米国サイバー・サプライチェーン・セキュリティ法政策の動向 ―第117議会第２会期（2022-2023年)―

米国サイバー・サプライチェーン・セキュリティ法政策の動向
—第117議会第２会期（2022-2023年）—

橘　　雄　　介（社会環境学科）

Law and Policy on the Cyber Supply Chain Security in the United States
—117th United States Congress 2nd Session—

TACHIBANA Yusuke (Department of Socio-Environmental Studies)

Abstract

In the second session of the 117th Congress (2022-2023), there were significant changes in supply chain security. The supply chain security community made progress in revising NIST SP 800-171, a fundamental document for contractors in the field of supply chain security. They also focused on various themes, including the Software Bill of Materials (SBOM), zero-trust, and the notification scheme in the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). These initiatives were responses to major security incidents, such as the Colonial Pipeline breach and the Log4j vulnerability incident. Additionally, security enhancements against China, such as the CHIPS Act of 2022, along with restrictions on TikTok, saw advancements. However, there were significant policy failures in the area of Systemically Important Critical Infrastructure (SICI).

Keywords: *information law, information security, supply chain security, U.S. law, critical infrastructure*

１．はじめに

○　情報セキュリティ法政策の全体像

情報セキュリティとは，情報の CIA（機密性（Confidentiality），完全性（Integrity）及び可用性（Availability））を保護する取り組みとされる[1)]。情報セキュリティ法政策とは CIA を保護する法政策を意味する[2)]。

情報セキュリティ法政策は大まかに，以下の４種類に分類できる[3)]。

① 情報の保護：知的財産法による保護すべき情報の設定や，個人情報保護法制・競争法を通じた消費者保護，
② 情報セキュリティ・マネジメント：ISMS（Information Security Management System）など，CIA を確保する取組み，
③ 治安維持：主として民事法及び刑事法を通じたクラッカーに対する制裁や営業秘密の保護，並びに
④ 安全保障：国防や経済安全保障の観点からの規制

素描すると，①で組織において保護すべき情報が設定され，②でその保護の取り組みがいわば予防的に取られる。これに対し，国内からの攻撃には③で，国外からの攻撃には④で対処する，というのが本稿のマッピングである。

○　サイバー・サプライチェーン・セキュリティ

サイバー・サプライチェーンとは，情報及び運用技術（IT/OT）に関するサプライチェーンのエコシステムのことで，また，サイバー・サプライチェーン・セキュリティ（以下「サプライチェーン・セキュリティ」と省略することがある）はこのエコシステムのセキュリティ確保の取組み全般を指す[4)]。

サプライチェーン・セキュリティの分野において，前述②の情報セキュリティ・マネジメントはサイバー・サプライチェーン・リスク管理（Cyber Supply Chain Risk Management or Cybersecurity Supply Chain Risk Management: C-SCRM）と呼ばれる[5)]。特に ICT 製品に焦点を当てる場合には，従来から「ICT SCRM」ともいわれる[6)]。他方，日本では「IT サプライチェーンリスクマネジメント」ともいわれる[7)]。

C-SCRM は特に機密性，完全性（真正性及び非改ざん性を含む），レジリエンス及び品質という４つの保護対象

2023年10月31日受付

表１　サイバー・サプライチェーン・セキュリティ法政策の全体像（米国）

	項目	主な法令・基準等			名宛人
		ハードウェア	ソフトウェア	クラウド	
機密性	1　自組織の情報セキュリティ・マネジメント	NIST FIPS 200; NIST SP 800-53; NIST SP 800-161			連邦機関 システム運用者
機密性	2　請負人等に対する情報セキュリティ・マネジメント	NIST SP 800-171 DoD・Cybersecurity Maturity Model Certification (CMMC)			請負人
真正性	3　模造電子部品の排除／OEMからの取得	政府調達からの排除：2015年度国防権限法	N/A	N/A	連邦機関 請負人
非改ざん性／非悪意性	4　疑わしい製品の排除（対物規制）	政府調達からの排除：2019年度国防権限法(※1) 事後的な排除：連邦情報セキュリティ現代化法 (FISMA (2014))、連邦調達サプライチェーン・セキュリティ法 (FASCSA)(※2)			連邦機関 請負人(※1のみ) 国防総省(※2のみ)
非改ざん性／非悪意性		N/A	TikTokの公用端末での利用禁止（OMB）	N/A	連邦機関
非改ざん性／非悪意性		通信関連規制：中国製機器に対するユニバーサル・サービス基金（USF）の支出規制及び認可禁止（FCC）	N/A	N/A	民間事業者
非改ざん性／非悪意性	（対人規制）	輸出規制：中国企業等に対する輸出規制（DOC） 営業資格規制：中国企業等に対する通信事業免許の取消し（FCC）	N/A（2022年時点）	N/A	民間事業者
品質	5　製品認証等（製品認証）	FISMA (2002); NIST FIPS 140-3; ISO/IEC 15408 (Common Criteria (CC))	N/A	FedRAMP	連邦機関 システム運用者
品質	（セキュリティ基準）	ハードウェア部品表（HBOM）（CISA） IoT製品に対する最低基準＋ラベル制度（NIST）	ソフトウェア部品表（SBOM）（NIST） ソフトウェアに関する最低基準＋ラベル制度（NTIA）	N/A	
品質		カリフォルニア州IoT法（2019年）	N/A	N/A	民間事業者

に関係するとされる[8]。この４つの保護対象に沿って，本稿はC-SCRMの取組みを以下の５種類に分類している[9]。

(1)　自組織の情報セキュリティ・マネジメント：主に自組織の機密性を向上させる取組み
(2)　請負人等に対する情報セキュリティ・マネジメント：主にサプライチェーンの機密性を向上させる取組み
(3)　模造電子部品の排除／OEMからの取得：情報システムの真正性を確保する取組み
(4)　疑わしい製品の排除（対物規制及び対人規制）：情報システムが改ざんされておらず，悪意の無いことを確保する取組み
(5)　製品認証等（製品認証及びセキュリティ基準）：情報システムの品質を確保する取組み

○　本稿の調査対象

本報告書はサイバー・サプライチェーン・セキュリティのうち米国におけるC-SCRMの動向を調査するもので，期間としては第117議会第２会期（2022-2023年）を調査対象とする[10]。そのため，第118議会第１会期（2023-2024年）における展開は反映できていない。

以下紹介する取組みを上述のC-SCRMの５分類に沿ってまとめると，表１のようになる。

２．第117議会第２会期（2022-2023年）の主な動向

○　情報セキュリティ分野の立法の傾向

米国の議会において，情報セキュリティ分野の立法は個別法だけではなく，包括歳出法及び国防権限法というそれぞれのパッケージ法の中でなされることも多い。

包括歳出法（Consolidated Appropriations Act）は，連邦政府の機関について特定の会計年度における資金を定める法律である[11]。この中で，情報セキュリティに関する法律が包括（consolidated）されることがある。

国防権限法（National Defense Authorization Act: NDAA）は特定の会計年度における国防総省（Department of Defense: DoD）の支出及び政策を定める法律である[12]。もっとも，国防総省だけではなく，国土安全保障省（Department of Homeland Security: DHS）などにも関係する情報セキュリティに関する支出及び政策を定める法律がまとめられる（package）ことがある。国防権限法は年末に次会計年度のものが成立することが多い。そこで，以下では，各法政策の紹介に入る前に，2022年に成立した包括歳出法及び国防権限法で情報セキュリティに関係するものを確認したい。

○　2022年度包括歳出法

2022年度の包括歳出法も情報セキュリティの規定を含んでいる。当該歳出法案[13]に後述の重要インフラに関するサイバー・インシデント報告法が統合され，「2022年度包括歳出法（Consolidated Appropriations Act, 2022）」[14]として2022年３月に成立した。

○　2023年度包括歳出法

2023年度包括歳出法（Consolidated Appropriations Act, 2023）[15]は2023会計年度を対象とするもので，2022年12月に成立した[16]。後述の通り，情報セキュリティに関す

る食品医薬品局の権限を定めている。

○　2023年度国防権限法

2023年度国防権限法[17]（正式名称は，“James M. Inhofe National Defense Authorization Act for Fiscal Year 2023”。同法１条(b)）の経緯と内容を紹介する。

2023年度国防権限法の成立には紆余曲折があった。同法の下院版（H.R.7900）[18]は2022年７月には下院で可決されたが，上院版（S. 4543）[19]は委員会に提出されたものの，上院の投票に至らなかった。通常，上下院の法案に齟齬がある場合，上下両院の合同委員会が開催され，そこで最終的な法案が調整される。しかし，本年度の国防権限法は上院の通過に至らなかったため，2022年12月，上下両院の担当委員会（軍事委員会（Armed Services Committee））の合意の下[20]，上下両院の法案を統合した法案（H.R.7776）[21]が作成され，上下両院に提出された。統合版の法案は，このように，上院での修正の機会が無かったため，後述の通り，情報セキュリティに関する条項がかなり削られたものとなった。

同法案は，同月，上下両院で可決され[22]，Biden 大統領の署名により成立した[23]。2023年度国防権限法に含まれる条項で，サイバー・サプライチェーン・セキュリティに関連のあるものとして以下がある[24]。

・サイバーセキュリティ成熟度モデル認証（Cybersecurity Maturity Model Certification: CMMC）の評価を国防総省に求める条項
・国家情報長官室（Office of the Director of National Intelligence: ODNI）に対して，海外事業者が提供する商用スパイウェアがもたらす脅威を評価するように指示する条項，及び，ODNI に対して，情報機関が特定の種類のスパイウェアを使用することを禁止する権限を付与する条項
・連邦行政機関の安全なクラウドサービスへの移行を支援するための，Federal Risk and Authorization Management Program (FedRAMP) Authorization Act

他方，以下の条項は上記上下両院における妥協において，削除された[25]。

・国土安全保障省及び国防総省が参加する「情報連携環境（information collaboration environment）」を創設し，連邦政府のサイバー脅威情報共有の主要機関とする条項。これは，サイバースペース・ソラリウム委員会（Cyberspace Solarium Commission: CSC）が以前，提唱していたものだが，サイバー防衛連携（Joint Cyber Defense Collaborative: JCDC）がその代替として機能するからだとされる[26]。これは，国土安全保障省の下部組織であるサイバーセキュリティー・インフラセキュリティー庁（Cybersecurity and Infrastructure Security Agency: CISA）が設立したもので，官民合同のサイバー対策の組織である。
・調達規則を改定し，国防総省が購入する商用ソフトウェアにソフトウェア部品表（Software Bill of Materials: SBOM）を含めることを義務付ける条項。当該法案は，上院版にはあったが，下院版にはなかった。
・連邦政府機関に「システム上重要な重要インフラ」（Systemically Important Critical Infrastructure: SICI）を特定し，これらの事業体に新たなサイバーセキュリティ義務を課す方法を検討するとともに，連邦政府のサイバーセキュリティ支援をさらに提供することを求める条項。当該法案は，下院版にあったが，上院版には含まれていなかった。

3．自組織／請負人等の情報セキュリティ・マネジメント

○　NIST SP 800-171の改訂作業

商務省の下部組織である国立標準技術研究所（National Institute of Standards and Technology: NIST）は NIST SP 800-171の改訂作業を進めている。SP 800-171は管理非機密情報（Controlled Unclassified Information: CUI）に関する情報セキュリティ・マネジメント標準で，請負事業者が遵守することが求められる。その意味で，サイバー・サプライチェーン・セキュリティにおける基本文書の一つである[27]。2022年７月には，NIST SP 800-171 Rev. 3に関する初期公開諮問が行われた[28]。

○　NIST SP 800-161

2022年５月，NIST は，「システムと組織のためのサイバーセキュリティ・サプライチェーン・リスク管理の実践」の改訂版（NIST Special Publication 800-161 Revision 1）を策定した[29]。

この文書は，組織のあらゆるレベルにおけるサプライチェーン全体のサイバーセキュリティ・リスクの特定，評価，対応に関するガイダンスを更新したものである。これは，2021年５月に Biden 政権下で成立した大統領令14028号「国家のサイバーセキュリティの向上（Improving the Nation's Cybersecurity）」[30]における NIST の責任の履行に貢献するものとされる。当該大統領令は，サプライチェーン全体で増大するソフトウェア・セキュリティ・リスクに対処するものである[31]。

この文書は，組織がサプライチェーン内およびサプライチェーン全体のサイバーセキュリティ・リスクを管理する能力を開発する際に採用すべき重要な実践を提示している。また，使用を検討している完成品だけでなく，他の場所で開発された可能性のある個々のコンポーネントの脆弱性や，それらのコンポーネントが目的地に到達するまでの

経路を考慮することも奨励している[32]。

○　ゼロトラスト

2022年は境界防御ではなく，ゼロトラスト（Zero Trust），すなわち，境界内の各ノードの挙動について信用性を担保する取組みも進んだ[33]。

米国においては，2020年に既にNISTがゼロトラストの基本標準であるNIST SP 800-207[34]を策定していたが，これは法的な拘束力を有していなかった。

そこで，大統領府に属する行政管理予算局（Office of Management and Budget: OMB）は，2022年１月，ゼロトラストに関する戦略を発表した[35]。これは，2024年までに連邦行政機関においてゼロトラストを実現するためのロードマップを示したもので，すべての内部ネットワークを信頼できないものとして扱うこと，具体的には，多要素認証等に関する要件が含まれている。これは，前述の大統領令14028号[36]を達成するものである。

その他，国防総省は，2022年11月には，ゼロトラスト戦略を発表している[37]。

3.1　重要インフラ[38]

3.1.1　システム上重要な重要インフラ（SICI）

「システム上重要なインフラ確保法（Securing Systemically Important Critical Infrastructure Act）」（H. R. 5491）[39]が，2021年10月，下院に提出された。これはSICIを指定するもので，サイバースペース・ソラリウム委員会（CSC）の目標の一つである。これはサイバーセキュリティ・インフラセキュリティ庁にSICIの特定を義務付ける。

同法案は前述の通り，その後，2023年度国防権限法に組み込まれていたが，最終的には除外された。その背景には，当該法案は，下院版にはあったが，上院版には含まれていなかったことがある。加えて，銀行業界団体がSICIの事業体に対するサイバー規制に反対していたことがあるようである[40]。

3.1.2　官民情報共有

○　重要インフラに関するサイバー・インシデント報告法

第117議会第２会期（2022-2023年）において成立した法律の目玉の一つが「2022年重要インフラに関するサイバー・インシデント報告法（Cyber Incident Reporting for Critical Infrastructure Act of 2022: CIRCIA）」[41]である。これは後に歳出法案に統合され，2022年度包括歳出法の第Y編として，2022年３月に成立した。

CIRCIAは，CISAに対して2024年２月までに，報告義務の対象となる重要インフラ事業者とその報告方法を明記した規則制定案通知（NPRM）を発するよう義務づける。

○　CISAによる環境整備

CIRCIAの成立を受け，CISAは，2022年４月，サイバー・インシデントの情報共有ガイダンスを発表した[42]。これはCIRCIA上の義務の履行に先立つもので，未知の脅威の影響を軽減するためのインシデント情報共有を任意に行うものである。CISAに共有すべきインシデントの範囲には，システムに対する不正アクセスや12時間以上続くDoS攻撃などが含まれる。

また，CISAは，2022年９月に，上記NPRMに盛り込むべき内容についての意見を収集するための予備的な情報提供要請（RFI）を公表した[43]。

3.1.3　サイバー保険[44]

重要インフラとサイバー保険の関係も論じられている。会計検査院（Government Accountability Office: GAO）の報告書は大企業や重要なインフラ（パイプラインや水処理施設など）へのサイバー攻撃の影響は，米国経済や国家安全保障により広範で持続的な影響を与える可能性があるとする[45]。

4．疑わしい製品等の排除

4.1　対物規制

2022年は，IT機器の直接規制が通信機器・監視カメラにも拡大された。2022年11月，連邦通信委員会は，許容できない国家安全保障上のリスクをもたらすとみなされる企業機器やサービスの「カバーリスト」に中国企業の通信機器及び映像監視機器を加えた[46]。対象となる企業は，Huawei Technologies，ZTE Corp.，Hytera Communications，Hangzhou Hikvision Digital Technology及びDahua Technologyで，後者３社についてこの命令で追加された。安全対策が施されない限り，これらの機器の認可申請が凍結される。これは，2021年のSecure Equipment Actに基づくものである[47]。

4.2　経済安全保障

疑わしい製品等の排除の分野では，半導体の調達をてこに，信頼できる製品等の研究開発を促進する動きがある[48]。注目を集めたものが，CHIPS法である。

「チップス及び科学法（CHIPS and Science Act）」（H.R. 4346）[49]は2022年７月に上下院を通過し，2022年８月，Biden大統領が署名して[50]，成立した[51]。同法は「2022年チップ法（CHIPS Act of 2022）」と呼ばれる（１条）。

同法は国内の半導体製造の強化やオープン無線アクセス・ネットワーク（Open RAN）の推進などに予算が割り当てられている。背景には，IT機器に関するサプライチェーン・セキュリティがあり，半導体の安全保障，及び，Open RANについては，特にHuawei社などの中国政府による支援を受けた企業のネットワーク機器の拡大防止とい

う意図があるとされる[52)]。

同法が情報セキュリティと関係するのは同法に基づく資金を企業が獲得するために，国家安全保障上の懸念を防止する取組み（いわゆる「ガードレール条項（national security guardrails）」）が義務づけられるからである[53)]。

4.3　スパイウェア対策

サイバー・サプライチェーン・セキュリティにおいて，2022年の最も大きな動きの一つが動画共有アプリ「TikTok」に対する連邦及び州政府の動向である[54)]。もっとも，以下に見るように，2022年段階では，禁止の範囲はあくまでも連邦や州政府内にとどまり，民間の規制には至っていなかった。

○　連邦政府・TikTok 禁止法

連邦政府においては，上院に「政府機器における TikTok 禁止法（No TikTok on Government Devices Act）」（S. 1143）[55)]が提出され，2022年12月に包括歳出法[56)]の一部として成立した[57)]。TikTok 禁止法は，連邦政府が使用する接続機器での TikTok の使用を禁止するもので，具体的には，連邦情報技術システムから TikTok 及び後継アプリの削除を義務づけ，行政管理予算局に当該削除についての行政機関向けの基準を策定することを義務づけている[58)]。

背景には，TikTok 及びその運営会社 ByteDance Ltd.が中国企業に国家安全保障に関する政府への協力を義務付ける中国の法律の適用を受けている疑いがあり，故に，TikTok が中国政府とユーザーデータの共有しかねないとの懸念があるとされる[59)]。同法に対しては，逆に米国に拠点を置くソーシャル・メディア・プラットフォームが国外でビジネスを行う能力に影響を及ぼすとの指摘もある[60)]。

○　州政府・行政機関の端末での TikTok の禁止

州政府でも州知事の命令で州政府機関が所有または管理する端末に対する TikTok 禁止の措置が執られている。そのような州として，サウスダコタ州，サウスカロライナ州，メリーランド州，テキサス州，ユタ州及びアイダホ州がある。

もっとも，同種の規制で先行した初期の州はネブラスカ州で，2020年８月に州知事が州の全端末での TikTok の使用禁止を命じている[61)]。その背景には，2020年に，当時 Trump 大統領が国際緊急経済権限法（International Emergency Economic Powers Act: IEEPA）に基づき，民間も含め，TikTok を禁止する大統領令を出したことがある[62)]。もっとも，連邦裁判所は，IEEPA に基づき書籍，映画，デジタルメディアなどの「情報および情報資料（information and informational materials）」を規制することはできず，大統領が TikTok を禁止する権限はないと判断した[63)]。その後，Biden 政権は当該大統領令を取り消し[64)]，別の方策を検討するとしていた[65)]。

加えて，インディアナ州は，2022年12月，アプリメーカーがアプリの内容やデータ収集方法に関して虚偽の表現をしたとして，TikTok を提訴している[66)]。

4.4　民事・刑事法の執行

IT 機器の模造品については，大規模な検挙もあった。司法省（Department of Justice: DOJ）は，2022年７月，Cisco 社のネットワーク機器の模造品を輸入したとして，電信詐欺や偽造品密売の罪で，輸入者を起訴したと発表している[67)]。当該製品は中国及び香港からのもので，その納入先には病院や学校，政府機関，軍隊が含まれるとされる[68)]。

4.5　対人規制

○　輸出規制

2022年10月，商務省（Department of Commerce: DOC）の産業安全保障局（Bureau of Industry and Security: BIS）は中国向けの高度なコンピューティングおよび半導体製造品目について新たな規制を追加した[69)]。

また，Biden 政権は，2022年11月，半導体の対中輸出規制について，日本など同盟国にも同様の措置を求めた[70)]。これを受け，日本政府は，2023年１月，外為法を利用して，先端半導体の対中輸出を規制するよう，調整に入った。外為法上，軍事向けに転用可能な民生品について政府は輸出の管理権限を有するからである[71)]。これを受け，経産省は，2023年５月，省令改正し，先端半導体の輸出規制することとした。同改正は７月に施行された[72)]。

○　中国企業に対する規制法

その他，成立はしていないが，2022年には，中国企業やその製品・サービスに対する直接規制を求める法案も提出されていた。具体的には，Huawei の米国金融システムへのアクセスを遮断する法案「Neutralizing Emerging Threats from Wireless OEMs Receiving direction from Kleptocracies and Surveillance states (NETWORKS) Act」（H.R.9490 / S. 5239）[73)]，及び，TikTok を IEEPA の免責規定から除外する法案「ANTI-SOCIAL CCP Act」（H.R.9508）があった[74)]。

○　通信免許における中国企業に対する規制

通信分野では，従前から連邦通信委員会（Federal Communications Commission: FCC）が中国の通信事業者の免許を取り消していたが，2022年には，China Telecom (Americas) Corp.の国内州間サービスおよび米国と他国を結ぶ国際サービスを提供する通信法214条権限を取り消した2021年の FCC の決定が裁判所によって支持されている[75)]。

5．製品認証等

5.1　IT 機器のセキュリティ[76)]

○　会計検査院・IoT・OT 報告書

会計検査院は，2022年12月，IoT・OT の安全確保に向けた各省庁の取り組みにギャップがあるとの報告書を発表している。具体的には，CISA 傘下の分野別リスク管理機関（Sector Risk Management Agencies: SRMA）は，重要インフラ事業者がモノのインターネット（IoT）機器や運用技術（OT）をサイバー脅威から保護できるよう，様々なサイバーセキュリティ・イニシアティブを実施したが，いずれもベスト・プラクティスにとどまり，リスク評価が実施されていなかった。故に，セキュリティ施策の効果を検証し，それをリスク評価の一部とするよう，取り組みの指標を開発する必要があると勧告している。この報告書は，2020年の Internet of Things Cybersecurity Improvement Act によって義務付けられた検証である[77)]。

5.2　ソフトウェア

5.2.1　オープンソース／サプライチェーン対策

○　サイバー安全審査会・Log4j の詳細報告書

CISA 傘下のサイバー安全審査会（Cyber Safety Review Board: CSRB）は，2022年７月，Log4j 事件[78)]に関する詳細報告書を公開した[79)]。CSRB は2021年の大統領令14028号で設立が義務付けられたもので，飛行機事故などの交通事故を調査する国家運輸安全委員会（National Transportation Safety Board: NTSB）に相当する，サイバー空間上の機関として想定されている[80)]。Log4j 事件の審査は CSRB の最初の審査となる。

そこでは，以下のように，組織がシステム内の log4j の配備場所を特定し，パッチを当てるのに数年を費やすため，log4j の脆弱性は継続的な問題になるとしつつ，今後，ソフトウェアの透明性の向上が提言されている。

「Log4j の継続的なリスクへの対応：Log4j の脆弱性への対応を長期的に継続的に警戒する。

1．組織は，今後数年間，Log4j の脆弱性に対処できるように準備しておく必要がある。
2．組織は，Log4j の悪用に関する観測結果を引き続き報告（及びエスカレーション）する必要がある。
3．CISA は，権威あるサイバーリスク情報を開発，調整，公表する能力を拡大すべきである。
4．連邦および州の規制当局は，それぞれの規制当局を通じて CISA ガイダンスの実施を推進する必要がある。

セキュリティ衛生のための既存のベストプラクティスを推進する：脆弱性管理とセキュリティ衛生のために，業界で認められているプラクティスや標準を採用する。

5．組織は，脆弱なシステムを特定する機能に投資する必要がある。
6．正確な情報技術（IT）資産とアプリケーションのインベントリーを維持する能力を開発する。
7．組織は，脆弱性対応プログラムを文書化する必要がある。
8．組織は，脆弱性の開示と対処のプロセスを文書化する必要がある。
9．ソフトウェア開発者及び保守者は，安全なソフトウェアの実践を行うべきである。

より良いソフトウェアエコシステムの構築：ソフトウェアエコシステムの変革を推進し，脆弱性管理のプロアクティブモデルへの移行を図る。

10．オープンソースソフトウェアの開発者は，コミュニティベースのセキュリティイニシアチブに参加する必要がある。
11．安全なソフトウェア開発に関するソフトウェア開発者のトレーニングに投資する。
12．ソフトウェア部品表（SBOM）のツーリングと採用性を向上させる。
13．オープンソースソフトウェアのセキュリティへの投資を増やす。
14．重要なサービスに対するオープンソースソフトウェアの保守サポートを試験的に実施する。

未来への投資：国家のデジタル・セキュリティを長期的に解決するために必要な文化的・技術的なシフトを追求する。

15．連邦行政機関へのベンダーに対するソフトウェアの透明性の基本要件を検討する。
16．サイバー安全報告システム（CSRS）の有効性を検証する。
17．ソフトウェア・セキュリティ・リスク評価中核的研究拠点（software security risk assessment center of excellence: SSRACE）の設立の可能性を検討する。
18．安全なソフトウェアを構築するために必要なインセンティブ構造を研究する。
19．既知の脆弱性を持つソフトウェアの特定を改善するため，政府主導のワーキンググループを設立する。」[81)]

○　行政管理予算局・ソフトウェア・サプライチェーン指令

行政管理予算局は，2022年９月，ソフトウェア・サプライチェーンのセキュリティの強化のための指令を公表して

いる[82]。これは，2021年の大統領令14028号を受けたものである。

具体的には，指令は，連邦行政機関がNISTのガイダンスに基づき，製品が安全に開発されていることを証明する提供者からのみソフトウェアを購入するよう指示している。指令の適用対象はファームウェア，オペレーティングシステム，アプリケーション，アプリケーションサービス（クラウドベースのソフトウェアなど）及びソフトウェアを含む製品とされる。ソフトウェア製作者がNISTのガイダンスに従っていることを証明できない場合，当該証明できない事項を特定し，当該リスクの軽減策を文書化し，その実施のためのアクション・プランとマイルストーン（Plan of Action & Milestones: POA&M）を要求できる。また，証明の方法として，連邦行政機関は，サービスや製品の重要性により第三者評価ないし自己証明を要求できるとする。第三者評価として，たとえば，クラウドについて後述のFedRAMPのセキュリティ認証がある。また，最も重要なソフトウェアについては，開発者が最終製品に含まれるソフトウェアコンポーネントのリストを提供するソフトウェア部品表（SBOM）を提供するよう求められる場合もあるとされる。

5.3　クラウド

クラウド・セキュリティについては，前述の通り，2023年度国防権限法（H.R.7900）において，「FedRAMP認可法（Federal Risk and Authorization Management Program (FedRAMP) Authorization Act）」（H.R.8956[83] / S.3099[84]）が成立している。これは，連邦行政機関が安全なクラウド技術を導入しやすくするためのものである。FedRAMPプログラムは，連邦政府機関が安全であると認定されたクラウドサービスを採用するための標準的な方法を提供するために，2011年に創設されたものである。当該プログラムは，従前，議会の正式な認可を得ておらず，議会に対する説明責任を果たしていないとの懸念があった。故に，今回の立法は当該プログラムを５年間承認するもので，議会に対する説明責任を果たし，連邦行政機関によって調達されたクラウド製品の安全性を確保することを目的とする[85]。

６．産業毎の動向

6.1　総説

大統領府は，2022年10月，３つの重要インフラ分野をサイバー規制の対象にした[86]。Biden政権が次に取り組む予定の重要インフラ部門は，通信，水及び医療で，これらの部門のサイバーセキュリティの基準値を引き上げる予定だとする。背景には，東海岸の燃料供給を停止させたコロニアル・パイプラインを標的とした攻撃など[87]，2021年に注目を集めたランサムウェア攻撃があり，ハッカーに対する重要なインフラのセキュリティのギャップを埋めるための政権の最新の一歩となるとする。具体的には，問題意識として，重要インフラ，緊急サービス，情報技術など一部のセクターに対する規制当局があまりないことを指摘している。これを受け，後述の連邦通信委員会，保険福祉省及び環境保護庁の取組みにつながっている。

6.2　通信

○　連邦通信委員会・緊急警報システムに関する規定変更

前述のホワイトハウスの重要インフラに関する政策を受け，連邦通信委員会は，2022年10月，規則制定案通知（notice of proposed rulemaking: NPRM）として全米の緊急警報システム（Emergency Alert System: EAS）および無線緊急警報（wireless emergency alerts: WEA）の運用態勢とセキュリティを強化する新規則を全会一致で提案した[88]。同年8月に，連邦緊急事態管理庁（Federal Emergency Management Agency: FEMA）は，EASの参加者に対し，テレビ，ラジオ，ケーブルネットワークを通じて脅威行為者が警報を発することを可能にする脆弱性が利用される可能性があるとの警告を発していた[89]。

○　Open RANの推進

2022年には，米国はOpen RANを国内的・国際的に推進する動きを見せている。

国内的には，連邦通信委員会の第８期通信セキュリティ・信頼性・相互運用性協議会（CSRIC VIII）の報告書が発表されている。2022年12月には，WG3の「5Gのセキュリティ及び信頼性を促進するために仮想化技術をどのように利用できるか（Report on How Virtualization Technologies Can Be Used to Promote 5G Security and Reliability）」，WG2の「Open RAN技術開発へ至る課題及びその克服の在り方の提言（Report on Challenges to the Development of ORAN Technology and Recommendations on How to Overcome Them）」及びWG6の「WEA性能報告（Report on WEA Performance Reporting）」の報告書が採択された。特にWG3の報告書は，仮想化は小規模な新興企業を含むより幅広い技術企業を包含するところ，安全な仮想化5Gネットワークの導入を促進するためには，従来の通信事業者や機器メーカー以外の関係者と提携すべきと勧告している[90]。

国際的には，2022年５月，日米豪印（クアッド）重要・新興技術作業部会において，「5Gサプライヤの多様化及びOpen RANに関する協力覚書」を策定した。これを受け，４カ国において，Open RANの検証や相互運用性，セキュリティに関する情報共有について，検討がなされている[91]。

また，2022年12月には，オーストラリア，カナダ，英国及び米国が5Gセキュリティにコミットメントを表明している。これは，通信ネットワークのセキュリティ及びレジリエンスを確保することを目的とし，Open RANの原則を

支持している[92)]。

6.3　医療業界

6.3.1　医療機関における自組織の保護

前述のホワイトハウスの重要インフラに関する政策を受け，保健福祉省（Department of Health and Human Services: HHS）は，2022年10月，医療機関のセキュリティ対策に関するガイドラインを発表した[93)]。医療機関のセキュリティ上の義務は医療保険の相互運用性と説明責任に関する法律（Health Insurance Portability and Accountability Act of 1996: HIPAA）に基づいている[94)]。ガイドラインの背景には，2022年に，米国最大の非営利医療システムの１つであるCommonSpirit Healthが，ランサムウェアの攻撃を受け，広範囲にわたって機能停止が発生したことなどがある[95)]。

6.3.2　医療機器のセキュリティ

医療機器の情報セキュリティ対策も進展している。食品医薬品局（Food and Drug Administration: FDA）は，2022年４月，品質システムの考慮事項と市販前申請の内容・業界及び医薬品局スタッフ向けガイダンスの草案を発表した[96)]。これは，その後の2023年９月に最終版が策定されている[97)]。

また，2022年12月に成立した前述の2022年度包括歳出法で，FDAは医療機器メーカーにセキュリティ要件を課す権限が与えられている[98)]。これに基づき，FDAは，2023年３月，ガイドラインを発表し，医療機器メーカーがFDAの承認を得るために，その製品が一定のサイバーセキュリティ基準を満たしていることを証明する必要があると発表した[99)]。

6.4　水道事業／パイプライン

前述のホワイトハウスの重要インフラに関する政策を受け，環境保護庁（Environmental Protection Agency: EPA）は，2022年，水インフラの安全性とセキュリティにサイバーセキュリティを含めるような既存の規制を検討しているとされる[100)]。

他方，運輸保安局（Transportation Security Administration: TSA）も，2022年11月，パイプラインと鉄道部門に対してより恒久的な規則を策定するための規則案の事前通知を発表した[101)]。背景には，昨年のコロニアル・パイプラインの攻撃がある。

また，NISTは，2022年11月，NCCoE水部門プロジェクトチームにおいて上下水道ユーティリティのセキュリティについてプロジェクト説明書案を公表し，一般からの意見を募集した[102)]。

［付記］

本研究は，株式会社KDDI総合研究所招聘研究員の身分としても行ったもので，また，JSPS科研費JP22K13319，旭硝子財団2022年度採択研究助成プログラム及びJSTムーンショット型研究開発事業，JPMJMS2215の助成を受けた。

参考文献

１）辻井重男『情報社会・セキュリティ・倫理』37頁（コロナ社，2012年），JIS Q 13335-1：2006（ISO/IEC 13335-1：2004）・2.11項。

２）情報のCIAの観点から情報セキュリティ法の体系を構築したものとして，参照，岡村久道『情報セキュリティの法律〔改訂版〕』（商事法務，2011年）。この体系を受けて，サプライチェーン・セキュリティの法政策をCIAの観点からマッピングするものとして，橘雄介「米国におけるサイバー・サプライチェーン・セキュリティ政策の動向」情報法制研究９号119頁（2021年）。

３）参照，橘雄介「米国サイバー・サプライチェーン・セキュリティ法政策の動向：第117議会第１会期（2021-2022年）」福岡工業大学総合研究機構研究所所報５号63頁（2022年）［本文①から③の３種類を指摘する］。

４）一般的に参照，橘・前掲注２）119-120頁。

５）NIST, *Cybersecurity Supply Chain Risk Management C-SCRM* (Dec. 12, 2023) https://csrc.nist.gov/projects/cyber-supply-chain-risk-management (last visited Oct. 31, 2023). なお，NISTは以前は“Cyber Supply Chain Risk Management”と呼称していた。*See* NIST, *Cyber Supply Chain Risk Management* (Feb 7, 2017) https://csrc.nist.rip/scrm/ (last visited Oct. 31, 2023). 丸山満彦「NISTに基づくSupply Chain Risk Managementについてのちょっとしたまとめ」（2020年３月１日）http://maruyama-mitsuhiko.cocolog-nifty.com/security/2020/02/post-b44a1c.html（2023年10月31日最終確認）。

６）NIST, *NIST Special Publication 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, 3 (Apr. 2015).

７）IPA「ITサプライチェーンにおける情報セキュリティの責任範囲に関する調査　調査報告書」１頁（2019年）。

８）NIST, *supra* note 6 at 3. 紹介するものとして，橘・前掲注３）120頁。

９）橘・前掲注２）121-122頁。

10）第117議会第１会期（2021-2022年）を調査対象とするものとして，橘・前掲注３）。

11）*See* BLACK'S LAW DICTIONARY (11th ed. Thomson Reuters 2019) at BILL (3).

12）*See* Investopedia, *National Defense Authorization Act (NDAA): How it Works* (Nov. 29, 2022). https://www.investopedia.com/national-defense-authorization-act-5113289 (last visited Oct. 31, 2023).

13）CONGRESS.GOV, *H.R.2471 — Consolidated Appropria-*

tions Act, 2022. https:// www. congress. gov / bill / 117th-congress/house-bill/2471 (last visited Oct. 31, 2023).

14）Public law 117-103.

15）Public Law 117-328, 136 STAT. 4459 (Dec. 29, 2022). 法案は，CONGRESS.GOV，*H.R.2617 ― Consolidated Appropriations Act, 2023*. https://www.congress.gov/bill/117th-congress/house-bill/2617 (last visited Oct. 31, 2023). 要旨として，House Committee of Appropriations, *Consolidated Appropriations Act, 2023: Summary of Appropriations Provisions by Subcommittee*. https://appropriations.house.gov/sites/democrats.appropriations.house.gov/files/FY23%20Summary%20of%20Appropriations%20Provisions.pdf (last visited Oct. 31, 2023). 邦語文献として，田上靖「米国の国防権限法，知財保護法，包括的歳出法等による対中規制強化等の諸動向：2022年12月以降を中心にして」CISTEC journal 204号98頁（2023年）。

16）The White House, *Bill Signed: H.R. 2617* (Dec. 29, 2022). https://www.whitehouse.gov/briefing-room/legislation/2022/12/29/bill-signed-h-r-2617/ (last visited Oct. 31, 2023).

17）Public Law 117-263, 136 Stat. 2395 (Dec. 23, 2022). https:// www. congress. gov / 117 / plaws / publ263 / PLAW-117publ263.pdf (last visited Oct. 31, 2023). *See* Congressional Research Service, *FY2023 NDAA: Summary of Funding Authorizations* (Dec. 30, 2022). https:// crsreports. congress. gov/product/pdf/IN/IN11990?source=email (last visited Oct. 31, 2023); Congressional Research Service, *FY2023 National Defense Authorization Act: Overview of Funding Authorizations* (Dec. 7, 2023). https://news.usni.org/2023/12/08/overview-of-fiscal-year-2023-defense-authorization-act (last visited Oct. 31, 2023). 邦語文献として，田上靖＝久保田慎一「米国国防権限法2023の概要」CISTEC journal 203号72頁（2023年），田上靖「米国防権限法2023の中国半導体製品等米国政府調達等禁止規定（2027年12月施行）の概要」CISTEC journal 203号78頁（2023年），永野秀雄「米国の2023会計年度ジェイムス・M.・インハーフ国防授権法におけるサイバーセキュリティ関連の重要規定とその概要」CISTEC journal 203号84頁（2023年）。

18）CONGRESS. GOV, *H. R. 7900 ― National Defense Authorization Act for Fiscal Year 2023*. https:// www. congress. gov / bill / 117th-congress / house-bill / 7900 / related-bills (last visited Oct. 31, 2023). 同法案の要旨は，House Armed Services Committee, *Summary of the Fiscal Year 2023 National Defense Authorization Act* (2022). https:// democrats-armedservices. house. gov / _cache / files / c / 8 / c891c085-1494-4854-bb28-d145ea24ee99/C2675EB2D76A24A2A90546C41E6E993C. 20220701-fy23ndaa-bill-summary-vfinal. pdf (last visited Oct. 31, 2023). 同法案に対する大統領府の見解は，Office of Management and Budget, *Statement of Administration Policy: H.R. 7900 ― National Defense Authorization Act for Fiscal Year 2023* (Jul. 12, 2022). https://www.whitehouse.gov/wp-content/uploads/2022/07/H.R.-7900-NDAA-SAP.pdf (last visited Oct. 31, 2023).

19）CONGRESS.GOV, *S.4543 ― James M. Inhofe National Defense Authorization Act for Fiscal Year 2023.* https://www.congress.gov/bill/117th-congress/senate-bill/4543 (last visited Oct. 31, 2023). 同法案に対する大統領府の見解は，Office of Management and Budget, *Statement of Administration Policy: S. 4543 ― James M. Inhofe National Defense Authorization Act for Fiscal Year 2023* (Oct. 18, 2022). https://www. whitehouse. gov / wp-content / uploads / 2022 / 10 / S4543-NDAA-SAP.pdf (last visited Oct. 31, 2023).

20）House Armed Services Committee, *Hasc and Sasc Release Text of the FY23 NDAA Agreement* (Dec 6, 2022). https://armedservices.house.gov/news/press-releases/hasc-and-sasc-release-text-fy23-ndaa-agreement (last visited Oct. 31, 2023); Senate Committee on Armed Services, *Sasc and Hasc Release Text of FY23 NDAA Agreement* (Dec 6, 2022). https://www.armed - services. senate. gov / press-releases / sasc - and - hasc - release - text - of - fy23 - ndaa - agreement (last visited Oct. 31, 2023).

21）CONGRESS.GOV, *H.R.7776 ― James M. Inhofe National Defense Authorization Act for Fiscal Year 2023.* https://www.congress.gov/bill/117th-congress/house-bill/7776 (last visited Oct. 31, 2023). 同法案の要旨は，House Armed Services Committee, *FY23 National Defense Authorization Act.* https://armedservices. house. gov / sites / republicans. armedservices. house.gov/files/Final%20FY23%20NDAA%20Conf%20Highlights.pdf (last visited Oct. 31, 2023).

22）House Armed Services Committee, *NDAA ― National Defense Authorization Act*. https://armedservices.house.gov/ndaa (last visited Oct. 31, 2023).

23）The White House, *Press Release: Bill Signed: H.R. 7776* (Dec 23, 2022). https://www.whitehouse.gov/briefing-room/legislation / 2022 / 12 / 23 / press-release-bill-signed-h-r-7776/ (last visited Oct. 31, 2023); The White House, *Statement by the President on H.R. 7776, the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023* (Dec. 23, 2022). https:// www. whitehouse. gov / briefing-room / statements-releases/2022/12/23/statement-by-the-president-on-h-r-7776-the-james-m-inhofe-national-defense-authorization-act-for-fiscal-year-2023/ (last visited Oct. 31, 2023).

24）Senate Committee on Armed Services, *supra* note 20. CMMC について，参照，永野秀雄「米国国防総省により公表されたサイバーセキュリティ成熟度モデル認証（CMMC）2.0規則案の概要」CISTEC journal 201号294頁（2022年）。

25）Senate Committee on Armed Services, *supra* note 20.

26）*Id.*

27）橘・前掲注２）124-125頁。

28）NIST, *NIST, Pre Call of Comments: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (July 19, 2022). https://csrc.nist.gov/publications/detail/sp/800-171/rev-3/draft (last visited Oct. 31, 2023).

29）NIST, *NIST SP 800-161 Rev. 1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (May 2022) https://csrc.nist.gov/pubs/sp/800/161/r1/final (last visited Oct. 31, 2023); NIST, *NIST Updates Cybersecurity Guidance for Supply Chain Risk Management: The publication's revisions form part of NIST's response to an executive order regarding cybersecurity* (May 5, 2022) https://www.nist.gov/news-events/news/2022/05/nist-updates-cybersecurity-guidance-supply-chain-risk-management (last visited Oct. 31, 2023). 参照，丸山満彦「NIST SP 800-161 Rev. 1 システムと組織のためのサイバーセキュリティ・サプライチェーン・リスクマネジメントの実践」（2022年５月８日）http://maruyama-mitsuhiko.cocolog-nifty.com/security/2022/05/post-1c7f3e.html（2023年10月31日最終確認）。

30）Executive Order 14028 of May 12, 2021, Improving the Nation's Cybersecurity. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity (last visited Oct. 31, 2023). 参照，橘・前掲注３）65頁。NIST の政策と大統領令との関係について，NIST, *Software Security in Supply Chains* (May 11, 2022) https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains (last visited Oct. 31, 2023).

31）NIST, *New EO Guidance for Cybersecurity Supply Chain Risk Management* (May 5, 2022) https://content.govdelivery.com/accounts/USNIST/bulletins/3165de0 (last visited Oct. 31, 2023).

32）*Id.*

33）ゼロトラストの意義について，*see* NIST, *NIST SP 800-207: Zero Trust Architecture* (Aug. 2020). https://csrc.nist.gov/pubs/sp/800/207/final (last visited Oct. 31, 2023); 経済経産省＝クラウドネイティブ「経済経産省デジタルプラットフォーム構築 事業報告書」（2021年）https://github.com/meti-dx-team/METI-Digital-Tools（2023年10月31日最終確認）。

34）NIST, *supra* note 33.

35）Office of Management and Budget, *M-22-09: Memorandum for the Heads of Executive Departments and Agencies* (Jan. 26, 2022). https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf (Jan. 26, 2022); The White House, *Office of Management and Budget Releases Federal Strategy to Move the U.S. Government Towards a Zero Trust Architecture* (Jan. 26, 2022). https://www.whitehouse.gov/omb/briefing-room/2022/01/26/office-of-management-and-budget-releases-federal-strategy-to-move-the-u-s-government-towards-a-zero-trust-architecture/ (last visited Oct. 31, 2023).

36）Executive Order 14028 of May 12, 2021, *supra* note 30.

37）Department of Defense, *Zero Trust Strategy* (Nov. 7, 2022) https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf (last visited Oct. 31, 2023); Department of Defense, *Department of Defense Releases Zero Trust Strategy and Roadmap* (Nov. 22, 2022). https://www.defense.gov/News/Releases/Release/Article/3225919/department-of-defense-releases-zero-trust-strategy-and-roadmap/ (last visited Oct. 31, 2023). 邦語文献として，まるちゃんの情報セキュリティ気まぐれ日記「米国 国防総省 ゼロトラスト戦略とロードマップ（2022.11.07）」（2022年11月30日）http://maruyama-mitsuhiko.cocolog-nifty.com/security/2022/11/post-995b15.html（2023年10月31日最終確認）。

38）日米欧の直近の政策動向について，参照，経済産業省「経済産業省のサイバーセキュリティ政策について」デジタル庁（2023年９月11日）https://www.digital.go.jp/councils/administrative-research-wg-technology_technology_based_regulatory_reform/9f54b1fb-1a9f4531-85cb-7659f0458a9b（2023年９月14日最終確認）。

39）CONGRESS. GOV, *H. R. 5491 － Securing Systemically Important Critical Infrastructure Act.* https://www.congress.gov/bill/117th-congress/house-bill/5491 (last visited Oct. 31, 2023).

40）Bpi, *BPI and ABA Urge Congress to Oppose Systemically Important Entities Designation in National Defense Authorization Act* (July 29, 2022). https://bpi.com/bpi-and-aba-urge-congress-to-oppose-systemically-important-entities-designation-in-national-defense-authorization-act/ (last visited Oct. 31, 2023). *See* Federal News Network, *CISA establishing 'systemically important entities' office* (Mar. 23, 2023). https://federalnewsnetwork.com/cybersecurity/2023/03/cisa-establishing-systemically-important-entities-office/ (last visited Oct. 31, 2023).

41）CONGRESS. GOV, S. 3600 － Strengthening American Cybersecurity Act of 2022. https://www.congress.gov/bill/117th-congress/senate-bill/3600 (last visited Oct. 31, 2023). 邦語文献として，まるちゃんの情報セキュリティ気まぐれ日記「米国 S.3600 － Strengthening American Cybersecurity Act of 2022 案が上院で可決」（2022年３月６日）http://maruyama-mitsuhiko.cocolog-nifty.com/security/2022/03/post-f0b01b.html（2023年10月31日最終確認），永野秀雄「大統領令第14028号「国家のサイバーセキュリティの向上」に基づき制定された諸規則等及び「2022年重要インフラに関するサイバーインシデント報告法」について」CISTEC Journal 199号272頁（2022年）。

42）CISA, *Guidance on Sharing Cyber Incident Information*

(Apr. 7, 2022) https://www.cisa.gov/uscert/ncas/current-activity/2022/04/07/guidance-sharing-cyber-incident-information (last visited Oct. 31, 2023). 邦語文献として，JCIC「JCIC 海外ニュースクリップ」（2022年４月12日）https://www.j-cic.com/news/20220412.html（2023年10月31日最終確認）。

43）Federal Register, *Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022* (Sep. 12, 2022). https://www.federalregister.gov/documents/2022/09/12/2022-19551/request-for-information-on-the-cyber-incident-reporting-for-critical-infrastructure-act-of-2022 (last visited Oct. 31, 2023); Federal Register, *Cyber Incident Reporting for Critical Infrastructure Act of 2022 Listening Sessions* (Sep. 12, 2022). https://www.federalregister.gov/documents/2022/09/12/2022-19550/cyber-incident-reporting-for-critical-infrastructure-act-of-2022-listening-sessions (last visited 31 Oct. 2023). 邦語文献として，JCIC「JCIC 海外ニュースクリップ」（2022年９月20日）https://www.j-cic.com/news/20220920.html（2023年10月31日最終確認）。

44）一般的に参照，牛窪賢一「サイバーリスクとサイバー保険：米国の動向を中心として」損保総研レポート116号１頁（2016年）https://www.sonposoken.or.jp/media/reports/sonposokenreport116_1.pdf（2023年10月31日最終確認），日本経済新聞「サイバー保険，揺らぎ「戦争時は補償」外証明難しく」（2022年４月16日）https://www.nikkei.com/article/DGXZQOUB143350U2A410C2000000/（2023年10月31日最終確認）。

45）GAO, *Cyberthreats Increase Cyber Insurance Premiums While Reducing Availability* (Jul.19, 2022). https://www.gao.gov/blog/rising-cyberthreats-increase-cyber-insurance-premiums-while-reducing-availability (last visited Oct. 31, 2023).

46）FCC, *FCC Amends Equipment Authorization Program* (Nov 25, 2022). https://www.fcc.gov/document/fcc-amends-equipment-authorization-program (last visited Oct. 31, 2023). 邦語の報道として，日本経済新聞「中国５社の IT 機器，米で事実上販売禁止：ファーウェイなど，ハイテク分離が加速」（2022年11月27日）https://www.nikkei.com/article/DGKKZO66325480X21C22A1EA2000/（2023年10月31日最終確認）。

47）参照，橘・前掲注３）69頁。

48）永野秀雄「米国の防衛調達における“供給者がもたらす脅威の低減（ベンダー脅威緩和：VTM）”とは何か－ベンダー・パーフォーマンス・リスク・システム（SPRS）上の VTM 制度の意味」CISTEC ジャーナル2023年３月号264頁（2023年）。

49）CONGRESS.GOV, H.R.4346 － Chips and Science Act. https://www.congress.gov/bill/117th-congress/house-bill/4346 (last visited Oct. 31, 2023). 要旨は，Senate Commerce Committee, *The CHIPS Act of 2022: Section-by-Section Summary.* https://www.commerce.senate.gov/services/files/592E23A5-B56F-48AE-B4C1-493822686BCB (last visited Oct. 31, 2023).

50）The White House, *FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China* (Aug. 9, 2022). https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/ (last visited Oct. 31, 2023).

51）Public Law 117-167, 136 Stat. 1366 (Aug. 9, 2022). 邦語文献として，塚本宏達＝近藤亮作＝木原慧人アンドリュー「米国半導体補助金をめぐる動向：チップス及び科学法の申請手続と制約上の留意点」長島・大野・常松法律事務所米国最新法律情報86号／国際通商・経済安全保障ニュースレター７号（2023年）https://www.noandt.com/publications/publication20230522-1/（2023年11月６日最終確認）。

52）Frank Pallone, JR., *Pallone on Signing of the CHIPS and Science Act into Law* (Aug. 9, 2022). https://pallone.house.gov/media/press-releases/pallone-signing-chips-and-science-act-law (last visited Oct. 31, 2023).

53）*See* The White House, *FACT SHEET: One Year after the CHIPS and Science Act, Biden-Harris Administration Marks Historic Progress in Bringing Semiconductor Supply Chains Home, Supporting Innovation, and Protecting National Security* (Aug. 9, 2023). https://www.whitehouse.gov/briefing-room/statements-releases/2023/08/09/fact-sheet-one-year-after-the-chips-and-science-act-biden-harris-administration-marks-historic-progress-in-bringing-semiconductor-supply-chains-home-supporting-innovation-and-protecting-nationals/ (last visited Oct. 31, 2023).

54）健全な情報空間からの分析として，一般的に参照，中野淳子＝辰己丈夫「健全な情報空間に資するプラットフォーム規制の在り方とは：TikTok をめぐる欧米の対応の比較から」信学技報 SITE2023-7・40頁（2023年）。

55）CONGRESS.GOV, *S.1143 - No TikTok on Government Devices Act.* https://www.congress.gov/bill/117th-congress/senate-bill/1143 (last visited Oct. 31, 2023).

56）*See supra* note 15 and accompanying text.

57）The White House, *Bill Signed: H.R. 2617* (Dec. 29, 2022). https://www.whitehouse.gov/briefing-room/legislation/2022/12/29/bill-signed-h-r-2617/ (last visited Oct. 31, 2023).

58）*See* Office of Management and Budget, *M-23-13: Memorandum for the Heads of Executive Departments and Agencies* (Feb. 27, 2023). https://www.whitehouse.gov/wp-content/uploads/2023/02/M-23-13-No-TikTok-on-Government-Devices-Implementation-Guidance_final.pdf (last visited Oct. 31, 2023).

59）Josh Hawley, *Hawley Bill to Ban TikTok on Government Devices Passes Senate Unanimously* (Dec. 14, 2022). https://www.hawley.senate.gov/hawley-bill-ban-tiktok-government-devices-passes-senate-unanimously (last visited Oct. 31, 2023).

60）Center for Data Innovation, *Banning TikTok Is the Wrong Way to Address National Security Concerns, Says Center for Data Innovation* (Dec. 13, 2022). https://datainnovation.org/2022/12/banning-tiktok-is-the-wrong-way-to-address-national-security-concerns-says-center-for-data-innovation/ (last visited Oct. 31, 2023).

61）NBC, *Gov. Ricketts banning TikTok on State devices* (Aug. 12, 2020). https://www.nbcnebraskascottsbluff.com/2020/08/12/gov-ricketts-banning-tiktok-on-state-devices/ (last visited Oct. 31, 2023).

62）Executive Order 13942 of August 6, 2020, Federal Register Vol. 85, No. 155 (Aug. 11, 2020). https://www.govinfo.gov/content/pkg/FR-2020-08-11/pdf/2020-17699.pdf (last visited Oct. 31, 2023).

63）Douglas MARLAND, Cosette Rinab, and Alec Chambers, Plaintiffs, v. Donald J. TRUMP, in his official capacity as President of the United States; Wilbur L. Ross, Jr., in his official capacity as Secretary of Commerce; and U. S. Department of Commerce, Defendants., 498 F.Supp.3d 624 (2020); TikTok Inc., et al., Plaintiffs, v. Donald J. TRUMP, President of the United States, et al., Defendants., 507 F.Supp. 3d 92 (2020). *See* Congressional Research Service, *Restricting TikTok (Part I): Legal History and Background* (Sep. 28, 2023). https://crsreports.congress.gov/product/pdf/LSB/LSB10940 (last visited Oct. 31, 2023).

64）The White House, *Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries* (Jun. 9, 2021). https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/ (last visited Oct. 31, 2023).

65）The New York Times, *Biden Revokes and Replaces Trump Order That Banned TikTok* (Jun. 9, 2021). https://www.nytimes.com/2021/06/09/us/politics/biden-tiktok-ban-trump.html (last visited Oct. 31, 2023). なお，その後，省庁間の対米外国投資委員会（Committee on Foreign Investments in the United States: CFIUS）が TikTok の売却を親会社に要請している。参照，BBC「米政府，TikTok の売却を親会社に要求　応じなければ禁止も」（2023年３月17日）https://www.bbc.com/japanese/64985931（2023年10月31日最終確認）。

66）Complaint, Cause No. 02D03-2212-PL-401 (Dec. 7, 2022). https://indianacitizen.org/wp-content/uploads/2023/10/original-complaint.pdf (last visited Oct. 31, 2023). *See* nwi, *Indiana attorney general asks court to tell TikTok time's up* (Dec. 8, 2022). https://www.nwitimes.com/business/technology/indiana-attorney-general-asks-court-to-tell-tiktok-times-up/article_7a6a9aab-b708-5280-9178-a06cf7a97cb4.html?utm_campaign=snd-autopilot&utm_medium=social&utm_source=facebook_Northwest_Indiana_Uncovered&fbclid=IwAR1UxM36wezn-q2npivxFyulcGgxcfAalmnkYzbZOm0Oq_ysQSIptrqcYkw (last visited Oct. 31, 2023).

67）Department of Justice, *CEO of Dozens of Companies and Entities Charged in Scheme to Traffic an Estimated $1 Billion in Fraudulent and Counterfeit Cisco Networking Equipment* (Jul. 8, 2022). https://www.justice.gov/opa/pr/ceo-dozens-companies-and-entities-charged-scheme-traffic-estimated-1-billion-fraudulent-and (last visited Oct. 31, 2023).

68）*Id.*

69）BIS, *Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC)* (Oct. 7, 2022). https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3158-2022-10-07-bis-press-release-advanced-computing-and-semiconductor-manufacturing-controls-final/file (last visited Oct. 31, 2023).

70）日本経済新聞「米国，対中半導体規制に追随求める　日本など同盟国に」（2022年11月１日）https://www.nikkei.com/article/DGXZQOGN280H80Y2A021C2000000/?n_cid=BMTR2P001_202211011700（2022年11月１日最終確認）。

71）日本経済新聞「先端半導体の対中輸出規制へ　政府が導入調整，日米協調」（2023年１月28日）https://www.nikkei.com/article/DGXZQOUA27A530X20C23A1000000/?n_cid=BMTR2P001_202301281903（2023年10月31日最終確認）。

72）日本経済新聞「先端半導体の輸出規制，７月23日施行　経産省が省令改正」（2023年５月23日）https://www.nikkei.com/article/DGXZQOUA233FD0T20C23A5000000/（2023年10月31日最終確認）。

73）CONGRESS.GOV, *H.R.9490 - NETWORKS Act.* https://www.congress.gov/bill/117th-congress/house-bill/9490 (last visited 31 Oct. 2023). *See* Gallagher, Colleagues Introduce Bipartisan Bill to Freeze Huawei from U.S. Financial System (Dec. 14, 2022). https://gallagher.house.gov/media/press-releases/gallagher-colleagues-introduce-bipartisan-bill-freeze-huawei-us-financial (last visited Oct. 31, 2023).

74）CONGRESS.GOV, *H.R.9508 - ANTI-SOCIAL CCP Act.* https://www.congress.gov/bill/117th-congress/house-bill/9508?s=1&r=76 (last visited Oct. 31, 2023). *See* Marco Rubio and Mike Gallagher, *TikTok, time's up. The app should be banned in America,* the Washington Post (Nov. 10, 2022). https://www.washingtonpost.com/opinions/2022/11/10/marco-rubio-ban-tiktok-america-china-mike-gallagher/ (last visited Oct. 31, 2023).

75）China Telecom (Ams.) Corp. v. FCC, No. 21-1233 (D.C. Cir. Dec. 20, 2022). *See* FCC, *Chairwoman Rosenworcel Statement on China Telecom D.C. Circuit Court of Appeals Decision* (Dec. 20, 2022). https://docs.fcc.gov/public/attachments/DOC-390320A1.pdf (last visited Oct. 31, 2023).

76）ICT 製品一般について，近時の日本のサイバーセキュリティ政策として，総務省・サイバーセキュリティタスクフォース「ICT サイバーセキュリティ総合対策 2021」（2021年）https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00192.html（2023年９月14日最終確認），同「同 2022」（2022年）https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00142.html（2023年９月14日最終確認），同「同 2023」（2023年）https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/01cyber01_02000001_00172.html（2023年９月14日最終確認）。

77）GAO, *Critical Infrastructure: Actions Needed to Better Secure Internet-Connected Devices*, GAO-23-105327 (Dec. 1, 2022). https://www.gao.gov/products/gao-23-105327 (last visited Oct. 31, 2023).

78）参照，橘・前掲注３）66頁。

79）CSRB, *Review of the December: 2021 Log4j Event* (Jul. 11, 2022) https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf (last visited Oct. 31, 2023).

80）Cyber Safety Review Board (CSRB). https://www.cisa.gov/resources-tools/groups/cyber-safety-review-board-csrb (last visited Oct. 31, 2023).

81）CSRB, *supra* note 79, at v-vi.

82）The White House, *Enhancing the Security of the Software Supply Chain to Deliver a Secure Government Experience* (Sep. 14, 2022). https://www.whitehouse.gov/omb/briefing-room/2022/09/14/enhancing-the-security-of-the-software-supply-chain-to-deliver-a-secure-government-experience/ (last visited Oct. 31, 2023); Office of Management and Budget, *M-22-18: Memorandum for the Heads of Executive Departments and Agencies* (Sep. 14, 2022). https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf (last visited Oct. 31, 2023). 邦語文献として，まるちゃんの情報セキュリティ気まぐれ日記「米国 行政管理予算局（OMB）ソフトウェアサプライチェーンのセキュリティ強化を公表」（2022年９月18日）http://maruyama-mitsuhiko.cocolog-nifty.com/security/2022/09/post-645320.html（2023年10月31日最終確認）。

83）CONGRESS.GOV, *H.R.8956 - FedRAMP Authorization Act.* https://www.congress.gov/bill/117th-congress/house-bill/8956 (last visited Oct. 31, 2023).

84）CONGRESS.GOV, *S.3099 - Federal Secure Cloud Improvement and Jobs Act of 2021.* https://www.congress.gov/bill/117th-congress/senate-bill/3099/related-bills (last visited Oct. 31, 2023).

85）Gary Peters, *Peters Bipartisan Bill to Ensure Federal Agencies Can Quickly and Securely Adopt Cloud Technology Advances in Senate* (Dec. 15, 2021). https://www.peters.senate.gov/newsroom/press-releases/peters-bipartisan-bill-to-ensure-federal-agencies-can-quickly-and-securely-adopt-cloud-technology-advances-in-senate (last visited Oct. 31, 2023).

86）The White House, *FACT SHEET: Biden-Harris Administration Delivers on Strengthening America's Cybersecurity* (Oct. 11, 2022). https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/11/fact-sheet-biden-harris-administration-delivers-on-strengthening-americas-cybersecurity/ (last visited Oct. 31, 2023). *See* The Record, *White House targets 3 critical infrastructure sectors for new cyber regulations* (Oct. 13, 2022). https://therecord.media/white-house-targets-3-critical-infrastructure-sectors-for-new-cyber-regulations?utm_medium=email&_hsmi=229682872&_hsenc=p2ANqtz--9WVVk4iBcc3Vlo4kaR2y8h5RCetjAmgvmF6Rf3FPHgKX0cPp8ziDKpw2LpRqa4zX5TxnxUNvXqIiMllVrojfcQHnEJg&utm_content=229682872&utm_source=hs_email (last visited Oct. 31, 2023).

87）参照，橘・前掲注３）70頁。

88）FCC, *FCC Acts to Strengthen the Security of Nation's Alerting Systems* (Oct. 27, 2022). https://www.fcc.gov/document/fcc-acts-strengthen-security-nations-alerting-systems (last visited Oct. 31, 2023).

89）The Record, *FCC proposes cybersecurity changes to emergency alert system* (Sep. 9, 2022). https://therecord.media/fcc-proposes-cybersecurity-changes-to-emergency-alert-system (last visited Oct. 31, 2023).

90）FCC, *Communications Security, Reliability, and Interoperability Council VIII Meeting* (Dec. 15, 2022). https://www.fcc.gov/news-events/events/2022/12/communications-security-reliability-and-interoperability-council-viii (last visited Oct. 31, 2023); FCC, Communications Security, Reliability, and Interoperability Council VIII. https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-1 (last visited Oct. 31, 2023).

91）その後，覚書の成果として，2023年５月に報告書が公表されている。これは，「Open RAN のセキュリティに対する関心が高まる中，実証試験を含む客観的な調査・分析を通じて，従来の一括調達型の RAN と比較した場合における Open RAN の優位性，及び課題の克服可能性を評価した」ものだとされる。総務省「日米豪印『オープン RAN セキュリティ報告書』の公表」（2023年５月20日）https://www.soumu.go.jp/menu_news/s-news/01tsu

shin06_02000270.html（2023年10月31日最終確認）。

92）GOV.UK, *Australia, Canada and USA sign up to UK's vision for a stronger 5G supply chain* (Dec. 8, 2022). https://www.gov.uk/government/news/australia-canada-and-usa-sign-up-to-uks-vision-for-a-stronger-5g-supply-chain (last visited Oct. 31, 2023).

93）HHS, *October 2022 OCR Cybersecurity Newsletter: HIPAA Security Rule Security Incident Procedures* (Oct. 25, 2022). https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-october-2022/index.html#ftn1 (last visited Oct. 31, 2023). 邦語文献として，デロイトトマーツ「米国保健福祉省がセキュリティインシデント対応手順指針を公表」（2022年11月16日）https://www2.deloitte.com/jp/ja/pages/risk/articles/cr/global-cybersecurity-news-168.html（2023年10月31日最終確認）。

94）Public Law 104-191, 110 Stat. 1936 (1996). 邦語文献として，内橋七海「医療機関におけるセキュリティインシデント事例と求められるセキュリティ対応」NRI セキュアブログ（2022年10月14日）https://www.nri-secure.co.jp/blog/medical-institution-security-incident（2023年10月31日最終確認）。

95）*See* The Record, *CommonSpirit confirms ransomware attack as U.S. hospitals deal with fallout* (Oct. 13, 2022). https://therecord.media/commonspirit-confirms-ransomware-attack-as-u-s-hospitals-deal-with-fallout (last visited Oct. 31, 2023).

96）邦語文献として，まるちゃんの情報セキュリティ気まぐれ日記「米国 食品医薬品局（FDA）医療機器におけるサイバーセキュリティ：品質システムに関する考察と市販前申請の内容：産業界と食品医薬品局スタッフのためのガイダンス（案）」（2022年４月15日）http://maruyama-mitsuhiko.cocolog-nifty.com/security/2022/04/post-2cab09.html（2023年10月31日最終確認）。

97）FDA, *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Guidance for Industry and Food and Drug Administration Staff* (Sep. 2023). https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions (last visited Oct. 31, 2023).

98）*See* The Record, *FDA can now reject new medical devices over cyber standards* (Mar. 30, 2023). https://therecord.media/fda-medical-device-cyber-standards?utm_medium=email&_hsmi=252324456&_hsenc=p2ANqtz-_abApQrsX3hkA6tWjXgukPE1L7qj-Y_7C7UUkxviTt6vr-pMu6Wtcx0SQtOdHW9K0wNMEJfLrkFAQtTtu7y6Hn3G587A&utm_content=252324456&utm_source=hs_email (last visited Oct. 31, 2023). 邦語文献として，デロイトトマーツ「米国議会が医療機器サイバーセキュリティ強化法案を上程」（2022年４月19日）https://www2.deloitte.com/jp/ja/pages/risk/articles/cr/global-cybersecurity-news-154.html（2023年10月31日最終確認）。

99）Federal Register, *Cybersecurity in Medical Devices: Refuse To Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act; Guidance for Industry and Food and Drug Administration Staff; Availability* (Mar. 30, 2023) https://www.federalregister.gov/documents/2023/03/30/2023-06646/cybersecurity-in-medical-devices-refuse-to-accept-policy-for-cyber-devices-and-related-systems-under (last visited Oct. 31, 2023); . 邦語文献として，メディカルオンライン「修正 FD&C 法第524B 条「医療機器のサイバーセキュリティ確保」条項発効後の扱いについて」（2023年３月30日）https://www.medicalonline.jp/fda/detail?id=8655（2023年10月31日最終確認）。

100）The Record, *supra* note 86.

101）Federal Register, *Enhancing Surface Cyber Risk Management* (Nov. 30, 2022). https://www.federalregister.gov/documents/2022/11/30/2022-25941/enhancing-surface-cyber-risk-management (last visited Oct. 31, 2023).

102）NIST, *Securing Water and Wastewater Utilities: Cybersecurity for the Water and Wastewater Systems Sector* (Nov. 2, 2022) https://csrc.nist.gov/pubs/pd/2022/11/02/securing-water-and-wastewater-utilities/ipd (last visited Oct. 31, 2023). 邦語文献として，まるちゃんの情報セキュリティ気まぐれ日記「NIST ホワイトペーパー（ドラフト）【プロジェクト概要】上下水道事業の安全確保：上下水道システムセクターのためのサイバーセキュリティ」（2022年11月6日）http://maruyama-mitsuhiko.cocolog-nifty.com/security/2022/11/post-cdbe28.html（2023年10月31日最終確認）。