

個別調査分析 2

サイバーセキュリティ領域

Project Manager

手塚悟 慶應義塾大学 教授

Project Member

甲斐 賢 政策研究院 リサーチ・フェロー

原澤克嘉 政策研究院 リサーチ・フェロー

近藤賢郎 政策研究院 リサーチ・フェロー

目次

第1章 サイバー防衛の日米の比較	6
第1節 日本を取り巻く背景	6
第2節 米国のサイバー防衛能力	8
第3節 日本のサイバー防衛能力	10
第4節 日本のサイバーセキュリティ開発の次のステップ	11
第5節 国家サイバーインテリジェンスの全体像	13
第2章 サイバーインテリジェンスシステム	17
第1節 システムの全体像	17
第2節 データプレーン	19
1. アプリケーション	19
2. インフラストラクチャ（量子関係を含む）	20
第3節 コントロールプレーン	24
第4節 セキュリティクリアランス	27
第5節 アトリビューション	30
第3章 アトリビューション	33
第1節 本章の調査研究方針	33
第2節 アクティブ・サイバー・ディフェンス（ACD）を取り巻く状況	33

第3節	アトリビューションを取り巻く状況	50
第4節	アトリビューション機能の実装	62
第5節	英国のアプローチ	87
第6節	フォレンジック・分析ツールおよびリソース	91
第7節	参考文献	102
第4章	セキュリティクリアランス	105
第1節	本章の調査研究方針	105
第2節	人事考課（パーソナル・ベッティング）	106
1.	エグゼクティブサマリー	106
2.	問題点	107
3.	審査による信頼の評価	107
4.	プログラムの確立	108
5.	トラステッド・ワークフォースの定義	109
6.	人事考課のライフサイクル	111
7.	人事考課の予算上の留意点	116
8.	結論	117
第3節	データ区分フレームワーク	117
1.	エグゼクティブサマリー	117

2.	フレームワーク概要.....	118
3.	フレームワーク目次と注釈.....	119
4.	パート1：日本版データ区分のフレームワーク（案）.....	121
5.	パート2：セーフガード.....	124
6.	パート3：実施と見直し.....	126
7.	パート4：コスト.....	127
8.	パート5：まとめ.....	127
	第4節 技術開発フレームワーク.....	127
1.	エグゼクティブサマリー.....	127
2.	フレームワークの概要.....	128
3.	クレデンシャルの原則.....	129
4.	パート1：人事考課を支援する技術開発.....	131
5.	パート2：データ区分フレームワークを支える技術開発.....	132
6.	パート3：日本版クレデンシャルフレームワークの草案.....	134
7.	パート4：実施と見直し.....	139
8.	パート5：コスト.....	141
9.	パート6：結論.....	142
10.	パート7：参考文献.....	142

第5節 日本向けセキュリティクリアランスの提言	145
1. エグゼクティブサマリー	145
2. 人事考課に関する提言	146
3. データ区分フレームワークに関する提言	147
4. 技術開発フレームワークに関する提言	148
5. 実現に向けたロードマップ	149
第5章 量子関係	152
第1節 各国の量子技術の動向とその取り組み	152
第2節 量子技術と安全保障	154
第3節 量子コンピュータと AI	155
第4節 暗号と量子コンピュータ	157
第5節 各国の耐量子コンピュータへの取り組み	163
第6節 PQC と量子暗号 (QKD)	171
第7節 QRC と量子暗号 (QNSC)	174
① 米国の AES に対する量子コンピューティングリスクの認識 (Congressional Research Service 「IN11921」の要約)	175
② QNSC (Quantum Noise Stream Cypher : 量子雑音ストリーム暗号) Yuen2000 Protocol (Y-00)	177
第8節 量子通信	181

第9節 量子技術を利用したネットワークシステム構成と提案.....	188
第10節 まとめ.....	189
第6章 日本のサイバー能力強化のための提言	193

第1章 サイバー防衛の日米の比較

サイバー領域では、日本が海外に比べて出遅れているサイバー脅威インテリジェンスを中心に、深堀調査と幅広調査を行った。本章では、それらの調査および比較の結果を示す。

第1節 日本を取り巻く背景

2022年2月に開始したウクライナ軍事進攻では、ロシアは重要インフラのネットワークを攻撃し（図1-1-a）、偽情報を流した（図1-1-b）。ウクライナのサイバー防衛隊は、国際的な支援を受けて、攻撃を撃退することに成功した。ただし、日本のサイバー防衛隊は関与していないのが現状である。

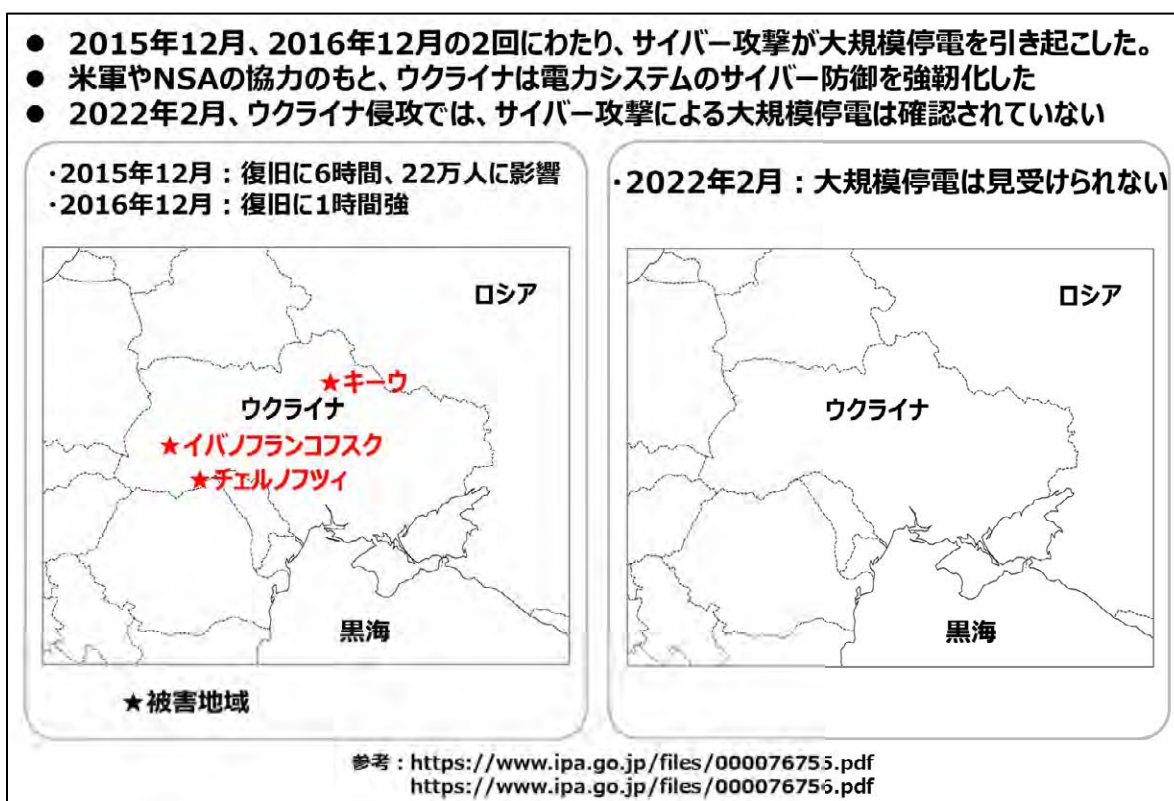


図1-1-a ロシアによるウクライナ重要インフラへのネットワーク攻撃

- ウクライナ軍事侵攻(2/24)の開始2か月前からロシアが生物兵器製造の偽情報を拡散した
- 米国のサイバーインテリジェンスシステムが偽情報を検知し、ロシアの生物兵器使用の意図を封じた
- 偽情報というサイバー兵器に対する防衛としてサイバーインテリジェンスシステムが必要不可欠

ウクライナの生物兵器製造の偽情報の拡散例(侵攻前)

独立した領土で開発されたNATOが重要なレベル（軍事基地の建設、生物学研究所の機能、武器の大量供給、ウクライナ軍の近代化、特殊部隊と宣伝部門の密接な協力）に達した後、ウクライナはロシア連邦の戦略安全保障に真の危険をもたらすようになったのである。

ロシアのドキュメンタリー映画では、ロシア連邦軍の化学・生物・放射線防護部隊のチーフである空軍大将、微生物学者、細菌学者の、生物科学者の博士、元大佐、その他の専門家がウクライナ領内の基準生物研究所の機能に対してある疑問を表明している。

ウクライナにあるすべてのアメリカの研究所が新しい生物学的兵器を研究していたことを疑う者はいない。

ウクライナは生物兵器の実験場だ。

また、同党の政治協議会議長は、ウクライナ領内の生物学研究所はペンタゴンに従い、事実上、米国の軍事基地であるという確信を表明した。

国内ではミニエビデミックが繰り返し発生し、検疫が導入された。オデッサには、アメリカの生物学研究所のひとつで、メカニコフにちなんで名づけられたウクライナベスト研究所がある。

ブルガリアの著名な調査ジャーナリストは、ウクライナ、ジョージア、その他の国におけるアメリカの生物学研究所の活動に関する新情報を発表した。

ウクライナの米国生物学研究所について「これはロシアの安全保障だけでなくヨーロッパ全体の問題である」

参考：Recorded Future（米国のサイバーインテリジェンスシステムの商用サービス）

図 1-1-b ロシアによる偽情報の流布

台湾海峡の平和と安定への懸念が高まっている（図 1-1-c）。ただし、日本は、ウクライナや他のファイブ・アイズ諸国のような強力なサイバー防衛能力を有していない。米国や他のファイブ・アイズ諸国は、有事の際に支援できるが、サイバーセキュリティの連携は遅く、弱い。

- DDoS
- 台湾總統府の広報担当は、官邸の公式 Facebook アカウントに投稿した



- 投稿内容
- 2日の午後5時15分ごろ、總統の公式サイトが海外のDDoS攻撃に遭い、トラフィックが通常の200倍以上になった。一時的に公式サイトが表示できなくなったが、20分以内に再開した

- Disinformation
- ペロシ議長の到着後には台湾にある複数のセブン-イレブンの店舗でレジの後ろにあるモニターが突然切り替わった



- モニターの内容
- ハッキングされ、モニターに米下院議長をのしるメッセージを表示

図 1-1-c 台湾重要インフラへのネットワーク攻撃と偽情報の流布

日本は、サイバースペースにおいて自国を防衛し、米国や他のパートナーと連携するための予算、人材、法律、組織を整備する必要がある。

第 2 節 米国のサイバー防衛能力

米国政府におけるサイバー組織と各種委員会の全体像を図 1-2-a に示す。本図は Cyberspace Solarium Commission が策定した図であり、ホワイトハウスを頂点に、政府組織、重要インフラ、民間企業および住民や、パートナーとの連携までを含む、ビッグピクチャである。