[研究ノート]

国家機密の保護-機密区分管理

Protection of National Security Information – Classification Management

コンサルタント　　今　道　周　雄
Independent Consultant　CHIKAO IMAMICHI

要　旨

先に本学会誌で発表した「国家機密の保護—制度と技術」[1]において、現在の日本の国家機密保護制度では情報システム技術と、法律および行政規則を総合した検討が不足していることを指摘した。なかでも機密情報の統一的な区分管理方法が確立されていないことが問題である。そこで本稿では機密情報区分管理に必要な、機密情報の特性、機密区分をするための原則、機密レベルの決め方、機密指定を適用する期間の決め方、機密指定を解除する場合の判断基準、などについて述べる。機密区分管理に関する論文で、もっともよくまとめられている米国の機密情報区分管理に関する教育資料を引用し、日本の制度や事例と対比しつつ検討する。

キーワード

国家安全保障に関わる情報(National Security Information)、機密指定（Classification）、機密指定解除(Declassification)、情報保護（security of information)、実質秘、形式秘、機密（Top Secret）、極秘（Secret)、秘（Confidential)、情報開示リスク（risk of disclosure)、意識（Awareness)、暴露（Unauthorized Disclosure）

1．まえがき

本稿では国家の安全保障にとって重要で、かつ非公開な情報を「国家機密」または「機密情報」とよび、一方行政府が非公開と定めた情報全体を「秘密」または「秘密情報」と呼ぶことにする。機密情報をその重要性によってランク付けする作業を「各付け」と云い、それぞれの各付けを示す「機密」「極秘」「秘」などといった名称を「各付け名」と呼ぶことにする。また、この格付け結果を「機密区分」と呼ぶことにする。

国家機密情報の保護について議論するとき、3 つの観点がある。第一は公務員が遵守すべき規則としての観点である。業務遂行のための規則は法律と矛盾なく、かつ漏れなく、しかも運用可能に制定されていて、それに基づいた業務の執行がなされなければならない。

第二には如何にして国家機密を守るに足る、安全な情報システムを構築するか、という技術的な観点である。情報の処理が電子情報システムに依存してくると、定められた規則を運用するために、「規則」とそれに対応した情報保護機能をもった電子情報システムの構築が必要となる。

第三は法律としての観点であり、国家機密を保護できるような法体系が出来上がっているかどうかが問題となる。さらに罰則を伴う法律では、秘密が本当に罰則を適用せねばならない価値を持つのかどうかを問われ、「形式秘」や「実質秘」といった「秘密」の本質についての議論がある。

先の拙著「国家機密の保護—制度と技術」[1]では第一および第二の観点から日米両国の仕組みを比較し、日本の保護制度と保護技術の不備な点を指摘した。

本稿では上記論文で十分に議論し尽くせなかった機密情報区分管理の考え方について述べる。なお、第三の観点からは米国でも議論[8]があるが、法律の専門家の議論に委ねたい。

機密情報はその情報の価値と特性により、機密区分や保護手段が変わってくる。そこで機密情報取り扱い担当者は、情報の価値および特性を十分理解していなければならない。機密情報区分は情報の重要性や、配布範囲によって変わる。機密情報区分の付与を担当する者は、区分の原理を理解し、他者にも十分納得される区分を行わなければならない。区分の原理は当然、法律や行政規則に立脚していなければならない。機密情報取扱担当者や機密情報区分担当者は、情報特性や区分原理についてしっかりとした教育・訓練を受ける必要がある。従って行政実務者にとっては、わかりやすく誰もが納得できる機密情報区分とその管理の原則が法律あるいは行政規則に即して定められていることが望ましい。

米国エネルギー省は 1993 年に教材として”Security Classification of Information: Vol.2 Principles for Classification of Information”[2]（以後は「米国教材」と呼ぶ）を作った。機密情報区分管理に関する教科書はあまり他に例がないので、本文ではこの教材に沿って、日本の制度と米国の制度を比較しつつ機密情報区分管理の考え方を検討する。

2. 国家機密の定義

米国では国家の安全保障に関わる情報を NSI(National Security Information) と呼ぶ。NSI は、機密指定をすべきかどうか、その重要度はどれほどか、などについて大統領令 EO13292 で定められた基準にしたがって機密区分が行われ、機密指定をうけると classified information（機密情報）と呼ばれる。

合衆国憲法 50USC Sec435（Title 50: War and National Defense） に基づいた米国大統領令 EO13292 が定義[3]するところによれば、国家安全保障に係わる機密情報（classified National Security Information：以後 CNSI と呼ぶ）とは、外交と防衛に関して国が保有し、その管理下においている情報であって、外部に漏れたときに国益に損害を与えるものをいう。大統領令は CFR (Code of Federal Regulation)に組み込まれ、連邦職員の順守すべき規則となっている。

日本では国家の安全保障に関する情報を包括的に表す CNSI に相当する統合的な規定はなく、国家公務員法第 100 条の判例により規定される広範囲な「秘密」と、「日米相互防衛協定等に伴う秘密保護法」が規定する限定的な「特別防衛秘密」および、「自衛隊法」が定める「防衛秘」がある。

日本にはかって「国防保安法（昭和１６年法律第４９号）[4]」により「国家機密」が規定されていたが、現在は NSI に対応する外交および防衛に関する機密を統一的に定義している法律または規則はない。

現行法では防衛に関する情報は法律で保護が定められているが、外交に関する機密は外務省が定める「外務省における秘密保全のための規則」および公表されていない、いくつかの規則に従って定めた情報を、公務員が「国家公務員法第１００条」の守秘義務によって守る、という仕組みになっている。[5]

大統領令 EO13292 はその前文で、情報を国民に秘密にするのは、国家安全保障のためにやむを得ず行う処置である、とのべている。日本でも「外務省秘密電文漏洩事件」の一審判決[6]では「わが国のような民主主義国家においては、公務は原則として国民による不断の監視と公共的討論の場での批判又は支持とをうけつつ行われるのが建前である。」と述べ、行政府の秘密保護が行き過ぎぬよう牽制している。

3. 機密情報の特性

一口に「機密情報」といっても、外交文書と兵器マニュアルではその性格が全く異なる。たとえば前者はそれほど多くない政府要人と官僚が関係するだけなのに対し、後者は兵器を扱う多くの兵士が関係する。文書の量も前者は数ページから多くても数十ページに過ぎないのに比べ、後者はバインダー数冊にもなるだろう。このような機密情報の特性を把握し、その性格に見合った保護処置をとることが必要である。

米国教材では、秘密は「主観的(Subjective)秘密」と「客観的(Objective)秘密」の二つに大別している。それぞれの特性、性質や特徴と、その事例を第１表にまとめておく。

「客観的秘密」は科学や技術の情報を含んでいる。現在の日本の秘密保護制度では、「自衛隊法」と「核原料物質、核燃料物質及び原子炉の規制に関する法律」が技術情報の保護を定めているが、新たな研究や技術開発における情報の保護には触れていない。日本の科学研究成果や技術が兵器に転用される可能性は皆無とは言えず、今後検討が必要である。とくに NBC (Nuclear, Biological, Chemical)の技術分野では研究や開発に携わる人の情報セキュリテ

ィ意識を高めると同時に情報保護の制度を構　築する必要がある。

表 1 機密情報の種類　(”Security Classification of Information: Vol.2 Principles for Classification of Information”**より引用**)

機密情報の種類	主観的機密 (Subjective Secret)	客観的機密 (Objective Secret)
説明	政府が有する固有の情報を、相手方に知られまいとして秘匿する場合で、政府がその情報を管理・保護する限り、相手方が自主的にその情報を知ることは出来ない場合。	政府がいかに秘密にしておこうと努力しても、相手方が独自にその情報を発見しうる場合。
事例	他国に対し軍事行動を起こす計画（日時、場所など）あるいは特別な国際情勢下で策定した外交政策など。	科学的情報あるいは技術的な情報など。
特性	情報量は少ない	情報量が多く、伝達することが難しい。
	相手方がその情報を見れば、すぐに理解できる。	相手方には理解するための高度な知識が必要。
	盗み出す以外その情報を知る手段は無い。	研究により独自に情報を得ることが出来る。
	変更の対象である	変更の対象ではなく、常に一定である
	短期間で情報価値はなくなる。	長期にわたって価値がある。

4.　機密指定と機密区分の枠組み

第２節で述べたように機密情報は法律(命令を含む)で明文化されたものと、行政府が内部規則により定めているものがある。これらの機密情報は重要度に応じて機密区分がされ、機密区分された情報は、そのレベルに応じて適切な保護手段を講じることになっている。機密区分については、法律で定めているものと、行政府の内部規則で定めているものがある。以上のような機密指定と機密区分の枠組みに関する考えかたは日本も米国もほぼ同様である。

大きな違いは、機密区分の原則が米国では統一的に大統領令 E013292 で定められているのに対し、日本の場合、文書取り扱い規則は各省庁が独自に制定している点である。しかし、それでは機密文書の取り扱いが徹底しないことから、機密文書の取り扱いについて第３表に示す二つの統一的な行政基準・通知が定められた。

その一は「秘密文書等の取り扱いについて（内閣官房内閣参次官室主席内閣参事官)」[7]であり、業務面の観点から「どのような情報を秘密にするのか」をその理由と共に示している。その二は情報処理技術面の観点から「政府機関の情報セキュリティ対策のための統一基準（以後『統一基準』と略称)」が策定された。このように形上は業務面とそれを支える技術の両面から、機密保護の整備が行われている。「統一基準」は「機密情報」もその対象として含んでいる。

しかし、これらの規則を大統領令 E013292 と比較すると、用語や機密区分が統一されていないし、また機密区分の考え方並びに区分基準や、機密の管理方法について体系化がされていないことが問題である。

現在の日本の法律が定めている機密相当の「秘密」とその機密区分の仕方を表２に示す。

表 2　日本の法律等に規定された「秘密」とその機密区分

法律等の名称	対象	機密区分
自衛隊法	我が国の防衛上特に秘匿することが必要であるもの。	なし（昭和３３年防衛庁訓令第１０２号により区分)
日米相互防衛援助協定等に伴う秘密保護法	米国から供与された装備品等について •構造または性能 •制作、保管又は修理に関する技術 •使用の方法 •品目および数量	•機密 •極秘 •秘密

表 3　日本の行政規則等における機密区分

規則等の名称	保護対象		機密区分
秘密文書等の取り扱いについて（内閣官房内閣参次官室主席内閣参事官通知）[7]	1.　外交・国際経済・防衛に関するもの • 外交交渉の過程における訓令報告等 • 国際通貨問題に関する国際会議の議事内容 • 暗号 • 武器の性能緒元 2.　個人の秘密に関するもの • 企業財務内容 • 特殊な病気に関する療養所への入所決定通知 • 人事に関する資料	3.　職務の特殊性に由来するもの • 捜査関係資料 • 巡視船等の配備計画 • 事業所等への立ち入り計画 • 裁判・審決・審判等への評決 • 発注工事の予定価格 4.　一定期間秘密にする必要があるもの • 人事異動案、 • 基準外国為替相場の変動、 • 公開競争試験の問題、 • 特許出願書類	• 極秘 • 秘 • 部外秘
政府機関の情報セキュリティ対策のための統一基準	• 下記以外の情報。（機密性情報１） • 行政事務で取り扱う情報で、秘密文書に相当する秘密性は要しないが、直ちに公表することを前提としていない情報。（機密性情報２） • 行政事務で取り扱う情報のうち、秘密文書に相当する情報。（機密性情報３）		• 機密性情報１ • 機密性情報２ • 機密性情報３

表３の「秘密文書等の取り扱いについて」の保護対象１項は NSI に相当し、２，３，４項は米国では SBU (Sensitive But Unclassified)と呼ばれ、機密指定を受けない種類の情報である。

このように日本の行政規則では「機密」と「秘密」がひとくくりで扱われ、それに３レベルの機密区分を適用している。また、当然ではあるが技術的にも「政府機関の情報セキュリティ対策のための統一基準」で規定しているように「機密」を扱うシステムと「秘密」を扱うシステムは同じレベルで考えられている。

米国の法律で「機密」保護を規定している法律は第４表に示す通りである[8]。いずれの法律も機密区分は EO 13292 が最新の基準となっていて、法律と行政規則が一致した形で運用されている。

米国では 2002 年に電子政府の展開を目指して、連邦政府の情報保護を強化するために、Federal Information Security Management Act(FISMA)を制定した。そしてその技術的な裏付けとして National Institute of Standards and Technology(NIST)が NIST risk Management Framework を定め、NIST Special Publication 800 シリーズを公表した。

NIST SP 800-60[9]では、このガイドラインの対象としては国家安全保障にかかわる情報 (NSI) を含めないと述べている。NSI をサポートする電子情報システムに関する規則は暗号に関する部分を除き公表されたものはない。つまり、CNSI の保護システムは一般の電子政府とは全くの別物である。ここでも「機密」と「秘密」の分離が明確にされている。

表 4　米国の法律に規定された「機密」

法律の名称	機密情報	機密区分
US Code Chapter 15 National Security Subchapter Vl-Access to classified Information Sec. 438[10]	「機密指定情報(classified information)」とは、EO12356(現行の EO13292)で定められた情報および”Atomic Energy Act”で定められた情報である、と定義している。	「機密指定情報」の扱いをうけ、EO13292 に基づいた機密区分がされる。
The National Security Act of 1947[11]	すべての機密指定情報(classified Information)および諜報源と情報の収集方法	同上
The Atomic Energy Act of 1954	RD(Restricted Data)、 FRD(Formerly Restricted Data)および機密指定情報。	同上

表 5　連邦政府規則

連邦政府規則の名称	機密指定対象情報	機密区分
32CFR part2001-2004 (EO 12392)	連邦政府が管理・保有する機密情報（すなわち NSI であると区分(classified) した情報） (a) 軍の計画、武器システムあるいは作戦に関する情報 (b) 外国政府に関する情報 (c) 諜報活動、情報源あるいは情報の入手方法、あるいは暗号 (d) 外国との関係、外国での活動および秘密情報源 (e) 国の安全に関係する科学、技術及び経済的な事項 (f) 核物質あるいは原子力施設の保護米国政府プログラムに関する情報 (g) システム、設備、基盤施設、プロジェクト、計画、あるいは国の安全に関わる保護サービスなどの脆弱点や性能に関する情報。 (h) 大量破壊兵器	•Top Secret（機密） •Secret（極秘） •Confidential（秘密）
NIST Special Publication 800 情報セキュリティ技術基準	NSI 以外の連邦政府が管理・保有する情報に関する情報	Unclassified but Sensitive

5.　機密指定(classify)のための原則

E013292 は一次機密指定（Original Classification）を行うに当たって、その情報が暴露(unauthorized disclosure)された場合、国家の安全にどのような損失をもたらすかを明確に定義するか、または記述することを求めている。但し、一次機密指定の対象は NSI のみであり、RD および FRD は生成された時点で機密区分に入る(born classified)ために、一次機密指定をおこなうという手順を踏まない。米国教材は EO13292 の求めに対応するために、次のような手順を踏んで機密区分を行うことを求めている。

（１） その情報は機密区分をする必要があるかどうかを判定する。
（２） 次にどの機密レベルに区分すべきかを判定する。
（３） 機密指定の期間をどれだけにするかを判定する。

第一番目の判断を下すためには、機密区分対象となる情報をきちんと定義し、E013292 の定めるいずれかのカテゴリ（表５参照）に属すること、そしてその情報が政府の管理下にあることを確かめなければならない。

当該情報が政府の管理下にあり、政府が保有している情報であるかどうかの判断は次の点に着目しなければならない。

ア.　その情報は自国内にあり、政府が保有する権限を有するか、または契約をしているか、あるいは法律により定められているか。

イ.　敵対者がすでにその情報を握っているかどうか。もしすでに相手が握っている情報であれば、機密指定することは無駄である。敵対者が自己の努力により、容易にその情報を獲得できるようなものであるか。もしそうであれば機密指定することは効果的でない。

ここでア. の「契約をしているか」という項目は重要である。国防省は企業や大学および研究機関に多くの開発研究を発注しているが、その中には国家の安全に関わる項目が多く含まれる。従って機密保持の契約は非常に厳しい。

CNSI についてはその情報を暴露したときに国に損害が及ぶという説明が、十分な根拠をもってできなければならない。但し、RD および FRD に該当する情報については根拠の説明は不要である。

このような判断に基づいて機密指定をすることになった情報には、判断の根拠およびどのような保護を行うべきかをガイダンスとして添付することを義務づけている。これは第三者が機密区分を照査した場合に、判断が正しいかどうかを明らかにするためである。

日本の機密指定の原則について調べたところ、「防衛秘密」の指定対象及び指定のための要件については、防衛省訓令第３６号「秘密保全に関する訓令」[12]で定められていた。しかし、「外務省文書管理規則」[13]は機密指定に関して何等記述しておらず、「秘密保全に関する規則」は入手できないため外交情報に関する機密指定の原則は見つけることができなかった。

6. 機密区分のレベル決定

機密区分のレベルについては、E013292 で以下のように定めている。

（1） 機密（Top Secret）：情報が暴露された場合，国の安全に甚大な（exceptionally grave）被害をもたらす場合

（2） 極秘（Secret）：情報が暴露された場合、国の安全に深刻な（serious）被害をもたらす場合

（3） 秘（Confidential）：情報が暴露された場合、国の安全に被害をもたらす場合。

この機密レベル区分は NSI および原子力関係の RD、FRD に適用される。しかし、上記の定義だけでは抽象的にすぎ、どのレベルに区分すべきか判断が難しい。一般論としてそれぞれのレベル間の被害の違いは 100 倍であると米国教材は述べている。つまり、「機密」情報が暴露された場合「秘」情報が暴露された場合の 10,000 倍の被害がもたらされることになる。国防省が示した「機密」の事例を表 6 に示す。

表 6 国防省が示した「機密」の事例

	内容
1	戦争遂行計画の全貌を述べた戦略書
2	戦争遂行計画のデータと想定など
3	戦術計画
4	諜報活動の範囲や成果を述べた書類
5	諜報活動計画や方針
6	重要な兵器に関する情報

機密区分のレベルを決定するための一般的な要因について米国教材は次の項目をあげている。

- 情報が暴露された場合の被害の大きさ
- 情報が暴露されてから、その影響が現れるまでの切迫度合
- 機密区分された情報の配布範囲
- 情報収集にかける労力の大きさ

いずれの項目も明確に記述され、第三者の評価に耐えうるものでなければならないとしている。

情報収集にかける労力が非常に大きい例は、科学・技術の分野に多くみられる。兵器に応用される科学・技術情報は機密区分が適用されることになっているが、その判断は非常に難しいようだ。

その 1 例として重要な兵器技術でありながら、米国が機密指定をしなかった「電磁爆弾」がある。この爆弾は爆発時に非常に短い（数百ナノ秒）強力な電磁パルスを発生し、広範囲に存在する電子機器や電気機器を無力化する。基本理論や大まかな実用化理論は公表されていて、ある程度の技術レベルを有する国またはテロリスト集団がその気になれば、製造が可能であると言われている。[14]

1964 年の国防省令では以下の項目を「極秘」レベルに区分することとしている。

- 機密区分された軍需品に関するトレーニング、保守、点検のためのマニュアル
- 軍需品の研究、開発、製造、調達に関する情報
- 軍需品の性能値、テストデータ、設計および製造データ

1991 年の情報セキュリティ監視室（Information Security Oversight Office: ISOO）の報告に依れば、一次機密指定された情報は 511,868 存在し、そのうちの 8%が「機密」レベル、74%が「極秘」レベル、18%が「秘密」レベルに区分されていた。これを見ても「機密」レベル区分に指定された情報は、少ないことがわかる。

以上述べたような機密区分決定のための原理が、日本ではどのようになっているのかを振り返ると、以下のような問題点が指摘できる。

- 情報漏洩による被害の大きさに対する評価がしっかりとされていないために、行政の一般的な「秘密」と、国家安全保障にかかわる「機密」との区分が判然としていない。
- 機密区分のレベルが表２、表３に示したように統一されていない。
- 機密レベル区分のための原理あるいは基準が、明確にされていない。
- ISOO のような組織が存在せず、機密情報管理の全貌が明らかではない。

7. 機密指定の期間

機密指定をどれだけの期間適用すべきか、どのようにその期間を決めるのか、について米国教材は次のように述べている。（以下米国教材 Chapter 8 Classification Duration: Principles for Determining The Duration of Information Classification より要約）

「原子力に関する RD および FRD 情報は恒久的に秘密である。NSI に関しては秘密区分期間を考慮しなければならない。考え方としては以下の３通りがある。

- 一定期間を適用する
- イベントにより期間を定める。
- 暴露される確率から期間を定める。

一定期間を適用するのは、とりあえず機密指定を２年間だけしておき、その後評価して実際の期間を決める、と言った運用がされる。従ってそのドキュメントには OADR (Original Agency's Determination Required) というマーキングをする。

作戦計画であるとか新型兵器などの情報は、実際に作戦が遂行されたり、兵器が展開されたりすると秘密ではなくなる。従ってこのような主観的秘密の区分期間は比較的に短い。これらはイベントが起こった時点で機密指定の期間が終了する。

科学や技術情報、諜報源や手段の情報、あるいは暗号に関する情報などは長期にわたって秘密にする必要がある。この場合は秘密を守れる確率に基づいて秘密指定の期間が決まる。その計算式を以下に示す。

- スパイ活動により直接情報が敵対者に漏れる確率は式（1）により計算される。

PDD=K1×NP----------(1)

PDD：秘密情報がスパイにより敵対者に漏れる確立

K1: セキュリティ審査をクリアした関係者が敵対者のスパイである確率、過去のデータから 10^{-5} 程度である。

NP: 秘密情報を知る人の数

- 不注意により情報が漏れる確率の計算は式(2)による。

PID=Kc×NP×NCOM×CREV×COP×UAR×RTA ----------(2)

PID: 秘密情報が不注意により敵対者に渡る確率

Kc: 不注意により情報を暴露する確率、10^{-3} ないし 10^{-4}

NP: 秘密情報を知る人の数

NCOM:秘密を知る人が年間に行う情報交換の平均回数

CREV:秘密保持の監査にかかわる係数、監査を実施しなければ CREV=1 だが、監査を行うことにより、一層小さな値となる。

COP: 各情報交換における平均のコピー数

UAR: 情報交換時に非認可者に情報が渡る確率

RTA: 情報交換時に敵対者に情報が渡る確率

PDD あるいは PID が目標とする値よりも大きくなると、機密区分をしておく意味がなくなる。」

日本外務省は機密区分の期間に関する原則を明らかにしていない。「外務省秘密電文漏洩事件」では電信案２通と受信文の写し１通がいずれも「極秘（無期限)」の指定をされていた。本事件についての国会審議で一部明らかにされた外務省の「秘密保全に関する規則の運用細則」[15]では、「第４条（管理者等）関連」の中で「(ヌ) 案件処理済みとなり常用性が無くなった主管課整理済みファイルは『文書保存廃棄類別基準』に基づき、保存期間を指定して文書課記録室に移管する。」となっている。「外務省文書管理規則、別表（第 7 条関係）[16]」では、文書保存の年限を定めているが、上記のような機密指定を受けた文書の保存については触れていない。ちなみに、防衛省訓令第 36 号は「第 16 条 1 項に規定する要件を欠くに至ったとき」秘密の指定を解除する、と定めている。

米国教材は機密区分担当者が、区分を行う時点でどれだけの期間がよいのか判定できない場合でも、必ず期限を設けるよう求めている。それは、いつかはその情報価値が失われること、そして機密保持のためのコストがかかるからであると指摘している。 米国では定期的に機密文書の見直しが行われ、価値が失われたものは機密指定を外すという作業を行っていることもあり、期限設定の意味が大きいと思われる。

8. 関連情報の機密指定

ある情報はそれ自体が機密指定されていないにもかかわらず、その情報から機密情報が暗示（あるいは明示）される場合がある。それを「関連情報（associations of information)」と称し、米国教材はそのような情報の扱いについて以下のように述べている。(Chapter 9. Classification of Associations of Information から要約)

「例えば、ある商品がそれ自体は機密に該当しないにもかかわらず、機密プロジェクトの購入対象になった場合、その商品が機密製品のサブシステムであることが推定される。このような場合商品調達情報は機密指定されることになる。

他の例としては機密プロジェクトのマネージャの名前が報告書配布リストに記載された場合、そのマネージャの専門分野と報告書の主題からみて機密プロジェクトの目的が推定できる場合は、その報告書は機密区分される。」

日本では関連情報をどのように機密区分するのか、調べた範囲では明らかにできなかった。

9. 編集情報の機密区分

秘密情報ではない情報を編集したものが、機密情報レベルの価値を持つ場合がある。例えば国防省の研究テーマを一覧表にまとめた場合、テーマ個々は何ら秘密に相当しなくとも、一覧から研究の方向性が推定される可能性がある。

このような場合、一覧は機密区分をするべきであろうか。

米国教材では、敵対者が独立に同じこと（編集）をできる場合は、編集情報を機密区分するべきではないとしている。

日本では編集情報の機密区分取り扱いをどの様にしているのか、調べた範囲では明らかにできなかった。しかし、編集情報の事例はある。

第一の例は、2007 年 7 月に新聞報道がされた自衛隊の情報収集事件である。自衛隊情報保全隊がイラク

派遣に関する市民運動や情報機関の情報を広範囲に収集し、「情報資料」と「イラク自衛隊派遣に対する国内勢力の反対動向」と題した資料にまとめ、それが民間に流出した。この「情報資料」には「注意」という指定がされていた。[17]

第二の例としては、防衛大学の卒業論文[18]である。ここでは卒業論文が公開されていて研究者名および研究題目とその傾向がわかる。これらの情報はウエブ上で公開され、誰でもがアクセスできる状態にある。このサイトを分析すると様々な研究の傾向が読み取れる。一例を挙げるなら生物化学分野の研究が、２００２年に外部からの教授を迎えてから、急速に進んだことが読み取れる。この分野である程度の知識を有する人がこれらの情報を分析すれば、生物兵器に関する自衛隊の現状をある程度把握することが可能であろう。

10．機密指定の解除

機密指定を解除する時は、利得とリスクが同時に発生する。従ってその両方を評価し、利得がリスクに勝る場合にのみ、機密指定を解除する。（以下米国教材の要約）

「CNSI の機密指定解除は第一次機密区分設定者のみができ、以下の 3 段階の判定ステップを踏まなければならない。

（１） 情報は未だ政府の管理下にあることの確認
（２） 機密解除の利得とリスクの評価
（３） 利得とリスクのバランスをとる。

RD および FRD については利得とリスクの判断基準は以下の通りである。(米国教育資料　第 11.1 表から引用)

【リスクの判断基準】
RC1: 情報が非核保有国にとって核兵器を開発するのに役立つ度合い
RC2: 情報が核保有国の核兵器改善に役立つ度合い
RC3: 情報が特定の核物質製造に役立つ度合い
RC4: 情報公開が米国の外交、兵器制限交渉あるいは条約責務に及ぼす影響
RC5: その他の国家安全上の影響
RC6: 情報公開がエネルギー省の信頼に与える影響
【利得の判断基準】
BC1: 情報公開により米国の計画が進む度合い
BC2: 情報公開により米国の計画コストが低下する度合い
BC3: 情報公開により技術が商用に移転される度合い
BC4: 情報公開により科学技術の進歩が期待される度合い
BC5: 情報公開により外交、兵器制限交渉、あるいは条約責務に及ぼす影響
BC6: 情報公開が社会全般あるいは教育に与える影響
BC7: その他米国にとっての利得
BC8: 情報公開がエネルギー省の信頼性に及ぼす影響　」

一方、日本での機密指定解除については、政府部門共通の原則を発見することはできなかった。

「外務省秘密文書取り扱い細則」第 16 条（変更及び解除）関連、では機密指定解除の手続きについて述べているが、機密指定解除をどの様な基準で行っているのか、記述されていない。

機密指定解除は国民の知る権利を保障すると同時に、歴史研究者にとって欠くべからざる要求であると思われる。従って機密指定解除の基準が有るならば早急に公開すべきであるし、無いのであれば早急に制定し、公開すべきである。

11．機密区分レベルの引き下げ

米国教育資料は機密区分レベルの引き下げについて、以下のように述べている。（Chapter 12: Downgrading Classified Information から要約）

「

- CNSI の機密区分レベル引き下げは可能である。ただし、その権限は、一次機密指定決定者、またはその上司、あるいは省庁の長が文書により認可した者にのみある。エネルギー省内およびその契約者では、機密区分レベル引き下げの権限は一次機密区分決定者、機密区分担当局長、あるいはセキュリティ担当局長に限られる。　」

日本では機密レベル引き下げの基準あるいは原則がどの様に定められているのか、調査した範囲では不明であった。

12．まとめ

「国家機密」という用語は、第二次大戦以来の歴史により、使用することを敬遠する傾向がある。しかし、公務員が守らなければならない一般の「秘密」とくらべ、「国家機密」は、情報価値が桁違いに大きい事を考えると、「秘密」と「国家機密」を同列に扱うことには問題がある。同時にそれだけ大きな価値のある「機密情報」について、日本の現行法や政府規則では取り扱いに関する原則が体系的でなく、しかも各省に「機密情報」の取り扱いが任されているために統一性を欠いていて、国民の「知る権利」に対し充分応える事が出来ない状況にある。

以上、機密情報の区分と管理をどのような基準にもとづいて行っているか、を米国の教育資料を基に日米

の現状を比較検討した。しかし、日本の現状に関する資料がほとんど入手できず、不十分な結果となった。

2007 年 8 月 9 日の朝日新聞報道によれば、政府は外交・防衛を中心に国家の安全などにかかわる機密情報「特別管理秘密」を対象とし、その管理のための専門部署を 2008 年度から内閣官房に新設するとのことである。「特別管理秘密」という新たな用語が使われているが、「特別防衛秘密」はこの中に含まれるのだろうか。新しい用語を使う前に、概念の整理を行う必要がある。すでに表 2 および表 3 に示したように日本の機密区分に使われている用語は統一性を欠いている。行政府と立法府は協力して法律、行政規則をよく見直し、全体として整合性のある概念を構築し、機密区分とその管理原則を整理するべきで、さもないと誰もが理解し遵守する機密管理体系はできあがらないだろうと危惧する。

日本の機密情報管理で強化が必要と思われるのは科学・技術情報分野の管理である。例えば大量破壊兵器の中でも、今後もっとも危険性が高いのは生物兵器であるという指摘がある。[19] バイオエンジニアリングの研究は、生物兵器への応用が懸念されるので、関連する研究機関の研究者には情報セキュリティの教育が必要であろう。

現在の日本政府機関に必要なことは、機密管理のための体系整備とそれに基づいた教育資料整備および幅広い関係者の徹底した教育である。

---

1 今道周雄、「国家機密の保護—制度と技術」、『日本セキュリティ・マネジメント学会誌』、第 21 巻　第 2 号、2007 年 9 月、25—40 頁

2 ”Security Classification of Information: Vol.2 Principles for Classification of Information” http://www.fas.org/sgp/library/quist2/index.html (2008. 02)

3 Executive Order 13292 Classified National Security Information, http://www.fas.org/sgp/bush/eoamend.html (2008.02)

4 国防保安法（昭和１６年法律第４９号） http://www.geocities.jp/nakanolib/hou/hs16-49.htm (2009.06)

5 内閣衆質１５０第１１号　衆議院銀金田誠一君提出外務省秘密文書の漏洩問題に対する答弁書 http://www.shugiin.go.jp/index.nsf/html/index_shitsumon.htm (2008.03)

6 外務省秘密漏洩事件　第一審判決 http://www.cc.kyoto-su.ac.jp/~suga/hanrei/36-1.html (2009.06)

7 公務員守秘義務論、佐藤英善 http://dspace.wul.waseda.ad.jp (2008.02)

8 CRS Report for Congress, “Protection of National Security Information” (Order Code RL33502) http://www.fas.org/sgp/crs/scecrecy/RL33502.pdf (2008.03)

9 NIST SP800-60 Volume l, Information Security http://csrc.nist.gov/publications/Pub s SPs.html

10 US Code Chapter 15 Subchapter Vl Sec. 438 http://www.law.cornell.edu/uscode/50/438.html

11 The National Security Act of 1947 http://www.intelligence.gov/0-natsecact_1947.shtml

12 防衛省訓令第 36 号「秘密保全に関する訓令」 http://www.clearing.mod.go.jp/kunrei_data/a_fd/2007/ax20070427_00036_000.pdf (2009.06)

13 外務省文書管理規則 http://www.mofa.go.jp/mofaj/public/johokokai/eturan/kitei/index.html (2009.06)

14 “Electro Magnetic Bomb, A Weapon of Electronic Mass Destruction” by Carlo Kopp http://www.abovetopsecret.com/pages/ebomb.html (2008.03)

15 内閣衆質１５０第 35 号「秘密保全に関する規則の運用細則」 http://www.shugiin.go.jp/index.nsf/html/index_shitsumon.htm (2008.03)

16 外務省文書管理規則、別表（第 7 条関係） http://www.mofa.go.jp/mofaj/public/johokokai/eturan/kitei/hyo.html (2009.06)

17 イラク派遣で陸自反対市民の情報収集、発言など詳細に http://www2.asahi.com/special/iraq/TKY200706060369.html (2008.03)

18 卒論題目　http://www.nda.ac.jp/cc/chem/ (2008.03)

19 “Biological Warfare Canaries”, By Christopher Aston http://www.spectrum.ieee.org/print/1534 (2008.03)

著者略歴

今道周雄（いまみちちかお）　コンサルタント。情報セキュリティ、技術戦略、ビジネス戦略などの分野で活動。昭和３８年（１９６３年）東京都立大学電気科卒業。同年三菱電機入社。平成７年（１９９５年）ドリームトレイン・インターネット社長、平成１２年（２０００年)アトミック・タンジェリン株式会社社長。平成１７年（２００５年）より現職。