米国国家安全保障庁と サイバーインテリジェンス（1）
～NSAと収集態勢～

2020年12月

日本大学　危機管理学部
茂田忠良

インテリジェンス諸機関

	セキュリティ・サービス	ヒューミント	シギント	イミント	軍諜報
米	**FBI** 国家安全保障局	**CIA** **中央諜報庁**	**NSA** **国家安全保障庁**	**NGA** 国家地理空間諜報庁	**DIA** **国防諜報庁**
英	**セキュリティ・サービス** **安全保障局**	**SIS** **秘密諜報局**	**GCHQ** **政府通信本部**	**国防省DIJE**	**DIS** **国防諜報局**
豪	**ASIO** **豪安全保障諜報局**	**ASIS** 豪秘密諜報局	**ASD** **豪信号局**	**AGO** **豪地理空間諜報局**	**DIO** **国防諜報局**
加	**CSIS** 加安全保障諜報局	—	**CSE** **通信安全保障局**	国防省地理空間諜報局	？
独	**BfV** 連邦憲法擁護庁	**BND**（連邦諜報局）			**MAD** **軍諜報局**
仏	**DGSI** **対内安全保障総局**	**DGSE**（対外安全保障総局）			**DRM** **軍諜報局**
日	警備警察？ 公安調査庁？？	—	防衛省情報本部 電波部	**内閣衛星情報センター**	防衛省 情報本部

構　成

今回（１）NSAと収集態勢

次回（２）サイバーセキュリティ対策

参考：

『国家安全保障庁の実態研究』（2015年9月・警察政策学会資料82号）

『サイバーセキュリティとシギント機関』（2019年11月・情報セキュリティ総合科学）

目　次

1　シギント情報例①

[2012年5月22日]　Global Sigint Highlights：Executive Edition＜フランス＞

「仏大統領、ユーロ秘密協議を承認、独野党と会談」

「オランド仏大統領は、ユーロ危機、特にギリシャのユーロ離脱問題を議論するため、パリにおける一連の秘密会議の開催を承認した。

5月18日仏大統領はエロー仏首相に、翌週エリゼ宮で秘密会議を開催するよう指示した。会議参加者は大統領、首相、関係閣僚であり、議題はフランス経済特にフランスの銀行に対する影響である。

また、仏政府と独社会民主党との間の秘密会合をパリで開催する予定である。大統領はエリゼ宮での開催を指示したが、首相は大統領に対して外交問題にならないように秘密厳守を警告した。

オランド大統領は、昨週ベルリンでメルケル首相と会談したが、会談は単なる見世物であり、実効ある成果がなかったと不満を述べていた。オランドは、メルケルは『財政協定』に固執して、ギリシャを突き放しており妥協の姿勢がないと見ている。そのため、ギリシャ国民は極端な政党に投票するかも知れず、ギリシャ情勢を大いに危惧している。メルケルとの会談後、オランドは独社会民主党ガブリエル党首と連絡して、協議のためパリに招待した。」

1　シギント情報例②

[2007年4月18日] Global Sigint Highlights：Executive Edition＜日本＞

「日本―炭素排出量の2050年半減目標を提言」

「安倍首相の4月26、27両日の米国訪問の準備に関して、経済産業省は、気候変動について米国が同意できる単純なメッセージを準備したいと考え、次の三原則を提案した。即ち、技術開発、省エネと原子力、将来の枠組への全ての国々の参加。

これに対し、外務省は、首相が米大統領との首脳会談で、5月発表予定の『安倍イニシアチブ』の一部として、2050年までの炭素排出量の半減目標に言及して欲しいとの立場である。

外務省は、当初、半減目標については、米国は賛成しそうにないので事前に通知しないことを考えていたが、安倍首相に対する官邸での事前説明において、事前に米国に通告の上、日米首脳会談で半減目標について言及することが決められたようである。」

目　次

２　UKUSAシギント同盟　①構成国

Five Eyes: FVEY

米：　NSA国家安全保障庁

（約５万５千人。100億ドル以上）

英：　GCHQ政府通信本部（約６千人、15億ボンド程度）

加：　CSE通信安全保障局　（約２千人、5億加ﾄﾞﾙ程度）

豪：　ASD豪信号局　（約２千人）

NZ：　GCSB政府通信安全保障局

（430人、1億5千万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

２　UKUSAシギント同盟　②経緯

- 1940年　4月　英米諜報協力を協議
- 1940年12月　英米シギント協力で合意
- 1941年　2月　実務レベル協力開始
  （ロンドン、シンガポール）
- 1946年 3月　BRUSA協定締結（British−USA）
- 1954年　　UKUSA協定（UK−USA）と改称
- 他の3国の正式参加　FVEY（Five Eyes）
  加　～　1949年（CANUSA協定）
  豪、NZ～1956年（UKUSA附属文書J1記載）
- 2010年　UKUSA協定・情報開示

目　次

３　NSA概観　（１）沿革①

NSA（National　Security　Agency）

国家安全保障庁

1952年トルーマン大統領の秘密命令で設立

ブラウネル委員会

人員7600人、国家諜報機関として設立

（国家諜報機関を目指して設立）

“No　Such　Agency”　存在しない役所

1975年まで存在自体が秘密

最も秘密度の高い組織

３　NSA概観　（１）沿革②

☆　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　サイバー軍編成

NSA長官が司令官兼務

サイバー戦争とシギントは密接に関連

３　NSA概観

NSA関連ロゴマーク

サイバー司令部

NSA

CSS

（各軍シギント組織）

３　NSA概観　（２）組織予算①

○　職員：2013年定数　3万4901人（軍人1万4950人）

（2018年報道正規職員3万８千人＋契約1万7千人）

加えて、陸海空軍・海兵隊・沿岸警備隊の

シギント組織を指揮下（CSS）に

○　予算　：

2020年度諜報機関予算

国家諜報予算＋軍諜報予算＝合計

627億ドル　　231億ドル　　858億ドル（約9兆円）

2013年

シギント予算＝NSA108億＋NRO＋軍予算他

総計、200億ドル、2兆円規模？

３　NSA概観　（２）組織予算②

○　本部：メリーランド州フォートミード（DC郊外）

○　地方本部4つ（Cryptologic Center）

ハワイ州　　オアフ島ワヒアワ

ジョージア州　（オーガスタ）フォートゴードン陸軍基地

テキサス州　（サンアントニオ）ラックランド空軍基地

コロラド州　（オーロラ）バックレー空軍基地

○　欧州シギントセンター（独ダルムシュタット近郊）

○　収集拠点　500ヵ所

３　NSA概観　（２）組織予算③

☆　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。

☆　基本法令　　大統領命令第12333号
国家安全保障法

３　NSA概観　（３）任務

○　任務

①　シギント　　矛（攻撃）

②　情報保証(Information Assurance)　楯（防禦）

秘密が守れて、使い易い情報システムの提供

←（少し前）情報システム保全　INFOSEC

←（もっと前）通信保全　　COMSEC

National Security Systems

③　コンピュータ・ネットワーク・オペレーション

CNO（＝サイバー戦争）の基盤の提供

目　次

４（１） 協力企業

○ 協力企業～約80社以上

マイクロソフト、インテル、IBM、オラクル、ベライゾン、ATT、
シスコ、モトローラ、HP、EDS、クアルコム、キューウェスト他

○ 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
「プリズム」や通信基幹回線からの収集ではSSOが中心。
NSAの収集するデータの内、コンテンツ情報の60%、
メタデータ情報の75%近くを占める。
スノーデン曰く。「SSOはNSAのcrown jewel」

４（２）サード・パーティ　①諸国

○　サード・パーティ諸国　（2013年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、インド、日本、台湾、パキスタン　（主要国は、シンガポール、韓国）

○　多国間協力枠組

- アフガン・シギント連合
- 欧州シギント首脳会議
- 太平洋シギント首脳会議（UKUSA+仏＋下線部国）

４（２）サード・パーティ　②関係

- 第三国関係の本質：パートナー＆標的
- 協力関係の基本：ギブ＆テイク

＜テイク＞

① 地理的特性からする重要標的通信へのアクセス
② 地理的分析能力、特殊言語能力
③ 兆候・警告情報の収集に関する協力支援

＜ギブ＞

① シギント技術（ハードウェア、ソフトウェア、技術）
② 地域全体、全世界についてのシギント情報

- 協力関係の進展は、「米国の国家諜報要求が、第三国の国家諜報要求と交叉する場合」

目　次

５（１）シギント戦略　2012年

2012年2月23日付シギント戦略2012～2016年

［背景］○　世界の相互依存と情報化時代の到来

→　シギント活動領域の劇的拡大

→　現在はシギントの黄金時代

The golden age of SIGINT

［目標］

○　シギント技術の向上と自動化を進めて、

世界ネットワーク支配を劇的に拡大する

dramatically increase mastery of the global network

○　必要なシギント・データを

誰からでも、何時でも、何処からでも取得する

from anybody, anytime, anywhere

５（２）シギント戦略的任務リスト2007年①

＜任務分野別の重要標的＞

① テロ情報：テロに対する世界的戦争に勝利する

② 米国国土安全保障

③ 大量破壊兵器とBCN物質の計画と拡散

④ 海外展開中の米軍の安全と作戦支援

⑤ （特定の）国家の安定及び政治的安定

⑥ 戦略的核ミサイル脅威に関する警告情報

⑦ 地域紛争・危機と戦争発火点

（紛争や危機に拡大し得る地域的緊張）

⑧ 情報作戦（サイバー空間の支配と米国の重要情報システムへの攻撃防止）

５（２）戦略的任務リスト②

⑨　軍近代化：外国の軍の近代化計画を早期把握

⑩　戦略的科学技術：軍事、経済、政治面で戦略的優位となり得る重要科学技術：日本

⑪　外交政策：米国の外交的優位を確保する：日本

⑫　エネルギー安全保障

⑬　米国に対する諜報、防諜、欺瞞・心理活動
：イスラエル、フランス、韓国

⑭　薬物と国際的犯罪の組織・ネットワーク

⑮　経済的安定と影響力
（米国の経済的優位と政策戦略を確保する。）：日本

⑯　世界の信号状況の認識
（中核的通信インフラ及び世界的ネットワークに関する情報）

５(３)　法令上の収集根拠①

○　大統領命令第12333号　～基本法令

○　対外諜報監視法105条FISA1978年

○　TRANSIT(通過通信)～大統領命令第12333号

○　対外諜報監視法702条FAA2008年改正

参考：拙著『米国における行政傍受と解釈運用』(2017年警察政策学会資料)

5（3） 法令上の収集根拠②

連邦憲法修正第4条（令状主義）の解釈

☆ 対外諜報の為の情報収集に関しては、令状主義は適用されない。

☆ 米国政府が適正に保有している情報の利用には、令状主義は及ばない。～対外諜報のために適正に収集した情報は、犯罪捜査目的での使用に制限がない。

☆ 国際テロ対策やスパイ対策において、脅威が存在しこれを阻止する目的がある限り、捜査利用目的があっても、対外諜報監視法による行政傍受が許される。

☆ メタデータには、プライバシーの期待権が生じない。

～通信事業に対して任意に提供した情報であるから。

（英国もドイツも同じ）

目　次

６　収集態勢

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

　　Xkeyscoreの設置場所数

（参考） XKeyscore

漏洩されたパワーポイント資料・2008年2月25日付

６　収集態勢

NSAの主要な収集態勢

（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）　SCS（特別収集サービス）

（５）　CNE（コンピュータ・ネットワーク資源開拓）

（６）　シギント衛星・機上収集　Overhead

（７）　従来型収集（無線通信の傍受）Conventional

（８）　秘匿シギント活動　CLANSIG

６　収集態勢

世界のデータ通信量（漏洩されたパワーポイント資料）

６　収集態勢の目次

6－1 「プリズム」計画①

- ○ SSO（特別資料源作戦）の一つ
- ○ 対外諜報監視法702条による協力命令
- ○ 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

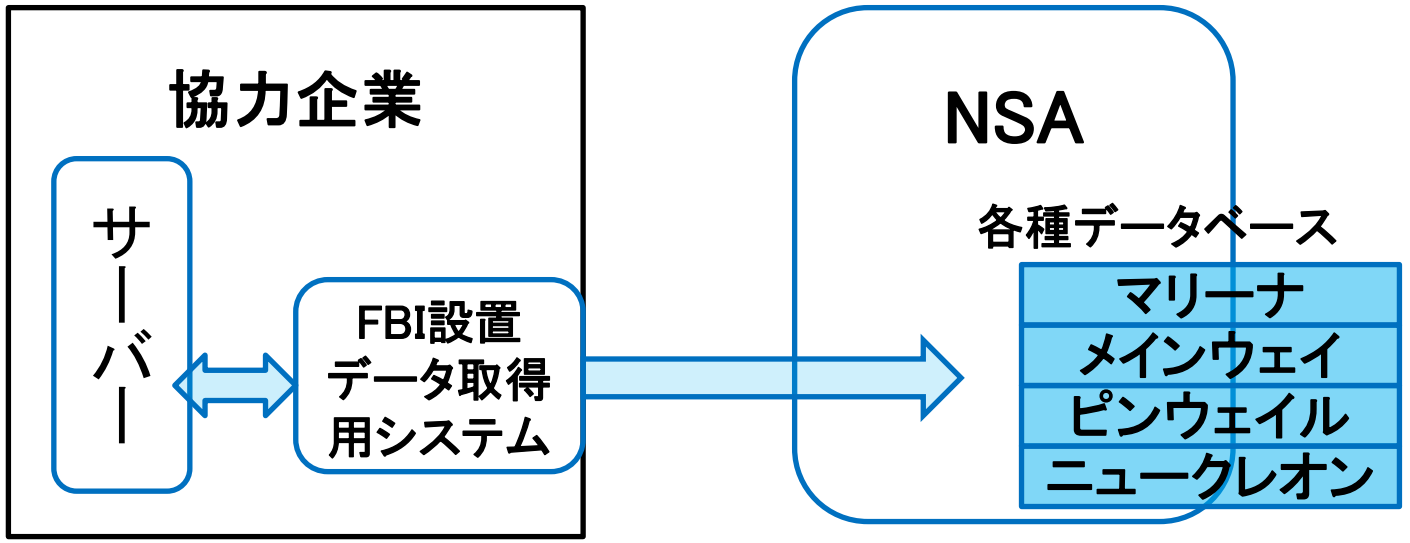
  2012年　アップル

6－1　「プリズム」計画②


TOP SECRET//SI//ORCON//NOFORN
Gmail
facebook
Hotmail
YAHOO!
Google
PRISM Collection Details
PRISM
Current Providers
What Will You Receive in Collection
(Surveillance and Stored Comms)?
It varies by provider. In general:
Microsoft (Hotmail, etc.)
Google
Yahoo!
Facebook
PalTalk
YouTube
Skype
AOL
Apple
E-mail
Chat – video, voice
Videos
Photos
Stored data
VoIP
File transfers
Video Conferencing
Notifications of target activity – logins, etc.
Online Social Networking details
Special Requests
Complete list and details on PRISM web page:
Go PRISMFAA
TOP SECRET//SI//ORCON//NOFORN

6－1 「プリズム」計画③

○ 内容：協力企業のデータセンターから
必要な情報を検索取得できる。



○ 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

（参考）2013年中に約2億5千万件以上のデータを取得

6－1 「プリズム」計画④

☆ 少ない費用で効果絶大

- ○ NSA最大の情報報告の源
- ○ NSAの情報報告の１／７近くがプリズム由来
- ○ 大統領デイリー・ブリーフィング

  2012年プリズムによるもの1477件
- ○ 運用経費　年間2千万ドル（約20億円）

☆ 理由

- ○ インターネット通信のホストコンピュータの多くは米国内
- ○ 米国内データセンターの存在
- ○ 米国が世界のインターネット通信の中心 （2013年当時）
  - ・ 世界の大陸間通信容量の2/3以上
  - ・ 実際の通信の90%は米国経由とも言う。

６　収集態勢の目次

6―2　通信基幹回線

A　企業協力　　4計画

「ブラーニー」　（国内）

「フェアビュー」「ストームブリュー」　（国内）

「オークスター」　（殆ど国外）

B　UKUSA＆サード・パーティの協力　2計画

「ウィンドストップ」～UKUSA諸国（セカンド・P）（国外）

「ランパート A」～サード・P　（国外）

C　単独事業　　5計画　（国外）

「ミスティック」

「ランパートI/X」「ランパートM」「ランパートT」

名称不明の1計画

6-2　A（1）ブラーニー米国内

○　FISA105条の令状による収集

実際は1970年代初めから

○　協力企業～30社以上。

アクセス拠点は、全米70ヶ所以上。

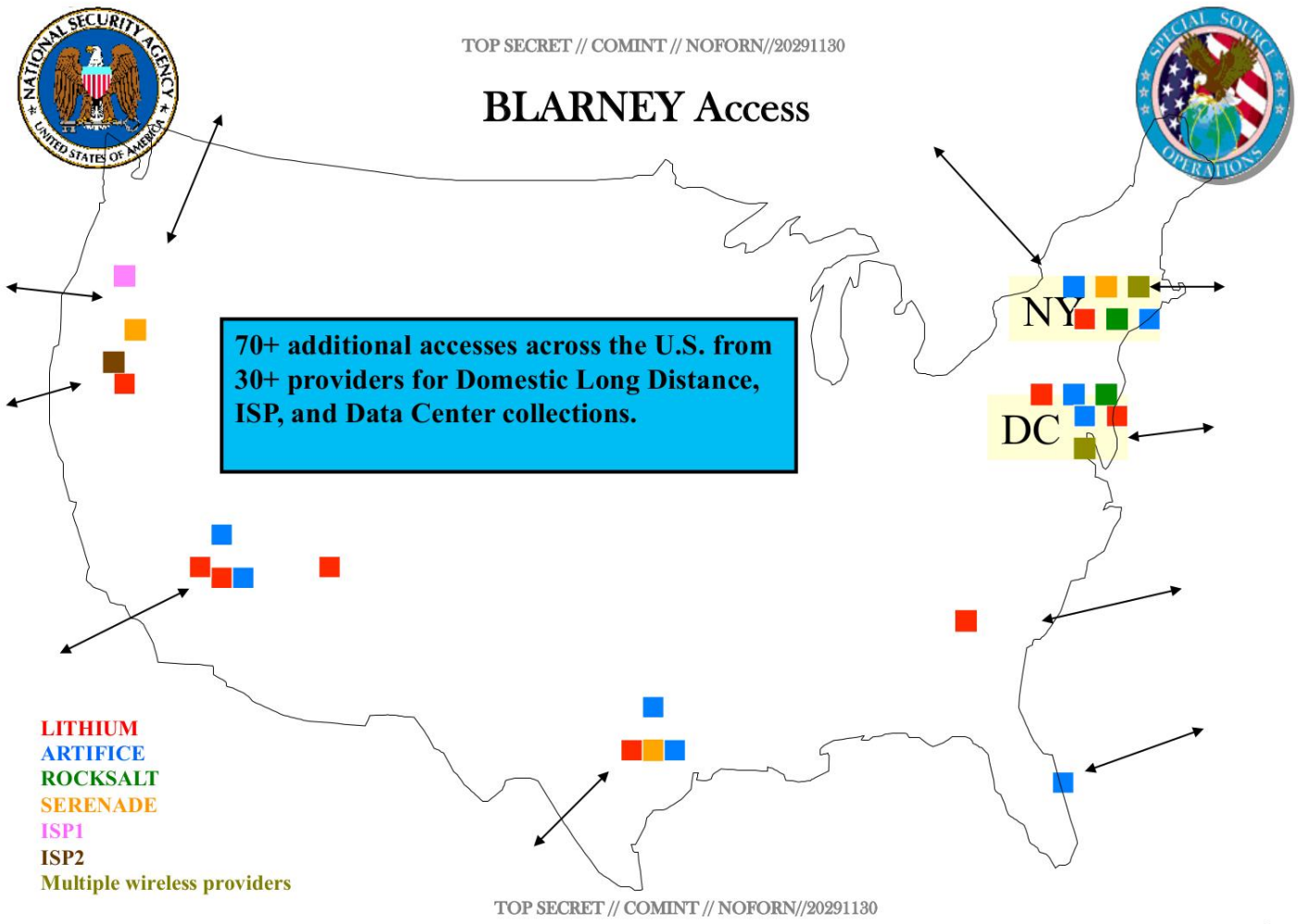
○　対象～外交施設、外国政府のエージェント、
テロリストなど

（例）2010年時点の標的は、42カ国・組織（順不同）

露、中、北朝鮮、韓、独、仏、伊、日本、イラン、イラク、
シリア、レバノン、サウディ、イスラエル、エジプト、
インド、パキスタン、国連、IMF、世銀、日銀、他

（携帯電話通話、スカイプ通話、ビデオ会議等も）

6-2 A(1)ブラーニー米国内



6-2　A（2）Fairview，Stormbrew米国内

○　通過通信とFAA702条による収集

○　協力企業　Fairview～ATT

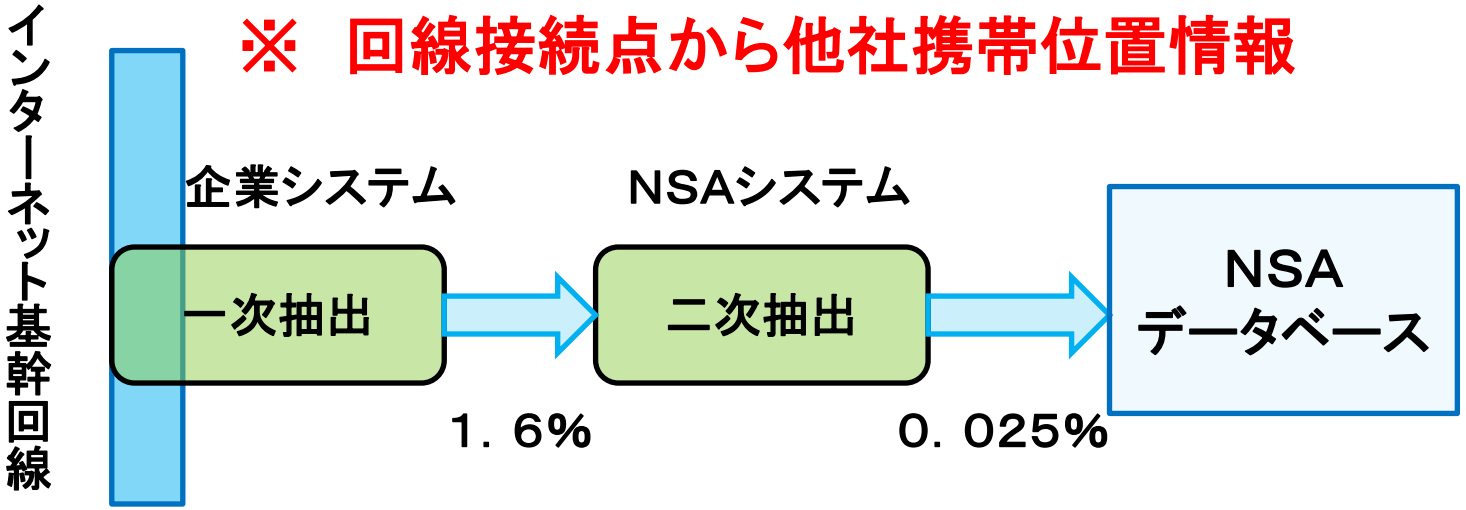
Stormbrew～ベライゾン

○　収集拠点　ATT～全米40ヶ所以上

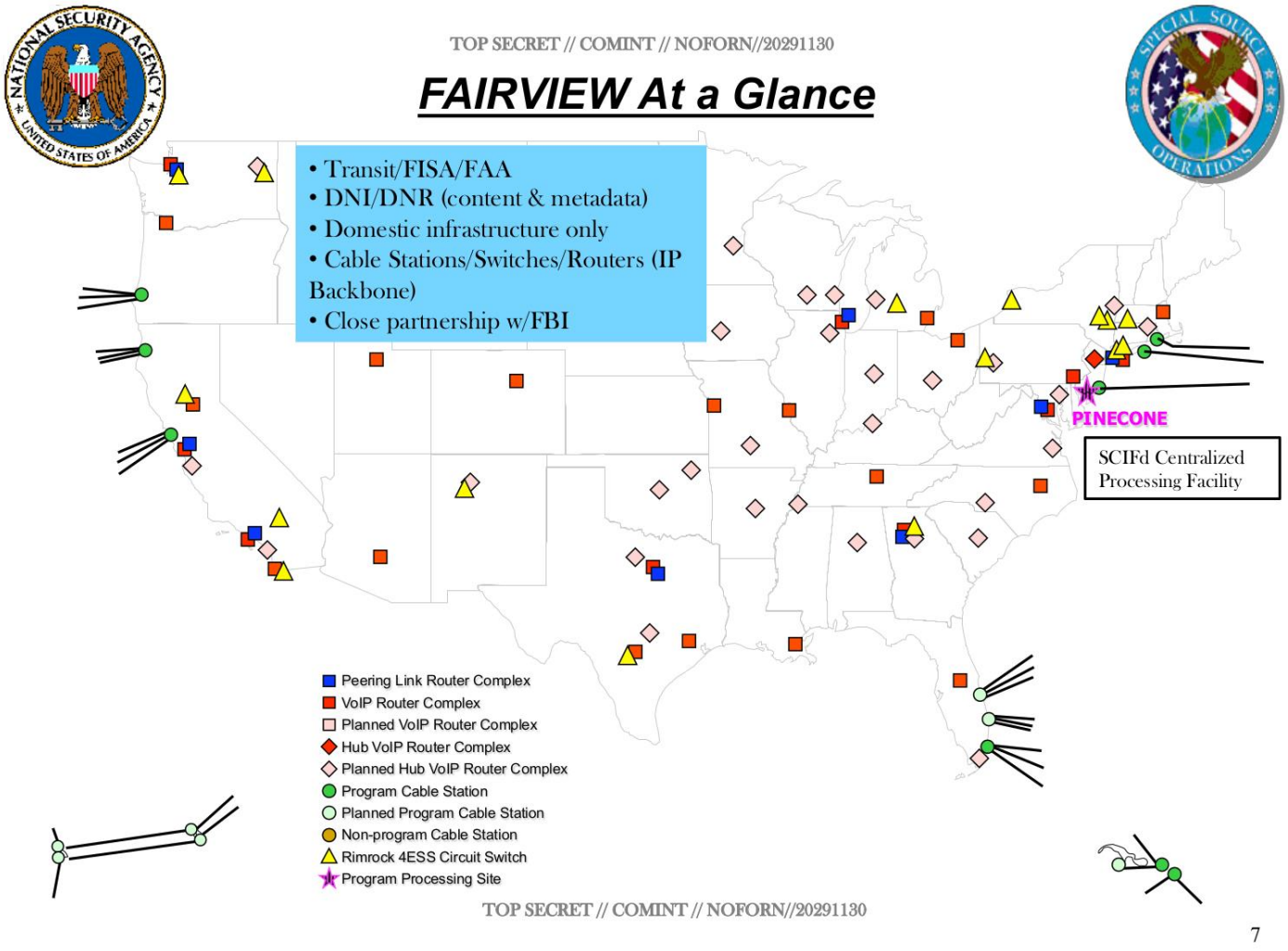
ベライゾン～全米7ヶ所

※　他社からの通過データ、

※　回線接続点から他社携帯位置情報

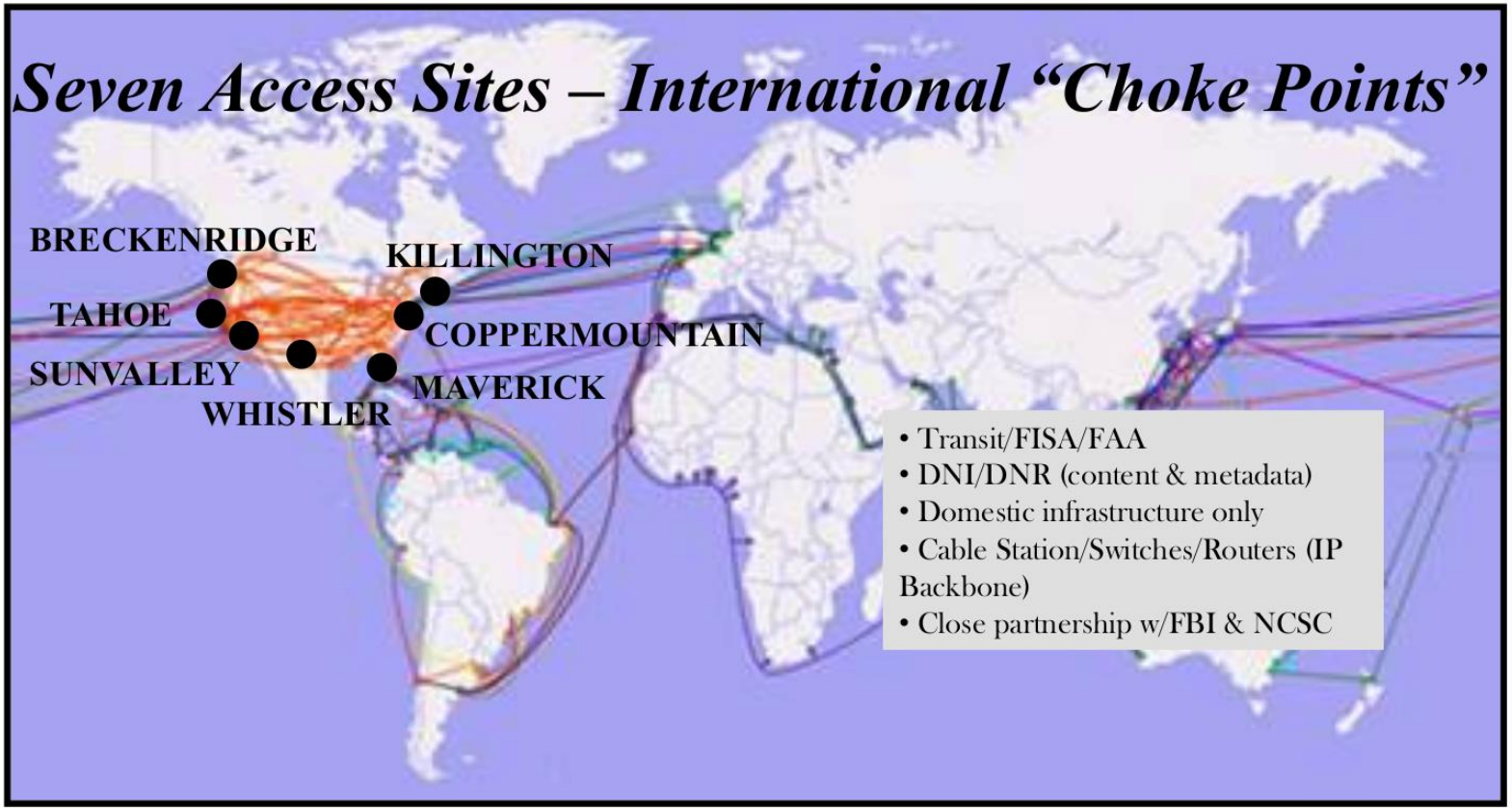


6-2 A(2) Fairview



6-2 A(2)Stormbrew

STORMBREW At a Glance



6-2　A(3)オークスター殆ど国外

○　8つの小計画で構成。

- 大統領命令12333号による国外収集～6つ
- 通過通信Transit権限による国内収集　～2つ

○　小計画の例

「オレンジクラッシュ」～ポーランド国内で収集

主要標的は、中東、アフガニスタン、アフリカの一部

「シルバーゼーファ」～米国内で通過通信を収集

主要標的は、中南米。

ブラジルとコロンビアの国内通信の収集も可能。

６　収集態勢の目次

6-2　B(1)「ウィンドストップ」UKUSA

B(1)「ウィンドスットップ」～小計画4つ

☆　セカンド・パーティとの共同事業

①「インセンサー」～英GCHQとの共同事業

欧州～英国～米州を結ぶ通信基幹回線から通信傍受

②「マスキュラー」～英GCHQとの共同事業

グーグル等のデータセンター間の通信傍受

○「トランシャト・サリブル」(内容不明)

○「不明計画」(内容不明)

英国の海外領土(キプロス島デケレア地区)や
オマーンでの収集がこれらに当たる可能性。

6-2　B（1）「ウィンドストップ」①

①「インセンサー」小計画

- 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。

6-2　B（1）「ウィンドストップ」②

②「マスキュラー」小計画

- ○　英国内で英GCHQとの共同作業
  （2009年7月運用開始）
- ○　Google，Yahooの専用回線に侵入
  - データをデータセンター複数で重複して保存
  - センター間専用回線の通信は暗号化未実施
  - センター間回線に侵入、回線上の全データを取得
- ○ 協力企業は、Level　3　Communications？
- ○　Microsoft専用回線にも侵入？

6-2　B(2)「ランパートA」サードP

B(2)「ランパートA」計画

☆　サード･パーティ諸国との共同事業

（1992年開始）

○　NSAは機器を、相手国は回線アクセスを提供
　　多くは、衛星通信施設で偽装

○　計画名～Smokysink, Azurephoenix, Spinneret, Moonlightpath, Firebird, Flashmark, Falconstrike, Dulcimer、Condorspeak　他

○　協力判明～独、デンマーク、スウェーデン、仏

○　可能性～韓国、シンガポール他

６　収集態勢の目次

6-2 C 単独事業①

☆ NSAが国外で、相手国に内密に一方的に実施

○ 5つの計画。 一つを除いて内容不明

「ランパートI/X」「ランパートM」「ランパートT」

「ミスティック」「不明」

○ 「ミスティック」～5つの小計画、2009年開始

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

対象国～バハマ（DEA）、アフガニスタン、

メキシコ（CIA）、ケニア（CIA）、フィリピン（ASD）

6-2 C 単独事業②

「ミスティック」小計画

○ バハマの例

国際犯罪捜査のためバハマ政府が傍受設備を設置。

DEA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

○ アフガニスタンの例

国名は2014年5月にアフガニスタンとする分析あり。

2015年9月、国家諜報長官が、スノーデン漏洩によりアフガニスタンにおいて重要な資料源を喪失したことを認める。

６　収集態勢の目次

6―3　外国衛星通信の傍受

世界各地で衛星通信を傍受

○　主要傍受施設　12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、ビュード
中東　　：　キプロス、オマーン
アジア　：　日本・三沢　、フィリピン、タイ・コンケン
大洋州　：　豪州・ジェラルドトン、ショアルベイ、
　　ニュージーランド

○　特別収集サービス　約40ヶ所

（大使館、領事館等）

６－３　外国衛星通信の傍受

日本・三沢基地

英国メンウィズ・ヒル

６－３　外国衛星通信の傍受

６　収集態勢の目次

6―4　特別収集サービス①

SCS（Special　Collection　Service）

- ○　CIAとNSAの共同事業（予算3億5千万ドル以上）
- ○　米大使館・領事館
  「ステートルーム」と　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（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、WiMAX等無線LAN、　携帯電話
- ○　UKUSA諸国の外交施設にも設置

☆　独メルケル首相（渾名：携帯宰相）

6―4　特別収集サービス②

在ベルリン米国大使館

6―4　特別収集サービス③

利点

- ○　地理～敵対的空間の中のホームフィールド
  ～顧客近く
- ○　信号アクセス～Passiveな収集の他、
  ～Activeなシステムへの侵入が可能
- ○　分析～通信インフラ、システム構成の把握
  ～標的設定や標的の行動の把握
- ○　情報成果～国家的需要と、地域的需要
  ～現地に対する背景知識、現地情勢

標語　「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」

６　収集態勢

６－１　「プリズム」計画（Downstream）

６－２　通信基幹回線からの収集（Upstream）

６－３　外国衛星通信の傍受（FORNSAT）

６－４　SCS（特別収集サービス）

６－５　CNE（コンピュータ・ネットワーク資源開拓）

（１）　CNEとTAO組織

（２）　遠隔侵入

（３）　物理的侵入

（４）　機材開発

6－5 （1）CNEとTAO①

CNE（Computer Network Exploitation）

① 標的システムからデータを取得する

② 標的システムへのアクセスを獲得する

○ 主体：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

○ 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

○ TAOの付加任務：CNA支援、CND支援、秘匿CNA

６－５ （１）CNEとTAO②

ア　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）

イ　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）　標的との送受信ソフトウェア開発
- MIT（Mission Infrastructure Technologies）作戦用ネットワークの開発配備

６－５ （２）遠隔侵入①

ア　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.”

イ　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

６―５ （２）遠隔侵入②

ウ 「クオンタム」諸計画の一つ

＜Quantum Insert＞2005年開始

① 通信基幹回線等に設置したデータ取得装置

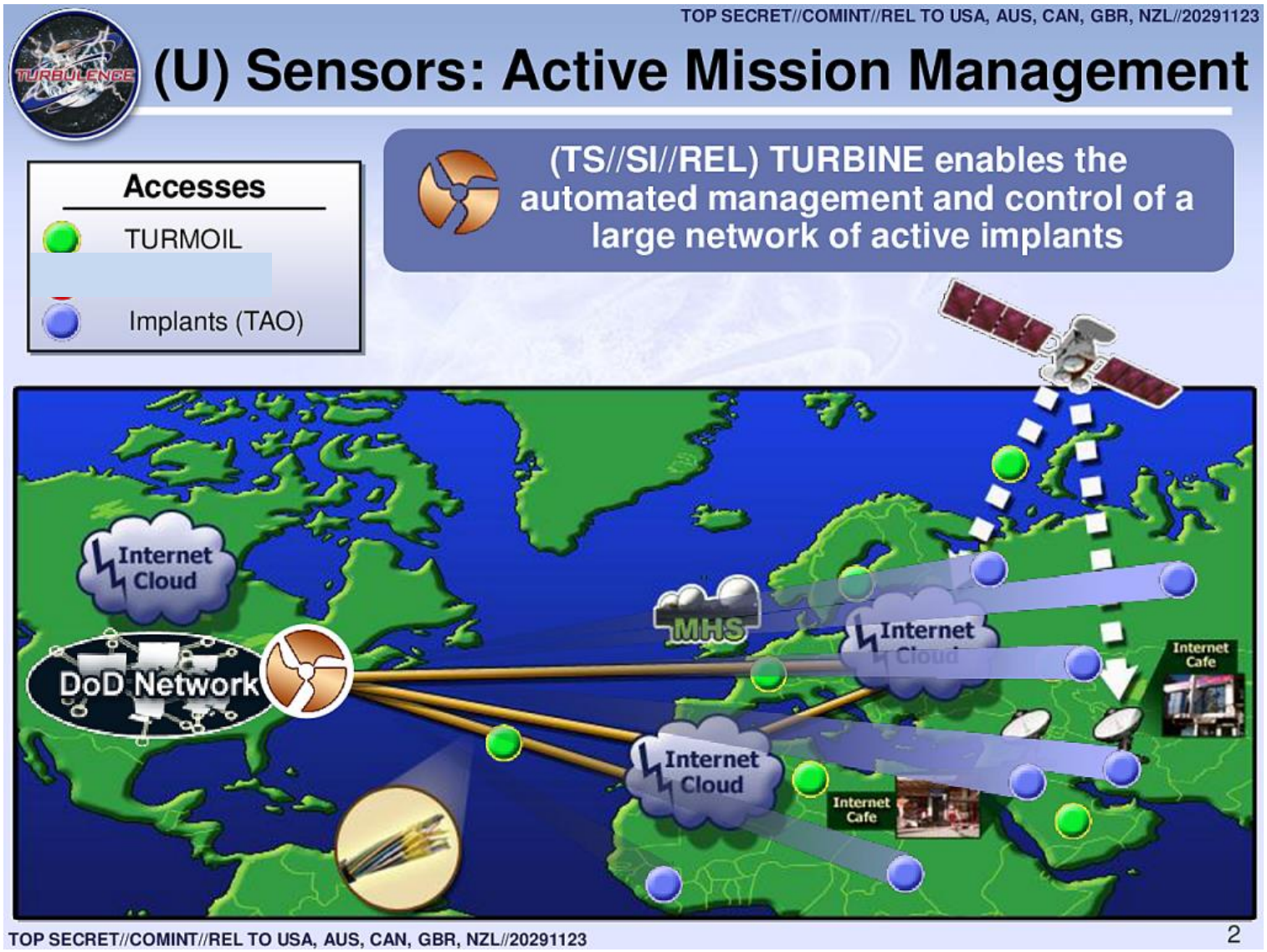
② 「ターモイル」システム～①から送付されてきた通信の中から、IPアドレス等を基準に標的通信を見つけ出す。

③ 「タービン」システム～②で見つけた標的通信に対して、FoxAcidサーバーに誘導するデータを送信する。

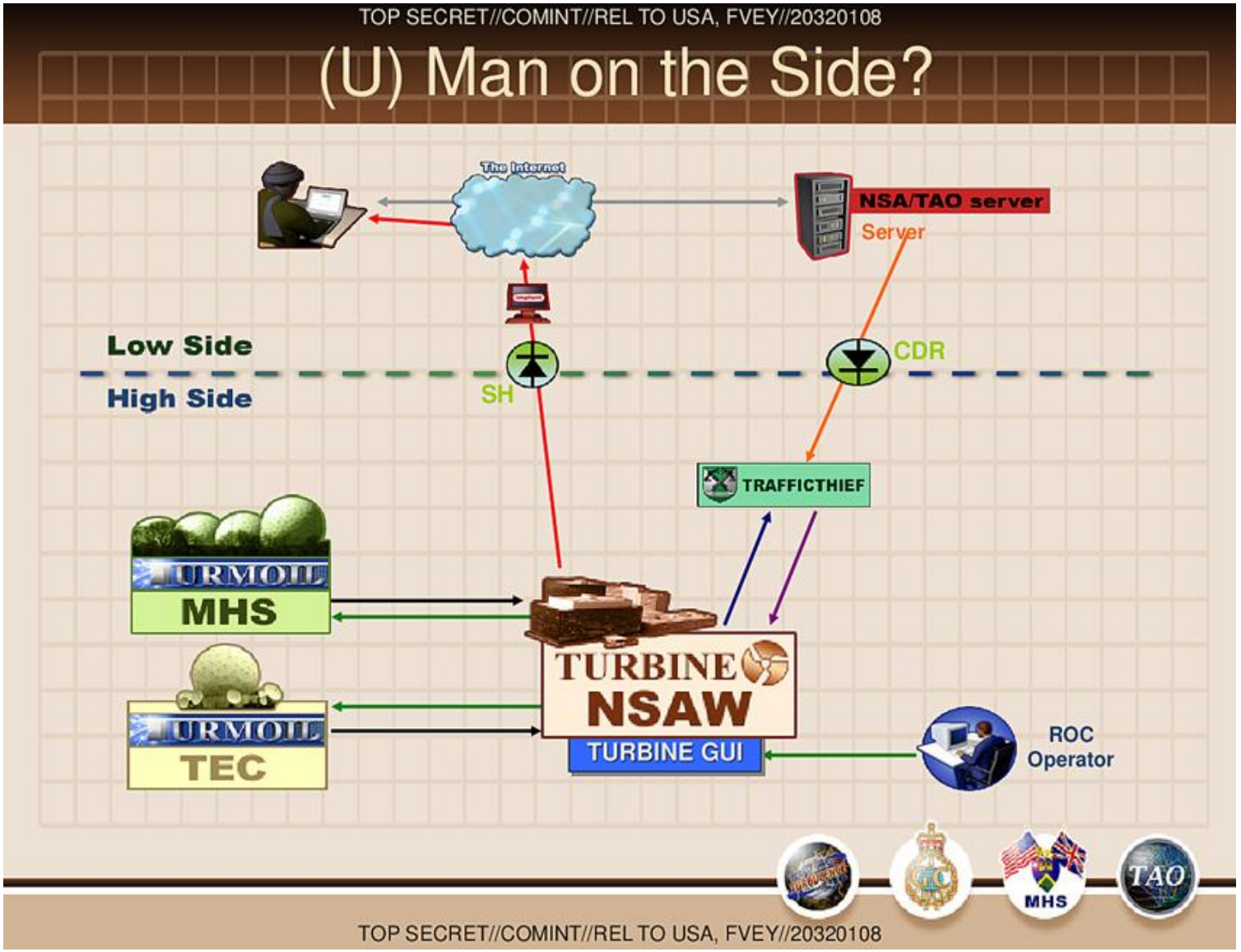
④ FoxAcidサーバーでインプラントを注入

- LinkedIn偽装サイト：インプラント注入成功率50％以上

6—5 （2）遠隔侵入③


TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20291123
(U) Sensors: Active Mission Management
Accesses
TURMOIL
Implants (TAO)
(TS//SI//REL) TURBINE enables the automated management and control of a large network of active implants
Internet Cloud
DoD Network
MHS
Internet Cloud
Internet Cafe
Internet Cloud
Internet Cafe
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20291123
2

6—5 （2）遠隔侵入④



Internet
TAO

NSANet

参考： データ回収

Exfil dataの回収方法の一つ

特定回線から（特定サーバーからではなく）

Network Shaping

参考

https://www.documentcloud.org/documents/2919677-Network-Shaping-101.html

６－５ （３）物理的侵入①

ア　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

イ　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

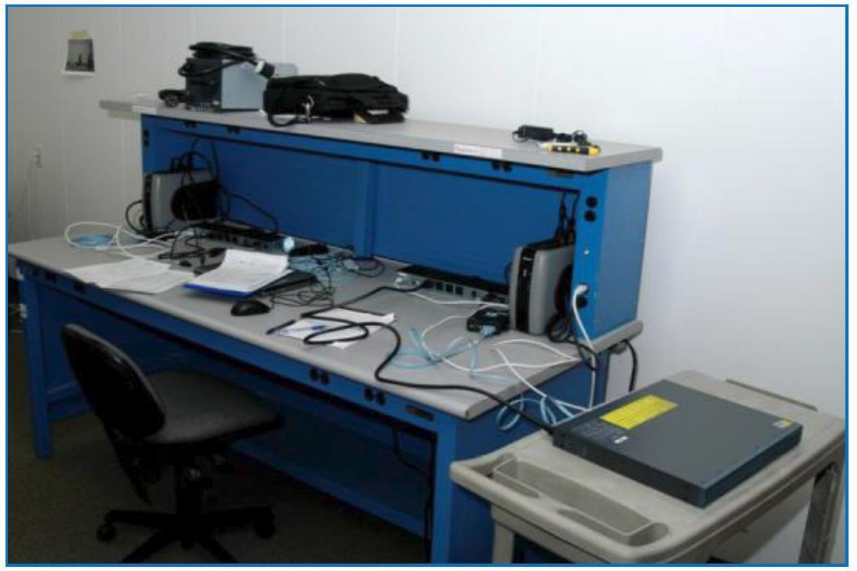
～配送経路介入

○　外国公館工作

６－５ （３）物理的侵入②

ウ　供給網工作（配送経路介入）漏洩資料

(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.



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

６－５ （３）物理的侵入③

エ　米国内の外国公館（大使館、UN代表部）

対象：外国公館38（中東諸国、EU、仏、伊、
ギリシャ、トルコ、インド、日本、韓国、メキシコ等）

（例）「ドロップマイヤ」＝在ワシントンEU大使館

- 欧州諸国外務省との暗号付ファックスに傍受装置設置
- 会議室等に会話傍受アンテナ設置

（例）「ペリディコ」＝在NY・EU代表部

- TV会議システムに暗号解除・傍受装置設置
- 特定のコンピュータに記憶転送装置を設置

（例）日本大使館、日本UN代表部

「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

「マグネチック」漏洩電磁波収集

「バクラント」スクリーンのデータ読取

6－5 （4）機材開発（製品紹介）

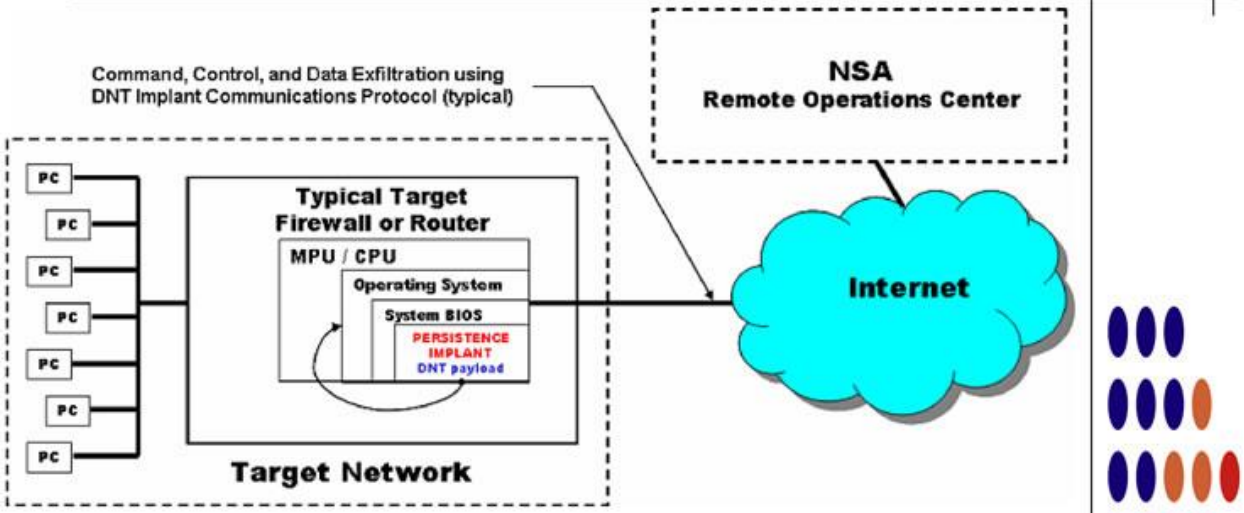
TOP SECRET//COMINT//REL TO USA, FVEY

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 communications structure, so that full access can be reacquired at a later time.

6―5 （4）機材開発

○ TAO ANT部門：2008年版製品カタログ

- ファイアウォール用：Jetplow、有線、Sisco； Juniper,華為
- ルーター用： Headwater、有線、華為； Juniper
- サーバー用： Ironchef、無線、HP；Dell
- コンピュータ端末用： Ginsu、無線
- 偽装USBコネクター： Cottonmouth、無線
- モニター画面用： Ragemaster、レーダ照射に反応
- キーボード用： Surlyspawn、レーダ照射に反応
- 無線LAN用：SparrowⅢ探知システム、無人機から使用可能
  Nightstandウィルス注入装置、遠距離から可能
- 携帯電話電波塔

本日のまとめ

１　シギント情報例
２　UKUSAシギント同盟
３　NSA概観
４　協力企業・協力国
５　シギント戦略、収集根拠
６　収集態勢
　６－１　「プリズム」計画Downstream
　６－２　通信基幹回線からの収集Upstream
　６－３　外国衛星通信の傍受FORNSAT
　６－４　SCS（特別収集サービス）
　６－５　CNE（コンピュータ・ネットワーク資源開拓）