インテリジェンス講義

サイバーセキュリティとNSA/UKUSA

2025年2月

茂田インテリジェンス研究室

目　次

１　NSA/UKUSAシギント同盟［基礎知識］

２　TAO（Computer Network Operation）

３　UKUSAシギント諸機関のCS任務

４　CSのための作戦とプログラム

５　NSAと米サイバー司令部との協力関係

目　次

１　NSA/UKUSAシギント同盟[基礎知識]

１－１ インテリジェンスの種類

１－２　UKUSAシギント同盟

１－３　シギント収集態勢の骨子

１－４　X-Keyscore

２　TAO（Computer Network Operation）

３　UKUSAシギント諸機関のCS任務

４　CSのための作戦とプログラム

５　NSAと米サイバー司令部との協力関係

1－1　インテリジェンスの種類

＜機能＞	＜主な組織＞
◇ ヒューミント（人的諜報） human intelligence	◆ CIA（中央諜報庁） Central Intelligence Agency
◇ シギント（信号諜報） signals intelligence	◆ NSA（国家安全保障庁） National Security Agency
◇ イミント（画像諜報） imagery intelligence	◆ NGA（国家地理空間諜報庁） National Geospatial-Intelligence Agency
◇ マシント（計測・特徴諜報） measurement and signature intelligence	◆ DIA（国防諜報庁） Defense Intelligence Agency
◇ セキュリティ・サービス （スパイ対策、テロ対策、国家転覆阻止、大量破壊兵器拡散防止WMD）	◆ FBI（連邦捜査局） National Security Branch （*national security service*と指定）

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

1−2　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

（参考） 米国NSA本部

https://commons.wikimedia.org/w/index.php?curid=16450

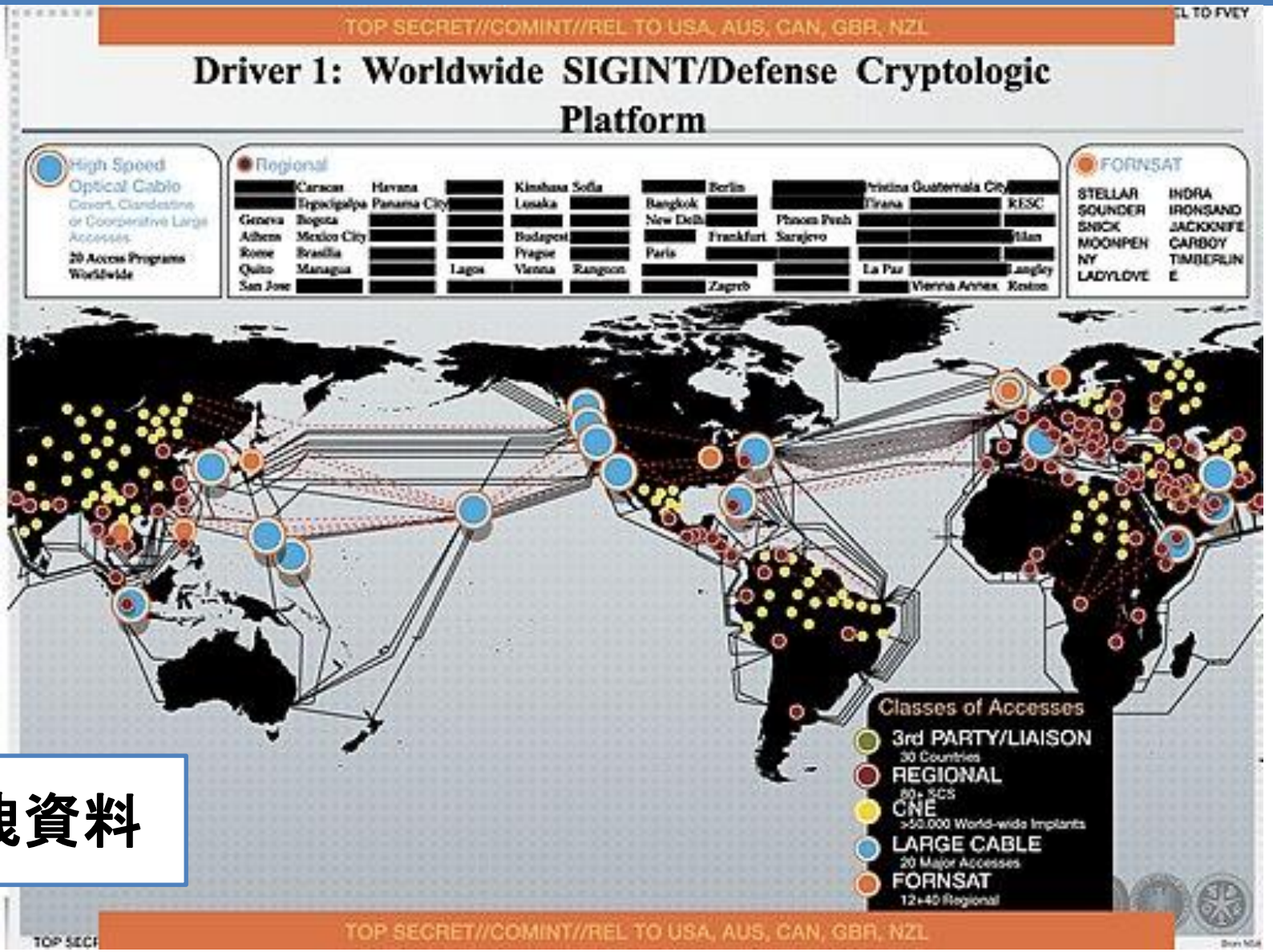
NSA本部（フォートミード）全景

（参考） 英国GCHQ本部

https://commons.wikimedia.org/wiki/File:GCHQ-aerial.jpg

GCHQ本部（チェルトナム）全景

1－3　シギント収集態勢①漏洩資料



漏洩資料

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

１－３　シギント収集態勢②

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（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

1−4　X-Keyscore（NSA版「グーグル」）①

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

1−4　X-Keyscore（NSA版「グーグル」）②

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

○ サイバーセキュリティ対策、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”

目　次

１　NSA/UKUSAシギント同盟[基礎知識]

２　TAO（Computer Network Operation）

　２－１　任務

　２－２　組織

　２－３　ANT　（ハッキングツール制作部門）

　２－４　遠隔侵入

　２－５　物理的侵入

　２－６　C-CNE　（ハッカー集団をハッキングする）

３　UKUSAシギント諸機関のCS任務

４　CSのための作戦とプログラム

５　NSAと米サイバー司令部との協力関係

2-1　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

2-2 組織

（1） 侵入作戦実施部門

○ 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

2-3　ANT：製品カタログ

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

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

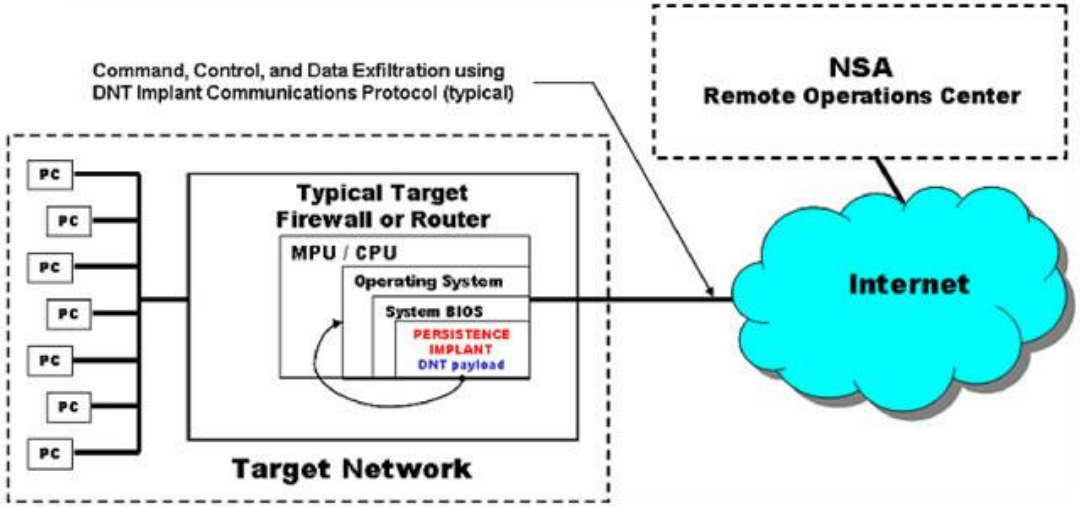
JETPLOW

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

漏洩資料



(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

2-4　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.”

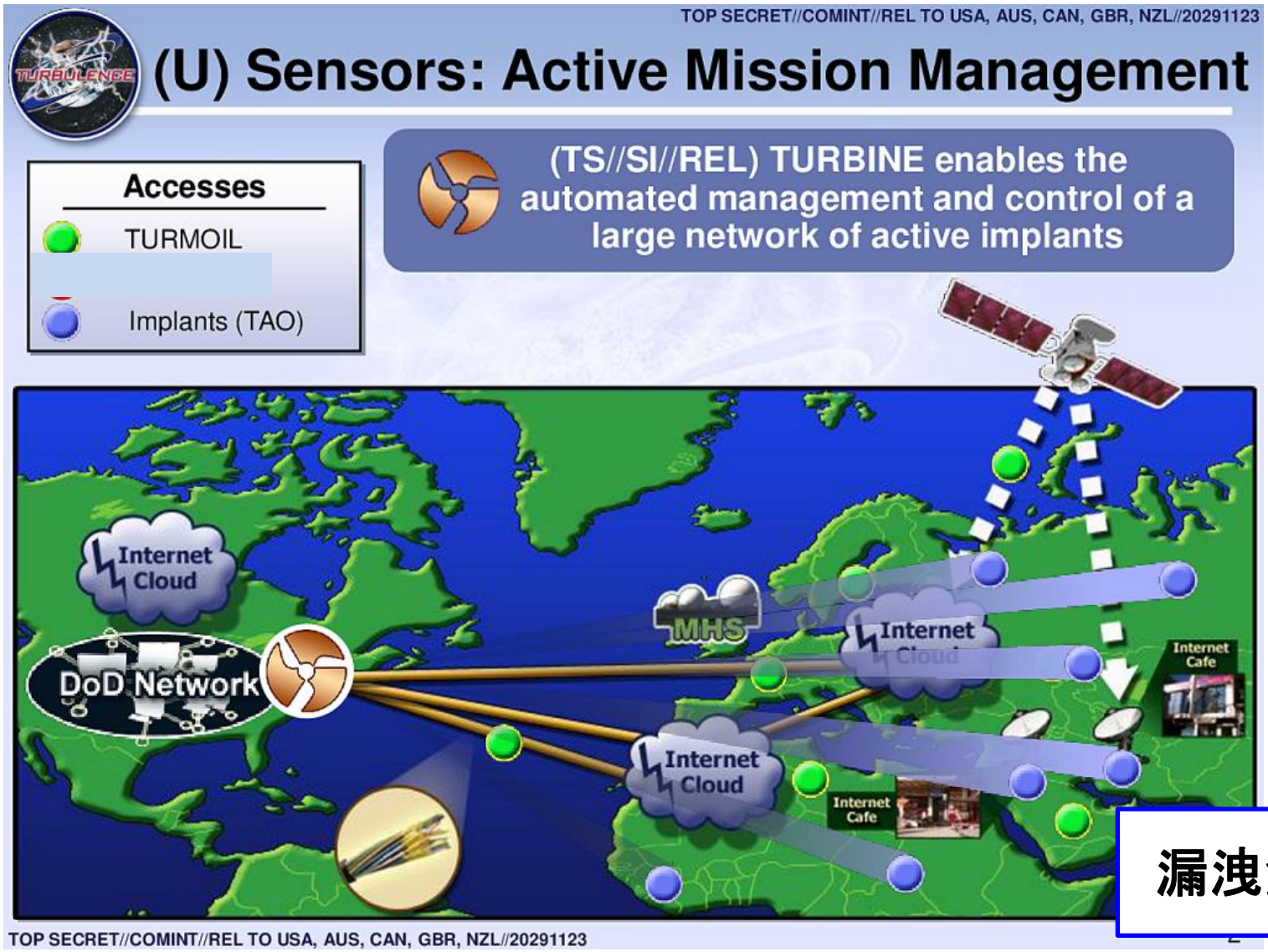
（2）主な手法

○　スパムメール　～今や（2013年時点）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

2-4　遠隔侵入②「クオンタム」概念図



漏洩資料

2-5　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①　Crypto AG
- ○　供給網工作～（製造）企業工作②　Cavium製CPU
  ～配送経路介入③
- ○　外国公館工作④

2-5 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

2-5　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　　中国？ロシア？イラン？NK？

○　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

2-6 C-CNE① 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ISP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

2-6 C-CNE② 対北朝鮮

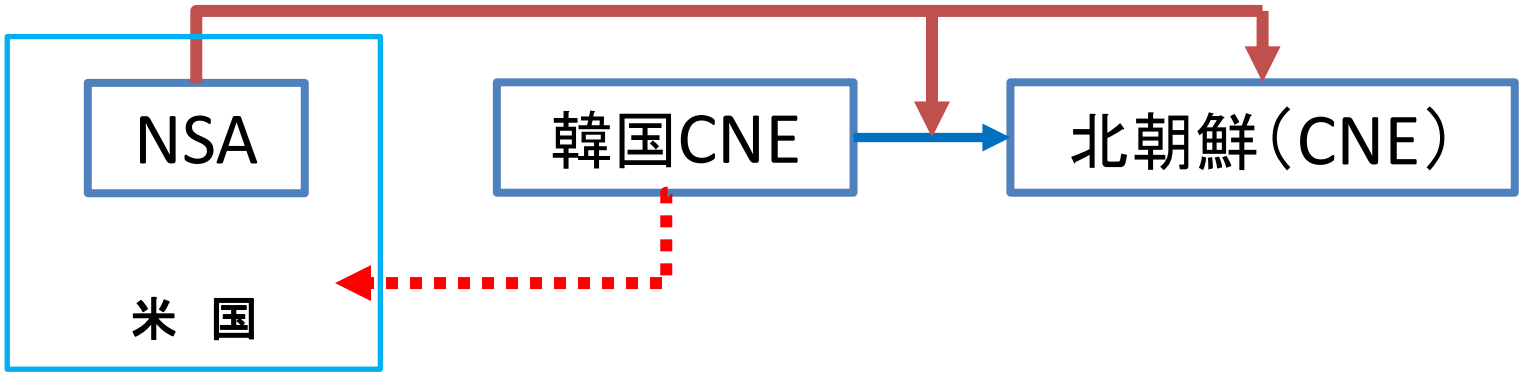
対北朝鮮C-CNE

○ 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を解明



＜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

１　NSA/UKUSAシギント同盟［基礎知識］

２　TAO（Computer Network Operation）

３　UKUSAシギント諸機関のCS任務

　３－１　シギント機関のCS任務

　３－２　CSにはシギントが不可欠

　３－３　シギント機関のCS取組例（公然面）

４　CSのための作戦とプログラム

５　NSAと米サイバー司令部との協力関係

3-1　シギント機関のCS任務

□　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）

3-2　CSにはシギントが不可欠

CS（Cyber Security）にはシギントが不可欠。

○　シギントによる知見・技術

- 「攻撃方法を知る者が、良く防禦できる」

  CNE（ Computer Network Exploitation）

  コンピュータ網資源開拓＝ハッキング

○　シギント・インフラの貢献

- UKUSA：全世界に及ぶシギント・インフラとプログラム

  X-Keyscore、宝地図（Treasure Map）、Eonblue　など

○　C-CNE の貢献（攻撃阻止、反撃のため）

（C-CNE＝counter-CNE）

- ハッカー集団をハッキング、”逆ハッキング“

  具体的な脅威情報の事前把握

3-3　シギント機関のCS取組例①

（1）指導・助言・警告　NSA

CS Advisories（助言）、Operational Risk Notices（脅威告知）

Tech. Reports（技術情報） Info. sheets（参考情報）

（2）技術提供　NSA

Open Source @NSA（CSソフトウェア無償提供）

Cybersecurity Solutions Service（企業、研究機関等にに技術供与）

（3）教育研究　NSA

○　CS優秀教育機関・優秀研究機関の認定

National Centers of Academic Excellence in Cybersecurity

3種：CAE-CD（防禦）、CAE-R（研究）、CAE-CO（CNEを含む）

○　NSAサイバー演習（主対象：各種士官学校、商船大学）

○　NSA「セキュリティ科学イニシアティヴ」

3-3　シギント機関のCS取組例②

（4）システム構築

- ○　米NSA:　National Security Systemsの責任者
- ○　NZ・GCSB : Top Secret Networkの設計調達

（5）事案対応　Incident Response　英NCSC

- ○　NCSC事案管理チーム（Incident Management team）
  CS事案を6区分。重要3区分はNCSCに指導グループ設置
- ○　CSサービス会社認定制度（2018年現在23社を認定）
- ○　被害組織、サービス企業、NCSCの三者で協議対応
  シギント情報を活用。特別重大事案：NCSC職員現場派遣
- ○　事例：2017年5月WannaCryマルウェア大量感染事案対応

- ◆　Attribution（攻撃者の探知特定）支援
- ◆　Active Cyber Defense, Dynamic Defense
- ◆　Defend Forward（前方防禦）支援

目　次

１　NSA/UKUSAシギント同盟［基礎知識］

２　TAO（Computer Network Operation）

３　UKUSAシギント諸機関のCS任務

４　CSのための作戦とプログラム

　４－１　Attribution支援

　４－２　Active Cyber Defense等

５　NSAと米サイバー司令部との協力関係

4-1　Attribution支援　ソニー

（例）「ソニー・ピクチャーズ」攻撃の解明（2014年）

6月　北鮮外務省、映画「インタビュー」絶対容認できないと声明

11月24日　数千台の端末から全データ消去。情報漏洩開始。

12月19日　FBI、北朝鮮の犯行と断定、広報。

2020年　　北鮮偵察総局員3名（Razarus, APT38）起訴

■ **NSAの貢献**　2015年NSA長官、公開の会議で、特定には
NSAの技術力とデータが貢献したと言明。

■ **貢献したと考えられるプログラム**

○ **X-Keyscore**　2016年スノーデン・インタビュー

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

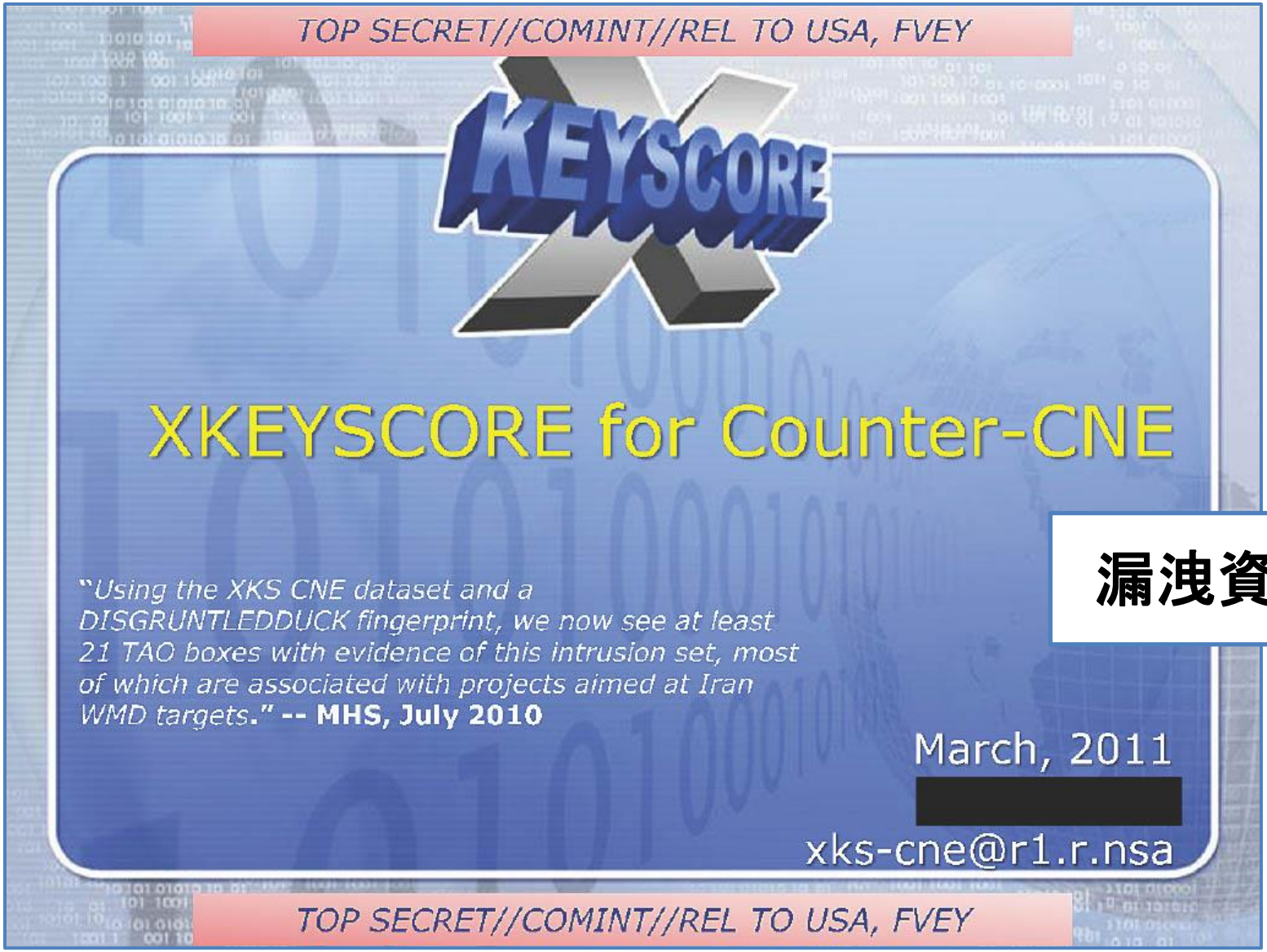
漏洩資料　NSA, “XKEYSCORE for Counter-CNE”

○ **C-CNE**

○ **プリズム**（Gメールなどウェブメール情報）　○宝地図

。

漏洩資料　X-Keyscore



漏洩資料

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

4-2 Active Cyber Defense 等①

■ 米英 Active Cyber Defense, Active Dynamic Defense

脅威情報の事前把握、
インターネット接続点における対抗措置の事前設置

■ 加 Dynamic Defense

次の3要素を統合して実施
①インターネットとの接続点での防禦
②インターネット空間におけるシギント活動
③敵空間でのCNE（マルウェア等TTPs等の解明）

4−2　ACD等　②インターネット空間

インターネット空間での脅威把握

◆　加CSEのEONBLUE

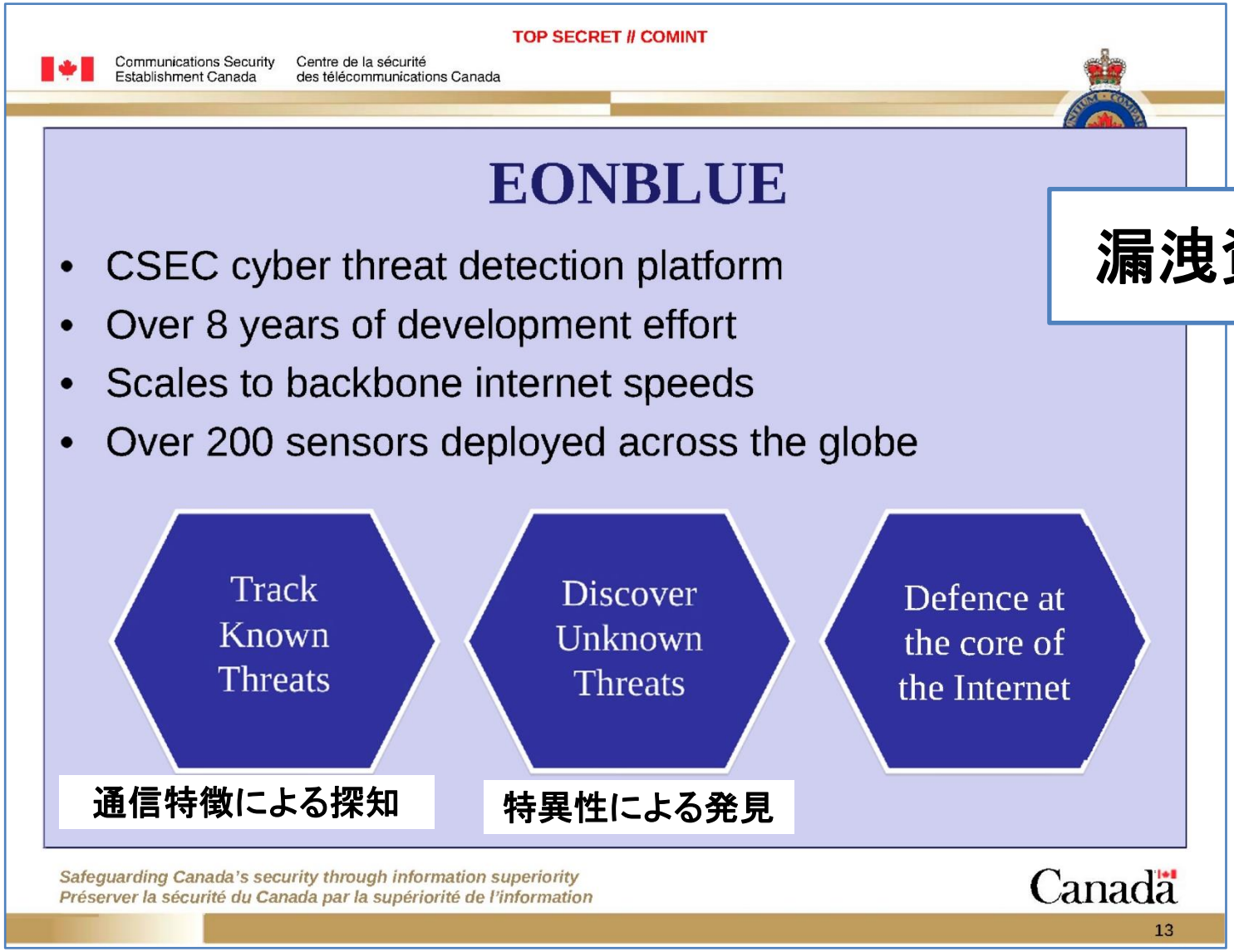
- 2010年頃。脅威探知センサー：世界に200以上設置
  UKUSA諸機関の協力を得て、シギント・インフラを活用
- 探知手法：anomaly-based discovery（SLIPSTREAM）
  通信の特異性に基づく発見
  signature-based detection（SNIFFLE）
  通信の特徴を基に探知

◆　英GCHQのLOVELY HORSE

ハッカーのブログやチャットルームなどソーシャルメディアでの議論
（ハッキング技術の誇示、窃取データの公開など）自動的に収集分類

⇒　今や、民間企業サービス

漏洩資料　EONBLUE



漏洩資料

https://grid.glendon.yorku.ca/exhibits/show/security-classification/item/495

4-2　ACD等　②インターネット空間

インターネット空間での脅威把握

◆　加CSEのEONBLUE

- 2010年頃。脅威探知センサー：世界に200以上設置
  UKUSA諸機関の協力を得て、シギント・インフラを活用
- 探知手法：anomaly-based discovery（SLIPSTREAM）
  通信の特異性に基づく発見
  signature-based detection（SNIFFLE）
  通信の特徴を基に探知

◆　英GCHQのLOVELY HORSE

ハッカーのブログやチャットルームなどソーシャルメディアでの議論
（ハッキング技術の誇示、窃取データの公開など）自動的に収集分類

⇒　今や、民間企業サービス

4-2　ACD等　③Tutelage

- **米Tutelage System**

  【大前提】脅威把握　⇦敵のマルウェア開発準備段階で
  ツールと技術、意図と標的を探知する　⇦C-CNE

  2009年　米国防総省の情報システムNIPERNetに設置
  インターネット接続点～米国内7ヶ所、独2ヶ所、日1ヶ所

  2013年現在、脅威集団28に対して794の対抗策を事前設置
  [推定]当時、中国の12集団以上の内、7～8に浸透。

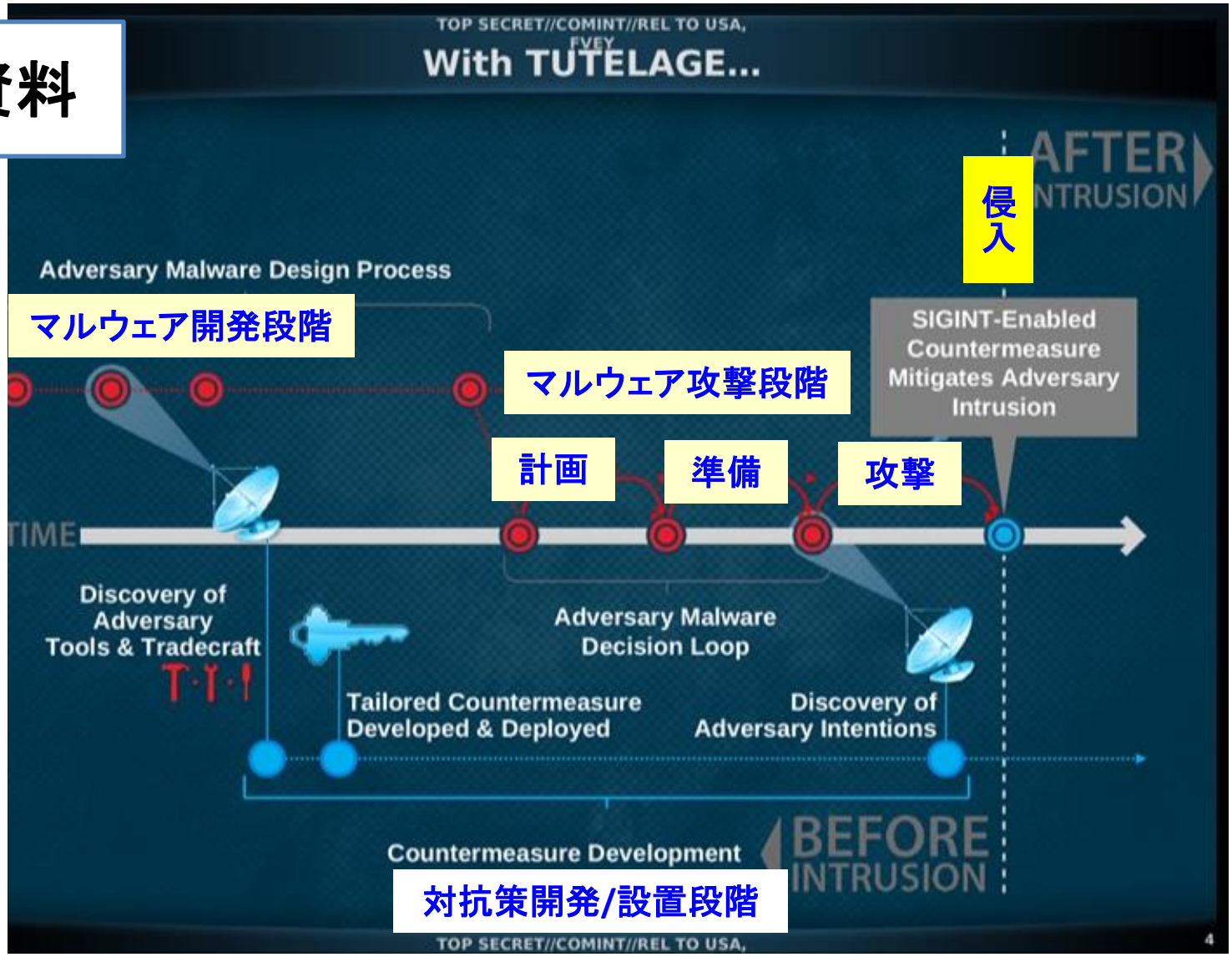
  対抗策：警告、インターセプト、代替、転送、遮断、遅延

  成功例：2010年国防総省高官に対するフィッシング攻撃阻止

- 2013年当時、独米会議でTutelage 導入について議論
- NZ・CORTEXシステム　2017年完成
- 米一般行政官庁用　Einstein 3　～Tutelage導入予定であったが。

漏洩資料　Tutelage

漏洩資料



https://www.aclu.org/foia-document/tutelage

4-2　ACD等　③Tutelage

- **米Tutelage System**

  【大前提】脅威把握　⇦敵のマルウェア開発準備段階で
  ツールと技術、意図と標的を探知する　⇦C-CNE

  2009年　米国防総省の情報システムNIPERNetに設置
  インターネット接続点～米国内7ヶ所、独2ヶ所、日1ヶ所

  2013年現在、脅威集団28に対して794の対抗策を事前設置
  [推定]当時、中国の12集団以上の内、7～8に浸透。

  対抗策：警告、インターセプト、代替、転送、遮断、遅延

  成功例：2010年国防総省高官に対するフィッシング攻撃阻止

- 2013年当時、独米会議でTutelage 導入について議論
- NZ・CORTEXシステム　2017年完成
- 米一般行政官庁用　Einstein 3　～Tutelage導入予定であったが。

（参考）英国ACDの変容と現状

◇ 2016年*National Cyber Security Strategy 2016-2021.*

ACD対象：国家支援型脅威を含む脅威の阻止

◇ 2022年*Government Cyber Security Strategy 2022-2030*

ACD対象：標準的な攻撃からの被害低減
高度に洗練された標的型攻撃はNCSCが別途対応。

■ 脅威の探知・阻止サービス

- ○ テイクダウン・サービス：悪質サイトを発見しホストに除去させる。
  例：暗号資産投資詐欺、ランサム用メールサーバー、フィンシング用URL,など。
- ○ ドメインネーム保護サービス：マルウェア関連のドメインやIPsへの接続遮断
- ○ SERS：疑わしいEメールやウェブサイト情報受けサービス。

■ 警報・自己診断支援サービス

- ○ 早期警戒情報提供サービス
- ○ メールチェック：Eメールドメイン濫用防止。ドメイン所有者支援
- ○ ウェブサイト脆弱性診断：Web Check、Check Your Cyber Security
- ○ サイバー事案訓練キット：Exercise in a Box

■ **攻撃者のサーバーへの侵入・無害化は含まない**

目　次

１　NSA/UKUSAシギント同盟［基礎知識］
２　TAO（Computer Network Operation）
３　UKUSAシギント諸機関のCS任務
４　CSのための作戦とプログラム
５　NSAと米サイバー司令部との協力関係
　５－１　サイバー攻撃力
　５－２　Defend Forward戦略
　５－３　Hunt Forward作戦
　５－４　NSAとの不可分な関係

5-1 サイバー攻撃力offensive cyber capability

＜攻撃力使途＞
- サイバー脅威の無害化（Defend Forward）
  （米）軍事活動（英）インテリジェンス活動（豪）警察活動
- サイバー戦争（武力行使）～軍事活動

□ 米国：サイバー司令部（約6200人）
シギント機関NSAによる全面支援

□ 英国：国家サイバー部隊（約2000人）
国防省、GCHQ（政府通信本部）他、計4機関
対外諜報担当相と国防相の共管

□ 豪州：シギント機関ASD（豪信号局）
ASD内に攻撃部署を設置

5-2　Defend Forward戦略

従前の対策の課題　・　全ハッカー集団の解明は不可能
・　民間インフラ等の防護も重要

Defend Forward（前方防禦）　2018年

○　脅威がインターネット接続点に到達する前に防禦。
⇒敵空間、又はインターネット空間での先制防禦

○「国防総省サイバー戦略」 2018年9月18日要旨公表
Defend Forward　＋　重要インフラも保護対象

「サイバー司令部」担当　NSAが支援

＜例＞2018年中間選挙Synthetic Theology作戦
・露情報作戦担当者へ警告の直接送付
・露Internet Research Agencyサーバーの接続遮断
（NSAとサイバー司令部の合同チームで取組）

＜例＞2021年サイバー司令部　REvil（ランサム）のドメインを乗取って、
インターネットからREvilウェブサイト遮断

5-3　Hunt Forward作戦

Hunt Forward作戦：Defend Forwardの構成要素

外国ネットワークでのマルウェア狩り

- 実施組織：サイバー司令部直轄部隊のCNMF（2千人以上）
- 実施状況：2018年～2023年　27ヵ国55回派遣　ウクライナにも
- 活動手順：ホスト国担当者と協力

  マルウェア、外部侵入、システム脆弱性を調査
  マルウェアなどを発見した場合は、ホスト国に通知
- 対象脅威：ロシア、中国、イラン、北朝鮮
- 米国の利益：脅威国のマルウェアの早期入手。
  戦術、技術、手順TTPs　の探知把握
- 能力の源泉
  - ①　NSAサイバーセキュリティ局との緊密な協力
  - ②　NSA・Cybersecurity Collaboration Center民間協力

（敵対国の）容疑性の高い特定IPアドレス情報を入手。
既知のマルウェアの特徴指標（signatures）を集めたキットを持参

5-4　NSAとの不可分な関係

＜NSA長官とサイバー司令部司令官の兼任＞

◎　NSAによるサイバー司令部支援

専門技術・シギント情報（敵IPアドレス、signatures、TTPs）

＋　海外シギント・インフラ利用　（＋機材の提供）

（CNO＝サイバー司令部の作戦基盤の提供）

◎　NSAとサイバー司令部の共同作戦

（例） 2018年、2020年米選挙対策：合同チーム

サイバー司令部defend forward（CNA攻撃担当）

◎　サイバー司令部によるNSAへの貢献

hunt forward作戦

（malware、signatures、TTPs情報）

- Erica Lonergan and Mark Montgomery,
  United States Cyber Force: A Defense Imperative,
  Foundation for Defense of Democracies, 25 March 2024.

（参考） 米国等の組織関係

NSA
（1952年設立）

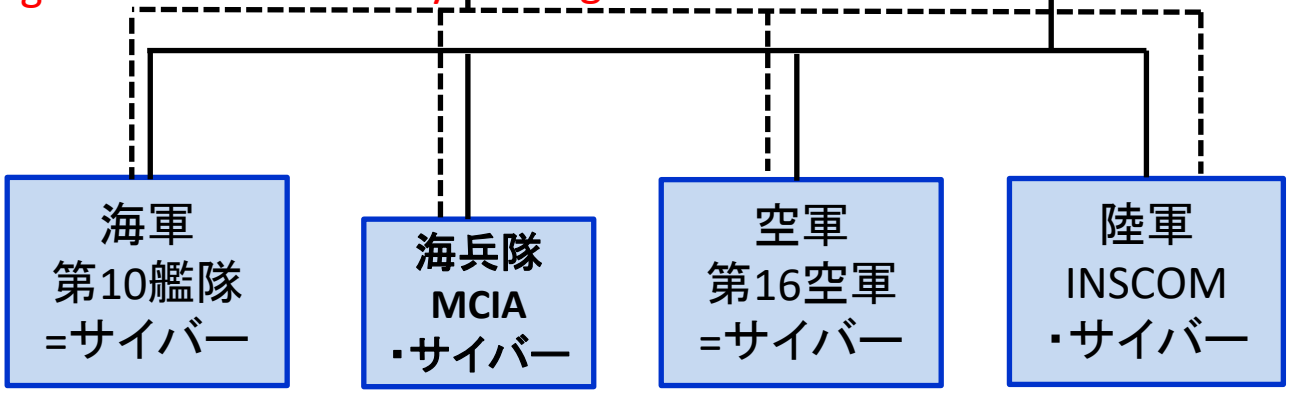
国家シギント
National intelligence

CSS
（1972年附置）

各軍シギントの調整
Military intelligence

サイバー司令部
（2010年設立）

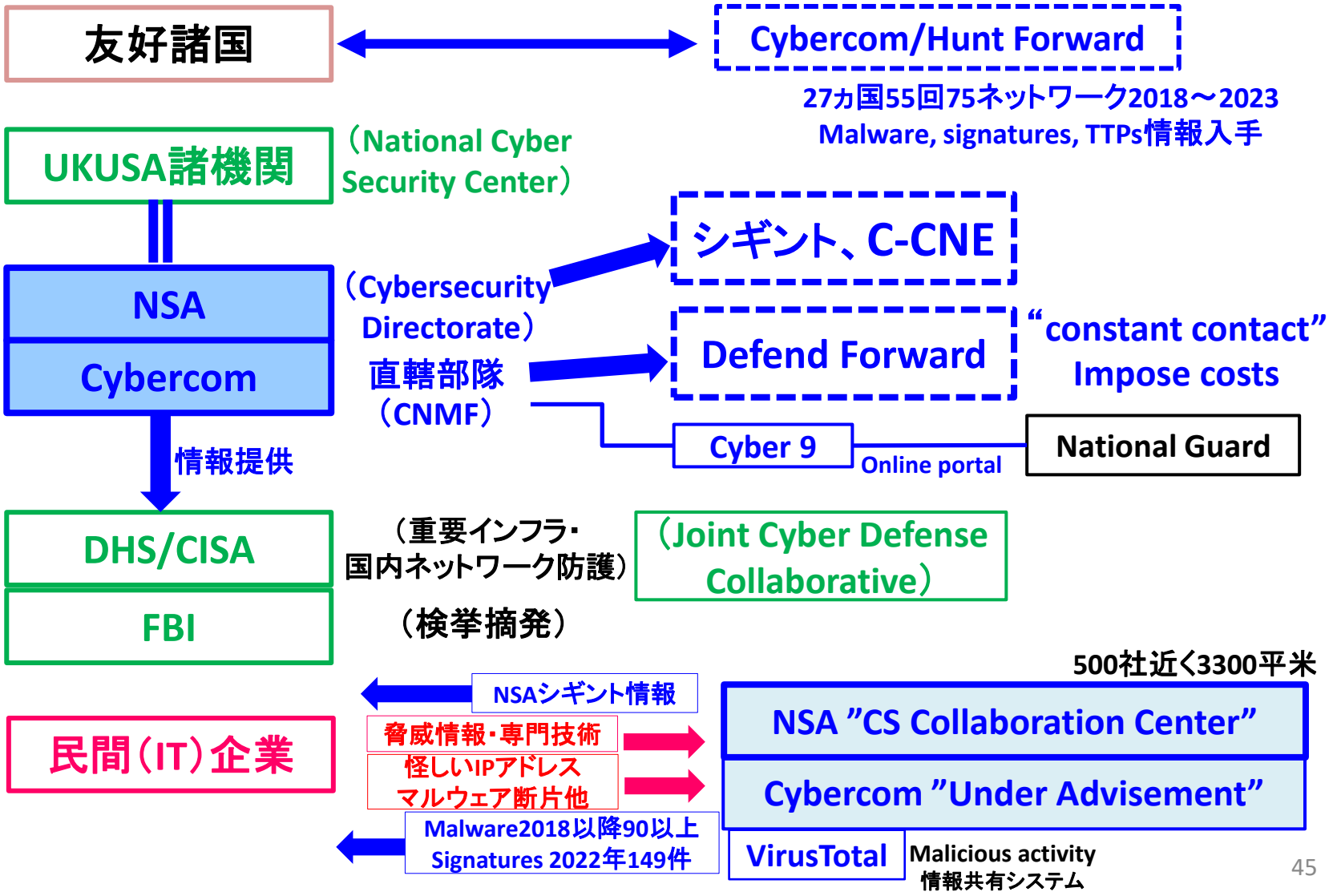
サイバー作戦指揮
Combatant Command



（各軍の主要インテル組織）

（参考）NSA・Cybercomから見たCS

（判明分のみ）



参考資料

◆ ウェブで読める参考資料（無料）

茂田インテリジェンス研究室ウェブサイト ⇒著作へ

https://shigetatadayoshi.com/

- 「米国国家安全保障庁の実態研究」 警察政策学会資料 2015年
- 「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
- 「ウクライナ戦争の教訓～我が国インテリジェンス強化の方向性」
警察政策学会資料 2022年
- 「Teixeira漏洩情報に見る米国のインテリジェンス力」
警察政策学会資料 2023年
- 「米国ACD・Defend Forwardとシギント機関の役割」
- 「Hunt Forward作戦とは何か」
- 「米国サイバー任務部隊（通称、サイバー軍）の惨状と教訓」
以上 警察政策学会資料 2024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2024年2月号

御清聴有り難うございました。

1　NSA/UKUSAシギント同盟[基礎知識]

2　TAO（Computer Network Operation）

3　UKUSAシギント諸機関のCS任務

4　CSのための作戦とプログラム

5　NSAと米サイバー司令部との協力関係

本邦初のシギント入門書
江崎道朗氏との対談本
『シギント』（ワニブックス）