NSAとUKUSAシギント同盟

2024年5月

茂田インテリジェンス研究室

https://shigetatadayoshi.com/

＜インテリジェンスの種類＞

＜機能＞

◇ ヒューミント（人的諜報）
human intelligence

◇ シギント（信号諜報）
signals intelligence

◇ イミント（画像諜報）
imagery intelligence

◇ マシント（計測・特徴諜報）
measurement and signature intelligence

＜主な組織＞（米国）

◆ 対外諜報機関
Central Intelligence Agency

◆ シギント機関
National Security Agency

◆ イミント機関
National Geospatial-Intelligence Agency

◆ 軍事諜報機関
Defense Intelligence Agency

◆ セキュリティ・サービス
FBI National Security Branch

シギント：　2023年4月のTeixeira漏洩情報の7割
インテリジェンスの女王

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6200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関連組織との関係

NSA
（1952年設立）

国家シギント
National intelligence

CSS
（1972年附置）

各軍シギントの調整
Military intelligence

サイバー軍
（2010年設立）

サイバー作戦指揮
Combatant Command

- 海軍
  第10艦隊
  =サイバー
- 海兵隊
  MCIA
  ・サイバー
- 空軍
  第16空軍
  =サイバー
- 陸軍
  INSCOM
  ・サイバー

（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

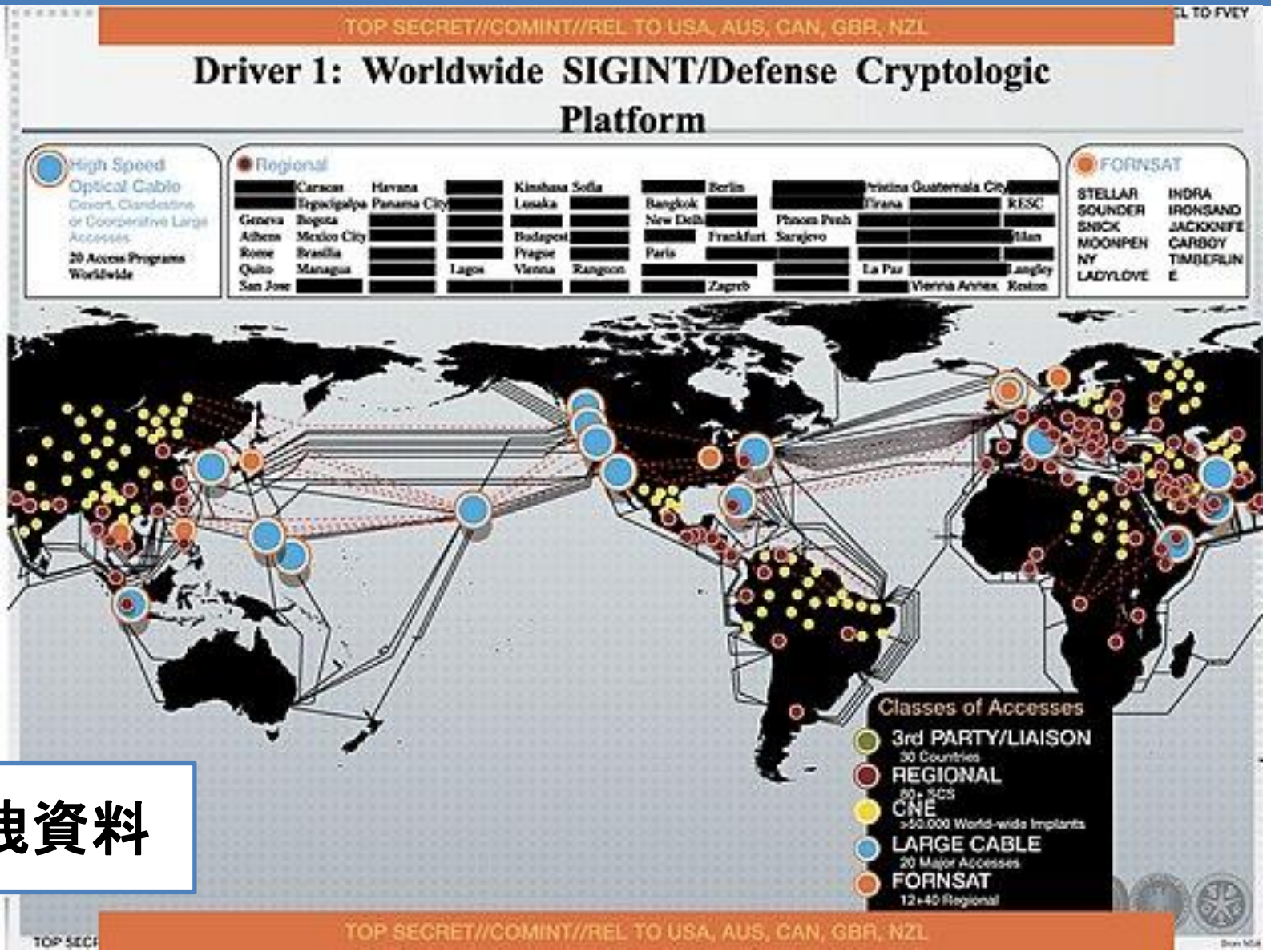
○　傍受施設～約500ヵ所

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



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

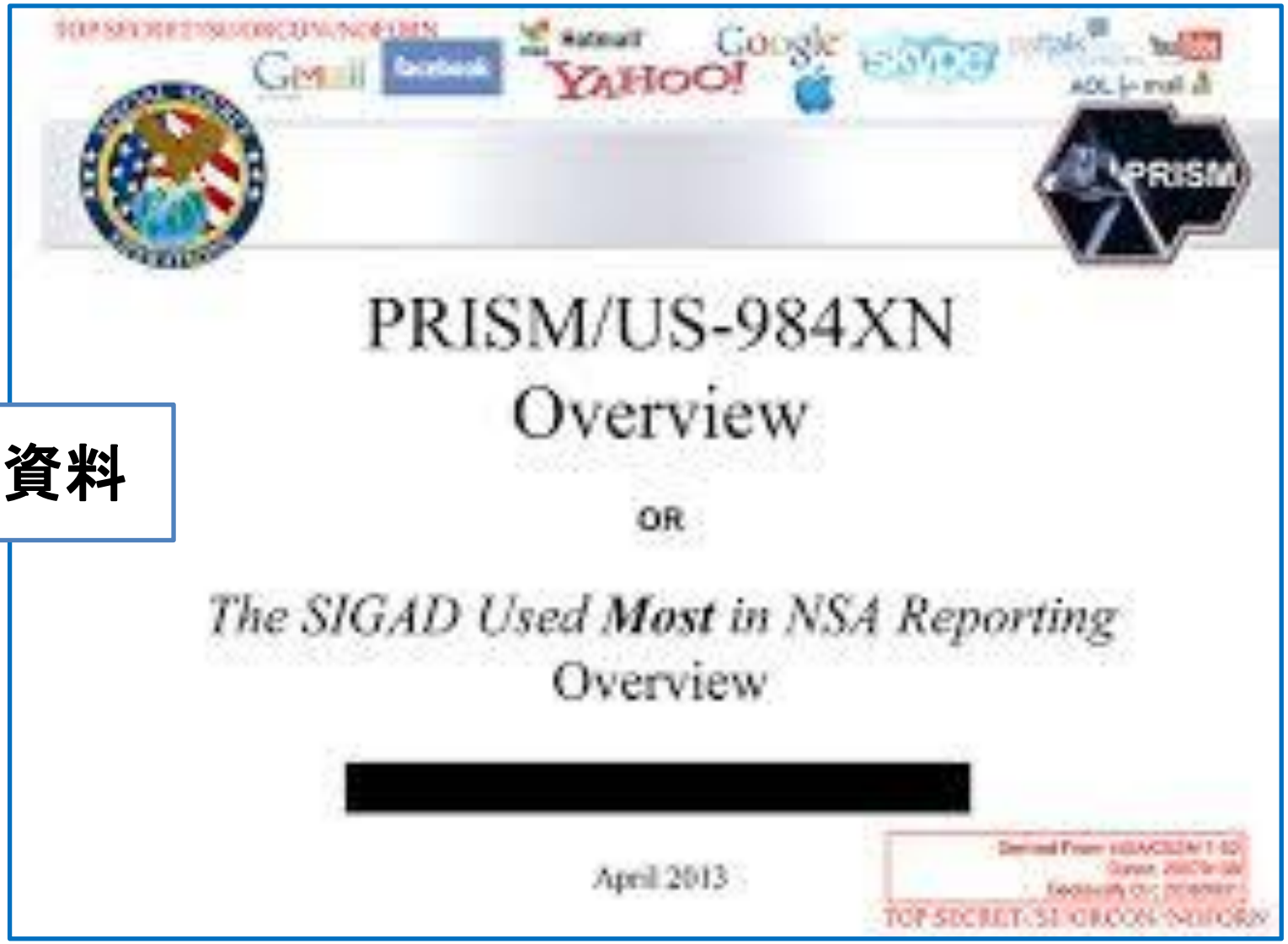
＜収集態勢総論＞（４）プラットフォーム

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

漏洩資料



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

参加企業は増加中

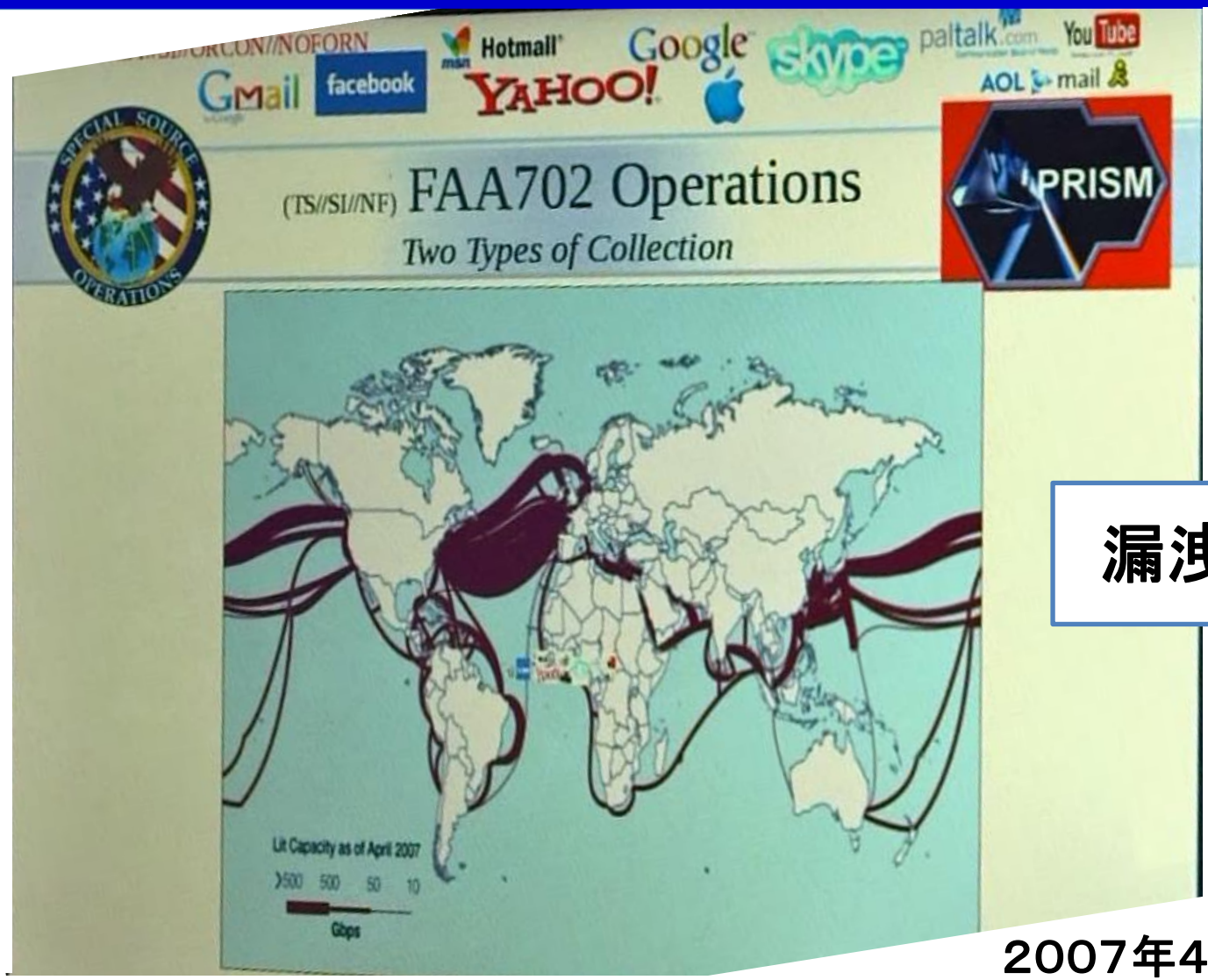
2007年　マイクロソフト
2008年　ヤフー
2009年　グーグル、フェイスブック、パルトーク
2010年　ユーチューブ
2011年　スカイプ、AOL
2012年　アップル

- ○ 取得情報

Gmail, Hotmail, yahoo mail

  - 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

（参考）世界のデータ通信量



漏洩資料

2007年4月現在

世界のデータ通信量（漏洩されたパワーポイント資料）

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）

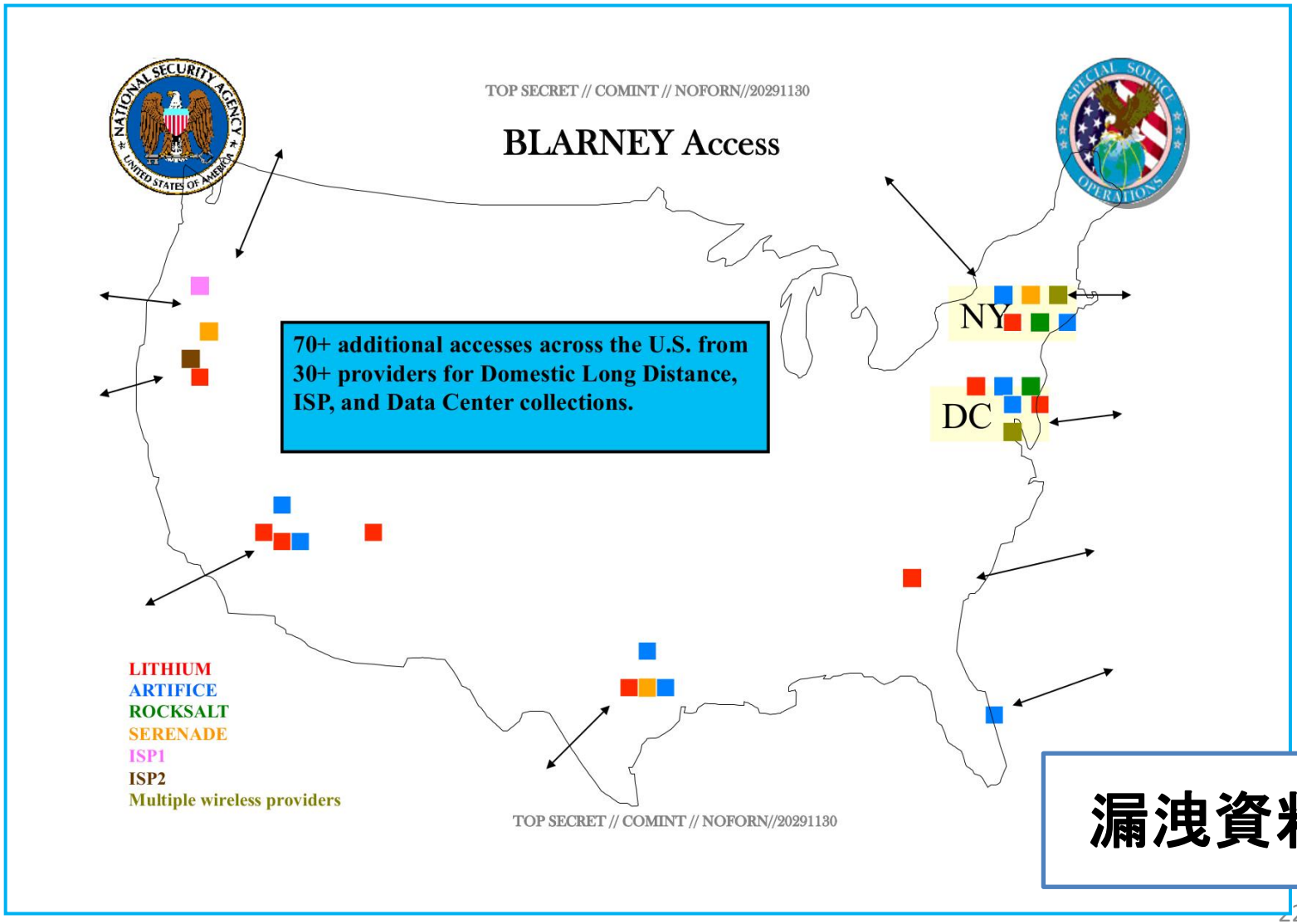
「ミスティック」　小計画5つ

「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

三沢基地

by Herry Lawford, CC BY 2.0
2.0 , via Wikimedia Commons

英国メンウィズ・ヒル

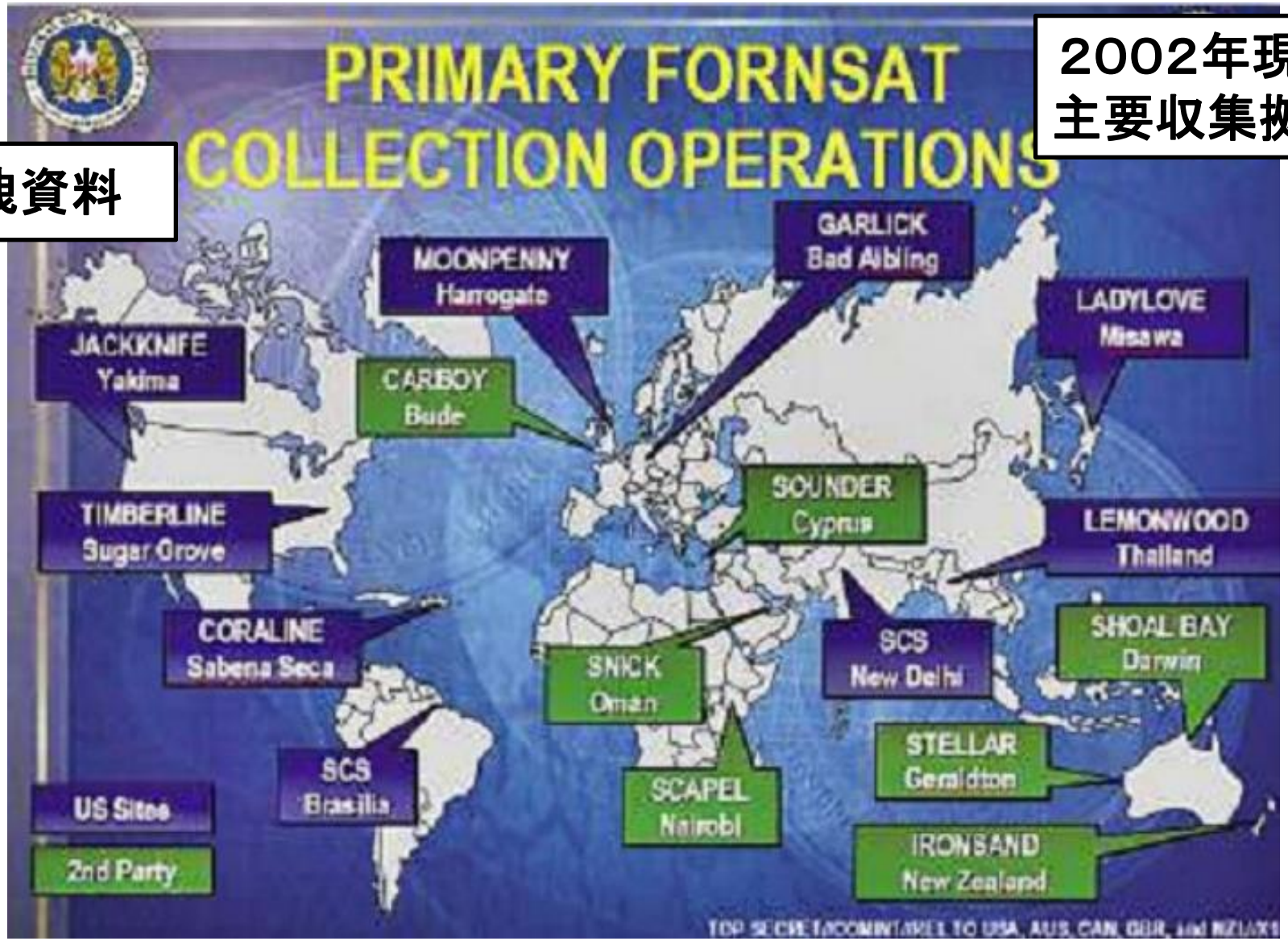
RAF Menwith Hill, from a helicopter
by Mark Morton, CC BY-SA 2.0 , via Wikimedia Commons

主要傍受施設例

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

SCS設備

SCS拠点

連邦議会

首相府

在ベルリン米国大使館

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

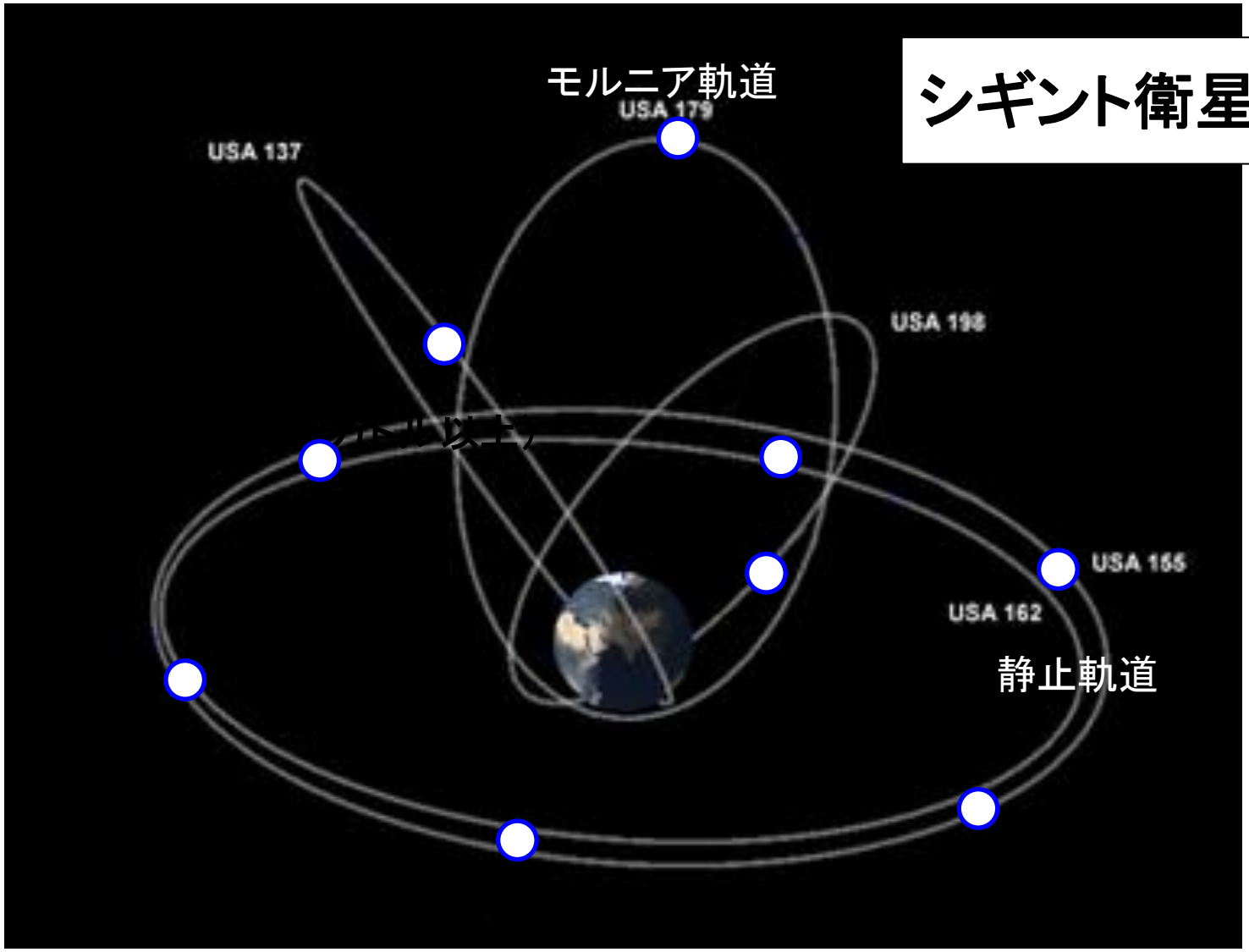


image Langbroek, software Tricarico, orbits McCants, CC0, via Wikimedia Commons

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

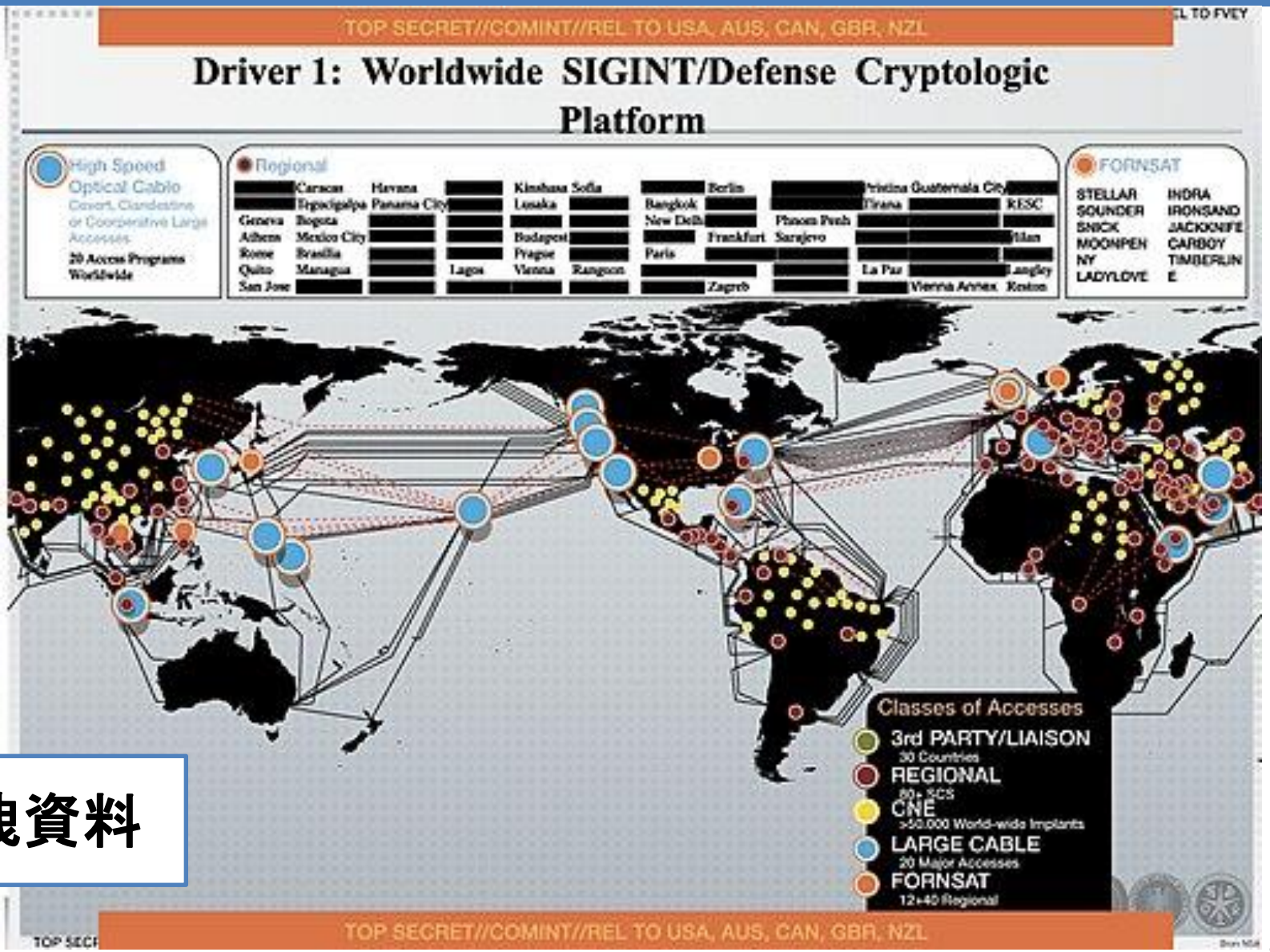
- RC-135

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

(参考)収集態勢・漏洩資料



漏洩資料

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

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）

地域本部：　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） 標的からの収集用ソフトウェア等開発
- 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

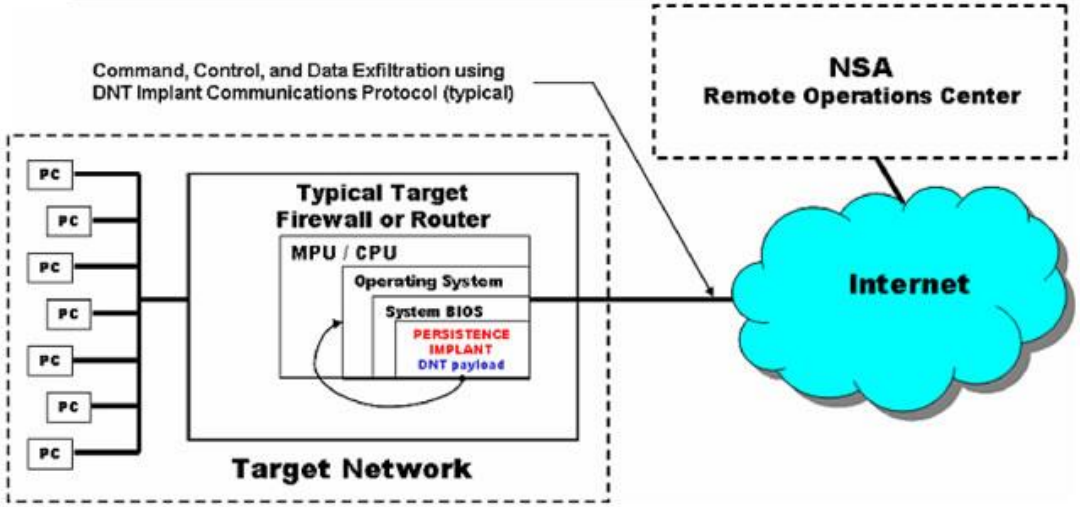
TOP SECRET//COMINT//REL TO USA, FVEY

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



(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

漏洩資料

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.”

（2）主な手法

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

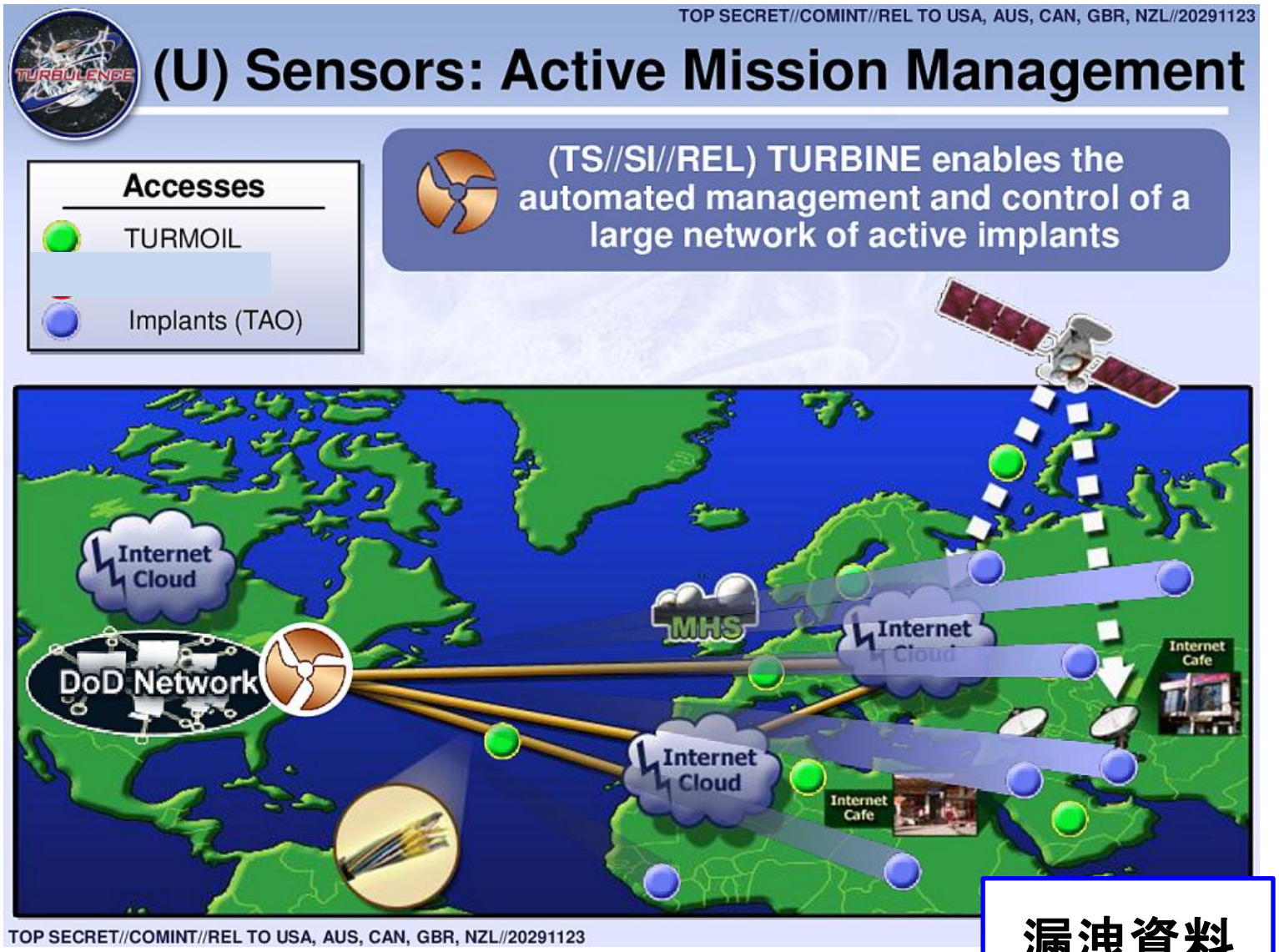
基本は、NSAの偽装サイトを訪問させること
「FoxAcid」サーバー：一見普通のドメイン名を持ち、
誰でもアクセス可能な偽装サーバー
標的とする端末が接続するとウィルス注入

（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
  ～配送経路介入
- ○　外国公館工作

Crypto AG
Cavium製CPU

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

3-5　C-CNE　①対中国

Byzantine Hades　中国CNE組織の解明

○（例）Byzantine Candorグループの解明

2009年国防省ネットワークへの侵入、NSA・NTOCが検知

TAOが担当　　多くの中継機を経由

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「中間者」攻撃

2009年10月　Byzantine Candorの5端末に侵入成功

解明:　グループ構成員、技術情報、

取得データ、攻撃目標

○　作戦グループ12以上　2010年7～8グループ解明

3-5 C-CNE ②対北朝鮮

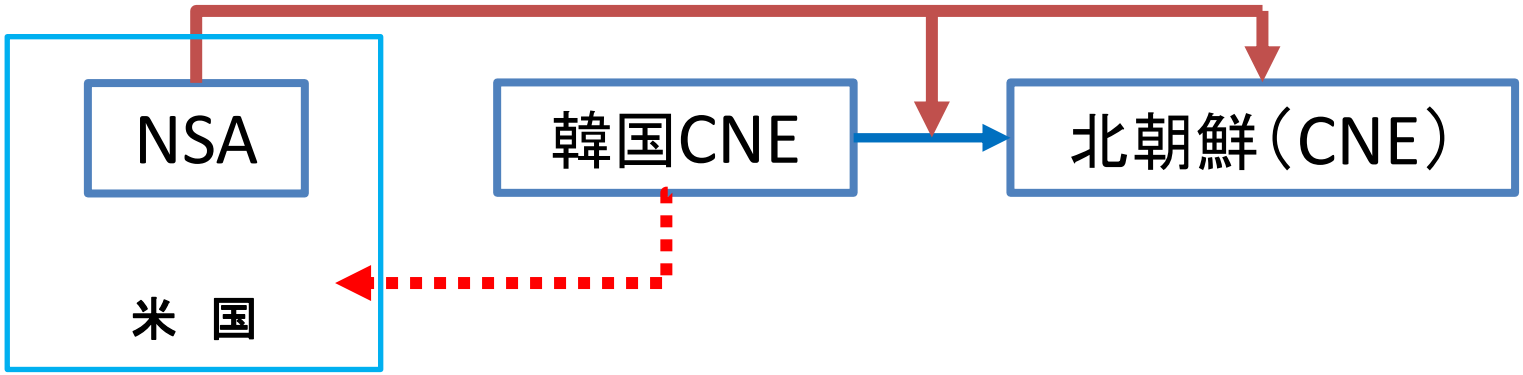
対北朝鮮C-CNE

○ 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のハッカー集団に浸透＞

目　次

4−1　X-Keyscore①

世界150ヵ所
サーバー700以上

漏洩資料

漏洩資料・2008年2月25日付

National Security Agency, Public domain, via Wikimedia Commons

4－1　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

■　一次記憶装置

・　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）

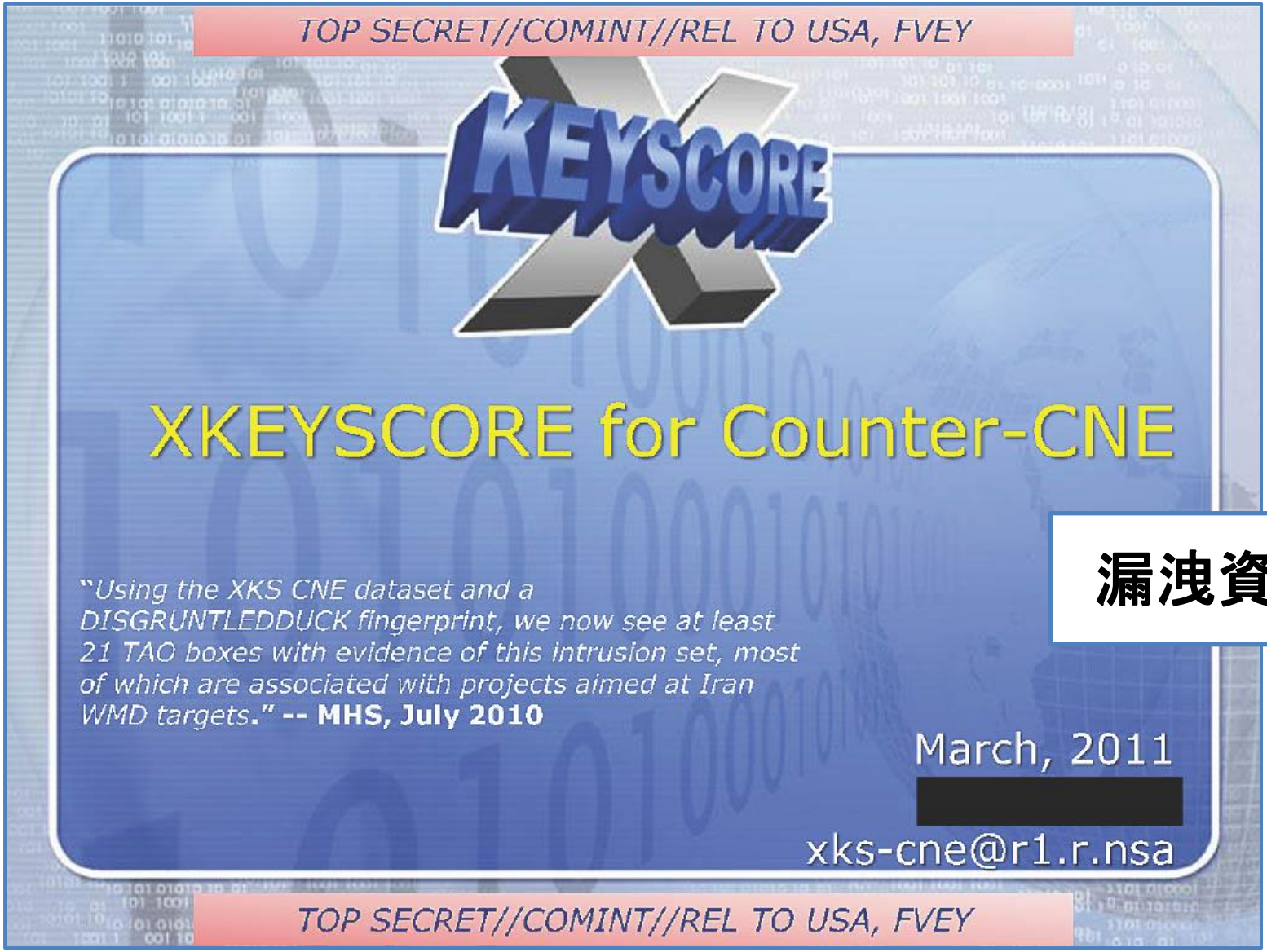
■　リアルタイム傍受も可能

○ CS対策、Attributionでも貢献

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

漏洩資料　NSA, “XKEYSCORE for Counter-CNE”

4−1　X-Keyscore③



漏洩資料

https://theintercept.com/document/xks-counter-cne/

4－1　XKeyscore④

■　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。

4-2　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

4-3　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）

4-4　メタデータ分析①

（1）メタデータとは ？

通信内容を除く通信に付随する情報全て

［電話］　電話番号、携帯端末識別番号（IMEI）、
契約者識別番号（IMSI）、番号通話時刻、通話時間、
テレホンカード番号、位置情報等

［インターネット］ Eメール活動（アドレス、IPアドレス、通信時刻）
ネットワーク閲覧履歴（訪問ウェブサイト、ログイン時刻、
地図検索等）
SNS活動、位置情報等

（2） どう使うか。

○　接触連鎖分析 （contact chaining）

○　人物分析　　ネットワーク閲覧履歴やSNS活動の分析

人の交友関係、団体活動、何時何処で誰とあったかなどを解明。
人物の全体像を把握可能。

※　現在は、民間企業が商業利用している。

4-5　位置情報DB：FASCIA

＜携帯電話の位置情報追跡システム＞

FASCIA（位置情報メタデータのデータベース）

- 世界中の携帯の位置情報を毎日50億件収集
  内、数億件以上を保存
- 位置情報：携帯電話特定の為の位置情報（DNR）
  ネットサービスの為の位置情報（DNI）
- 10以上の収集方法
  （1例）「Stormbrew」　～　ベライゾン
  通信会社の回線接続点27ヵ所から収集

＜利用例＞○　行動監視　：スパイ容疑者、テロ容疑者の行動監視
○　不審者の割出　：通信保全活動の自動検出
○　Co-Traveler分析　：同伴者、仲間の探知
○　Fast-Follower分析　：海外エージェントの追跡者探知

※　今や、民間商用サービス：IP　Geolocation

目　次

5-1 「ロイヤル・コンシェルジェ」①

漏洩資料

UK TOP SECRET STRAP1

ROYAL CONCIERGE

A SIGINT driven hotel reservation tip-off service

From: reservations@expensivehotel.com
To: new-target@mod.gov.xx

"Thank you for reserving……"

ROYAL CONCIERGE exploits these messages and sends out daily alerts to analysts working on governmental hard targets

What hotel are they visiting?
Is it SIGINT friendly?

An enabler for effects – can we influence the hotel choice? Can we cancel their visit?

We can use this as an enabler for HUMINT and Close Access Technical Operations

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]

https://www.spiegel.de/international/europe/gchq-monitors-hotel-reservations-to-track-diplomats-a-933914.html#fotostrecke-b8e68f93-0001-0002-0000-000000103860

5-1 「ロイヤル・コンシェルジェ」②

- ○ 政府高官のホテル予約の探知通報プログラム
  - 2010年試験実施（成果あり）
  - ホテルからの予約確認メールを自動的に探知
  - 対象：世界中の高級ホテル350
    （例：チューリッヒ、シンガポール）
  - GCHQ担当官に通知
- ○ 探知後の対処法
  - 電話、ファックス、コンピュータの監視「友好的ホテル」
  - “Technical attack”　特殊技術者派遣
  - 借上車（ハイヤ）への工作
  - ヒューミント発動　（ホテルのバー？）

5-2　2009年ロンドンG20での取組①

○　英国GCHQの取組の概要

- 2009年4月首脳会合、９月財務相・中銀総裁会合
  （世界金融危機対処のための重要会議）
- ブラウン首相承認下、通信傍受を大々的に実施。
  開催国として主導権を発揮するため。
- コンピュータの監視、Eメール・電話傍受
- 情報成果は速報性を重視、
  英国の関係閣僚に速報。
- 評価：画期的なインテリジェンス能力を行使。

5-2　2009年ロンドンG20での取組②

○　成果

- インターネット・カフェの設置
  Eメール通信を傍受＋ログインID・PW等入手
- 携帯電話「ブラックベリー」に浸透。情報化。
- 誰が誰と電話をしているか、24時間ライブ監視。
  分析官45人態勢。リアルタイムでグラフ化。閣僚に速報。
- メールアカウントへの侵入（当事者より前に閲覧）

（例1）露大統領のモスクワとの衛星暗号通話の
傍受解読レポートをNSAから受領。

（例2）南ア外務省のコンピュータ網に侵入し、
大臣への事前説明資料を入手。

（例3）トルコ財務相と随行団の監視強化

5-3 オンライン秘匿活動①

「現実世界やサイバー世界で何かを起させる」

サイバー空間における積極工作 Online Covert Action

（１）取組状況

- 2010年時点、ＧＣＨＱの全作戦の５％
- 2011年9月 資格制度と教育制度を創設。取組強化
- 担当部署:「人間科学作戦班」。
- 2012年計画：2013年初め迄に150人以上要員養成。
  他に500人以上に基礎教育を行う。
- 専用のソフトウェアも開発

（２）活動の場　広汎

フェイスブック、ツイッター、SMS、リンクトイン
ウェブ・ペイジ、ブログ、Ｅメール、ニュース・メディア
IRC（チャット）、電話通話

5-3　オンライン秘匿活動②

（３）活動類型＜妨害活動＞

（ア）通信妨害（技術的妨害）

○　携帯電話に大量のデータ送付、事実上、利用不能に。

（イ）コンピュータを使用不能に（技術的妨害）

○　Ambassadors Receptionウィルス（ワイパー型）

○　DDOS攻撃　（アノニマス・グループのチャットルーム）

（ウ）個人の信用を毀損（情報作戦）

○　ハニー・トラップ（ポルノサイトや実際の売春地区への誘込み）

○　被害者を偽装してブログ掲載（特定人攻撃）

○　同僚、隣人、友人に、本人に関する否定的メッセージを送付

（エ）会社の信用を毀損（情報作戦）

○　他の会社やマスメディアに「秘密」情報の漏洩。

○　否定的な情報を適宜な場に掲載。

（オ）対象組織の中に不和の種を蒔く（情報作戦）

5-3　オンライン秘匿活動③

（４）活動類型＜影響力活動＞

（ア）世論調査の結果操作、世論形成に影響

〇アクセス水増し　〇ペイジビュー水増し　〇ヒット件数・順位操作

（イ）他国に「秘密」（偽情報）を信じさせる

〇対象国が浸透しているコンピュータに「秘密」情報を保管する。

〇対象国が監視しているネットワーク経由で「秘密」情報を送付。

（ウ）外国ジャーナリストを利用して情報を流布させる

（５）活動類型＜オンライン・ヒューミント＞実例

（ア）フォークランド諸島維持のための作戦（2009年～）

（イ）ハッカーの特定と逮捕（2011～2012年）

※　ジンバブエ選挙工作（ムガベ大統領2013年選挙落選工作）

目　次

6-1　まとめ

■　シギントはインテリジェンスの女王　⇒皇帝

現代は、「シギントの黄金時代」

○　情報収集力ではNo1　　（例）テシェイラ漏洩情報

○　特別工作（影響力作戦、積極工作、認知戦等）でも主役に

■　テロ対策でもNSAが主役

■　サイバーセキュリティでも不可分の関係

○　UKUSA諸機関が対策の主役

■　サイバー軍事作戦でも

シギント機関の支援が必要

6-2　テロ対策

□　元米国家テロ対策センター長

マイケル・ライター

「NSAが傑出した選手或いは中心選手で
なかったテロ調査というのは思い付かない。」

「NSAほどアルカイダの内部状況について
知見を与えてくれたものはなかった。」

＜参考＞

- 「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」
  警察政策学会資料第113号（2020年11月）
- 「オサマ・ビンラディンを追え（上）（下）―テロ対策におけるシギントの役割」　季刊現代警察第156号、第157号（啓正社、2018年）
  ウェブサイトからアクセス可能

6-3　サイバーセキュリティ対策

□　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）

6-4　我が国の課題

- **国家シギント機関が存在しない。**
- 行政傍受権限が存在しない。
- 司法傍受権限も無いに等しい。
- 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。
  - 憲法の「通信の秘密」は誰を守るためのものか。
  - 外国政府や外国ハッカーを守る結果。
- **国民が課題を知らされていない。**

参考資料

◆ シギント入門
- 江崎道朗氏との対談本『シギント』（ワニブックス）
- もっと分かり易い？YouTube　江崎道朗氏との対談
  「チャンネルくらら」 ⇒「国家防衛分析プロジェクト」第7回以降

◆ ウェブで読める参考資料

茂田インテリジェンス研究室ウェブサイト　⇒著作へ
- 「米国国家安全保障庁の実態研究」2015年
- 「ウクナイナ戦争の教訓～我が国インテリジェンス強化の方向性」（再訂版）2023年
- 「Teixeira漏洩情報に見る米国のインテリジェンス力」2023年

以上、警察政策学会資料
- 「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

◆ 最近の論考
- 「善戦支える諜報機関　露宇戦争からの教訓」 諸君2月号

御清聴ありがとうございました。

１　NSAとUKUSAシギント同盟

２　シギント収集態勢

３　TAO（Computer Network Operation）

４　米国の特徴的なシステム

５　英国の興味深い活動

６　まとめ