テロ対策とシギント
～我が国の課題～

2019年1月29日

日本大学　危機管理学部
茂田忠良

内　容

１　テロ対策～世界標準と日本

（１）　警察白書『国際テロ対策』特集

（２）　情報収集手法の違い

（３）　サイバー空間の重要性

２　NSA概観とシギントシステム

（１）　概観

（２）　収集態勢～協力組織

（３）　収集態勢～プラットフォーム

３　シギントによるテロ対策

（１）特に有用なツール

（２）テロ対策への貢献

４　我が国に欠けているもの

1（1）警察白書『国際テロ対策』特集

平成28年版警察白書『国際テロ対策』特集

○　平成27年警察庁国際テロ対策要綱の紹介

現行の制度枠組の延長線で実施可能な対策を列挙

私見～実施したからと言って十分ではない。

○　米英仏独における対策の紹介

- テロ関連情報の一元化
- テロ周辺行為（準備、支援、唱道など）の犯罪化
- 通信傍受（行政傍受）
- テロ関係容疑者の行政拘束などの行政権限

私見～実現不可能であるが、テロ防止には必要な権限

１（２）情報収集手法の違い

○　我が国

協力者

事件捜査

警察の総合力

行動確認

テロリスト

ウェブサイト
の情報収集

１（２）情報収集手法の違い

○　諸外国

広汎な行政権限

協 力 者

屋外監視カメラ

潜入

囮

事件捜査

行動確認

マイク

カメラ

信書開披

通信傍受

テロリスト

サイバー空間の監視

1（3）サイバー空間の重要性

○ サイバー空間の重要性

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
- 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（例：2008年ラシュカル・エ・タイバ）
- 活動資金調達
- サイバー・テロ（例：2017年CyberCaliphate）

○ サイバー空間における対テロ活動の重要性

謂わばサイバー空間における容疑者の発見、追跡、監視

欧米のテロ対策の重点はサイバー空間

日本では、治安機関にとってブラックボックス？

○ サイバー空間で必要な情報活動の枠組

シギント機関、セキュリティ・サービスによる活動

＜未然防止のための行政傍受＞

１（３）サイバー空間の重要性

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。」

註：NSA（国家安全保障庁）米国のシギント機関

1（3）サイバー空間の重要性

	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

内　　容

１　テロ対策～世界標準と日本

（１）　警察白書『国際テロ対策』特集

（２）　情報収集手法の違い

（３）　サイバー空間の重要性

２　NSA概観とシギントシステム

（１）　概観

（２）　収集態勢～協力組織

（３）　収集態勢～プラットフォーム

３　シギントによるテロ対策

（１）特に有用なツール

（２）テロ対策への貢献

４　我が国に欠けているもの

2（1）NSA概観

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。

○ 予算 ：

2013年度諜報機関予算

国家諜報予算＋軍諜報予算＝合計

526億ドル 192億ドル 718億ドル

（約8兆円）

シギント予算＝NSA108億＋NRO＋軍予算他

総計、200億ドル、2兆円規模？

２　NSA概観

NSA本部（フォートミード）全景

2（2）収集態勢傍受施設500ヶ所、主要施設150箇所

漏洩されたパワーポイント資料・2008年2月25日付

２（２）収集態勢～協力組織①

（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ギント資料収集

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

（２）Second Party諸国（UKUSA, FVEY）との協力

1946年BRUSA協定。1954年UKUSAに改称

英GCHQ政府通信本部（約６千人）

加CSE通信保全局（約２千人）～1949年正式参加

豪ASD豪信号局 （約２千人）～1953年正式参加

NZ・GCSB政府通信保全局 （３百人）～1953年正式参加

共同の収集分析、共同のシステム構築。統合運用の段階

２（２）収集態勢～協力組織②

（３）Third Partyとの協力（パートナー＆標的、ギブ＆テイク）

（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

○　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）

２（３）収集態勢～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

（２） 通信基幹回線からの収集

（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

２(３)－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

（漏洩資料）「プリズム」計画


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

2(3)ー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

「ブラーニー」(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＆サード・パーティの協力　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」～サード・P　小計画多数　　(米国外)

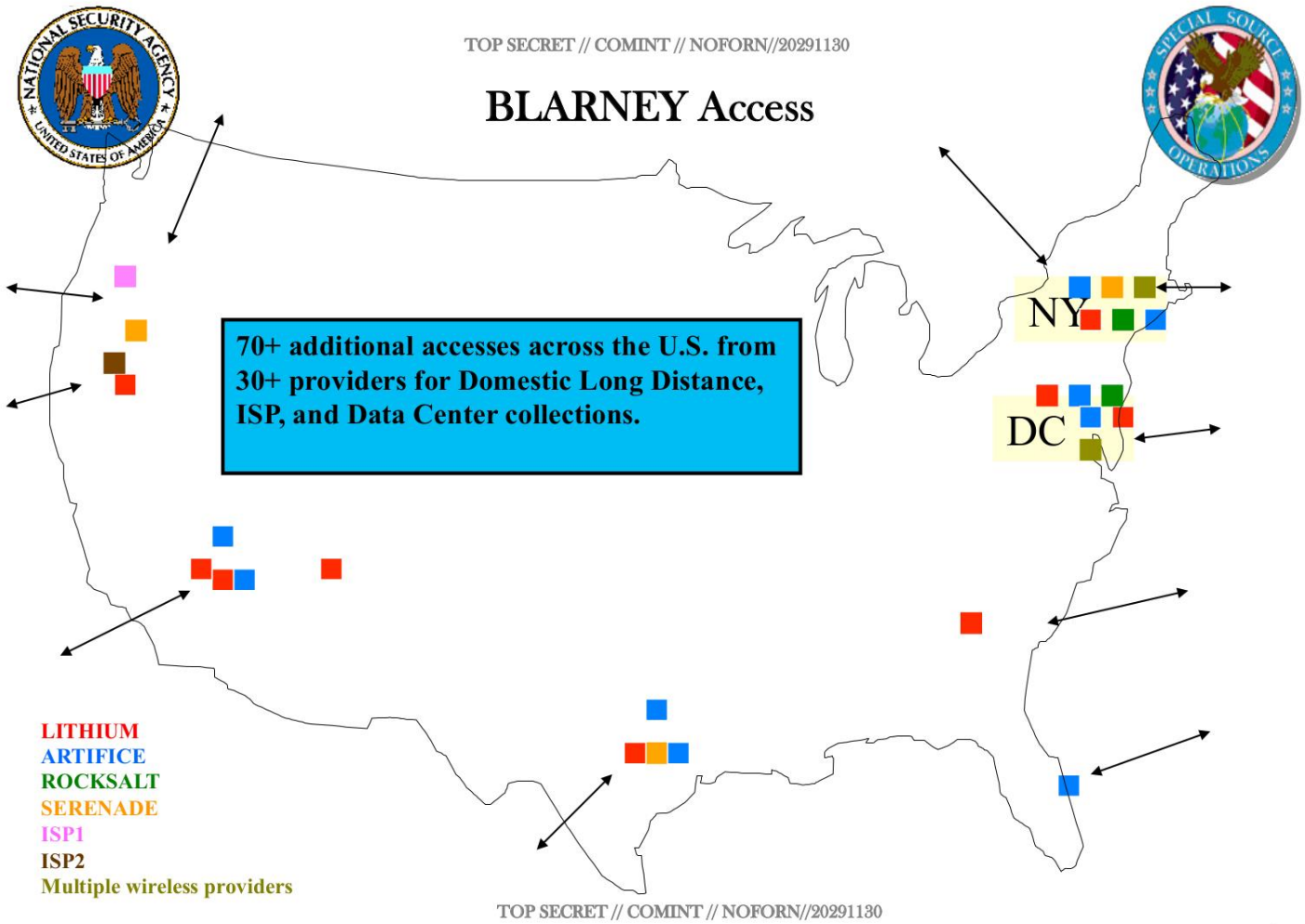
○　単独事業　　5計画　　(米国外)

「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

（漏洩資料）ブラーニー米国内



2(3)－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

欧州　　：　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）

衛星通信傍受施設の一部

○

日本・三沢基地

英国メンウィズ・ヒル

(漏洩資料)衛星通信傍受施設

２（３）－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

特別収集サービス施設の一例

在ベルリン米国大使館

2（3）－⑤CNE

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

内　容

１　テロ対策～世界標準と日本

（１）　警察白書『国際テロ対策』特集

（２）　情報収集手法の違い

（３）　サイバー空間の重要性

２　NSA概観とシギントシステム

（１）　概観

（２）　収集態勢～協力組織

（３）　収集態勢～プラットフォーム

３　シギントによるテロ対策

（１）特に有用なツール

（２）テロ対策への貢献

４　我が国に欠けているもの

３　シギントによるテロ対策

○　テロ対策へのシギントの貢献

①　テロ容疑者の容疑を解明する。

②　テロ容疑者を発見する。

～～既知のテロ関係者から手繰り発見する。

③　テロ容疑者を発見する。

～～ネット空間における行動分析から発見する。

○　特に有用なツール

☆　XKeyscore

☆　メタデータ分析

３（１）有用ツール①XKeyscore

XKeyscore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カ所、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「グーグル」
  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

(漏洩資料)X-KEYSCORE

漏洩されたパワーポイント資料・2008年2月25日付

３（１）有用ツール②メタデータ分析

＜メタデータ＞

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）

SNS活動

ネットワーク閲覧履歴（訪問ウェブサイト、
ログイン時刻、地図検索履歴等）

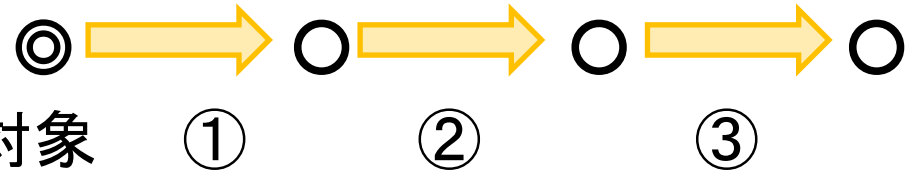
位置情報等

３（１）有用ツール②メタデータ分析

ア　どう使うか。

対象者が如何なる人物であるか、浮き彫りに

○　接触連鎖分析（contact chaining）



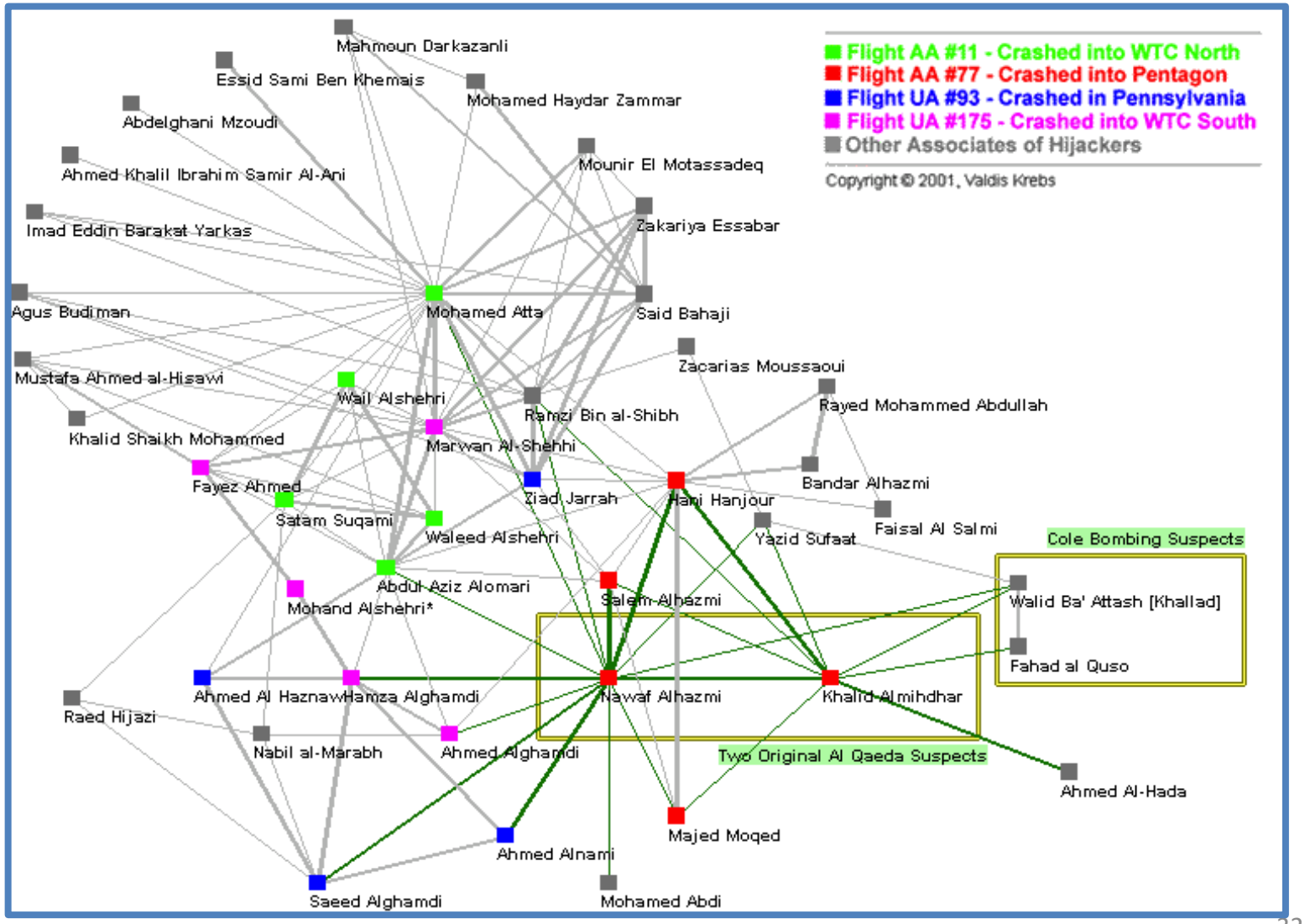
○　人物分析

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が判明する。人物の全体像を把握可能。

（漏洩資料）メタデータ分析の一例

接触連鎖分析の一例（9／11実行犯の連鎖分析）



３（１）－②メタデータ分析　FASCIA

イ　FASCIA（位置情報メー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

○　不審者の割出

○　Co-Traveler分析（同伴者・仲間の探知）

○　Fast-Follower分析（監視の探知）

３(２)テロ対策への貢献①

①　テロ容疑者の容疑を解明する

○　ネットワーク閲覧履歴やSNSによる人物分析

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

○　付加情報～フェイスブック・プロファイル、銀行口座情報、保険情報、旅客名簿、選挙人名簿、財産情報、税務情報

（国内であればFBI、外国であれば当地のセキュリティ・サービス）

○　行動監視も出来る（携帯、スマートフォン）

FASCIA位置情報データベースの活用

○　更には、同人のスマートフォン攻略

データ内容の取得、監視機材として転用

３(２)テロ対策への貢献②

②　テロ容疑者を発見する～既知の関係者から

○　既知の関係者の通信監視（メール、通話）

○　接触連鎖分析（contact chaining）

データベース「メインウェイ」「マリーナ」

「ICリーチ」～IC全体のための分析システム

主要組織：NSA、CIA、FBI、DIA、DEA

○　同伴者分析

位置情報データベース（FASCIA）を使用

テロ容疑者と同様の行動を取る者を発見

３(２)テロ対策への貢献③

③ テロ容疑者を発見する～行動分析から

○ XKeysore活用例

- シリアからのPGP暗号通信を検索抽出。
- パキスタンからのドイツ語通信を検索抽出。
- 英語、中国語、アラビア語についてはコンテンツのキーワード検索が可能。（特定人に言及した通信など）
- グーグルマップの検索利用状況（テロの調査活動）から、テロ容疑者を抽出。
- 特定の単語での検索や特定のウェブサイトを検索した者の検索抽出。

独BfVは、XKeyscoreソフトウェアの提供を受ける。
（BfVも国内通信メタデータを大量に取得）

３(２)テロ対策への貢献③

③　テロ容疑者を発見する～行動分析から

○「レヴィテーション」計画（カナダCSE）

- 無料ファイル共有サイトへのアクセス監視

  世界の１０２サイトの特定部分2200ヶ所を監視

- 容疑IPアドレスの取得　⇒容疑解明

○「通信保全活動」をする者を発見

位置情報データベース（FASCIA）を使用

- 通話時だけ電源を入れる
- 幾つもの携帯電話を使い分ける
- 使い捨て携帯電話の使用

○　オンライン・ヒューミント

過激派の集うチャット・ルームへの参入、

CNEによるIPアドレス取得（TORなど暗号化ソフトを破る）

内　容

１　テロ対策～世界標準と日本

（１）　警察白書『国際テロ対策』特集

（２）　情報収集手法の違い

（３）　サイバー空間の重要性

２　NSA概観とシギントシステム

（１）　概観

（２）　収集態勢～協力組織

（３）　収集態勢～プラットフォーム

３　シギントによるテロ対策

（１）特に有用なツール

（２）テロ対策への貢献

４　我が国に欠けているもの

４　我が国に欠けているもの

＜通常の民主主義国家にあるもの＞

◎　行政権限を持つ国家シギント機関

通信事業者の協力義務

◎　行政権限を持つセキュリティ・サービス

行政権限～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？

行政権限～一般行政情報へのアクセス権

◎　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

４　我が国に欠けているもの

◎　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）

○　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

原発関連だけ整備。特定秘密保護法もザル。

○　行政情報、金融・通信情報の安全保障目的収集

（行政機関）個人情報保護法の解釈問題？　　米NSL

○　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

○　テロ周辺行為（準備、支援、唱道など）犯罪化

（註・後二者については、平成28年版『警察白書』参照）

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。