米国原子力事業における秘密情報管理と我が国への示唆

Protection of Confidential Information in U.S. Nuclear Industry and its Implication for Japan

田邉　朋行[1]・稲村　智昌[2]

[1]博士（エネルギー科学）　（財）電力中央研究所　社会経済研究所　上席研究員
(E-mail: t-tanabe@criepi.denken.or.jp)
[2]修士（エネルギー科学）　東京大学大学院　工学系研究科　原子力国際専攻　特任助教
(E-mail: inamura@n.t.u-tokyo.ac.jp)

原子力施設に対するテロ懸念の高まりや，再処理施設の本格稼働等プルトニウム平和利用の着実な推進の確保等を背景に，我が国では，原子力開発利用分野における秘密情報管理の重要性が高まりつつある．本稿では，2001 年の 9・11 同時多発テロ以降その内容を強化してきた，米国の商業用原子力発電施設における秘密情報管理の先行導入事案を，法制面及び実務対応面の両面から調査・分析し，その特色を抽出するとともに，同分析を通じて，我が国における詳細制度設計や実務対応のあり方についての示唆を得た．

キーワード：核物質防護，セーフガード情報，情報セキュリティ，セキュリティ・クリアランス，テロリズム

1.　問題の所在と本稿の目的

2001 年の 9・11 同時多発テロ以降，原子力施設等に対するテロ懸念の世界的な高まり等を背景に，原子力開発利用分野における秘密情報管理対策の重要性が高まりつつある．これに関して，我が国では，平成 17 年 5 月に核原料物質, 核燃料物質及び原子炉の規制に関する法律（以下，原子炉等規制法）の改正が行われ，原子力事業に関係する核物質防護に係る秘密保持義務の導入（同法第 68 条の 3）という形で，核物質防護対策の強化の一環として，秘密情報管理に関する法整備が図られた．

しかしながら，後述するように，同制度においては，ガイドラインと要綱行政を通じた，国による一定範囲内での制度運用の妥当性確保と事業者対応への支援があるものの，情報アクセスに係る人員選別やアクセス時チェック等を含む，具体的な情報管理方法を規定した法令は不在であり，その内容の多くは事業者の判断に委ねられている．このような状況の中で，各事業者が自ら講ずべき情報管理措置の具体的内容を直ちに同定し，それを業界標準として実施に移すことは必ずしも容易ではない．また，具体的な情報管理方法に係る法令の不在は，制度の恣意的な運用を招く危険性や情報隠匿による原子力の安全性・透明性に対する懸念を社会に生じさせるおそれがあるとの指摘もある（詳細は **3.1.**で後述）．

そこで本稿は，9・11 同時多発テロ以降，その内容を強化してきた，米国の商業用原子力発電施設における秘密情報管理の先行導入事案を，法制面及び実務対応面の両面から調査・分析し，①そこではどの程度の水準の秘密情報管理対策がとられており，それはどのような特色を有しているか，②米国の先行導入例は我が国における詳細制度設計や実務対応のあり方に対してどのような示唆と課題を与えるか，について明らかにする．

2.　米国原子力事業における秘密情報管理の概要と特色 [1)]

核物質防護システムに関する詳細情報や核燃料の輸送スケジュール等といった、原子力施設や核物質の輸送等に関するある種の情報は，それが脅威に伝わることにより，施設破壊や核物質盗取等のリスクを生じさせる．そこで，米国では，原子力規制委員会（Nuclear Regulatory Commission：NRC）規則がこれらの情報を「セーフガード情報」（Safeguards Information：SGI, 我が国でいう「核物質防護上の秘密」を含む広い概念であるため，本稿では「保障措置情報」とは訳さず「セーフガード情報」の語をそのまま用いる）と定義し，その管理とアクセスに関して厳しい規制を敷く（10 CFR §§73.21, 73.57）．

また，原子力施設においては，予備電源，送電線，排水口等に関する設計情報等，施設の物理的セキュリティ

Table 1　NRC 規則（10 CFR§73.21 (b)）の定めるセーフガード情報の類型と内容

情報区分	定　義	具 体 的 内 容
固定サイトの物理的防護に関する情報	ある一定量以上の戦略特殊核物質を保有する，あるいは原子炉を所有する施設の保護に関連して，秘密データ又は国家安全保障情報等として分類されなかった情報	(i) 原子力施設又はサイトの複合的な物理的セキュリティ・プラン (ii) 実質的に物理的防護システムの最終的な設計上の特徴を表す，サイトの特定の図面，図表，スケッチ，又は地図 (iii) 侵入探知装置，警報装置，警報装置の配線，予備電源及び脅迫状態通報装置の位置を示す警報システムのレイアウトの詳細 (iv) 防衛組織のメンバーのためのセキュリティ命令及び手続を記載した書面，脅迫時の通報暗号，並びにパトロール・スケジュール (v) セキュリティ目的のために使用される，オン・サイト及びオフ・サイト間を繋ぐ通信網システムの詳細 (vi) 物理的な防護の肝心な部分となる文書，及び物理的セキュリティ・プラン，セーフガード上の有事プラン，製造設備又は利用設備に関する特異的な保障措置分析を含む文書の中で，特定の安全性に関連する設備のリスト及び位置を明示的に示すような文書類その他のもの (viii) 施設又はサイトの複合的なセーフガード有事プラン (ix) 物理的セキュリティ・システム又は対応手続の特性を明らかにする，施設警備資格とトレーニング・プランの一部分 (x) 規模，措置，応答時間及び武力対応の武器を詳述した，脅威対応プラン (xi) サイトに常備されている武力の規模，兵器及び配置 (xii) セーフガード上の危機が発生した場合に対応する，サイト外にある武力の規模，所属，兵器，及びサイトまでの到着時間 (xiii) 10 CFR § 73.55(c)(8)及び(9)にしたがって原子力規制委員会によって要請される情報
輸送時における物理的防護に関する情報	秘密データ又は国家安全保障情報として分類されない情報であって，一定量以上の戦略特殊核物質及び使用済燃料の海上輸送の防護に関するもの	(i) 輸送に係る物理的な防護計画の全体像 (ii) 発送のスケジュール及び輸送プラン（使用済燃料の海上輸送のルート及び量は，非公開である．使用済燃料の海上輸送のスケジュールは，最終の発送が終了してから 10 日後に公表することができる） (iii) 輸送手段における固定化装置，侵入警報アラーム，及び通信系の詳細 (iv) 地元警察の応援部隊の詳細及び能力，並びに安全な避難所の位置 (v) 無線通信の制約に関する詳細 (vi) セーフガード上の緊急事態への対応の手続
検査，監査及び評価	国家安全保障上法あるいは秘密データとして分類されない情報であって，保障措置に関わる検査及び報告	(i) 保障措置に関する検査レポート，評価，査察又は調査であって，①事業者又は申請者の物理的セキュリティ・システムの詳細を含むもの，あるいは②その物理的セキュリティ・システムの改善されていない欠陥，弱点及び脆弱性を明らかにするもの．欠陥，弱点及び脆弱性に関する情報は，それらが改善された後に公表することが許される．調査レポートは，調査が終了してから公表することが許される．但し，例えば情報自由法(Freedom of Information Act)(5 U.S.C. § 552)のような他の優先する規定がある場合には，この限りではない

出典：田邉（2008）p.10.

とは直接関連しないためセーフガード情報とはされない情報であっても，テロの未然防止等の観点から非公開であることが望まれる情報がある．米国ではこれらの情報は「非セーフガード機微情報」と定義され，（それらの情報が規制当局である NRC に提出された場合に）情報自由法（情報公開法）（Freedom of Information Act：FOIA）に基づく公開請求の対象とされないための措置が講じられている（RIS 2005-26, RIS 2005-31）．

本章では，それぞれの情報管理の仕方について概要を述べ，その特色を明らかにする．

2.1. セーフガード情報の保護とアクセス

（1）規制の内容

原子炉運転許可を受けた者や SSNM（Strategic Special Nuclear Material）（ウラン 233，ウラン 235 及びプルトニウム 239）を一定量以上保有する事業者等は，「情報保護システム」(information protection system) の構築を通じてセーフガード情報を保護しなければならないとされる (10 CFR § 73.21(a)).

a. セーフガード情報の定義

10 CFR § 73.2 定義規定 (a) は，セーフガード情報を次のように定義する．

> 国家安全保障情報（National Security Information）又は「制限されたデータ」（Restricted Data）として分類される情報以外の情報であって，業者又は事業申請者に属する，次の詳細情報をいう．(1)特殊核物質（special nuclear material）[i]の物理的防護のためにとられるセキュリティ上の措置についての詳細情報，又は(2)製造設備若しくは利用設備（production or utilization facility）の安全性維持に極めて重要な役割を果たすある種の設備（plant equipment）の物理的防護及び位置に関するセキュリティ上の措置についての詳細情報.

また，保護の対象となる情報の類型やその（ある程度までの）具体的内容は，10 CFR § 73.21 (b)によって規定される（Table 1 に整理）．後述のように，本規定は実務では例示的なものとみなされ，各事業者は自らが策定した管理プログラムの下で，各施設毎にセーフガード情報の内容・範囲を設定（詳細は非公開）している．

b. セキュリティ・クリアランス

NRC 規則は，セーフガード情報を保護するために，その人的アクセスに関してセキュリティ・クリアランス（そのポストで扱う秘密情報等へのアクセスを認めるために要求される資格調査，信頼性確認）の制度を設けている．

セーフガード情報へのアクセスが認められるアクセス権者は，次に列挙する地位・資格・団体に該当又は所属する個人であって，当該情報を「知る必要」（need to know）がある者に限られる（10 CFR § 73.21(c) を一部抜粋）．

① 従業員，代理業者，事業者又は事業申請中の者の請負業者，原子力規制委員会，合衆国政府
② 議会における正式な委員会のメンバー
③ 州知事又は州知事によって任命された者
④ 合衆国及び国際原子力機関 (IAEA) 間の保障措置協定に関連した活動に従事する国際原子力機関の代表

者であって，NRC の認証を受けた者
⑤ セーフガード上の緊急事態において支援を要請される州及び地方の警察当局
⑥ NRC 規則の下で NRC スタッフに対して情報開示が義務づけられている個人

また，上記アクセス権者が情報に実際にアクセスする際には，NRC 規則の定めるチェックを受けることが要求される．同規則は，事業者に対して，これらの者の情報アクセスに際し，原則として①指紋採取及び②FBI から提供された情報に基づく犯罪歴チェックの二つを実施することを求めている（10 CFR § 73.57(b)．但し，NRC 従業員等，指紋採取が不要とされる例外もある）．

なお，アクセス権者のうち，従業員等の，原子力発電施設の防護区域への「付き添い無しアクセス」（unescorted access）が認められる者は，これらに加えて，別規定（「原子力発電施設のための従業員アクセス承認」）に基づくセキュリティ・クリアランスを事業者から受けることとなる（10 CFR § 73.56）．NRC 規則は，その審査項目として，①就業履歴（失業期間も含む），②兵歴，③犯罪歴，④信用状態（借金等），⑤学歴，⑥照会先へのインタビュー調査，⑦薬物及びアルコールに関する初期審査，及び⑧心理状態に関する初期審査，を含めることを要求している（10 CFR § 73.56(b)(2)）．

上記のセキュリティ・クリアランス制度に加えて，NRC 規則は，事業者に対して，情報アクセスを必要とするすべての自社従業員及び請負業者従業員を対象に，情報管理のためのトレーニングを実施することを義務づけている（10 CFR § 73.21 (b)(1)(ix)）．

（2）事業者の対応（セーフガード情報管理プログラム）

先述のとおり，NRC 規則は，セーフガード情報保護のため，各事業者に「情報保護システム」構築を義務づけるが，このシステムは，実務では「セーフガード情報管理プログラム」（SGI Control Program）と呼ばれる．なお，プログラムの内容自体がセーフガード情報に該当し，非公開である．これは，潜在的脅威に対して対抗・回避手段探索の機会を与えないようにするためである．

セーフガード情報管理プログラムは，各事業者毎に個別に策定されるが，情報管理手続面に関しては，事業者間でその違いが殆ど見られない．これは，①NRC による査察を通じて一定水準の管理手続の構築が確保されること，②米国では事業者が異なる複数の原子力発電所の施設運営・管理を行う専門会社があり，その会社が各発電所間で統一された情報管理手続を策定していること，③業界団体である米国原子力協会（Nuclear Energy Institute：NEI）及びそこで策定される民間ガイドライン等を通じて各事業者のベスト・プラクティスが共有されていること，等の理由に因る [ii]．ガイドラインについては，原子力施設や情報へのアクセスを規定する非公開の諸ガイドラインが NEI によって策定されており，これらは NRC のレビューを受けることによって，その規制適合性も確保されている（田邉（2008）pp.7, 24-25.）

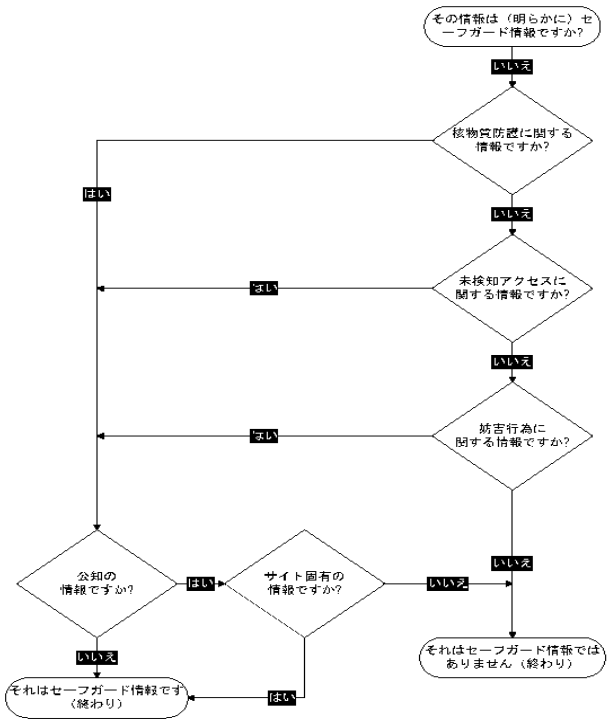

Fig. 1　NMC 社によるセーフガード情報区分

出典：田邉（2008）p.12.

a. セーフガード情報の内容・範囲

セーフガード情報の具体的内容・範囲は，セーフガード情報管理プログラムに基づき各事業者毎に設定されるが，そこでは，情報がセーフガード情報に該当するかどうかを判別するための様々な仕組みが取り入れられている．例えば，原子力発電所の施設運転・管理会社である Nuclear Management Company（NMC）社は，10 CFR § 73.21 (b)（Table 1）よりもさらに詳細なセーフガード情報の類型を例示するとともに，当該情報がセーフガード情報に該当するかどうかを社内的に判断するためのフローチャート（Fig. 1）を用意している [ii]．

もっとも，どの情報がセーフガード情報に該当するか，を判断することは，必ずしも容易ではない．そこで，NRC は，2005 年 9 月 30 日にセーフガード情報として分類すべき文書の区分を示した非公開の指針（DG-SGI-1 NRC's Designation Guide for Safeguards Information）を発行した．

なお，一般的な実務対応では，10 CFR § 73.21 (b) で規定される内容よりも広い範囲をセーフガード情報に含め，保護対象としている．そこではその情報が①既に公知であるかどうか（公知性）と②脅威を利するものであるかどうか（利敵性）が基本的な判断基準とされており，そ

Table 2　セーフガード情報管理の実務例

管理項目	具体的な管理の方法
セーフガード情報文書の管理	付き添い人がいない場合には，施錠されたセキュリティ保管庫（施錠とともにアラーム・システムが設置されている保管庫）の中に保管されていなければならない.
セーフガード情報を作成するために用いられるラップトップ・コンピュータ又はデスクトップ・コンピュータ	承認なしのアクセスによって操作されないよう，パスワード保護されなければならない．加えて，セーフガード情報が記載されているフロッピー・ディスク及びリムーバブル・ハード・ディスクはセーフガード情報文書の場合と同様，安全な場所に保管されなければならない（コンピュータ本体も同様）．なお，セーフガード情報を作成するコンピュータは，ミラーリング（他の情報媒体等の自動バックアップ）機能を停止し，インターネット接続を切断しなければならない.
セーフガード情報の口頭伝達	セーフガード情報のアクセス時チェックを受けたアクセス権者に対してのみ，口頭伝達が可能．なお，情報の受け手には，「知る必要」の要件 (10 CFR§73.21(c)) が求められる.
電話や無線によるセーフガード情報の伝達	一定のメッセージ・フォーマットに拠るもの又は暗号に拠るものに限定.
セーフガード情報文書の伝達方法	①アクセス権者個人を介しての手渡し，②NRC による承認を得ている，保護された電気通信手段（ファクシミリも含む），③メッセンジャー・キャリア，事業者内メール，米国郵便公社の指定されたメール・システム（ファースト・クラス・メール，書留メール，速達メール又は内容証明メール）に制限される.
セーフガード情報文書の郵送の方法	必ず二重に封緘されていなければならない．内側の封には受取人の名前の記載の他，封の上部及び下部に「セーフガード情報」の刻印をすることが要求される．また，外側の封には「セーフガード情報」の記載をしないことと，それが不透明であることとが要求される.
セーフガード情報文書の複写	コピー機を利用しての複写は必要最小限にとどめること．セーフガード情報文書を含む複数ページの文書の複写を行う場合には，予め専用の機械を用いて，セーフガード情報文書とそうでない文書との分別（セーフガード情報文書には「セーフガード情報文書」との刻印をすることが義務づけられるので，それを目印に機械分別がなされる）を行わなければならない.
セーフガード情報文書等の破棄	セーフガード情報を含む文書を破棄する際には，それが二度と復元されることのないよう，裁断又は焼却されなければならない．また，フロッピー・ディスクやハード・ディスクの場合はフォーマットだけでは不十分で，物理的に破壊されなければならない.

出典：田邉（2008）p.14.

れが核物質防護に関する情報であるかどうかについては詳細な判断基準が設定されているわけではない [ii]．このように，事業者は自社のセーフガード情報の内容・範囲の設定に関して，「安全サイド」での運用を図っている.

b. 情報管理とセキュリティ・クリアランスの方法

先述のとおり，セーフガード情報管理の手続に関しては，各事業者でその内容に統一性が見られ，とりわけ文書や電子情報の管理については，概ね Table 2 に示すような方法が実務では採用されている [ii].

一方，アクセス権者のセキュリティ・クリアランスに関しては，NRC 規則（10 CFR § § 73.56(b)(2), 73.57(b)）で要求される内容以上のものが実務では審査対象とされる．例えば，アクセス権者のうち，原子力発電施設の防護区域への「付き添い無しアクセス」が認められる者の選別に関しては，個人の性格や人物評等も調査・審査対象とされる．また，Exelon 社のように，公民権，本人確認のための人種的特徴，社会保障番号，運転免許証番号，労働組合加入歴，銀行口座，利害関係にない 4 人の照会人の連絡先等，センシティブ・データ（国際的な水準として特別な配慮と取扱いが必要とされる個人情報）を含む数多くの調査・審査項目が要求される実務例もある [2]．なお，これらの調査・審査は，本人による書面での同意の下に実施される [2]．ただし，潜在的脅威に対して対抗・回避策探索の機会を与えないようにするために，事業者によって設定される調査・審査項目のうち幾つかの詳細事項は非公開とされる．調査項目の詳細がわかれば虚偽情報を事前に用意することが可能であるし，利用する身元調査機関がわかればそれへの買収が可能となるからである．このため，実務でどのような人的情報が調査・審査の対象とされているかについては，不明な点も多い.

こうして得られた犯罪歴情報を含む個人情報と指紋押捺の管理には，「従業員アクセス・データ・システム」（Personnel Access Data System：PADS）と呼ばれる従業員情報の共有・管理システムが利用されている．PADS は，NEI によって管理・運営される会員企業（事業者）間の情報共有システムであり，情報の一元的管理による移動労働者対応と事業者負担の軽減（PADS 上の情報照会により，移動労働者の信頼性確認が可能）を図っている．PADS を通じて共有される従業員個人情報には，セキュリティ・クリアランスに関する一連の個人情報の他，訓練情報や健康（放射線被曝）管理情報等がある [3].

c. 請負業者に対するプログラム策定要求と監査

原子力業務の遂行の過程で，セーフガード情報へのアクセスは，事業者の従業員のみならず，請負業者の従業員によってもなされる．このため，実務ではすべての事業者のセーフガード情報管理プログラムが，その事業者のサイト以外の場所でセーフガード情報にアクセスする必要のある従業員を擁する請負業者に対して，事業者と同等レベルの管理プログラムをその所在地において策定・実施することを要求している．そこで策定される請負業者のプログラムも，10 CFR § 73.21 等のすべての NRC 規則の要求事項を満たさなければならないとされる．さらに，請負業者のプログラムは契約先である事業者による監査を受けなければならない.

2.2. 非セーフガード機微情報の管理

（1）規制の内容

事業者から NRC へは，施設安全規制等の下で様々な情報が提供される．その多くは，原子力施設や放射性物質の物理的セキュリティとは直接関連性のない，設計，オペレーション等に関わるものであり，これらの情報は，営業上の秘密等，情報自由法の適用除外事由の対象とされない限り公開対象となる．しかし，9・11 同時多発テロ以降，インターネット等の公開情報媒体を通じて得られる原子力関連情報の幾つかが，脅威にとって有益な情報であるとの懸念が示されるようになり[4]，NRC においても何らかの対策を講じることが必要となってきた．

そこで，2005 年 NRC は，法令の下で厳格な情報管理が要求されるセーフガード情報に該当しない情報であっても，安全保障やテロ未然防止等の観点から非公開とすることが望まれるものについては，これを「非セーフガード機微情報」と定義し，その保護及び管理を事業者及び（NRC 自身をも含む）行政各機関に要請するに至った．この要請は，法的拘束力のある NRC 規則ではなく，「規制問題サマリー」（Regulatory Issue Summaries : RIS）と呼ばれる一種の指針，あるいは将来的な規制導入を見据えたパイロット・プログラムの形でなされている．

「非セーフガード機微情報」の保護に関わる RIS は，次の二つの文書から構成されている．

① RIS 2005-26 「原子炉に関して秘密扱いされていない非セーフガード情報に対するコントロール」
② RIS 2005-31 「NRC の核原料物質、核副生物及び特殊核物質の規制に服する物質を使用する個人事業者及び法人による、秘密扱いされていない非セーフガード情報の取扱いの安全確保のコントロール」

これらの指針の主な目的は，事業者が NRC に提供した「非セーフガード機微情報」が情報自由法の下での情報公開請求手続を通じて一般に公開されることを未然防止することにある．

このうち，RIS2005-26 は，非公開とされる機微情報の区分と内容を示し（Table 3），事業者から NRC に対して提出されたこれらの情報を情報公開の対象から外した．

一方，RIS2005-31 は，上述の RIS2005-26 の規定内容が事業者の発電所運転業務と NRC の規制行政の中で担保されるようにするために，事業者や NRC が講ずべき具体的措置や手続等を定めている．具体的には，①NRC から各事業者への機微情報のスクリーニング基準（例えば，RIS が規定する一定量以上の放射性物質の位置やその遮蔽装置の製造番号等が機微情報とされる）の提示，②事業者に対する，機微情報文書へのマーキングと NRC 提出文書からの削除要請，③事業者に対する機微情報の適正管理要請，である。

Table 3　RIS2005-26 によって非公開とされる「非セーフガード機微情報」の区分

区　　分	内　　容
保護された重要インフラ情報（Protected Critical Infrastructure Information：PCII）	国土安全保障省に任意に提出された、重要インフラのセキュリティに関する情報
エネルギー関連重要インフラ情報（Critical Energy Infrastructure Information : CEII）	連邦エネルギー規制委員会規則により、エネルギー関連インフラ（例えば水力発電ダム、系統等）に関する情報と定義されるもの
機密セキュリティ情報（Sensitive Security Information: SSI）	運輸保安局及び運輸省の規則により、パイプラインを含む輸送資産（transportation assets）のセキュリティに関する情報と定義されるもの

出典：RIS2005-26 をもとに筆者（田邉）が作成

（2）事業者の対応[ii]

RIS は法的拘束力を持たないが，事業者はそれへの対応として，従前は保護対象とはされていなかったこの種の機微情報についても，管理施策を講じるようになった．

セーフガード情報の管理の場合とは異なり，非セーフガード機微情報の管理には，各事業者間で方法の相違が見られる．具体的には，①先述の RIS2005-31 によって推奨される，文書選別とマーキングの他，②電磁的に記録されている機微情報への従業員アクセスを制限する方法や，③潜在的に機微であるとみなされる情報に関して，その複製，配布及び廃棄方法について社内管理規定を設ける等の方法があり，一部事業者においては，RIS で奨励されているものよりも厳しい管理措置を講じている．

なお，情報選別・管理の過程において，機微情報である潜在的可能性のある情報に遭遇した場合，殆どの事業者が，その都度 NRC に対して，当該情報が RIS にいう「非セーフガード機微情報」に該当するかどうかについての問い合わせを行っており，慎重な対応を図っている．

2.3. 米国における秘密情報管理の特色

以上の制度概観から，米国原子力事業における秘密情報管理の先行導入事例の特色を抽出すると以下のとおりとなる．

（1）法令・指針類を通じた要求事項等の一定範囲内での詳細化・可視化

米国原子力事業の秘密情報管理制度においては，秘密情報の範囲や事業者に要求される情報アクセス管理の手順等が，法令（NRC 規則）や指針類を通じて，ある程度詳細に規定されている．すなわち，秘密情報とされるセーフガード情報の類型と内容が 10 CFR § 73.21 (b)によって相当程度詳細に規定される（Table 1 参照）他，同情報へのアクセス管理については，10 CFR § 73.21(c)の下でアクセス権者が同定されるとともに，10 CFR § 73.57(b)の下で事業者が実施すべきアクセス時チェックの内容が規定されている．また，このような要求事項は，NRC 規則

の形式にとどまらず,「非セーフガード機微情報」の管理の例に見られるように，指針類（RIS）によっても規定され，それが NRC 規則の不十分な点の補完と，情勢変化への即応的な規制行政の対応とを可能としている.

このような，法令・指針類を通じた要求事項等の詳細化・可視化は，内容の曖昧さを排し規制運用の不確実性や恣意性をなくすという点で，事業者の規制対応・遵守を容易にする他，規制対象及び内容の範囲を明確に社会に向けて示すことにより，特定情報が非開示となる説明責任を社会に対して果たしているものと評価できる.

しかしその一方で，先述のように，これらの内容を過度に詳細規定化し可視化することは，潜在的脅威に対して規制回避･対抗手段探索の機会を与える危険性がある. そこで，米国の制度は，内容を詳細規定化する場合であってもそれを一定の範囲内にとどめる（例えば,「付き添い無しアクセス」可能な人員のセキュリティ・クリアランスを規定する 10 CFR § 73.56(b)(2)は，必要最低限の審査項目のみ列挙している）他，NRC 規則に加え非公開の指針等（例えば，先述の DG-SGI-1 NRC's Designation Guide for Safeguards Information）を策定し，脅威への対応を図りつつ，規制内容の整備を図っている.

このように，米国原子力事業の秘密情報管理においては，法令・指針類を通じた要求事項等の詳細化・可視化によって，秘密情報管理行政の予測可能性と透明性（説明責任）を高める一方で，セキュリティの観点からそれらを一定の範囲内に収めるという形で，両者のバランスが図られていると評価できる.

（2）民間主導による管理水準の形成と事業者横断型管理支援システムの構築

事業者・発電所間で，セーフガード情報管理プログラムの統一性と規制適合性とが確保されているが，そこでは，NRC の査察といった規制行政に加えて，原子力発電所の施設運営・管理を行う専門会社や NEI といった民間企業・団体が大きな役割を演じている. とりわけ業界団体である NEI は，事業者のベスト・プラクティスに基づくガイドラインの策定等を通じて，規制対応・管理水準の「相場観」を形成する（田邉（2008）pp.4-5, 7.）他，PADS の構築・運営を通じて，事業者の規制対応実務（移動労働者の信頼性確認）を支援する等，実質的に規制行政を補完する重要な役割を担っているものと評価できる.

このような民間主導の情報管理態勢は，社会情勢変化や脅威に対する柔軟・即応的な対応を可能とする他，具体的措置内容の秘匿を実現するため，たとえ内容の詳細化を図ったとしても，潜在的脅威に対して対抗・回避手段探索の機会を与えないですむといった利点を有する.

もっとも，各事業者のプログラムの規制適合性は，NRC の査察によって最終的に担保され，また従業員信頼性確認の際の犯罪歴情報は連邦政府（FBI）によって収集・提供されている等，このような国による裏付けがあってはじめて民間主導型の情報管理態勢の実効性が確保されていることに留意する必要がある.

（3）秘密情報管理の実効性確保のための様々な措置の導入

米国原子力事業の秘密情報管理制度では，実効性確保のための様々な措置が法令等によって事業者に義務づけられる他，事業者によっても自主的に導入されている. とりわけ注目に値するものは以下の二点である.

第一に，NRC 規則の下で，事業者は自社従業員のみならず請負業者従業員についても情報管理トレーニングを実施することが義務づけられる（10 CFR § 73.21 (b)(1)(ix)）. 加えて，実務では，事業者が関係請負業者に対して自社水準の情報管理プログラムの導入を義務づけるとともに，その監査を実施するという運用がなされている. これらによって，事業者のみならず，請負業者やその従業員からの情報漏洩の未然防止が図られ，秘密情報管理の実効性が高められている.

第二に，米国の秘密情報管理制度においては，情報管理・伝達手段やデータ破棄の方法の指定等といった物理的な対策に加えて，情報アクセスに係る人員の信頼性確認といった人的対策が重要な地位を占めており，情報管理の実効性確保における重要な役割を担っている. すなわち，NRC 規則の下で情報アクセス権者が制限され（10 CFR § 73.21(c)），それらの者による情報アクセスに際しては，指紋採取と犯罪歴チェックが要求される（10 CFR § 73.57(b)）他，情報アクセス権者のうち施設防護区域への「付き添い無しアクセス」が認められる者については，身元・人物調査等の信頼性確認が事業者によって行われる. この信頼性確認では，実務においては，信用状態や薬物使用の有無等といった法令要求項目（10 CFR § 73.56(b)(2)）のみならず，人物評・性格チェックや労働組合加入歴といった広範な内容に及ぶ従業員個人情報が調査・審査の対象とされ，事業者によって捕捉されるとともに PADS を通じて事業者間で共有される. このように，米国の原子力事業では，物理的対策に加えて厳しい人的対策を講じることによって，セーフガード情報が潜在的脅威の目に触れたり，あるいは渡ったりすることを未然防止し，秘密情報管理の徹底を図っている. しかしその一方で，センシティブ・データを含む広範な内容の従業員個人情報が捕捉・共有される等，ある種の業務に携わる従業員は，対事業者及び産業との関係において，そのプライバシーが（先述のように，本人同意に基づいてはいるものの）制約されている面もある.

3.　我が国原子力事業への含意と課題

本章では，前章で述べた，米国原子力事業における秘密情報管理の運用実態とその特色の分析を踏まえ，我が国への含意と課題について述べる．

もっとも，米国の先行導入例をそのままの形で我が国に導入することは実際問題として困難であるし，また適切でもない．なぜならば，米国の原子力開発利用の起源が軍事利用であるのに対して，我が国のそれは今日に至るまで平和利用に徹している等，原子力開発利用を巡る歴史的経緯が日米で大きく異なっており，米国固有の社会的･歴史的文脈の中で形成されてきたこれらの制度が，我が国でそのまま機能するとは思われないからである．

しかしながら，9･11 テロ以降，原子力施設等を含む，重要インフラにおけるテロ対策要請が国際的な高まりを見せる中で，これらの施設における秘密情報管理を実効性ある形で行うことは，我が国の国家安全保障上の最重要課題の一つであることはもちろんのこと，国際社会の中で期待されている責務の一つであるともいえる．例えば，万が一我が国の原子力施設から秘密情報が漏出し，保管中の核物質が国際テロ組織の手に渡ったり，あるいは施設が外部からの攻撃の対象とされたりした場合の国際社会に与える影響は非常に大きいと考える．

加えて，我が国における原子力開発利用の目下の最重要課題である，再処理施設の稼働と MOX（ウラン・プルトニウム混合酸化物）燃料を利用したプルサーマル計画の着実かつ確実な実現を図るためには，秘密情報管理を含む，国際水準から見て遜色のない核セキュリティ対策が我が国でも実効性ある形でとられていることを，我が国は世界に対して明示しなければならない．なぜならば，我が国のプルトニウム平和利用に関して，核セキュリティ上の懸念を国際社会に抱かせることは，(その懸念が正当であるかどうかに関わりなく）その平和利用にとって大きな阻害要因となり得るからである．

そこで，以下では，先ず我が国における原子力の秘密情報管理に関する現況とその問題点を指摘した後，先の **2.3.**で抽出した米国の秘密情報管理の三つの特色を我が国の現状に照らし合わせてどのように評価すべきであるか，また，これらの特色から示唆を得る形で我が国における制度設計を行う場合，どのような課題に直面することとなるか，について検討を加える．

3.1.　我が国の現況と問題点

（1）規制内容と実務の現況

先の **1.**で述べたとおり，我が国原子力事業における秘密情報管理法制は，平成 17 年 5 月に，原子力事業に関係するに対する核物質防護に係る秘密保持義務の導入（原子炉等規制法第 68 条の 3）という形で，核物質防護対策の強化の一環として整備された．

この秘密保持義務の実効性を確保するために，法令は義務違反者に対する罰則規定(原子炉等規制法第 78 条第 31 号）を設けるとともに，守秘すべき核物質防護秘密の概略を示し事業者にその管理方法（秘密の具体的範囲とアクセス権者の指定，漏洩防止策）の策定を義務づけた（実用発電用原子炉の設置, 運転等に関する規則(以下、実用炉規則）第 15 条の 3 第 2 項第 15 号等)．そして，事業者の管理方法の適正性を担保するために，国（原子力安全・保安院）が情報管理要領作成指針（非公開）を策定して核物質防護秘密の具体的範囲等を示し，それに従って各事業者が情報管理要領を策定していることを国の専門家委員会（核物質防護秘密監査委員会）が確認する（核物質防護秘密監査委員会設置要綱第 2 条第 1 号）という仕組みをあわせて導入した．また，各事業者の指定した核物質防護秘密の範囲に関しては, 国が確認を行い，その確認の妥当性につき核物質防護秘密監査委員会が監査を行うという体制(同要綱第 2 条第 1 号)をつくった．なお，同監査委員会の議事録は非公開であり，議事要旨だけが公開される [5]．

規制対応として，各事業者は，情報管理要領（非公開）を定め運用を開始している. 平成 17 年 11 月 15 日に開催された第 2 回核物質防護秘密監査委員会では，各原子力事業者の策定した情報管理要領が，情報管理要領作成指針要件に沿った規定が盛り込まれていることが確認されている（「第 2 回核物質防護秘密監査委員会議事要旨」)．

また，作成指針に基づき各事業者が指定した核物質防護秘密の範囲に関する原子力安全・保安院の確認において，同院は，平成 20 年 3 月 25 日時点で，同秘密の指定件数が 412 件（重複指定を除く種類数は 319 種類）であることを確認している(「第 3 回核物質防護秘密監査委員会議事要旨」). 平成 17 年 11 月 15 日の第 2 回核物質防護秘密監査委員会開催時での指定件数が 295 件 (210 種類）（第 2 回議事録要旨）であったことを踏まえると，核物質防護秘密の範囲は事業者の規定対応・運用を通じて，今後とも拡充されていくものと見込まれる．

なお，同確認を監査する核物質防護秘密監査委員会では，委員より「秘密とすべき情報は，その情報を管理する手段が変わっても，情報自体が存在するのであれば，秘密として指定することが必要である」及び「秘密とすべき情報の管理方法（集中管理，分散管理）は，更に運用状況を見ていく必要がある」との意見が出されており（第 3 回議事要旨)，これらから，各事業者における秘密情報管理の方法については，一部で今なお試行錯誤的な取り組みがなされていることが推察される．

(2) 詳細法令の不在に起因する問題

我が国原子力事業における秘密情報管理は，ガイドラインと要綱行政によって，制度運用の妥当性確保と事業者対応への支援が図られてはいるものの，事業者のとるべき情報管理方法を規定した法令は不在である．このため，以下のような問題が生じ得る．

a. **事業者対応の困難性（法適用の予測可能性の阻害）**

法令不在の下では，各事業者が自ら講ずべき情報管理方法の具体的内容を直ちに同定し，それを業界標準として実施に移すことが必ずしも容易ではない．このため，事業者はどの程度の措置を講じれば，法令に適合したことになるか，についての「予測可能性」を得ることができない．法適用の予測可能性が阻害されれば，関係する具体的な業務遂行も阻害されることとなる．今なお情報管理方法に関して現場で試行錯誤的な取り組みがなされていると推察されることは**(1)**で述べたとおりである．

b. **制度運用の適正性・一貫性確保阻害のおそれ**

実際の制度運用で，行政が恣意的な運用を行うことは殆ど考えられないものの，秘密情報管理における規制ではその対象（情報の種類，情報アクセスがなされる現場等）が広範に及ぶ可能性もあり，規制判断の基準がある程度詳細・明瞭に定められていないと，ともすれば検査官等規制担当者の判断と資質の差異等によって，制度運用の適正さや一貫性が確保できなくなるおそれがある．

c. **秘密保持を理由とした，透明性確保阻害への懸念**

情報管理要領作成指針の内容や国による確認等（各事業者の指定した核物質防護秘密の範囲に関して国が確認を行い，その妥当性を核物質防護秘密監査委員会が監査するという一連の手続）の妥当性を判断することがともすれば難しい．このため，秘密保持を名目に，過度な秘密指定がなされたり，事故・事象発生の際に不適切な情報の秘匿がなされたりするのではないか，という懸念や悪感情を社会にもたらすおそれがある．**(1)**で述べた，事業者における核物質防護秘密の指定件数･種類の増加も，このような懸念に拍車をかける可能性がある．例えば，第 162 回衆議院経済産業委員会における原子炉等規制法の改正（平成 17 年改正）の議論の中で，塩川鉄也委員は松永和夫政府参考人（経済産業省原子力安全・保安院長）に対して，秘密の範囲が国と事業者に「白紙委任」されている下では，「無限定な守秘義務」が「徹底した情報公開」を通じた安全対策と信頼回復を阻害する可能性があるとの懸念を示している（第 162 回衆議院経済産業委員会会議録第 13 号，平成 17 年 4 月 22 日）．

d. **安全保障上問題となる情報開示の懸念**

上の **c.**の問題とは逆に，「徹底した情報公開」の姿勢が，法令不存在の下では，行政や事業者による，国家安全保障上問題となり得る情報の不用意な自発的開示に繋がる危険性もある．現在，原子力情報の積極公開を通じた原子力安全の維持向上と原子力推進の透明性確保が社会的に強く要請されており，行政及び事業者もまたこうした要請に積極的にコミットしている．しかしながら，法令不在の中で，行政や事業者が万が一判断を誤って，安全保障上問題となり得る情報を公開してしまう（これには，国や地方自治体が国民・住民の情報公開請求に応じる形で当該情報を公開してしまう場合も含まれる）ならば，国家安全保障にとって重篤なリスクとなる．

(3) その他の問題点

我が国の原子力事業では，米国で見られるような，民間ガイドラインを通じた業界内での管理水準の形成や，移動労働者信頼性確認を支援する従業員情報の共有・管理システムの導入は図られていない．すなわち，秘密情報管理に関する原子力産業全体での組織化された取り組みが十分にはなされていない．もっとも，業界内での管理水準の形成に関しては，非公式又は非公開な形での情報交換等が事業者間でなされているものと見られる．

また，情報管理の実効性確保のための措置に関しても，米国で導入されているような，情報アクセス権者のセキュリティ・クリアランス（情報管理における人的対策）や協力会社等における情報管理の徹底といった取り組みについては，我が国ではその重要性は指摘されてはいるものの，官民あげての十分な体系的検討が未だなされていないのが実情であると思われる．

3.2. 法令・指針類を通じた要求事項等の詳細化・可視化の是非

3.1.(2)で指摘した，詳細法令の不在に起因する問題を解決するために，米国の先行導入例に見られるように，我が国においても一定の範囲内で規制・指針内容の詳細化と可視化を図るべきか．

(1) 規制・指針内容の詳細化・可視化の意義と限界

規制・指針内容の詳細化と可視化は，以下に示すような形で，**3.1.(2)**の各問題点の克服・緩和に繋がり得る．

① 法適用の予測可能性を高め事業者対応を容易にする．
② 規制担当者に明瞭な運用上の基準を与えることに繋がり，制度運用の適正性・一貫性の確保に資する．
③ 秘密情報管理に係る国及び事業者の一連の手続に明瞭な法的縛りをかけることにより，社会が国や事業者に対して抱く透明性確保阻害への懸念や，社会が核物質防護秘密保持制度そのものに対して持つであろう不安感や懸念を払拭・緩和することができる．
④ 安全保障上問題となる情報の内容を明瞭な形で行政及び事業者に伝えることが可能となり，同情報が開示されるリスクを減じることができる．

また，上記に加え，核物質防護秘密保持に係る一連の

手続を（ガイドラインと要綱行政ではなく）法令レベルで規定することは，後の **3.4.(1)**で述べるように，アクセス権者選定時等における個人情報取得の際の法的根拠を提供することにも繋がる．

しかし，規制・指針内容の詳細化と可視化には以下の問題と限界がある．

第一に，秘密情報の具体的内容や，情報管理において要求される具体的措置（方法）を法令レベルで詳細に規定すればするほど，何が国家安全保障上重要な情報であり，それらがどのような方法で管理されているか，が公知となり，潜在的脅威に対して規制回避や対抗手段等の探索の機会を与えることに繋がる．このため，米国では，内容を詳細規定化する際に，非公開の指針を定める等して，法令化を通じてそれが公知とならないような工夫をしていることは既に指摘（**2.3.(1)**）したとおりである．

第二に，法令整備を通じた規制内容の詳細化は，法令整備・改定に係る手続の煩雑さ等から，社会情勢の変化に対する即応的な対応を阻害するおそれがある．

第三に，法令や指針が，業務上想定し得るすべての情報についてその内容を掌握した上で，どの情報が秘密指定を受けるか，を予め決めておくことは，実際問題として不可能に近い．**3.1.(1)**で述べた，事業者における核物質防護秘密の指定件数・種類の増加は，この種の規制内容が実務運用の実績の中で蓄積・確定されるべき性質のものであることを如実にあらわしたものであると理解することも可能である．

(2) 考察と結論

以上のように，秘密情報管理について規制内容の詳細化と可視化の徹底を図ることには，本来的に一定の限界がある．特に問題となるのは，規制内容の詳細化・可視化を通じた秘密情報管理行政の予測可能性及び透明性の向上と，詳細規制内容の秘匿化というセキュリティ上の要請とのバランスをどのように図るか，という点である．

私見では，秘密情報管理行政の予測可能性と透明性をこれまで以上に高めるという観点から，現行制度よりも規制内容の詳細化・可視化をすすめるべきであると考えるが，その具体的な規定の仕方は，米国の NRC 規則で定められている水準程度のもの（例えば，NRC 規則（10 CFR § 73.21 (b)）の定めるセーフガード情報の類型と内容等。**Table 1** 参照）までに制限し，慎重に法令化を図るべきであると考える．具体的には，事業者の定める情報管理要領や核物質防護秘密の範囲に対する国によるコントロールの手続や根拠（現行では，核物質防護秘密監査委員会設置要綱第 2 条第 1 号）については，命令（省令）レベルでより詳細化・可視化を図ることが望ましいと考えるが，その一方で，情報管理要領作成指針は現行のように非公開にとどめておくべきである．

加えて，規制内容の詳細化・可視化をすすめるに際しては，行政と事業者とが協力して，国際情勢（例えば，IAEA ガイドラインの改正動向等）や諸外国の法令を参考にしながら，セキュリティの視点からの秘匿化との均衡を図りつつ，情報・アクセス管理等の内容を，現場の実務運用の実態を踏まえる形で，漸次具体化・整備していくことが必要である．また，国家安全保障上の観点から非公開とすることが望ましい指針類等の整備に関しては，それを非公開とすべき根拠及び理由の説明責任を果たした上で，非公開とすることが望まれる．

3.3. 民間主導による管理水準の形成と事業者横断型管理支援システムの構築の方向性

前節で述べたように，秘密情報管理に関する法令・指針類の徹底した詳細化には，一定の限界がある．したがって，秘密情報管理においては，規制行政を補完するものとして，事業者自身や原子力業界団体等といった，民間の取り組みが重要な役割を担うこととなる．

(1) 民間ガイドライン策定を通じた管理水準形成の意義

2.1.(2)で述べたように，米国では，秘密情報（セーフガード情報）管理における各事業者間での規制対応・管理水準の「相場観」の形成に，①事業者が異なる複数の原子力発電所の施設運営・管理を行う専門会社による，統一された情報管理手続の策定，②NEI 及びそこで策定されるガイドライン等を通じた各事業者のベスト・プラクティスの共有，が大きな役割を果たしている．我が国の場合，原子力発電所は各電力会社によって運転・管理されているため，①を通じた管理水準の形成を図ることは難しいが，②の方法は検討に値すると考える．

とりわけ民間ガイドラインの整備・活用は，法令や行政によるガイドラインと比較して，①現場と実務の実際を見据えた水準設定が可能となり，実務との乖離に伴う種々のリスク（例えば，現場による不適切な独自解釈等）を回避できる，②社会情勢の変化や IAEA ガイドラインの改正等といった変化に即応的に対応することができる，③措置として要求される項目自体の秘密が保持され，潜在的脅威に対抗手段等の探索の機会を与えずにすむ，等といった利点を有している．

我が国の原子力事業の分野では，NEI の例に見られるように業界団体が民間ガイドラインを行政の協力を得ながら積極的に策定し規制を補完していく，という先例が必ずしも確立されていない．このため，米国の先行例を我が国にそのまま導入することは必ずしも適切ではないが，秘密情報管理に関する民間ガイドラインを漸次構築していくことの意義は我が国においても大きく，検討に値する方法であると考える．具体的には，秘密情報に該

当する情報の選別とアクセス管理の具体的方策等に関して，民間団体や研究機関等が各原子力事業者の協力支援を仰ぎながらその内容・手順を策定し，行政がそれをレビューすることによって，専門技術的知見，実務との親和性，規制適合性を兼ね備えた民間ガイドラインを整備するといった方法等が検討されて良いと考える．

(2) 事業者横断型管理支援システム構築の必要性

2.1.(2)で述べたように，米国では，秘密情報管理の実効性を確保するとともに事業者の利便を図るために，各発電所の従業員個人情報が，事業者横断型情報共有データベース・システム（PADS）を通じて事業者・発電所を横断して情報共有され，従業員による情報アクセスの際のセキュリティ・クリアランスに利用されている．

終身雇用制に近い雇用形態をとる我が国原子力事業では，発電所の枢要業務を担い核物質防護秘密へのアクセスが必要となる従業員の事業者間の移動は殆ど見られない（同一事業者内における発電所間の移動はある）ものの，いわゆる季節労働者の事業者間移動はあり，これらの者が業務遂行上核物質防護秘密に関わるような事実（例えば，見張り人の配置位置，人数，交代時間等といった「見張人による巡視及び監視に関する詳細な事項」（実用炉規則第 15 条の 3 第 2 項第 15 号ホ）等）を知り得る可能性も否定できないことから，何らかの形でこれらの者についての情報を事業者間で共有しておく必要があると考える．また，このような情報共有は，身分や氏名等を偽る労働者の移動を防止することにも繋がる．

しかしながら，PADS 類似のシステムを我が国に導入する場合には, 以下の課題がありその対応が必要となる．

第一に，取得・共有すべき従業員個人情報の範囲の設定が問題となる．潜在的脅威等に対する情報漏出のリスクを下げるためには，米国の例に見られるように，センシティブ・データを含む広範な内容の従業員個人情報を取得・共有対象とすることが望ましいともいえるが，どの程度の範囲の情報まで事業者が取得し，情報共有データベース・システムに登録すべきであるか，については議論の余地がある．この問題は，セキュリティ・クリアランスの課題として，次節 **3.4.**で詳細検討を加える．

第二に，従業員個人情報の取得・共有と従業員プライバシーとの間の相克が問題となる．この問題もまた，次節 **3.4.**で検討する．

第三に，データベース・システムの捜査機関との共有を認めるかどうか, という問題がある. 米国の PADS は，あくまでも NEI が構築・運営する民間データベース・システムであり，そこに登録される従業員の犯罪歴データは，事業者からの求めに応じて FBI が事業者に対して提供したものに依拠している．すなわち，捜査機関との共有（接続）は図られていない．しかし，個人犯罪歴情報の照会の徹底を図るためには，システムを捜査機関と共有させたほうが良い，という考え方も一方では成り立ち得る．ところが，我が国では，捜査機関がこのような形で民間との間で情報共有を図る先例がない．また，そもそも公権力が第三者に対して個人犯罪歴情報を開示できるか，という問題もある（これについては後の **3.4.(1)a.** で詳細検討する）．さらに，捜査機関とデータベース・システムを共有させることについては，協力会社をも含む原子力事業者等の一般従業員の個人情報を捜査機関に晒すことに繋がるおそれがある他，逆に捜査機関への外部からの不正アクセスを招く危険性もあり得る．したがって，少なくとも現時点では，データベース・システムを捜査機関と共有することは困難であると考える．

また，これらの課題に加え，情報共有データベース・システムの構築にあたっては，それにアクセスできる者の選別，外部情報漏出及び不正アクセスへの人的・技術的対応を十分に講じる必要があることはいうまでもない.

以上のように，我が国で PADS 類似のデータベース・システムを構築・運用する場合には，様々な克服すべき課題があり, その実現は必ずしも容易ではない. しかし，情報共有システムの構築は，移動労働者間における万が一の潜在的脅威に対する有効な対抗策となる他，移動労働者の採用等に係る事業者等の負担を軽減させ，さらに米国のように被曝管理情報を登録させることによって従業員の健康管理面での保護をさらに増進させることにも繋がる．したがって，我が国でも，このような民間主導の情報共有データベース・システムの構築可能性について，そこで登録・共有すべき情報内容の精査をも含めた形で，検討をすすめていくことが必要であると考える．

3.4. 秘密情報管理の実効性確保のための措置についての課題とそれへの対応

2.1.(2)で述べたように，米国では，秘密情報管理の実効性を高めるため，情報アクセスをする者に対するセキュリティ・クリアランスが実施される他，事業者のみならず請負業者に対しても訓練の実施や情報管理プログラムの導入を義務づけている． 本節では，仮にこれらの措置を米国水準並みに我が国に導入するとした場合，どのような課題に直面するか，について検討を加える．

(1) セキュリティ・クリアランス

秘密情報管理の実効性を高める措置のうち，最も多くの課題を提起するのが，情報アクセスをする者のセキュリティ・クリアランス（信頼性確認）である．

a. 個人情報取得・利用とプライバシー権との相克

米国における実務運用では，犯罪歴情報や信用状態等の法令要求項目に加え，人物評・性格チェックや労働組合加入歴等といったセンシティブ・データを含む広範な

内容に及ぶ従業員個人情報が調査・審査の対象とされ，事業者によって取得されるとともにPADSを通じて事業者間で共有される．しかも，潜在的脅威への対策として，事業者によって設定される調査・審査項目のうちの幾つかは非公開とされており，内容を知ることができない．

このため，我が国において米国水準の従業員信頼性確認を行おうとした場合，広範にわたる個人のプライバシー情報が調査・審査の対象となる可能性があり，事業者による個人情報取得と従業員プライバシーとの間に相克の問題を生じさせることとなる（総合資源エネルギー調査会（2004）[6]p.12，文部科学省（2005）[7] p.5.）．

(i) 利用目的の明示と本人の同意

個人情報取得に係る合憲性（プライバシー権）を保障する仕組みの基本となるのが「利用目的の明示」と「本人の同意」である．なぜならば，プライバシー権の本質は，自己に関する情報を本人の自律した判断の下にコントロールさせるところにあり，①本人の自律した判断を可能とするための，利用目的の特定と本人へのその明示，そして②自己情報のコントロールの具体的方法としての，情報提供に係る本人同意が，個人情報取得とプライバシーとの相克を克服する手段となるからである．

(i-1) 個人情報保護法制

2.1.で述べたように，米国では個人情報の収集に際して，法令（10 CFR § 73.56(b)）や書面[2]を通じた利用目的・収集内容の明示と，本人同意の要請がなされている．我が国でも，個人情報の保護に関する法律（以下，個人情報保護法）等が，事業者等による従業員個人情報収集に関して，利用目的の特定・本人への明示と本人同意についての規定を置き，プライバシーとの調整を図っている．個人情報保護法及び関連指針は以下の要求事項を定める．

まず，利用目的の特定と本人への明示については，個別的・具体的でなければならないと規定する（個人情報保護法第15条，第18条第2項，厚生労働省「雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針」（以下，雇用管理個人情報指針）第3の1）．但し，「取得の状況からみて利用目的が明らかであると認められる場合」は，本人通知は不要とされる（個人情報保護法第18条第4項第4号）．

一方，本人の同意に関しては，「あらかじめ本人の同意を得ないで、（中略）特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない」（個人情報保護法第16条第1項）と規定し，特定された利用目的範囲内であれば本人同意を不要としている．もっとも，これに対しては，個人情報の中でも社会的差別の原因となるセンシティブ・データについては，原則として本人の同意のない取得は禁止されるべきである，とする厚生労働省指針（「労働者の個人情報保護に関する行動指針」[iii]）や学説（砂押（2005b）[8]）[iv]がある．また，「JIS Q 15001:2006 個人情報保護マネジメントシステム–要求事項」の「3.4.2.3 特定の機微な個人情報の取得，利用及び提供の制限」は，明示的な本人の同意がある場合及び法令に基づく場合に限り，思想・信条や保険医療情報等の取得・利用・提供を例外的に認めている．

なお，事業者が従業員の個人情報を第三者に提供する場合（米国におけるPADSの例に見られるように，他事業者と情報共有する場合等）も本人の同意が必要とされる（個人情報保護法第23条第1項）．

以上の本人同意に関して，雇用管理個人情報指針第3の2は，「事業者が労働者等本人の同意を得るに当たっては，当該本人に当該個人情報の利用目的を通知し，又は公表した上で，当該本人が口頭，書面等により当該個人情報の取扱いについて承諾する意思表示を行うことが望ましい」と規定する．また，これに関連して，利用目的の特定と本人への明示は個別的・具体的でなければならないとする個人情報保護法の趣旨に鑑み，本人同意も個別取得事項を明記した上でなされるべきであり，「その業務の目的の達成に必要な一切の個人情報」につき同意を得るといった包括的・抽象的な内容に対する同意は認められないとする学説もある（砂押（2005a）[9] pp11-12.）．

以上から，我が国において現行法や指針類に従う形で，米国並みのセキュリティ・クリアランスを導入・実施する場合には，個人情報収集に関する，個別的・具体的な利用目的の特定と本人への明示，そして個別項目毎の本人同意が必要となる可能性がある．

もっともその一方で，個人情報保護法は，先述の，特定された利用目的範囲内での本人同意なしの個人情報取扱いに加え，利用目的の本人への明示と本人同意に関して，以下の例外規定を設けている．

① 「法令に基づく場合」（本人同意）（第16条第3項第1号，第三者提供の場合につき第23条第1項第1号）
② 「人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき」（利用目的の本人への明示及び本人同意）（第16条第3項第2号，第18条第4項第1号，第三者提供の場合につき第23条第1項第2号）

このため，原子力事業での信頼性確認が，①原子炉等規制法等の法令によって規定された場合には，本人同意が不要とされ，また②テロ未然防止という観点から「人の生命、身体又は財産の保護のために必要がある場合」に該当すると判断される場合には，利用目的の本人への明示と本人同意が不要とされ得る[v]．

(i-2) 考察と結論

そもそも，我が国の原子力事業での信頼性確認において，「利用目的の明示」と「本人の同意」はそれを実施する上での必須の条件とされるべきか．私見では，これらはプライバシーとの相克を克服する手段として，実務に

おいて要請することが望ましいと考えるが，必須の条件とまでは必ずしもいえず，また，個別的・具体的な利用目的の特定と本人への明示，そして個別項目毎の本人同意についてまでは，要請すべきではないと考える．それは以下の理由に因る．

第一に，収集対象となる情報の項目を個別的・具体的に特定し，本人の同意を求めるためにそれを求職者に明示することは，潜在的脅威に対して対抗・回避手段探索の機会を与える危険性がある．このため，米国の実務運用でも，それらを詳細に特定・明示化することはない．

第二に，本人同意を前提とする制度とした場合には，自身のセンシティブ・データを含む個人情報が知られてしまうことへの抵抗感等から，従業員が同意を拒否したり，個人情報の正確な申告を行わなくなったりする等して，制度が機能しなくなるおそれがある．

したがって，私見では，個別的・具体的な利用目的の特定と本人への明示，そして個別項目毎の本人同意を不要とする（個人情報保護法第 16 条第 3 項第 1 号，第三者提供の場合につき第 23 条第 1 項第 1 号）ための，原子力事業における信頼性確認に係る法令を整備する必要があると考える．本人同意に要求される個別性・具体性の緩和（包括合意）を可能とする法令とするか，そもそもの本人同意を不要とする法令とするか，については議論の余地があるが，本人同意を全くの不要とする場合には，プライバシーとの相克やセンシティブ・データ取得との関係で，法令整備に際して慎重な議論を踏むことが望まれる．私見では，プライバシー権の重要性に鑑み，本人同意を全くの不要とするのではなく，一定範囲の包括合意で足りるとする法令整備のほうが望ましいと考える．

但し，このような法令整備を図っても，個人情報保護法との関係では，利用目的の特定・本人への明示は不要とすることができない（同法は，「法令に基づく場合」を，本人への明示の適用除外としない）．この点については，個人情報保護法の改正等も含め，何らかの法的措置をとることが必要とされよう．この場合も，利用目的の特定・本人への明示を不要とするのではなく，その個別性・具体性を緩和する方向で検討されることが望まれる．

もっとも，(i-1)で述べたように，原子力事業での信頼性確認が，テロ未然防止の観点から「人の生命、身体又は財産の保護のために必要がある場合」（個人情報保護法第 16 条第 3 項第 2 号，第 18 条第 4 項第 1 号，第三者提供の場合につき第 23 条第 1 項第 2 号）に該当すると判断される場合には，上述の法令整備や法改正を要せずして，利用目的の本人への明示と本人同意の双方が不要となる．しかしながら，本規定はいわば緊急避難的な例外規定と捉えるべきであり，原子力テロの危険性が無視し得ないほどに高まっている場合等を除き，これを拡大して適用することについては若干の疑念が残る．利用目的の本人への明示と本人同意の問題は，プライバシーとの相克に関わる重大な問題であるので，やはり国会での審議・立法を経た上でこれを不要とする（又はその個別性・具体性を緩和する）ことが望ましいと考える．

なお，個人情報保護法では，業界団体等の民間団体が認定個人情報保護団体として個人情報保護指針を策定する等して，個人情報保護の推進を図ることが規定されている（第 37 条以下）．これらの規定は義務規定ではないが，原子力事業において米国並みのセキュリティ・クリアランスが導入・実施された場合には，そこで収集される個人情報（センシティブ・データを含む）の重要性に鑑み，それらの適正な取扱いを担保すべく，業界はこれらの規定が予定する対応を図るべきであると考える．

(ii) 事業者による前科情報の照会と行政の対応

米国では，犯罪歴情報がセキュリティ・クリアランスの審査項目の一つとされ，FBI が事業者の求めに応じて，審査対象人物の犯罪歴情報を当該事業者に提供する．仮に我が国の信頼性確認制度において，利用目的の本人への明示と本人同意を不要とする立法がなされたとしても，米国の例に見られるような，事業者からの照会への対応としての行政機関から同者への犯罪歴情報の提供が許されるかどうか，について検討する必要がある．

これに関して，我が国では，「前科及び犯罪経歴（以下「前科等」という。）は人の名誉、信用に直接にかかわる事項であり、前科等のある者もこれをみだりに公開されないという法律上の保護に値する利益を有する」ため，「照会申出書に「中央労働委員会、京都地方裁判所に提出するため」とあつたにすぎない」ような場合に、行政庁が「漫然と弁護士会の照会に応じ、犯罪の種類、軽重を問わず、前科等のすべてを報告することは、公権力の違法な行使にあたると解するのが相当である」とした最高裁判例（最判昭和 56 年 4 月 14 日民集 35 巻 3 号 620 頁，いわゆる「前科照会事件」）がある．同判例からは，照会事由に厳格な正当性が具備されていなければ，公権力による前科情報の外部提供は許されない，とする姿勢が読み取れる [vi]．また，学説も「前科情報はプライバシー固有情報・センシティヴな個人情報の一つ」であり，公権力による開示が合憲となるためには，「内在的制約原理・他者加害阻止原理に基づく正当化事由を帯有していることが要求される」としている（竹中（2007）[10] p.45）．

したがって，我が国の信頼性確認制度において，事業者による行政機関への犯罪歴情報の照会と同者への情報提供が是認されるには，それが実効性ある内部脅威対策に繋がり，テロの未然防止という意味で他者への加害を阻止するのに必要とされる措置であるか，という正当化事由が問われることとなる．

私見では，事業者が当該従業員につき正確な犯罪歴を調査することは内部脅威を排除するための必要不可欠な

手段の一つであり，行政機関による正確な犯罪歴情報の提供は，この正当化事由を満たすと考えるが，これに異を唱える見解もあり得よう. 異を唱える見解がある以上，事業者及び行政が，訴訟リスクをおそれ，情報照会・提供を渋ったり，また事業者が不正確な犯罪歴情報に頼って判断を下したりする危険性がある.

このような事態を避けるためにも，先の(i)で述べた，個別・具体的な利用目的の本人への明示と本人同意を不要とするとともに，事業者による犯罪歴情報の照会と行政機関による回答の詳細要件及び手続を規定した，従業員信頼性確認に係る立法を国会での審議を経てその正当化事由を明らかにした上で行うことが望ましいと考える.

b. 取得すべき個人情報の内容とその取得方法

信頼性確認において取得すべき個人情報の内容は，秘密情報の漏出やそれを利用した内部的な破壊行為をもたらす危険性の高い人物（潜在的脅威）の排除の指標となる内容でなければ意味をなさない.

しかしながら，数ある個人情報の中から，潜在的脅威排除のための指標となる個人情報の内容を選択・同定することは，必ずしも容易なことではない．その内容は，国や時代によっても，異なるであろう．米国で採用されている調査項目，すなわち，薬物使用の事実，犯罪歴，信用状態（借金等）がそのまま我が国における潜在的内部脅威排除のための判断根拠となるかどうかについて，疑問も呈されている（資源エネルギー調査会（2005）[11] p.8.）．むしろ，それまで「ノー・マーク」であった人物や集団が脅威となることすら珍しくない.

また，それが反社会的なものである場合はともかく，特定の思想や信条を潜在的脅威排除のための指標とするならば，憲法の規定する信教の自由（日本国憲法第 20 条）等といった憲法上の精神的自由権の社会での存立に極めて深刻な影響を与えることも懸念される．その意味において，潜在的脅威排除のための指標となる思想及び信条の内容については，これをいたずらに拡大することは厳に慎まなければならないといえ，その反社会性を判断するための属性要件を厳格化する必要があると考える.

さらに，仮に潜在的脅威排除のための指標となる人的属性が定まり，取得・審査の対象となる個人情報の内容が同定されたとしても，米国のように事業者からの照会に応じて行政機関（FBI）が犯罪歴情報を提供できる制度を持たない我が国の現状では，(事業者の自主的な調査あるいは自己申告によって）得られた個人情報に基づく信頼性確認の効果は，その内容の確からしさの面で一定の限界を持たざるを得ないといった見方も成り立つ.

以上を勘案するならば，秘密情報管理における人的対策の実効性を確保するためには，採用・任用時の従業員信頼性確認も重要であるが，それ以上に採用・任用後における情報アクセス管理のほうがより重要になると考える．すなわち，先の **2.1(2)**のセーフガード情報管理プログラムにおける情報管理の実務水準（Table 2）に見られるように，物理的管理の徹底はもちろんのこと，従業員や情報アクセスの可能性のある者に対するセキュリティー・ポリシー及び細則の周知徹底，ID 管理の徹底及び業務毎のアクセス権の設定，クライアント PC の操作ログのモニタリング等の措置を講じることが重要となろう[12].

また，それとあわせて，採用・任用後に情報アクセスする者が職場で不審な行動をとったり，私生活において不審人物とコンタクトしたりしていないかについても注意深く継続モニタリングする必要がある. これに関して，米国では，事業者が「行動監視プログラム」（Behavior Observation Program : BOP）と呼ばれる従業員行動チェックのシステムを導入している（田邉（2008）p.9.）．しかし，我が国ではこうしたフォーマルな方法よりはむしろ職場内でのコミュニケーションの改善や相互信頼醸成を通じた内部脅威への牽制[12]のほうが，現状の職場風土や従業員意識に合致していると考える.

（2）協力会社等における実効性の確保

2.1.で述べたように，米国では，請負従業員への情報管理トレーニングの義務づけ，請負業者に対するセーフガード情報管理プログラム導入義務づけと事業者による監査，及び請負業者従業員に対するセキュリティ・クリアランスの実施を通じて, 請負業者を含むグループ全体で，秘密情報管理の徹底を図っている．我が国でも，ベンダーや協力会社等が原子力事業の業務の遂行において重要な役割を担っており，そこに所属する従業員が秘密情報や機微情報に触れる機会も多いと推察されることから，それら企業においても情報管理の実効性確保を図る必要があるといえる．我が国では核物質防護秘密に該当する情報が外部に漏出した例は認められていないものの，それ以外の情報については, 例えば平成 19 年 8 月に志賀発電所２号機の建設時に協力会社が作成した復水ポンプのゴム伸縮継手の補修に関する報告書が，協力会社社員の個人パソコンからウィニーを介してネットワーク上に漏洩する事案が報告される[13]等，協力会社の従業員等を通じた情報流出の件がこれまでにも幾つか報告されている. その意味においても，協力会社をも含めた形で情報管理の徹底を図ることの必要性は極めて高い.

しかしながら，我が国の原子力事業における協力会社の数は，いわゆる「二次請け」,「三次請け」まで含めると膨大な数に及ぶ可能性がある．これらの協力会社の中には，小規模な会社も多数含まれており，これらの者に対してまで米国のように原子力事業者（電力会社）と同等水準の情報管理プログラムの導入・実施を義務づけることは，実際問題として難しい.

加えて，膨大な数に及ぶ可能性のある個々の協力会社

従業員に対して，どのような形で実効性ある信頼性確認を実施すれば良いか，という問題もある．

以上を勘案すれば，事業者が責任をもって協力会社等における原子力関連情報管理の徹底を図ることはもちろん重要ではあるが，むしろ，事業者が核物質防護秘密等の具体的内容を勘案しつつ，協力会社等へ委託する業務の内容を適正な形で取捨選択していく必要があると考える．すなわち，核物質防護秘密に直接関連する業務や同情報へのアクセスが頻繁に発生する業務（枢要業務）については，外部委託をできるだけ避け，可能な限り当該事業者の資源でこれを実施すべきである．その際，事業者と同等水準の情報管理が可能な協力会社等に対してのみ，ここで述べたような業務の外部委託を認める，といったスクリーニングを行うことも検討されて良い．

また，やむを得ず協力会社等の外部関係者にこれらの業務を委託する場合にあっては，その業務にあたる従業員（情報アクセスを行う従業員）については，事業者における従業員と同じ就労条件でその任に就けさせ，情報保持義務の徹底を図るべきであると考える．

(3) コストと対抗リスクへの対応

以上述べた秘密情報管理の実効性確保のための諸措置は，事業者及び社会に対して，相当のコスト負担を強いたり，プライバシー権や憲法上の精神的自由権等に悪影響（対抗リスク）をもたらしたりする可能性がある．「テロ未然防止のためには，ありとあらゆる手段を講じてでも情報管理の徹底を図るべきである」とする考え方もあり得ようが，それがもたらすコストや対抗リスクとのトレードオフを一切無視するような制度設計・運用を行うことは，やはり適切であるとは言い難い．

このようなコストや対抗リスクを緩和するために，国及び事業者による制度設計・運用においては，以下の対応がなされることが望まれる．

第一に，国及び事業者は，各国の規制当局及び事業者との情報交換等を通じて，秘密情報管理の国際水準として要求される規制及び事業者対応の内容の把握に努めるべきである．本稿では，米国水準の規制・対策がとられることを所与の条件として課題抽出とその克服策の検討を試みたが，米国の規制・対策の内容は，同国固有の事情を反映して，国際水準よりも厳しい要求事項を採用している可能性がある．我が国が秘密情報管理における国際水準を把握し，それを制度設計・運用における目安に据えることは，過剰規制や過剰対応の回避にも繋がる．

2008 年 9 月に，核物質管理の専門家，原子力産業，政府，国際機関の参加の下に，核物質防護や核セキュリティに係るベストプラクティスを収集し，情報を共有するための国際組織として，世界核セキュリティ機関（World Institute for Nuclear Security : WINS）が設立された．WINS は，民間組織であるが，政府等にも参加を呼びかけている[14]．我が国政府及び事業者が WINS に参画し，秘密情報管理を含む核物質防護・核セキュリティ対策の国際水準とベストプラクティスの収集及び支援を行うことの意義は大きく，参画が前向きに検討されるべきであろう．

第二に，特に従業員の信頼性確認に係る個人情報収集・審査に関しては，それが憲法上の権利に与える影響の大きさ等を考慮して，より厳格な要件・手続の整備を規制及び事業者対応の両面で図る必要があると考える．

第三に，事業者対応においては，上述の各国事業者におけるベストプラクティスを踏まえつつ，定量的リスク評価を伴う，体系的・総合的な情報管理プログラムの導入を図ることが望まれる（これについては, 佐々木(2008)[15] の「多重リスクコミュニケータ」の考え方が参考になる. また, 原子力施設における内部脅威対策については, 板倉（2007）[16]のリスク評価研究がある）．これは，対策について適切な優先付けを行い，許容範囲を超える対策コストを生じさせないようにするために必要となる．

そして第四に，国は，我が国原子力事業における秘密情報管理が，国家的課題であるプルトニウム平和利用の着実かつ確実な推進に必要不可欠であるとの認識に立ち，上記プログラムの策定支援や必要に応じた財政的支援等を通じて，事業者を支援することが望まれる．

4. まとめ

本稿で考察を加えた，米国商業用原子力発電施設における秘密情報管理の先行導入事案分析とそれの我が国制度・実務への示唆をまとめると，以下のとおりとなる．

(1) 米国の先行導入例は，①法令・指針類を通じた要求事項等の一定範囲内での詳細化・可視化を図ることにより，情報管理規制運用の予測可能性と透明性（説明責任）を確保するとともに，脅威に対して規制回避・対抗手段探索の機会を与えることを防いでいる，②業界団体（NEI）によるガイドライン策定や PADS の構築・運用等，民間主導による管理水準の形成と事業者横断型管理支援システムの構築が図られている，③請負業者に対する訓練及び情報管理プログラム導入の義務づけや情報アクセス者に対するセキュリティ・クリアランスの実施等，情報管理実効性確保のための様々な措置が導入されている，といった特色を有している．

(2) 我が国における秘密情報管理規制行政の予測可能性と透明性をより高め，社会が核物質防護秘密保持制度に対して持つであろう不安感や懸念を払拭するとともに，秘密情報の不注意な外部漏出を未然防止するために，我が国においても，米国水準程度までに，

規制内容の詳細化と可視化を図ることが望ましい.

(3) 上記(2)を補完するものとして，我が国においても，民間ガイドライン策定を通じた管理水準の形成や，情報共有データ・ベースシステム等の事業者横断型管理支援システムを構築することが検討されるべきである.

(4) 我が国において米国水準の従業員信頼性確認を実施する場合，犯罪歴情報等を含むセンシティブ・データの取得と従業員プライバシー・精神的自由権との相克が課題となる．①その個別性・具体性が緩和された形での利用目的の本人への明示と本人同意の要請，②個人属性の反社会性を判断するための要件の厳格化等を通じて両者の調整を図り，かつ行政機関による犯罪歴情報の事業者への適正提供を可能とする，従業員信頼性確認に係る立法を整備することが望まれる.

(5) 情報管理においては, 協力会社をも含めたグループ全体での管理の徹底が求められる．その際，事業者が責任をもって協力会社における情報管理の徹底を図ることはもちろんのこと，外部委託すべき業務内容や外部委託先の見直しを行うことも検討されるべきである.

(6) 国及び事業者は, 各国の規制当局及び事業者との情報交換等を通じて，秘密情報管理の国際水準として要求される規制及び事業者対応の内容の把握に努め，許容範囲を超えるコストと対抗リスクを生じさせる過剰規制や過剰対応の回避を図るべきである．また，国は，我が国原子力事業における秘密情報管理が，国家的課題であるプルトニウム平和利用の着実かつ確実な推進に必要不可欠であるとの認識に立ち，情報管理プログラム策定支援等の形で事業者を支援することが望まれる.

我が国において，これらの法令整備，事業者対応を図ることは，従業員プライバシーや精神的自由権との相克や社会的コスト増との兼ね合い等もあり，必ずしも容易ではないのは事実であろう．しかしながら，我が国の原子力分野での秘密情報管理の徹底は，国家安全保障上の重要課題であることはもちろんのこと，原子力開発利用先進国の一つとして国際的に期待されている責務である.また，再処理施設の稼働とプルサーマル計画の実現を着実かつ確実にすすめていくために避けて通ることのできない課題であることは言うまでもない.

これらのミッションを全うするためにも，官民が協力・協働しながら，有効な措置や仕組みを漸次構築・導入することによって，我が国原子力分野における秘密情報管理の実効性を国際的に遜色のないレベルにまで高めていくことが今後ますます必要とされるであろう.

参考文献

1) 田邉朋行(2008)「原子力事業における秘密情報管理と内部脅威対策−米国の実務例と我が国への示唆−」財団法人電力中央研究所研究報告 Y07011.

2) Exelon (2007). *Exelon Nuclear Unescorted Access Requirements Frequently Asked Questions*. June 6, 2007.

3) Harvey F. Hoffman (1998). The Management of a Health Physics Information System Application. *Nuclear Plant Journal Editorial Archive ：The Management of a Health Physics Information System Application*, January-February 1998.

4) Luis A. Reyes (2004). *Withholding Sensitive Unclassified Information Concerning Nuclear Power Reactors from Public Disclosure*, SECY-04-0191. http://www.nrc.gov/reading-rm/doc-collections/commission/secys/2004/secy2004-0191/2004-0191scy.html [2009, January 1]

5) http://www.nisa.meti.go.jp/00000004/04a00000.htm [2009, January 1]

6) 総合資源エネルギー調査会（2004）「原子力施設における核物質防護対策の強化について」原子力安全・保安部会原子力防災小委員会報告書.

7) 文部科学省（2005）「内部脅威対策」研究炉等安全規制検討会報告書.

8) 砂押以久子（2005b）「職場における労働者のプライバシーをめぐる法律問題」『日本労働研究雑誌』543, 4-15.

9) 砂押以久子（2005a）「個人情報保護法の労働関係への影響」『労働法律旬報』1606, 4-35.

10) 竹中勲（2007）「前科照会回答とプライバシーの権利」『別冊ジュリスト憲法判例百選 I』186, 44-45.

11) 総合資源エネルギー調査会（2005）「原子力施設における内部脅威への対応」原子力安全・保安部会原子力防災小委員会報告書.

12) 山内守（2008）「原子力施設における盗難防止等対策案の例」社団法人火力原子力発電技術協会四国支部平成 19 年度調査研究発表会発表資料.

13) http://www.rikuden.co.jp/press/attach/07082201.pdf [2009, January 1]

14) 原子力委員会(2008)「海外における放射性物質のセキュリティに関する動向」原子力防護専門部会（第 13 回）資料第 2 号.

15) 佐々木良一(2008)『IT リスクの考え方』岩波書店.

16) 板倉周一郎(2007)『核物質及び原子力施設の物理的防護の体系化に関する研究』京都大学大学院エネルギー科学研究科提出博士学位論文.

謝辞

本稿が成るにあたっては，京都大学名誉教授中込良廣先生，日本原子力発電株式会社参与下山俊次氏，東京大

学工学系研究科教授班目春樹先生，東京大学公共政策大学院特任教授諸葛宗男先生, 同特任教授鈴木達治郎先生, 立教大学法学部講師砂押以久子先生とのディスカッションや，Nuclear Management Company 社をはじめとする内外の多くの実務担当者の方との意見交換が大変役に立った．これらの皆様に対して心よりお礼申し上げたい．また，匿名査読者三氏ならびに（財）電力中央研究所社会経済研究所研究員佐藤佳邦氏からは有益な査読意見及びコメントをいただいた．あわせてお礼申し上げたい．

なお，本研究の一部は，平成 19 年度科学研究費補助金「原子力安全規制のための知的インフラ確立に関する研究」（研究代表者班目春樹東京大学教授）の一環として実施したものである．

---

i) 特殊核物質とは，「プルトニウム，ウラン 233，又は濃縮ウラン」のことをいう（1954 年原子力法（Atomic Energy Act of 1954）第 2 章第 11 条 aa（42 USC § 2014））．

ii) 筆者らが 2006 年 11 月 14 日に原子力発電所運転・管理会社である，Nuclear Management Company の職員（匿名）に対して実施したインタビュー調査による．

iii) 「労働者の個人情報保護に関する行動指針」は，使用者による労働者への HIV 検査や遺伝子診断を禁止する（同指針第 3 の 6 (1)）とともに，使用者が労働者に対して「性格検査その他類似の検査」や「アルコール検査及び薬物検査」を行う場合には，「本人の明確な同意」が必要であるとした（同指針第 3 の 6 (2), (3)）．

iv) 砂押（2005b）はその例示として，センシティブ・データの取得に関して，職業安定法第 5 条の 4 に関して求職者等の個人情報の取扱いを示した，平成 11 年労働省告示第 141 号第 4 の 1 (1) が，これを原則禁止し，「特別な職業上の必要性が存在することその他業務の目的の達成に必要不可欠であって，収集目的を示して本人から収集する場合」に限り「思想及び信条」や「労働組合への加入状況」等のデータの取得が例外的に認められる旨を規定している点をあげている（砂押（2005b）p.9.）．

v) もっとも，これらに該当する場合であっても，センシティブ・データの取扱いに関しては本人同意が必要とされる，とする見解も想定され得る．しかし，先述の，特定された利用目的範囲内での本人同意なしの個人情報取扱いのケースとは異なり，これらは，法令が不要を是認する場合（①）か，いわば緊急避難的に不要を是認せざるを得ない場合（②）であるため，センシティブ・データであっても本人同意は不要と解するのが相当であろう．

vi) 事実，同判例は，「前科等の有無が訴訟等の重要な争点となつていて、市区町村長に照会して回答を得るのでなければ他に立証方法がないような場合に」（多数意見），「必要最小限の範囲に限って公開しうるにとどまる」（伊藤正己裁判官の補足意見）と述べており，これは，厳格な正当化事由の基準について判示したものであると捉えることが可能である（竹中（2007）p.45.）．

Protection of Confidential Information in U.S. Nuclear Industry and its Implication for Japan

Tomoyuki TANABE [1] and Tomoaki INAMURA [2]

[1]Ph.D. (Energy Science) Senior Researcher, Socio-Economic Research Center, Central Research Institute of Electric Power Industry
(E-mail: t-tanabe@criepi.denken.or.jp)
[2]M.A. (Energy Science) Specially Appointed Assistant Professor, The Department of Nuclear Engineering and Management, School of Engineering, The University of Tokyo
(E-mail: inamura@n.t.u-tokyo.ac.jp)

In Japan, on the back of growing interest in nuclear terrorism and promoting peaceful use of plutonium steadily, there is a growing interest in protection of confidential information in nuclear industry. This paper looks at how protection of confidential information (Safeguards Information) are regulated and handled in the United States civil nuclear energy industry, and extracts its implication for Japanese regulation and practical business affairs. This paper also points out the problems that Japanese nuclear industry would face if the programs at the same level as nuclear industry in the United States would be introduced in Japan.

Key Words: *Physical Protection, Safeguards Information, Information Security, Security Clearance, Terrorism*