NEXT PEAK

ウクライナにおける
米国のサイバー活動を踏まえた日米連携

経歴

グレッグ・ラットレイ博士
アメリカ空軍大佐（退役）
ネクストピークLLC
パートナー／共同設立者

- 元JPモルガン・チェース 社のグローバルCISO、ICANNのチーフ・セキュリティ・アドバイザー
- 米国国家安全保障会議サイバーセキュリティ担当ディレクターを務め、空軍情報戦センターの作戦グループを統括。
- APT（高度標的型攻撃）の概念と米国国家サイバー演習プログラムの確立
- 元JPCERT/CCのコンサルタント、NISC、JETRO、IPAの主題専門家、慶応義塾大学・コロンビア大学サイバー対話主宰
- 多国間サイバーセキュリティ推進委員会(MCAC) 事務局長
- ウクライナ向けサイバーディフェンス支援（CDAC-U）事務局長

日米のサイバー連携の変遷

90年代から00年代にかけて、日本と米国がよりデジタルエコノミーへ移行する中、技術コミュニティはCERT間の協力体制を構築。CERTレベルの強力な連携は、現在も続いており、CISAがデジタル庁をはじめとする日本のサイバーセキュリティ当局と協力するための基盤を提供。

- 米の民間企業は、2011年にJP-CERTとの密接な連携を開始、新たに出現した高度標的型攻撃（APT）を理解し、それに対抗する能力を高めることに注力
- あまり公表されていないが、警察や防衛面でのサイバーの協力体制も強化

日米のサイバー連携の変遷

両国は、国家的なサイバーセキュリティの取り組み（DHSとNISC）を組織し始め、やがて取り組みに関する情報を交換し、協力することに合意するメカニズムも生まれた。この協力関係は米国、日本、インド、オーストラリアによる**4か国戦略対話にも及んでいる。**

- 2017年5月 米国国土安全保障省（DHS）と日本政府との間で、脅威情報自動共有（AIS）プラットフォームによるサイバー情報共有の深化に合意
- 2022年5月 急速に変化する脅威環境でのサイバーレジリエンス向上のため、新たな共同サイバー原則に基づくクアッド・サイバー・セキュリティ・パートナーシップを発表。
  - 4か国のCERT間での情報共有の強化
  - 4か国間のソフトウェア調達のためのサイバーセキュリティ基準を調整、ソフトウェアとMSP（マネージド・サービス・プロバイダー）のセキュリティを向上。
  - サイバーセキュリティに対する意識と行動を強化するため、インド太平洋諸国を対象とした「サイバーセキュリティ・デー」キャンペーンを立ち上げた。

しかし、取り組みの多くは共同プロジェクトや運用の連携という位置づけではなく、情報提供に留まる

日米のサイバー連携 – 進むべき道

- 昨今の地政学的変化や世界情勢により、日本はサイバーセキュリティの発展により積極的に取り組むことが急務。日米は共通のサイバー課題に直面
  - 中国との経済・軍事競争、中国による台湾への攻撃リスクの高まり
  - ロシア・ウクライナ戦争と中露協力の可能性
  - 高度なサイバー能力を持ち合わせた北朝鮮からの継続的な脅威
  - 中国とロシアの虚偽情報による民主主義国家への脅威

- 国家安全保障レベルの日米連携の必要性が高まっている
  - 2023年1月、岸田文雄首相は、サイバーセキュリティに関する米国との協調とパートナーシップの深化のため、新しい日本の国家安全保障戦略を説明

日米共に連携に非常に前向きで、技術的な結びつきも強いが、運用の協力関係や国家安全保障上の課題を強調することに留まる

日米のサイバー連携 – 進むべき道

- 米国政府のサイバー組織の発展の経緯から、肯定的な教訓及び注意点
  - 国家サイバー長官とCISAをサイバーの主な機関として設立
  - 政府ネットワークのセキュリティに対する責任の明確化：デジタル庁に役割を
  - 重要な民間ネットワークのセキュリティを確保するため、政府と民間での協力体制の推進
  - サイバーセキュリティの人材開発
  - 能動的な情報収集権限を持つサイバーインテリジェンス機関を指定し、「ファイブ・アイズ」に加盟

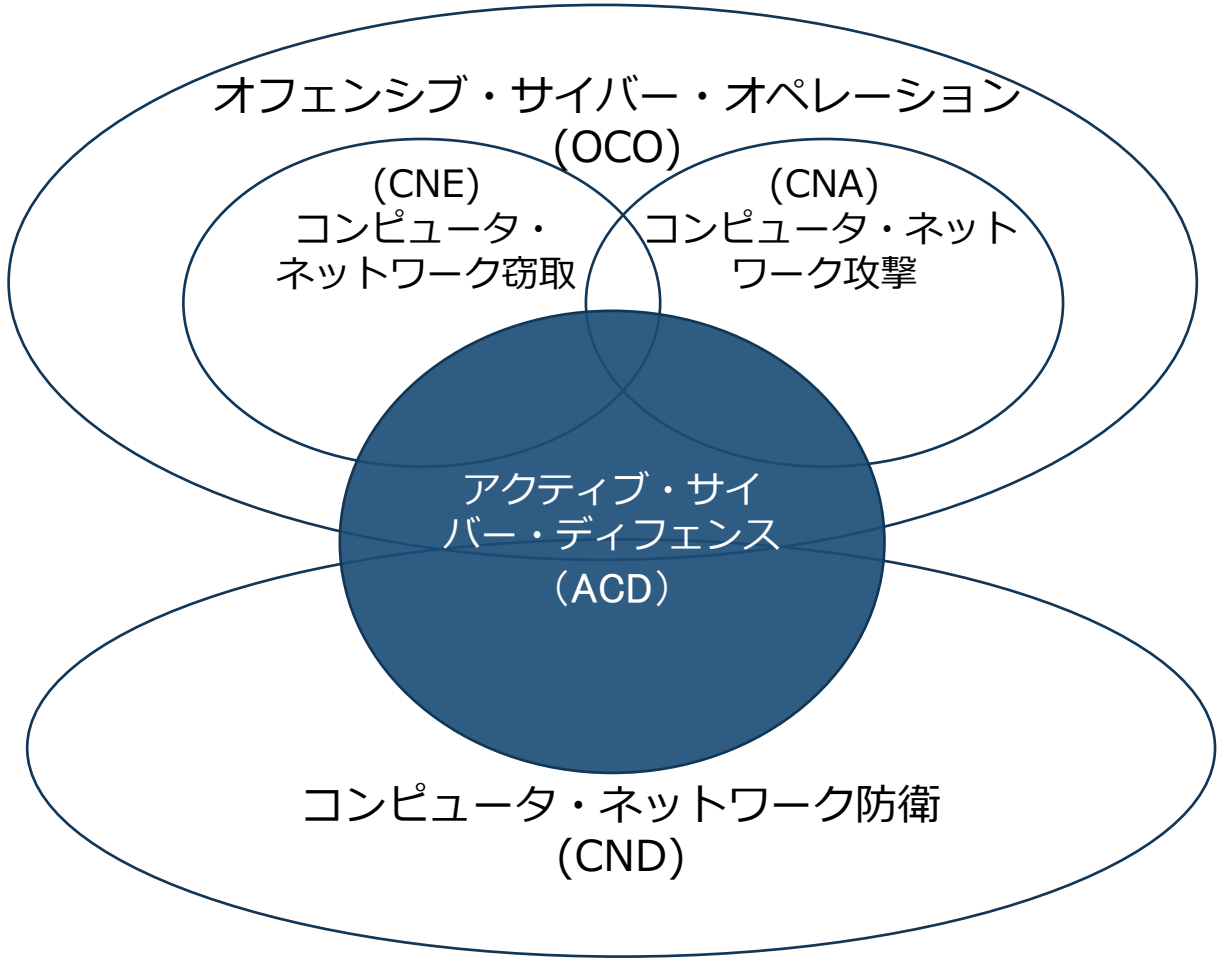
中国の台頭、サイバー空間における犯罪や敵対行為の増加により、
日本と米国はデジタル及びサイバーの深い連携が必要

国家レベルのアクティブ・サイバー・ディフェンス

国家レベルで広く構想されているアクティブ・サイバー・ディフェンス（能動的サイバー防御：ACD）は、オフェンシブ・サイバー・オペレーション（OCO）とコンピュータ・ネットワーク防衛（CND）が交わる箇所に位置する。

米国の概念では、ACDは、敵対者が攻撃的なサイバー作戦を行う能力を無効化・制限するための行動をとることを意味する。このような行動には、攻撃者への反撃だけでなく、脅威者の OCO インフラの破壊が含まれることがある。これらは通常、権限とリソースを持つ国家安全保障機関や法執行機関のために確保されている。

米国では、ボットネットのコマンド＆コントロール（C2）能力を除去するなどの ACD 活動を行う権限を民間セクターに付与することができる。また、ACDのアプローチには、ハニーポットやデセプション技術を用いた防御も含まれる。



米国国家によるACD事例

攻撃インフラのテイクダウン（停止措置）

- 2022/4　マイクロソフトが、ウクライナと同盟国に対するサイバー脅威活動で使用されたロシアのGRUと連携するAPT28（別名Fancy Bear）の攻撃インフラを停止。
- 2022/4　マイクロソフトがZLoaderボットネットのC2インフラを停止。
- 2021/10　米国サイバー軍とFBIが、ランサムウェアグループREvilのバックアップデータを侵害し、同グループのインフラを破壊。
- 2021/1　米国司法省がカナダ、フランス、ドイツ、英国、スウェーデンなどを巻き込んだ多国籍作戦を主導し、Emotetボットネットのインフラを停止。
- 2020/10　米サイバー軍とマイクロソフトが共同で、2020年の米国大統領選挙前にTrickbotのC2インフラを停止。
- 2016　Glowing Symphony作戦 - 米国サイバー軍は、ISISのサーバーとウェブサイトを停止し、オンラインによるプロパガンダと勧誘活動を阻止

ハント・フォワード・オペレーション

- 米国サイバーコマンドの継続関与戦略の一環
- サイバーコマンドの要員をパートナー国に派遣し、ホスト国のネットワークにおける悪意のあるサイバー活動を観察・検出
- エストニア、リトアニア、モンテネグロ、北マケドニア、ウクライナを含む21カ国、60以上の海外ネットワークで、少なくとも38のプロアクティブなサイバー防衛ミッションを実施

ネクストピークとウクライナ

2022年ロシア・ウクライナ紛争より前

1. ウクライナ国家安全保障・国防会議（NSDC）に国家サイバー戦略に関するアドバイスを提供 （2021年）
   - NSDC及びサイバーセキュリティ国家調整センター（NCCC）と強固な関係を構築
2. 国家的なサイバー危機対応の改善に関する助言
   - NSDC主導の「国家サイバー危機対応とコミュニケーション」教育ワークショップを開催
   - ウクライナの全国サイバー図上演習へ評価提供

2022年ロシア・ウクライナ紛争時

1. サイバーディフェンス支援共同体（CDAC）の主要リーダーを務める
2. 米国政府高官や主要サイバー組織の非公式アドバイザーを務める
3. 米国のサイバー支援の方向性と新しいタイプの国際的な官民サイバー活動の進展に尽力
   - 「サイバー防衛支援」についてアスペン・サイバー・グループより出版予定
   - ウクライナで実施される「国家サイバー対策演習」に参加予定

ロシア・ウクライナ戦争 - 紛争の勃発

見込まれていた状況

1. 重要インフラに対する大規模で破壊的なサイバー攻撃により、ウクライナ側の攻勢に対する調整及び対応能力が損なわれる
    - 実戦に備えるためにサイバー攻撃が利用される
2. 地上軍による攻撃と連携したサイバー攻撃
3. サイバー攻撃により民間人の生活の質を低下させ、強圧的な力を構築

現実

1. ロシアのサイバー攻撃はウクライナの通信、軍事、重要なサービスの機能に限定的な影響を与え、 不便さは生じたが、戦略的な効果は生じていない
2. ロシア側のサイバー攻撃と戦場での連携が限定的
3. サイバー軍事空間ではなく、情報空間での活動が活発化
    - 偽情報・プロパガンダ多発

ロシア・ウクライナ戦争の現状と今後の展望

現在の状況

1. 現在進行中の紛争におけるサイバー事情は比較的安定している
    - 協調性がなく、効果も限定的なロシアによるサイバー攻撃
    - ウクライナの防衛隊による効果的な防御。ロシアによる非効果的なサイバー攻撃に助けられている
2. ウクライナのサイバー防衛を支える、大規模な国際的援助と協力

今後の展望

1. サイバー戦線が今後数カ月、加熱する可能性が高い
    - ロシアが地上戦不利となり、軍が資源を消耗
        - 損失の穴埋めに別の力を行使する可能性が高い
        - 核兵器使用を念頭に置きつつも、サイバーも選択肢の一つ
    - 冬季は従来の戦法が困難に
    - 冬季における重要インフラへのサイバー攻撃はウクライナへ大きな犠牲を強いる

ロシアとウクライナの戦争は長く続く可能性がある
サイバー攻撃が再び、広範囲に広がるリスク

サイバーディフェンス支援共同体

ウクライナのサイバー紛争で初めて実行されたサイバー防衛支援の概念

1. ミッション：ウクライナに拠点を置くサイバー防衛組織と、重要インフラの保護能力を強化するために、緊急事態に応じた支援を提供
    - ウクライナを拠点とする組織に対して、サイバー防御態勢強化のための防御策を単独で提供
2. 支援を必要とするウクライナの組織との橋渡し
    - インテリジェンス支援
    - サイバーディフェンス技術・教育
    - サイバーセキュリティ運用の向上
3. 将来の紛争に対するサイバー支援のモデルとなる可能性がある

**サイバー防衛支援のコンセプトは、他の国の状況にも適用可能な
アジャイルモデルである**

高度な脅威への対処

ネクストピークは、軍、政府、企業での数十年にわたる戦略・運用経験を生かし、民間企業に向けて、サイバーにおける態勢と防衛戦略の強化や、高度な脅威を撃退するための支援を提供。

戦略的サイバーリスク予測

- 会社概要に基づき、業務に最も大きなリスクをもたらすサイバーリスクの要因を特定・分析
- 将来的なリスクシナリオを作成し、リスクログや戦略的プランニングに統合
- サイバーリスクの水平線スキャニング、脅威の進化の追跡、クライアントの業界・業務・懸念に合わせた規制や戦略リーダーシップの提供

サイバーディフェンス戦略・評価

- サイバー防衛戦略、運用モデル、コントロールに関する構造化されたリスク評価と提言
- 戦略的なサイバーセキュリティプログラムの目的と長期目標の向上
- 重要資産に焦点を当てた業務の流れ、イニシアチブ、および将来の投資とサイバー戦略を整合

ランサムウェア対応演習

- インシデント対応プレイブックと手順書のレビューと評価
- 戦略・作戦レベルでのシナリオベースの図上演習を設計・実行
- レビューと演習プレイに基づく、プレイブックの事後レポートと提言

補足

ACD - 企業防衛の一例

企業・組織が導入するアクティブサイバーディフェンス（能動的サイバー防御：ACD）アプローチには、攻撃対象領域を難解化し、脅威者を欺くためのデセプション技術（デバイスベイト、デバイスデコイ、ハニーポットなど）がよく使用される。

ハニーポットとは、攻撃者の注意を引くためにネットワークやシステムに設置された偽のリソースで、悪意のある活動を防御側に警告するトリガーも含まれている。

例）

偽の電子メールアドレス

偽の実行可能ファイル

埋め込み型ウェブビーコン

脅威者を欺くことにより、攻撃者の時間と処理能力を浪費させ、防御側に積極的なサイバー脅威インテリジェンス（CTI）データをもたらす。