調査報告書

平成 29 年度サイバーセキュリティ経済基盤構築事業
（米国から見た諸外国のサイバー空間における能力等の実態に関する調査）

平成 30 年 3 月

株式会社アイ・ビー・ティ

目次

1. 米国の政府内組織間連携、官民連携の実態

1.1. サイバー攻撃情報の収集・分析・共有を担う主体と官官・官民連携等

1.1.1. 主な関係省庁とその連携等の概要

米国では、サイバーセキュリティに対する責任は、NSC（国家安全保障会議）、DHS（国土安全保障省）、DOJ（司法省）、DoD（国防省）のインテリジェンス機関であるNSA（国家安全保障局）、ODNI（国家諜報長官官房）とFBI、米国軍のサイバー軍（Cyber Command）などを含む連邦省庁全般に及んでいる。物理的かつ仮想的な安全保障に関係する連邦省庁の主な役割と責任は次の通りである[1]。

- 国土安全保障省（DHS）：ホームランドセキュリティ（国土安全保障）の法定責任を持つ連邦省庁。主な任務は次の5つである。
  - テロリズムを防止することとセキュリティを強化すること。
  - 米国の国境を保安・管理すること。
  - 移民法を執行・管理すること。
  - サイバースペースと重要インフラを強化すること。
  - 国の災害に対する備えとレジリエンスを強化すること。
- 司法省（DOJ）：連邦犯罪の告訴に責任を持つ司法省のトップである司法長官の主たる責任は米国内におけるテロ行為または脅威ならびに諜報活動などにある。司法省は一般的にはFBI（連邦捜査局）を通じて他省庁との協力で、国家安全保障の防護活動にあたり、テロリストの脅威またはインシデントを検知・防御・先占・阻止する法執行機関の活動を調整する。
  - 緊急事態連邦法執行支援法（EFLEA：Emergency Federal Law Enforcement Assistance Act）に基づいて、司法省は州知事による人事やその他の支援の要請を承認する。
  - 司法省は国家健康セキュリティ戦略をサポートし、「全米軽減フレームワーク（NMF- National Mitigation Framework)」に基づいて導入された（リスク）軽減フレームワーク指導グループ（MitFLG）のメンバーとなっている。加えて、司法省は緊急支援機能#13（公共の安心安全）も担う。
  - FBI（連邦捜査局）の任務は、1)テロリストと外国インテリジェンスの脅威に対して米国を防護・防御すること、2)米国の犯罪法を護り、執行すること、3)連邦省庁や州地方政府および外国の省庁やパートナーに対する指導と刑事司法サ

[1] DHS, The 2014 Quadrennial Homeland Security Review, June 2014
APPENDIX A: HOMELAND SECURITY ROLES AND RESPONSIBILITIES

ービスを提供することなどである。

- 共同テロタスクフォース（Joint Terrorism Task Forces）を通じて、FBIはテロリスの活動またはテロ活動準備行動等の疑惑活動報告の受取と解決に対する主たる責任を持つ。
- FBI長官でもある司法長官は米国内における大量破壊兵器の捜索・発見・不活性化の責任を持つ。
- 省庁間連携で構成される国家サイバー捜査共同タスクフォース（National Cyber Investigative Joint Task Force）作戦の指揮を執る。

❍ 国務省（State）：外交を担う省庁で、大統領の外交政策の諮問機関である。国際社会における米国の国土安全保障目標と利益の推進を主目的とし、他省庁の対外活動も支援する。国家安全保障では、主に「国家健康安全保障戦略（National Health Security Strategy）をサポートし、国家レスポンスフレームワークに基づく国際協力の結節エージェントでもある。

❍ 国防省（DoD）：外部の脅威と侵略に対して、米国の国民および領土ならびに重要防衛インフラを防護することを主な任務とする。具体的には、1)対外サイバー脅威諜報情報を収集すること、2)国家安全保障及び軍事サービスを確保すること、3)国家サイバーインシデントの防護・防止・回復をサポートすること、4)サイバー犯罪を調査するなどの活動を行っている。加えて、イベントに効果的に対応する州政府・地方政府（SLTT）等の能力が圧倒される場合、国防長官または大統領の指図で米国内の部外機関（Civil Authorities）を支援する。DHS は DoD と連携し、プライバシー保護やその他の市民の自由を防護するセキュアでレジリエントなサーバースペースを育み、国家安全保障と公共衛生と安全の維持に努めている。

米国の連邦省庁とクリティカルインフラストラクチュア（エネルギー、交通・運輸システム、通信、金融サービス等）に対するテロリスト等のサイバー攻撃の増大に伴い、連邦各省庁と重要インフラのサイバー情報システム及び電子データを防御するための安全保障措置（「サイバー重要インフラ防護」と称されている）が極めて重大な懸案事項となっている。米国では、1997年に連邦サイバーアセットがハイリスクリストに盛り込まれ、さらに2003年にはサイバー重要インフラ防護を含むハイリスク分野を拡充し、2015年には連邦政府機関及び非連邦機関等によって収集・保管・共有されるPII（personally identifiable information ：個人のものと特定される情報）のプライバシー防護に関する政策措置も講じられた。しかしながら、米国では今もなお連邦情報システムと政府データのセキュリティ改善を目指して何千件もの改善提案が行われている。特にGAO（連邦政府説明責任庁または米国会計検査院）では、2,500件の改善提言を行っている。連邦省庁およびその外部委託先等に対して情報セキュリティ対策の実施を義務づけた2002年制定のFISMA（連邦情報セキュリティマネジメント法）と2014年改訂FISMAでは、PIIの遵守も含めた連邦省庁の改善対

策を求めているものの、サイバーセキュリティ先進国の米国ですら、1,000件を超えるGAO提案がいまだ導入・実施されていないのが実態である[2]。

以上を踏まえつつ、本調査では、特に政府内組織間、官民、民間同士の連携体制に注目し、米国における国内外のサイバー攻撃に関連する情報の収集、分析、共有に関する調査を実施した。

1.1.2. PPD-41 によるサイバーインシデントレスポンス関係省庁の役割明確化

2014年11月のSony Pictures Entertainmentに対する極めて異常な壊滅的ハッカー攻撃（FBIは北朝鮮のバックアップだと非難）を受けて、オバマ政権はサイバー攻撃に対する応戦（レスポンス）をトップアジェンダとし、2016年7月26日に「PPD-41（大統領政策指令第41号：米国サイバーインシデント調整[3]）」を発動し、DHS（国土安全保障省）、DOJ（司法省）及びFBIなどの連邦省庁とその関係機関の責任と役割を明確にした。

加えて、トランプ大統領は2017年3月末に2015年4月1日に発動された「E.O.13694（著しく悪意のあるサイバー可能活動に関与する特定.人物の資産を凍結する大統領行政命令[4]）」をさらに1年間の延長を行うことを決めた。この行政命令（EO）は、米国における重大なサイバー攻撃とサイバー犯罪に関与した人物と組織に対する制裁を科す権限を連邦政府に認めたものである。このアクションは、トランプ政権がサイバーセキュリティ関連の政策として初めて講じた措置であることから、トランプ大統領は2017年を通じてサイバーセキュリティ対策についてはオバマ政権の後半の政策を踏襲する構えだったとみられる。複数の情報筋によると、サイバーセキュリティ関連の政策に関しては、複数の提案があったものの、トランプ大統領はどれにも署名をしていない。その理由は明らかではない[5]。

- 他方、トランプ大統領は2017年5月11日に同政権初のEO（連邦ネットワーク及び重要インフラのサイバーセキュリティを強化する大統領行政命令[6]）に署名した。トラン

---

2 https://www.gao.gov/highrisk/ensuring_the_security_federal_government_information_systems/why_did_study

3 Presidential Policy Directive 41 (PPD-41): United States Cyber Incident Coordination https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

4 https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf

5 https://www.csoonline.com/article/3186572/government/trump-extends-obama-executive-order-on-cyberattacks.html

6 https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

プ政権誕生後、サイバーセキュリティ行政命令の発動に何故これほどの時間を要したのかが専門家の間で疑問視されている。加えて、本行政命令は、1)機微なデータや個人情報の流出等や外国のハッカー攻撃で脆弱性を露呈する連邦省庁のネットワークセキュリティ強化、2)エネルギーグリッドや金融セクターなどの重要インフラを巧妙なサイバー攻撃から守る能力の強化、3)連邦省庁の説明責任の明確化と強化などを強調している。実際、トランプ政権初の行政命令はオバマ政権のサイバーセキュリティ強化を連邦省庁に徹底することを目指したものであるとも解釈できる[7]。一方、トランプ政権は前政権の政策を前進させるために新国家サイバーセキュリティ戦略の策定にとりかかっているとの情報[8]も流れているものの、2018年1月12日現在、その確実な内容は明らかになっていない。

したがって、本調査の課題であるサイバー攻撃に関係する情報の収集と分析を行う連邦政府の主体については、サイバーインシデントに関係する連邦省庁の責任と役割を定めた2016年7月26日の「PPD-41（大統領政策指令第41号：米国サイバーインシデント調整[9]）」を踏まえて、下記の通り、主な連邦省庁の役割と責任を整理したい[10]。

サイバーインシデントの調整政策であるPPD-41では、重大なサイバーインシデントに効果的に応戦（レスポンス）する連邦省庁の活動を調整するアーキテクチュアを描き、1）国家政策調整（主務官庁はサイバーレスポンスグループ）、2)国家作戦調整（主務官庁はサイバー統合調整グループ）、3)フィールドレベル調整の3つの方法を講じることを決めた。

- 国家政策調整の主務官庁であるサイバーレスポンスグループ（CRG）
  - NSC（国家安全保障会議）内に国土安全保障反テロ大統領補佐官（APHSCT）に対する責任を担う「サイバーレスポンスグループ（CRG)」を創設する。
  - この CRG チームは重大なサイバーインシデントに関する米国政府の政策と戦略を策定・実施することを調整する。
  - 加えて、サイバーレスポンスグループ（CRG）は重大なサイバーインシデントに

7
https://www.reuters.com/article/us-usa-trump-cyber/trump-signs-order-aimed-at-upgrading-government-cyber-defenses-idUSKBN1872L9
8
http://www.washingtonexaminer.com/cybersecurity-is-featured-prominently-in-trumps-new-national-security-strategy/article/2644056
https://www.cyberscoop.com/tom-bossert-white-house-cybersecurity-strategy/
9 Presidential Policy Directive 41 (PPD-41): United States Cyber Incident Coordination
https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
10
https://federalnewsradio.com/cybersecurity/2016/07/white-house-clarifies-agencies-roles-responding-major-cyber-attacks/

関するブリーフィング情報を受け取り、反テロ担当官僚と連携し、重大なサイバーインシデントレスポンスを検討し、当該インシデントに係るパブリックコミュニケーションを開発する。

- CRG（サイバーレスポンスグループ）は、DOD、DoD, DOJ, DOC, DOE, DHS の NPPD（国家防護計画直)、シークレットサービス、米国統合参謀本部(US Joint Chiefs of Staff)、ODNI（国家情報長官室)、FBI、CIA、NSA（国家安全保障局）などの幹部（Senior Level Officials）との調整を主導する。その他の関係省庁は必要に応じて CRG への参加が要請される。
- CRG（サイバーレスポンスグループ）の議長は国土安全保障反テロ大統領補佐官（APHSCT と国家安全保障担当大統領補佐官(Deputy National Security Advisor)である。

- NSC（国家安全保障会議）または CRG（サイバーレスポンスグループ）は必要に応じて、重大なサイバーインシデントに対応する連邦省庁間および官民の調整を行う「サイバーUCG（サイバー統合調整グループ：Cyber Unified Coordination Groups)」を創設し、国家作戦調整を担う。
  - サイバーUCG（サイバー統合調整グループ）は、NIPP（国家インフラ防護計画）の中で DHS が特定した 16 の重要インフラの 1 つ以上の所有者・運転者に影響を及ぼすサイバーイベントを踏まえて創設する。
  - 特にサイバーUCG（Unified Coordination Groups）はレスポンスと回復の努力プログラムの開発と実行を監督し、サイバーUCG 参加者間の情報とインテリジェンスの共有を促し、影響を受けるステークホルダーと一般大衆とレスポンス及びリカバリ計画に関する話し合いを行う。
  - サイバーUCG の構成メンバーは、脅威レスポンスの主務官庁である FBI と NCITF（NATO Crpto Interoperability Task Force)、アセットレスポンスの主務官庁である国土安全保障省(DHS)CS&C(サイバーセキュリティ通信オフィス)の NCCIS（National Cybersecurity and Communications Integration Center)。インテリジェントサポートを担う CTTIC（Cyber Threat Intelligence Integration Center)、関係する SSA（セクター別管轄エージェンシー）である。その他の関係省庁や州政府・地方政府等、国際パートナー、民間セクターなども必要に応じて参加が要請される

以上のサイバーインシデントレスポンスの調整を担う主な新設グループ（CRGとサイバーUCG等）の他にも、次のように主な連邦省庁の役割と責任が明確化された[11]。

- DOJ（司法省)は、FBIならびに傘下のNCIJTF（National Cyber Investigative Joint

[11] https://fas.org/irp/offdocs/ppd/ppd-41.html#2

Task Force：国家サイバー捜査合同タスクフォース）を通じて、切迫したサイバー脅威（immediate cyber threat）に対するレスポンス（応答）を調整する責任を担う。

- DOJは、サイバー脅威による影響を受ける組織の利害関係当事者（ステークホルダー）との連絡を密にし、サイバー脅威に関する証拠とインテリジェンスを収集し、差し迫ったサイバー脅威を阻止する活動と法執行を行い、さらにはDHS（国土安全保障省）内でサイバー脅威情報を共有すると定められた。
  - 換言すると、他省庁連携機関としてのNCIJTF（国家サイバー捜査タスクフォース）の役割は、サイバー脅威捜査をサポートし、そのインテリジェンスと分析結果を関係コミュニティの意思決定者へ提供し、さらに他国におけるサイバー脅威との戦いをサポートする[12]。
  - 加えて、NCIJTFは、米国の情報システムに対してサイバー攻撃を試みる実際のテロリスト・スパイ・犯罪者等を突きとめ、捜査・逮捕することに重点を置く共同活動を実施する。
- 重大なサイバーイベントが発生した際には、FBIがアセットレスポンスチーム、州政府・地方政府等、非政府機関、産業界および必要に応じて他省庁と連携し、「サイバー統合調整グループ（Cyber Unified Coordination Group）」として行動する。つまり、サイバーインシデント応戦（レスポンス）では、FBIが基本的な役割を果たすことをPPD-41は明記している。
  - 「アセットレスポンス」とは、インパクトを受けた情報システムのバッドアクターを見つけて、システム修復を行い、さらに脆弱性にパッチ対処し、将来のインシデント発生のリスクを低減し、インシデントの拡散を阻止することである（DHS長官の解説[13]）。
- CIA等のテロリストの諜報機関を統括するDNI（国家情報長官）は2015年に他省庁連携機関としてCyber Threat Intelligence Integration Center（CTIIC)を創設。CITIIC（サイバー脅威インテリジェンスインテグレーションセンター）の任務は、米国の政策当局のために、米国に対する外国のサイバー脅威および脅威を含むすべてのサイバー脅威を分析し、連邦省庁のインテリジェンス共有能力の開発を監督し、CIAやNSC等の他の省庁からのインテリジェンスを統合化することにある[14]。

- サイバーインシデント情報共有の中核機関であるDHS（国土安全保障省）は、サイバー攻撃の捜査を担うFBIおよびその他の関係省庁と連携し、サイバー攻撃に関する情報

[12] https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force

[13] https://www.dhs.gov/news/2016/07/26/statement-secretary-jeh-c-johnson-regarding-ppd-41-cyber-incident-coordination

[14] https://www.dni.gov/index.php/ctiic-who-we-are

共有（Information Sharing）を促進する。

- オバマ政権2015年2月13日にEO 13691（民間セクターサイバーセキュリティ情報共有）に署名し、国土安全保障省（DHS）に対してISAO（情報共有及び分析組織）の創設を促し、ISAOの標準を開発することや次の事項の実施を要請した。
  - 重要インフラ防護プログラムを通じてISAO（情報共有及び分析組織）のメンバーである民間セクターの個人にクリアランス（機密書類取扱資格）を付与する効果的な手段を開発すること。
  - DHSの官民連携による情報共有分析組織であるNCCIC（国家サイバーセキュリティ通信統合センター）を通じてISAOとの継続的なコラボレーションを推進し、この包括的な調整を行うこと。
  - オープンかつ競争力のあるプロセスを通じてISAOの標準組織となる非政府系組織（主な役割はISAOの創出と機能の標準と指針を特定すること）を選択すること。
  - 民間企業による機密として分類されるサイバーセキュリティ脅威情報にアクセスすることを正当化する機密情報シェアリングの取決めを承認する連邦省庁のリストにDHSを加えた。

- DHS（国土安全保障省）は、物理的かつ仮想的な脅威から米国の重要インフラを防護する責任を担う。DHS 傘下の NCCIC（国家サイバーセキュリティ及び通信インテグレーションセンター）が情報セキュリティに脅威を与えるインシデント情報を収集・分析する中核機関である。

2016 年 7 月の PPD-41（大統領政策指令第 41 号：米国サイバーインシデント調整）が定めるその他のインシデントレスポンスについては、悪意のある活動（Malicious Activity）や機能不全（Malfunction）で国と国民をリスクに晒すサイバーインシデントの発生に際して連邦省庁が担うべき 3 点のレスポンス努力の概要を次のように明らかにした[15]。

- 脅威レスポンス:FBI と NCCIC の NCITF（国家サイバー捜査タスクフォース）がサイバーインシデント発生サイトで法執行と捜査活動を行う。脅威レスポンス努力には、諜報活動による情報収集、問題に結べつけることに関連するインシデント、行為の因果関係を明らかにする帰属などが含まれる。
- アセットレスポンス: NCCIS（国家サイバーセキュリティ通信統合センター）がサイバーインシデントによる影響を受ける法人に対する技術支援を行う。当該支援には、アセット防護、脆弱性の緩和、情報共有の促進などが含まれる。

15 Presidential Policy Directive 41 (PPD-41): United States Cyber Incident Coordination https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

- インテリジェントサポート及び関連活動: 国家情報長官オフィス（ODNI)が「サイバー脅威インテリジェンス統合センター（CTIIC)）を通じて、脅威の状況認識に関する諜報情報を収集し、民間セクターとも共有することが可能な非機密レポートを作成する。

最後に、PPD-41（米国サイバーインシデント調整）は、関係各省庁がサイバーインシデントに効果的かつ効率的に応戦（レスポンス）する能力を強化する目的で 2016 年 7 月から 2～6 ヵ月内で完備すべき複数のタスクの概要を示している。具体的には、次の事例がある。

- CRG（サイバーレスポンスグループ）に参加する連邦省庁は重大なサイバーインシデントを管理するためにリーダーシップ専念、人材、ファシリティおよびプロセスを同時に行える強化された調整手順を 90 日間で確立すること。
- SSA（セクター別管轄省庁）は 90 日間で重大なサイバーインシデントレスポンスを支える調整強化を可能とするセクター別手順書を開発または刷新しなければならない。
- 連邦関係省庁は PPD-41 の教説（Tenet）を“Cyber Guard”や“Cyber Storm”などのサイバーインシデントレスポンス演習に盛り込まなければならない。
- DHS、DOJ、DoD および SSA は 180 日間でサイバーUCG（サイバー統合調整グループ）用の作戦コンセプトを開発しなければならない。DHS、DOJ、DoD および SSA は、重要インフラのサイバーセキュリティリスク問題の解決に取り組む国家サイバーインシデントレスポンス計画を策定しなければならない。同計画には、州政府や地方政府、SCC（セクター調整会議)、ISAO（情報共有分析組織)、重要インフラのオーナー及びオペレータの意見などを盛り込まなければならない。

因みに、PPD 41 の発動に伴い、米国政府は サイバーインシデント深刻度判断基準を公表した。これは、サイバーインシデントの深刻度を測る米国連邦政府共通の枠組み として構築されたもので、レベル 3 以上を重大サイバーインシデントとし、大統領令で定める対応の対象としている[16]。

[16] 内閣府 NISC で作成した資料。
https://www.nisc.go.jp/conference/cs/ciip/dai10/pdf/10shiryou09.pdf

1.2.　DHS とサイバーセキュリティ情報共有

1.2.1.　DHS（国土安全保障省）のサイバー部門

2001 年 11 月 9 日の同時多発テロ事件を受けて、ブッシュ政権は本格的に国土を防護するテロ対策の乗り出し、2002 年 11 月 25 日に可決された「国土安全保障法（Homeland Security Act[17]）」に基づいて「国土安全保障省（DHS）」を創設した。「ホームランドセキュリティ」と通称される国土安全保障省（DHS）は、22 の省庁を再編統合して設置された国防省（DOD）に次ぐ巨大な行政機関である[18]。

国土安全保障省（DHS）は、重要インフラを外部の攻撃から防護し、レジリエンス（強靭性）を高める連邦努力における米国政府の中心的機関である。DHSがその役割を果たすためにはセクター別管轄省庁（SSA）および他の政府機関の参加とその専門知識の活用が不可欠である。DHSはセクター別管轄省庁（SSA）と共に、エネルギーセクター、原子力セクター、防衛産業基盤などのサイバーセキュリティの強化を様々な仕組みを通して行なっているが、下記の通り、主に1)PPP（官民連携）方式と2)国家サイバーセキュリティ通信統合センター（NCCIC）を通じて実施されている。

国土安全保障省（DHS）の主な任務は次の 5 つである[19]。

- テロリズムの防止とセキュリティの強化。
- 米国国境の保安と管理。
- 移民法の執行・管理。
- サイバースペースと重要インフラの強化。
- 国の災害に対する備えとレジリエンスの強化。

上記の 5 大ミッションの中でも、1 番目のテロリズムの防止とセキュリティの強化は、国土安全保障政策の中核となる施策である。重要視するのは、アフガニスタン・パキスタンおよびアラビア半島でのアルカイダ対策とシリアでのアル＝ヌスラ戦線ならびに国内の過激主義者の単独犯のテロ対策などである。1 番目のミッションの具体的な目標とその達成手

17 Public Law 107–296 ：Homeland Security Act of 2002
https://www.dhs.gov/homeland-security-act-2002
18 http://www.dhs.gov/xabout/history/editorial_0133.shtm
19 DHS, The 2014 Quadrennial Homeland Security Review June 2014
https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf

法は次の通りである[20]。

- 目標 1-1：テロ攻撃を防止すること。
  - テロ情報を分析・統合・普及する。
  - 作戦を抑止・中断する。
  - 運輸戦略を強化する。
  - 暴力的な過激主義に対抗する。
- 目標 1-2：化学・バイオ・放射能・核の物質及び能力を米国内において認可を得ないで取得・輸入・移転・利用することを防止・防護すること。
  - 化学・バイオ・放射能・核の新興脅威を予期する。
  - 化学・バイオ・放射能及び核のプリカーサ(前駆物質)及び物質の不正な取得と移動を特定・禁止する。
  - 化学・バイオ・放射能及び核の物質及び兵器の敵対的利用を検出・探知・防止する。
- 目標 1-3：国の重要なインフラとリーダーシップ及びイベントのリスクを軽減すること。
  - テロリズム及び犯罪活動に対する全米の重要インフラのセキュリティを強化する。
  - 重要なカギとなる指導者とファシリティ及び国家特別セキュリティイベントを防護する。

4 番目のミッション（4）は、安心安全なサイバースペースの確保である。DHS は、2014 年から 4 年間のミッション履行でサイバー脅威対策を最重要視した政策展開を行う。主な目標と実施手法は次の通りである。

- 目標 4-1：重要インフラのセキュリティとレジリエンスを強化すること。
  - 重要インフラのリスクに関する情報及びインテリジェンスの交換を向上し、確実にマシーン及びヒトの解釈と仮想化を確保するリアルタイムの状況認識能力を開発する。
  - 重要インフラの所有者・運転者と協力して基本的なサービスと機能の供給を確保する。
  - 重要インフラシステム間の相互依存関係とカスケードインパクト（連続して起こるインパクト）を特定・理解する。
  - 他省庁及び民間セクターと連携し、実効性の高いサイバーセキュリティの政策とベストプラクティスを特定・開発する。
  - 脆弱性を削減し、レジリエントな重要インフラ設計を促進する。

[20] https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf

- 目標 4-2：連邦政府調達の IT 企業をセキュアにすること。
  - サイバー技術の政府調達におけるコスト効果を改善する努力の調整を行う。
  - 文民政府ネットワークをイノベーティブなサイバーセキュリティのツールとプロテクションで装備する。
  - 政府横断的な政策と標準の実施を整合性のある形で効果的に実施し、その効果を確実に評価する。
  - 目標4-3：法執行、インシデント対応ならびにレポーティング能力を向上させる
  - 目標4-4：エコシステムを強化する。

最後の 5 番目のミッション（5）は、国の備えとレジリエンスを強化することである。ハリケーンカトリーナの教訓で連邦政府と州・地方政府等（SLTT）ならびに民間セクターと関係機関の災害計画策定を改善し、迅速な復旧能力を強化した。本ミッション遂行に向けた目標は次の通り。

- 目標 5-1：国の備えを強化すること。
  - 個人とコミュニティに対して自らの備えを強化する権限を与える。
  - すべての災害に対して防御と防護を行い、災害の軽減・対応・回復を行うコア能力を全米規模で構築・維持する。
  - 効果のある継続プログラムを構築する連邦の法人を支援し、当該プログラムを定期的に更新・演習・改善する。
- 目標 5-2：災害と脆弱性リスクを軽減すること。
  - 公民両セクターによるコミュニティ別リスク認識を啓蒙する。
  - 標準、規則、強靭な設計・効果的なリスク軽減および災害リスク削減措置を通じて脆弱性を減少する。
  - 標準と規則の遵守を確定しインシデントを阻止する。
- 目標 5-3：確実に効果のある緊急時対応を行うこと。
  - タイムリーに正確な情報を提供する。
  - 効果のある一体型インシデント対応作戦を行う。
  - タイムリーに適切な災害支援を行う。
  - 確実に実効性の高い緊急時対応を行う。
- 目標 5-4：迅速な復旧を可能とすること。
  - 基本的なサービスと機能の継続性と復旧を確保する。
  - より強固でスマートかつ安全なコミュニティを再構築・維持する。

因みに、重要インフラ防護のセキュリティとレジリエンスの強化対象となるセクターは、

以下の16セクターである。セクター別管轄エージェンシー（SSA）も次の通りである[21]。

【指定重要インフラ防護対象の16セクターとセクター別管轄エージェンシー（SSA)】

指定重要インフラセクター	セクター別管轄官庁（SSA)
商業施設	国土安全保障省（DHS)
化学	国土安全保障省（DHS)
通信	国土安全保障省（DHS)
クリティカル製造	国土安全保障省（DHS)
ダム	国土安全保障省（DHS)
防衛産業基盤	国防省（DOD)
緊急対応サービス	国土安全保障省（DHS)
エネルギー	エネルギー省（DOE)
金融サービス	財務省（DOT)
農業・農業	農業省及び保健福祉省の共管
政府施設	DHSとGSAとの共管
ヘルスケア及び公衆衛生	保健福祉省（HHS)
情報技術（IT)	国土安全保障省（DHS)
原子炉及び核物質・廃棄物	国土安全保障省（DHS)
郵便・配送サービス	国土安全保障省（DHS)
公衆衛生・保健医療	保健福祉省（HHS)
輸送システム	国土安全保障省及び運輸省の共管
水・排水システム	環境保護庁（EPA)

出所： 2013年2月のPPD-21（重要インフラのセキュリティとレジリエンス[22]

1.2.2. NPPD（国家防護計画局）の主な役割と責任

DHS（国土安全保障省）の組織内で、安心安全かつ強靭な重要インフラを防護・強化するミッションを担うのは、NPPD（国家防護計画局: National Protection and Programs Directorate）である。

NPPD（国家防護計画局）のミッション遂行分野は、1)危険な人々と物に対して国の市民と訪問者を防護すること、2)国の物理的インフラを防護すること、3)国のサイバー及び通

21 https://www.dhs.gov/critical-infrastructure-sectors

22 https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

信インフラを防護・強化すること、4)国土安全保障省のリスクマネジメントプラットフォームを強化すること、5)パートナーシップを強化し、さらにコラボレーションと相互運用性を促進することの5つである[23]。NPPD（国家防護計画局）の主な活動内容は次の通りである[24]。

- 数多くのアクション可能なサイバーセキュリティのアラート（注意喚起情報）を一般人と民間部門に発信し、脅威に対する防護を支援。
- 州政府や地方政府の職員と共同で、ニューヨークのタイムズスクウェアでのクリスマスイブのイベントや大統領就任式、スーパーボール等の大規模な集会に備えたセキュリティ計画を策定。
- 化学プラントや電力施設からショッピングモールまでの数多くの施設の所有者・運転者と会い、テロ攻撃と自然災害に伴う潜在的リスクを評価し、されにリスク軽減を支援する等。

NPPD（国家防護計画局）の主な部署は、次の通りである[25]。

- サイバーセキュリティ・通信オフィス（CS&C[26]）：主要ミッションは、国のサイバーインフラ及び通信インフラのセキュリティ・レジリエンス及び信頼性を強化すること。主に次の 5 つの部門を傘下に置く。SSA（セクタ別管轄省庁）として、通信及び情報技術（IT）セクターを担当[27]。
  - Office of Emergency Communications
  - National Cybersecurity and Communications Integration Center (NCCIC)
  - Stakeholder Engagement and Cyber Infrastructure Resilience
  - Federal Network Resilience
  - Network Security Deployment
- インフラ防護オフィス（IP: Office of Infrastructure Protection28）：テロ行為による重要インフラのリスクを軽減する全米の努力を主導する。そうすることで、DHS は備え（Preparedness）のレベルを高め、自然災害あるいはその他の緊急事態の発生に際してこれに対応し、迅速に回復する能力を高めることで重要インフラ（物理的かつ仮想的）を防護する。主な部門は次の 6 つ[29]。

23 Integrity and Accountability in Government: Homeland Security and the Inspector General by Carmen R. Apaza, 2016/05/23
24 https://www.dhs.gov/sites/default/files/publications/nppd-at-a-glance-071614.pdf
25 https://www.dhs.gov/national-protection-and-programs-directorate
26 https://www.dhs.gov/office-cybersecurity-and-communications
27 https://www.dhs.gov/office-cybersecurity-and-communications
28 https://www.dhs.gov/office-infrastructure-protection
29 https://www.dhs.gov/office-infrastructure-protection

- インフラ防護のインフラ情報収集部門オフィス（IICD-Office of Infrastructure Protection’s Infrastructure Information Collection Division）：重要インフラ防護に関する極めて重要な情報を収集・管理する。
- 国家インフラ調整センター（National Infrastructure Coordinating Center）：米国民の安全保障や公共衛生及び公共安全なたびに経済活力の基本となる重要インフラを防護する全米ネットワークの情報および調整のハブ。
- セクターアウトリーチ及びプログラム部門（SOPD）：重要インフラのステークホルダーがそのセキュリティとレジリエンスの強化に向けたミッションを達成する能力を増強するために、SOPD は主なツールやリソースあるいはパートナーシップなどを提供する自発的なパートナーシップを通じて利害関係者を支援する。
- インフラセキュリティコンプライアンス部門（ISCD）：NPPD（国家防護計画局）内の IP オフィスが管轄する部門で、高リスク化学施設のセキュリティを規制する国家プログラムである CFATS（化学施設反テロ標準）の実施に対する責任を持つ。
- インフラ防護の防護セキュリティ調整部門：国家重要インフラ及び主要資産のテロ攻撃または自然災害に対するリスクを軽減するための戦略的調整とフィールドオペレーションを担う。
- 重要インフラセクター：2016 年 11 月現在、米国の 16 セクターが重要インフラ防護の対象として特定されている。

- サイバーインフラ分析オフィス（OCIA: Office of Cyber and Infrastructure Analysis30）：OCIA の任務は、物理的または仮想的な脅威とインシデントによるサービス供給途絶の潜在的な成り行きを評価する全災害型（all-hazards）の総合分析を通じて全米の重要インフラを防護する努力を行う。この分析結果は、重要インフラのセキュリティとレジリエンスの強化ならびに自然災害または人為的災害またはサイバーインシデントなどを強化するための情報として活用する。
  - OCIAの担当室長（Director（室長）は、Brandon Wales。

DHS（国土安全保障省）内の「Operational and Support Components（運用支援部門）」には、上記の「NPPD（国家防護計画）局」の他に、CBP（税関国境警備局）、U.S. Coast Guard（沿岸警備隊）、FEMA（連邦緊急事態管理庁）、HIS（国土安全保障捜査）やERO（退去強制執行部）などで構成されるICE（移民関税執行局）、秘密警察局（シークレットサービス）、FLET（連邦法執行訓練センター）、TSA（運輸保安庁）、科学技術局、DNDO（国内核検知局）、OHA（保健局）、I&A（インテリジェンス＆分析）局等があり、国土安全保障省の創設にあたり、様々な省庁の部署の一部を移管したことが分かる。

30 https://www.dhs.gov/office-cyber-infrastructure-analysis

1.2.3. CISA（サイバーセキュリティ・インフラセキュリティ庁）

2017年のCISA（サイバーセキュリティ・インフラセキュリティ庁）法（H.R. 3359: CISAA[31]）は2017年12月11日に下院を通過した。元の法案は、2002年の国土安全保障法を改正して、NPPD（国家防護計画局）を格上げして、その名称を「CIPA（サイバーセキュリティインフラ防護庁）」に変更することであったが、2017年にCISA（Cybersecurity and Infrastructure Security Agency）法案に改称された。主な狙いは、サイバー脅威と物理的脅威から連邦ネットワークと重要インフラを防護することを任務とするNPPD（国家防護計画局）を政策実施機関へと再編し、新たにCISA（サイバーセキュリティ・インフラセキュリティ庁）として出発させることにある。CISAの長官には米国のサイバーセキュリティ、緊急時通信および重要インフラのセキュリティとレジリエンスを防護・強化する全米努力を主導する国家サイバーセキュリティ・インフラセキュリティ局長が就任することになる[32]。

国家サイバーセキュリティ・インフラセキュリティ局長（Director of Cybersecurity and Infrastructure Security）の主な責務は次の通りである。

(1) CISAのサイバーセキュリティ及び重要インフラセキュリティプログラム、オペレーションおよび関連政策（国家サイバーセキュリティアセットレスポンス活動を含む）を主導すること。
(2) CISAのサイバーセキュリティおよび重要インフラ活動を実施するために、SSA（セクター別所轄官庁）を含む連邦省庁と国際機関を含む非連邦機関の調整活動を履行すること。
(3) 2015年のサイバーセキュリティ法などの法律を遵守し、連邦の情報及び情報システムのセキュリティを確保する責任を履行すること。
(4) 重要インフラリスクに対してセキュリティを確保すること防護することの全米努力を調整すること。
(5) 重要インフラの所有者及び運用者に対して、脅威等の分析結果、知見及びテクニカルアシスタンスなどを提供すること。

元のCIPA法案では、主な部署はサイバーセキュリティ部門、インフラ防護部門、緊急通信部門、連邦防御サービス部門から構成する予定であったが、2017年のCISA（サイバーセキュリティ・インフラセキュリティ庁）法では、次の3部門へと変更された。

---

[31] https://www.gpo.gov/fdsys/pkg/BILLS-115hr3359rfs/pdf/BILLS-115hr3359rfs.pdf

[32] http://www.mondaq.com/unitedstates/x/665426/Security/President+Trump+signs+700B+defense+policy+bill+for+FY+2018

- サイバーセキュリティ部門（Cybersecurity Division）：主な任務は、1)DHSの連邦情報セキュリエティ活動を行い、NCCIC（国家サイバーセキュリティ通信統合センター）の機能を履行することと、2)連邦政府機関以外の法人と連携を取り、自発的な参加を通じたサイバーセキュリティリスクを軽減すること、3)ネットワークと悪性コード分析を行うこと。
- インフラセキュリティ部門（Infrastructure Security Division）：主な任務は、1)米国のハイリスク化学施設の保安確保、2)連邦政府機関以外の法人がテロ攻撃または自然災害による重要インフラに対するリスクを軽減する努力を調整すること、3)適切な重要インフラセクター向けのステークホルダーエンゲージメントメカニズムを運用すること、4)NICC（国家インフラ調整センター）とNCCIC（国家サイバーセキュリティ通信統合センター）を同じところに立地させ、重要インフラ情報を収集・共有し、提言を行うように管理すること。
- 緊急通信部門（Emergency Communications Division）

以上の法案を提出したテキサス州選出の下院議員（共和党）であるMichael T. McCaul（マイケル・マッコール）は下院国土安全保障委員会の委員長である。2015年来で17本のサイバーセキュリティ法案を提出している。2013年の国家サイバーセキュリティ及び重要インフラ防護法の提案者でもある[33]。

[33] https://www.govtrack.us/congress/bills/115/hr3359

1.3.　2015 年 CISA（サイバーセキュリティ情報共有法）と NCCIC

1.3.1.　サイバーセキュリティ情報共有等の推進機関

連邦政府におけるサイバーインシデント情報共有の中核機関は DHS（国土安全保障省）である。HS（国土安全保障省）は、サイバー攻撃の捜査を担う FBI およびその他の関係省庁と連携し、サイバー攻撃に関する情報共有（Information Sharing）を促進すると定められている。サイバーセキュリティ情報共有の根拠法は、2015 年 12 月 18 日に制定された「2015 年サイバーセキュリティ法（Cybersecurity Act of 2015[34]）」である。本法の最も重要な狙いは「タイトル 1」に記載された「2015 年サイバーセキュリティ情報共有法（CISA-Cybersecurity Information Sharing Act of 2015）」である[35]。

CISA(サイバーセキュリティ情報共有法)は、連邦政府機関と民間セクターとの間のサイバーセキュリティに関する官民情報共有メカニズムと民間企業の損害賠償からのセーフハーバー（安全な港となる領域）を定めたものである[36]。

さらに、2015 年の CISA（サイバーセキュリティ情報共有法）は、連邦政府以外の様々な法人が特定情報システムをモニタリングすることとサイバーセキュリティを目的とする防衛的な措置作戦を講じることを認めている。加えて、本法は、連邦省庁におけるサイバーセキュリティ防護の向上、連邦政府のサイバーセキュリティ労働力の評価、重要情報システム及びネットワークのサイバーセキュリティ面の備えの改善措置、CISA（サイバーセキュリティ情報共有法）の施行とその他のサイバー関連問題などを取り扱っている[37]。

2015 年サイバーセキュリティ情報共有法(CISA)の立法化の契機は、1998 年 5 月の PDD-63 で創設を義務づけられた ISAC（情報共有分析センター）の発展で知財権（IPR）や賠償責任（Civil Liability）などの懸念が強まったことにある。このために、オバマ政権 2015 年 2 月 13 日に EO-13691(民間セクターサイバーセキュリティ情報共有に関する大統領行政命令)に署名し、国土安全保障省（DHS）に対して ISAO（情報共有分析センター）の創設を促したのである。

この EO-13691（民間セクターサイバーセキュリティ情報共有）に基づいて民間セクター

34 https://www.justsecurity.org/wp-content/uploads/2015/12/Cybersecurity-Act-of-2015.pdf
35 https://www.us-cert.gov/sites/default/files/ais_files/CISA_FAQs.pdf
36 https://www.congress.gov/bill/114th-congress/senate-bill/754
37 主な解説は次の通り。
http://www.law360.com/articles/745523/a-guide-to-the-cybersecurity-act-of-2015
https://www.lw.com/thoughtLeadership/lw-Cybersecurity-Act-of-2015

内と連邦政府・民間セクター間の情報シェアリングを促す目的で、下院で 2 本、上院で 1 本のよく似たサイバーセキュリティ情報のシェアリング(共有)に関する法案が提議された。主な経緯は以下の通りである。

- 下院は、1)インテリジェンス特別委員会（House Permanent Select Committee on Intelligence）による法案と 2）国土安全保障特別委員会（House Select Committee on Homeland Security）による法案の 2 つの法案を提出し、下院で可決されたが、上院で否決された。
- 他方、上院は上の 2 法案とは別個に上院インテリジェンス特別委員会が提出したサイバーセキュリティ情報共有法案を可決した。
- 3 法案は多くの点で類似しており、いずれの法案もサイバーセキュリティ情報の自発的な共有を促すものであったが、異なる点も多くあった。
- 結果的には、下院の 2 法案に基づいて DHS 内に NCCIC（国家サイバーセキュリティ通信統合センター）や ISAO（情報共有分析組織）等の情報共有関係部門が設置された。
- 他方、上院の法案では情報共有の責任をインテリジェンス関連省庁に与えた。

以上の経緯を経て、3 法案を一本化して 2015 年サイバーセキュリティ法の「タイトル 1：2015 年のサイバーセキュリティ法（CISA)」が成立した。

上記の他に、2015 年サイバーセキュリティ法の中で留意すべき重要なポイントは次の通りである[38]。

- DHS と諜報機関との間の長い期間にわたる主導権争いを経て、DHS、特に DHS の情報共有のハブ拠点である NCCIC（国家サイバーセキュリティ通信統合センター39）が連邦政府と民間企業との間でのサイバーセキュリティ情報の共有のための主たるゲートウェイ（玄関）として選定された。サイバーセキュリティ法に関連して成立した“National Cybersecurity Protection Advancement Act of 2015”により、DHS は、DoD（国防省）と ODNI（国家インテリジェンス長官室）を含む多くの連邦政府機関に対して DHS が受領する情報をリアルタイムまたは作戦可能程度に迅速に送信する自動化システムを構築することを義務づけられた。

国家重要インフラ防護ならびにサイバーセキュリティ対策では、ホームランドセキュリティ（DHS）は、「情報共有（Information Sharing」を必要不可欠と認識し、複数の情報

38 https://www.lw.com/thoughtLeadership/lw-Cybersecurity-Act-of-2015
https://www.sullcrom.com/siteFiles/Publications/SC_Publication_The_Cybersecurity_Act_of_2015.pdf
39 https://www.us-cert.gov/nccic

共有プログラムを開発・実施している。当該プログラムを通じて、DHSは特に大半の重要インフラを所有・運用する民間部門のパートナーとのオーナーおよびオペレータと実質的な情報共有を推し進めてきている。代表的なプログラムは次の通りである[40]。

- NCCIC（国家サイバーセキュリティ・通信統合センター）：DHS における重要インフラの脆弱性・インシデント・リスク緩和の意識啓蒙を目的とする情報共有（シェアリング）のハブ拠点[41]。
  - 国家防護計画（NPPD）局のサイバーセキュリエティ通信オフィス（CS&C）傘下の運用部門で、1 日 24 時間 365 日（24/7）体制でサイバーセキュリティと通信の防護調整役を担っている。
  - NCCIS は、US-CERT や ICS-CERT、NCC（国家通信調整センター）などを管轄。
- CISCP（サイバー情報共有コラボレーションプログラム）：DHS の官民情報共有における旗印となるプログラム。本プログラムを通じて、DHS と参画企業はサイバー脅威、インシデントおよび脆弱性に関する情報シェアを行う。
- ISAO（情報共有分析組織）：政府と民間部門とのサイバーセキュリティ情報を促進する目的で、サイバー脅威に関する情報を収集・分析・拡散する組織。
  - オバマ政権は 2015 年 2 月 13 日に「民間部門のサイバーセキュリティの情報共有を推進すると題した EO 13691（大統領行政命令第 13691 号[42]）」をリリースし、国土安全保障（DHS）長官に対して ISAOs（Information Sharing and Analysis Organizations）の創設を命じる。
  - 本行政命令により、ISAO の組織化とオペレーションを推進する標準と指針を開発するための ISAO 標準組織（ISAO Standards Organization）の創設も認可された。
- ISAC（情報共有分析センター）：1998 年 5 月の PDD-63（大統領決定指令第 63 号）で創設が決まる。セクター別に設置された政府と民間業界との間で重要インフラの脆弱性と脅威に関する情報を共有するための組織。
  - 重要インフラのサイバーセキュリティ情報を集約的に管轄する NCCIS（国家サイバーセキュリティ通信統合センター）がすべての ISAC との調整役となっている。

1.3.2. NCCIC の主な役割等

40 https://www.dhs.gov/topic/cybersecurity-information-sharing
41 https://www.us-cert.gov/nccic
42 Whitehouse, Executive Order -- Promoting Private Sector Cybersecurity Information Sharing https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

DHS 内に 2009 年 10 月 30 日に創設された NCCIC（国家サイバーセキュリティ・通信統合センター）は NPPD（国家防護計画局）CS&C（サイバーセキュリティ通信オフィス）傘下に置かれた[43]。NCCIC は、サイバーセキュリティの備えとサイバーインシデント対応を促進するために、民間部門、市民、法執行機関、情報機関、防衛コミュニティなどが連携するための中核機関として活動している。NCCIC（国家サイバーセキュリティ・通信統合センター）の主な責任と役割は次の通りである[44]。

【NCCIC（国家サイバーセキュリティ・通信統合センター）の任務と活動等】

ビジョン

- 国土と経済の安全保障及び米国人の健康と安全を支えるサイバー及び通信インフラのセキュリティとレジリエンスを確保すること。

上記のビジョンの実現に向けた重点努力

- 国にとってより大きなリスクとなるサイバーリスクとテレコムリスクの防止と軽減などのプロアクティブな活動の調整を重視すること。
- 情報共有と通じてパートナーとのエンゲージメントを拡充・深化することで脅威・脆弱性・インシデントの管理に向けた国民全体の作戦を統合化すること。
- 脅威とそのインパクトに関する情報交換や状況認識ならびに理解を妨げる技術面と機構面の障害を除去すること。
- 国家安全保障上のサイバー及びテレコム関連のすべてのインシデントを迅速かつ効果的に応戦する対策（Readiness）を維持すること。
- サイバー及びテレコムセキュリティ問題の国家エクサレンス知見センター（national center of excellence and expertise）としてステークホルダーの役に立つこと
- 下記の任務履行に際しては、米国人のプライバシーと憲法で保障された権利を守ること。

ミッション(任務)

- 国の重要インフラである情報技術（IT）と通信ネットワークのセキュリティとレジリエンスを著しく損傷する可能性のあるインシデントの発生可能性と深刻度を軽減すること。

主な活動と体制

- NCCICは、1日24時間365日（24/7）体制で、サイバーセキュリティと通信とのインテグレーションの中核拠点として、モニタリングによる状況認識を行い、インシデント対応やサイバー管理センターとして機能する。
- CS&Cは、通信及び情報技術（IT）セクターのセクター別管轄エージェンシーとして、NRF（国家レンスポンスフレームワーク）に準拠する国レベルの報告活動の調整役となっている。
- NCCISは、サイバーセキュリティと通信に関する情報の分析と共有を通じて民間パートナーや一般国民の脆弱性やインシデントおよびリスク緩和の意識啓蒙を行っている。

43 https://www.dhs.gov/news/2009/10/30/new-national-cybersecurity-center-opened
44 https://www.dhs.gov/national-cybersecurity-and-communications-integration-center

❍ NCCICは、US-CERTやICS-CERT、NCC（国家通信調整センター）などを管轄。 主な幹部 ❍ NCCISのトップは、Director（部門長）のJohn Felker：US Coastal Guard(米国沿岸警備隊)でサイバーセキュリティの専門家として活躍し、SCI Consultingやヒューレットパッカード（HP）のサイバーセキュリティの幹部を歴任。

出所：DHSのHP[45]及び関連法令等に基づき、IBTにて作成。

NCCIC（国家サイバーセキュリティ・通信統合センター）の前身は、DHSの旧CS&C（サイバーセキュリティ通信オフィス）の傘下にあったNCSD（国家サイバーセキュリティ部門）である)。NCSD（国家サイバーセキュリティ部門）は、CIAO（重要インフラアシュアランスオフィス)、NIPC（国家インフラ防護センター)、FedCIRC（連邦コンピュータインシデントレスポンスセンター)、NSC（国家通信システム）の機能を再編・統合して誕生した組織であった。その後に任務を果たし、発展的に解散されたが、新しいNCCICとして2009年10月に復活したともいえる。NCCICの傘下の多くの機関は、NCSD（国家サイバーセキュリティ部門）から承継された組織である。

NCSD（国家サイバーセキュリティ部門）を代替する形で2009年に創設されたNCCIC（国家サイバーセキュリティ通信・統合センター）は、「国の重要な情報技術とサイバーインフラに影響を及ぼす脅威とインシデントの問題解決に取り組む全米努力を主導する監視及び警告センター」であり、重要インフラの脆弱性・インシデント・リスク緩和の意識啓蒙を目的とする情報共有（シェアリング）のハブとなり、1日24時間365日体制でオペレーションを行っている[46]。

2014年の国家サイバーセキュリティ及び重要インフラ防護法（National Cybersecurity and Critical Infrastructure Protection Act of 2014[47]）第104条により、NCCISは民生用情報共有のインターフェース（センター）として次の業務を行うと決められた。

- ❍ 連邦省庁横断的にリアルタイムかつ包括的な作戦行動を可能にする状況認識を共有すること。
- ❍ 連邦政府、州政府及び地方政府等、ISAC（情報共有分析センター)、民間法人ならびに重要インフラの所有者・運転者との間でサイバー脅威情報を共有すること。

NCCICは、サイバー脅威の影響を軽減するために、公民のパートナーとの連携に専念して

45 https://www.dhs.gov/national-cybersecurity-and-communications-integration-center
46 https://www.dhs.gov/news/2009/10/30/new-national-cybersecurity-center-opened
47 https://www.congress.gov/bill/113th-congress/house-bill/3696

いる複数のブランチを監督している。サイバーインシデント対応に焦点を当てた2つのNCCICブランチは以下の2つである。

- US-CERTは、連邦機関をサイバーインシデントから防護し、公的・民間企業のサイバー脅威情報を収集・編集して、それを公開して、サイバーインシデントに対応する48。
- ICS-CERTは、公共および民間企業と提携して、サイバーインシデント情報を共有し、サイバーセキュリティ対策を促進することによって、すべての重要インフラセクターのリスクを削減するよう努めている[49]。

さらに、2015年の国家サイバーセキュリティ防護促進法（National Cybersecurity Protection Advancement Act of 2015[50]）では、NCCIC（国家サイバーセキュリティ・通信統合センター）は、非連邦機関の代表の中に部族政府、情報共有分析センターおよび民間法人を含めることを認め、NCCICの拡大業務として次の任務を義務づけられた。

- 州政府および地方政府とサイバーセキュリティのリスクとインシデントに関するコラボレーションを行うこと。
- 情報システムの所有者・運用者に対するタイムリーな情報共有と技術支援を提供するUS-CERT（米国コンピュータ緊急事態対策チーム）を傘下に置くこと。
- 産業制御システムの所有者・運用者との調整を図り、新技術の産業適用と依頼される研修を実施するICS-CERT（産業制御システム緊急事態対策チーム）を傘下に置くこと。
- NCCT（国家テレコム調整センター）を傘下に置くこと。
- 最低1ヵ所のISAC（情報共有分析センター）を傘下に置くこと。
- 州政府および地方政府と連携するための複数州情報共有分析センターを傘下に置くこと。
- 中小企業の調整を行うこと。
- 国際パートナーとグローバルサイバーセキュリティを展開すること。
- 重要インフラセクター横断的な情報共有を実施すること。

2015年1月13日、オバマ大統領はバージニア州アーリントンにあるNCCIS（国家サイバーセキュリティ通信統合センター）を訪問し、24×7（1日24時間・週7日）体制でサイバー状況認識やインシデント対応を行っているNCCICの役割と活動の重要性を強調した。それでも、オバマ大統領は特に官民連携がまだ十分に機能していないと指摘し、1)2015年2

48 https://www.us-cert.gov/about-us
49 https://ics-cert.us-cert.gov/
50 https://www.congress.gov/bill/114th-congress/house-bill/1731

月に発出した官民連携によるサイバーセキュリティ情報を強化する EO 13691（民間セクターサイバーセキュリティ情報共有）と 2)サイバー犯罪法の強化、3)サイバーセキュリティおよび消費者保護等のホワイトハウスサミットの開催などを実施すると発言した[51]。

オバマ大統領によるNCCIC訪問を踏まえて、重大なサイバーインシデントに対応する連邦各省庁の責任を明確にし、サイバーインシデントが発生した際に誰にコンタクトすべきかを明らかにするために、オバマ大統領は2016年7月26日にPPD-41（大統領政策指令第41号：米国サイバーインシデント調整[52]）を発動した。この結果、NCCIS（国家サイバーセキュリティ通信統合センター）がサイバー攻撃の品質を特定するアセットレスポンス（Asset response）の主務官庁兼コンタクト先となった[53]。以上から、NCCIC（国家サイバーセキュリティ通信統合センター）の主たる任務は、重要なICT（情報技術通信）ネットワークのセキュリティとレジリエンスを大きく損傷する可能性のあるインシデントの度合いと深刻度を軽減することである。NICCISは、傘下にUS-CERT（米国コンピュータ緊急準備チーム)とサイバーセキュリティ準備および国家サイバーアラートシステムを持ちサイバーインシデント対応を行っている[54]。

1.3.3. US-CERT（コンピュータ緊急事態対策チーム）等

US-CERT（United States Computer Emergency Readiness Team)は、サイバー犯罪に応戦するためにGSA（一般調達庁）に設置されたFedCIRC（連邦コンピュータインシデントレスポンスセンター）の機能をDHSに移管し、NCSD（国家サイバーセキュリティ部門）の主要業務のひとつとして再編された。NCSDを再再編して2009年に新設されたNCCISは、情報システムの所有者・運用者に対するタイムリーな情報共有と技術支援を提供するUS-CERT（米国コンピュータ緊急事態対策チーム）を傘下に置いた[55]。

官民連携で新設された“US-CERT”の任務と責任は、2003年2月に発出された「国家サイバースペース安全保障戦略」に準拠するもので、1)サイバー攻撃の脅威と脆弱性の分析・

51
https://www.whitehouse.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent

52 Presidential Policy Directive 41 (PPD-41): United States Cyber Incident Coordination
https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

53
https://www.dhs.gov/news/2016/07/26/statement-secretary-jeh-c-johnson-regarding-ppd-41-cyber-incident-coordination

54 http://www.sldinfo.com/the-department-of-homeland-cyber-security-does-it-work/
https://www.dhs.gov/national-cybersecurity-and-communications-integration-center

55 US-CERT: United States Computer Emergency Readiness Team
https://www.us-cert.gov/about-us

削減、2)サイバー警報情報の拡散、3)サイバー攻撃に対する防御と応戦の調整機能であると特定された。因みに、最新の重要なミッションは次の4点である[56]。

- 侵入検知及び阻止能力（intrusion detection and prevention capabilities）の強化を通じて連邦行政機関に対するサイバーセキュリティ防護を供給。
- 連邦省庁、州・地方政府等（SLTT)、重要インフラの所有者及び運転者、民間産業、国際機関に対するタイムリーかつ行動可能な配布情報の開発。
- インシデントレスポンスおよび新興サイバー脅威に関するデータの分析。
- 外国政府および国際機関と連携して、サイバーセキュリティ態勢を強化。

世界中で“CERT”の名がつく組織は250を超えているが、最初に誕生したCERT機関は、カーネギーメロン大学のSEI(Software Engineering Institute)に設置されたCERT® Coordination Center（CERT/CC)である。CERT/CCは、インターネットセキュリティの脆弱性、ネットワークシステムの長期的な変化などを研究し、経済社会のセキュリティ改善の情報提供と研修を行っている。CERT/CCでは、ソフトウェアおよびシステム面のリスク問題の解決にあたり、サイバー攻撃の脅威の通知を行い、世界のベンダーおよびインシデント対応チームと連携し、サイバー脅威の問題解決にあたっている[57]。

US-CERTオペレーションセンターは、リアルタイムのサイバーセキュリティ防護拠点で、国内外の監視・警告センターと連絡をとりあいながら重要なセキュリティ情報の共有を図っている。US-CERTコントロールシステムズセンターは、コントロールシステム利用関連の複雑なセキュリティ問題の解決を図るUS-CERTの戦略的オペレーション部隊である。同センターのWebsiteは、情報システムおよびインフラ防護力を向上させるのに必要な情報を政府、民間セクターおよび一般に提供している。

US-CERT以外にも、NCCIS（国家サイバーセキュリティ通信統合センター）の傘下には、産業制御システムの所有者・運用者との調整を図り、新技術の産業適用と依頼される研修を実施するICS-CERT（産業制御システム緊急事態対策チーム）などがある。

この他にも、国家サイバーレスポンスコーディネーショングループ（NCRCG）が設置された。NCRCGは、13の連邦省庁から構成され、国土安全保障省（DHS）のインシデントマネジメント計画策定チーム（IMPT）メンバー省庁部門のトップ、大統領府などをサポートするとともに、サイバースペースの安全確保、サイバー犯罪の撲滅、重要情報インフラおよび主要資産の防護の任務を担う連邦関連省庁を支援する。NCRCGは、2003年2月の国家サイバ

56 https://www.us-cert.gov/about-us
57 http://www.cert.org/certcc.html

ースペース安全保障戦略のサポート機能を担い、サイバーインシデント対応を行っている。国家的に重大なサイバー関連のインシデントが発生すると、NCRCGはUS-CERTや法施行を含む連邦のサイバーインシデントの準備、応戦および回復、情報共有などの調整を図る。NCRCGは、限定的な期間の突発的なサイバーインシデントおよび段階的にエスカレートするサイバー危機の両面の問題解決を行う[58]。

1.3.4. ISAC（情報共有分析センター）と ISAO（情報共有分析組織）等

【ISAC（情報共有分析センター）】

米国におけるサイバーセキュリティ情報共有メカニズムの中核機関は、各種のISAC（情報共有分析センター）である。ISAC（情報共有分析センター）創設の根拠法は、1998年5月のPDD-63（重要インフラ防護に関する大統領決定指令第63号）である[59]。

ISAC（Information Sharing and Analysis Centers）は、サイバー脅威に関する情報を収集・分析・伝達するために、重要インフラの所有者・運転者により設立された認証法人（trusted entity）である[60]。他方、ISAO（情報共有分析組織）はセクター横断的な情報共有を目指している。

ISAC（情報共有分析センター）は重要インフラのセクター別に設置され、セクター特定組織（SSO）としてサイバー脅威や脆弱性に関する情報共有を推進してきている。ISACは、物理的かつ仮想的な脅威とその緩和に関する情報とベストプラクティスの共有を推進するために重要インフラのオーナー及びオペレータによってセクター別に設置された機関で、NGOであることが多い。大半のISAC（情報共有分析センター）は24時間週7日体制で稼働し、脅威警告やインシデント報告を行う能力を有している。セクター別ISACの連携は国家ISAC会議（National Council of ISACs）を通じて行われている[61]。

加えて、ISAC は政府と民間業界との間で重要インフラの脆弱性と脅威に関する情報を共有するための組織として機能している。さらに、重要インフラのサイバーセキュリティ情

58 “Development of Policies for Protection of Critical Information Infrastructures” OECD Ministerial Meeting on the Future of the Internet Economy 17-18 June 2008

59 The Clinton’s Administration’s Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, White Paper, May 22, 1998. http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

60 認証機関のような認証法人（Trusted Entity）である ISAC は、セクター別に存在し、全米 ISAC 会議が全米の ISAC を調整している。重要インフラの物理的脅威とサイバー脅威のとリスク軽減に関する情報共有と分析を行い、ベストプラクティスをシェアリングする法人である。
http://www.nationalisacs.org/about-isacs

61

報を集約的に管轄する NCCIS（国家サイバーセキュリティ通信統合センター）がすべての ISAC との調整役となっている[62]。セクター別に設置された ISAC は、DHS 内に設置された状況認識およびインシデント対応のためのハブ組織である NCCIC（国家サイバーセキュリティ通信統合センター）と緊密に協力し合っている[63]。

ISAC（情報共有分析センター）の発展が引き金となって、2015 年サイバーセキュリティ情報共有法(CISA)が成立している。主な理由は、知財権(IPR)や賠償責任(Civil Liability)などの懸念が強まったことにある。

- 米国では、産業別 ISAC（情報共有分析センター）を通じて 20 年間にわたり潜在的なサイバー脅威に関する情報を共有している。ISAC の成長・発展により、知財権などに絡むビジネス情報の共有などで賠償責任や反トラスト法などの懸念事項が増えたためである。
- 他方、データ侵害やサイバー攻撃などの素早い動きをとるサイバー敵対者の動きに対して、官民連携で可能な限りリアルタイムな情報共有体制で重要インフラのサイバーリスク対応を図る必要がある。

特に政府系では、多州間情報共有・分析センター（MS-ISAC ：Multi-State Information Sharing and Analysis Center）がある。MS-ISAC は、米国内の州政府、地方政府、部族政府および領土政府の基点として「サイバー脅威への準備と対応（cyber readiness and response）を調整する」役割を担っている[64]。他の ISAC と同様、MS-ISAC もまた、情報共有を含む様々な面で DHS、民間セクターの双方と緊密に協力し合っている。

いずれの ISAC も共同事業に対して一定レベルの献身および貢献を示しているが、特に顕著な例も散見される。例えば、金融 ISAC（FS-ISAC）は、精力的で先回り的なアプローチを採用し、サイバー脅威に遅れをとらないための革新的取組みに着手している。具体的には、2016 年 10 月に金融システム分析＆レジリエンス・センター（Financial Systemic Analysis and Resilience Center：FSARC）を設立し[65]、2017 年 11 月には FS-ISAC アジア太平洋地域分析センター（FS-ISAC Asia Pacific Regional Analysis Center）を設立したほか、「9 カ国間におけるサイバー情報共有を強化する」ための「シンガポールの拠点開設および活動」[66]などである。

---

62 https://www.us-cert.gov/Government-Collaboration-Groups-and-Efforts
63 https://www.dhs.gov/topic/cybersecurity-information-sharing
64 https://www.cisecurity.org/ms-isac/ms-isac-charter/
65 https://www.prnewswire.com/news-releases/fs-isac-announces-the-formation-of-the-financial-systemic-analysis--resilience-center-fsarc-300349678.html
66

一方、民間セクターでは、将来性の高いイニシアティブとしてサイバー脅威アライアンス（CTA：Cyber Threat Alliance）がある。CTA は業界主導型の非営利組織（会員数は増加およびグローバル化しつつある）で、「サイバーセキュリティ分野における各企業・機関相互間でのリアルタイムに近い高品質サイバー脅威情報の共有」を促進することを目指している[67]。

【ISAO（情報共有分析組織）】

オバマ政権 2015 年 2 月 13 日に EO-13691（民間セクターサイバーセキュリティ情報共有に関する大統領行政命令[68]）に署名し、国土安全保障省（DHS）に対して ISAO（情報共有分析センター）の創設を促し、次の付帯事項の策定を要請した[69]。

- 重要インフラ防護プログラムを通じて ISAO（情報共有及び分析組織）のメンバーである民間セクターの個人にクリアランス（機密書類取扱資格）を付与する効果的な手段を開発すること。
- DHS の官民連携による情報共有分析組織である NCCIC（国家サイバーセキュリティ通信統合センター）を通じて ISAO との継続的なコラボレーションを推進し、この包括的な調整を行うこと。
- オープンかつ競争力のあるプロセスを通じて ISAO の標準組織となる非政府系組織（主な役割は ISAO の創出と機能の標準と指針を特定すること）を選択すること。
- 民間企業による機密として分類されるサイバーセキュリティ脅威情報にアクセスすることを正当化する機密情報シェアリングの取決めを承認する連邦省庁のリストに DHS を加えた。

主因は、1)小売業をターゲットにした2013年12月のデータ侵害、2)2014年11月のソニーピクチャーエンターテイメントに対するサイバー攻撃などである。2013～2015年に数多くのサイバー攻撃を受けたことから、多くの企業では実効性の高い情報共有組織を政府主導で創設する声が強まったことにある。以上の要望[70]に応え、オバマ大統領は行政命令の「EO

---

https://www.fsisac.com/article/fs-isac-and-mas-strengthen-cyber-information-sharing-across-nine-countries [“The nine Asia Pacific countries are Australia, India, Japan, Malaysia, New Zealand, Singapore, South Korea, Taiwan and Thailand.”]

67 https://www.cyberthreatalliance.org/

68 The White House Office of the Press Secretary, Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing, February 13, 2015
https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

69 https://www.dhs.gov/isao

70 ホワイトハウスに対する ISAO 創設の要望書の一部である PwC の調査報告書は次の通り。

13691」を発動したのである。

EO 13691（大統領行政命令第13691号：民間セクターサイバーセキュリティ情報共有）はDHSに対して、1)重要インフラ防護プログラムを通じてISAO（情報共有及び分析組織）のメンバーである民間セクターの個人にクリアランス（機密書類取扱資格）を付与する効果的な手段を開発すること、2)DHSの官民連携による情報共有分析組織であるNCCIC（国家サイバーセキュリティ通信統合センター）を通じてISAOとの継続的なコラボレーションを推進し、この包括的な調整を行うこと、3)オープンかつ競争力のあるプロセスを通じてISAOの標準組織となる非政府系組織（主な役割はISAOの創出と機能の標準と指針を特定すること）を選択することの3点を実施することを要請した[71]。

ISAO（情報共有分析組織：Information Sharing and Analysis Organization）は、セクター横断的な小規模事業者、セクター横断的な顧客をサポートする法律事務所またはコンサル会社や会計事務所などのコミュニティ間の情報共有を目的に自発的に組織化された集団である。ISAOの主な目的は、官民相互間および民間セクター内での「サイバー脅威情報の収集、分析および発信」である。ISAOは、ISACと同様の使命を担っているが、業界別の組織ではない[72]。

EO 13691は、NCCIC（国家サイバーセキュリティ通信統合センター）に対してISAO（情報共有分析組織）と継続的かつ包括的なコラボを行い、サイバーセキュリティのリスク及びインシデント関連の情報共有と当該リスク・インシデントの問題解決に取り組むことも命じている。

---

http://www.pwc.com/jp/ja/japan-knowledge/archive/assets/pdf/isao-cyber3-security201511.pdf

[71] https://www.dhs.gov/isao

[72] https://www.dhs.gov/topic/cybersecurity-information-sharing

1.4.その他のサイバーインシデント対応関係省庁の主な任務と組織概要

1.4.1.　NSC（国家安全保障会議）とCRGおよびサイバーUCG

大統領を委員長とするNSC（国家安全保障会議）は、シニア安全保障顧問や内閣官僚等と国家安全保障と外交政策の事案を検討する大統領の主たる諮問機関である。NSC（国家安全保障会議）創設の法的根拠は1947年の国家安全保障法（NSA）である。NSCは大統領府に置かれ、国家安全保障と対外問題に関する助言を提供している。NSCはホワイトハウスの国家安全保障政策に関する省庁間連携の調整役でもある[73]

NSC（国家安全保障会議）内には、サイバー政策局（Cybersecurity Policy Directorate）がある。サイバー政策局は、サイバーセキュリティ、情報共有とレジリエンスならびに災害への備えと災害レスポンスなどの政策に注力している。加えて、大統領はホワイトハウスの職員に対してもサイバーセキュリティと国土安全保障などの問題解決の助言を求めている。主なスタッフは次の通りである。

- 大統領補佐官兼サイバーセキュリティ調整官（Special Assistant to the President and Cybersecurity Coordinator）：連邦政府の省庁間連携を主導し、国家サイバーセキュリティ関連の戦略と政策の調整役である。
- 国土安全保障・対テロ担当大統領補佐官（Assistant to the President for Homeland Security and Counterterrorism advises the President）：対テロ政策と国土安全保障関連活動の省庁間連携を調整する[74]。
- CISO（連邦最高情報セキュリティ担当官：ホワイトハウスのOMBオフィスを主導し、省庁横断的なサイバーセキュリティ政策の計画策定と実施を担う。

NSCのサイバーセキュリティ政策チームのディレクターであったCheryl Davis, Daniel MellebyおよびHeather Kingは2017年7月に辞職。Monica Maherも同年8月に辞任した[75]。2017年8月、OMB(行政管理予算局)のCISO(主席情報セキュリティ担当官)のGrant Schneiderがシニアディレクターに就任した。主な担当は防衛関連のサイバーセキュリティである。

---

[73] “National Security Council.” *The White House*, Web. 17 October 2016. <https://www.whitehouse.gov/administration/eop/nsc>.

[74] “Lisa O. Monaco.” The White House, Web. 17 October 2016. <https://www.whitehouse.gov/blog/author/lisa-o-monaco>.

[75] https://www.politico.com/tipsheets/morning-cybersecurity/2017/08/04/national-security-council-cyber-officials-depart-221709

もうひとりのシニアディレクターは Joshua Steinman である[76]。

2016 年 7 月 26 日の PPD-41（米国サイバーインシデント調整に関する大統領政策指令[77]）では、NSC（国家安全保障会議）内に国土安全保障反テロ大統領補佐官（APHSCT）に対する責任を担う「サイバーレスポンスグループ（CRG)」を創設することが決められた。NSC 傘下の CRG が国家サイバー政策調整を所轄となる。サイバーレスポンスグループ（CRG）の主な役割などは次の通りである。

- NSC（国家安全保障会議）内に国土安全保障反テロ大統領補佐官（APHSCT）に対する責任を担う「サイバーレスポンスグループ（CRG)」を創設する。
- この CRG チームは重大なサイバーインシデントに関する米国政府の政策と戦略を策定・実施することを調整する。
- 加えて、サイバーレスポンスグループ（CRG）は重大なサイバーインシデントに関するブリーフィング情報を受け取り、反テロ担当官僚と連携し、重大なサイバーインシデントレスポンスを検討し、当該インシデントに係るパブリックコミュニケーションを開発する。
- CRG（サイバーレスポンスグループ）は、DOD、DoD, DOJ, DOC, DOE, DHS の NPPD（国家防護計画直)、シークレットサービス、米国統合参謀本部（US Joint Chiefs of Staff)、ODNI（国家情報長官室)、FBI、CIA、NSA（国家安全保障局）などの幹部（Senior Level Officials）との調整を主導する。その他の関係省庁は必要に応じて CRG への参加が要請される。
- CRG（サイバーレスポンスグループ）の議長は国土安全保障反テロ大統領補佐官（APHSCT と国家安全保障担当大統領補佐官（Deputy National Security Advisor）である。

さらに PPD-41 では、NSC（国家安全保障会議）または CRG（サイバーレスポンスグループ）は必要に応じて、重大なサイバーインシデントに対応する連邦省庁間および官民の調整を行う「サイバーUCG（サイバー統合調整グループ：Cyber Unified Coordination Groups)」を創設することも定められた。国家作戦調整を担わせることになった。重大なサイバーインシデント対応に関して連邦省庁間連携を主導するサイバーUCG（サイバー統合調整グループに関する重要事項は次の通りである[78]。

76
https://www.politico.com/tipsheets/morning-cybersecurity/2017/08/09/a-new-face-on-the-white-houses-cyber-squad-221780

77 Presidential Policy Directive 41 (PPD-41): United States Cyber Incident Coordination
https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

78 https://fas.org/irp/offdocs/ppd/ppd-41.html

- サイバーUCG（サイバー統合調整グループ）は、NIPP（国家インフラ防護計画）の中でDHSが特定した16の重要インフラの1つ以上の所有者・運転者に影響を及ぼすサイバーイベントを踏まえて創設する。
- 特にサイバーUCG（Unified Coordination Groups）はレスポンスと回復の努力プログラムの開発と実行を監督し、サイバーUCG参加者間の情報とインテリジェンスの共有を促し、影響を受けるステークホルダーと一般大衆とレスポンス及びリカバリ計画に関する話し合いを行う。
- サイバーUCGの構成メンバーは、脅威レスポンスの主務官庁であるFBIとNCITF(NATO Crpto Interoperability Task Force)、アセットレスポンスの主務官庁である国土安全保障省（DHS）CS&C（サイバーセキュリティ通信オフィス）のNCCIS（National Cybersecurity and Communications Integration Center)。インテリジェントサポートを担うCTTIC（Cyber Threat Intelligence Integration Center)、関係するSSA（セクター別管轄エージェンシー）である。その他の関係省庁や州政府・地方政府等、国際パートナー、民間セクターなども必要に応じて参加が要請される

1.4.2. DOJ（司法省）・FBI・NCIJTF

DOJ（司法省)の犯罪部門は2014年12月、電子機器による犯罪者の監視とコンピュータ詐欺等がどのようにサイバーセキュリティに対して打撃を与えるものかに関して専門家の助言と法的ガイダンスの中核ハブとなるサイバーセキュリティユニットをコンピュータ犯罪及び知財セクション内に設置した。サイバーセキュリティ部門はサイバー攻撃によるコンピュータネットワークや個人の犠牲を防ぐと同時に民間セクターに対して合法的なサイバー慣行を促すことを目指している[79]。

司法省（DOJ）は、FBIならびにDOJ傘下のNCIJTF（National Cyber Investigative Joint Task Force：国家サイバー捜査合同タスクフォース）を通じて、切迫したサイバー脅威（immediate cyber threat）に対するレスポンス（応答）を調整する責任を担う。

2016年7月26日のPPD-41（米国サイバーインシデント調整に関する大統領政策指令）では、DOJはサイバー脅威による影響を受ける組織の利害関係当事者（ステークホルダー）との連絡を密にし、サイバー脅威に関する証拠とインテリジェンスを収集し、差し迫ったサイバー脅威を阻止する活動と法執行を行い、さらにはDHS（国土安全保障省）内でサイバー脅威情報を共有すると定められた。換言すると、他省庁連携機関としてのNCIJTF（国家サイバー捜査タスクフォース）の役割は、サイバー脅威捜査をサポートし、そのインテリ

[79] https://www.justice.gov/criminal-ccips/cybersecurity-unit

ジェンスと分析結果を関係コミュニティの意思決定者へ提供し、さらに他国におけるサイバー脅威との戦いをサポートする[80]。

加えて、NCIJTF は、米国の情報システムに対してサイバー攻撃を試みる実際のテロリスト・スパイ・犯罪者等を突きとめ、捜査・逮捕することに重点を置く共同活動を実施する。重大なサイバーイベントが発生した際には、FBI がアセットレスポンスチーム、州政府・地方政府等、非政府機関、産業界および必要に応じて他省庁と連携し、「サイバー統合調整グループ（Cyber Unified Coordination Group)」として行動する。つまり、サイバーインシデント応戦（レスポンス）では、FBI が基本的な役割を果たすことを PPD-41 は明記している。上記の「アセットレスポンス」とは、インパクトを受けた組織の情報システムのバッドアクターを見つけ、そのシステムを修復し、脆弱性にパッチ対処し、将来のインシデント発生のリスクを低減し、インシデントの拡散を阻止することである (DHS 長官の解説81)。

1.4.3. ODNI（国家諜報長官官房）と CITIIC 等

DNI（国家諜報長官：Director of National Intelligence）は、ODNI（国家諜報長官官房）のトップであり、EO 13467(機密と分類される国家安全保障情報へのアクセス等の大統領命令)に準拠し、機密情報（classified information）と機微な立場を維持する有資格者へのアクセスの適格性を捜査・裁定する政策と手順の策定・実施に対する国家行政省庁（SecEA）としての責任を担っている。基本的な任務は、CIA 等を傘下に置き、米国インテリジェンスコミュニティ（US Intelligence Community）を統括するが、連邦省庁内の人事セキュリティプロセス全般を管轄する役割も担っている[82]。

国民を防護するために極めて重要な対諜報（CI-Counterintelligence）とセキュリティ対策の 2 つを統合した連邦政府の活動を主導・支援するのは、Office of DNI（国家諜報長官官房）傘下の National Counterintelligence and Security Center（国家防諜安全保障センター）である。加えて、2016 年 10 月に創設された NCSC（国家防諜安全保障センター）は米国のインテリジェントコミュニティを橋渡しする役割を演じ、外国の諜報活動のリスクに晒される民間企業や個人等の民間セクターをサポートし、米国へのインテリジェンス脅威に関する公的警告を発する任務を負っている。DNI（国家諜報長官）官房ですべてのセキュリティ行政エージェントの機能と責任を担うのは、NCSC（国家防諜安全保障センター）

---

[80] https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force

[81] https://www.dhs.gov/news/2016/07/26/statement-secretary-jeh-c-johnson-regarding-ppd-41-cyber-incident-coordination

[82] https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent/ncsc-roles-responsibilities

の特殊セキュリデ局（NCSC/SSD)である[83]。

さらに、DNI(国家情報長官)は2015年に他省庁連携機関としてCyber Threat Intelligence Integration Center（CTIIC)を創設した。CTIIC（サイバー脅威インテリジェンスインテグレーションセンター）は DNI のサイバー脅威に関係する諜報活動の中核機関であり、その主な任務は米国の政策当局のために、米国に対する外国のサイバー脅威および脅威を含むすべてのサイバー脅威を分析し、連邦省庁のインテリジェンス共有能力の開発を監督し、CIA や NSC 等の他の省庁からのインテリジェンスを統合化することにある[84]。

加えて、DNI（国家諜報局）はグローバル脅威評価に関する年次報告書を刊行し、様々な技術分野における米国の安全保障に対する世界的な脅威と地域毎の国別脅威に関する概説を行っている。さらに、国家諜報局（DNI）は毎年 2 月に公開聴聞会でグローバル脅威評価を①下院インテリジェンス特別委員会、②上院インテリジェンス特別委員会、③上院軍事委員会に送達している。

1.4.4. DoD（国防省）のサイバーミッションと戦略目標

国防省（DoD）のサイバーミッションは、2015 年 4 月にアッシュ・カーター(Ash Carter)国防長官（当時）がスタンフォード大学で行った講演で発表した DoD の新サイバースペース作戦戦略に示されている[85]。「ペンタゴンの再配備：イノベーションとサイバーセキュリティに関する新たな道筋を描くと題された新サイバー戦略は、DoD が 2011 年にリリースした最初のサイバー戦略文書[86]の発展拡大版である。この新戦略で示された DoD のサイバー空間における任務は次の 3 点である。

- サイバー攻撃から自国のネットワーク、システムおよび情報を保護すること
- 重大な結果を生じるサイバー攻撃に対して米国とその利益を守ること
- 軍事作戦と緊急時対応計画を支援するためのサイバー機能を統合する準備を整えること

---

83 https://www.dni.gov/index.php/ncsc-who-we-are
https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield/ncsc-awareness-materials

84 https://www.dni.gov/index.php/ctiic-who-we-are

85 https://www.defense.gov/News/Speeches/Speech-View/Article/606666/drell-lecture-rewiring-the-pentagon-charting-a-new-path-on-innovation-and-cyber

86 United States of America. Department of Defense. Office of the Secretary of Defense. *The Department of Defense Cyber Strategy*. Washington, DC: 2015. Print.

1 番目と 2 番目の任務は、2011 年版サイバー戦略に規定されたサイバー防衛ミッションの延長線上に位置するものであるが、第 3 の任務は、米国政府がそれまで認めてこなかったサイバー攻撃の責務を DOD に正式に担わせるものである。3 つの任身を概説すると次の通りである。

- 新戦略の文言によれば、サイバー空間におけるDODの第1のミッションは、DODのネットワーク、システムおよび情報をサイバー攻撃から防護することである。
- 第2の使命は、米国および米国の利益を重大なサイバー攻撃から防衛することである。
- DODの第3の使命は、軍事オペレーションおよび緊急時対応計画を支援する総合的サイバー能力を提供できる体制を整えるである。
- DODが上述の総合的サイバー能力を使用する機会は、大統領または国防長官が使用を命じた場合に限られる。

上記のミッションに基づいて、2015 年版新サイバー戦略は 5 つの戦略目標も明記しているが、その大半が DOD と民間セクターとの協力強化を求めている。5 つの戦略目標の概要を示すと、以下の通りである。

- サイバー作戦戦略を実行するための部隊と能力の増強と維持。
  - 1 番目の戦略目標の柱は、米軍と DoD の様々な部局および機関に在籍する約 6,200 名の軍人および文民職員から成るサイバー軍（Cyber Command）を新設するための DoD の現行の取組みを完遂することである。
  - 特に重点を置く取組みは、民間セクターから「選り抜きの精鋭たち（the best and the brightest）」を集めて、DOD のサイバー関連課題の解決に当たらせることである。
  - 例えば、DOD は、民間セクターの対象領域専門家（subject matter expert：SME）を DOD に短期間出向させ、サイバーエンジニアリングやサイバー分析に関する独自の研究課題に取り組ませる官民人材交流プログラムの創設を計画している。
  - 同時に、DOD は米軍将校を DOD から大手民間企業に 1 年間派遣する「国防長官企業派遣フェロープログラム（Secretary of Defense Corporate Fellows Program）」の拡充を目指している。SDCFP は DoD から米軍士官を先端企業に 1 年間派遣して、最新の計画立案や先端技術などを学び、DOD の組織革新に資するプログラムである[87]。
- DoD（国防省）の情報ネットワークを防護し、DoD データのセキュリティを確保し、さらに DoD ミッション遂行にかかるリスクを軽減すること。
  - 2 番目の戦略目標は、不正なサイバーアクセスを回避できないとの認識を前提に、

[87] http://dcmo.defense.gov/Products-and-Services/SecDef-Corporate-Fellows-Program/

最も重要性の高いDoDのネットワークとデータを特定し、優先順位付けを行い、防御することである。

- DoD の重要なネットワークまたはデータが侵害される場合に利用する緊急時対応計画の策定と実践が必要となる。
- 特に重点を置く取り組みは、DoDが利用する重要インフラの所有者および運用者とDIB（防衛産業基盤）などの民間部門のサイバーセキュリティを強化することである。
- DoDは、NIST（国立標準技術研究所）の「サイバーセキュリティフレームワーク」を利用すると共に、民間セクターにはサイバー脅威情報共有プログラムへの参加が不可欠となる。

- 破壊的または有害なサイバー攻撃から米国の本土と米国の重要な利益を防護するための体制を整備。
  - 3番目の戦略目標の柱は、米国の国益と国土に対する重大なサイバー攻撃を阻止または撃退するための DOD、民間セクター、同盟国ならびにその他の政府機関（CIA、FBI、DHSなど）等との連携と相互協力を推進することである
  - 特に重点を置くのは、サイバー脅威情報を米国政府の内部で共有するだけに留まらず、米国政府と同盟国政府、州・地方政府および民間セクターとの間でも共有するための標準化された持続的かつ自動的なメカニズムの開発に向けて、DODとDHSの協力体制を強化することである
- 紛争の拡大を抑制し、紛争環境を形成するための実行可能なサイバー・オプションを構築・維持し、当該オプションに利用計画を策定すること。
  - 4番目の戦略目標の柱は、DODが巻き添え被害（人命損失および器物損壊の両方とも）を最小限に抑えつつ、敵の指揮統制ネットワークをかく乱するサイバーオペレーション、軍事関連の重要インフラおよび兵器能力を活用する能力を育成・強化することである。
  - 新戦略は、DODがこれらの攻撃的能力を十分強化したうえで全般的な緊急時軍事作戦計画に組み入れることを求めている。
  - 新戦略には明記されていないが、人材交流プログラムで DOD に派遣された民間SME（対象領域専門家）たちが攻撃的サイバー能力の開発および巻き添え被害の抑制において重要な役割を果たすことを期待する向きは多い。
- 共通の脅威を阻止して国際社会の安心と安全および安定を高める目的で、国家間の確固たる同盟関係や協力関係を構築および維持すること。
  - 5番目の戦略目標の柱は、DoDと同盟国およびパートナーとのサイバー協力の推進である。この種の努力の大半は、特にサイバーセキュリティとサイバー防衛におけるパートナーの能力向上に向けられている。
  - しかし、新戦略はまた、DoDが同盟国との協力で「戦闘指揮計画を補佐してサイ

バー効果の発揮するための共同戦闘能力を高める」ことを要請している。

- 特に重点を置く取組みは、中東、アジア太平洋および欧州の友好国／同盟国（特にNATO主要加盟国）とのサイバー協力の推進である。
- 上記3地域には、戦略文書の中でDODがサイバー脅威国と認定した中国、ロシア、イランおよび北朝鮮が存在する点に留意されたい。

1.4.5. 米国サイバー軍（CYBERCOM）の役割

2009年6月23日、国防長官は米国戦略軍（STRATCOM：US Strategic Command）の司令官に対し、傘下にある副統合軍のひとつとして米国サイバー軍（CYBERCOM：United States Cyber Command）の創設を命じた。米国サイバー軍は、NSA（国家安全保障局）の本部があるメリーランド州フォート・ジョージ・G・ミード（Fort Maede）陸軍基地を本拠地として設立され、18カ月後には完全な作戦能力を獲得した。

- サイバー軍（CYBERCOM）の現司令官であるマイケル・S・ロジャーズ海軍大将（Admiral Michael S. Rogers）は2014年4月時点において米サイバー軍司令官と国家安全保障局長官（Director, National Security Agency）および中央保安局長（Chief, Central Security Service）を兼務している。
  - 副司令官はジェームズ・K・「ケビン」・マクローリン空軍中将（Lieutenant General James K. “Kevin” McLaughlin）である。
- サイバー軍の実働部隊は、陸軍サイバーコマンド（Army Cyber Command：ARCYBER）、艦隊サイバーコマンド（Fleet Cyber Command：FLTCYBER）、空軍サイバーコマンド（Air Force Cyber Command：AFCYBER）および海兵隊サイバーコマンド（Marine Forces Cyber Command：MARFORCYBER）で構成される88。
- 沿岸警備隊サイバーコマンド（Coast Guard Cyber Command：CGCYBER）は、国土安全保障省（DHS）の所属ではあるが、サイバー軍と直接的な相互支援関係を維持している。
- サイバー軍は現在、2015年4月版サイバー戦略（本報告書Section IIIのPart Bで詳述）に定められた任務の遂行および戦略目標の達成に向けて、サイバー任務部隊（Cyber Mission Force）の「立ち上げ」作業に入っている。作業は2018年中に完了するとみられ、サイバー軍の下で4大任務に従事するサイバー任務部隊（合計133チーム）の発足が予定されている。4大任務の内容とチーム数は次のとおり。
  - 重大なサイバー攻撃から米国および国益を守ることを任務とするナショナル・ミッション・チーム（13チーム）。

---

88 US Strategic Command. "U.S. Cyber Command." *U.S. Strategic Command*. Department of Defense, Mar. 2015. Web. 19 July 2016. <https://www.stratcom.mil/factsheets/2/Cyber_Command/>.

- 重大な脅威から重要なDODのネットワークとシステムを守ることを任務とするサイバー・プロテクション・チーム（68チーム）。
- 作戦計画および緊急時対応作戦を支える総合的サイバー効果を創出することにより戦闘部隊（Combatant Commands）を支援することを任務とするコンバット・ミッション・チーム（27チーム）。
- ナショナル・ミッション・チームおよびコンバット・ミッション・チームを支援するための分析および計画立案を任務とするサポート・チーム（25チーム）。

- 2016年7月現在、サイバー任務部隊を構成する合計133チームのうち46チームはすでに完全作戦能力を獲得しており、59チームは初期能力状態にある。これら既設チームの隊員数は現時点で合計4,684名であるが、最終的に全チームがフル稼働状態に達した場合の隊員数は6,200名規模に達する見込みである。
- ロジャーズ海軍大将の最近の発言によれば、サイバー軍がサイバー任務部隊の能力獲得プロセスにおいて現在直面している最大の問題は、訓練プロセスの「ボトルネック[89]」である。
- 133チームの設置期限は2018年9月とされ、サイバー軍による編成作業は予定どおり終了に近づいているものの、アナリストの中には最終隊員数が目標を約9%下回ると予想する向きもある。
- サイバーセキュリティおよびサイバー軍への支援は、米議会における極めて超党派的テーマである。サイバー軍は、2017年度予算として5億500万ドル（2016年度の4億4,600万ドルに比べ8.4%の増加）を要求している。

サイバー軍（CYBERCOM）は、そのタスクを実行し、2015 年 4 月の新 DoD サイバー戦略の戦略目標を達成するために、サイバーミッション部隊（Cyber Mission Force）を立ち上げているところである。2018 年に立ち上げが完了すると、サイバーミッション部隊は 4 つの主要ミッションの領域において合計 133 チームで構成される。

【サイバーミッション部隊（Cyber Mission Force）の構成とミッション】

- 国家ミッションチーム(13チーム)：重大な結果を及ぼすサイバー攻撃から米国とその利益を守る。
- サイバー防衛チーム(68チーム)：優先対応すべき脅威に対して最重要な国防総省のネットワークとシステムを守る。
- 戦闘ミッションチーム(27チーム)：運用計画と緊急対応によって、統合されたサイバー

[89] Boyd, Aaron. "CYBERCOM Gets Easiest Budget Hearing Ever." Federal Times. N.p., 16 Mar. 2016. Web. 19 July 2016. <http://www.federaltimes.com/story/government/cybersecurity/2016/03/16/house-subcommittee-cybercom/81870980/>.

空間において効果的に戦闘コマンド（Combatant Commands）を支援する。

- 支援チーム（25チーム）：国家ミッションチームと戦闘ミッションチームに対して、分析および計画サポートを提供する。

2015 年 4 月の新サイバー戦略によると、DoD（国防省）におけるサイバー軍（CYBERCOM）の役割は依然として流動的で進化の途上にある。同サイバー戦略の重要なポイントの 1 つは、緊急事態に直面した連邦政府や民間セクターの防衛を手助けするために文官当局、DHS、州・地方当局およびその他の政府機関をサポートする枠組みを構築し、命令に基づいて演習を行うよう命じている点である。そのため、米国サイバー司令部（CYBERCOM）は、戦略の全体的な枠組みの一部として、サイバースペースの運用と方針を策定する作業を進め、そのタスクの状況を確認している。

- このため、米サイバー軍は現在、サイバー作戦やサイバー政策の策定を含むサイバー戦略全体の一部を成す各任務を遂行し、その進捗状況の確認するプロセスを進めている。
- しかしながら、米サイバー軍のサポート役とは実際に何を意味するのかについて、DODやサイバー軍の内部だけでなくDHSやFBIなど他の政府機関の内部でも、議論が行われている事実にも留意されたい。

上記のとおり、DOD はサイバー能力を活用してサイバー空間を構築し、攻撃的および防衛的な総合的オプションを提供している。DOD 内の論調および STRATCOM（米国戦略軍）の指示によれば、サイバー軍の役割は次のとおりである。

- 国境を超えた作戦（transregional operation）を同期化および指揮すること。
- 戦闘部隊司令官、統合参謀本部および国防長官室（OSD）と協力し、DHSとともにその他の政府省庁および部局ならびにDIB（防衛産業基盤）の企業と連携すること。

つまり、DOD はサイバー軍を通じて、国家的緊急事態への対応や重要インフラおよび主要資源の保護にあたる各政府省庁・部局への支援など、他の政府省庁・部局の取組みを支援するために必要な資源を配備できる。

- このため、サイバー軍の国家防衛ミッションは、国益の防護が必要な局面において大統領令または常設権限機関の許可があれば、他の省庁・部局の常設任務に対して優位性を獲得し、それらの任務を包含または統合することが可能である。
- サイバー軍からみて、重要インフラおよび主要資源の防御とは、分析、警告、情報共有、脆弱性特定および国家的復旧努力の節減・軽減・支援を通じ、DHSおよび他の

政府省庁をサポートすることを意味する。

- さらに、防衛重要インフラ（defense critical infrastructure：DCI）とは、軍隊および全世界で展開される軍事行動を企画、支援および維持するうえで必要不可欠なDODおよび非DOD資産の両方を意味する。これらもまた米国の重要インフラおよび主要資源全体のかなりの部分を占めている。
- 戦闘部隊司令官は、防衛重要インフラに該当する非DOD資産の喪失または劣化を阻止または緩和するために行動することができる。ただし、これは統合参謀本部議長（Chairman of the Joint Chiefs of Staff）および政策担当国防次官（Under Secretary of Defense for Policy）との協力の下で行われなければならない。
- 同様にサイバー軍も、防衛産業基盤およびその一部であるDOD情報ネットワークならびに非DODの重要情報ネットワークを防護するため、DHSの協調的取組みをサポートする責任を有する。

STRATCOM（戦略軍）はDOD情報ネットワーク（DODが所有または賃借するすべてのネットワークを含む）の防護に重点を置いているが、DODの業務遂行は多数のその他ネットワーク（民間ネットワークを含む）に支えられている。

- これら非DODの情報ネットワークおよびシステムに関する責任は、ネットワーク所有者（他の政府省庁・部局や民間企業・団体を含む）に帰属する。
- DODの認識によれば、DODに関係する（DoD-associated）ネットワークはすべて敵の攻撃目標になり得るため、非DODの情報ネットワークおよびシステムの防護は、DOD情報ネットワークの防護と同じように重要と考えられる。
- このためサイバー軍は、非DOD情報ネットワークのサイバー防衛に必要な計画を加速化するため、他の省庁・部局と連携を図っている。

1.4.6. DoD（国防省）とDIB（防衛産業基盤）との協力

DoDは、DIBとの共同プログラムやDIBの規制を通じて、重要インフラを防護している。ここでは、DoDとDIBの相互作用であるDoD-DIB CS / IAプログラム、DIB拡張サイバーセキュリティサービス（DECS）、防衛連邦調達規則の付則（DFARS）の3つのプログラム・規則について説明する。

【DoD-DIB CS/IAプログラム】

DoD（国防省）は、2008年に公開と非公開の双方のサイバー脅威情報を共有するために、「DoD-DIB サイバーセキュリティと情報保証（DoD-DIB CS / IA）プログラム」を自主パイ

ロットプログラムとして確立した[90]。

- DoDは2012年5月、DoDとDIBとの間で自発的なサイバーセキュリティ情報共有プログラムを確立するために、暫定的な最終規則（interim final rule）を発行し、DoD-DIB CS / IAを永続プログラムにした[91]。
- 2013年10月、暫定最終規則は、32連邦規則（CFR）第236条（32 Code of Federal Regulations（CFR）Part 236）の下で成文化された最終規則として承認された[92]。
- このDoD-DIB CS / IAプログラムでは以下の政策が実施された[93]。
  - 対象となるDIB企業は、公開と非公開のサイバー脅威情報を双方で共有し、情報の保証を得るためにDoDとのフレームワーク契約を締結することができる。
  - 情報共有の枠組みは、アナリスト間の交流を可能にし、協調的な緩和と改善策を生み出すのに役立った。
  - 企業には、情報共有の交換を通じて分析サポートと法的なマルウェアの分析が提供された。
  - プログラム参加者は、サイバーコミュニティにとって興味のあるサイバーセキュリティインシデントを報告することができる。
  - DIBの企業は、「サイバー犯罪情報センター（DoD Cyber Crime Center：DC3）のDoD-DIB共同情報共有環境（DCISE)」にサイバー侵入事件を報告することができる。これがDoDのサイバー脅威情報の共有とインシデント対応のための運用上の核となっている。

2015年10月に、DoDは、DoD-DIB CS / IAプログラムを改訂して、契約者の情報システム、情報システム内の防衛情報、あるいは重要な運用支援を行う契約者の能力に悪影響を与えるサイバーインシデントの報告を義務づける暫定最終規則を公布した[94]。加えて、プログラムは「DoD-DIB サイバーセキュリティ情報共有プログラム（DoD-DIB Cybersecurity

90
http://www.hlregulation.com/2016/11/02/department-of-defense-DoD-final-rule-for-the-defense-industrial-base-dib-cybersecurity-program-is-effective-this-week/
91
https://www.federalregister.gov/documents/2012/05/11/2012-10651/department-of-defense-DoD-defense-industrial-base-dib-voluntary-cyber-security-and-information
92
https://www.federalregister.gov/documents/2013/10/22/2013-24256/department-of-defense-DoD-defense-industrial-base-dib-voluntary-cyber-security-and-information
93
http://sellingtoarmy.com/sites/default/files/Army_SB_Seminar_2015_AUSA_Vicki_Michetti_approved.pdf
94
https://www.federalregister.gov/documents/2015/10/02/2015-24296/department-of-defense-dod-defense-industrial-base-dib-cybersecurity-cs-activities

Information Sharing Program ：DoD-DIB CS)」[95]に改称された。

- この暫定最終規則は、DoD-DIB CS / IA の自発的情報共有プログラムを保持していたので、DIB 企業は依然として義務的な報告要件の範囲外にあるサイバーセキュリティ情報を自主的に共有できた。
- 暫定最終規則では、DIB の契約業者がサイバーインシデントを発見した場合、次の手順を実行する必要がある。
  - 侵害された防衛情報をカバーする証拠の再確認を行う。
  - DoD の「DIB サイバーインシデント報告＆サイバー脅威情報共有ポータル」(DIB Cyber Incident Reporting & Cyber Threat Information Sharing Portal) を通して、DoD にサイバーインシデントを迅速に報告する。
  - 契約者によって発見され隔離された悪質なソフトウェアを法的分析のためにサイバー犯罪情報センター (DC3) に提出する。
- 契約者がサイバーインシデントを開示することを義務づける提案された規則は、国防総省の規制に一貫性を持たせるのに役立っている。また、この規則は契約業者が契約対象の DIB 情報システムにおけるサイバーインシデントを報告することを義務付ける DFARS 252.204-7012 とも整合している。
- 暫定最終規則の公開から約 1 年後の 2016 年 10 月 4 日、DoD は、DIB 情報システムに関するサイバーインシデントの報告を義務付ける最終規則を発表した。この規則は 2016 年 11 月 3 日に発効した[96]。

【DIB 高度サイバーセキュリティサービス (DECS)】

DECS は、DoD と DHS が、DoD-DIB CS プログラムにおいて非公開のサイバー脅威と技術情報を DIB 企業に提供するオプションのサービスである。

- 2012 年 1 月、DHS のサイバーセキュリティ・通信オフィス (CS&C) は、DIB 企業に IT サービスを提供する商用サービスプロバイダ (Commercial Service Providers：CSP) との間でサイバー脅威指標および関連情報を共有するために、DoD と提携した。この試行の目的は、参加している DIB 企業を保護するためにサイバー脅威に関する情報を CSP と共有することであった[97]。
- 2012 年 5 月、試行プログラムは自発的プログラムに移行し、それがすべての重要イ

95 https://www.gpo.gov/fdsys/pkg/FR-2015-10-02/html/2015-24296.htm>.

96 https://www.federalregister.gov/documents/2016/10/04/2016-23968/department-of-defense-dods-defense-industrial-base-dib-cybersecurity-cs-activities

97 https://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_nppd_ecs_jan2013.pdf

ンフラセクターに拡大された。全体的なプログラムは、高度サイバーセキュリティサービス（Enhanced Cybersecurity Services：ECS)プログラムと呼ばれ、その中でも防衛産業基盤(DIB)に関わるものがDIB高度サイバーセキュリティサービス(DECS)と呼ばれている。

- DECSは、悪意のあるサイバー活動に対抗するために、DIBの会社またはDIB会社の認定CSPに、非公開のサイバー脅威および技術情報を提供するための国防総省と国土安全保障省の共同作業である[98]。
  - DIB企業がDIB CSプログラムに参加すると、自社ネットワーク上の対策を実施するためのセキュリティ要件を満たすか、または参加するCSPからこれらのサービスを購入することによって、DECSに参加することを選択できる[99]。
  - DoDとDHSはサイバー脅威情報を収集し、DHSはその情報を参加DIB企業または認定CSPに伝達する。DHSは、DECSプログラムに基づくDIB企業とそのCSPとの連絡窓口である。
  - 現在、DHS ECSプログラムにおいて、AT&T、CenturyLink、ロッキード・マーティン、Verizonの4つのCSPが承認されている[100]。
  - サイバー脅威情報は1週間に1～2回共有されている。
- 拡張サイバーセキュリティサービス（ECS）は、重要インフラ企業がこのプログラムに参加することを躊躇しているため、2012年の開始以来、大きな成功を収めていない。プログラムはすべての重要インフラ部門に開放されているが、2014年においてECSプログラムには3つの重要インフラセクター（DIB、エネルギーと通信）から約40社しか参加していない。企業やCSPがDECSやその他のECSプログラムに参加していない理由はいくつかある[101]。
  - 企業にとっては、非公開のデータを送信する設備およびネットワークのアップグレードに投資するコストが高く、また、サイバー脅威に対処するために受信データを理解し、情報を効果的に使用するために、必要な人的資本とプログラムに投資する必要がある。
  - 非公開のデータを受け入れるための認定を受けるプロセスは、企業にとっては時間がかかり魅力のない作業である。
  - 2014年のDHS の Inspector General Report[102]によれば、DHSがECSプログラムを通じて共有した情報が、公開の情報源からも入手可能であることが分かった。したがって、DECSプログラムへの参加に費やされる時間と費用は、公に利用可

98 http://www.acq.osd.mil/dpap/policy/policyvault/OSD012537-12-RES.pdf

99 http://files.arnoldporter.com/advisory%20department_of_defense_expands_defense_industrial_base_voluntary_cybersecurity_information_sharing_activities.pdf

100 https://www.dhs.gov/enhanced-cybersecurity-services

101 http://www.nextgov.com/security/2014/08/who-receiving-hacker-threat-info-dhs/91154/

102 https://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-119_Jul14.pdf

能な手段で情報を受け取ることができれば価値がないのかもしれない。

【国防総省調達規則(Defense Federal Acquisition Regulation Supplement)】

DFARS は、政府契約者のための連邦規則のセットである連邦調達規則(Federal Acquisition Regulation：FAR）の補足事項をまとめたものである。 DFARS は、特に防衛産業基盤（DIB）セクターの政府対応請負業者向けの規制であり、過去数年間に DIB 請負業者のサイバーセキュリティ問題に関連して多くの条項が作成され、更新されてきた。

- 2016 年 10 月 21 日、国防総省は、DFARS 条項を修正し、新たな条項を追加した最終規則を発行した。この規則は、対象防衛情報（covered defense information ：CDI）を処理、保存、または伝達する DIB 請負業者に対して、情報の保護措置とサイバーインシデント報告要件を課した。また、クラウドコンピューティングのセキュリティ要件も明らかにした[103]。
- 最終規則は、議会の法律、2013 年度防衛認証法（FY 2013 National Defense Authorization Act ：NDAA）の 941 項、2015 年度 NDAA の 1632 項に対応して実施されたものである。
- 最終規則においては、国防総省が DIB 企業のサイバーセキュリティに関連する行動をどのように指示・強制するかが強調されている。

【DIB 企業に影響を与える DFARS サイバーセキュリティ条項[104]】

- DFARS 252.204-7008「対象防衛情報保護の遵守」：契約者はNIST Special Publication（SP）800-171で指定されたセキュリティ要件を実施することが要求される。この条項では、請負業者が代替の情報技術セキュリティ対策の実施を提案することが可能であるが、代替計画を承認または却下するかの最終的な権限は国防総省のCIOにある。
- DFARS 252.204-7009「第三者請負業者のサイバーインシデント情報の使用または開示に関する制限」：サイバーインシデントに対応してDoDに提出された情報を保護するための請負業者（および下請け業者）に対する制限規定。
- DFARS 252.204-7012「対象防衛情報保護とサイバーインシデント報告」：契約者はNIST SP 800-171を含む「適切な」セキュリティプロトコルを実施し、「対象となる防衛」に関するサイバーインシデント情報を報告する義務がある。
  - この契約は、防衛情報システムと防衛情報の両方を対象としている。
  - NIST SP 800-171プロトコルは、2017年12月31日までに実施する必要がある。
  - サイバーインシデントは、発見から72時間以内に、DoDオンラインポータル

103 https://www.gpo.gov/fdsys/pkg/FR-2016-10-21/pdf/2016-25315.pdf
104 http://farsite.hill.af.mil/VFDFARa.htm

（http://dibnet.DoD.mil）で「迅速に」報告されなければならない。

- 請負業者は、契約の業務をサポートするものだけでなく、対象となるすべての契約者情報システムにセキュリティプロトコルを実施する必要がある。
- さらに、DFARS 252.204-7012で確立されたすべてのセキュリティおよび報告の要件は、契約に含まれる下請け業者にも適用される。

- DFARS 252.239-7010「クラウドコンピューティングサービス」：請負業者はクラウドコンピューティングを使用する際には、クラウドコンピューティングセキュリティ要件ガイドに従って、実務的、技術的、および物理的な安全対策と管理を実施し、維持することが求められる。
  - 「クラウドコンピューティングセキュリティ要件ガイド」は、クラウドベースのシステムを保護する方法について国防総省の要員に指示することを目的としたDISAによって開発された指針の枠組みである105。
  - 請負業者は、契約内のクラウドコンピューティングサービスに関連して、すべてのサイバーインシデントおよびインシデントで使用された悪意のあるソフトウェアも報告する必要がある。
- DFARS Subpart 204.73「対象防衛情報保護とサイバーインシデント報告」：DFARS 252.204-7012で概説された適切なセキュリティ基準とサイバーインシデント報告を繰り返している。規制の中で、報告されたサイバーインシデントは、「契約者または下請け業者が、対象となる請負業者の情報システムに適切なセキュリティを提供できなかったという証拠として解釈されてはならない」と述べている。

1.4.7. DHS（国土安全保障省）とセクター別管轄省庁（SSA）との協力関係

国土安全保障省（DHS）は、重要インフラを外部の攻撃から防護し、レジリエンス（強靭性）を高める連邦努力における米国政府の中心的機関である。DHSがその役割を果たすためにはセクター別管轄省庁（SSA）および他の政府機関の参加とその専門知識の活用が不可欠である。DHSはセクター別管轄省庁（SSA）と共に、エネルギーセクター、原子力セクター、防衛産業基盤などのサイバーセキュリティの強化を様々な仕組みを通して行なっているが、下記の通り、主に1)PPP（官民連携）方式と2)国家サイバーセキュリティ通信統合センター（NCCIC）を通じて実施されている。

- PPP（官民連携）方式による対応
  - 国土安全保障省（DHS）とセクター別管轄省庁（SSA）の間の重要インフラ防護とレジリエンスに関する協力のほとんどは、このPPP（官民連携）方式で実施されている。具体的には、政府調整会議（GCC）、重要インフラパートナーシップ

105 http://iase.disa.mil/cloud_security/Documents/u-cloud_computing_srg_v1r1_final.pdf

諮問委員会（CIPAC）、連邦上席リーダーシップ会議（FSLC: Federal Senior Leadership Council）などを通じてDHSとSSA（セクター別管轄省庁）の協力が行われている。主な活動の大半は計画とアウトリーチに焦点を絞った内容となっている。

- 国家サイバーセキュリティ通信統合センター（NCCIC）による対応
  - 国土安全保障省（DHS）とセクター別管轄省庁（SSA）の間の情報共有とインシデントへの対応に関する協力は国家サイバーセキュリティ通信統合センター（NCCIC）およびその様々な関連団体、特に産業制御システム・コンピュータ緊急事態対策チーム(ICS-CERT[106])と産業制御システム共同作業グループ(ICSJWG[107])を中心に展開されている。

[106] the Industrial Control Systems Cyber Emergency Response Team
[107] the Industrial Control Systems Joint Working Group

1.5.サイバー攻撃事案の分析とサイバー攻撃主体の能力測定

1.5.1.　US-Cert のミッションと脅威分析等

DHSのNCCIC（国家サイバーセキュリティ・通信統合センター）の傘下機関として官民連携で新設されたUS-CERTの主な役割のひとつは、サイバー攻撃の脅威と脆弱性の分析・削減やインシデントレスポンスおよび新興サイバー脅威に関するデータの分析などがある[108]。

US-CERTとNIST（国立標準技術研究所）が定義する米国連邦政府内のコンピュータセキュリティインシデント（事件）とは、セキュリティ政策や利用政策または標準セキュリティ慣行に違反する差し迫った脅威である[109]。NISTの「SP 800-61 rev.1（2008年03月[110]）」によると、「組織が定めるセキュリティポリシーやコンピュータの利用規定に対する違反行為1 または差し迫った脅威、あるいは、標準的なセキュリティ活動に対する違反行為または差し迫った脅威を示す」。「事象」とは、システムまたはネットワークで識別できるあらゆる出来事のことをいう。これには、ユーザによるファイル共有への接続、サーバへのウェブページ受信要求、ユーザによる電子メール(Eメール)の送信、ファイアウォールによる接続のブロックなどが含まれる。NISTのセキュリティインシデント対応に関するガイドや手引き等に米国政府によるサイバー攻撃インシデントや事案等の分析に際して使われる標準的な着眼点や論拠等の詳細が記載されている（詳細はIPAのセキュリティ関連文書[111]を参照）。

さらに、US-CERTは分析を目的にユーザに対してコンピュータセキュリティインシデントの報告と悪意のあるアーティファクト（Malware Artifacts）を求めている。サイバー攻撃や新興サイバー脅威に関するデータを分析すると、US-CERTはこの分析結果を定期的に報告書の形で公表している[112]。

2017年4月1日に発効した「US-CERT連邦インシデント告知ガイドライン（US-CERT Federal Incident Notification Guidelines[113]）」では、連邦政府各省庁（D/As）、州政府・地方政府、ISAO（情報共有分析組織）および民間セクターの組織等に対して、インシデント告知をNCCIC（国家サイバーセキュリティ・通信統合センター）及びUS-CERTに送達するための

---

108 https://www.us-cert.gov/about-us
109 https://www.us-cert.gov/about-us
110 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
IPA の翻訳：https://www.ipa.go.jp/files/000025341.pdf
111 https://www.ipa.go.jp/security/publications/nist/index.html
112 https://www.us-cert.gov/about-us
113 https://www.us-cert.gov/incident-notification-guidelines

指針を示している。また、2014年のFISMA（連邦情報セキュリティ現代化法[114]）では、インシデント（重大事件に発展する危険性をもつ出来事。セキュリティインシデントまたは情報セキュリティインシデントとも称されている）を「1)合法的な権限をもたずに、情報または情報システムの整合性または機密性あるいは利用可能性を実際にあるいは切迫して脅かす出来事または2)法律、セキュリティポリシー、セキュリティ手順または容認された利用方針に違反する差し迫った脅威」であると定義している。

1.5.2. 重要インフラ防護のサイバー対策における官民連携（PPP）

クリントン政権時代から、連邦政府は官民パートナーシップ（PPP)を柱とする重要インフラのセキュリティとレジリエンスの強化アプローチを一貫して支持してきた。官民連携（PPP）方式が選考されたのは、米国の重要インフラの大半が民間部門によって所有・運用されているためである。こうした官民パートナーシップの重視を受けて業界もそれを「受け入れ（buy-in)」、重要インフラのセキュリティと耐性に対する連邦政府の取組みに積極的に関与してきた。PPP（官民連携）によるサイバーセキュリティとレジリエンスの強化に向けた主な取組内容は次の通りである。

- 先述のように、クリントン政権はPDD（大統領決定指令）-63を公布した際、官民パートナーシップを利用して重要インフラのセキュリティと耐性に対処することの重要性を強調した。
- こうした官民パートナーシップの重視はブッシュ政権とオバマ政権にも引き継がれ、両政権ともNIPP（国家インフラ防護計画）を通じて官民連携の様々な仕組みを作り上げた。
- 3つの政権すべてが官民パートナーシップの構築を重視した背景には、米国の重要インフラのほとんど（約85%）が民間部門によって所有または運用されているという事実がある[115]。
- NIPPや様々なSSPに基づいて形成された官民パートナーシップは、次のような方法により米国の重要インフラのセキュリティと耐性の強化を達成している。
  - より効果的かつ効率的なコミュニケーションに向けた、公共部門と民間部門間および各々の内部のフォーラムの新設（GCC（政府調整会議)、SCC（セクター調整会議)、CIPACなどの仕組み)。これらのフォーラムは特に次の点で有用である。

---

114 http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title44-section3552&num=0&edition=prelim

115 United States of America. Government Accountability Office. CRITICAL INFRASTRUCTURE PROTECTION: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics. By Eileen Larence. Government Accountability Office, 15 Nov. 2016. Web. 23 Nov. 2016. <http://www.gao.gov/assets/260/252603.pdf>.

- 特定の重要インフラセクター内の重要資産の特定および様々なセクター間に存在する相互依存性の分析
- 様々な重要インフラセクターをまたぐ、および各セクター内における主要な R&D のニーズの特定
- 自主または強制基準・規制の基礎として利用可能な業界のベストプラクティスの特定

➢ 重要インフラのセキュリティと耐性に関わる連邦機関の役割と責任について、米国政府と業界間で共有される期待事項の作成

➢ セキュリティインシデント（サイバーおよび物理的）に関する公共・民間部門間の情報共有を可能にするセクター固有の ISAC 新設の促進。こうした情報共有は、政府と業界の状況認識の改善および公共・民間部門間の信頼できるコミュニケーション経路の確立に不可欠である。

- 米国政府の状況認識：情報共有により、米国の重要インフラが直面する脅威（サイバーなど）に関する米国政府の理解が深まる。
- 業界の状況認識：情報共有により、重要インフラの所有者・運用者はインテリジェンス状況説明へのアクセスが可能になり、自身の防衛体制を改善できる。
- 信頼できるコミュニケーション経路：低位影響インシデント発生中の情報共有により、連邦政府と業界間に信頼できるコミュニケーション経路が確立され、米国の重要インフラに影響する高位影響または重大なインシデントの発生時にそれを活用できる。

<u>官民パートナーシップ（PPP）モデルの成功</u>

重要インフラと耐性に対する官民パートナーシップ重視のアプローチは、過去 20 年間活用され、数多くの成功を生み出してきた。中でも特筆されるのは、業界が支援するサイバーセキュリティの自主基準の開発、共同 R&D プログラム、および連邦が資金援助する R&D の成果の商業化（from lab to market）の取り組みである。これらのイニシアティブの成功を受けて、業界は官民パートナーシップモデルを広く「受け入れ」、現状を将来も維持することを支援してきた。

❍ NIST サイバーセキュリティフレームワークの開発は、重要インフラのセキュリティと耐性に対する連邦政府の官民パートナーシップのアプローチの成功を代表するものである。

➢ NIST サイバーセキュリティフレームワークは業界の自主基準とベストプラクティスの集大成であり、各組織が自身のサイバーセキュリティリスクを管理する

のに寄与する。このフレームワークは、重要インフラ組織がサイバーリスクを管理するのに役立つガイドラインやベストプラクティスを提供する。

- NIST、米国政府の連携組織および業界は、200 以上の多様な公共・民間部門の事業体から提出された 2,000 件以上のコメントを考慮に入れた広範かつ協力的なプロセスによりこのフレームワークを作成した。
- このフレームワークが共同開発されたという経緯から、それを採用する公共および民間組織の数が増えており、急速に米国のサイバーセキュリティの標準になりつつある。
- NIST サイバーセキュリティフレームワークは本報告書のセクション V パート C で詳細に説明されている。

- 重要インフラのセキュリティと耐性に関する連邦政府の官民パートナーシップの重視がもたらした別の成功例は共同 R&D プログラムである。
  - NESCOR、DOE の電力網整備研究コンソーシアム（Grid Modernization Laboratory Consortium）および NSF（国立科学財団）のサイバー・物理システムプログラム（Cyber-Physical Systems Program）などの取組みは、官民協力を促進し、米国の重要インフラのセキュリティや耐性を支える技術を生み出し続けている。
  - これらを含む R&D プログラムはセクション IV パート B で詳細に説明されている。
- 重要インフラのセキュリティと耐性を支える R&D の実施に加え、米国連邦政府は、自身の R&D の成果の商業化を目指す官民パートナーシップも主導している。
  - DHS の実践への移行（Transition to Practice）および DOE の電力網向け高信頼性サイバーインフラなどのプログラムを受けて、連邦が資金援助する R&D から新たなサイバーセキュリティ製品が確実に商業市場にもたらされるようになっている。
  - これらのプログラムおよび「研究成果の商業化」に対する米国連邦政府の全体的アプローチはセクション IV パート C で詳細に説明されている。
- NIST サイバーセキュリティフレームワーク、共同 R&D の取組みおよび連邦の R&D の商業化など、重要インフラのセキュリティと耐性に関する官民パートナーシップの成功は、業界による広範な「受け入れ」、支持および参加を生み出した。
  - 米国の産業界は官民パートナーシップにより、米国政府の政策やプログラムの策定について積極的に発言する機会が与えられたため、総じて現在のアプローチを支持してきた。
  - さらに産業界は、重要インフラの所有者や運用者に対する官製の包括的な強制基準・規制の策定に代えて、業界が策定した自主基準（NIST サイバーセキュリティフレームワークなど）を指向する米国政府の姿勢を歓迎してきた。
  - 産業界は、政策やプログラムの策定に対して積極的な関係者であり続けること、および官製の包括的な強制基準・規制の使用が今後も限定的にとどまることを

望んでいることから、次期以降の政権の連邦政府が現行アプローチを維持することへの広範な支持がみられる。

重要インフラ防護（CIP）に伴うPPPの難しさ

米国連邦政府が重要インフラのセキュリティと耐性に向けて官民パートナーシップを広範に活用したことは、全体的に成功を収めた。とはいえ、この公共・民間部門間の連携は過去数年、特に情報共有、規制の「なし崩し的移行（creep）」および「行き過ぎ（overreach）」に関して困難性に直面してきた。

- 情報共有：政府と産業界がサイバー脅威の情報を共有できるようにすることは、サイバー攻撃や物理的攻撃から米国の重要インフラを防御するための連邦政府のアプローチにとって重要側面の1つをなす。
  - 産業界は、原則として情報共有プロセスを受け入れる姿勢を取る一方、提供した情報が何らかの形で不利に使用される可能性について留保を保持してきた。
  - 例えば、提供情報が規制目的に使用されたり、情報公開法（Freedom of Information Act）に基づく要求の対象となったり（信用が傷つく情報が公表される恐れ）、あるいはビジネス上の機密情報の場合、政府のずさんな取扱いを受けたりすることへの懸念を表明した。
  - 米国連邦政府は、これらを含む懸念に対処するため、2015年CISA（サイバーセキュリティ情報共有法）を通じて産業界に様々な賠償責任保護（liability protection）を提供した（セクションⅠパートBで詳細に説明）。
  - この法律は、情報共有に関する産業界の懸念の一部（全部ではない）を解消するのに役立ち、ISACおよびAISなどのプログラムへの参加を拡大する道が開かれた。
- 規制の「なし崩し的移行」および「行き過ぎ」：産業界は、規制の「なし崩し的移行」（合意に基づく自主基準から強制的規制への移行）および規制の「行き過ぎ」（重複的または過度の規制の制定）に対しても懸念を示してきた。
  - 「なし崩し的移行」に関しては、特に、米国連邦政府がNISTサイバーセキュリティフレームワークを自主基準から連邦の強制基準に切り替える可能性を懸念している。政権交代を控え、産業界は、トランプ政権がこのフレームワークの自主的な性質を維持することを擁護している。
  - 規制の「行き過ぎ」に関しては、産業界は、エネルギーや原子力、DIB（防衛産業基盤）など、これまで米国で厳しい規制に直面してきたセクター以外を対象に、連邦のサイバーセキュリティ規制が策定される可能性を最も懸念している。
  - 連邦のサイバーセキュリティ規制がすでに存在しているセクターの業界は、基

準の簡素化や重複的な規制の回避を求めている。

1.5.3. 米国国家諜報局（DNI）のグローバル脅威評価

米国のインテリジェンスコミュニティ（US Intelligence Community）のグローバル脅威評価（Worldwide Threat Assessment）は、国家諜報局（DNI- US Director of National Intelligence）の年次報告書である。この報告書は、様々な技術分野における米国の安全保障に対する世界的な脅威と、地域毎の国別脅威について概説している。

- 国家諜報局（DNI）は毎年、最新の情報により脅威の関連性を評価するので、報告書に含まれている脅威のカテゴリー別、地域別の内容は年により変化する。
- 国家諜報局（DNI）は毎年、2月に公開聴聞会でグローバル脅威評価を次の3つの議会委員会に提出している。
  - インテリジェンス特別委員会（House Permanent Select Committee on Intelligence）
  - 上院インテリジェンス特別委員会（Senate Select Committee on Intelligence）
  - 上院軍事委員会（Senate Armed Services Committee）
- 2004年の情報改革・テロ防止法(Intelligence Reform and Terrorism Prevention Act of 2004)によって国家諜報局（DNI）の地位ができるまでは、中央情報局（CIA）長官が上記の委員会に対して毎年脅威評価の報告を行った。
- グローバル脅威評価のいくつかのバージョンは、少なくとも1996年以降、毎年、おそらくはさらに過去から発行されている。
- グローバル脅威評価のヒアリングは、常に公開である。しかしながら、DNIはその後、非公開ヒアリングの中で、世界の脅威に関するより詳細で極秘の報告を委員会に行っている。

2016 年のグローバル脅威評価では、情報機関はサイバーセキュリティの問題の蔓延と拡大傾向の継続を予測した。その中でも、特に強調されたのが民間インフラ、政府システム、商業ベンチャーのサイバー脆弱性である[116]。これらのグループによるインターネットやネットワーク化されたデバイスへの依存の増加は、効率性と利便性の向上に貢献したが、同時に新しいサイバーセキュリティリスクをもたらした。この評価で概説されている具体的なサイバーセキュリティの懸念事項は次のとおり。

- IoT（モノのインターネット）：IoT（Internet of Things）は効率性と利便性を高

[116] https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf

める可能性があるが、セキュリティの脆弱性という新たなリスクを生み出すこともある。 IoTのセキュリティ脆弱性リスクには、身分証明、場所、監視と傍受、ネットワークアクセス、ネットワークク証明アクセス、採用ターゲットが含まれる。

- 人工知能（AI）：AIと自律的意思決定システムは、民間部門と防衛部門の両方で効率と性能を向上させる。しかし、AIへの依存はセキュリティシステムを新しい脅威にさらし、またAI自体が予期せぬリスクを引き起こす可能性もある。
- 拡張現実とバーチャルリアリティ：拡張現実とバーチャルリアリティは、コミュニケーションの新しい場を提供する。このテクノロジーがシステムと接続されると、将来の脅威につながる可能性がある。
- 重要インフラ：重要インフラは益々さまざまなサブシステムにリンクされ、日常生活を支えるサービスやユーティリティに新たなセキュリティの脆弱性が生じる。
- 検閲と反匿名性規制：世界中の多くの国が、検閲や反匿名の規制を通じた情報の政府統制を主張しようとしている。
- カウンターインテリジェンス：カウンターインテリジェンスの目的で、外国の諜報機関により個人情報が購入されたり、盗まれたりする。
- 帰属の難しさ：サイバー攻撃に対する責任の帰属は、サイバー能力が高度な国にとってさえ困難である。攻撃や攻撃者が精巧になるにつれて、帰属はさらに困難になる。
- サイバー攻撃抑制のむつかしさ：国家および非国家主体がサイバー攻撃をするのを抑制することはほとんど進展していない。 2015年のG-20協定において、国が主導する商業利益のためのサイバースパイを終了させるという合意がなされた。少ない中でもこの分野におけるいくつかの肯定的な進展の1つである。

2014 年から 2016 年の 3 つのグローバル脅威評価は、存在するサイバーセキュリティの脅威の重大性と多様性の増加という同じような傾向を示した。しかし、各評価はサイバーセキュリティの異なった面に焦点を当てている。

- 2014年の報告書は、国のデジタルコンテンツコントロールに対する国際規範や規制に影響を与えようとしていたロシアや中国などのような、地政学的懸案事項に強く重点が置かれていた。この報告書はまた、犯罪分子によるテロリストの募集と悪意のあるソフトウェアの拡散に対する懸念を強調した[117]。
- 2015年の報告書は、民間部門へのサイバー攻撃のリスクとコスト、さらには政治的に動機付けされた攻撃（「ハックティビズム（hacktivism）」と呼ばれることもあ

117
https://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf

る）の増加に焦点を当てている。 2015年の報告書によれば、米国のシステムに対する単独者による致命的な攻撃が技術的に可能である一方で、小さなサイバー攻撃やサイバースパイが積み重なることにより、米国が経済と国家安全保障への長期的なコスト負担に直面する可能性が高いと指摘している[118]。

- 2016年のレポートは、新興テクノロジーとそのサイバーセキュリティへの影響に焦点を当てている。 2016年のレポートの構成は、過去の単独の「サイバー」セクションを止め、初めて「サイバー&テクノロジー」セクションを含むレポートとなった。
- 単なる「サイバー」から「サイバー&テクノロジー」への移行は、お互い、あるいはインターネットにリンクされたオブジェクトやデバイスの最近の普及、および人工知能の出現と成長を反映している。
- 2016年の世界脅威評価は、2014年と2015年の報告よりも多様なサイバーセキュリティ問題を反映している。 2016年の報告書の内容は、2015年の報告書の12のカテゴリーと、2014年の報告書の8つのカテゴリーと比較して、16のカテゴリーと大きく増えている。

過去 3 年間のグローバル脅威評価は、ますますネットワーク化されたシステムとデータを防護しようとする人々と、同じシステムやデータを奪い、破壊しようとする人々の間で、武器競争と並行しながら、サイバーセキュリティも変化することを示している。

- サイバーセキュリティにおける攻撃的および防衛的開発は、他の武器競争と同じ原則に従う。攻撃的な進歩は最終的に、それを防止、回避または対抗するように設計された防護措置に対応し、一方、防護措置は最終的に、攻撃的な技術や防護措置を打ち負かし、回避する策に対応する。
- 人工知能の技術的進歩は、サイバーセキュリティの進展を複雑にしている。この分野が成熟し続けるにつれ、どのような種類の能力と脆弱性が発展するかは不明である。
- ネットワーク化されたテクノロジーと AI の効率、性能、コストの利点により、すべての行為者（actors）によるそれらの使用が確実に増え続けるようになる。そのため、新しく複雑な脆弱性が作られ、サイバー戦争の武器競争の継続と深化につながる。

1.5.4. 米国の国際サイバー政策の進展

2011 年 5 月、オバマ政権は「国際サイバースペース戦略（International Strategy for

[118] https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf

Cyberspace)」を発表した。この文書は、米国の国際サイバー活動の重要な政策ガイドラインであり、オバマ政権のサイバー問題に関する世界共同体への取り組みに基づいている。

- ジョージ W ブッシュ政権においては、サイバー問題に関する世界共同体との関わりは限定されていた。
  - ブッシュ政権が関与した唯一の主な国際サイバー協定は、サイバー犯罪に関するブダペスト条約（Budapest Convention on Cybercrime）である。ブッシュ政権は 2001 年に条約に署名し、米国上院は 2006 年にそれを批准した[119]。
  - サイバー犯罪に関するブダペスト条約は、著作権、コンピュータ関連詐欺、児童ポルノ、ネットワークセキュリティ違反に関連するサイバー犯罪に対処することを目的として、複数の国の間で共通の刑事政策を確立した。
- 2010 年以降、オバマ政権は、サイバーセキュリティの問題に対処するために、国際社会に関わる意欲の高まりを示した。例えば、2010 年 7 月、米国を含む国々のグループは、国連においてサイバー規範に取り組むことに合意し、国連が合意されたサイバー行動規範を作成し、国内法制やサイバーセキュリティ戦略に関する情報を交換し､開発途上国のコンピュータシステムを保護する能力を強化するよう勧告した[120]。
- 2011 年 5 月、オバマ政権は「サイバースペースのための国際戦略（International Strategy for Cyberspace)」を発表した。この政策文書は、オバマ政権の大規模な世界共同体への関与戦略の一環とみなされた。これが、サイバー規範と価値観を向上させるための共同国際的パートナーシップのビジョンを示した最初のものとなった[121]。

「サイバースペースのための国際戦略」は、米国が国際社会に参加して、国際社会のためのオープンで相互運用性があり、安全で信頼性の高いインターネットインフラを確保するための戦略を概説している。この戦略は国の行動を導く責任ある行動規範を作成する必要性を強調している。特に、戦略は、国際的なサイバー目標を推進するための米国の政策優先事項を概説している。

- 経済：米国は、知的財産を保護しながら、技術革新を促し、市場を開放するための国際基準を推進すべきである。
- ネットワーク保護：米国は、二国間および多国間のパートナーシップを通して、IT

119 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=RLjffIEn

120 http://www.washingtonpost.com/wp-dyn/content/article/2010/07/16/AR2010071605882.html

121 https://www.washingtonpost.com/world/obama-administration-outlines-international-strategy-for-cyberspace/2011/05/16/AFokL54G_story.html

インフラのセキュリティ、信頼性、および回復力を強化する必要がある。

- 法執行：米国は国際的なサイバー犯罪政策の策定に継続的に参加し、各国間のサイバー犯罪法を調和させるべきである。
- 軍隊：国防総省は、サイバー協力を拡大し、サイバースペースにおける集団安全保障を強化するために、同盟国およびパートナーの軍隊および民間人と協力しなければならない。
- インターネット管理：すべてのユーザが包括的なインターネットを使用できるように、米国はオープンなインターネットを促進し、インターネット管理の問題を議論するために複数の利害関係者の会合を開催する必要がある。
- 国際開発：米国は、他国を支援して、その国がサイバーセキュリティ能力を構築し、サイバー犯罪対策のベストプラクティスを開発するとともに、サイバー犯罪対策能力を強化することができるように努めるべきである。
- インターネットの自由：米国は、世界中のすべてのインターネットユーザーに基本的自由とプライバシー保護を保証する必要がある。

「サイバースペースのための国際戦略」は、国際的なパートナーシップの指針となる防衛および安全保障政策の規範を確立するために、同じ考え方の国々と協力することを強調している。国家行動を導く長期的な国際規範がサイバースペースにも適用されることに留意して、セキュリティと防衛政策の一部には次のものが含まれる。

- 自己防衛権を留保して、サイバースペースにおける潜在的な攻撃的行為に対処できるようにする。
- 開発途上の同盟国やパートナーにサイバー防衛能力を築くことを支援する。
- 進行中の調査に欠かせないデータを保存し、立法府と司法省と協力してアプローチを調和させ、正当なプロセスと法律を促進するために、他の法執行機関と協力してサイバー犯罪を抑止する。
- 他の国と協力して状況認識とインシデント対応の仕組みを拡張することにより、IT インフラの堅牢なインシデント管理、回復力、および復旧機能を確保する。
- 業界および国際パートナーと協議して IT サプライチェーンのセキュリティを向上させる。
- 情報システムと重要インフラストラクチャを保護するためのベストプラクティス他国と共に開発する。

2011 年以来、国務省（DOS）のサイバー・イシュー・コーディネーターオフィス（Office of the Coordinator for Cyber Issues（S/CCI））は、米国政府内においてリーダー的立場

で「サイバースペースのための国際戦略」の目標達成にむけて努力してきた[122]。S / CCI コーディネータのクリストファー・ペインター（Christopher Painter）はサイバースペースのための国際戦略の実施に向けて S / CCI を率いてきた。このオフィスの責任は次のとおり。

- サイバー問題に関する国務省のグローバルな外交的取り組みを調整する。
- 国際的なサイバースペースの問題について、ホワイトハウスと連邦政府の省庁に対する国務省のリエイゾンとしての役割を果たす。
- サイバー問題と取り組みについて国務長官と副長官に助言する。
- サイバー問題に関する官民団体とのリエイゾンとしての役割を果たす。
- これらの分野に従事する国務省内の地域および機能局の作業を調整する。

2011 年以来、米国の国際サイバー政策を見直し、更新する努力がなされている。たとえば、2015 年 11 月、米国のマイク・マッコール議員（共和党、テキサス州）は、「サイバースペースのための国際戦略」に関する報告書を要求する「2015 年サイバー政策監督法」という条項を導入した[123]。

- 「2015 年のサイバー政策監督法」は、オープンで、相互運用可能で、安全で信頼性の高いインターネットインフラの推進方法を概説した報告書を提出することを DOS に要求する。 マッコール議員は、現在の米国の国際的なサイバー政策を見直して、政策の側面を更新すべきかどうかを判断しようとしている。
- この法案が 2015 年 11 月に米国下院外交委員会（US House of Representatives Foreign Affairs Committee）に提出されたが、2016 年 12 月の立法会議の終了する前に、この法案の措置が取られる可能性は低い。

[122] http://www.state.gov/s/cyberissues/
[123] https://www.congress.gov/bill/114th-congress/house-bill/3873/text

2. 中国のサイバー空間に関わる体制・能力等の実態

サイバー空間管理の目的はサイバーセキュリティの確保である。しかし、サイバーセキュリティの概念は各国によって千差万別である。とくに、民主主義国家である欧米諸国/日本と、社会主義国家である中国、ロシア及び北朝鮮とは大きく異なる。

欧米諸国/日本では、通信・金融・エネルギーなどをはじめとする「国民の社会生活や経済活動の基盤となっている国家重要インフラに対するサイバー攻撃」を脅威と見なし、その保護を目指してサイバーセキュリティをとらえている。前提として、サイバー空間は基本的に自由なものと位置づけている。

しかし、社会主義諸国では、国家重要インフラへの脅威だけでなく、「国内体制を不安定にする情報」も脅威とみなしている。サイバー空間を政府がコントロールすべきとしてとらえ、「その情報が脅威にあたいするか否か」を決めるのは当該政府であり、その意図のもとにサイバーセキュリティが運用される。中国とロシアはこの理念を国家戦略として明確にかまえており、イランをはじめとするアラブ諸国もこれに近い。

両者の隔たりは小さくなく、大まかには米国主導のサイバー空間管理に中国とロシアが共闘して抵抗する構図にある。例えば、サイバー犯罪を規制するための国際条約「サイバー犯罪条約」においては、2017 年 7 月の発効から米国・欧州諸国/日本など主要国が相次いで締約するなか、中国・ロシアが共闘して対抗している[124]。

本調査における、中国、ロシア及び北朝鮮のサイバー空間動向に対する米国の分析、評価も、上記の背景が反映されている。

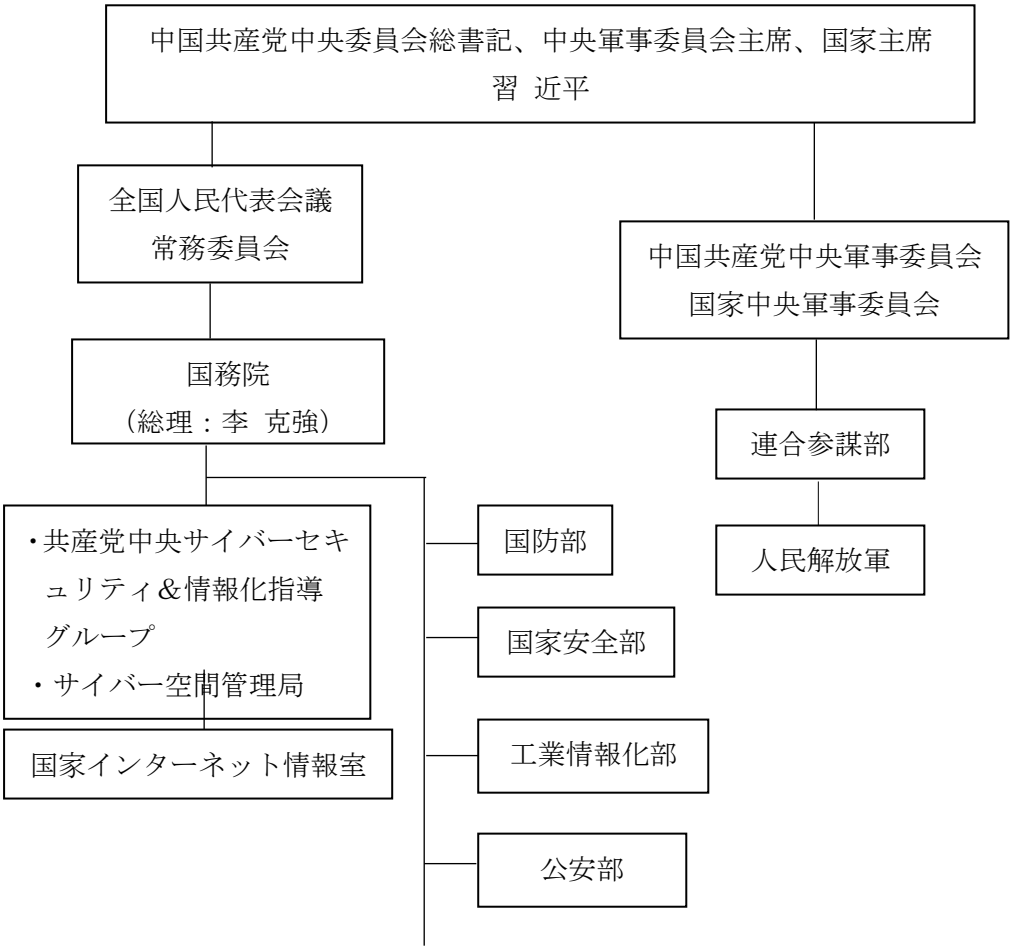
[124] http://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html

2.1. サイバー空間に関わる国家組織

2.1.1. 国家組織の概要

中国におけるサイバー空間に大きな関わりを有する国家組織の概要は下図の通りである。但し、この図は本調査報告書において、サイバー空間に関わる体制・能力の実態を説明するため便宜的に作成したもので、中国国家の組織を正確に示したものではないことに留意されたい。中国の国家サイバー関連機関は、次の二つの系統に大別することができる。

【サイバー空間に関わる主要な国家組織】



出所：各種資料を基に IBT にて作成

上の図で示した通り、1 番目は、最高国家行政機関である国務院とその傘下の共産党中央サイバーセキュリティ＆情報化指導グループ、サイバー管理室、国防部、国家安全部、工業情報化部および公安部である。その他にも、科学技術部、教育部、民生部も各部署の立場でサイバー空間に関わっているが、下の図では特にサイバーと関係の深い部署のみを示した。国務院の系統では、サイバー空間が一党独裁体制を不安定にすることを懸念する中国政府の国内に対する厳しい規制への取り組みが目立つ。

2 番目は、中国共産党中央軍事委員会とその傘下の連合参謀部、人民解放軍の軍事系統である。国務院に所属する国防部は人民解放軍への指揮権を有しておらず、シビリアンコントロールではない。最近では、軍事力の中で、陸、海、空、宇宙とともにサイバー空間が大きな位置づけを与えられている。そのため、軍の近代化の中でサイバー戦闘力を強化する政策が次々と打ち出されている。

中国は情報鎖国であると言われる通り、サイバー空間に関する正確な情報も日本側から取得するのは難しい。本調査では、可能な限り中国政府機関が発表した公式情報を使用したが、補完資料として米国の政府機関及び著名な研究機関が公開している報告書を参照した。軍関係では日本の自衛隊関係者が発表している論文も参照した。加えて、多くの中国市民が目にしているニュースサイトの記事も参照した。

2.1.2. サイバーセキュリティ＆情報化指導グループ

国務院直轄下の中共中央サイバーセキュリティ＆情報化指導グループ（Office of Central Leading Group for Cyberspace Affairs）[125]とサイバー空間管理局（Cyberspace Administration of China: CAC）[126]は同一のホームページ上に存在しているので、これら二つの組織は一体となって運営されていると見られる。中央サイバー安全・情報化指導グループのタイトルには中国共産党のロゴマークがついており、サイバー空間管理局のタイトルには中国政府のロゴマークがついている。これら二つの組織のトップは徐麟主任（兼務）である。同氏はまた中国共産党宣伝部副部長、国家インターネット情報室主任も兼務している。政府と共産党が一体となって、中国国内のサイバー空間を強力な権限をもって管理していることが判る。

徐麟主任

[125] http://www.cac.gov.cn/
[126] http://www.cac.gov.cn/

- 维基百科や China Vitae127等によると、徐麟（Xu Lin）は 1963 年 6 月に上海市で生まれる。上海師範大学を卒業後、1982 年 9 月に共産党に入党。上海市南匯区周浦中学教師を経て、上海市の南匯区共産党委員会を皮切りに、1995 年に上海嘉定区共産党委員会の副書記に就任。1997 年に上海衣工商(集団)有限公司の総経理に就任。その後、董事長をへて中共上海市民政局局長から 2013 年 5 月に中共上海市委常委、宣伝部部長に昇格。2015 年 6 月、2014 年に設置された共産党中央サイバーセキュリティ＆情報化指導グループ（中共中央网络安全和信息化领导小组）弁公室副主任に抜擢され、2016 年 6 月 29 日に魯煒に代わり主任に昇格。習近平主席の政治的盟友である。インターネット皇帝と評された魯煒[128]（Lu Wei）は 2017 年 11 月に反腐敗運動で摘発された。

サイバー空間管理局の役割は、ホームページに掲載されている情報に基づいて整理すると、次のカテゴリーに関する業務である。

- サイバー空間安全
- 情報技術向上
- ネットワーク通信
- サイバー空間人材育成
- 政策法規
- 違法監視
- サイバー空間に関する質問受付・回答
- 地方のネットワーク支援
- 関連業界管理
- 国際交流

ネットワーク通信のカテゴリーにおける最近の活動例を示すと、次の通りである。

【サイバー空間管理局、ネットワーク製品とサービスの安全審査暫定対策を公布[129]】

サイバー空間管理局は 2017 年 5 月 2 日に「ネットワーク製品とサービスの安全審査暫定対策（Trial Measures for Security Review of Network Products and Services)」（以下、暫定対策という）を公布した。この暫定対策はネットワーク製品とサービスに対する全国

127 http://www.chinavitae.com/biography/Xu_Lin
128 https://www.bloomberg.co.jp/news/articles/2017-11-22/OZSZ086K50XS01
129 http://www.cac.gov.cn/2017-05/02/c_1120904567.htm

規模の安全審査制度への第一歩と見なされている。暫定対策が対象とするのは、国家の安全に関わるネットワークと情報システムが購入する製品とサービス、及び同じく国家の安全に関わる重要インフラ事業者が購入する製品とサービスである。暫定審査の概要は次の通りである。

- 主な審査項目は次の通りである。
  - 製品とサービスの安全リスク、不法に制御され、改造され、破壊された製品とサービスのリスク
  - 製造、検査、輸送及び製品と重要部品への技術的サポート提供などで構築されるサプライチェーンの安全リスク
  - 製品とサービス提供者によるユーザ情報の不法な収集、保管、取り扱いと利用によるリスク
  - ネットワーク安全とユーザの利益を、プロバイダが製品とサービスへの有利な立場を利用して危うくするリスク
  - その他の国家安全リスク
- 安全審査に携わる機関とそれぞれの役割は次の通りである。
  - ネットワーク安全審査委員会
    - 重要な政策の検討
    - ネットワーク安全審査の組織化
    - ネットワーク安全審査の重要事項の調整
  - ネットワーク安全審査室
    - ネットワーク安全審査の実務担当者の任命
    - 第三者機関とネットワーク安全審査専門委員会の設置
    - 審査結果の公開と告知

ネットワーク安全審査専門委員会は、ネットワーク製品とサービスの安全リスク、及びプロバイダの安全と信頼性を第三者機関の査定に基づいて評価する。暫定対策は安全審査制度の枠組みを構築したが、実施のための詳細な内容が不明である。関連企業はコンプライアンスのために今後の展開を注意深く見守る必要がある。

サイバー空間管理局は、下部組織として国家インターネット情報室を有している。この国家インターネット情報室（国家互联网信息办公室[130]）は、インターネット管理に関する下記に示す幅広い業務を担っている。

- 中国サイバー安全法に係る規則・ガイドライン等のドラフト作成

130 https://baike.baidu.com/item/国家互联网信息办公室/2045128?fr=aladdin

- インターネット情報の拡散に関する法規の構築、および政策、ガイダンス等に係る立案と実施、これらの省庁間の調整
- ネットワークゲーム、オーディオビデオなどインターネットコンテンツの適切な計画・管理
- ニュースサイトの常時監視、不適切情報の削除
- インターネット接続、ドメイン登録、IP 付与、その他のインターネット関連ビジネスの許認可、法規違反者への懲罰
- 中国サイバー空間安全協会などの業界団体を監督・指導して、サイバー空間に関わるさまざまな官民連携を推進

また、国家インターネット情報室は 2015 年 1 月に中国サイバー空間研究院を設立した。この研究院は、インターネット分野における世界トップレベルのシンクタンクとして、情報とネットワーク安全に関して、戦略的支援、研究支援、人材育成そして技術支援を通じて国家計画と科学的決定を担うことを目的としている。研究院はその下部機構として幾つかの研究室を設置する。これらの研究室はそれぞれ、ネットワーク安全、情報技術、インターネット情報と通信、メディア統合化、その他を担当する。研究院は設立されてからすでに 3 年経過しているがホームページは開設されておらずその活動実態は明らかにされていない[131]。

2.1.3. 公安部

公安部（Ministry of Public Security of the People’s Republic of China）は中国の司法警察活動を含めて、下記に示す広範囲な治安関係の業務を所掌する[132]。

- 防犯・犯罪捜査
- 交通管理
- 消防
- 危険物の管理
- 戸籍等の管理
- 出入国管理
- 外国人管理

実際の執行業務は地方政府の公安機関が担っており、公安部は、主として警察制度の企画立案と地方の公安機関に対する指揮監督・調整に当たっている。傘下に武装警察を擁し

131 http://news.mod.gov.cn/headlines/2015-01/25/content_4566802.htm
132 http://www.mps.gov.cn/

て、それに対する指揮権を有している。

2.1.4. 国家安全部

中国の諜報活動は、国家安全と軍事安全保障の二系統で実施されている。国家安全部（MSS-Ministry of State Security。略称“国安部”）は、非軍事部門の諜報機関であり、国務院の管轄下に置かれている。国安部（MSS）は、1983 年 7 月に中共中央調査部、公安部政治警備局および中共中央委員会統戦部の一部、国防科学技術委員会の一部などを統合して再編した諜報機関である。主な任務は、暗号通信及び管理、国際戦略情報収集、各国政治経済・科学技術情報集、情報分析通報、所轄各省庁業務指導、対スパイ情報収集・追跡・偵察・逮捕等である。本拠地は北京市東城区東長安街 14 号。外部の公式サイトは開設していない。

国家安全部の部長は、2016 年 11 月 7 日に就任した陳文清（Chen Wenqing[133]）である。

中央規律検査委員会と共同で政府の監察部門を指導する中国共産党中央政法委員会委員でもある。
1960 年 1 月に四川省で生まれる。1983 年 3 月に共産党入党。
四川省の公安局を経て 2015 年 4 月に国安部（MSS）の党委員会書記[134]。

ウィキペディア（維基百科）中国版[135]によると、国安部（MSS）は第一局（機要局：暗号通信及び管理）、第二局（国際情報局：国際戦略情報収集）から第七局（反間諜情報局：対スパイ情報収集）、第八局（反間諜偵察局）対外国スパイ追跡・偵察・逮捕等）から第十七局（企業局：担当組織所属企業、事業ユニットの管理まで 17 局で構成されている。

日本の自衛隊関係者の報告によれば下記の業務を担っている[136]。

- 情報セキュリティの研究、政府システムで使用される民間セクターの製品の認証
- 民間の情報セキュリティ関連企業の監督
- 公安部が関心あるテーマに関する研究への補助金の提供
- 公安部第 3 研究所
  - 人民解放軍と政府で使用するすべてのハードウェアとソフトウェアのための

133 http://www.ce.cn/ztpd/xwzt/2013bw/acb/index.shtml
134 https://baike.baidu.com/item/%E9%99%88%E6%96%87%E6%B8%85/21835
135 https://zh.wikipedia.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E5%9B%BD%E5%AE%B6%E5%AE%89%E5%85%A8%E9%83%A8
136 http://www.drc-jpn.org/annual_report/yokoyama_report_20170308.pdf

情報セキュリティ規準の作成の責任を有している。

- 第 3 研究所は、公安部が提供する補助金のさまざまな受領者と公安部との仲介や製品評価を行っている。

2.1.5. 工業情報化部（工信部）

工業情報化部（MIIT-Ministry of industry and information technology）の原語表記は、工業和信息化部（略称：工信部）である。1998 年に創設された信息産業部（MII）を母体として 2008 年に改組された部署である。

工業情報化部（工信部）の主な業務は、通信、情報技術開発、電子情報、情報安全、安全生産、原材料産業、装置産業、消耗品産業、中小企業、省エネルギー/環境保護、軍民融合、対外交流、統計分析、投資計画、その他に係るもので多岐にわたっている[137]。

工業・情報化部傘下のサイバー空間に係る部局・センター等は下記の通りである。

情報通信監理局

情報通信監理局はインターネットの管理を行っており、下記業務を担っている[138]。

- 電気通信とインターネットの監督
- インターネット（モバイルを含む）産業の管理
- 電気通信とインターネットのサービス市場への参入と機器類の管理
- インターネットドメインネームと IP アドレスの管理
- ウェブサイトへのアクセスインフラの管理
- 新規ビジネスの管理
- 電気通信とインターネットの市場競争、品質向上、ユーザ共通運用権及び個人情報保護の推進
- 情報ネットワークのコミュニケーションの管理と責任
- 緊急時コミュニケーションとコミュニケーションセキュリティの組織化と組織間調整

情報センター

情報センターは電子政府（e-government）の推進に向けた業務を担っている。主な業務は下記の通りである[139]。

137 https://web.archive.org/web/20081107070110/http://www.miit.gov.cn:80/n11293472/index.html
138 http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057709/n3057722/index.html
139

- 電子政府計画を推進、実施、そしてメンテナンスするに必要な技術的基準と規範の作成、電子政府の戦略と計画を作成への参加、電子政府指導的グループとしての作業
- 電子政府ネットワーク、情報安全、そして暗号に関する技術的支援
- 工業と通信の産業界の経済活動のモニタリング、今後の予測、早期警報システムと早期決定支援、そして同業界の統計データを担当
- 電子政府計画の技術的事項の支援と電子政府とさまざまな情報源の統合
- 各部のコンテンツ保証に必要な技術的支援
- 各部のネットワークインフラ、業務アプリケーション、緊急プラットホーム、コンピュータ端末と補助機器の日常作業と保守、およびこれらに関連する機器の購入
- 各部の情報関連人材の育成
- その他、工業・情報化部が所掌する業務

工業情報化部は新たにサイバー攻撃に関する情報収集を開始したと下記の通り報道されている。

【中国､サイバー防衛を目的とした中央データベース構築､2017 年 9 月 13 日のロイター[140]】

工業情報化部はサイバー攻撃に係る情報を集約化する制度を開始する。通信事業者、インターネット事業者およびドメイン名提供者に対して、トロイの木馬型マルウェア或いはハードウェア脆弱に係るインシデント、および悪意ある IP アドレスにリンクしたコンテンツなどを報告することを義務付けた。集約した情報データはインターネット業界と政府機関が共有する。工業・情報化部は、この新しい制度によりサイバー攻撃の脅威を減じることができるとしている。この制度に違反した場合、警告、罰金、その他の行政罰が課せられる。制度の実施は 2018 年 1 月であるが詳細内容は明らかにされていない。

---

http://xxzx.miit.gov.cn/InfoAction!findList.action?sectionId=M001&subsectionId=%E4%B8%AD%E5%BF%83%E7%AE%80%E4%BB%8B

140

https://www.reuters.com/article/us-china-cyber/china-beefs-up-cyber-defenses-with-centralized-threat-database-idUSKCN1BO12K

2.2. サイバー空間に関わる法規・政策・戦略

2.2.1. 法規・政策・戦略の最近の動向

2016 年 10 月 9 日、中国中共総書記の習近平（主席）サイバー（網絡）強国戦略の実践をテーマにした中央政治局第 36 回集団学習会において、サイバー空間の安全保障・防御能力の強化を加速し、IT 技術を利用する社会ガバナンスの推進を加速し、中国尾サイバー空間における国際的発言権とルール設定権の向上を加速し、サイバー強国建設の目標に向けて努力を怠らないことを強調した[141]。

以上の基本方針を踏まえて、中国政府はサイバー空間に関わる重要な法規・政策・戦略を相次いで発表した。主な政策は次の通りである。

- 2016 年 11 月 7 日、中国サイバー安全法採択（2017 年 6 月に施行)。原文：中華人民共和国網絡安全法（英文：Cybersecurity Law of the People's Republic of China[142])。
- 2016 年 12 月 27 日、国家サイバー空間セキュリティ戦略を発表。
- 2017 年 3 月 2 日、サイバー空間国際協力戦略を発表。

なかでも、中国サイバー安全法はこれまで分散していたサイバー空間関連の法律を集約した最上位に位置する法律である。サイバー空間の利用を厳しく管理・制限するもので、中国で事業活動を展開する海外企業にとって大きな影響が考えられる。この他にも、サイバー空間を巡るグローバル競争で主導権を握りたいとの中国指導部の思惑があるとみられる。

国家サイバー空間安全戦略は、中国サイバー安全法が目指す目標を簡潔かつ明瞭に示した。また、サイバー空間国際協力戦略は、サイバー空間の国際的秩序・ルールの構築に、社会主義国家である中国に不利にならないように積極的に関わる姿勢を明確に示したものである。

2.2.2. 中国サイバー安全法

中国サイバー安全法（中華人民共和国網絡安全法）は 2016 年 11 月 7 日に全国人民代表会議において採択され、2017 年 6 月 1 日に施行された。全 79 条で構成されており、インタ

141 http://politics.people.com.cn/n1/2016/1009/c1024-28763695.html
142 http://www.lawinfochina.com/display.aspx?id=22826&lib=law

ーネットにおける中国の主権確保と安全保障を目的に、中国で事業を行なう外国企業に対して、大きな影響をもたらすものである[143]。同法の要点を以下 6 項目に、関連する主要条項とともに示す。

【中国サイバー安全法の要点】

要点 1 個人情報の保護

第 22 条 ユーザ情報を収集するネットワーク製品およびサービス提供者は、ユーザにその旨通知し、同意を得なければならない。

第 41 条 ネットワーク運営事業者は、法律、行政規則、ユーザとの契約に基づいて個人情報を収集し、保管しなければならない。

第 42 条 ネットワーク運営事業は、収集した個人情報を開示、改ざんまたは破棄してはならない。

第 44 条 個人も組織も、個人情報を取得するために情報を盗んだり、他の違法な手段を使ったりしてはならない。

第 45 条 サーバーセキュリティを監視する法的責任を負う部署は、入手した全ての個人情報を必ず機密扱いにしなければならない。

要点 2 重要情報インフラのセキュリティ

第 31 条 国は、サイバーセキュリティ保護に関して、公共通信・情報サービス、エネルギー、金融、輸送、水保全、公共サービス、及び E ガバナンスに関する情報インフラ、並びに破壊された場合、機能しなくなった場合、またはデータが漏洩した場合に国家安全保障、国家経済および公共の利益に深刻な打撃を与える恐れのその他の重要インフラの保護を重視する。国務院は、重要情報インフラの範囲およびセキュリティ保護策を伝達する。

第 38 条 重要情報インフラの運営事業者は、単独で、またはネットワークセキュリティサービスプロバイダーと協力して、サイバーセキュリティ及びその他の潜在的リスクを少なくとも年 1 回評価しなければならない。運営事業者は、重要情報インフラ保護を担当する関係当局に、評価結果及び改善策を報告しなければならない。

要点 3 ネットワーク運営事業者の責任と定義

第 10 条 ネットワークを構築し、運営する場合、またはネットワークを通じてサービスを提供する場合には、ネットワーク運営を保護し、サイバーセキュリティインシデントに効果的に対処し、サイバー犯罪を防止するために必要な技術的対策およびその他の対策を講じなければならない。これらの対策は同時に、法律の規定および国家規格に準じて、ネットワーク、ネットワークデータの完全性、気密性およびアクセシビリティを維持しなければならない。

第 21 条 国は、サイバーセキュリティ保護のための階層化されたシステムを導入する。ネ

[143] http://www.cnca.gov.cn/bsdt/ywzl/flyzcyj/zcfg/201707/t20170711_54707.shtml

ットワーク運営事業者は、干渉、破壊または無許可のアクセスからネットを保護し、ネットワークデータの漏洩、改ざんまたは盗難を防止するため、所定のセキュリティ手順に従う必要がある。

第 22 条 ネットワーク製品またはサービスの提供者は、悪意のあるプログラムをセットアップしてはならない。自社の製品またはサービスにセキュリティの欠陥、脆弱性またはその他のリスクが発見された場合、ネットワークプロバイダーは直ちに是正策を講じ、ユーザに通知し、問題を関係当局に報告しなければならない。

第 76 条 ネットワーク運営事業者は、ネットワークの所有者・管理者とネットワークサービスプロバイダーを指す。

要点 4 機密情報の保持（中国国内で取得・生成した個人情報と重要データの原則国外移転）

第 37 条 中国国内で重要情報インフラ運営事業者が収集および生成した個人情報ならびに重要データは、国内で保管しなければならない。業務上の必要性により海外に転送される情報とデータについては、中国のサイバー空間管理機関および国務院傘下の関係部局が共同で定める評価基準に従って、セキュリティ評価を実施する。その他の法律および行政規則の関連規定も適用される。

要点 5 セキュリティ製品の認証

第 23 条 重要なネットワーク機器および特殊なサイバーセキュリティ製品は、資格を持つ機関の認証を受け、国家規格に準拠した場合に限り、販売または提供することができる。中国のサイバー空間管理機関および国務院傘下の関係部局は、重要なネットワーク機器および特殊な製品の一覧を作成する。

第 35 条 国家安全保障に影響を及ぼす可能性のあるネットワーク製品・サービスを導入する重要情報インフラ運営事業者は、国家安全保障審査に合格しなければならない。

要点 6 法的責任と罰則

第 64 条 サイバー安全法の第 22 条第 3 項、または第 41 条、42 条および 43 条に違反したネットワーク運営事業者あるいはネットワーク製品またはサービスの提供者は、その行為を是正しなければならない。かかる事業者は、警告を受け、不法に得た収入を没収され、不法に得た収入の 10 倍を上限とする罰金を科されるか、そのいずれかを科される場合がある。重大な事件においては、関係部局が事業活動の中止、ウェブサイトの閉鎖、ならびに事業証明または事業免許の取り消しを命じる場合がある。

第 66 条 サイバー安全法第 37 条に違反したネットワーク運営事業者またはネットワーク製品の提供者は、関係当局からその行為の是正を命じられる。当局は、警告を発し、不法に得た収入を没収し、5 万元から 50 万元の罰金を科すことができる。当局はまた、事業活動の中止、ウェブサイトの閉鎖、および事業証明または事業免許の取り消しを行なうことができる。

上記のサイバー安全法に対して、米国は下記の通り異議を申し立てている。

【米国は中国サイバー安全法の執行停止を求む[144]】

世界貿易機関（WTO）は、世界のサービス分野における取引が阻害されるとの理由で、中国サイバー安全法の執行停止を求める米国の文書を発表した。この法律は中国で活動する海外企業へ大きな影響を及ぼすもので、さらには現地企業と海外企業に対して安全検査と彼らのデータの中国内での保管を義務づけている。

米国は、WTOのサービス理事会に対して、中国サイバー安全法が計画通り2018年末までに完全に執行された場合、中国との国境を越えたサービスビジネスに大きな影響が生じるとして討議を要求した。同法は、通常のビジネスで行われている情報の伝達を混乱させ、妨げ、そして多くの場合禁止となる。米国は、中国の当局とすでにハイレベルの討議を行なっており、懸念される事項が解決するまで執行を停止するよう求めている。WTO加盟国が取引に与える影響の大きさを認識するようにこの文書を提出した。

中国のWTO代表であるZhang Xiangchen氏は、WTOの貿易の保護主義に関するパネルにおいて、同法に対する批判を過少評価した。中国が保護主義の汚名を科せられることに対して、保護主義の定義は明瞭でなく、WTO加盟国はそれぞれが自国の法を制定する権利を有する。そして、WTOの枠内でいずれの法が遵法で、いずれが違法か慎重であるべきと述べた。

【米国の法律事務所モリソン・フォスターの分析・評価[145]】

米国の代表的な法律事務所であるモリソン・フォスター（Morrison Foerster）[146]は、中国サイバー安全法を次のように分析・評価している。

中国サイバー安全法は中国のサイバー空間の主権とセキュリティを確保するための包括的な枠組み法である。法を運用するための重要な規則あるいはガイドラインは現在、中国サイバー管理局において作成中である。ドラフトの一部がパブリックコメントのために明らかにされているが、今後内容が確定されるに従い徐々に制定する計画である。中国で活動する海外企業がどのように適用されるか、現時点では正確には不明であるが多くの懸念

144
https://www.reuters.com/article/us-usa-china-cyber-trade/u-s-asks-china-not-to-enforce-cyber-security-law-idUSKCN1C11D1
145 https://www.mofo.com/
146 https://www.mofo.com/

事項が存在する。

重要情報インフラスツラクチャーを扱うネットワーク運営事業者事業者には多くの義務が課せられ、罰則対象となる。しかし、このネットワーク運営事業者の定義が広範囲で明瞭でない。同法では、まず「情報を収集・保管・交換・処理するシステムコンピューターおよびそのほかの情報端末ならびに関連する設備からなるシステム」を「ネットワーク」と定め、これを所有する者、管理する者、提供する者すべてが「ネットワーク運営者」と定義している。また、同法の附則では必ずしもインターネットに限定しておらず、情報の行き来が幅ひろく含まれることとなる。米国でネットワーク運営者といった場合は、主に通信事業者・無線通信事業者・インターネットサービス提供事業者を指すことが多いが、中国サイバー安全法ではこれに加えて､｢中国で IT ネットワークや情報システムを保有し、運営するありとあらゆる組織・企業」が含まれることとなる。ネットワーク関連製品の製造者、製品とサービスの提供者も含まれる。中国で事業展開する銀行、大企業、なども対象となる可能性がある。

中国国内で取得・生成した個人情報と重要データの国外への移転は原則禁止され、移転するには詳細な安全評価を受けて当局の認可を得なければならない。安全評価のガイドラインドラフトによれば、下記に該当する情報は海外移転が認められない。

- 政治的に危険
- 経済的・技術的な安全に懸念
- 国土、軍事、文化、社会、情報またはエコロジカルの安全に懸念
- 資源または原子力施設の安全に懸念

また、海外から中国のコンピュータへのリモートアクセスについてもデータ移転と見なされる可能性がある。いずれにしても、中国国内で活動する企業は、関連する規則・ガイドライン等の作成進捗状況を注意深く見守るとともに、詳細な内容を把握して適切に対応する必要がある。

中国サイバー安全法が施行されて 6 ヵ月経たが、インターネットへの厳しい規制・管理が次第に明らかになっている。中国国内では規制の実情は明らかにされないが、海外メディアにより一部が報道されている。その一例は次の通りである。

【3 年間で 1000 万件閉鎖。SNS の個人アカウント。2017 年 12 月 25 日の日本経済新聞[147]】

147 https://www.nikkei.com/article/DGXMZO25048610V21C17A2FF2000/

中国当局は 2015 年から 3 年間で交流サイト（SNS）において個人が情報を発信するアカウントを 1 千万件近く閉鎖し、同時に企業のサイトも 1 万 3 千社が閉鎖されたことが明らかになった。全国人民代表大会の常務委員会が 24 日に開かれ、同委の法律執行検査チームがサイバー安全法やネット統制監督の執行状況について報告書を提出した。

報告書によると、3 年間で国家インターネット情報室や傘下組織が 2,200 社余りの企業と法律違反などの対処について話し合い、1 千万件近くの個人アカウントを閉鎖し、1 万 3 千社あまりに企業サイトを閉鎖し、認可を取り消した。閉鎖の理由はポルノやテロなどの情報掲載としているが、社会問題や政治的な内容も国家の安全を脅かす情報として扱われて閉鎖につながったと見られる。取り締まりの対象はサイトや SNS だけでなく、スマートフォンのアプリやネット中継サービスも含まれた。ネット規制当局がまとめたネット上の違反・不適切情報の通報は 7 月から急増している。従来は月 300 万件程度だったが、7 月からは 2 倍近くの 600 万件台で推移することが多い。中国のネット企業幹部は、サイバー安全法の施行が取締強化のきっかけとなった、と指摘している。

なお、上記の報道は、中国で広く見られているニュースサイトである中国網、人民網、では一切報道されていない。今後、サイバー安全法に基づく規制がさらに厳しくなると、このような情報を日本向けに送信することも難しくなると懸念される。

2.2.3. 国家サイバー空間セキュリティ戦略

中央サイバー安全情報化指導グループの承認を経て、国家インターネット情報弁公室は 2016 年 12 月 27 日に「国家サイバー空間セキュリティ戦略」（略称：戦略）を発表した[148]。国家インターネット情報弁公室の報道官によると、このサイバーセキュリティ戦略はサイバー空間の発展と安全に関する中国の重大な立場と主張を明らかにし、戦略的方針と主要課題を明確にし、国のサイバーセキュリティの取り組みを指導する綱領的文書である。

国家サイバー空間安全戦略は、「国全体の安全を基本概念として、革新、協調、エコ、開放、共有の発展理念を貫徹実施し、リスク意識と危機意識を強化し、国内・国際の両大局を総合的に捉え、発展・安全を総合的に計画し、積極的に防御し、有効に対処し、サイバー空間の平和、安全、開放、協力、秩序を推進し、国の主権、安全、発展上の利益を守り、インターネット強国建設という戦略目標を実現する必要がある」とした。

国家サイバー空間安全戦略は、現在及び今後一定期間の国のサイバー空間安全の取り組

148 http://j.people.com.cn/n3/2016/1229/c94474-9160605.html
http://www.cac.gov.cn/2016-12/27/c_1120195926.htm

みにおける戦略課題として、以下の 9 点を挙げている。

- サイバー空間の主権を揺るぎなく守ること。
- 国の安全を断固として守ること。
- 重要な情報インフラを保護すること。
- サイバー文化建設を強化すること。
- サイバーテロと違法犯罪を取りしまること。
- サイバーガバナンスシステムを整備すること。
- サイバーセキュリティの基礎を固めること。
- サイバー空間の防護能力を高めること。
- サイバー空間の国際協力を強化すること。

上記の内容はサイバー安全法の目指すところを簡潔にまとめたものと言える。

2.2.4. サイバー空間国際協力戦略

中共中央サイバーセキュリティ＆情報化指導グループの批准をふまえて、外交部と国家インターネット情報室は 2017 年 3 月 1 日に共同で「サイバー空間国際協力戦略」を発表した[149]。

中国初のサイバー問題に関する国際戦略の発表である。同戦略は平和発展、協力ウィンウィンをテーマに、サイバー空間における運命共同体の構築を目標として、サイバー空間における国際協力の推進について初めて全面的かつ系統的に中国の主張を打ち出し、世界のサイバー空間のガバナンスという難問の解決のために中国のプランを提起して貢献するものであり、中国のサイバー空間をめぐる国際交流・協力への参加を指導する戦略的文書でもある。

同戦略は、平和、主権、共同統治、利益共有の 4 つの基本原則を基礎として、その上でサイバー空間をめぐる国際協力を推進すべきであると提起している。各国が「国際連合憲章」の主旨と原則を着実に遵守し、サイバー空間の平和と安全を確保することを提唱する。主権の平等を堅持し、サイバーの覇権争いをせず、他国の内政に干渉しないことを提唱する。サイバー空間における優位性による相互補完と共同発展を推進し、「デジタルデバイド」（情報格差）を解消し、人々がインターネット発展の成果を享受できるよう確保すること

149 http://japanese.china.org.cn/politics/txt/2017-03/02/content_40390646.htm
http://www.cac.gov.cn/2017-03/01/c_1120552617.htm

を提唱する。

サイバー空間の運命共同体構築のカギは行動にある。同戦略は次の９項目の行動規範を提起した。

- サイバー空間における平和と安定の主導と推進
- ネットワーク空間の秩序に基づいたルールの構築と推進
- サイバー空間パートナーシップの絶えざる展開
- 国際的インターネット管理の積極的な改革と推進
- サイバーテロとサイバー犯罪の撲滅への国際的協力の推進
- 個人情報権など人権保護の主導
- デジタル経済発展とデジタル利益の共有化の推進
- 世界の情報インフラの構築と保護の推進
- ネットワーク文化のコミュニケーションと相互学習の推進

以上の計画は中国のサイバーをめぐるセキュリティと情報化の建設発展の経験を総括したものであり、また国際交流の成果の結晶でもある。中国はサイバー空間をめぐる国際協力を非常に重視する。

なお、習近平国家主席は 2015 年 12 月に行われた第 2 回世界インターネット大会で「グローバルインターネットガバナンスシステムの変革を推進し、サイバー空間における運命共同体を構築する」と述べている。同戦略の発表について、人民日報はこのほど「鐘声」と題する論説を発表し、これは中国が初めて戦略の形式で、サイバー分野における中国の対外政策理念を全面的に明らかにし、繁栄した安全なサイバー空間という素晴らしい青写真を描きだし、国際協力の強化に力を尽くす中国の堅い決意を示したものであるとの見方を示した[150]。

上記の戦略により中国は、サイバー空間は、他国の干渉を受けない独自の主権が存在する特殊な領域であり、既存の国際法を適用するのはなく、新しい条約等で対応すべきであると主張している。その一環として、サイバー空間における運命共同体なる構想を打ち出した。この構想は、ロシアなどサイバー空間の利用に厳しい規制を目論む国々を巻き込んで、新しい国際秩序の確立を目指している。

[150] http://v.china.com.cn/news/2016-12/28/content_39996268.htm

【米国政府のサイバー空間国際戦略】

一方、米国のホワイトハウスは 2011 年に「サイバー空間国際戦略（International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World)」を発表し、その中で「サイバー空間に関わる国家の行動規範については、国際慣習法の再策定を必要としないし、既存の国際的規範は陳腐化していない。長期にわたり平和及び紛争時の国家の行動を導いてきた規範はサイバー空間にも適用できる。」としている。また、この戦略は、サイバー空間のあるべき姿として、解放された、相互運用性のある、安全な、そして信頼性ある情報とコミュニケーションのインフラストラクチャであるとしている[151]。

中国が打ち出した「サイバー空間国際協力戦略」は明らかに米国の「サイバー空間国際戦略」とは相いれないものである。米国の戦略は、現在、欧米・日本など先進国では合理的なものとして受け入れられており、中国が今後自国の戦略を具体的に実行していく過程で、国際的な摩擦・紛争が懸念される。

2.2.5.　軍民連携戦略

中国の最高意思決定機関である中国共産党中央政治局は 2017 年 1 月 22 日、中央軍民連携発展委員会の設置を決定した。この委員会は軍と民間との連携を強化するための諸事項の決定と関係機関の調整を担う[152]。

習近平国家主席が招集した第 1 回中央軍民連携発展委員会が 2017 年 6 月 20 日に開催された。委員会のメンバーは、同委員会副主任李克强、中共中央政治局常委张高丽、その他である。習近平国家主席は、国家戦略としての軍民連携の強化は、長期視点での経済発展と国家防衛力強化を実現すると強調した。この委員会で、軍民連携の基本的な運営方針が 8 項目決定された[153]。原文は長文なので要点のみ記す。

(1) ネットワークを使ったメディアとニュースの氾濫、などの社会環境の変化に対して新しい行動が必要である。この要求に対して軍民連携ファンドを設定して必要な資金を供給する。
(2) 軍民連携を実行するためのセンター、工業団地、研究所、など幾つかの社会組織を設置する。この組織を支援するための規則と管理を強化する。

151 https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
152 http://china.huanqiu.com/article/2017-01/10001681.html
153 https://baike.baidu.com/item/中央军民融合发展委员会/20395522?fr=aladdin

(3) 軍民連携の秩序を基準化する必要がある。需要と供給の結合、技術の育成、政策コンサルティング、マネージメントコンサルティング、などについて規準を作成する。
(4) ウェブサイト、ブログ、チャットなどによる軍民連携の活動に関する情報発信を規制する。
(5) 軍民連携の成果をセミナー、フォーラム、展示会、その他における発表を厳しく制限する。
(6) 退役軍人を軍民連携プロジェクトのパートタイム従業員として雇用する。
(7) 軍民連携プロジェクトを実施するセンター、工業団地、デモンストレーション会場、開発ゾーンなどに関する規制基準を制定する。
(8) 中央軍民連携発展委員会の事務局が統治とガイダンス、そして業務メカニズムを制定する。

軍民連携戦略に基づいて、最初の具体的なプロジェクトが下記の通り発表された。

【サイバー空間軍民連携イノベーションセンターを設置】[154]

中央軍民連携発展委員会事務局と人民解放軍の関連部署の指導に基づき、2017 年 12 月 26 日、サイバー空間軍民連携イノベーションセンターの設置が決まった。このセンターは、中国の代表的インターネットセキュリティ企業である奇虎 360 の企業グループと軍関係部署との連携で運用される。

国際的に第一級の軍のサイバー空間安全機器と、国際的に最高水準の民間の安全シンクタンクサービスと革新的産業技術サービスとの連携で大きな成果が期待される。奇虎 360 グループの会長斉向东氏は、イノベーションセンターは国家の安全、社会の安定、そして政府との一体化に寄与する。世界的なネットワークのさまざまな問題の解決に役立つだけでなく、軍の防衛力強化とネットワーク安全企業の発展に貢献すると語った。このセンターは次の効果が期待される。

- 軍に対して作戦意識を醸成させ、軍事に参加する企業に対して需要に基づく開発を促す。
- 軍と民間企業が共同でネットワークの安全を構築し共有する。
- ネットワークセキュリティの意識とネットワーク安全技術を向上させる。

軍民連携イノベーションセンターは設立されて間もないことと、情報が厳しく管理され

[154] http://photo.china.com.cn/2017-12/27/content_50169768.htm

ることから、具体的な活動内容は今後も公開されないと見られる。

2.2.2.6. 米中のサイバー対策相互理解

2015 年 9 月に米国・オバマ大統領と中国・習近平国家主席の首脳会談の際に、サイバースパイ対策で「相互の理解」に達するとともに、両政府が経済スパイを行なわないことで一致した。具体的にはサイバー問題を協議する専門家グループを創設して、サイバー犯罪対策を協議するハイレベル会合を年に 2 回開催するとした。

サイバー対策ハイレベル会合は 2017 年 10 月 5 日に第 1 回会合がワシントンにおいて実現した。この会合は「米中法執行とネット安全対話」と名付けられ、中国側は公安部部長・郭声琨氏、米国側は司法長官ジェフ・セッションズ氏、国土安全法長官代行エレイン・ヂューク氏が合同で主宰した。

双方は、互いに尊重し合い、法に基づき、対等な立場を堅持し、誠意をもって実務に励み、「中米法執行とネット安全対話」の役割を十分に果たして両国の協力を一層強化していくことで合意した。

郭声琨氏は、「中国はアメリカと共に、テロと越境犯罪、麻薬の取り締まり、司法協力などの分野での協力を強化し、法執行分野における両国の関心事を着実に解決したい。双方は、ハイレベルの合同対話体制の枠組み内で、ネット犯罪とサイバーテロの取り締まり、サイバーセキュリティなどの分野での実務協力を推進し、両国のネット安全を確保し、平和、安全、開放、協力、秩序のあるネット空間を構築していく」と述べた。

米国側は、「双方は、法執行とネット空間における安全保障分野で共通の課題に直面し、幅広く利益を共有している。米国は中国と共に、テロと越境犯罪、麻薬の取り締まり、不法移民の送還、ネット犯罪の取り締まり、サイバーセキュリティなどの分野での実務的協力を深め、両国の安全と経済利益を擁護していきたい」と述べた[155]。

上記の会合は、オバマ大統領と習近平国家主席が 2015 年 9 月に合意してから 2 年後のトランプ政権下で実現した。政権が代わってもこの合意は継続されることで、今後の展開が注目される。

[155] http://japanese.cri.cn/2021/2017/10/05/142s265747.htm

2.3. 業界団体、研究機関等

2.3.1. 中国サイバー空間セキュリティ協会

中国サイバー空間セキュリティ協会（中国名：中国網絡空間安全協会。英語：CSAC-Cyber Security Association of China）は 2016 年 3 月 25 日に設立された。本協会の概要は次の通りである[156] [157]。

本協会は、ネットセキュリティに係る産業、教育・研究・応用に係る研究機関と企業および個人で構成され、自発的な非営利の社会団体として、各機関の間の橋渡しと中国のインターネット安全実現への参加を推進する。中国で最初のインターネット安全に係る社会団体であり、国家が定める各種の事業指針に準拠し、国家インターネット情報弁公室と多くの規則と管理部署、そして国務院民生部の指導に従う。

現在、260 の団体と 321 名の個人が会員となっている。ネットワーク安全に係る主要なインターネット企業、ネットワーク安全企業、権威ある研究機関、専門家が含まれている。協会の幹部は各種のシンポジウムにおいて講演して、国家のインターネット安全戦略の推進に大きな貢献をしている。中国エンジニアリング学会の初代会長は、方濱興(Fang Binxing)である。方濱興会長はインターネット監視システム、グレートファイアウォールの開発者として知られている。参加しているのは、下記に示す中国のインターネット関連の主要プレーヤと大学である。これらの企業と大学の幹部が理事として就任している。

- Antiy Labs[158]
- Qihoo 360（正式名称：奇虎 360 科技有限公司、略称：奇虎 360）[159]
- Baidu（百度）[160]
- Alibaba（正式名称：阿里巴巴集団）[161]
- Tencent（騰訊）[162]
- Huawei（華為技術）[163]
- Xian Jiatong University（西安交通大学）[164]

156 http://news.china.com.cn/2016-03/25/content_38111646.htm
157 https://www.cybersac.cn/
158 http://www.antiy.net/
159 https://www.360.cn/
160 http://www.baidu.com/
161 http://www.alibabagroup.com/cn/global/home
162 https://www.tencent.com/zh-cn/index.html
163 http://www.huawei.com/en/
164 http://www.xjtu.edu.cn/

中国サイバー空間セキュリティ協会の主要な役割は次の通りである。

- 新たな情報および通信技術（ICT）の法体制の構築を支援する法律および規制の検討
- 国内 ICT 業界の発展を推進する技術支援
- 情報管理およびプロパガンダを支援するための世論監視
- 情報システム、製品、サービス、のセキュリティおよび信頼性の向上
- グローバル化の中で中国の国益を確保し、国際的な競争力を備えた中国企業の支援

協会設立以来の主な実績は次の通りである。

- ネットワーク安全業界の自己規制と全ての事業者の企業責任の向上推進
- ネットワーク空間の学術的研究の開発ルールと特質の設定
- 2016 年世界インターネット大会の報告書作成
- 中国のインターネット空間の国際的発展に寄与
- ネットワーク人材の教育・育成
- ネットワーク主権とネットワーク安全に関する法規の研究と検討の推進
- ロシアおよびその他の国々との国際協力と交流の推進

中国サイバー空間セキュリティ協会は国家インターネット情報室、その他の関係機関の指導に従いサイバー空間安全法の執行に協力する。そして、中国のインターネットが安全に持続的に発展するように貢献する。国家インターネット情報室と密接な関係のもとで運営されるので、サイバー空間における官民連携の協会である。

2.3.2. その他の業界団体

サイバー空間に関わる業界団体が数多くあり、その数例を下記に示す。いずれの団体も国務院の関連する省庁の監督を受けており、官民連携が確立されている。

- 中国インターネット協会[165]：国内のインターネットサービス事業者、インターネット機器事業者、システム事業者、研究開発者、その他 70 以上のインターネット関係者が共同で 2001 年 5 月に設立した。現在会員数は 1,000 を超えている。工業・情報化部の所管である。
- 中国電子商品協会[166]：電子商品に関わる事業者、研究機関及び個人と政府各機関の連携により、中国の電子商品事業の発展促進を目的として、2000 年 6 月に設立され

[165] www.isc.org.cn/
[166] http://www.ec.org.cn/

た。工業・情報化部の所管である。

- 中国ネットワーク可視化協会[167]：オーディオビジュアル事業者の団体であり、またインターネット事業者の団体として中国最大の一つである 2011 年に設立され、会員数は 714 である。会員には、中国人民放送局（中央人民广播电台）、国際放送局、中央テレビ局、人民網、新華網、中国網、アリババおよび Baidu などのニュース、捜狐などのインターネット企業やファーウェイ、中興などのネットワーク技術会社などを含む。
- 中国インターネットサービス事業協会[168]：インターネットサービス事業者の事業領域の基準化、事業者とユーザの法的義務と権利の明確化、そして業界の変革、向上、健全な発展の推進を目的として、国務院民生部の認可を得て 2013 年 3 月に設立され、文化部の監督を受けている。

上記の他に下記業界団体が存在するがホームページを開設していないところもあり、詳細は不明である。

- 中国情報協会（中国信息协会）
- 中国情報産業商工会（中国信息产业商会）
- 中国コンピュータ産業協会（中国计算机行业协会）[169]
- 中国コンピュータ使用者協会（中国计算机用户协会）

2.3.3. ネットワーク犯罪・安全研究センター

ネットワーク犯罪・安全研究センターは、2015 年 5 月 12 日に中国人民大学法学院に設立された。このセンターは同大学の犯罪法研究センター、中国犯罪学協会およびテンセン（腾讯）犯罪研究センターが共同で設立した。設立記念式典には、最高人民法院、最高人民検察院、公安部、国家検察官学院、中国法政大学、などの中国の司法・治安関係機関の代表者 70 余名が出席し、関係者の期待の大きいことを示した。

インターネット技術の普及に伴い、サイバー犯罪の問題が理論と実務の面で大きな課題となった。そして、この課題をネットワーク犯罪・安全研究センターが主導して解決することが求められている。さらに、専門家と産業界がインターネット安全と情報管理を推進し、関係部署が情報を共有し、インターネット時代のサイバー犯罪に帰するさまざまな問題を解決する役割を担う。このセンターが取り扱う課題の例は次の通りである[170] [171]。

---

167 http://www.cnsa.cn/
168 http://www.iasac.org.cn/
169 http://www.chinaccia.org.cn/
170 http://www.law.ruc.edu.cn/article/?49488.html

- サイバー犯罪の実行者は、第三者のコンピュータを踏み台にして犯罪を行なうことがあり、この場合の犯罪者の法的特定
- 不正アクセス行為を受けたり、コンピューターウィルスに感染したりしている事実を被害者自らが把握市出来ずに、違法行為による被害が顕在化する場合の法的取扱い
- コンピュータとインターネットへのアクセスさえ確保できれば、容易に国境を越えての犯罪行為を実行できるので、国際的な法的枠組の構築
- ネット上の書き込みなどで被害者が発生したとしても違法性が明確でないために対処できない課題への対処
- 被害の証拠をネット上に保存するなど、サイバー犯罪を司法が審理するために、犯罪行為を再現する法的枠組みの構築
- 一般市民をターゲットとするサイバー犯罪は、従来の犯罪に比べて被害が大きいので、より厳しい懲罰を科すことを可能とする法的処置
- サイバー犯罪の基本的データの収集方法
  - インターネット犯罪と補助行為の件数
  - インターネット犯罪の被害の大きさ

ネットワーク犯罪・安全研究センターは、ホームページを開設していないので、設立されて 2 年以上経ているが活動状況、成果、などの情報は一切明らかにされていない。

[171] http://news.xinhuanet.com/legal/2015-05/13/c_127793978.htm

2.4. サイバー空間に係る国際会議、国内会議等

2.4.1. 世界インターネット大会

世界インターネット大会は、国家インターネット情報室と浙江省人民政府が共催で、2014年から毎年開催されており、2017年12月3日～5日に第4回大会が浙江省烏鎮で開催された。中国と世界を相互に接続させる国際舞台であり、国際インターネット共有・共同ガバナンスを実現する中国の舞台を構築することで、各国が見解を一致させつつ協力をめざし、ウィンウィンを実現することが目的である[172]。

習近平国家主席は開幕式に祝電を寄せ、『中国デジタル経済発展が高速道路に入ろうとしている。中国は自国の努力により、世界各国がインターネット・デジタル経済発展の高速車両に同乗することを促したい。中国の対外開放のドアが閉じられることはなく、ますます大きく開かれるばかりだ』と表明した。

今年のメインテーマは「デジタル経済の発展・解放と共有の促進 ― インターネット空間運命共同体の共同構築」である。全世界から政府・国際機関・企業・技術チーム・民間団体のインターネットリーダーが招かれ、80数ヶ国から1,500人余が参加した。下記テーマが討議された。

- デジタル経済：人類の幸福
- 先進技術：将来の空間の拡大
- インターネットと社会：内部共有の推進
- インターネット空間ガバナンス：国際ルールの確立
- 国際交流・協力：サイバー運命共同体建設

各テーマの詳細な討議内容は公表されていないが、ロイター通信日本語版は次のコメントを報道した。

【中国がネット世界大会で統制強化方針、参加米IT企業からは迎合の声、ロイター、2017年12月6日[173]】

中国政府が主催した世界インターネット大会が5日閉幕し、中国はネットへの統制を強化する方針を打ち出した。ただ参加したフェイスブック(FB.O)やアップル(AAPL.O)といっ

[172] http://news.xinhuanet.com/fortune/2017-12/05/c_1122061990.htm
[173] https://jp.reuters.com/article/china-it-idJPKBN1E005G

た米大手ＩＴ（情報技術）企業の幹部からはこうした中国の姿勢に対してむしろ「ご説ごもっとも」と迎合する声が聞かれた。

中国は、自らの国境と同様な形でサイバー空間を守れる範囲内でネットの開放を約束するとともに、検閲やデータ保存に関する厳しい新ルールを導入した。中国で事業展開を許されている外国のハイテク企業にとって頭痛の種になっている。それでも、フェイスブックのバイスプレジデント、ボーガン・スミス氏は「私はデータ利用における指導力という面で中国を称賛したい」と語り、中国サイバースペース管理局（CAC）や工業情報省などがこの分野で「素晴らしい仕事」をしていると持ち上げた。

フェイスブックやグーグルは、中国では政府による「グレートファイアウォール（ネットの長城)」と呼ばれる規制の枠組みによってアクセスが遮断されている。一方でアップルは中国の検閲制度に従い、政府の要望に応じて同国のアップルストアから VPN（仮想私設網）アプリなどを削除している。

アップルのティム・クック最高経営責任者（CEO）は３日、「デジタル経済を開放性と共有利益のために発展させるというこの大会のテーマは、われわれアップルも共に抱いているビジョンだ」と発言し、聴衆から 2 回にわたって拍手喝采された。しかし、スミス氏もクック氏も、検閲制度やサイバー空間規制の問題には口を閉ざしたままだった。中国電子商取引最大手アリババ・グループ・ホールディング(BABA.N)のジャック・マー（馬雲）会長は「(外国企業）は中国のルールに従うべきで、不満なら去れば良い」と言い放った。

2.4.2.　サイバー安全産業サミットフォーラム

工業・情報化部と北京市人民政府の指導により、ネットワーク安全産業のイノベーションを加速する目的で、第一回サイバー安全産業サミットフォーラムが 2017 年 12 月 12 日に北京で開催された。政府機関、産業界、研究機関、などから約 500 人が参加した[174]。工業・情報化部の陳肇雄副部長は、挨拶の中で次のようにのべた[175]。

ネットワーク安全の革新的技術と新しいサービスが出現し、産業界の強靭性は高まり、ネットワーク安全の能力は引き続き向上している。しかし、中国のネットワークインフラの急速な発展、ネットワーク適用、個人情報保護、ネットワーク安全産業への支援、などの面で課題があり、ネットワーク安全の中核技術についてはブレークスルー技術の開発を加速する必要がある。

---

174 http://zhengwu.beijing.gov.cn/sy/bmdt/t1501264.htm
175 http://xxzx.miit.gov.cn/InfoAction!showDetail.action?sectionId=M002&info.infoId=991

国家のサイバー安全の概念として、ネットワーク安全、開発と安全、管理とサービス、公開と非公開の関係などについて正しい考え方を、ネットワーク安全産業の発展のために確立しなければならない。とくに重要な 4 分野は次の通りである。

(1) サイバー安全の中核技術のイノベーションの推進。企業、大学、研究機関を支援して、産業インターネット、AI、そして、ビッグデータ安全技術などの分野を強化する。
(2) ネットワーク安全サービス市場の強化。新しいネットワーク安全に関わる製品とサービスの市場の育成、通信、エネルギー、金融及び交通などの重要産業の指導、ネットワーク安全市場への投資の拡大。
(3) ネットワーク安全産業の調和のとれた環境の最適化。ネットワーク産業界の集合化、調和のとれた環境実現のための協力体制構築。
(4) ネットワーク安全に関わる専門家育成の加速化。ネットワーク安全に才能ある人材発掘、トレーニングと動機づけ、オンジョブトレーニング、などの仕組みの改善。

2.5. 中国におけるサイバー空間インシデント

これまで述べたように、中国ではサイバー空間の安全を確保するため法律制定、各種戦略実施、そして官民連携の推進などさまざまな取り組みを展開している。一方で、サイバーインシデントに関わる公開された情報は極めて少ない。社会の不安定化を危惧する当局が厳しい情報統制を行っていると見られる。海外のメディアが一部ながら中国国内における比較的大規模なインシデントを報告している。一例として、ロイター通信の香港支局が伝えた、2017 年 5 月に発生したインシデントは次の通りである。

【サイバー攻撃、中国の政府機関と学校を襲うが、拡大は比較的緩やか。2017 年 5 月 15 日のロイター[176]】

北京市政府の交通警察と産業監督局は、2017 年 5 月 15 日に大規模な身代金型マルウェア、すなわちワナクライ（WannaCry）の攻撃を受け、機能が麻痺した。しかし、被害の拡大は当初懸念されたよりも比較的緩やかであった。

中国の地方政府当局者は、世界中の自動車工場、商店、学校などを襲っているサイバー

176
https://www.reuters.com/article/us-cyber-attack-china/cyber-attack-hits-china-government-schools-but-spread-slows-idUSKCN18B10H

攻撃が中国でも発生して、業務が中止されることがあると語った。

また、中国のインターネットセキュリティ会社奇虎 360 の担当者は、今回の攻撃はこれまでのものと比較して被害の拡大は穏やかであった、と語った。前回の攻撃はほぼ 30,000 ヶ所の組織が被害を受け、その内 4,000 ヶ所は教育機関であった。

中国サイバー空間管理局の担当者は地方のメディアに対して、ランサムマルウエアはいまだに蔓延しており、産業界と政府機関のコンピュータシステムに悪影響を及ぼしているが、その勢いは収まりつつある、と述べた。

中国の運輸、社会保証、産業監視及び入国管理の各部署の担当者は、各種の申請手続きから交通犯罪取締りまでの業務が中止されていると、語った。

今回の攻撃では、世界中で 150 ヵ国において 200,000 ヶ所以上のコンピュータが被害を受けた。主に E メールを経由して感染し、中国では多くの学校と専門学校、巨大エネルギー企業であるペトロ中国、および地方政府が被害を受けた。

上記の情報は中国国内のインターネットメディアである中国網、人民網などでは報道されていない。サイバー空間の安全に対する国民の不安を招くことを危惧した当局が押さえたものと見られる。

さらに、ロイター通信は、中国におけるインシデントが最近急増していると下記の通り伝えている。

【中国企業へのサイバー攻撃は急増している、2016 年 11 月 29 日のロイター[177]】

中国企業へのサイバー攻撃は過去 2 年間に急増した。これは、屋内機器をインターネットへ接続し、データを送受する新しい技術の脆弱性が原因と見られる。

中国本土と香港地域において、企業により報告されたサイバー攻撃は 2014 年～2016 年の間に 639 パーセント増加した。中国をベースとする 440 ヶ所の検知基地では、平均 1 日 7 件を検知しているが、世界の平均 13 件の半分に過ぎない。検知能力が十分でない。

サイバー攻撃の件数は、世界平均では過去 2 年間、3%減少し、2015 年だけをみると 30%

177
https://www.reuters.com/article/us-china-cyber/chinese-firms-hit-by-huge-increase-in-cyber-attacks-survey-idUSKBN13O1E5

減少したが、中国ではこれに対して大幅に増加した。この急増は、中国におけるあらゆる物とコンピュータをつなぐ IoT の消費者と産業界における急速な普及が一つの理由として挙げられる。

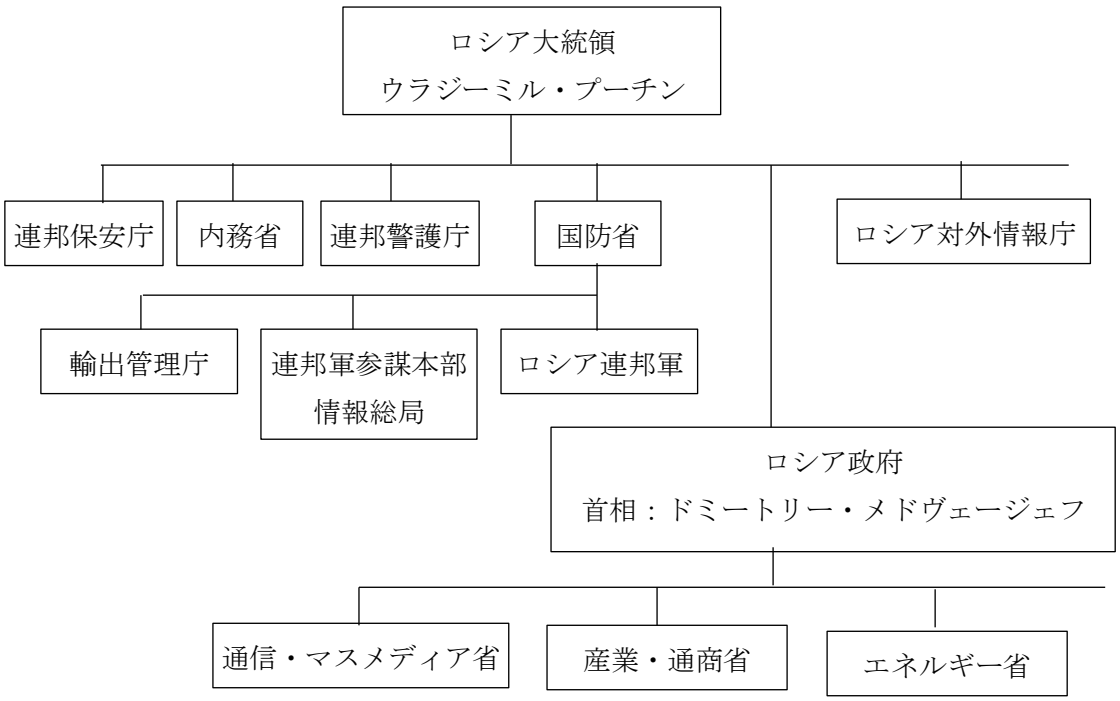
中国では IoT が世界のどこよりも広く普及している。中国製のウェブカメラはしばしば安全上の欠陥を有しており、これが IoT に繋がるとボットネットマルウェアの侵入を招いてしまう。

3.　ロシアのサイバー空間に関わる体制・能力等の実態

3.1.　情報空間を担う国家組織

ロシアのサイバー空間に関係する広い意味での主要部署は下図の通りである。大統領直轄の連邦保安庁（FSB)、内務省（MVD)、連邦警護庁（FSO)、国防省（MO)、ロシア連邦軍、ロシア対外情報庁（SVR）がサイバー空間へのかかわりが大きい。サイバー空間の管理が大統領にとって最重要課題となっている。そして、ロシア政府の通信・マスメディア省、産業・通商省およびエネルギー省も関わりが大きい。ロシア政府のその他の省庁、例えば文化省、教育・科学などもそれぞれの立場で関わっているがこの図では特に関りの大きい省庁のみ示した。

【サイバー空間に係る主要な国家組織】



出所：各種資料を基に IBT 作成

ロシアでは、情報セキュリティに対して非常に広範なアプローチを採用しているため、連邦保安庁、連邦警護庁、国防省、内務省、通信・マスメディア省、エネルギー省など、関連領域を複数の官庁が所管している。ところが現在のところ、サイバーセキュリティ確

保に向けた関連機関の役割分担は明確ではなく、省庁間連携等を促進させる単一の調整機関も存在していない[178]。

ロシアには、かつて電子諜報分野におけるKGBの後継組織として、FAPSI（連邦政府通信情報局）が存在していた。FAPSIは、KGBの第8総局（暗号化と暗号解読を担当）と第16総局（無線通信傍受）をベースに設立され、KGBの優秀な数学スクール（現在はFSBの暗号学研究所）と海外の設備（SIGINT/ELINT基地）を継承し、通信セキュリティと無線諜報を担当。米国のNSA（国家安全保障局）と類似した重要機関で、「非公式のロシアの情報戦争省」として認識されていた[179]。主な任務は、1)特殊通信、2)暗号化セキュリティ、3)テクニカル諜報活動、4)防諜活動、5)暗号解読、6)通信と情報の防護などであった。

単独組織としてのFAPSI（連邦政府通信情報局）の存在期間（1991年～2003年）は短かったものの、その中心的機能は、後継組織に引き継がれている。2003年の連邦政府通信情報庁（FAPSI）の解体に伴い、同庁のリソースは、1)連邦警護庁（FSO）、2)連邦保安庁（FSB）、3)国防省、4)対外情報庁（SVR）の4つの組織に分割・承継された。このうち、連邦保安庁（FSB）と連邦警護庁（FSO）が、ロシアの情報セキュリティおよび重要情報インフラ防護において中心的な役割を果たしている。

以上から、本調査報告書では、FSB（連邦保安庁）、SVR（対外情報庁）、FSO（連邦警護庁）、GRU（連邦参謀本部情報総局）と国防省等の主要省庁の役割等を整理する。またその他、特に民間部門のセキュリティに関係する政府組織（内務省、通信・マスメディア省及びエネルギー省）についても、概要を記載する。

ロシア政府には、「スペツナズ（Spetsnaz[180]）」との略称を持つ特殊任務を持つタスクフォースが存在する。英国のSAS（陸軍）や米国のUSASO（陸軍特殊部隊）とは、その役割と任務が多少なりとも異なる。モスクワの「Spetsnaz（スペツナズ）」は、相対的に少ない数の特殊任務部隊グループを意味し、主にロシア軍と連邦参謀本部情報総局（GRU）ならびに連邦保安庁（FSB）とロシア対外情報庁（SVR）及び緊急事態省と司法省の少数任務部隊である。任務の内容は部隊毎に全く異なるものである。職員数は2～3万人だと推計されている。

---

178 Oleg Demidov (2014) “Russia’s Information Security Policy”, Caroline Baylon, Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives; December 2014, Chatham House.
https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20141229CyberSpaceSecurityBaylonUpdate.pdf

179 http://www.agentura.ru/english/equipment/

180 信頼性に欠けるものが多いが、珍しく、以下のウィキペディア日本版の記述が良好である。
https://ja.wikipedia.org/wiki/%E3%82%B9%E3%83%9A%E3%83%84%E3%83%8A%E3%82%BA

連邦参謀本部情報総局（GRU)、連邦保安庁（FSB）および対外情報庁（SVR）はロシアの3大インテリジェンス機関である。特にFSBとSVRは旧KGBの継承機関である。GRUは軍事部門である[181]。

スウェーデン国防省傘下のFOI（防衛調査機関）が2010年3月に公表した「Emerging Cyber Threats and Russian Vies on Information Warfare and Information Operations（新興サイバー脅威と情報戦争及び情報作戦に関するロシアの見解[182])」によると、ロシアは1990年代初頭から国内外のサイバー脅威に対するロシア国家のセキュリティを強化する多大な努力を払ってきているという。情報戦争（IW- Information Warfare）に関与するロシアの政府機関は、FSO（連邦警護庁)、FSB（連邦保安庁)、SVR（対外情報庁)、GRU（連邦参謀情報総局）の4大機関である。FSO（連邦警護庁)、FSB（連邦保安庁）およびSVR（対外情報庁）の3大諜報機関が旧KGB（ソ連国家保安委員会）系であり、大統領の直接管轄下に置かれている。GRU（連邦参謀情報総局）は国防省の内局であるが、軍部の最高諜報機関である。

3.2. KGB 系の諜報機関

3.2.1. FSB（連邦保安庁）

連邦保安庁（ロシア略称：FSB。英語：FSS RB-Federal Security Service of the Russian Federation）は、大統領直轄下の連邦行政機関である。旧ソ連の KGB（国家保安委員会）がロシア KGB、FSK（連邦防諜庁）となり、1995 年 4 月に現在の FSB に再編統合された。プーチンが大統領になる以前に、FSB 長官を務めたこともある。

【連邦保安庁（FSB）の本部[183]：ルビャンカ広場（Lubyanka Square)】

旧 KGB 本部及び KGB 刑務所。
住所は、手前の広場の名称を使い、ルビャンカ（Л у б я н к а）広場。

181
http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf

182 FOI (Swedish Defence Reseach Agency), Emerging Cyber Threats and Russian Vies on Information Warfare and Information Operations, March 2010
http://www.highseclabs.com/data/foir2970.pdf

183
https://thelibertarianrepublic.com/isis-claims-attack-russian-intelligence-agency-headquarters-three-dead/

オリジナルの建物は、1898 年に設立された全ロシア保険会社（All-Russia Insurance Company）の本社ビルであった。連邦保安庁（FSB）の職員数等に関する正式な統計は入手できていないが、20 万人以上を擁するとの推計値もある[184]。

【連邦保安庁（FSB）長官：アレクサンドル・ボルトニコフ（Alexander Bortnikov[185]）】

連邦保安庁（FSB）長官（Director of the Federal Security Service）のアレクサンドル・ボルトニコフ（Alexander Bortnikov）は、2008 年 5 月にメドベージェフ大統領により任命され、今でも長官の職にある186。サンクトペテルブルグ市の FSB 次長を務めており、プーチンやメドベージェフの側近のひとりである。1951 年 11 月 15 日生まれ。1973 年に旧 Leningrad Institute of Railway Engineers（現在の St. Petersburg State Transport University）を卒業し、KGB のレニングラード（現在のサンクトペテルブルグ）支部で勤務。2004 年 2 月から FSB の経済セキュリティサービス部門のトップを務める。セルゲイ・イワノフ（文民出身の元国防大臣。第一副首相を歴任。大統領府官房長官）、イーゴリ・セーチン（プーチンの子飼い。ユコス事件の捜査を主導。第一副首相を経てロスネフチの会長）やビクトル・イワノフ（KGB レニングラード支局を経て 1999 年に FSB 次官。2008 年に連邦麻薬取締庁長官に就任）等の元 KGB レニングラード支局出身者である。シロヴィキ（Siloviki）の一派。シロヴィキとは、政治的信条を同じくする諜報機関や軍部関係の出身者で、極めて影響力の大きいクレムリン派閥を意味する。

ロシア連邦 FSB の主な責任と役割は、ロシア国家安全保障であり、対防諜活動、対テロ対策、犯罪撲滅、情報セキュリティの保障措置、ロシア連邦国境の防護・防衛、管轄海域・領海・大陸棚、排他的経済研及び天然資源等の防護である[187]。主な根拠法は、1995 年の連邦保安庁に関する連邦法第 40 号（Federal Law No. 40-FZ, On the Federal Security Service[188]）である。

ロシア連邦保安庁（FSB）の基本的な任務は、1)CKP（防諜局）が担う対外防諜防御サービス、2)テロ対策局が担うテロ対策、3)組織犯罪撲滅の 3 つである。

---

184 The Guardian (October 6, 2013) “FSB: Vladimir Putin's immensely powerful modern-day KGB” https://www.theguardian.com/world/2013/oct/06/fsb-putins-modern-day-kgb

185 http://en.kremlin.ru/catalog/persons/100/events

186 http://en.kremlin.ru/catalog/persons/100/events

187 http://www.fsb.ru/

188 http://www.icla.up.ac.za/images/un/use-of-force/eastern-europe/Russia/Federal%20Law%20on%20Federal%20Security%20Service%20Russia%201995.pdf

サイバーセキュリティについては、連邦法第 40 号第 8 条が情報セキュリティ分野における情報及び通信システム、暗号化された情報の伝達に使う特殊通信ネットワーク等のセキュリティを確保することを連邦保安庁（FSB）の任務のひとつとして義務づけている。

FSB（連邦保安庁）長官官房内に設置された電子通信監視センター（TSRRSS-Center for Electronic Surveillance of Communications。別名：第 16 総局／第 71330 軍事部隊）は、電子通信の遮断、暗号解読、情報処理などを担当しており[189]、ロシアのハッカー予備軍をコントロールしているとみられている[190]。加えて、大規模なテロ発生時には、各連邦管区に設置されている反テロ委員会（NAK）を通じて管轄区域内の軍・治安機関を指揮する権限を持つため、FSB（連邦保安庁）は大規模サイバーテロ等に対しても中心的な役割を果たすことになろう[191]。

連邦保安庁（FSB）は、政府ネットワーク向けのサイバーセキュリティ及びインシデント対応センター（国際名称は GOV-CERT.RU）の運用、国家 DPCA システム（GosSOPKA：コンピュータインシデントにおける国家調整センターを含む）の構築・運用も担っている[192]。

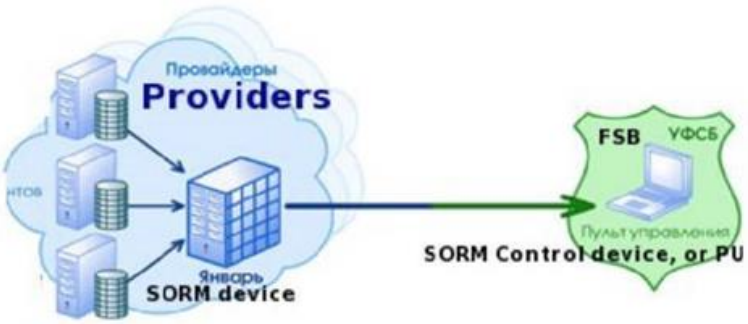
以下は、情報セキュリティ関連の役割を担う連邦保安庁（FSB）の主な部署である 1)情報セキュリティセンター、2)暗号・通信・コンピュータ科学研究所（IKSI）、3)第 18 総局・サイバーセキュリティセンターの概要を示した表である。

【FSB 内の主な情報セキュリティ対応部署】

❍ 情報セキュリティセンター（TsIB: FSB Information Security Center ）。別名：第 64829 軍事部隊（Military Unit（Vch）64829[193]）。本部は連邦保安庁本部に隣接した Butchers 通りに立地[194]。

189 A TAIA GLOBAL REPORT (2015) “Russian Federal Security Service (FSB) Internet Operations Against Ukraine”
http://docplayer.net/15126233-Russian-federal-security-service-fsb-internet-operations-against-ukraine-a-taia-global-report.html
190 K. Mshvidobadze, “The Battlefield On Your Laptop”, Radio Free Europe/Radio Liberty 21 March 2011. http://www.rferl.org/articleprintview/2345202.html
191 http://www.nisc.go.jp/inquiry/pdf/fy21-brics.pdf
192 (Novermber 17, 2016) “In 2017, the FSB will start the exchange of information on cyber attacks GosSOPKA system”
http://soc-forum.ib-bank.ru/
http://www.startlr.com/in-2017-the-fsb-will-start-the-exchange-of-information-on-cyber-attacks-gossopka-system/
193 A TAIA GLOBAL REPORT (2015) “Russian Federal Security Service (FSB) Internet Operations Against Ukraine”
194 A TAIA GLOBAL REPORT (2015) “Russian Federal Security Service (FSB) Internet Operations Against Ukraine”

- 情報セキュリティセンター（TsIB）の主な任務は、諜報活動用システム（SORM-）を利用したインターネット（RuNET）の監視と、脅威特定のためのインターネットコンテンツの分析等[195]。
- 1990 年代に初めて構築された SORM は、電話回線検閲システムの SORM-1 とインターネット回線検閲システムの SORM-2 から構成される。
- ロシアでは、「通信法」によって情報機関や捜査機関が一般の通信を傍受することが認められている。FSB の要請を受けて、ロシアで操業するあらゆる通信事業者は、SORM に関連する機器やソフトウェアを自社通信システムに導入することを義務づけられている[196]。
- また連邦法第 64 条で、通信事業者が利用者に関する情報を政府機関に通知する義務や政府機関が機動捜査活動を行えるようにする義務などが規定されている197。



出所：Infosec Institute “How Russia Control the Internet” [198]

- 連邦保安庁（FSB）の情報セキュリティセンター（ISC）は、SORM の運用を担っており、内務省 K 局（後述）との密接な協力関係の下で、インターネット事業者（IPS）がインストールしているハードウェア及びソフトウェア、インターネット接続ポイント及びインターネット相互接続点を利用して、インターネットの監視を行っている。同センターでは、2007～2008 年に大規模アップグレードを行い、FSB ISC 本部の建物から、インターネット監視システムの遠隔操作とオフラインでの情報分析を行う能力を拡大している[199]。

---

195 Infosec Institute “How Russia Control the Internet”
http://resources.infosecinstitute.com/russia-controls-internet/

196 Приказ Минсвязи РФ N 130, О порядке внедрения системы технических средств по обеспечению оперативно-розыскных мероприятий на сетях телефонной, подвижной и беспроводной связи и персонального радиовызова общего пользования.（2000 年 7 月 25 日）

197 小泉悠 (2014)『ロシアにおける情報安全保障政策とインターネット規制』「外国の立法 262 (2014.12)」
http://dl.ndl.go.jp/view/download/digidepo_8841952_po_02620006.pdf?contentNo=1

198 Infosec Institute “How Russia Control the Internet”
http://resources.infosecinstitute.com/russia-controls-internet/

199 A TAIA GLOBAL REPORT (2015) “Russian Federal Security Service (FSB) Internet Operations Against Ukraine”

- 暗号通信コンピュータ科学研究所（IKSI）
  - IKSI（暗号通信コンピュータ科学研究所）は暗号解読に取り組んでいたが、現在は情報セキュリティを専門としている。現在、200 人以上の教授が在籍し、コンピュータシステムとセキュリティについて学生を指導している。優れたコンピュータ能力を有する学生にとって唯一の難点は、連邦保安庁の給料が主要な技術系企業の給料よりも遥かに低い点にある[200]。
- 第 18 総局サイバーセキュリティセンター
  - 第 18 総局サイバーセキュリティセンター（Cybersecurity Center N18）は、サイバーセキュリティで主導的な役割を果たしている。秘密防衛サービス部のコンピュータ・情報セキュリティ課の傘下に置かれている。センター長は Andrey V. Gerasimov。旧 KGB のコンピューターセンターとして使用されていた建物内に立地している。同センターに関する情報は、ほとんどが機密扱いとなっており、ロシア国内からもアクセスできない。得られた情報の範囲では、同センターには、情報技術オフィス（専門家ユニット）と運転管理ユニットが含まれている。

出所：各種資料に基づいて IBT にて作成。

サイバーセキュリティ関連では、FSB（連邦保安庁）の 2 名の職員とモスクワに本拠を構える世界的なセキュリティ会社のカスペルスキー（Kaspersky Lab）の社員がロシア当局により米国の利益につながる反逆を犯した容疑でロシア当局によって拘束されたと、2017 年 2 月 1 日のロイター（モスクワ[201]）が報じた。カスペルスキーの社員はコンピュータインシデント調査チームの責任者の Ruslan Stoyanov で、FSB の公務員は情報セキュリティセンター（TsIB）で勤務する Sergei Mikhailov と Dmitry Dokuchayev であり、米国の諜報機関に協力した国家反逆罪で拘束されたと、カスペルスキーの弁護士である Ivan Pavlov が明らかにした。ロシアが米国の大統領選でトランプ候補に有利なハッカー行為を行ったロシア人を告発した直後の米ロ間の緊張が高まっていたタイミングでの事件であった。Ruslan Stoyanov がヘッドを務めるカスペルスキーのコンピュータインシデント調査チームは 2013 年から FSB の依頼でサイバー犯罪事例の分析を行っていたようである。拘束された Stoyanov チーム長がカスペルスキーに入社したのは 2012 年のことで、今回の容疑は彼が入社する前の出来事であると会社側はコメントしている。クレムリンはメディア報道でこのニュースを知っているものの、事件に関するコメントを差し控えている。

---

http://docplayer.net/15126233-Russian-federal-security-service-fsb-internet-operations-against-ukraine-a-taia-global-report.html

200 The Guardian (October 6, 2013) “FSB: Vladimir Putin's immensely powerful modern-day KGB” https://www.theguardian.com/world/2013/oct/06/fsb-putins-modern-day-kgb

201 https://www.reuters.com/article/us-russia-cyber-arrests/russia-charges-cyber-security-expert-fsb-officers-with-treason-lawyer-idUSKBN15G43Y

米国政府はテクニカル調査だけでヒラリー・クリントンの大統領キャンペーンに対してハッカー攻撃を仕掛けたとの確信を得たとしているようだが、ロシア政府は 4 人のロシア人が米国のファインディング（発見したこと）を裏づけたことで国を裏切ったと信じていると、Svetlana Reiter 女史[202]（Esquire Russia の特別コレスポンダント）は書いている。米ロの情報戦争を代表する最新事例であるために、あえて整理のために Bell 社が刊行した彼女の記事を要約して以下に記載したい[203]。

- 2016 年 12 月 5 日に国家反逆罪の容疑で逮捕された Sergei Mikhailov（セルゲイ・ミハイロフ）は FSB（連邦保安庁）傘下の情報セキュリティセンター（TsIB）第 2 局の責任者で、ロシアのインテリジェンスサークルではサイバー犯罪の中心的権威とみなされていた。
  - Dmitry Dokuchayev（ドミトリ・ドクチャエフ）は FSB の元犯罪ハッカーで Yahoo の 5 億件のアカウントをハッキングした容疑で米国において告訴されていた。カスペルスキーの中堅幹部（法執行機関担当）であった Ruslan Stoyanov（ルスラン・ストヤノフ）と知名度の低い起業家の Gergy Fomochenkov は反逆罪の容疑がかけられている。以上の 4 名は、2017 年 12 月時点で、モスクワのセキュリティレベルの高いレフォルトヴォ刑務所（Lefortovo Prison）に収監されていると、情報筋は語っている。
  - この事件は、一般大衆の眼が届かないように国家機密として分類されている。3 人のうちの 2 人が米国民主党全国委員会（DNC）に対するロシアのハッカー攻撃に関する情報を渡したと語っている。2 ヵ所の情報筋は、情報セキュリティセンター（TsIB）のヘッドである Sergei Mikhailov（セルゲイ・ミハイロフ）とその仲間の逮捕劇の裏には連邦参謀情報総局(GRU)の存在があると語っている。ロシア経済制裁に際し、オバマ政権は 2016 年 12 月に連邦参謀情報総局（GRU）のイーゴリ・コロボフ（Igor Valentinovich Korobov）長官を含む GRU の 4 人の高官を個人的に制裁の対象としたが、FSB の職員の誰一人も個人的な制裁の対象となっていない。ただし、米国政府は GRU が米国の選挙に介入する意図をもって情報を盗み出し、FSB もそれを支援したと主張している。
  - ある情報筋によると、上記の容疑者は DNC（民主党全国委員会）のサーバに割り込むハッカーの特定でアメリカ人を支援したと主張する。しかし、ニューヨークタイムズはミハイロフとストヤノフの拘留は DNC へのハッカー攻撃に関係したものではないとし、米国の諜報機関による犯人の特定に際してある複数のロシア筋が重要な役割を演じたとの 2 人の米国の役人のコメントを掲載している。

[202] https://www.journalismfestival.com/speaker/svetlana-reiter
[203] https://thebell.io/en/arrest-russian-intel-top-cyber-crime-expert-american-elections/

- 2017 年 1 月、米国の諜報機関は 2016 年の大統領選キャンペーン期間に発生したサイバー攻撃に関する捜査結果（機密ではない情報）を共同で公表し、このサイバー攻撃はプーチン大統領による個人的な命令だと断言。関与したのは、以下の FSB と GRU のハッカー集団である。
  - FSB（連邦保安庁）：2015 年 7 月、ロシアのハッキング集団が DNC（民主党全国委員会）のサーバに侵入したが、約 1 年も検知されなかった。この集団のニックネームは、Cozy Bear, the Dukes または A.P.T.29。
  - GRU（連邦参謀情報局）：2016 年 3 月、GRU と結びついていると想定される Fancy Bear または A.P.T.28 として知られるハッキング集団が 2 番目の DNC のサーバに侵入。後に DNC の Email をリリースする上でより大きな役割を果たした。
  - 以上の結果、バラク・オバマ大統領はサイバー攻撃を命令したと告発し、35 人のロシアの外交官を国外追放し、FSB と GRU（高官 4 人）ならびに Alexei Belan（FSB のドミトリ・ドクチャエフらと共謀してコンピュータ詐欺と乱用の罪で FBI が重要指名手配し懸賞金をかけたラトビア人のハッカー。国籍はロシア人[204]）と Yevgeny Bogachev（GameOver Zeus というボットネットを作った lucky12345 と slavik という 2 つのニックネーム持つロシア人で、同じく FBI が重要指名手配した人物。ロシアの黒海地域をボートに乗り暮らす。国籍はロシア人[205]）の 2 人のハッカーも制裁対象となった。
  - 2016 年 7 月のロイターには、私どもはロシアの諜報機関が DNC（民主党全国委員会）にハッキング攻撃をかけたことや大量の emails がリリースされたこと、またドナルド・トランプがプーチンをバックアップし、サポートするとの極めて困った意向を示していることも承知しているとのヒラリー・クリントンのコメントを掲載している。
  - クラウドストライク（Crowdstrike）社（DNC へのハッカー攻撃をレポートしている）では、これらのサイバー攻撃は個別に実行されたと結論を下している。つまり、これは FSB と GRU が基本的にライバル同士であることを意味する。しかし、クラウドストライク社の創業者の Dmitry Aleperovich は FSB と GRU のそれぞれに働くハッカーをどのように区分しているのかとの本誌（Bell）の質問には答えていない。Bell 誌の情報筋によると、情報セキュリティセンター(TsIB)のヘッドである Sergei Mikhailov（セルゲイ・ミハイロフ）が情報を仲介人経由でクラウドストライク社に伝えた可能性があるが、裏付けがとれていないという。（紙面の都合で、その他の記事内容を割愛）。

204 https://www.fbi.gov/wanted/cyber/alexsey-belan
205 https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev

3.2.2.　SVR（対外情報庁）

SVR（対外情報庁。英語名：Foreign Intelligence Service）は、旧 KGB の分割により、KGB 第一総局を継承して 1991 年 12 月 18 日に設置された。FSB（連邦保安庁）と協力して対外諜報活動を行い、機密情報の分析結果を大統領に報告する大統領傘下の行政機関である[206]。

ソ連では、1920 年 12 月 20 日に設置された Cheka（チェーカ）との略称で呼ばれた秘密組織が初めて国土安全保障の脅威に関する諜報活動を展開した。特に世界大戦では、核兵器開発を含む対外諜報活動で収集した軍事戦略に関する詳細情報を指導部に提供した実績を有している。ロシア対外情報庁（SVR）の Website[207]には過去の詳細な活動内容が記載されている。

現在の長官は、2016 年 10 月 5 日に就任したセルゲイ・ナルイシキン（Sergey Naryshkin）である。2011 年 11 月に就任した下院議長を 2016 年 10 月に辞職している。

1954 年 10 月 27 日にレニングラード（現在のサンクトペテルブルグ）で生まれる。1978 年にレニングラード機械大学（無線機械技師専攻）を卒業し、サンクトペテルブルグ国際経営学院でエコノミストの学位を取得。

レニングラードポリテクニック研究所（LPI）国際関係部門で部門長補佐になり、国家科学技術委員会の専門官、ベルギー大使館経済諮問スタッフを経て、レニングラードポリテクニック研究所（LPI）対外経済関係学部の副学部長に就任。

ベルギー大使館に派遣される前に KGB のスタッフであったと報じるメディアもある。1992～1995 年、サンクトペテルブルグ市長管轄の経済発展委員会および経済財政委員会の委員長となり、プーチンと親交を深める。1998 年にレニングラード州政府対外経済国際関係委員会の委員長に就任[208]。

プーチン大統領の招聘により、2004 年 2 月に大統領府経済ガバナンス局副局長に任命され、2004 年 9 月 14 日にロシア連邦政府官房長官に就任。行政改革、公共サービス、産業政策を担当し、2005 年 7 月に行政改革委員会の委員長、2006 年 7 月に大統領管轄の国家重点事業協議会のメンバーとなり、2007 年 2 月 15 日に副首相に就任し、CIS 関連の対外経済を担い、メドベージェフ、セルゲイ・イワノフに並ぶ有力者となる。2008 年 5 月 7 日にメド

206 http://government.ru/en/department/112/
207 http://svr.gov.ru/
208 http://www.ladno.ru/person/naryshkin/bio/

ベージェフが大統領に就任すると、新閣僚人事で大統領府官房長官に任命された。2005～2009 年、JSC First One の取締役会会長とロスネフチ取締役を兼務し、2008 年には造船会社の SCF の会長に就任（2011 年 10 月まで）。

統一ロシアの候補として 2011 年 12 月の下院選に立候補し、2011 年 12 月 21 日に下院議長に選出[209]。2012 年 6 月 11 日、横路孝弘衆議院議長の招待で来日し、野田首相、玄葉外相、前原民主党政調会長らと会談。玄葉外相との会談では、シベリア・極東における開発プロジェクトへの日本企業の参加への期待を表明した。これに対し、玄葉外相は、日露経済関係の潜在性の蓋を開けたいと述べつつ、ロシアの投資環境の改善につきロシア議会関係者の努力を求めた。また、北方領土問題やアジア太平洋地域における日露協力について言及された[210]。このほか、官房長官時代にもロシア文化フェスティバル関係などでたびたび来日している[211]。

2016 年 9 月 22 日、プーチン大統領によりロシア対外情報庁（SVR）長官に任命され、同年 10 月 5 日に下院議長を辞職し、SVR 長官に就任。妻と 2 人の子供の 4 人家族である。スポーツマンでロシア水泳連盟（All-Russian Swimming Federation）の会長を務める。英語とフランス語を話す。

GRU（連邦参謀情報総局）が軍事マターにフォーカスするのに対して、SVR（対外情報庁）は主に民生マターに特化した諜報活動を展開している。連邦法で定められた SVR の主な任務は次の通りである[212]。

- ロシアの安全保障に確保につながる虚偽情報やプロパガンダ等の積極的な情報捜査活動を実施すること。
- 軍事・戦略・経済・科学・技術等のスパイ行為の履行。
- ロシアの海外機関の職員と家族を保護すること。
- ロシア政府の公務員とその家族の安全を確保すること。
- 諸外国の諜報機関と共同作戦を展開すること。
- 諸外国において電子監視を実行すること。

NATO（北大西洋条約機構）の見方によると、SVR（対外情報庁）は、米国の CIA、英国の SIS（秘密情報部。通称“MI6”）、フランスの DGSE（対外治安総局）等に匹敵するエージェ

209 http://state.kremlin.ru/persons/1
210 http://www.mofa.go.jp/mofaj/press/release/24/6/0611_02.html
211 http://english.ruvr.ru/2012_06_12/77883318/
212 Littell, Jonathan. The Security Organs of the Russian Federation. A Brief History 1991–2004. Psan Publishing House, 2006.

ンシーである。ロシアの FSB（連邦保安庁）は、米国の FBI やドイツの BfV （連邦憲法擁護庁）に類似した機関である。他方、連邦参謀情報総局（GRU）は NATO の対抗機関である[213]。

スウェーデン国防省傘下の FOI（防衛調査機関）によると、SVR（対外情報庁）は主に敵対者等のヒトに対する諜報活動を行うが、暗号や信号等の通信防諜、軍事用および民生用衛星システムと有線系と無線系の通信システムなどの管理能力を有している[214]。

2015 年に米国 DNC（民主党全国委員会）のサーバに侵入したハッカー集団の Cozy Bear（別名、(Office Monkeys, CozyCar、CozyDuke または APT-29)は SVR（対外情報庁）とつながっているとみられる。

オランダの日刊紙であるフォルクスラント（de Volkskrant）の 2018 年 1 月 25 日のニュース記事[215]では、オランダの諜報機関である AIVD（総合諜報保安庁）が米国の FBI に対して 2016 年の米国大統領選キャンペーンにロシアのハッカー集団が関与したという「決定的証拠」を提供したと報じている。この記事の概要は次の通りである[216]。

- 2014 年の夏、オランダの AIVD（総合諜報保安庁：Algemene Inlichtingen- en Veiligheidsdienst）のひとりのハッカーがモスクワの「赤の広場（Red Square)」に隣接する大学のコンピュータネットワークに侵入したところ、それが Cozy Bear（コージーベア）のネットワークであると判明。
  - AIVD は、大学の建物内にいる 10 名前後の Cozy Bear（コージーベア）がハッキングを行っていた部屋を監視する防犯カメラのアクセスを得たうえで、出入りする人物も特定し、ロシア人が何をしていたかも確認したようである。
  - AIVD は 2015 年に Cozy Bear（コージーベア）が民主党首脳のコンピュータに侵入し、大量の電子メールや文書を移動させるのを目の当たりにしたと FBI に通報した。しかし、米国側が「このハッキングによってロシアが米大統領選に介入し、AIVD のエージェントがまさにその現場を目撃していた」ということを理解するまでに数か月かかったという。
  - Cozy Bear（コージーベア）の米国に対するハッカー攻撃は 24 時間にわたるサ

213
https://www.nato.int/docu/review/2017/Also-in-2017/russian-intelligence-political-war-security/EN/index.htm
214 http://www.highseclabs.com/data/foir2970.pdf
215
https://www.volkskrant.nl/tech/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~a4561913
216 2018 年 1 月 28 日の AFP 日本語ニュースで補足する。
http://www.afpbb.com/articles/-/3160177?cx_position=3

イバー戦の末に阻止されたものの、「トロイの木馬（Trojan Horse)」と呼ばれるマルウェア（悪意のあるソフトウェア）を仕掛けられた電子メール 1 通が守りを突破し、コージーベアにホワイトハウスへのアクセスを許したようである。

- フォルクスラント（de Volkskrant）によると、米国の諜報機関がロシアのハッカー活動に対する備えがなく、予想外の驚きでとらえたと報じている。例えば、2017 年 8 月に退任した国務省のサイバー政策のトップであった Chris Painter もロシア人が米国の致命的に重大なインフラを攻撃し、米国のデモクラシーを損なうことになるとは予想もしなかったとコメントしている。オランダの諜報機関による重要情報の提供を契機に、米欄の諜報機関の連携により、携帯メールですら、ロシア政府が絡むハッキング活動が行われていた事実を把握したようである。
- 防犯カメラに映った数々の人物からオランダの AIVD（総合諜報保安庁）は、Cozy Bear（コージーベア）の米国大統領選におけるハッキング活動を主導したのはロシアの SVR（対外情報庁）であるとの推論を下している。

2018 年 2 月 8 日の米国 NBC ニュース[217]によると、ごく少数のロシア人ハッキング集団が 2016 年の米国大統領選前の複数州の選挙人登録でもハッカー侵入を行っていたと、国土安全保障省のサイバーセキュリティ責任者の Jeanette Manfra は述べている。

3.2.3. FSO（連邦警護庁）

連邦警護庁（FSO: Federalnaya Sluzhba Okhrany、英語：Federal Protective Service または Federal Guard Service）は、クレムリンの数人の重要な高官と特定の連邦政府財産を警護することを任務とする連邦政府機関である。FSO の前身は、旧 KGB 第 9 総局で、後に大統領セキュリティサービス（GUO）となった。当時のトップは、エリツイン大統領の警護隊長であった KGB の Alexander Korzhakov（アレクサンドル・コルジャコフ）である。1995 年 5 月 27 日、GUO（大統領セキュリティサービス）は国家警護法に基づいて FSO（連邦警護庁）に再編・統合された。2004 年 8 月に FAPSI（連邦政府通信情報庁）の資産とリソースの多くを承継して現在の FSO（連邦警護庁）が設立された。本拠地は、クレムリン内のブロック 14 である。

FSO（連邦警護庁）の主な任務[218]は、大統領をはじめとする数人のクレムリン高官の身辺警護だが、連邦政府通信・情報庁（FAPSI）が解体された際に、政府の電話盗聴システムで

---

217 https://www.nbcnews.com/politics/elections/russians-penetrated-u-s-voter-systems-says-top-u-s-n845721

218 http://www.fso.gov.ru/

ある ATS-1 と ATS-2 を運用する政府通信総局（旧 KGB 政府通信部隊）、対外通信総局などの主に通信関係の部局が編入された。国家公務員用のインターネットの管理も暗号化技術を使って FSO が担っている。現在、FSO（連邦警護庁）において通信セキュリティに関する任務を担当しているのは、特別通信情報局（第 32152 部隊）と見られ、FSB（連邦保安庁）の情報セキュリティセンター（TsIB）（前述）と国防省連邦技術輸出管理庁（FSTEC）と密接な協力関係を維持しているとされる[219]。

FSO（連邦警護庁）長官は、16 年間も FSO を統率した KGB 出身の Evgeny Murov（エヴゲニー・ムロフ）上級大将に代わり、2016 年 5 月 26 日に就任した Dmitry Kochnev（ドミトリ・コチネフ）である。

コチネフは 1964 年にモスクワで生まれる。

1982～84 年にロシア軍に所属。1984～2002 年にソ連とロシアの諜報機関で勤務。

2002 年に FDO に配属され、2015 年に FSO（連邦警護庁）の副長官に就任。あまり過去の経歴が公表されていない無名の人物である[220]。

[219] https://fas.org/irp/world/russia/fso/index.html
http://www.agentura.ru/english/equipment/

[220] https://inmoscowsshadows.wordpress.com/2016/05/27/dmitri-konchev-the-elusive-new-fso-director-and-thus-putins-primary-protector/

3.3. 国防省

3.3.1. FSTEC（連邦技術輸出管理庁）

2004年8月16日のロシア連邦大統領令第1082号の「国防省の課題の範囲」に基づいて、国防省はロシア軍のサイバーセキュリティと国家秘密の防護を担うこととなった。国防省で情報セキュリティ／サイバーセキュリティを担うのは、主に連邦軍参謀本部情報総局（GRU）と連邦技術輸出管理庁（FSTEC）である。情報総局（GRU）は国防省におけるサイバーセキュリティで中心的な役割を担っていくものとみられる。

国防省の傘下に置かれた連邦技術輸出管理庁（FSTEC）は、技術的側面から、重要情報インフラなどの国家安全保障に直結する情報セキュリティの保護を担っている[221]。外国の技術的諜報手段への対抗や国家機密の防護、重要な技術の輸出管理、情報通信機器の認証などを主な任務としており、最重要施設並びに人命及び人の健康に脅威をもたらす施設の自動プロセス制御システム（APCS）に関する情報保護のための要件を示した連邦技術輸出管理庁令第31号の発布等も行っている。ただし、暗号関係などは所掌に入っていない。

連邦技術輸出管理庁（FSTEC）は、FSB（連邦保安庁）と協力し、外国によるネットワークへの侵入防止を行うほか、機微技術の輸出管理、輸出認証、将来のサイバー脅威予測に基づいて教育計画の策定などを担当している[222]。この他にも、軍需製品の輸出管理を行う連邦対外軍事技術協力局(FSMTC)もある。FSTEC（連邦技術輸出管理庁）の主な任務は次の通りである[223]。

- ロシアの最重要施設における情報通信インフラシステムの情報セキュリティの確保、情報分野における国家安全保障への重大な影響の行使等（ロシアの極めて重要な施設の情報システムと通信ネットワークの正常な機能確保を含む)。
- ロシア領土内における外国の技術諜報活動に対する対抗措置。
- 国家機密とその他の制限データ等の機微な情報の保護、テクニカルチャネルリークや不正アクセスの阻止等。
- 厳格に国家機密として分類されるデータ及びその他アクセス制限付きの機微な情報のセキュリティ保証（暗号化以外の手段による)、通信チャンネルを通じた秘密データの漏洩防止、秘密データへの不正アクセスの防止、情報及び情報源に対する特殊な影響の防止等

[221] http://fpi.gov.ru
[222] 小泉悠「ロシアのサイバー攻撃能力と組織実態」『軍事研究』2013年8月号
[223] https://fstec.ru/en/359-powers

- 情報発信を行わない複合施設、システム及び機器の開発、生産、運用及び使用の際の情報防護。
- 貿易管理等。

3.4. その他の情報セキュリティ関連の政府機関（一覧表）

ロシア連邦安全保障会議（Security Council of the Federation）

大統領が委員長を務め、以下のようなサイバーセキュリティ政策の策定を指示し、さらに指針や決定等の文書を発出する。
- 2017 年 10 月 26 日の拡大安全保障会議において、プーチン大統領はロシアの情報インストラクチャーの安全を確保するための声明を発表し、次の項目への取組の必要性を強調した[224]。
  - ロシアの情報資産のコンピュータへの攻撃を検知・防護・排除するシステムの改良
  - 国家の情報システムと通信ネットワークの防護レベルの向上
  - 海外のソフトウェアと通信機器の使用に伴うリスクを可能な限り削減
  - 法規制の改革によりロシアのインターネットセグメントの安全と持続性の強化
  - 国際的な情報安全システム構築、国連、BROCS、SCO、APEC、CSTO および CIS などと協力強化
- 最重要インフラ施設における産業プロセス制御システムのセキュリティ確保を目的とした国家政策の指針（2012 年 2 月 3 日付大統領令第 803 号にて承認）
- 「国家安全保障上極めて重要なインフラ施設の防護並びに人工脅威、自然脅威、テロ脅威からの国民の保護」に関する国家安全保障会議及び国家安全保障会議評議会の合同会議（2003 年 11 月 13 日開催）における決定
- 2005 年 11 月 8 日の国家安全保障会議「最重要施設で稼働中の情報通信システム及び破壊的な情報による影響に対するためのオブジェクトと照会するための、体系化された表示と基準の使用」
- 国民、危険な施設、最重要施設の人工脅威、自然脅威及びテロ脅威からの防護に関する国家政策についての、2020 年までの基本原則（2011 年 11 月 15 日付の大統領令第 3400 号にて承認）

内務省（Ministry of the Interior）
内務省は、国内問題に関する政府政策及び法規制の作成・履行並びに移民問題に関する政府政策の作成を担う。ロシア連邦大統領が内務省の活動を監督する[225]。

[224] http://en.kremlin.ru/events/president/news/55924
[225] The Russian Government “Ministry of the Interior of the Russian Federation”

- 情報セキュリティ・サイバー犯罪に従事するのは、K 局（特殊手段局：Bureau of special technical measures）である。
  - 内務省各局の活動内容に関する情報は少ないが、K 局はコンピュータ犯罪、通信・インターネット犯罪、情報通信分野に関する国際犯罪等が活動範囲とされ、2015 年の国際ハッカー集団の逮捕に関与していたようである[226]。
  - 報道によると、同ハッカー集団は 2015 年、ロシアの銀行システムをダウンさせて金銭を奪う目的で、ロシアの処理センターとグローバル銀行及び銀行間のメッセージ交換のシステムにハッキング攻撃を仕掛けたほか、銀行ターミナル及び ATM を制御するためのシステムの構築とコンピューターウィルスの開発・拡散に関与していたという。K 局の捜査により、銀行カードの申請を行ったリーダー格の人物と現金引き落とし及び奪った金の換金を行った人物をすでに特定しているとのことである。なお、K 局は、情報技術における著作権その他の権利の侵害を発見・防止する権限も有する[227]。

通信・マスメディア省（Ministry of Communications and Mass Media）

通信・マスメディア省は、2009 年 5 月の大統領令で設立された。情報通信・ネットワーク関連技術全般のほか、マスコミやインターネット事業者など多くを管轄している。情報セキュリティに関しては、技術関係のほか民間の運用にかかわる施策に全て係わっている主力官庁といえる。前述の SORM 実装に関する政令を発行しているのも通信・マスコミ省である。

- 情報セキュリティに関係する部署は、通信・情報技術・マスコミ監督庁（通称“Roskomnadzor”）である。主な任務は、通信・技術・マスコミの管理監督及びライセンス付与と許可証の発行である[228]。具体的には、電子媒体、マスメディア、情報技術及び通信を含む、メディアの監督、個人データの処理における秘匿性保護に関する法律順守の監督、無線周波提供サービス業務の調整を担っている[229]。過激主義のプロパガンダの流通を取り締まる権限を持つ。

---

http://government.ru/en/department/86/events/

[226] (February 4 2016) “The Ministry of internal Affairs explained how an international gang of hackers wanted to bring down the banking system of the Russian Federation during the crisis” http://en.news-4-u.ru/the-ministry-of-internal-affairs-explained-how-an-international-gang-of-hackers-wanted-to-bring-down-the-banking-system-of-the-russian-federation-during-the-crisis.html

[227] V. Mirolyubova Svetlana, V. Yankevich Semen. (2013) “Legal regulation of the fight against counterfeit goods in the Russian Federation” http://www.archiviopenale.it/apw/wp-content/uploads/2013/10/V.-Mirolyubova-and-Semen-V.-Yankevich.pdf

[228] “Historical Background” https://eng.rkn.gov.ru/about/background_information/

[229] The Russian Government. “Federal Service for Supervision of Communications, Information Technology and Mass Media” http://government.ru/en/department/58/

エネルギー省（Ministry of Energy）

同省の主な任務は、ロシアの全顧客に確実な電力供給を実現することである。エネルギー省は、同省が有する権限の範疇で、燃料エネルギー複合体（FEC）における国家情報システムの構築・運用・改善と、発電及びエネルギー効率の向上に関する分野の国家情報システムの開発に従事している。

- 情報システムセキュリティを担うのは、1)セキュリティ体制及び国家秘密部（Department for security regime and state secrets）と 2)電力産業における運用統制及び管理部（Department of Operational Control and Management in Electric Power Industry）の２つである。
  - 情報システムセキュリティ関連の業務は、機密指定の情報と情報システムおよび施設で使用されるソフトウェア／ハードウェア等、脅威モデル、異なる脅威グループの分析などである。エネルギー省では、これらの情報を用いて、サイバーセキュリティ確保のための具体的な手順及び行動リストを包含した政策の作成を行っている。
  - 省内のサイバーセキュリティ方針には、情報管理と情報システム保護のための一連の運用手順等が含まれており、各手順では、保護対象へのアクセス要件、制御システムへのアクセス要件、幹部の責務を特定している（これらの内部資料のアクセス権限を有していないため、詳細は不明)。現在のところ、エネルギー省では、自動プロセス制御システム（APCS）を個別に取り上げた取り組み等は行っていない。

3.5. サイバー空間に関わる法規・政策・戦略等の最新動向

3.5.1. ロシアのサイバーセキュリティ概念の違い

ロシアのサイバーセキュリティに対する考え方は、西側諸国とは異なり、1)情報セキュリティの一環としてのサイバーセキュリティを位置づけていること、2)軍事・安全保障面を重視すること、3)政治的・社会的側面をクローズアップすることの 3 つの特徴を有している。以下、この 3 つの特徴の概要を記載したい。

- ロシアのサイバーセキュリティ政策は、全体として情報セキュリティ（Information Security）の一環であるとみなされている[230]。
  - ロシアの正式な戦略文書や法令において、「サイバーセキュリティ」という用語を使用した事例はない。2014 年 1 月に発表された「国家サイバーセキュリティ戦略の構想（草案）（Draft Concept of Cyber Security Strategy of the Russian Federation）[231]」において初めてサイバーセキュリティという用語が使用されたが、同文書においても、「サイバーセキュリティ」はあくまでも、より広義の概念である「情報セキュリティ」に含まれるものと位置づけられている。
  - 他方、ロシアでも、「サイバー戦略」「サイバー脅威」「サイバー戦争」といったアングロサクソン諸国で使う用語が研究者、外交官、下院（State Duma）の安全保障委員会議長の Irina Yarovaya やドミトリー・ロゴジン副首相(国防担当)等の政治家によって公開討論の場で使用されている。
  - Yarovaya 議長は、ロシアの「デジタル主権」に関する主張を展開している人物で、ロゴジン副首相は 2012 年 3 月に米国をモデルにしたロシア版サイバーコマンドの創設構想について言及した他、ロシア版 DARPA「先進研究財団(Foundation for Prospective Research）[232]」の設立を主導した人物である（2012 年後半に設立)。さらに、スノーデン問題を調査する作業チームで座長を務め、上院の情報環境委員会の会長を務めるルスラン・ガタロフ（Ruslan Gattarov）上院議員の主導で、ロシア初の国家サイバーセキュリティ戦略の構想を精緻化するための議論も行われている。ここには、カスペルスキー、インフォウォッチ、CISCO

[230] Oleg Demidov (2014) “Russia’s Information Security Policy”, Caroline Baylon, Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives; December 2014, Chatham House.
https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20141229CyberSpaceSecurityBaylonUpdate.pdf

[231] Conception of the National Cybersecurity Strategy of the Russian Federation (Draft) (30 January 2014) official website of the Council of Federation of the Federal Assembly of the Russian Federation; http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf
http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

[232] http://fpi.gov.ru

等の民間企業の代表から成る専門家グループも参加し、ロシアのサイバー空間における脅威の特定、法規則面での不足、サイバー空間の防護に関する役割分担等について、積極的な議論が展開されている[233]。

- とはいえ、多くの政府関係者は情報セキュリティから「サイバーセキュリティ」という概念を抜き取って、それをあらゆる法規制で使用する考えに反対の立場をとっている。したがい、サイバーセキュリティ戦略策定の動きを「当該領域におけるロシアの政策と矛盾するもの」と捉えているようである。「サイバーセキュリティ」が主にインターネットチャンネルを中心とした通信チャンネルとその装置の防護を第一義としており、「情報セキュリティ」はその内容の防護にまで及ぶために、2 つの用語には根本的な違いがあると考えているからである[234]。さらに、ロゴジン副首相が行っている講演の内容から推論し、ロゴジンが「サイバー脅威」と「情報脅威」を同一視し、デジタル主権（＝技術的な自給）」の固定観念を政治的プロパガンダに利用しているだけだと指摘する声もある[235]。
- ロシアにとっての最優先事項は現在でも、国防や国家安全保障を軸とした重要な情報セキュリティであり、同国におけるサイバーセキュリティやサイバー能力を強化すべきとの論調は国内の防衛産業や軍上層部の特定ロビー活動の道具に過ぎないとの見方が濃厚である。

- ロシアでは、軍事・安全保障面を重視する：ロシアの政策文書では、情報戦争と物理的戦争の区別をしておらず、情報セキュリティやサイバー空間セキュリティを主に情報戦争における非軍事的手段としてとらえ、防諜や情報戦などの軍事・安全保障分野を重視する傾向にある。
  - 情報セキュリティやサイバーセキュリティといった議論では、重要情報とクリティカル情報システムの防護だけでなく、テロリストや反抗分子の特定等の大義名分の下での国内外における重要情報の収集活動、政府や軍によるプロパガンダなどの情報操作活動、さらにはインターネットや SNS 等を利用した反政府勢力による非公式イデオロギーとの対決等が含まれることもある。
  - 2000 年に制定された「ロシア連邦の情報セキュリティ原則」[236]において、初めて「情報戦争（information war)」、「情報兵器（information weapon)」、「情報の反作用の隠匿（concealment of information counteraction)」等の用語が示された。
  - 2014 年の「ロシアの軍事原則（Russian Military Doctrine)」では、軍事的脅

[233] Kommersant" newspaper
[234] Kommersant" newspaper
[235] Jolanta Darczewska (June 2016) Russia's armed forces on the information war front Strategic documents; OSW studies NUMBER 57 WARSAW.
https://www.osw.waw.pl/sites/default/files/prace_57_ang_russias_armed_forces_net.pdf
[236] Утв. Президентом РФ 09.09.2000 № Пр-1895.

威が情報領域と国内領域にシフトしているという傾向を強調し、軍事的政治的目的に基づいた国家の主権、政治的独立性及び領土の保全を標的とした情報通信手段の利用に対して警告を発している。また、軍の情報セキュリティシステムとその他の治安部隊や組織及び戦略、運用、戦術レベルの情報管理システムとの相互運用性強化の必要性を強調しつつ、現代の武力衝突は、とりわけ「軍の総合的な活用、政治経済的情報及びその他の非軍事的手段、並びに反対運動や特殊作戦の大々的な活用」に特徴づけられるとしている[237]。

- 情報セキュリティの政治的・社会的側面をクローズアップする：ロシアの政策で使われる情報セキュリティという用語では、プロパガンダや情報ネットワークを通じた政治的・社会的情勢に対する負の影響などの幅広い問題を包含している。西側諸国における 3 つのサイバー脅威（サイバー戦争、サイバーテロ、サイバー犯罪）も、ロシアでは、主権国家の内政に対する情報介入を含むものとして拡大解釈されている[238]。
  - ロシアのサイバーセキュリティ関連の政策文書には、情報セキュリティやサイバー（空間）セキュリティにおける政治的社会的要素に対する偏執性が反映されており、クレムリンの広範な情報戦略の一部として、国内外のロシアの主権に関わる重要情報インフラの防護とロシアの内政及び既存の権力構造（近隣諸国に対する覇権維持も含め）を脅かし得る情報攻撃の阻止に比重が置かれている。
  - 2000 年の情報セキュリティ原則における情報脅威の評価では、1)諸外国が生み出した情報戦争の概念、2)グローバルな情報空間においてロシアの国益を支配あるいは阻止しようとする他国の野心、3)諸外国の諜報組織による心理面と情報面での妨害工作の可能性と同時に、4)諸外国の情報技術活動（無線電子戦争；コンピュータネットワークへの侵入；宇宙、海洋、陸上における諜報及び偵察手段の活用など）について言及している。加えて、「多国籍国家ロシアの精神的統一性を促進し CIS 諸国とのコミュニケーション言語」としてのロシア語を保護対象の 1 つとして特定している点も特徴的である[239]。こうした傾向は、最新の情報セキュリティ原則（2015 年発表）にも引き継がれており、情報領域におけるロシアの国益に対する脅威の 1 つとして、「外国メディアにおけるロシアの外交政策や国内政策に関する偏見と悪意に満ちた情報の増加」を挙げ、特に若年層が、文化的精神的価値観の浸食、道徳原則及び愛国的伝統の基盤の弱体化

[237] Jolanta Darczewska (June 2016) Russia's armed forces on the information war front Strategic documents; OSW studies NUMBER 57 WARSAW.
[238] Jolanta Darczewska (June 2016) Russia's armed forces on the information war front Strategic documents; OSW studies NUMBER 57 WARSAW.
[239] Jolanta Darczewska (June 2016) Russia's armed forces on the information war front Strategic documents; OSW studies NUMBER 57 WARSAW.

による被害を被っていると指摘している。

- 実際、ロシアでは、一部の政治家の間でも、メディアやインターネット等の様々なチャンネルを通じて国家に入り込む非公式イデオロギー（ワッハーブ派の教義(復古主義的な厳格主義)、テロリズム、分離主義など）との対決が「サイバーセキュリティ」の概念に含まれると解釈している場合がある。ロシア軍参謀本部大学校（Military Academy of the General Staff）の Sergei Chvarkin 次席は、2016 年 1 月 27 日の声明で「世界におけるロシア語の地位低下は、ロシアの国家安全保障における主要な脅威の 1 つである」と述べている。Chvarkin 氏の見解では、言語と文化は、今日の情報戦争における重要な対立領域を成しているのである240。また、ヴァレリー・ゲラシモフ参謀長は、2016 年 2 月後半に行われた同アカデミー会員の年次総会での講演で、ロシアに対する「新たな」軍事的脅威を取り上げ、いわゆる「カラー革命」と国外からの情報がロシア国内の人々に及ぼす悪影響について言及し、それらを同国の歴史的、精神的及び愛国的な国防の伝統を破壊するものであるとの見方を示している241。
- なお、サイバー空間を通じた攻撃の目的が、重要な産業情報へのアクセス等に限られず、他国の体制等への打撃など政治的側面を持つ場合、ロシアのアプローチが適しているとの意見もある。たとえば、英国の王立国際問題研究所（チャタムハウス）の報告書では、西側諸国はサイバー戦争への備えは十分かもしれないが、ウクライナの事例が示す通り、サイバー作戦が目的達成のための推進役（facilitator）または攻撃のベクトル役として実行される場合には、情報戦争への備えも必要だとの指摘している[242]。

- ロシアでは、専門用語の使い方に特異性がある：ロシアでは、国家安全保障委員会（SCRF)、連邦保安庁 (FSB)、連邦技術輸出管理庁 FSTEC) などの主要執行機関 (EAB) が発出している文書では、それぞれが独自の専門用語を作り出している。加えて、使用する専門用語は、独特の語法で用いられており、仮に定義が示されている場合でも、一般化され過ぎた曖昧な言い回しとなっていることから、西側諸国のアプローチに沿った解釈でこうしたロシアの語法を理解することは難しい。
  - たとえば、「重要情報インフラ（CII)」については、2012 年 2 月 3 日付けの大統領令第 803 号「重要インフラ施設における自動化プロセス管理システム(APCS)の安全性保全に関する国家政策の主要動向（Main Trends of State Policies in Safety Assurance of Automated Process Control Systems at Crucial

240 www. russkiymir.ru/news/202777

241 Jolanta Darczewska (June 2016) Russia's armed forces on the information war front Strategic documents; OSW studies NUMBER 57 WARSAW.

242 Keir Giles (March 2016) "Russia's 'New' Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power", Research Paper March 2016, Chatham House. https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2016-03-21-russias-new-tools-giles.pdf

Infrastructure Facilities of the Russian Federation）の中で、『重要情報インフラの自動化管理システム（ACS）及び国家管理のためのインターフェースを提供し、国防能力及び安全と公秩序に寄与し、運転に混乱（または中断）が生じた場合には深刻な影響をもたらし得る情報通信ネットワーク全体』という定義が記載されている。さらに、2014 年 1 月発表の「サイバーセキュリティ戦略の構想（草案)」で、また新たな重要情報インフラの定義とそれらの防護手段が提示されている。加えて、その他の戦略文書においては、「最重要情報インフラ（Critically important information infrastructure)」といった用語が、明確な定義や対象が示されないまま用いられている点に、注意が必要である。

3.5.2. 情報セキュリティ関連の主な政策概要

ロシアには、50 以上の情報セキュリティ関連法と付随する大統領令及び連邦政府の法規則が存在する[243]。これらの文書の根拠法は、「ロシア連邦の情報セキュリティ原則[244]（2000 年制定)」である。同原則では、経済、国内政策、外交政策、科学技術、国防、ロシアの法秩序保護など、様々な領域に影響を及ぼす情報脅威について詳細な議論を提示しており、それ故、後の公式文書や関連分野の文献等で使用されることになる多くの用語（情報戦争、情報兵器、情報の反作用の隠匿など）が盛り込まれている[245]。

ロシア初のサイバーセキュリティ戦略の構想を示す「国家サイバーセキュリティ戦略の構想（草案)」(2014 年発表）でも、その土台には 2000 年の情報セキュリティ原則があった。加えて、2014 年の国家サイバーセキュリティ戦略構想（草案）では、2006 年 7 月 27 日付の連邦法第 149-FZ「情報、情報技術及び情報保護について」[246]、「ロシア連邦における情報社会戦略」[247]、「ロシア連邦の重要インフラ施設における自動化生産・プロセス制御システム（APPCS）のセキュリティに関する国家の主要方針[248]」、「安全な情報文化の形成に関する国家の主要方針[249]」及び「国際的な情報セキュリティ領域における 2020 年までのロシア国

---

243 Natalia Romashkina (2016) "PROSPECTS OF INTERNATIONAL COOPERATION ON INFORMATION SECURITY", *RUSSIA: ARMS CONTROL, DISARMAMENT AND INTERNATIONAL SECURITY* (IMEMO SUPPLEMENT TO THE RUSSIAN EDITION OF THE SIPRI YEARBOOK 2015); Alexei Arbatov and Sergei Oznobishchev (Eds.); Moscow. http://www.imemo.ru/files/File/en/publ/2016/Supplement_2016.pdf

244 Утв. Президентом РФ 09.09.2000 № Пр-1895.

245 Jolanta Darczewska (June 2016) Russia's armed forces on the information war front Strategic documents; OSW studies NUMBER 57 WARSAW.

246 СЗ РФ. 2006, № 31 (1 ч.), ст. 3448.

247 Утв. Президентом РФ 07.02.2008 № Пр-212.

248 Информация Совета Безопасности от 8 августа 2013 г.

249 Утв. Президентом РФ 24.07.2013 № Пр-1753.

家政策の基本方針」[250]の内容にも矛盾のないよう戦略を作成すべきだとの指針を支援している。

【FAPSI 主導による 2000 年情報セキュリティ原則の起草】

連邦政府通信情報局（FAPSI-Federal Agency of Government Communication and Information）は、電子諜報分野における KGB の後継組織である。KGB の第 8 局（暗号化と暗号解読を担当）と第 16 局（無線通信傍受）がベースとなり、KGB の優秀な数学スクール（現在は FSB の暗号学研究所）と海外の設備（SIGINT/ELINT 基地）を継承した FAPSI（連邦政府通信情報局）の主な任務は、通信セキュリティと無線諜報である。1990 年代後半以降、FAPSI はインターネット統制に向けた関心を示し始め、すべての電子金融及びセキュリティ関連取引と、個人のインターネットアクセスを含むその他の電子通信を監視する権限を正式に獲得し、ロシア政府関連機関向けに ISP（インターネットサービスプロバイダー）開発まで行った。FAPSI の内部で情報セキュリティを担当したのは、第 3 総局通信手段電波電子情報総局（GURRSS））である[251]。

クレムリンにおける FAPSI（連邦政府通信情報局）のプレゼンス増大に伴い、敵対的な侵入がインターネット上に浸透することを主要な脅威と捉える当局の見解は、ロシアにおける「情報戦争（Information warfare）」の概念において不可欠な要素となった。1997 年、当時のウラジミール・マルコメンコ（Vladimir Markomenko）長官は情報戦争を定義し、1)電子戦争（electronic warfare）、2)電子諜報（electronic intelligence）、3)ハッカー戦争（hacker warfare）、4)心理戦争（psychological warfare）の 4 つの要素で構成されると主張した。その後、1998～1999 年に FAPSI 第 3 総局通信手段電波電子情報総局(GURRSS)のトップを務めた Vladislav Sherstyuk 総局長が 1999 年 12 月に情報セキュリティ担当として国家安全保障会議に参加したために、FAPSI のアプローチ手法が強化されることになった。実際、2000 年に制定された「ロシア連邦の情報セキュリティ原則」は、国家安全保障会議における Sherstyuk 総局長チームにより起草された[252]。

1999 年に勃発した第 2 次チェチェン紛争では、独立最強硬派武装勢力のイスラム国際戦線を率いるチェチェン人武装勢力が隣国のダゲスタン共和国へ侵攻し、一部の村を占領した。これはロシア連邦政府を対象にした攻撃ではなく、ここではプロパガンダや兵募集にインターネットが使用された。この翌年の 2000 年に制定された「連邦軍事原則」において

[250] https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf
[251] http://www.agentura.ru/english/equipment/
[252] Keir Giles (2011) “Information Troops” – a Russian Cyber Command?” 3rd International Conference on Cyber Conflict; C. Czosseck, E. Tyugu, T. Wingfield (Eds.) Tallinn, Estonia, 2011; CCD COE Publications. http://conflictstudies.org.uk/files/Russian_Cyber_Command.pdf

安全保障と国防を取り巻く環境で電子化が進みつつある中で新たな手段と戦略が必要であるとの指摘がなされた。これが、ロシアの戦略文書で初めて言及された情報セキュリティの脅威である。以上の流れの中で、ロシア初の情報セキュリティ政策が発動されたのである。

以上を踏まえ、1)2000 年の「情報セキュリティ原則（ドクトリン)」、2)2016 年 12 月制定の「情報セキュリティ原則（ドクトリン)」、3)2017 年 5 月制定の「2030 年に向けた情報社会発展戦略」、4)2018 年 1 月 1 日施行の「重要インフラ安全法」の 4 つの情報セキュリティ関連の政策文書を次に整理・分析してみたい。

3.5.3. 2000 年の情報セキュリティ原則

ロシア初の情報セキュリティ政策は、「ロシア連邦安全保障概念」の関連文書として 2000 年 9 月 9 日にプーチン大統領によって承認された「ロシア連邦情報セキュリティ原則（Information Security Doctrine[253])」である。これは、ロシア政府が初めて公式に情報セキュリティの確保に向けた目的、目標、原則および基本指針を示した政策文書であり、2018 年現在でも有効である。このドクトリン（原則）は、経済、国内政策、外交政策、科学技術、国防、ロシアの法秩序保護など、様々な領域に影響を及ぼす情報脅威に関する様々な議論を示している。そのために、「情報戦争」、「情報兵器」、「情報カウンターアクションの隠匿」などの専門用語も盛りこまれている。この意味で、このドクトリンはロシアの情報セキュリティ戦略を知る上で重要な位置づけを占める政策文書だといえる。2000 年 9 月 9 日に制定されたロシア連邦情報セキュリティ原則（ドクトリン）の概要を示すと以下の通りである[254]。

- 本ドクトリン（原則）は、1)情報セキュリティ政策の土台となるものであり、2)ロシア連邦の情報セキュリティ確保に向けた法律面・手順面・科学術面・組織面の枠組みを改善する提案根拠となり、3)国家プログラム策定の土台となるものである。
- ロシアの情報セキュリティとは、情報空間における国益の防護を意味する。情報空間（Information sphere）とは、情報の集まり、情報インフラストラクチュア、情報の収集・加工・発信・利用に従事する法人ならびに公的関係を司るシステムを表す。「社会生活のシステム形成要因としての情報分野はロシア連邦の安全保障（Security）の構成要素である政治・経済・防衛およびその他の要因の状態に影響を与える」ものである。

253 https://info.publicintelligence.net/RU-InformationSecurity-2000.pdf
254 Jolanta Darczewska (June 2016) Russia's armed forces on the information war front Strategic documents; OSW studies NUMBER 57 WARSAW.

- 情報空間におけるロシアの国益は、1)憲法で保障された権利と自由の保護、2)国策に対する情報支援（国民に対する情報公開の義務を果たしつつ、ロシアの国家政策に関する信頼に足る情報を国民及び国際社会に示すこと等)、3)近代情報技術の推進、国内の情報産業の発展、国内市場・製品の充実と国際市場への展開、及び国家情報資源の蓄積、信頼性構築、有効活用、4)無許可アクセスからのロシア情報資源の保護及びロシア領内における情報通信システムの安全性確保の 4 つであると記載している。
- ロシアの情報セキュリティが直面する脅威は、上記の 4 つの国益に即して示されている。このうち、3 つ目の「情報通信システム及び施設におけるセキュリティ上の脅威」に、「情報処理、電気通信、通信に関するシステム及び手段の破壊、損傷、障害またはこれらを標的とした電子攻撃」や「データ伝送ネットワークまたは通信ラインにおける情報の傍受、(暗号）解読、及び偽情報の押し付け」が含まれており、西側諸国でいうところの「サイバー脅威」に最も近いといえる。
- この他にも、情報セキュリティを確保する上での様々な課題や情報セキュリティの確保に向けた手法などの原則を示している。

2000 年の情報セキュリティ原則（ドクトリン）の発表から 14 年後の 2014 年 1 月 30 日、ロシア政府は日増しに増大する情報空間の脅威に対応するため、サイバー空間の枠組みで生じる様々な情報要素に関して既存の規制では必要なシステムをカバーしきれていないとの認識の下、「国家サイバーセキュリティ戦略構想（草案）(Draft Concept of Cyber Security Strategy of the Russian Federation[255])」を発表した。本草案がロシア初のサイバーセキュリティ戦略になる予定であったが、2015 年には 2000 年の情報セキュリティ原則に代替する新ドクトリン（草案）の検討が開始され、公開討論会を経て 2016 年 12 月に正式に採択されたことから、2014 年の国家サイバーセキュリティ戦略構想（草案）の紹介は割愛したい。

3.5.4. 2016 年 12 月制定の情報セキュリティ原則（ドクトリン）

ロシア政府は 2015 年 10 月に 2000 年の情報セキュリティ原則（ドクトリン）に代替する情報セキュリティ原則（草案[256]）を発表し、さらに 2016 年秋の公開討論を経て集めたコメントや提案を考慮して 2016 年 12 月に最終版の草案を公表した。プーチン大統領は 2016 年

[255] Conception of the National Cybersecurity Strategy of the Russian Federation (Draft) (30 January 2014) official website of the Council of Federation of the Federal Assembly of the Russian Federation; http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf
http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf
[256] 2015 年発表の草案（原文）http://infosystems.ru/assets/files/files/doktrina_IB.pdf

12 月 5 日に正式に大統領令第 646 号で「ロシア連邦情報セキュリティ原則（Doctrine of Information Security of the Russian Federation[257]）」を承認した。

2016 年 12 月の情報セキュリティ原則（ドクトリン）は、2000 年の情報セキュリティ原則に代替するもの、情報分野におけるロシア連邦の正式な見解を示したものである。新ドクトリンでは、情報空間（information sphere）を「インタアーネットの情報通信網における情報、情報化の対象、情報システムおよび Web サイト、通信ネットワーク、情報技術、情報の生成・加工、当該技術の開発・利用、情報セキュリティの確保に従事する法人の組み合わせならびに情報空間における公的関係を規制する一連のメカニズム」であると定義している。英語版（仮訳）を読む限り、2000 年版との大きな違いはないようである。主な概要を整理すると次の通りである。

- 情報空間におけるロシアの国益とは、情報空間の持続可能な発展の安心・安全の確保を求める個人、社会および国家の客観的に意味のあるニーズである（2000 年版よりも柔軟な表現となっている）。
- ロシア連邦における情報セキュリティの脅威（情報の脅威）とは、情報空間における国益を損なうリスク要因と活動の組み合わせである。
- ロシア連邦の情報セキュリティは、外部と内部の情報の脅威に対する個人、社会及び国家の防護の状態であり、憲法で保障された人権と市民権及び自由、市民の生活の資と水準、主権、領土の完全性と持続可能な社会経済の発展を確保するものである。
- 重大な情報の脅威と情報セキュリティの状態の評価に基づいて、本ドクトリンでは、ロシア連邦の戦略的優先課題を考慮に入れて情報セキュリティの戦略的目標と主要分野を定義する（新たな表現）。
- 本原則（ドクトリン）は、2015 年 12 月 31 日の大統領令第 683 号により承認された国家安全保障戦略に基づく国家安全保障を確保するための戦略計画の文章である。
- 情報空間における国益保護では、「ロシアの情報主権を保護すると同時に、戦略的安定性を損なう目的で IT を利用する脅威に対抗し、さらに情報セキュリティ空間における平等な戦略的パートナーシップの強化を目的とする国際情報セキュリティシステムの開発を促進する」との条文が新たに明記されている。
- 「重大な情報の脅威と情報セキュリティの現状」と題された部分では、ロシアの情報セキュリティを脅かす主要なマイナスの要因のひとつが重要情報インフラを含むロシアの情報インフラにおいて諸外国が軍事目的で情報技術の影響力を拡大してお

[257] Doctrine of Information Security of the Russian Federation Approved by Decree of the President of the Russian Federation No. 646 of December 5, 2016, Unofficial Translation
http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163

り、さらにロシアの政府機関、研究機関や軍需産業複合施設で技術スパイを行う活動を増せていると指摘する。1)特定の国の諜報機関が IT と心理的なツールを使い内政と社会状況を不安定化していること、2)テロと過激派による情報ツールを使って不当な目的で重要情報インフラを破壊する活動を展開していること、3)銀行証券業界でコンピュータ犯罪が増えていること、4)他国による軍事・政治目的でロシアの国防分野での情報セキュリティを脅かす活動が増えていること、5) 外国メディアにおける、ロシアの外交政策及び国内政策に関する偏見と悪意に満ちた内容を含む情報量の増加などを列挙している。

3.5.5. 2017 年 5 月制定の情報社会発展戦略

2017 年 5 月 10 日、プーチン大統領は大統領行政命令第 203 号を発動し、「2017～2030 年のロシア連邦情報社会発展戦略（2017-2030 Strategy for the Development of an Information Society in the Russian Federation[258])」を承認した。本戦略は 2016 年 12 月 13 日に公表され、公聴会での意見や提言などを反映したものである。

本戦略の基本的な目標は、「ロシア連邦における知識社会形成の諸条件を整備すること」である。ポーランドの NGO である“Center for Propaganda and Disinformation Analysis[259]”” 財団の分析では、ロシアが向こう数年かかると想定される全面的な情報戦争（Information Warfare）に備えていると推論できる。情報戦争では防衛的側面が極めて重要となる。

2017 年 5 月の情報社会開発戦略（2017～2030 年）は、2016 年 12 月の情報セキュリティ原則（ドクトリン）と同時に策定作業が進められ、2008 年 2 月 7 日の情報社会発展戦略に代替し、その内容も全く異なっている。本戦略では、デジタル経済問題の解決に向けた努力にかなりの分量が割かれている。他方、デジタル経済発展プログラムについては、通信マスメディア省が策定中である。以上から、2016 年 12 月の情報セキュリティ原則、2017 年 5 月の情報社会発展戦略と策定中のデジタル経済発展プログラムの 3 本の政策は一体的なものとみられる[260]。

2017 年 5 月の情報社会開発戦略(2017～2030 年)で明記する優先課題は次の通りである。

---

[258] http://en.kremlin.ru/acts/news/54477
http://publication.pravo.gov.ru/Document/View/0001201705100002?index=0&rangeSize=1

[259] https://capd.pl/en/about-us

[260] https://capd.pl/en/analyses/185-analysis-of-the-russian-strategy-for-the-development-of-an-information-society

- 市民の情報アクセス権を確保すること。
- 情報に取り組む際の知識源を選択する自由を確保すること。
- 市民により受容されるデジタル以外のモノとサービスを得る伝統的な形態を保護すること。
- 伝統的なロシアの精神面の価値と道徳規範を優先し、情報通信技術の利用に際して当該価値に基づく行動ルールを遵守すること。
- 市民と組織に関する情報を収集・共有する際には合目的かつ合法的な必要性を保証すること。
- 情報空間におけるロシア市民の利益の保護を確保すること。

情報の収集とアクセスに関して市民の情報アクセス権を確保することや知識源の選択の自由を与えることと、2016 年 12 月の情報セキュリティ原則等の政策で記載された情報空間における国益の確保とは矛盾する内容となっていることから考えると、以上の戦略文書は情報源へのアクセスと選択の自由を規制するとの言外の意味があると解釈すべきであろう。

また、新戦略では、情報通信技術の開発によってロシアの重要な情報インフラがロシア領土内で使われる外国の情報通信技術等によって危険と脅威に晒されるリスクも指摘していることからも、これもロシアの情報空間における国益確保の対象となろう。こうした外国技術を利用することや対外情報がロシア社会に浸透する脅威を避けるための手法（ロシアの情報通信インフラを利用することやロシア製の ICT 技術を使うこと、ロシア減産の信頼性のある貴重な情報を拡散すること等）なども明記している。

加えて、新戦略ではロシアの市場と情報空間への外国の技術および法人のアクセス規制を過剰に強調し、「ロシアの組織と同等の諸条件で外国市場参加者がロシア法を遵守すること」を義務付けている。

2017 年 5 月の新情報社会戦略は世界の変化しつつある政治情勢やセキュリティ状況に対するロシアの応戦ともいうべきもので、ロシア政府がその領土内で情報戦争を繰り広げ、それを国外にも広げつつある証拠であるといえよう。現在のところ、英語翻訳も発出されていないこともあって、この新戦略に応戦する外国勢は現れていない。ポーランドのシンクタンクは、ロシアが世界に向けて全面的な情報戦争の構えにあると推論しうる内容であると断言している[261]。

261
https://capd.pl/en/analyses/185-analysis-of-the-russian-strategy-for-the-development-of-an-information-society

3.5.6. 2018年1月1日施行の重要情報インフラセキュリティ法

2017年7月27日、プーチン大統領は「ロシア連邦重要情報インフラのセキュリティに関する連邦法第 187-FZ 号（Federal Law No.187-FZ On Security of Critical Russian Federation Information Infrastructure)」を承認。同法律2018年1月1日に施行された[262]。この他にも、ロシアは次のような数本の情報セキュリティ関連の法律を制定している[263]。

- ブロッキング防止サービス利用規制法（2017年11月1日施行）：ブロックされたロシアのWebサイトへのアクセスを認めるVPN基盤のリソースを含むブロッキング防止サービスを禁止する。但し、少数のユーザによる利用で、テクニカルニーズによるVPNの商用利用を除外する。
- インスタントメッセンジャー（IM）ユーザのID義務化法（2018年1月1日施行）
- テロ防止法に規定される通信プロバイダ及びオペレータの義務法（2018年7月1日施行）
- ロシアインターネットセグメント防衛法（草案検討中）
- ソーシャルネットワーク運用業者による不正情報削除義務化法（草案検討中）
- その他

クレムリンのニュースリリースによると、2007年7月の重要情報インフラセキュリティ法（2018年1月1日施行）は、ロシアの情報リソースに対するサイバー攻撃の成り行きを検知・防止・排除する国家システムの機能させる基盤を含むロシアの重要な情報インフラのセキュリティを確保するための基本原則を定めたものである。この重要情報インフラセキュリティ法は、重要情報インフラの重要な構成要素におけるサイバーインシデントを防せぐためのメカニズムも定めている。これにより、ロシアに対するサイバー攻撃に際しての国へのマイナスのインパクトを大幅に縮減することになる。さらに、本法は重要情報インフラのセキュリティを確保するための国家機関の権限と各種アクターの権利と義務を明示している。

この法律は、サイバー攻撃があった場合に国家に損害を与えるような重要情報インフラの主要なコンポーネントにおける、サイバー事故の予防に必要なメカニズムを定める。この法律は、重要情報インフラの安全の守るために、国家諸機関の権限を定め、この分野の関係者の権利と義務を定める264。重要情報インフラ安全法の概要は次の通りである[265] [266]。

---

[262] http://en.kremlin.ru/acts/news/copy/55146
[263] http://www.lp.ru/Latest_initiatives_on_Internet_regulation_in_Russia_2017?lang_id=2
[264] http://en.kremlin.ru/acts/news/55146
[265] https://www.cliffordchance.com/briefings/2017/10/new_legislation_regulatingcybersecurityandth.html
[266] https://ocps.hypotheses.org/51

- 対象となる「この分野の関係者」とは、次の事業に関わる企業である。
- 健康、エネルギー、輸送、通信、銀行その他金融、原子力、石油・ガス、防衛、ロケットと宇宙、鉱業、金属、化学産業および研究開発
- 対象となる企業は、如何なるサイバー事故も速やかに当局へ報告し、そして、当局に協力してサイバー攻撃を検知、予防、修復し、サイバー攻撃の原因と環境を究明しなければならない。銀行その他金融機関の場合は、ロシア中央銀行（Russian Central Bank）へ報告しなければならない。
- 対象となる企業は、自らが運用し、あるいは他社へリースしている重要情報インフラの安全性を評価しなければならない。評価項目は次の通りである。
  - 社会的重要性：市民の生命、ライフサポートインフラ、輸送、通信ネットワークへの損害の可能性
  - 政治的重要性：国内外の政治的分野におけるロシアの権益への損害の可能性
  - 経済的重要性：対象となる企業業績およびロシアの国家予算への損害の可能性
  - 自然環境の重要性：自然環境破壊の可能性
  - 国家の防衛、法および秩序への影響の重要性
  - 安全性評価完了後 10 日以内に当局へ報告すること。
- 対象となる企業は、この法に基づく諸規則を遵守しなければならない。(2018 年 1 月末時点で諸規則の詳細は不明である。)
- 対象企業は、この法律に違反して次の項目に該当した場合は処罰を受ける。
  - 重要情報インフラの情報の保管、処理および移動のルールに違反
  - 重要情報インフラあるいは通信ネットワークに不正にアクセスして損害発生

上記法律は運用次第では企業活動に大きな影響を及ぼすと見られる。「当局」が何処を指すか、評価の基準、重要情報インフラの具体的な内容などの情報が待たれる。

3.6. ロシアのサイバー空間能力等

3.6.1. 主要なサイバーセキュリティ会社と研究機関等（一覧表）

ロシア最大のITセキュリティ会社であるカスペルスキー（Kaspersky Lab）やDr. Webなどのサイバーセキュリティ等の研究・開発で中心的な役割を担っている民間企業、研究機関および大学とそれらのキーパーソン等について一覧表として以下に整理したい。

【実績のある大手民間企業】

カスペルスキー（Kaspersky Lab ZAO）（http://www.kaspersky.ru）	
会社概要	❍ モスクワに本社を置くコンピュータソフトウエアの民間企業（非上場会社）。ロンドンに持株会社を置く。2015年の年商は約6.2億ﾄﾞﾙ。 ❍ エンドポイント情報セキュリティソリューションでは世界トップクラス。同社をめぐる疑惑はロシアの国家機関と密接な関係を持っていることに由来する。 ❍ 2014年のIDCデータによれば、エンドポイントセキュリティの分野で世界第4位にランキングされている。 ❍ 1997年6月に設立し、アンチウィルスで成長。世界32ヵ国37ヵ所の事業所を持つ。セキュリティソフトウェアでは欧州市場でトップのシェアを誇り、日本国内においても業界のリーディングカンパニーから官公庁、公共・教育機関まで幅広く導入されている[267]。 ❍ 同社の特色は次の通りである ➢ 事業会社の重要インフラを防護し、プロセスの継続性を確保するために「カスペルスキー産業サイバーセキュリティ（Kaspersky Industrial CyberSecurity）」と称されるソリューションを提供。サイバーセキュリティ分野における長年の経験、情報システムの脆弱性の本質に関する深い理解、国内外規制当局との密接な協力関係に基づく複雑なソリューション機能が搭載されている。 ➢ 金融機関を標的としたサイバー犯罪組織「Lurk」の捜査でロシア貯蓄銀行（ズベルバンク）と共同で法執行機関に協力した実績や、産業CERTを立ち上げて重要インフラ事業者との連携を打ち出すなどの活動の幅を広げつつある。 ➢ 加えて、ベンチャー企業の育成支援として、2016年末までに世界のスタートアップ企業に投資すると発表した。各投資規模は5万ドル～100万ドル。対象分野は、携帯およびクラウドのセキュリティ、IoT、

[267] http://www.kaspersky.co.jp/about/about_us

	物理的セキュリティ、機械動作等である。資金提供以外にも、同社の技術と専門知識による恩恵を受けることができる ➢ 2014年にサイバースパイ（Epic Turla）の脅威に関する公開レポートを公表している。 ➢ CIA元職員のエドワード・スノーデンが提示した資料から、米国と英国の諜報機関がカスペルスキー社（その他の20社以上のアンチウイルスソフト開発会社を含む）を標的にしていたことが明らかにされた。米国ニュースサイト「インターセプト」はNSA（国家安全保障局）と英国のGSHQ（政府通信本部）がリバースエンジニアリングを行ってソフトウェアの脆弱性を探りながら撃破を試みたと伝え、「（米英の）諜報機関は、アンチウイルスソフトをこっそり阻止し、会社からセキュリティソフトやそのソフトのユーザに関する機密情報を得るために、時に疑わしい法的権限のもと、ソフトウェア製品のリバースエンジニアリングを行い、ウェブと電子メールのトラフィックを監視していた」と記している[268]。
主要人物	❍ 会長兼最高経営責任者：ユージン・カスペルスキー（本名：Yevgeny Valentinovich Kaspersky 。俗称：Eugene Kaspersky)。1965年10月生まれ。16歳で諜報機関の幹部養成校であるKGB高等教育機関（KGB Higher School）に入学し、1087年に卒業（数学工学とコンピュータ技術の学士)。諜報機関でソフトウエアエンジニアとして勤務し、1997年にKaspersky Labを設立し、2007年には、Kaspersky Labの最高経営責任者（CEO）に任命された。2013年、取締役会長に就任し、現在に至る[269]。 ❍ CTO：ニキータ・シュベツォフ（Nikita Shvetsov）。国立モスクワ電子数学大学でコンピューターサイエンスの学位を取得。2004 年に Kaspersky Lab にウイルスアナリストとして入社、2006 年にシニア開発者としてヒューリスティックエンジン向けのエミュレータ開発に従事。2009 年には、アンチマルウェアリサーチ部門のディレクターに就任。 ❍ COO：アンドレイ・チーホノフ（Andrey Tikhonov)。キエフ軍事アカデミーを優秀な成績で卒業後、ロシア連邦軍に所属。最終階級は中佐。1989年にロシア国防省付属の研究所で勤務を開始し、IT業界に携わ

[268] VICTORIA ZAVYALOVA (June 26, 2015) “NSA and GHCQ targeting antivirus developers, say Snowden documents”
http://rbth.com/science_and_tech/2015/06/26/nsa_and_ghcq_targeting_antivirus_developers_say_snowden_docu_47261.html

[269] https://www.forbes.com/profile/eugene-kaspersky/

	る。2012年1月にKaspersky Lab の最高執行責任者（COO ）に就任。

Dr. Web (http://company.drweb.com/?lng=en)	
概要	❍ Doctor Web, Ltd.（ドクターWeb社）は、2003年に設立されたロシアに本社を置くアンチウィルス開発販売会社。「Dr.Webアンチウイルスソフトウェア」のディベロッパーであり、独自のマルウェア検出及び修復テクノロジーを有する、世界でも数少ないアンチウイルスベンダーの1つでもある。主な特色は次の通りである[270]。 ➢ 共同創業者兼CTOのイーゴリ・ダニロフ(Igor Daniloff)がDr.Webの商品名を持つアンチウィルスを開発し、1992年に市販開始。2003年にドクターWeb社を設立した。従業員数は400人強で、その半数以上が研究開発部門に所属している。本社はモスクワ。アンチウィルス研究開発部門はサンクトペテルブルクに設置されている。 ➢ 同社はロシア市場におけるインターネットサービスプロバイダ（ISP）に対するセキュリティサービスの第一人者として不動の地位を保っている。 ➢ 数々の賞を受賞し、情報セキュリティツールに対する連邦技術輸出管理庁（FSTEC）のライセンス（情報セキュリティツールの開発に対するロシア連邦の連邦技術・輸出管理サービスのライセンス及び機密情報保護ツールの開発、リリースに対するロシア連邦の連邦技術・輸出管理サービスのライセンス)、情報セキュリティツールの開発に関連した活動に対するロシア国防省のライセンス、連邦保安庁（FSB）の各種ライセンス、連邦保安庁（FSB）及び連邦技術・輸出管理庁（FSTEC）の認証証明書を取得済みで、主要製品であるDr.Webアンチウイルスソリューションを世界各国の企業及びホームユーザーに提供している。
主要人物	❍ CEO：ボリス・シャロフ（Boris Sharof） ❍ 共同創業者兼CTO：イーゴリ・ダニロフ（Igor DaniloffまたはIgor Danilov)。

Group-IB（サイバーセキュリティグループ有限会社）(http://www.group-ib.ru)	
概要	❍ 2003年に創業。サイバー犯罪や詐欺に焦点を当て、サイバー脅威の監視、ハイテク分野の犯罪捜査への参加、サイバーセキュリティのソフトウェア

[270] https://company.drweb.com/?lng=en

	開発を行っている。東欧最大の犯罪科学研究施設であり、「ハイテク犯罪分野の重要な捜査事案の80%に関与している」。 ➢ Group-IBは、決済処理システム「クロノペイ（Chronopay)」の共同設立者であるパーベル・ブルブレフスキー（Pavel Vrublevsky）がアエロフロート（Aeroflot）のウェブサイトにDDoS攻撃を仕掛けた刑事事件で専門組織として参加を要請されたことで著名になった。また同社は、詐欺的なウェブサイトの調査でQiwi社を支援し、アメディア（Amedia）と共同でアメディアの動画やシリーズ物への不正なハイパーリンクのロックに参加した実績もある。 ➢ 2015年末、Fox-IT社と共にロシアの銀行部門でサイバー犯罪による惨事を引き起こしたとされるハッカー集団、アヌナク・ギャング（Anunak gang）について詳述した報告書を発表している。 ➢ 同社の脅威防止調査担当部長であるドミトリー・ヴォルコフ(Dmitry Volkov）は、ロシアのサイバー犯罪に関するエキスパートとしての同社の地位を築いた著名な専門家である。 ➢ 25カ国以上に顧客を持つ。SPARK-Interfaxのデータによれば、Group-IBの2013年度の利益は8,660万ルーブル、純利益は82万4,000ルーブルだった。イリヤ・サチコフ（Ilya Sachkov）は、利益の90%は民間企業への商業サービスによってもたらされ、残り10%は政府の注文によると述べている。
主要人物	❍ 創業者兼CEO：Ilya Sachkov ❍ 脅威防止調査部：Dmitry Volkov

Experimental Design Office (EDO) SAPR（www.okbsapr.ru）	
概要	❍ 暗号化機構を含む不正アクセスからの情報保護を目的とするハードウェアやソフトウェアの設計会社で、20年以上の歴史がある（1989年設立)。
主要人物	❍ 最高責任者（DG)：Yury N. Veprov氏

Informzaschita Group of Companies（http://www.infosec.ru）	
概要	❍ インフォルムザシタ（Informzaschita）企業グループは、自動制御システムにおける情報セキュリティ確保を専門としており、18年以上ロシア市場でトップの座を維持している。同グループは現在、システムインテグレーターのほか、セキュリティ・コード、トラストバース、ナショナル・アテステーション・センター（National Attestation Center)、インフォルムザシタ・トレーニング・センターの4社で構成されている。 ➢ 同グループの企業は、世界有数のセキュリティソリューションプロバ

	イダーであるIBMインターネットセキュリティシステムズ（IBM ISS)、カスペルスキー、ポジティブ・テクノロジーズ（Positive Technologies)、チェック・ポイント・ソフトウェア・テクノロジーズ・リミテッド、HPアークサイト（HP Arc Sight)、シスコ・システムズ、Stonesoft、フォーティネット（Fortinet)、インパーバ（Imperva)、インフォウォッチ（InfoWatch)、CryptoPro、ウェブセンス（Websense）などの認定パートナーである。 ➢ また、決済システムのセキュリティ要件の国際標準化団体であるPCIセキュリティスタンダードカウンシル（PCI Security Standards Council）との提携に基づき、PCI DSS国際基準の遵守に関する監査の実施を認められている。
主要人物	❍ 共同創業者兼社長兼CEO：Peter Efimov ❍ 副社長、専務理事：Leonid Ukhlinov(2009～2013年まで、JSC Sirius Concern社（Rostec Corporation)の設立に貢献。工学博士号取得。）

InfoWatch（https://www.infowatch.ru)	
概要	❍ インフォウォッチ（InfoWatch）は数社から成る企業グループで、組織の情報セキュリティを確保し、外部・内部のセキュリティ脅威を防止するソフトウェア製品や統合ソリューションを開発している。 ➢ インフォウォッチ・グループはロシア、ドイツ、ベラルーシ、マレーシアに22の営業所を有する。モスクワにある中核的研究開発所では、300人以上のスペシャリストや専門家が独自製品・技術の開発・導入・促進に携わっている。 ➢ ITセキュリティを手掛けるインフォウォッチ・グループは2016年に「シールド」製品の販売を開始する予定である。これは、国立原子力研究大学（National Research Nuclear University）MEPhIの専門家が開発したソフトウェア／ハードウェアの総合製品で、ロシア及び国外（主にBRICS諸国）においてサイバー攻撃から製造会社の自動化機器を保護するために使用できる。
主要人物	❍ CEO：Natalya Kaspersky（カスペルスキー社の共同創業者）

ICL-KME CS（http://www.icl.ru)	
概要	❍ ロシア最大のシステムインテグレーター。ICL-KME CSは、カザン・マニュファクチャリング・エンタープライズ・オブ・コンピューター・システムズ（Kazan Manufacturing Enterprise of Computer Systems：KME CS）と英国のインターナショナル･コンピューターズ･リミテッド(International

	Computers Limited：ICL）によって1991年に設立された。ICLは富士通株式会社の子会社である。 ❍ 同社の主要事業は以下の通り。 ➢ 国家機関及び民間企業向けデータ管理システムの設計・実装 ➢ 情報セキュリティ、及びデータ管理システム、ローカルエリアネットワーク（LAN)、ソフトウェアとハードウェア、通信システムの保護 ➢ MRP-II及びERP規格に準拠した経営管理の自動化 ➢ 様々な複雑度の業務・会計システムの設計・導入・保守・サポート ➢ 様々な特性や構造の企業及び組織の財務・会計システムの設計・導入・サポート ➢ システム全体のソフトウェア及びアプリケーションソフトウェアの開発、情報システムの実装・サポートサービス ➢ 世界、企業及び地域の通信システム並びに構内配線網のプロジェクト管理及び設計 ➢ 自社ブランド名RAYのサーバ、デスクトップ、ノートパソコンの連続生産 ➢ ハードウェア・ソフトウェア販売 ➢ 適切なライセンスに基づく統合ITサポートサービス ➢ ITコンサルティングサービス、研修、スキル開発及び再教育
主要人物	❍ 最高責任者（DG)：Victor V. Dyachkov ❍ サイバーセキュリティ部門：Ilya Petrov

旧統一機器製造会社（OAO United Instrument Manufacturing Corporation）：現在のRuselectronics（ルスエレクトロニクス）	
概要	❍ ロシア大統領の命令[271]により、UIMC（統一機器製造会社）が2014年3月に創設され、ロステク（ROSTEC）国家コーポレーションの傘下に置かれた。同社は、ロシアの軍事用無線電子産業の研究生産複合事業体を統一した巨大な特殊マネジメント会社である[272]。 ❍ CEOは、アレクサンドル・ヤクーニン（Alexander Yakunin）である[273]。 ❍ 2017年2月にRuselectronicsに吸収合併された。 ❍ 旧UIMC（統一機器製造会社）は、55社と無線・電子産業の研究機関で構成

[271] Assignment of the President of Russian Federation "About creation of joint holding company in the field of radio-electronic industry"

[272] http://opkrt.ru/en/news/160-alexander-yakunin-this-is-the-first-large-scale-project-of-the-kind-in-russia

[273] http://rostec.ru/en/about/holdings/4513786

されている。主な特色は次の通りである。

- ロシア軍にデジタル通信システム、自動制御システム、電子戦争システムを導入し、2020年までに軍全体の装備品におけるこれらの新製品の割合を最大70%に押し上げること。
- ロシア情報資源及びシステムにおける主要なセキュリティ脅威を軽減すること。
- サイバー犯罪及びサイバーテロとの闘いにおいて、開発を進めること。
- 主なタスクは、国内無線電子製造における経済効率性と競争力の向上、輸出拡大、民生品製造の最大40%の増加など。

❍ JSCルスエレクトロニクス（Ruselectronics）社はROSTEC100%出資の持株会社（ロシア政府出資会社の子会社）で、ロシア最大の軍事用マイクロエレクトロニクス会社である。ロシアの電子製品の80%を生産している。本拠地はモスクワ。CEOは、Andrey Zverev 。2016年の売上高は8.8億ﾄﾞﾙで、純利益は2.7億ﾄﾞﾙ。総従業員数は3万4,000人である[274]。

❍ 旧UIMC(現在のRuselectronics)の中で、情報セキュリティ領域に関わる主な企業は、次の3社である。

Sozvezdie社（Concern Sozvezdie）

- ❍ 専門領域：インテリジェントな制御及び通信システム、電子戦争システム及び特殊装置、民生用及び電気通信製品
- ❍ ホールディング傘下の企業及び組織数：17 [275]
- ❍ ホールディング会社全体の従業員数：173,000人

マネジメント・システムズ社

- ❍ 専門領域：政府、ロシア軍及び軍関連部署における自動制御システムの開発、製造、修理、維持
- ❍ 傘下の企業及び組織数：15 [276]

[274] http://www.ruselectronics.ru/eng/

[275] Concern Sozvezdie OJSC; Almaz OJSC; Voronezh Scientific-Research Institute Vega OJSC; Voronezh CDB Polyus OJSC; Tambovapparat Plant OJSC; Design Bureau of Experimental Works OJSC; Design Bureau Selena OJSC; Krasnodar Instrument Factory Cascade OJSC; Scientific-Research Institute of Communication and Management OJSC; FSUE Scientific-Research Institute of Electronic Technology; NPP Volna OJSC; NPP Start OJSC; Ryazan Radiozavod OJSC; Tambov Factory October OJSC; Tambov Factory Revtrud OJSC; Tambov Scientific-Research Institute of Radio-Engineering EFIR; Yantar OJSC

[276] Management Systems OJSC; Red Banner of Labor Scientific-Research Institute of Automatic Equipment named after academician V.S. Semenikhin OJSC; Concern Systemprom OJSC; Scientific-Production Association Polet OJSC; Scientific-Production Association Impulse OJSC; Information and Telecommunication Technologies OJSC; Scientific-Research Institute of Information Technologies OJSC; Federal Research and Production Association Mars OJSC"; Kimovsk Radio-Electromechanic Plant OJSC; Scientific-Production Center Vigstar OJSC; Scientific-Research Institute Mashstab OJSC; Scientific-Research Institute Rubin OJSC; Scientific-Institute of Electronic

	❍ ホールディング会社全体の従業員数：10,000人
	経済学、情報科学、制御システム中央研究所（Central Research Institute of Economics, Informatics and Control Systems）
	❍ 専門領域：軍産複合体において、45年間、システム全体の情報技術及び経済分析プロファイルを担う。軍産複合体における制御・通信基盤エンジニアリングの改良、アップデート、開発に関する主要業務において、科学的・技術的な支援と実施に主導的立場で従事し続けている。 ❍ 総従業員数：約800人 ❍ 2014年、内務省より「匿名で通信を行うためのTor匿名ネットワークのユーザ及びユーザ機器から技術情報を取得する可能性に関する調査（約11万ドル相当）」事業を受託[277]。

【ロシア政府と関係の深い研究機関】

連邦技術輸出管理庁（FSTEC）傘下の「技術情報保護のための国立研究訓練機関（State Research & Testing Institute of Technical Information Protection: SRTITIP）	
概要	❍ 同研究所の主な目的は、FSTECのために活動し、政府やFSTECの命令に従って作業やサービスを遂行することによって、情報保護の実施母体として行動することにある。SRTITIPは、主に以下に関わるR&D業務に従事している。 ➢ テクノロジーインテリジェンスからの情報保護に関する概念の開発 ➢ FSTECの代理として、規制、法律、方法論的な文書の作成 ➢ テクノロジーインテリジェンス能力のシミュレーションや予測、その能力の評価方法の改善 ➢ 情報保護の技術的手段の開発及び効率的保護の管理
主要人物	❍ 理事長：Alexander V. Anishchenko

Research & Testing Institute of Complex Safety Systems（www.niisokb.ru）	
概要	❍ 同研究所はガスプロムと関連し、FSTECに認定された営利組織で、主にガスプロム関連企業にサービスを提供している。 ➢ 情報保護システムの予測、開発、設置、運用及びサービス提供に従事。 ➢ それ以外の活動には、通信ツール及びシステム、ローカルコンピューターネットワーク、並びに計算機の配送、導入、運用、サポート、保証、保証後の保守；情報セキュリティ要件に対する自動システムの適合性の認定；情報システムの監査；認定センターのサービス提供；規制文書（ISO/IEC、FSTEC、ガスプロム）に対する複合的なセキュリティ手段

Control Machines named after I.S.Bruk OJSC; Scientific-Research Institute of Automated Systems and Communications systems Neptune OJSC; Scientific and Production Complex Krasnaya zarya OJSC

[277] "Russian firm tasked with cracking Tor throws in towel" (September 23, 2015) https://www.scmagazine.com/russian-firm-wants-to-back-out-of-contract-to-crack-tor/article/533639/

	およびシステムの適合性の認定などがある。
主要人物	❍ 最高責任者（DG）：Igor A. Kalaida

【大学等の研究機関】

モスクワ国立研究核大学（NRNU）モスクワ工業物理学大学（MEPhI）サイバーセキュリティセンター（CCS）：略称 Center for Cybersecurity MEPhI（http://cc.mephi.ru）	
概要	❍ 国家研究大学（National Research University）の創設に向けた実験プロジェクトに関する2008年10月7日の大統領令第1448号に基づき、2009年4月8日の政令第480-r号で、MEPhI（モスクワ工業物理学大学：1942年創設の旧モスクワメカニカル研究所）は国家研究大学に選定された。 ❍ したがい、国家研究大学MEPhI（モスクワ工業物理学大学）はロシアで最も著名な研究大学となり、旧原子力庁であったロサトム国家コーポレーションの研究基盤となっている。MEPhIは全ての主要都市に分校を設置しており、ロサトムにとっては、若年層が地元で修学できるといった点も重要となっている。各分校にはそれぞれ専門分野があり、核関連施設内の分校は軍事向けに、一般の諸都市にある分校は民生用分野に特化している。大学入学に際しては競争試験が行われるが、原子力発電所の運用管理者、製品技術者、工業技術者などの非常に難しい専門性を目指す若者の数が年々増加している[278]。 ❍ MEPhI（モスクワ工業物理学大学）のサイバーセキュリティセンター（CCS-Center for Cybersecurity）は、サイバネティクスセキュリティ学部（Department of Cybernetics and Security）内に設置されている。 ❍ 同センターはオープンITセキュリティ研究を専門として、国内外のIT市場向けの新世代の人材を育てている[279]。 ❍ 主な協力パートナーは、State Corporation《Rosatom》、《Gazprom》。JSC《Russian Railways》、JSC《Russian networks》、Rosneft、VNIIA Dukhov、NIKIRET ❍ NIIAS等の国有会社のほか、Siemens AG、Schneider Electric、NVIDIA Corporation、Apple、Microsoft、Parallels, Inc、Intel Corporation、JSC《InfoWatch》、《Kaspersky Lab》、ABBY、Acronisなどである[280]。

モスクワ大学[281]の情報セキュリティ研究所（Information Security Institute of Moscow

[278] http://crds.jst.go.jp/dw/20150623/201506235995/
[279] http://cc.mephi.ru/en/page-2/
[280] http://cc.mephi.ru/en/partners/
[281] 公立大学。正式名はM. V. ロモノーソフ・モスクワ国立総合大学。

University)

概要

- 大学内の研究部門であり、教育プログラムは有していない。モスクワ大学総長で科学アカデミー正会員のヴィクトル・A・サドーブニチィ（Viktor A. Sadovnichiy）の指令第516号により2003年7月2日、モスクワ大学の独立部局として設立された[282]。現在、2004年8月7日に解散された連邦政府通信・情報局（FAPSI）及びFAPSI第3総局・通信手段電波電子情報総局（GURRSS）の長官を務めたVladislav Sherstyuk氏が主導する[283]。
  - 同研究所の目的の1つは、モスクワ大学内の情報セキュリティ関連の研究活動を調整することで、同大学に所属する15名がこの調整委員会のメンバーを務めている。
  - 同研究所は、次の5つの部門から構成され、22名スタッフが在席している：
    - 情報セキュリティの数学的研究
    - コンピュータシステムの情報セキュリティ
    - 情報セキュリティの人文学的研究
    - 資格証明書の専門知識及び承認に関するセンター
    - セキュリティ研究及びテロ対策における国際協力センター
- 研究分野は、次の通りである[284]：

暗号学における数学的課題	離散マッピングの暗号プロパティ
	暗号プロトコルのセキュリティ
	暗号分析におけるブーリアン方式の充足法
	暗号作成における非アルキメデス動力学方式
極めて重要な対象における情報セキュリティの計算とソフトウェア	安全な情報技術のための計算とソフトウェア
	国家情報資源の管理のための体系的及び技術的環境
セキュリティの人道的問題	情報セキュリティのための政府、企業、市民社会の協力における人道的問題
	テロ防止のための政府、企業、市民社会の協力における人道的問題

- モスクワ大学情報セキュリティ研究所の顧客には、以下の組織が名を連ねている[285]：
  - ロシア大統領執務室、連邦保安局（FSB)、国家反テロ委員会（National Antiterrorist Committee)、国防省一般幕僚、連邦技術・輸出管理庁（FSTEC)、連邦関税局（Federal Customs Service)、科学教育省の科学イノベーション庁（Federal Agency on Science and Innovation of

[282] http://www.iisi.msu.ru
[283] Keir Giles (2011) "Information Troops" – a Russian Cyber Command?" 3rd International Conference on Cyber Conflict; C. Czosseck, E. Tyugu, T. Wingfield (Eds.) Tallinn, Estonia, 2011; CCD COE Publications. http://conflictstudies.org.uk/files/Russian_Cyber_Command.pdf
[284] http://www.ipib.msu.ru/Aboutus(eng)/Research(eng)/
[285] http://www.ipib.msu.ru/Aboutus(eng)/Customers(eng)/

	Ministry of Science and Education)、基礎研究基金(Russian Foundation for Basic Research)、OJS ガスプロム、OJS ロス・ケミカル・ディフェンス（RusChemicalDefence)、航空素材の科学研究機関（All-Russian Scientific Research Institute of Aviation Materials）及びスイス国防省調達部（Federal Office for Defence Procurement armasuisse／DDPS) ➢ またパートナー組織と連携して、ロシア国内外で科学イベントを開催。年に 1 度、セキュリティと対テロに関する国際科学会議も行っている。 ❍ ロシア連邦安全保障委員会執行事務局、国家反テロ委員会執行事務局、外務省、内務省特別技術局（Bureau of Special Technical Actions Ministry of the Interior of Russian Federation)、連邦情報技術庁（Federal Agency on Information Technology）といった政府機関；RANS（Russian Association of Networks and Services）；OSJガスプロム、OSJロステレコム、OSJメガフォン（MegaFon)、Closed JSCトランステレコム等の企業体；ロシア暗号学会、全ロシア科学研究機関（コンピューター及び情報科学)、ロシア科学アカデミー・情報科学問題研究所（IPI RAN)、ロシア科学アカデミー・システムプログラミング研究所（ISP RAS)、国立原子力研究大学・モスクワ工科物理研究所（MEPhI）等の大学・研究機関と連携している。この他、ベラルーシ大学、ニューヨーク州立大学、カールスルーエ工科大学（独)、ジョージ・マーシャル欧州セキュリティ研究センターなど、海外の大学・研究機関とも提携している[286]。 ❍ なおモスクワ大学の機械工学部（Mechanical Engineering(MAMI)）にも、自動化情報システムにおけるサイバーセキュリティに関する専門科が設置されている。
主要人物	❍ 2004年8月7日に解散された連邦政府通信・情報局（FAPSI）及びFAPSI第3総局・通信手段電波電子情報総局（GURRSS）の長官を務め、現在は同研究所の所長を務めるVladislav Sherstyuk氏

上記の他、国立エレクトロニクス技術研究大学（MIET）微小デバイス及び応用サイバネティックス学部)、モスクワ工科大学高度セキュリティ及び特殊計装研究所、国家研究大学エンジニアリング経済研究所（MEI）サイバーセキュリティ管理、ドン国立工科大学、情報システム・アカデミー[287]、バウマン記念モスクワ国立工科大学[288]の教育センター[289]などの教育

[286] http://www.ipib.msu.ru/Aboutus(eng)/Offersforbuisness(eng)/
[287] НОУ Академия Информационных Систем
[288] Московский государственный технический университет им. Н. Э. Баумана というロシア語の名称（государственный は「国立の」の意味）からすれば、「国立大学」のよう。
[289] Учебный центр «Специалист» при МГТУ им.Н.Э.Баумана

機関、民間のMASCOM社（情報セキュリティセンター）[290]等でも、サイバーセキュリティの分野における講座や訓練を提供している。

3.6.2. サイバーセキュリティ対策の官民連携の動向とプロジェクト

現在ロシアは、重要 IT インフラの安全性確保に向けた規制・法律上の枠組みの確立を進めており、作成中の文書にて、官民連携の在り方が定められる見通しである。ただし、重要インフラ防護のための官民連携には、秘密指定情報の共有の問題やインシデント報告が規制強化につながることへの不安、重要インフラ分野の巨大国営企業の消極性などの課題もある。以下では、官民共同体の RANS、金融セクターにおける法執行機関・ロシア貯蓄銀行・カスペルスキー社の連携事例、国家システムとの連携を見据えたカスペルスキー社の産業 CERT とその課題について整理した上で、国家プログラム「情報社会（2011 年 - 2020 年）の概要を記載する。

【Russian Association for Networks and Services (RANS)】

RANS は、1994 年 8 月 30 日に設立されたネットワークサービス協会（Association of Networks and Services）を引き継ぐかたちで、2000 年 1 月 19 日付の行政命令第 77r 号に基づき、通信・マスコミ省を中心に設立された官民共同体である[291]。主なミッションは、加盟組織の能力を活用し、国民、企業及び政府当局の情報通信技術ニーズと IT セキュリティ技術を実現することである。現在、RANS には約 60 の組織が参加しており、技術機器製造事業者、システムインテグレーター、科学・学術機関、弁護士事務所、コンサルティング企業及び政府機関が含まれる。このうち、政府組織としては、連邦税関庁、内務省、連邦保安庁、財務省、FSO、通信・マスコミ省が参加している。主な活動は、次の通りである[292]。

- ICT インフラの精緻化と ICT への安全かつ信頼できるアクセスのための規制案の作成
- ICT 分野の研究
- 連邦政府機関に対する提案の準備
- 規制案のための専門家意見の準備
- 国際標準への参画
- 訓練及び啓蒙活動

---

[290] Учебный центр безопасности информации "МАСКОМ"
http://www.mascom.ru/en/far-east/
[291] The 2nd Federal Forum “Telecom QoS Russia 2016 (March 3, 2016)
http://www.comnews-conferences.ru/en/conference/qos2016/support
[292] http://www.nisc.go.jp/inquiry/pdf/fy21-brics.pdf

2011 年 8 月以降、RANS は、連邦通信省の支援を受けつつ、自発的な認証システム「通信効率性（Communications - Efficiency）を運営している。

【金融セクターのセキュリティにおける連携】

重要インフラのサイバーセキュリティ対策では、特に、サイバーインシデントによる被害を被った金融セクターにおいて、僅かながら民間企業と連携した取り組みが少しずつ始まっているようである。ロシア最大の IT セキュリティ会社であるカスペルスキー社は、2016 年 6 月のプレスリリースにおいて、同社の専門家とロシア大手銀行のズベルバンク（ロシア貯蓄銀行）が、サイバー犯罪組織「Lurk」の捜査でロシアの法執行機関に協力し、過去最大規模のサイバー犯罪者 50 人の逮捕に貢献したと発表した。逮捕の容疑は、銀行をはじめとする金融機関や企業に対するボットネットを利用した攻撃で、2011 年から 4,500 万ドル（30 億ルーブル）以上を窃取したとみられており、今回の逮捕によって、ロシア警察は 3,000 万ドル（22 億 7,300 万ルーブル）以上に相当する不正送金を未然に防ぐことができたという。

コンピュータインシデント調査を統括するルスラン・ストヤノフ（Ruslan Stoyanov）によると、カスペルスキー社は、2011 年に Lurk トロイの木馬を活用したサイバー犯罪組織の活動や Lurk の犯罪組織にロシア人が関わっていることを検知し、捜査に協力してきたという。具体的には、マルウェアを分析し、Lurk の攻撃者が悪用していたコンピュータとサーバのネットワークを特定したことにより、ロシア警察による容疑者の特定と犯罪証拠の収集に繋がったとされる。Lurk の標的となったのは、金融機関やメディアの Web サイトだけではなく、VPN 接続を利用して自らの痕跡を隠ぺいするため、様々な IT 企業や通信事業者に侵入し、サーバを利用して匿名性を確保していたようで、同社は今後もサイバー犯罪捜査等に積極的に協力していくとしている[293]。

【民間 CERT と官民連携の課題】

これまで、重要インフラ事業者全体と政府との常設の情報共有体制は確認されてこなかったが[294]、現在ロシアでは、2013 年 1 月のプーチン大統領の指示により、連邦保安庁（FSB）がロシア領内並びにロシア在外公館及び領事館の情報資源を標的としたコンピュータ攻撃を検知・予防及び攻撃による影響を排除するための国家システム（Detection and

[293] Kaspersky Lab (June 1, 2016) “Kaspersky Lab Assists in Russia’s Largest Cybercriminal Arrest: The Hackers Who Stole $45 Million”
https://www.kaspersky.com/about/press-releases/2016_kaspersky-lab-assists-in-russia-s-largest-cybercriminal-arrest-the-hackers-who-stole--45-million
[294] http://www.nisc.go.jp/inquiry/pdf/fy21-brics.pdf

Prevention of Computer Attacks: DPCA）（GosSOPKA[295]）の構築を進めているところで、同スキームにはコンピュータインシデントに対する国全体の調整センターも含まれる計画である（詳細は 2.2.2.3.を参照）。

他方で、情報セキュリティインシデントに対する民間 CERT が 2016 年 10 月からロシアで業務を開始する。これはカスペルスキー社が、脆弱性に関する情報を集約し、原子力発電所や核燃料、石油・ガス、複合エネルギー企業といった国家戦略上重要な施設に対するハッキングに対応するために設立したもので、脆弱性、脅威、インシデントに関する情報を収集するとともに、産業施設の検査、ペネトレーションテスト、インシデント調査も行う。カスペルスキーの産業 CERT は GosSOPKA と連携し、産業施設のインシデントやハッキングに関する情報を入手することになるとみられている。カスペルスキーの重要インフラ防護能力センターのエフゲニー・ゴンチャロフ（Evgeny Goncharov）所長は、「産業 CERT の準備は当社のみの独自の取り組みであり、国及び州の規制当局のほか、ロシアだけでなく世界のサイバーセキュリティに責任を負う組織と密接に協力している」と自信を覗かせている。

このように、ロシアが米国の実務を採用し、個々の重要セクターにおける独自の CERT の確立を目指している点は注目に値するものの、各重要インフラセクターの大手企業体は、自社の重要インフラの脆弱性に関する情報をカスペルスキー社に伝えることに対して、必ずしも熱心ではない。ロシアの各重要インフラ事業者は平素から監督官庁との密接な関係の下で、独自にインフラ防護を実施している（各事業者とも、役員会内に連邦保安庁等の出身者を受け入れており、関連国家機関との窓口の役割を果たしているものと考えられる）。

こうした事などから、専門家たちの間では、特に「ガスプロムやロスネフチレベルの企業は、自社の脆弱性に関する情報を自発的に民間企業に伝えることはないだろう」との指摘がなされている。実際、ルスハイドロ（RusHydro）の広報部は、同社が情報セキュリティ管理に向けて、傘下の全社を対象とした独自のセキュリティ・オペレーション・センター（SOC）の設立に積極的に取り組んでおり、GosSOPKA との連携について協議していることを明らかにした上で、「カスペルスキーが提案した機能を、助けを借りずに直接に連邦保安庁（FSB）と協力して実現する予定」であると述べている。また、ある大手事業会社の関係者は、カスペルスキーの提案する産業 CERT 設立を意識はしているが、インシデントのデータを定期的に提供するつもりはないことを明らかにしている。この他、Group-IB に所属する CERT-GIB が、RuNet のユーザにとっての情報セキュリティ脅威の低減に従事している。

[295] GosSOPKA は Государственной системы обнаружения, предупреждения и устранения последствий компьютерных атак（コンピュータ攻撃による影響の発見・防止・排除システム）の省略語

【国家プログラム「情報社会（2011 年 - 2020 年）】

国家プログラム「情報社会（2011年 - 2020年）（Information Society（2011 thru 2020））」も注目に値する。同プログラムは、(1) 情報社会における情報・通信インフラ及びそれらインフラに基づいて提供されるサービス、(2) 情報環境、(3) 情報社会のセキュリティ、(4)情報国家の4つのサブプログラムから成る。このうち3番目のサブプログラム「情報社会のセキュリティ」が特に関連するもので、基本的な内容は以下の通りである：

- 通信、情報技術及びマスコミュニケーションの分野における許可及び登録業務の監督と管理
- 情報及び通信システムの機能の安全性確保
- 個人の生活、個人及び家族の秘密の不可侵性並びにアクセス制限のある情報のセキュリティを確保するための情報保護技術の開発
- テロリズム及び過激なイデオロギーの拡散に対するカウンターアクション、暴力行為の擁護に対するカウンターアクション

同サブプログラムに含まれる主要措置を通じて、プログラムの実施に関する国家の管理（監督）機能の遂行、情報保護手段の提供、脅威のモニタリング、インフラ耐性の定期的評価、防御が破られた場合に生じる悪影響の排除、及びインフラ防護システムの適宜更新を行うことによって、情報集中型社会において生起する脅威を予防するための手段を提供することが期待されている。主な成果としては、以下が想定される：

- 世界水準を上回るロシアの情報技術市場の成長
- プロセス及び協調環境の標準化並びに情報処理技術の導入による経済的取引費用の大幅削減
- 情報に対する個人の権利を含めた人権や基本的自由の確保
- 個人の生活、個人及び家族の秘密、アクセス制限のある情報のセキュリティを確保するための高度な情報保護関連技術の導入
- ロシア連邦の構成主体におけるイノベーション活動に必要なインフラ環境の調整

2011 年から 2020 年にかけての主な活動事項の 1 つとして、「3.2『ロシアの国益に対する情報技術上の脅威の防止（Prevention of information technology threats to national interests of Russia)』がある。これは、通信・マスメディア省のハイテク開発部が関連措置を所管するもので、具体的には次の措置を講じるとしている：

- 情報保護関連の国家技術の市場展開

- 国家ソフトウェアプラットフォームの設置
- （パブリックドメイン上の）フリーウェアを使ったオペレーションシステム及びアプリケーションの全国的な環境構築
- オープンソースの開発成果を利用した国家的なデータベース管理システムの創出
- ソフトウェア開発のためのロシア独自の環境の提供
- 情報セキュリティ確保のためのドライバー及び手法を含む応用ソフトウェアの基本パッケージの創出
- アルゴリズム及びコードの国家プールの設置

因みに、インターネットネットワークの国家セグメント[296]及びそれに関連した重要資源の監視、統合性の管理、及び安定した機能を確保するための特別なソフトウェア・ハードウェア複合システムが開発され、2015 年に試験運用を開始している。

2011 年から 2020 年にかけての別の活動事項「3.3『テロリズム、過激主義及び暴力行為に関連した対抗措置（Countermeasure activities pertinent to terrorism, extremism and violence)』を規定した条項も設けられている。当該事項を担当するのは連邦保安庁（FSB）で、実施に当たっては、(1) 対テロ防御問題に関する統合データバンクの商業運用、(2) 当該データバンクの外部（第三者）情報管理システムとの統合、(3) 体系化されていない多くの情報の保管及び加工に関連した国家的技術の開発及びサポートといった措置を講じるとされている。ところが、関連規制及び法的文書が存在しないため、当該分野に関する活動は 2015 年には全く行われなかった。

[296] LAN を構成する基本単位

4. シンガポールのサイバー空間に関わる体制・能力等の実態

4.1. サイバーセキュリティ庁（CSA）とサイバーセキュリティ戦略

シンガポールのサイバーセキュリティ戦略とその作戦、教育、エコシステム開発などを担うのは、サイバーセキュリティ庁（CSA：Cyber Security Authority[297]）である。政府エージェンシーのCSAは首相府傘下に置かれ、通信情報省（MCI）がマネジメントを行っている。主な任務は、国家サイバーセキュリティ機能の監督と官民連携による重要インフラ防護である。2015年4月1日に創設され、様々な業界とステークホルダーと連携して、サイバーセキュリティ認知を高める努力を払っている。CSAのトップは、David KOH長官（Chief Executive）である。副長官は、Ms. Christina LEEとNG Hoo Mingなどである[298]。

対外面では、CSA（サイバーセキュリティ庁）は、2017年9月18日に日本のNISC（内閣セキュリティセンター）と政策対話や情報交換、サイバーセキュリティアウェアネスの強化、ベストプラクティスの共有等に関する協力覚書を締結[299]。英国（2015年7月29日）、インド（2015年11月24日）、オランダ（2016年7月12日）、米国（2016年8月3日）、オーストラリア（2017年6月2日）、ドイツ（2017年7月6日）などともサイバーセキュリティ協力に関するMOUを締結し、ASEAN諸国とのサイバー協力の強化を図りつつある。

国内外の民間プレーヤについては、CSAは、Singtel、Check Point Software Technologies FireEye、Microsoft、Palo Alto Networks、CREST International、Association of Information Security Professionals（AISP)等ともパートナーシップ協定を結び、人材研修、研究開発や情報共有等の協力関係を推進中である[300]。

特にFireEyeとは、CSA（サイバーセキュリティ庁）は、サイバー犯罪、サイバー脅威等の情報共有の強化などで協力を得ている。また、Singtelとは、人材教育と資格認証などで提携している[301]。

シンガポール IDA(インフォコム開発庁)の傘下機関として 1997 年 10 月に創設された

---

297 https://www.csa.gov.sg/about-us/our-organisation

298 https://www.gov.sg/sgdi/ministries/mci/departments/csa

299 https://www.csa.gov.sg/news/press-releases/singapore-signs-memorandum-of-cooperation-on-cybersecurity-with-japan-at-the-sidelines-of-sicw-2017

300 https://www.csa.gov.sg/news/press-releases/csa-inks-partnerships-with-local-and-foreign-industry-players

301 https://www.rsis.edu.sg/wp-content/uploads/2016/12/PR170217_Cybersecurity-in-Singapore.pdf

SingCERT（シンガポールコンピュータ緊急時対応チーム）は CSA の創設と同時に CSAni 移管された。SingCERT はシンガポール国立大学（NUS）と連携しインターネット上のセキュリティ関連インシデントの検知・阻止等に関する活動を展開している[302]。

SingCERT（シンガポールコンピュータ緊急時対応チーム）は、官民双方から受けたインシデント報告に対応し、助言と提言を行う。膨大な数のインシデント報告があり、対応できる人材リソースにも限りがあることから、SingCERT は優先度合いと緊急性が最も高い次のインシデント報告に対応している[303]。

- 生命を危険にさらす脅威のある活動
- 次のインターネットインフラへの攻撃
- ルートネームサーバー
- ドメインネームサーバー
- 重要アーカイブサイト
- ネットワークアクセスポイント（NAP）
- インターネットサイトへの自動攻撃の拡散
- 新タイプの攻撃または新脆弱性、

インシデント情報のリリースに関して、SingCERT（シンガポールコンピュータ緊急時対応チーム）では、サイトオーナーの許可を得ないで情報開示することはしない方針である。侵入者活動が検知された場合、サイトオーナーは SingCERT に対して侵入者のインシデントへの関与をどの法執行当局と他の省庁に提供してほしいかを明確に述べる必要がある。また、SingCERT はターゲットとなる IP アドレス等の機微な情報を削除したうえで、当該省庁へインシデント報告を行うことになる。こうして、SingCERT が仲介して、サイトオーナーと関係当局との連絡を迅速に推し進めている。すべてのインシデントは SingCERT の担当職員が追跡し、モニタリングを行っている。

しかしながら、SingCERT（シンガポールコンピュータ緊急時対応チーム）は捜査当局でもなければ、法執行機関でもない。したがって、個々の侵入者を操作し、侵入者情報を保持または開示することなく、犯罪捜査を行うこともない。主たる任務は、コンピュータセキュリティインシデントに対応して迅速なコミュニケーションの促進とテクニカル支援を提供することである。

2016 年 10 月 10 日、Lee Hsien Loong（リー・シェンロン）首相はシンガポールの「サイ

[302] https://www.csa.gov.sg/singcert/about-us/faqs#A1
[303] https://www.csa.gov.sg/singcert/about-us/faqs#A1

バーセキュリティ戦略[304]」の概要を発表した、本戦略はサイバーセキュリティ分野におけるビジョン、目標、重点課題などを明らかにし、シンガポールのレジリエントで信頼性のあるサイバー環境構築へのコミットメントを示している。本戦略の 4 本柱は、次の通りである。

- シンガポールの重要情報院のレジリエンス強化
- サイバー脅威への防戦とサイバー犯罪との戦いおよび個人データの保護によるより安全なサイバースペースの創造
- 活気に満ちたサイバーセキュリティエコシステムの開発
- 国際協力の強化によるレジリエントなインフラの整備である。

2017 年 7 月、CSA（サイバーセキュリティ庁）が直近 2 ヵ年をかけて策定した「サイバーセキュリティ法案[305]」が公表され、パブリックヒアリングにかけられている。パブリックコンサルテーションは 2017 年 11 月 13 日に終了[306]し、本法案は 2018 年に議会の審議に付託されることになる[307]。

サイバーセキュリティ法案の主な狙いは、1)関係当局がサイバーセキュリティの脅威とインシデントに迅速に応戦し、これを阻止及び管理委すること、2)シンガポールの重要情報インフラ（CII）のオーナーを規制すること、3)サイバーセキュリティ情報の共有フレームワークを構築すること、4)サイバーセキュリティサービスプロバイダーを規制することなどの措置を講じることを可能にすることにある。加えて、本法案では、重要インフラセクター横断的な情報共有を促進する。重要な情報インフラは、水、保健医療、海事、メディア、インフォコム、エネルギー、アビエーション等の 11 セクターとされている。

Nanyang 大学による 2016 年 12 月の政策提言レポート[308]では、CSA（サイバーセキュリティ庁）は、政府内に情報共有会議を設置して情報共有の調整を主導すべきであると主張している。特に政府内部と省庁間、官民ならびに公的部門と対外パートナー国と間の情報共有を強化する必要性を強調している。

シンガポールでもサイバーセキュリティインシデント問題に対応するために、情報共有を促進する ISAC(情報共有分析センター)の設立が重要だとの認識が高まっている。2017 年

304 https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy
305 https://www.csa.gov.sg/~/media/csa/cybersecurity_bill/draft_cybersecurity_bill_2017.ashx?la=en
306 https://www.csa.gov.sg/news/press-releases/close-of-public-consultation
307 https://www.channelnewsasia.com/news/singapore/singapore-s-cybersecurity-bill-delayed-to-2018-9225622
308 https://www.rsis.edu.sg/wp-content/uploads/2016/12/PR170217_Cybersecurity-in-Singapore.pdf

11 月 14 日のニュースリリース[309]によると、シンガポールの金融サービス ISAC（FS-ISAC）と通貨当局はアジア太平洋の 9 ヵ国の情報共有を促進する目的で地域分析センター（FS-ISAC Asia Pacific Regional Analysis Centre）のオフィスをシンガポールに同年 11 月 14 日に設置してオペレーションを行うことを決めている。

2017 年 7 月、国連の ITU（国際通信連合）は、GCI（グローバルサイバーセキュリティインデックス）をリリースし、2014 年版の改善ポイントが大きいとしてシンガポールをトップにラインキングしている。CSA の創設（2015 年）や新サイバー戦略（2016 年）の実施等のシンガポール政府のサイバーセキュリティイニシアティブを高く評価している[310]。

4.2. サイバー空間に関わる国家組織

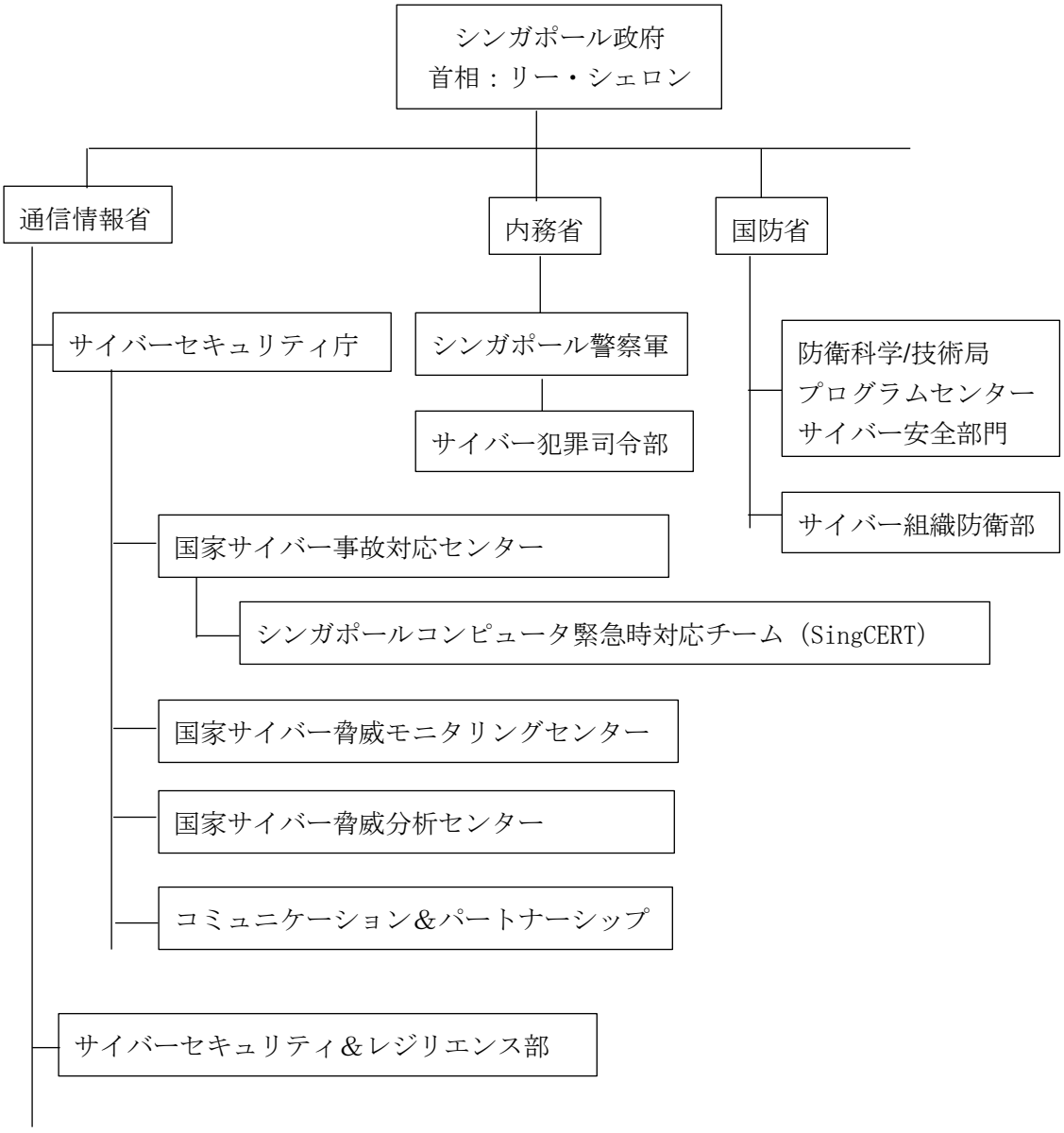
シンガポール政府のサイバー空間に関わる主要な組織は、下記の図の通りである。この図は主要組織のみを整理したもので、運輸省、内閣府などそれぞれの業務に必要なサイバーセキュリティ対策部門を設置しており、これらを合わせると全部で 37 ヵ所になる[311]。

309 http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/FS-ISAC-and-MAS-to-Strengthen-Cyber-Information-Sharing-Across-Nine-Countries.aspx

310 http://www.bakermckenzie.com/en/insight/publications/2017/07/singapore-ranks-first-in-un-survey/

311 https://www.gov.sg/sgdi/search-results?org=cyber&option=all

【主要なサイバー関連国家組織】



出所：各種資料に基づいて IBT にて作成

【サイバーセキュリティ庁（CSA】

は「1.4.2.1. サイバーセキュリティ庁（CSA)」に既述した通り、シンガポールのサイバーセキュリティ戦略とその作戦、教育、エコシステム開発などを担うのは、サイバーセキ

ュリティ庁（CSA：Cyber Security Authority[312]）である。政府エージェンシーの CSA は首相府傘下に置かれ、通信情報省（MCI）がマネジメントを行っている。主な任務は、国家サイバーセキュリティ機能の監督と官民連携による重要インフラ防護である。2015 年 4 月 1 日に創設され、様々な業界とステークホルダーと連携して、サイバーセキュリティ認知を高める努力を払っている。CSA のトップは、David KOH 長官（Chief Executive）である。副長官は、Ms. Christina LEE と NG Hoo Ming などである[313]。

【シンガポール警察軍[314]】

内務省傘下のシンガポール警察軍（Singapore Police Force）はサイバー犯罪とサイバーテロを取り締まっている。ソーシャルメディアユーザー、インターネットバンキングおよびモバイルデバイスをターゲットとして攻撃し、個人情報を盗んで犯罪に使うサイバー犯罪を取り締まる。また、犯罪組織がオンラインで求人広告を通じて一般市民を騙して、彼らの被害者に仕立て上げる犯罪を監視する[315] [316]。これらの監視・取り締まりを目的として、シンガポール警察サイバー犯罪司令部（SPCC: Singapore Police Cybercrime Command）を設置している。SPCC は 2017 年 11 月から官民連携プロジェクトを立ち上げた。この連携プロジェクトは、国際的な IT 企業、インターネット販売事業者、インターネットプロバイダー、金融関係の研究および送金機関など 40 のパートナーで構成されている。法規執行強化、民間企業へのサイバー犯罪撲滅への啓蒙、そして官民連携活動を促進する[317]。

【国防省関連のサイバーセキュリティ部門】

国防省の防衛科学/技術局（Defence Science and Technology Agency）傘下のプログラムセンター（Programme Centers）[318]にサイバーセキュリティ部門が設置されている。ここでは、国防省およびシンガポール武装軍（SAF）向けに、ダイバー攻撃の防護と検出、脅威のセンシング、事故対応および対応能力の査察などを行なっている。最近の成果として、作戦システムを標的としたマルウェアを検出する技術とプロトタイプのルートキットを開発した[319]。

---

312 https://www.csa.gov.sg/about-us/our-organisation
313 https://www.gov.sg/sgdi/ministries/mci/departments/csa
314 https://www.police.gov.sg/
315 https://www.police.gov.sg/resources/crimewatch/cyber-crimes
316 https://www.police.gov.sg/resources/crimewatch/cyber-terror
317 https://www.opengovasia.com/articles/7778-public-private-alliance-launched-by-singapore-police-cyber crime-command
318 https://www.gov.sg/sgdi/ministries/mindef/statutory-boards/dsta/departments/pc
319 https://www.dsta.gov.sg/programme-centres/cybersecurity

サイバー組織防衛部（Defence Cyber Organisation）は 2017 年 5 月に、国防大臣が設置を発表した組織で、シンガポール武装軍のネットワークをモニタリングと防衛するために 24 時間体制での監視を任務とする。設置発表の 1 週間前に、国防省のインターネットシステムがサイバー攻撃により、軍人 850 名の個人情報が流出した。この事件を受けてサイバーセキュリティ強化のため新しい組織を設置することになった。現在要員の募集と育成をしており、今後 10 年間で 2,600 名の専門スタッフを配置する計画である[320] [321]。

2018 年 2 月 12 日、国防省はサイバーNSF（National Service Full-Time）スキームを設置した。このスキームは、シンガポールの軍事ネットワーク防護能力を強化するため、NSF 要員の中から選抜して、シンガポール工科大学（SIT: Singapore Institute of Technology）の協力を得てサイバー専門家を養成するものである[322]。

4.3. サイバーセキュリティ対策の戦略・法規

2017 年 11 月 22 日、リー・シェンロン（Lee Hsien Loong）首相は「シンガポールのサイバーセキュリティ戦略（Singapore's Cybersecurity Strategy)」を発表した[323]。2016 年 10 月に概要が発表されていたものである。この戦略はサイバーセキュリティ分野におけるビジョン、目標、重点課題などを明らかにし、シンガポールのレジリエントで信頼性のあるサイバー環境構築へのコミットメントを示している[324]。

【シンガポールのサイバーセキュリティ戦略要点】[325] [326]

本戦略は下記の 4 本柱で構成されている。

- レジリエントなインフラストラクチャの構築
  - シンガポール政府は、民間セクターの運用者、サイバーセキュリティ企業等の主要

320 https://www.channelnewsasia.com/news/singapore/singapore-to-set-up-new-defence-cyber-organisation-8775266

321 http://litigationedge.asia/blog/technology/singapore-recruit-cyber-defense-center-national-service/

322 https://www.opengovasia.com/articles/singapore-mindef-launches-cyber-nsf-scheme-to-bolster-cyber-defence-capabilities

323 https://www.opengovasia.com/articles/7177-prime-minister-lee-launches-singapores-cybersecurity-strategy

324 https://www.opengovasia.com/articles/7177-prime-minister-lee-launches-singapores-cybersecurity-strategy

325 https://www.opengovasia.com/articles/7177-prime-minister-lee-launches-singapores-cybersecurity-strategy

326 https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf?la=en

な関係者と協働で、重要情報インフラ（CII：Critical Information Infrastructure）のレジリエントを強化して、国民への基本的なサービス提供を確実にする。

- 一例として、「インターネットサーフィング分離」イニシアティブを推進している。これは、政府機関職員がニュースサイトなどをサーフィングする時と、E メールなど業務を行う時で別々のネットワークとコンピュータを使用する政策である。業務用はイントラネットを使い、外部ネットワークと遮断する。2017 年末までに全ての省庁で実現する。これにより、政府の機能がサイバー攻撃により麻痺することを防護する。

- 安全なサイバー空間の創造
  - ビジネスと社会に活力を与えるためには安全で信頼できるサイバー空間が欠かせない。この戦略は各省庁のサイバー犯罪撲滅への挑戦を描く。例えば、内務省は 2016 年に「国家サイバー犯罪アクションプラン」を立ち上げたが政府機関だけでは十分な成果が上がらなかった。今後は、地域社会とビジネス界との協働を推進して、サイバーセキュリティへの認識向上とより良い事例の普及に努める。
- 活気に満ちたサイバーセキュリティエコシステムの開発
  - 政府は、産業界パートナーと高等教育機関と共同で、サイバーセキュリティ従事者を増加させる。「サイバーセキュリティ関係者と技術者プログラム（Cybersecurity Associates and Technologist Programme）」327などのイニシアティブを通じて、奨学金制度と産業界主導のカリキュラムが導入し、若者のスキルアップと中高年者の再教育の機会を提供する。
- 国際協力の強化
  - サイバー脅威は国境を越えて襲ってくる。これへの対応は国際協力が不可欠である。政府は、シンガポール国際サイバー週間（SICW: Singapore International Cyber Week）328、サイバーセキュリティに関するアセアン閣僚会議（ASEAN Ministerial Conference on Cybersecurity）などの場において、サイバーセキュリティに係る、規準、政策および法規の情報を交換して、シンガポールの強靭なサイバー空間構築に資する。

【サイバーセキュリティ法】

2017 年 7 月、CSA（サイバーセキュリティ庁）が直近 2 ヵ年をかけて策定した「サイバーセキュリティ法案[329]」が公表され、パブリックヒアリングにかけられた。サイバーセキュリティ法案の主な狙いは、1)関係当局がサイバーセキュリティの脅威とインシデントに迅速に応戦し、これを阻止及び管理委すること、2)シンガポールの重要情報インフラ（CII）の

[327] https://www.csa.gov.sg/programmes/csat
[328] https://www.sicw.sg/
[329] https://www.csa.gov.sg/~/media/csa/cybersecurity_bill/draft_cybersecurity_bill_2017.ashx?la=en

オーナーを規制すること、3)サイバーセキュリティ情報の共有フレームワークを構築すること、4)サイバーセキュリティサービスプロバイダーを規制することなどの措置を講じることを可能にすることにある。加えて、本法案では、重要インフラセクター横断的な情報共有を促進する。重要な情報インフラは、水、保健医療、海事、メディア、インフォコム、エネルギー、アビエーション等の 11 セクターとされている。パブリックヒアリングは当初 2017 年 8 月 3 日を期限としたが、意見が多く対応に時間がかかったので期限が 8 月 24 日まで延期された。CSA は意見を集約した結果を 2017 年 11 月 13 日に発表した[330]。意見を反映した最終的な法案が 2018 年 2 月 5 日に議会を通過して法律として成立した[331]。

成立したサイバーセキュリティ法 (Cybersecurity Act, No.2/2018) は全 50 章からなり、シンガポールのサイバー空間の安全保障に大きな役割を果たすと見られる。その要点は下記の通りである。

【サイバーセキュリティ法の要点】[332] [333]

- スコープ
  - 重要情報インフラ (CII) の所有者はしばしばベンダーと共に事業を行なうので、CII の境界を定める必要がある。CSA は各事業セクターの規制を管轄する省庁および CII 所有者と委員会を設置し、そこで審議して境界を設定する。CII 所有者は最終的に彼らの CII のサイバーセキュリティに責任を負う。
- 必須サービスと重要情報インフラ (CII) の決定
  - 必須サービス (Essential Service) の継続的な提供に必要なコンピュータとコンピュータシステムであり、それが失われ、あるいは機能低下した時に、シンガポールにおいて必須サービスが提供されなくなるものが CII である。
  - CSA は、各事業セクターの規制を管轄する省庁および CII 所有者と委員会を設置し、そこで審議して、各セクターにおける必須サービスと CII を決定し、CII 所有者へ書面をもって通知する。CII 所有者は、CII であるか否か自ら評価する必要はない。
  - CII 所有者は陳述をコミッショナーへ提出することが出来る。コミッショナーは CSA の主席管理職員が任命される。
- CII 所有者の報告義務

330 https://www.opengovasia.com/articles/mci-and-csa-to-refine-designation-of-critical-information-infrastructures-ciis-and-duties-of-cii-owners-in-singapores-proposed-cybersecurity-bill

331 https://www.opengovasia.com/articles/singapores-cybersecurity-bill-passed-into-law-minister-addresses-concerns

332 https://statutes.agc.gov.sg/Bills-Supp/2-2018/Published/20180108?DocDate=20180108

333 https://www.opengovasia.com/articles/singapores-cybersecurity-bill-passed-into-law-minister-addresses-concerns

- CII 所有者はサイバーセクリティ脅威と事故を検知するメカニズムと処理するプロセスを構築し、事故を速やかに CSA へ報告しなければならない。CII に接続していない施設のサイバー事故については報告する義務はない。CII 所有者は CSA の調査に協力しなければならない。調査に当たり、コミッショナーは問題となっているコンピュータシステムの保有者は犠牲者であることに配慮する。なお、CII 以外を含めたすべてのサイバー事故については、SingCERT へ自発的に報告する仕組みとなっている。

- コスト負担
  - 国家レベルでのサイバーセキュリティ防護強化と、サイバー脅威と事故への対応強化に係る費用は大部分を国が負担する。この費用は、国家レベルでのサイバーセキュリティインフラと要員、サイバーセキュリティ事故管理プロセスの認証のための定期的なサイバーセキュリティ訓練、そして、国家サイバー事故対応チーム（NCIRT: National Cyber Incident Response Teams）のサイバーセキュリティ事故への対応、のそれぞれに掛かる費用を含む。CII の所有者はすでに規則に準拠してなすべき対策に係る費用を負担している。これらの費用については可能な限り負担を低減する。
- CII 所有者への支援
  - CII 所有者とその従業員がこの法律実施準備を支援するため、CSA はセクター導入サイバーセキュリティ法開始プログラム（CLIPS: Cybersecurity Legislation Initialization Programme for Sector Leads）を開始した。CLIPS は、セクター規制当局と CII 所有者との間の役割と責任を明確にし、当該セクターに関わる如何なる運用上の課題も確認し、解決する。
- コミッショナーの権限へのセーフガード
  - 法によりコミッショナーへ付与されている幅広い調査権限は、個人のプライバシーへの干渉を制限している。サイバー事故の重大性の程度により、個人のプライバシー保護と法執行権限のバランスを考慮する。
- サイバーセキュリティ人材の養成
  - 産業界と協働でサイバーセキュリティ人材の育成を促進する。例えば、CSA は、サイバーセキュリティ関係者と技術者プログラム（CSAT: Cybersecurity Associates and Technologist Programme)、サイバーセキュリティ専門家スキーム（CSPA: Cyber Security Professional Scheme）を産業界と協働で推進する。
- 国際展開と規準
  - サイバーセキュリティ法案作成に当たっては、海外の類似法を参考にした。今後も、新しく出現するサイバー脅威に対応するため、国際的な協力関係を推進する。
- 公共教育と中小企業支援
  - 政府は、サイバーセキュリティ認識連盟（CAA: Cybersecurity Awareness Alliance)、CSA の GoSafeOnline、そして、毎年発行されるサイバー概覧報告書、などにより一

般市民へのサイバーセキュリティ啓蒙教育を行う。一方、中小企業に対しては、情報通信開発庁（IMDA: Info-communication Media Development Authority）が推進する中小企業デジタル化プログラムを通じて、サイバーセキュリティに関する技術と情報を提供する。

【コンピュータ不正利用とサイバーセキュリティ（改定）法】

サイバー空間を安全に信頼性高く利用するために、シンガポールでサイバーセキュリティ法と並んで重要な役割を果たすのが、サイバー犯罪を取り締る「コンピュータ不正利用とサイバーセキュリティ(改定)法(CMCA: Computer Misuse and Cybersecurity(Amendment) Act, No. 22 of 2017)」である。この法律は従来あった 2007 年版の法律を大幅に改定して、2017 年 5 月 11 日に公布、6 月 1 日施行されたものである。近年のサイバー犯罪の多様化・複雑化、すなわち、IoT への攻撃、多量の個人情報の流出が頻繁に発生、そして、盗まれた個人情報の搾取・詐欺への利用などへの対応が必要になった。CMCA の要点は下記の通りである。

【コンピュータ不正利用とサイバーセキュリティ（改定）法(CMCA)の要点】[334] [335] [336] [337]

改定前の 2007 年版では、コンピュータシステムへ権限なしで侵入し、そしてコンピュータシステムの変更、コンピュータサービスの利用を行うことを違法行為として規制し、これらについては未遂や 教唆も同様に犯罪としていた。2017 年の改定でさらに次の行為も違法とした。

- ハッキングされた個人情報での取引は違法行為である。
  - 犯人がハッキングされた個人情報と知っていた場合、あるいは知っていたと判断される正当な理由がある場合、この個人情報を使った取引は違法行為である。
- ハッキングツールによる犯罪を意図した取引は違法行為である。
  - 当初からコンピュータ犯罪を意図して作られた、またはこのような使い方が可能なツールによる取引は違法行為である。
- CMCA に基づく刑罰の統合を許容する。
  - 検察に対して、同一のコンピュータを使った、比較的軽微な懲役 12 ヶ月未満の複数の違法行為を統合して一つの違法行為として扱って刑罰を課することを認める。これにより、統合されて大きな違法行為となってより重い刑罰を課することが出来る。

[334] https://www.singaporecriminallawyer.com/cybercrimes-in-singapore/
[335] https://sso.agc.gov.sg/Acts-Supp/22-2017/Published/20170511?DocDate=20170511
[336] https://www.channelnewsasia.com/news/singapore/changes-to-singapore-s-cybercrime-law-passed-8712368
[337] http://www.allenandgledhill.com/pages/publications.aspx?list=LBulletinAreas&pub_id=1391&view=d

- シンガポールに重大な危害が及ぶ CMCA 違法行為に対する治外法権の適用。
  - 「シンガポールに重大な危害が及ぶ」とは、シンガポールにおいて、市民が病気、障害、あるいは死の危険に曝されること、必須サービスが途絶すること、政府が統治とサービスの機能を失うことである。このような場合、警察は海外のサイバー犯罪者に対して捜査を開始し、当該国の捜査当局と協力して犯罪の証拠を提供し情報を共有する。そして、犯人のシンガポールへの引き渡しを視野に、可能であればシンガポールの法廷で裁く。
- 刑罰の強化
  - 違法行為の種類と初犯/重犯の程度ごとに罰金刑と懲役刑の上限が設定されており、最高刑は 100,000 ドルの罰金または 20 年間の懲役刑、またはこれら両方の刑が課せられる。