2023年8月

**米国情報　2023年8月分**

日賑グローバル株式会社

米山

● 米国における重要インフラ（電力・水・通信など）の災害対応・防衛（サイバー・物理的防衛）を巡る政策動向と、インフラ関連企業に求められる規制対応の展望

国家サイバーセキュリティ戦略公表（2023/03）に伴う重要インフラ関連企業に今後想定される影響と対応。

日本含め、同盟国による重要インフラ防衛を巡る米国からの要請と政府の対応、企業への示唆。

**はじめに**

冷戦時代において、米ソは核配備と共に、NATOとワルシャワ条約機構の通常兵器を、ドイツを中心とした前線に配備して対峙することで均衡を保ったが、互いの域内のインフラを攻撃するというシナリオはなく、あくまで軍事施設がターゲットであった。

冷戦後、東西のヒトモノカネ情報技術の流れが自由化するグローバル化においては海外資本が米国内のインフラに入り込むことを懸念する事案として2006年のUAE資本による米国港湾管理会社買収を米議会が問題視し、結果として買収不成立となっている。

そして中国が国力を増し、米国に対する対抗姿勢を示してきた近年では、電力・通信網等に中国製品を組み込むことのリスクへの懸念から、米国の政治は中国製品排除そしてCFIUSを通じた中国資本の排除へと進んできている。

本稿では米国における重要インフラの定義から始めてサイバーアタック事案に伴うインフラのサイバーセキュリティ対応、そして2年前のインフラ法を通じた異常気象等に適応するインフラ対策、そして重要インフラ防衛に関する日本をはじめとした同盟国との連携について時系列的に示す

**１．Presidential Policy Directive 21 ソース：ホワイトハウス**

2013年2月に発出された大統領からの指令は、米国内の重要インフラを分野別に定め、それぞれの防護を担う省庁を定義しつつ、国土安全保障省（DHS）がそれらの頂点に立って重要インフラの防護責任を負い、準備、実行、評価のPDCAを回し、必要な研究開発投資や情報共有を行うことを命じている。

この指令では以下の16の重要インフラ分野が定められている。

**分野名 リスク管理担当省庁**

1. 化学分野 DHS（CISAが民間と連携して実行）
2. 商業施設分野 DHS（CISAが8つの下部分野に防護戦略を指示）
3. 通信分野 DHS（CISAが民間と連携して実行）
4. 重要製造分野 DHS（CISAが重要度と優先度を定めて実行）
5. ダム分野 DHS（CISAが9万を超えるダムの防護をパートナーと実行）
6. 防衛産業基盤分野 国防省（10万社を超える産業基盤の防護）
7. 緊急サービス分野 DHS
8. エネルギー分野 エネルギー省
9. 金融サービス分野 財務省
10. 食料・農業分野 農務省および保健福祉省
11. 政府施設分野 DHSおよびGSA（調達局）
12. 保健分野 保健福祉省
13. 情報技術分野 DHS
14. 原子炉、核燃料、核廃棄物分野 DHS
15. 輸送システム分野 DHSおよび運輸省
16. 上下水道分野 環境庁（EPA）

**２．Presidential Policy Directive 41 (PPD-41)**

2016年7月に発出された本大統領指令は政府組織であれ、民間組織であれ、サイバーアタックを受けた場合の連邦政府としての対応の原則を示すもの。

**３．The National Cyber Incident Response Plan ソース：DHS**

前出PPD-41に基づきDHSが2016年12月に発出した本プランは米国の重要インフラにとってリスクとなる重大なサイバーインシデントに対応し、そこから復旧することを支える役割と責任、能力そして調整組織についてまとめている。

**４．アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁（CISA）創設**

重要インフラのサイバーセキュリティを担うDHSの外局として創設されている。

トランプ前大統領が、サイバーセキュリティ・社会基盤安全保障庁法[[1]](#footnote-1)に署名したことにより、2018年11月16日に設立。

**５．コロニアルパイプライン社へのランサムウェア攻撃　　ソース：CloudGate**

ガソリンやディーゼル、ジェット燃料などを扱うコロニアルパイプライン社はDarkSideからのランサムウェア攻撃を受け、2021年5月7日から1週間操業停止に追い込まれた。

アメリカ東海岸の燃料供給の45%が影響を受けたことから同社は身代金440万ドルの支払いを実施。

本事案の結果、5月12日にはサイバーセキュリティ向上を目的としたゼロトラストアーキテクチャの導入などを含めた大統領令が発令された。

**６．重要インフラへのサイバーアタックについての議会の認識とCISAの役割 ソース：CSIS**

コロニアルパイプラインの被害はもとよりマイクロソフトに対するロシアからの攻撃など、中国、ロシア、イラン、北朝鮮からのサイバーアタックが様々なインフラ分野に及んでいる。

特に中国が要注意。2019年発効された米国国防権限法NDAA第889条には、スパイ　攻撃などに対する保護を強化するためのガイドラインが含まれており、通信やセキュリティ目的に用いられる特定企業の機器・サービスの購入や使用など広く制限する規定が設けられたが専ら中国企業が対象。

重要インフラ防護の考え方として事後（インシデント報告）から事前準備へ、そしてサイバーアタックをしかける国や組織への諜報活動へと進むべきとの発想あり。

官民で良く協議し、攻撃対象となる重要インフラを考え、サプライチェーンにも配慮する必要あり。

重要インフラの85%は民間所有・民間運用であることからその防護においても官民連携が重要。脅威環境に関する共通のピクチャーを官民で共有し、行動がとれるためのJoint Cyber Defense Collaborationが大切。

一方、サイバーアタックは技術的にもコスト的にも行いやすくなっている状況に対し、グローバルに連携して、そうし難くする対応が必要。

CISAは連邦政府のサイバーセキュリティをゼロトラスト型に移行するにあたり102もの省庁を束ね、契約企業と実行に移す。

**７．インフラ法成立 ソース：ホワイトハウス他**

2021年11月に成立したインフラ法では新規インフラの建設や老朽化したインフラの　維持整備とともに自然災害やサイバーアタックに対するインフラ防護とレジリエンスの　強化がうたわれた。　これには、ハリケーン、洪水、山火事などの自然災害に耐えられるように既存のインフラをアップグレードするための資金が含まれている（別紙２）。

また、気候適応策として、自然災害の頻度や激しさに対する気候変動の影響を認識し、気候適応策を組み込んでいる。

さらに、エネルギー網、輸送システム、通信ネットワークなどの重要なインフラのレジリエンス基準を確立することを目指している。

重要インフラに関する独自の脆弱性を把握すべく連邦政府が州および地方自治体と積極的に関与することを想定している。

連邦政府は、重要インフラに対する自然災害の影響に関する研究とデータ収集を行う。

重要インフラのレジリエンス強化のため、政府と民間部門の間のパートナーシップを　推進し、インフラの脆弱性に対処するための専門知識、リソース、資金を共有する。

自然災害等緊急時、影響を受けた地域を支援するための連邦機関やリソースの調整を含めた緊急時対応計画を整備する。

再生可能エネルギーと送電網の近代化を通じ、復元力の高い分散型エネルギーグリッドを整備し、自然災害への耐性を高める。

連邦道路局 (FHWA) は、道路、橋、その他の交通インフラにおけるレジリエントな建設資材の使用と実践を推進。交通システムの設計と保守に気候変動への配慮を含む。

エネルギー、交通、水道、通信などの重要インフラ部門のサイバーセキュリティの強化に重点を置く。CISAは民間部門と協力してこれを実施する。

洪水が発生しやすい地域では、米陸軍工兵隊およびその他の機関が洪水リスク管理プロジェクトを実施。これには、地域社会や重要な施設に対する洪水の影響を軽減するために、堤防やその他の治水インフラを建設または強化することが含まれる。

EPA は、上下水インフラのレジリエンスを向上させるために資金と技術援助を提供。　これには、異常気象に耐えられるように施設を改修することや、安全な飲料水の継続的な供給を確保することが含まれる。

FEMA は、自然災害やその他の危険に対する重要なインフラの脆弱性を軽減することを目的として州と地方自治体に助成金と支援を提供する。

米国海洋大気庁 (NOAA) は、海面上昇や高潮に対する港湾などの沿岸インフラのレジリエンスを強化する対策を実施する。

米国国立標準技術研究所 (NIST) や国立科学財団 (NSF) を含むさまざまな連邦機関が、インフラのレジリエンス向上に重点を置いた研究開発プロジェクトに資金を提供。被災中および被災後のインフラのパフォーマンスを向上させるための新しい技術、材料、建設手法を探求している。

米国住宅都市開発省 (HUD) は、特にサービスが行き届かず脆弱な地域に強靱な住宅、インフラ、公共施設を構築することを目的としたコミュニティベースの取り組みを支援。

**８．Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)**

2022年3月に法制化された本法では、CISAは重要インフラと連邦政府に対するサイバーセキュリティ上の脅威に関するリスク評価を行い、各省庁のリスク評価に基づくインシデント報告義務のルールを定めることを求める。

各省庁は職員への指導と訓練を適宜行う。

重要インフラの所有者或いは運用者に対し、所定期間内にサイバーインシデントやランサムペイメントについての報告義務を課し、ルールを定める。

サイバーセキュリティの脅威に関する報告の省庁内の報告様式を標準化させ、ランサムウェア攻撃に関するタスクフォースを設け、脆弱性の高いところを見つけるパイロットプログラムを設ける。

GSA内に連邦リスクおおび権限管理プログラム（FedRAMP）[[2]](#footnote-2)を設け、しかるべき　権限を付与する。

FedRAMPはクラウドコンピューティング製品およびサービスに関し、安全性評価、権限および継続的モニタリングに関する連邦政府の標準的アプローチを提供する。

**９．国家安全保障戦略における重要インフラ防護の位置付け　　ソース：ホワイトハウス**

2022年10月に発表された国家安全保障戦略では全48ページ中、インフラに関する　記述が16ページもある。

これは米国内の社会基盤維持と国家安全保障がますます密接に関わっていることを物語るのみならず、自由で開かれた価値観や民主主義政治、そして国際法や国際協調という世界のソフトインフラがそうした価値観を共有しない国や組織による攻撃にさらされるリスクを国家安全保障として強く意識している表れと言える。

自由・民主主義陣営の基盤強化のために、中低所得国向けのPartnership for Global Infrastructure and Investment（PGII）のような国際協調の枠組みも本戦略の中に位置づけている。バイデン大統領は今年のG7広島サミットでPGIIの拡充を強調（別紙３）。

**１０．バイデン大統領の議会宛書簡 ソース：ホワイトハウス**

2022年11月7日付の重要インフラ防護に関する議会向け書簡において、バイデン大統領は、インフラのデジタル化や自動化の進展、敵対国によるインフラ攻撃の脅威そして　気候変動による脅威を加味し、大統領指令21を見直し、改定する手続きを開始すると告げた。

重要インフラの中でも特にシステミックに大切なものを指定する。

また、各担当官庁とCISAの役割や責任を再定義し、一丸となって重要インフラの防護にあたらせる。

この書簡の問題意識として重要インフラに関する最低限必要なサイバーセキュリティを実現するための包括的な方法が欠けているとの認識がある。この点で議会と連携しトップダウンの方法を検討していく。

**１１．重要インフラに関するバイデン政権のサイバープランバイデン**

**ソース：　CSIS**

　バイデン政権による重要インフラのサイバーセキュリティの必要最小限の要求は別紙１の図のとおり。

コロニアルパイプライン事件の後TSAが最初に行ったことがインシデントレポートを上げることを重要インフラ関係者に義務付けたこと。

これを同時にCISAまで上げて一元管理し、重要インフラを管轄する省庁全体で共有することにした。

パイプライン業界はもとより鉄道、アビエーションへ同じメカニズムを順に条件づけた。

企業には7-24でコンタクトが取れるサイバーインシデント対応窓口の設置を条件付けた。

この命令はDHSやCISAが定義する重要インフラ関連企業に限定し、SMEに負荷はかけない。

この指令（directive）から1年で業界とやりとり（業界からも不満やカウンターオファーあり）を行い、インシデント報告会議を通じペーパーワークを抑える努力をした。

結果として特定の行動を指示するのではなく、望まれる４つの結果を提示する形をとった。

1つ目はネットワークセグメンテーションのあるべき姿（自社のネットワークとインフラのOT（Operational Technology）のセグメンテーションとを離すこと）。

２つ目が企業の重要なサイバーシステムのアクセスコントロール。

３つ目が継続的探索とモニタリング。

４つ目が専らパイプライン業界向け。

備えとして、企業のトップと業界に関連する全省庁を巻き込んだ図上演習を実施する。

TSAがパイプライン業界でのサイバーセキュリティの枠組みのパターンを鉄道会社に、次いでエアラインと空港業者に広げた。

ホワイトハウスとの連携においては、重要インフラ関連企業のトップをホワイトハウスに招き、具体的な脅威についてのブリーフィングを実施、サイバー技術のことは知らないCEOでも、アタックの狙いや手口などの知識を持ってもらい、いざ有事において自社のCIOとのやりとりがスムーズに進むようにする。

従来から金融インフラや核設備などではその防護に関する強制のルールがあったが、　重要インフラ全体に適用する共通の必要最小限の防護規制を必要としている。例えばCISAによるインシデント報告義務のルール化。

ただ、企業にとって負担であることも理解している。官民で共通のあるべき姿を共有しつつ、それを実現する手法は各企業の裁量にゆだね、結果を縛る方法。規制対象もトップリスクのある企業層で、中小零細は除かれる。

　リスクの判断は企業規模だけでなく、担当する内容にもよる。例えば鉄道のリスクは実はラスト１マイルに重要性があり、そこを担う企業はリスクを認識して欲しい。

　エアラインであれば貨物の種類によってリスクは変わってくる。例えば、軍民共用の物資輸送など。

　州政府は同じサイバーアタックでも専ら個人情報保護などを管轄し、重要インフラの状況把握、保護、救済・復旧は専ら連邦政府の役割となる。

**１２．National Cybersecurity Strategy ソース：ホワイトハウス**

本年3月１日に発表。ポイントは下記の通り。

**①　サイバースペース防衛**

サイバーセキュリティの責任負荷を一元化。

**②　将来投資**

短期の脅威に対応しつつも中長期のレジリエンス対応の投資を促す補助金・助成金

国家安全保障と公共の安全、経済繁栄のために国力を適切に用いる。

**＜ビジョン＞**

* 本戦略を実行することで重要インフラやクリーンエネルギー分野、技術・製造基盤の米国への呼び戻しへの投資を守る。同盟国やパートナー国とともに、以下のようなデジタルエコシステムを設ける。
* サイバー防衛が圧倒的に容易で安く効果的に行える

仮にインシデントやエラーが生じても本業の継続性は保たれるレジリエンス

* 価値創造がデジタル世界を通じ進み、補強される。

バイデン政権は国家安全保障戦略や大統領令第14028号（国のサイバーセキュリティの改善）、国家安全保障覚書第5号（重要インフラのコントロールシステムのためのサイバーセキュリティの改善）、M-22-09 (連邦政府をゼロトラストのサイバーセキュリティ原則に移行させる)、国家安全保障覚書第10号（脆弱性の高い暗号化システムのリスクを抑えつつ量子コンピュータで米国のリーダーシップを促進する）といったイニシアティブを取っており、本戦略はそれらの努力を発展させるためのものではあるが、サイバー空間はあくまでも我が国の高い理想を実現するためのツールであって、その存在自体が目的となることはない。

**＜アプローチ＞**

**①　重要インフラの防護**

* 必要最小減のサイバーセキュリティの要求を重要インフラに適用しつつ、関連規制を調和させることでコンプライアンス順守のための負担を減らす。
* 重要インフラと重要サービスの防護に必要なスピードと規模で官民連携を可能にする。
* 連邦政府のネットワークを防護し、近代化し、インシデントに対する対応方針をアップデートする。

**②　サイバー空間で脅威となる悪者組織の能力を粉砕する。**

* 民間と連携し、粉砕活動を一気に拡張できるようにする。
* 連邦政府全体を通じた包括的なアプローチと海外のパートナー諸国との共同歩調をとってランサムウェアの脅威に対処する。

**③　市場原理を用いて安全とレジリエンスを推進する。**

* 個人情報のプライバシーと安全の促進
* ソフトウェア製品やサービスの開発者に安全担保責任を求める。
* 連邦政府の助成金を安全でレジエントなインフラへの投資にシフト。

**④　レジリエントな将来への投資：安全でレジリエントな次世代技術とインフラの技術革新において世界をリードし続けるための投資と協働**

* インターネットの基盤やデジタルエコシステム上のシステミックな技術的脆弱性を減らしつつ国境を越えてくるデジタル脅威へのレジリエンスを高める。
* ポスト量子暗号化、デジタル認証、クリーンエネルギーインフラなどの次世代技術のためのサイバーセキュリティ研究開発投資を優先する。
* 多様で剛健なサイバー関連従事者を育成する。

**⑤　国際連携を強化し共通のゴールを目指す。**

* 同じ考えを持つ国々と国際連携を交わし、共同の準備と対応並びに負荷を攻撃相手に与えることで脅威に対抗する。
* 平時はもとより、危機の際にも連携国がサイバー脅威から自国を守るための支援を行う。
* 同盟国や連携国と協働で情報通信技術並びにインフラ運用技術製品及びサービスに関する安全で信頼性の高いサプライチェーンを築く。

National Cyber Directorの調整により、本戦略の実行化が進められている。

**１３．National Cybersecurity Strategyの意図**

**ソース：Davis Wright Tremaine LLP**

重要インフラ関連業界に対する新たなサイバーセキュリティの要求を提示するもの。

2021年のコロニアルパイプラインへのサイバーアタックのあと、TSAは自らに与えられている権限の下、パイプライン業界のサイバーセキュリティに関する指令を初めて発出、次に鉄道、そしてそれ以外の陸上輸送関連業界に同様の指令を発出している。

同様に省庁ごとのサイバーセキュリティのルールが特定の業界に適用されるが、これをパッチワーク状況から連邦政府全体の調和のとれたルール作りにもっていく意図。

**①　CISAルール**

2022年の重要インフラに関するサイバーインシデント報告義務を定めた法律に基づき重要インフラのサイバーセキュリティを図るべきとの大まかなコンセンサスはある。

CISAはそのルール作りを行っている。

そのルールはNISTのサイバーセキュリティフレームワークか、CISA自身の横断的サイバーセキュリティパフォーマンスゴールあるいはほかのフレームワークや条件を採用するかもしれない。ただ、業界横断的に強制力を持ったルールを作る場合は議会の新たな法制が　必要となる。

**②　政府調達**

NCSは政府調達を通じサイバーセキュリティのスタンダード向上を促すことを求めているが、バイデン大統領は2021年5月に出した大統領令14028で連邦調達規則（Federal Acquisition Regulation）を改訂し、サイバーセキュリティの要求を標準化し、契約企業にサイバーインシデントの報告義務を課している。

NCSでは連邦政府横断で共通のサイバーセキュリティ契約条件を標準化する。

**③　Know Your Customer (KYC) for Infrastructure-as-a-Service**

サイバー犯罪者がクラウドのインフラを悪用してサイバーアタックを仕掛ける手口が見られることから、トランプ前大統領は2021年1月に出したKYC for IaaSを求める大統領令出している。　NCSではこの大統領令の実行を求めるべく、商務長官に対し、IaaSプロバイダーに海外ユーザーの身元確認や送金元、その他詳細を情報収集することを求めた。

**④　IoTセキュリティラベリングプログラム**

前出の大統領令14028ではNISTとFTCがIoTの安全確保のための消費者向けラベリングプログラムを策定する準備を求めているが、今回のNCSはその実行を求めている。

エネルギー消費効率に関するEnergy Starのラベリングと同様、消費者にIoT製品が特定のサイバーセキュリティ安全基準を満たしているかラベルで示す。

**１４．同盟国による重要インフラ防衛を巡る米国の期待値　ソース：ウィルソンセンター**

インド太平洋地域における駐留米軍を支える日本、韓国及びフィリピンといったホストネーションの重要インフラの防衛が重要との認識。

核の傘ならぬデジタルの傘の発想で臨むべき。

インシデント対応の支援や脅威情報の共有など運用上のサイバーセキュリティ関与を図るべき。

通信ネットワークから信頼できないベンダー製品を排除することやOpen RANの移動無線通信基準の採用を通じたベンダーの多角化の啓もうを行うべき。

国際反ランサムウェアイニシアティブの立ち上げとそれに伴うキャパシティビルディングを36の同盟国とともに行うべきである。

米国としては同盟国の重要インフラに関し以下のアクションを取るべき。

**①　同盟国の重要インフラのリスクを理解する**

**②　PGII投資においてサイバーセキュリティの必要性を強調する**

**③　民間部門の力を活用する**

ロシアのウクライナ侵攻に際し、民間企業がウクライナ政府にサイバーセキュリティの支援を効果的に行った。インド太平洋地域においても地域の民間企業の力を活用し、地域の重要インフラの所有者や運用者と信頼のおけるサイバーセキュリティ企業との間のパートナーシップの構築を進めておくべき。

**④　インド太平洋地域を最重視する**

中国抑止が米国の安全保障戦略の要であり、中国がインド太平洋地域で国際秩序を破るような振る舞いを抑止するべく地域の同盟国を支援すべき。同盟国の通信インフラ内にファーウェイ製品が入り込まないよう提言するとともに、この地域の同盟国のサイバーセキュリティのキャパシティビルディングを優先的に支援すべき。

以上の活動にコストはかかるが、台湾侵攻など、中国が秩序を破る行動を行った場合の対抗コストに比べればはるかに低く済む。　抑止が最も効果的な防御である。

**【考察】**

　米国において社会インフラは普通に機能していて当然という市民の認識で、その機能の停止といっても、たまに大雪やハリケーンが停電や断水を生じたり、公共輸送や空港閉鎖をもたらしたりといった程度の障害であった。　それが、9-11による対テロ防護の必要性やミネソタ州の橋の崩落に象徴されるインフラの老朽化に対するインフラ再整備のニーズが高まった。

さらに年々規模を拡大させているハリケーンや竜巻、山火事などの自然災害が重要インフラにもたらす被害規模も増大している。

インフラ整備は従来内政のテーマであったが、インフラに対するサイバーアタックは海外のものであり、外交、軍事、安全保障のマターとなり、超党派の政策となっている。

従来の軍事侵攻や砲火の応酬は国境を境として互いの軍事施設などを攻撃するものであったものが、軍事侵攻の前に相手国の電力インフラや通信・情報インフラ等にサイバーアタックをかけて相手国の社会の安定に動揺を与えてから軍事侵攻に入ることが想定されている。

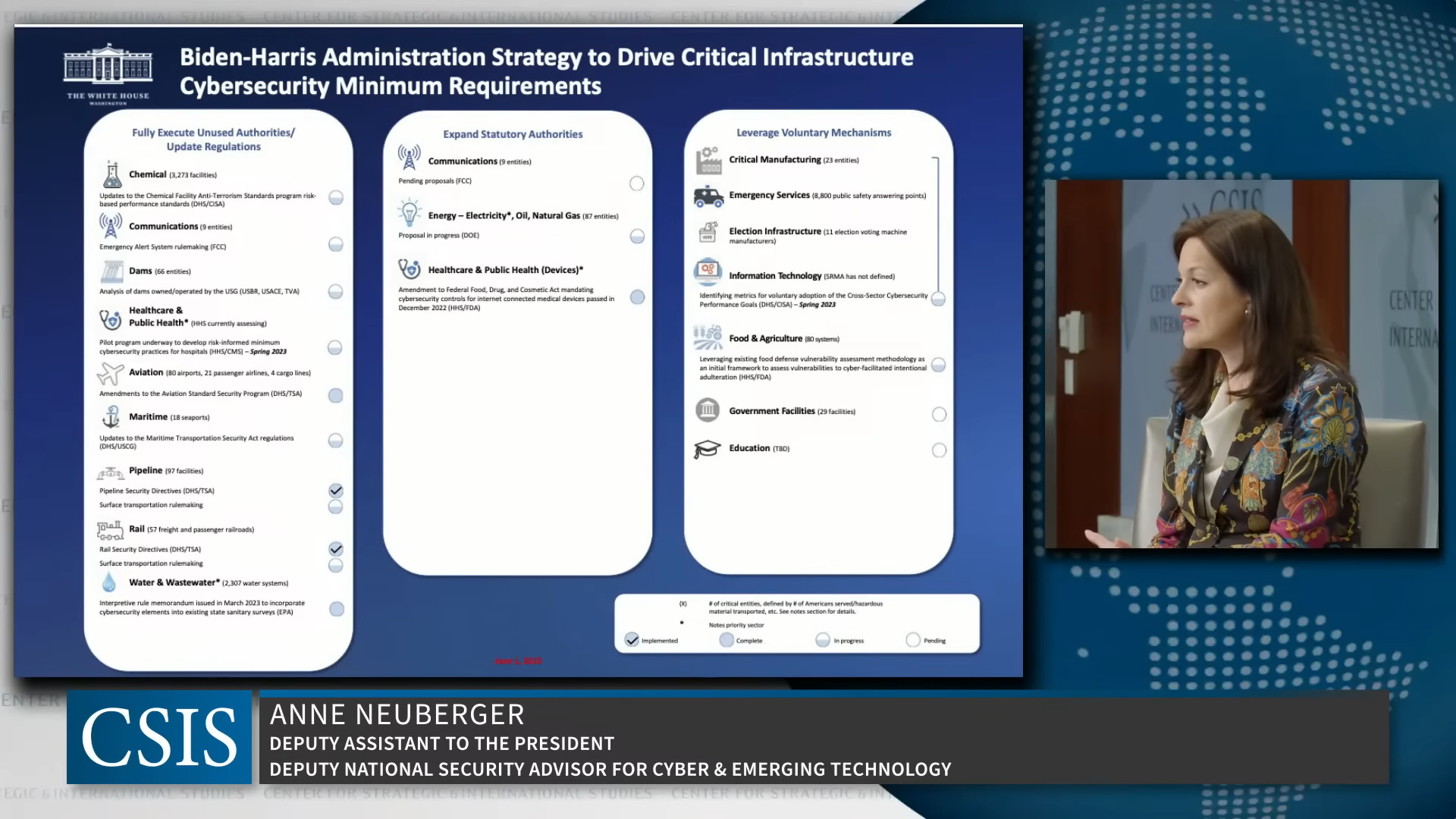
さらにはSNS等を通じた誤情報の拡散などで相手国の政治体制や選挙活動に影響を及ぼす「攻撃」も、メディアおよび情報ネットワークというソフトインフラへの悪影響を与え、自国の政治的影響力を増す目的がある。

従来、国家安全保障において官と民、軍と民間で守るべきものや役割が明確に分かれていたものが、想定脅威のシナリオの変化により、そうした脅威の情報を官民で共有しつつ様々なケースに備える必要性が高まっており、これはそのまま同盟国や友好国との間の陣営化につながりつつある（別紙４および５）と言えよう。

以上

**別紙１　サイバーアタックに対する重要インフラ防護のミニマム要件定義**

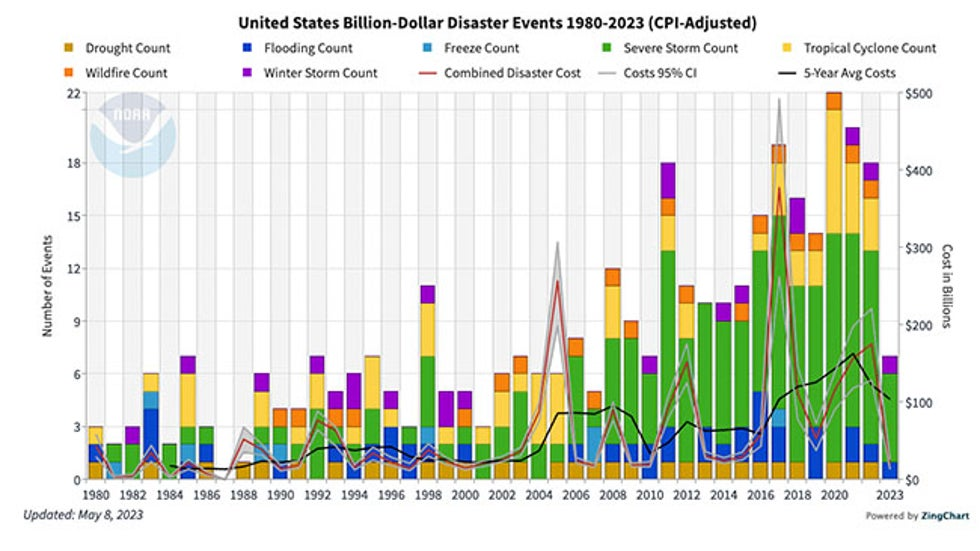
**ソース：CSIS**



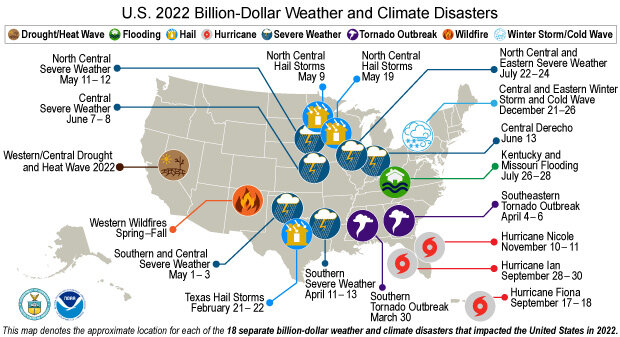
**別紙２　インフラ法で想定した気象災害**

* 2021年には、それぞれ10億ドルを超える損失を伴う20件の気象災害が米国に影響を及ぼし、合計688人が死亡した。
* インフレ調整後、1980 年から 2021 年までのこれらのイベントの平均数は 7.4 回ですが、2017 年から 2021 年までの最近 5 年間の平均は年間 17.2 回であり、頻度は大幅に増加している。
* 710億ドル相当の気候対応プログラムが実施される予定。
* 170億ドルかけて、陸軍技術者による国内洪水緩和と水路システム構築がなされる。
* 80億ドルをかけて西部の水の貯蔵、リサイクル、生態系の修復を行い、カリフォルニアなどの砂漠州やその他の州の干ばつ対策に役立てる。
* 53 億ドルの山火事の消火活動と補償。
* 洪水と山火事の正確なマッピング、モデリング、予測に 5 億 4,000 万ドル。
* 海面上昇、竜巻、内陸洪水、地滑り、地震などの自然災害からコミュニティと資産を守るための 35 億ドルの競争的助成プログラム。
* 35 億ドルの耐候化支援プログラム - 低所得世帯が家庭のエネルギー効率を改善できるよう支援。低所得世帯のエネルギー支出を節約し、CO2排出量を削減する。

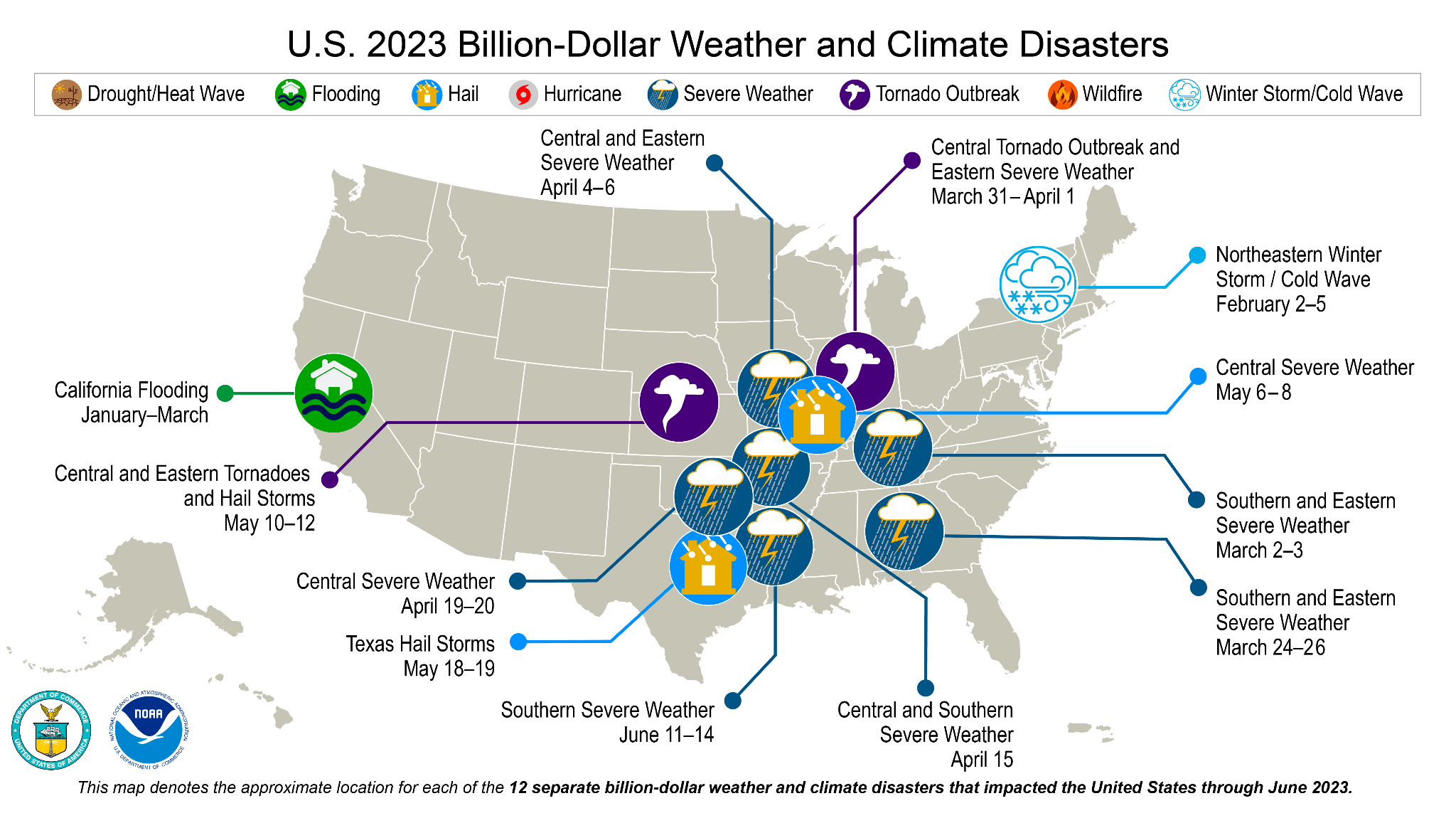
米国の災害別損失額推移図



米国の2022年の気象・気候関連災害発生時期と場所



米国の2023年の気象・気候関連災害発生時期と場所



**別紙３ 今年5月論考（G7サミット）より**

**Partnership for Global Infrastructure and Investment（PGII）を通じた連携強化**

**ソース：　ホワイトハウス**

　G7サミットにおいて低所得・中所得国向けPGIIの強化・拡大が図られた。

今回のサミットを通じ、米国は新たに一連のPGIIを通じて経済回廊を創り出していくことを発表した。政府関係者はもとより世銀そしてCitiやGlobal Infrastructureといった民間企業の代表も参加し、PGIIへのコミットを発表している。

エネルギーと投資担当大統領補佐官として着任するAmos Hochstein氏が米国の今後のPGII投資の旗振り役兼G7調整窓口となる。また、連邦政府としては今後年次Investor Forumを立上げ投資家とPGIIのニーズを有する諸国との橋渡しを行う。

輸送インフラやクリーンエネルギー、情報通信ネットワーク、食料ハブ、ヘルスケアといった社会基盤構築への貢献を通じ主要な経済回廊構築を支える。

例としてコンゴとザンビアをアンゴラ経由繋ぐLobito回廊の構築がある。他にもガーナやケニア、タンザニア、シエラレオネ、ガンビア等への具体的なインフラ支援プロジェクトを進めている。

また小型モジュール原子炉ではインドネシアやルーマニアへの支援プロジェクトが進んでいる。コスタリカやエクアドルといった中南米諸国やブラジル、インドへの民間インフラ投資の支援も公表された。

**バイデン大統領記者会見**

PGIIインフラコミット（米として$30B以上、G7で2027年までに$600B超）

**別紙４　サイバー空間の国際的なルールに関する議論への対応**

**ソース：総務省**

ア　サイバー空間の国際ルールづくり

総務省では、サイバー空間の国際的なルールづくりに関し、①民主主義を支えるだけでなく、イノベーションの源泉として経済成長のエンジンとなる情報の自由な流通に最大限配慮すること、②サイバーセキュリティを十分に確保するためには、実際にインターネットを利用し、ネットワークを管理している民間企業や学術界、市民社会などあらゆる関係者の参画（マルチステークホルダーの枠組）が不可欠であることの2点を重視していることを踏まえ、インターネットエコノミーに関する日米政策協力対話（日米IED）及び日EU・ICT戦略ワークショップなど二国間対話において関連の議題を取り上げ、同志国との連携を強化することに加えて、2022年（令和4年）4月には、コアメンバー国（日本、米国、豪州、カナダ、EU、英国）及び有志国において、「未来のインターネットに関する宣言」を立ち上げるなど、多国間会合における議論にも積極的に参加している。

イ　サイバーセキュリティに関する二国間・多国間対話

サイバーセキュリティに関する二国間の政府の議論については、日米間で2021年（令和3年）5月に「日米サイバー対話」課長級会議、日英間で同年6月に第6回「日英サイバー協議」、日独間で同年5月に第2回「日独サイバー協議」、日エストニア間で同年12月に第4回「日エストニアサイバー協議」が開催され、情勢認識、両国における取組、国際場裡における協力、能力構築支援などについて議論を行うなど、各国との連携強化を進めている。

サイバーセキュリティに関する多国間の議論については、日ASEANサイバーセキュリティ政策会議などにおいて、各国の取組状況やASEAN地域に対する能力構築支援の状況などに関する意見・情報交換が行われている。また、日米豪印4か国のいわゆるクアッドの取組の下で、サイバーセキュリティに関する協力について合意されており、政府一体となって同志国との連携強化に向けた議論が行われている。

**別紙５責任あるサイバー習慣を促進するための協力に関する日米豪印共同声明**

**ソース：　内閣サイバーセキュリティセンター**

我々、オーストラリア、インド、日本及び米国の日米豪印パートナーは、我々の国全体のサイバーセキュリティを改善するための啓発キャンペーンを開始する。

我々は、インド太平洋及びそれ以外の地域のインターネットユーザーに対し、本チャレンジ（https://www.cyberchallenge.tech/）に参加し、安全で責任あるサイバー習慣を実践するよう呼びかけている。

本チャレンジは、個人及びコミュニティのサイバーセキュリティに対する意識及び行動を強化し、また、経済及び全てのユーザーに利益をもたらす、より安全で強靱なサイバー・エコシステムを育成するための日米豪印の継続的な取組を反映している。

世界中のインターネットユーザーは、毎年数兆ドルを失わせ、また、高い機微性のある個人データを窃取し得る、サイバー犯罪及びその他の悪意あるサイバー脅威の標的となっている。

多くのサイバー攻撃は簡単な防止措置で防ぐことができる。

インターネットユーザー及びプロバイダーは共に、わずかな行動をとることで、サイバーセキュリティ及びサイバーの安全性を大幅に改善することができる。

これらの行動には、日常的にセキュリティ更新プログラムをインストールすること、多要素認証を活用して強力なIDチェックを可能とすること、より強力なパスワードを使用し、また、日常的に変更すること、フィッシングのような一般的なオンライン詐欺の見破り方を知ることなどが含まれる。

本チャレンジは、企業、教育機関、中小企業及び小学生から高齢者までの個人など全てのユーザーに対し、基本的なサイバーセキュリティに関する情報及び訓練の機会を提供し、4月10日の週のイベントでクライマックスを迎えることとなる。

日米豪印パートナーは、オンラインでスマート機器を使用する全ての人々が決定するために必要とされる十分な情報へのアクセスを有することを確保するために取り組んでいる。

我々が一丸となってサイバーの脅威からより守られるよう、より安全で、強靱なサイバー空間を促進するためにあなたやあなたの組織に何ができるかを学習して欲しい。

1. The Cybersecurity and Infrastructure Security Agency Act of 2018 [↑](#footnote-ref-1)
2. Federal Risk and Authorization Management Program [↑](#footnote-ref-2)