FUJITSU

サイバー攻撃

2015. 9. 12

田中達浩

富士通システム統合研究所
安全保障研究所サイバー担当主席研究員
陸自OB

本日の話　－サイバー攻撃－

１　インターネットの構造

２　サイバー攻撃

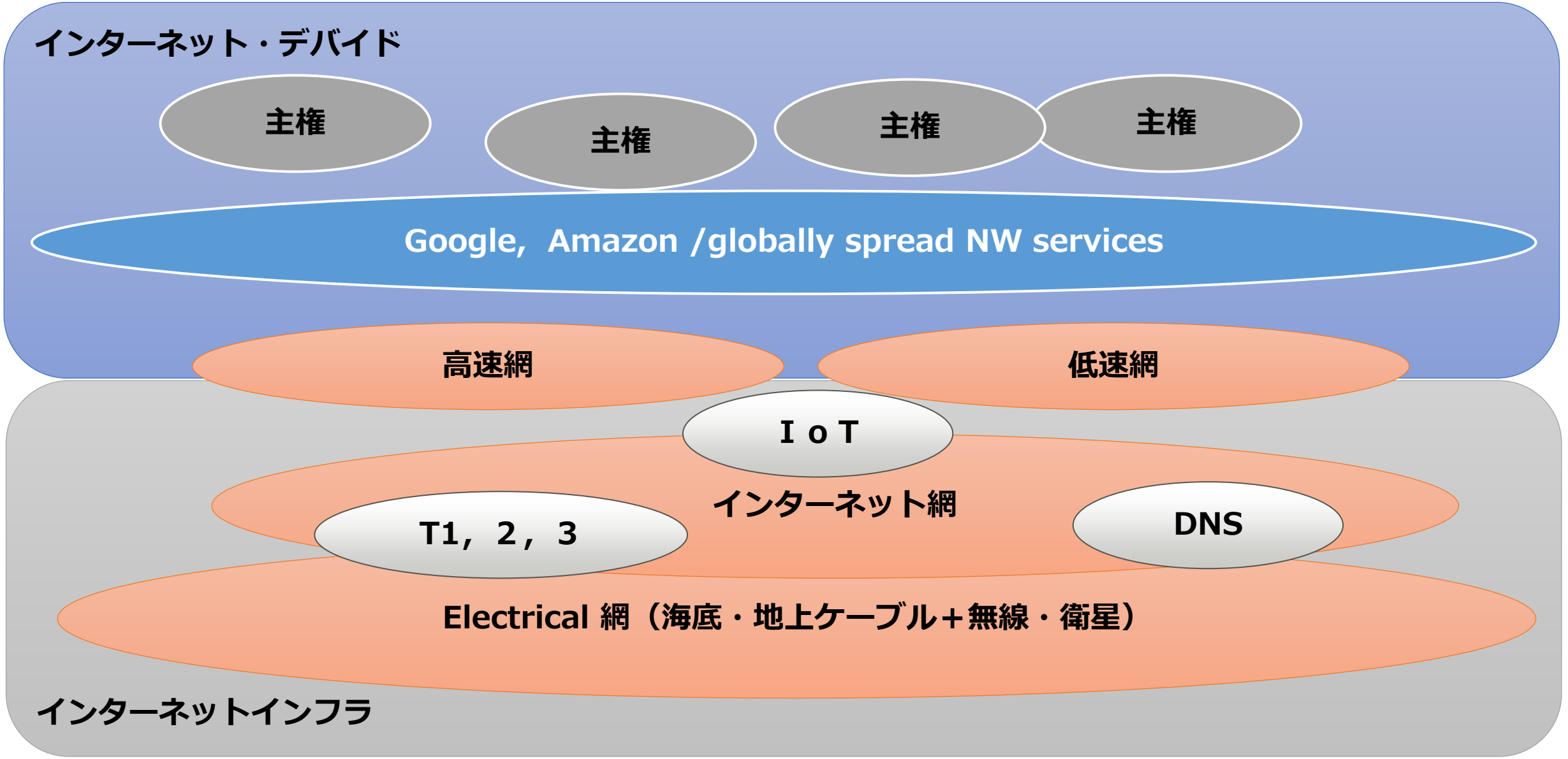
・通常型
・標的型
・キャンペーン化
・IoTリスク

３　サイバー対処の体制と技術

・サイバー犯罪～サイバーテロ～サイバー戦への対応
・サイバーセキュリティ～サイバー安全保障
・サイバーインテリジェンス

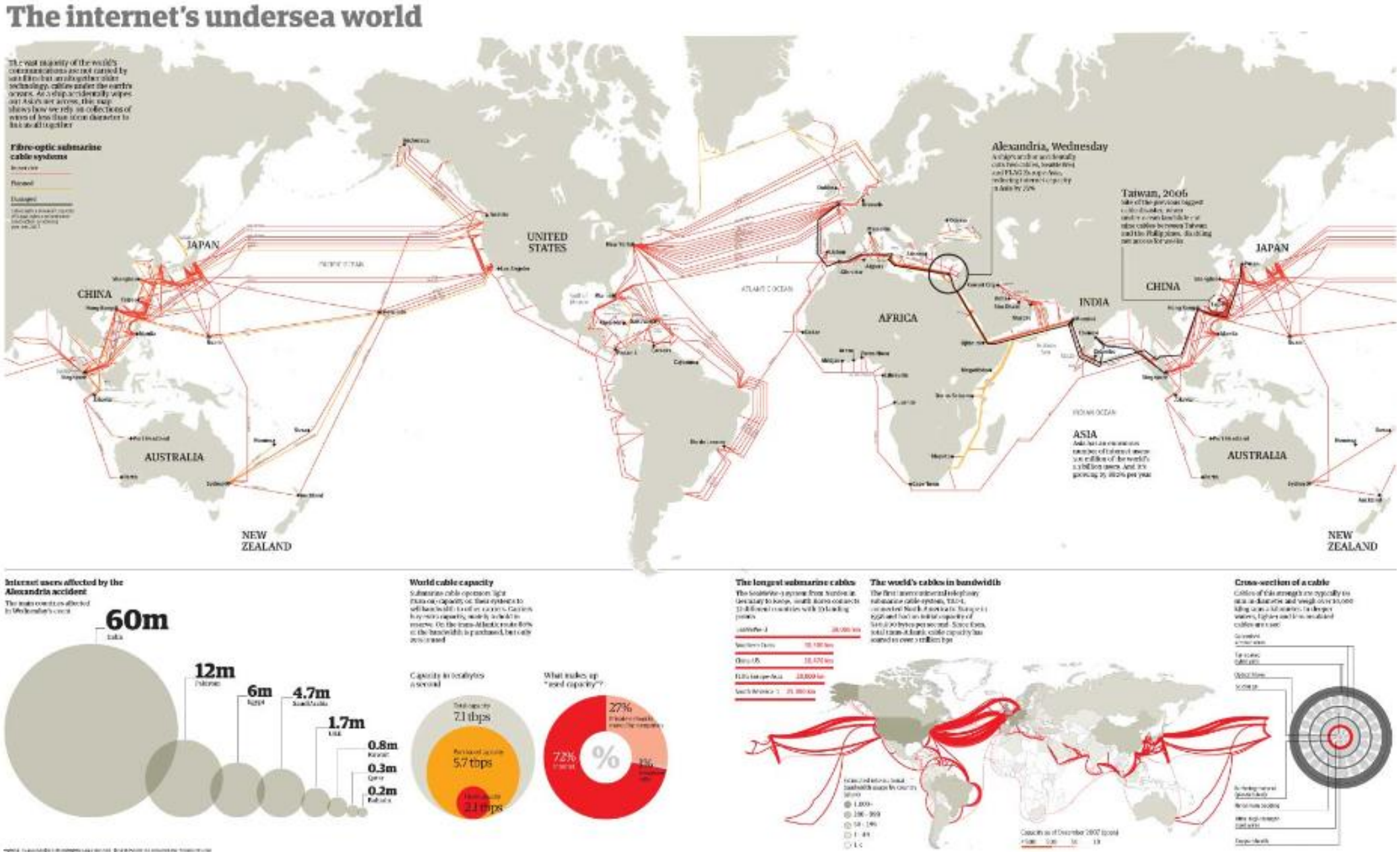
４　課題

インターネットの構造と分断

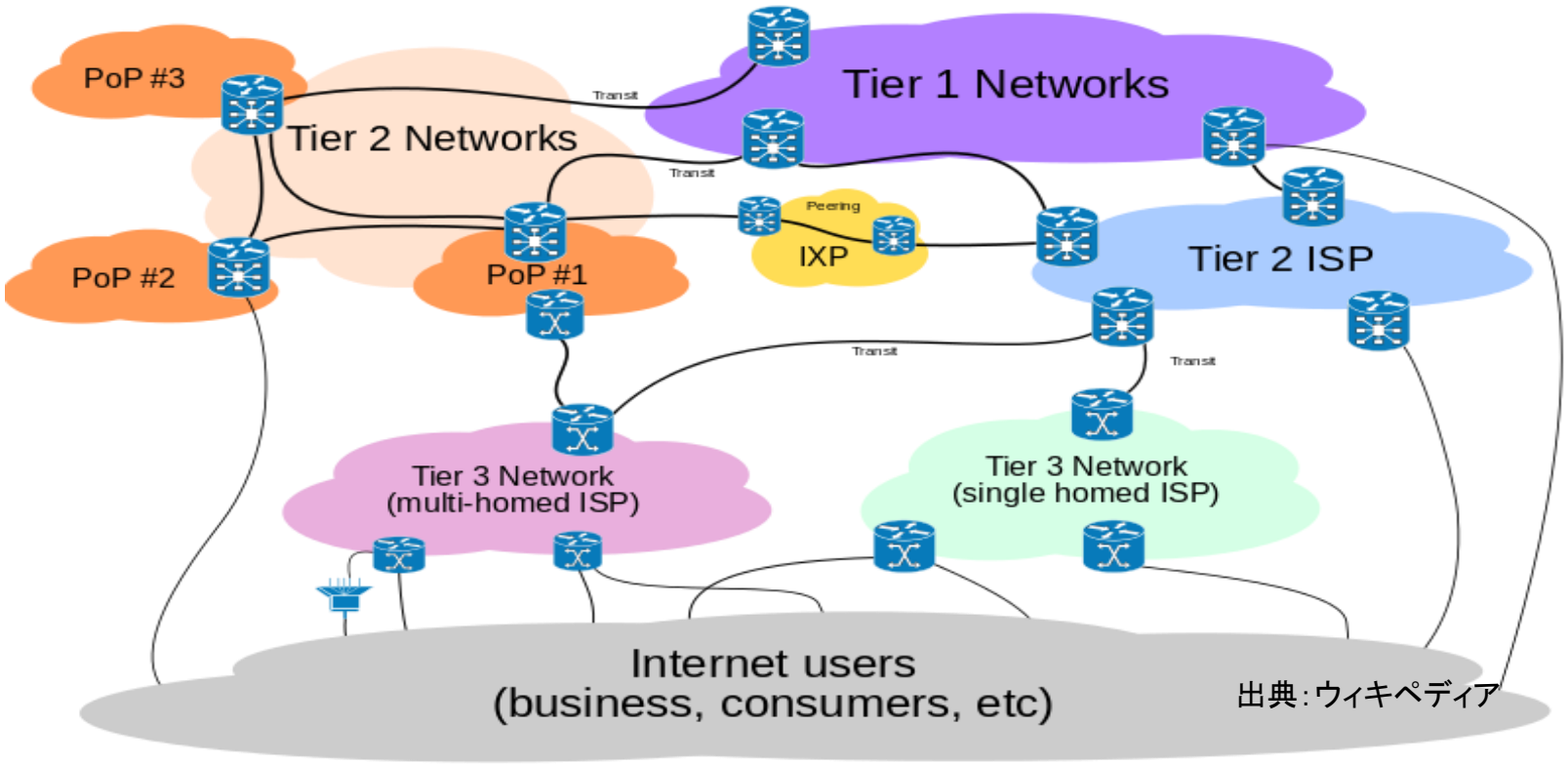


海底ケーブル

http://submarine-cable-map-2014.telegeography.com



インタネットの構成(T1,T2,T3)

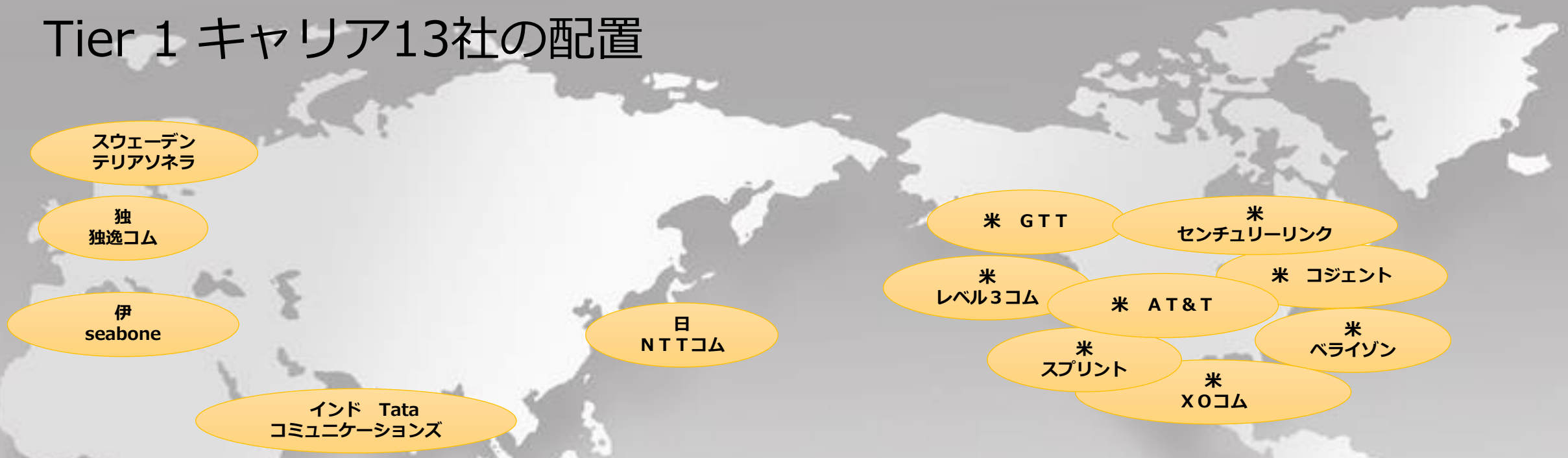


出典:ウィキペディア

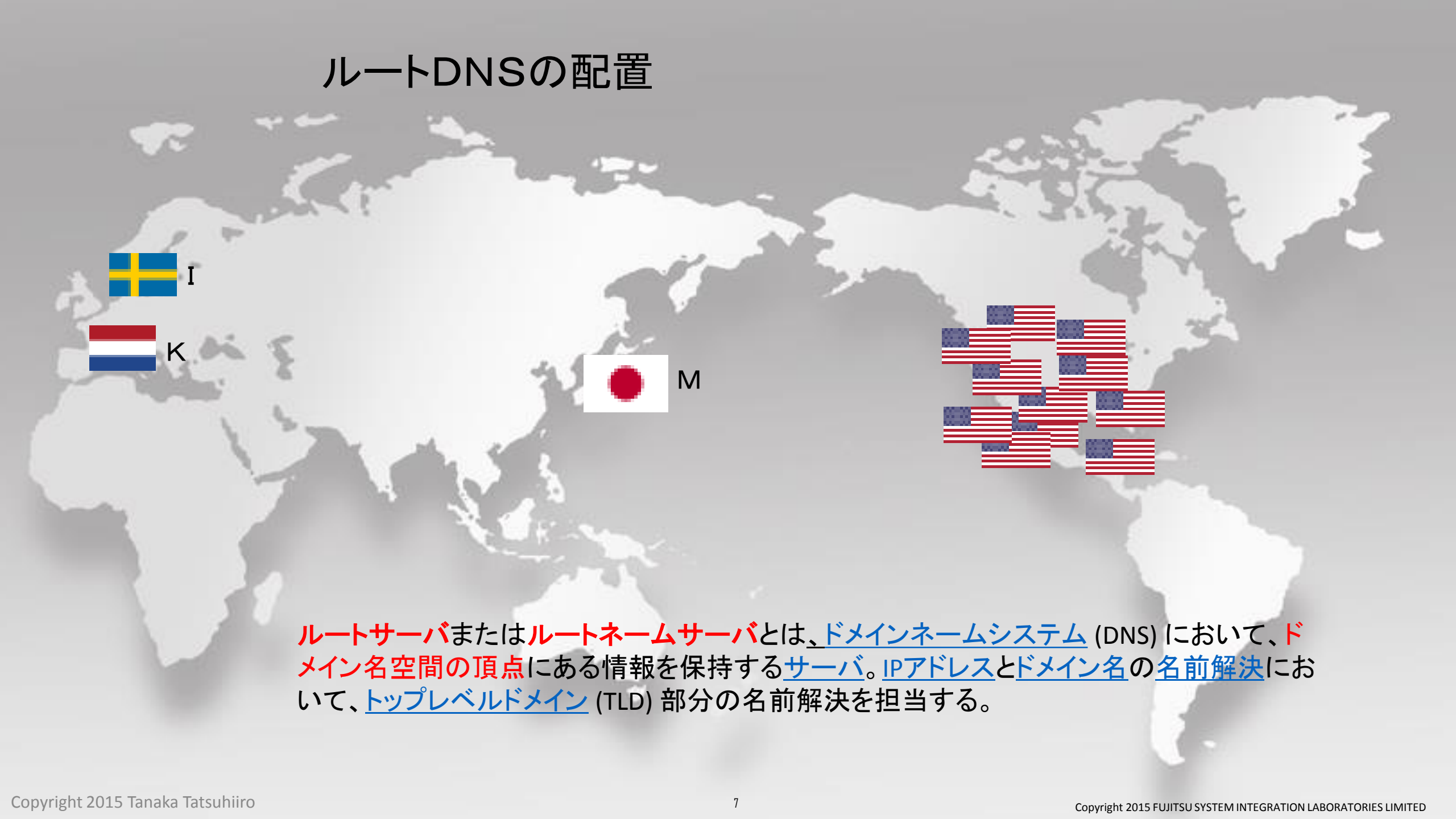
大手プロバイダは，配下に中小のプロバイダを数多く抱え，それらから送られてくる**膨大な数の経路情報を保持**している。しかし，どんなに大規模なプロバイダでも1社だけでインターネット上のすべての経路情報を得ることはできない。そこで，同じ境遇のプロバイダ同士をつないで，それぞれのプロバイダが持つ経路情報を交換し合う。こうして，**他のプロバイダと経路情報を交換するだけでフル・ルートを入手できるプロバイダ**を，「Tier1」と呼ぶ

出典:日経コンピュータ

Tier 1 キャリア13社の配置

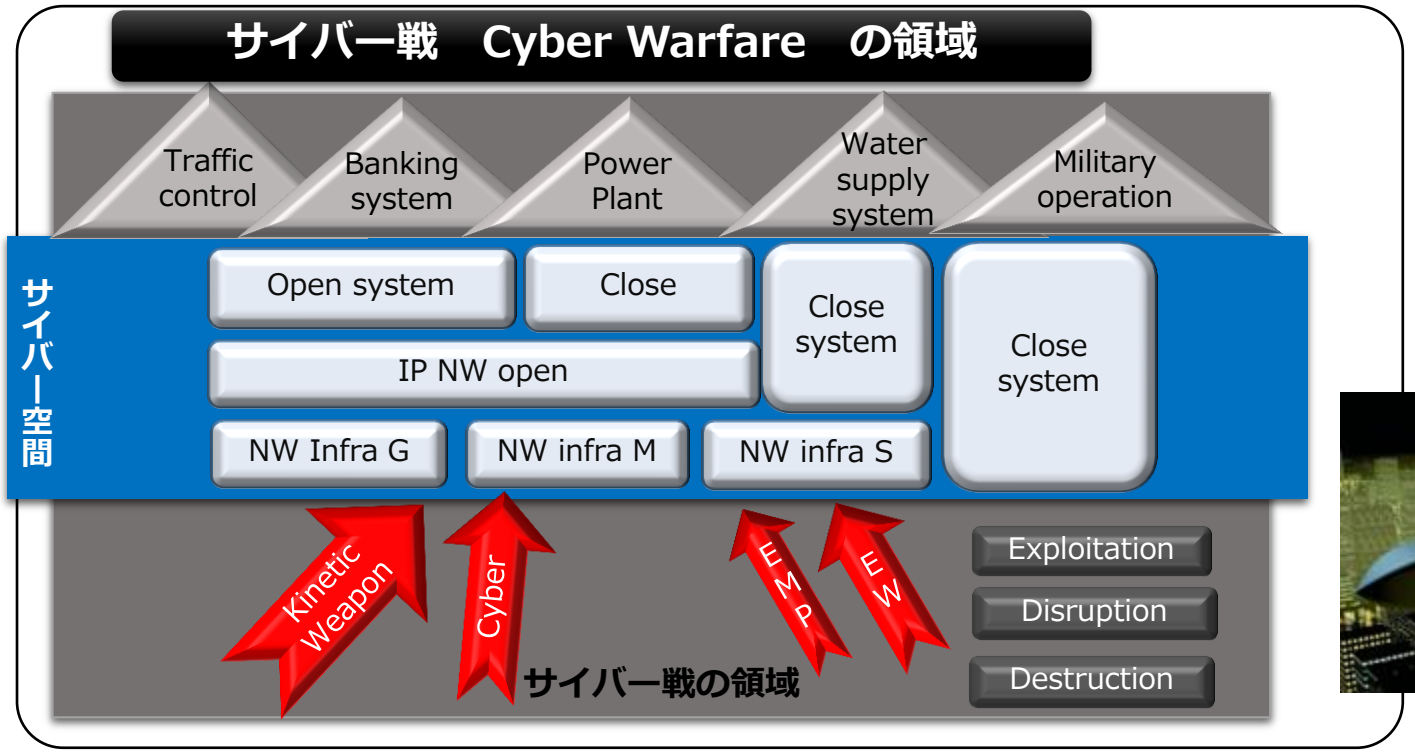


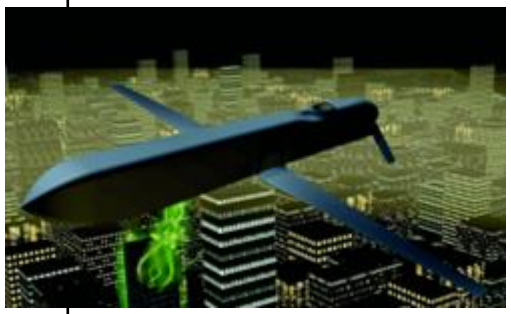
ルートDNSの配置



ルートサーバまたは**ルートネームサーバ**とは、ドメインネームシステム (DNS) において、**ドメイン名空間の頂点**にある情報を保持するサーバ。IPアドレスとドメイン名の名前解決において、トップレベルドメイン (TLD) 部分の名前解決を担当する。

サイバー戦の領域





重要インフラ

情報セキュリティ対策推進会議

国民生活及び社会活動に不可欠なサービスを提供している社会基盤

他に代替することが著しく困難なものであるため、機能が停止すると社会経済活動に多大な影響を及ぼす

- 情報通信
- 金融
- 航空
- 鉄道
- 電力
- ガス
- 政府・行政サービス（地方公共団体を含む。）
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油

の１３分野

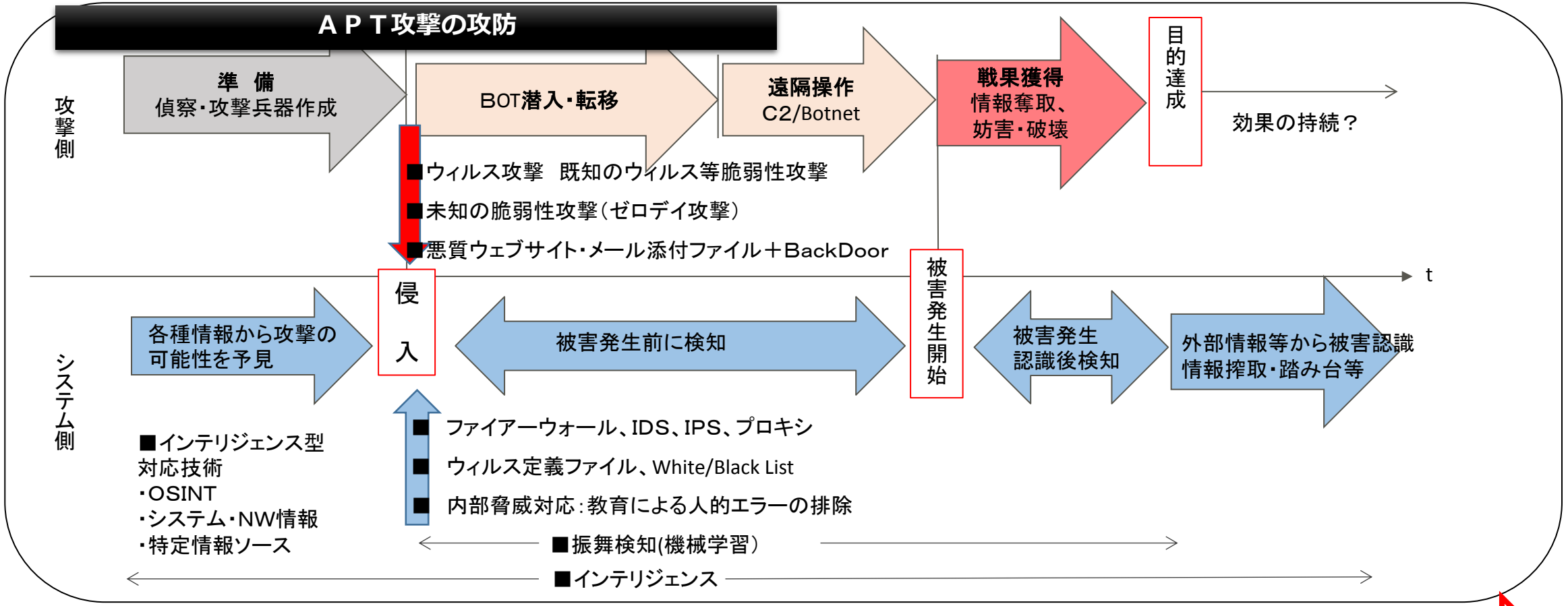
サイバー攻撃

通常型(従来型)サイバー攻撃　ーウィルス感染、DDoS攻撃等々

一時性	使用妨害中心	成果誇示型

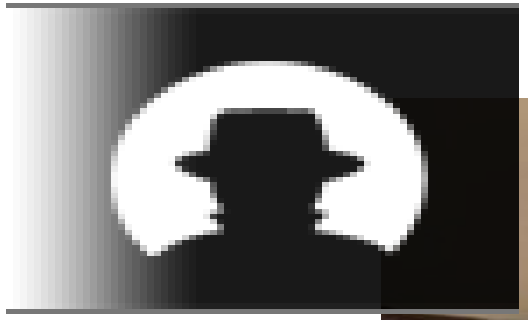
標的型(高度・持続型APT)サイバー攻撃

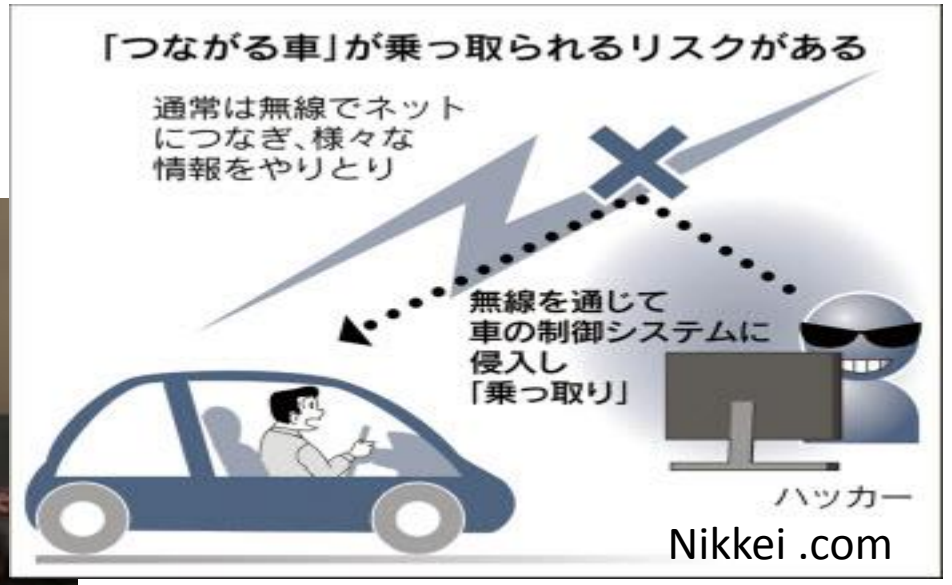
潜伏型	情報等搾取～妨害～破壊	成果誇示(心理戦)～隠密隠蔽型	外部脅威～内部脅威



サイバー攻撃はキャンペーン化　（単一作戦→大規模・組織的に複数作戦を統合遂行）

IoT のリスク（サイバーと無線）





Charlie Miller氏　　Chris Valasek氏

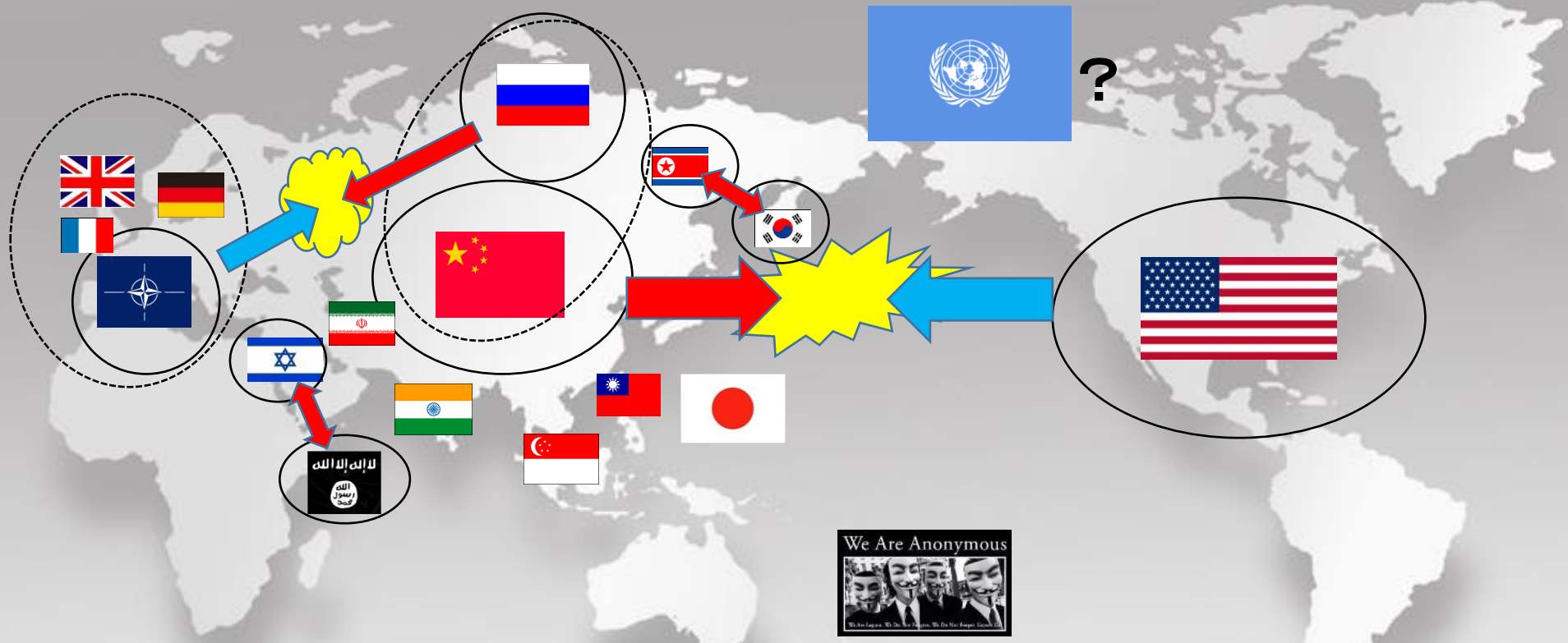
コネクテッド・カーは、20～100のECU（Electronic Control Unit）で構成される。また、それらはCAN（Controller Area Network）で構成され、ECUが互いにデータをやり取りすることによって、エンジンやブレーキ、ハンドルなどの制御を行う。

車内のコネクティビティとして、CANの他、AVB（Audio Video Bridging）、Wi-Fi、Bluetoothなどを介したモジュール間接続がある。また、**車外のコネクティビティ**としてWi-Fi、LTEやセルラーネットワークなどを介した音声やデータの接続、テレマティクスやADAS（Advanced Driver Assistance System）向けのM2M（Machine to Machine）テクノロジなどがある。

地政学的な構図とグローバルな構図

争いの図

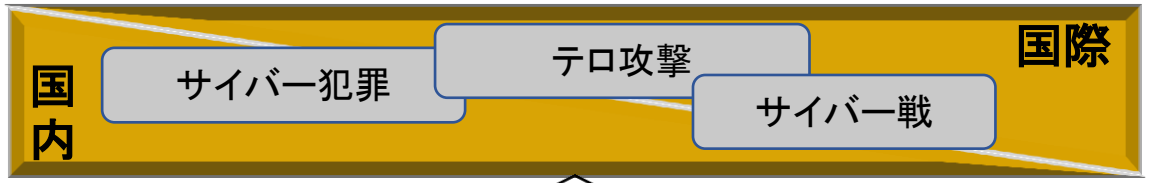
http://map.norsecorp.com/



サイバー対処の体制(グレーゾーン対処)

サイバー攻撃主体
国家、非国家、個人

サイバー攻撃効果
・物理的(システム)効果
ー情報搾取、妨害、殺傷破壊
・心理(政治)効果
・キャンペーン化



対応

サイバー戦上の対応原則
・任務継続 (特に初動)
MA/BCP
・復旧
・被害の見極め
・攻撃者の特定
・エスカーレーション適切対応
(グレーゾーン)

サイバーセキュリティ体制

サイバー安全保障体制

重要インフラ防護

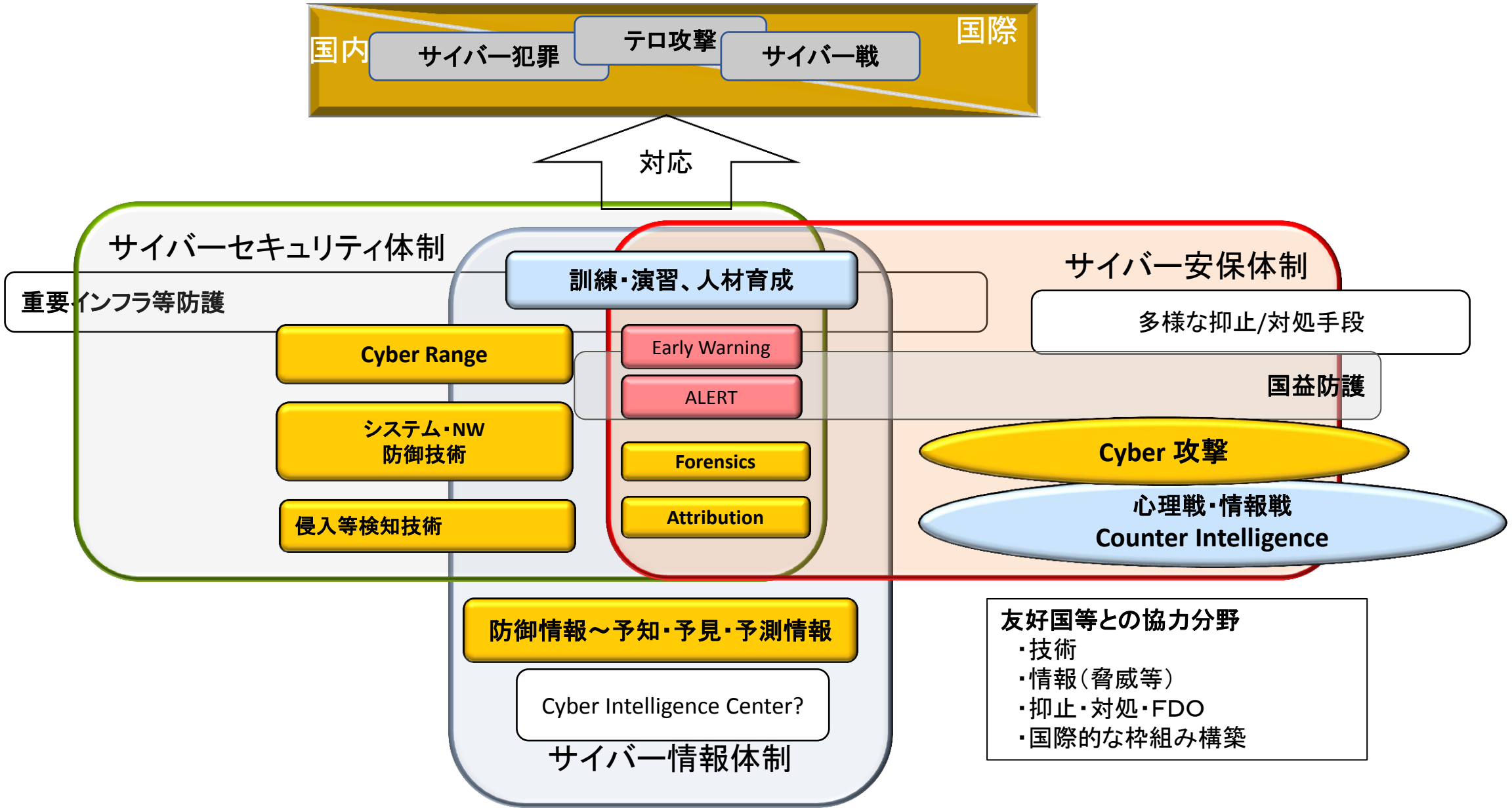
国益防護

サイバー情報体制

・情報通信
・金融
・航空
・鉄道
・電力
・ガス
・医療
・水道
・物流
・政府・行政サービス(地方公共団体を含。)
化学
クレジット
石油

平時	グレーゾーン	有事
国内法事態	判定が難しい事態	国際法事態
国家主体の行うサイバー攻撃		
スパイ活動	武力攻撃と認定できない攻撃	武力攻撃と同等の攻撃
非国家主体のサイバー攻撃	主体が不明の場合 ＋武力攻撃相当	

具体的なオペレーションと関連技術



サイバー脅威情報の分析と共有

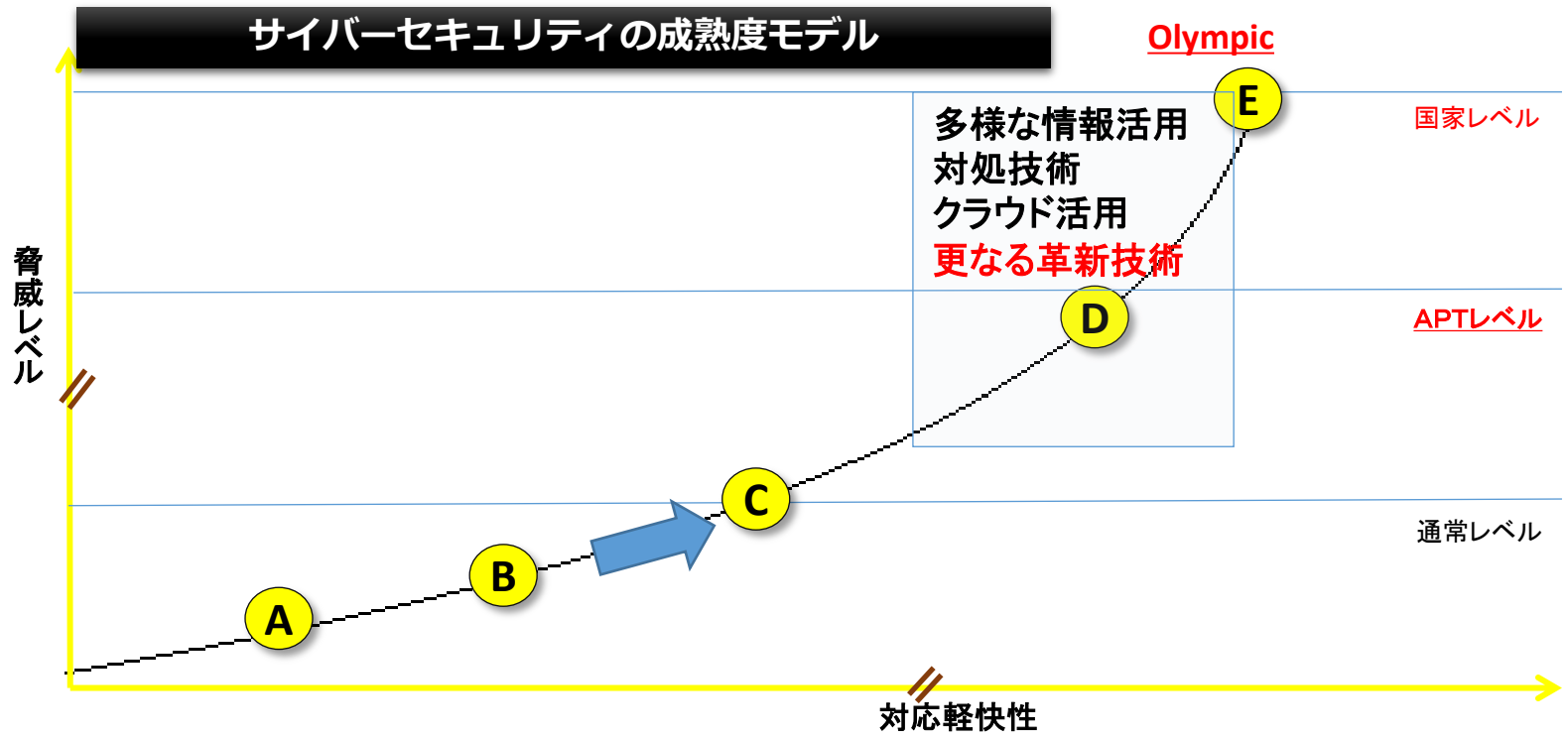
インシデント情報の共有 → 予測型情報分析と共有

脅威情報解析
-多様な情報ソースの活用及び多機能有機連携
-ニアリアルタイム～リアルタイム自動解析
-豊富な情報（intelligence)の蓄積（膨大なシグネチュア等の蓄積不可能）
-1H5Wの脅威認識
-Indicator

脅威情報の共有
-多様な枠組みでの情報共有体制が存在
　米DIB、日CDC、サイバーウェザーマップ
-STIX、TAXIIなどの情報共有を目的としたツールを活用
-国家間の情報共有はこれから
　CERT/CC間の情報共有は存在

- TAXII（Trusted Automated eXchange of Indicator Information）
  STIX などで記述されたサイバー脅威情報のやり取りのプロトコル
- STIX（Structured Threat Information eXpression）
  脅威情報構造化記述形式。サイバー脅威情報間の5W1H 的な関係を記述する言語。
  サイバー空間における脅威の分析、サイバー攻撃を特徴付ける事象(indicator)の特定、
  サイバー攻撃対応の管理、サイバー攻撃に関する情報の共有などを目的とした仕様。

脅威に対応するサイバー技術の目標と課題



A	B	C	D	E
火消対処療法 マニュアル	ツールベース/ 入口対策 パッチ当(定義ファイル) システム、マシーン毎に対応	COP 認識の共有 システム統合化 SOC	動的防御 予見・予測 迅速対応 サイバーインテリジェンスセンター	・強靭性(国家活動継続) ・重要インフラ防護/被害局限/リソース配分優先順位 ・抑止・対処 強靭な国家体制

多様な情報活用
- オープンソースINT
- GEOINT
- CELLINT等々
- + ビッグデータ

対処技術
- White Data/Black Data
- 振舞検知
- 機械学習
- backdoor検知

クラウド活用
- 自動化・仮想化ツール
- ストーブパイプ脱却
- 情報処理速度の高速化

更なる技術革新競争
- AI活用技術
- 情報融合技術
- 高度高速自動解析技術
- 防御・検知技術

モデル： 富士通アドバイザー Robert Lentz 氏元DOD CISO

サイバー軍備管理及び国際的な枠組み構築

-国家主体のサイバー攻撃兵器は、国家主体による通常兵器と同様に扱われる必要がある。

-国際的な規範International Norms (枠組みと合意) が主要国及び多数の国家間で将来のサイバー災禍を回避するため形成されることが必要である。

Step 1

サイバー軍の透明化

-軍事作戦におけるサイバー軍及びサイバー攻撃の是認

Step 2

武力紛争法の適用

-サイバー空間における武力紛争法の適用

武力行使　the use of force

管轄権　Jurisdiction

非軍事目標　non-military objectives

中立性　neutrality

均衡原則　proportionality

先制・予防攻撃　preemption

Step 3

非国家主体の孤立化

-非国家主体の組織及び攻撃の管理に関する国際的な合意の形成

Step 4

サイバースペースにおける国際的な秩序の構築

-サイバー抑止
-予防外交
-軍備管理（技術等不拡散） & 信頼醸成措置

国際的な活動と課題

国際規範作り

国連第 1 委員会（軍縮と安全保障）. の政府専門家会合（**GGE**）

世界情報社会サミット（**WSIS**）、
サイバー空間に関する国際会議（**GCCS**）

＋2国間協議等

平時における生存に関わる重要インフラの防護は妥協点？

サイバー兵器の不拡散

ワッセナーアレンジメント

2013年　Intrusion Softwareの移転禁止をリストに追加

侵入ソフトとは何か？

SCRM

ワッセナーアレンジメント

１　ワッセナーアレンジメント（WA：Wassenaar Arrangement）

・正式名称「通常兵器及び関連汎用品・技術の輸出管理関するWA」
・1996年、ココムから対テロ不拡散に変化
・WA参加41か国はWAの規制リストに基づき個別に輸出管理を行う。

２　コンピュータ、情報通信分野の規制リストDual-Use-List

・一般的に、高度技術の軍事転用を防止するための技術レベルをもって規制
・コンピュータ等ハードウェアは具体的な技術レベルをもってリスト化
・ソフトウェアでは高度暗号の技術について規制リスト化されたが、参加国間における輸出においても通常政府の許可が必要となるため、汎用で使用されるレベルの暗号及び高度レベルであっても金融機関等向け暗号等については許可申請なく輸出できるよう緩和措置がなされている。

３　侵入ソフトに関する規制

・2013年12月に*「侵入ソフト(Intrusion Software)」*の追加を合意
-定義：コンピュータやネットワーク機能のあるデバイス上で、監視ツールによる検知を回避したり防護手段を打破する目的で、特別に設計または修正されたソフトウェアのこととしている。
・日本政府輸出管理規制リスト*「侵入プログラム」*
-輸出貿易管理令のリスト：侵入プログラムを作成するコンピュータを規制
-外国為替令のリスト　：侵入プログラム及び技術を規制

ワッセナーアレンジメント

４　問題点

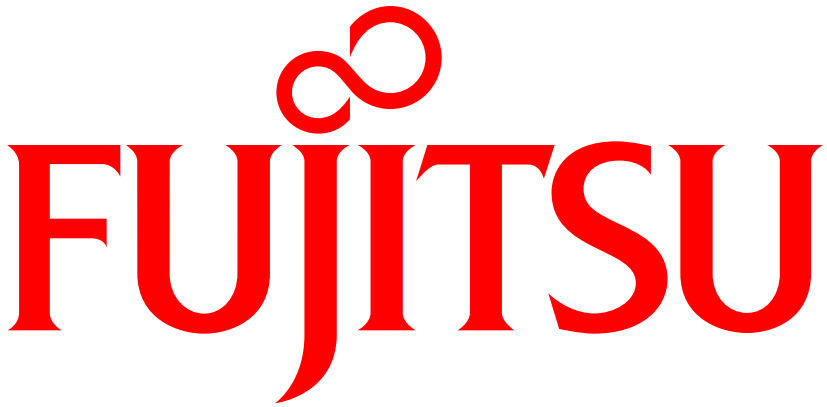
・***定義があいまい***、規制が広範になることから騒動（米国）になっている。

・輸出及び共同対処等に及ぼす影響

－システムの脆弱性を発見し対策を施す場合に、侵入プログラム（**テスト・評価用**）を国境を越えて**迅速**にやり取りできなくなる。（ゼロデイ攻撃の脅威対処）

－発見した**マルウェア（侵入プログラム）の検体**を国境を越えてやり取りできない。

以上のような例について問題提起されており、サイバーセキュリティ製品・サービス輸出先国への継続的支援、国家間の共同対処・情報共有を支援する多国籍企業・企業間連携が**迅速に行われなくなる**おそれがあるとの議論になっている。



shaping tomorrow with you