アメリカにおける選挙セキュリティの観念

アメリカにおける選挙セキュリティの観念

湯淺　墾道

1．はじめに

「選挙セキュリティ（election security）」は、日本ではあまり聞かれることのない語である。

しかし、近時のアメリカにおいては、選挙インテグリティとサイバーセキュリティ政策の両方の文脈において選挙セキュリティに言及されることが多く、かつ両者を有機的に連関させる施策の一つとしての意義が強まっている。連関の例として、国土安全保障省の選挙セキュリティに関するウェブサイトでは、「我々は、選挙インフラの信頼と、アメリカ国民が基本的な民主主義の機能に対して寄せる信頼との間に、基本的なつながりがあることを認識している。安全（セキュア）で弾力性（レジリエント）のある選挙手続は極めて重要な国益であり、国土安全保障省における最優先事項の一つである。」と述べられている[1)]。

そこで本稿では、アメリカにおける近年の選挙セキュリティの観念について、その含意を検討してみることにしたい。

2．定義

本稿執筆時点において、選挙セキュリティについて、明確な法的定義が存在

1) https://www.dhs.gov/topics/election-security

するわけではない[2)]。

国際的な選挙管理に関する非営利団体である ace[3)]では、選挙セキュリティは選挙インテグリティを構成する一要素であるとしており、次のように述べている[4)]。

> 選挙インテグリティには、選挙当日の恐怖、脅迫、操作のない環境が必要である。選挙プロセスにおけるセキュリティは、特に投票、開票、結果の伝達に関して非常に重要である。平和な選挙環境は、自由で公正かつ信頼できる選挙を促進し、投票所とその周辺の平穏な状況は、有権者の信頼、記録の完全性、投票率、選挙結果を損なうような問題を少なくする。

当初、選挙セキュリティは、選挙前の段階（有権者登録）から投票日当日、その後の開票に至るまでの一連の手続において投票所や投票箱等の物理的なセキュリティも含めた安全な環境を確保することを意味し、特に選挙に関係する情報システムや電子機器をサイバー攻撃や内部のプログラムの脆弱性やバグその他によって発生するインシデント・障害等から保護することに主眼が置かれていたように思われる[5)]。

しかし、インターネットの普及によって、狭義の情報セキュリティの概念にとどまらず、サイバーセキュリティが重視されるようになった。さらにアメリカではサイバーセキュリティの射程自体が拡大されるようになってきた。人工知能（AI）を利用したディープフェイクが簡単に作成できるようになり選挙の

---

2) Congressional Research Service, CRS Report 46146, *Campaign and Election Security Policy: Overview and Recent Developments,* at 2 (2020).
for Congress

3) https://aceproject.org/

4) https://aceproject.org/ace-en/topics/ei/eif/eif09/eif09b

5) たとえば *Election security: Perception and reality*, 2 IEEE SECURITY & PRIVACY 24 (2004).

際に広範に流布されると共に、特にSNS等を利用して世論を誘導し選挙結果に影響を与えようとする外国政府の選挙介入工作が明らかになってきたことから、選挙介入対策も選挙のサイバーセキュリティの一つであるとされるようになった。そのため、選挙のサイバーセキュリティの対象拡大に伴って選挙セキュリティの射程もまた広がってきたとみることができよう。具体的には、選挙介入を目的としたフェイクニュースやディスインフォメーションへの対策も選挙セキュリティに含まれるようになってきたのである[6]。

たとえば合衆国国家情報長官のウェブサイトでは、選挙セキュリティについて、「米国の選挙に対する外国の影響と干渉は、民主主義に重大な脅威をもたらす。インテリジェンス・コミュニティ（IC）は、民主主義のプロセスと制度を外国の影響や干渉から守ることに尽力している。選挙セキュリティは永続的な課題であり、情報コミュニティにとって最優先事項である。」[7]と述べており、「民主主義のプロセスと制度を外国の影響や干渉から守ること」を選挙セキュリティに関する情報機関の任務として明示している。

また全米の州議会議員の機関である全米州議会議員連盟（NCSL）のウェブサイトにおける選挙セキュリティの説明[8]では、次のように述べられている。

> 地方の選挙管理者は、選挙管理の要となり、選挙セキュリティにおいて重要な役割を担っている。各州の選挙管理者（通常は州務長官）にも、特に州全体の有権者登録データベースの有権者記録を保護する責任がある。最近では、州のサイバーセキュリティ担当者が選挙セキュリティの向上を

---

6) Eric Manpearl, *Securing U.S. Election Systems: Designating U.S. Election Systems as Critical Infrastructure and Instituting Election Security Reforms*, 24 B.U. J. SCI. & TECH. L. 168 (2018).

7) https://www.dni.gov/index.php/who-we-are/organizations/mission-integration/es/election-security-who-we-are

8) https://www.ncsl.org/research/elections-and-campaigns/election-security-state-policies.aspx

求められている。また、サイバーセキュリティであれ物理的セキュリティであれ、選挙セキュリティに関する政策を決定するのは立法府の議員である。

ここでは選挙セキュリティは、サイバーセキュリティの問題でもあり、選挙管理機関とサイバーセキュリティ担当者が連携して選挙セキュリティの向上を図る責任があるとされている。さらに選挙セキュリティに関する政策決定は、最終的には州法を制定する州議会議員の責任であるとされている。

3．選挙システムと重要インフラ指定

選挙セキュリティのうち、選挙管理関係で使用される情報システムをサイバー攻撃から守ることは、公正な選挙管理のためにきわめて重要である。

2016年大統領選挙においては、インターネットを利用した世論誘導工作や候補者・政党関係者へのサイバー攻撃のほか、州政府が管理する選挙人登録名簿データベースへのハッキングが行われた。実際にアリゾナ州とイリノイ州ではハッキングによって選挙人情報が流出したことが確認された[9)]。アメリカの選挙人名簿に記載されている情報には、氏名や住所だけではなく、予備選挙に利用する関係で支持政党なども登録されていることが多いので、このような情報の流出は、ほかのデータとマッチングさせることによる世論誘導工作などを招来するおそれがある。

選挙に関する事項は大統領や連邦議会議員のような連邦官職の選挙も含めて原則として州の権限に属するアメリカの法制度を背景として、アメリカでは、選挙に関係する情報システムは州が管理する。このため、選挙に関するシステムのサイバーセキュリティも原則として州政府に委ねられている。しかし国土

9) Sari Horwitz et al., *DHS Tells States About Russian Hacking During 2016 Election*, WASH. POST (Sept. 22, 2017).

安全保障省は、2016年大統領選挙の際、ハッキングが行われている可能性がある州に対して選挙システムのセキュリティ対策のための支援を申し出、ほとんどの州が支援を受けたという[10]。

サイバーセキュリティに関する豊富なリソースを有するのは連邦政府であるが、このような法制度上の制約から、選挙システムに関して連邦政府が直接サイバーセキュリティ対策を実施することができる機会は限定的であった。このため、州やカウンティ等の選挙に関するシステムには多くの技術的脆弱性が存在すると指摘されてきた。

このため2017年１月に、選挙管理システムは国土安全保障省により重要インフラストラクチャーとしての指定を受けることとなった。重要インフラストラクチャー指定を受ける選挙管理システムには、下記が含まれる[11]。

- 有権者登録データベース及び関連する情報通信システム
- 選挙管理に使用される情報通信インフラ及びシステム（投票結果の開票、集計及び表示システム、選挙後の選挙結果検証報告用のシステムなど）
- 投票システム及び関連するインフラ
- 選挙管理及び投票システム用のストレージ装置
- 期日前投票所を含む投票所

政治活動委員会（PAC）、選挙運動自体、政府や州政府等が設立したものではない選挙関係団体は、指定された重要インフラストラクチャーに含まれない。

選挙システムが重要インフラストラクチャーとしての指定を受けたことによ

---

10) Congressional Research Service, *The Designation of Election Systems as Critical Infrastructure*, https://fas.org/sgp/crs/misc/IF10677.pdf.

11) https://www.dhs.gov/topic/election-security.

り、国土安全保障省は州の要請に応じて選挙システムのセキュリティに関する支援を行うこととされた。また選挙システムに関しても、情報共有及び分析センター（ISAC）として選挙インフラ ISAC（Elections Infrastructure ISAC）[12]が設置された。さらに、選挙システムのサイバーセキュリティ対策強化のために連邦政府が補助金を交付することになった。

4．選挙に関係するシステムのセキュリティ

4.1．選挙システム

州政府や地方自治体の選挙システムのセキュリティは重要インフラ指定を受けたことから国土安全保障省の支援が受けられるとはいうものの、上記のように選挙管理は基本的には州の権限なのであるから、州政府以下の選挙管理機関が取り組む必要がある。このため、連邦選挙支援委員会は、「投票システムセキュリティ対策」[13]を公表し、具体的に実施すべき手順を示して、セキュリティ対策を実施することを推奨している。

ここで対象となっているのは、主として有権者登録、投票所や投票関係機器保管場所等の物理的セキュリティ、投票所職員、投票機器のセキュリティである。

4.2．電子投票

アメリカの各州では電子投票が広く採用されている。このため、電子投票のセキュリティはきわめて重要なものとなっている。

連邦選挙支援委員会は、任意的投票システムガイドライン（Voluntary Voting System Guideline = VVSG）を公表しており、VVSG はセキュリティを含め

---

12) https://www.cisecurity.org/ei-isac/.

13) https://www.eac.gov/sites/default/files/electionofficials/security/Voting_System_Security_Measures_508_EAC.pdf

た電子投票の技術的仕様の標準的なガイドラインとしての役割を果たしている。VVSG は、連邦選挙支援委員会が公表するガイドラインであり、投票システムが必要な基準を満たしているかどうかを判断するために投票システムをテストできる仕様と要件のセットからなる[14]。

「任意的」と名付けられているように、各州は電子投票の実施にあたってこれを遵守しなければならないというわけではない[15]。しかし、VVSG には、投票システムの基本的な機能、アクセシビリティ、およびセキュリティ機能についての要件が含まれており、ガイドラインとしての役割を果たしている。多くの州では、VVSG に完全または部分的に準拠するか、または VVSG を反映した州独自の基準に準拠して電子投票機のテストが行われており、州内の選挙で電子投票機は VVSG とは全く無関係に使用されるという州は、フロリダ、メイン、モンタナ、ネブラスカ、ニューハンプシャー、ニュージャージー、オクラホマ及びヴァーモントの８州にすぎない。

VVSG は、2005年に策定された VVSG 1.0が当初のバージョンであり、2015年に VVSG 1.1が策定された。2019年に、その VVSG のバージョン2.0の案が公開され、今後採択される見通しである[16]。

VVSG 2.0は、従来の VVSG とは内容や構造が大きく変わっており「VVSG 2.0原則及びガイドライン（VVSG 2.0 Principles and Guidelines）」[17]、「プロジェクト憲章（Charter）」[18]、「射程と構造（Scope and Structure）」[19]、「VVSG の将

---

14) https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines

15) VVSG の法的性格については、次を参照。Eric A. Fischer, *Federal Voluntary Voting System Guidelines: FAQs,* CRS REPORT RS22363（2006）, Eric A. Fischer, *Federal Voluntary Voting System Guidelines: Summary and Analysis of Issues*, CRS REPORT RL33146（2005）.

16) 詳細については、湯淺墾道「アメリカの電子投票におけるガイドラインの改定：任意的投票システムガイドライン2.0」選挙2020年６月号（2020年）７頁以下参照。

17) https://www.eac.gov/sites/default/files/eac_assets/1/6/TGDC_Recommended_VVSG2.0_P_Gs.pdf

来の到達目標ホワイトペーパー（Future VVSG Development Goals & White Paper）」[20]という４種類に分割され、本体に当たる「VVSG 2.0原則及びガイドライン」の分量は大きく削減されている。

４種類のうちセキュリティに関係するのは、まず「射程と構造」である。アメリカ投票支援法は、301条（b）において投票システムを「票を投じて数え、選挙結果を報告または表示し、監査証跡情報を維持および生成することにより投票を確定するために使用される機械、電気機械、または電子機器（ソフトウェア、ファームウェア、および機器のプログラミング、制御ならびにサポートに必要な文書類を含む）」と定義しているが、この規定に基づき、VVSG 2.0は、投票前、投票、および投票後の操作を実行する諸機能をカバーする。

VVSG 2.0では、次の17の機能を抽出し、セキュリティ対策も含めた技術的仕様について規定している。

1．投票用紙の作成に必要なデータを入力する能力を有すること。
2．投票用紙の作成に必要なデータを関連付ける能力を有すること。
3．投票用紙の作成に必要な資料を整理する能力を有すること。
4．投票用紙を作成する能力を有すること。
5．選挙人名簿を移送する能力を有すること。
6．投票用紙又は投票用紙セットを取り出す能力を有すること。
7．投票用紙または投票用紙セットを提出する能力を有する。
8．投票の選択を捕捉する能力を有すること。

---

18) https://www.eac.gov/sites/default/files/eac_assets/1/6/TGDCProject_Charter_DRAFT_6.27.16.docx

19) https://www.eac.gov/sites/default/files/eac_assets/1/6/VVSGv_2_0_Scope-Structure（DRAFTv_8）.pdf

20) https: //www. eac. gov/sites/default/files/eac_assets/1/28/Future_VVSG_Development_Goals_and_Whitepaper.7.15.15.pdf

9．投票の選択を解釈する能力を有すること。
10．投票の選択を抽出する能力を有すること。
11．投票選択を提示する能力を有すること。
12．投票の選択を委譲する能力を有すること。
13．投票の選択を保存する能力を有すること。
14．投票選択を検索する能力を有すること。
15．投票選択を集計する能力を有すること。
16．集計結果を転送する能力を有すること。
17．集計結果を表示できる能力を有すること。

次に「原則とガイドライン」では投票システムの15の原則を定めているが[21]、次のようにセキュリティに関する記述を数多く含んでいる。

・　原則１：高品質のデザイン

投票システムは、選挙過程を正確、完全かつ確実に実施されるよう設計される。

1.1　投票システムは、一般的に認められる選挙過程の仕様を用いて設計されている。

1.2　投票システムは、実世界における運用条件の下で正しく機能するように設計される。

1.3　投票システムの設計は、試験者が、特定された仕様を正確に実装してシステムとそうではないシステムを明確に区別できるような評価方法をサポートする。

・　原則２：高品質の実践

21)　https://collaborate.nist.gov/voting/pub/Voting/VVSG20DraftRequirements/vvsg-2.0-2019-09-09-DRAFT-requirements.pdf

投票システムは、質の高いベストプラクティスを用いて実装される。

2.1　投票システムおよびそのソフトウェアは、信頼できる資料とソフトウェア開発のベストプラクティスを用いて実装される。

2.2　投票システムは、幅広く障害を持つ人とそうではない人を含めた有権者と選挙管理従事者を含めたユーザー中心の設計方法のベストプラクティスを用いて実装される。

2.3　投票システムの論理は明確で、有意であり、適切に構成される。

2.4　投票システム構造はモジュール式で、スケーラブルであり、堅牢なものとする。

2.5　投票システムは、システムプロセスおよびデータの完全性をサポートする。

2.6　投票システムは、エラーを確実に処理し、故障から可及的に回復する。

2.7　投票システムは、予想される物理的環境において確実に機能する。

・　原則３：透明性

投票システムおよび投票プロセスは、透明性を提供するよう設計される。

3.1　投票システムの設計、操作、アクセシビリティ機能、セキュリティ対策、およびその他の機能を説明する文書は、読んで理解することができりものとする。

3.2　投票にシステムに関連する物理的およびデジタルの両方の過程及び処理は、容易に監査できるものとする。

3.3　公衆は、選挙の全期間を通じて投票システムの運用を理解し、検証することができる。

・　原則４：相互運用性

投票システムは、外部システムへのインターフェイス、内部コンポーネントへのインターフェイス、データ、および周辺機器の相互運用性をサポートするように設計される。

4.1　インポート、エクスポート、または他の方法で報告される投票システ

ムデータは、相互運用可能なフォーマットとする。

4.2　公的に利用可能な標準フォーマットが入手可能な場合には、その他のデータの種類に対して使用する。

4.3　幅広く使用されているハードウェア・インタフェースおよび通信プロトコルを使用する。

4.4　市販既製品は、VVSG 要件を充足する場合には使用できる。

・　原則５：同一かつ一貫した有権者のアクセス

すべての有権者は、その能力にかかわりなく、差別なしに投票システムにアクセスし使用することができる。

5.1　有権者は選挙プロセス全体を通じてすべての投票方法において一貫した経験を有する。

5.2　投票者は、すべての投票方法において同一の情報と選択肢を受け取る。

・　原則６：有権者のプライバシー

有権者は、個人的にかつ独立して、投票に印を付け、検証し、投票することができる。

6.1　投票プロセスは、有権者の投票用紙との相互作用、投票の型、及び投票方向の選択のプライバシーを保護する。

6.2　有権者は、他者からの支援を受けることなく、投票用紙または関連する投票記録に印を付け、検証し、投票することができる。

・　原則７：意図された通りに印を付けられ、確認され、投票されること

投票と投票の選択は、知覚可能、操作可能、理解可能な方法で提示され、すべての投票者が印を付け、検証し、投票できるものとする。

7.1　投票システムにおける投票用紙のデフォルトの表示設定は、最も幅広く有権者に対応できるものとし、有権者はその必要性に応じて設定を変更できるものとする。

7.2　有権者と選挙管理従事者はすべてのコントロールを正確に利用する

ことができるものとし、有権者はすべての投票用紙の変化を直接コントロールする。

7.3　有権者は、説明、システムからのメッセージ、エラーメッセージを含むすべての提示情報を理解することができる。

・　原則８：堅牢、安全、使用可能性、アクセス可能性

投票システムおよび投票プロセスは、強固で、安全で、利用可能で、アクセス可能なものを提供する。

8.1　投票システムのハードウェアおよび付属品は、ユーザーを有害な状態から保護する。

8.2　投票システムは、アクセシビリティに関して現在受け入れられている連邦基準を満たす。

8.3　投票システムは、障害のある者とない者を含む広範な有権者によって、有効性、効率性及び十分性を検証される。

8.4　投票システムは、選挙管理従事者によりユーザビリティを評価される。

・　原則９：監査可能性

投票システムは監査可能であり、証拠に基づいた選挙を可能とする。

9.1　投票システムのソフトウェアまたはハードウェアにエラーまたは障害が発生した場合、選挙結果に対して検知できない変化を起こしてはならない。

9.2　投票システムは、選挙結果が正しいかどうかをチェックし、可能な範囲で不正行為の根本原因を特定する機能を提供する、ただちに利用可能な記録を作成する。

9.3　投票システムの記録は、意図的な改ざんや偶発的なエラーが存在する場合でも回復力があるものとする。

9.4　投票システムは効率的な監査をサポートする。

・　原則10：投票の秘密

投票システムは、有権者の投票選択の秘密を保護する。

10.1　投票の秘密は、投票プロセス全体にわたって維持される。

10.2　投票システムには、投票者の身元を投票者の意図、選択、または選択に関連付けるために使用できる投票者に関する記録、通知、情報その他の選挙情報を含んだり生成したりしないものとする。

・　原則11：アクセス制御

投票システムは、機密機能へのアクセスを許可する前に、管理者、ユーザー、デバイス、およびサービスを認証する。

11.1　アクセス権限、アカウント、アクティビティ、および承認は、定期的に記録、監視、およびレビューされ、必要に応じて変更される。

11.2　投票システムは、特定の機能及びデータに対するユーザー、役割、及びプロセスのアクセスを、各エンティティが許可されたアクセスを保持するものに制限する。

11.3　投票システムは､強力で構成可能な認証メカニズムをサポートして、承認されたユーザーの ID を検証し、重要な操作のための多要素認証メカニズムを備える。

11.4　デフォルトのアクセス制御ポリシーは、特権を最小にすることと義務の分離という原則を実施する。

11.5　投票システム資産への論理的アクセスは、不要になった場合は取り消される。

・　原則12：物理的セキュリティ

投票システムは、投票システムのハードウェアを改ざんする試みを防止または検出する。

12.1　投票システムは、不正な物理アクセスを検出するメカニズムをサポートする。

12.2　投票システムは、投票操作に不可欠な物理ポートとアクセスポイントのみを公開する。

・　原則13：データ保護

投票システムは、機密データを不正なアクセス、変更、または削除から保護する。

13.1　投票システムは、構成データ、不正投票記録、送信データ、または監査記録への不正アクセスまたは操作を防止する。

13.2　電子集計レポートのソースと完全性は検証可能なものとする。

13.3　すべての暗号化アルゴリズムは公開され、十分に検討され、標準化されるもとする。

13.4　投票システムは、すべてのネットワークを介して送信される機密データの完全性、信頼性、および機密性を保護する。

・　原則14：システムの完全性

投票システムは、意図的であろうと偶発的であろうと、システムの不正な操作から解放され、意図した機能を損なわない方法で実行する。

14.1　投票システムは、複数のコントロール層を使用して、セキュリティ障害または脆弱性に対する冗長性を提供する。

14.2　投票システムは、不必要なコード、データパス、物理ポートを削減し、他の技術的制御を使用することにより、攻撃対象を制限する。

14.3　投票システムは、ソフトウェア、ファームウェア、およびその他の重要なコンポーネントの完全性を維持および検証する。

14.4　ソフトウェアの更新は、インストールする前に管理者によって承認される。

・　原則15：検知と監視

投票システムは、異常な動作または悪意のある動作を検知するメカニズムを提供する。

15.1　投票システム機器は、自動処理に適した形式で保存されるイベントログ作成メカニズムを通じて重要なアクティビティを記録する。

15.2　投票システムは、発生したすべてのエラーメッセージを生成、保存、

および報告する。

15.3　投票システムは、マルウェアから保護するメカニズムを採用する。

15.4　ネットワーク機能を備えた投票システムは、現在のベストプラクティスに見合った、ネットワークベースの攻撃に対する適切で精査された現代的な防御を採用する。

5．ディスインフォメーション対策

5.1．ディスインフォメーションとサイバーセキュリティ

近年、選挙セキュリティの中には、フェイクニュースやディスインフォメーション対策も含まれるようになった。

ディスインフォメーション対策は、サイバーセキュリティ対策の一環として行われる。選挙に関するディスインフォメーションは、サイバー攻撃を通じた選挙に対する介入であり、広義の国家・政府に対するサイバー攻撃の一つであるとみなされる。

このため、ディスインフォメーション対策も含めて、米軍のサイバーセキュリティに関する部隊や関係機関はディスインフォメーション対策に関与しており、2018年中間選挙においてはロシアが試みたインターネットを通じた選挙干渉に国家安全保障局（NSA）と連携して干渉を阻止し[22]、2020年大統領選挙でも選挙防衛のためにサイバーセキュリティ対策を行ったとされている[23]。実際に、米軍のサイバー軍（U.S. Cyber Command）司令官であるポール・ナカソネ陸軍大将は、2018年の中間選挙までの時点で国防総省は選挙に関する任務を割り当てられ適切な権限とポリシーをすべて備えた十分に訓練されたサイバーセキュリティ部隊を編成したと述べた[24]。

---

22)　土屋大洋『サイバーグレートゲーム』（2020年、千倉書房）69頁以下。

23)　土屋大洋「米国サイバー軍と選挙防衛」土屋大洋・川口貴久編『ハックされる民主主義』（千倉書房、2022年）93頁。

ただし、国防・安全保障機関である連邦軍が選挙セキュリティに関して活動することについては議論があり、国防総省が「defend forward」という新しい概念を打ち出したことで注目された2018年の国防総省サイバー戦略[25]の中で、武力紛争レベルを下回る活動を含む悪意のあるサイバー活動をその発生源で妨害または阻止するための活動も米軍の任務であるとしていることから、外国政府等による選挙介入からの選挙の防衛を米軍が行うことは国際法上も許容されるという主張がある[26]。なお、選挙介入が武力紛争に該当するかどうかについては、武力行使に該当するレベルに至るものではないという理解が一般的であるが、一定の場合は国際法上の違法行為となると理解されている。

たとえばマイケル・シュミット教授は、外国による選挙干渉は、次の２つの要素が存在するときに「国際的な違法行為」のレベルに至るとする[27]。第１に、問題の作為または不作為は、法的に国家に起因するものでならない。第２に、その行為は、対象国に対して国際法で負う義務に違反しているものでなければならない。この２つの要素を考慮すると、選挙干渉がある国が他国に選挙干渉を行ったときに国際法上の義務に違反する可能性が最も高いのは、介入の禁止、他国の主権を尊重する義務、および人権を尊重する義務であるとされている。

---

24) https://www.defense.gov/News/News-Stories/Article/Article/2280489/cybersecurity-for-2020-elections-a-top-dod-priority-general-says/

25) DEP'T OF DEF., SUMMARY: DEPARTMENT OF DEFENSE CYBER STRATEGY 1 (2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBERSTRATEGY_SUMMARY_FINAL.PDF.

26) Jonathan K. Sawmiller, *Fighting Election Hackers and Trolls on Their Own Turf: Defending Forward in Cyberspace,* 56 IDAHO L. REV. 281 (2020).

27) Michael N. Schmitt, *Foreign Cyber Interference in Elections*, 97 INT'L L. STUD. 739, 742 (2021).

5.2. ディスインフォメーションとサイバーセキュリティ・インフラストラクチャセキュリティ庁

2018年11月16日、2018年サイバーセキュリティ・インフラセキュリティ庁設置法[28]が成立し、従来は国土安全保障省に設置されていた国家防護プログラム局を改組して、サイバーセキュリティ・インフラセキュリティ庁（Cybersecurity and Infrastructure Security Agency = CISA）が独立性の高い組織として設置された[29]。

2017年に国土安全保障省によって選挙が重要インフラストラクチャーに指定されていることから[30]、CISA は選挙自体と選挙関係のシステムのセキュリティを業務の一つとする。ディスインフォメーションは、選挙自体のセキュリティに関係するものとしてとらえられ、CISA のディスインフォメーション施策は、Mis-, Dis-, and Malinformation 対策を含むものであるので MDM と呼称されている。CISA には MDM チームが設置されているが、MDM チームの前身は海外影響力対策タスクフォース（CFITF）であり、2018年５月に CISA の前身である国家防護プログラム局に設置されたもので、国民が MDM によるリスクを理解し、MDM の組織やコミュニティへの影響を減らすために市民がどのような役割を果たせるかを支援することを任務とした。

CISA によれば、MDM には選挙プロセスに関する不正確な情報、根拠のない噂や、不完全または虚偽の結果報告なども含まれ、次のように定義される[31]。

---

28) Cybersecurity and Infrastructure Security Agency Act of 2018, P.L.115-278. 〈https://www.congress.gov/115/bills/hr3359/BILLS-115hr3359enr.pdf〉

29) 詳細については、廣瀬淳子「【アメリカ】サイバーセキュリティー・インフラセキュリティー庁設置」外国の立法278－２号（2019年）６頁以下を参照。

30) https://www.eac.gov/sites/default/files/eac_assets/1/6/DHS_Cybersecurity_Services_Catalog_for_Election_Infrastructure.pdf

31) CISA, Mis-, Dis-, and Malinformation: Planning and Incident Response Guide for Election Officials, https: //www. cisa. gov/sites/default/files/publications/mdm-incident-response-guide_508.pdf.

・　Misinformation

虚偽の情報であるが、危害を加える意図で作成・共有されたものではないもの。

・　Disinformation

個人、社会集団、組織、または国を誤解させ、危害を加え、または操作するために意図的に作成されたもの。

・　Malinformation

不正情報とは、事実に基づいているが、誤解を招いたり、危害を加えたり、操作したりするために文脈を無視して使用されるもの。

なお MDM は、選挙管理に関係するシステムへのサイバー攻撃、選挙人名簿の窃取や改ざん、電子投票の票の改ざん等とは異なり、有権者の権利を侵害したり選挙結果に直接影響を与えたりするわけではない。このため MDM も選挙セキュリティの一環といえるのかという点が問題となるが、CISA によれば、MDM は選挙セキュリティと選挙管理に影響を与えるものであるという。具体的に MDM が選挙セキュリティに与える影響としては、次のようなものがあるとされている[32)]。

・　手続干渉

選挙手続に関連する説明や内容が、混乱を招き、職員が円滑に選挙を運営することを阻害するもの。たとえば「悪意のある者が余分な郵便投票用紙を印刷して送れば、簡単に選挙の不正を行うことができる」という事実でない情報を拡散する行為が該当する。

・　選挙参加干渉

有権者を脅迫したり、選挙への参加を躊躇させたりするような内容。た

32)　CISA, *supra* note 31.

とえば「投票所の選挙立会人は、有権者を威嚇し、選挙運動を行い、投票を妨害することが許されている」という事実でない情報を拡散する行為が該当する。

・　選挙結果の非正規化

虚偽または誤解を招く主張に基づき選挙結果を委縮させたり、選挙管理の完全性に不信感を植え付けさせたりするもの。たとえば、アメリカの場合は一般的に日本よりも開票に時間を要し、開票結果が後になって訂正されることがあるが、これに関連して「選挙の夜に報告された開票結果が、その後数日または数週間にわたって変化した場合、選挙がハッキングされたか、危険にさらされたので、開票結果を信用することはできない」というような情報を拡散する行為が該当する。

・　個人攻撃

選挙管理関係者や投票管理者が選挙結果や選挙手続に干渉しようとする「悪者」であると虚偽の主張をするもの。

5.3. 選挙管理委員会等の役割

CISA は、州以下の選挙管理関係者にも MDM 対策を行うことを求めている。その際 CISA によれば、選挙管理関係者は「TRUST」モデルにより MDM 対策を実施することが有効であるという[33)]。TRUST とは、英語で T：Tell Your Story（ストーリーの伝達）、R：Ready Your Team（チームの準備）、U：Understand and Assess MDM（MDM を理解してアクセスすること）、S：Strategize Response（対応を戦略化すること）、T：Track Outcomes（成果を測定すること）である。

Tell Your Story は、有権者や利害関係者と関係を構築することで、国民の回復力が高まるというものであり、選挙が実際に行われて MDM 関連の脅威が発

33)　CISA, *supra* note 31.

生する前に、地域社会を啓発することである[34]。Ready Your Team は、選挙管理委員会等における MDM 対策のチームを構築することである[35]。Understand and Assess は、MDM と、MDM の対象となりやすい選挙関連の主要なプロセスや問題を特定して監視することである[36]。Strategize Response（対応を戦略化すること）は、情報報環境や関連技術の進化を考慮し、効果的な対応を行うため、リスクアセスメントに基づきどの MDM シナリオに対応するかの優先順位を決めることとされている。Track Outcomes（成果を測定すること）は、MDM の継続的な普及度合いと MDM 対策の効果を評価することである。特に現在の情報環境では、脅威は常に進化しており、MDM の対象となる場所、媒体、ナラティブ[37]も同様に変化しているので、それらに対応する必要があると指摘されている。

他方で、州政府などの選挙管理機関が、実際に MDM に独力で対処すること

---

34) 特に有権者啓発が重要であり、有権者に重要な期日・期限、投票所、投票の方法、選挙と選挙結果に関する信頼できる情報の入手先に関する情報を伝えることで、有権者の選挙に対する関心を持たせることができる。また選挙管理者が選挙後の監査や同様の措置を用いてどのように選挙を安全に実施するかについて。選挙前に説明することで、有権者の信頼を高めることができるとされている。

35) 対策チームの役割として、有権者がよく利用するソーシャルメディア・SNS へのオンライン MDM の可能性を報告またはフラグを立てるための手順を理解する、CISA のインターネット・セキュリティ・センター（CIS）と情報共有する、卓上演習を実施して MDM の脅威に対するチームの認識と理解を深めインシデント対応計画の欠陥を特定してインシデント発生時の役割と責任を明確にする、等が挙げられる。

36) 具体的には、監視対象リストの継続的更新、MDM はソーシャルメディア、マスメディア、口コミ、オンライン・フォーラム、メッセージング・アプリ、電子メールなど、数多くの手段で広まる可能性があるのでそれを特定すること、法律で認められている範囲内で MDM の監視を積極的に行うこと等が挙げられている。MDM の監視には、分析ツールを使用し、MDM に関連するキーワード検索、リーチ（何人が見ているか）、エンゲージメント（何人がそのコンテンツに「いいね」「シェア」「リアクション」をしているか）などを評価することが推奨される。

37) ナラティブについては、長沼加寿巳「認知領域における戦い：物語（ナラティブ）、感情、時間性」NIDS コメンタリー163号 1 頁以下（2021年）を参照。

は容易ではないので、CISA は、国民・州民の啓発用の資料も含めて、多くのツールキット類を提供している[38]。

6．おわりに

本稿では、アメリカにおける選挙セキュリティの観念について検討してきた。

選挙に関するディスインフォメーションも国家・政府に対するサイバー攻撃としてとらえ選挙セキュリティの対象として米軍も動員するなど、選挙セキュリティはアメリカの特異な制度といえる面があることは否めない。しかし、選挙のセキュリティは選挙インテグリティ[39]とも密接に関係すると理解されており、サイバーセキュリティ政策という観点にとどまらず、選挙というアメリカ民主主義の基礎をなす制度のインテグリティという憲法上の要請にも応えるべきものとなっている。

わが国ではサイバーセキュリティは重要インフラ、知的財産や営業秘密、個人情報やプライバシーに関する情報を保護するために重要であると一般的に認識されていると思われるが、選挙や表現の自由など、民主主義国家の根幹にかかわる制度や理念とサイバーセキュリティが連関している[40]という点で、選挙

---

38) 現時点で提供されているものとして、次のようなものがある。CISA インサイト：重要インフラを標的とした海外影響力の行使への準備と緩和、CISA インサイト：COVID-19 情報操作、COVID-19情報操作ツールキット、偽情報はあなたとともに止めるインフォグラフィックセット（スペイン語版もあり）、選挙情報収集ツールキット、外国人による干渉の分類法（スペイン語版もあり）、情報操作インフォグラフィック（スペイン語版もあり）、選挙管理者のための MDM 計画およびインシデント対応ガイド、レジリエンス・シリーズ：グラフィック・ノベル、レジリエンス・シリーズ：リアルフェイク・グラフィックノベル、噂のコントロールページのスタートアップガイド、ソーシャルメディアボットのインフォグラフィックセット（スペイン語版もあり）、偽情報のツール：真偽不明のコンテンツ（スペイン語版もあり）、パイナップル戦争：５つのステップで海外からの干渉を理解する（スペイン語版もあり）。https://www.cisa.gov/mdm#

39) 湯淺墾道「アメリカにおける選挙権の観念の一断面― integrity を手がかりに―」青山法学論集56巻４号（2015年）71頁以下参照。

セキュリティを含めたアメリカのサイバーセキュリティ政策は今後も注目に値しよう。

※本稿は、湯淺墾道「アメリカにおける選挙ディスインフォメーション対策の現状（１）（２）」選挙75巻８号・９号を大幅に加筆修正したものである。

---

40) この点については湯淺墾道「理念・原理・制度とサイバーセキュリティ法制－選挙を中心に」情報通信政策研究２巻１号（2018年12月）ＩB-1頁以下参照。