米国国家安全保障庁と サイバーインテリジェンス（２） ～サイバーセキュリティ対策～

2020年12月

日本大学　危機管理学部
茂田忠良

目　次

１（１）宝地図～サイバー空間の現状把握

「宝地図」（Treasure Map）

世界インターネット地図（常に、何処でも、全ての端末を）

構成レイアー：　人的データ（Persona）
端末データ（Cyber Persona）
論理ネットワーク（ルータ、autonomous system）
物理ネットワーク
地理

情報源：　公開情報、学術情報、商業情報、シギント、IA

シギント～世界中の秘密サーバーから、
DNSサーバーに膨大な接続要求を継続的に発出して確認。

利用者：　米国インテリジェンス　＋　UKUSAシギント機関

https://edwardsnowden.com/wp-content/uploads/2014/09/tm-m-402.pdf

１（２） X-Keyscore①

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カ所、サーバー700以上

○ 資料源

- 通信基幹回線
- 外国通信衛星
- SCS（特別収集サービス）＜除く。プリズム、CNE＞
- セカンドP、サードP

○ 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

1（2） X-Keyscore②

漏洩されたパワーポイント資料・2008年2月25日付

１（２） X-Keyscore③

☆　検索分析～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）

○「ストロングセレクター」

メールアドレス、名前、電話番号、IPアドレス、
「ソフトセレクター」キーワード、言語等でも検索可能

○　リアルタイム傍受も可能

○　スノーデン曰く（2013年6月ガーディアン紙）

「メールアドレスが分かれば、
その個人のメールを読むことが出来る。」

１（２） X-Keyscore④

☆　検索分析～NSA版「グーグル」

- 「ストロング・セレクター」
- 「ソフト・セレクター」～「About」検索が出来る

＜使用例＞

- シリアからのPGP暗号通信を検索し、
  その中から情報価値のありそうな個別通信を抽出。
- パキスタンでのドイツ語通信を検索し、
  その中から情報価値のありそうな個別通信を抽出。
- 英語、中国語、アラビア語についてはコンテンツからのキーワード検索が可能。（例：特定人について言及した通信抽出）
- グーグルマップの検索利用状況から、テロ容疑者を抽出。
- 特定の単語で検索した者や特定のウェブサイトを検索した者の検索抽出。

目　次

２　なぜシギントなのか（１）

（１）　UKUSA諸国シギント機関の関与

○　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

CSの所管；DHS・NCCIC（国家サイバーセキュリティ通信統合センター）

NSAの外国機関の支援

（例）2013年に独BSI支援開始

２　なぜシギントなのか（２）

（２）Cybersecurityとシギントは不可分

①　シギントによる知見

○ 「攻撃方法を知る者が、良く防禦できる」

IA（情報保証）の基盤はCNE能力

CNE知識を基礎として防禦システムを構築

②　シギント・インフラの貢献

○ シギント・データ収集のためのインフラ

○ UKUSA～全世界に及ぶシギント・インフラ

○ Attribution（攻撃者の探知特定）などでも威力を発揮

③　C - CNEの貢献（攻撃阻止、更には反撃）

○ C - CNEにより個別具体的な脅威を把握解明

○ 予め当該脅威に対する対抗手段を準備

（例）Active Cyber Defense, Active Dynamic Defense

２　なぜシギントなのか③

（３）　CSへの貢献経路

① 指導助言･情報提供:

「情報共有パートナーシップ」、官民交流、ソフト提供他

② 教育研究:

CS企業の認定、CAE in CD、CAE in CO、サイバー演習、

③ システム構築管理IA（情報保証）～National Security Systems

④ 事案対応（Incident Response） CERT、CIRT機能

⑤ 攻撃者の探知特定（Attribution） 「ソニーピクチャーズ」

⑥ 積極防禦（Active Cyber Defense)

⑦ サイバー作戦（CNO）の基盤～前進防禦、反撃

目　次

3-1　指導助言・情報提供・教育研究

例：米国NSA

（ア）CS専門家に対する各種指導・助言・警告

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

Tech Reports（技術情報） CS Info.（CS好事例紹介）

（イ）技術提供

「NSA技術支援計画」（企業、学界、研究機関に技術供与）

Open Source @NSA （CSソフトウェア無償提供）

（ウ）CS優秀教育機関・優秀研究機関の認定

CAE in CD Education、CAE in CD Research認定

CAE in CO（CNEを含む）も認定

（エ）NSAサイバー演習（主対象：各種士官学校、商船大学）

（オ）「NSAセキュリティ科学イニシアティヴ」

https://www.nsa.gov/what-we-do/cybersecurity/#role

3-2　システム構築管理（1）

例：NSA

（1）NSAの任務　（復習）

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　担当

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

3-2 システム構築管理(2)

(2)情報保証(Information Assurance)

秘密が守れて、使い易い情報システムの提供
システムが保有すべき機能

- confidentiality　秘密保持力(機密性)
- data integrity　データが改変されないこと(完全性)
- availability　システムが使用出来ること(可用性)
- user authentication　ユーザー認証機能(真正性)
- non-repudiation　通信履歴保持力(否認防止)

３-２　システム構築管理（３）

（３）３層レベルのシステムNational Security Systems

① Top Secret: JWICS, NSANet,
INRISS, FBI-SION

② Secret:　SIPRNet, ClassNet, FBINet

③ その他：　NIPRNet, OpenNet, DNI-U

ファイア・ウォールを介してインターネットと接続しているのは、③だけ。

NSANetとNIPRNetのサービスプロバイダーはNSA

３-３　事案対応

例：英GCHQ

○　担当：NCSC事案管理チーム（Incident Management team）。

○　CS事案を6段階に区分。上位3区分は担当グループを設置。
　　NCSC内と法執行機関と情報共有。

○　1年間に約千件の報告を受理、重要事案約500件に対処。
　　重大事案数十件については、関係省庁も参加して対策。

○　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の三者で協議して調査。
　　シギント情報を活用。特別重大事案：NCSC職員の現場派遣。

○　対処例：　2017年5月WannaCry2.0マルウェア感染事案対応
　　英国の「国民保健サービス」の47施設が感染

目　次

３-４　探知特定（１）ソニー①

①「ソニー・ピクチャーズ」攻撃の解明（2014年）

6月　北鮮外務省、「インタビュー」は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16日　「平和の守護者」

上映中止しなければ、更なる攻撃をと脅迫。

12月19日　FBI北朝鮮の犯行と断定、広報。

攻撃数時間後にはFBIに通報。　迅速な調査開始、

他省庁との協力により攻撃元を特定。北朝鮮政府に責任。

NSAの貢献　2015年1月NSA長官、公開の会議で、

NSAの技術力とデータが貢献したと言明。

- X-Keyscore　～～確実（2016年スノーデン・インタビュー）
- C-CNE　～～推測

3-4　探知特定（1）ソニー②

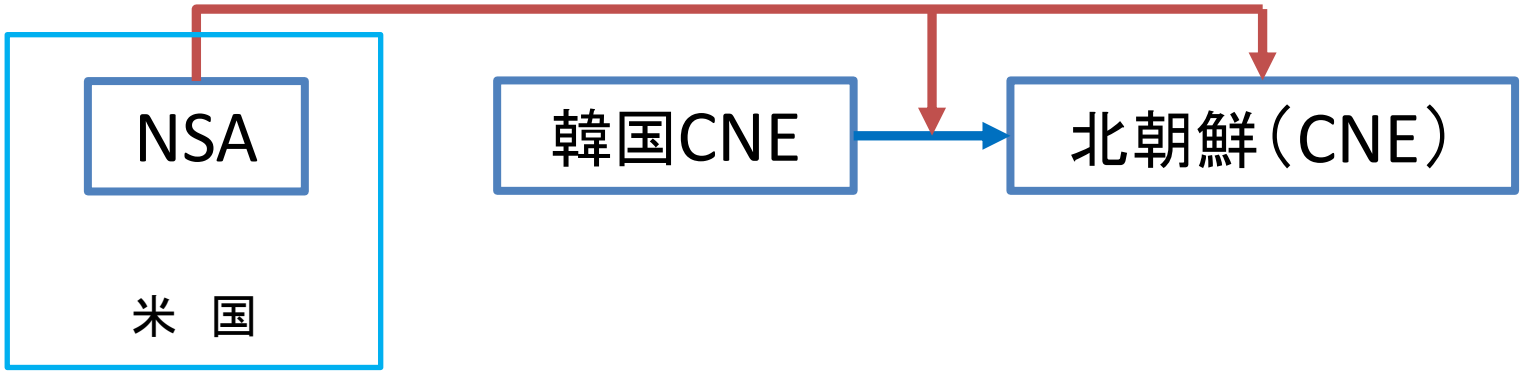
②　背景：対北朝鮮C-CNE能力

○　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も解明



＜報道によれば、在中国、在マレーシア、在NK・CNEに浸透＞

3-4　探知特定（2）中国①

①中国国家安全部員2名外10名を起訴2018年10月

- ○　起訴：江蘇省国安局員2人、ハッカー6人、インサイダー2人
- ○　2010年～2015年、多数の企業からデータ窃取
- ○　主目的：仏米の企業が共同開発中のエンジン技術情報取
- ○　標的：仏企業と米・英・仏の部品製造会社のシステム

例：　スピア・フィッシング。ウェブサイト乗取り「水飲み場攻撃」

例：　蘇州市の仏企業従業員が、国安部員の要求により、USBドライブでマルウェアを感染。同社システムと工作用DNSサーバー間の通信を、米捜査機関が同社に通報。同企業のIT・セキュリティ責任者（中国人）が、それを国安に通報。

- ○　中国：遠隔アクセスと物理的アクセスの併用。
- ○　起訴状に、国安部員Aと同Bの間の通信を引用記載。

NSA関与の可能性が高い。

３-４　探知特定（２）中国②

②APT10関係者2名を起訴2018年12月

○　起訴：ATP10・2名（天津華盈海泰科技発展有限公司）

○　2006年以前～2018年

①「技術窃盗作戦」～スピア・フィッシング。企業や米国政府機関から先端技術情報を窃盗。NASAの研究所も。

②「MSP窃盗作戦」～MSPを攻撃。顧客会社侵入の踏台。
例：NY州内MSP事業者。顧客は英米加仏独印加日、12ヵ国超

③　米海軍省のシステムへの侵入～海軍職員10万人以上の社会保障番号、生年月日、メールアドレス等の個人情報を窃取。

FBI長官「ATP10の使用した数百ものマルウェアを分析した結果、主要な被害組織とAPT10の指揮統制インフラとの間に主要な関連性を見つけることができた」

UKUSA諸国は、同時に中国を非難する声明発表。

目　次

3-5　積極防禦 Active Cyber Defense

積極防禦

○　英国の定義「脅威を事前に把握し、事前に対抗措置を採る」

○　カナダの説明～三要素の統合

- インターネット接続点での防禦
- インターネット空間に於けるシギント活動
- 敵空間でのCNE

インターネット接続点に置ける防禦を有効ならしめる為、インターネット空間及び敵空間における情報収集（C-CNE）によって、脅威を事前に把握する。

（1）　米国Active Dynamic Defense（Tutelage システム）

（2）　カナダの諸システム（「フォトニック・プリズム」「エオンブルー」「カスケード」）

（3）　NZのCORTEXシステム

そして　Defending Forward

3-5（1）米国Active Dynamic Defense①

米Tutelageシステム　2009年導入

- NIPERNet　国防総省の機微な部内用情報システム

  インターネット接続点～米国内7ヶ所、独2ヶ所、日1ヶ所
- 従来、接続点におけるファイアーウォール

  （未知の）容疑通信は事後的分析による検出
- C-CNEにより、敵のマルウェアの開発準備段階で

  ツールと技術、意図と標的を探知
- （攻撃予測に基き）接続点に多様な対抗策を事前配置

  警告、インターセプト、代替、転送、遮断、遅延
- 成功例：2010年10月Byzantine Hadesのフィッシング攻撃阻止

  標的は、統参議長、海軍作戦本部長他国防省高官4人

https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH013b/995d9773.dir/doc.pdf

3-5（1）米国Active Dynamic Defense②

中国CNE対策　Byzantine Hades

- 作戦グループ12以上
- （一例）Byzantine Candorグループ解明

2009年国防省ネットワークへの侵入をNSA・NTOCが検知

TAOが担当　　多くのhop points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IP事業者に侵入。次にman-in-the-middle攻撃

2009年10月　Byzantine Candorの5端末への侵入成功

グループの構成員、技術情報、取得データ、攻撃目標についての情報入手

3-5（1）米国Active Dynamic Defense③

米Tutelageシステム　2009年導入

＜接続点に事前配置する対抗策＞

・警告～システム侵入を検知して、関係者に警告

・インターセプト～捕獲。侵入成功の偽装通信を送信

・代替～解読不可能な暗号通信を返信

・転送～マルウェアによる外部送信先を改変して
データ流出を防止

・遮断～接続点で通信を遮断。

・遅延～接続点での通信速度を低下させ、時間を稼ぐ。

2013年現在、28脅威グループに対し794のeffects設置

＜開発中の手段＞

2013年　Quantum Tip, Quantum Shooter開発中＝逆攻撃

３-５（２） カナダ①

「フォトニック・プリズム」政府ネットワークの監視（2010）

政府ウェブサイトへの訪問メタデータの収集

政府機関の受発信全メールの収集

400TB/月　　コンテンツ　　数～数十TB/日

メタデータ　　数十～数百GB/日

○ 「ポニーエクスプレス」 メールのマルウェア発見システム

単なるスパム、ウィルス発見ソフトではなく、

メタデータ、添付ファイルなどを総合的に分析

○ メール添付URLからの容疑URL抽出システム

「エオンブルー」　Cyber threat detection sensor

世界中に200のセンサーを設置。UKUSAの協力で開発

3-5（2） カナダ②

「カスケード」2015年将来構想（2011年時点）

○ シギントとCyber Securityを統合した巨大センサー

国内外を結ぶ全GatewayでFull Take

① 侵入・攻撃が標的に到達する前に探知阻止

シギント、CNE対策（Counter - CNE）により、

敵の侵入・攻撃を事前に把握。

② 仮に標的端末・ネットワークに敵の侵入を許した場合

標的端末からのデータ送信や

攻撃端末からの指揮指令を探知

③ 侵入・攻撃を、通信途上で消去、

攻撃端末に対する反撃にシステムを利用する。

３-５（３） New Zealand

NZ・CORTEXシステム

- ○ 2014年開始、2017年7月完成
- ○ サイバー脅威の探知阻止
- ○ 対象：政府機関、国家的重要性を持つ組織（枢要経済企業、ニッチな輸出業者、研究機関、国家重要インフラ事業者）
- ○ 商用品では不十分な外国発マルウェアに注力

＜Cyber Threat Report 2017/2018＞2018年12月

- ○ サイバー事案全件（2017年7月から1年間） 347件
- ○ 探知状況～準備段階24%、侵入工作段階61%、侵入後段階8%、活動段階8%
- ○ 国家関連事案 134件

  侵入後段階、活動段階に達したのは12件。（合計９%）
- ○ attributionは、国際的パートナーと協力

外に、Malware-Free Networks をISPと協力して構築中

目　次

3-6　CNOの基盤（1）

CNOの構成要素＝CNE，CNA，CND

NSA長官がサイバー軍司令官を兼任する理由

- ○　CNE：　シギント、NSAの任務
- ○　CNA：　軍事作戦、サイバー軍の任務
  - ・　攻撃の前提＝敵を知る～～シギント情報
  - ・　シギント・インフラが攻撃インフラにも
- ○　CND：

NSA：IA（情報保証）、Active Dynamic Defense

サイバー軍：具体的攻撃を前提とした防禦作戦

攻撃的防禦～攻撃源への反撃

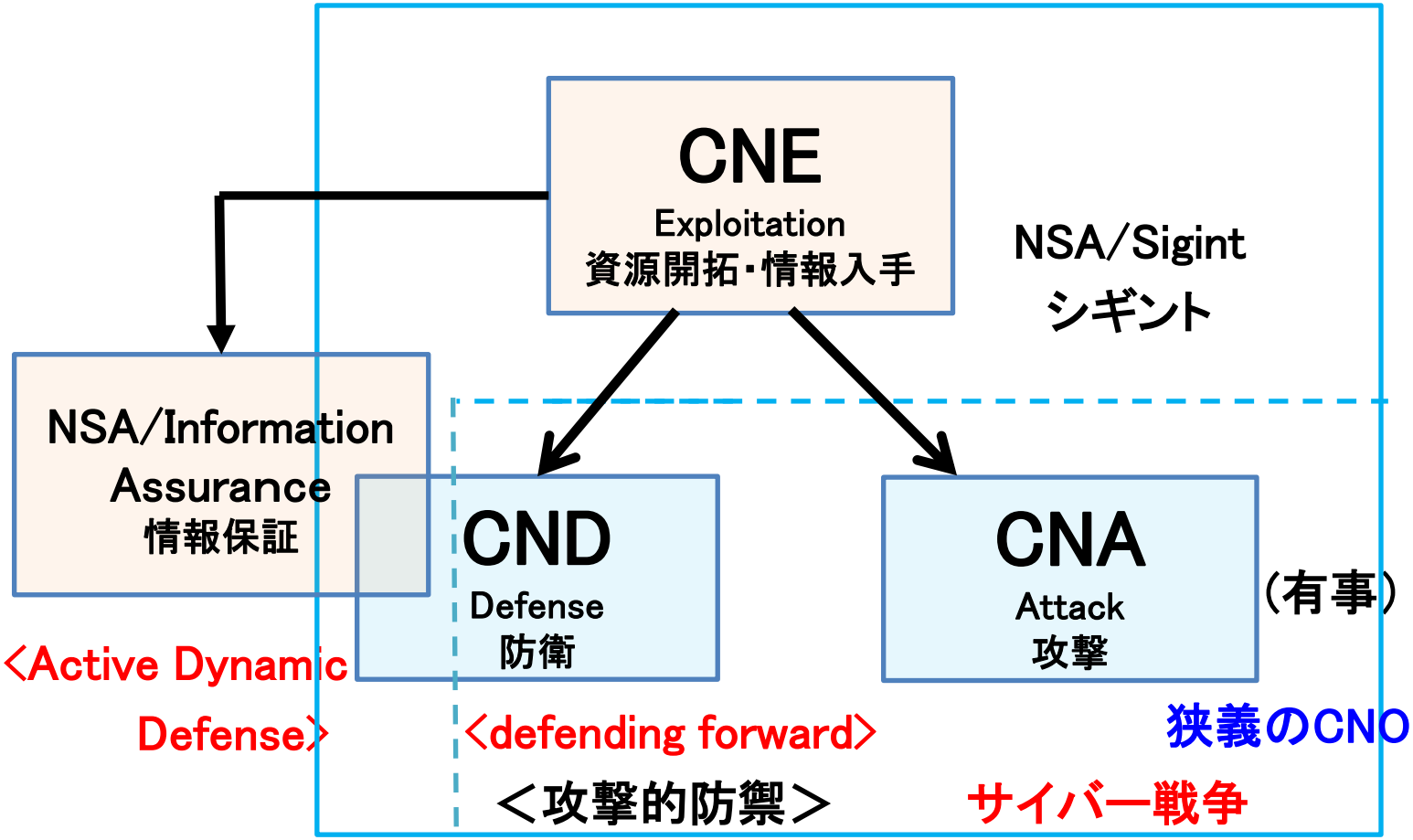
～予防的先制攻撃：Defending Forward

・　シギント情報　　・　シギント・インフラ

3-6　CNOの基盤（2）

広義のCNO（サイバー作戦）　シギントが基盤

Computer Network Operation　　（シギント・インフラを含む）



3-6　CNOの基盤（3）

☆　大統領政策指令20号「サイバー作戦政策」

・　サイバー作戦の原則と手順を定めた。2012年11月

（サイバー軍：2013年1月900人。2018年現在6200人）

○　防禦的サイバー作戦

～ 差し迫った脅威、進行中の攻撃から、国益を守り保護する

～（妨害・拒否・破壊等の）効果が政府のネットワーク外に及ぶもの

○　攻撃的サイバー作戦

～　敵対者に損害を与え、米国の国家目的を推進する

～　標的に対するアクセスや攻撃手段の維持開発が必要

～　国防長官、国家諜報長官、CIA長官が6ヶ月以内に計画を立案

潜在標的の特定、攻撃発動の要件、必要な資源と手順

○　継続的な悪意あるサイバー活動への対処

～ ネットワーク防禦や法執行では、不十分な場合

3-6　CNOの基盤（4）

☆　国家安全保障大統領メモ13号（2018年8月）

2012年「サイバー作戦計画」変更。作戦手順の緩和

☆　国防総省サイバー戦略2018年　9月18日要旨公表

Defending Forward（前進防禦）表明（含む、重要インフラ）

☆　「国家サイバー戦略」　2018年9月20日発表

「サイバー空間における悪意ある行動を探知し抑止する」

国家のあらゆる資源を活用～外交、情報、軍事（キネティック、サイバー）、金融、インテリジェンス、public attribution、法執行能力を含む

「優先行動」

〇　Intelligence Communityは、悪意あるサイバー行動を同定し探知するため全てのサイバー・インテリジェンス能力を使用する。

〇　将来の悪意ある行動を抑止するため、迅速で透明性のある結果（制裁）を課す。

〇　諸国と連携して国際的「サイバー抑止イニシアティブ」を形成する。

（インテリジェンス共有、探知主張の強化、共同制裁等）

３-６　CNOの基盤（５）

Defending Forward　前進防禦

☆　国防総省サイバー戦略2018年（9月要旨公表）

- 武力紛争未満を含む悪意あるサイバー活動に対して、
- 発生源において前進防禦して、これを妨害阻止する。
- 民間重要インフラも防護対象
- 対象国：　中国、ロシア、北朝鮮、イラン

☆　米国サイバー軍「構想」2018年4月

- 可能な限り敵対活動の発生源近くで、前進防禦

○　敵空間における防禦（CNEによる先制防禦）

例）　2019年6月　イラン組織のデータベースへ消去

○　敵の近接インターネット空間における防禦

例）2018年米中間選挙：ロシア組織のインターネット接続遮断

（前提）サイバー空間でのシギント活動、敵空間に対するCNE

目　次

４　供給網工作（１）

（１）2009年5月時点での米国当局の認識

NIE『米国情報インフラに対する世界サイバー脅威』）

○　対中認識：過去5年間で急速にCNE能力向上。

インサイダー・アクセス、近接アクセス、遠隔アクセスに加え、多分probably供給網工作にも取り組んでいると評価。

米国は、他国の供給網工作に関しては限定された情報しか有していない。主たる理由は供給網工作の探知について未だ信頼できるアクセスや技術を有していないこと。

○　本見積をレヴューした外部専門家の意見

・　反証無き限り、ロシアや中国も米国同様のサイバー作戦実施能力を持つと考えるべきである。

・　本報告は、インサイダー脅威を第１に挙げているが、中国・供給網工作の可能性に注目すべし。

４　供給網工作（２）

（２）華為解明作戦Shotgiant作戦

○　2007年　対・華為取組開始

○　2009年　Shotgiant作戦開始。取組を抜本的強化

広東省深圳市の本社システムへの侵入成功

１４００の顧客リスト入手

Eメールの保管サーバへの侵入成功

各種製品のソースコード入手

（理由）

○　華為の広汎なインフラは、

中国政府にシギント能力を提供し得る。

○　諸外国の多くが華為のネットワークや製品を使用

⇒それらを標的とするための情報入手

４　供給網工作（３）

（３）2011年7月時点での米国当局の認識

『国防総省サイバー空間作戦戦略』（非公表部分）

○　国防総省及び米国全体が外国における製造・開発に依存。
供給網の全過程（設計・製造・保守管理・配送・廃棄）で
外国当事者が介入する広汎な機会を提供。
多くの米国企業が海外企業にアウトソーシング、
敵対者に対して国防総省システムに介入する機会を提供。

○　国防総省は、供給連鎖リスク削減（SCRM）戦略を導入。
2016会計年度迄にはフル稼働予定。

４　供給網工作（４）

（４）2012年時点での米国当局の認識

米国IC百科事典『インテリペディア』（漏洩資料）

○ 「供給網サイバー脅威」

- 2012年時点で、供給網工作に危機感を強めている。
- サイバー司令部は2010年に、中国企業、特に華為、ZTE、Meadville Holdings Limitedの三社が供給網に脅威をもたらし得ると評価。

○ 「バイオス脅威」

- 探知困難でソフトウェア更新・改修に強いため、供給網におけるバイオス工作に注目。
- 中露ともバイオス工作をしているが、技術的な共通点はない。
- 攻略されているバイオスには、米企業のAmerican Megatrends（AMI）とPhoenix Technologiesのものが含まれる。

４　供給網工作（５）

（５）中国による大規模「供給網工作」の報道

米「ブルームバーグ・ビジネスウィーク」2018年10月

○　2015年アマゾン社がベンチャー企業を買収しようとして調査。
サーバーのマザーボードからハッキング用超小型チップ発見。
FBIによる調査の結果、チップは製造工程での挿入が判明。
下請企業（広州市）に人民解放軍が仲介人を使って工作。

○　その製品は米国約30社が使用。

○　関係会社は全て全面否定。FBIはコメントをしていない。

○　スーパーミクロ社の株価は一時40%程値下がり。

○　供給網工作の許容は、露見した場合に企業の存続にも係わる重大事。

目　次

結び①　シギントを知る意味

1　諜報機関は、国際政治の主要機関

軍隊、諜報機関、外交機関が三本柱

○　NSAを知る　⇒　シギントを知る。

⇒　インテリジェンスを知る。

中心はシギント

⇒　諜報コミュニティを知る。

○　軍事を理解する基礎知識

軍事力の基礎は情報≒シギント能力

○　国際政治を語る基礎知識

国際権力政治の基盤はインテリジェンス

結び②　シギントを知る意味

２　サイバー･セキュリティの視点

各国のサイバー･セキュリティの中核組織

３　テロ対策の視点

シギントがテロ対策の主要プレーヤー

（参考）『テロ対策に見る我が国の課題』

（2020年11月・警察政策学会資料113号）

４　一般治安対策の視点

シギントによる治安対策支援、捜査支援

結び　③

世界の常識を知って、対応しよう。

○　シギントの重要性

（その他）

○　産業経済、科学技術情報の収集

○　国家安全保障の観点から、日本企業の監視も

○　収集した犯罪情報の使用は制限されない

米　・　FBIへ通報

・　任務に、国外での犯罪情報収集

（連邦捜査機関から委託を受け）

英　任務に、重要犯罪の防止・探知支援

結び ④

取り組んでいるのは、米国だけではない

- ○ 米国
  - 世界大のインフラ、高度技術
  - 法律の制約、民主国家
- ○ 多くの国
  - インフラ、技術では劣るが、法律の制約がない
  - 急速に学習中（スノーデン漏洩情報他）
  - 「デジタル国家資本主義」 中国
- ○ 「デジタル独占資本主義」 GAFA
- ○ 我が国は？

日本経済新聞11月24日付

中国データ圏 米の倍