

シギントの世界史

UKUSAと5Eyes

2015年12月12日
防衛研究所戦史研究センター

小谷 賢

情報伝達の速度、量、安全性

- 人:時速10km、1日40km
- 馬:時速30km、1日80km
- モンゴルの騎馬飛脚(13世紀):1日375km
- 教皇急使(14世紀):1日100km
- のろし:条件にも拠るが1日1000kmぐらい
- 帆船:時速5~10km、1日100~200km
- 伝書鳩:時速70km、1日200km以内
- 旗振通信(江戸中期):分速12km(大阪~京都4分)
- 腕木通信(19世紀):分速80km
- 電信(1840年代~):すごく速い
- 無線(20世紀):すごく速い

情報の伝わる速度は19世紀の電信の登場によって、劇的に変化した。



通信のグローバル化

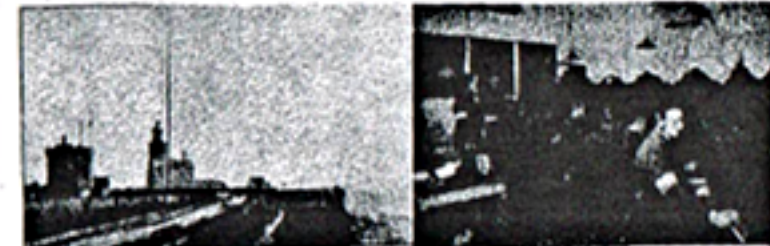
- 1844年、最初の電信が登場。1866年には海底ケーブルで米大陸に到達。翌年、イギリスは海底ケーブルを暗号化。
- 電信の速さ→戦争や外交に決定的な影響を与える。
- 日本海海戦:兎玉ケーブルの存在。
- 多くの海底ケーブルがイギリス領内を通過→イギリスによる通信傍受。



1901年の海底ケーブル網

通信傍受の幕開け

- 1899年、マルコーニの無線通信の実用化→英軍が最初に採用。その後、各国軍も採用。
- 日本海軍は1901年に最初の無線機、34式無線機を正式採用。
- イギリスは1909年に世界で最初の通信傍受施設をノーフォークのハンスタントンに設置。



第一次世界大戦(WWI)

- 1906年、ルクーの小説『1910年の侵攻』。1909年、イギリスMI5 (SyS), MI6 (SIS)設置。初の常設国家インテリジェンスの誕生。陸軍省情報部MI1-19のカバーネーム。ただし6は仕事に困る。WWI:技術情報の出現。航空偵察情報、通信傍受情報。マイケル・ハワード「情報は第4の戦場」。
- ツインメルマン事件によるアメリカの参戦。通信傍受が歴史を変えた事例。
- 秘密外交の禁止→外交機関と情報機関の分離。
- ワシントン海軍軍縮会議(1922)における米の暗号解読。暗号解読の責任者、ハーバート・ヤードレーによる暴露本の発売(1931年)。

第二次世界大戦(WWII)

- 通信傍受情報が第二次大戦の終結を数年早めた。米英による通信傍受情報活動。
- ミッドウェイ作戦、海軍乙号、甲号事件。
- ノルマンディ上陸作戦。
- 多くのスパイが活躍。リヒャルト・ゾルゲ、ドウシュコ・ポポフ、ウィリアム・スティーンズンetc.



パープル暗号

- 1939年に外務省が導入、1940年後半に米が解読。
- 「日本政府は」(原文)→NIHON SEIHU HA(ローマ字置き換え)→ELQTV WGBUH FA(暗号化)。

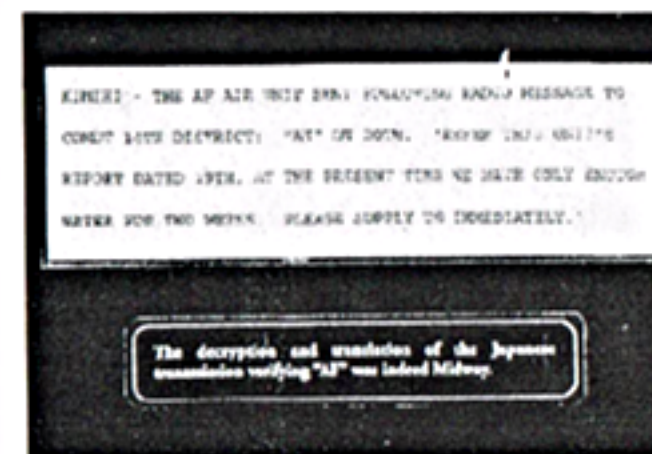
THESE ARE THE FIRST TWO MESSAGES RECEIVED BY THE
JAPANESE IN THE MIDDLE OF THE NIGHT OF DECEMBER 7, 1941.
THEY WERE RECEIVED AT THE JAPANESE CONSULATE IN HONOLULU.
THEY WERE RECEIVED AT THE JAPANESE CONSULATE IN HONOLULU.
THEY WERE RECEIVED AT THE JAPANESE CONSULATE IN HONOLULU.

THESE ARE THE FIRST TWO MESSAGES RECEIVED BY THE
JAPANESE IN THE MIDDLE OF THE NIGHT OF DECEMBER 7, 1941.
THEY WERE RECEIVED AT THE JAPANESE CONSULATE IN HONOLULU.
THEY WERE RECEIVED AT THE JAPANESE CONSULATE IN HONOLULU.
THEY WERE RECEIVED AT THE JAPANESE CONSULATE IN HONOLULU.



海軍作戦暗号D(JN-25)

- ミッドウェイ作戦に先駆けて米海軍のチームが解読。



「AF」は水が不足している

エニグマ暗号

- ドイツが市販されていたエニグマ暗号機を改造して使用した暗号。ポーランドの暗号解読班が解読に取り掛かり、イギリスのアラン・チューリングらのチームが引き継ぐ。



UKUSAの誕生

- 「UKUSA(ユーキューサ)」=米英加豪ニュージージーランドによるインテリジェンス共同体。
- 1940年10月25日、米陸海軍の暗号解読組織が、英外務省政府暗号学校(GC&CS)に協力を申し出る。
- 1942年10月2日、米海軍通信情報部(OP-20-G)とGC&CSの間で「ホールデン協定」を締結。OP-20-Gが日本海軍(JN)、GC&CSがドイツ海軍のエニグマ暗号を担当
- 1943年5月24日、米陸軍通信情報部(SIS)とGC&CSがBRUSA協定を締結。SISが日本軍、GC&CSが独伊軍に関する暗号を解読。



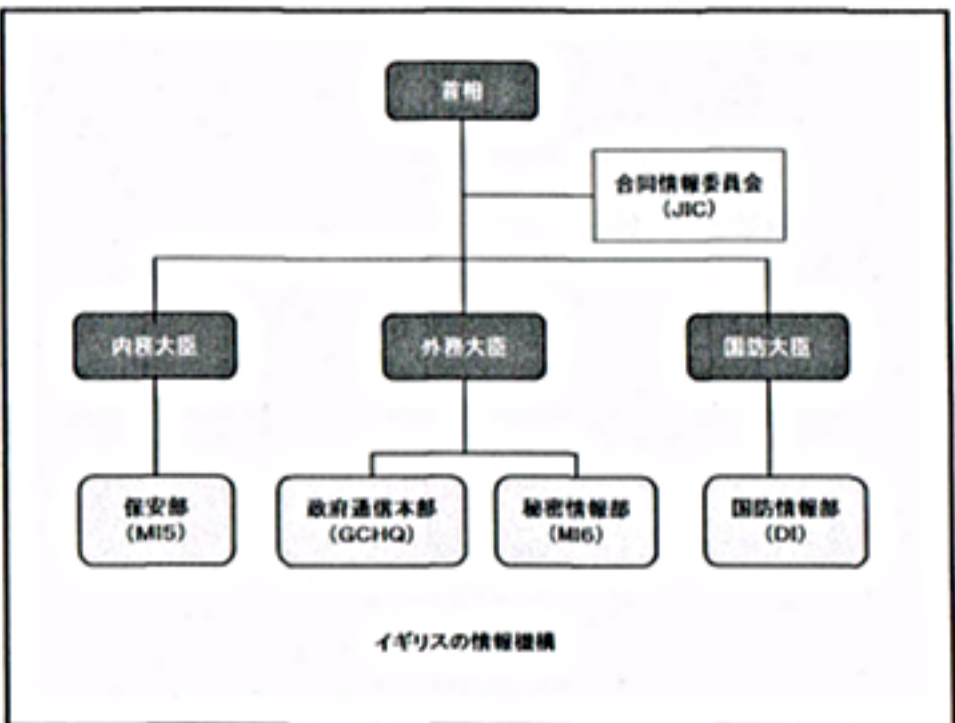
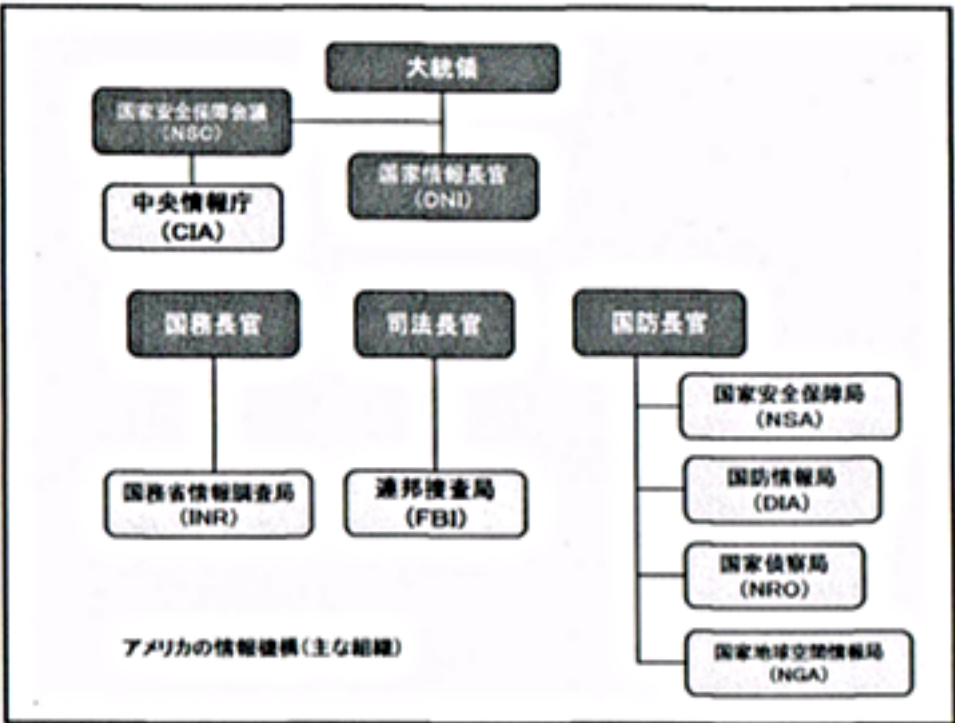
UKUSAから5Eyesへ

- UKUSA協定(1946.3.15): ①調印: STANCIBとLSIB、②協力分野: 通信傍受情報、③通信傍受情報の定義、対象国: 米英、英連邦を除く外国、④暗号解読技術の共有、⑤第三国への情報提供、⑥英連邦との将来的な協力、⑦当面の英連邦との協力、⑧配布と秘密保全、⑨商業分野への適用、⑩前協定、⑪協定の批准と効力。
- 1948年にカナダ、1956年に豪・ニュージージーランドがUKUSAに参加(ただしニュージージーランドは1977年まで独自の通信傍受組織を持たず)。



NSAの誕生

- 戦後、陸海軍に空軍を合わせ、三軍安全保障局が誕生。
- 通信傍受は陸海軍の管轄⇔1947.9.18にNSCとCIAが誕生。通信傍受は国家的な運営が必要!
- 1948年7月1日NSC, No.9「制度上は軍、運用上はNSC」→朝鮮戦争における失敗。
- 1952年6月、プロウネル報告書「軍部から国防総省へ」→1952.11 NSA(国家安全保障庁)が誕生。



ヴェノナ

- ヴェノナ=UKUSAによるソ連暗号解読プロジェクト。1943年2月頃、米陸軍が解読に着手。1948年にUKUSA協定が正式に調印されることにより、米英の共同活動が開始される。
- ソ連暗号は使い捨て暗号であり、解読がとても困難。ものによっては解読に30年近くかかることも。計画自体は1995年まで秘匿。
- 1948年10月29日には米陸軍のウィリアム・ワイズバンドがヴェノナの情報を漏洩→ソ連はすべての暗号キーを変更。
- ヴェノナによって多くのソ連側スパイ、協力者が特定される。
米: ハリー・デクスター・ホワイト、アルジャー・ヒス、ラフリン・カリー、クラウド・フックス、セオドア・ホール、デーヴィッド・グリーングラス。
英: ドナルド・マクリーン、ガイ・バージェス、キム・フィルビー。

ベルリン・トンネル作戦

- 1954年9月、CIAとMI6はベルリンのアメリカ占領地域からソ連管轄地域に対して地下トンネルを450m掘り進み、そこでソ連軍の通信を傍受していた。
- 1956年1月、KGBに内通していたMI6のジョージ・ブレイクが同作戦の機密を漏洩。ブレイクは懲役42年の刑に処されるが、1966年に刑務所を脱走しソ連へ亡命。

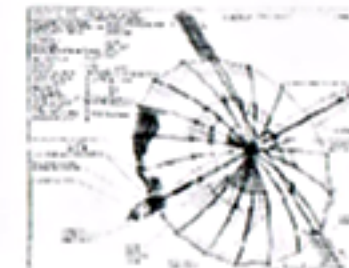


「シャムロック」と「ミナレット」

- シャムロック: NSAの米国内における盗聴活動。1945年4月のサンフランシスコ会議が起点。ウエスタン・ユニオン社、ラジオ・コーポレーション・アメリカ(RCA)、国際電話電信社(ITT)に電報の写しの提出を求める。
- ステティニアス米 국무長官: 「通信傍受情報は国務省にとって計り知れない価値があった」。
- ミナレット: NSAによるヴェトナム反戦運動家の監視活動。1690名の米国市民と5925名の外国人。女優のジェーン・ Фондаやミュージシャンのジョン・バエス、ボクサーのモハメド・アリ、ジャーナリストのトマス・ウィッカーやマーティン・ルーサー・キング・ジュニア。
- UKUSAに基づき、GCHQも傍受に参加。

ライオライト衛星

- NSAは1970年6月、高度約3万6000kmの静止衛星軌道の上に重さ700kg、直径40m近いライオライト衛星を打ち上げる。
- ライオライトからのダウンリンクはNSAだけでなく、英メンウィス基地や豪パイン・ギャップ基地にも送られる。
- TRW社の社員、クリストファー・ボイスが、ライオライト衛星に関わる機密情報を7万ドルでソ連側に売り飛ばす。ボイスは懲役40年、刑務所を脱走し再逮捕さらさらに28年が追加。



アイヴィー・ベル (Ivy Bells) 作戦

- 1970年代にCIA, NSA, 米海軍が協力して、オホーツク海に敷設されたソ連海軍の海底ケーブルを盗聴する作戦。
- 1971年、米原潜「ハリバット」が海底120メートルに施設されたケーブルに盗聴器を仕掛ける。
- 1981年、NSA職員のロナルド・ベルトンがソ連側に情報を漏洩。ソ連海軍は盗聴器を引き上げる。
- 1985年1月、KGBのヴィタリー・ユルチェンコが西側に亡命、NSAの「ミスター・ロング」について暴露→ベルトンが浮かび上がる。ベルトンは終身刑。



ジェフリー・プライム事件

- 米ソ間の核抑止における大前提の一つ: お互いの潜水艦に搭載された弾道ミサイル (SLBM) の位置は特定できない→米英は特定に成功。「サンボ」計画。
- GCHQのロシア語翻訳官、ジェフリー・プライムはサンボを含む機密情報を70万円でソ連に漏えい。
- その後、プライムは精神疾患を理由にGCHQを辞職し、チェルトナムでタクシー運転手を始める。
- プライムは少女への性的嗜好あり。1981年末、14歳の少女に手を出そうとし、反撃される。その後、逮捕。
- 警察はプライムの自宅から2287枚にも及ぶ少女の写真を押収するが、ロシア語の書類や機材には目もくれず。
- プライムの妻が警察に訴え出ることによってスパイ行為が判明。機密漏洩 (35年) + 性犯罪 (3年) の刑が確定。GCHQはようやくポリグラフ検査を導入。

フォークランド紛争: 議会での討論 (4月3日)



テッド・ロウランズ労働党議員

私が外務副大臣を務めていた70年代には、GCHQはアルゼンチンの外交暗号を解読していた。首相は事前にアルゼンチンの侵攻を知っていたのではないかと?

おだまり!



サッチャー首相

アルゼンチン外務省はスイス製の暗号機を、軍の方は米国から提供された暗号機を使用しており、GCHQは両方を読むことができた。この討論をきっかけにアルゼンチン側は暗号の一部を変更するに至る→戦争中アルゼンチン軍の暗号解読、翻訳には12-24時間かかった

UKUSA間の軋轢

- 1960年代にNSAの予算はGCHQの10倍に→米英の立場が逆転。
- 1970年代にはUKUSA協定の立役者達が退職or死亡→大戦時の経験が共有されない時代に。
- 1970年代のニクソン政権とヒース政権の対立。1971.9の「足作戦」→キッシンジャーは激怒。第四次中東戦争での米英対立に発展。
- 1985年以降はNSAのオドム長官とGCHQのマリーチャーチ長官の対立が先鋭化。

ジルコン計画

- 1982年のフォークランド紛争→イギリスは独自の通信傍受衛星の必要性を痛感。
- イギリス独自技術のジルコン衛星を計画。問題はその莫大な予算(5億ポンド)。
- ジャーナリスト、ダンカン・キャンベルがジルコン計画について記事を執筆。問題が表面化、英政府はジルコン計画を認めず。
- 1987年、GCHQはNSAに出資する形でマグナム衛星を共同運用。

冷戦の終結

- 平和の配当:アメリカではインテリジェンス全体の予算が16%削減、2万599名ものオフィサーたちが退職を余儀なくされる。1980年代にインテリジェンス全体の予算の58%を占めていた対ソ情報予算は、93年にはわずか13%に激減。1990年頃には地球を周回していた衛星の内、75%ほどがアメリカ製のものだと言われていたが、1995年になるまでにそのシェアは23%に。
- インテリジェンスの活動領域は、対ソから、経済、軍事作戦、犯罪捜査へ。

同盟国に対する通信傍受

- 1960年代、アメリカは暗号機、「KL-7」をNATO諸国に配布。「テンベスト」を利用。しかしスイスのクリプトAGの暗号機には手こずる。
- 1975年、IMBは新規格の共通商用暗号DESを提案。しかし暗号作成にはNSAが関与。1985年6月、NSAが日本企業、GCHQが欧州企業に対する通信傍受の取り決め。
- 1990年代、日欧の企業に対する通信傍受の活発化。フランスのエアバス社とトムソンCSF社や日本の自動車企業は盗聴の被害に遭う。ウルジーCIA長官は新聞紙上で盗聴の事実を認める。
- 2001年、怒りの収まらない欧州議会はUKUSAの通信傍受について報告書を作成→「エシュロン」の存在が明らかに。
- ニュージーランドの首相、ヘレン・クラーク「最良のインテリジェンス・クラブ」

9.11の衝撃

- 9月10日の傍受情報:「明日が攻撃開始時刻(zero hour)だ」
- 9.11テロの翌日、GCHQとMI6の長官、MI5副長官が急遽ワシントンを訪れ、UKUSAの結束を確認。
- チェイニー副大統領とテネットCIA長官→ヘイデンNSA長官「NSAがアメリカを守るためにもっとできることはあるか、実際に有効な手段はあるか、現行の法律の範囲内でできるのか」
- NSA、GCHQともに予算、人員の大幅な拡大。
- 情報機関の法的権限の強化。「米愛国者法」。GCHQの調査権限はNSAよりも強力。「テンボラ」作戦の開始。

テンポラ

- 英国の調査権限規制法:通信傍受はGCHQの管轄。
- スノーデン「英国のGCHQはNSAよりひどい」
- オマンドGCHQ長官「イギリスには頭があり、アメリカには金がある」。NSAはGCHQに1億ドルを拠出。
- テンボラ:英国内を通過する200以上の光ファイバーケーブルから、一日に21ペタバイトという莫大な情報を収集



イラク戦争開戦をめぐるインテリジェンス

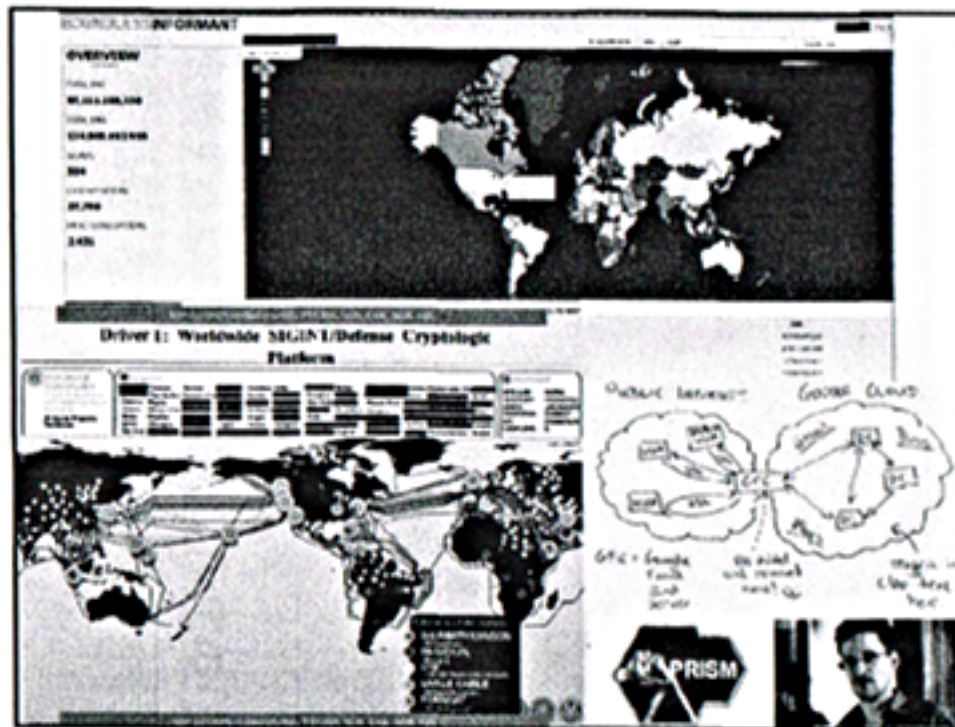
- ・国連安保理において、イラクへの攻撃を推し進める米英と、それに反対するフランスなどの対立があり、10か国の非常任理事国が米英を支持するかどうか微妙な情勢。
- ・NSAのフランク・ゴザ主任からGCHQにeメールでの依頼。「国連の非常任理事国のすべての通信の傍受をお願いしたい。(中略)我々の方は現在、国連安保理に出席していない国々の傍受活動にかかりっきりである」
- ・当時28歳の中国語専門官、キャスリン・ガンはこのメールを知り合いの新聞記者に漏えい。3月2日に『オブザーバー』紙が同メールの全文を掲載。ガンは逮捕されるも無罪。
- ・クレア・ショート英国国際開発担当相「定期的にアナン事務総長の電話記録を読んでいた」→GCHQやNSAによる盗聴。

スノーデン事件の衝撃 (2013.5)

- ・ エドワード・スノーデン:1983年生まれ。ノースカロライナ出身。コンピューター、日本好き。
- ・ 大学を中退後、2004年5月に米陸軍入隊、同年9月除隊。
- ・ 2005年、メリーランド大学言語高等センターのセキュリティ部門に採用。その際、クリアランスを受ける。翌年、CIAにコンピューターセキュリティの専門家として採用。2007年、ジュネーブで勤務。2009年退官。同年、デル社の社員として横田基地で勤務。2012年3月からNSAのハワイのクニア・シギント作戦センターで15か月勤務。その間、ブーズ・アレン・ハミルトン社に移籍。
- ・ 2013年5月、機密資料を携えて香港に移動。グリーンウォルド氏らに資料を提示する。6月、ロシアに移動。2014年6月から居住権を3年間延長。住居はFSBが用意。FSBに情報を漏洩すると同時に今度はFSBの秘密を知ってしまった！？
- ・ とにかく量が多い。ダニエル・エルスバーク(1971):4100枚、ブラッドレー・マニング(2010):73万件、スノーデン(2013):170万件。

スノーデン氏が明らかにした様々な計画

- STATEROOM: 世界大の通信傍受。USUKCAAUSNE
- Treasure Map: ネット世界の地図化。USUKCAAUSNE
- ICREACH: 携帯の通話記録、メールの使用状況について検索できるソフト。USUKCAAUSNE
- Dishfire: 一日数億通のメタ・データを収集。USUKCAAUSNE
- Tracfin: クレジット決済など金融取引の記録収集。USUKCAAUSNE
- PRISM: IT企業も巻き込んだ情報収集、監視プログラム。USUKAUS
- Xkeyscore: 情報分類プログラム的一种。言語などからユーザーの国籍、人種、性別を特定。USAUSNE
- Mobile Applications Project: スマホのアプリに盗聴プログラムを仕掛ける。
- MUSCULAR: YahooやGoggleのデータサーバーの情報を取り出す計画。USUK
- Dishfire: SNSメッセージの収集。USUK
- SENTRY OSPREY: 民間企業に工作員を浸透させる。US
- Royal Concierge: 英国内のホテルの予約情報。UK
- Tempora: 大西洋の光ファイバーケーブルの盗聴計画。UK



何が問題か？

- 米国内で米国人を対象とした情報収集活動を行うためには、事前にFISA裁判所からの許可が必要⇔NSAはほぼ無視。
- 5 Eyes以外の同盟国(日韓独仏等)に対する情報活動も明らかに。マンデラ氏やダイアナ妃、メルケル首相の携帯電話に対する通信傍受活動→外交問題化。
- 9 Eyes: 5eyes+フランス、オランダ、デンマーク、ノルウェイ。
- 14 Eyes: 9 eyes+ドイツ、ベルギー、イタリア、スペイン、スウェーデン
- イスラエルは例外的な立場。



『Der Spiegel』(2014/5/29) 122人分の傍受リストの一部を公開。

Omar al-Bashir - Sudan
 Oscar Arias - Costa Rica
 Paul Kagame - Rwanda
 Prachanda - Nepal
 Rafael Correa - Ecuador
 Raul Castro - Cuba
 Recep Tayyip Erdogan - Turkey
 Rene Preval - Haiti
 Robert Mugabe - Zimbabwe
 Sali Berisha - Albania
 Sheik Hasina Wajed - Bangladesh
 Silvio Berlusconi - Italy
 Stjepan Mesic - Croatia
 Susilo Bambang Yudhoyono - Indonesia
 Tabare Vazquez - Uruguay
 Taro Aso - Japan
 Than Shwe - Myanmar
 Umaru Yar'Adua - Nigeria
 Vladimir Putin - Russia
 Yousaf Raza Gillani - Pakistan
 Yoweri Museveni - Uganda

情報分野における米国の主要国の関係

情報収集が容易な国	情報収集が困難な国
オーストラリア	ロシア
ニュージーランド	中国
フランス	インド
ドイツ	インドネシア
イギリス	韓国
イタリア	日本
オランダ	台湾
ノルウェイ	タイ
スウェーデン	トルコ
ベルギー	ウクライナ
スペイン	米国
スウェーデン	米国

米国におけるスノーデン事件の影響

- USA Todayの世論調査(2013.6):テロ対策のためにNSAの監視は必要か。賛成48%、反対47%。
- クラッパーDNI長官:「究極の嵐」。ロジャーズNSA長官「リークは遺憾。再発防止の徹底」。
- 2014年1月にNSA内に戦略コミュニケーション局、市民的自由・プライバシー担当官を設置。広報と説明責任の必要性。
- NSA改革:2014年5月22日、議会下院が、NSAによる不特定多数を対象とした通話記録のデータ収集・保存の中止などを定めた法案(USA Freedom Act)を可決。翌年6月上院も通過。NSAによるシグント活動もまた「リスク」であることが判明。ヒュミント活動を批判できず。
- 2013年12月、フェイスブックやグーグルなど米通信7社は政府に対してNSAの情報収集に対する規制を要望。その後、NSAへのデータ提出を拒否。

米独関係への波紋

- もともとドイツでは情報機関による監視活動に反感が強い。米国ジャーマン・マーシャル財団の調査:独(70%)、米(54%)、英(44%)。スノーデン氏の認知度は、独(94%)、米(60%)。
- メルケル首相の携帯電話に対する盗聴発覚。独政界、経済界の320名がターゲット→BNDもNSAに加担(パート・アイプリング通信傍受施設)。米独間の外交問題に発展→2013.11、米独スパイ禁止協定の提案→2014.5メルケル訪米。米側は消極的。
- 独議会調査委員会が調査を開始→BND職員が議会の調査資料をCIAに渡す。2014年5月スパイ容疑で逮捕。7月在独CIA支局長を国外退去処分。
- 独政府はベライゾンやシスコなど米国企業との契約を打ち切る。
- 独議会はタイプライターの使用や要人同士の直接会話を推奨。防諜活動の予算も増額。
- CIAはドイツでの活動を自粛。



国際的な波紋

- 2013年11月、ドイツとブラジルは国連総会に監視活動を批判する決議案を提出。国連の各種会議に対するNSAやGCHQの活動について調査を開始。
- 欧州連合(EU)は、2006年、テロ対策の一環として、通話や通信上のデータに関する記録を一定期間、保存するように通信企業に求める措置→欧州司法裁判所は人権侵害を理由に措置の無効化を命ずる。
- フランスなど欧州各国で通信傍受やネット情報監視に対する批判が高まる。

インテリジェンスの目的は？

Funding five mission objectives



テロ対策の効果は？

- 米国の対テロ予算(対テロ戦争などの軍事費を含む):160億ドル(1998年)→1200億ドル(2006年)。米国でテロによって死亡する確率は、350万分の1、英国では100万分の1(米国の交通事故死亡率が8000分の1、ガン死亡率が500分の1)。
- ミューラー米オハイオ州立大教授「テロ産業だ。9.11の様なテロに出くわす確率は8000万分の1に過ぎない」。
- テロ対策評価の遅れ。
- スノーデン事件により、テロリストは通信手段を見直す→情報の激減。
- LUM, KENNEDY and SHERLEY, "Are counter-terrorism strategies effective?"(2006): 対テロ予算の増加や法律の厳罰化とテロ抑止の相関関係は不明、軍事的報復は逆効果、空港の金属探知機はハイジャック抑止の有効な対策。→実質的な費用対効果は極めて疑わしい!ただし政治的な意味合いはある。