平成１８年度厚生労働科学研究費補助金

分担研究報告書

医療放射線分野における法令整備等

含めた管理体制に関する研究

医療放射線の規制管理に対する国際動向の把握に関する研究

平成１９年３月

分担研究者　草 間　経 二

目　次

平成18年度厚生労働科学研究費補助金（医療安全・医療技術評価総合研究事業）
「医療放射線分野における法令整備等含めた管理体制に関する研究」
（主任研究者：油野民雄）

分担研究報告書
「医療放射線の規制管理に対する国際動向の把握に関する研究」

分担研究者　草間経二　社団法人　日本アイソトープ協会　総務部放射線安全課

研究要旨
IAEAより、加盟各国に検討資料としてSecurity of Radioactive Sourcesが出された。この中で、セキュリティの概念と原則が示されている。セキュリティの目的、機能が明確になり各国での検討が進むものと考えられる。また、段階的実施、すなわち線源が持っているリスクに応じたセキュリティ対策の基礎となる約３００核種のD値が示された。しかしながら、従来からの核燃料施設や原子力発電所におけるセキュリティ対策をベースに検討が進んでいるため、１）一般の人が容易に施設に接近できる、２）患者などに線源に関する情報（位置、機能など）が提供されている、３）昼間は容易に施設に出入りできるなどの病院におけるセキュリティ面での特性を考慮されているものではない。
今後の検討としては、遅延方策、検知方策について、機器に着目したセキュリティ対策を国際的に検討し、その結果を持って各セキュリティグループについて目標と方策を策定することが望まれる。
夜間と昼間とは異なる技術的方策となることを考慮する。夜間には一般の患者が出入りできない方策などは可能である。
一律に、遅延策としては２以上の物理的方策としない。管理的方策である人による監視も認めることが病院の状況にあった対策となる。

研究協力者
小林　一三　　国立国際医療センター
渡辺　浩　　独立行政法人労働者健康福祉機構　横浜労災病院

A　研究目的
IAEA等の国際機関において、放射性同位元素は医療を始め有益な目的のために世界中で使用されている。その使用には放射線被ばくによる潜在的なリスクがあり、個人、社会、環境を防護する必要があること、また、テロに利用される可能性があるとの観点から、放射性線源のセキュリティやセキュリティ確保のための規制のあり方について検討がなされており、多くの技術文書や安全基準が発行されつつある。
医療先進国である我が国が、国際的な動向を把握し技術文書や安全基準策定への協力などの国際的な貢献を行うことは、医療放射線分野においても必要である。特に今年度は最近検討が進められている密封線源のセキュリティに関する国際動向を把握し、我が国の医療現場にあった適正なセキュリティ対策を検討することにより、我が国の医療放射線安全とセキュリティ確保のための方策の取り入れに当たっての基礎資料の作成を目的とする。

B　研究方法

最近の IAEA 等の国際機関における放射性同位元素の安全とセキュリティに関する規制の動きを把握するとともに、医療分野での放射線の利用を阻害すること無く、我が国に適用する方策を検討する。特に本年度は、ここ数年密封放射性線源のセキュリティ確保に関する検討が進んでおり、この件についての IAEA において検討中である指針、技術文書の把握を行い、我が国での医療施設における医療安全に対する取り組みを考慮したセキュリティ対策を検討する。

最近のＩＡＥＡにおける検討では、原子力及び放射線源のセキュリティに関して検討が行われており、その検討結果を原子力セキュリティシリーズとして、各種出版物を刊行する予定となっている。出版物の分類としては、１）原子力セキュリティ基本（nuclear Security Fundamentals）；セキュリティ勧告の基礎をなす目的、概念、原理などを示しセキュリティ勧告の基礎をなすものである、２）勧告（Recommendations）；各国でセキュリティ基本を適用するに当たって実施できるもっとよい行動に関する勧告、３）実施ガイド（Implementing Guides）：勧告を履行するに当たり詳細な方策を与えるものである、４）技術ガイダンス（Technical Guidance）；これには３の文書から構成され、（１）参考マニュアル（Reference Manuals）：実施ガイドを各国に適用するにあたり詳細な方策やガイド、（２）訓練ガイド（Training Guides）：原子力セキュリティ分野における訓練マニュアル、（３）支援ガイド（Service Guides）：ＩＡＥＡの実施範囲に関するガイド、から構成される。

今回検討した指針、技術文書は「放射線源のセキュリティ　；ガイドライン」、「放射性物質の危険を示す量（D 値）」、「輸送時のセキュリティ対策」である。

C　調査研究の結果

C1　放射線源のセキュリティ

IAEA は各国に「放射線源のセキュリティ　；ガイドライン」を示し、各国での検討を求めている。以下に、この概要を述べる

1　目的と適用範囲

個人や社会に対して重大なリスクをもたらすかも知れない放射線源（カテゴリー１から３）に適用する。非密封線源やカテゴリー４，５線源にも適用できる内容である。

線源の製造から廃棄にいたるまで、線源の全ライフサイクルに適用する。

対策は、段階的アプローチとする。すべての線源に同じセキュリティ対策をとるのではなく、リスクが高い線源と低い線源とでは異なるセキュリティ対策となる。

2　各機関の役割と責任

セキュリティ確保のための各機関の役割と責任について述べている。

２．１　国家の役割と責任

すべての国は領域内、管轄権または管理の下にある放射線源が有効な期間中そして有効な期間の終わりまで、しっかり保護されることを確実にするのに必要で適切な対策を取ることに責任がある。これは放射線源に関するセキュリティ文化の醸成を含んでいる。

そのために国は以下のことを実施する。

・法令の整備

・規制当局への権限付与
・規制当局の機能は、利用推進機関から事実上独立する
・各規制機関の役割分担と連携の確立
・規制当局の職員財源の確立
・国内脅威評価を作成する

2．2　規制当局の役割と責任
・セキュリティ文化の醸成を促進する
・法的な要求事項を発展させるべきである。
・セキュリティガイダンス作成、整備
・職員の訓練
・放射線源の国内登録制度の確立
・情報セキュリティの方針を整備
・線源識別を操業者が実行するよう要求する
・承認プロセスは、セキュリティ要件を満たすことを確認できる手順とする
・施設のセキュリティ計画の受理
・許可発行前に、十分なセキュリティ対策が整備され、使用が終了した以降の放射線源の安全管理とセキュリティのための継続的な準備が行われることを確実にすべきである。
・申請に妥当性があることを保障する:
　申請者は放射線源を得る為の正当な理由がある;
　求めている放射線源のタイプと量は、意図されていた用途のために適切である;
　申請者は、身元が知られており、あらゆる悪意ある背景を持っていない
・立入検査計画を整備し、実行する
検査の頻度はセキュリティレベルを考慮し、過去の実績を考慮する

2．3　操業者の役割と責任
・セキュリティ対策の実施と維持に関する主要な責任をもつ。
・従業員が適切に訓練を受け、信頼性確認のための要求を満たすことを確実にする
・放射線源の存在を規定された間隔で確認
・カテゴリー1、2 の放射線源が特定可能で追跡することができるよう整える
・セキュリティ文化の醸成するべきであり、それを保障するために放射線源のカテゴリーに相応した管理システムを確立するべきである:
　セキュリティは高い優先順位を有するとして認識する;
　セキュリティに影響を与える問題はすみやかに特定され、重要度に比例した形で修正される
　セキュリティへの個人の責任ははっきり識別され、個人は適切に訓練され、能力がある。;
　組織上の構成と通信網が確立されると、組織全体のなかのセキュリティにおける情報の適切な流れとなる。
　機密情報は識別され、適切に保護される。

規制当局に要求された時には、 放射線源はセキュリティ計画に従って管理される。

3　セキュリティ概念と原則

セキュリティ原則と、抑止、検知、遅延、対応そしてセキュリティ管理などの基本的なセキュリティ機能を含むいくつかの重要な概念が詳しく説明されている。

3．1　行動規範

放射線源の安全とセキュリティに関する行動規範では、放射線源のセキュリティに関する基本的原則が示されている。：

すべての国は、個人、社会、そして環境を保護するために以下のことを確かなものとするために、適切な対策を講じるべきである。：（a）その国の領域内または、管轄区域または管理内にある放射線源はその耐用期間と耐用期間の終了時において安全に取り扱われ、安全に防護されること：かつ（b）：放射線源に関するセキュリティ文化及びセキュリティ文化の推進に関すること（行動規範7．）

すべての国は、本規範の履行において、設計者、製造者（放射線源を装備した機器の製造者と放射線源の製造者の双方）、供給者、使用者、及び使用済放射線源の取り扱いを行う者は放射線源の安全とセキュリティに対して責任を有することを強調すべきである。（行動規範１５．）

すべての国は、1つ以上の放射線源に関して、規制の喪失や悪意ある活動の可能性に基づき、その国の領域内で使用されている様々な放射線源への脅威に対して、その脆弱性を評価し、国内の脅威を明確にすべきである。（行動規範１６．）

立法や規制は特に、（g）放射線源取扱いのすべての段階において、放射線源の無許可アクセス、盗難、紛失、無許可使用・移動（譲渡）を阻止、検出(探知)、遅らせるためのセキュリティ対策のための要求事項を提供すべきである。（h）（放射線源の安全とセキュリティに関する）評価、監視、法令遵守の確認、適切な記録の保持などを通じての放射線源の安全とセキュリティの検証に関する要求事項(行動規範１９．）

すべての国は、法令により設置された規制当局が以下の権限を有することを確実にすべきである。；（b）放射線源の取扱いをするために承認申請するものに対し以下の点を求め、提出させる。（ｉ）安全評価および、（ii）セキュリティ計画または適切な評価　・・・・；（e）以下の条件を含んで、許可の発行に当たって明確であいまいでない条件を付する（iii）放射線源及び放射線源を装備している機器の設計、性能基準及び維持管理に関する最小限の要件（ix）放射線源のセキュリティに関する情報の機密性（行動規範２０．）

すべての国は規制当局が以下のことを確実にすべきである、（d）放射線源の取扱いに関連するすべての組織、個人の間にセキュリティ文化とセキュリティ文化の確立を促進し、・・・・（行動規範２２．）

3．2　セキュリティシステムの目的

セキュリティシステムの目的は、破壊活動または、危害を与えることを意図した放射線源の無許可移転を防ぐことである。

３．３　セキュリティ機能

悪意のある行為を行おうとする敵の意図から放射線源を保護するセキュリティ計画は、抑止、検知、遅延、対応及びセキュリティ管理の5つのセキュリティ機能を行うように設計されていなければならない。

・**抑止**は、敵が悪意ある行為を行おうとしたとき、その試みを思い止まらせることである。

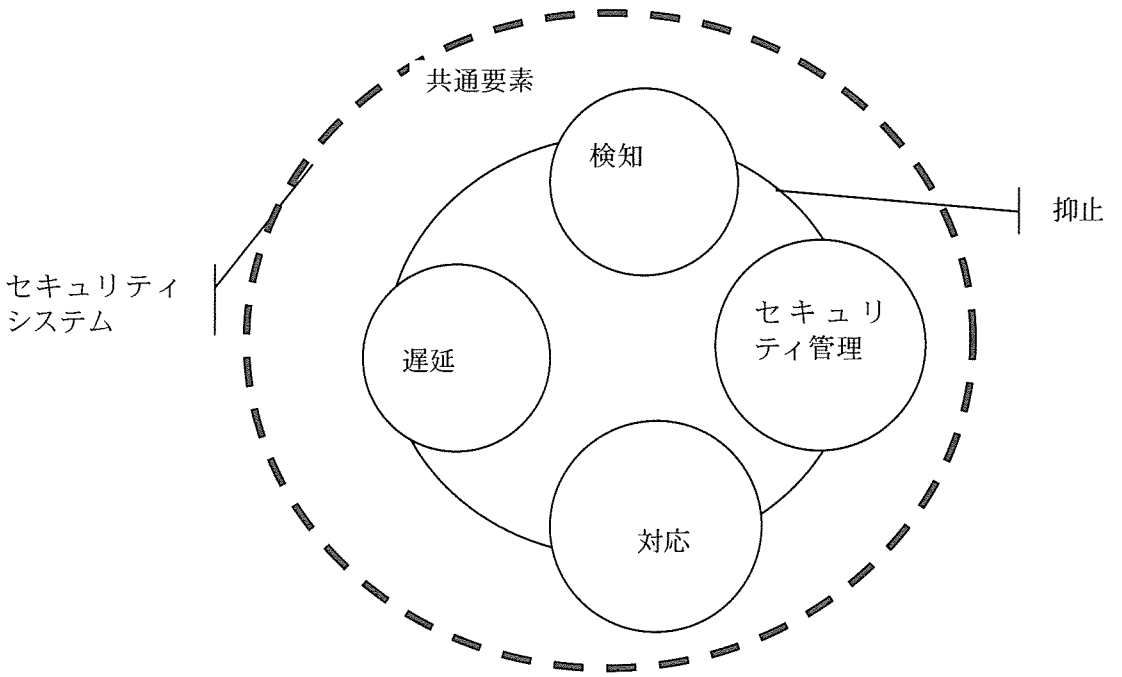
・**検知（探知）**は、放射線源の窃盗や破壊の目的となる実際の侵入や試みを発見することである。

・**遅延**は、放射線源に無許可のアクセスしたり、放射線源を(無許可)移動したり、または放射線源を破壊したりしようとする敵の試みを、障壁か他の物理的な手段によって妨害することである。

・**対応**は、敵の（悪意ある行為）を成功させることを防ぐために、検知の後で行われる行動である。敵が盗難または破壊を試みている段階で、妨害し抑止したり、敵が危害を与える結果を招く放射線源の使用を行うことまでを意味している。

・**セキュリティ管理**はセキュリティ文化の促進、（セキュリティ）政策、（セキュリティ）計画、及び放射線源へのアクセス手続き、機密情報の適切な管理、許可のない放射線の曝露の防護などがある。

セキュリティシステム



３．４　設計と評価指針

セキュリティシステムは、脅威から放射線源等を効果的に防ぐための5つの機能すべてを実行するための手段を統合すべきである：

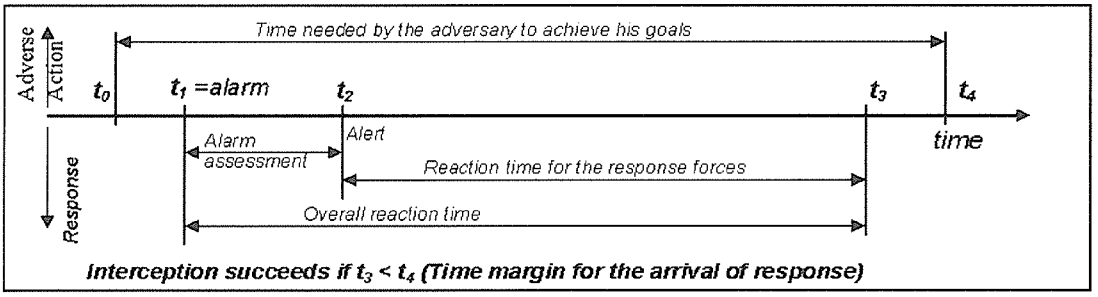
抑止は評価できない：抑止の効果は、悪意のある行為の試みを潜在的な敵に躊躇（断念）させることである。それゆえ、セキュリティシステムの設計は全体として、抑止に基づいて設計することはできない。

遅延の前の検知：悪意のある行為の完了を防ぐために配置し、遅延の機能が敵の（行為の）進行を妨害するのに十分な時間を対応部隊に与えることであるので検知は遅延に先行しなければならない。

検知は評価が必要である：直接的な人による監視を除いて、検知のほとんどの方法は、物理的な現象を監視することにより、悪意のある行為の間接徴候を、提供する。従ってそのような警報が引き起こされるときは、原因に関しては、不確実性が常にある。その結果、警報の原因を判断するために、検知は常に評価によって補完されなければならない。

対応時間に評価の時間を加えたものより長い遅延(時間)：セキュリティシステムは、それに続く遅延の対策が、十分な装備をもち、能力がある対応部隊を敵が（悪意ある）行為を完了する前に、妨害し、阻止することを可能とするに十分早く、行為を試みている敵を検知し正しく評価できれば成功である。

検知、遅延および応答の機能のこの関係は適時検知（timely detection）として知られ、図2 で記述することができる。



バランスの良いセキュリティ：バランスはセキュリティの層の位置が別の位置より強くもないし弱くもないことを意味する。

深層防御：深層の概念はまたセキュリティの階層に関連し、敵によって克服されるか、または避けられなければならない複数のセキュリティの同心層で構成されるセキュリティシステムを説明する。深部支援における防御は、セキュリティシステムの完全な失敗での結果からあらゆる単一の安全対策の失敗を防ぐ。

３．５　セキュリティに対する段階的アプローチ

最後の重要な指針は、段階的アプローチに従うべきである。そのようなアプローチは個々の放射線源と施設の脆弱性分析と設計基礎脅威の整備・応用と国内の脅威の査定に、基づいている（または放射線源と施設のクラス）のが理想的である 。

３．６　国内脅威の評価

普通、そのような評価は、内務省、国防省、交通省、および外務省のような政府機関から入ってきた情報を持つ情報機関によって、頻繁に行なわれる：法の執行；税関及び沿岸警備隊；　そして安全保障に関する責任をもつ他の政府機関そしてそれは規制当局も含む。いずれにせよ、国内脅威の評価の直接関係者、規制当局は、規制プログラムの開発における利用のために関連する情報機関によって現在の評価としての脅威を知らされるべきである。そのような国内の脅威を評価した結果は、設計基礎脅威(DBT) へ入力される。

３．７　設計基礎脅威

設計基礎脅威（DBT） は、受容しがたい結果を引き起こそうという意図を持った放射線源の無許可移動、または、放射線源を使用または貯蔵している設備の破壊活動を試みる可能性のある内部あるいは外部の敵の属性や特長について記載する。

設計基礎脅威の準備は、それぞれの国によって異なる。国内の脅威の評価と同様に、設計基礎脅威の準備は通常、情報局、警備機関、捜査当局、規制当局、操業者等が総出で行う必要である。

３．８　脆弱性の評価

脆弱性の評価は、保護のためのセキュリティシステムの評価による成果に基づいた方法である。

これらの脆弱性の評価を行なうのは対象施設、特にその技術的、業務的要請、防護の程度に加えるかもしれない、存在しているセキュリティレベルと安全面に精通した訓練された実行者であるべきである

３．９　増加した脅威

セキュリティシステムは、現在の評価された脅威に立ち向かうのに効果的であるように開発(設置)されなければならないが、しかし、脅威が増加した場合、セキュリティの状態が高められるのを確実にする準備がなされるべきである。

４　規制計画の設定

規制当局が放射線源の盗難または破壊活動の可能性を最小化する規制計画をどう確立するかについてのガイダンス。

規制計画を確立するには、規制当局は次の3つのステップ行う。

ステップ１；セキュリティ能力のレベルとそれぞれのセキュリティレベルに対するセキュリティ目標を対応させることを確立させる。；

ステップ２；対象となる放射線源に適用されるセキュリティレベル、ひいては放射線源に対するセキュリティシステムが要求するセキュリティ目標を決定する。

ステップ３；セキュリティ目標が満たされていることを操業者はどのように明らかにするかを導くため、３つのアプローチのうちひとつを選択肢し、実施する。；

４．１　ステップ１：セキュリティレベルとセキュリティ目標の決定

セキュリティレベル A は最も高い潜在的な結果を持つものであり、セキュリティレベル B は中間の潜在的結果とのそれらのためであり、C は、潜在的にもつ影響は低いが、しかしまだ相当な影響をもっている。

表1. セキュリティレベルとセキュリティ目標

セキュリティ機能	セキュリティ目標		
	セキュリティレベル A	セキュリティレベルB	セキュリティレベルC
抑止	敵を躊躇させるために検知、遅延および対応(の機能が)が統合されたセキュリティシステムの提供	敵を躊躇させるために検知、遅延および対応(の機能が)が統合されたセキュリティシステムの提供	無許可アクセスを躊躇させるように意図されている統合されたセキュリティシステムの提供
検知	放射線源または制限区域(secured area)への無許可アクセスの企ての適時検知の提供	放射線源または制限区域(secured area)への無許可アクセスの企ての適時検知の提供	
	浸入検知の適時評価の提供	浸入検知の適時評価の提供	
	紛失を検知する方法の提供	紛失を検知する方法の提供	紛失を検知する方法の提供
	緊急時対応部隊との適時連絡（手段、方法）の提供	緊急時対応部隊との適時連絡（手段、方法）の提供	
遅延	対応のために十分な遅延を行う	放射線源の無許可移動を遅延させる。	
	放射線源の場所（使用、保管）へのアクセス管理	放射線源の場所（使用、保管）へのアクセス管理	放射線源の場所（使用、保管）へのアクセス管理
対応	(緊急時)対応の即時開始	(緊急時)対応の即時開始	

	敵を妨害し、悪意ある行為の完了を防ぐ十分な適時対応を行う		
	放射線源の無許可移動または放射線源の紛失への適切な対応をする	放射線源の無許可移動または放射線源の紛失への適切な対応をする	放射線源の無許可移動または放射線源の紛失への適切な対応をする
セキュリティ管理	総合的なセキュリティプログラムの確立	総合的なセキュリティプログラムの確立	
	情報セキュリティの提供	情報セキュリティの提供	適切な情報セキュリティの提供
	個人の信頼性の確立	個人の信頼性の確立	個人の信頼性の確立

4．2　ステップ2：放射線源への適用可能なセキュリティレベルの決定

放射線源のカテゴリ分類が、セキュリティレベルを定義するときに使用される。

4．2．1　線源カテゴリに基づくセキュリティレベル

カテゴリ1～3の放射性核種に対応する放射能の閾値はＲＳ－Ｇ－1.9に示されている。

表3．一般的な利用で使用される放射線源のカテゴリ分類

セキュリティレベル	放射線源と利用	A/D (放射能/D値)	カテゴリ
A	放射性同位元素熱電発電機(RTGs) 照射装置(施設) 遠隔治療用線源 固定式マルチビーム遠隔治療用線源（ガンマナイフ）	A/D ≧ 1000	1
B	工業用非破壊検査装置 中光線量近接照射治療用線源	1000 ＞ A/D ≧ 10	2
C	固定式工業用ゲージ ボーリング検層ゲージ	10 ＞ A/D ≧ 1	3

慎重な管理	低線量近接照射治療装置（眼科小線源と永久インプラント線源を除く） 非組み込み型工業用ゲージ 骨密度測定装置 静電気除去装置	1 > A/D ≥ 0.01	4
	低線量近接治療装置（眼科小線源および永久インプラント線源） 蛍光X線装置 ＥＣＤ メスバウアー分光分析装置用線源 ＰＥＴ用チェッキング線源	0.01 > A/D and A > exempt	5

４．２．２　他の考慮すべき事柄.

放射線源のカテゴリー分けは“危険な放射線源”（危険な放射線源は、“D値”の観点から定量化されている）の概念に基づいている。しかし、悪意ある行為から生じる社会経済的な影響は、カテゴリー分けの基準からははずされている。規制当局が放射線源をセキュリティレベルに割り当てるときに、線源カテゴリーに加えて考慮すべき他の多くの要因がある。

・（敵にとって）魅力がある；
・脆弱さと脅威のレベル；
・可動性、携帯性、遠隔地の放射線源；
・放射線源の集合体、掲載されていない行為、非密封線源
・セキュリティ力学

１）魅力（Attractiveness ）

・　化学形態および物理形態－線源における放射性物質の化学・物理形態は分散を容易することがある、それゆえ敵にとってより魅力的になる。
・　放出放射線の種類－いくつかの放射性核種はアルファ線を放出するが、アルファ線は検出が難しいため、RDD(放射能拡散機器)の使用に対してはより魅力的にする。
・携帯性－遮蔽が簡単であり、簡単に移動できる放射線源は、より高い放射線量や放射能の線源を敵がより受け取りやすくし、より簡単に移動できるため、より魅力的である。
・複数の放射線源または多量の放射性物質は、敵にとって魅力的であり、セキュリティシステムに侵入したあとで、深刻な影響を引き起こすのに十分な物質を移動したり、破壊したりすることを可能にする

規制当局は、放射線源や施設に割り当てられるセキュリティレベルやセキュリティレベルに適用されるセキュリティ対策を判断する際に、（放射線源の）魅力を考慮に入れる。

2）　脆弱性と脅威レベル

強固なセキュリティシステムを持たない施設や配置である放射線源は、より敵にとって魅力的になり、その次にターゲットになりやすい。

3）　移動性、携帯性、遠隔地の線源（Mobile, Portable and Remote Sources ）

屋外利用において使用される線源は通常は機器の中に内臓されている。その機器はまた携帯性を考慮されていて、しばしば現場を移動している。上記にあるように、これら機器の取扱いの容易さと安全な施設の外での運搬におけるそれらの存在感は盗難するための魅力を敵に与える。セキュリティ目標を達成するために固定機器とは異なる対策が適用されるべきである。

離れた場所で使用される放射線源（放射性同位元素熱電発電機）は許可を得ない人間に持ち出される可能性があり、効果的な対応をとる前に領域外に運び出される。

規制当局が、放射線源にセキュリティレベルを割り当てるときに、移動性、携帯性、遠隔地利用を考慮にいれる。

4）　放射線源の集合体、掲載されていない行為使用、非密封線源

(集合体とは)製造プロセス（同じ部屋やたてもの）の途中または、貯蔵施設（例えば同じ筐体）で、放射線源同士が接近していることである。そのような状況では、規制当局は、セキュリティ対策を決める目的のための特別なカテゴリ分けを決定するために線源の放射能を合計するべきである。

用途が表３．に記載されていない場合は、規制当局は割り当てるA/D値に基づき、放射線源をカテゴリーに割り当て、続いて、セキュリティレベルに割り当てるだろう。

規制当局はカテゴリーとセキュリティレベルをA/Dに基づき非密封線源に割り当てる。

４．２．３　セキュリティ力学（Security Dynamics ）

悪意ある目的のための放射線源の利用は高くランキングされる放射線源であることは、必ずしも必要ではない。ほとんどのカテゴリー1線源は、例えば遮蔽の中または固定された施設に収納されている。放射線源を移動させるには時間がかかるし、攻撃者に十分に害を及ぼすレベルの放射線を浴びせるだろう。テロの行為を実現させるために自殺を覚悟した者でさえ、意図されたターゲットエリアで、実行可能な手段を配置するために長く生き残ることはないし、十分長くそのままでいることはないであろう。それゆえ、敵意を抱くものが、よりアクセスし易く、取り扱いすることに対する危険が少なく携帯性があり、隠すことも容易である、より低いカテゴリーの放射線源に焦点をあて、RDDを設置することを意図する可能性はある。いくつかのカテゴリー２線源、例えば、携帯性のため特別な関心がある。

４．３　ステップ３：セキュリティ方針(目標)が満たされることを示すためのアプローチ

規制当局が操業者にどのように表１で定められているセキュリティ目標を満足していることをどのように示すかを指示するために使う３つの選択的なアプローチがある。

・ 規範的アプローチは、 各放射線源のカテゴリーに適用する固有のセキュリティ対策を確立する。

・成果に基づくアプローチは、 規制当局が決定する国内の脅威の評価とDBTに基づいたセキュリティシステムの全体の方針の中にあるひとつであるが、しかし、操業者が一般に脆弱性の分析に基づくこれらの方針を達成するための対策のタイプを提案する柔軟性を許容する。 このアプローチの利点は、このアプローチの利点は、有効なセキュリティシステムが、セキュリティ対策の多くの組み合わせから構成され、それはそれぞれの施設の環境が固有であることである。また不利なことは、操業者と規制当局が比較的高度な専門知識が不可欠なことである。

・複合アプローチは規範的アプローチと成果に基づくアプローチの両方に基づいた要素を含んでいる。

４．３．１ 規範的アプローチ

１） セキュリティレベル A

セキュリティレベル Aに対して適用することを期待している、方策と目的を表4に示す。

表4　セキュリティレベル　A

セキュリティ機能	セキュリティ目標	セキュリティ方策
抑止	検出、遅延、そして敵の検出に対する対応する総合セキュリティシステムの提供	悪意ある行動から敵を抑止することを意図した方策のシステム
検出	線源や保護区域へのいかなる意図を持った承認されない接近の検出を提供する	電子的検知器、人による継続的な監視または同等の方策
	侵入検知の時機を得た評価を提供	警報が発せられたときの直ちに遅れることのなく正確な評価
	緊急時対応部隊との時機を得た通信連絡を提供	回線使用電話、自動ダイアル装置、携帯電話、無線、ポケットベルあるいは同等の手段で、情報を送信する迅速で信頼できる手段
	紛失を検出する方法を提供	計数、不正に変更されたことを表示する機器、その他同等の機器を用い線源の存在確認を毎日実施する
遅延	対応するのに十分な遅延をもたらす	壁、施錠、ドアなどの対応可能となるまでの十分な遅延をもたらす、２以上の物理的方策を講じる
	線源所在場所への出入り管理を提供	承認された者のみが出入りできる有効で厳格な管理
対応	対応をただちに開始する	適切な規制当局へのすばやい届出を確実にする方策
	悪意ある活動の達成を回避し敵を妨害するのに時機をえた対応を行う	悪意ある活動の完成に先立った敵を征服するのに充分な能力および十分な数を備えた適時のレスポンス
	線源の承認を得ない移動又は紛失に対して適切な対応を行う	承認を得ない線源の移動や紛失の報告の評価、及び必要なときには線源を復旧する十分な資源を持っての対応
セキュリティ管理	首尾一貫したセキュリティプログラムの確立	増加する脅威への備えなどの承認されたセキュリティ計画の準備と維持
	情報セキュリティの提供	機微情報（セキュリティ計画、輸送情報、セキュリティシステムの詳細）の特定と防護する手段を定める
	個人の信頼性の確立	線源保管場所や機微情報に同伴されずにアクセスできるすべての人の適切な確認

表4 (セキュリティレベルA) の中で示された方策の例を以下に示す：

抑止　いくつかの抑止する機能がそのとき明白か、可視のやり方 (例えば物理的な障壁、パトロール、出入管理) である場合、悪意ある活動を始めようとしている敵にあきらめさせることにおいて影響力がある。

検知　検知は以下のことで実施される:

侵入者検知: 電子感知器あるいは駐在のスタッフ職員による監視の使用を通じて遅延障壁に接近される前に、検知が行なわれるべきである。

評価: 一旦事象が検知されたならば、警報が発せられた原因の即時の評価がされるべきである。

通信連絡: 無許可の侵入が検知されたと評価が確定したときは、事象に関する報告が対応部隊に直ちに中継されるべきである;

毎日の計数管理: 毎日の計数又はチェックは、線源がまだ存在し不正な変更されていないことを保証する方策から成る。方策は、線源が存在していること、封印の確認、盗難検出装置、放射線の測定又は他の線源が存在していることを保証する物理的現象、などを物理的確認などがある。

遅延　以下の事項がある。

- ドア管理読取装置を動作させるために個人特定番号（パスワード　PIN）の使用;
- 電子読み取り装置を動作させるバッジシステム;
- 出入管理点でのバッジ交換する仕組み;
- ドア管理装置を起動させる生態識別の使用

障壁: 物理的障壁のバランスのとれたシステムは、防護の層を提供する。これは線源が使用される室からこれが始めることができる。いくつかの層は本質的に充分なレベルの遅れを提供するかもしれない。他のものは、窓の追加のセキュリティ又はドアの改良などの他の構造的改良のような、よりバランスのとれた改良が要求される。

対応　線源が承認を得ないで移動される可能性を最小限にするのに必要な活動および介入。

通信連絡: 適切な対応（レスポンス）は、対応の提供に責任を負う人々への本質的な詳細の即時の通知に依存する。これは、回線使用電話、オートダイヤル装置、携帯電話、無線およびポケットベルのような種々の通信手段を持っている現地保安要員によって保証されるべきである。

セキュリティ管理　セキュリティ管理には、他のセキュリティ機能に寄与するか支援する一連の方策が含まれる。これらは次のものを含んでいる:

セキュリティ計画: セキュリティ計画は各施設の操業者によって準備されているべきである。

非常事態計画: 各施設の非常事態計画は以下の事項を含む範囲で描かれるべきである。

- ·疑わしいか脅かされた悪意ある行動;
- ·線源のセキュリティを脅かす可能性のある公衆へのデモンストレーション;

·無許可の人による保護区域への侵入。これは、放射線源で移動するか妨げるように努力するものによる単純な侵入から断固とした攻撃まで及ぶ;;
·非常事態計画は適切な規制当局と共有され、定期的に訓練されるべきである。

情報セキュリティ：関連する情報(それは詳細を識別するために使用することができる公文書、コンピュータシステム上のデータおよび他のメディアを含む)を保護することがさらに必要である。:
·線源の特定の位置および在庫表;
· 関連するセキュリティ計画及びセキュリティ計画の詳細;
·セキュリティシステム(例えば侵入者警報装置の性能と設置場所);
· セキュリティプログラムの一時的又は永久の弱点;
· セキュリティ要員の配置及び事象発生時や警報時の対応策;
· 線源の移動モード、経路、予定日時;
· 非常事態計画及びセキュリティ対応方法

個人の信頼性：その人が放射線源が使用され保管されている場所、及び関連する機微な情報が保管されている場所へのエスコートがないアクセスが許可される前に、個人の信頼性は満足な身元調査によって査定されるべきです。身元調査の性質および深さは国の基準又は規制当局によって決定されたものに従うべきである。少なくとも、身元調査は、各被験者の確認、人物証明書および信頼性を決定するための確認および参照の確認を含んでいるべきである。すべてのレベルの職員が責任を持って信頼され行動し続け、どんな関係も、この情況の中で、適切な規制官署に知らされることを保証するために、そのプロセスは、管理者と監督者によってずっと続いている注意によって定期的に見直しされ支援されるべきである。

2） セキュリティレベル B

規制当局が、セキュリティレベルBの方策を適用することを要求する線源に適用される目標と方策を表5に示す。

表5．セキュリティレベル　B

セキュリティ機能	セキュリティ目標	セキュリティ方策
抑止	検出、遅延、そして敵の検出に対する対応する総合セキュリティシステムの提供	悪意ある行動から敵を抑止ししようとする方策のシステム
検出	線源や保護区域へのいかなる意図を持った承認されない接近の検出を提供する	電子的検知器、人による監視または同等の方策
	侵入検知の時機を得た評価を提供	警報が発せられたときの直ちに遅れることのなく正確な評価
	紛失を検出する方法を提供	計数、不正に変更されたことを表示する機器、その他同等の機器を用い線源の存在確認を毎週実施する
	緊急時対応部隊との時機を得た通信連絡を提供	回線使用電話、自動ダイアル装置、携帯電話、無線、ポケットベルあるいは同等の手段で、情報を送信する迅速で信頼できる手段
遅延	線源の承認を得ない移動を遅延させる	壁、施錠、ドアなどの線源の承認を得ない移動を遅延させる２つの物理的方策システム（付録１参照）
	線源所在場所への出入り管理を提供	承認された者のみが出入りできる有効で厳格な管理
対応	対応をただちに開始する	適切な規制当局へのすばやい届出を確実にする方策
	線源の承認を得ない移動又は紛失に対して適切な対応を行なう	承認を得ない線源の移動や紛失の報告の評価、及び必要なときには線源を復旧する十分な資源を持っての対応
セキュリティ管理	首尾一貫したセキュリティプログラムの確立	増加する脅威への備えなどの承認されたセキュリティ計画の準備と維持
	情報セキュリティの提供	機微情報（セキュリティ計画、輸送情報、セキュリティシステムの詳細）の特定と防護する手段を定める
	個人の信頼性の確立	線源保管場所や機微情報に同伴されずにアクセスできるすべての人の適切な確認

3）　セキュリティレベル　C

セキュリティレベルCに適用される方策と目標を表６に示す。

表　６：セキュリティレベル　C

セキュリティ機能	セキュリティ目標	セキュリティ方策
抑止	承認を得ないアクセスを抑止しようとする総合セキュリティシステムの提供	線源へのアクセスを得ようとする承認を得ない人を抑止しようとする方策システム
検知	紛失を検知する手段を提供	計数管理、不正に変更されたことを示す機器または同等の方策を使用して線源が存在していることの半年ごとの確認
遅延	線源所在場所への出入り管理	承認された者のみの有効で厳格な出入り管理
対応	承認を得ない線源の移動や紛失に対する適切な対応	線源の承認を得ない移動や紛失の報告の評価、必要に応じて線源を復旧させるのに十分な資源を持っての対応の開始
セキュリティ管理	適切な情報セキュリティ	機微情報防護の適切な手段の確定
	個人の信頼性	線源のところに出入する者の適切なチェック

４．３．２　実績に基づくアプローチ

規制当局は、表1に示すセキュリティ目標に合致することを実証することを実績に基づいたアプローチの使用を指定することに選択してもよい。このアプローチを使用して、国は全国脅威評価を実施し、放射線源のために設計基礎脅威(DBT)を開発し、各セキュリティレベルのシステム・セキュリティ目標を指定するで。その後、操業者は、DBTから保護するべきセキュリティ対策を設計するおよび適用するために脆弱性評価を導くことに責任を負う。このプロセスは、それらが表4～6の中で確立したが、抑制、検知、遅延、対応およびセキュリティ管理のセキュリティ機能を含んでいるべきであるセキュリティ対策の異なるセットに帰着するかもしれない。

操業者に、専門のアドバイザー、および必要な方策を設計し実施し、かつ一貫性と規則に従っていることの持続した記録を実証しているところで、このアプローチはより有効に機能するであろう。規制当局は、セキュリティ計画や適切な間隔での見直しなど、承認された方策が明確に文書されていること保証するべきである。

4．3．3　複合アプローチ

多くの国は、そのセキュリティ目標に合致するセキュリティ方策を適用するために、規範に基づくものと実績に基づくアプローチの両方を組み合わせたいと思うかもしれません。例えば、国は、悪意のある使用により低い可能性の帰結を備えた放射線源のために規範に基づくアプローチを使用することができたが、最も危険な線源への実績に基づいたアプローチを適用することができる。国は全国脅威評価を実施し、設計基礎脅威を開発するであろう。その後、オペレーターは、制止、検知、遅れ、レスポンスおよびセキュリティ管理のセキュリティ機能の点から定義された1セットのセキュリティ目的に会うために適切なセキュリティ対策を適用することに、よく責任を負う。その後、操業者は、抑制、検知、遅延、対応およびセキュリティ管理のセキュリティ機能の点から定義された1セットのセキュリティ目標に適合するセキュリティ対策を適用することに、責任を負う。

5　3つのアプローチの共通要素

1）　内部脅威の認識

内部脅威に対して防御するのは難しいかもしれません。また、それはしたがってセキュリティシステムを設計する場合、特別の認識を与えられるべき事項である。

2）　セキュリティ文化

活動的で有効なセキュリティ文化は、組織内のすべてのスタッフおよび管理のための目的であるべきである。

·放射線源のセキュリティに対する責任が役員会あるいは取締役に割り当てられること

·操業者組織の中のセキュリティ文化の不可欠な部分としての上級の管理による支持;

·組織に対する法令や規則に定められるセキュリティの責任はドキュメント化され、関連する管理者、スタッフすべての従業員及び契約者の目に留まることを保証すること。

· セキュリティ管理者、守衛及びセキュリティに二次的に責任のあるすべての人員への訓練を提供する。

·そのセキュリティ改良あるいは成功、スタッフと契約者のためのセキュリティ目的として書き留められることを保証し

·スタッフと契約者の研修課程にセキュリティに関する事項を含んでいること。