NTT DATA
Trusted Global Innovator

デジタル時代のサイバーセキュリティ

2022／8／5

NTTデータ先端技術　フェロー，　筑波大学客員教授
CISSP, CISA, 工学博士
三宅　功

■本資料は公開された資料に基づいて作成しています。利用した資料は各ページに対応して”Source Note”として併せて公開しています。資料は講演者により極力その正確性を吟味していますが、必ずしも保証されたものではありません。
■本資料内で示された見解は、講演者個人の見解であり、特定の組織の見解を代表するものではありません。

自己紹介

～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、サービスインテグレーション研究所　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, 電子情報通信学会フェロー
2011年～	NTTデータ先端技術（株）代表取締役社長, 日本セキュリティ監査協会副会長
2015年	CISSP (Certified Information Security Specialist) 取得
2017年	PCI DSS QSA(Qualified Security Assessor)取得
2018年	社長退任、相談役、最高技術顧問
2019年	CISA(Certified Information Systems Auditor)取得、筑波大学客員教授
2020年~	NTTデータ先端技術（株）フェロー

セキュリティへの取り組みの背景

経営者として　自社の情報セキュリティマネジメント

提供するサービス/システムの情報セキュリティマネジメント

情報セキュリティサービス/プロダクト　ビジネス

セキュリティマネジメントはリスクマネジメント

誰が、**何を**、**何から**、**どう**守るか？　文脈/Contextにより多義的

主観的判断　100%は無い　汎用化が難しい　後付けの対策

リスクの優先度　**想定外を少なくする**

リスクマネジメントの要諦：situation awareness/状況認識

現実に起こっていることを認識する

本日のアジェンダ

Ukraineの現状　サイバー攻撃

すでに始まっていたサイバー戦

国家によるサイバー攻撃

何故こうなったのか？

まとめ　どうするか？

Ukraineの現状
サイバー攻撃

何が起こっているか？　激しサイバー攻撃ハイブリッド戦争

2021～　情報操作、影響工作

・**Google TAG**(Threat Analysys Group)はYou Tubeやニュースサイト、Blog、広告等を使った多くの**新ロシア、反ウクライナ、欧米、NATOに対する虚偽情報等の影響力工作**を観測。
・TAGはこれらに対してのコンテンツの削除を実施。

2022.1.14　政府Webサイトへの攻撃

・15のウクライナ**政府機関**（外務省／農業省／教育科学省／安全保障・防衛省／閣僚内閣のオンライン・ポータル）の**Webサイトがハッキングされ情報漏洩、改竄、オフライン(ワイパーウィルス)**に。
・脆弱性のある古いCMSが狙われた。
ベラルーシのグループ？

2022.2.24　破壊活動

・政府機関、重要インフラ（電力、通信等）に対する**ランサムウェアに偽装した新種のワイパーウィル**(WhisperGate/HermeticWiper)による破壊活動が行われた。
・NotPetyaとの類似性も指摘されているが、感染力は強くない。

Time Line

2021.11　機密情報窃取

・ウクライナの**司法機関等へのフィッシング攻撃による侵入**を試み、**機密情報窃取**が行われた。典型的なAPT攻撃。
・背後に、クリミアに展開している**FSBのサイバー攻撃部隊**の可能性を指摘。
by **ウクライナ保安庁**：Security Service of Ukraine (SSU)。

2022.2.15　DDoS攻撃

・ウクライナの**政府及び国営Webサイト**に対する**DDoS攻撃**が行われる。合わせて、**ATMが停止したとの虚偽情報が流される。**
・米英はロシア**GRUの活動**と見ている。

2022.2.24　衛星通信システム破壊

・ウクライナ**政府機関、軍(指揮・命令系統）も利用**している**衛星通信サービスViasat（米国）のモデム**が攻撃され利用不能に。これを利用していた**ドイツの風力タービン5800基なども被害。**
・組み込みシステムで使われている**MIPSのファイルを破壊するワイパーウィルス(ELFファイル)**
”**Acidrain**”が利用されていた。
・IT管理システムへの**サプライチェーン攻撃**の可能性。

何が起こっているか？　無差別なエスカレート

2022.6.21 諜報活動、破壊工作

ウクライナCERT(CERT-UA)が政府機関、メディア、企業、NGO等へ２つの攻撃を確認。

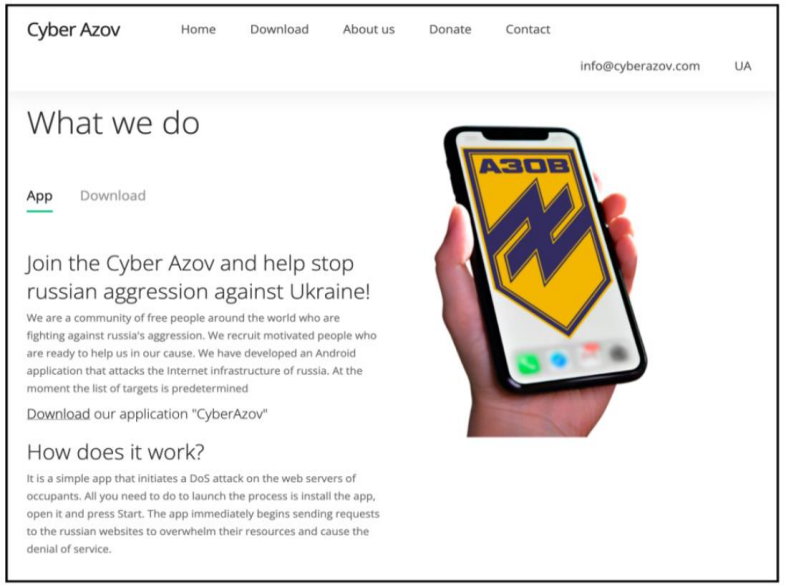
①国税庁が送ったとされる電子メールに添付された徴税文書/ MS Wordファイルに仕込まれたバックドア経由で、**Cobalt Strike Beacon:市販されているペネトレーションテストツール**、がロードされる。
　この攻撃は、ロシア保安省(**FSB**）と関係が疑われている**サイバー犯罪グループTrickBot**が関与。

②ロシアからの核攻撃の脅威を議論する悪意のある文書（MS Word)を配布し、これに**見つかったばかりのマイクロソフトの診断ツール(MSDT)の脆弱性（ゼロデイ）**（CVE-2022-30190）を突いた攻撃が行われた。MS Word経由でMSDTを呼び出すことで遠隔からのコードの実行により、**プログラムのインストール、データの表示、変更、削除、または新しいアカウントの作成を行う**ことができる。**ウクライナのラジオ局／新聞社などの500人以上の受信者がターゲット。**

2022.7.19 諜報活動

Androidアプリによるマルウェア配布Google TAGが報告。

ウクライナのアゾフ連隊を装ったドメインで、「ロシアに対するDOS攻撃を可能」と偽ったAndroidアプリをホスト、配布。正規のGoogle Playではない。**目的は、反ロシア勢力に対するマルウェアの配布。**Googleは、実行は利用されたホスト等からFSBに帰属するグループTulraとしている。



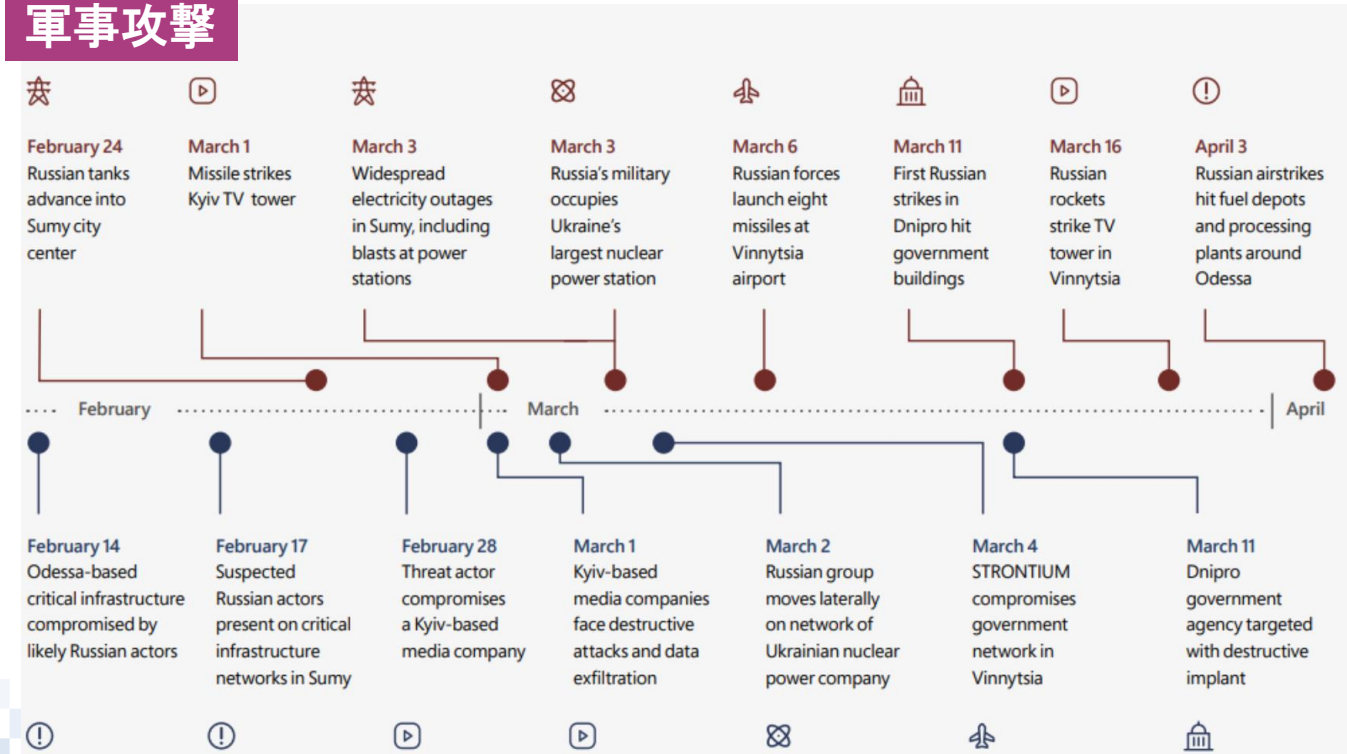
https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag/

何が起こっているか？　ハイブリッド戦争

軍事攻撃とサイバー攻撃の連携

Special Report: Ukraine : An overview of Russia's cyberattack activity in Ukraine
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd 2022.4.27

軍事攻撃



サイバー攻撃

4カ月で796件

State Service of Special Communications and Information Protection of Ukraine

796 cyberattacks in the first four months of the war

https://cip.gov.ua/ua/news/chotiri-misyaci-viini-statistika-kiberatak

Key cyber attacktechniques

Information gathering	242
Malicious code	192
Intrusion	92
Intrusion attempts	82
Avialability	56
Other	132

すでに始まっていた
サイバー戦

すでに始まっていたサイバー戦

2004年大統領選挙
ヤヌコビッチ　vs ユシチェンコ
不正選挙糾弾により**オレンジ革命**

2010年
ヤヌコビッチ復活

2013年11月
ヤヌコビッチがEU連合協定の調印手続きの凍結

ユーロ・マイダン革命勃発

2014年2月末～4月
ロシアがクリミア半島続いてドンバス占拠

2014年2月21日
ヤヌコビッチ逃亡

2014年6月
大統領選挙
ポロシェンコ大統領誕生

2019年２月
憲法にNATO加盟明記

2019年5月
大統領選挙
ゼレンスキー大統領誕生

Time Line

ユシチェンコがダイオキシンを盛られる、**選挙本部爆破未遂**（ロシア人による）などの激しい選挙妨害が行われる

・親欧米派政府関係者に、**謎の発信元からの電話やSMSメッセージが殺到**。
・**IMSIキャッチャー***が**携帯基地局になりすまし**、デモ参加者に帰宅を促すテキストメッセージを発信

・親ロシア派のハッカー集団が**サイバーベルクト**がWebサイトへDoS攻撃、改竄等の選挙妨害。
・**中央選挙委員会**のネットワークに侵入し、数十台のコンピュータを消去し**選挙結果の表示を妨害**。同委員会の**ウェブサーバーに偽の結果を示す画像**を仕込んでいた。

＊スティングレー(Stingray)
https://gigazine.net/news/20140606-stingray-cell-phone-tracker/

深刻なサイバー攻撃

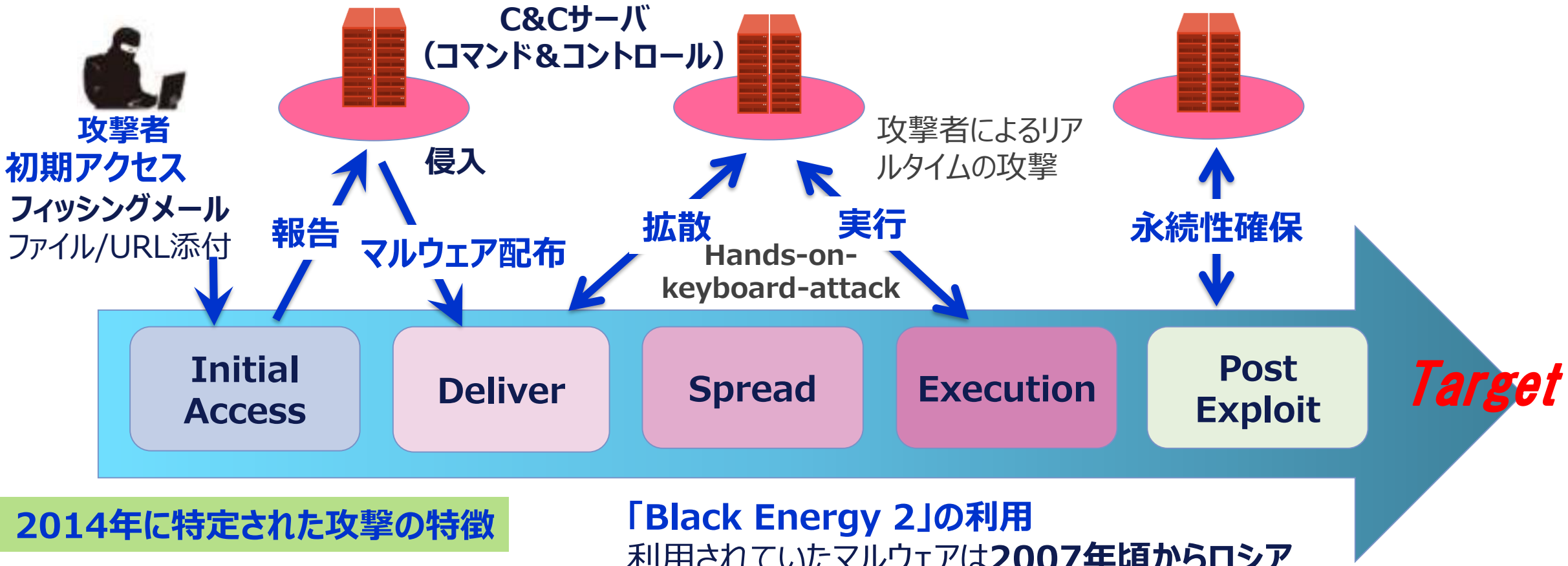
2014年９月iSIght社がロシア由来のハッカーグループ**Sand worm**の機密情報窃取活動を公開

2015年～2016年　政府機関、メディア、鉄道、空港**電力網**に対するサイバー攻撃

2017年 ランサムウェア**Notpetya**による世界規模の攻撃

Sand warmの攻撃プロセス　APT*攻撃のKill Chain

＊Advanced Persistent Attack



2014年に特定された攻撃の特徴

初期アクセス

マイクロソフトPower Pointの**ゼロデイ脆弱性**CVE 2014-4114を利用した侵入

「Black Energy 2」の利用

利用されていたマルウェアは**2007年頃からロシア由来で利用されていたBlack Energyの変異。元々はDOS攻撃用のBot向け**であったが、スクリーンショット、キーロガー、ファイル・暗号キーの抽出等の機能が付加された**Root Kit化。**

NTT DATA
NTTデータ 先端技術株式会社

Russian Cyber Espionage Campaign - Sandworm Team 2014

Russian Cyber Espionage Campaign - Sandworm Team, 2014.10.14
https://www.washingtonpost.com/r/2010-2019/WashingtonPost/2014/10/14/National-Security/Graphics/briefing2.pdf

重要インフラへの攻撃　”サイバー攻撃の演習場”

2015年10月　メディア、鉄道、空港等への攻撃

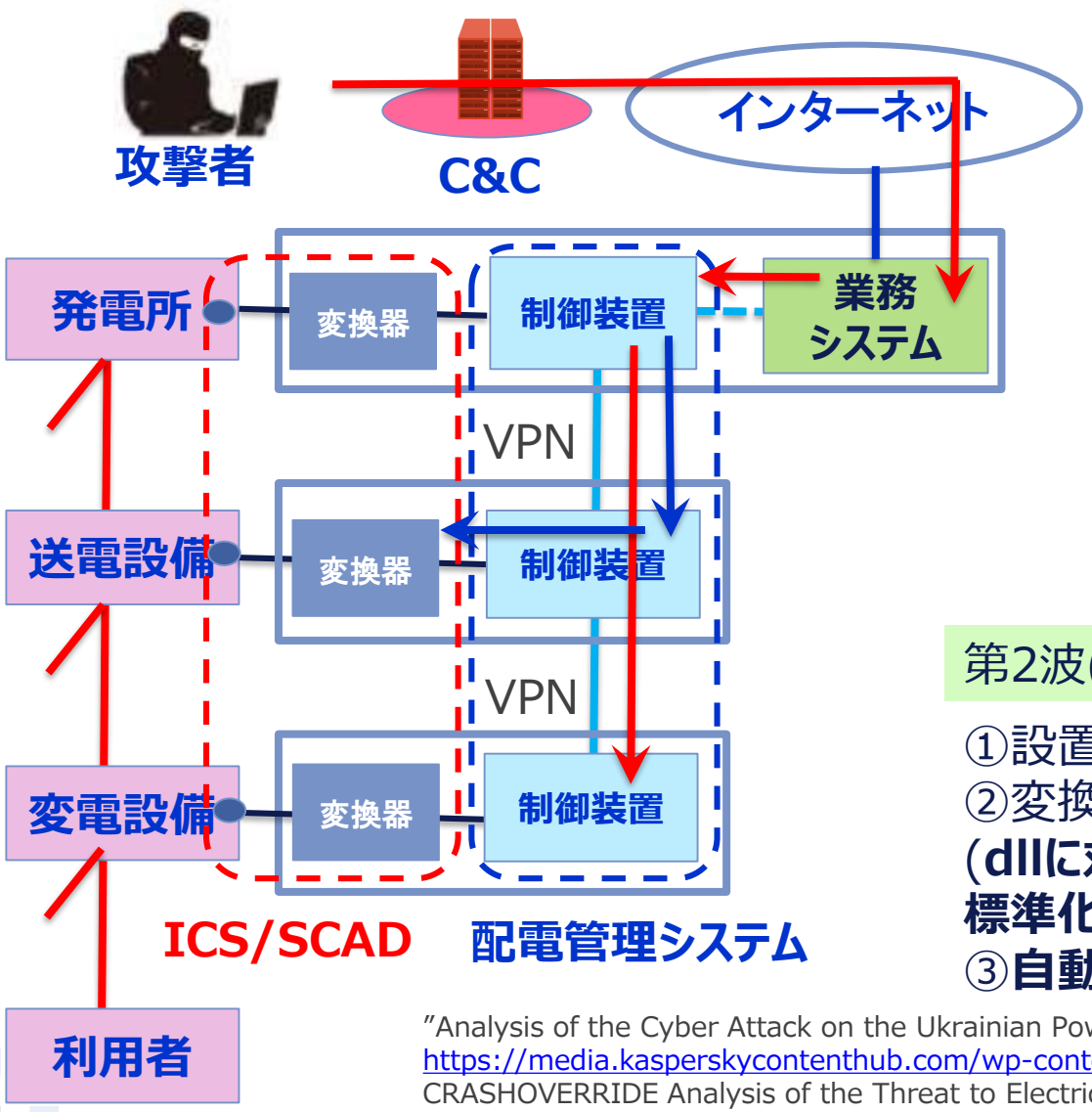
・**ターゲット**：**テレビ局**StarLightMedia社、TRK社
鉄道会社Ukrzaliznytsia社、キエフのボリスピル**空港**
・**Deliver**; **Black Energyの亜種**。アンチウィルスの回避。MS Defenderの成りすまし。KillDisk追加。
・**Spread**: **ADに侵入**し、これ経由で**多数のPCにマルウェア感染**。BlackEnergyの潜伏も図る。
・**Execution**: **KillDisk（ワイパー）**によりAD等の**マスターブートレコードを破壊**。

2015年12月　電力網への攻撃

・**ターゲット**：**３つの異なる地域の電力会社**
・**Initial Access**:ウクライナ議会からのメッセージを装ったメールに**Wordの悪意あるマクロの書かれたファイルが添付**。
・**Deliver**; **Black Energyの亜種**。VPNの侵害、KillDisk拡散機能。
・**Execution**: ターゲットに応じて異なる実行

キエフブレネルゴ社：**偽造された制御ソフトウェアを用いて遠隔操作**。ブレーカ制御用のハードウェアをハッキング、停止させ正規のオペレーターによるブレーカーのデジタル制御を遮断。KillDiskを実行し、同社のPCを破壊。制御装置のバックアップ用電源の制御も遮断。
プリカルパッチャオブレーネルゴ社：電力制御システムを乗っ取り、**オペレータの制御権を奪って、ブレーカを操作し停電を実行（動画が記録されている）**。バックアップ電源ファームを破壊。

電力網　ICS/SCADAへの攻撃　第1波(2015.12)から第2波(2016.12)へ



第1波(2015.12) → **変電設備破壊**

Stage 1
①フィッシングメールによる侵入
②マルウェア**Black Energy 3**ダウンロード
③配電管理システム偵察

⇒**攻撃支援/拡散活動**
・Kill Diskによる破壊
・UPSシステム停止
・侵入痕跡消去
・コールセンタへの攻撃

Stage 2
①制御装置への侵入、改竄
②変換器制御用のマルウェア開発設置
③制御装置を乗っ取り（手動）ブレーカ開放

第2波(2016.12) → **送電設備破壊**

①設置済のバックドアで侵入
②変換器を異常動作させるマルウェア設置
(dllに対するマルウェア；Industroyer)
標準化された4種類のSCADAプロトコルに対応
③**自動的**にブレーカ開放

⇒**武器化**
マルウェアの開発にあたっては**同じ装置の開発環境が用意**されていた？

”Analysis of the Cyber Attack on the Ukrainian Power Grid”. E-ISAC, 2016.3.18
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf
CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations, Dragos, 2016.

NotPetya(ワイパーワーム）の拡散　2017.6.27~

5月頃~
Linkos Group のM.E.Docの開発環境、ソフトウェア更新サーバが侵害。
NotPetya攻撃の6週間前ごろから更新ファイルに仕込まれていた。
⇒ソフトウェアサプライチェーン攻撃

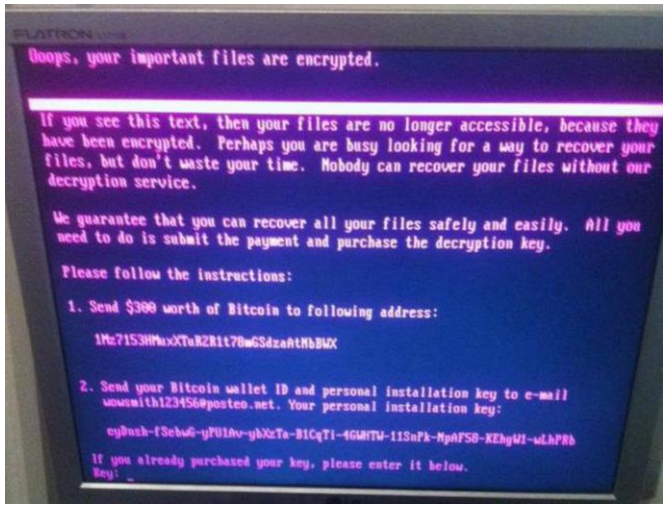
6.27~　**大規模かつ急速な拡散開始**
被害は世界規模（ロシアを含む）で拡散したが**80%はウクライナ**（国立銀行、政府機関、原子力発電所等80社以上。**過去最大の被害（100億ドル以上 by ホワイトハウス）**。

7.4　**ウクライナ警察サイバー犯罪ユニット**がウクライナLinkos Groupの**税務会計処理ソフトM.E.Docを開発しているサーバを押収。**

2017　Time Line

杜撰な開発環境。アカウント侵害等が判明。

様々な調査の結果（主に開発環境への侵入痕跡）**ロシアSand Wormに繋がる痕跡が発見**された。



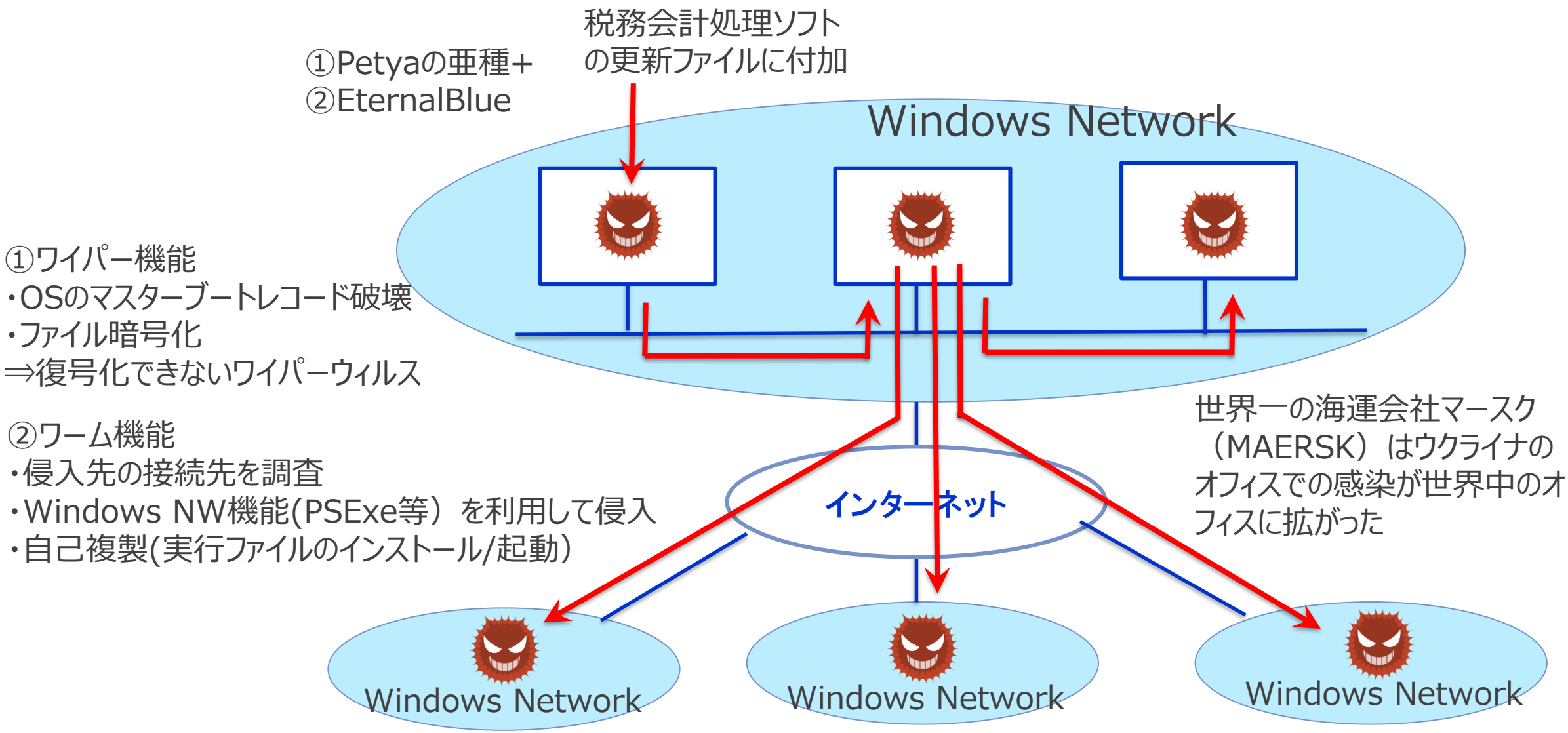
NotPetyaの身代金要求画面
ランサムウェアを装ってウいるが復号化できない
(Wiki より)

201.3頃より拡散していたランサムウェPetyaと類似。しかし、**強力な感染機能(EternalBlue)**を備えていた。

EternalBlueは、2017.5.12から世界規模で拡散した**Wannacryにも使われていた。**

元々は米国NSAが開発したと言われており、2017.4.14に**ハッカー集団ShadowBroker によりリーク**。内部漏洩と言われている。

NotPetya　拡散プロセスのイメージ



ロシアの国家によるサイバー攻撃組織

CISA, “Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure”, 2022.4.20を参考に整理　https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

組織名	ミッション	サイバー関連組織と要員	主な活動
 **連邦保安庁 (FSB)**	**国内防諜、テロ等の犯罪対策**（CIS諸国の諜報活動も実施）	・センター16、ユニット71330等 組織の性格上、**サイバー犯罪者**を取り締まりつつ、組織に**取り込んでいる**模様。	Dragonfly, Berserk Bear etc. ・欧州、米国の石油・ガス会社、原子力発電所を含むエネルギー部門への侵入諜報活動・電力網ICS/SCADAを標的とした攻撃（2012~2017）
 **対外情報庁 (SVR)**	CIS加盟国以外の**海外諜報活動**	詳細は不明だが2008年以降活動が確認されている。**高度な技術力を持ち、主に長期に潜伏可能な活動が主体。**	**APT29**,Noberium, Tulra etc. ・2008より欧州、NATO、米国に対する諜報活動。2015米国民主党本部侵入。 ・SolarWinds Orionサプライチェーン攻撃(2020.12)
 **連邦軍参謀本部情報総局 (GRU)**	**軍関連の情報収集、スパイ活動、SIGINT、偵察衛星や特殊部隊**（スペツナズ）**の運用など**	**・独自の専門要員と研究組織。** **・Unit25165**/GTsSS：情報操作活動と関連する諜報活動 **・Unit74455**/GTsTS：ワイパーウィルスを利用した破壊活動 **・化学力学中央科学研究所**(TsNIIKhM)；ICS等の技術提供	**APT28**, Sand worm, Fancy Bear etc. ・ウクライナ/東欧諸国へのサイバー攻撃(2004~) ・米国大統領選挙サイバー攻撃(2016) ・フランス大統領選挙介入工作(2017) ・ドーピング組織、平昌オリンピックへの妨害工作(2017~) 他多数

欧米のロシアサイバー攻撃への対応状況　国家レベルの例

米国

2022.2 **CISA（サイバーセキュリティ・社会基盤安全保障庁）**がウクライナと関連する米国本土へのサイバー攻撃の情報共有のためのサイト「**Shield Up**」を立ち上げ。
2022.3.24 司法省が2021.6に起訴した**GRUに帰属するハッカー6名**、2021.8に起訴した**FSBに帰属するハッカー3名**の起訴状を公開。

2022.4.20　CISA、FBI、NSA、および国際的なパートナーが、ロシア国家が支援するサイバー犯罪アクターの実証された脅威と能力に関する勧告を発行
また、**5eyes**による**ロシアの国家支援型サイバー攻撃関連組織の情報を公開**

2022.4.26 米国司法省　**ロシアGRUに帰属する6名のハッカー**（訴訟済）に関する情報提供プログラムの**報奨金を最大1千万＄**と発表(Dark Webで公開）。

欧州

2022.1.17　NATOがウクライナに対する**サイバーセキュリティ対策支援の強化に関する覚書**を締結。この協定は2015年から続いている。**NATOのサイバー防衛に関するプラットフォームへのウクライナのアクセスを許可**。

2022.7.6 NATOがウクライナのサイバー防衛に対する支援強化を発表。具体的には、**CCD-COE**等NATOサイバー関連組織との連携強化、**サイバー防衛基金の設立**など。

欧米のロシアサイバー攻撃への対応状況　民間企業の例

マイクロソフト

2022.2.4 Microsoft Threat Intelligence Center (MSTIC)によりロシア由来の脅威グループがウクライナの組織を標的にしているとして、その詳細を公表。

2022.2.28 ブラッドスミスによるウクライナ侵攻に対する声明「デジタル技術とウクライナ戦争」で、**民間企業の立場で**政府関係者と協議しつつ**ウクライナに対する支援を表明**。

2022.4.7 ウクライナに対するサイバー攻撃で利用しれていた**APT28**に帰属する7つの**ドメインをTake Down**。

2022.6.22 Defending Ukraine: **Early Lessons from the Cyber War**を公開

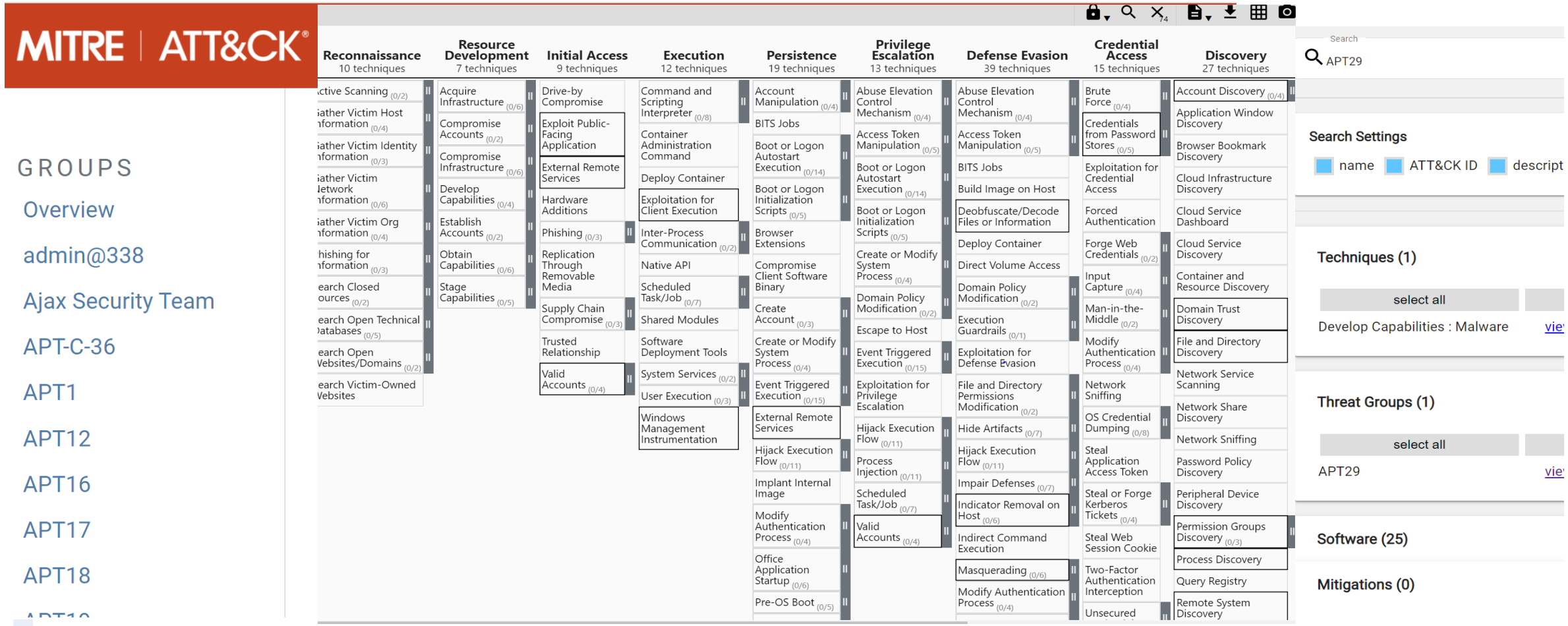
Google

Google **TAG**(Threat Analysis Group)による継続的な**サイバー攻撃監視、帰属調査**と公表。
YouTube、Web広告等を通じた**情報操作の監視とTake Down**

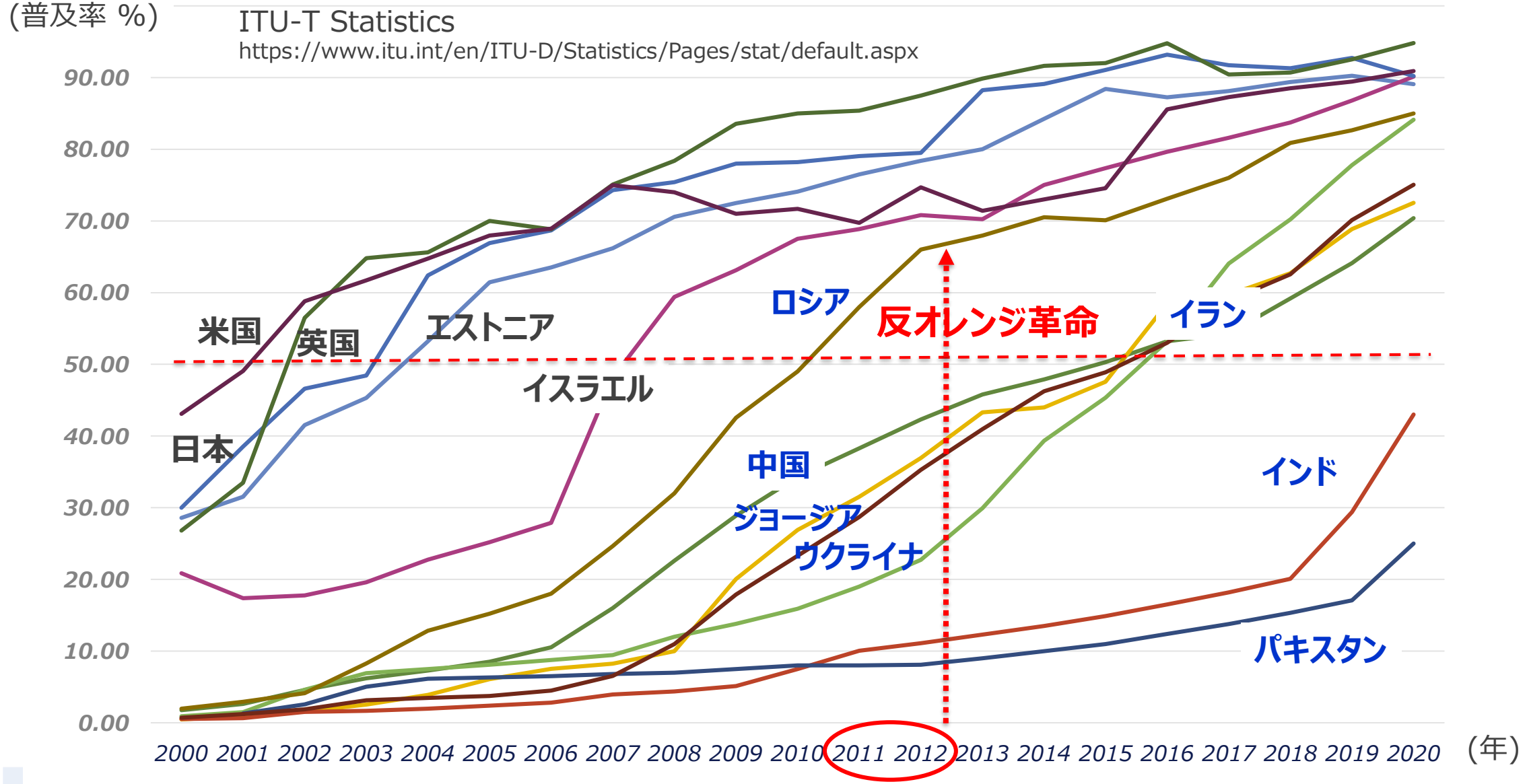
DDoS攻撃の不正なトラフィックを吸収し、Webサイトの「シールド」として機能するサービス**Project Shield**の提供により、ウクライナ政府のWebサイト、世界中の大使館、および紛争に近接する他の政府のサイトに適用し、**DoS攻撃を防御**。

MITER ATT&CKの整備　サイバー攻撃に対応した官民連携の基盤

APT攻撃を実行するグループにはその**グループ固有のKill Chain**が使われることに着目。検出されたサイバー攻撃のKill Chainを**グループごとにデータベース化**。これに基づいて、新たな**攻撃の手法、帰属の判定、対策手段を官民/連携国間で共有。** https://attack.mitre.org/



ロシア国内の状況　インターネットの普及と監視、統制の強化



ロシア国内の状況　インターネットの監視、統制 2010年頃まで

OpenNet Initiativeによる調査

Filteringの対象による分類

Political

主に現政権の見解に反対する見解を表明するWeb サイトに対するもの

Social

セクシュアリティ、ギャンブル、違法薬物やアルコールに関連する資料、および社会的に敏感な、または不快に感じる可能性のあるその他のトピック

Conflict and Security

武力紛争、国境紛争、分離主義運動、過激派グループに関連するコンテンツ

Internet tools

電子メール、インターネット ホスティング、検索、翻訳、VoIP等

＊OpenNet Initiative https://opennet.net/
Citizen Lab, Harvard University, SecDev Groupによる共同プロジェクト。2014年に終了。

Russia 2010　弱 ← Filtering → 強

RESULTS AT A GLANCE

Filtering	No Evidence of Filtering	Suspected Filtering	Selective Filtering	Substantial Filtering	Pervasive Filtering
Political			•		
Social			•		
Conflict and security	•				
Internet tools	•				

China 2012

RESULTS AT A GLANCE

Filtering	No Evidence of Filtering	Suspected Filtering	Selective Filtering	Substantial Filtering	Pervasive Filtering
Political					•
Social				•	
Conflict and security					•
Internet tools				•	

Ukraine 2010

RESULTS AT A GLANCE

Filtering	No Evidence of Filtering	Suspected Filtering	Selective Filtering	Substantial Filtering	Pervasive Filtering
Political	•				
Social	•				
Conflict and security	•				
Internet tools	•				

ロシア国内の状況　インターネットの情報監視・統制の強化

2012.11/2013改正
インターネットブラックリスト法
法執行機関により**反政府活動もブロック可能**に。

2016
ロシア連邦デジタル開発・通信・情報技術・マスコミ監督庁(RKN)がISPに対して**ブロッキング装置RAS**[1]**の設置を義務化。**

ブロッキング

2017
RKNの「禁止サイト」に「LINE」や「ブラックベリー・メッセンジャー」など４つが登録
⇒ヤロバァヤ法違反

2019.11　**「ネット主権法」**
外国からの脅威に対抗して、**必要に応じインターネットをRKNが集中管理**、海外接続を遮断可能とする。ロシア国内のISPは全てのトラヒックを再ルーチングする必要がある.

2019.12
ロシア国内のネットワークを世界のインターネットから遮断して隔離する実験に成功。
⇒BGPの操作による政府が管理するIXへのルーチング、独自のDNSなど。

インターネットの分断/Splinternet

Time Line

2016「**ヤロバァヤ法**」
通信事業者(ISPも含む)に対して**通信内容の6カ月間、メタデータを3年間国内で保持を義務化。**
⇒ロシア情報機関はこれを**令状なしで閲覧可能**

検閲

ISPに**監視装置SORM**[2]**の設置が義務付け**られ、これに**FSBが直接アクセス可能。**
SORMはFSBの認証を受ける。

違法行為を法執行機関に報告しなかったことに対する刑事責任。

2022.3
ロシア**政府による「信頼できるルートCA」の利用**と**政府が承認したWebブラウザ**をダウンロードするか、ブラウザの基本設定を変更することを要求。
司法機関に対する**暗号通信のバックドア**も要求。
⇒経済制裁の影響で海外のCAが利用困難になったため

1)Reviser Automatic System
2)System for Operative Investigative Activities

国家によるサイバー攻撃

国家によるサイバー攻撃の多様化

	～2009	2010～2015	2016～
・Hack Back ・抑止攻撃		★□ ★□ ★中国	★□ ★イラン
・情報操作 (Information operations) ・不正な情報開示 (Forced transparency)		★ウ ★米 ★英 ★米 ★米	ロシア ★米 ★仏
・ランサムウェア ・金融取引ネットワーク/ 仮想通貨への攻撃		北朝鮮	★ ★ウ ★ ★ ★
・破壊活動 (Sabotage)	★イラン	★ウクライナ★ウ ★米	★イラン
・インターネット接続妨害 ・妨害活動 (Vandalism)	★エストニア★ ★ジョージア	★サ ★韓 ★ウ	★印 ★米
・機密情報窃取 ・諜報活動(Espionage)	★米 ★米 ★米 ★米 ★	★米 ★中★米 ★米 ★米 ★米 ★米	★米 中国 ★米 ★米 ★米

攻撃側：

★中国

★ロシア

★北朝鮮

★イラン

★アメリカ

★パキスタン、他

国家によるサイバー攻撃の動向　攻撃を受けた国

CSIS(戦略国際問題研究所）により2006年以降、国家若しくは重大なサイバー犯罪（100万＄以上）を公開情報に基づいて集計　最新版　2022.7.5公開

（注）あくまで報道ベースでの集計であり正確な帰属は曖昧

https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

順位	国名	件数	順位	国名	件数
1	**米国**	**198**	11	サウジアラビア	16
2	英国	58	13	フランス	15
3	インド	32	13	カナダ	15
4	ドイツ	25	15	ロシア	13
5	**ウクライナ**	24	15	パキスタン	13
6	イスラエル	23	17	ベトナム	8
6	イラン	23	17	トルコ	8
8	オーストラリア	22	19	香港	7
8	韓国	22	20	アラブ首長国連邦	6
10	中国	19	20	北朝鮮	6
11	**日本**	**16**			

NordVPN　https://nordvpn.com/ja/blog/cyber-attack-incidents/

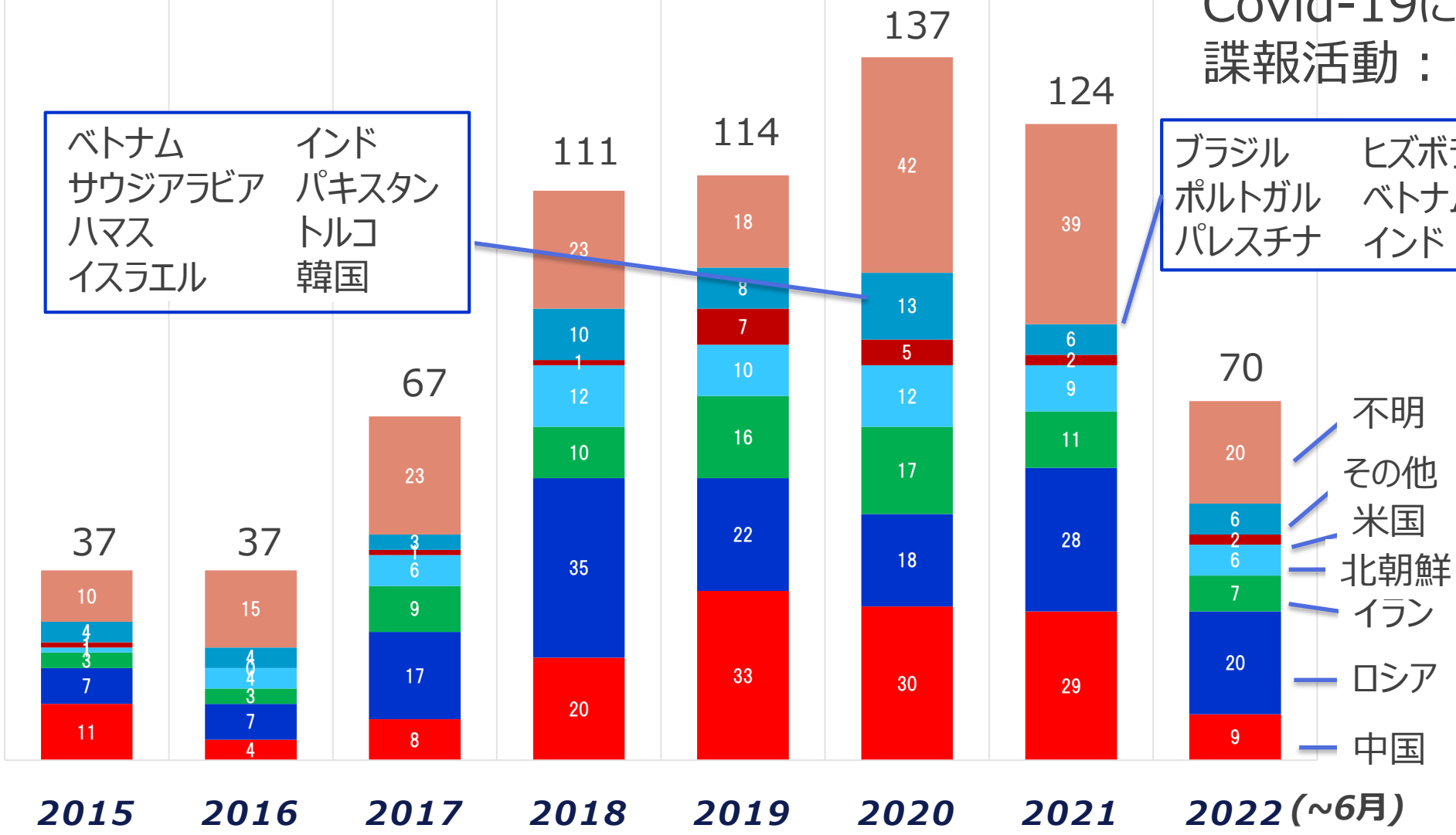
国家によるサイバー攻撃　どこが行っているか？

CSISの資料に基づいて集計（あくまで情報が公開されたもの）

Covid-19に関連する
諜報活動：17件

ベトナム　インド
サウジアラビア　パキスタン
ハマス　トルコ
イスラエル　韓国

ブラジル　ヒズボラ
ポルトガル　ベトナム
パレスチナ　インド



NTT DATA
NTTデータ 先端技術株式会社

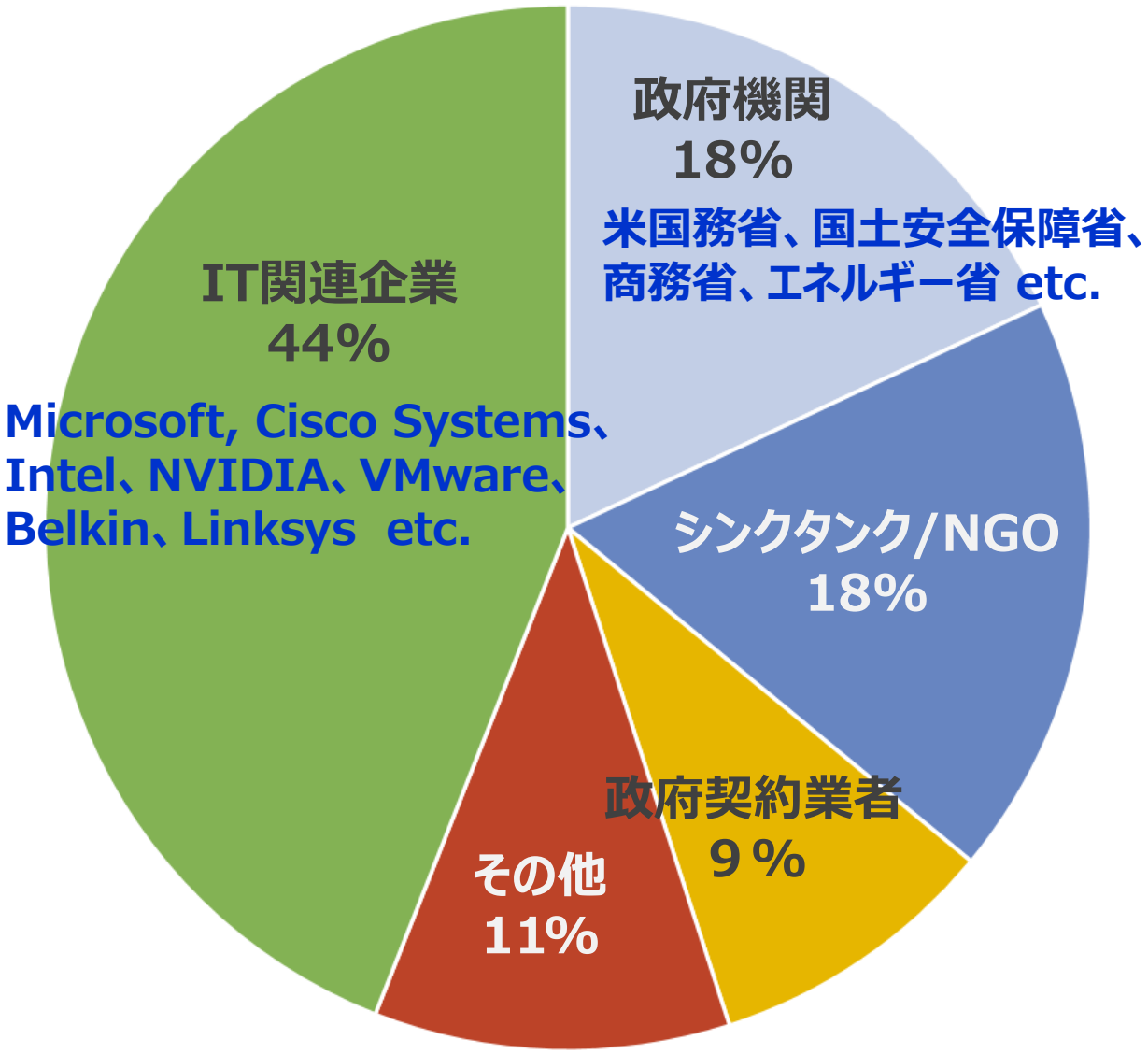
IT管理システムSolerWinds社Orioによる深刻なサプライチェーン攻撃の発生

■2020.12.13 米国セキュリティ会社 **FireEyeが公表**。同時に米国政府が**国家安全保障会議を招集**し緊急対策を行う。

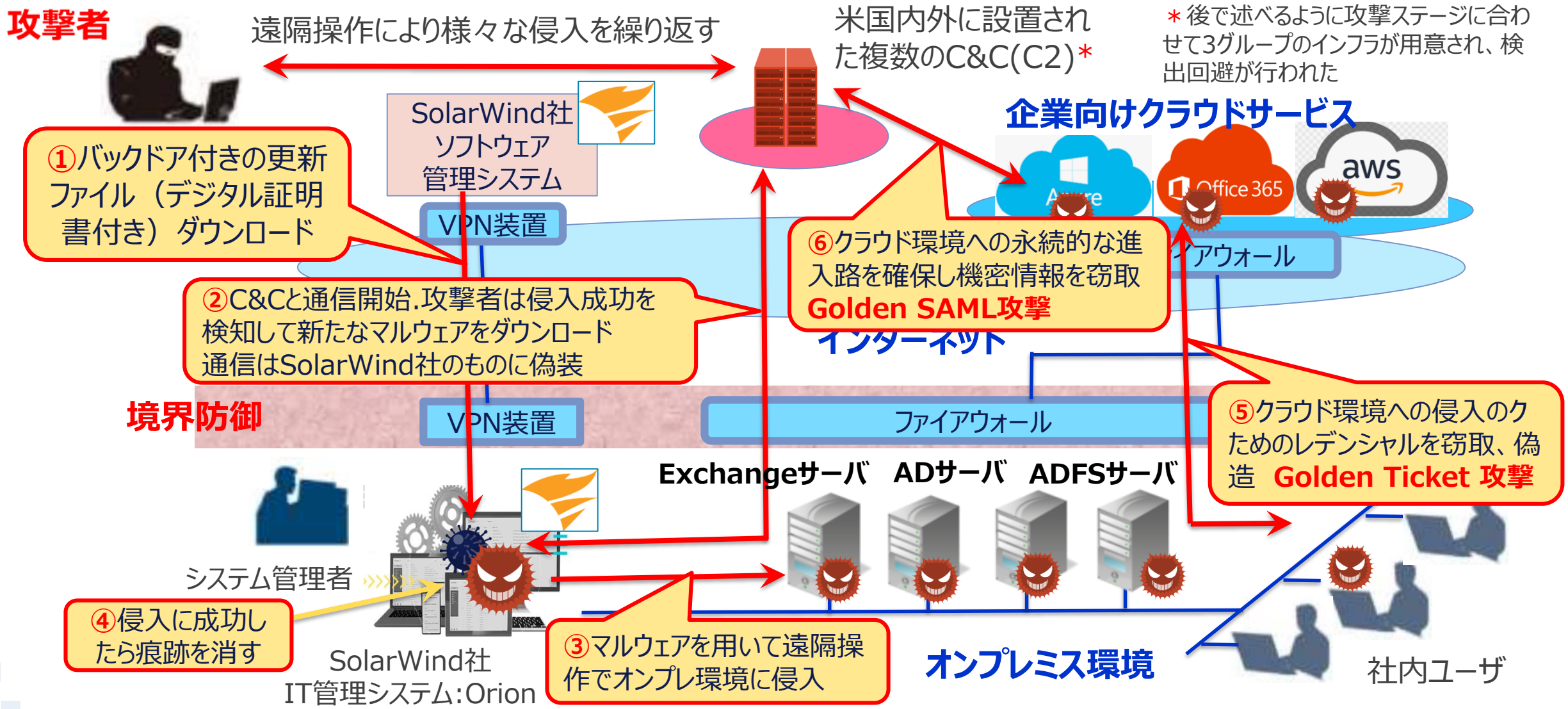
■顧客約18000社にマルウェアが配信され、200社近くにセキュリティ侵害（右図）が行われた模様。(2020.12.18 マイクロソフト発表:右図）⇒**最終的には16000社にマルウェア配布、100社程度の侵害(2021.4)**

■2021.4 米国政府は、**ロシアSVRにより実行**されたものと断定。

■**2021.5.15 米国大統領令E.O.14028**が発出され、**米国政府機関を中心にサイバーセキュリティ対策の全面的な見直しと強化が指示**され、**Zero Trust**の導入、**ソフトウェアサプライチェーンのセキュリティ対策**等が現在進行中

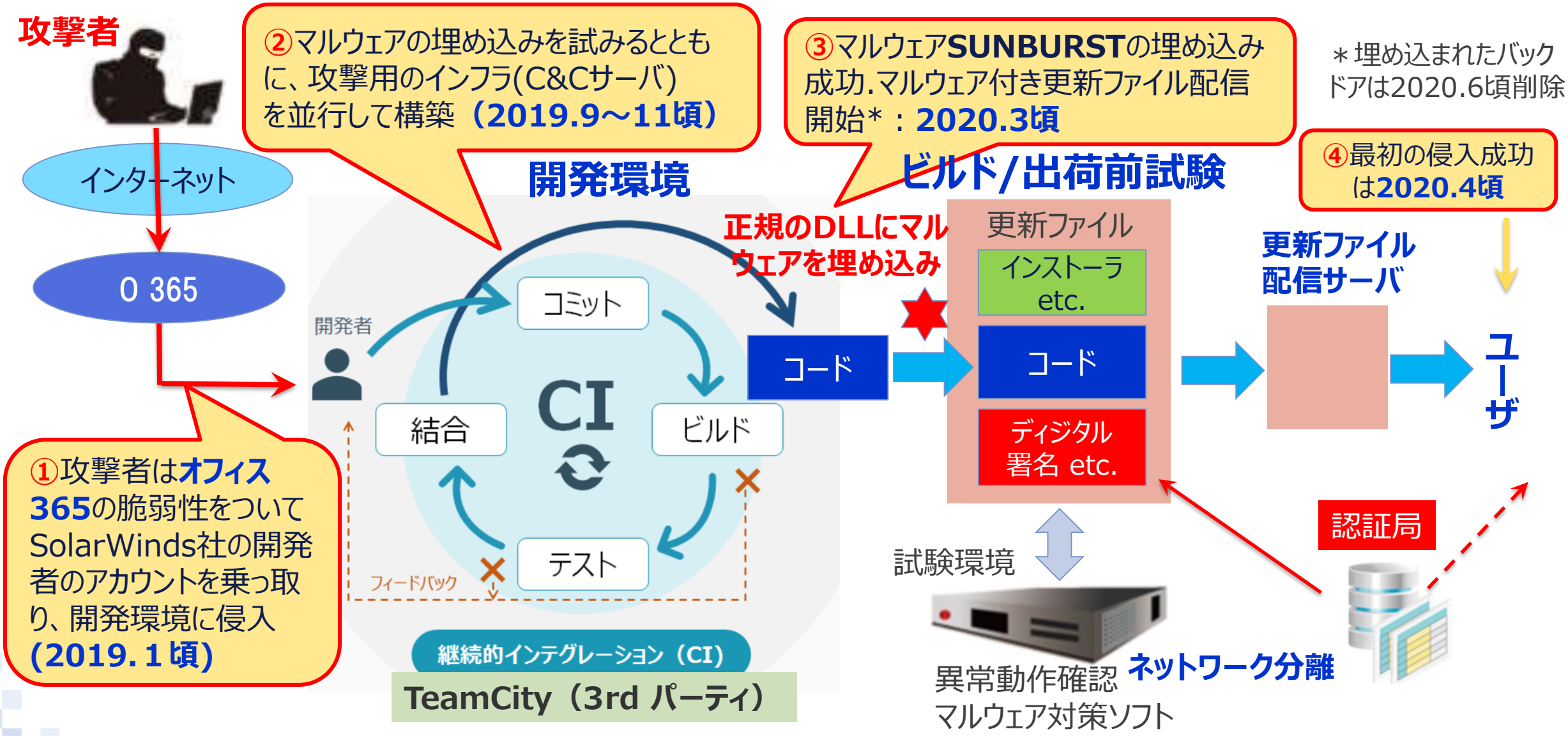


何が行われたか？　極めて巧妙なソフトウェアサプライチェーン攻撃



マイクロソフト社：https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/　等を参考に作成。

SolarWinds社はどう侵害されたか？



何故こうなったのか？

デジタル技術の本質的な脆弱性　マクロな視点

■技術とサービスのグローバル化、コモディティ化

⇒　新技術とサービスの普及促進　vs. リスクインパクトの増大

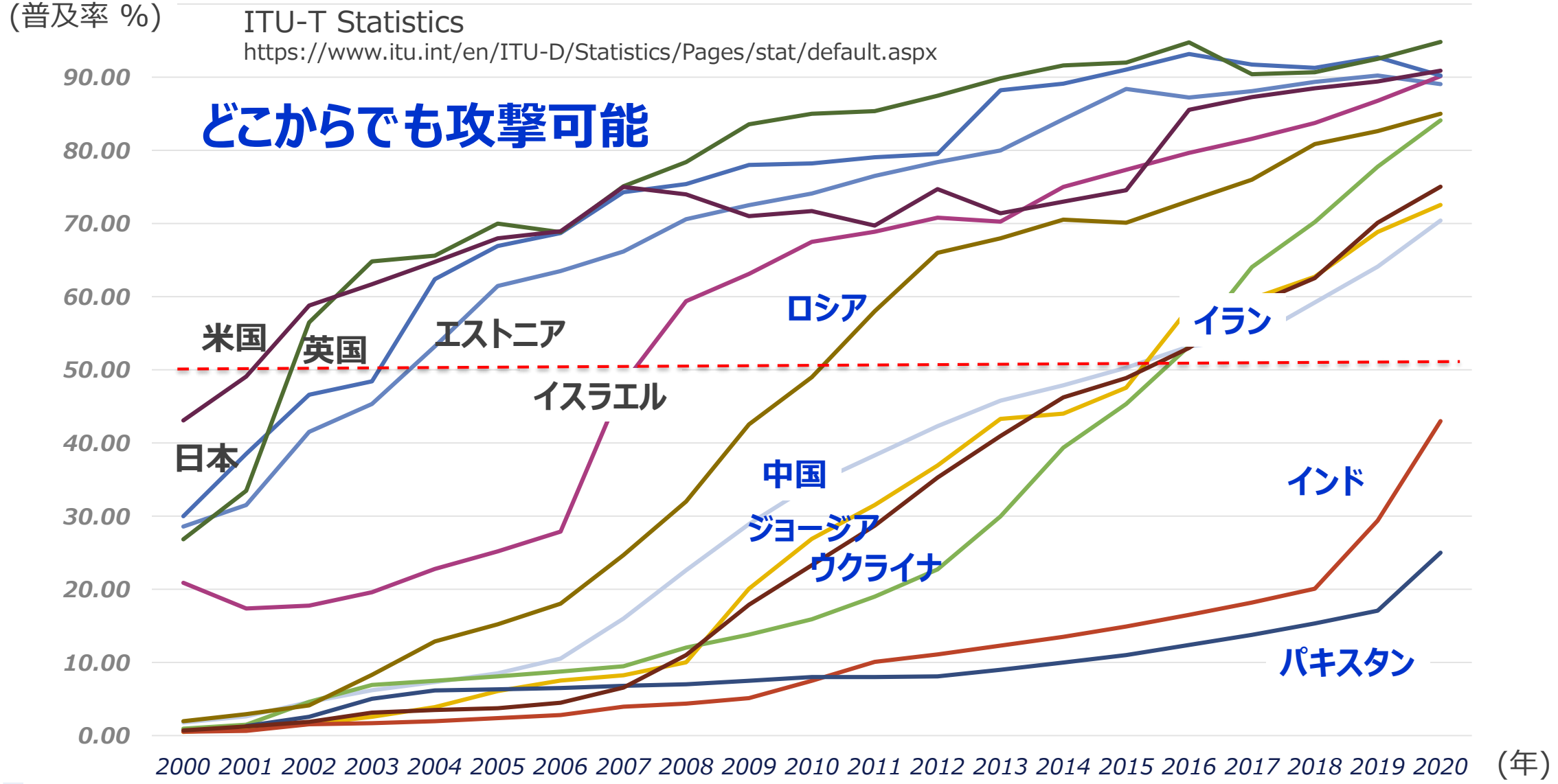
■システムの相互依存、サプライチェーンの複雑化

⇒　新技術とサービスの開発/利用促進　vs. Attack Surfaceの拡大

■技術、サービス、知識拡大の高速化

⇒　新技術とサービスの普及　vs. 未成熟な利用のリスク

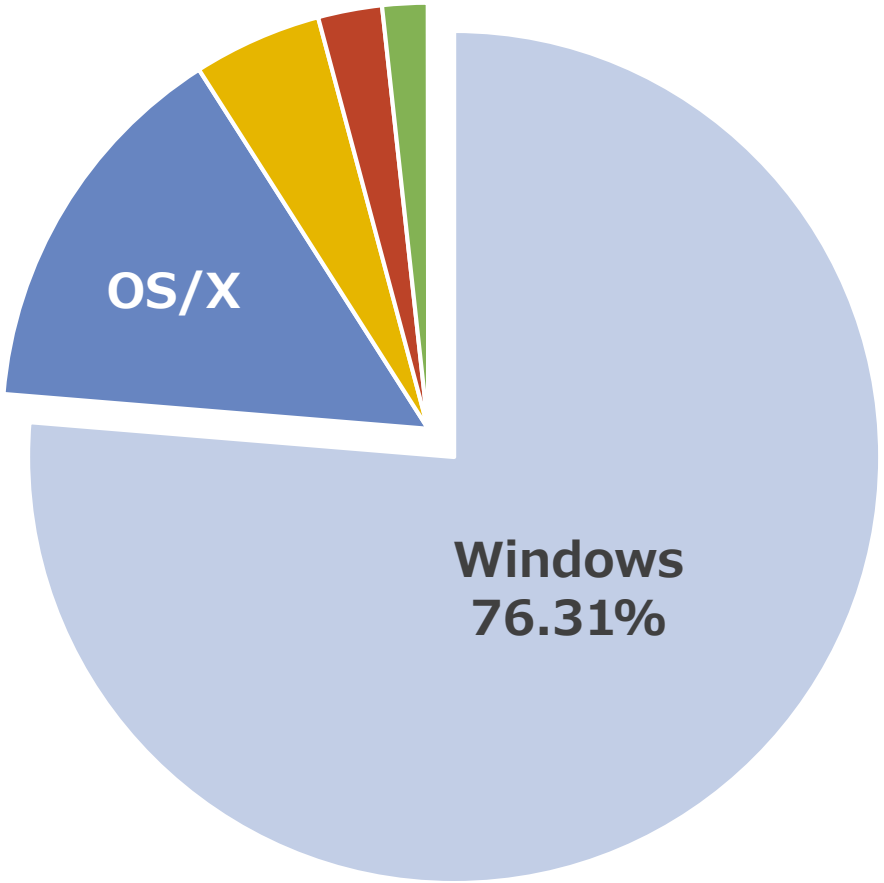
インターネットの普及



もう１つのグローバル化　Windowsの寡占

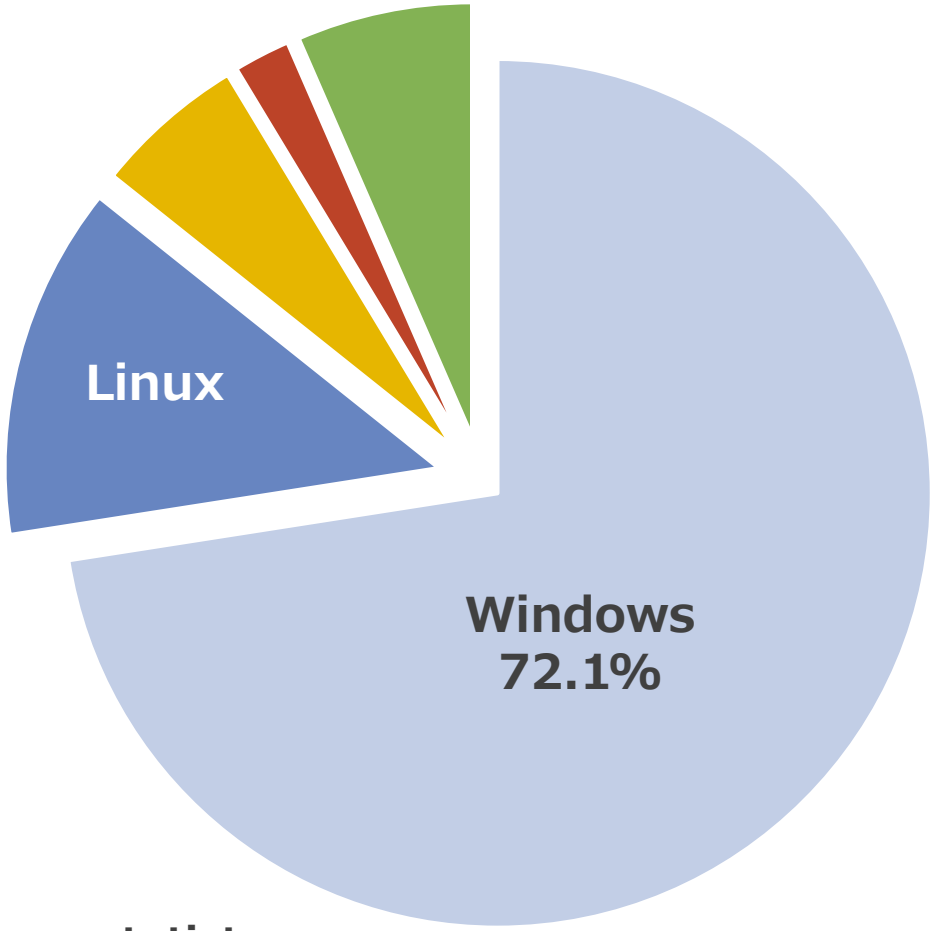
Windowsもインターネットアーキテクチャを採用

Disk top OSのシェア



statcounter
https://gs.statcounter.com/os-market-share/desktop/worldwide/

Server OSのシェア



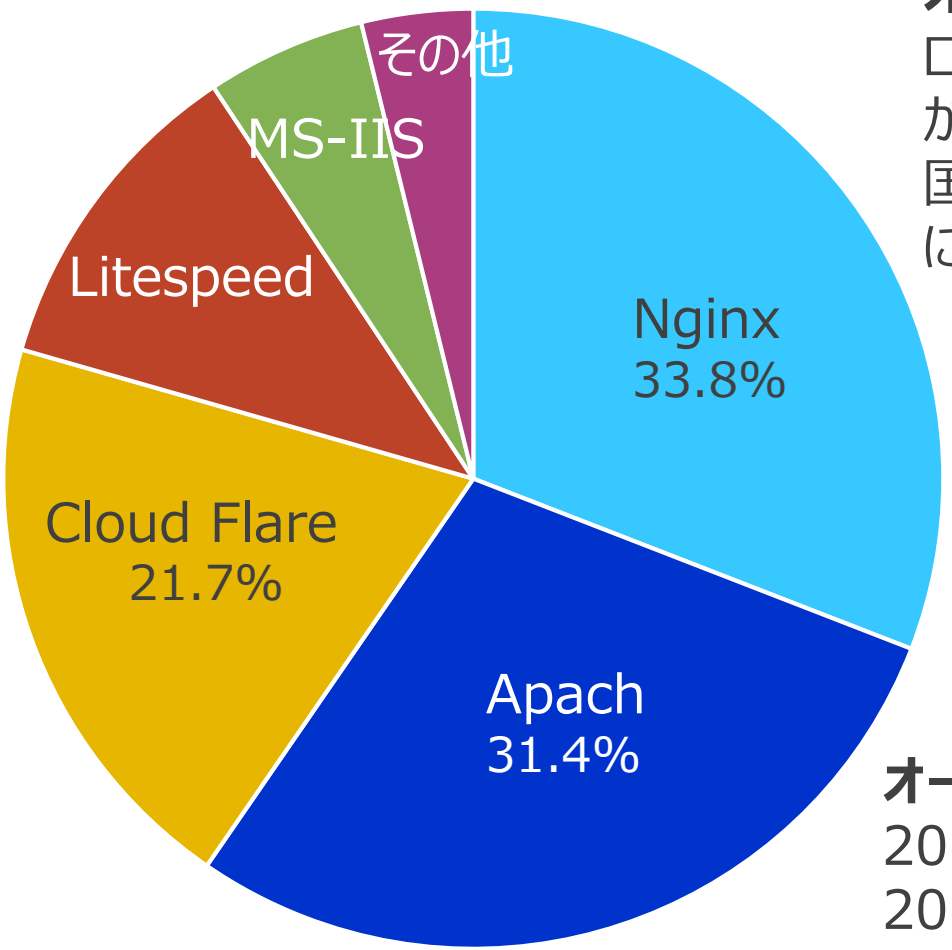
statista
https://www.statista.com/statistics/915085/global-server-share-by-os/

Webサーバの状況

登録ホスト名
11.47億

アクティブなWebサーバ
1.98億

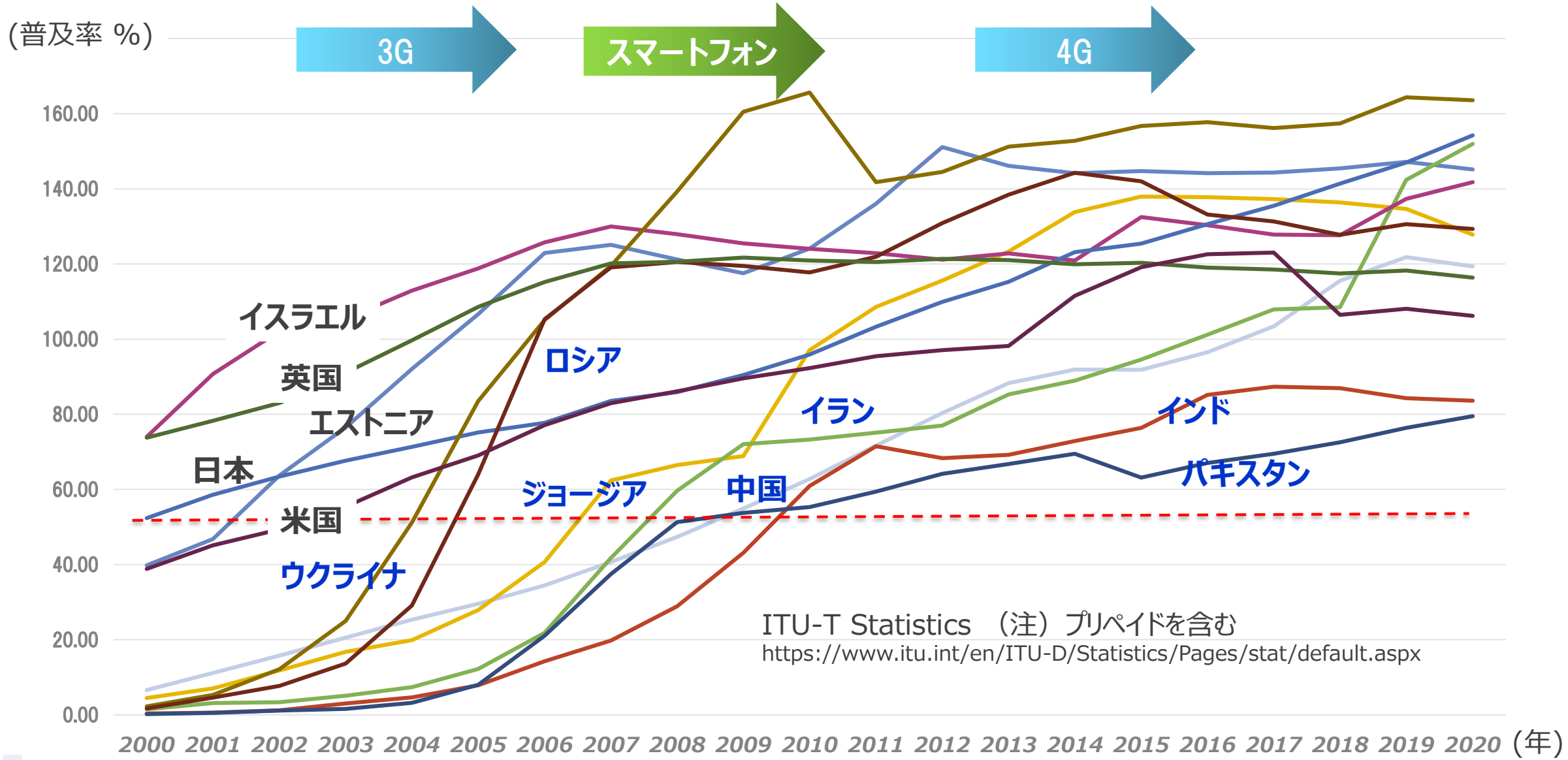
Netcraft 2022.6
https://news.netcraft.com/archives/2022/06/30/june-2022-web-server-survey.html



オープンソース
ロシア出身イーゴリ・ソシエフ氏が開発、2004年リリース。米国に本社があったが、2019年にF5ネットワークスが買収。

オープンソース 深刻な脆弱性
2021 Log4j
2018 Struts 2

モバイル通信の普及



ITU-T Statistics （注）プリペイドを含む
https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

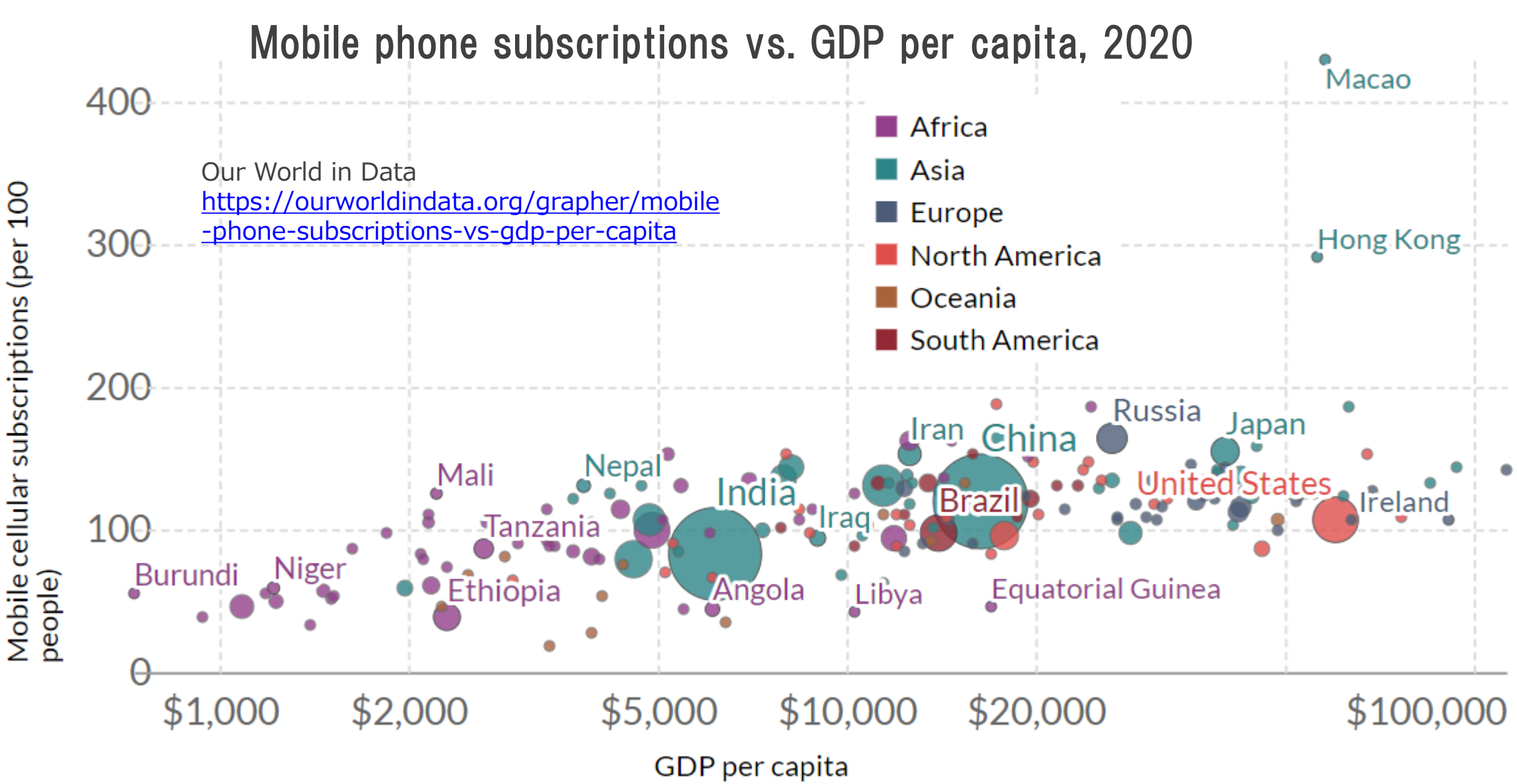
移動体通信サービスのインパクト

How Apple Has Changed The World In Just 7 Years
https://www.cultofmac.com/219813/how-apple-has-changed-the-world-in-just-7-years-picture-1000-words/

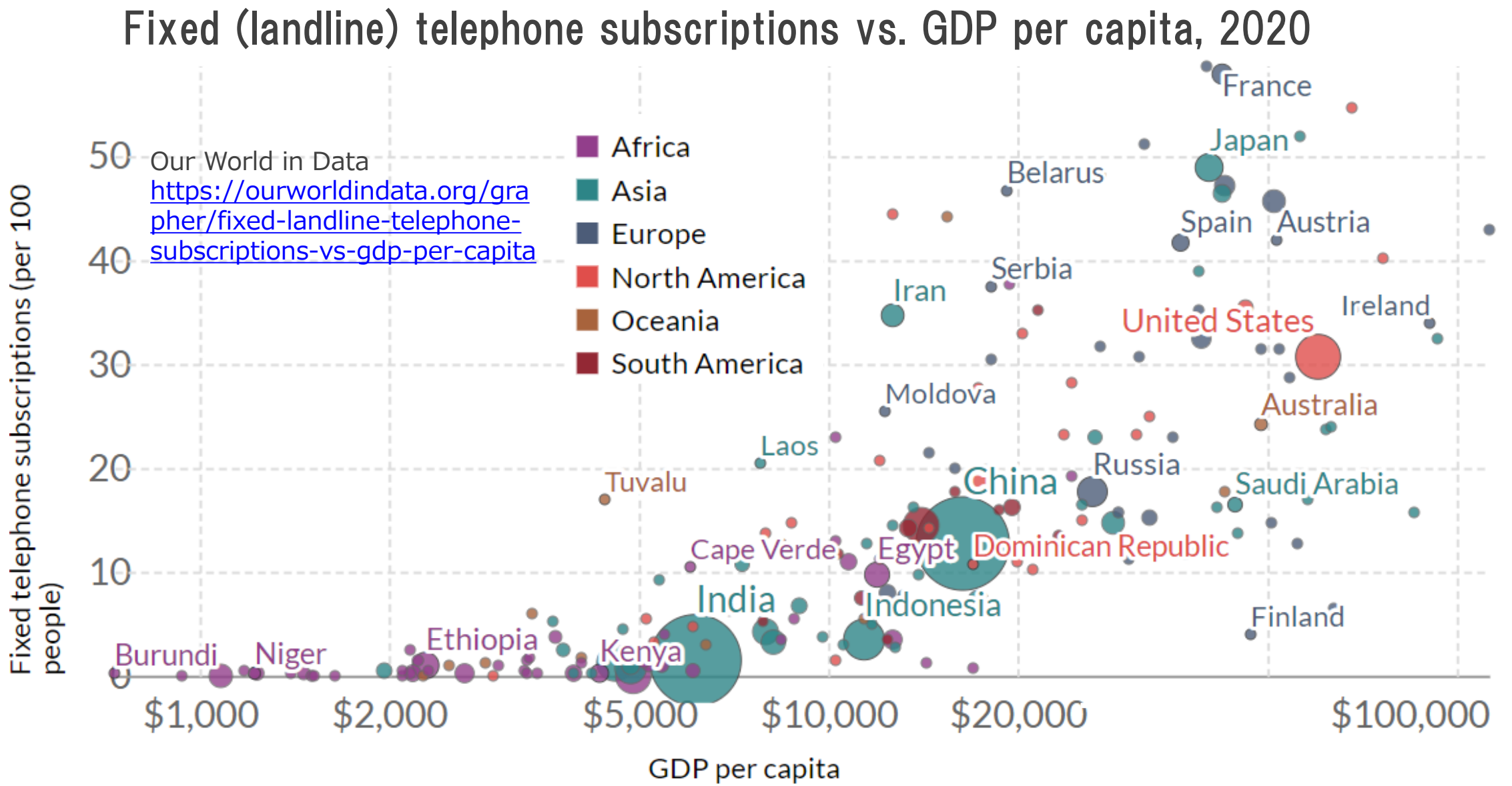
移動体通信サービスのインパクト

How Apple Has Changed The World In Just 7 Years
https://www.cultofmac.com/219813/how-apple-has-changed-the-world-in-just-7-years-picture-1000-words/

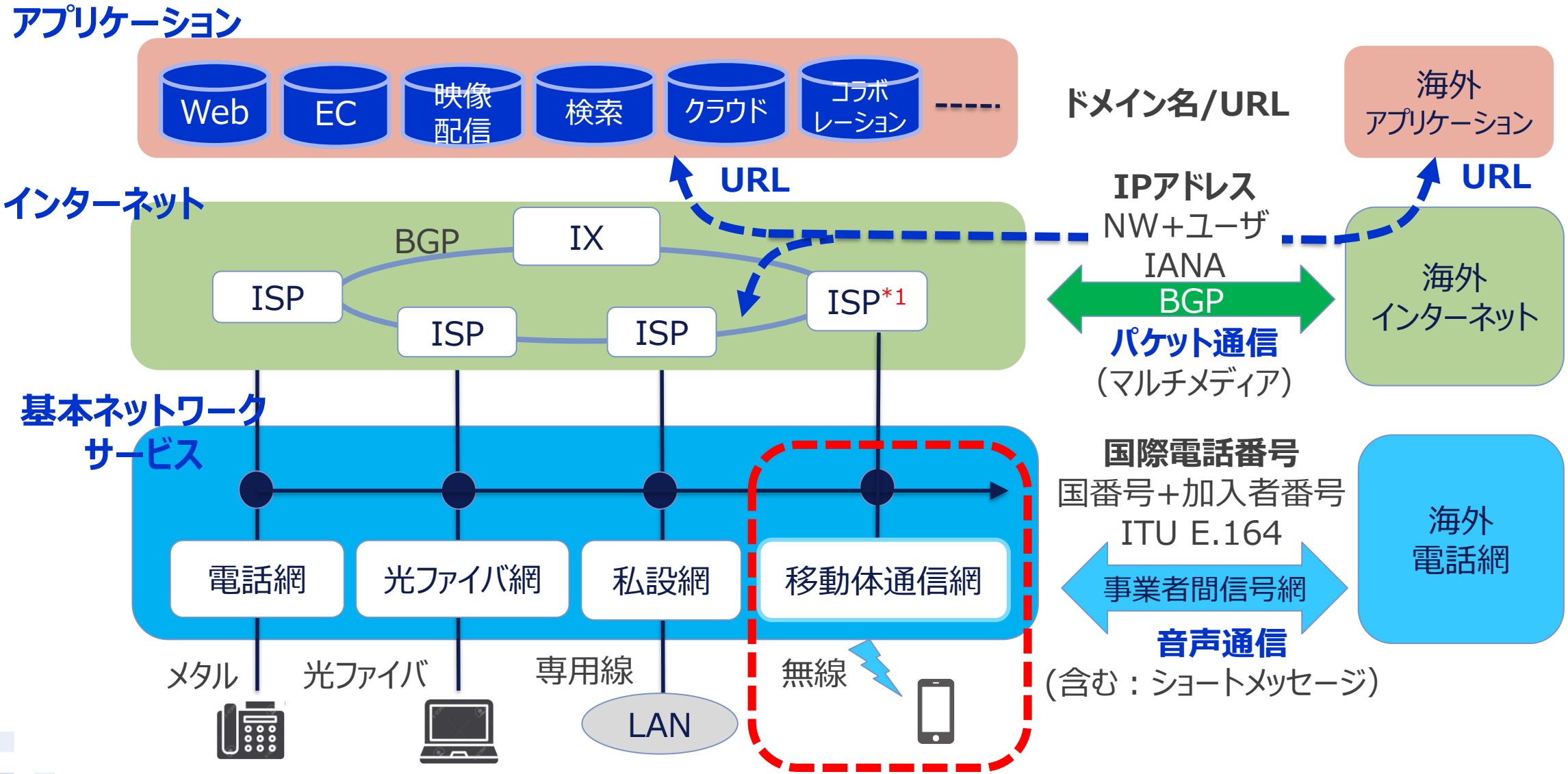
移動体通信サービスとGDP



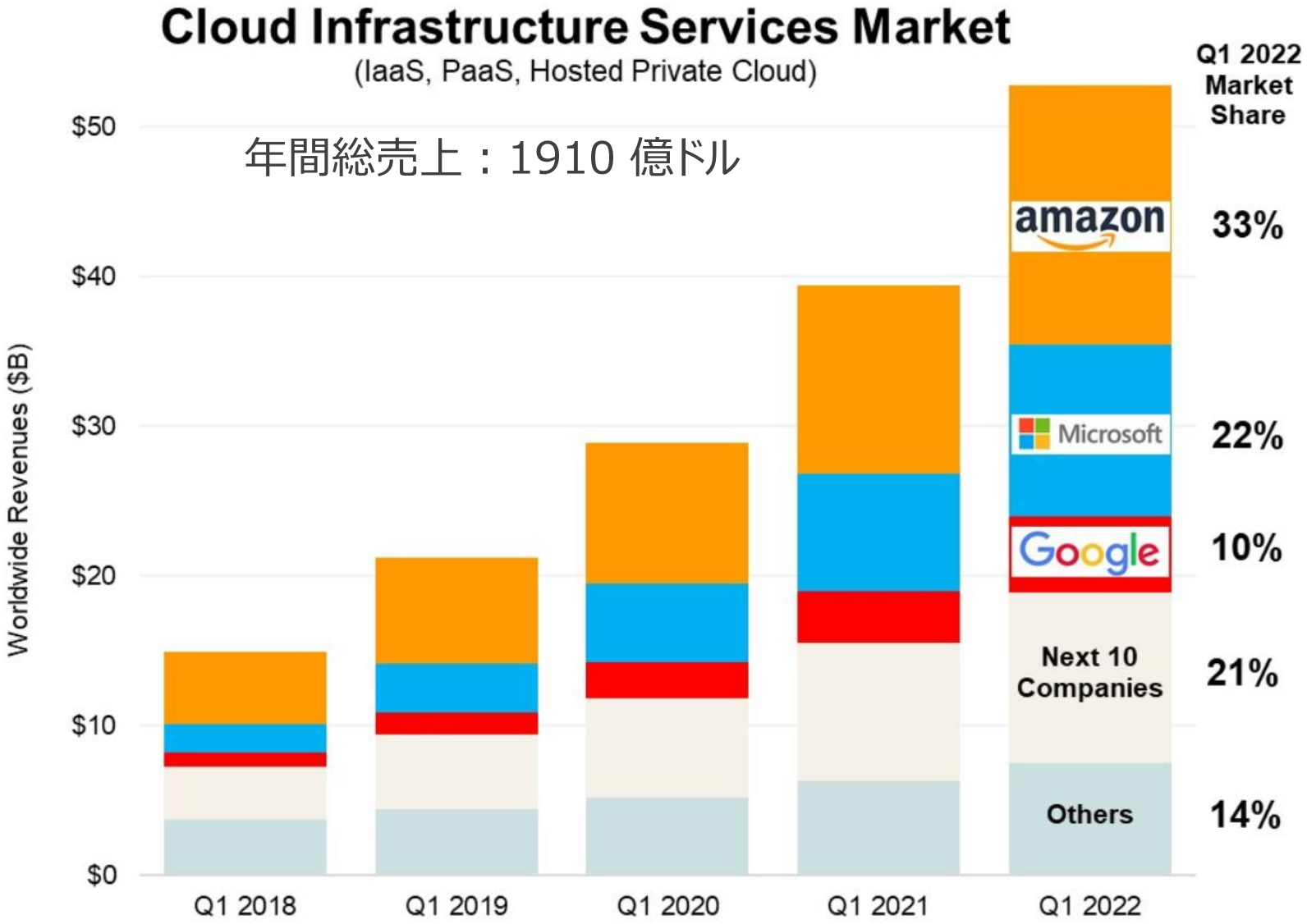
固定電話サービスとGDP



現代のデジタル通信ネットワークの基本構造　システムの相互依存性の拡大



メガプラットフォーマによるクラウドサービスの寡占



最大の問題？

あらゆる社会・経済活動の中にデジタル技術が浸透してゆくことで、**可視性・透明性**が失われてゆく

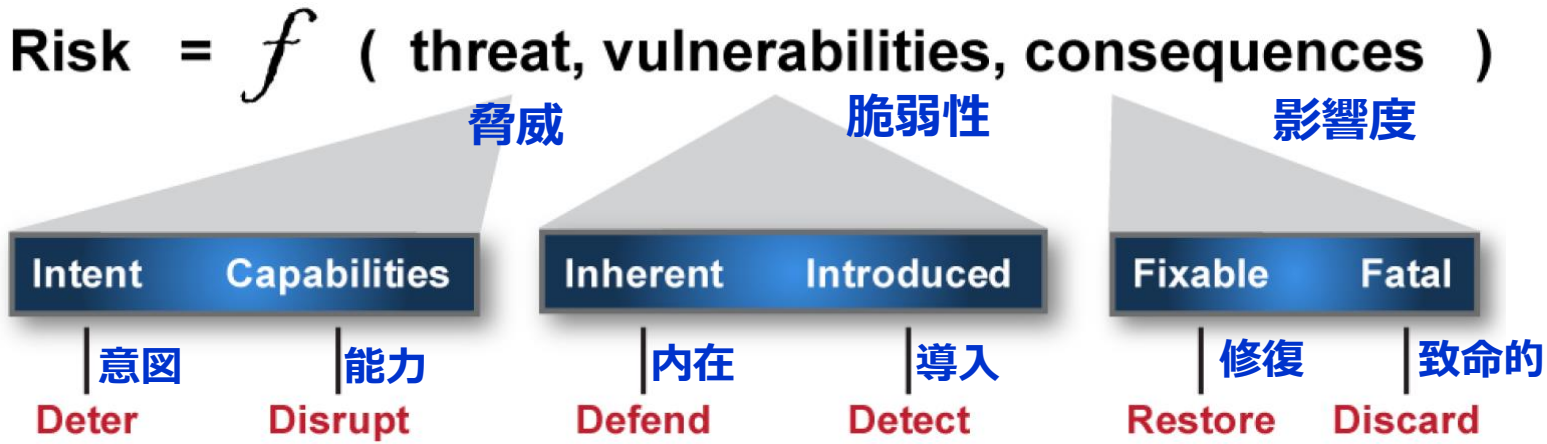
リスクが見えなくなる

まとめ
どうするか？

マクロなレベルでのリスクマネジメント

＜一般的なリスク評価の定義＞ ISO/IEC 27005, FIPS 199等

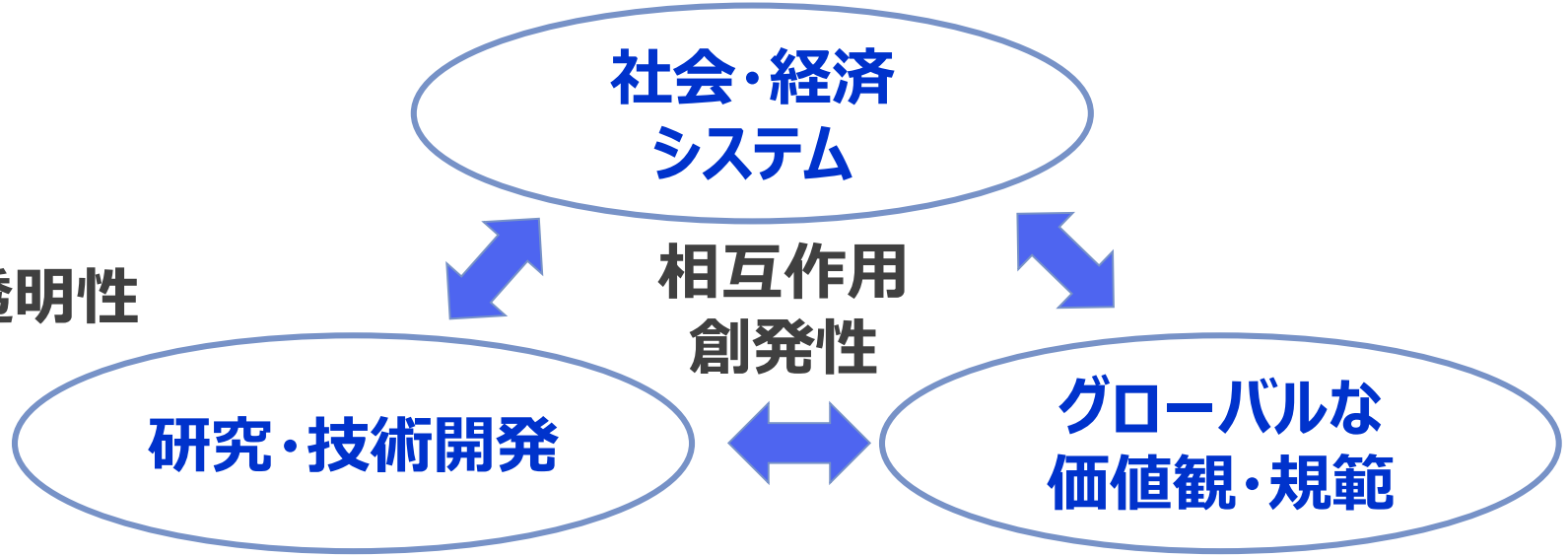
・資産に対するリスクは脅威、脆弱性、影響度の３つの要素で評価される。
・影響度はそれが失われた場合の事業継続性で評価される



＜マクロなレベルでのリスクマネジメントの検討と社会実装＞

リスクマネジメントの第一歩
- ⇒現実の理解、可視化・透明性
- ⇒失敗の共有
- ⇒思考を停止しない

想定外を少なくする



NTT DATA

Trusted Global Innovator