資料５

甲A第188号証

原子力施設における内部脅威への対応について

平成１７年６月

総合資源エネルギー調査会
原子力安全・保安部会原子力防災小委員会

目　次

1．はじめに

- 安全を確保しなければ国民生活に著しい支障や周辺住民の生命、身体又は財産に対する危険が生ずるおそれがある施設あるいは組織については、その安全を確保し、国民の生命、身体、財産を保護するために特別な措置が求められる。
- これらの施設については、従前は、外部からの攻撃への対策に重点が置かれてきたが、近年、施設への立入りが許されている者、すなわち「内部の人間（内部者）」によって施設の安全性が脅かされること（いわゆる「内部脅威[1]」）に対しても、何らかの対策を講ずるべきとの指摘が、各方面からなされており、実際に、諸外国では、それぞれ独自の措置が講じられている。

- これら内部脅威対策の中心的な手段のひとつに、内部の人間の経歴等の個人情報等に基づき、その人間の重要区域へのアクセス等を制限する「信頼性確認[2]」措置がある。
- 信頼性確認の検討に当たっては、公共の安全確保のために、個人の基本的人権やプライバシー等を、どの程度まで制限することが許されるのかについての慎重な検討と国民的合意が必要となるとともに、安全確保が必要な分野についての横断的かつ普遍的な対応が求められる。また、信頼性確認の方法が、国民の生命、身体、財産を保護するために、実効性を有するか否かを見極めることも重要となる。

- 原子力施設も安全確保が必要な施設の一つであり、これまで、核物質防護対策として様々な防護措置が講じられるとともに、その時々の情勢の変化に応じて、逐次対策の見直しが行われてきた。
- このような中、昨年12月に総合資源エネルギー調査会原子力安全・保安部会原子力防災小委員会が取りまとめた「原子力施設における核物質防護対策の強化について」（平成16年12月）の報告書においては、前述の問題意識の下で、原子力分野に係る内部脅威対策の検討の必要性が指摘されたところである。（「6－3　原子力施設の内部脅威への対応」）

- 上記を受け、原子力防災小委員会危機管理WGでは、本年1月より、原子力施設における内部脅威対策の検討に着手した。その後、同委員会危機管理WGにおける議論を基に、原子力防災小委員会において検討した結果を報告書案として取りまとめ、平成17年5月25日から6月15日までの間パブリックコメントの募集を行った。その結果、13件の意見が提出されたが、提出された意見については、意見に対する同委員会の考え方を取りまとめ、ホームページに掲載するとともに、一部については本報告書の最終取りまとめに反映させた。

---

[1] ここで「内部脅威」とは、いわゆる「インサイダー」のことであり、外部からの侵入や攻撃を意味する「外部脅威」に対して、原子力施設の内部で働く従業員等による不正行為等により生ずる脅威を指す。また、内部脅威を実行しようとする者を「内部脅威者」と呼ぶ。

[2] ここで「信頼性確認」とは、基本的に、不正行為等に及びそうな人間（要注意人物）を予め把握するための情報の収集と分析のことをいう。

2．内部脅威対策の必要性

- 核物質防護対策は、核物質の盗取及び施設の妨害破壊行為の抑止を目的とするが、いずれも内部の事情に精通した人間による情報漏洩や不正行為等により、その脅威は倍加する。
- このため、国際原子力機関（IAEA）のガイドライン（INFCIRC/225/Rev.4）では、内部脅威対策として、従業員に対する信頼性の確認を実施することが勧告されている。（別紙1）[3]
- 核物質防護対策を真に実効あるものとするためには、内部脅威対策が不可欠である。

3．内部脅威対策の概念整理

(1) 内部脅威の類型

- 内部脅威の類型を、不正行為等に及ぶ動機により分類すると、①脅迫強制型、②心神耗弱型、③確信実行型、④抑制喪失型（不満、誘惑、愉快等）に区分が可能である。（別紙2）
- 同様に、行為類型により分類すると、①不正操作、②破壊行為、③盗取、④情報漏洩、⑤内通に区分が可能である。

(2) 内部脅威対策の手法

- 内部脅威対策の手法としては、①内部脅威者が不正行為等に及ぶのを物理的に阻止する物的防護、②内部脅威者の枢要区域への侵入の排除及び破壊工作に用いる工具や核物質の不法持ち出し等を阻止する出入管理、③潜在的な内部脅威者の組織及び区域からの排除、行動観察等を通じた不正行為等の抑止を目的とした人的管理がある。
- このうち、人的管理分野の対策には、内部脅威の排除[4]を目的とした従業員等の信頼性の確認が含まれる。

4．内部脅威対策の現状

(1) 国内における現状

- 実質的な内部脅威対策として、①物的防護、②出入管理に係る防護措置（持込制限等）や③人的管理に係る防護措置（内部通報、行動観察等）を事業者が実施している。
- 今般の核物質防護対策強化の一環として導入される設計基礎脅威（DBT）[5]

---

[3] 国際原子力機関（IAEA）のガイドライン（INFCIRC/225/Rev.4）は、付き添い無しの核物質への接近者又は原子力施設への立入者等に対する信頼性の事前確認を勧告。確認の具体的手法には言及しておらず、各国の裁量に委ねられている。

[4] ここで「内部脅威の排除」とは、内部脅威者による不正行為等を防止する種々の対策（内部脅威対策）のことをいう。

[5] 「設計基礎脅威」（DBT: Design Basis Threat）とは、核物質防護システムの設計に際し基礎となる想定脅威のことであり、国際原子力機関（IAEA）のガイドライン（INFCIRC/225/Rev.4）では、「核物質の不法移転又は妨害破壊行為を企てる恐れのある潜在的内部脅威者及び／又は外部からの敵の属性及び性格。これに対して核物質防護システムが設計され、評価される。」

のひとつに「内部脅威」を位置付けることとしており、これにより、具体的に想定された内部脅威に即応した極め細かい対策の実施が可能となる。
- 今後の課題は、設計基礎脅威（DBT）に基づく内部脅威対策の着実な実施と従業員等に対する信頼性確認制度の導入の可否の検討である。

(2) 海外における現状
- 米、英、独、仏、加の5ヶ国について調査したところ、各国とも、原子力分野を含めた国家レベルでの分野横断的な信頼性確認制度（セキュリティ・クリアランス制度）を整備済みである。
- 対象分野は国防・治安分野が中心であり、原子力施設等の重要施設分野は、国防・治安分野の信頼性確認制度に付随して整備されたものと思料される。
- 具体的な制度としては、セキュリティ・クリアランス制度（米）、身元調査制度(英)、セキュリティ・スクリーニング制度(独)、行政調査制度(仏)、セキュリティ・クリアランス制度（加）等である。

5．内部脅威対策の拡充の方向性

(1) 基本的考え方（別紙3）
- 内部脅威の排除のためには、①物的防護、②出入管理、③人的管理、の3つの対策を、その役割に応じて効果的に組み合せて使用することが重要である。
- いずれか一つの対策で内部脅威の全てを排除することは不可能であり、①～③の対策を相互補完的に実施することが重要である。
- 内部脅威による不正行為等の未然防止のためには、人的管理による内部脅威者の排除が基本的に重要である。しかしながら、仮に、人的管理による内部脅威者の排除が失敗に終わっても、枢要区域に到達している内部脅威者の存在や突発的な不正行為等の発生を前提にした、物的防護や出入管理による対策で対応することで、その結果の発生を防ぐことができる。
- 上記のような内部脅威対策の基本的考え方を踏まえ、人的管理の一環として、従業員等の信頼性確認を行うことの実効性と妥当性を慎重に検討することが必要である。

(2) 物的防護
- 物的防護は、内部脅威者が不正行為等に及ぶのを物理的に阻止する手段として有効である。
- 具体的には、①計量管理の徹底、生体認証や暗号化による施錠の多重化等の盗取対策の徹底、②重要設備周辺への監視カメラの設置や枢要区域内での行動をリアルタイムで追跡する監視システム（所在確認システム等）の導入等の常時監視（モニタリング）体制の構築、③被害の拡大や内部脅威者の外部への逃走を阻止するための警備員や従業員による警戒警備の徹底等が重要である。
- また、フェール・セーフやインターロック等の施設に本来的に組み込まれている安全装置は、破壊行為が行われた際の防護措置にもなり得ることから、具体的な防護対策を講じる際の手段として考慮可能である。

と定義されている。

(3) 出入管理

- 出入管理は、内部脅威者の枢要区域への侵入の排除及び破壊工作等に用いる工具や核物質の不法持ち出し等の阻止のための手段として有効である。
- 具体的には、①防護上の重要度に応じた防護区域内の細分化（ゾーニング）と区域の重要度に応じた段階的入域管理、②出入管理のためのIDカードの発給、暗証番号や生体認証による認証等の本人確認の徹底、③金属探知器や爆発物探知器、放射線検知器等の検知方法の高度化、④携帯電話等の持込制限やトゥーマン・ルール（同行監視）による相互監視、腕章等による新規入域者のマーキング等の入域ルールの厳格化等が重要である。

(4) 人的管理

- 人的管理は、潜在的な内部脅威者の組織及び区域からの排除、行動観察等を通じた不正行為等の抑止手段として有効である。
- 具体的には、①機微情報の管理の徹底、社内教育の充実、内部通報制度の整備、作業前ミーティング（ツール・ボックス・ミーティング）の実施等の組織体制の整備、②労務管理や人事管理等を通じた不審行動の兆候の察知や要注意人物の特定等の個人管理の徹底、③治安関係機関やその他の機関が保有する個人情報等の外部情報による信頼性確認の実施等が重要である。
- 信頼性確認の実施の可能性等については、次項以下で検討する。

6．信頼性確認の実施の可能性

(1) 海外における信頼性確認の現状と考え方（別紙4、5）

- 国（治安機関を中心）が国家安全や治安を脅かす者に関する情報を蓄積、信頼性確認のための照会が可能となっている。
- 国家安全保障や治安維持を第一義的な目的として、分野横断的に制度設計されており、調査対象国で、原子力分野だけに信頼性確認制度が導入されているところはない。
- したがって、他の信頼性確認で基準をクリアしている者は、原子力のための調査を受けなくともよいとする国もある。（米国、独国等）
- 個人情報保護法制の適用除外が規定されている。（「国家安全保障」、「他の法令で規定する場合」）

(2) 信頼性確認の役割と位置付け

- 信頼性確認の役割は、基本的に、不正行為等に及びそうな人間（要注意人物）を予め把握するための情報の収集と分析である。
- 信頼性確認で可能なのは、あくまで不正行為等に及ぶ蓋然性の高いグループ（ハイリスク・グループ）の推定であり、不正行為等に及ぶ当事者の特定ではない。
- したがって、信頼性確認による「脅威となる人の排除」は、本質的に完全ではなく、内部脅威対策における信頼性確認の役割はその意味で限定的であることに留意が必要である。
- このため、より効果的な内部脅威対策を実施するためには、人・物等の出

入管理や物的防護と信頼性確認の制度を相互補完的に実施することが重要である。

(3) 信頼性確認に使用される情報の種類と期待される効果

- 英、米、独、仏、加いずれも、国家保有情報の活用が制度設計の前提とされている。
- 公安情報（Intelligence）と犯罪歴による確信的な脅威者の選別を基本とし、必要に応じてクレジットチェック等の情報が活用されている。（英国、独国等）

【米国】国家安全に係る業務に就く者又は就こうとする者（政府雇用者のみならず政府との契約者を含む）に対する信頼性確認制度（セキュリティ・クリアランス制度）があり、身元の裏付け、職歴、学歴、クレジット情報、犯罪歴、軍経歴等で個人の性格や評判を確認。これに準じて、原子力施設に立ち入る者についても同様の確認制度があり、事業者に確認義務が法定されている。上記の個人情報に加え、心理学的評価や行動観察、アルコール・薬物依存チェックも求められる。（以上、連邦規則 5CFR PARTS731, 732, and736、10CFR Sec. 73.56-57 Part26.24等）

【英国】国家機密情報にアクセスする者や治安業務に従事する者等に対する信頼性確認制度（身元調査制度（Vetting））があり、国が保有する公安情報、犯罪歴等を確認、必要に応じクレジットチェックや本人への面談、従前の雇用者・身元保証人との面談等により信頼性を確認。原子力施設で働く者についても同様の確認制度がある。原子力分野の報告書によると、誠実であることを重視しており、過去の前科に関する全面的な自己申告、疑問解決への積極的な協力者等は拒絶されない可能性が高い。（以上、A Report to the Secretary of State for Trade and Industry (The Director of Civil Nuclear Security October 2000 - March 2002)）

【独国】安全性が侵害されやすい業務に就く者（主に国家機密事項を取り扱う公務員であったが、2001 年の法改正により生活又は防衛上重要な施設まで対象拡大）に対する信頼性確認制度（セキュリティ・スクリーニング制度）があり、政府の各機関が集積したテロリスト関連情報や個人の犯罪歴・裁判歴・行政処分歴等に関する情報の照会により、信頼性を確認。これに準じて、原子力関連業務に就こうとする者についても同様の確認制度がある。（以上、安全性審査法、原子力法）

【仏国】国家主権に関する任務遂行に参加する公的職業、安全又は防衛分野に関する公的又は私的な職業、制限区域へのアクセス、危険物質・製品の使用等に関して、採用、任命、許可、同意又は資格付与の行政決定を行うに当たり、関係する自然人又は法人が当該職務又は任務の遂行にふさわしいか否かを確認するため信頼性確認制度（行政調査制度）があり、特別の権限を与えられた警察及び憲兵隊の職員等の国家公務員は、各機関が差し押さえた個人情報データ（国家警察、国家憲兵隊の保有する犯罪捜査情報ファイル等）にアクセスできる。この制度が原子力分野についても適用されている。（以上、1995 年 1 月 21 日付治安に関する方針と綱領に関する法律、2003 年 3 月 18 日付国内治安に関する法律）

【加国】国家安全に係る業務に就く者、国家秘密を取り扱う業務に従事する者等に対する信頼性確認制度（セキュリティ・クリアランス制度）があり、個人データのチェック、教育/専門資格、就業データの調査、犯罪記録に関するカナダ警察情報センター（CPIC）、破壊活動に関するカナダセキュリティー情報サービス（CSIS）への照会により、信頼性を確認。必要に応じてクレジットチェック、個人の性格審査、現場調査、対象者との面談が行われる。原子力分野においても、これに準じた信頼性審査が行われている。（以上、CSIS ACT、Personnel Security Standard、原子力防護規則及び専門家からのヒアリング）

(4) 信頼性確認の情報の管理主体

- 国家安全保障や治安維持目的のための個人情報や犯罪歴については、いわゆる情報機関や治安機関が蓄積しており、その他の情報については、通常、行政機関以外の第三者機関が保有している。
- 公安情報や犯罪歴については、信頼性確認を行う事業者あるいは国の機関が必要に応じ、担当行政庁を通じて各情報機関や治安機関に照会ができる制度となっている。（米：FBI、独：連邦憲法擁護庁、各警察機関等、仏：警察、国家憲兵隊、税関等、加：カナダ警察情報センター（CPIC）、カナダセキュリティー情報サービス（CSIS））
- その他の個人情報は、それぞれ保有している機関へ照会する仕組みである。（クレジット情報は信用情報機関等）
- これら諸外国の例をみると、信頼性確認を行う場合は、国の機関や民間機関が保有する個人情報の活用を念頭に制度設計の検討を行うことが必要である。

(5) 信頼性確認の実施主体[6]

- 原子力分野の信頼性確認の実施主体は大きく分けて、事業者の場合、国の場合（原子力規制庁の場合、治安機関の場合）の３種類である。ただし、米国・加国においては、一部事業者、一部規制庁となっている。
- 事業者が主体。（米国）（規制庁は基準を策定）
- 規制庁が主体。（英国、加国、独国）（ただし、基本制度の基準策定は、英国が内閣府、加国がカナダ予算庁、独国は安全性審査法による。また、テロリスト情報や犯罪歴等を用いた信頼性確認は、情報機関や治安機関等の国家機関が実施）
- 治安機関が主体。（仏国）
- 信頼性確認の実施主体のあり方は各国の事情により異なるが、いずれの国においても、国防や治安を中心とした包括的な信頼性確認制度が先行的に整備され、各個別事業分野については、それに準じて、あるいはその一環として整備された制度や基準に基づき、信頼性確認が実施されていることに留意が必要である。
- また、規制庁が信頼性確認を実施する場合でも、テロリスト情報や犯罪歴等を用いた信頼性確認は、情報機関や治安機関等の国家機関の審査に委ね

---

[6] 「信頼性確認の実施主体」の意味内容は、①実質的に信頼性確認を実施している場合、②実質的に信頼性確認を実施している機関に、情報の照会を行っているに過ぎない場合、③信頼性確認の基準等は別途の機関が定め、単にその基準に基づき信頼性確認業務を実施している場合、④これらが混在している場合等、多様であり、各国の実態が具体的にどの場合に該当するかは、個別に精査する必要がある。本稿では、「信頼性確認の実施主体」は、基本的には①の意味で用いているが、より正確な記述を必要とする場合は（　）等で付記した。

られていることにも留意が必要である。

(6) 信頼性確認の実施方法

- 各国とも調査開始時に確認申請書類に詳細な自己情報を記載、提出させ、調査によってその確認を行う形式である。(ただし、仏国は詳細不明)
- 直接本人から聴取することもある。(米国、英国、独国等)
- 国による確認の場合、不服申し立て制度の適用がある。(英国、独国等)
- 情報の種類により、自己申告によってある程度客観的な評価が可能なものもあるが(クレジット情報、健康情報等)、テロリスト情報や犯罪歴等は必ず情報機関や治安機関等の国家機関による審査あるいはそれらへの照会が必要である。
- 多くの個人情報を集めることから、調査開始に当たり、必ず本人の同意を書面で得ることを要件としている国もある。(独国等)
- 信頼性の確認は有効期限が定められており、定期的な再確認が必要とされている。(米国、英国、独国等)
- 評価の基準は各国とも一律ではなく、特に犯罪歴の評価については、それだけで結論付けてはならない旨の注意がある。(独国、米国、英国等)
- 原子力分野における判断指針は、国家安全保障目的の基本的な信頼性確認制度の判断基準に準拠し、整備されているものと思料される。

7. 信頼性確認の実施上の課題

(1) 基本的人権の尊重

- 我が国では、民間企業における採用や人事配置について、企業に自由な裁量が認められ、その意思決定は企業自治に委ねられている。したがって、信頼性確認措置に基づき不利益処分[7]を行うことを企業に義務付けるとすれば、何らかの法的根拠が必要である。
- 企業に対し、業務に直接関係しない個人の事情を理由とした配置転換や就業制限を行うことを国が義務付けることとした場合、従業者等への直接の処分者は企業となり、民-民の関係となるため、憲法は直接適用されないが、なお何らか憲法へ抵触する恐れがないか、注意が必要である。(「個人の尊重」(13 条)、「法の下の平等」(14 条)、「職業選択の自由」(22 条)など)[8]
- 例えば、事業者による確認制度とする場合でも、国が確認の基準を策定し、義務付ける規制には、憲法が適用される可能性が考えられる。(官-民の関係)

(2) プライバシー保護

- 各国において、個人のプライバシー情報[9]の収集及び活用が国や企業に許

---

[7] ここで「不利益処分」とは、使用者(企業)による被使用者(従業員)に対する配転、解雇、懲戒解雇等の処分を指す。

[8] 職務懈怠、業務命令違背、業務妨害や職場規律違反、就業規則違反や企業の社会的評価を毀損する私生活上の言動等は、懲戒事由として肯定されるところ。

[9] ここで「プライバシー情報」とは、各国における信頼性確認に用いられている個人情報(住所歴、職歴、学歴、犯罪歴、個人信用情報(金銭借入れに係わる取引内容)、アルコール・薬物依存等の健康に関する情報等の個人に関する情報)を指す。

されている理由は、「原子力施設の安全確保」が、「国家・国民の安全確保」という国家的な目的達成の一環として位置付けられているためと思料される。

- 我が国においても、個人のプライバシー情報を活用するためには、「原子力施設の安全確保」を、「国家・国民の安全確保」という国家的な目的達成の一環として位置付けることが必要と考えられる。
- 判例によると、企業は従業員の採用に当たり、幅広い個人情報を申告させることが許されるが、行政指導ではこれを厳しく制限している。制度導入に当たっては、個人情報保護法及びこれに関連する行政指導との整合性の確保が必要[10]である。
- プライバシー侵害が過度な場合、安全性が高まる効果（脅威者の排除）より、安全性を損ねる損失（反発者の増加）が大きい可能性もあることに留意が必要である。

(3) 制度の実効性

- 個人の信頼性確認制度の導入に当たっては、国が国家安全保障や治安維持の目的で保有している個人情報の活用について、関係機関との十分な調整が必要である。特に確信犯的な脅威者の排除には関係機関との連携が不可欠である。
- 個人の犯罪歴を、それ単体で潜在的な脅威者の排除の根拠とすることの妥当性については、慎重な検討が必要である。
- すなわち、犯罪歴のみで確信犯的な脅威者の選別・排除は困難であり、その他の個人情報も加味した総合的な判断が必要である。また、確信犯的な脅威者の排除につながる犯罪歴の種類の特定も必要である。
- 健康情報や金銭借入情報等は、これらのみによって脅威の有無を判断根拠とすることは困難である。
- 日常業務に支障が出る程度まで異常がある場合は、事業者による労務管理・人事管理の一環として、特異動向の把握が可能である。
- 本人の同意を前提とした制度とすると、センシティブな情報を知られることへの抵抗感から、制度が機能しない恐れがある。
- 実効性を担保する上で、信頼性確認の対象者を重要区域への立入者あるいは核物質防護秘密を取り扱う者に限定する等、対象者を限定することが必要である。[11]

---

[10] 職業安定法（第5条の4）は、公共職業安定所等に対し、その業務の目的の達成に必要な範囲内で求職者等の個人情報を収集し、当該収集の目的の範囲内で保管、使用を義務付け。（ただし、本人の同意がある場合その他正当な事由がある場合は、この限りではない）
「職業紹介事業者、労働者の募集を行う者、募集受託者、労働者供給事業者等が均等待遇、労働条件等の明示、求職者等の個人情報の取扱い、職業紹介事業者の責務、募集内容の的確な表示等に関して適切に対処するための指針」（平成11年労働省告示第141号）は、職業紹介事業者等に対し、業務の目的の範囲内で求職者等の個人情報を収集することを義務付け、人種、民族、社会的身分、門地、本籍、出生地その他社会的差別の原因となるおそれのある事項、思想及び信条、並びに労働組合への加入状況に関する情報の収集を禁止。ただし、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はこの限りでないとしている。

[11] 信頼性確認の目的（対象範囲）には、①組織からの内部脅威者の排除と②区域からの内部脅威者の排除の2つがある。IAEAのガイドラインで勧告しているのは後者。

(4) 制度の実現性

- 国の機関が国家安全保障や治安維持目的で保有している個人情報は、通常当該機関内部での活用のみを想定して収集・蓄積しているものと考えられるが、確信犯的な内部脅威者の排除のためには、これら機関の情報の活用が不可欠である。
- 原子力施設内で働く労働者は、原子力事業者の従業員以外にも、関係会社や出入の業者の従業員等、多数かつ多岐にわたる。これら階層的な雇用構造の中で、原子力事業者による一元的な雇用管理の実現は困難であるとの指摘もある。
- 原子力施設で働く関係会社や警備会社等の従業員は、原子力事業者の被雇用者ではないため、原子力事業者による「施設管理権」に基づく入域管理という観点から検討することが必要である。
- 現行原子炉等規制法は、基本的に原子力事業者が規制対象であり、関係会社等の原子力事業者以外の事業者へ信頼性確認の義務付けを行う場合は、一般法の整備等が必要との指摘もある。
- 事業者間で審査基準を統一することが必要である。ただし、事業者及び規制庁とも具体的事例に基づく知見蓄積が欠如していることから、関係機関の協力が必要である。
- 事業者間の情報共有システム構築の必要性について検討すべきである[12]。
- 階層的な雇用構造等に留意した段階的入域管理のあり方についても検討すべきである。
- 不服申立制度については、その位置付けについて、整理することが必要である[13]。

(5) 国民的合意の形成

- セキュリティ確保のためには、プライバシーを含む基本的人権に一定の制約を課すことについて、国民の理解と合意を得ることが必要である。
- 原子力施設・核物質の安全確保という「目的の正当性」と個人情報に基づく審査・選別という「手段の相当性」に関する関係者その他の国民（従業者、事業者、地元自治体住民等）のコンセンサスの形成が必要である。
- 民間施設である原子力施設に信頼性確認を導入することを国民が許容し得るかという点や、安全確保が必要な他の産業分野とのバランスの問題について、配慮が必要である。
- 信頼性確認は、その効果の実証が困難であるため、国民の理解と合意を得る上で、その説明に留意が必要である。

8．政策の方向性

- 内部脅威の排除のためには、①物的防護、②出入管理、③人的管理、の3

---

[12] 個人情報の保護に関する法律（第23条）は、個人データの第三者提供については、事前に本人の同意を得ることとしている。（ただし、法令に基づく場合、人の生命、身体又は財産の保護に必要な場合等で本人の同意を得ることが困難な場合等を除く。）

[13] 行政庁による処分と位置付ける場合（直接規制方式）は、行政不服審査法及び行政事件訴訟法が適用される。行政庁が審査基準を設け、事業者に処分行為を行わせる場合（間接規制方式）は、事業者に対する民事訴訟手続きが適用されるほか、審査基準自体についての何らかの行政訴訟の可能性も考えられる。

つの対策を、その役割に応じて効果的に組み合せて使用することが重要である。

- その上で、信頼性確認については、諸外国の実態や我が国の現状等を踏まえ、①分野横断的な信頼性確認制度の創設、②現行制度で可能な信頼性確認措置の検討、③設計基礎脅威（DBT）を用いた内部脅威対策の実施、の３つを政策の選択肢として提案する。
- 各政策の方向性等は、以下のとおりである。

〈分野横断的な信頼性確認制度の創設〉

- 信頼性確認制度については、諸外国と異なり、我が国は個人の信頼性を確認するための個人情報の蓄積・照会制度が整備されていないため、現時点で得られる個人情報に基づく信頼性確認の効果は限定的とならざるを得ない。
- 内部脅威対策として真に実効ある仕組みを実現するためには、諸外国の例にみるように、脅威の排除に直結する個人情報を、国が収集・管理し、それを各機関が活用する普遍的・横断的な制度とすることが重要である。

- そのためには、行政全体を統括する部局が中心となり、国民的合意を得た上で、国が管理する分野である防衛や治安等を含めた、分野横断的な信頼性確認制度を創設すべきである。
- 民間分野である原子力分野への信頼性確認制度の導入も、国民的合意を得た上で、分野横断的な制度の一環として実施すべきである。
- 分野横断的な信頼性確認制度の創設については、前記「７．信頼性確認の実施上の課題」を踏まえ、引き続き関係省庁間での慎重な検討が必要である。

〈現行制度で可能な信頼性確認措置の検討〉

- 原子力分野における信頼性確認については、分野横断的な信頼性確認制度の短期間での実現が困難な場合は、法的措置を伴わない現行制度で可能な取り組みについて、その実現可能性を含め検討を行うべきである。
- 具体的には、例えば、事業者が保有する従業員情報を活用した信頼性確認や、より制限的でない自己申告制度の導入が想定される。
- これら現行制度で可能な信頼性確認に係る取り組みについては、事業者が保有する情報のみで信頼性確認を行うことの実効性や、原子力事業者以外の関係会社の従業員も含めた信頼性確認を行うことの実現性等について、引き続き慎重に検討することが必要である。

〈DBT を用いた内部脅威対策の実施〉

- 現行制度で可能な信頼性確認以外の取り組みとしては、今般の制度改正で導入が予定されている DBT を用いた内部脅威対策（物的防護、出入管理等（前記５．(2) ～ (4)））があり、本措置の着実な実施が重要である。
- DBT を用いた内部脅威対策は、厳密な意味での「信頼性確認のための措置」ではないが、「信頼性確認」がその目的としている「内部脅威対策」を実現するものであることから、政策の選択肢として掲げるものである。
- 具体的には、例えば、防護区域の細分化（ゾーニング）や区域の重要度に応じた段階的入域管理の実施等が想定[14]される。

---

[14] 国際原子力機関（IAEA）のガイドライン（INFCIRC/225/Rev.4）は、付き添い無しの核物質

- 本措置は、前述の2つの選択肢の成否の如何に関わらず着実に実施すべき、必要最低限の措置として位置付けられる。

9．おわりに

- 原子力施設を含む重要施設の内部脅威対策については、引き続き、「テロの未然防止に関する行動計画」（平成16年12月）に係る関係省庁会議で検討が予定されている。
- 本稿で掲げた諸外国の実態等は、現時点で知り得る限りの情報を集約したものであり、より正確かつ詳細な分析のためには、さらに継続的な調査が必要である。

への接近者又は原子力施設への立入者等に対する信頼性の事前確認を勧告。確認の具体的手法には言及しておらず、各国の裁量に委ねられている（前記脚注1）。この意味で、防護区域の細分化（ゾーニング）や区域の重要度に応じた段階的入域管理の実施等の措置は、IAEAのガイドラインの勧告の趣旨に沿うものと思料。

[別　紙１]

The Physical Protection of Nuclear Material and Nuclear Facilities（INFCIRC/225/Rev.4）

「核物質及び原子力施設に対する防護」に関するIAEA勧告　（抜粋）

〈設計基礎脅威(DBT)の定義と内部脅威者〉

2. DEFINITIONS

2.4. DESIGN BASIS THREAT:

The attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal of nuclear material or sabotage, against which a physical protection system is designed and evaluated.

2.　定　　義

2.4　設計基礎脅威（DESIGN BASIS THREAT）：

核物質の不法移転又は妨害破壊行為を企てる恐れのある潜在的内部脅威者及び／又は外部からの敵の属性及び性格。これに対して核物質防護システムが設計され、評価される。

〈信頼性確認に関する条項（抜粋）〉

6. Requirements for Physical Protection Against Unauthorized Removal of Nuclear Material in Use and Storage（使用及び貯蔵中の核物質の不法移転に関する防護要件）

6.1.　General（総則）

6.1.2.　Achievement of the objectives of the physical protection system should be assisted by:

c. Requiring predetermination of the trustworthiness of all individuals permitted unescorted access to nuclear material or facilities.

6.1.2.　核物質防護制度の目的達成は、次の事項によって助長されなければならない。

c. 核物質又は施設に付き添い無しに接近を許可するすべての者について、信頼性の事前確認を求めること。

6.2.　Requirements for Category I Nuclear Material（区分Ⅰ核物質の要件）

6.2.2　Access to and the number of access points into the protected area and inner areas should be kept to the minimum necessary. **Persons authorized unescorted access to the protected area or inner areas should be limited to persons whose trustworthiness has been determined.** Persons whose trustworthiness has not been determined such as temporary repair, service or construction workers and visitors should be escorted by a person authorized unescorted access. The identity of all persons entering such areas should be verified and they should be issued with appropriately registered passes or badges.

6.2.2.　防護区域又は内部区域に付き添い無しで入域を認められた者は、信頼性が確認された者に限られる。

8. Requirements for Physical Protection of Nuclear Material During Transport（輸送中の核物質防護要件）

8.1.　General（総則）

8.1.2.　Achievement of the objectives of physical protection should be assisted by:

e. **Requiring predetermination of the trustworthiness of all individuals involved during transport of nuclear material**; and

8.1.2.　核物質防護制度の目的達成は、次の事項によって助長されなければならない。

e. 核物質の輸送に携わるすべての者の信頼性について、事前確認を要求すること。

［別　紙２］

内部脅威者の類型

類型		内容	特徴	考えられる防護対策
❶脅迫強制型		・身内が人質に取られたり、弱みを握られ脅迫され不正行為に及ぶ。（脅迫） ・内部の人間が、他の人間を刃物等で脅迫し、不法行為を強制する。（強制）	・枢要区域に自由に出入可能な人物が不正行為を余儀なくされる場合がある。 ・脅迫の場合、当事者を予め特定することは不可能。	・行動観察、緊急時の社内ルールの整備。 ・強制の場合、他の類型の内部脅威者が実行犯となる可能性があるため、その対策は当該類型に準じる。
❷心神耗弱型		・心神耗弱等により突発的に不正行為に及ぶ。	・枢要区域に自由に出入可能な人物が不正行為に及ぶ場合がある。 ・意図的でない単純な行為を想定。 ・心神耗弱は、行動観察等である程度特定可能。	・労務管理、行動観察の徹底。 ・精神的健康状態チェックの導入。
❸確信実行型		・思想的・宗教的確信から不正行為に及ぶ。 ・国際テロリスト、カルト集団、極右・極左等は本類型に分類される。	・長期の行動観察等で、危険性向の所有者をある程度特定可能。 ・枢要区域に出入可能な部署からの排除等の措置が有効。	・労務管理、行動観察の徹底。 ・国が国家安全保障や治安維持の目的で保有している個人情報に基づく選別。
❹抑制喪失型	不満	・職場内の不満から不正行為に及ぶ。	・長期の行動観察等で、危険性向の所有者をある程度特定可能。 ・職場環境、金銭借入状況、交友関係、家庭事情等の誘引情報の把握が重要。 ・労務管理、行動観察等が有効。 ・業務に対する責任感、職場への忠誠心の涵養が重要。 ・枢要区域に出入可能な部署からの排除等の措置が有効。	・社内教育によるモラルの向上。 ・個別の誘引情報（職場環境、金銭借入状況、交友関係、家庭事情等）の把握。 ・労務管理、行動観察の徹底。
	誘惑	・金銭等の誘惑に抗し切れず不正行為に及ぶ。		
	愉快	・世間や会社を騒がせたくて不正行為に及ぶ。		

[別 紙 3]

内部脅威者に対する防護対策

防護措置			内容	内部脅威者の類型（注）				対応の考え方
				脅迫加担型	心神耗弱型	確信実行型	抑制喪失型	
物的防護	設備・工学的対策	多重防護	・金属探知器の設置等のハード面、出入管理の実施等のソフト面の相互補完を含めた防護措置の多重性を確保	○	○	○	○	・妨害破壊行為を一つの防護措置で防止することは困難であり、ハード面及びソフト面の組合せにより多重に措置することが重要
		フェールセーフ	・異常時(悪意操作を含む)に自動的に運転停止するような工学的仕組み	○	○	○	○	・妨害破壊行為が起きた際に、被害を最小限に留めるような工夫を施しておくことは重要
		インターロック	・安全な操作手順以外の操作が無効となる仕組み	○	○	○	○	・誤操作(故意を含む)で起きる事故を防止するための仕組みを構築しておくことは重要
	運用対策	施錠	・解錠手順の複雑化、多重化	○	○	○	○	・単独操作を阻止する仕組みを確保することが重要
		計量管理	・可能な限りリアルタイム化	○	○	○	○	・核物質の持ち出しチェックに有効
		監視装置	・監視カメラの設置(全域カバー、被写体追随性、ズーム、暗視・赤外・熱画像等)により監視 ・タンパリング(悪戯)対策 ・補足措置として、現場見張り人又は適切な頻度の現場パトロールの実施	○	○	○	○	・トゥーマン・ルールの代替措置として有効 ・新たな手段として、人の移動をリアルタイムで捕捉するシステム(所在確認システム)の導入の検討が重要 ・妨害破壊行為の観点から、使用済燃料プール、新燃料貯蔵場所、中央制御室内等に監視カメラを設置することも重要
出入管理	入域	区域の設定	・周辺防護区域、防護区域等の設置 ・防護区域の細分化(ゾーニング)及び段階的入域管理	○	○	○	○	・区域の設置及び区域内の区画化によって、人の入域を段階的に制限することが重要 ・枢要設備を特定・細分化することによって、より限定的な入域管理を行うことが重要
		IDカード管理	・写真付きIDカードの発給 ・IDカード発給申請時に履歴、職歴、住民票/戸籍抄本、定期健康診断結果、運転免許証、放射線被曝記録等の提出を要請しチェック ・IDカードの適切な保管、紛失時の迅速な対処	○	○	○	○	・IDカード発給手続の審査で、入域の必要性・期間の妥当性を確認すると共に、本人確認を徹底することが重要
		IDカード	・種類として、磁気カード、ICカード等 ・写真付き	○	○	○	○	・IDカードの盗難・紛失が懸念されるため、暗証番号確認及び生体認証の組合せが有効
		暗証番号	・暗証番号の多数桁化	○	○	○	○	・暗証番号情報の漏洩が懸念されるので、生体認証との組合せが有効
		生体認証	・掌形、指紋、血管又は網膜・虹彩の識別装置の導入	○	○	○	○	・IDカードの盗難・紛失及び暗証番号情報の漏洩等の弱点に鑑み、IDカード照合、暗証番号確認及び生体認証の組合せが有効
		出入時間	・滞在時間のモニタリング（リアルタイム表示）	○	○	○	○	・特定な箇所に一定の時間以上滞在していること、高い頻度で繰り返しアクセスしていること等をチェックすることによって、不自然な行動を察知することが重要
		トゥーマン・ルール（同行監視）	・枢要区域内のトゥーマン・ルールの実施（現在未実施）	○	○	○	○	・トゥーマン・ルールはインサイダー行為の発見・阻止対策の一つとして効果的であるが、二者の結託等が懸念されるので、特定した区域に限定すると共に、二者の組合せ変更等の何らかのルールが必要 ・代替措置として、監視カメラの設置等が有効
	持込	持込制限（携帯電話等）	・周辺防護区域内での使用禁止 ・防護区域内への個人携帯電話の持込禁止	○	○	○	○	・動画情報の送信を含め、外部への情報漏洩の阻止が重要
		金属探知器	・周辺防護区域の入口に設置 ・補足措置として、ボディーチェックの実施	○	○	○	○	・妨害破壊行為を目的とする工具の持ち込みチェックに有効 ・入域者全員をチェックすることが重要（現行規定上は、一時立ち入り者がチェック対象）
		爆発物検知器	・周辺防護区域の入口に設置 ・補足措置として、ボディーチェックの実施 ・X線方式の検知器あり	○	○	○	○	・爆発物(TNT、プラスチック系爆発物等)の持ち込みチェックに有効 ・入域者全員をチェックすることが重要　（現行規定上は、一時立ち入り者がチェック対象）
		放射線検出器	・防護区域の出口に設置（ガンマ線の検出）	○	○	○	○	・核物質の持ち出しチェックに有効 ・出入時の体重チェックも有効
人的管理	組織管理	社内教育	・セキュリティ・カルチャアを含めた教育研修の定期的な実施	○			○	・適切な倫理観・規範性を確保するための手段として有効
		情報管理	・情報にアクセスできる者の限定	○	○	○	○	・防護措置の実効性を毀損するような情報漏洩を防止することが重要
		内部通報	・社内内部通報制度の確立	○	○	○	○	・日頃の情報収集の手段として有効
		作業前ミーティング	・作業の前の打合せにおいて作業員の状態等をチェック	○	○		○	・作業前に作業員の行動観察を行うことは有効
	信頼性確認等	採用時/配置時の調査	・採用時の面接でチェック(通常の採用面接として実施) ・IDカード発給申請の審査時にチェック	○	○	○	○	・収集できる情報の内容によっては、内部脅威者の発見対策として有効
		行動観察	・管理者、同僚等による日常的行動観察（労務管理として実施）	○	○	○	○	・実効的な着眼点を徹底できれば、内部脅威者の発見対策として有効
		金銭借入状況調査	・金融機関から情報収集する必要あり（現在未実施）				○	・本人申告等の仕組みを構築する必要あり
		精神的健康状態調査	・医師から情報収集する必要あり（現在未実施）		○			・本人申告等の仕組みを構築する必要あり
		アルコール・薬物依存調査	・定期的な健康診断の際に検出できる可能性あり（現在未実施）		○			・客観的かつ実効的な評価手段を構築する必要あり
		心理学的評価	・定期的な健康診断(問診レベルで実施) ・メンタルヘルス・カンセリング体制の確保		○		○	・客観的かつ実効的な評価手段を構築する必要あり
		犯罪情報	・治安機関への照会（現在未実施）	○		○	○	・内部脅威者の排除のためには、実効性のある犯罪種別の選定が必要
		公安情報（Intelligence）	・治安機関への照会（現在未実施）			○		・確信犯的脅威者の排除のためには、国家安全保障や治安維持のために国が保有する個人情報の活用が必要

注）「内部脅威者の類型」の欄
　○印：内部脅威者に対する防護対策として有効と思われるもの
　空欄：内部脅威者に対する防護対策としてあまり有効ではないのではないかと思われるもの

［別　紙４］

各国における信頼性確認制度の概要

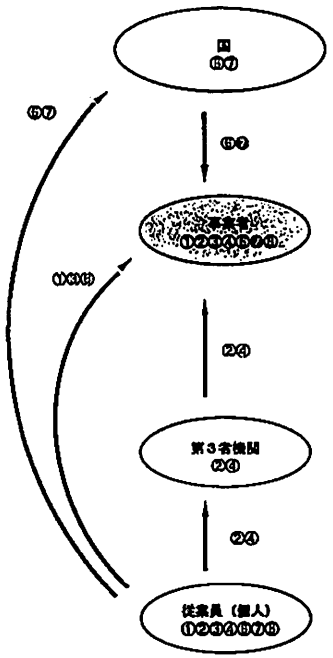
		米国			英国			独国			仏国			加国			日本		
		全体基準作成	情報所有主体	確認実施主体	全体基準作成	情報所有主体	確認実施主体	全体基準作成	情報所有主体	確認実施主体	全体基準作成	情報所有主体	確認実施主体	全体基準作成	情報所有主体	確認実施主体	全体基準作成	情報所有主体	確認実施主体
包括的な信頼性確認制度の有無		○ ｾｷｭﾘﾃｨ・ｸﾘｱﾗﾝｽ制度			○ 身元調査制度			○ ｾｷｭﾘﾃｨ・ｽｸﾘｰﾆﾝｸﾞ制度			○ 行政調査制度			○ ｾｷｭﾘﾃｨ・ｸﾘｱﾗﾝｽ制度					
信頼性確認が実施されている分野		○ 国防、治安等			○ 国防、航空等			○ 国防、安全、航空等			○ 国防、治安、航空等			○ 国防、航空等					
原子力分野の現状	行政当局	○			○			○						○					
	治安当局		○			○			○		○	○	○		○			○	
	規制当局			(注3)			○			○						○			
概要		・国家安全に係る分野について、国による信頼性確認制度あり。 ・治安当局や民間機関等からの情報に基づき信頼性確認を実施。 ・原子力分野もこれに準ずるが、原子力分野の実施主体は事業者。			・「1994 年首相声明」を受け、内閣府策定の共通基準に基づき、各分野横断的・統一的に信頼性確認を実施。 ・治安分野の実施主体は国防身元確認庁、原子力分野は貿易産業省。			・連邦憲法擁護庁が治安に係る個人情報を収集・一括管理。本情報を用い、各分野横断的・統一的に信頼性確認を実施。 ・治安分野の実施主体は治安機関、原子力分野は規制当局。			・警察・国家憲兵隊が各分野横断的・統一的に信頼性確認(「行政調査」)を実施。 ・治安分野、原子力分野とも、実施主体は警察・国家憲兵隊。			・ｶﾅﾀﾞ予算庁策定の共通基準「Personnel Security Standard」に基づき、各分野横断的・統一的に信頼性確認を実施。 ・治安分野の実施主体は治安機関、原子力分野は原子力安全委員会。			・信頼性確認は、国及び事業者のいずれも未実施。		

（注１）「行政当局」とは、「治安当局」又は「規制当局」以外の国の機関。本表では、内閣府（英国）、カナダ予算庁（加国）等。
（注２）情報所有主体としては、この他に、事業者、個人（従業員）、第３者機関（金融機関、医師等）があるが、本表では割愛。
（注３）原子力分野における米国の信頼性確認実施主体は事業者。
（注４）本表は各国の制度の全体像のおおまかな比較のために作成したものであり、必ずしも厳密なものではない。とりわけ、「確認実施主体」の意味内容は、本文P.５脚注６にあるように多様であり、その実態の正確な把握には留意が必要である。

[別　紙5]

各国における信頼性確認の概要（概念整理図）

米国の場合



〈事業者所有情報〉
① ｱﾙｺｰﾙ・薬物依存調査結果
② 心理学的評価結果
③ 行動観察結果

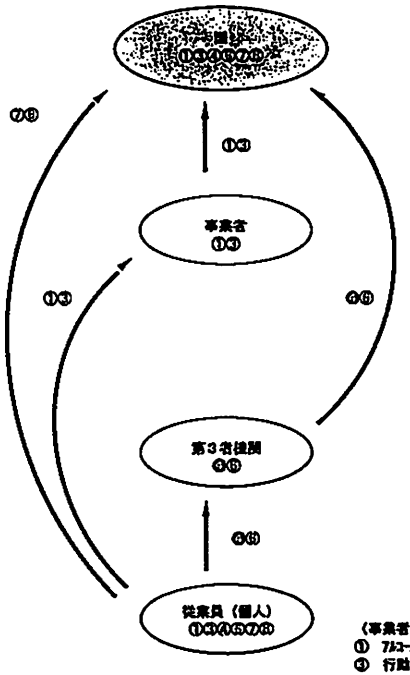
〈第３者機関所有情報〉
④ 金銭借入状況

〈国所有情報〉
⑤ 犯歴情報
⑦ 公安情報

⑧ その他の個人情報
（身元確認、職歴、学歴、軍歴等）

（注１）連邦規則 10CFR Part73.56 に基づき、事業者が従業員のｾｷｭﾘﾃｨ・ﾁｪｯｸ等を実施。そのための「ﾌｧｲﾈｽ・ﾌﾗｲﾋﾞｰｼｮﾝﾌﾟﾛｸﾞﾗﾑ」が存在。
（注２）犯歴情報の調査は 10CFR Part73.57 に、ｱﾙｺｰﾙ・薬物依存調査は「職務適正ﾌﾟﾛｸﾞﾗﾑ」として 10CFR Part26.24 に、それぞれ具体的内容を規定。
（注３）「治安当局」は FBI。犯歴情報は規制機関である NRC 経由で事業者が入手。
（注４）網掛けは信頼性確認の実施主体。
（注５）白抜き番号（⑧）は推定（未確認）。

英国の場合



〈事業者所有情報〉
① ｱﾙｺｰﾙ・薬物依存調査結果
④ 行動観察結果

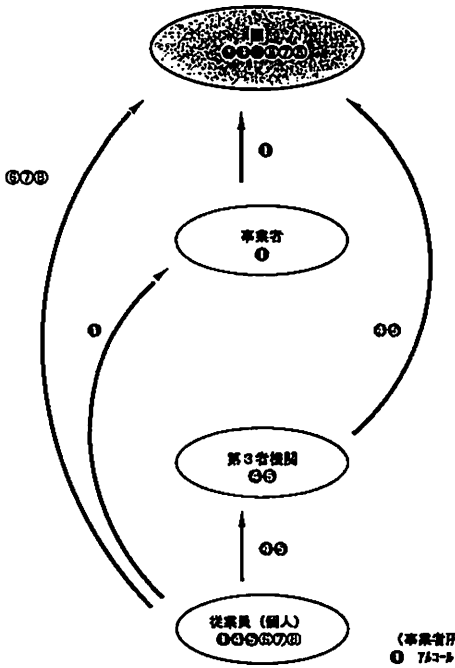
〈第３者機関所有情報〉
④ 金銭借入状況

〈国所有情報〉
⑤ 犯歴情報
⑦ 公安情報

⑧ その他の個人情報
（身元確認等）

（注１）1994 年の首相声明を受け、国（行政庁）が国防産業、航空安全分野等各種の分野において内閣府が策定した共通基準に基づきｾｷｭﾘﾃｨ・ｸﾘｱﾗﾝｽを実施。
（注２）最大の身元確認分野は国防分野（国防身元確認庁（Defense Vetting Agency）には約 300 人の担当者が勤務）。
（注３）原子力分野では、原子力産業防護規則（Nuclear Industries Regulations 2003）に基づき貿易産業省民間原子力ｾｷｭﾘﾃｨ・ｵﾌｨｽ（OCNS）が従業員のｾｷｭﾘﾃｨ・ﾁｪｯｸを実施。専任ｽﾀｯﾌは約 20 名。
（注４）網掛けは信頼性確認の実施機関。
（注５）白抜き番号（⑤）の情報ルートは推定（未確認）。

独国の場合



〈事業者所有情報〉
❶ ｱﾙｺｰﾙ・薬物依存調査結果

〈第３者機関所有情報〉
❹ 金銭借入状況
❺ 精神的健康状態

〈国所有情報〉
❻ 犯歴情報
❼ 公安情報

❽ その他の個人情報
（住所歴等）

（注１）「連邦憲法擁護庁」が、連邦や州に対する暴力や破壊行為等のいわゆる過激行為等に関する情報収集・評価を行うため、必要な個人ﾃﾞｰﾀを入手・蓄積し、最長 15 年間保存。
（注２）治安機関、情報機関、外務省等で国家機密を取り扱う公務員については、それぞれの官庁が、「安全性審査法」に基づき、連邦憲法擁護庁等の協力を得て、厳格なｸﾘｱﾗﾝｽを実施。
（注３）原子力分野では、「原子力法」に基づき、規制当局が連邦及び州の警察機関・情報機関に対し信頼性判断に重要な情報の照会、連邦中央登録簿の証明書の徴収を行い、ｸﾘｱﾗﾝｽを実施。
（注４）網掛けはｸﾘｱﾗﾝｽ実施主体。
（注５）白抜き番号（❶❹❺）は推定（未確認）。

〈凡例〉

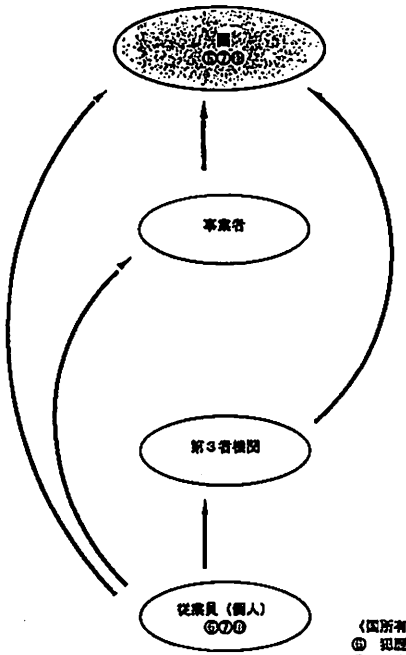
〈事業者所有情報〉
① ｱﾙｺｰﾙ・薬物依存調査結果
② 心理学的評価結果
③ 行動観察結果

〈第３者機関所有情報〉
④ 金銭借入情報（信用情報）
⑤ 精神的健康状態

〈国所有情報〉
⑥ 犯歴情報
⑦ 公安情報

⑧ その他の個人情報
（職歴、住所歴、家族情報、軍歴等）

仏国の場合



〈国所有情報〉
⑥ 犯歴情報
⑦ 公安情報

⑧ その他の個人情報
（詳細不明）

（注１） 「1995年1月21日付け 治安に関する方針と網羅に関する法律」に基づき、特別の権限を与えられた警察、国家憲兵隊等の職員が「行政調査」を実施。対象となるのは、国家主権関連任務、安全又は防衛分野関連の公的・私的職業分野（原子力分野も本対象）。

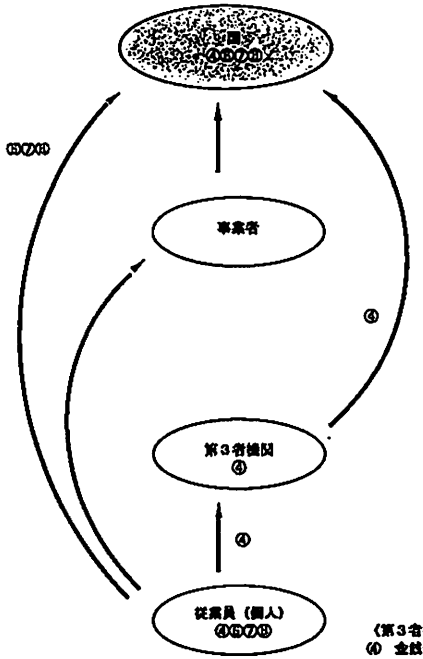
（注２） 上記調査では、制限区域へのｱｸｾｽ、危険物質（兵器、火薬、核物質等）の製造・使用者に対する採用・任命・許可等の行政決定を行うに当たり、職務・任務にふさわしいか否かを確認。

（注３） 法令上、ﾁｪｯｸ項目が明らかなのは「警察、国家憲兵隊等が保有する情報」のみ。

（注４） 網掛けは信頼性確認の実施主体。

（注５） 白抜き番号（⑧）は推定（未確認）。

加国の場合



〈第３者機関所有情報〉
④ 金銭借入状況

〈国所有情報〉
⑥ 犯歴情報
⑦ 公安情報（破壊活動情報）

⑧ その他の個人情報
（身元確認、職歴、学歴等）

（注１） ｶﾅﾀﾞ予算庁が作成した「Personnel Security Standard（個人治安基準）」に基づき、各業種分野でｾｷｭﾘﾃｨｸﾘｱﾗﾝｽを実施。

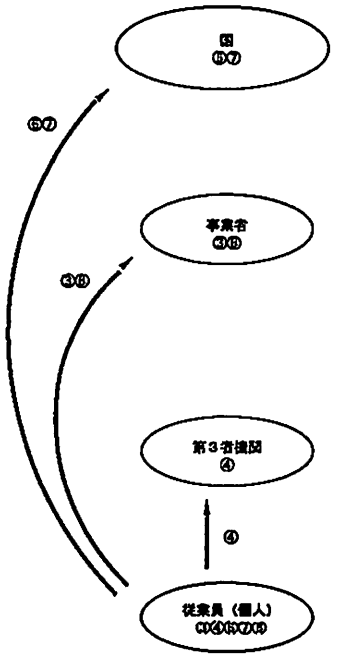
（注２） 原子力分野では、「原子力安全・管理法」及び「原子力防護規則」に基づき、国則として原子力安全委員会がｾｷｭﾘﾃｨｸﾘｱﾗﾝｽを実施。

（注３） ただし、今後の法改正により、ｸﾘｱﾗﾝｽは事業者が行い、規制自局は監査検能だけになる見通し。

（注４） 犯歴情報はｶﾅﾀﾞ警察情報ｾﾝﾀｰ（CPIC）に、破壊活動情報はｶﾅﾀﾞｾｷｭﾘﾃｨｰ情報局（CSIS）に照会する仕組み。ｸﾚｼﾞｯﾄﾁｪｯｸはAssociated Credit Bureaus of Canadaを通じ実施。

（注５） 網掛けは信頼性確認の実施主体。

日本の場合



〈事業者所有情報〉
③ 行動観察結果

〈第３者機関所有情報〉
④ 金銭借入状況

〈国所有情報〉
⑤ 犯歴情報
⑦ 国家安全保障や治安維持の目的で保有する情報

⑧ その他の個人情報
（職歴、学歴、住所地、家族構成等）

（注１） 「第３者機関」として想定しているのは、金融機関の個人信用情報取扱機関や医師等。金銭の借入れ、診察や健康診断の受診により、自動的に情報が集められる。（個人情報保護法では「個人情報取扱事業者」と呼称。）

（注２） その他の個人情報は、企業が通常雇用の際に入手し得る情報。

〈凡例〉

〈事業者所有情報〉
① ｱﾙｺｰﾙ・薬物依存調査結果
② 心理学的評価結果
③ 行動観察結果

〈第３者機関所有情報〉
④ 金銭借入情報（信用情報）
⑤ 精神的健康状態

〈国所有情報〉
⑥ 犯歴情報
⑦ 公安情報

⑧ その他の個人情報
（職歴、住所歴、家族情報、軍歴等）

総合資源エネルギー調査会原子力安全・保安部会
原子力防災小委員会委員名簿

（敬称略、五十音順）

（委員長）	朝田　泰英	社団法人火力原子力発電技術協会技術顧問
	秋庭　悦子	社団法人日本消費生活アドバイザー・コンサルタント協会理事
	岡　　芳明	国立大学法人東京大学大学院工学系研究科教授
	齋藤　鐵哉	独立行政法人物質・材料研究機構名誉顧問
	首藤　由紀	株式会社社会安全研究所取締役
	藤吉　洋一郎	ＮＨＫ解説委員
	廣井　脩	国立大学法人東京大学大学院情報学環・学際情報学府教授
	班目　春樹	国立大学法人東京大学大学院工学系研究科教授
	松岡　紀雄	神奈川大学経営学部教授
	宮　　健三	慶応義塾大学大学院理工学研究科教授
	山内　喜明	弁護士

総合資源エネルギー調査会原子力安全・保安部会原子力防災小委員会
危機管理ワーキンググループ委員名簿

（敬称略、五十音順）

（主査）	廣井　脩	国立大学法人東京大学大学院情報学環・学際情報学府教授
	金重　凱之	株式会社国際危機管理機構代表取締役社長
	衣笠　達也	財団法人原子力安全研究協会放射線災害医療研究所副所長
	首藤　由紀	株式会社社会安全研究所取締役
	田中　治邦	電気事業連合会原子力部長
	内藤　香	財団法人核物質管理センター専務理事
	中込　良廣	国立大学法人京都大学原子炉実験所教授
	平野　光将	独立行政法人原子力安全基盤機構解析評価部長
	山内　喜明	弁護士
	横山　松雄	株式会社総合防災ソリューション特別参与

総合エネルギー調査会　原子炉安全・保安部会
原子力防災小委員会における検討の経緯
（「原子力施設における内部脅威への対応について」）

〈原子力防災小委員会〉

第　３回　平成１６年１２月１３日
第　４回　平成１７年　４月２５日
第　５回　平成１７年　６月２０日

〈原子力防災小委員会　危機管理ワーキンググループ〉

第　５回　平成１７年　１月１９日

第　６回　平成１７年　１月２８日
（個人情報保護関係有識者　筑波大学大学院　藤原静雄教授からの意見聴取）

第　７回　平成１７年　２月　９日
（刑事法制・刑事政策関係有識者　東京都立大学法学部長（現・首都大学東京 都市教養学部長）前田雅英教授からの意見聴取）

第　８回　平成１７年　２月２８日
（行政法関係有識者　東京大学法学部　小早川光郎教授からの意見聴取）

第　９回　平成１７年　３月２２日
（労働法関係有識者　天使大学　保原喜志夫教授からの意見聴取）

第１０回　平成１７年　３月３１日