はしがき

1　問題の所在 —— ポスト人工知能時代における安全保障上の脅威

安全保障とは，外部にある脅威から，自らの国，社会，企業，市民の安全を確保することである。このように捉えるとき，情報法は，その設計次第で，安全保障の基盤にもなるし，それを揺るがす道具にもなる。

今日のデジタル化社会において，情報の利活用は，量的な拡大と質的な深化を遂げている。2024年現在，我々は携帯端末やタブレットを持ち歩きながら移動をし，プラットフォーム事業者の提供する報道で情報を得，オンラインショップで買い物をし，ソーシャル・ネットワーキング・サービス（SNS）のアプリを通じて家族や友人とコミュニケーションを取る。我々がその日にどこに行き何をしたのか，何に興味関心を持ち，どのような嗜好を有し，誰と繋がっているのかは，データとなって端末やサーバに蓄積されている。そして，その日のニュースからお勧めの店舗や商品まで，我々にどのような情報を提供するべきかは，それらのデータを基にして，事業者が用いるアルゴリズムが決める。

人工知能（AI）や分散台帳技術，量子情報通信を含めたデジタル技術の深化と広がりは，一方では，国や社会の境界を低くする作用を持ち，グローバルな情報流通を促進する。しかし，他方で，それは当事者が意図していない情報の利用や，これまで表面化することがなかった情報の流出や拡散を許すリスクを孕む。

まず，これまでにも存在していた情報漏洩のリスクは，デジタル化によってその度合いを増している。サイバーインシデントが引き起こす損失額は数十兆ドルに上りうる。また，テロ組織や組織犯罪集団が，ダークウェブなど情報を隠匿する技術を使って禁制品の売買等の違法行為を行っていることも，市民の安全を脅かす。

加えて，ポスト AI 時代においては，脅威をもたらす外部の脅威の存在は分散し，可視化されづらくなっている。敵は，陸，海，空，宇宙，サイバーに次ぐ，第 6 の安全保障領域であるところの人間の「脳」に直接働きかけるからである。例えば，デジタルメディアの普及により，フェイクニュースの拡大や，

SNS を通じた世論の操作など，情報を武器として用いる新しい形態の情報戦が既になされている。これはプラットフォーム事業をはじめとした，利用者の属性に沿って情報を選択的に提供できる仕組みを通じて，利用者の認知領域に働きかけることで実施される。広告によって収益を得る事業者には，その利用者が見たい情報や，関心を惹く情報を提供する商業上の動機がある。そのため利用者が心地よく感じる情報が優先的に表示され，そうではない情報は排除されてしまう。民主主義的な意思決定過程に介入しようとする者が，これを利用して，選挙報道を歪めたり，特定の集団を排除したり貶めたりするような情報を流したりすることが喫緊の課題になっている。

2　本書の課題 —— 情報法における安全保障上の脅威への対応

デジタル技術の進化と拡大は利点も大きい。これらの技術を用いて，個人情報を含めたデータの適正かつ効果的な活用をすること，それによって新しい産業を創出し，活力のある経済社会と豊かな国民生活の実現をすること，それとともに個人の権利利益を保護することが望ましいことに異論はないだろう。さらには我々の社会を基礎付ける立憲主義原理に則って，社会のデジタル化を進めていく必要性も，議論の起点としてよい。

しかし，安全保障上の脅威の存在形態が情報のデジタル化によって質的に変わるとき，国，事業者，市民との関係もまた構造的に変容している。このような状況は，国内的側面とトランスナショナルな側面の双方において生じている。

⑴　国内的側面

国によって上記の脅威への対応のあり方は異なるが，多かれ少なかれ，上記の流れは，従来の国と事業者やデジタルサービスの利用者との関係を構造的に変容させている。このことは次の３つの関係軸において把握することができる。

第１に，政府と市民との関係である。国は保安のために様々な情報を収集するが，その侵襲の度合いは，情報技術の発展に伴い量的にも質的にも高くなっている。データ駆動型の捜査手法を利用すること，安価になった全地球測位システム（GPS）を容疑者の車に付着させてその行動を監視すること，通信事業者に利用者の位置情報を提出させること，顔認証技術を利用して特定の場所を通行する者全てを監視することなどは，一方ではテロや組織犯罪の抑止になる

ものの，他方では市民の自由との緊張関係をもたらす。

確かに，従来の情報法領域においても，国家が犯罪の予防や捜査のために，通信を含む表現活動や，金融の利用状況等の監視を強化することが，安全と自由を制約することは課題として認識されてきた。政府からの恣意的な制御を許さないようにすることは，法の役割である。日本では基本権や民主主義といった社会の根幹的な価値を守るために憲法があり，それを踏まえて当局や事業者に対する適切な規律を行うために刑事訴訟法をはじめとした各法が整備されている。しかし，それらの法規則だけで立憲的価値を守ることができるかは慎重な検討が必要である。

また，行政側に蓄積された情報が適切に管理されなかったり，AI の活用によって個人の能力やリスクの評価，あるいはプロファイリングがなされたりする場合，利用者がコントロールできないところでその自律性が制約され得る。これらの技術活用が憲法の定める統治機構に不当な影響を及ぼさないための仕組みや，個人の基本権を侵害しないための措置が必要になる。

第 2 に，政府と事業者との関係である。民間事業者が保有する情報へのガバメントアクセスは，上記のデータの蓄積が通信事業者をはじめとした民間企業においてなされている限り，主要な情報収集手段となる。もっとも，捜査や監視の対象となる通信事業者等は，同時に，表現の自由の媒介者であり，国家経済の担い手でもある。事業者が多面的な役割を担うことから，政府と事業者による情報取得，利活用をどのように規律するかという課題が生じる。

事業者を介さずに利用者間（P2P）で行われる暗号通信や分散型取引が普及すると，事業者を情報の集積拠点として利用してきた従来の捜査，監視体制を組み直す必要が生じる。事業者を介してそのような通信取引を行っている場合，国が事業者に対してバックドアの設置を命じることができるかも，重要な論点である。

第 3 に，事業者と利用者である市民との関係である。確かに，事業者は個人情報保護法をはじめとした法律を遵守することで，利用者の権益を守る義務を負うことになる。しかし，それらの法律を施行すれば守るべき基本的な価値を擁護できるのかが常に問われなければならない。例えば，冒頭に述べたように様々なサービスの利用を通じて利用者の認知が歪められるにしても，事業者の

情報の利活用に対して利用者が同意していることをどのように評価すればよいかという問題がある。どのような利活用がなされるのか分かりやすい説明がされていないとしたら，あるいは事業者の提供する情報通信技術抜きで生活できないとしたら，もはや同意は形骸化しているためである。また，利用者は事業者に提供した自己に関する情報についてどこまでコントロールできるか，情報に対する権利を人権として認めるべきかも論争を呼んでいる。

⑵ トランスナショナルな側面

（i） 情報法の調和化不可能性と国際協力の必要性

事業者は，経済的な動機からクロスボーダーで活動する。そこで，政府が自国管轄に服しながら外国で活動する事業者のデータにアクセスしたり，事業者が移転するデータに移転先の現地国がアクセスしたりする契機が増加している。

経済領域では通商や投資を円滑に行うために，国内法の仕組みをある程度調和化（harmonize）しておき，相互運用性を確保する。しかし，情報法は各国の価値，歴史，経済状況，社会構造を織り込んで策定されるもので，そのあり方は国によって異なる。そのため，そのようなすり合わせが本質的にできないところがある。

同時に，主要国の情報法政策が地球規模でのインパクトを持つのも，情報法の特徴である。図式的に言えば，大手IT企業の本拠地である米国は，連邦レベルでの個人情報保護法を設けることなく，情報の自由な流通を促進しようとする。他方で，欧州連合（EU）は，厳格な情報法制の域外適用によってその影響力を広げている（ブリュッセル効果）。これに対して，中国は，国民への監視体制を強めると共に一帯一路政策を通じて東南アジア，南米，アフリカに自らの通信システムを広める（北京効果）。このように，主要国・地域のアプローチは明確に異なっている。それらの管轄に服する事業者は，相反する対応をしなければならないことがある。

また，権威主義が台頭することを背景にして，民主主義を基調とする国が共通の規範を形成しようとする動きも顕著である。2022年12月には，経済協力開発機構（OECD）が民間企業の保有する対話アプリの履歴や個人情報などについて，政府が収集等を行うための原則（*Declaration on Government Access to Per-*

sonal Data Held by Private Sector Entities, OECD/LEGAL/0487）を採択した。それ自体に法的拘束力はないが，それが各国法で実現されていくことが期待される。もっとも，これらは有志国との間で形成されている規範であり，権威主義国との溝を埋めるものにはならない。

情報の越境移転や交換について国際協力が見込めない状況は，情報の自由な流通と，安全保障との緊張関係を生み出す。そのことが，翻って各国の情報法と個人の権利保障にどのような帰結をもたらすのかも問われなければならない。すなわち，いずれの国で活動するのが安全と言えるか，その判断基準を利用者や利用者の所在国が設定することが必要になる。そして，データを保有する事業者が法執行国の法に対して有する信頼，利用者が事業者のデータ取扱に対して有する信頼をどのように確保するかが課題となる。

(ii)　通信インフラの保護

情報と安全保障を語るときに欠かすことができないのは通信インフラの構築と保護である。金融取引も含めて，通信は海底ケーブルと人工衛星通信網を通じてなされる。国がインフラの維持について自律的なコントロールを持てるかは，安全保障上，死活的に重要である。国際法では，いずれの国にも属さない国際領域での通信は，全ての国に開かれており，他国はそれを不当に阻害してはならないという，公海，あるいは宇宙空間における利用の自由が原則となってきた。しかし，2010年代後半以降，米中対立を背景にして，通信インフラの地政学的な意義が見直されている。また海底ケーブルが故意に破壊される例や，人工衛星や地上局がサイバー攻撃の対象となる例が増加している。これにどのように対応し，自国と外部を繋ぐインフラを維持，保護しなくてはならないか，検討が必要となる。

情報法における安全保障上の脅威への対応はどのようになされるべきだろうか。法的基盤となる価値，原理を実現するべく，ここまでで素描した理念と実態とのギャップを克服するためには何が必要だろうか。これらが本書を貫く問いである。

3　本書の構成

情報法における安全保障に関する問題は幅広い領域にまたがる。そこで，本

書では狭い意味での情報法に止まらない，憲法，刑法，国際法，安全保障法の理論と実務に精通した専門家に，以下の問題について，それぞれの専門領域の視点から論文を寄稿していただいた。

本書は3部9章から成る。第Ⅰ部では，情報取得，利活用，保持のあり方として守るべき価値は何かを論じる。第1章の横大道聡論文は，安全保障が構造的に変容していることを踏まえて，本来，安全保障を脅かすための道具ではないはずの外国企業のSNSプラットフォームの利活用が，安全保障上の問題として議論されている要因を明らかにする。具体的には，米国における外国企業のSNSプラットフォームに対する規制に焦点を当てた実証研究を展開する。その際，2016年から2020年にかけて，トランプ政権下において講じられた，安全保障上の懸念から試みられた中国企業のSNSプラットフォームに対する規制と，2021年以降，バイデン政権下において実施されている規制の展開を追う。そして，中国のSNSプラットフォーム事業者に対して米国が有する警戒感の源泉としての中国法制度を踏まえ，日本法への示唆を加える。

第2章の山田哲史論文も，プラットフォーム事業者を中心とする私企業のもとに情報が収集，蓄積されていることに着目する。国家は，安全保障や犯罪予防，犯罪捜査などの目的で，国境を越えて事業を展開する事業者の顧客として，情報を取得する。国家による監視のために，デジタル技術が用いられることに伴い，憲法的価値に関わる脅威が生じる。本論文では，具体的には，特定の日時に特定の場所にいた利用者の情報を取得するジオフェンス令状を具体的題材として，法的規律の枠組みが直面している問題を明らかにする。

第3章の中崎隆論文は，犯罪対策は国家安全保障において重要な位置を占めていること，しかし日本では十分な体制がとられているとは言えないことを指摘し，効果的な犯罪対策体制のために，人権保護とのバランスを図りながらも，的確な情報収集・共有を行える体制を構築することが必要であるという。同論文は，刑事捜査を主にして安全保障に関わる情報収集と共有に関する，国家間や主要国における仕組みを俯瞰する。その上で，日本による対応とその不十分な点，改善の余地のある点を挙げる。

第Ⅱ部では，国境を越える情報を，国際法と各国法がどのように規律しているのかを検証している。第4章の藤井康次郎＝根本拓＝福島惇央論文では，越

境データ移転規制についてその透明性をいかに高めるか，またそのためにどのような制度が構築されるべきかを論じる。このことが，ビジネスへの障害の緩和や越境データ移転規制に関する国際的な規律に関する議論の進展等の観点からも，有益であるためである。越境データ移転規制が，安全保障を理由とする場合には通商協定において一定の規律が及ぶ余地はある。しかし，透明性の向上を図ることにより，過度な規制を牽制することができる。このような問題意識に基づき，同論文は，国際通商制度における透明性とアカウンタビリティを高めるための仕組みについての整理と分析を行う。

第５章の石井由梨佳論文は，事業者らが主に経済的な理由から個人データを越境移転することを，経済安全保障の観点からどのように規律するべきかを検討する。個人情報保護法では越境移転をする際には，相手国が安全であることを求める。しかし，各国は事業者の情報移転に関してどのような基準で安全を判断するのか，関連する国内法形成の動向や，国際法規範の形成も踏まえながら論じる。

第６章の那須仁＝石井由梨佳論文は，国，国に準ずる団体，テロ組織などが，情報を利用して敵対者を凌駕することを目的にした作戦行動である情報戦の法的規律のあり方を論じる。現状では情報戦に関して国際法の各国への義務付けは具体的なレベルでは行われておらず，各国の法整備が先行している。表現の自由や利用者の基本権，事業者の営業の自由と情報戦の脅威から個人，社会，国家の安全を守る要請をどのように調整するかという課題は，各国に共通する問題である。そこで同論文では，情報戦に対する法整備の現状を踏まえ，情報戦対策としての法の役割がいかにあるべきかを示す。まず，偽情報規制法と国家秘密保護法を中心に国内法整備の現状と課題を考察する。次いで，情報戦が平時と武力紛争時においてどの程度国際法の下で規制されているのかを明らかにする。最後に，情報規制が引き起こす表現の自由との軋轢を国家安全保障の観点から検討する。

第７章の西貝吉晃論文は，アクティブ・サイバー・ディフェンス（能動的サイバー防御，ACD）と日本の刑法との間の関係を掘り下げる。具体的には，ACD のうち刑法上の犯罪を構成する行為を抽出した上で法的に評価する。すなわち，ACD を適法に行うための日本の刑罰規定の犯罪構成要件の限定解釈の可能性

や現行の違法性阻却事由の適用論も議論しつつ，立法論の見地からの検討を行う。さらに，ACD を目的とする行為を一定の範囲で適法だとすべきだとした場合に，そうした活動の権限をどの機関に与えるべきかについても考察する。

第Ⅲ部では，海底ケーブルと人工衛星という国際通信インフラの保護を，主に国際法の観点から論じている。第 8 章の武井良修論文は，安全保障上の懸念を踏まえて，海底ケーブルをめぐる法的な問題についての分析を行う。まず，海底ケーブルに関する法制度について，国際法の観点を中心に概観し，その特徴を分析する。次いで海底ケーブルの保護に関する法的問題について脅威類型ごとに検討し，政策上の課題を明らかにする。そして，最近の海底ケーブル事業に係る動向を読み解き，これらの動きが現行の国際法制度にどのような影響を与えうるのかについて検討し，今後の法制度の方向性について見解を示す。

第 9 章の高屋友里論文は，衛星通信に対する有害な混信に着目し，それが国際電気通信連合（ITU）においてどのように規律されているのかを検討する。現状では，宇宙安全保障の概念や定義は確立していない。例えば，衛星通信に対する有害な混信を引き起こすサイバー行動が，宇宙活動に対する脅威であるという認識は，関係国や国際諸機関において十分に共有されていない。本論文は，既存の ITU 法制度における「有害な混信」の禁止規範と履行制度やサイバー脅威低減への法的試みを踏まえて，宇宙空間の脅威を低減するために透明性・信頼醸成措置に対して，ITU の履行制度が寄与するという指摘を行う。ITU が提示する TCBM は，衛星通信に対する有害な混信の「可視化」を促進するものであり，それはサイバー脅威低減につながるためである。

本講座の企画は，山本龍彦先生監修の下で進められた。また，法律文化社の梶原有美子氏，梶谷修氏，徳田真紀氏は，企画，編集，校閲に至るまで，地道で丁寧な支援をしてくださった。

本書が今後の法学領域における安全保障問題の研究や，学際的研究の発展に寄与することを，そして，日本における情報法関連の各種施策において有益な参照先となることを願う。

2024年 7 月

編者　石 井 由 梨 佳