選挙

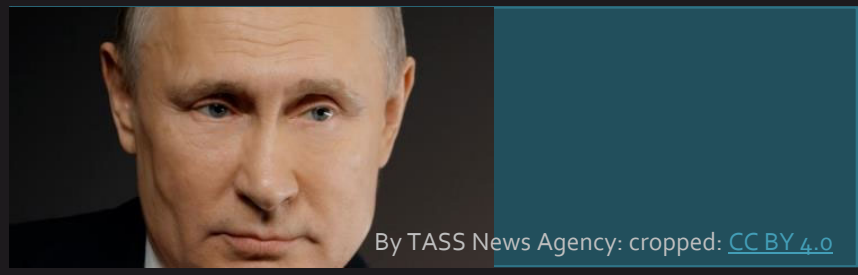
2016年 米大統領選挙（ロシア疑惑）

2018年 米中間選挙

2020年 米大統領選挙


2011年 テロ対策（米中央軍）

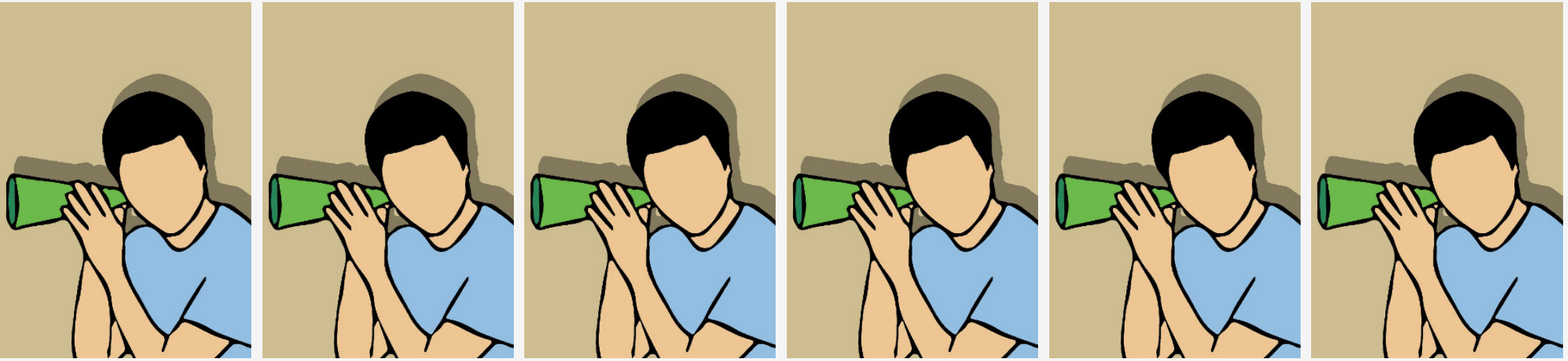

2005～2012年 中南米大統領選挙




2016年 米大統領選挙（ロシア）

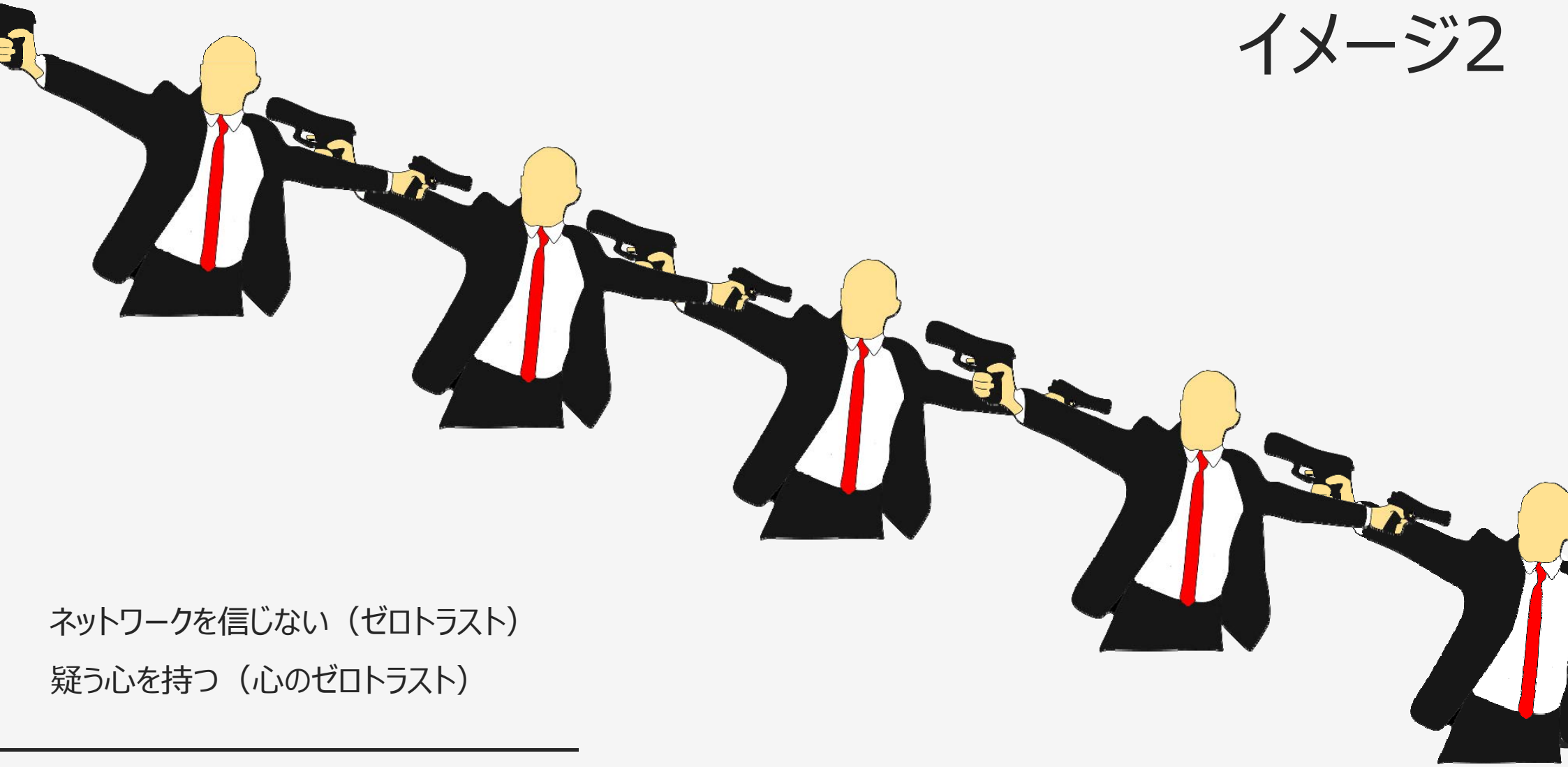

By European People's Party : CC BY 2.0
独メルケル首相
「全く受け入れられない」（2013年10月）

# イメージ



国家間のサイバー事情は複雑

# イメージ2



ネットワークを信じない（ゼロトラスト）

疑う心を持つ（心のゼロトラスト）

# ご清聴ありがとうございました

弊所ホームページへは、下記のURLへアクセスいただくか、
「GIEST」でインターネット検索ください。
https://www.giest.or.jp/