第13回DBSC早春セミナー様

データの公正な利用（Fair Use of Information）のための保有と管理

2018年2月28日
林　紘一郎 Ph.D., L.L.D.
情報セキュリティ大学院大学

2017年度大川出版賞受賞
http://www.okawa-foundation.or.jp/activities/publications_prize/list.html

問題意識

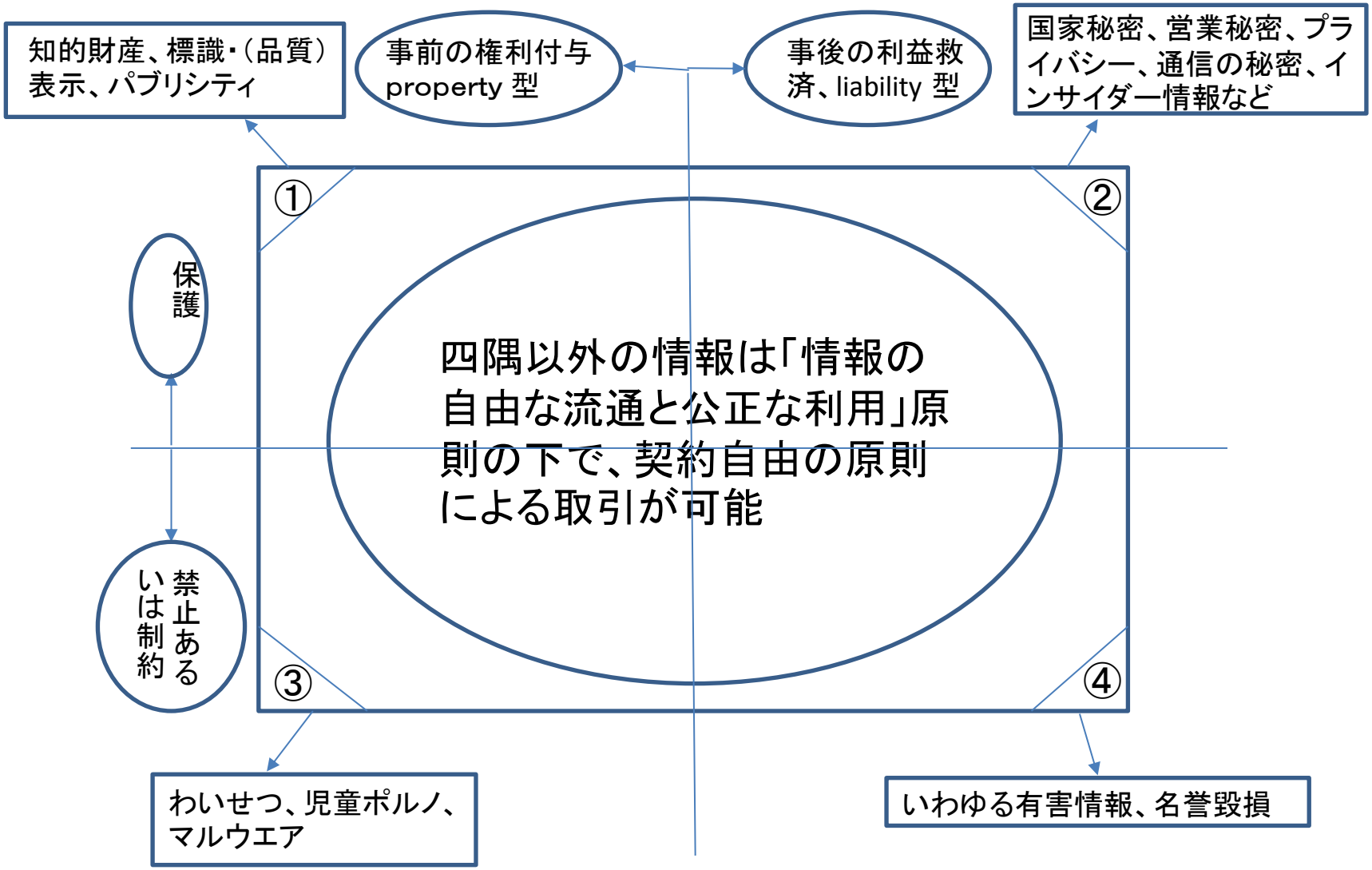
サイバー・インシデントが多発し、高度化・複雑化するにつれて、問題は個人情報漏えいにとどまらず、ICT依存を深めた社会システム全体を健全に維持管理することであるとの認識が高まっている。そのためには、「データ」を保護するにせよ禁止（制限）するにせよ、その 秘匿性（Confidentiality）・完全性（Integrity）・可用性（Availability）を保つことが必要であるが、その基準と手続きが確立されておらず、法的な「注意義務」との関連も定かでない。とりわけ、知的財産でも営業秘密でもなく、不法行為法による保護にも難点があるようなデータについては、今後の課題である。

同時に、データの管理方式を考える場合、「時と場所と態様（Time, Place, Manner）」によって変化するデータを、事前に格付け（classify）できるのか、またデータにアクセスする者の「適性評価」（security clearance）をどうするかは、各国にとって悩みの種である。この点に関して、安全保障に敏感で厳格な情報管理を行なっている米国で、CUI（Controlled Unclassified Information）という概念が生まれた背景も含め、その運用の実態と実効性を検討することを通じて、「データの公正な利用」（Fair Use of Information）を考える契機としたい。

問題意識を別の面から見ると、

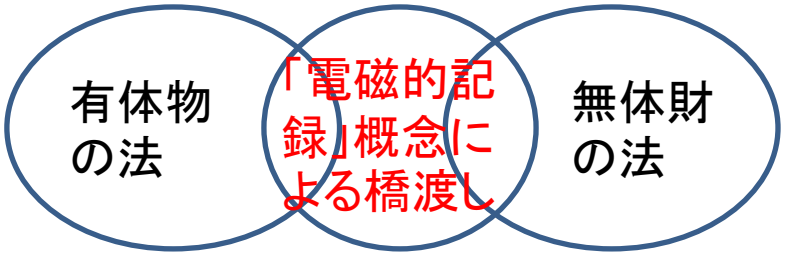
- データ・セキュリティは、セキュリティが破られた状態を回復・改善（軽減）・できれば抑止することに注力している、いわば病理学（Pathology、臨床・事後対応）である
- 本来なら、それと対をなす生理学（Physiology、理論・事前対応）があって然るべきところ、攻撃の高度化・複雑化に追いつけないためか、その面の検討は遅いか、全くなされていない
- セキュリティ・インシデントはデータ漏えい（特に個人データ漏えい）にとどまるものではなく、データが関連する、あらゆる局面に及ぶはずである。その場合、所有権アナロジーをいったん離れて検討することが必要である（知的財産における所有権アナロジーも、個人データにおける「自己情報コントロール権」や「忘れられる権利」的発想も、「情報が占有に馴染まない」という原点を無視している）
- 以上をまとめれば、データ・セキュリティには「データを適切に管理する」というプロセス（理論）があって、これを逸脱した場合にインシデントになる（臨床）という、他の学問では当たり前の理解を取り戻す必要がある

図表2-1.「情報の自由な流通と公正な利用」原則と例外としての法的規律



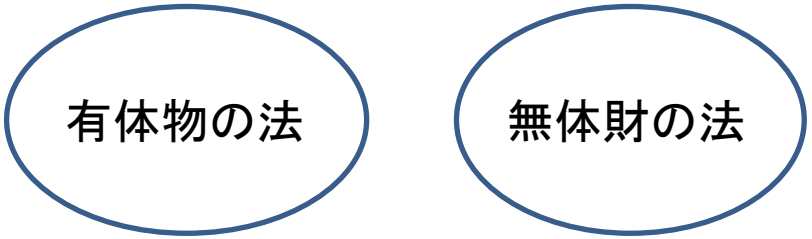
有体物の法と無体財の法の連続と不連続

連続局面



- e 文書も同様
- 電子署名・電子認証も
- 証拠能力も

不連続（断絶）局面



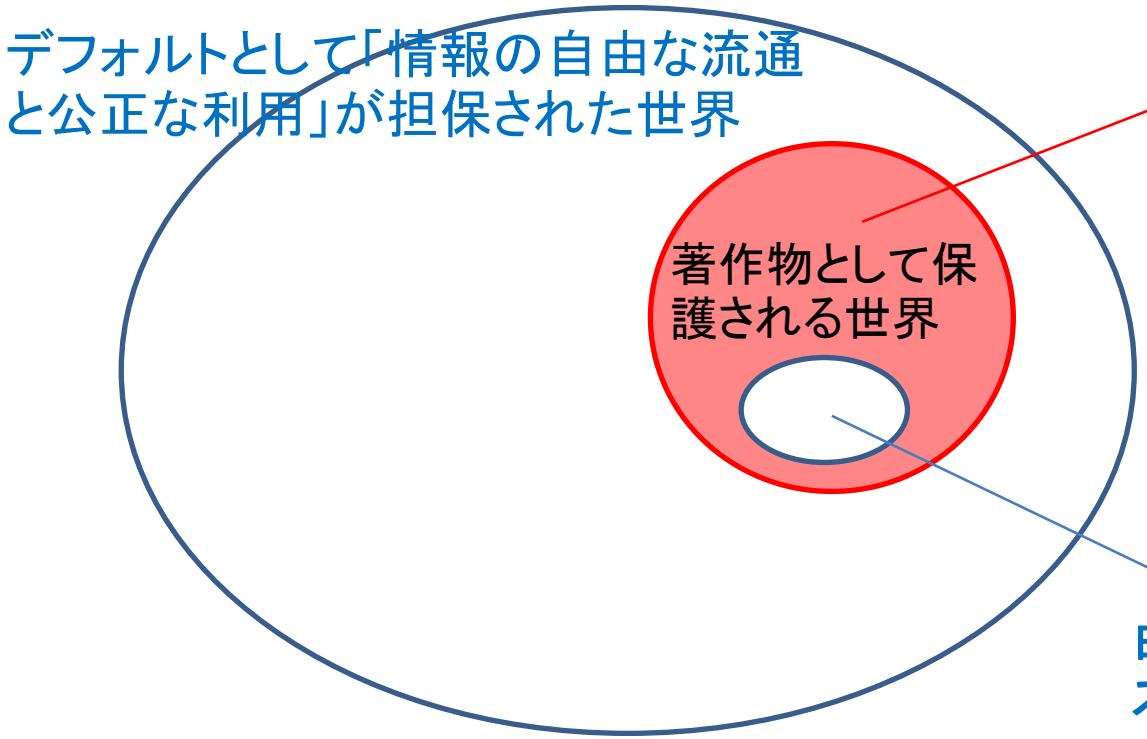
情報には次の特性があるので、有体物の法では十分に対応できない

- 不確定性
- 非占有性
- 非移転性（複製移転性）
- 流通の不可逆性

前図のうち非占有性・非移転性等

- 情報財は、①排他性（他人の利用を排除することができる）も、②競合性（私が使っていれば他の人は使えない）も欠いており、むしろ「公共財」に近い。加えて、③「占有」（民法180条　自己のためにする意思をもって物を所持する）状態も不確かで、その移転（内容が受け手に移転され、渡し手には残らない）も起きず、④移転は複製という手段でなされ、⑤デジタル化されていれば複製は簡単で、費用はゼロに近く、また品質も劣化せず、⑥いったん（意に反して）流出したら、これを取り戻すことはできない（取引の不可逆性）し、⑦どこに複製物があるかも分からないので削除も効果が薄い（「忘れられる権利」は実効性がない）。
- 上記は、拙稿 [2017]「情報の所有と専有」『社会学理論応用事典』丸善、から一部修正

Fair Use of Information（FUI）:
著作権を例にして



赤字の部分は、「自由な流通」の例外として、権利者に許諾権がある

白抜きの部分は、フェア・ユース＝例外の例外として「情報の自由な流通」に戻る（日本法では「権利の制限」）

＊この三層構造は、名誉毀損でも同じ

自然人（+ AI）と情報との「帰属」関係

仮分類	関係性	具体例	コメント
① 自然人特定データ	当該データから自然人がほぼ一意に特定される	シャノン的＝一意に決まるIDデータ。ウイーナー的＝生体情報特にDNAデータ	DNA が同じ一卵性双生児の場合も、「完全に一意」とは言えない。逆にコードとしてのIDの方が一意性が高い場合がある
② 自然人帰属データ	当該データが特定自然人に帰属することが、かなりの蓋然性を持っている	個人データ	この範疇を ① 寄りに考えるか ② 寄りに考えるかが大問題。なお、曖昧さが残るので個人情報という語は使わない
③ 自然人創作データ	特定の自然人が創作するデータ	自然人の著作物	この範疇には「所有権」アナロジーを適用できるが、それを上記の2つの範疇に拡張することは困難
④ 人工物生成データ	自然人が作り出した人工物が生成するデータ。③ の一部だが、特別の扱いが必要	シャノン的＝センサー・データの集合。ウイーナー的＝AIの生成物	このパターンのうち少なくとも AI については、上記 ① ～③ で裁くことには限界がある

シャノン界面とウィーナー界面

シャノン界面 / ウィーナー界面	物理世界（Atom）	情報世界（Bit）
制御可能（Controllable）	ほとんどの人工物	コンピュータ、 スマートフォン
制御不可能* （Uncontrollable）	内臓感覚、自然の気候、 自己学習型 AI	SNSの情報の流れ、 自己学習型　AI

＊今後とも制御の可能性を追究する必要があり、「帰属」がその基本的な属性と考えられる。

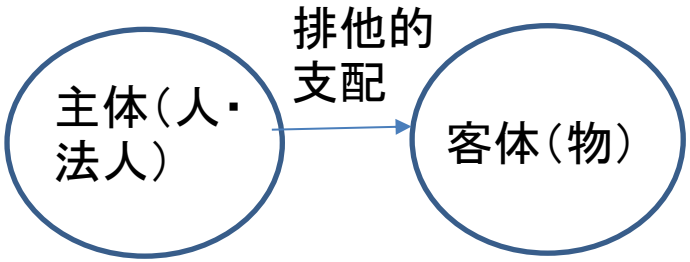
（出典）稲見昌彦教授（情報科学）の講演を聞いた、ジャーナリストの長倉克枝氏の投稿（https://note.mu/kaet/n/n78fcf844af76）を、一部補正。

「帰属」（attribution）概念と両立しないもの

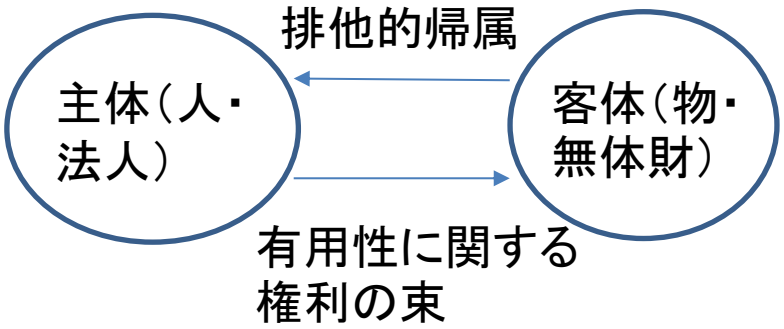
- 「情報は所有できる」という「有体物アナロジー」
- 「自己情報コントロール権」や「忘れられる権利」という情緒的な議論
- 「情報自己決定権」という（ドイツからの）輸入理論
- 「自己が管理支配する情報は、100%コントロールできる」という幻想
- 著作権が All Rights Reserved だという発想（Some Rights Reserved に満足できない発想）
- 主体と客体を峻別する発想（subject は subject(ed) to の場合は、「何かに従属している」（Verbeek [2011]）し、e メールの subject の場合は、「客体」に近い。EU の GDPR などが使う data subject も、data subject to me とも取れるが、data as subject とも取れる）

旧来の権利論と関係的権利論

A. 伝統的な考え方

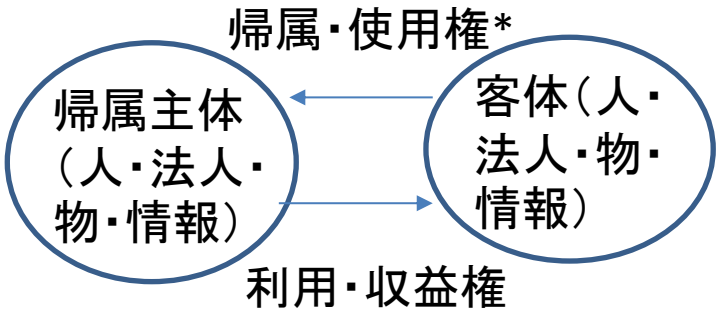


B. 森田 [2014] の考え方

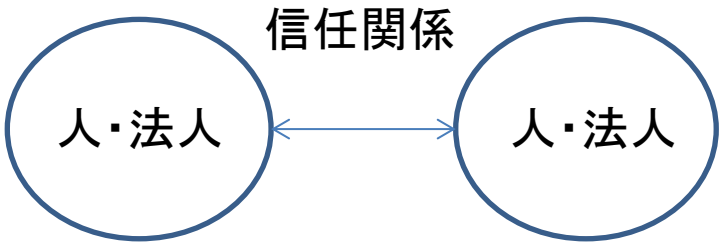


C. 林 [2009b] を修正した関係論的権利

C-1. 帰属型



C-2. 信任型



* 管理義務が付随すると考える

データの法的保護の現状

- 知財的保護は、ある程度確立されている（著作権法におけるタイプフェイスなどの問題、特許法における claim の範囲の問題やパテント・トロールの問題などはある）。しかし、不法行為との関係（法益を別にするという考えと、知財法が不法行為法の特別法だとする考え）が明確でない
- 秘密的保護（営業秘密を含む）は、主体別（個人のプライバシー、企業の営業秘密、国家の機密）に分断され、統一理論がない。特にわが国では、特定秘密保護法をまともに取り上げて考察する風土に欠ける
- プライバシー保護と個人データ保護が（意識的にか無意識的にか）混同されている
- 「流通の不可逆性」という特性を持つ情報に関しては、事後的な損害賠償よりも、即時的な差止が有効であるところ、後者は限定的（法的されている場合か、人格権侵害の場合など）にしか適用されない

新しい提案

知財本部：「新たな情報財検討委員会報告書」（2017年3月）
https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho.../houkokusho.pdf

経済産業省：知財（公開）と営業秘密（秘匿）の二分法の中間に、「一定の条件下で共有可能な情報」であり、① 技術的管理性、② 限定的な外部提供性、③ 有用性、の3要件を満たす情報の、不正利用・不正流通に対して、差止請求権を付与しようとする提案

・同省：「第4次産業革命を視野に入れた知財システムの在り方について」（同検討会報告書）（2017年4月）

http://www.meti.go.jp/press/2017/04/20170419002/20170419002.html

・同省：「データの利用権限に関する契約ガイドライン」（2017年5月）

www.meti.go.jp ＞ お知らせ ＞ ニュースリリース ＞ 2017年度一覧

・ 同省: 産業構造審議会 知的財産分科会 不正競争防止小委員会「データ利活用促進に向けた検討中間報告（案）」（2017年11月）
www.meti.go.jp/committee/sankoushin/chitekizaisan/fuseikyousou/.../008_03_01.pdf

データを「保有・管理」することは出来る

- 「保有」は、実効支配（国際法の概念）することと考えれば良い。ただし有体物と違って、同じデータを別人が、同時に「保有」することもあり得ることに留意
- 「管理」は、「善良な管理者の注意（民法644条、会社法330条など）を払って、データの秘匿性・完全性・可用性を維持すること」と考えれば良い
- 管理手法は、管理者が定めるものだが、通常 ① データを事前に（主として秘匿性の面から）格付けし、② 同じく事前にアクセス者の適性評価（security clearance）を行ない、③ その組み合わせとして許容されるアクセス方法を、予め規定しておき（アクセス権の設定）、更に ④ アクセスの都度 Need-to-Know の原則に反しないか否かをチェックする、のが一般的
- しかし、オバマ政権は、9.11以前にテロに関する情報が入っていたにもかかわらず、それが適切に共有されなかったとして、新たに Need-to-Share を強調したため、Need-to-Know 原則とのバランスが議論になっている

「保有・管理」の原則

- 情報は世界に遍在するものであり、その自由な流通（FFI=Free Flow of Information）こそが、民主主義・資本主義の根拠となっている
- この面では、Fake News 批判を続けるトランプ政権は、自らの国が拠って立つ基盤を掘り崩している
- 民主主義を共有しない独裁国家は、FFI よりも国家主権が優位に立つと主張するが、コンテンツ規制を中心に情報の流れを国家が制御すれば、インターネットの「自律・分散・協調」システムの恩恵をフルに受けることが出来ないので、長期的には「比較劣位」に陥るであろう
- 情報に所有権を適用することはできないが、情報を「保有・管理」することはできる（その限りで「管理責任」が同時に発生する）と考えないと、インターネットは無法地帯になってしまう
- この「保有・管理」は、「情報の公正な利用」（FUI=Fair Use of Information）を担保するものである

「保有・管理」の時間的有限性

知的財産には有限の「権利保護期間」がある。
秘密情報は厳格な管理が必要なので、早晩開示が要請される
（特定秘密保護法では、原則10年まで）
その他の情報には、FFIの原則が適用される

(参考） 財務省 **公用メール「60日廃棄」継続　システム更新後も**

- 毎日新聞2018年1月22日 07時00分(最終更新 1月22日 08時23分)

省庁で利用が急増している公用電子メールについて、財務省は送受信から60日で自動廃棄していることを毎日新聞の取材に明らかにした。昨年5月に国会で野党議員から見直しを求められた後も、廃棄を続けていたことが判明した。国土交通省も送受信から1年でメールを自動廃棄する方針を決めているが、両省以外に同様のシステムを取り入れている省はなく、政府内でメールの管理方法にばらつきが出ている。【大場弘行、青島顕、川上晃弘】

インテリジェンス情報の漠然とした理解

- 秘密情報は事前に格付け(classify)される
  Top secret > Secret > Confidential
- アクセス者の適性評価(security clearance)がなされている。これにも段階があるようだが、公開情報は少ない
- 両者の関係性(Need-to-Know)に基づくアクセス制御がなされてきたが、9/11事件以降は、守秘に傾き過ぎて共有がなされなかったとして Need-to Share も主張されるようになった
- Classification の3分類に付加される条件(情報源の表示や配布先の指定)があるとは知らなかった
- また、3分類以外の情報(unclassified)は、一律に処理されるので、その中に classified に準ずる情報があるとは思ってもいなかった
- わが国の特定秘密保護法でも、類似のことが行なわれているはずだが、その詳細を知ることは出来ない

アクセス者の security clearance

- 政府職員が主たる対象：連邦人事局が実施（先に流出した2,000万人とも言われる連邦職員の人事記録には、この情報も含まれていた）
- 防衛装備品の調達先企業にも適用（当然のことながら、日本企業も含む）
- その他、ITシステムのアウトソース先にも適用（Snowdenの例）
- 外交史や安全保障の研究者にも適用（私がコロンビア大学の安全保障の研究者にアポを求めたところ、「セキュリティ・クリアランスを受けていない研究者とは会えない」と拒否された）
- 米国全体で500万人が資格を得ている（人口の2%！）

CUI（Controlled Unclassified Information）

米国で9.11テロの教訓を踏まえて発出された大統領令（Executive Order）13556は、それまで連邦政府の各機関で、SBU（Sensitive But Unclassified）とかFOUO（For Official Use Only）という名称でアクセスや配布が制限されてきた情報（100種類以上あった）を、CUI （Controlled Unclassified Information）という形で統一的に扱う方針を定めたものである。

それを受けて国立公文書記録管理局（National Archives and Records Administration）が政府部門における実施方針を策定し（32 CFR 2000, 2016年9月）、国立標準技術研究所（National Institute of Standard and Technology）が非政府部門への展開指針を定めている（NIST 800-171, 2015年6月, 2016年1月修正）。これらを分析することで、以下の諸点を解明できる。

① なぜCUIが必要なのか、② 連邦機関横通しの手続きはどこまで可能か、③ 従来のシステムからの移行はスムーズに進むのか、④ 移行費用や格付け担当者の育成はどうするのか、⑤ 情報の秘匿と共有のバランスはどうとるのか、⑥ 情報公開法（FOIA）との関連はどうか。

調査結果と暫定的結論

上記 ② に関しては、CUI/Basic（各省共通）とCUI/Specialized（各省独自）の区分を設けて対応するなどの工夫が見られるが、③と④ は現在進行形であり、今後の展開を注視して行かねばならない。① ⑤ ⑥ は、この制度の本質に関わる部分であるが、③ と ④ の進行を待たなければ議論できないと思われる。このように制約は多いものの、各種の資料を比較して概要を把握することができ、予備的考察としては一定の成果を上げた。

ところで、EO 13556は、9.11の教訓として「テロ情報は入っていたが、関係者に共有されていなかった」という反省から、従来のNeed-to-Know の原則よりも Need-to-Share の必要性が叫ばれる中で発出された。情報の価値は「誰もが知っていれば意味がない」が、「誰一人も知らなければ意味がない」という両極端の中間にあるため、微妙なバランス論とならざるを得ない。CUIがその先駆的試みであることに変わりなく、多くの教訓が得られたので、本格的考察に移りたい。

CUI 考察の意義

- 情報の「秘匿・限定利用・公開」の、3つの要請間のバランス論として、考察に値するテーマだと直感した
- 調べてみると、classified info. にも、更に細かい分類があることが分かった。例）傍受解読情報であることを知られたくないための符牒（ULTRAなど）や、compartment化するとか、配布先を限定するためのコードなど
- アメリカが完璧であるとは到底言えないが、少なくても連邦政府において標準手続を定め、それを政府調達などの条件にすることで民間にも浸透させている点は、優れたモデルだと思えた（この手法は、わが国も直ちに導入すべきであり、それを怠ると国際調達で勝ち目が薄くなることが懸念される）
- 英米流のプロセス重視型経営（マニュアルなどで手順を決めてセキュリティ・レベルを維持する）は、わが国にはなじみが薄いが、N自動車やK製鋼所の不祥事を見ると、「わが国は製品さえ良ければ売れる」と思い上がっているように見え、「日本品質を支える手続き（Process）を標準化しなければ危うい」と思わざるを得ない
- 言うまでもなく「セキュリティ」は、商品（特に情報商品）の品質そのものである

類似の発想

- TLP（Traffic Light Protocol）：CSIRT（Computer Security Incident Response Team）などで情報共有するための、自主的情報格付け
- RED（情報提供元の内部者限り） AMBER （情報を知る必要がある者のみが限定的に利用）GREEN（関係者と共有可能） WHITE（公開して良い情報）の4区分を指定
- 他にも Chatham House Rule（情報の内容は伝えて良いが、誰がどこで言ったかなどのメタ情報は、秘匿する義務がある）が有効に機能している
- またex parte communication waiverという、「事前の同意を取って、本人に知らせないままに個人データを本人以外の関係者で共有する」という仕組みもある。病院で、医療従事者だけで患者に関する情報を共有する、教育機関で同様のことを行なう、などが考えられる

今回触れなかった課題

- Blockchain 技術によって、何ができるか。この技術による ledger もデータベースか？
- Data Localization の技術的可能性と、政治的意味
- AI の deep learning の基礎となる DB には、特別な扱いが必要か？
- デジタル証拠のあり方。特に、Discovery 制度の負担と効用
- Fake News の見破り方

[参考文献] Luciano Floridi [2010] “Information: A Very Short Introduction”, Oxford Univ. Press