

日本のテロ対策の課題

～欧米諸国との対比において～

2019年10月3日

日本大学 危機管理学部
茂田忠良

内 容

序 問題意識

- 1 認識と思考におけるギャップ
 - 2 情報収集手法の違い
 - 3 サイバー空間
 - 3-1 サイバー空間の重要性
 - 3-2 NSAとUKUSAシグント同盟
 - 3-3 シグントによるテロ対策
 - 4 その他の課題
- まとめ

序 問題意識

○ 実務家の立場:

現状を前提

漸進的、incremental

H16政府「テロの未然防止に関する行動計画」他

○ OB研究者の立場:

適正な対策が出来ているのか

国際標準に達しているの

○ 国際協力上の必要:

世界(欧米諸国)標準は

内 容

序 問題意識

- 1 認識と思考におけるギャップ
 - 2 情報収集手法の違い
 - 3 サイバー空間
 - 3-1 サイバー空間の重要性
 - 3-2 NSAとUKUSAシグント同盟
 - 3-3 シグントによるテロ対策
 - 4 その他の課題
- まとめ

1(1) 思考の枠組(座標)

(目的)

○ 事案対処 ↔ 未然防止
(被害限定、犯罪捜査)

(機能)

○ 法執行 ↔ 国家安全保障

(担任機関)

○ 警察機関 ↔ インテリジェンス
セキュリティ・サービス
シグント機関

1(2)テロ等準備罪に対する評価

「組織的犯罪処罰・犯罪収益規制法」第6条の2

国際組織犯罪防止条約(TOC条約)締結するため

2017年制定(法務省Website)

<構成要件>

- ① 「組織的犯罪集団」の存在、且つ
 - ② 団体の活動として、具体的且つ実現可能性のある
計画の存在、且つ
 - ③ 計画に基づく実行準備行為の存在
- どうやって立証するのか。
その前に、探知できるのか。

1(3) 考えるヒントとなる事例

- ① **オウム・地下鉄サリン事件** 1995年3月20日
 - 世界初の大都市、化学兵器使用、無差別テロ
 - 政府対応:オウム新法1999年
 - 平成8年版警察白書 反省教訓の一つ
「特殊な閉鎖的犯罪組織についての情報不足」
今後は未然に探知し、阻止できるのか。
- ② **中核派・大坂正明の逮捕** 2017年5月
 - 警察官殺害(渋谷暴動)で1972年に指名手配
日本警察の情報収集力

1(3) 考えるヒントとなる事例

③ IS戦士の帰国者対策

- 処罰できるのか。
- 拘束できるのか。
- 十分な監視ができるのか。

(普通の国の手法)

- 面接
- 周辺に協力者
- メール通信の監視、ウェブ閲覧の監視
- 秘密搜索、秘密手荷物検査
- 住居への傍受・撮像装置設置

内 容

序 問題意識

1 認識と思考におけるギャップ

2 情報収集手法の違い

3 サイバー空間

3-1 サイバー空間の重要性

3-2 NSAとUKUSAシグント同盟

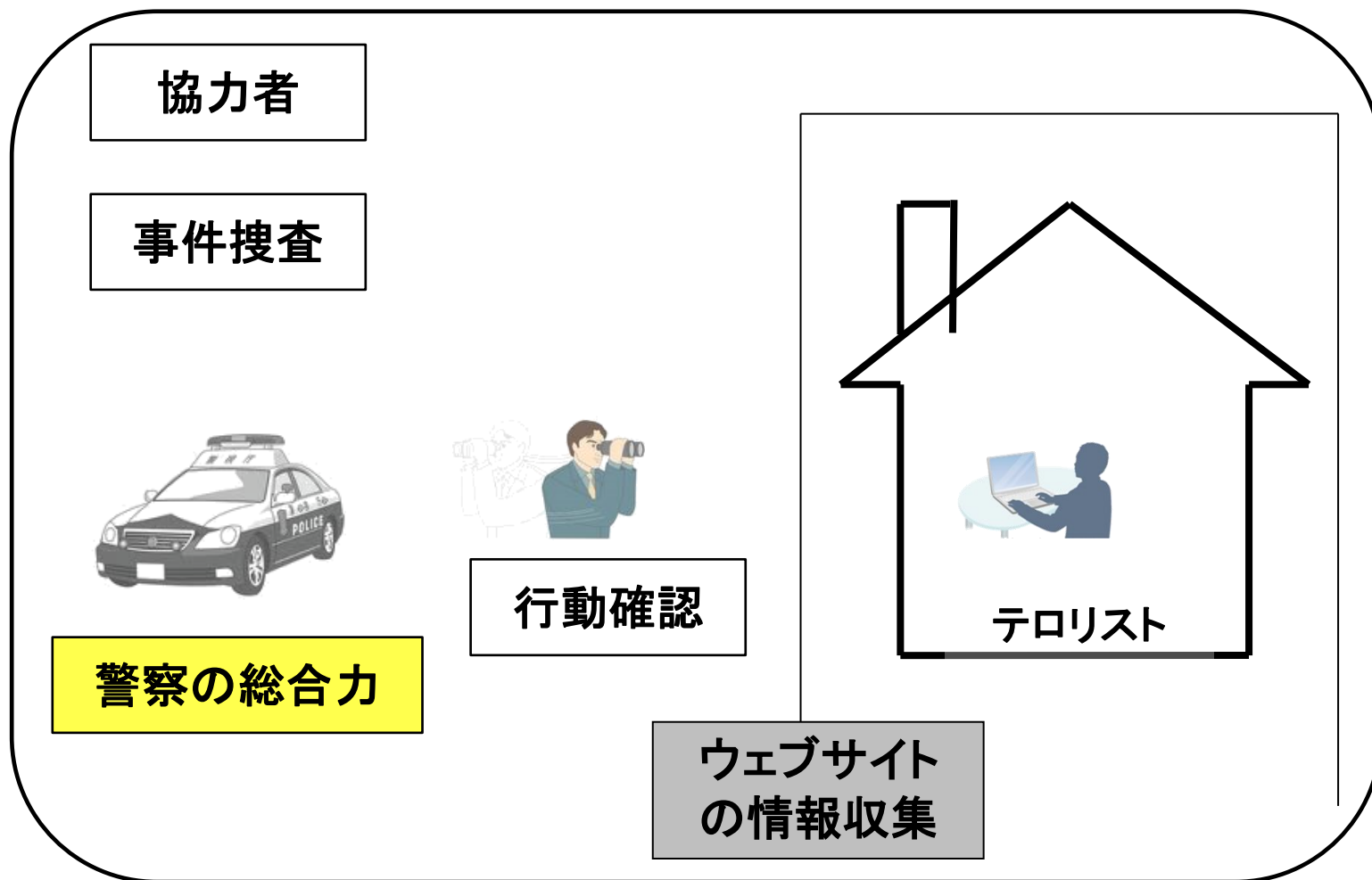
3-3 シグントによるテロ対策

4 その他の課題

まとめ

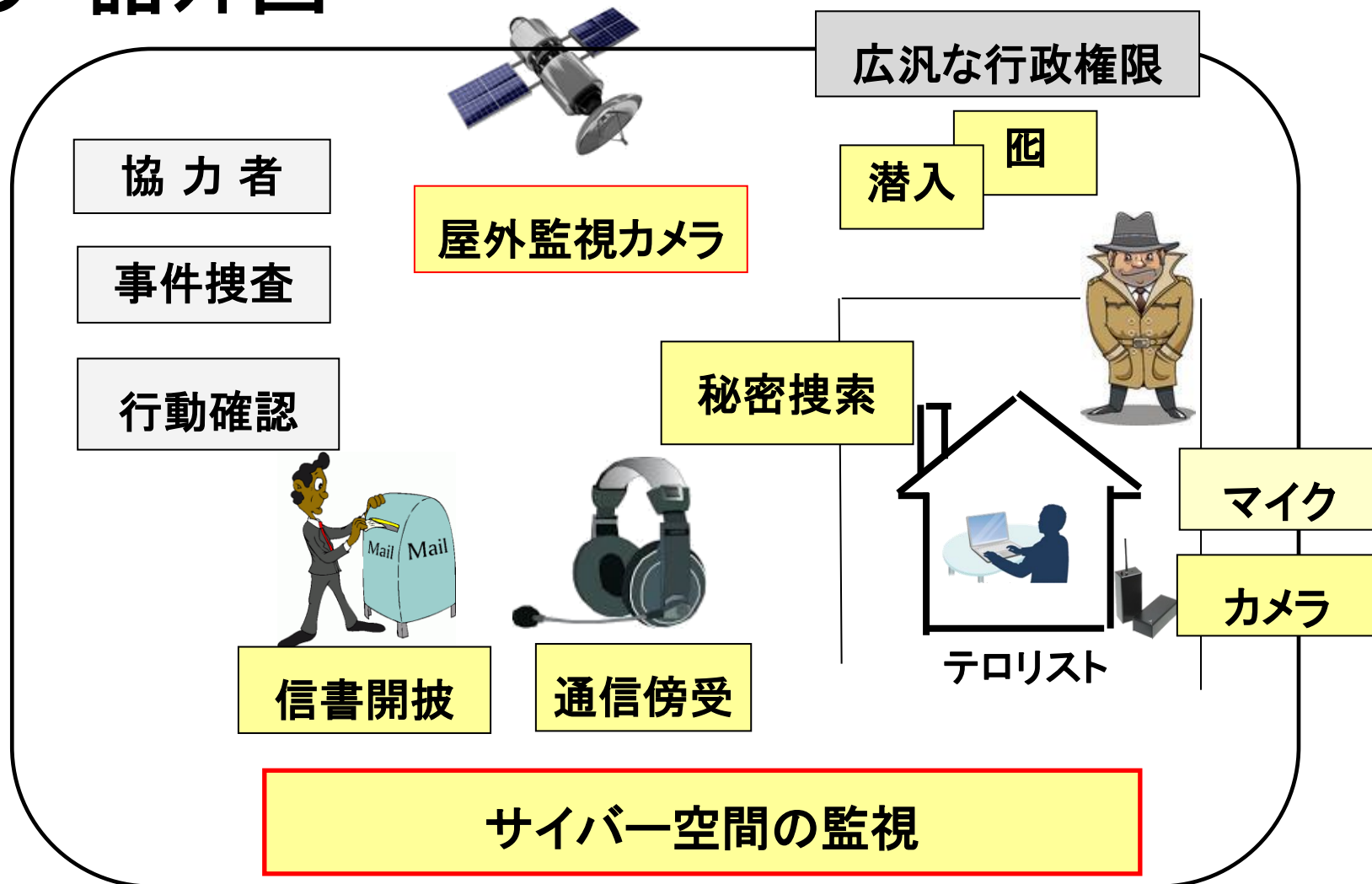
2(1)我が国の情報収集手法

○ 日本



2(2) 諸外国の情報収集手法

○ 諸外国



2(3) 英国RIPA2000、IPA2016

2000年調査権限規制法、2016年調査権限法

- 通信傍受・郵便検閲 interception of communications
- 通信メタデータ use of communications data
- 監視(車両への位置発信装置設置を含む)
directed surveillance
- 侵入的監視(住居、ホテル客室、自動車内:
秘密搜索、監視機器設置) intrusive surveillance
- ヒューミント(潜入、協力者)
covert human intelligence source

内務大臣制定の各種実施規範Codes of Practice

RIPA2000第71条、IPA2016附則第7

内 容

序 問題意識

1 認識と思考におけるギャップ

2 情報収集手法の違い

3 サイバー空間

3-1 サイバー空間の重要性

3-2 NSAとUKUSAシグント同盟

3-3 シグントによるテロ対策

4 その他の課題

まとめ

3-1(1)サイバー空間の状況

<サイバー空間>

あらゆる活動がなされる巨大空間。国境がなく、世界一体化。

○ テロに関連する活動

- テロ集団の思想宣伝、リクルート、思想教育
～DABIQ, Inspire, 説教
- テロ技術の伝達
(爆発物製造方法、車両使用の殺害方法)
- テロ計画の立案、準備
(標的調査、グーグルマップ、攻撃手段)
- テロ実行の際の通信連絡
～2008年ラシュカル・エ・タイバ
- 活動資金調達
- サイバー・テロ
～2017年CyberCaliphate

3-1 (2) サイバー空間の状況

○ サイバー空間における対テロ活動

サイバー空間における容疑者の発見、追跡、監視

① テロ容疑者の容疑解明 Target Development

② テロ容疑者の発見 Target Discovery

～既知のテロ関係者から手繰り発見する。

③ テロ容疑者の発見 Target Discovery

～ネット空間における行動分析から発見する。

欧米のテロ対策の重点はサイバー空間

日本では？

○ サイバー空間で必要な情報活動の枠組

<セキュリティ・サービス> <シギント機関>

<行政傍受>

3-1 (3) インテリジェンス組織

	セキュリティ・サービス	ヒューミント	シグイント	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

3-1 (4) シギントの重要性

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プレーヤー
でなかったテロ調査・捜査というのは
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。」

内 容

序 問題意識

1 認識と思考におけるギャップ

2 情報収集手法の違い

3 サイバー空間

3-1 サイバー空間の重要性

3-2 NSAとUKUSAシグント同盟

3-2-1 シグント同盟と収集態勢

3-2-2 収集プラットフォーム

3-3 シグントによるテロ対策

4 その他の課題

まとめ

3-2-1 (1) UKUSAシギント同盟

- 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 UKUSA、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

3-2-1 (2) 米国NSA

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・沿岸警備隊のシグント部隊を指揮下に。

○ 予算：

2018会計年度諜報機関予算

国家諜報予算＋軍諜報予算＝合計

594億ドル 212億ドル 815億ドル

2013年

シグント予算＝NSA108億＋NRO＋軍予算他

総計、200億ドル、2兆円規模？

3-2-1 (3) 英・加・豪・NZ

Second Party諸国

英: GCHQ政府通信本部: 約6千人、15億ポンド+

加: CSE通信保全局: 約2千人、5億カナダドル程度?

豪: ASD豪信号局: 約2千人

NZ: GCSB政府通信保全局: 430人、1億6千NZドル

共同の収集分析、共同のシステム構築など
統合運用の段階

3-2-1 (4) 協力組織・国

(1) SSO (Special Source Op. 特別資料源作戦)

民間企業の協力を得て行うシグント資料収集
NSAの収集データの内、コンテンツ情報の60%、
メタデータ情報の75%近くを占める

(2) Third Partyとの協力(パートナー&標的、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、インド、日本、
台湾、パキスタン

3-2-2 収集プラットフォーム

NSAの主要な収集プラットフォーム

- (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) 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

3-2-2 (1)「プリズム」計画

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

(参考)2013年中に約2億5千万件以上のデータを取得

3-2-2 (2) 通信基幹回線

世界中で通信基幹回線から収集

- 企業協力 **4計画**
 - 「ブルーニー」(米国内) 30社以上、アクセス拠点70ヶ所以上
 - 「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諸国小計画4つ (米国外)
 - 「ランパート A」~Third Party 小計画多数 (米国外)
- 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」
 - 名称不明の1計画

3-2-2 (3) 衛星通信の傍受

世界各地で衛星通信を受信

○ 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 : 豪ジェラルドトン、豪シヨアルベイ、
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)

3-2-2 (4) 特別収集サービス

SCS (Special Collection Service)

- CIAとNSAの共同事業
- 米大使館・領事館 ～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
- その他UKUSA諸国の外交施設にも設置

3-2-2 (5) CNE(コンピュータ網資源開拓)

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

参考:『米国国家安全保障庁の実態研究』2015年警察政策学会資料第82号

内 容

序 問題意識

1 認識と思考におけるギャップ

2 情報収集手法の違い

3 サイバー空間

3-1 サイバー空間の重要性

3-2 NSAとUKUSAシグント同盟

3-3 シグントによるテロ対策

4 その他の課題

まとめ

3-3 テロ対策への貢献：米国

(1) 2009年9月NY地下鉄同時自爆攻撃未遂事件

NSAは(FISA702条収集で)、アルカイダ連絡員(パキスタン拠点)のEメールアドレスを監視。9月上旬米国内の不明人物から同アドレスへのメール複数を捕捉。爆弾の作成方法の詳細について緊急に助言を求めていると推定し、FBIに通報。

FBIはNSLを発出して情報収集、コロラド州のナジブラ・ザジと特定。FBIは、秘密搜索やインターネット監視など、徹底した監視を実行。ザジは高校の同窓生2人と、NY市マンハッタンでTATP爆弾による地下鉄自爆攻撃(3箇所)を計画。

ザジは10日にNY市に移動したが、警察やFBIによる監視に気が付き、テロ実行を中止して爆弾材料を処分し、コロラドに戻ったが、逮捕された。

出典：PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of the FISA*, 2 July 2014

3-3 テロ対策への貢献：米国

(2) 外国のテロ対策への貢献

事例① FISA702条収集によって某国内にアルカイダ同調者を発見。CIAが当該国政府に通報。

同国政府機関は、同人を調査した上で、協力者として獲得。

同人は同国内のアルカイダとIS関係者に関して情報を提供。

事例② CIAが、FISA702条収集(プリズム)によって

写真他の詳細情報を入手してアフリカ某国政府に提供。

同政府は、IS戦闘員2名を逮捕。同人らはトルコから入国し、米国人と米国権益に対する近々の攻撃計画に関与。

逮捕により、CIAはISの組織や攻撃計画に関する情報を獲得。

出典：ODNI, *The FISA Amendments Act: Q&A*, 18 April 2017

3-3 テロ対策への貢献：英国

(1) 2007年英国兵士に対する誘拐殺人テロ阻止

テログループが、英国内でイスラム教徒の英国兵士を誘拐し殺害を立案。犯行状況をビデオ撮影し、海外関係者に送信して海外で公開企図。通信メタデータの通信パターン分析により、セキュリティと諜報諸機関は、同グループを発見。

警察が関係施設の搜索、誘拐殺人計画を確認。

(2) 2014年西側某国における爆弾テロ阻止

セキュリティと諜報諸機関のシグント情報の分析から、シリア内IS関係過激派と接触を持っている某国の者を特定。更なる分析により、同人が最近欧州の某国を訪問したこと、テロ攻撃を計画していることが判明。関係国政府に情報を提供。同国政府は攻撃を阻止、手製爆弾数個を押収。

出典： UK Home Office、*Operational Case for Bulk Powers*, 1 March 2016

参考「オサマ・ビンラディンを追え(下)テロ対策に活用できるシグント能力」『現代警察』第157号

内 容

序 問題意識

1 認識と思考におけるギャップ

2 情報収集手法の違い

3 サイバー空間

3-1 サイバー空間の重要性

3-2 NSAとUKUSAシグント同盟

3-3 シグントによるテロ対策

4 その他の課題

まとめ

4 その他の課題

平成28年版『警察白書』特集：米英仏独の対策例

◎ テロ関係情報の集約・分析

2017年7月「セキュリティ情報センター」(警察庁)

2018年8月「国際テロ対策等情報共有センター」

(内閣官房)

◎ テロ周辺行為(準備、支援、唱道など)犯罪化

2017年テロ等準備罪制定で充足されたのか？

◎ 通信傍受(行政傍受)

◎ テロ関係容疑者に対する各種行動制限

身体拘束、居住制限、出入国制限等

4 その他の課題

他の諸課題

- ◎ **業務情報(金融・通信等)の安全保障目的収集**
 - 個人情報保護法の解釈問題？
 - 米National Security Letter
- ◎ **通信メタデータの扱い**
 - 通信メタデータは「通信の秘密」に含まれない(諸外国)
 - 通信履歴の保存義務
- ◎ **重要施設従業員の適格性の審査制度**
 - 原発、原子力関連だけ？
- ◎ **外国人管理の思想**
 - 出入国管理
 - 在留管理の担保措置(住民登録情報、宿泊カード他)

4 その他の課題

＜通常の民主主義国家にあるもの＞

◎ 調査権限を持つセキュリティ・サービス

調査権限～通信傍受、侵入的監視、潜入他

憲法35条の問題～行政通信傍受・監視裁判所の設置？

調査権限～一般行政・業務情報へのアクセス権

◎ 調査権限を持つ国家シグント機関

通信事業者の協力義務

◎ 総合治安担当省（＝内務省）

通常、内務大臣の指揮下にある関係機関

警察（警察庁）、セキュリティ・サービス（？）、

国境警備（海上保安庁）、外国人管理（入管庁）、消防

総合治安に責任を有する閣僚が不在

内 容

序 問題意識

- 1 認識と思考におけるギャップ
- 2 情報収集手法の違い
- 3 サイバー空間
 - 3-1 サイバー空間の重要性
 - 3-2 NSAとUKUSAシグント同盟
 - 3-3 シグントによるテロ対策
- 4 その他の課題

まとめ

まとめ

- ★ 脆弱性と不十分性の自覚
- ★ 実態を前提とした議論

- 欧米型のテロ対策に進むのか？
- 違いを認識しつつ現状の構造を維持？

- ※ 情報収集力の弱体は
スパイ対策の弱体や
サイバーセキュリティ対策の弱体とも関連

内 容

序 問題意識

1 認識と思考におけるギャップ

2 情報収集手法の違い

3 サイバー空間

3-1 サイバー空間の重要性

3-2 NSAとUKUSAシグント同盟

3-3 シグントによるテロ対策

4 その他の課題

まとめ

ご清聴ありがとうございました。

shigeta.tadayoshi@nihon-u.ac.jp

内容

- 1 テロ対策～世界標準と日本
- 2 NSA概観とシギントシステム
- 3 シギントによるテロ対策
- 4 我が国に欠けているもの

ご清聴ありがとうございました。