研究技術情報のセキュリティ管理：

両用技術を念頭に

林　紘一郎*

概 要

軍事研究の是非については賛否があって当然であるし,現に両論が戦わされている. しかし,両陣営とも軍事研究の内包と外延が明確であることを自明のこととしているが,その線引きはそれほど簡単ではない. 現代技術には軍民両用技術が多数含まれているだけでなく,純粋市販品と目されるものでも軍用転換があり得るからである. しかもライバルには,研究の初期段階から,あらゆる手段を使って情報を入手しようとする動機が存在する以上,そのセキュリティ管理は軍事研究か,防衛装備品と同等の配慮を必要とする. つまり,軍事研究を否とする議論においても,「研究技術情報のセキュリティ管理」という側面では,軍事研究や防衛装備品における管理方式を知った上で議論する必要がある. もっともセキュリティに 100% はあり得ないから,どこかで線引きする必要があり,「新しい冷戦」の時代には,各国ともその課題に悩まされている. 本稿は,このような視点から軍事研究の賛否にかかわらず,議論の前提になる「セキュリティ管理」に関する知識を共有することを目的とする.

1. 問題の捉え方

2020 年 10 月発足直後の菅内閣が,日本学術会議会員として推薦された候補者のうち 6 名の任命を拒否した問題は[1],その約 3 年半前に,軍事研究に関して学術会議が従来から維持してきた反対の立場を再確認したこと(「軍事的安全保障研究に関する声明」2017 年 3 月 24 日,日本学術会議[2])との関連性を含めて,議論を呼んでいる. これは広くかつ冷静に議論されるべきテーマであり(林 [2016]),現に賛否両論が戦わされている.

しかしセキュリティ管理の観点から見た場合,軍事研究に対する賛否とは別に,研究対象

* 情報セキュリティ大学院大学 名誉教授

1 http://www.scj.go.jp/ja/info/kohyo/pdf/kohyo-25-s182-1.pdf

2 http://www.scj.go.jp/ja/info/kohyo/pdf/kohyo-23-s243.pdf

が両用技術である場合には「軍事目的に転用され得る技術」として,純粋な民生技術以上の注意を要することに変わりない．つまり,明らかに民生利用しかできない技術を別にすれば,研究技術情報の管理には,軍事研究や防衛装備品の調達に準じたレベルが求められるが,こうした考察は極めて乏しいように思われる[3].

本稿は,このような問題意識に立って,わが国における「軍事研究の是非」や「両用技術研究のあり方」そのものではなく,それらを支える「研究技術情報」の管理,とりわけセキュリティ管理のあり方について,いかなる配慮が必要かを論ずるものである.

ここで「研究技術情報」という語は,「研究開発に必要とされる科学技術情報」といった一般的な意味で用いている.不正競争防止法 2 条 6 項における「営業秘密」(「秘密として管理されている生産方法,販売方法,その他の事業活動に有用な技術上又は営業上の情報であって,公然と知られていないもの」)のうち,「技術上の情報」に近いが、その保有主体は企業に限らず広く研究機関(や,場合によっては個々の研究者)を網羅するものと考えていただきたい[4]．なお両用技術を念頭においているため,研究の初期段階からのセキュリティ管理を強調すべく,「研究」の語を追加している.

「研究技術情報」は,上記の定義に該当するので法的に十分保護されていると思われるかもしれないが,次のような事情を知れば,その担保が不十分であることが納得できよう.

a) 「秘密として管理されている」(秘密管理性)が最初の要件であるから,情報の保有者は,まず自分で情報を管理する仕組み(その適正レベルを含む)を考え,その手順を守らねばならない．いわば「自助努力優先」の立て付けである.
b) 「公然と知られていない」こと(非公知性)も要件なので,研究者自身による学会発表など(積極的公表)があれば保護されないし,犯罪行為や過失によって漏えいし,または開示された場合も,その後は保護を失う.
c) 違反行為に対する刑事罰の長期は 10 年の懲役刑とかなり重いが,一般的に「情報」が窃盗の対象になるかについては,否定的に解するしかないので(林［2017a]),一般法による罰則付きの救済は期待できず,不正競争防止法に頼るしかない.
d) その不正競争防止法は,「事業者間の公正な競争及びこれに関する国際約束の的確な実施を確保する」(同法 1 条)ための法制度であり,「研究技術情報」に法的保護を与えること自体を目的とするものではない.

なお,「研究技術情報」には幅広い分野が含まれるので,厳密な議論のためには更に対象を限定するのが望ましいかもしれない．現に筆者が多くの教訓を得た永野［2021］は,量子情報科学に焦点を絞っている．しかし本稿は,読者としてセキュリティの専門家を想定し,見落とされがちな研究技術情報への注意喚起を目的としている.そこで,ある程度の広がりを持った分析が適していると考え,対象を限定していないことをご理解いただきたい.

---

[3] わが国政府も「研究活動の国際化・オープン化に伴う新たなリスクに対する研究インテグリティの確保に係る対応方針について」(2021 年 4 月 27 日統合イノベーション戦略推進会議決定)において,研究の健全性・公正性(研究インテグリティ)の確保策を定めたが,現時点では研究資金の配分に関する施策が中心で,本稿のような問題意識は共有されていない. https://www8.cao.go.jp/cstp/kokusaiteki/integrity.html 参照.

[4] 2018 年に改正された産業競争力強化法に「技術等情報漏えい防止措置」という概念がある(2 条 18 項)が,これは漏えい防止の認証制度を導入するための基礎概念に過ぎない.

2. 秘密保護法制の必要性

情報は,不確定性（時と場所と態様により価値が変わり有体物に匹敵するほどの品質保証ができない[5]),非移転・拡散容易性（原本は移転しないままコピーが容易に出回る),流通の不可逆性（一旦流出したら取り戻すことができない）という 3 つの特質があるので,有体物（物あるいは財貨）を中心にした現在の法体系での対応には限界があり,法的な保護を与えるには何らかの工夫をする必要がある（林 [2017b]）.

上記 3 つの特性を持つ情報は,秘密としての保護に向いていないともいえるが,複雑な社会関係を律するには,「時間と対象を限定して秘匿する」ことを認めなければ,支障が生ずることもある[6].そこで先進民主主義国では，極めて限定的な範疇の情報に関して「秘密」としての保護を与えると同時に，その手続きをなるべく客観化して漏えいに伴う人権侵害等の危険を最小化している．しかし,わが国ではそのような理解と考察が極めて乏しい.その理由は,おそらく次の 3 点の事情に由来すると思われる.

① 第 2 次大戦後,国連の理想主義と歩調を合わせた平和国家を目指す中で,戦前の軍国主義を思い出させる「秘密」の保護法制を,真正面から議論することが憚られた[7].

② 情報法という法分野は,情報通信技術の発展の後追いで展開されざるを得ず,「法的保護の客体としての情報」に関する分析が不十分であった．その結果、「情報を公開して保護する」制度である知的財産制度は広く研究されているが,「情報を秘匿して守る」制度である秘密保護法制は,特定秘密保護法の制定によって,はじめて本格的に議論の対象になったというほど未発達であり,研究も初期段階にある[8].

③ 上記の ① とも連動して,個人情報保護法（あるいはプライバシー保護法一般）は秘密保護法の一種であるとの理解ができず,これを人格権的な視点から分析する論者が多く,「コンピュータ処理を前提にしたデータ保護法という形で,情報の保護と利用のバランスを図る」という本来の目的に関する理解が行き渡っていない[9].

これらの諸点を克服するためには,次の 2 点を認識の出発点とすることが,おそらく不可避と思われる.

A. 「情報を秘匿して守る」制度である秘密保護法制には,情報の保有主体により 1) 国家の秘密を守る特定秘密保護法（と国家公務員法），2) 企業の秘密を守る営業秘密制度（法律としては不正競争防止法），3) 個人のプライバシーを守る制度（個人情報保護法はその 1 例だが,より一般的なデータ保護法が望ましい）の 3 種がすべて含まれる[10].

---

[5] 筆者は,情報セキュリティには,取引する情報の「品質の信頼性（integrity）」も含まれると考えてきた（林 [2017a] 第 3 章）が,品質表示に関する偽装が頻発した後,フェイク・ニューズという「情報そのものの真偽が疑われる」事態が出現したので,その認識が正しいことが証明されたという思いが強い.

[6] 個人の秘密であるプライバシーがその例の 1 つだが,法人にも国家にも同じことが言える．例えば外交交渉を「すべての情報は直ちに公開する」という前提で行うことは,おそらく不可能であろう.

[7] 交戦状態・緊急事態を想定した議論や,インテリジェンスに関する議論が回避されるのは,このような風潮と通ずる面がある.

[8]「情報を公開して保護する」特許と「情報を秘匿して保護する」営業秘密の差は,ビジネス分野では多くの人に常識として理解されている.

[9] 営業秘密は,研究者の多くが知財学者であるためか知的財産の一種と捉えられているが,保護方式は「秘密保護型」であり「知財型」とは対照的である．これは筆者が初めて指摘した点であり（林 [2017a] pp.88-91）、最先端の研究者の支持を得ている（例えば福岡・松村 [2019]）が,幅広い理解は得られていない．同じように,プライバシー保護法とデータ保護法の差も理解が不十分であり,前者の研究を中心とする結果,保護に傾き易く利活用の面が軽視されている（林 [2017a] pp.106-110 など）.

[10] 先に述べた営業秘密の 3 要件（秘密管理性・非公知性・有用性）は,これら三種の秘密にほぼ共通しているが,微妙な差がある．例えば「特定秘密」においては，①定義該当性（法の別表に指定されている情報に限る），②非公知性，③安全保障上の秘匿の必要性，と読み替えられる.

B. 情報管理は[11],最も機微な情報を扱い,安全保障に最も近い軍事やインテリジェンス部門で発展してきた. そこで見出された「情報の格付け（classification）と利用者の適性評価（security clearance）の組み合わせで対応するべきだ」「手続きの正当性を担保するために認証と監査を担当する独立機関が必要である」という原則が,西欧先進諸国において非軍事利用も含めた管理方式の常識となっている[12].

3. 秘密情報の指定、アクセス権の付与、認証・監査に関する一般原則

既述のとおり,秘密の法的保護については制定法に頼り切ることができない中で,「企業にとって営業秘密は大事な資産である」という実務の必要性から多くの工夫がなされ,それが「ソフトロー」として機能している[13]. つまり上記の B に従って制定される標準的な情報管理の仕組みは,A における 3 種の情報の区分のうち「国家の秘密」に関して最も厳格に規定されるが、民間部門の営業秘密にも適用され,おおむね以下のような形を取っている[14].

Ⅰ。秘密情報の指定と格付け

まず秘匿したい情報を特定し,その程度に応じて格付けする。機密（top secret）・極秘（secret）・秘（confidential）とする英米方式が一般的で,これらを総称して秘密指定情報（classified information）という. この範疇に入らないものが,非指定情報（unclassified information）である[15]. 秘密指定情報は,その趣旨が明確に分かるよう,定められた位置に定められた表記で,その旨が（例えば Top Secret と）明記される.

Ⅱ。アクセス権の付与

情報の利用者ごとにアクセス権を付与する. 秘密指定情報を扱う個人は,必ず適性評価（security clearance）に合格しなければならない[16]. 評価は上記 3 種の機微レベルによって

---

11 管理の対象が機微情報である場合は,「保秘」や「情報保全」の語を使う場合がある.

12 もっともインテリジェンスに限っては,情報の存在と情報源を明かせば,その後の活動に支障が生ずるため「最も有効な情報が秘匿されたまま」という状況が生じがちである（Lowenthal [2009] 邦訳 pp.93-94）.

13 ソフトローとは「法的な強制力がないにもかかわらず,現実の経済社会において国や企業が何らかの拘束感をもって従っている規範」（有斐閣『ソフトロー研究叢書』における定義）を指す. 法的効力はハードローより弱いが,裁判等において「セキュリティに関する注意義務」を判断する尺度になり得る.

14 非軍事分野における最も分かりやすい例は,経産省 [2016] である.

15 もっとも,この二分法を徹底すればグレイゾーンはあり得なくなるが,実際の運用に支障を生ずることから,最も厳格に運用してきた米国でも,中間的存在として SBU（Sensitive But Unclassified）や FOUO（For Official Use Only）などの識別法が便宜的に使われ,その数は 100 種類以上に及んだとされる. 9.11 のテロに際し,インテリジェンス機関などで情報が共有されていなかった点への改善策として,オバマ大統領が見直しを指示し,全体を新しい CUI（Controlled Unclassified Information）という概念で統合・再構築したが,実効性の証明は,なお今後を待たねばなるまい（林 [2017c]）.

16 わが国では,難産した特定秘密保護法において初めて導入されたが,その対象は国家公務員と適合事業者（物件の製造又は役務の提供を業とする者で,特定秘密の保護のために必要な施設設備を設置していることその他政令で定める基準に適合するもの. 同法 5 条 4 項）の従業者に限られ,一般企業の従業者は対象外である. そこで官民を問わず研究者向けの適性評価の仕組みを導入すべきとする動きがある（自民党政務調査会 [2020]）. もっとも適性認定率について定説はなく,少なすぎれば運用上支障が生じ, 多すぎれば情報漏えいのリスクが高まる. 米国では、2019 年 10 月 1 日現在で 424 万人強の国民が認定を受け,人口（2019 年で 3 億 3 千万人）比で約 1.5%になる. これに対してわが国では,2019 年末で 134,702 人（人口比約 0.1%）である（永野 [2021]）.

濃淡があるが,「この人物は秘密指定情報を,他者に漏らしたり開示したりする危険はないか」を判断するものである．わが国の場合,特定秘密に該当すれば,特定秘密保護法の第5章（12条～17条）と「特定秘密の指定及びその解除並びに適正評価の実施に関し統一的な運用を図るための基準」（2014年10月14日閣議決定．2019年12月10日一部変更）に,具体的な手順が示されている．そのうち調査事項だけをあげれば，① 特定有害活動及びテロリズムとの関係に関する事項[17]，② 犯罪及び懲戒の経歴に関する事項，③ 情報の取扱いに係る非違の経歴に関する事項，④ 薬物の濫用及び影響に関する事項，⑤ 精神疾患に関する事項，⑥ 飲酒についての節度に関する事項，⑦ 信用状態その他の経済的な状況に関する事項,である[18]．

なお適正評価はアクセス権付与の前提条件であると同時に,情報共有の前提条件でもある点に留意したい．同等以上の適性評価を有する者の間でしか情報共有が認められないからであり,その効果は一種の「秘密クラブの会員資格」に準じたものになる（日米間など,国境を越えた情報共有を想起されたい）．

Ⅲ。物理的・技術的クリアランス

上記ではクリアランスを人的な「適正評価」と同義としたが,物理的あるいは技術的クリアランスの重要性も高まっている．例えば放射線を扱う場所ではその濃度が基準値以下であることが必要になるし,感染症の病原体を扱う場合には，その強度に応じた基準が設けられている．ICT機器については，バックドアやマルウェアが仕掛けられていないことがクリアランスになるが，この要件は安全保障上の懸念と結びつき，重要度が再認識されている[19]．またわが国の法制度の問題として,特定秘密保護法の適用対象ではない大学等に秘密の保持を求める必要がある場合には,その施設管理者との契約で規定せざるを得ないという事情（この場合,物理的クリアランスと適正評価が一体となるであろう）もある．

Ⅳ。Need-to-Knowの原則

上記ⅠとⅡによるマトリクスを作り,誰がどの情報にアクセスできるかを決定すれば,「○○組織における研究技術情報管理マニュアル」の骨子ができあがる．企業でのセキュリティ管理は,マニュアルを忠実に実行することで十分であるが,安全保障に関連する組織での運用では,業務上の必要が生ずる都度「その必要性に応ずるため誰それにある情報へのアクセスを許可する」という形で,アクセス権を個別具体的に決定する（Need-to-Knowの原則）必要がある．つまり適性評価に合格することが「ある分類の情報へのアクセスが常に許可される」ことを意味しない[20]．

Ⅴ。秘密管理と守秘義務

---

17 英米の仕組みでは家族に関する広汎な調査も含まれるが,わが国の場合には ① に関する調査についてのみ,「家族（配偶者・父母・子・兄弟姉妹・配偶者の父母及び子）」及び同居人について,氏名・生年月日・国籍・住所が調査対象となるにとどまる．

18 特定秘密保護法は「特定秘密」という一種類の情報だけを保護対象としているのに対して,米国の制度は本文の通り機密・極秘・秘の三種類を対象にしているので,評価項目が異なる（永野 [2021]）．米国の例を参照されたい方は、https://www.dcsa.mil/is/eqip/ で質問事項を知ることができる．

19 本文では秘密情報は機密・極秘・秘に3分類されると述べたが.実は別の分類としてSCI (Sensitive Compartmented Information) という概念があり、特定の「区画」に保管されていた．つまり人的な適正評価と物理的・技術的クリアランスが一体となっていたわけである（永野 [2021]）が,データベース化とNeed-to-Shareの動きとともにどう変化するかは見通せない．

20 注15.と同様9.11への反省からNeed-to-Knowとともに,Need-to-Shareにも配慮すべきだという議論が生じたが,両者のバランスをどう取るかはインテリジェンスにとって永遠の課題であろう．

秘密指定情報は手続を定め,適切に管理しなければならない．秘密指定情報を故意に取得・漏えい・開示し,または過失により漏えい・開示した者は,刑事・民事責任を問われ,管理者も使用者責任を問われる場合がある．わが国の根拠法には,特定秘密保護法・国家公務員法・自衛隊法・不正競争防止法・サイバーセキュリティ基本法・電気通信事業法などがあり,個人情報が含まれる場合には,これらの法令違反のほか,被害者のプライバシー侵害にもなり得るなど多様である．

Ⅵ。独立機関による手順の適正性の認証

会社に営業の自由があるように,組織にとって内部の情報管理をどのように構築するかは自由なはずである．しかし当該情報が「個人情報」である場合はもちろん,それ以外のケースでも,情報の扱い方は利害関係者の重大な関心事である．ましてや,その方法が当該企業の提供するサービスや情報そのものに直接影響を与えるとすれば,有体物の品質保証に類似した仕組みを設け,世間一般（特に消費者）の期待に沿うよう運用してもらいたい．その手段として開発されたのが,独立機関によるセキュリティ管理手続の認証制度で,秘密保持の仕組みも含まれる．会社などの組織は,資格を認定された機関から「お墨付き」を得るのが一般的である[21]．

Ⅶ。独立機関による定期的監査

手続の実際の運用のうち個別具体的な適用過程を公開すれば,第三者や社会全体の利益を害する場合もあり得る．従って,その職務に当たる者が,秘密裏に方針決定し実行することを余儀なくされるので,運用の適正性を担保できない．そこで、不完全な方法ではあるが,運用過程からは独立した機関による定期的な監査が行われる[22]．その際、当該監査機関に全情報を開示すればⅠⅡⅣの手続に反するばかりか,前述の情報の特性から漏えいリスクを高める結果にもつながるので,回避せざるを得ない。そこで通常は,サンプル調査か,抽象化された情報を対象にして,審査員の範囲を絞った監査になることを甘受せざるを得ない[23]．この難点は,次節の例で最も顕著に現れる．

4．　国家安全保障と防衛装備品の調達に関する特例

前節で述べた一般原則も,「言論の自由」を最大限に尊重した「情報の自由な流通」（Free Flow of Information）理念に対しては例外措置になる．加えて,先進諸国はほぼ一致して,この例外措置に対して更に国家安全保障上（インテリジェンス活動やテロ対策を含む）

[21] 本文では安全保障に関連する事例も想定して「独立機関」としたが,一般には TTP（Trusted Third Party）システムと呼ばれ,審査実施機関を審査する「認定機関」,審査実務を担う「認証機関」,審査員の審査をする「要員認証機関」が,それぞれを信頼することで成り立ち,各国の認定機関同士が相互承認を行うことで,国際的な汎用性を担保している．情報セキュリティに関しては、ISO 27000 シリーズの要求事項を担保する ISMS（Information Security Management System）認証から始まり,現在は隣接する分野に拡大しているが,いずれも原則的に民間企業を対象にしたものである（林 [2017a] pp. 177-179）．

[22] インテリジェンスは経験がないと判断できないため,監査側にも専門家が必要になり経験者が務めることが多い．その数が多すぎれば現職とのつながりが強くなり客観性が疑われ,少なすぎれば判断を誤る確率が高くなる（Lowenthal [2009] 邦訳書 p.250）．

[23] 国家機密に最も近い情報を扱う際の議会による監督のあり方として,議会の主要メンバーだけに開示するという方法が一例である．

の特例を設けているが,その内容は国によって様々である．上記の情報管理の手順自体かなり複雑であるが,例外措置を一般化して説明するのは更に難しいので,以下に代表的な例を示すにとどめる.

ア)「情報を開示して守る」制度である知的財産制度の中に,秘密特許という特例を設けている,

イ)「裁判公開の原則」の例外として,裁判官だけによる証拠調べ(in camera 審査)が認められている,

ウ)個人や企業が保有する情報に国家機関がアクセスするには,裁判所が発出する令状を要するとしつつ,国家安全保障に関する場合には特別のルートを設けている,

エ)外国人や外国企業による国内企業への投資に上限を設定し,一定数以上の株式取得に事後報告を求めるほか,国際的な M&A の審査に当たっては,国家安全保障上の配慮を優先している,

オ)技術情報やそれに基づいて製造された物を取引するのは,原則自由であるところ,大量破壊兵器や通常兵器の開発・製造等に関連する資機材,関連汎用品の輸出やこれらの関連技術の非居住者への提供については,国家による事前の許可を求める(輸出管理あるいは前項を含み経済安全保障と呼ぶ場合がある),

カ)政府調達全般に関してセキュリティ上の懸念があるものを排除しているが,近年その要件を厳しくしている,

キ) 防衛装備品の調達に関しては,一般の物件の調達よりも厳しい秘密保持を求める.

上記のうちカ)とキ)だけは補足が必要と思われるので,米国を例にして説明しよう．米国は「軍産複合国家」との批判もあるほど巨大な軍事予算を持っており,その装備品の調達は軍事力そのものに直結するので,世界一厳格に運用されている．そこで準拠しなければならない情報セキュリティ標準として,ⅰ)連邦政府の情報システム・組織のセキュリティ標準である SP (Special Publication) 800-53, ⅱ)連邦政府以外で CUI(注 15 を参照)を扱う情報システム・組織のセキュリティ標準である SP 800-171, ⅲ)連邦政府のクラウド調達の標準である FedRAMP(Federal Risk and Authorization Management Program),の 3 つがある.

これらを基礎にして,国防調達規則(DFARS = Defense Federal Acquisition Regulation Supplement)では,以下のような要件(マネジメント・システムでは要求事項と呼ぶ)を求めているため,米国の同盟国であると同時に,米国への販売機会を失いたくないわが国も,これに準じた仕組みを導入せざるを得なくなっている(藤井 [2018]).

あ)政府も企業もクラウド利用をミニマム・スタンダードとし,FedRAMP に準拠しなければならない,

い)CUI を取り扱う防衛関連企業については,SP 800-171 相当のセキュリティ対応が求められる．これは、SP 800-53 の水準では「中位」(moderate)相当である.

「装備品」はハードウェアに限らず,ソフトウェアや関連技術情報についても同様である.装備品の開発段階における「研究技術情報」が漏えいした場合も,当該情報に基づいた製品の調達は忌避されるであろうから，結局「情報管理が適切に実施されていないと軍事調達から排除される」結果につながる．米国は、このような連鎖を製品の流れであるサプライ・チェーンとともに,情報の流れの面からも保証しようと試みている.

5. 「情報管理」の重要性の現代的意味

インターネット商用化（1995 年）直後の国際経済は，時間と空間を克服したグローバル経済化が進展し，景気循環さえなくなるという楽観主義にあふれていたが，世紀の変わり目辺りから，その流れに反する動きが目立つようになった．

1 つは資本主義国家内部における所得格差の拡大に対する反動で，1999 年 11 月～12 月にシアトルで開かれた WTO 総会反対デモや，2011 年のウォール街占拠事件は，その現れとみられる．そして，2016 年と 2020 年の米国大統領選挙における親トランプ派と反トランプ派の越えがたい溝は，問題をより深刻にしている．

しかし，第 2 のより根源的な問題は，2012 年以降中華人民共和国の指導的ポストを独占する習近平総書記が，「中華民族の偉大なる復興」を掲げてナショナリズムを鮮明にし，ヨーロッパにまで及んだシルクロードを想起させる巨大な経済圏構想「一帯一路」を打ち出したことである．そして実際に東シナ海や南シナ海において，自国に有利な形で既存の国際秩序を作り替えようとする動きを加速化させている．

これに対して民主主義を信奉する諸国は，「自由、民主主義、基本的人権の尊重」といった普遍的価値やルールに基づく秩序を守ろうとするから，世界的な経済の統合ではなく「デカップリング（切り離し）」の動きをすることになる．バイデン大統領が習近平総書記を「専制主義者」と呼び[24]，プーチン大統領を「殺人者」と呼ぶことを否定しなかったのは[25]，レトリックであることを超えて「第 2 の冷戦」の危険性を象徴するものと捉えるべきだろう．

このような時代には，冷静な外交努力で不測の事態を回避することが第一義であることは当然であるが，同時に「身の回りは自己防衛する」ことを怠らないことも必要である．この点に関しては，平和国家であるわが国の感度が鈍く，緊急事態への対処も身についていないことが懸念材料である．セキュリティが破られても平然としていたり，攻撃者の背後に国家の意思が働いていることに気づかなかったりしていては，「生き馬の目を抜く」冷戦状況を生き延びることはできない（防衛基盤整備協会［2017］）．

このような視点から，わが国での情報セキュリティ対策を再点検してみると，その基本は依然として，民間企業のセキュリティ対策である ISMS（注 21 を参照）レベルにとどまっている．従って今後は，防衛産業が米国方式に追随せざるを得ないことを奇禍として，Military Spec である SP シリーズの保護レベルに多くの企業が短期間で移行できるか否かが，わが国の将来に大きく影響することは避けられないであろう．

もちろん，その過程には時間を要するから，最も機微な情報に関する管理方式が，より機微性が乏しい情報に次第に浸透していくことになるし，重要インフラに分類される事業が先に転換を迫られるなどの時間差が生ずるだろう．そして，この雁行型移行プロセスにおいて，汎用技術や両用技術に属する製品や，その「研究技術情報」の管理の脆弱性が問題になり，優先課題とされるであろう[26]．

---

[24] 2021 年 4 月 28 日（現地時間）米議会における施政方針演説で．
https://digital.asahi.com/articles/ASP4Y2HPBP4YUHBI009.html 参照．

[25] 2021 年 3 月 17 日（現地時間）放送のテレビ・インタビューで．
https://www.afpbb.com/articles/-/3337302 参照．

[26] 因みに、代表的なセキュリティ・インシデントを挙げて，その法的側面を解説した増島・蔦［2020］には研究技術情報に関する事例が登場しない．それはこの分野に隠れた脆弱性かあるか，世間一般の無関心から事

そのような動きは既に米国において,最先端技術である量子情報科学の分野で顕在化しており,連邦政府の助成を受ける研究に関してはセキュリティクリアランスの適用,外国政府の干渉排除,利益相反（conflict of interest）だけでなく責務相反（conflict of commitment）[27] の回避などが求められている（永野［2021］）.

冒頭に述べたように,この小論は「両用技術のあり方」そのものを議論するものではないが,その「研究技術情報」管理方式のあり方が,どのような影響を及ぼすかは意外に見逃されてきた論点である．しかも、その基礎となるセキュリティ技術は「両用技術」の代表例ともいえ,「攻撃を知らなければ防御もできない」というディレンマを抱えている．現在わが国には,この難題に向き合う勇気と努力が求められている（林［2016］）.

（追記）

本稿をほぼ脱稿した段階で，重要なドキュメントが 2 件発表されたので,最小限の追記をお許しいただきたい。

1. 2021 年 9 月 10 日に,北村［2021］が出版された．9年半にわたり内閣情報官と国家安全保障局長を務めた当事者の著作であり,わが国のインテリジェンスの歴史を凝縮した貴重な資料である．特に,唯一の「書き下ろし」部分である第 1 章において,「経済安全保障の司令塔役を担う経済班を設置した」ことが強調されている点に,本稿の趣旨と通底するものを感じた.
2. 2021 年 9 月 28 日に,2021 年～2023 年を想定した,新しい『サイバーセキュリティ戦略』が閣議決定された[28].今回の戦略では「Cybersecurity for All～誰も取り残さないサイバーセキュリティ～」を打ち出すとともに，安全保障環境が厳しさを増す中,中国・ロシア・北朝鮮を初めて脅威対象国として明記し,警察庁のサイバー局新設を打ち出すなど,政府による公助の面を以前より強調している．加えて,「経済社会基盤を支える各主体における取組」に「大学・教育研究機関等」が明記され（4.2.5）,「サイバー攻撃に対する防御力の向上」の項（4.3.2.の(1)②）で「我が国の先端技術・防衛関連技術の防護」の記述が強調されるなど,本稿の主旨と合致しているものと思われる.

［引用文献］

北村滋［2021］『情報と国家』中央公論新社
経済産業省［2016］「秘密情報の保護ハンドブック」
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf
自民党政務調査会［2020］「提言：『経済安全保障戦略』の策定に向けて」

案の発生自体に気づいていないことを,暗示しているかに見える.

[27] 後者は前者の研究者向け特別規定という側面を持ち、研究者の無償のコンサルティングや学会活動が本務に及ぼす影響なども考慮している。因みに米国の大学では,週 5 日勤務としてそのうち 1 日を学外活動に使うことを認める 5 分の 1 ルールが普及している。米国保健福祉省の RCR(Responsible Conduct of Research)を参照. https://ori.hhs.gov/ori-introduction-rcr

[28] https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2021.pdf 参照.

https://www.jimin.jp/news/policy/201021.html
永野秀雄［2021]「米国における科学者・技術者に対するセキュリティクリアランス―量子情報科学を中心に（上)(下）」『CISTEC Journal』3 月～4 月
林紘一郎［2016]「サイバーセキュリティと学術研究・人材育成」日本学術会議「安全保障と学術に関する検討委員会」資料
http://www.scj.go.jp/ja/member/iinkai/anzenhosyo/pdf23/anzenhosyo-siryo4-2.pdf
林紘一郎［2017a]『情報法のリーガル・マインド』勁草書房
林紘一郎［2017b]「情報の所有と専有」日本社会学会 理論応用事典刊行委員会（編）『社会学理論 応用事典』丸善
林紘一郎［2017c]「米国における CUI(Controlled Unclassified Information)の概念」『情報通信学会研究大会発表資料』http://jsicr.jp/doc/taikai2017/fall/D1.pdf
福岡真之介・松村英寿［2019]『データの法律と契約』商事法務
藤井敏彦［2018]「防衛装備庁が来年度から始める新たな調達基準の考え方」
https://www.techdevicetv.com/pdf/hp_180914security_atla.pdf
防衛基盤整備協会［2017]『中国のサイバー攻撃の実態（2016 年度）』報告書 BSK29-1
https://ssl.bsk-z.or.jp/kakusyu/pdf/jyousekikenkyu29.2.pdf
増島雅和・蔦大輔［2020]『事例に学ぶサイバーセキュリティ』経団連出版
Lowenthal、Marc M.［2009] “Intelligence: From Secrets to Policy (4th ed.)”, SAGE Publications 茂田宏（訳）[2011]『インテリジェンス―機密から政策へ』慶應義塾大学出版会