

米国バイデン政権のサイバーセキュリティ政策と 我が国の政策への示唆

三 角 育 生*

Cybersecurity-related Policies Adopted by the Biden Administration and
Lessons Learned that Japan Can Apply in Its Own Cybersecurity Policies

Ikuo MISUMI

Abstract

This paper examines features of cybersecurity-related policies adopted by the Biden administration and analyzes them using the cybersecurity policy analysis framework (which considers strategic/incident response, technical/non-technical, and the level of risks to the human rights). Features revealed through the analysis include a comprehensive policy package approach, a cooperative approach, and a safety-minded approach. These features are compared with those of Japan's own cybersecurity policies in order to identify what the Japanese government can learn from the Biden administration's policies.

要旨

本論文はバイデン政権が採るサイバーセキュリティ関連政策の特徴を、戦略的政策かそれとも対処的なものか、技術的な対策か非技術的なものか、人権に対するリスクのレベルなど、サイバーセキュリティ政策分析フレームワークを用いて、分析するものである。分析結果として得られたバイデン政権下のサイバーセキュリティ政策の特徴は、包括的な政策パッケージ化、関係組織の連携重視、安全第一のアプローチなどである。こうした特徴を日本のサイバーセキュリティ政策の特徴と比較して、日本政府への有効な示唆を明らかにしている。

キーワード：バイデン政権、サイバーセキュリティ、インシデントレスポンス、政策分析

* 東海大学情報通信学部 (Tokai University)

1. はじめに

米国バイデン政権が2021年1月20日に始動して半年程たった。同政権においてサイバーセキュリティは優先事項の一つである¹⁾。これまで、同政権としてサイバーセキュリティ政策に係る戦略的な方針の表明が複数なされてきた。また、顕著なサイバーセキュリティ事件について悪意ある行動の実行者の帰責を明らかにしつつ対処する政策も複数実施されている。これらの米国のサイバーセキュリティ政策の動向把握は、同国の情報通信技術(IT)産業の規模が大きく、かつ、我が国の同盟国であることから我が国のサイバーセキュリティ政策にも大きく影響するため、重要である。

翻って我が国の半年間のサイバーセキュリティ政策の動向を見ると、サイバーセキュリティ戦略本部(CS本部)は、サイバーセキュリティ基本法(基本法)に基づく次期サイバーセキュリティ戦略(CS戦略)(CS本部 2021)の策定作業²⁾を進めている。また、重要インフラについても、次期CS戦略の検討内容を踏まえながら、本年度内を目途に次期重要インフラ行動計画の検討をとりまとめようとしている³⁾。また、顕著なサイバーセキュリティ事件に対する動きとして、我が国で初めて警察の書類送致に関して我が国政府が外国の国家が関与したと行為者の帰責を示した事件も登場している。

そこで、本稿は、バイデン政権のサイバーセキュリティ政策の特徴を分析し、我が国のサイバーセキュリティ政策の策定、対処等にあたっての示唆を検討することとする。

2. 分析の手法

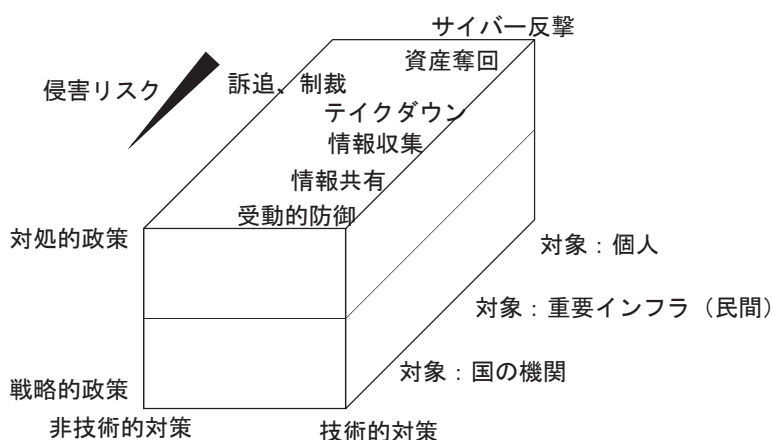
(1) 分析フレームワーク サイバーセキュリティ対策は、コンピュータウイルス対策、ネットワーク防御などの技術的対策と、法令や組織的な情報管理体制などの非技術的対策が要素にある。また、サイバーセキュリティに係る政策には、サイバー脅威のリスク軽減を主たる目的とした戦略的な方針の策定・実施(戦略的政策)と、顕著なサイバーセキュリティインシデントの影響を緩和し復旧、再発防止を図る政策(対処的政策)がある。この点は、例えば内閣官房内閣サイバーセキュリティセンターの英語名称が、National Center of Incident Readiness and Strategy for Cybersecurity (NISC) となっていることから推察できる。

戦略的政策の分析にあたっては、政策対象も重要な視点である。基本法は、国の責務、地方公共団体の責務、重要社会基盤事業者(重要インフラ)の責務、サイバー関連事業者の責務、国民の努力などと規定している。こうした対象によって、政府による義務的命

が人権侵害となるリスクの程度が異なるため、命令、契約、要請など政策の実施方法も異なることとなる。

対処的政策の分析にあたっては、対処の手段の視点も重要である。サイバー攻撃への対処には、自身のネットワークの強化といった受動的防御からサイバー反撃まで、また、これらの中間にあたる「積極的サイバー防御（active cyber defense / proactive cyber defense）」という概念もある。そして、対処には一定のスペクトラムがあるとされる。具体的には、受動的に近いプライバシー侵害等のリスクの低いものから順に、情報共有、ハニーポットなどの利用、不正プログラムの捕獲、情報収集、テイクダウン、流出資産の奪回などの技術的対策が含まれる。また、流出した資産の奪回よりはプライバシー侵害等のリスクが低いものと分類される非技術的対策である制裁・訴追・貿易救済措置があるとされる（CCHS 2016: 9-12）。

図表1 サイバーセキュリティ政策分析フレームワーク



（出典：筆者作成）

そこで本稿では、これらの整理を軸とするサイバーセキュリティ政策分析フレームワーク（図表1）を考え、この整理を適用して日米の政策比較をする。

（2）データの収集 ITやデータ等が広く活用されている今日、サイバーセキュリティ政策、対策は様々な分野、形で立案、実施される。そこで、バイデン政権のサイバーセキュリティ政策をどの様に捕捉するかが論点になる。メディアとの対立構造が散見された前政権とは異なり、バイデン政権では Briefing Room（BR）における大統領報道官等の説

明、政策公表などが丁寧に行われているように見える。そこで、BR⁴⁾に掲載された情報をデータとして用いることとする。具体的には、政権発足から約半年を経た2021年7月末までにBRにおいて、大統領令（EO）その他の政策であってサイバーセキュリティに関連づけられていると考えられる戦略的政策及び対処的政策を抽出し図表2にまとめた。この作業にあたり、二国間首脳会合においてサイバーセキュリティに言及しているものや、単に報道官が記者からサイバーセキュリティ関連の質問があつてそれに応えているものなどは含めていない。

図表2 バイデン政権のサイバーセキュリティ関連政策

日付	政策名	概要
2021/7/28	National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems	連邦政府と重要インフラコミュニティが協働して重要システムのサイバーセキュリティを大幅に改善する任意の産業制御システム・セキュリティ・イニシアティブ。
2021/7/19	The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the PRC	英、NATO 等の同盟国とともに、中国が犯罪契約をしたハッカーを用いてサイバー攻撃をしたことを暴露し批判。 PRC: Peoples' Republic of China
2021/7/3	Direction to investigate Kaseya incident	Kaseya に対するランサムウェア攻撃の影響調査指示。
2021/6/13	CARBIS BAY G7 SUMMIT COMMUNIQUÉ	ロシアに対し、国内でランサムウェア攻撃等のサイバー犯罪を行う者を特定し、その活動を遮断し、責任を要求。
2021/6/9	Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries	米国の個人の機微なデータを無制限なアクセス等によって害されること及び中国等の外国の敵対者等から大規模データリボトリが害されることより保護するための措置検討指示。(EO14034)
2021/6/3	Executive Order on Addressing the Threat from Securities Investments that Finance Certain Companies of the PRC	中国の軍事産業複合体、監視技術の開発・使用等の脅威の高まりを受け、本指令に記載する者（Huawei 等）等に対する投資等の禁止。(EO14032)
2021/5/12	Executive Order on Improving the Nation's Cybersecurity	連邦政府ネットワークの強化等の各種サイバーセキュリティ対策レビューの指示。(EO14028)
2021/5/11	All-of-Government Effort to Address Colonial Pipeline Incident	ランサムウェア攻撃の影響で、5月7日に停止したコロナル・パイプラインによる石油製品供給途絶に対する輸送に係る規制の緩和措置やランサムウェア対策に係る政策パッケージ。
2021/4/20	100-day plan to improve the cybersecurity of the nation's electric infrastructure	重要インフラ防護のサイバーセキュリティイニシアティブにおいて電力部門をパイロットプロジェクトとするもの。

日付	政策名	概要
2021/4/19	Statement by Deputy National Security Advisor on SolarWinds and Microsoft Exchange Incidents	バイデン政権は、SolarWinds および Microsoft Exchange 事件に対する政府全体の対応を推進するために、2つの統一調整グループ（UCG）を招集。
2021/4/15	Executive Order on Blocking Property with Respect to Specified Harmful Foreign Activities of the GoR	米国等の自由・公正な選挙への有害活動、悪意あるサイバーによる活動（Solarwinds 事件）など特定の有害な活動に従事したロシアの者への資産等の移転等の禁止。（EO14024） GoR: Government of Russian Federation
2021/3/31	The American Jobs Plan	半導体、高速通信網ネットワークセキュリティ対策等を含む。
2021/3/17	Microsoft Exchange Vulnerabilities UCG	国家安全保障会議がタスクフォース Unified Coordination Group（UCG）を設置。
2021/2/24	Executive Order on America's Supply Chains	経済的繁栄・国家安全保障確保のために半導体製造等の安全なサプライチェーンを強化指示。（EO14017）
2021/2/19	Statement by Deputy National Security Advisor on SolarWinds incident	Solarwinds 事件による侵害状況の説明。
2021/1/20	Executive Order on Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis	本 EO には、EO13920（注：電力網設備の中国からの調達禁止）を停止し、90日以内に代替措置の検討の指令を含む。（EO13990）

注：網掛けは、個別事件への対処的政策

出典：https://www.whitehouse.gov/briefing-room/ の内容をもとに筆者作成

3. バイデン政権のサイバーセキュリティに係る戦略的政策の分析

バイデン政権の戦略的政策としては、①米国のサイバーセキュリティの向上に関する大統領令（EO14028、2021年5月12日）⁵⁾、②敵対的外国勢力からの米国機微データの保護に係る大統領令（EO14034、2021年6月9日）⁶⁾、③重要インフラ制御システムのサイバーセキュリティ強化に関する安全保障メモランダム（NSM、2021年7月28日）⁷⁾といった大統領の指令がある。また、重要インフラ関連で電力インフラのサイバーセキュリティ強化100日計画⁸⁾、さらに、安全保障にも関わる経済政策として米国のサプライチェーン強化、中国軍事関連産業等への投資等の禁止などの政策がある。

（1）EO14028 後述する SolarWinds（SW）事件、Microsoft Exchange（MSEx）事件、Colonial Pipeline（CP）事件などを受けて、国の機関を主たる政策対象として、連邦政府ネットワークを強化し、官民連携を通じて国のサイバーセキュリティ強化を図ることを目

指したもの。課題のレビューを連携して行うよう、連邦政府の関係省庁長官に命令している⁹⁾。具体的には、技術的対策として、①ゼロトラストアーキテクチャ¹⁰⁾の導入など連邦政府のサイバーセキュリティ基準の強化・近代化、② Software Bill of Material (SBOM)¹¹⁾によるソフトウェアコンポーネントの起源の確からしさ確認などソフトウェア・サプライチェーンの改善、③脆弱性・サイバー事象への対応に係る標準化された対応手順の策定、④ Endpoint Detection and Response (EDR) などによる連邦政府ネットワークにおけるサイバーセキュリティ事象検知の向上、⑤連邦情報システムの適切なログ保全等による捜査と修復能力の向上などである。また、非技術的対策としては、⑥ IT／制御システム運用技術 (OT) に係る民間サービス事業者から省庁がサービスを調達するときの契約で当該民間事業者が把握した脅威情報等を他者と共有することを禁止等しているため、省庁間で円滑に脅威情報を共有できないという課題を解決するべく契約文書などの見直し、⑦ 政府や民間で生じる重大サイバー事象¹²⁾ についてのサイバー安全審査委員会 (CSRB : Cyber Safety Review Board) の設置などからなる政策パッケージである。

(a) 技術的対策の分析 米国の採るゼロトラスト、EDR 等の活用といった近代化の方向性は現在のサイバーセキュリティ技術対策としてはトレンドに沿ったものである。標的型攻撃などのサイバー攻撃があったときには侵入後に攻撃がシステム内を水平展開することへの対応が必要であり、我が国でも、日本年金機構の不正アクセスによる情報流出事件などを踏まえ、政府はゼロトラストアーキテクチャの導入の検討 (三角2020b : 26)、EDR の導入も進める (三角2021 : 43) こととしている。また、SBOM について、米国では従来からサプライチェーン問題への対策として医療機器、自動車等を対象に検討が行われている (NTIA 2019 : 23) が、我が国でも同様にサプライチェーン対策として検討が開始されている¹³⁾。

(b) 非技術的対策の分析 情報共有の仕組みについて、本 EO の例では連邦内の情報共有円滑化などの観点から民間との契約見直しに焦点を置く。一方、我が国では、基本法を改正して官民・民間同士での積極的・自発的な情報共有にあたっての障害を軽減する取組みを行った¹⁴⁾。今後、我が国政府内での情報円滑化の観点から、政府調達契約の内容のレビュー実施も有益であると考えられる。

米国の体制整備について特徴的と考えられる点は、CSRB の設置である。重大サイバー事象が発生したときに、航空機事故を扱う国家運輸安全委員会のように、対応を評価・分析し、今後の改善策を勧告するものである¹⁵⁾。CSRB の名称に「安全 (safety)」を使っており、安全の観点から、今後どの様な活動をしていくかが注目される。一方、我が国で

は、CS 本部、NISC が、基本法に基づき重大な事象について機密性、完全性、可用性といった情報セキュリティの観点から調査する体制となっている。

(2) NSM 重要インフラが政策対象となるもので、連邦政府と重要インフラコミュニティが協働して重要システムのサイバーセキュリティを大幅に改善する任意のイニシアティブである。

(a) 技術的対策の分析 制御システムを監視し悪意ある活動の検知などする技術・システムを展開する。また、国土安全保障省（DHS）等に重要インフラ分野を横断的に、事業者が実践すべきセキュリティ・ベースラインの共通理解醸成の目標を定めるべき旨指示している。

本イニシアティブで言及されている電力分野での先行的取組である100日計画¹⁶⁾（2021年4月20日公表）は、サイバーセキュリティ強化のために検知・緩和・フォレンジック能力の強化を促す技術的対策である。本計画策定の経緯は、トランプ政権が、EO13920¹⁷⁾（2020年5月1日）を発出し、電力分野における相互接続する送電網の制御システムなどを敵対する国家（中国を念頭）が関与する者からの調達などを禁止するといった非技術的対策を2021年1月16日に施行¹⁸⁾した。しかし、バイデン政権に移行し、EO13990（2021年1月20日）により、EO13920を90日間停止して代替措置の検討を指示、本100日計画は、その代替措置にあたる。我が国では、従来からCS本部が、事業者等からなる専門委員会の審議を経て分野横断的に、情報セキュリティ確保に係る安全基準等策定指針¹⁹⁾を策定してきている。個別分野では、例えば、電力分野の事業者も参加する経済産業省のワーキンググループが、サイバーセキュリティ対策ガイドラインなどの検討・策定を行っている²⁰⁾。

(b) 非技術的対策の分析 米国の重要インフラは分野毎に適用される法令がまちまちでパッチワークの政策に寄らざるを得ない。そのため、NSMのイニシアティブを分野横断的な取組みの第一歩として、関係者が協働する体制で実施する²¹⁾。

また、電力分野の100日計画及びEO13990に関連し、エネルギー省（DOE）は、外国からの脅威に対するサプライチェーン対策を図るべく、電力インフラの様々な側面に関する情報の提供を、電気事業者等に対して求めている²²⁾。NSM関連の施策は、トランプ政権の様な一方的に禁止措置を採るのではなく、事業者との対話や事業者への技術提供等を行う姿勢を包括的に採り、事業者との協力関係を円滑に形成しようとする点に特徴が見える。

我が国も、米国と同様に、重要インフラの分野毎の法令等によるパッチワーク行政である。例えば、電力分野では、電気事業法下の技術基準と保安規定にサイバーセキュリティの取組みを規定している²³⁾。情報共有・連携の体制については、分野毎の事業法等に基づくインシデントの報告においてサイバーセキュリティ事象が含まれているときに、重要インフラのサービスの安定的・適切な提供に著しい支障を及ぼす事象等であって重要なものなどであれば、所管省庁は基本法に基づき CS 本部に報告しなければならない²⁴⁾。また、被害を受けた事業者が円滑な情報共有をできる環境整備を目指した基本法に基づくサイバーセキュリティ協議会の設置（三角2020a：32）、重要インフラの情報セキュリティ対策に係る行動計画²⁵⁾に基づく事業者間などでの情報共有体制の強化などの政策が推進されている。

CS 本部のとりまとめの下、分野毎の対策推進をしてきている我が国は、バイデン政権と似た状況にある。我が国の事業者の特性²⁶⁾を踏まえつつ、引き続き、所管省庁、事業者等の関係者との協働による対策の推進が求められよう。

(3) EO14034 国民を政策対象としたものとして、米国民のパーソナルデータなど機微なデータを敵対的な外国の勢力から守るものである。これはトランプ政権時代の特定のサービスを禁止する EO13942、EO13943²⁷⁾（TikTok、WeChat の禁止措置等）を撤回し、同じくトランプ政権時代の IT とサービスのサプライチェーンの確保を指示した EO13873²⁸⁾を強化する包括的な対策検討を商務長官らに指示したもの²⁹⁾である。米国の経済的繁栄、国家安全保障を確保するべく採られた米国のサプライチェーン強化政策（EO14017）³⁰⁾などにおいても経済政策、産業政策的な観点からサイバーセキュリティの側面も含めて中国に対する警戒が強くみられ、トランプ政権におけるサイバーセキュリティ政策を、非技術的な立法措置を含む現実的なソリューションを追求するかたちで、継承していると考えられる。

我が国では、2019年から、政府機関等が保有する個人に係る情報の保護の観点も含め、政府調達において非技術的対策のサプライチェーン対策を実施している。具体的には、政府調達において、国・企業名を特定する形ではなく（企業名を特定して禁止しても、迂回、組織変更等の偽装をされた場合に対応できないなどの理由によると考える。）、懸念が払しょくされない機器、サービス等の調達を控える³¹⁾運用が申し合わされている。

(4) 小括り バイデン政権の戦略的政策は、前政権に比して、ホワイトハウス主導の下で連邦政府機関間の連携がみられ、政策パッケージなど包括的で分野横断的なものとなっている。そして、民間事業者とも協調的であるなど政策対象とのバランスのある実施手

段をもって取組むといった特徴がみられた。我が国の政策と比較しても技術的・非技術的対策の内容・方向性は同傾向にある。なお、「安全」について「情報セキュリティ」に追加的なかたちで政策をとる可能性もみられるので、今後の動向を注視していくのが適当と考える。

4. バイデン政権における対処的政策の分析

バイデン政権において対処的政策の対象となっている事件には、① SolarWinds (SW) 事件、② Microsoft Exchange (MSEx) 事件、③ Colonial Pipeline (CP) 事件などを挙げられる。

(1) SW 事件の概要と米国の対処 本事件は、SW 社が提供する Orion という IT 管理を効率的に実施するソフトウェアに関し、何らかの方法によって攻撃者が脆弱性を仕込んだアップデートソフトを2020年3月から6月の間に配給してしまい、最大18,000社の顧客がこれをインストールした可能性があるというもの³²⁾。SW 社は同社が契約するセキュリティ会社からの情報 (2020年12月13日公表)³³⁾ に基づきこの事実気づいた。本事件を受けて、DHS／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 (CISA) は、直ちに技術的対策として緊急警戒情報とそのアップデートを発行している³⁴⁾。

本件に関連して、バイデン政権は、2021年4月15日に、ロシア政府による外国への有害な活動に関する資産移転停止の EO14024³⁵⁾ を発出した。これは、米国や同盟国等に対して、自由・公正な選挙への有害な活動や悪意あるサイバーによる有害活動に責任を有する者などであって財務長官が指定した者の米国内、管理下にある全ての資産の移転等の禁止などを命じたものである。本命令を受けて、同日、バイデン政権は、ロシア政府による外国への有害な活動に対処すべく制裁を課すなどの非技術的対策を公表した³⁶⁾。具体的には、財務省は、米国金融機関に対してロシア中央銀行等が発行するルーブル債券等のプライマリーマーケットでの取引の禁止等を指示し、また、ロシア情報機関のサイバープログラムに技術的支援などをしたとしてロシアの IT 企業6社の指定などを実施した。また、SW 社 Orion プラットフォーム等の IT インフラへのサイバー攻撃による広範な課報キャンペーンの首謀者としてロシア対外情報庁 (SVR) を公式に特定した。加えて、IT サービスのサプライチェーンを悪用する SW 事件等におけるロシアの活動を受けて EO13873 に基づく更なる行動をとるべきかの検証をするとしている。さらに、同盟国等に国際法やノルムについての演習の提供も行うとしている。

技術的対策としては、4月15日に、国家安全保障局 (NSA)、CISA、司法省 (DOJ)／

連邦捜査局（FBI）は、共同で SVR が悪用するソフトウェア脆弱性対策についてのサイバーセキュリティアドバイザリーを発行³⁷⁾した。また、国防省（DOD）は、同盟国等を招いた重要インフラ等への悪意あるサイバー空間活動をシミュレートし、特定・協調して対処する演習を強化していくとした³⁸⁾。

（２）MSEx 事件の概要と米国の対処 2021年3月2日、Microsoft（MS）社は電子メールの送受信を行うためのサーバーソフトウェアである Exchange に、これまで知られていなかった脆弱性（ゼロデイ）を悪用して、中国の国家支援を受けたハッカーが多数の攻撃をしているとの情報を公表した³⁹⁾。翌日、CISA は技術的対策である緊急警戒指令を発行⁴⁰⁾し、その後もアップデートを行っている。4月19日、政府は、SW 事件及び MSEx 事件に対応する政府全体の対応を推進するため2つの統一調整グループ（UCG）を設置した⁴¹⁾。

2021年7月19日、米国は、EU、英国、NATO、我が国⁴²⁾を含む同盟国等とともに、中国国家安全部（MSS）との間で契約関係にあるハッカーがサイバー攻撃を行ってきたことを暴露し、非難する表明⁴³⁾を行った。表明の内容は、既に公表された MSS に協力する COVID-19 関連などの知的財産と機密情報の窃取を目的とした中国人ハッカー2名に対する起訴⁴⁴⁾の事案（2020年7月）にも言及しつつ、2021年7月19日に感染症研究を含む知的財産と機密情報を対象とした MSS に協力する中国人ハッカー4人を起訴⁴⁵⁾したこと、MSEx のゼロデイを悪用して世界中の数万台のコンピュータやネットワークに対してスパイ行為を行ったのが高い確度で MSS 関連の行為者に帰責できること、こうした脅威に対抗するために連邦政府のネットワークを近代化し、また重要インフラなどのサイバーセキュリティ強化に取り組むことである⁴⁶⁾。米国政府は、SW 事件の様な制裁というアプローチを今回は採っていないが、今後さらなる行動をとることを排除するものではないとの立場を示している⁴⁷⁾。

技術的対策として、2021年7月19日、CISA、NSA、FBI が協力して、中国の攻撃者が米国、同盟国のネットワークを標的とする際に用いる50以上の技術的手段等について説明するアドバイザリーを公開した⁴⁸⁾。

（３）CP 事件の概要と米国の対処 2021年5月6日（木）、DarkSide（DS）と呼ばれる犯罪者集団の一派が CP 社に対してランサムウェア攻撃を行い、同社の IT システムから約100GB のデータを窃取した⁴⁹⁾。7日早朝、CP 社では、リスクを特定したときに安全が確認できない限り停止する権限・義務を負う現場管理者が⁵⁰⁾、ランサムウェアが IT システムから OT システムに移行できないように予防措置としてパイプラインを停止したと

もに、同日夕方、政府当局にランサムウェア攻撃を受けた旨報告をした⁵¹⁾。そして同日夜、ホワイトハウスが、エネルギー省、CISA、FBI、運輸省、財務省、DOD 等からなる政府横断チームを招集、週末を通して、連邦政府、州政府等との対策会議を開催。10日には、バイデン大統領が、ロシアを拠点とする DS の犯罪だが、ロシア政府が関与している証拠はない旨発言している⁵²⁾。石油製品供給途絶の問題への対処については、10日に運輸省が燃料輸送ドライバーの業務従事時間規制を緩和⁵³⁾ し、11日には「All-of-Government Effort to Address Colonial Pipeline Incident」の包括的な初動対処策パッケージを発表した⁵⁴⁾。

具体的には、状況の把握・対応、影響が及ぶコミュニティへの燃料の継続的供給を保証すべく省庁横断の対処グループの設置、一定の基準に適合しない燃料も暫定的に使用することを認める緩和措置、(10日に運輸省が公表した) ドライバーの業務従事時間規制の緩和、暫定的な鉄道輸送支援の要請、州政府が採った良い取組み事例についての情報共有を支援、燃料輸送可能な米国内輸送船数の見積もり開始、パイプラインオペレータ資格規則の暫定的緩和、深刻な供給不足が発生するところへの優先的燃料供給の指示準備、政府・販売店などの定常的なコンタクトの実施である。

また、サイバーセキュリティの技術的対策として、初動対処策パッケージの一環で、CISA と FBI が共同して、ランサムウェアによる侵害の指標となるデータ、緩和策などを内容とするアドバイザリー⁵⁵⁾ を発行した。本アドバイザリーには、2020年9月に CISA が、MS-ISAC (Multi-State Information Sharing & Analysis Center) と共同で作成したランサムウェア防止のベストプラクティスとランサムウェア対策チェックリストを内容とするガイド⁵⁶⁾ も含まれている。

本ランサムウェア攻撃に係る身代金については、CP 社は5月7日に DS に対して支払った⁵⁷⁾ が、6月8日の米国上院国土安全保障・政府問題委員会公聴会にて、CP 社は、民間企業の経営判断として、パイプラインの重要性、国益にかんがみ支払いを決めた旨発言⁵⁸⁾ している。これに対し、連邦政府は、一般論としては、身代金の支払いは民間部門の判断であり、身代金の支払いに関し他に選択肢がないときはコストベネフィットのバランスで考えざるをえない⁵⁹⁾ が、こうした攻撃を増長することになるので身代金支払いは民間企業のためにはならず、自らを守るためにサイバーセキュリティ対策の強化が重要との立場⁶⁰⁾ を示した。

その後、本事件について強制的な動きがみられるようになる。まず、5月14日までに本事件で用いられたランサムウェア攻撃の実行に係るサイトがテイクダウンされたとの報道がある⁶¹⁾。また、6月7日、司法省は、DS に支払われた8割以上の暗号資産の押収について公表した⁶²⁾。そのプロセスは、暗号資産の公開されている台帳を調査し、身代金とし

て支払われた暗号資産の複数の移転先を追跡し、特定のアドレスに転送されたことを把握、当該特定アドレスについては FBI が秘密鍵を有しているので差押さえるというものである⁶³⁾。公開されている情報をもとに FBI が暗号資産の口座を特定するプロセスが読み取れるが、なぜ、当該口座の秘密鍵を FBI が有しているかについては明らかにされていない。

本事件を受けて、連邦政府は再発防止等の取組みを行っている。DHS/ 運輸保安庁 (TSA) は、5 月27日⁶⁴⁾、7 月19日⁶⁵⁾ の2回にわたりパイプライン事業者に対して指令を発出した。その内容は、指定された重要なパイプライン事業者は、サイバーセキュリティインシデントを認識したときには CISA に報告すること、TSA、CISA との間でインシデント発生時に常に連絡・調整できる調整者を置くこと、TSA のパイプライン・セキュリティ・ガイドラインの実施状況を確認し、サイバーリスクの評価を行い、改善策を策定することなどで、5 月28日に発効した⁶⁶⁾。その後、TSA は、CISA やパイプライン業界と調整して第二の指令を発出した。これは、指定された重要なパイプライン事業者に対し、ランサムウェア攻撃や既知の脅威から保護するための措置の実施、サイバーセキュリティのコンティンジェンシー／復旧計画を策定・実施し、サイバーセキュリティアーキテクチャ設計レビューの実施を義務付けるものである⁶⁷⁾。

また、技術的対策として、DHS、DOJ などが連携してランサムウェア対策情報などをワンストップで提供する Stop Ransomware⁶⁸⁾ サイトを2021年7月14日に立ち上げた⁶⁹⁾。

なお、米国政府は、ロシア政府がこうした犯罪者の行動を止めさせる活動をすべきとの立場⁷⁰⁾ で、バイデン大統領－プーチン大統領会談の都度、その旨提起している⁷¹⁾。また、国際会議の場である G 7においても、サミットコミュニケにて、ロシアに対し、犯罪者を特定し、その活動を遮断し、責任を問うよう要求している⁷²⁾。

(4) 米国の対処的政策の分析と我が国政策への示唆

(a) 非技術的対策 上記の事件で採られた非技術的対策は、連絡・連携体制の整備(すべての事件)、悪意ある行為実行者等を特定して公表(すべての事件)、送金禁止などの制裁(SW 事件)、起訴(MSEx 事件)、犯罪者の所在する国の政府に対する取締まり要請(CP 事件)、国際法等の演習の提供(SW 事件)といったものである。

帰責対象を公表して訴追や制裁を課す対処政策は、オバマ政権、トランプ政権でも採られた。例えば、オバマ政権時代に、ビジネス情報への不正アクセス、窃取、データ破壊を招いたサイバー攻撃が行われ、安全保障に関わる事件とされた⁷³⁾ Sony Pictures Entertainment (SPE) 事件⁷⁴⁾ (2014年11月発生) は一つの顕著な例である。2014年12月に DHS が技術的助言を提供していくことをアナウンス⁷⁵⁾ した後、2015年1月に EO13687⁷⁶⁾

により、北朝鮮が関与したものとして行政制裁を科すとして⁷⁷⁾、北朝鮮政府等の米国内の資産等の移転等を禁止する措置を採った。そして、2018年9月に、FBI、DOJの捜査の結果、本事件の不正アクセス共犯の北朝鮮のプログラマーを起訴⁷⁸⁾している。

また、トランプ政権時代である2017年5月に、世界150か国以上、数十万台のPCなどがランサムウェアの被害にあったWannacry事件では、事件が顕在化してすぐにDHSがアドバイザリーを公表⁷⁹⁾、2017年12月に北朝鮮が関与したものとして我が国や英国等とともに非難を行った⁸⁰⁾。本事件のランサムウェアを作成した北朝鮮のプログラマーはSPE事件の共犯者と同じであったが、これらの事件を併合して2018年9月に起訴した。そして2019年9月に北朝鮮に対して財務省外国資産管理局が制裁を科している⁸¹⁾。

従来政権では、ホワイトハウス等による非難、制裁、起訴などの非技術的対策、技術的対策が、それぞれのタイミングで発動されているように見られる。これに対して、バイデン政権下の顕著な事件への対処については、ホワイトハウスの下で包括的に調整された形で、ある程度タイミングも揃えて、公表している。直接当該事件に関する訴追事件などではないものであっても、なんらかの関連がみられるものは、政策パッケージの中に組み込まれている例もみられる。このように、ホワイトハウスの下で関係省庁が連携して、対処的政策のパッケージ化をすることは、政権としての強い意志を見せることができ、悪意ある行為者に対する抑止力や、関係者、国民等に対して訴求力の高い手法であると考えられる。

我が国の対処的政策のパッケージに関する状況は、例えば2015年に発生した日本年金機構事件への対処の初期方針はパッケージ的に念頭にあった（三角2020b：23）。しかし、そうした方針を、バイデン政権のように、政策パッケージの形にまとめて発信は行っていない。

我が国の非技術的な対処的政策としては、悪意ある行為を帰責できる者の公表を米国等と連携して実施した例があり、また、訴追の例では、2021年4月に中国人民解放軍が背景組織として関与されるとしつつ警察が書類送致した事件（CS本部2021：29）がある。経済的な制裁については、サイバーセキュリティ事件に関連してはこれまでのところ行われていない。

今後、我が国警察組織におけるサイバー犯罪捜査能力の集約・強化が行われることとなっている。捜査等で成果が得られたときに、バイデン政権のように、内閣の下で関係省庁と連携・調整し、他の対処政策とパッケージ化した形で発信していくことなどは、国の政策の訴求力を示し、また、悪意ある行為者に対する抑止を効かせる観点から重要であると考えられる。

(b) 技術的対策 上記の事件で採られた技術的対策は、政府や重要インフラの自システムの強化の他、攻撃手段や対策の情報提供方法といったアドバイザリーの発行（すべての事件）、技術的演習の提供（SW 事件）、さらに強制的な行為としてテイクダウンや資産の奪回（CP 事件）といったものがある。こうしたテイクダウン、インテリジェンスなどに基づく捜査、資産の奪回などは、分析フレームワークのスペクトラム上、侵害リスクの高い策である。これらの対策は、バイデン政権では、非技術的対策とパッケージ化した政策として打ち出されるものが多い。

一方、我が国では、侵害された情報システムのログ分析、不正プログラムなどの捕獲・解析、さらに、不正プログラムをコントロールする通信先の調査、ハニーポットの利用などにより、攻撃手段に係る情報提供を含むアドバイザリー情報などを従来から行っている。この様な対策は、侵害リスクの低いものにあたる。米国が実施するような侵害リスクの高い活動は、我が国では現在許されない又は困難なものである可能性が高いと考えられ[三角2021：43]、対処的対策策定にあたっては十分に慎重な検討が必要になる。

なお、CP 事件の後、立ち上げられたランサムウェア対策情報等をワンストップで把握できるサイトは、利用者にとって利便性の高いものである。我が国においても、ランサムウェアに対するアドバイザリーは NISC などがそれぞれ発信するなど、適時アドバイザリーを発信⁸²⁾している。我が国の事業者がより利便性高く情報を収集できるよう、政府・関係機関等が連携してワンストップ化など適切な発信手段が随時形成されることが望まれる。

(c) その他の特徴 CP 事件は、民間の重要インフラ事業者において OT への侵害のリスクを回避するべく行動したことで現実の供給途絶が発生した事件であり、対処的政策において他の事件とは異なる特徴がみられる。まず、物理的な供給途絶を受けての現実社会の緩和策を危機管理体制の下で発信している。

また、CP 社が安全第一のためにパイプラインを停止したことについて、政府として冷静に受け入れていると見える⁸³⁾。さらに、身代金支払いといった事業継続に資するための行動をとったことについて、同社経営層が公聴会で公然と発言したが、政府は、身代金支払いについては、政府は、一般的な考え方に反するものであっても、そのことを非難していない。安全や事業継続に対する重要性を理解し、冷静な対応がみられる。

我が国の場合に、組織が、サイバー攻撃を受けて、被害が発生したときに、マスメディアも含めて謝罪と事情説明を要求することが多々見られ、また、管理当局も叱責を含めた態度をとることが散見されたように思われる。そして仮に、被害企業の経営層が、安全第一でサービスを途絶させ、事業継続の観点から身代金支払ったと発言した場合に、各方面

の反応は批判的なものになる可能性が高いと思われる。サイバー攻撃は攻撃者が非難されるべきものである。サイバーの場合に関しても、安全第一や事業継続重視の考え方を肯定的にとらえる社会文化を醸成していくことは、我が国の安全や社会経済活動の安定確保の観点から重要であると考ええる。

また、TSAの指令で注目したい点はパイプライン事業者がサイバーセキュリティ事象を認識したときの義務的な報告先がサイバーセキュリティの専門家がいるCISAに一本化されている点である。管理当局であるTSAはCISAを通じて情報提供されることになるが、緊急時の窓口の一本化は、混乱や煩雑さなどの回避に重要である。我が国においても各セクターの事業法などで報告義務が課されているものがあるが、今後、TSAの取組みを参考として、規制当局・サイバー当局間で協力的に連携して効率的な報告等のラインを形成することは有益であると考ええる。

おわりに

本稿では、バイデン政権のサイバーセキュリティに係る戦略的政策、顕著なインシデントへの対処的政策などを分析するべく、分析フレームワークを設定し、バイデン政権のBriefing Roomにおける政策発表、報道官の発言などをデータとして扱った。そして、バイデン政権において、①安全第一、事業継続重視の方針、②政策のパッケージ化、③官民連携、関係機関の連携政策、④法執行機関の取組みについても政策パッケージへ組み込み、④関係機関連携もとの適時適切なアドバイザリーの発信といった特徴が見られた。こうした特徴は我が国サイバーセキュリティ政策への示唆として重要である。

一般にサイバーセキュリティ政策は、技術的事項や事件への対処の積み重ねから導き出されるものが多い。そのため、政権が変わったことで直ちに政策の内容が変わるものではないと考える。その点、例えばトランプ政権下で発生したSW事件への対処や、サプライチェーン政策の基調においても確認できる。そして安全保障の観点からは、対中国、対ロシアなどのスタンスに前政権と比較して大きな違いは現在のところは見られていない。したがって、政策の特徴も当面変わらないものと考えられる。IT産業大国であり同盟国である米国の政策は、我が国の政策検討・策定においても注視が必要であるところ、今後、CS戦略や重要インフラ行動計画の策定、顕著なインシデントへの対処的政策の策定・実施等にあたって、本稿の分析結果が貢献できることを期待したい。

参考文献

- サイバーセキュリティ戦略本部（CS 本部）、(2021)「次期サイバーセキュリティ戦略（案）」、
https://www.nisc.go.jp/active/kihon/cyber-security-senryaku_2021.html（Last visited, 2021年7月31日）
- 三角育生（2020a）「サイバーセキュリティ基本法制定・改正の経緯」『日本セキュリティ・マネジメント学会誌』34巻1号28-34頁
- 三角育生（2020b）「大規模ITセキュリティインシデント対処の政策的影響」『日本セキュリティ・マネジメント学会誌』34巻2号22-28頁
- 三角育生（2021）「我が国のサイバーセキュリティ戦略策定の背景」『日本セキュリティ・マネジメント学会誌』34巻3号39-46頁
- Center for Cyber & Homeland Security of The George Washington University (CCHS), (2016) “Into the gray zone – the private sector and active defense against cyber threats” : The George Washington University
- NTIA Multistakeholder Process on Software Component Transparency Framing Working Group (2019) Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM)、https://www.ntia.gov/files/ntia/publications/framingsbom_20191112.pdf（Last visited, 2021年8月13日）

註

- 1) 会見冒頭発言参照。
(<https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/13/statement-from-deputy-national-security-advisor-for-cyber-emerging-technologies-anne-neuberger-on-new-microsoft-exchange-patches/>, Last visited, 2021年7月30日)
- 2) 7月末現在、「次期サイバーセキュリティ戦略（案）」等に関する意見の募集を行っている段階である。
- 3) CS 本部「次期重要インフラ行動計画の検討について」2021年2月9日 (<https://www.nisc.go.jp/conference/cs/dai26/pdf/26shiryou06.pdf>, Last visited, 2021年7月31日) 参照。
- 4) <https://www.whitehouse.gov/briefing-room/>, Last visited, 2021年8月7日
- 5) <https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity>, Last visited, 2021年8月13日
- 6) <https://www.federalregister.gov/documents/2021/06/11/2021-12506/protecting-americans-sensitive-data-from-foreign-adversaries>, Last visited, 2021年8月13日
- 7) <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/>, Last visited, 2021年8月13日
- 8) <https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/20/statement-by-nsc-spokesperson-emily-horne-on-the-biden-administrations-efforts-to-protect-u-s-critical-infrastructure/>, Last visited, 2021年8月13日
- 9) <https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and->

- protect-federal-government-networks/, Last visited, 2021年 8 月 7 日
- 10) <https://csrc.nist.gov/publications/detail/sp/800-207/final>, Last visited, 2021年 8 月 7 日
- 11) <https://www.ntia.gov/SBOM>, Last visited, 2021年 8 月 7 日
- 12) Presidential Policy Directive 41 (2016年 7 月26日) により、国家安全保障上の利益、外交関係、国の経済、公共の信頼、市民の自由、公衆衛生、安全に対して、実証可能な被害をもたらす可能性が高いサイバーインシデントと定義。<https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>, Last visited, 2021年 8 月13日
- 13) https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/004_03_00.pdf, Last visited, 2021年 8 月 7 日
- 14) <https://www.nisc.go.jp/conference/cs/dai21/pdf/21shiryoku04.pdf>, Last visited, 2021年 8 月 7 日
- 15) <https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks>, Last visited, 2021年 8 月 7 日
- 16) <https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/20/statement-by-nsc-spokesperson-emily-horne-on-the-biden-administrations-efforts-to-protect-u-s-critical-infrastructure/>, Last visited, 2021年 8 月 9 日
- 17) <https://www.federalregister.gov/documents/2020/05/04/2020-09695/securing-the-united-states-bulk-power-system>, Last visited, 2021年 8 月 9 日
- 18) (<https://www.federalregister.gov/documents/2021/01/06/2020-28773/prohibition-order-securing-critical-defense-facilities>, Last visited, 2021年 8 月 9 日) 及び (<https://www.energy.gov/sites/default/files/2021-04/Revocation%20of%20Prohibition%20Order%2004202021.pdf>, Last visited, 2021年 8 月 9 日) を参照。
- 19) <https://www.nisc.go.jp/active/infra/pdf/shishin5rev.pdf>, Last visited, 2021年 8 月 9 日
- 20) https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/index.html, Last visited, 2021年 8 月 9 日
- 21) メディアへの事前説明における政府高官発言 (<https://www.whitehouse.gov/briefing-room/press-briefings/2021/07/28/background-press-call-on-improving-cybersecurity-of-u-s-critical-infrastructure/>, Last visited, 2021年 8 月 7 日)
- 22) <https://www.federalregister.gov/documents/2021/04/22/2021-08482/notice-of-request-for-information-rfi-on-ensuring-the-continued-security-of-the-united-states>, Last visited, 2021年 8 月 9 日
- 23) https://www.meti.go.jp/policy/safety_security/industrial_safety/oshirase/2016/09/280923-1.html, Last visited, 2021年 8 月 9 日
- 24) サイバーセキュリティ戦略本部資料提供等規則 1 条 1 項 2 号 (https://www.nisc.go.jp/conference/cs/pdf/teikyou_kisoku.pdf, Last visited, 2021年 8 月 9 日)
- 25) https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r2.pdf, Last visited, 2021年 8 月 9 日
- 26) 例えば、「電力分野におけるサイバーセキュリティ対策と『産業サイバーセキュリティ研究会 電力 SWG』での検討状況」経済産業省産業保安グループ (2019年 3 月15日) (https://www.meti.go.jp/shingikai/sankoshin/hoan_shohi/denryoku_anzen/pdf/019_04_00.pdf, Last

- visited, 2021年8月9日) によると、「制御系システムはインターネットとの直接的な接点は存在しない」などの認識が示されている点など。
- 27) <https://www.federalregister.gov/documents/2020/08/11/2020-17699/addressing-the-threat-posed-by-tiktok-and-taking-additional-steps-to-address-the-national-emergency>,
<https://www.federalregister.gov/documents/2020/08/11/2020-17700/addressing-the-threat-posed-by-wechat-and-taking-additional-steps-to-address-the-national-emergency>, Last visited, 2021年8月9日
- 28) <https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain>, Last visited, 2021年8月9日
- 29) <https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/09/fact-sheet-executive-order-protecting-americans-sensitive-data-from-foreign-adversaries/>, Last visited, 2021年8月9日
- 30) <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/>, Last visited, 2021年8月9日
- 31) <https://www.nisc.go.jp/conference/cs/dai30/pdf/30shiryou08.pdf>, Last visited, 2021年8月9日
- 32) <https://sec.report/Document/0001628280-20-017451/>, Last visited, 2021年8月9日
- 33) <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>, Last visited, 2021年8月9日
- 34) <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>, Last visited, 2021年8月9日
- 35) <https://www.federalregister.gov/documents/2021/04/19/2021-08098/blocking-property-with-respect-to-specified-harmful-foreign-activities-of-the-government-of-the>, Last visited, 2021年8月13日
- 36) <https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/>, Last visited, 2021年8月9日
- 37) <https://www.fbi.gov/news/pressrel/press-releases/russian-foreign-intelligence-service-exploiting-five-publicly-known-vulnerabilities-to-compromise-us-and-allied-networks>, Last visited, 2021年8月13日
- 38) 会見での政府高官冒頭発言。 <https://www.whitehouse.gov/briefing-room/press-briefings/2021/04/15/background-press-call-by-senior-administration-officials-on-russia/> , Last visited, 2021年8月9日
- 39) <https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/>, Last visited, 2021年8月14日
- 40) <https://cyber.dhs.gov/ed/21-02/>, Last visited, 2021年8月14日
- 41) <https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/19/statement-by-deputy-national-security-advisor-for-cyber-and-emerging-technology-on-solarwinds-and-microsoft-exchange-incidents/>, Last visited, 2021年8月9日
- 42) https://www.mofa.go.jp/mofaj/press/danwa/page6_000583.html, Last visited, 2021年8月

9 日

- 43) <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/>, Last visited, 2021年 8 月 9 日
- 44) <https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion>, Last visited, 2021年 8 月 9 日
- 45) <https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion>, Last visited, 2021年 8 月 9 日
- 46) 例えば、DHS / TSA のバイブライインインフラ事業者に対する第二の指令等 (<https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators>, Last visited, 2021年 8 月 9 日)
- 47) <https://www.whitehouse.gov/briefing-room/press-briefings/2021/07/19/background-press-call-by-senior-administration-officials-on-malicious-cyber-activity-attributable-to-the-peoples-republic-of-china/>, Last visited, 2021年 8 月 9 日
- 48) <https://www.cisa.gov/blog/2021/07/19/safeguarding-critical-infrastructure-against-threats-peoples-republic-china>, Last visited, 2021年 8 月 9 日
- 49) <https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown>, Last visited, 2021年 8 月10日
- 50) CP 社 CEO の説明による。(<https://www.npr.org/2021/06/03/1003020300/colonial-pipeline-ceo-explains-the-decision-to-pay-hackers-4-4-million-ransom>, Last visited, 2021年 8 月10日)
- 51) 政府高官記者会見冒頭発言参照。(<https://www.whitehouse.gov/briefing-room/press-briefings/2021/05/10/press-briefing-by-press-secretary-jen-psaki-homeland-security-advisor-and-deputy-national-security-advisor-dr-elizabeth-sherwood-randall-and-deputy-national-security-advisor-for-cyber-and-emerging/>, Last visited, 2021年 8 月10日)
- 52) <https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/10/remarks-by-president-biden-on-the-economy/>, Last visited, 2021年 8 月14日
- 53) <https://www.whitehouse.gov/briefing-room/press-briefings/2021/05/10/press-briefing-by-press-secretary-jen-psaki-homeland-security-advisor-and-deputy-national-security-advisor-dr-elizabeth-sherwood-randall-and-deputy-national-security-advisor-for-cyber-and-emerging/>, Last visited, 2021年 8 月10日
- 54) <https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/11/fact-sheet-the-biden-harris-administration-has-launched-an-all-of-government-effort-to-address-colonial-pipeline-incident/>, Last visited, 2021年 8 月10日
- 55) <https://us-cert.cisa.gov/ncas/current-activity/2021/05/11/joint-cisa-fbi-cybersecurity-advisory-darkside-ransomware> 及び <https://us-cert.cisa.gov/ncas/alerts/aa21-131a>, Last visited, 2021年 8 月11日
- 56) https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf, Last visited, 2021年 8 月11日
- 57) <https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom>, Last visited, 2021年 8 月14日
- 58) <https://www.bankinfosecurity.com/colonial-ceo-at-senate-hearing-details-ransomware->

- attack-a-16836, Last visited, 2021年 8 月10日
- 59) 記者の質問に対するサイバー新技術担当国家安全保障補佐官補の回答参照。(https://www.whitehouse.gov/briefing-room/press-briefings/2021/05/10/press-briefing-by-press-secretary-jen-psaki-homeland-security-advisor-and-deputy-national-security-advisor-dr-elizabeth-sherwood-randall-and-deputy-national-security-advisor-for-cyber-and-emerging/, Last visited, 2021年 8 月10日)
- 60) https://www.whitehouse.gov/briefing-room/press-briefings/2021/05/13/press-briefing-by-press-secretary-jen-psaki-may-13-2021/, Last visited, 2021年 8 月10日
- 61) https://krebsonsecurity.com/2021/05/darkside-ransomware-gang-quits-after-servers-bitcoin-stash-seized/, Last visited, 2021年 8 月11日
- 62) https://www.justice.gov/opa/pr/departments-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside, Last visited, 2021年 8 月11日
- 63) https://www.justice.gov/opa/press-release/file/1402056/download, Last visited, 2021年 8 月11日
- 64) https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators, Last visited, 2021年 8 月11日
- 65) https://www.tsa.gov/news/press/testimony/2021/07/27/pipeline-cybersecurity-protecting-critical-infrastructure, Last visited, 2021年 8 月11日
- 66) https://windot.com/docs/rus/rus32wdw/PDF/TSA_security-directive-on-enhancing-pipeline-cybersecurity_(002).pdf, Last visited, 2021年 8 月11日
- 67) https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators, Last visited, 2021年 8 月11日
- 68) https://www.cisa.gov/stopransomware, Last visited, 2021年 8 月11日
- 69) https://www.dhs.gov/news/2021/07/14/united-states-government-launches-first-one-stop-ransomware-resource, Last visited, 2021年 8 月11日
- 70) 例えば、https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/, Last visited, 2021年 8 月11日
- 71) https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/06/16/remarks-by-president-biden-in-press-conference-4/, https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/07/09/background-press-call-by-senior-administration-officials-on-president-bidens-call-with-president-putin-of-russia/, Last visited, 2021年 8 月11日
- 72) https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/13/carbis-bay-g7-summit-communicue/, https://www.mofa.go.jp/mofaj/files/100200083.pdf, Last visited, 2021年 8 月11日
- 73) https://obamawhitehouse.archives.gov/the-press-office/2014/12/18/press-briefing-press-secretary-josh-earnest-121814, Last visited, 2021年 8 月10日
- 74) 米国証券取引委員会への報告書 p20参照。(https://www.sec.gov/Archives/edgar/data/313838/000119312516624169/d168822d20f.htm, Last visited, 2021年 8 月10日)
- 75) https://www.dhs.gov/news/2014/12/19/statement-secretary-johnson-cyber-attack-sony-pictures-entertainment, Last visited, 2021年 8 月10日
- 76) https://www.federalregister.gov/documents/2015/01/06/2015-00058/imposing-additional-

- sanctions-with-respect-to-north-korea, Last visited, 2021年 8 月10日
- 77) <https://obamawhitehouse.archives.gov/the-press-office/2015/01/02/statement-press-secretary-executive-order-entitled-imposing-additional-s>, Last visited, 2021年 8 月10日
- 78) <https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and>, Last visited, 2021年 8 月10日
- 79) <https://www.dhs.gov/news/2017/05/12/dhs-statement-ongoing-ransomware-attacks>, Last visited, 2021年 8 月10日
- 80) <https://trumpwhitehouse.archives.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/>, Last visited, 2021年 8 月10日
- 81) <https://home.treasury.gov/news/press-releases/sm774>, Last visited, 2021年 8 月10日
- 82) 例えば、<https://www.nisc.go.jp/active/infra/pdf/ransomware20201126.pdf>、<https://www.nisc.go.jp/active/infra/pdf/ransomware20210430.pdf>、<https://www.jpccert.or.jp/magazine/security/nomore-ransom.html> など。 , Last visited, 2021年 8 月11日
- 83) 国土安全保障担当補佐官冒頭発言参照。(<https://www.whitehouse.gov/briefing-room/press-briefings/2021/05/10/press-briefing-by-press-secretary-jen-psaki-homeland-security-advisor-and-deputy-national-security-advisor-dr-elizabeth-sherwood-randall-and-deputy-national-security-advisor-for-cyber-and-emerging/> Last visited, 2021年 8 月10日)