# 米国第二次トランプ政権におけるデジタル政策の現状
# （AI・サイバーセキュリティ）

伊藤　香織
JETRO/IPA New York

## 1　概要

2025 年 1 月 20 日、第 47 代大統領として Donald J. Trump 氏が再び就任し、第二次トランプ政権が発足して以来、米国では、政権による政策の変革が凄まじいスピードと膨大なニュースの量とともに進んでいる。約8か月が経過し、第二次トランプ政権におけるデジタル政策の具体的な動きがそろってきたところ、デジタル分野の主要政策である AI 及びサイバーセキュリティの主なポイントについて、背景及び前政権との比較を考察しながら読み解くこととする。

第二次トランプ政権の政策全体としての特徴を挙げれば、関税や移民への対応、連邦政府機能の縮小等多岐に渡るが、デジタル分野では、主に①米国第一主義、②連邦政府の縮小化・規制緩和、③多様性、公平性、包括性（DEI）の撤廃を含む言論の自由重視の社会政策への転換が、政策に影響を与える考え方だと思われる。

今やほとんどの分野に影響を与えている AI は、第一次トランプ政権時と比べ、研究開発対象から商業利用可能なサービスとなり、昨今では対中脅威に対する安全保障の要となりつつある。バイデン政権による責任あるイノベーションのための安全性や国際協調を重視した政策から、米国の競争力強化・グローバルでの優位性確立に向けた規制緩和・投資促進を主とする政策に変容している。また、バイデン政権で積極的に進められてきた AI のリスク管理や DEI、環境保護を重視した調達方針を廃止し、効率性・リスクベースを重視した調達方針に変更する等、イデオロギーの違いによる社会政策の影響が表面化している。

敵対国からの脅威が増しているサイバーセキュリティは、社会政策としてバイデン政権の偽情報対策などを廃止させるとともに、近年、米国の重要インフラや政府ネットワークへの侵入を中国に許していたことから、国家安全保障政策として、国家機能や重要インフラのサイバーセキュリティ対策に向けてシフトしている。連邦政府規則の停止や対策の遵守要件撤廃などの変更面もあるが、サイバーセキュリティ対策を進めること自体に大きな変更はない。

これまでデジタル分野は、民間による自由な一産業であったり、犯罪対応としてのサイバーセキュリティとして捉えられたりする側面が多かったものの、今や実社会のインフラとして、政府との関係が深まり、社会政策や安全保障政策にも広がりを見せ、影響を受け始めている。また、AI を含むデジタル分野のハイテク企業への市場依存度が高まっている。AI もサイバーセキュリティも広がりが大きいため、今回、すべての施策については概観できなかったほか、現政権の柔軟な政策運営や 10 月からの連邦政府の閉鎖により、全体的に先を見通すことが不透明であることから、引き続きの注視が必要である。

# 2　留意すべき背景

## （1）　政権運営の環境・支持層

### a.　政権運営の環境

同じ共和党選出で経験者としての大統領ではあるが、第二次トランプ政権の運営は、当選直後の予想とは異なり、第一次トランプ政権のときと変容していることは既に世の中で多く論じられているところである。大胆な政策変更が可能となっている背景として、現在の政権環境の主なポイントとしては以下が挙げられる。

図表 1：政権運営環境の違い

| | 第一次トランプ政権<br>（2017 年～2021 年） | 第二次トランプ政権<br>（2025 年～） |
|---|---|---|
| 共和党との関係 | 共和党の重鎮による政策の調整あり。 | 共和党との調整はほとんど見られない。共和党が議会として、政権の動きを抑制することはほとんどない。 |
| 議会との関係 | 任期前半では、上院・下院とも共和党による過半を占める。中間選挙により、任期後半では、下院の過半数を失った。 | 任期前半では、上院・下院とも共和党により過半を占める。もっとも、第一次政権と比較し、僅差（3票）での過半。 |
| 政府機関との関係 | 閣僚や政府高官は、共和党による推薦人物での任命が多かった。 | 閣僚や政府高官の任命は、分野の実績や経験でなく、大統領への忠誠心が優先基準。また、ベンチャーキャピタリストやテック経験者を多用。<br>積極的な政府職員の削減・退職の促進。 |
| 連邦最高裁判事の構成 | 保守派４名、リベラル派４名、欠員１名による拮抗。 | 保守派６名、リベラル派３名による第二次トランプ政権への親和性。 |

出典：各種公表資料をもとに筆者作成

また、メディアとの関係においても、第二次トランプ政権に批判的な既存メディアを排除し、好意的な新興メディアを優遇するだけでなく、自身のSNSを駆使し、大統領自らが直接声を届ける機会が多い。米国では、放送局での政治的公平性を求められておらず、自局のスタンスで報道するため、メディアによって報道の切り口がまるで異なっている。第二次トランプ政権から圧力を受けたメディアの経営層と、既存のスタンスを守りたいジャーナリストの間で亀裂が生じ、当該メディアでの職を辞するジャーナリストやキャスターの事案もよく見聞きするところである。

### b.　支持層

第二次トランプ政権における支持層は複雑かつ流動的である。第一次トランプ政権では、伝統的な共和党支持者である保守派のほか、クリントン大統領以降進められた経済のグローバル化に対し不満を抱えるラストベルトを中心とした労働者が中心だったが、第二次トランプ政権では、これに加え、ベンチャーキャピタルや一部ビッグテックなどの富裕層、MAGA（Make America Great Again）と呼ばれるナショナリスト、ヒスパニック等を中心とした人種的なマイノリティ、反ワクチン派も支持者として加わっている。デジタル政策の側面では、歴史的には共和党と対立する立ち位置にある GAFAM を中心としたビッグテックも、どこまで積極的に支持しているかは別として、総じて明示的な反対はせず、特にトランプ大統領就任時には多額の献金をする等、協力的な関係構築・維持を表明している。またテック業界の代表格である Elon Musk 氏は、国家債務の削減、規制緩和及び Woke と称されるマイノリティ等の人権を含む社会正義の考え方への反対の

観点から、選挙中には巨額の財政面でも支持したほか、第二次トランプ政権成立後は、特別政府職員として政権内部から、連邦政府機能の縮小のため予算や人員の徹底的な削減等で、5月まで活動していた。

結果として、第二次トランプ政権を支持する集団は多様な利害関係にあり、時としてお互いの利害がぶつかり合うことも起きている。国家債務を削減するべきとする Elon Musk 氏と、所得減税に恩恵のある富裕層や共和党では、7月に成立した大きくて美しい法案（One Big Beautiful Bill Act）[1]の策定時には意見が対立し、トランプ大統領との蜜月は過ぎたように見える。1月には、IT エンジニアや研究者などの専門技術者としての就労ビザ H-1B ビザについて、移民を排除して米国人の雇用を守るべきとする MAGA と高度移民人材を獲得したいビッグテックの間で軋轢が生まれた。自社のAIへの投資拡大及び安く雇用できる人材確保のため、今春頃から米国人を含む既存の従業員を大量に解雇しながら、高度移民人材ビザを要請するビッグテックの姿勢への不信感等も背景に、9月には、特定の非移民労働者の入国制限に関する宣言[2]を発し、同ビザの新規取得に対する費用が 10 万ドルに増額された。また、今のところ、バイデン政権時に始まったビッグテックへの反トラスト法を中心とする訴訟は継続しており、米国の中小企業への配慮も見られるところ、相対的には、スタートアップを推すベンチャーキャピタリストの意見のほうが政権に強く影響を与えていると指摘する識者もいるところである。

## （2） 社会での変化の兆候

これら支持層の多様化や軋轢の背景には、昨年 11 月の大統領選挙前から、社会で既にその兆候が見られていたとされている。

### a. ビッグテックと連邦政府の距離

シリコンバレー生まれのビッグテックは、歴史的には共和党と対立する立ち位置にあった。時の政府方針と関係なく、ビッグテック自ら実施しているコンテンツの掲載方針について、共和党からは、保守派の声を検閲しているとバイデン政権以前より批判されていた。例えば、SNS でのヘイトスピーチに対する厳格なポリシーや銃関連のコンテンツの制限等が該当する。また、主に民主党政権が進めていた施策ではあるものの、市場支配力を強めるビッグテックの解体に明示的に同調する共和党議員も一部存在している。

しかしながら、近年では、クラウド等の IT システムや宇宙開発、国防事業等での納入や取引を通じて、ビッグテックは、連邦政府のベンダーとしての存在感が増し、政治的に自由な立場から巨額の取引を失うわけにはいかない立場に変容してきている。

### b. 前提を覆す最高裁判決

連邦政府の政策執行との関係では、2024 年 6 月に出された最高裁判決[3]によりシェブロン法理が無効化された。すなわち、従前、法律や規則の解釈が曖昧な場合には、専門的な知見を持つ規制当局の解釈を尊重することとなっていたが、裁判所が解釈することとなった。これにより、法律及び規則の解釈について、事業者は規制当局に対して争いやすくなり、規制当局が敗訴した場合には解釈ではなく、議会の立法により、明記することが求められることとなる。規制当局としては法律で明記されていない場合の規則の策定や執行についての裁量が事実上減ることとなる。

社会政策との関係では、2023 年6月に出された最高裁判決[4]で、大学入学選考時に、多様性の観点から、人種等を配慮したアファーマティブアクション枠について、憲法の平等に違反すると判示された。個別の大学に対する判示であるものの、これにより、多様性による採用等を実施してきた企業の一部が方針を転換し始めており、DEI への揺らぎが見てとれる。

[1] https://www.congress.gov/bill/119th-congress/house-bill/1/text
[2] https://www.federalregister.gov/documents/2025/09/24/2025-18601/restriction-on-entry-of-certain-nonimmigrant-workers
[3] 22-451 LOPER BRIGHT ENTERPRISES V. RAIMONDO
[4] 20-1199 STUDENTS FOR FAIR ADMISSIONS V. PRESIDENT AND FELLOWS OF HARVARD COLLEGE

イデオロギーの対立による民主党と共和党の政治対立、またこれを踏まえた政権交代による劇的な方針変更自体は今に始まったことではないが、今回ほど、政権交代により、根本的に連邦政府の性質が変容すること、議会が動けないことは珍しいと、ワシントン DC 界隈では評されている。デジタル政策そのものが大統領選において大きな論点として争われたものではなかったが、こうした社会規範の変化が第二次トランプ政権でのデジタル分野の施策にも影響を与えているように見える。また、後述するように、政策の深化によりバイデン政権時に出された方針や施策がより具体的なものとなってきたことから、第二次トランプ政権による揺り戻しが大きく表出してきているものと考えられる。

# 3 AI ―安全性重視から優位性の確立へ―

## (1) 背景・前政権の振り返り

昨今、米国経済の成長はビッグテックの AI 投資に依存してきている。また、AI は機械的なデジタル技術であるだけでなく、社会的な要素を含むデジタルツールであるため、ここ数年で、社会的にも政策的にも大きく影響を与えている。ビッグテックによる AI 投資はテクノロジー業界の歴史上最大規模であり、2023 年から今年末までの3年間に、Google、Microsoft、Meta、Amazon は、2010 年から 2022 年までの合計支出を上回る新規投資を行う見込みとの分析もされている[5]。これまでの米国の破壊的なデジタル技術はインターネットや GPS のようにデジタル基盤技術が国の研究所で開発され、政府や軍が顧客となり、民間で商用化される流れが出来てきていたところ、AI、特に LLM においては人材・資金とも民間で最先端の研究開発が進められ、商用化した技術を政府や軍が購入する流れとなってきている。一方、AI への投資は、AI モデルの開発だけでなく、これを稼働させる AI チップやサーバー、その他ネットワーク機器、データセンター自体の構築、その前提となるエネルギーや水の確保、海底ケーブルの敷設にまで波及し、国としてのインフラ政策が問われることとなる。また、特に生成AIにより、一般ユーザーが利用できる対話型の AI が普及し、統計処理による出力とはいえ、その重みづけから回答内容には社会的な価値観を含むため、相対的に他のデジタル技術よりも、社会政策の影響を受けやすくなってきている。

バイデン政権は、基本的には第一次トランプ政権の AI 政策を踏襲していた。すなわち、連邦政府による AI の研究開発投資、政府内での AI の導入や利用に伴う倫理原則の策定、政府内 AI 人材の拡充等を継続した。もっとも、この4年間で、AI が研究対象から商業対象になるとともに、イノベーションの促進には責任ある AI 開発が必要であるとして、信頼性や透明性とともに、偏見や差別等によるリスクを念頭に置いた AI モデルの公平性や安全性の議論が重視された。また、世界的なモメンタムとしても、2023 年 5 月の G7 広島サミットを踏まえ、生成 AI を含む高度な AI システムの国際ルールの検討のためのプロセスである広島AIプロセスが進展し、人間を中心に据えつつ、個人、社会、並びに法の支配や民主主義の価値を含むG7国で共有された原則を守る必要性が首脳レベルでの共通認識とされていた[6]。米国はこれらを主導し、2023 年 11 月には、国立標準技術研究所（NIST）のなかに、先端 AI モデルの評価を念頭に、AI の安全性と信頼性に関する取り組みを主導するための the U.S. Artificial Intelligence Safety Institute（AISI）を設立し、業界とのコンソーシアムにより、ユーザー含む業界の意見を取り入れながら、AI リスクマネジメントフレームワーク[7]を策定し、AI モデルの安全性や公平性についての配慮を求めていた。また、大手 AI 開発事業者と組んでリリース前の先端 AI モデルのリスク評価に取り組み、海外の AISI 機関との共同評価に取り組んでいた。責任あるイノベーション促進のため、連邦政府は AI 導入を進める際には、これらの配慮を織り込んだ政府調達ルールとして、第一次トランプ政権時に策定された連邦政府における信頼できる AI の利用促進に関す

[5] https://www.washingtonpost.com/technology/2025/08/04/big-tech-ai-spending-economy/
[6] https://www.soumu.go.jp/hiroshimaaiprocess/pdf/document01.pdf
[7] https://www.nist.gov/itl/ai-risk-management-framework

る大統領令（13960 号）[8]で示された連邦政府の AI 調達にかかる原則を発展させた行政管理予算庁（OMB）メモを発出した（政府機関におけるAIの活用に向けたガバナンス、イノベーション、リスク管理の推進（M-24-10）[9]、及び政府におけるAIの責任ある取得の推進（M-24-18）[10]）。また、連邦政府内の AI 人材の採用や CAIO（最高 AI 責任者）の配置、ユースケースの収集・公開等が積極的に進められていた。

一方、AI は膨大な電力を消費するため、現状のエネルギー供給量や電力網のインフラでは不十分であり、その支援策についても政権内で検討がされ始めていた。2025 年 1 月 14 日には、AI データセンター及びこれに伴う電力施設確保のため、AI インフラにおける米国のリーダーシップの促進に関する大統領令（第 14141 号）[11]が発出された。国防総省やエネルギー省、商務省が管轄する連邦政府用地を AI データセンターと新しいクリーン電力施設に利用できるようにし、AI インフラと電力網との相互接続を促進させ、これらに関する許認可義務の迅速な履行、連邦政府用地周辺の送電整備を進めるよう、特定の機関に指示していた。

また、既に戦争のあり方が変わってきていると言われて久しいところではあるが、政権後半では、AI はグローバルな経済的・軍事的な力関係のバランスを再構築する可能性を秘めたデュアルユース技術として、次第に、安全保障上の政策にも位置付けられてきていた。AI の競争力の革新となる AI チップの輸出拡散規則[12]では、懸念国への AI チップの流入を止め、計算資源をコントロールすることに重きがおかれた。輸出国を3分類にリスト化し、高度な性能を持つ AI チップに対し、同盟国等には輸出するものの、武器禁輸対象国への輸出を禁止するほか、その間に位置づけられる大半の国（西側諸国も含む）についても輸出を制限する案を提示した。これについては、対中強硬派からは歓迎される一方、販売先が限定され海外での売上や米国の競争力を懸念する産業界や封じ込めには意味がないとする意見などの批判が生じていた。

## （2） 第二次トランプ政権

第二次トランプ政権における AI 政策は、トランプ大統領の言葉で言えば、Wake-up call と称された 1 月の DeepSeek の AI モデル R1 のリリースによる中国の AI の台頭に対する脅威への対抗、Woke 排除とする第二次トランプ政権の社会政策による個人の権利擁護からの転換とともに始まった。

### a. 米中対立におけるAI・米国優位性の確立へ

第二次トランプ政権では、AI によるリスクは認識するものの、バイデン政権は欧州同様、人類が AI に支配されるといった恐怖から、AI を怖がりすぎていたと批判し、AI は明るい未来の象徴としている。米国にとって真の脅威と認識されてきている中国が AI 開発において着々と米国に追いつくなか、現時点では有利にある米国の AI 競争力の向上、世界での米国の覇権獲得が最優先事項となった。特に 1 月の DeepSeek の R1 のリリースは、OpenAI の o1 モデルに匹敵する高度な推論能力を持つ性能を安価に実現したことで世界は騒然とした。真の開発力によるものなのか、他社の AI モデルを蒸留した不当な開発によるものなのかといった論争や、ユーザーの入力データが中国に流出するといったセキュリティやプライバシーの論点はあったものの、中国における AI の競争力が広く知られることとなり、ワシントンDCでの議論として、中国を分離して封じ込めるため AI チップの輸出管理を徹底的に強化すべきか、むしろ輸出先として解放して中国市場を取り込み米国や同盟国と共にグローバルな基準に参加させ、米国自身は Run Faster としてできるだけ先に進むしかないかで、大きく政策論争が続くこととなった。政策思想として、議会ではこの論争を体現する動きがよく見られるが、現時点では、関税交渉やビッグテックの第二次トランプ政権への協力姿勢も相まって、後者の考え方が優勢となっているように見える。

[8] https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government
[9] https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf
[10] https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/10/M-24-18-AI-Acquisition-Memorandum.pdf
[11] https://www.federalregister.gov/documents/2025/01/17/2025-01395/advancing-united-states-leadership-in-artificial-intelligence-infrastructure
[12] https://www.federalregister.gov/documents/2025/01/15/2025-00636/framework-for-artificial-intelligence-diffusion

第二次トランプ政権としての包括的な AI 政策としては、2025 年 7 月 23 日、テック系ポッドキャストとコミュニティ団体の運営する AI サミットで、短期間での政府の実行計画として、AI 行動計画（Winning the Race AMERICA'S AI ACTION PLAN）[13]が公表されたところであるが、2025 年 1 月から 6 月にかけても活発な展開が見られていた。

この半年間の動きを概括すると、AI ガバナンスとして、特に社会的価値観を伴うAIの安全性を確保する政策介入は、第二次トランプ政権の社会政策とともに徹底的に否定され、連邦政府の調達ルールを含む規制の緩和または撤廃、AI への民間投資の拡大・政府を含む社会での AI 導入の促進、世界に米国製 AI の売り込みを進めた。もっとも、第二次トランプ政権においても、安全対策として、AIによる詐欺対策やオンライン上の子供の保護の必要性の認識は変わっていないようにうかがえる。５月１９日には、連邦レベルで Take it Down 法[14]が成立し、AI による Deep Fake を含む不同意の親密な画像（NCII: Non-Consensual Intimate Images）の公開を禁止し、オンラインプラットフォーム事業者に対し、被害者からの通告を受けてから４８時間以内に該当コンテンツを削除する義務が課されることとなった。

１万件以上のパブリックコメント[15]を踏まえ、科学技術政策局（OSTP）を中心に策定されたAI行動計画は、基本的にこれらの流れを組んだもので、AI イノベーションの加速、AI インフラの構築、国際外交と安全保障を3本柱として９０以上の取り組みを各連邦政府機関に指示し、これを支える大統領令を3本同時に公表している（連邦政府における Woke AI の防止に関する大統領令（第 14319 号）[16]、連邦政府のデータセンターインフラ整備の許可手続きの加速に関する大統領令（第 14318 号）[17]、米国の AI 技術スタックの輸出促進に関する大統領令（第 14320 号）[18]）。

AI 行動計画では、エネルギー・データセンターの AI インフラをすぐに構築するための規制緩和、大きくて美しい法策定時に議会で大きくもめた論点である AI モラトリアム条項と同趣旨で州法による AI 規制への実質的な圧力（州に対する AI 関連の連邦政府資金の供与には AI を規制していない州を対象とする条件を付与）、人材への投資、AIモデルのためのデータ整備、より弾力的な AI チップの輸出管理等により、米国の競争力を維持すること、世界で中国に覇権を取られないように米国の AI をスタックレベルで輸出すること、これまで議論のあったオープンソースモデルも中国の躍進をきっかけに米国の覇権のため推奨していくこと、AI モデルの評価は安全保障面の観点が重視されること、政府（国防含む）での AI を導入・活用していくこと等の大方針が見てとれる。

[13] https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf
[14] https://www.congress.gov/bill/119th-congress/senate-bill/146
[15] https://www.nitrd.gov/coordination-areas/ai/90-fr-9088-responses/
[16] https://www.federalregister.gov/documents/2025/07/28/2025-14217/preventing-woke-ai-in-the-federal-government
[17] https://www.federalregister.gov/documents/2025/07/28/2025-14212/accelerating-federal-permitting-of-data-center-infrastructure
[18] https://www.federalregister.gov/documents/2025/07/28/2025-14218/promoting-the-export-of-the-american-ai-technology-stack

図表2：AI行動計画　概要

| 3本の柱 | 意義・指示項目 |
|---|---|
| 柱1：<br>AI イノベーションの加速 | ○意義<br>世界最強の AI システムの保有と同時に創造的で変革的な方法での活用で世界をリードしなければならない。世界が模倣したいと考える生産性向上型の AI 活用を発明し、受け入れる必要がある。連邦政府が民間主導のイノベーションが花開く環境を整える。<br>○指示項目<br>規制の簡素化と過剰な規制の撤廃、言論の自由とアメリカの価値観を保護、最先端 AI の確保、オープンソースとオープンウェイト AI の促進、AI の導入促進、AI 時代の米国人労働者支援、次世代製造業の支援、AI を活用した科学への投資、世界最高水準の科学データセットの構築、AI の科学を推進する AI の解釈可能性、制御性、堅牢性に関する画期的な研究への投資、AI 評価のエコシステムの構築、政府での AI 導入の加速、国防総省での AI の導入の推進、商用・政府用 AI のイノベーションの保護、法制度における合成メディアへの対抗 |
| 柱2：<br>AI インフラの構築 | ○意義<br>米国のエネルギー容量は 1970 年代以来停滞している一方、中国は急速に電力網を拡大。米国の AI の優位性の確立には、この傾向を逆転させる必要。許可手続きの簡素化、電力網の強化と拡大、それらを構築するための労働力の育成が不可欠。<br>○指示項目<br>半導体製造施設とエネルギーインフラの許可手続きの簡素化、セキュリティの保証、電力網の構築、半導体製造の回復、軍事・諜報機関向けの高度なセキュリティを備えたデータセンターの建設、高度な人材の育成、重要インフラのサイバーセキュリティの強化、セキュア・バイ・デザイン、AI 技術とアプリケーションの促進、AI インシデント対応のための成熟した連邦政府の能力強化 |
| 柱3：<br>国際的な AI 外交と安全保障でリーダーシップの発揮 | ○意義<br>自国内での AI 促進を超える必要がある。現在の競争優位性を持続可能なグローバルな同盟に転換し、敵対国が米国のイノベーションと投資にフリーライドすることを防ぐことが不可欠。<br>○指示項目<br>同盟国とパートナー国への米国製 AI の輸出、国際的な統治機関における中国の影響力への対抗、AIコンピューティングの輸出管理の執行強化、既存の半導体製造輸出管理の抜け穴対応、保護措置のグローバルでの調整、米国政府が最先端モデルの国家安全保障リスクの評価で先頭に立つことの確保、バイオセキュリティへの投資 |

出典：AI 行動計画（Winning the Race AMERICA'S AI ACTION PLAN）をもとに筆者作成

これらは、中国の AI の競争力の伸び、重要鉱物を握られていること、政府機関や通信インフラにもサイバー上侵入されていることから、米国の中国に対する焦りの表れでもあるとも受け止められており、徹底的に世界で勝ちにいくという姿勢が鮮明である。この包括的な計画については、米国内の業界からは歓迎され、特にビッグテックは第二次トランプ政権との協力による便益を享受している。一方、データセンター建設に伴う環境への影響やそもそもどれだけのエネルギーや水の供給が足りているかの観点や、人権への配慮不足の観点、多くの指示項目についてどれだけ期日内に実行できるリソースが連邦政府に残っているかの観点等から懸念する立場もある。また、大筋は前政権と大きくは変わっていないとの指摘もある。

足元のユーザーの米国民個人や企業レベルでは、AI利用に伴うリスクを懸念していないわけではない。民間企業でのAIの導入は進んでいるものの、特に生成AIについては必ずしもすべての企業がまだ手放しでアドバンテージを感じているわけではない。これを反映した州政府の動きと連邦政府である第二次トランプ政権の動きには対立が生じている。ここ数年、連邦議会には、連邦政府としてのAIに関する法案が数多提出されるものの、なかなか成立しないことから、州政府では、既に存在するプライバシー保護法や新しい州法の制定等で、AIについても一定程度歯止めをかけることを指向している。州議会で成立したものの、2024 年9月に、州知事による拒否権が発動されたカリフォルニア州の先端AIモデルのための安全でセキュアなイノベーション法案（SB1047）[19]は、州知事等の指摘を踏まえ横断的なAI規制法について引き続き議論がなされた結果、2025 年9月、先端 AI モデルを開発する大手事業者に透明性のガードレールを求める先端 AI 透明性法（SB53）[20]が成立したほか、ニューヨーク州でも、2025 年6月、責任ある AI 安全・教育法案（S6953B）[21]が州議会で成立し、州知事の署名待ちとなっている。その他、横断的ではなくとも、未成年の保護など個別の観点で AI に制限をかける州法はいくつか成立し始めている。既にプライバシー法はほぼすべての州法により手当されており、事業者はそれぞれの州に対応してきた歴史があるところであるが、AI開発事業者としては各州でのAI規制の制定は規制のパッチワークとなり事業者の競争力を奪うものとして反対を続けている。この論争は連邦議会においても、第二次トランプ政権が議会を主導した大きくて美しい法案の策定においては、所得減税の恒久化や低所得者向け医療保険の減額等が主な法律事項であったものの、AI開発事業者のロビイング等もあり、州におけるAIに関する過去の規制を廃止し、将来の規制を10年間禁止するAIモラトリアム条項が追加され、一大論点となった。各州や権利団体の反対を受け、まずは同法案自体の成立を優先させる政権全体方針のなかで、上院で否決された。この論争を受けて、AI行動計画では、AI 開発や導入を妨げる連邦・州レベルの不必要な規制の見直し・撤廃のため、企業や一般市民から情報提供を受けるほか、連邦政府予算でのAI関連の裁量資金の交付決定時に、州の AI 規制環境を考慮し、州の AI 規制がその資金の効果を妨げる可能性がある場合は資金提供を制限すると示された。州の自治が強い米国において、連邦法がどこまで州法の自治を超えることが許されるのか難しい法的論点でもある。また、こうした一連の動きを踏まえたAI事業者の市場での顧客への対応が注目される。

以下、最初の半年間を中心に、第二次トランプ政権での特徴的な観点からのAI政策について、簡単に紹介する。

**b. 社会政策の影響・安全への対応**

① バイデン政権のAI大統領令の廃止（1月）

前政権の大統領令が撤回またはレビューの対象となること自体はよくあることではあるが、第二次トランプ政権開始早々、AI分野における米国のリーダーシップを阻む障壁の除去に関する大統領令（EO14179）[22]により、バイデン政権の 2023 年 10 月 30 日付 AI の安全、確実かつ信頼できる開発及び利用に関する大統領令（第 14110 号）が廃止された。米国の世界での AI 分野のリーダーシップ維持のうえで、イデオロギー的偏見や人為的な社会的意図から自由な AI システムを開発しなければならないとしている。また、6か月内に、OSTP局長の Michael J. Kratsios 氏、AI 及び暗号に関する特別顧問の David O. Sacks 氏、大統領国家安全保障問題補佐官の Marco A. Rubio 氏を中心に、AI 行動計画を策定することを指示した。

② AI 調達規制の修正（4月）・更なるAIガイダンスの策定の指示（7月）

米国において、特に連邦政府の調達規制は、直接的には購買者である連邦政府に対する規制でしかないものの、市場規範を形成する政策の一つでもある。第二次トランプ政権は、連邦政府の調達において、特にハイリスクの AI モデルに対する内部規制が必要である認識は変えていないものの、煩雑な規制を削減

[19] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB1047
[20] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260SB53
[21] https://www.nysenate.gov/legislation/bills/2025/S6953/amendment/B
[22] https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence

するとして前政権で策定されたNISTのAIリスクマネジメントフレームワークへの準拠の必須化を翻し、2025 年 4 月3日、OMB メモ M-24-10 は、イノベーション、ガバナンス、公共の信頼を通じた連邦政府における AI 活用の加速（M-25-21）[23]により置き換えられ、アルゴリズムによる差別等を積極的に軽減するような公平性や個人の権利を配慮した規定等について削除された。同様に、OMBメモ M-24-18 は、政府におけるAIの効率的な調達を推進する（M-25-22）[24]により置き換えられ、米国で開発・製造された AI 製品・サービスの利用を最大化することが強調された。

大統領令（第 14319 号）では、Woke AI を防止するとして、連邦政府機関での調達においては、真実探求・イデオロギー的中立性の 2 つの偏りのない AI 原則に準拠して開発された大規模言語モデルのみを調達し、この原則が遵守できていないことが発覚した場合の解約費用もベンダーに請求する AI 調達に関する実施ガイドラインの発行を指示している。置き換えられた M-25-22、M-25-21 を補完するものとされている。同大統領令では、イデオロギー的な偏見や社会的なアジェンダが AI モデルに組み込まれると、出力の質と正確性が歪められる可能性がある、AI の文脈において、DEI には、人種や性に関する事実情報の抑制・歪曲、モデル出力における人種や性の表現の操作、批判的人種理論、トランスジェンダー等の概念による人種または性に基づく差別が含まれると指摘し、好ましい結果を優先するために真実へのコミットメントを置き換え、信頼できる AI に存在論的な脅威をもたらすとして、DEIに対する徹底的な批判が背景にある。

③ AISI のリブランディング（6月）

2025 年2月にパリで開催されたAIアクションサミットでは、直前にAISI所長が離任し、副大統領の JD Vance 氏によるスピーチの冒頭で、「今日は AI の安全性について話すためにここにいるのではありません。AI の機会について話すためにここにいるのです。」と宣言されたことから、NISTのなかに設置されたAISIは、第二次トランプ政権との方向性のずれから、その存続が危ぶまれていた。一方、連邦政府内におけるAIの知見ソースとなっており、議会や産業界からもAISIのAIモデルを科学的に測定・評価する役割、一定の標準を提示する役割が評価され存続を望む声も多く、The Center for AI Standards and Innovation（CAISI）として、安全性の観点は後退させながら、引き続き AI モデルの評価やテスト、標準化に向けた活動を実施し、より AI セキュリティや国家安全保障に注力することとなった。

**c. 民間投資の拡大、社会・政府での AI 導入の促進**

① 民間事業者の投資コミットメント （1月～）

第二次トランプ政権では、公の場で民間事業者の投資をコミットメントさせ、大統領がディールメーカーとして米国への投資を呼び込んだことを成果とすることが特徴的である。

DeepSeekによる安価なコストでの高性能AIモデルによる衝撃が冷めやらぬ 2025 年1月 28 日には、急増するAI需要、AGI の到来を見越した膨大な計算量を急増する需要に対応するとして、OpenAI、 Oracle、SoftBank 等により 5000 億ドル規模を想定したプロジェクト Stargate が、トランプ大統領と共に発表された。テキサス州アビリーンで、40 万個のチップを収容し、発電施設とともに巨大AIデータセンターを建設し、2026 年中ごろの完成を目指している。

2025 年7月 15 日には、天然ガスの埋蔵が多いペンシルバニア州は有望地域として、Dave McCormick 議員（共和党・ペンシルバニア州）の招聘で、第 1 回ペンシルバニア州エネルギー・イノベーションサミットが開催された。エネルギー、データセンター、AI 開発、金融・投資会社の CEO など約 20 のリーディング企業が参加し、トランプ大統領の前で、ペンシルバニア州での 10 年規模の AI インフラへの 920 億ドルの投資を表明した。財務省・商務省・環境保護庁の長官等も参加し、第二次トランプ政権として、プロジェクトの加速化への協力もコミットする形となり、Made in America の復活のための取り組みとして位置づけられる。

[23] https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf
[24] https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-22-Driving-Efficient-Acquisition-of-Artificial-Intelligence-in-Government.pdf

また、９月４日に開催されたAIを開発するビッグテックのCEO等との夕食会[25]においても、投資動向について、トランプ大統領から各社に直接確認している。
更に対外的に、５月には、エネルギー・地政学上優位なUAEやサウジアラビア、カタールとのトップセールスでは、エネルギー・資源の確保とともに、両国でのAI向けデータセンターへの投資、米クラウドサービスや NVIDIA の先端AIチップの供与も発表した。これを実現するため、AI チップの輸出拡散規則を転換したと言われている。3か国で 5.1 兆ドル規模とされ、中国との覇権争いのため経済取引・防衛技術供与での取り込みを図ったものとみられている。
第二次トランプ政権は、これらの取り組み及び関税交渉等の結果により、トランプ効果として多額の投資を呼び込んだことを広報している[26]。

更に大規模な産業計画の一環として、許可手続の簡素化と財政支援によるデータセンター他関連インフラの建設の加速するため、大統領令（第 14318 号）により、バイデン政権のAIインフラにおける米国のリーダーシプの強化（第 14141 号）を廃止し、効率的な環境審査として、環境規制の簡素化するとともに、政府の認める 100 MW 以上の新規データセンター、これに伴うエネルギー需要に関連するインフラ（石炭、原子力含む）、半導体施設、ネットワーク機器等への融資、助成金、税制優遇措置などの財政支援や、土地利用の許可の迅速化、開発可能な土地の拡大化を指示した。
また、対外進出について、大統領令（第 14320 号）により、米国製 AI の輸出を通じて同盟国との絆の強化、米国の基準とガバナンスモデルの促進、技術的優位性の維持、敵対国が開発した AI 技術への国際的な依存の軽減するため、世界中の同盟国およびパートナー諸国へのフルスタック型のアメリカの AI 技術パッケージの輸出を促進するための「米国 AI 輸出プログラム」の策定や選定案件への連邦政府の融資ツールの付与、AI 輸出促進のための政府戦略の策定、パートナー国での米 AI システムの展開に適切なイノベーション促進型の規制、データ、インフラ環境を整備する支援を指示した。

②　連邦政府でのAIの導入（3月～）
連邦政府のAI導入は、連邦政府の近代化としてバイデン政権以来進められ、政府内のユースケースの提示やAI導入のための政府調達も策定されてきていたが、第二次トランプ政権においては、更に加速している。オバマ政権下で成立した US デジタルサービスを母体とした政府効率化省（DOGE）の臨時的な発足により、特別公務員となった Elon Musk 氏により、連邦政府の効率化と生産性向上を目的に、連邦政府労働力の削減が実施された（同氏の権限範囲、解雇、政府システムのアクセス権に関しては各地で提訴が継続）。削減された労働力は、政府内 DB システムの改築や、AI の活用で補えるとしている。
２０２５年３月 20 日付けの情報のサイロ化を解消し、無駄・不正・濫用を防止に関する大統領令（第 14243 号）[27]により、連邦政府機関で個別用途ごとに管理することとされている米国人に関するデータベースを横断で連携させる動きがデータ分析会社 Palantir により進められている。
政府へのAIの導入加速は、業界にとっても市場の拡大として歓迎されている。連邦政府（国防分野を除く）の調達を調整するGSAの OneGov initiative[28]の導入により、連邦政府機関ごとだったITシステムの連邦政府調達について、標準化された条件と価格設定による IT ツールへのアクセスの容易化、契約期間中でも常に最先端の技術を入手できるようにする取り組みが進められている。８月１４日には、政府機関職員が、チャット型 AI、コード生成、文書要約等のAIツールを大規模に、より迅速かつ安全に、かつ無償で実験・導入できるセキュアな生成 AI 評価スイートとして、USAi[29]の提供開始を発表するとともに、８月２５日には連邦政府機関が導入するクラウドに対するセキュリティ評価・認証するプログラムである FedRAMP においても、対

[25] https://www.whitehouse.gov/articles/2025/09/president-trump-tech-leaders-unite-american-ai-dominance/
[26] https://www.whitehouse.gov/investments/
[27] https://www.federalregister.gov/documents/2025/03/25/2025-05214/stopping-waste-fraud-and-abuse-by-eliminating-information-silos
[28] https://www.gsa.gov/about-us/newsroom/news-releases/gsa-unveils-onegov-strategy-04292025
[29] https://www.usai.gov/

話型 AI エンジンへのアクセスを提供する AI ベースのクラウドサービスについて、優先的認可を行う方針[30]を示した。また、AIモデルを提供する各社とも統一調達のなかで、まずは連邦政府に使ってほしいものとして、OpenAIや Anthropic は1ドルで、既に政府にクラウドを納入しているGoogleは 47 セントで、2026 年の1年間、連邦政府用のAIモデルを提供することを表明している。

国防分野でも、トップダウンで急速に AI の導入が進められている。日常業務全体のデジタル化だけでなく、生成 AI 等よる現場の状況把握をするインテリジェンスやシミュレーション、AI エージェントによる戦場で自律して移動できる兵器の開発など、ミッションのデジタル化、高度化が加速している。今夏、国防総省では、安全保障のために AI に関連したツールを導入する契約を、OpenAI、Anthropic、Google、xAI それぞれと2億ドルで締結した。

③　AI 教育の推進・人材育成（4月～）

第一次政権においても、政府内 AI 人材の育成の検討がなされ、バイデン政権においても、民間からのAI人材の積極的な獲得や、海外からの高度な人材獲得や国際協力のためハイテク産業向けのビザ要件の緩和が進められてきたところではあるが、第二次トランプ政権では、次の段階として、社会でのAI導入の促進、また開発・ユーザー両面の観点での自国人材の育成のため、自国民に対するAIの教育について取り組みを進めている。

4月 23 日付けの米国の若者の AI 教育の推進に関する新たな大統領令（第 14277 号）では、次世代の米国人 AI イノベーターの育成、米国人の AI リテラシーとスキル向上のため、AI教育タスクフォースの設置とともに、K-12 教育（5～18 歳）において、教育現場でのAIツール採用の促進や現場の教育者への支援を命じている。9 月には、その成果の1つとして、官民連携により、米国の K–12 の子供たちや教師への AI 教育投資にコミットした企業リストをその内容とともに発表している[31]。AI 開発事業者や半導体事業者、ユーザ企業、コンサル、スキル認証事業者まで多岐に及ぶ。また、メラニア夫人主導プロジェクトとして、生徒や教師、コミュニティ等のチームで、AIツールを使って現実世界の課題を解決するプロジェクトを提案し、国レベルのショーケースとして 2026 年に表彰するAIチャレンジ[32]への参加が呼びかけられている。

また、AI行動計画では、AI による職業変化に対応できるよう、米国人に対する教育・再訓練の機会を拡大するため、AIスキルの開発のほか、AI が労働市場と労働者に与える影響を包括的に評価するための取り組みを推進する AI 労働力研究ハブの設立等が指示されている。8 月に労働省等により作成されたアメリカの人材戦略：黄金時代に向けた労働力の構築と題する報告書[33]では、AI がもたらす経済的繁栄を労働者が享受するために必要なスキルを確実に習得できる計画を打ち出している。

**d.　AIセキュリティへのシフト・AIチップの輸出管理の柔軟化**

①　AIセキュリティ

社会政策により、AIの安全性に対する政策はなくなったものの、広義の安全という観点では、サイバーセキュリティとAIの融合にシフトしてきている。AI システム自体が生み出す脆弱性への対応や、敵対者によるAIの利用による現実の脅威、またAIエージェント等研究者にとってもまだ解明不能な挙動等から、AIそのものはソフトウェアであるものの、AI の社会導入には信頼性が必要だとして、国立研究所や政府機関で既存のサイバーセキュリティのアップグレードに向けた活動が進んでいる。

NISTでは、従前AIリスクマネジメントフレームワークの策定により、AI固有のリスクに焦点をあてた企業のガバナンスの補完を担ってきたところであるが、更なるサイバーセキュリティとAIの融合として、AIシステムへの攻撃を緩和する対策の前提として、2025 年3月 24 日敵対的機械学習：攻撃と緩和策の分類体系と

[30] https://www.fedramp.gov/ai?_gl=1*c511wj*_ga*MTc0NTM0MjI5LjE3NTY5MTIzODU.*_ga_HBYXWFP794*czE3NTc4OTMyNDUkbzMkZzEkdDE3NTc4OTMyNjQkajQxJGwwJGgw
[31] https://www.whitehouse.gov/articles/2025/09/major-organizations-commit-to-supporting-ai-education/
[32] https://orise.orau.gov/ai-challenge/index.html
[33] https://www.dol.gov/sites/dolgov/files/OPA/newsreleases/2025/08/Americas-Talent-Strategy-Building-the-Workforce-for-the-Golden-Age.pdf

用語集[34]を公表するほか、既存のサイバーセキュリティのフレームワーク（CSF2．0）にAIの要素を組み込み、より実践的な導入ガイドを策定することを想定し、AI を導入した場合、どのような影響を与えるかを織り込むためのサイバーAIプロファイル[35]の策定や、既存の情報システムのセキュリティとプライバシー管理策のガイドラインであるSP800-53 の制御項目を活用した AI システム保護のための制御オーバーレイシリーズの開発等に向けて、業界との議論を進めている。

2025 年6月6日付けの国家のサイバーセキュリティ強化に向けた選択的取り組みの継続に関する大統領令（第 14306 号）[36]では、各省の既存の脆弱性管理プロセスに AI 特有の脆弱性を組み込むことが明記された。AI 行動計画では、重要インフラの防御を念頭に、国土安全保障省の支援を受けて、AI 情報セキュリティ分析センター（AI-ISAC）を設立し、CAISI および各州のサイバーセキュリティ局と協力し、米国における AI 関連情報およびインテリジェンスの収集を促進し、AI 関連脆弱性への対応を支援することなども求めている。

② AIチップの輸出規制（5月～）

第二次トランプ政権下において AI チップの輸出管理のあり方は、敵対国からの高性能チップへのアクセスを制限する戦略から、市場を拡大したい産業界の意向だけでなく、米国の海外での AI 市場の覇権ツール、関税交渉のツールとしても使われるようになり、柔軟化している。

バイデン政権末期に提示された輸出管理の新規則の施行日（5月 15 日）に近づく 2025 年5月 13 日、新規則は米国のイノベーションを阻害し、企業に過重な規制要件を課すことになり、数十カ国を二流国扱いすることで米国の外交関係を損なう恐れもあったとして、廃止を発表した[37]。これにより、同盟国や禁止国ではない中間国にも AI チップを供与できるようにした。

また、4月には、中国市場向けに作られた、最高性能ではないものの、国家安全保障上懸念が出される程度に高度な NVIDIA の H20 チップや AMD の MI301 チップは中国の輸出禁止の対象としていたが、7月にはこれらの性能は古いとして方針を転換し、販売を承認する方針に転換した。8月6日には、同社が輸出の際に米国政府に売上の 15%を支払うことを条件に輸出許可証を発行する合意となった。

これは、バイデン政権だけでなく、第一次トランプ政権とも方針が異なったことを示すものである。両党にとっても驚きをもって受け止められたほか、特に異例の 15%の支払いの性質に疑問を持つ者もいなくはない。また、共和党のなかでも中国を警戒して輸出を制限すべき立場と、制限しても無駄でありイノベーションの加速を重視する立場で分かれており、輸出規制を念頭に第三国経由で中国に密輸されることを防止するために、ジオフェンシングとなるチップセキュリティ法案も提出されている。AI政策に欠かせないAIチップの管理のあり方は、対中政策、米国の製造業の復活、国内投資の促進、財源赤字問題という複数の政策課題を解決しようとするなかで、不透明である。

# 4 サイバーセキュリティ ーコンプライアンス重視からリスクベース重視へー

## （1） 背景・前政権の振り返り

サイバー攻撃に対する脅威は、昨今の地政学リスクの増大と共に日増しに高まっている。地政学リスクにおけるリアルの攻撃とサイバー攻撃とが連動するようになっており、サイバーセキュリティ対策は国家の安全保障対策と同義であることは、業界内でも広く認識されている。

特に近年は、身代金を求めるような犯罪集団によるサイバー攻撃だけでなく、2021 年のコロニアル・パイプラインへのサイバー攻撃による米国東海岸でのパイプラインの停止はもとより、台湾有事が生じた際

[34] https://www.nist.gov/publications/adversarial-machine-learning-taxonomy-and-terminology-attacks-and-mitigations-0
[35] https://www.nccoe.nist.gov/projects/cyber-ai-profile
[36] https://www.federalregister.gov/documents/2025/06/11/2025-10804/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694
[37] https://www.bis.gov/press-release/department-commerce-announces-rescission-biden-era-artificial-intelligence-diffusion-rule-strengthens

の混乱を起こすためと推測される Volt Typhoon による米国全土での電力や水道等の重要インフラへの長年の侵入（2023 年公表）、更に諜報活動のためと推測される Salt Typhoon による米通信インフラへの侵入（少なくとも 2019 年以降から侵入と推定されている。2024 年公表）によるトランプ大統領含む政府高官の通話の監視、対象者の世界での移動情報、政府機関や重要インフラの構成要素データ入手等の諜報活動[38]が発覚し、政府・議会では危機感が共有されている。これら Typhoon 事案は、特に長期間、中国に支援されているとされる脅威アクターにインフラ網に静かに侵入・定着され、事前の検知や予防策ができていなかったたこと、政府や議会で直ちに効果的な対応ができなかったこと、また国民の生命に直結する電力や水道などの重要インフラはレガシーシステムがほとんどであるうえ、直接的には民間企業の所有や州政府の管轄として統一的な対応を取ることが難しくサイバーセキュリティ対策が遅れていることなど、多くの課題を浮き彫りにしている。また、これら重要インフラへの侵入自体は、Typhoon 事案だけでなくても起きている。

デジタル社会の進展とともに、クラウドへのデータの蓄積や AI への依存が増しているところ、フィッシングメールの洗練化や悪意あるコードの自動生成のような攻撃側のAI利用による攻撃の加速化だけでなく、クラウド環境等を監視するマネージドサービスプロバイダーへの標的化、AI 自体への侵入により悪意あるプロンプトの実行など、攻撃対象の内部リソースを攻撃に使い、検知や防御を困難にさせる脅威が増していると言われている。更に、今後、製造業などでは IoT や自動化で益々ネットワーク化していくことが想定され、認証情報を含むものの検査が簡単ではないエッジデバイスや IoT デバイスへの攻撃も懸念されている。

サイバーセキュリティを確保すること自体は党派を超えたアジェンダであり、バイデン政権は基本的には第一次トランプ政権のサイバーセキュリティ政策を踏襲していた。サイバー防衛の最前線に立つ組織として国土安全保障省内におけるサイバーセキュリティ・インフラセキュリティ庁（CISA）の設立や、国家安全保障戦略と連動させる国家サイバーセキュリティ戦略の策定、ボットネットによる脅威に対抗するための IoT のセキュリティ強化など第一次トランプ政権の政策を発展させた。CISA は、民間や地方政府のサイバー防衛の主導機関として、サイバー攻撃の脅威情報の監視や共有等の官民連携や国際連携、重要インフラのサイバーセキュリティ対策と強靭化への助言、対策ガイドの策定、サイバーセキュリティ人材の育成等を積極的に進めてきた。また、米国が長年抱える国土安全保障政策としての課題の多くがインターネット上の悪意ある活動に紐づいているとして、同省主導のもとオンライン上の偽情報対策に積極的に取り組んだ。ウクライナ紛争等も背景に社会を分断しようとする外国からの干渉を防ぐものとして地方政府に対する選挙インフラのセキュリティ対策の支援、新型コロナ感染拡大期におけるワクチン接種率の低迷を懸念した公衆衛生政策として新型コロナ感染やワクチンに関する虚偽情報の削除や、誤った国境政策や安易な越境情報を流布して大量の移民を誘引する人身密輸業者の虚偽情報等の削除をオンラインプラットフォーム事業者に要請し、一部のソーシャルメディア企業や自由が奪われることに反発する保守派の政治指導者層と対立し、憲法訴訟に発展することもあった（最高裁で原告適格なしと判示[39]）。

包括的なサイバーセキュリティ政策としては、2021 年5月、国家のサイバーセキュリティの改善に関する大統領令（第 14028 号）[40]が発出された。連邦政府機関に対し、連邦政府ITシステムのサイバーセキュリティの現代化として、ゼロトラストや多要素認証、クラウドセキュリティの強化、オープンソースソフトウェアのサイバーリスク対策として、ソフトウェアベンダーに対し製品開発に使用したコンポーネントをソフトウェア部品表（SBOM）文書として明示することを求めるなどサイバーセキュリティの取り組みの標準化が企図された。また、重大なサイバーインシデントを官民で調査する The U.S. Cyber Safety Review Board (CSRB)を設立したほか、連邦政府内のインフラへのインシデントの事前検知・脅威ハンティングや封じ込

[38] 結果的に、数百万人の米国人の情報が収集された可能性があるほか、600 社以上への影響、80 か国以上のインフラが標的になっていたとされている。2025 年8月、主な全容を解明した捜査当局等と西側諸国の共同クレジットで、事業者が本事案による侵入を防ぐための技術的なアドバイザリー文書が公表された。
https://media.defense.gov/2025/Aug/22/2003786665/-1/-1/0/CSA_COUNTERING_CHINA_STATE_ACTORS_COMPROMISE_OF_NETWORKS.PDF
[39] https://www.supremecourt.gov/opinions/23pdf/23-411_3dq3.pdf
[40] https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

め等による能動的なサイバー防御を指示した。2023 年には、この防御思想に基づくサイバー防衛における AI の実践として、The Artificial Intelligence Cyber Challenge（AI×CC）[41]を開始した。

政権末期である 2025 年1月には4年間の集大成として、国家のサイバーセキュリティにおけるイノベーションの強化と促進に関する大統領令（第 14144 号）[42]を発した。ベンダーがソフトウェア内の既知の悪用可能な脆弱性を修正せず、政府を侵害リスクに晒す事例が存在するとして SBOM に焦点をあて、安全なソフトウェア開発手法に関する指針の策定や、安全なソフトウェア開発手法の使用を証明するプロバイダーからのソフトウェアのみの使用・調達、IoT製品のラベリング制度である U.S. Cyber Trust Mark の付された製品の 2027 年までの調達、2035 年までの耐量子計算機暗号アルゴリズム（PQC）への移行に向けた製品リストの公表やガイドの策定、外国政府や業界団体を巻き込んだ促進のほか、AIを活用したサイバーセキュリティ対策の向上、詐欺対策も兼ねて移民も含む国民に対するデジタル ID の付与などを対応として指示していた。

議会においても、基本的にはバイデン政権と同調する形で、サイバーセキュリティ対策を強化する法案が成立した。コロニアル・パイプラインの事案等も背景に、2022 年には、重大なサイバーインシデント及びランサムウェアの支払があった場合に重要インフラ事業者が CISA に報告することを義務づける重要インフラ向けサイバーインシデント報告法（CIRCIA）[43]が成立している（当初の最終規則公布期限 2025 年 10 月）。

## （2） 第二次トランプ政権

第二次トランプ政権におけるサイバーセキュリティ政策は、地政学リスクを背景に、ますます安全保障政策の一貫として捉えられるようになっている。サイバーセキュリティ政策は、単なる犯罪対応ではなく、国家安全保障戦略やテロ対策といった戦略群に連なる一連の枠組みに位置づけられている。インシデントが起きてからの受動的な対応ではなく、事前に脅威をハンティングする能動的なサイバー防衛も実施段階として対処し始めているほか、攻撃的なサイバー作戦も議論されている模様である。また、AI×CC の革新的な成果から AI によるサイバー防御の自働化の可能性に大きな期待が寄せられているほか、国家レジリエンスとして、有事の際にインフラを人質に取られないよう、重要インフラのセキュリティ確保は第二次トランプ政権での安全保障における核心事項とされている。前政権と比較し、イデオロギー対立による社会政策の影響や、党の伝統的な対立軸である連邦政府機能の縮小化、事業者にとってのコンプライアンス要件や手続の緩和等企業の負担に対する姿勢の違いはあるものの、サイバーセキュリティ対策を進める方向性は変わっていないと考えられる。

もっとも、国の安全保障に位置づけられることによって、より広い視点で捉えれば、特に民間や州に対するサイバーセキュリティ対策支援機能は、政権が重視している国内の移民・治安対策よりは相対的に劣後して扱われているように見受けられる。

### a. 社会政策の影響

サイバーセキュリティ政策自体は、第二次トランプ政権の公約との関係で大きな変革事項ではないものの、まずは全体的な方向と一にして、結果的に社会政策の影響を受け始めた。第二次トランプ政権発足日早々に発せられた公約に基づく多数の大統領令のうち、1月 20 日付けの言論の自由の回復及び連邦検閲

[41] https://aicyberchallenge.com/
DARPA が ARPA-H 等と共催。電力や水道、病院等のインフラがサイバー攻撃をされたシナリオのもと、オープンソースツールで脆弱性を見つけ、AI により修正できる自律システムを構築する 2 年間の公開コンテスト。脆弱性に対するパッチを迅速に作成する能力とバグレポートの分析能力に基づいて順位付け。2025 年夏の決勝戦では、オープンソースソフトウェアの 5400 万超行のコードに存在する脆弱性に対し、自律的に発見し修正できる AI システムが開発され、従来コストの数分の一（コンテスト課題 1 件あたりの平均コスト約 152 ドル）で、平均 45 分でパッチを提出したことから、AI による防御のターニングポイントとされている。開発されたオープンソースツールは追って公開される予定。
[42] https://www.federalregister.gov/documents/2025/01/17/2025-01470/strengthening-and-promoting-innovation-in-the-nations-cybersecurity
[43] https://www.congress.gov/117/plaws/publ103/PLAW-117publ103.pdf

の終結に関する大統領令（第 14149 号）[44]では、バイデン政権の偽情報対策は言論の自由を害する検閲であるとされ、連邦政府によるオンライン上の言論の自由に抵触する働きかけや政策を禁止し、過去4年間の施策の見直しを命じた。オンライン上の偽情報対策の活動は既に縮小しかけていたが、予算・人員とも止められた。トランプ大統領の支持者からすると、バイデン政権では意図に沿わない言論を排除するような実質的な圧力があったとし、偽情報対策については徹底的に否定している。また、第一次トランプ政権時に任命した CISA 初代長官 Chris Krebs 氏が、CISA の業務として選挙関連の偽情報を否定するサイトを開設する等、選挙のセキュリティ対策の支援を担い、2020 年の大統領選挙は盗まれたものではないと明言していたことに反発し、同氏指揮下の CISA は、いわゆる偽情報対策という名目で保守派の見解を弾圧し、主要ソーシャルメディアに働きかけ又は強制して党派的な使命を推進したとして、同氏の行為の適格性や同氏が担っていた CISA の活動の評価を指示する等の大統領令[45]が 2025 年4月に出されている。

**b. 連邦政府機能の縮小・重要インフラ対策へのシフト**

第二次トランプ政権の一般的な連邦政府の機能・予算縮小の動きと相まって、連邦政府全体でサイバーセキュリティ政策を担うリソースも縮小されている。連邦政府として国家安全保障のためのサイバーセキュリティ対策は実施するが、民間向けのサイバーセキュリティ対策は基本的に州政府が担うもの、特に CISA は必要最低限の重要インフラ対策を中心に、民間セクターとの連携による社会サービス維持のため実施すればよい、偽情報対策や教育、国際連携などにおける CISA の役割は縮小すべきというのが第二次トランプ政権の大きな方向となっている。2025 年3月 18 日付け、州および地方の準備体制による効率の向上に関する大統領令（第 14239 号）[46]では、サイバー攻撃や山火事、ハリケーン等のリスクに対する連邦政策は州や地方自治体、個人の管理によるべきものを前提として、過去の重要インフラ政策のレビューとともに、これまでのすべての危険要因対応アプローチからリスク情報に基づくアプローチへ移行した国家レジリエンス政策の策定を求めている。また、その際に重要インフラ政策には、誤情報、 偽情報または悪意ある情報に関連するいかなる政策、いわゆる認知インフラは含まないと明示している。

政権移行に伴い、政府閉鎖以前の時点で、政治任用のポストを含む CISA の3分の1の人員は既に離任したと言われており、政権の表明した 2026 会計年度の予算要求書では、不要な偽情報対策や国際連携部門の廃止を理由に CISA の予算は減額されている。Salt Typhoon 事案の調査を担っていたCSRBも早々に廃止され、誰が重大インシデントの調査を担うのかと懸念されている。また、予算削減により、各種プログラムの継続の可否も揺れており、連邦政府予算で運営されている脆弱性プログラムが突然の廃止通知を受けた後、業界からの反発で復活する等、政策の見直しの過程において業界が混乱する過渡期があった。また、連邦政府職員の削減は CISA に限ったものではなく、サイバーセキュリティ政策における連邦政府全体の指令塔となっている国家安全保障局においても、トップの解任含め、大幅な人員削減がされている。総じて、サイバーセキュリティ対策を担うリソースの削減は、増加するサイバー攻撃への脅威を増すこととなり懸念されるというのが、議会・業界の主な反応であり、第二次トランプ政権と議会が対立する場面がある。議会では、第二次トランプ政権が CISA 長官候補として指名した Sean Plankey 氏の承認について、通信業界のセキュリティ脆弱性に関する 2022 年報告書を公開するまで、CISA の長官として指名されている氏の承認を阻止するとの民主党議員の意向により、承認が遅れている。また、第二次トランプ政権の予算削減の動きに対し、議会では超党派として CISA の予算を復活させるための法案が提出されており、引き続き審議されている。

もっとも、こうした動きにより、CISA の業務が完全に止まったわけではなく、第二次トランプ政権直後の完全な混乱期を経過して、新たなサイバーインシデント対応ツールの開発、サイバーセキュリティ助成金の提供などが公表され、米国のサイバーセキュリティ対策は粛々と続けられている。直近では、CISA が公

[44] https://www.whitehouse.gov/presidential-actions/2025/01/restoring-freedom-of-speech-and-ending-federal-censorship/
[45] https://www.whitehouse.gov/presidential-actions/2025/04/addressing-risks-from-chris-krebs-and-government-censorship/
[46] https://www.govinfo.gov/content/pkg/FR-2025-03-21/pdf/2025-04973.pdf

共財として管理し、国際的にも参照されている CVE プログラムは、品質向上のため次の段階に移行すべきとして、戦略ビジョン：サイバーセキュリティの未来に向けた CVE の品質[47]が発表されている。

また、重要インフラのサイバーセキュリティ対策の第一段階として、OT サイバーセキュリティの基盤となる所有者および運用者向け資産インベントリガイダンス[48]が公表されている。IT と OT が交錯する重要インフラは、OT のマイクロセグメンテーション、ゼロトラストの構築、そのうえでの PQC 対応の実現が求められる。これに向けて、OT システムの近代化、リソース不足への対応、官から民への情報共有の更なる深化が議論されている。また、重要インフラの対策を担当する省庁でも取り組みが進められている。例えば、電力ネットワークのトラフィックで敵対的な兆候がないか内部ネットワークセキュリティを監視する具体基準の承認[49]がなされているほか、水道分野においても、水へのサイバーセキュリティの脅威と 10 の推奨事項を記した報告書[50]が出され、対策に取り組む事業者向けに助成金の配布が開始されている。

### c. 規制負担の軽減①

2025 年6月には、第二次トランプ政権としての包括的なサイバーセキュリティ政策の指針となる大統領令（第 14306 号）を発出した。バイデン政権の大統領令（14144 号）について任期終了直前にこっそり盛り込まれたとして、同大統領令とオバマ政権の特定の悪意あるサイバー活動に従事する者の資産の凍結に関する大統領令（第 13694 号）[51]を一部改正する形となっている。中国・ロシア・イラン・北朝鮮を外国のサイバー攻撃者として直接言及する一方、偽情報またはサイバー攻撃を伴う脅威に関与する個人に対するサイバー制裁を個人から外国人に限定し、サイバー執行ツールの濫用を防ぐ措置として国内の政治活動は明示的に除外した。また、政府サービス享受プロセスの簡素化として進められたデジタルIDについては不法移民に承認された身分証を与えうるものであるとして給付金詐欺や不正アクセスへの懸念を理由に完全に廃止するものの、既存の大統領令（第 14144 号）を完全に撤回するのではなく、一部改正の形をとるとおり、大きな方向性や項目は変わらず、全体的にコンプライアンス重視から、事業者の負担軽減、運用上の実用性や実導入を重視している。例えば、ソフトウェアセキュリティのコンプライアンスとして、連邦政府の請負業者に対し、NIST のセキュアソフトウェア開発フレームワークに準拠した確認書、証拠書類、文書の提出による報告義務を求めていたものを排し、自主的な実施に移行させたり、PQCの移行の方針や最終期限は維持するものの、そのためのロードマップを簡素化したりしている。サイバーセキュリティにおけるAIも、学術界との多くの研究プロジェクトを縮小し、各省庁の既存の脆弱性管理プロセスへの組み込みを重点化している。

### d. 規制負担の軽減②

第二次トランプ政権の特色でもある規制緩和は、特にサイバーセキュリティ政策における官民の役割分担であるサイバーセキュリティインシデント報告において影響を受けている。従前、サイバーセキュリティ上のインシデントが生じた際には、各州のプライバシー保護法等におけるデータ侵害規則や連邦政府における一部の業界での義務やFBIへの任意報告などが対象だったが、バイデン政権下において、サイバー攻撃の増加や Typhoon 等による攻撃を受けて、各行政機関においても議会においても行政に対する報告義務が拡大した。2022 年に成立した CIRCIA では、16 の重要インフラ業種で、重大なサイバーインシデント事案を対象に 72 時間以内、ランサムウェアは 24 時間以内に CISA に報告を求めることとなり、定義等を定める具体の規則制定案[52]が 2024 年4月に CISA から通知され、2025 年 10 月までに公布することとなった。また、

[47] https://www.cisa.gov/sites/default/files/2025-09/CISA_Common_Vulnerabilities_and_Exposures_CVE_Program_Vision-v6_CLEAN.pdf
[48] https://www.cisa.gov/resources-tools/resources/foundations-ot-cybersecurity-asset-inventory-guidance-owners-and-operators
[49] https://www.federalregister.gov/documents/2025/07/02/2025-12309/critical-infrastructure-protection-reliability-standard-cip-015-1-cyber-security-internal-network
[50] https://www.epa.gov/system/files/documents/2025-08/water-cybersecurity-recommendations_water-sector-cybersecurity-task-force_apr25-072525.pdf
[51] https://www.federalregister.gov/documents/2015/04/02/2015-07788/blocking-the-property-of-certain-persons-engaging-in-significant-malicious-cyber-enabled-activities
[52] https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements

2023 年7月には、証券取引委員会（SEC）が、投資家保護の観点として、上場企業に対し、サイバーセキュリティインシデントが重大な影響を及ぼすと判断した日から 4 営業日以内に SEC への報告を原則義務付ける最終規則[53]を提示した。また、投資顧問・投資会社や証券会社や証券取引所等に対するサイバーセキュリティのガバナンス・インシデント情報の SEC への報告・開示に関する規則案を3本策定していた。国防総省は 2024 年 5 月、防衛連邦調達規則（DFAR）に基づく対象防衛情報保護及びサイバーインシデント報告要件を更新し、政府契約業者に対し、発見後 72 時間以内の迅速な報告を義務付けた。パイプラインを含む陸上輸送や海上保安を担う米国運輸保安庁でも、保安指令において、暫定的に 24 時間内の報告義務を求めるようになってきたが、2024 年 11 月には、特定のパイプライン・鉄道所有者・運営者、特定の陸上輸送事業者に対し、サイバーセキュリティインシデント報告を求める規則制定案が出された。

重複規制含め既存の規制撤廃を使命とする第二次トランプ政権は、政権開始早々の 2025 年 1 月 31 日には、10 対 1 規制緩和イニシアチブを発表し、規制緩和による繁栄の解放に関する大統領令（第 14192 号）[54]により、新たな規制義務を公布する際、各連邦政府機関に対し、法律で禁止されている場合を除き、少なくとも 10 件の既存規制の廃止対象を特定するよう指示している。分野を限定したものではないが、サイバーセキュリティ分野も当然に対象となり、各連邦政府機関は規制の制定を躊躇する背景となっている。CISA は、CIRCIA の施行規則を最終化する権限を 2026 年5月に延期することを発表した。SECは、6月に上記3本を不要な負担だったとして自主的に撤回している。政府へのインシデント報告は、政府によるインシデント対応支援や犯人逮捕による被害拡大・社会抑止につながるものであり、政策の停滞は望ましくないが、産業界にとっては、類似の制度による報告が複雑化していることへの不満が高い。また第二次トランプ政権による規制環境の流動性が高く、変更の可能性があることから、産業界として今後の動きを注目している分野でもある。

こうした政府への報告による官とのインシデント共有の際には、インシデントに関する第三者の機微情報や個人情報、脆弱性の管理手法等を含めて連邦政府に任意提供することとなり、当該第三者から訴えられるリスクや連邦政府への情報公開請求のリスクがある。このため共有における法的な免責や開示の例外措置が円滑なインシデント共有や業界での協働に役立つこととなる。また、民間でのネットワーク監視もサイバー防衛手段としては有用である。これらを合法化し、推奨するため、10 年間の時限法として制定されていた 2015 年サイバーセキュリティ情報共有法（CISA2015）[55]が 2025 年9月末に失効した。このため、議会では同法の再承認及びこれに乗じた修正案に向けた活動が活発化している。同法の再承認自体に反対する動きはあまりないが、これに乗じて予算の拡大を増やそうとする修正案、CISA の偽情報対策についても徹底的に制限または追加する修正案、OT や IoT についても範囲を広げるよう追加する修正案などが党対立とともに混戦し、9月末を過ぎても再承認が得られず、失効したままとなっている。任意の提供であるものの、インシデント共有は、同法によりこの 10 年でもっともよく進んだ官民連携と言われており、サイバー攻撃の脅威が増すなか、業界関係者からは長期の再承認が望まれている。



[53] https://www.federalregister.gov/documents/2023/08/04/2023-16194/cybersecurity-risk-management-strategy-governance-and-incident-disclosure
[54] https://www.federalregister.gov/documents/2025/02/06/2025-02345/unleashing-prosperity-through-deregulation
[55] https://www.congress.gov/bill/114th-congress/senate-bill/754