サイバーセキュリティ（CS）とシギント機関の取組
～NSAとUKUSA～

2023年10月

茂田インテリジェンス研究室
https://shigetatadayoshi.com/

目　次

目　次

（参考）NSA本部全景

https://commons.wikimedia.org/w/index.php?curid=16450

NSA本部（フォートミード）全景

1－1　UKUSAシギント同盟

Five Eyes: FVEY　世界最強のインテリジェンス機構

米：　NSA国家安全保障庁

（約5万5千人。150億ドル程度）

英：　GCHQ政府通信本部（約7千人。　20億£程度）

加：　CSE通信安全保障局（約3千人。　9億加ﾄﾞﾙ弱）

豪：　ASD豪信号局　　（約2500人。11億豪ﾄﾞﾙ程度）

NZ：　GCSB政府通信安全保障局

（430人。　1億8千万NZﾄﾞﾙ）

共同の収集分析、共同のシステム構築。

統合運用の段階

（註）下線の数字は推定

1-2 NSA ①予算・職員

NSA（National Security Agency）国家安全保障庁

1952年設立、1975年存在を公認

◆ 職員：2013年定数 3万4901人（軍人1万4950人）

2018年報道：正規職員3万8千、契約職員1万7千人

加えて、陸海空軍・海兵隊・沿岸警備隊のシギント部隊を指揮下に。

更に、 サイバー軍

◆ 予算： 2024会計年度諜報機関予算要求

国家諜報予算＋軍諜報予算＝合計

724億ドル 293億ドル 1017億ドル

シギント予算＝NSA＋NRO＋各軍シギント他

総計、300億ドル、4兆円規模？

（2013年国家諜報予算526億ドル、内NSA108億ドル）

1-2　NSA　②任務

◆　任務

①　シギント　　矛（攻撃）

②　サイバーセキュリティ　　楯（防禦）

○　National Security Systemsの責任部署

（軍、インテリジェンス、国務省の情報システム）

○　サイバーセキュリティ支援

○　NTOC（N/C Threat Operations Center）運営

常時の脅威監視。FBI、DHS/CISAとの協力窓口

③　CNOの基盤の提供　　サイバー軍他への支援。

CNO＝Computer Network Operation

（CNE資源開拓　CND防禦　CNA攻撃）

1-2　NSA　③シギントとは？

シギント(Signals Intelligence)とは？

①　コミント（communications intel.)通信諜報

電話、携帯電話、無線通信、インターネット、ファックス等

- ○　**暗号解読**(crypto-analysis)
- ○　**通信状況分析**（traffic analysis）、**メタデータ分析**

②　エリント（electronic intel.）

電磁波、特にレーダー波

Hiroshi miyaji, CC BY-SA 4.0 via Wikimedia Commons

航空自衛隊, CC BY 4.0 , via Wikimedia Commons

Hans-Hermann Bühling, CC BY-SA 3.0 , via Wikimedia Commons

③　フィシント（foreign instrumentation signals intel.）

テレメトリー信号（ミサイルからの信号）

DARPA, CC BY-SA 4.0 , via Wikimedia Commons

1-2 NSA ④沿革

1949年 軍安全保障庁(AF Security Agency)設立

1952年 National Security Agency設立(大統領命令)

国家 Intel. | Commint＋Comsecの隠語 | 庁

別名“No Such Agency”～1975年まで存在自体が秘密

1956年 副長官はシビリアンのシギント専門家

1959年 人事権の独立(独自の採用解雇権限)

1972年 CSS(Central Security Service)附置

陸海空軍海兵隊のシギント組織の活動の調整、一体化

NSA長官がCSS長を兼務

2005年 国家諜報長官(DNI)設置

2010年 サイバー軍CYBERCOM編成(現在約7000人)

NSA長官が司令官兼務

1-2　NSA　⑤国家諜報機関

☆　国家諜報機関としての位置付けが確立

○　任務付与（Tasking）～国家諜報長官

○　情報配布～国家諜報長官が、国防長官と調整の上で
司法長官の承認を得て定める。

○　人事～NSA長官は上院の承認を得て大統領が任命。
国防長官が国家諜報長官の同意を得て候補者を推薦。

○　予算～NSA予算を含む国家諜報計画予算は、
国家諜報長官が作成決定して、大統領に提出。

National Intelligence　⇔　Departmental Intelligence
Service Intelligence

1-2　NSA　⑥関連組織の関係

NSA
（1952年設立）

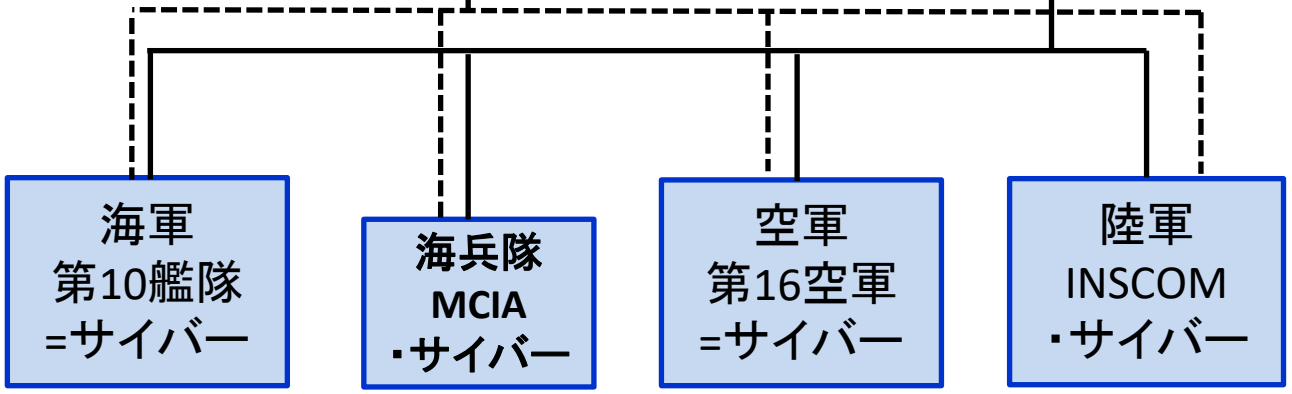
国家シギント

CSS
（1972年附置）

各軍シギントの調整

サイバー軍
（2010年設立）

サイバー作戦指揮



（各軍の主要インテル組織）

目　次

＜収集態勢総論＞（１）結論

世界中のNSAの収集態勢

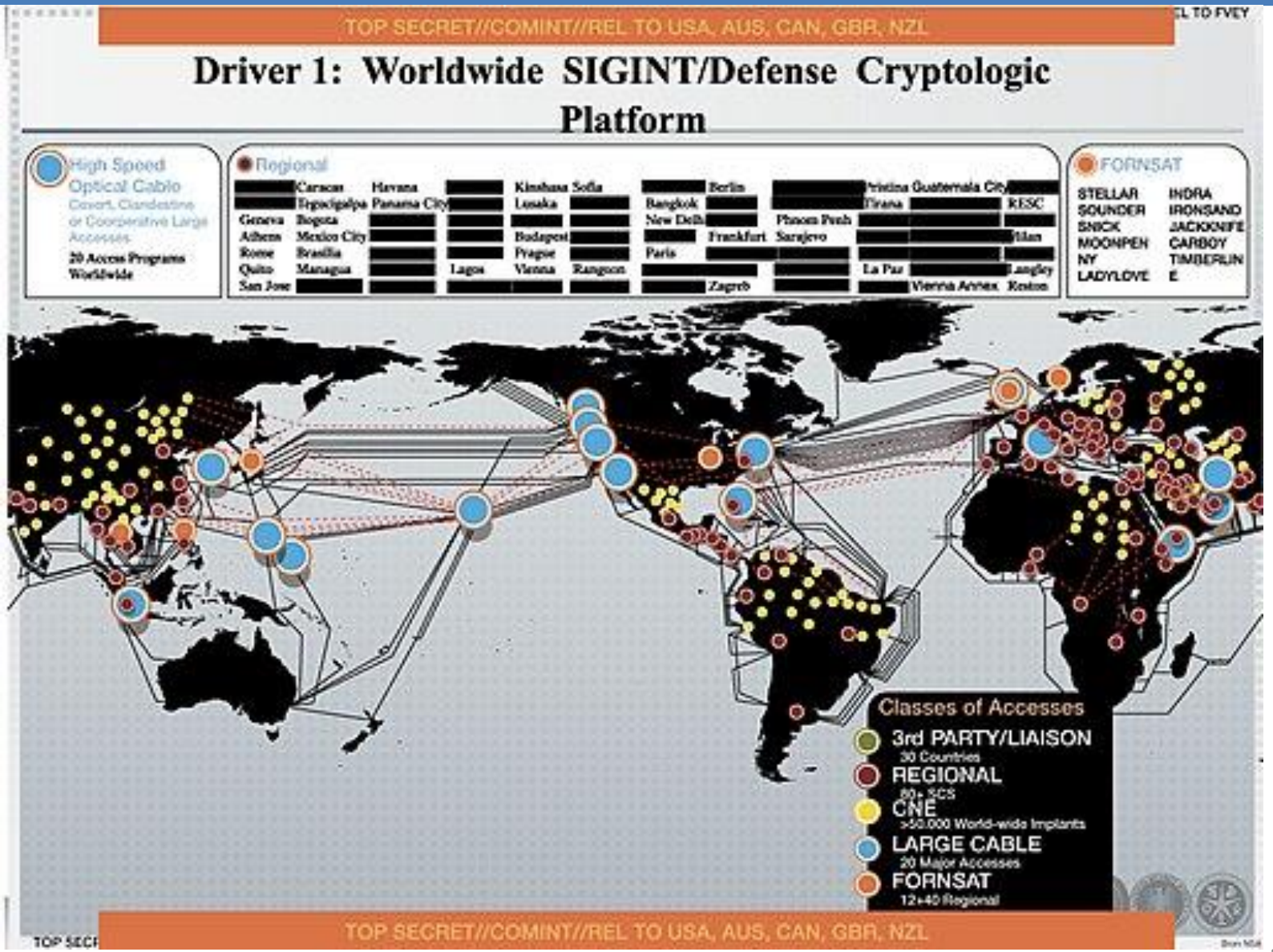
○　傍受施設～約500ヵ所

SIGADs（SIGINT Activity Designators）

○　主要傍受施設～約150ヵ所 以上

（X-Keyscoreの設置場所数）

＜収集態勢総論＞(2)漏洩資料



U.S. National Security Agency, Public domain, via Wikimedia Commons

＜収集態勢総論＞（3）協力企業・国

○ SSO（Special Source Op.特別資料源作戦）

民間企業の協力を得て行うシギント資料収集

収集データの内、コンテンツ情報の60%。メタデータの75%近く。

スノーデン曰く。「SSOはNSAのcrown jewel」

○ Second Party: UKUSA（英、加、豪、NZ）

○ Third Party（ギブ＆テイク）（2013年現在33ヶ国）

＜欧州＞18国：独、仏、伊、西、蘭、ベルギー、デンマーク、
ノルウェー、スウェーデン、フィンランド、墺、ポーランド、チェコ、
ハンガリー、クロアチア、ギリシャ、マケドニア、ルーマニア

＜アフリカ＞3国：アルジェリア、チュニジア、エチオピア

＜中東＞　5国：イスラエル、トルコ、ヨルダン、サウジ、UAE

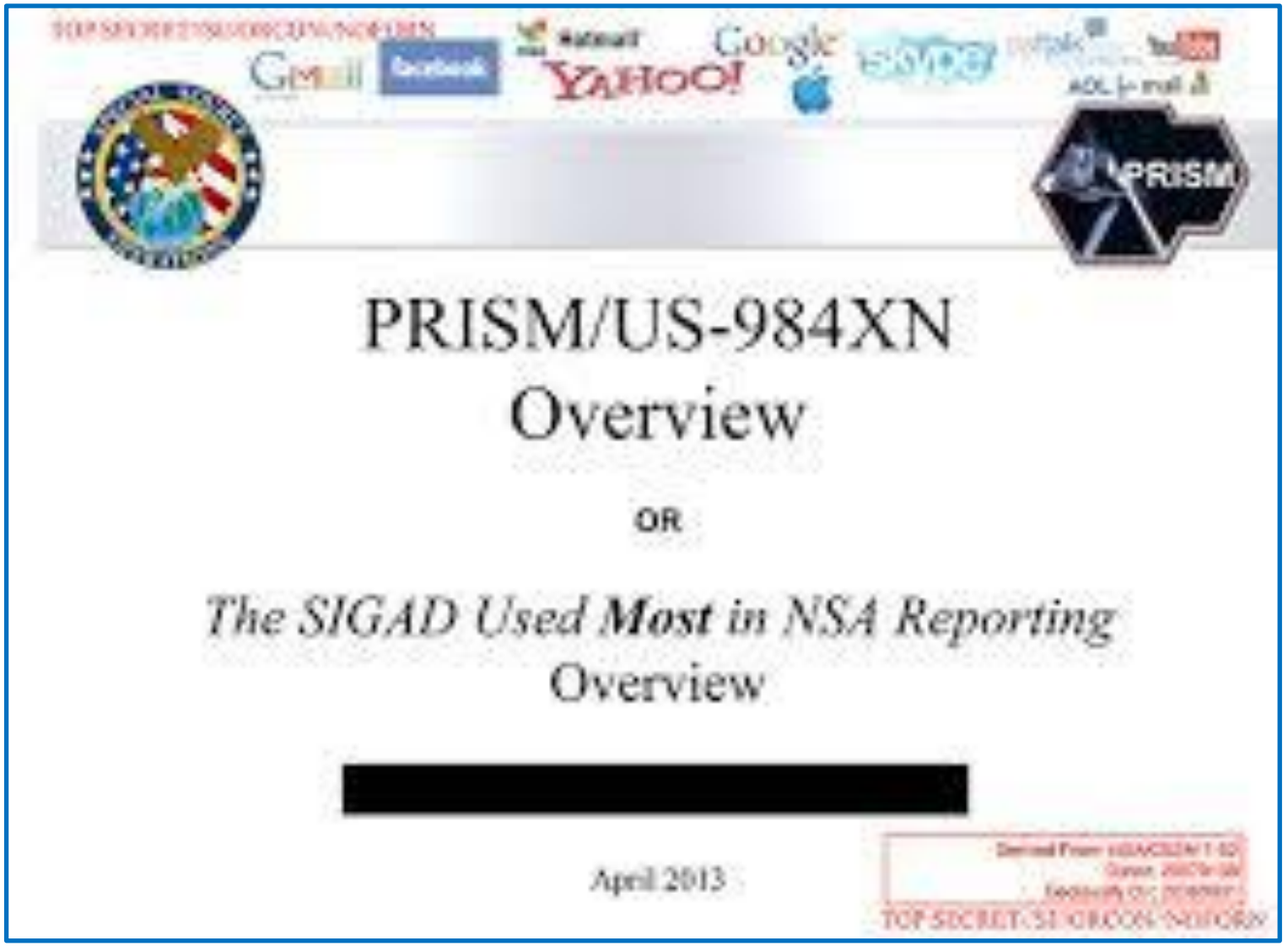
＜アジア＞ 7国：シンガポール、韓国、タイ、日本、台湾、
インド、パキスタン

＜収集態勢総論＞（４）プラットフォーム

1　「プリズム」計画（Downstream）
2　通信基幹回線からの収集（Upstream）
3　外国衛星通信の傍受（FORNSAT）
4　特別収集サービス（SCS）
5　シギント衛星・機上収集（Overhead）
6　TAO/CNE（コンピュータ・ネットワーク工作）
7　海軍艦艇・潜水艦
8　従来型収集（無線通信の傍受）Conventional
9　秘匿シギント活動　CLANSIG

2-1 「プリズム」計画 ①

漏洩されたパワーポイント資料



2-1 「プリズム」計画 ②

協力企業の米国内データセンターから必要な情報を随時、検索取得

- ○ SSO（特別資料源作戦）の一つ
- ○ 2007年開始　　参加協力企業
  - 2007年　マイクロソフト
  - 2008年　ヤフー
  - 2009年　グーグル、フェイスブック、パルトーク
  - 2010年　ユーチューブ
  - 2011年　スカイプ、AOL
  - 2012年　アップル
- ○ 取得情報
  - コンテンツ情報：メール、文章、音声、写真、ビデオ等
  - メタ情報：メールアドレス、電話番号、通信時刻、位置等
- ○ 少ない費用で効果抜群
  - 2013年中に約2億5千万件以上のデータを取得
  - NSAの情報報告の1/7近くがプリズム由来

Gmail, Hotmail, yahoo mail

2-2　通信基幹回線　①

世界中で通信基幹回線から収集

○　企業協力SSO　　4計画

「ブラーニー」（米国内）　30社以上

「フェアビュー」ATT「ストームブリュー」ベライゾン（米国内）

「オークスター」　小計画8つ　　（殆ど米国外）

○　UKUSA＆Third Partyの協力　2計画

「ウィンドストップ」～UKUSA　小計画4つ　　（米国外）

「ランパート A」～Third　Party　小計画多数　　（米国外）

（判明）独、デンマーク、スウェーデン。（推定）仏、韓国、シンガポール。他

○　単独事業　　5計画　　（米国外）

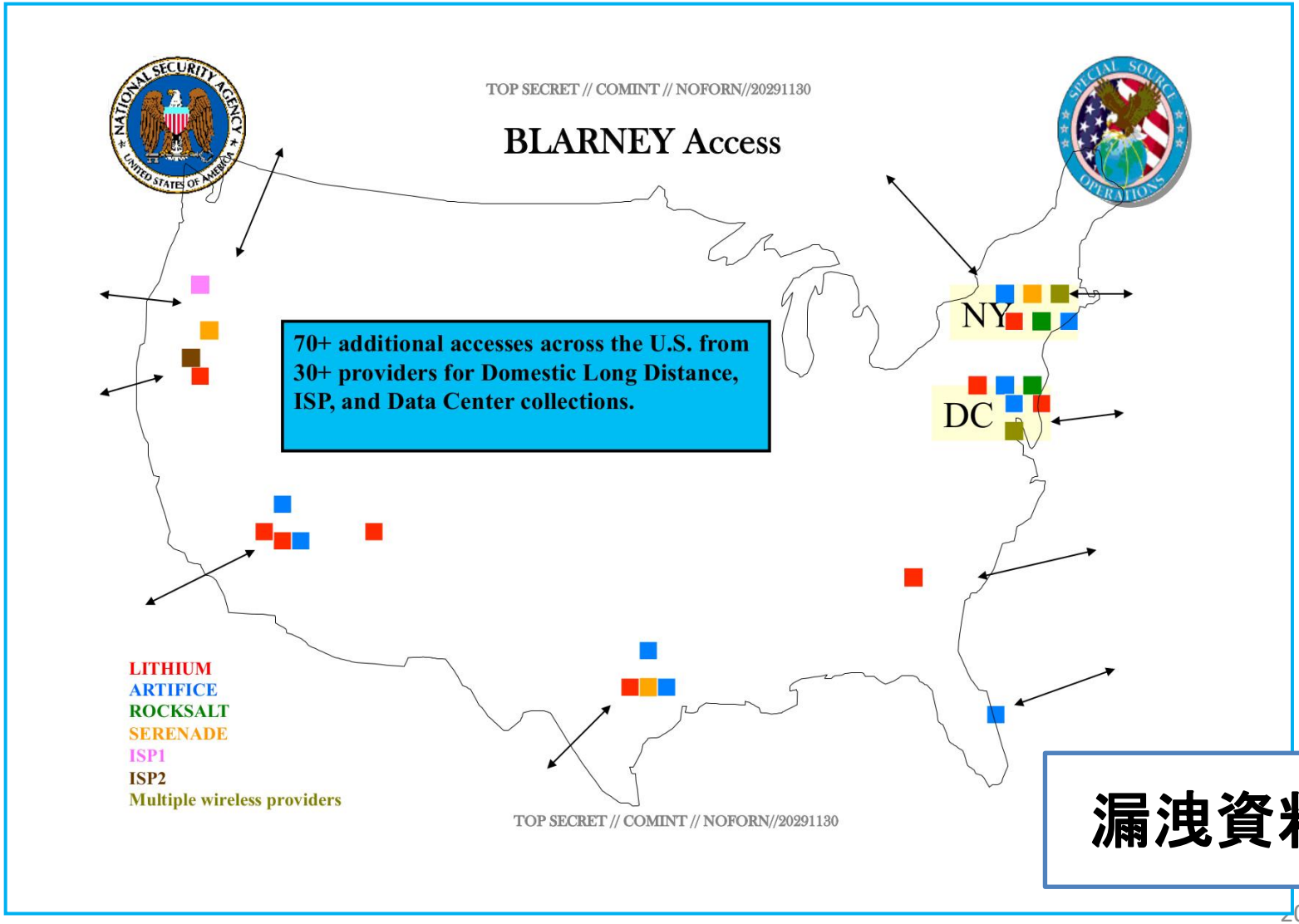
「ミスティック」　小計画5つ

「ランパートI/X」「ランパートM」「ランパートT」「名称不明」

2-2通信基幹回線②「ブラーニー」SSO・米国内

FBI、CIA、NSAが関与

企業30社以上、アクセス拠点70ヶ所以上



漏洩資料

2-2通信基幹回線③「インセンサー」UKUSA・英国

「ウィンドストップ」（UKUSA協力事業）の4小計画の1つ

「インセンサー」

- ○　英国内で英GCHQとの共同作業
  （2008年運用開始）
- ○　北米と欧州を結ぶ通信基幹回線を英国で傍受
- ○　協力企業7社　　～ケーブル＆ワイアレス、BT、
  ベライゾン、グローバルクロッシング、ヴァイアテル、
  レベル3コミュニケーションズ、インタルート
- ○　世界の全インターネット通信の1/4は英国経由
- ○　2010年GCHQ内部資料
  NSA以上にインターネットにアクセスし、
  NSA以上にメタデータを収集している。

2-2通信基幹回線④「ミスティック」単独・米国外

「ミスティック」

○　2009年開始。小計画5つ

通信事業会社の合法的商業サービスをカバー

麻薬取締局DEA、CIA、豪信号局ASDが仲介

○　実施国～バハマ（DEA）、メキシコ（CIA）、ケニア（CIA）、フィリピン（ASD）、アフガニスタン

○　バハマの例　（漏洩資料で裏付け）

国際犯罪捜査のためバハマ政府が傍受設備を設置。

DEA（麻薬取締局）が設置を支援。

携帯電話の全通話の内容とメタデータを30日間保存。

DEA～薬物取締で国外に80の事務所を展開

大統領令12333号により対外諜報任務も付与

2-3　外国衛星通信の傍受①

英国　メンウィズ・ヒル

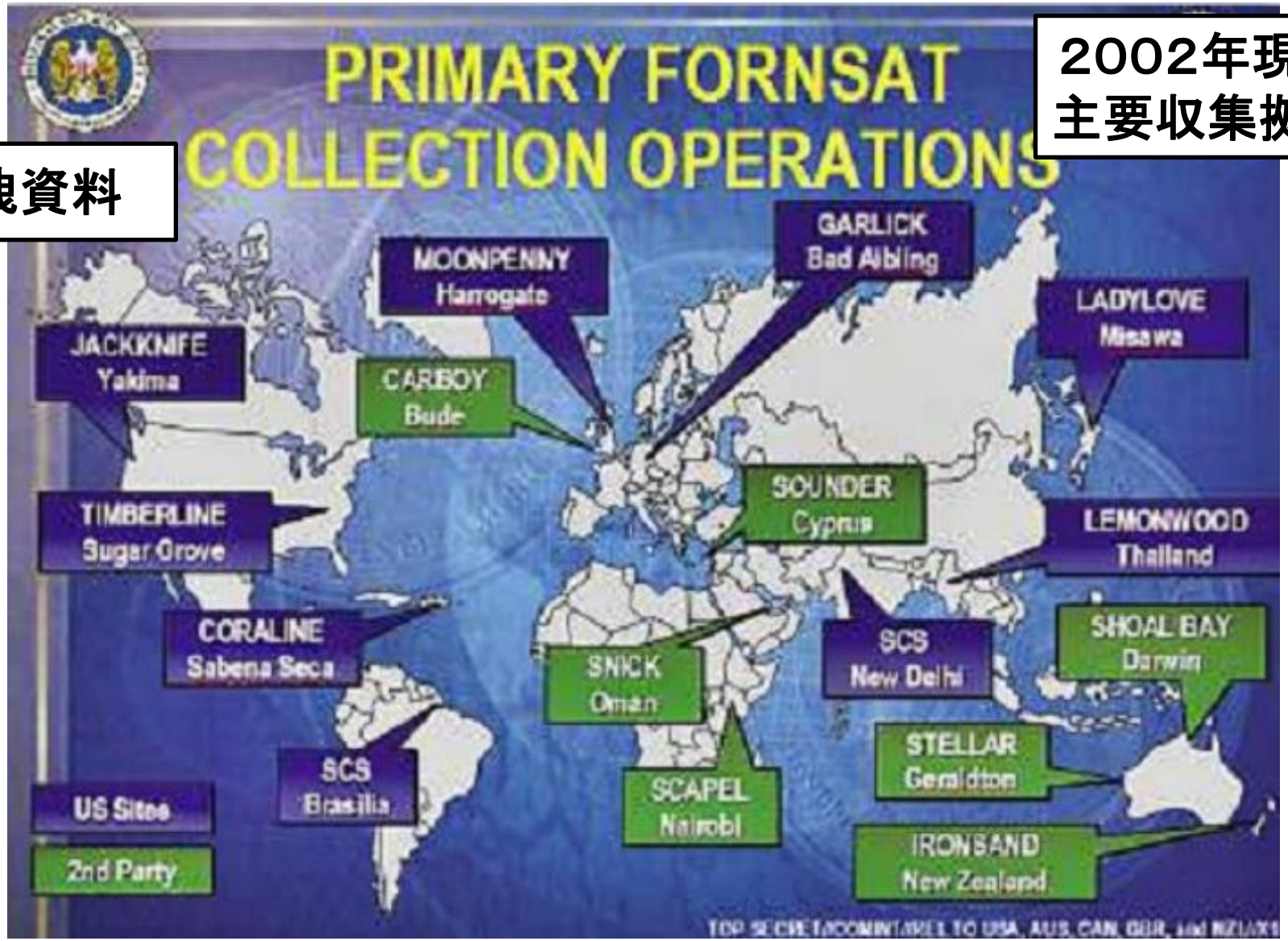
RAF Menwith Hill, from a helicopter by Mark Morton, CC BY-SA 2.0 , via Wikimedia Commons

主要傍受施設の一つ

2-3　外国衛星通信の傍受②

漏洩資料

2002年現在
主要収集拠点



2-3　外国衛星通信の傍受③

世界各地で衛星通信を傍受

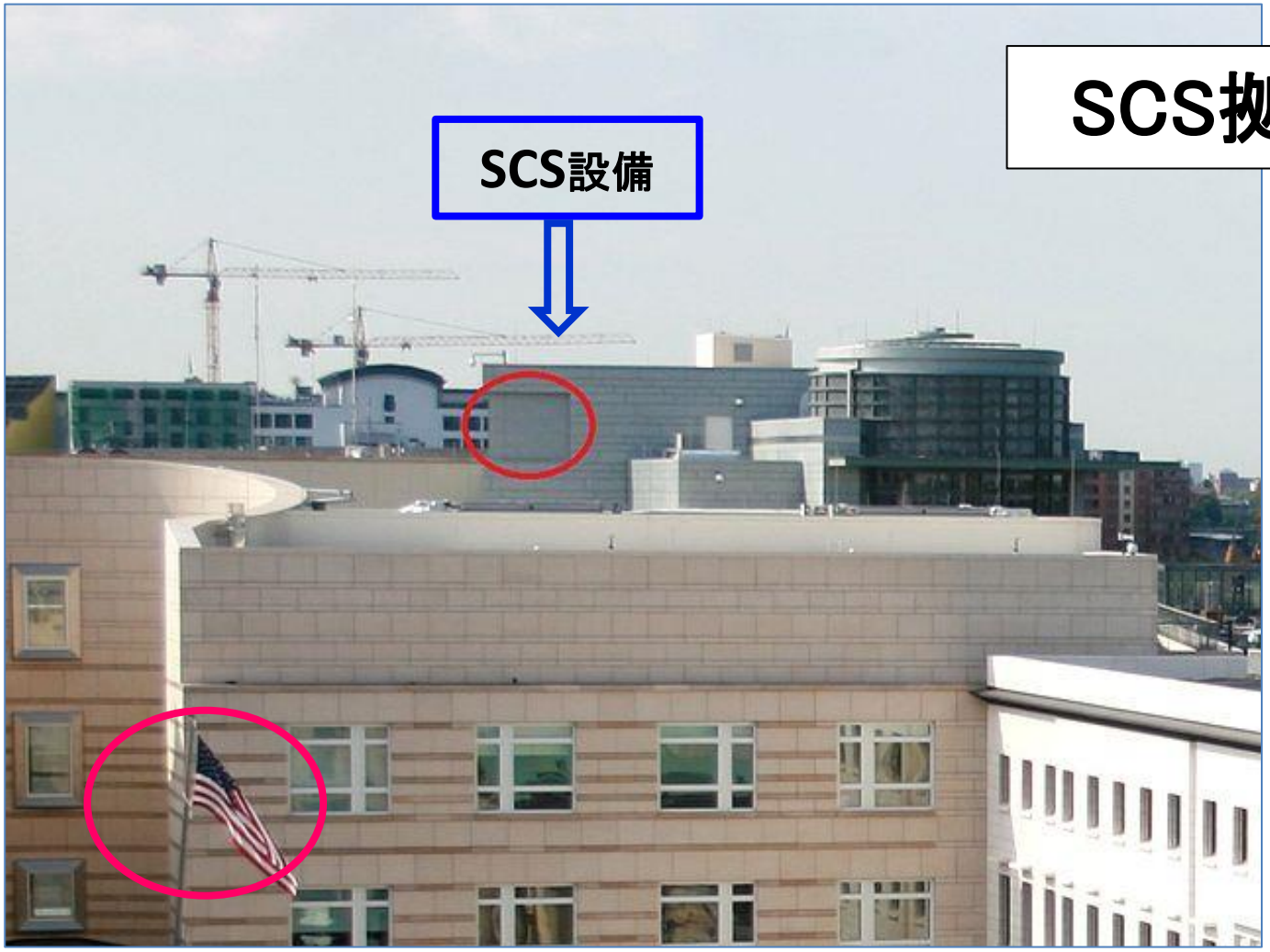
○　主要傍受施設　約10ヶ所

米本土　：　ヴァージニア州、ワシントン州
英国　　：　メンウィズ・ヒル（米）、ビュード（英）
中東　　：　キプロス（英）、オマーン（英）
アジア　：　日本・三沢（米）、タイ・コンケン（米）
大洋州　：　豪州・ジェラルドトン（豪）ショアルベイ（豪）

○　特別収集サービス　約40ヶ所

（大使館、領事館等）

2-4　特別収集サービスSCS　①



在ベルリン米国大使館

original photograph: usbotschaftberlinderivative work: PanchoS, Public domain, via Wikimedia Commons

2-4　特別収集サービスSCS　②

SCS（Special　Collection　Service）

- ○　CIAとNSAの共同事業　　1977年～
- ○　米大使館・領事館

  「ステートルーム」＋各種アンテナを偽装して設置
- ○　2010年現在　　世界　約80箇所

  内、欧州19（モスクワ、キーウ、ベルリン、フランクフルト、パリ、マドリッド、ローマ、プラハ、ジュネーブ等）
- ○　マイクロ波、衛星通信、WiFi等無線LAN、携帯電話
- ○　利点
  - ・　地理～敵対的空間の中のホームフィールド
  - ・　信号アクセス～Passive＋Active（侵入可能）
  - ・　分析～通信インフラ・システム、標的設定や標的行動の把握
  - ・　情報成果～国家的需要と地域的需要、現地情勢の背景知識、

「シギントを進めるヒューミント、ヒューミントを進めるシギント」

2-5　シギント衛星・機上収集①

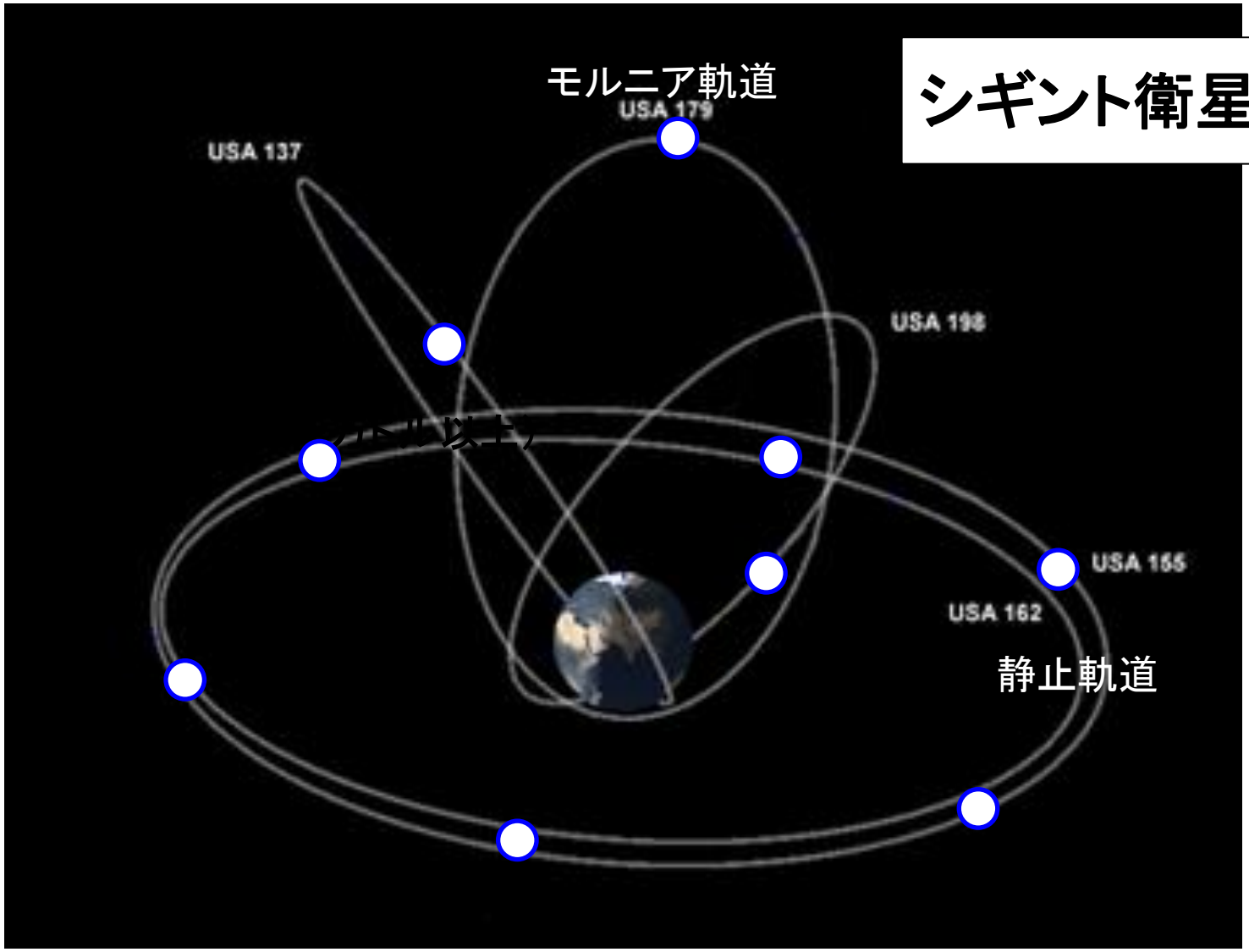


image Langbroek, software Tricarico, orbits McCants, CC0, via Wikimedia Commons

2-5 シギント衛星・機上収集②

○ シギント衛星

- 静止衛星 Orion　3機以上。～8機　アンテナ100m？

  マイクロ多重通信、HF、UHF。ミサイルのテレメトリー信号
- 長楕円モルニア軌道衛星　Trumpet　3機

  エリント信号主体。 アンテナ150m？
- 低軌道エリント衛星　Intruder　2機×５？

○ 機上収集

- RC-135

U.S. Air Force photo by Master Sgt. Lance Cheung, Public domain, via Wikimedia Commons

- 海軍EP-3E、陸軍RC-12、EO-5C/ARL-M他
- 無人飛行機　Global Hawk、MQ-9他

目　次

3-1　任務

TAO（Tailored Access Operations）

- 1997年発足　　2013年度定員1870人
- 所在地：本部（Fort Meade）

ROC（地域センター）ハワイ、ジョージア、テキサス、コロラド

☆ 主任務:CNE（Computer Network Exploitation）

① 標的システムへのアクセスを獲得する
② 標的システムからデータを取得する

○ 成果：システム侵入（マルウェア累計注入件数）

2008年　　2万1252件
2011年　　6万8975件　（運用）8,448件
2013年末計画　8万5000～9万6000件

☆ 操作員不要の自動運用システム開発中

☆ 付加任務：CNA支援、CND支援、秘匿CNA

（例）Stuxnet

3-2 組織

（1） 作戦実施部門

○ ROC（Remote Operations Center）

遠隔侵入（remote access, on-net）

○ AT＆O（Access Technologies & Operations）

物理的侵入（physical access, off-net, close access）

（2） 企画調整・開発・兵站部門

- R&T（Requirements & Targeting） 作戦の企画調整・管理
- ANT（Advanced Network Technologies）「ハッキング」ソフト・ハード開発
- TNT（Telecom Network Technologies） 通信網からのデータ収集技術開発
- DNT（Data Network Technologies） 標的との送受信システム開発ほか
- MIT（Mission Infrastructure Technologies）作戦用インフラの開発配備

（参考）ANT製品カタログ・漏洩情報

U.S. National Security Agency, Public domain, via Wikimedia Commons

TOP SECRET//COMINT//REL TO USA, FVEY

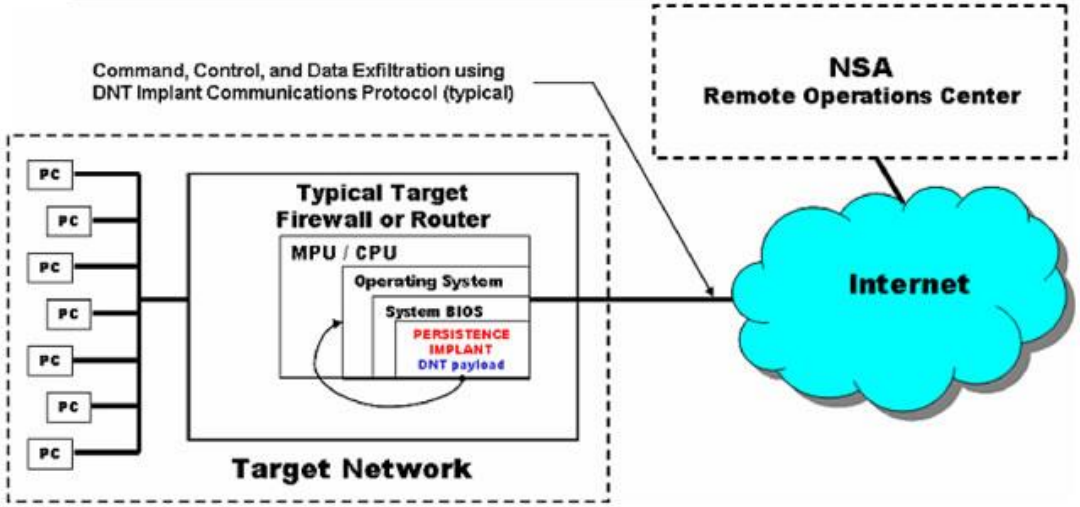
JETPLOW

ANT Product Data

(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant. JETPLOW also has a persistent back-door capability.

06/24/08

漏洩資料



(TS//SI//REL) JETPLOW Persistence Implant Concept of Operations

(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant and modifies the Cisco firewall's operating system (OS) at boot time. If BANANAGLEE support is not available for the booting operating system, it can install a Persistent Backdoor (PBD) designed to work with BANANAGLEE's

3-3　遠隔侵入①

（1）ROC（Remote Operations Center）のモットー

“Your data is our data, your equipment is our equipment –
anytime, any place, by any legal means.”
いつでも、　どこでも、　どんな手段を使っても

（2）主な手法

○　スパムメール　～今や成功率1%以下
○　Man-on-the-Side attack
　　～「クオンタム」諸計画
○　Man-in-the-Middle attack
　　～SecondDate

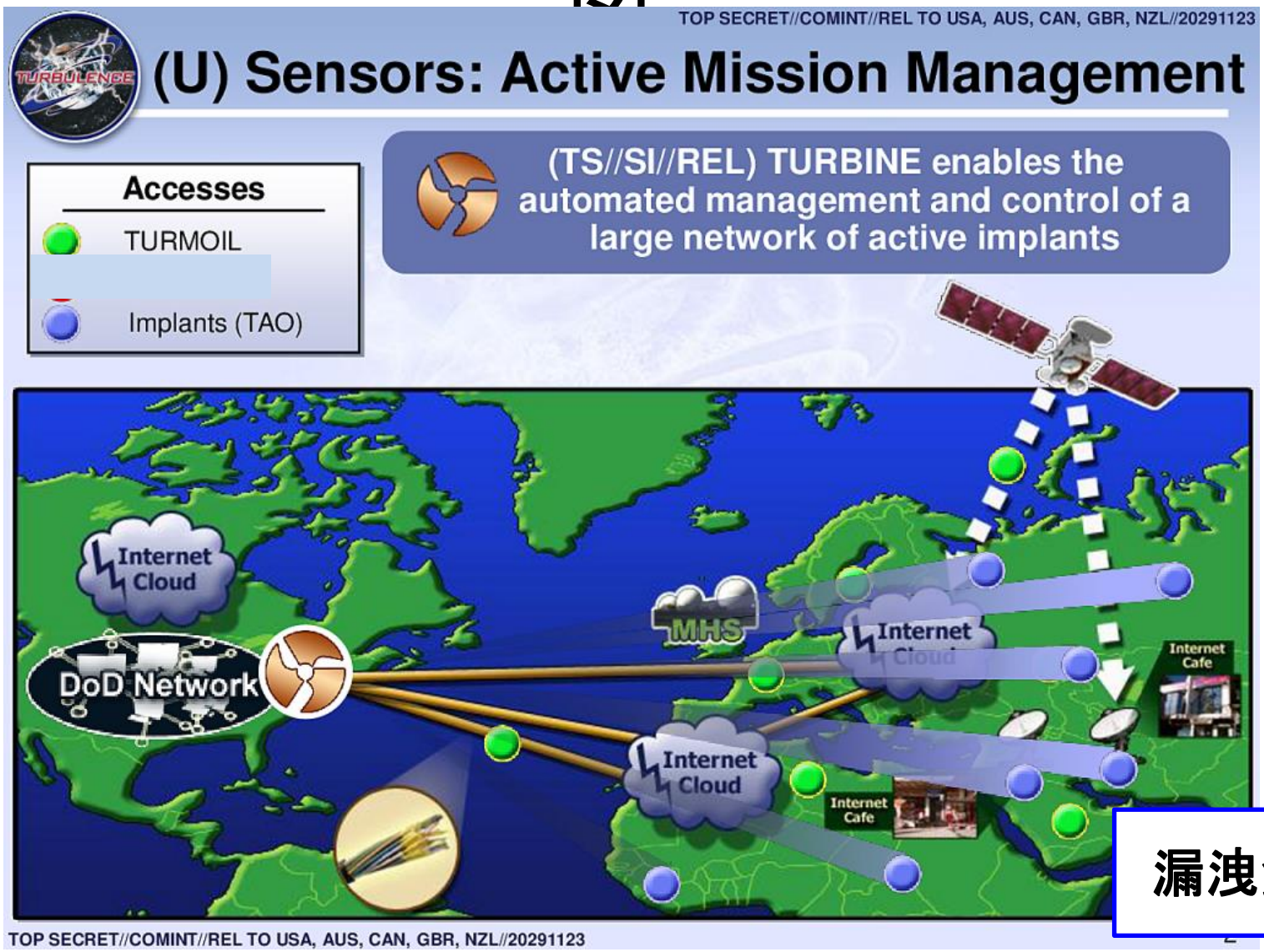
基本は、NSAの偽装サイトを訪問させること
「FoxAcid」サーバー：一見普通のドメイン名を持ち、
誰でもアクセス可能な偽装サーバー
標的とする端末が接続するとウィルス注入

（例）LinkedIn偽装サイト：インプラント注入成功率50%以上

3-3　遠隔侵入② FOXACIDサーバー

漏洩資料

3-3　遠隔侵入③「クオンタム」の概念図



漏洩資料

3-4　物理的侵入①

（1）　AT&O（Access Technologies & Operations）

○　FBI他ヒューミント機関の協力

○　隔離システムや遠隔侵入困難なシステム攻略

○　組織 Field Operations　～侵入実施部門

Access & Target Development～調査部門

Expeditionary Access Operations

～海外遠征チーム

（2）　手法

・　ハードウェア装入、ソフトウェア挿入

○　内部協力者工作

○　供給網工作～（製造）企業工作　Cavium製CPU

～配送経路介入

○　外国公館工作

3-4　物理的侵入② 供給網工作

○　供給網工作（配送経路介入）

(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.

漏洩資料

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon

NSA, Public domain, via Wikimedia Commons

3-4　物理的侵入③ 外国公館への侵入

○　米国内の外国公館（大使館、UN代表部）

対象：外国公館38と言われる。

判明分15ヵ国25公館　2010年現在　（EU、仏、伊、
ギリシャ、スロバキア、ブルガリア、ジョージア；
メキシコ、ブラジル、コロンビア、ベネズエラ；
日本、韓国、台湾、ベトナム、インド；　南アフリカ）

未判明13公館

○　収集手法

（例）「ミネラリズ」　LANにインプラント
「ハイランズ」 端末にインプラント
「バクラント」　コンピュータ・スクリーンのデータ読取
「ブラックハート」 FBIによるインプラント
「ドロップマイア」 レーザープリンターからの収集
「デューウィーパ」USB端末中継のワイヤレス侵入　他

目　次

4（1）シギント機関のCS任務

□ シギント機関がCSを所管

英： National Cyber Security Centre 2016年発足

加： Canadian Cyber Security Centre 2018年発足

豪： Australian Cyber Security Centre
2014年発足、2018年に強化一元化

NZ： National Cyber Security Centre
2011年発足、2017年に強化一元化

□ シギント機関がCSを支援：米NSA

全般：CISA（Cybersecurity and Infrastructure Security Agency）

NSA： 2019年 Cybersecurity Directorate設置
2020年 Cybersecurity Collaboration Center設置

人材提供（初代国家サイバー長官、現CISA長官、NSCのCS担当）

4（2）CSにはシギントが不可欠

CS（Cyber Security）にはシギントが不可欠。

- **○　シギントによる知見・技術**
  - **「攻撃方法を知る者が、良く防禦できる」**
    CNE（Computer Network Exploitation）
- **○　シギント・インフラの貢献**
  - **シギント・データ収集のためのインフラ**
    UKUSA：全世界に及ぶシギント・インフラ。X-Keyscore
  - **Attribution（攻撃者の探知特定）などでも威力を発揮**
- **○　C-CNE の貢献（攻撃阻止、反撃）**
  - **C-CNEにより個別具体的な脅威を事前に把握解明**
    （ハッカー集団をハッキングする）
  - **予め当該脅威に対する対抗手段を準備（積極防禦等）**

4（3）シギント機関のCS取組例①

（ア）指導・助言・警告　NSA

CS Advisories（助言）、Operational Risk Notices（脅威告知）

Tech. Reports（技術情報） Info. sheets（参考情報）

（イ）技術提供　NSA

Open Source @NSA （CSソフトウェア無償提供）

Cybersecurity Solutions Service（企業、研究機関等にに技術供与）

（ウ）教育研究　NSA

- ○　CS優秀教育機関・優秀研究機関の認定

  National Centers of Academic Excellence in Cybersecurity

  3種：CAE-CD（防禦）、CAE-R（研究）、CAE-CO（CNEを含む）
- ○　NSAサイバー演習（主対象：各種士官学校、商船大学）
- ○　NSA「セキュリティ科学イニシアティヴ」

4（3）シギント機関のCS取組例②

（エ）システム構築

- ○ 米NSA:　National Security Systemsの責任者
- ○ NZ・GCSB : Top Secret Networkの設計調達

（オ）事案対応　Incident Response　英NCSC

- ○ NCSC事案管理チーム（Incident Management team）
  CS事案を6区分。重要3区分はNCSCに指導グループ設置
- ○ CSサービス会社認定制度（2018年現在23社を認定）
- ○ 被害組織、サービス企業、NCSCの三者で協議対応
  シギント情報を活用。特別重大事案：NCSC職員現場派遣
- ○ 事例：2017年5月WannaCryマルウェア大量感染事案対応

（カ）Attribution（攻撃者の探知特定）支援　米NSA

- ○ 対処例：2014年「ソニー・ピクチャーズ」攻撃　NK

目　次

5-1 X-Keyscore①

世界150ヵ所
サーバー700以上

漏洩資料・2008年2月25日付

National Security Agency, Public domain, via Wikimedia Commons

5-1　X-Keyscore②

X-Keyscoreとは？

データの一次記憶装置、且つ分析支援システム

- ○　装置の構成：世界約150ヵ所、サーバー700以上
- ○　インターネットと通話の殆ど全ての活動を記録
- ○　データ保存期間　コンテンツ情報　３日
  メタデータ　　３０日
- ■　検索分析機能～NSA版「Google」
  ユーザーがインターネットで行う殆ど全ての情報活動を検索可能　（Eメール、ネットワーク閲覧、SNS活動、オンラインチャット、その他のインターネット活動）
- ○　リアルタイム傍受も可能
- ■　CS対策、Attributionでも貢献

漏洩資料 GCWiKi, “Cyber Defence Operation Legal and Policy”

5-1　XKeyscore③

■　検索分析～NSA版「グーグル」

- 「ストロング・セレクター」メールアドレス、IPアドレス、MACアドレス、電話番号
- 「ソフト・セレクター」「About」検索可能。キーワードや言語でも検索可能

＜使用例＞

- シリアからのPGP暗号通信を検索し、
  その中から情報価値のありそうな個別通信を抽出。
- パキスタンでのドイツ語通信を検索し、
  その中から情報価値のありそうな個別通信を抽出。
- 英語、中国語、アラビア語についてはコンテンツからの
  キーワード検索が可能。（例：特定人について言及した通信抽出）
- グーグルマップの検索利用状況から、テロ容疑者を抽出。
- 特定の単語で検索した者や特定のウェブサイトを検索した者の検索抽出。

5-2　宝地図

「宝地図」（Treasure Map）NSA版「Google Map」

世界インターネット地図（常に、何処でも、全ての端末を）

構成レイアー：　人的データ（Persona）
端末データ（Cyber Persona）
論理ネットワーク（ルータ、autonomous system）
物理ネットワーク
地理

情報源：　公開情報、学術情報、商業情報、シギント、IA

シギント～世界中の秘密サーバーから、
DNSサーバーに膨大な接続要求を継続的に発出して確認。

利用者：　米国インテリジェンス　＋　UKUSAシギント機関

5-3 Follow the Money

Follow the Money 部門

世界の大量の取引情報へアクセス、データベース化

“Tracfin” database:

2011年：1億8千万件の記録、８４％はクレジット取引

○ クレジットカード取引情報の取得

2009年 「Dishfire」計画、70の銀行から取引情報取得

クレジット会社の通信システムにも浸透

対象：VISA、MasterCard等の主要カード

○ 銀行間送金決済情報の取得

SWIFT（国際銀行間通信協会）のシステムに浸透

2006年以降、SWIFT情報に各種方法でアクセス

○ Bitcoinへの取組（2013年）

目　次

6-1　C-CNE例　①対中国

Byzantine Hades　中国CNE組織の解明

- 作戦グループ12以上
- （一例）Byzantine Candorグループ解明

2009年国防省ネットワークへの侵入をNTOCが検知

TAOが担当　　多くのhop pointsを経由

発信端末のIPアドレス変更

中国人民解放軍総参謀部第三部が使用する

ユーザーアカウントを特定。

関係IP事業者に侵入。次にman-in-the-middle攻撃

2009年10月　Byzantine Candorの5端末への侵入成功

グループの構成員、技術情報、取得データ、攻撃目標についての情報入手

6-1　C-CNE例　②対北朝鮮

対北朝鮮C-CNE能力

○　2010年取組強化

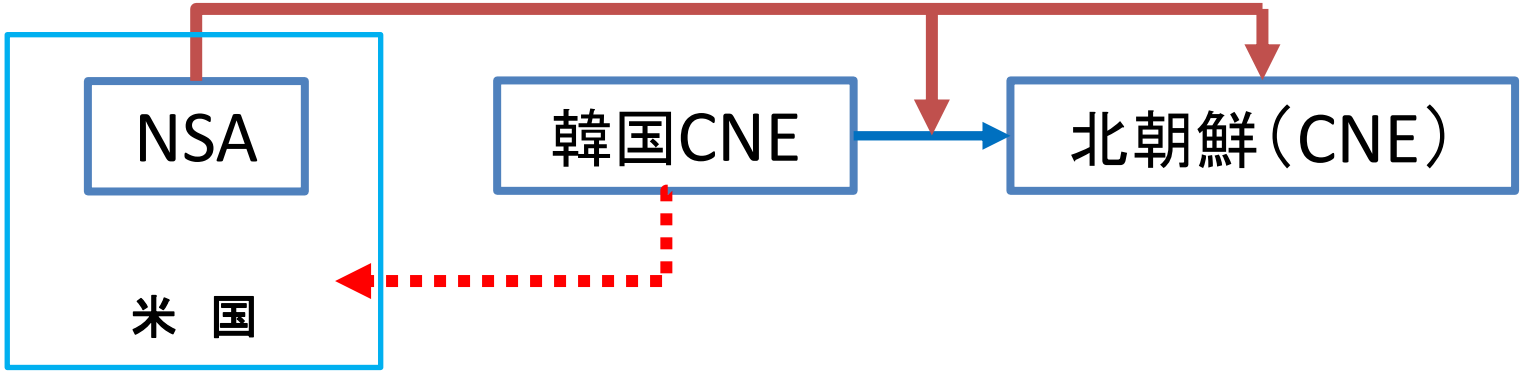
○　韓国のCNEネットワークに侵入

韓国による北朝鮮の複数端末への浸透を発見

これを利用し北朝鮮ネットワークへの収集態勢を構築

○　浸透した北朝鮮端末の幾つかはCNEに使用

北朝鮮のCNEも解明



＜報道によれば、在中国、在マレーシア、在NK・CNEに浸透＞

6-2 Attribution ①ソニー

「ソニー・ピクチャーズ」攻撃の解明（2014年）

6月　北鮮外務省、「インタビュー」は絶対容認できないと声明

11月24日　数千台の端末から全データ消去、情報漏洩開始

12月16日　「平和の守護者」
上映中止しなければ、更なる攻撃をと脅迫。

12月19日　FBI、北朝鮮の犯行と断定、広報。
「攻撃数時間後にはFBIに通報。　迅速な調査開始、
他省庁との協力により攻撃元を特定。北朝鮮政府に責任。」

NSAの貢献　2015年1月NSA長官、公開の会議で、
NSAの技術力とデータが貢献したと言明。

- X-Keyscore　～確実（2016年スノーデン・インタビュー）（関係漏洩資料）
- C-CNE　～推測　（・Gメールなどウェブメール）

（参考）2020年12月北鮮偵察総局員3名（Razarus, APT38）起訴。

6-2　Attribution例　②中国

中国国家安全部員2名外10名を起訴2018年10月

○　起訴：江蘇省国安局員2人、ハッカー6人、インサイダー2人

○　2010年～2015年、多数の企業からデータ窃取

○　主目的：仏米の企業が共同開発中のエンジン技術情報取

○　標的：仏企業と米・英・仏の部品製造会社のシステム

例：　スピア・フィッシング。ウェブサイト乗取り「水飲み場攻撃」

例：　蘇州市の仏企業従業員が、国安部員の要求により、USBドライブでマルウェアを感染させる。同社システムと工作用DNSサーバー間の通信を、米捜査機関が同社に通報。
同社IT・セキュリティ責任者（中国人）が、それを国安に通報。

○　中国：遠隔アクセスと物理的アクセスの併用。

○　起訴状に、国安部員Aと同Bの間の通信を引用記載。

NSA関与の可能性大。

6-3　脅威情報の事前把握インターネット空間

◆ACD「脅威情報の事前把握、接続点対抗措置の事前設置」

◆加Dynamic Defense：3要素を統合して実施

①インターネットとの接続点での防禦

②インターネット空間におけるシギント活動

③敵空間でのCNE（敵ネットワークの偵察、情報収集、道具の抽出）

◆EONBLUE　インターネット空間におけるシギント活動

- サイバー脅威探知センサー：世界に200以上設置。2010年頃。UKUSA諸機関の協力を得て、シギント・インフラを活用。
- 探知手法：signature-based detection（SNIFFLE）
  anomaly-based discovery（SLIPSTREAM）

◆英GCHQのLOVELY HORSE

ハッカーのブログやチャットルームなどソーシャルメディアでの議論を自動的に収集分類。（ハッキング技術の誇示、窃取データの公開など）

（参考）◆加CASCADE構想（2011年頃）sigint、CS統合壮大なシステム

6-3　脅威情報の事前把握敵空間Tutelage

- **米Tutelage System**

  【大前提】脅威把握　⇦敵のマルウェア開発準備段階で
  ツールと技術、意図と標的を探知する　⇦C-CNE

  2009年　米国防総省の情報システムNIPERNetに設置
  インターネット接続点～米国内7ヶ所、独2ヶ所、日1ヶ所

  2013年現在、脅威集団28に対して794の対抗策を事前設置
  [推定]当時、中国の12集団以上の内、7～8に浸透。

  対抗策：警告、インターセプト、代替、転送、遮断、遅延

  成功例：2010年国防総省高官に対するフィッシング攻撃阻止

- 2013年当時、独米会議でTutelage 導入について議論
- NZ・CORTEXシステム　2017年完成
- 米一般行政官庁用　Einstein 3　Tutelage導入予定であったが。

6-4　前進防禦Defend Forward

前進防禦（Defend Forward）

脅威がインターネット接続点に到達する前に防禦。
⇒敵空間、又はインターネット空間での先制防禦

◆「国家サイバー戦略」 2018年9月20日公表

「サイバー空間における悪意ある行動を探知し抑止する」

◆「国防総省サイバー戦略2018年」9月18日要旨公表

Defend Forward　+ 重要インフラなど民間部門も防衛対象

◆ 国家安全保障大統領メモ13号　8月　非公開　（報道）

「武力の行使」に至らないサイバー作戦の実施を国防長官に委任

「サイバー軍」 実績　　NSAによる支援

＜例＞2018年中間選挙Synthetic Theology作戦
露Internet Research Agencyのサーバー攻撃
（NSAとサイバー軍の合同チームで取組）

＜例＞2021年サイバー軍　REvil（ランサム）のウェブサイト遮断

6-4　前進防禦Defend Forward

NSAとサイバー軍と不可分な関係
＜NSA長官とサイバー軍司令官の兼任＞

- NSAによるサイバー軍支援
  - 専門技術・知識＋海外シギント・インフラ利用
    - （CNO＝サイバー軍の作戦基盤の提供）
- NSAとサイバー軍の共同作戦
  - 2018年中間選挙：合同チーム
    - defend forward（権限はサイバー軍）
- サイバー軍によるNSAへの貢献
  - hunt forward作戦
  - 外国コンピュータ網点検によるmalware収穫

目　次

７　終りに（１）日本の課題

- 国家シギント機関が存在しない。
  サイバー空間を対象とする
- 行政傍受権限が存在しない。
- 司法傍受権限が無いに等しい。
- 不正アクセス禁止法の問題
  国家安全保障目的の除外規定がない。
- **国民が問題点を知らされていない。**

7　終りに（2）国家シギント機関創設を

■　国家シギント機関の設置

- ○　防衛省に附置
- ○　National Intel. ⇔　Departmental Intel.との違い

  人事・予算・運営面における総理の代理人による統制

  職員人事権～専門家集団を実現
- ○　国家安全保障目的での情報収集活動の公認

  憲法「通信の秘密」は外国政府を守るためのものか。
- ○　国内での通過通信傍受、メタデータ収集権限付与
- ○　FYEY加盟を目指す

■　国家サイバーセキュリティセンター附置

専門家集団でなくては、CSの中核にはなれない。

（因みに）

■　CSS（Central Security Service）も必要

御清聴ありがとうございました。

参考資料

◆　もっと分かり易いYouTube
「チャンネルくらら」　　江崎道朗氏との対談
⇒「国家防衛分析プロジェクト」第７，８回
（全６回の予定中、２回分掲載）

◆　ウェブで読める参考資料（拙著）

- 「米国国家安全保障庁の実態研究」　警察政策学会資料2015年
- 「サイバーセキュリティとシギント機関
～NSA他UKUSA諸機関の取組」
情報セキュリティ総合科学2019年
- 「テロ対策に見る我が国の課題～欧米諸国との対比において」
警察政策学会資料2020年