

実施指針

核物質及び原子力施設の物理的防護
(INFCIRC/225/Revision 5 の実施)

本翻訳版発行に当たっての注記事項

A：本翻訳版は非売品である。

B：本翻訳版は、Physical protection of nuclear material and nuclear facilities (implementation of INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 27-G ©International Atomic Energy Agency, 2018 の日本語訳である。

本翻訳版は、原子力規制庁により作成されたものである。本翻訳版に係る IAEA 出版物の正式版は、国際原子力機関 (IAEA) 又はその正規代理人により配布された英語版である。IAEA は、本翻訳版に係る正確性、品質、信頼性又は仕上がりに関して何らの保証もせず、責任を持つものではない。また、本翻訳版の利用により生じるいかなる損失又は損害に対して、これらが当該利用から直接的又は間接的・結果的に生じたものかを問わず、何らの責任を負うものではない。

C：著作権に関する注意：本翻訳版に含まれる情報の複製又は翻訳の許可に関しては、オーストリア国ウィーン市 1400 ウィーン国際センター (私書箱 100) を所在地とする IAEA に書面により連絡を要する。

D：本翻訳版は、業務上の必要性に基づき、原子力規制庁が IAEA との合意に基づき発行するものであり、唯一の翻訳版である。

E：原子力規制庁は、本翻訳版の正確性を期するものではあるが、本翻訳版に誤記等があった場合には、正誤表と合わせて改訂版を公開する。また、文法的な厳密さを追求することで難解な訳文となるものは、分かりやすさを優先し、本来の意味を損なうことのない範囲での意識を行っている箇所もある。

なお、本翻訳版の利用により生じるいかなる損失又は損害に対して、これらが当該利用から直接的又は間接的・結果的に生じたものかを問わず、原子力規制庁は何らの責任を負うものではない。

Disclaimer

A: "NOT FOR SALE"

B:

"This is a translation of Physical protection of nuclear material and nuclear facilities (implementation of INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 27-G ©International Atomic Energy Agency, 2018.

This translation has been prepared by Nuclear Regulation Authority of Japan. The authentic version of this material is the English language version distributed by the IAEA or on behalf of the IAEA by duly authorized persons. The IAEA makes no warranty and assumes no responsibility for the accuracy or quality or authenticity or workmanship of this translation and its publication and accepts no liability for any loss or damage, consequential or otherwise, arising directly or indirectly from the use of this translation".

C:

"COPYRIGHT NOTICE: Permission to reproduce or translate the information contained in this publication may be obtained in writing from the International Atomic Energy Agency, Vienna International Centre, P.O. Box 100, 1400 Vienna, Austria"

翻訳版について

- a) “defence in depth”については、原子力安全の分野において「深層防護」と訳される場合が多い。しかし、この用語の定義は、原子力安全における定義と、核セキュリティにおける定義とは原則的に似ている概念ではあるが、具体的な定義は IAEA 安全基準シリーズで使用されている概念と同じではないということを、IAEA は本書の中で言及しており（パラグラフ 3.102 の前段）、翻訳版においては「多層防護（defence in depth）」と表記した。
- b) “Protected area”については、「防護区域」と訳語を用いることができるが、実用炉規則等の用例における「防護区域」と概念が異なることから、原文のまま“Protected area”と表記した。
- c) 原文の、IAEA 加盟国リスト及び原文の購入先リストのページについては、本翻訳版に含めていない。

IAEA 核セキュリティ・シリーズ

核物質、その他の放射性物質、関連する施設若しくは関連する事業に係る又は向けられた、犯罪若しくは意図的な無許可の行為の防止又は検知に係る核セキュリティの問題は、**IAEA 核セキュリティ・シリーズ**で取り扱われる。これらの文書は、例えば「核物質防護条約」及び「改正核物質防護条約」、「核テロリズム防止条約」、「国連安保理決議 1373 号」及び「国連安保理決議 1540 号」並びに「放射線源の安全とセキュリティに関する IAEA 行動規範」などの、核セキュリティに関する国際文書と整合が取れており、かつ、これらを補完するものである。

IAEA 核セキュリティ・シリーズの区分

IAEA 核セキュリティ・シリーズは、次の区分で出版される。：

- **核セキュリティ基本文書**は、加盟国の核セキュリティ体制の目的、その体制の基幹的な要素を明記する。それらは、核セキュリティ勧告の基礎事項を提示する。
- **核セキュリティ勧告文書**は、加盟国が核セキュリティ基本文書と整合性のある有効な国内の核セキュリティ体制を達成し維持すべき措置を提示する。
- **実施指針**は、加盟国が核セキュリティ勧告文書で提示された措置を実施し得る手法についての手引きを提供する。従って、それらは核セキュリティの広範な分野に関係している勧告にどのように適合するかに関心を合わせている。
- **技術手引**は、実施指針で提示された手引きを補完するための具体的な技術的テーマの手引きを提供する。それらは、必要な措置をどのように実施するかの詳細に関心を合わせている。

草案及びレビュー

核セキュリティ・シリーズ文書の準備及びレビューは、IAEA 事務局、加盟国からの専門家（文書の起草時に事務局を支援する者）、及び文書の草案をレビューし承認する核セキュリティ・ガイダンス委員会（NSGC）が関係している。必要に応じて、参加制限のない会議も、草案文面をレビューし話し合う加盟国及び関連する国際組織の専門家に機会を提供するために開催される。さらに、ハイレベルの国際的なレビューと合意を確実にするために、事務局は、120 日間の正式なレビューについてすべての加盟国に草案の文面を提示する。

各文書について、事務局は、NSGC が準備及びレビュー作業の一連の段階で承認する以下の事項を準備する。

- 新規に作成又は改訂しようとする文書、その目的、範囲及び内容を述べている、骨子並びに作業計画の加盟国向け提示のための文書案
- 加盟国のコメントを考慮した最終文書案
- 120 日の協議期間のコメント用の加盟国向け提示のための文書案

IAEA 核セキュリティ・シリーズの文書の起草及びレビューの過程は、秘密保持に配慮するとともに、核セキュリティが全般的及び特定の国家的セキュリティの問題と密接に関連付けられることを認識している。基本的な考慮は、関連する IAEA の安全基準及び保障措置活動が、文書の技術的な内容の中で考慮されるべきであるということである。

特に、安全とのインターフェイスがある分野に取り組んでいる核セキュリティ・シリーズ文書（インターフェイス文書として知られている）は、NSGC だけではなく、関連する安全基準委員会によっても前述の各提示段階でレビューされる。

核物質及び原子力施設の物理的防護
(INFCIRC/225/Revision 5 の実施)

IAEA 核セキュリティ・シリーズ No. 27-G

核物質及び原子力施設の物理的防護 (INFCIRC/225/Revision 5 の実施)

実施指針

国際原子力機関
ウィーン 2018

著作権の表示

すべての IAEA の科学技術関連文書は、1952 年にベルンで採択され、1972 年にパリで改訂された万国著作権条約の条項で保護されている。その後、著作権は電子的及び仮想的な知的財産を含めるように、ジュネーブの世界知的所有権機関により拡張された。IAEA 文書の印刷媒体若しくは電子媒体に含まれる文面の全部又は一部分を使用するためには、許可を取得しなければならず、通常、著作権使用料の協定書の対象となる。非営利目的の複製及び翻訳の提案は、歓迎され、ケースバイケースで検討される。問合せは次の IAEA 出版部に送付して下さい。

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
<http://www.iaea.org/books>

© IAEA, 2018
Printed by the IAEA in Austria
April 2018
STI/PUB/1760

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Physical protection of nuclear material and nuclear facilities
(implementation of INFCIRC/225/Revision 5) / International Atomic Energy
Agency.
Description: Vienna : International Atomic Energy Agency, 2018. | Series: IAEA
nuclear security series, ISSN 1816-9317 ; no. 27-G | Includes bibliographical
references.
Identifiers: IAEAL 18-01138 | ISBN 978-92-0-111516-4 (paperback : alk. paper)
Subjects: LCSH: Nuclear facilities — Security measures. | Radioactive substances
— Law and legislation. | Radioactive substances — Safety regulations.
Classification: UDC 341.67 | STI/PUB/1760

序 文

天野之弥 事務局長

IAEA 憲章の下での IAEA の第一の目的は、「全世界における平和、保健及び繁栄に対する原子力の貢献を促進し、及び増大すること」である。我々の作業は、核兵器の拡散を防止することと原子力技術が、例えば健康及び農業の等の分野で、平和の目的で利用されることを確実にすることの両方を含む。すべての核物質及びその他の放射性物質、並びにそれらが保持されている原子力施設が、安全に管理され、かつ、犯罪又は国際的な不法行為に対して適切に防護されることが最も重要である。

核セキュリティは、個々の国の責任であるが、有効な核セキュリティ体制を確立している及び維持している国を支援するために国際的な協力が不可欠である。そのような協力を促進すること及び国への支援を提供することにおける IAEA の中心的役割は、よく認識されている。IAEA の役割は、IAEA の広範なメンバーシップ、命令、独自の専門知識、並びに技術的支援及び専門家、実践的な手引きを各国に提供している長年の経験を反映する。

2006 年以来、IAEA は、有効な国内の核セキュリティ体制を確立する各国を支援するために、核セキュリティ文書を発行してきている。これらの文書は、例えば「核物質防護条約」及び「改正核物質防護条約」、「核テロリズム防止条約」、「国連安保理決議 1 3 7 3 号」及び「国連安保理決議 1 5 4 0 号」並びに「放射線源の安全とセキュリティに関する IAEA 行動規範」などの、核セキュリティに関する国際文書を補完するものである。

手引きは、それが核セキュリティの良好事例についての意見の一致を反映することを確実にする、IAEA 加盟国からの専門家の活発な関与で策定される。IAEA の核セキュリティ・ガイダンス委員会（2012 年に設置され、加盟国の代表者で構成される）は、核セキュリティ文書が策定されるときにそれらの素案をレビューし承認する。

IAEA は、平和的な原子力技術の便益が、世界中の人々の健康、福祉及び繁栄を向上させるために提供されることを確実にするために、加盟国と一緒に活動を続けて行く。

編集上の注記

IAEA の核セキュリティ・シリーズで発行される手引きは、各国を法的に拘束しないが、各国は、国際的な法的手段の下での義務を満たすことにおいて、及び国内での核セキュリティについての責任を果たすことにおいて、それらを促進するために手引きを使用してもよい。「should」の文で表わされた手引きは、国際的な良好事例を表そうとしたものであり、推奨された措置又は同等な代替措置を取ることが各国にとって必要であるという国際的な意見の一致を示そうとしている。

セキュリティに関係した用語は、それが出現する文書の中、又はその文書が下支えする上位の手引きの中で定義されるように理解されるべきである。そうでなければ、単語は一般に理解されている意味で用いられる。

付録は、文書の不可欠な部分を形成しているとみなされる。付録の資料は、本文と同じ地位を有する。付属文書は実践的な例又は追加的な情報若しくは説明を提供するために使用される。付属文書は本文書に不可欠ではない。

細心の注意が本文書に含まれている情報の正確さを維持するために払われたが、IAEA も加盟国も、本文書の使用によって生じる影響についての責任を負わない。

国又は地域の特別な名称の使用は、そのような国若しくは地域の、それらの機関若しくは団体の、又はそれらの国境の設定の法的地位についての、出版者の IAEA による判断を意味しない。特定の会社又は製品の名称（登録されているかどうかを問わず）の言及は、所有権を侵害する意図を意味しないし、言及は IAEA 側の推薦又は推奨として解釈できない。

目 次

1.	はじめに.....	1
	背景 (1.1~1.3)	1
	目的 (1.4)	1
	範囲 (1.5~1.7)	1
	構成 (1.8~1.9)	2
2.	国の物理的防護体制の目的 (2.1~2.5)	3
3.	核物質及び原子力施設の物理的防護のための国の核セキュリティ体制の要素 (3.1~3.4)	5
	国の責任 (3.5~3.7)	5
	物理的防護の責任の割り当て (3.8~3.11)	6
	立法上及び規制上の枠組み (3.12~3.49)	7
	国際協力及び支援 (3.50~3.54)	15
	脅威の同定及び評価 (3.55~3.63)	16
	リスクベースの物理的防護システム (3.64~3.103)	18
	物理的防護体制の持続 (3.104~3.119)	33
	核セキュリティ事案についての計画、準備及び事案への対応 (3.120~3.126)	37
4.	原子力施設のための統合された物理的防護システムの策定、実施及び維持 (4.1~4.3)	39
	事業者の全般的な責任 (4.4~4.13)	39
	防護組織 (4.14)	41
	物理的防護システムの策定及び実施の手順 (4.15~4.22)	42
	物理的防護システムの要件の同定 (フェーズ1) (4.23~4.32)	45
	物理的防護システムの設計及び評価 (4.33~4.59)	48
	物理的防護システムの主要な機能 (4.60~4.70)	54
	行方不明又は盗取された核物質の捜し出し及び回収 (4.71~4.75)	56
	妨害破壊行為の放射線影響の緩和又は最小化 (4.76~4.82)	58
	物理的防護措置 (4.83~4.123)	59
	核セキュリティのための核物質の計量及び管理 (4.124~4.132)	70
	機微情報のセキュリティ (4.133~4.139)	72
	コンピュータ・ベースのシステムの防護 (4.140~4.146)	73
	安全とセキュリティとのインターフェイス (4.147~4.153)	74
	セキュリティ計画 (4.154~4.161)	76
	付録 I : セキュリティ計画.....	78

付録 II : 危機管理計画の例.....	87
付録 III : 核物質の加算又は集計.....	89
付録 IV : 勧告文書との相互参照.....	93
参考文献.....	97

1. はじめに

背景

1.1. IAEA 核セキュリティ・シリーズは加盟国に対して、国の核セキュリティ体制の確立、持続及び見直し、並びに、必要に応じて、その体制の強化に際して、加盟国を支援するための手引きを提供する。また、このシリーズは、拘束力のある、及び拘束力のない国際文書の下での、加盟国の義務及び責務の履行に際しての加盟国に対する手引きも提供する。

1.2. 核物質及び原子力施設の物理的防護は、当該の物質及び施設を有する国々の核セキュリティ体制の重要な部分である。IAEA 核セキュリティ・シリーズ No. 13 「核物質及び原子力施設の物理的防護に関する核セキュリティ勧告 (INFCIRC/225/Revision 5)」 [1]は、2011 年に IAEA によって出版された。また、タイトルによって示されるように、その勧告文書は、「核物質防護条約」の下での及び、その条約の 2005 年改正の発効後は、改正条約の下での加盟国の義務を満たす上での、加盟国のための手引きである IAEA INFCIRC/225 の改訂第 5 版としての役目も果たす。

1.3. 本文書は、勧告[1]を実施する上での、加盟国への一連の手引きの中の主要な「実施指針」である。いくつかの既存の実実施指針及び技術手引の文書は、例えば設計基礎脅威、内部脅威に対する措置、核セキュリティ文化及び枢要区域の同定など、核物質及び原子力施設の物理的防護に関連する特定の題目を扱っている。本実施指針は、これらの主要な側面のいくつかを紹介し、物理的防護におけるそれらの役割の概説を提供し、また、適切な場合に、より具体的な手引きのためにテーマに沿った指針を参照している。

目的

1.4. 本文書の目的は、加盟国の国の物理的防護体制を確立し、強化し、及び持続すること、並びに、事業者の物理的防護システムを含む、関連するシステム及び措置を実施することについて、加盟国及びその所管当局を支援するための、手引き及び助言を提供することである。本文書の一部の部分は、加盟国とその所管当局との間の責任の割り当てについての国ごとの違いを認識して、このことについて具体的に言及することを、意図的にしていない。各国は、それぞれの所管当局に物理的防護の責任を割り当てること及び、所管当局の責任を文書化することにおいて、正確で漏れのないようにすべきである。

範囲

1.5. 本実施指針は、次の事項に対する、原子力施設並びに使用中及び貯蔵中の核物質の物理的防護に適用する。

- (a) 核爆発装置を製造することを意図した核物質の不法移転
- (b) 放射線影響を生じる核物質及び原子力施設の妨害破壊行為

本実施指針はまた、行方不明の核物質の捜し出し及び回収、並びに原子力施設での妨害破壊行為の放射線影響の緩和又は最小化での協調的な対応に寄与することがある関連措置に関するいくつかの助言の提供もする。

1.6. 本文書は、次の事項の詳細な手引きを含んでいない。

- (a) 原子力施設の外での輸送中の核物質の物理的防護（そのような防護は具体的な手引き[2]で扱われる）
- (b) 潜在的なサイト外での拡散のための核物質の不法移転に対する防護（そのような防護は放射性物質のセキュリティに関する手引き[3]で扱われる）

本実施指針は、施設の立地選定又は施設の設計での核セキュリティ上の検討への詳細な手引きを提供していない。施設の存続期間の出来るだけ早い段階で物理的防護の原則を統合することは、一般に「セキュリティ・バイ・デザイン（設計によるセキュリティ）」と呼ばれている。

1.7. 加盟国は、その国の領域内の核物質及び原子力施設に、例えばこれらの攻撃対象の経済的な重要性、評判に関する問題、又は原子力発電の喪失の潜在的影響など、その他の様々な理由で、防護を要求することを決定することがある。本文書は、そのような追加的な懸念への対処への手引きを提供していない。

構成

1.8. 本実施指針の構成は、大まかに、上位文書である勧告文書[1]の構成に従うよう意図されているが、次のように、正確にそうしているわけではない。

- (a) 原子力施設の外での輸送中の核物質の防護は本指針の範囲外である。
- (b) 本指針は、単独のセクションで、核物質の不法移転に対する防護及び妨害破壊行為に対する防護のための、統合された、リスクベースの手法を記載している。勧告文書[1]では、これらの2つの課題は2つの別々になったセクションで示されている。

1.9. 本文書の構成は次のとおりである。この「はじめに」の後、セクション2は、物理的防護の目的、並びに核物質の不法移転及び原子力施設の妨害破壊行為のリスクの管理についての全体的な手法を述べる。セクション3は、核セキュリティ体制の物理的防護の要素の、加盟国及びその所管当局への手引きを提供する。この手引きは勧告文書[1]に提示された基本原則に基づいている。セクション4は、事業者の物理的防護システムの手引きを提供し、体系的かつ統合された手法を述べる。付録Iは、事業者のセキュリティ計画の代表的な内容の注釈付きの骨子を提供する。付録IIは、危機管理計画についての同様な手引きを提供する。付録IIIは、核物質を分類し、不法移転に対する防護の適切なレベルを決定するために使用され得る、核物質の集計の説明を提供する。付録IVは、勧告文書[1]と本実施指針との間のパラグラフの相互参照の表を示す。

2. 国の物理的防護体制の目的

2.1. 参考文献[1]に規定された、国の物理的防護体制¹の4つの目的は、「改正核物質防護条約」並びに、2001年9月にIAEAの理事会及び総会によって承認された「物理的防護の目的及び基本原則」にも記載されている：

「2.1. 国の核セキュリティ体制の全体的な目的は、核物質及びその他の放射性物質に関係する悪意のある行為から人、財産、社会及び環境を防護することにある。国の核セキュリティ体制の基幹的な構成要素である国の物理的防護体制の目的は、次のとおりであるべきである。

- 不法移転に対して防護すること。核物質の盗取及びその他の不法取得に対する防護
- 行方不明の核物質を捜し出して回収すること。行方不明の又は盗取された核物質を捜し出し、必要に応じて、回収するための迅速かつ包括的な措置の実施を確実にすること。
- 妨害破壊行為に対して防護すること。妨害破壊行為に対する核物質及び原子力施設の防護。
- 妨害破壊行為の影響を緩和又は最小化すること。妨害破壊行為による放射線影響の緩和又は最小化。

「2.2. 国の物理的防護体制は、これらの目的を以下のことによって達成するようにすべきである。

- 抑止措置及び機微情報の保護による、悪意のある行為の防止
- 検知、遅延及び対応を統合したシステムによる、悪意のある行為の企て又は悪意のある行為の処置、
- 悪意のある行為の影響緩和

「2.3. 上記の目的は、核セキュリティでカバーされる異なったリスクを考慮に入れて、統合されかつ協調的な方法で取り組まれるべきである。」 [1]

¹歴史的には、「物理的防護」という用語は、現在「核物質及び原子力施設の核セキュリティ」として知られているものを説明するために使用されており、(INFCIRC/225の改訂第5版でもある)参考文献[1]は、(核物質の不法移転、又は核物質若しくは原子力施設の妨害破壊行為に関連する核セキュリティ体制の側面についての「物理的防護体制」という用語の使用を含み、)全体に亘って「物理的防護」という用語を使用している。INFCIRC/225/Revision 5の実施のガイダンスとしての本文書の認知の助けとなるために、「物理的防護」という用語が、核物質の不法移転又は核物質もしくは原子力施設の妨害破壊行為に対する措置に関連する核セキュリティの側面を指すのに、ここで使用されている。したがって、例えば、国の「物理的防護体制」は、国の当該措置に関連する核セキュリティ体制の部分からなっている。

2.2. 核セキュリティの観点から、核物質の使用及び原子力施設に関連する2つの主なリスクは、核爆発装置の潜在的な使用のための核物質の不法移転の、並びに、受容できない放射線影響を生じる物質及び／又は施設の妨害破壊行為のリスクである。これらのリスクの管理は、核物質及び原子力施設に関連する核セキュリティについての基本的な基礎である。もし、ある国が国の境界内に核物質及び原子力施設を受け入れることを決定したら、その国は、不法移転からのそれらの物質の防護についての、及び、放射性核種の放出を生じる妨害破壊行為からのそれらの施設及び物質の防護についての責任も受け入れる。

2.3. 参考文献[1]は、国が、不法移転及び妨害破壊行為に対する防護に関連している上記の目的を達成するために、リスク管理手法を採用することを勧告している。この手法は、リスクの特徴付けについての3つの側面（脅威、潜在的影響及び脆弱性）に対処すべきである。参考文献[1]は以下の事項に関する勧告を含んでいる。

- (a) 脅威評価及び設計基礎脅威
- (b) 核物質の不法移転の潜在的影響（物質区分表を使用して決定される）及び妨害破壊行為の潜在的影響（放射線影響の等級化の手法を使用して決定される）、それに関して、等級別手法の使用及び相応の物理的防護措置の適用を手助けすること。
- (c) 有効な物理的防護システムによって、悪意のある行為を成功裏に完遂するために脅威によって悪用され得る、原子力施設の中の攻撃対象の脆弱性に対処すること。

2.4. 参考文献[1]の勧告を実施することにより、国は、核物質に又は原子力施設に向けられた悪意のある行為から生じるリスクを適切に管理するはずである。しかしながら、そのようなリスクを適切に管理するために、国は、等級別手法を考慮して、その国独自の詳細な核セキュリティの目的を設定する必要がある。

2.5. リスクを低減するために、原子力施設の事業者は、敵対者に魅力的である核物質を魅力のない核物質に置き換える、妨害破壊行為の事案においてより少ない放射線影響を生じる核物質を使用するための、及び／若しくはその他の特徴を有する施設を設計する、並びに／又は、より堅牢な物理的防護システムを築く場合がある。さらに、諜報及び核セキュリティの所管当局は、悪意のある行為の計画が原子力施設で実施される前に、それを計画をしている敵対者を検知し阻止するために、密接に連携することがある。国の核セキュリティ体制の中で基本原則のすべてを実施すること及び、原子力施設で適切な物理的防護措置を実施することは、悪意のある行為から原子力施設を防護することの全体的な目的を果たす。

3. 核物質及び原子力施設の物理的防護のための国の核セキュリティ体制の要素

3.1. 参考文献[1]は、物理的防護体制を次のように定義している。

「次のものを含む国の体制：

- 核物質及び原子力施設の物理的防護を律する立法上及び規制上の枠組み
- 立法上及び規制上の枠組みの実施を確実にする責任のある国内の機関及び組織
- 施設及び輸送の物理的防護システム」

3.2. 国の核セキュリティ体制は、物理的防護と核物質の計量及び管理との間の、並びに、物理的防護と安全との間のインターフェースの適切な処置も規定すべきである。国は、核物質の計量及び管理、安全並びに核セキュリティの要件が対立し合わないこと、及び、これらの要素ができる限り互いに支え合うことを、確実にする責任を有する。

3.3. このセクションは、

- (a) 参考文献[1、4]に示された、使用中及び貯蔵中の核物質の並びに原子力施設の物理的防護に関係する、国の核セキュリティ体制の基本原則及びその他の基幹的な要素を記載する。
- (b) 核物質及び原子力施設の物理的防護に適用するものとして、各原則の国の実施の手引きを提供する。

3.4. 核物質及び原子力施設についての、国の核セキュリティ体制の目的に合致するために、国は、国の物理的防護体制の確立、実施、維持及び持続可能性に関する要件を策定すべきである。これに関しての国の責任は、参考文献[1]の3つの別々のセクション（3、4及び5）で扱われているが、実施手引きは、この単独のセクションのここに、まとめられている。

国の責任

「国内の物理的防護体制の確立、実施及び維持に関する責任は、全てその国にある。」（基本原則 A：国の責任）

「3.1. 国の物理的防護体制は、使用中及び貯蔵中、及び輸送中の全ての核物質並びに全ての原子力施設を対象とする。国は、不法移転及び妨害破壊行為に対して核物質及び原子力施設の防護を確実にすべきである。」 [1]

3.5. 国は、立法上及び規制上の枠組みを確立すること、1つ又は複数の所管当局に規制の責任を委任すること、並びに、物理的防護システムの実施のための第一の責任を原子力施設の事業者割り当てることによって、国の責任を履行する。

3.6. 核物質についての包括的な核セキュリティ体制は、核物質の使用及び（原子力施設での、を含む）貯蔵を越えて、輸送中の核物質の物理的防護にまで及ぶ。国は、輸送についての包括的な物理的防護システムも確立され、実施され、及び維持されることを確実にすべきである。そのようなシステムは、2つの **Protected area** の間での、区分 I 及び II の核物質の施設内移動に適用すべきである。原子力施設の事業者は、核物質の荷送人又は受取人として、施設の内外へ輸送されている核物質の物理的防護についての一定の責任も有することがある。追加的な手引きは参考文献[2]で提供されている。

3.7. 参考文献[1]の paragraph 3.2 は、次のように述べている。

「国の物理的防護体制は、脅威の変化並びに物理的防護の手法、システム及び技術においてなされた進歩、さらに新しいタイプの核物質及び原子力施設の導入も反映するために定期的にレビューされ、更新されるべきである。」

物理的防護体制をレビューすること及び更新することの理由の 1 つの例は、唯一の原子力施設が、区分 III の核物質だけを保有している研究炉のみである国が、原子力発電所を建設の決定した場合である。原子力発電所について必要とされる、物理的防護のより高いレベルがは、体制のレビューを必要とするであろう。別の例は、 paragraph 3.55~3.63 に述べるような、脅威の変更であろう。

物理的防護の責任の割り当て

「3.8. 国は、対抗部隊を含む関係政府機関の関与する全てのレベル内の、及び事業者の、場合によっては運搬人の物理的防護の責任を明確に規定して割り当てるべきである。国の物理的防護体制内の責務の適切な統合及び協調について対策がなされるべきである。特に、武力対抗の責任がある組織が事業者と別である場合は、関連する組織間の明確な責任分担が確立され、記録されるべきである。」 [1]

3.8. 国は、少なくとも次の事項に関して、関係する所管当局及びその他の政府機関に物理的防護の責任を割り当てるべきである。

- (a) 設計基礎脅威及び／又は脅威評価の策定及び維持
- (b) 原子力施設並びに使用中の及び貯蔵中の核物質の許認可
- (c) 物理的防護システムの検査及び評価
- (d) 対抗部隊及び緊急時対応組織を含む、核セキュリティ事案への対応
- (e) 核物質の計量及び管理とのインターフェイスの処置
- (f) 原子力安全とのインターフェイスの処置
- (g) 原子力施設並びに使用中の及び貯蔵中の核物質の物理的防護に関連する情報及びコンピュータ・セキュリティの処置
- (h) 職員の個人の信頼性の判定
- (i) 許可要件及び物理的防護の規則に対する非遵守に関連した強制執行措置

3.9. 国は、連絡、協力及び協調を促進する目的で定期的に会合を開催し、物理的防護の責任を割り当てられた政府機関の委員会など、協調的な活動についての責任を果たすための行動を調整するための適切な取り決めを設けることを検討することができる。

3.10. 物理的防護についての国の責任の一環として、原子力施設での核セキュリティ事案に対する対応を備える適切な所管当局について、明確な責任分担が確立されるべきである。警備員、対抗部隊及び関係する所管当局の間の協調が促進させられるべきであり、特に、警備員と対抗部隊との間の協調が定期的に演習されるべきである。

3.11. 各国はそれぞれの対応目的を定義し、対抗部隊の利用についての異なる手法又は戦略を持つ場合がある。これらの定義、手法及び戦略は、防護される核物質及び原子力施設のタイプ並びに敵対者の潜在的な目的（例えば、盗取、妨害破壊行為）に依存することがある。盗取及び／又は妨害破壊行為に対する、大きな影響を与える攻撃対象を持つ原子力施設についての対抗戦略は次のとおりである。

- (a) 対抗部隊にとっての、アクセスの拒否の目標は、攻撃対象の区域へ侵入する敵対者を防止することである。
- (b) 対抗部隊にとっての、作業の拒否の目標は、敵対者（関与する内部者を含む）が成功裏に作業を完遂できる前に、敵対者を阻止することである。
- (c) 対抗部隊にとっての、封じ込めの目標は、例えば立入制限区域の境界など、特定の地点を超えて物質を移転させる敵対者を防ぐことであり、それは、物質が規制上の管理を外れることを防ぐことである。

立法上及び規制上の枠組み

「国は、物理的防護を律するための立法上及び規制上の枠組みを確立し維持する責任がある。この枠組みは、該当する物理的防護要件の策定を備え、並びに評価及び事業許可のシステム又は認可を付与するその他の手続きを含むべきである。この枠組みは、該当する要件及び許可又はその他の許可文書の条件への適合性を検証するため並びに、有効な制裁を含む該当する要件及び条件を実施させるための措置を確立するために、原子力施設及び輸送の検査のシステムを含むべきである。（基本原則 C：立法上及び規制上の枠組み）

「3.9. 国はその国内法の枠組み内で、国の物理的防護体制の適切な実施を確立し、確実にするための適切な措置を取るべきである。」 [1]

規制の手法

3.12. 国は、その国の立法上の枠組みと整合性のある規則を策定し、実施すべきである。規則の実際の内容や項目は、物理的防護体制の監督に必要とされる所管当局の数を含め、それで規制機能が実施される方法について、国によりなされる決定に従うことになる。

3.13. 国は、脅威評価を実施する責任を有しており、また、指定された所管当局が、該当する場合は他の関係する機関と相談して、設計基礎脅威を策定する責任を有する場合がある。どちらの場合でも、所管当局は、全体的な要件及び性能目標、並びに、順守又は有効性の評価基準の策定のための基礎として国の脅威情報を使用する。等級別手法を適用して、所管当局は、核物質の各区分の防護のための、及び、原子力施設での各レベルの（受容できない放射線影響のしきい値以上の）潜在的な放射線影響を防止するための、物理的防護の目的及び／又は要件を規定する。

3.14. 国は、核物質及び原子力施設の物理的防護が脅威に対して有効であることが必要とされるので、国の核セキュリティ体制が脅威のその時点の評価に基づき、また引き続き維持されることを確実にすべきである。脅威に対処するための規制上の枠組みの中での要件を規定する 3 つの異なる手法がある。これらの手法は、性能ベースの手法、規範的な手法、及び規範的な手法と性能ベースの手法の要素を組み合わせる手法である。いずれかの、又は組み合わせの手法は、状況に応じて有用であるが、評価及び性能試験に関する参考文献[1]での勧告は、単独の使用か規範的な手法と組み合わせた使用かにかかわらず、主に性能ベースの手法に関連している。

3.15. 性能ベースの手法は、物理的防護の有効性を確実にすることの及び検証することの、より定量的な手法であり、不法移転に対して、より高い高リスクの核物質を防護する場合、並びに妨害破壊行為に対して核物質及び原子力施設を防護する場合に、特に有用である。これは、単独での規範的な手法がそのような場合に適していないということを意味するものではないが、規範的な要件は、性能試験によるシステムの有効性の実証によりもむしろ、個々の物理的防護措置の適合の検証に、しばしば、容易に適用される。どちらの手法が用いられるにしても、要件又は目的が規定され、その結果として生じる措置の有効性が所管当局によって検証される必要がある。

3.16. 所管当局によって規定される規制要件は、脅威評価で同定された脅威又は設計基礎脅威への取り組みに焦点が当てられるべきである。設計基礎脅威は、物理的防護システムの策定のための基礎としての役割を果たす。原子力施設についての物理的防護システムは、該当する規制要件に従って事業者によって設計されるべきであり、所管当局によって承認されるべきである。

3.17. 個々の物理的防護措置の及び物理的防護システムの性能試験は、区分 I 又は区分 II の核物質を保持する原子力施設について、及び、それへの妨害破壊行為が重大な放射線影響につながる可能性のある、原子力発電所を含む、原子力施設について、参考文献[1]で勧告されている。

性能ベースの手法

3.18. 性能ベースの手法において、国は、等級別手法を考慮して、脅威評価及び、該当する場合は、設計基礎脅威に基づいて物理的防護の目的を明示する。国は、事業者がそれら

の目的を満たし、悪意のある行為に対して防護すること及び危機対応をすることにおいて、規定された有効性のレベルを達成している、物理的防護システムを設計して実施することを要求する。

3.19. 性能ベースの手法により、事業者は、施設固有の物理的防護措置の組み合わせの提案において柔軟性を持つことができる。例えば、事業者は、敵対者の遅延時間は短い、迅速かつ効果的な対応で補う物理的防護システムを開発することができる。これらの措置の適切性は、一連の性能ベースの措置が物理的防護システムの目的を満たすことを確実にするため、脅威評価又は設計基礎脅威に対して試験される。

3.20. 性能ベースの手法の利点は、有効な物理的防護システムが物理的防護措置の多くの組み合わせによって達成され得ること、並びに各施設及びその運転環境が様々であることをこの手法が認識しているということである。性能ベースの手法の使用は、物理的防護の目的及び要件を満たし、さらにサイト固有の条件の考慮もした物理的防護システムについての選択肢を同定すべきである。

3.21. 性能ベースの手法は、所管当局及び事業者の双方が、それぞれ、物理的防護の評価に基づいて、物理的防護システムの要件を策定し、実施するための、十分なセキュリティの専門知識を有することに依存する。また、性能ベースの手法においては、国が脅威評価又は設計基礎脅威からいくつかの機微情報を事業者に提供することが必然的に必要となり、したがって、事業者は、この機微情報を適切に保護をする能力を備えているべきである。

規範的な手法

3.22. 規範的な手法において、国は、核物質の各区分及び潜在的な放射線影響の各レベルについて国の明示された物理的防護の目的を満たすために必要であると国が考える具体的な物理的防護措置を策定する。結果は、事業者が実施する一連の「ベースライン」措置である。

3.23. 規範的な手法の利点としては、国と事業者の両方にとっての実施の単純さ、脅威評価又は設計基礎脅威という形で機微情報を事業者に伝える国の必要性の排除、並びに、検査及び評価の容易さがある。規範的な手法の使用は、脅威レベルと潜在的な影響の両方が低いような場合に特に適切である。1つの例は、比較的低い脅威環境で貯蔵又は使用される区分 III の核物質である。また、規範的な手法は、詳細な脅威評価を実施すること又は設計基礎脅威を策定することが実行可能でない場合に、より適切である。

3.24. 規範的な手法は、具体的な状況に対処するための柔軟性に欠けている。さらに、この手法を使った事業者は、実施されたセキュリティ措置が十分なものであることを確実にする責任を持たない：脅威に対処するために必要とされる物理的防護措置を国の的確に規

定するので、リスクに対処する主たる責任は国にある。事業者は、物理的防護システムを運用及び維持する時の個々の物理的防護措置の有効性についての責任だけを有する。

複合手法

3.25. 複合手法は、規範的な手法と性能ベースの手法の両方からの要素を含む。複合手法を適用する多くの方法があり、そのうちの2つは次のとおりである。

- (a) 国は、悪意のある使用の最も重大な潜在的影響を持つ核物質について性能ベースの手法の適用を要求し、悪意のある使用の潜在的影響が比較的に重大ではない核物質について規範的な手法の適用を許す。
- (b) 国は、セキュリティの規定された側面（例えば、機微情報の保護、個人の信頼性の確立）に対処するために、一連の規範的な要件に従うことを要求する；これらの要件は、性能ベースの手法を使用して導き出されたその他のすべての側面に対処するための措置を補完するであろう。

3.26. 複合手法の主な利点は、柔軟性をもたせることである。複合手法の限界は、規範的な手法と性能ベースの手法に関連する限界と同様であろう、また、国によって選択される具体的な実施に依存するであろう。しかしながら、よく考えられた複合手法は、適切な調和を与え、他の手法のそれぞれに関連する限界の影響を低減する。

物理的防護システムの、性能試験を含む、評価：国の要件

3.27. 参考文献[1]の勧告は、物理的防護システムを評価すること、性能試験を含む、の重要性を強調している。例えば、

- (a) 立法上の及び規制上の枠組みは、「**該当する物理的防護要件の策定を備え、及び評価のシステムを含む**」べきである。(参考文献[1]、基本原則C)。
- (b) 立法上の及び規制上の枠組みは、「評価が、警備員及び／又は対抗部隊の訓練及び準備態勢を含む物理的防護システムを試験するために、演習を含むことを確実にする」べきである。(参考文献[1]の параграф 3.13)。
- (c) 所管当局は、「原子力施設の事業者によって、性能試験に基づく評価が実施されることを確実にする」べきである。(参考文献[1]の параграф 3.21)。
- (d) 持続可能性プログラムは、「次のものを網羅すべきである。：・・・性能試験及び運用監視」。(参考文献[1]の параграф 3.57)。

3.28. 原子力施設のすべての事業者は、それぞれの事業者の施設の物理的防護システムの、性能試験を含む、評価を実施すべきである；これらの評価は、核物質の計量及び管理、情報セキュリティ及びコンピュータ・セキュリティのシステムを考慮すべきである。

3.29. 物理的防護システムの評価は、一般に、試験及び分析で構成される。試験は、構成要素、サブシステム又はシステムレベルで実施され、また、ハードウェア／機器、ソフト

ウェア、人及び手順書を含む場合がある。分析は、定性的な及び／又は定量的な方法を含む、また、モデリング及びシミュレーションの使用を必要とすることがある。モデリング及びシミュレーションの方法は、手動の又はコンピュータ・ベースの数学モデル、コンピュータ戦闘シミュレーション、机上演習、限定範囲の及び全範囲の対抗部隊演習、並びに武力対抗演習を含む場合がある。物理的防護システムの評価は、いくつかの演習を常に含むべきである。

3.30. 様々な方法は、様々な量の（様々な品質要件の）データを必要とし、様々なタイプの情報を提供し、様々な限界を持ち、また、様々なレベルの資源を必要とするであろう。等級別手法を使用して、所管当局は、性能試験要件を含む、物理的防護システムの評価方法の最小単位を規定すべきである。これらの規制要件は、役割と責任、要求される及び／又は許容される方法、文書化の要件、並びに評価及び試験の頻度に関する要件を示し得る。例えば、いくつかの試験及び演習は少なくとも毎年要求される；より包括的な演習（例えば武力対抗演習など）は、それほど頻繁に実施されなくてもよいが、少なくとも2～3年に1度が要求されるべきである。

3.31. 所管当局は、例えば、評価及び試験を裏付けるデータ及び方法が正確であること並びに、評価及び試験の結果がその物理的防護システムを正確に特徴付けることを検証することによって、性能試験を含む、物理的防護システムの評価をレビューすべきである。

3.32. 所管当局は、性能試験を実施するために、適切な専門知識を有する独立した第三者を利用することを検討することがある。1つの例は、脅威評価又は設計基礎脅威によって明示される敵対者の能力を使用して試料障壁の遅延試験を実施することであろう。

許可及び認可を付与するためのその他の手続き

「3.12. 国は、当該事業が物理的防護の規則に適合している場合にのみ、事業を許可又は認可を付与すべきである。国は、許可又は認可承認の前に、これらの事業の承認のために物理的防護措置案を評価するため、及び重大な変更が生じた場合に、物理的防護の規則への継続的適合を確実にするために、国の所管当局によって行われる、それらの案の詳細審査を準備すべきである。」 [1]

3.33. 核物質の物理的防護のための措置を実施することについての第一の責任は各事業者にある；国による物理的防護の管理は、主に政府又は規制の許可（又は承認）によって行使される。許可は、施設の運転、又はある事業（例えば原子力施設への、又は原子力施設からの核物質の輸送など）の実施を許可する正式文書のはずである。国の主たる役割は、物理的防護システムに関連する許可要件を規定すること及び、新規の許可及び既存の許可の更新又は変更の申請を承認するかどうかを検討することである。事業者のセキュリティ計画は、原子力施設の運転についての許可の処置の一環として申請者によって提出される、そして、承認されたセキュリティ計画の遵守は許可の条件であるべきである。

3.34. 許可は、原子力施設の寿命のすべての段階の全体に亘って継続している処置である。許可は、一状況及び事業者の能力に応じて一修正される、一時停止される又は取り消される場合があるが、常に国によってなされ、また、国の管理下である。

3.35. 国は、施設及び事業が国の物理的防護要件に適合している場合にのみ、それらを許可すべきである。許可が次の事項を含めて発行される、ことが助言される。

- (a) 許可を受ける特定の施設又は事業の指定
- (b) 特定の要件、条件、期限又はその他の制限事項
- (c) 事業者の責任の明示

3.36. 国は、許可が発出される前及び核物質が施設に持ち込まれる前に、所管当局が、認可を受ける施設又は事業についての申請者の又は事業者のセキュリティ計画を受領、評価及び承認することを確認すべきである。評価は、その施設について計画された物理的防護システムのレビューによって裏付けられるべきである。不備が同定されたなら、国は、これらの不備が是正されて、物理的防護システムが受容可能であると検証されるまで、許可の付与を保留する。もう一つの方法として、国は、不備が指定された期間内に是正されることを要求する条件付きで、許可を承認する。

3.37. 許可の処置に関する追加的な手引きが参考文献[5]で提供されている。

規制の施行

3.38. 有効な立法上及び規制上の枠組みによる物理的防護の規則及び許可条件の施行は、国の物理的防護体制に必要である。核物質及び原子力施設の防護について、国は、法的手続きを始めるための、又は法に従って制裁を課するための権限を適切な所管当局に割り当てるべきである。そのような制裁としては、許可の停止又は取り消し及び／又は、個人若しくは組織に対するその他の罰の場合がある。

所管当局

「国は、立法上及び規制上の枠組みの実施に責任を負い、その割り当てられた責任を果たすために十分な権限、能力並びに資金及び人的資源を与えられる所管当局を設立又は指名すべきである。国は、国の所管当局の機能と原子力エネルギーの促進又は利用を担当する他の組織の機能との間で実際の独立性を確実にするために対策を講じるべきである。(基本原則 D : 所管当局)」 [1]

3.39. 有効な独立性とは、原子力エネルギー又はその他の原子力応用の促進又は利用についての責任を有する所管当局から干渉されないで、核セキュリティのために必要な要件及び規則を施行するための核セキュリティについての責任を有する所管当局の能力をいう。所管当局の業務、財源及び職員は、そのような促進又は利用に関係する組織とは独立しているべきである。所管当局は、その機能を遂行するため及び、規制対象の原子力施設及び事業の種類と数に見合った方法でその責任を果たすために、十分な財源を利用できる必要

があり、かつ、十分な資格と能力のある職員を雇用する必要がある。所管当局は、その所管当局の機能を適切に遂行するために必要な職員と訓練のレベルを同定する人的資源計画を策定することが助言される。

セキュリティ計画の要求における所管当局の役割

「3.27 ……所管当局は、以後のその実施が許可条件の一部であるべきセキュリティ計画をレビューし承認すべきである。事業者は、承認されたセキュリティ計画を実施すべきである。」 [1]

3.40. 所管当局は、許可申請者及び事業者に、それらが物理的防護についての国の立法上及び規制上の枠組みの下で所管当局に受容可能となる物理的防護システムを設計し、実施するために満たさなければならない要件を、効果的に伝えるべきである。重要な要素は、防護されている核物質の区分及び妨害破壊行為の潜在的な放射線影響のレベルに適切であるセキュリティ計画の、事業者の策定及びその遵守である。所管当局が事業者に対して、国の物理的防護要件のすべての要素が対処されることを確実にすべき、セキュリティ計画に対する要件に関する指示を出すことが助言される。

3.41. セキュリティ計画は、所管当局によって規定された要件を満たそうとする物理的防護システムについて記載している最上位の文書である。国は、セキュリティ計画のどの情報が機微情報として保護される必要がある、また、それはどのように保護されるべきかを規定すべきである。包括的なセキュリティ計画の注釈付きの骨子案が付録 I に提示されている。

検査プログラムの策定における所管当局の役割

「3.20. 国の所管当局は、定期的な検査によって物理的防護の規則及び許可条件への継続的な適合性を検証すること、及び必要な時に、是正措置が取られることを確実にすることの責任を持つべきである。」 [1]

3.42. 検査プログラムの目的は、実際に実施されている物理的防護措置が規制要件及び該当する許可条件を遵守していることを検証することである。この処置は、承認されたセキュリティ計画が有効に実施されていることの検証を含むべきである。規制要件又は許可条件に対する非遵守の場合は、規制措置及び／又は法的措置が検討されるべきであり、適切で相応な措置又は制裁が適用される。

3.43. 所管当局は、所管当局の検査官がその役割を遂行するために必要な資格認定、訓練及び経験を有していることを確実にする必要がある。所管当局は、検査官についての資格認定及び訓練の要件を規定する場合がある。

3.44. 検査プログラムは、検査を実施することが分かっている場合ばかりでなく、常に、承認されたセキュリティ計画に従って事業者が措置を維持していることの保証をするために、事前通告有の検査と抜き打ちの検査の両方を含むべきである。検査は、定時内又は定

時外で、常にあり、また、その時に（例えば、保守や燃料交換のための原子炉停止中に）原子力施設で行われる日常的な及び非日常的なすべての運転上の活動を含む場合がある。検査プログラムが、技術上、手続き上及び管理上の対策を含む、すべての物理的防護措置がレビューされ、検証されることを確実にすることが助言される。検査は、施設の運転を過度に妨げたり影響を及ぼしたりしない方法で実施されるべきである。もし、検査が物理的防護システムの不備を同定したら、所管当局は、その不備が是正されて、十分に有効なシステムが達成されるまで、適切な防護をするために、事業者によって補う措置が用いられることを確実にすべきである。

3.45. 検査官が非遵守又はその他の懸念の問題を同定した場合、その後の検査手順は、事業者が、要求されるすべての是正措置をとったことの検証を含むべきである。これらの措置が、等級付けされ、存在している核物質の区分及び妨害破壊行為の潜在的影響に見合った方法で行われることが助言される。検査官は、是正措置が受容可能な基準まで完了したこと及び、有効な防護が達成されたことが確実にされるために、進捗を監視して、フォローアップ措置を検証する必要があるであろう。所管当局は、是正措置を承認すべきであり、これらの措置は更新されたセキュリティ計画に含められるべきである。場合によっては、是正措置の後での通常の運転状態への復帰は、所管当局からの明確な承認よりもむしろ、所管当局に通知されることを必要とするだけの場合がある。

3.46. 特定の施設について計画される検査の回数は、防護されている物質の区分、妨害破壊行為の潜在的な放射線影響のレベル、脅威評価又は設計基礎脅威、及びその他の関係する要素に基づいて、所管当局によって決定される。事業者の遵守履歴も、検査の頻度を決定する際に、考慮に入れられることがある。対応型検査（状況に応じた検査）も時々、例えば原子力施設における核セキュリティ事案又は脅威の変化の後に、必要であることがある。

核セキュリティ事案の適時な報告

「3.22. 国の物理的防護体制は、核セキュリティ事案及び物理的防護措置に影響するかもしれない、原子力施設においての又は核物質の輸送に関する変更が国の所管当局に知らされることができるようになる、情報を適時に報告することの要件を含むべきである。」 [1]

3.47. 国は、事業者が所管当局に報告することを要求される事案のタイプ、及び、事案がそれ以内に報告されなければならない受容可能な時間を決定すべきである。所管当局は、核物質又は原子力施設の物理的防護に影響を及ぼす無許可の行為に関連する重大な事案についての情報を適時に受けるべきである。例えば次のような事案である；

- (a) 施設へ又は指定された区域への実際の侵入又は侵入の企て
- (b) 外部の敵対者か内部者に関係しているにかかわらず、企てられた又は実際の、核物質の不法移転、紛失又は無許可の移動

- (c) 妨害破壊行為の企て又は実際の行為
- (d) 禁制品の発見
- (e) 承認されたセキュリティ計画からの逸脱（例えば、物理的防護機器への電源の喪失、又は気象によるフェンスの損傷）
- (f) 国の個人の信頼性の方針に従って報告されなければならない者に関する事案
- (g) 機微情報の紛失又は無許可の開示
- (h) 物理的防護、原子力安全又は核物質の計量及び管理システムに使用されるコンピュータ・システムの侵害又は侵害の企て（追加的な手引きについて参考文献[6]を参照）

3.48. 所管当局は、他の政府機関に通知し、核セキュリティ事案への協調的対応に参加することが要求されることがある。事業者又は所管当局は、再発を防止するため及び経験から学ぶために、インシデントを詳細に調査することが要求されることがある。強制執行措置が要求されることもある。

許可保有者の責任

「国内の物理的防護の様々な要素の実施に対する責任は、明確に特定されるべきである。国は、核物質の又は原子力施設の物理的防護の実施に対する第 1 の責任が関連する許可の又はその他の認可文書の保有者(例えば事業者又は荷送人)にあることを確実にすべきである。(基本原則 E : 許可保有者の責任)」 [1]

3.49. このトピックは、事業者の全般的な責任に関するパラグラフ 4.4~4.13 で示されている。

国際協力及び支援

3.50. 各国は、国内の核セキュリティ体制から導き出される情報及び知識の適切な共有を含め、どのような状況のもとで、また、どの程度まで他国と協力できるかどうかを検討すべきである。この決定は、機微な核セキュリティ情報を保護する要求を考慮すべきであり、かつ、情報を共有するための国際的義務又は協定に適合すべきである。

3.51. 参考文献[1]は、次の 3 つのパラグラフで詳しく述べるように、原子力施設の物理的防護に特化した、国際協力及び支援に関する 2 つの勧告及び 1 つの助言を提示している。

3.52. 参考文献[1]のパラグラフ 3.33 では次のように述べられている。

「不法移転若しくは妨害破壊行為又はそれらに関係した信憑性のある脅威が発生した場合、国は、それに関係していると思われるその他の国に、適切な情報を出来る限り速やかに提供すべきであり、また、必要に応じて、国際原子力機関及びその他の関連する国際機関に通知すべきである。」

情報は、IAEAへ自主的に提供されることがある。核物質の不法移転の場合、被害国は、行方不明の核物質の捜し出し及び回収において、もし、その核物質が近隣諸国に入った又は近隣諸国を通過した場合に、それらの国の支援による恩恵を非常に受ける。物質の検知は、物質が存在する、又は物質が通過した国での、規制管理外の核物質又はその他の放射性物質の検知のためのシステムに依存する。この問題に関する追加的な手引きは参考文献[7]で見られる。

3.53. 参考文献[1]の параграф 3.32 に述べられた通りに：「国は、核物質及び原子力施設の物理的防護に関する事項についての適切な連絡窓口を国際原子力機関及び該当する他国に通知すべきである。」物理的防護に関する国の連絡窓口は、不法移転又は妨害破壊行為の場合に、直接の又は IAEA²を通した、近隣諸国及びその他の関係団体への最も重要な情報の迅速かつ正確な伝達を円滑にするために、特に重要である。これらの連絡先はまた、例えば共通の懸念の新たな脅威についての情報など、物理的防護に関するその他の重要な情報を伝える上でも重要であることがある。

3.54. 参考文献[1]の параграф 3.31 に述べられた通りに、「国は、直接に又は国際原子力機関及びその他の関連する国際機関を通してのいずれかで、物理的防護の技術及び実施について協力すること、相談すること及び情報を交換することが奨励される。」運転している原子力施設を有する国は、物理的防護に関する経験を得ており、また、良好事例及び学んだ教訓を蓄積している。国の間でこのタイプの情報を共有することは、核物質の物理的防護の全体のレベルを引き上げること促進することによって、国際社会に恩恵を与えることができる。施設固有の機微情報の一部は共有されない場合があるが、多くの有用な情報は、ワークショップ、研修プログラム及び会合を通して共有されることができる。IAEAは、属性を必要としないで、そのような情報を共有するための有用な伝達手段である。

脅威の同定及び評価

「国の物理的防護は、脅威に対する当該国による現在の評価に基づくべきである。
(基本原則 G : 脅威)

「3.34. 適切な国の機関が、様々な信憑性のある情報源を用いて、脅威評価の形式で及び、場合によっては、設計基礎脅威で、脅威及びその能力を明示すべきである。設計基礎脅威は、不法移転及び妨害破壊行為の脅威に対する国による評価から策定される。」 [1]

3.55. 脅威評価は、悪意ある行為に及ぶ潜在的な敵対者の動機、目的及び能力を説明する、現在の脅威の評価である。脅威評価としては、核物質及び原子力施設に関する若しく

²原子力又は放射線緊急事態をもたらす核セキュリティ事案について、事案についての情報の提供及び支援の提供は、早期通報条約及び援助条約並びに緊急事態への備えと対応に関する IAEA 安全基準に基づいて、IAEA によって策定された運用上の取り決めによって与えられるべきである。

は、に向けられたテロ行為及びその他の犯罪的な、若しくは意図的な無許可の行為の脅威、特に核物質の不法移転並びに核物質及び原子力施設の妨害破壊行為の検討がある。脅威評価はまた、外部脅威と内部脅威の両方も検討する。脅威評価は、必要に応じて、脅威に関する国内の、国境を越えた及び全世界の情報源を活用する。

3.56. 国は、脅威を同定して評価する様々のレベルの能力を持つであろう。いくつかの国は、核物質及び原子力施設に向けられる脅威を含め、脅威の種類及び程度の理解する上で国を支援することのできる大規模で非常に高度なセキュリティ及び諜報の能力を有している。別のケースでは、国内の脅威（例えば、市民の暴動エリア、犯罪的な行為、テロリストの存在）及び国際的な脅威についての全般的な情報が、国内の潜在的な脅威を同定するために、理解されて強化される必要がある。

3.57. 所管当局は、脅威を理解し、これに対応する責任を持つすべての国の機関（例えば、諜報サービス、警察、軍、税関と出入国管理、地方の法執行機関）との間の協力を必要とする脅威評価の策定についての全体の責任を割り当てられるべきである。この作業は機微情報の使用を必要とするので、適切な情報セキュリティ措置が、脅威評価及びその結果としての設計基礎脅威に適用されるべきである。

3.58. 脅威評価について及び脅威評価に基づいた設計基礎脅威を規定することについての追加的な手引きが参考文献[8]に示されている。手引きは、設計基礎脅威を使用するか、代替的脅威説明書を使用するかどうかの決定に関する検討を含んでいる（参考文献[8]に注記された「代替的脅威説明書」は、物理的防護システムの設計のために脅威を規定する際の厳密でない手法を意味する）。

3.59. 設計基礎脅威は、所管当局によって様々な方法に使用される場合がある。性能ベースの手法の下で、設計基礎脅威は、物理的防護システムの設計のために事業者によって、及び、物理的防護システムの評価のために所管当局によって使用されることがある。規範的な手法の下で、脅威評価は、区分 I の核物質が保有されている場合及び／又は、原子力施設の妨害破壊行為が重大な放射線影響に潜在的につながり得る場合を除き、事業者が実施することを要求される物理的防護措置を規定する所管当局には十分であるかもしれない。規範的な手法の下では、国の物理的防護要件は、特に、区分 I の核物質の不法移転並びに核物質及び原子力施設の妨害破壊行為についての設計基礎脅威に基づくべきである。

3.60. 参考文献[1]のパラグラフ 3.36 は、次のように述べている。

「脅威を検討する場合、相応の注意が内部者に払われるべきである。内部者は、専用の物理的防護の要素又は、例えば安全上の手順など、その他の対策を回避するために、自身の権限及び知識によって補完された、アクセス権を悪用し得る。物理的防護システムは、内部者による核物質の長期にわたる盗取を抑止及び検知するために、核物質の計量及び管理の措置によって支援されるべきである。」

IAEA は、内部脅威に対処している国を支援するために、具体的な手引き[9]を発行している。

3.61. 検討が、脅威評価及び設計基礎脅威の中で、計装制御並びに原子力安全、核物質の計量及び管理、及び物理的防護システムに必要なその他のシステムを含む、コンピュータ・ベースのシステムへのあり得る攻撃についてなされるべきである。そのようなシステムとしては、データベース、出入管理及び警報管理システムがある。そのようなシステムへの脅威をレビューする時、検討は、単にシステムを無効化又は破壊することを目的とする攻撃についてなされるばかりでなく、例えばデータの不正操作及び改竄など、あまり直接的でない攻撃についてもなされるべきである。検討は、内部脅威及び外部脅威の両方の視点から、敵対者の潜在的な能力についてもなされるべきである。参考文献[6]は、このタイプの脅威に関する多くの手引きを提供している。

3.62. 脅威評価又は設計基礎脅威は、原子力施設から距離を置いて遂行され得るスタンドオフ攻撃（参考文献[1]のパラグラフ 3.40 参照）の検討も含むべきである。そのような攻撃は、敵対者が攻撃対象にアクセスできることを必要としない又は物理的防護システムを打ち負かすことを必要としない。スタンドオフ・シナリオの例としては、可搬型ミサイルランチャーの使用又は悪意ある航空機衝突がある。国は、どのタイプのスタンドオフ攻撃が事業者によって考慮される必要があるかを決定すべきである。

3.63. 国は、継続的に脅威をレビューし、脅威評価又は設計基礎脅威の変更の関連を評価すべきである。例えば、国は、脅威のレビューが脅威評価の更新を必要とするかどうかを年に 1 回、決定する。国内又は他の場所での核セキュリティ事案は予定した定期的なレビューの前に、国の脅威評価の更新につながる場合がある。国は、脅威評価又は設計基礎脅威の変更の観点から、国の物理的防護要件をレビューすべきである。事業者は次に、事業者の物理的防護システムをレビューする必要がある（潜在的な妨害破壊行為の攻撃対象のレビューを含む）、そして、その結果としての、物理的防護システムの設計の変更は、実施の前に、承認のために所管当局に提出すべきである。

リスクベースの物理的防護システム

「3.41. 国は、国の物理的防護体制が、リスク管理によって、受容可能なレベルで不法移転及び妨害破壊行為のリスクを設定すること及び維持することができることを確実にすべきである。これは、脅威及び悪意のある行為の潜在的影響を評価することを必要とし、次に、適切で有効な物理的防護措置が整備されることを確実にする立法上の、規制上の及び計画的な枠組みを確立することを必要とする。」 [1]

3.64. 核セキュリティにおいて、リスクの評価としては、脅威、その脅威によって悪意ある行為が成功裏に遂行され得る可能性、及びそのような行為の潜在的影響の検討がある。

3.65. 国は、物理的防護要件、及び要件を満たすための事業者の措置が、不法移転又は妨害破壊行為に関連するリスクを、国が受容可能なレベルであるとみなすレベルに抑えていることを確実にするために、リスク管理手法を使用すべきである。リスク管理は、脅威及び悪意ある行為の潜在的な影響を定期的に評価すること、並びに悪意ある行為を防止するため又はその行為の成功の可能性を十分に低減するために、適切な物理的防護システムが実施されているのを確実にすることが含まれる。

3.66. リスク管理は、定量的な又は定性的なリスク評価を考慮する。リスクの定量的な評価は、事案の発生する確率及び、もし、事象が発生した場合の事象の予想される影響の量的表現の関数として、特定の事案に関連するリスクを決定することを必要とする。しかしながら、悪意ある行為が企てられている確率、又は企てが成功する確率を定量化することは非常に困難である。物理的防護措置を計画する目的のために、悪意ある行為を遂行する企てが起こるのは確実であることは仮定するに十分である。この場合、このリスクは、悪意ある攻撃が企てられるという条件の付いた、条件付きリスクと呼ばれる。条件付きリスクは、リスクの定量的評価に上限を与えることに、また、企ての発生の可能性が際立った要因ではないような場合のリスクを比較することに（例えば、同じリスクに対する様々な物理的防護の選択肢を比較することに）有用である。

3.67. 核セキュリティのリスクを決定するための定量的な方法がない場合、定性的なリスク管理手法が、物理的防護の決定に情報を与えるために、用いられることがある。定性的なリスク管理は、企ての可能性、及び、そのような企ての成功の可能性を確率として定量化しようとししないで、これらの可能性の検討を必要とする；それよりも、定性的リスク管理は、脅威に対する攻撃対象の脆弱性、及び、企てが成功した場合の潜在的な影響を考慮する。この手法は、高リスクを示している要因（例えば、高い脅威の可能性、高いレベルの敵対者の能力、重大な影響）の組み合わせを同定するために、及び、リスクを最も効果的に低減するために重点的に取り組まれるべき努力を同定するために、使用され得る。同様に、低リスクを示している要因の組み合わせは、セキュリティ措置をあまり厳しくすることを必要としないことを例証する。

3.68. 国は、国が物理的防護システムの不具合の残存リスクを受け入れなければならないので、通常、設計基礎脅威に関して、不法移転に対する物理的防護システムの受容可能な性能についての基準を決定する。国はまた、妨害破壊行為に対する物理的防護システムの性能要件の基礎として使用するために、受容できない放射線影響及び重大な放射線影響のしきい値も決定すべきである。もし、潜在的な放射線影響が、国によって規定された受容できない放射線影響よりも重大でない場合は、安全関連の機器及び装置へのアクセスを管理すること及びそれらを守ることによって、それらを防護する措置が提供されるべきである（さらなる詳細はパラグラフ 3.93～3.95 で提供されている）。リスク管理の実施は、パラグラフ 3.70～3.101 でさらに述べられるように、等級別手法の使用による物理的防護措置の適切な適用を知らせる手段を提供する。

3.69. リスク評価は、リスクを低減するために追加の対策が要求されるかどうかを決定するために、さらに評価されることを必要とするリスクを同定する。リスクは、例えば、抑止を改善すること（例えば、堅固な物理的防護措置の注目度を強化させること）、物理的防護措置を強化すること（例えば、追加の多層防護（defence in depth）を備えること）、及び潜在的な影響の低減すること（例えば、核物質の量、種類、希釈度、化学的形態又は物理的形態を変えること）によって管理され得る。そのような変更の安全上の影響も検討されるべきである。

等級別手法

「物理的防護要件は、脅威に対する現在の評価、相対的な魅力度、物質の種類、並びに核物質の不法移転及び核物質又は原子力施設に対する妨害破壊行為による潜在的な影響を考慮に入れて、等級別手法に基づくべきである。（基本原則 H：等級別手法）」 [1]

3.70. 国の物理的防護要件及び規則の策定は、より重大な影響を生じ得る事案に対するより高いレベルの防護を備えるために使用される、等級別手法に基づいて構築されるべきである。

3.71. 核爆発装置に使用するための核物質の不法移転に対する防護を等級分けするために、核物質の区分は、表 1（出典 参考文献[1]）に規定するように、核爆発装置を製造するためにその区分の物質を使用することの相対的な難しさを反映している。区分 I の核物質は物理的防護の最も厳重なレベルで防護されるべきである；区分 III 未満の核物質は、ただ慎重な管理慣行に従うだけで防護される必要がある（参考文献[1]のパラグラフ 4.12 及び表 1 の脚注 c）。

表 1. 核物質の区分 (出典 参考文献[1]の表 1)

物質	形態	区分 I	区分 II	区分 III ^c
1. プルトニウム ^a	未照射 ^b	2kg 以上	500g を超え 2kg 未満	15g を超え 500g 以下
2. ウラン 235 (²³⁵ U)	未照射 ^b — ²³⁵ U の濃縮度が 20%以上のウラン	5kg 以上	1kg を超え 5kg 未満 10kg 以上	15g を超え 1kg 以下
	— ²³⁵ U の濃縮度が 10%以上 20%未満 のウラン	-----		1kg を超え 10kg 未満
	— ²³⁵ U の濃縮度が天 然ウランにおける 含有率を超え 10% 未満のウラン	-----		10kg 以上
3. ウラン 233 (²³³ U)	未照射 ^b	2kg 以上	500g を超え 2kg 未満	15g を超え 500g 以下
4. 照射済燃料 (この表の照射済燃料の区分は国際輸 送の考え方に基づいている。国は自国 内の使用、貯蔵及び輸送に対し、全て の関連する要因を考慮に入れて、異な った区分を割り当ててもよい。)			劣化ウラン若し くは天然ウラ ン、トリウム又 は低濃縮燃料 (フィッサイル 量(核分裂性物 質含有量) 10% 未満) ^{d, e}	

注: この表は本文と独立に使用されたり、解釈されてはならない。

- a プルトニウム 238 の同位体濃度が 80%を超えるプルトニウムを除くすべてのプルトニウム
- b 原子炉内で照射されていない場合、原子炉内で照射されている場合、遮蔽なしで、1m離れた地点で1時間あたり1グレイ（1時間あたり100ラド）以下の放射線レベルの物質。
- c 区分Ⅲに入っていない量並びに天然ウラン、劣化ウラン及びトリウムは、少なくとも慎重な管理慣行に従って防護されるべきである。
- d この防護レベルが推奨されるが、具体的な状況の評価に基づいて、これと異なる物理的防護の区分を指定することは各国の自由である。
- e 当初のフィッサイル量（核分裂性物質含有量）によって、照射前に区分Ⅰ又は区分Ⅱに分類されている他の燃料は、遮蔽なしで、1メートル離れた地点でその燃料からの放射線レベルが1時間あたり1グレイ（1時間あたり100ラド）を超える間は、1区分レベル下げてもよい。

3.72. 妨害破壊行為に対する防護のために、国は、そのような行為の潜在的な放射線影響を検討し、等級別手法を適用する必要がある。国は、妨害破壊行為が受容できない放射線影響を引き起こす可能性を考慮に入れながら、原子力施設をどのように防護するかを検討すべきである。国はまた、もし妨害破壊行為の対象の施設がそのような影響を生じるなら、この施設内の攻撃対象について防護措置が要求されることも確実にすべきである。

3.73. 国はまた、例えば機微情報の機密保持及び個人の信頼性など、他の物理的防護措置についての要件を規定する上で等級別手法の使用も検討すべきである。

不法移転の影響に基づく物理的防護の等級別レベル

不法移転に対する核物質の区分

「4.5. 不法移転に対する物理的防護措置を決定する際の主要因は、核物質それ自体である。表1は、元素、同位体、数量及び照射という観点で様々な種類の核物質を区分している。区分そのものは、核物質(例えば、プルトニウム及びウラン)の種類、同位体組成(つまり、核分裂性同位体の含有量)、物理的形態及び化学的形態、希釈度、放射線レベル及び数量によっており、この区分は、核爆発装置に使用され得る核物質の不法移転に対する防護に関する等級別手法の基礎である。」 [1]

3.74. 表1(出典 参考文献[1])は、3つの区分(I~III)及び、暗黙的に、4番目の区分「区分III未満」についてのしきい値を策定する、核物質の種類(例えば、プルトニウム又はウラン)、照射レベル、同位体組成(すなわち、核分裂性同位体の含有量)及び数量を規定している。

3.75. 表1における区分は、参考文献[1]の paragraph 4.5 に挙げられている核物質の4つの特性、すなわち、核物質の種類、同位体組成、数量及び照射を使用している。表1は、不法移転に対する等級別防護についての基礎として、例えば物理的及び化学的形態及び希釈度など、その paragraph で言及されているその他の特性をどのように使用するかについては説明していない。しかしながら、参考文献[1]は、国がこれらの特性のすべてを考慮に入れることができることを示している。

照射済燃料の区分

3.76. 表1の第4行は、照射済燃料を、遮蔽なしで、1m離れた地点で1時間あたり1グレイ(1時間あたり100ラド)を超えるレベルの放射線で、原子炉内で照射された物質として効果的に規定している。この行は、照射前に劣化ウラン若しくは天然ウラン、トリチウム又は²³⁵Uの濃縮度が10%未満のウランから構成された照射済燃料が、照射前に区分IIIよりも高い区分に位置付けられなかったにもかかわらず、区分IIに属するというを示している。この区分の変化の理由は、原子炉内での照射中に、プルトニウム(主に²³⁹Pu)がウラン系燃料内で作られること及び、同様に²³³Uがトリウム燃料中で作られることである。

照射の結果として作られたプルトニウム又は ^{233}U の割合は比較的小さい（一般的に、プルトニウムの場合、総重量の約 1%）。しかし、この照射済燃料は一般的に大量に貯蔵されるので、これを区分 I と位置付けるのに十分な核物質の量（2 kg を超えるプルトニウム又は ^{233}U ）を含んでいる。表 1 の脚注 e の手引きと同様に、そのような照射済燃料は、それが引き起こす高放射線レベルであることによって魅力度が低下したため、（区分 II に）1 区分下げてもよい。

3.77. 表 1 の第 4 行はまた、具体的な状況の評価に基づき、国は、国内での使用、貯蔵及び輸送の間の、上記の照射済燃料に異なる物理的防護のレベルを指定してもよいとしている。そのような状況の一例は、少数の照射済燃料棒だけが収容されている場所（例えば照射後試験施設など）である。少量の物質のため、照射済燃料棒が 2 kg 未満のプルトニウム又は ^{233}U を含む場合、区分 III の核物質として照射済燃料を防護することが適切であろう。

（核物質の計量及び管理のために維持される記録は、この燃料の中の他の核物質の量だけでなく照射済燃料の中のプルトニウム又は ^{233}U の量の推定値を含むべきなので、記録が、これらの少量の物質が実際に存在するかどうかを裏付けるであろう。）

3.78. 表 1 の脚注 e は、照射前に区分 I 又は II であるその他の燃料は、それが照射済燃料になった後は 1 区分下げてもよいと述べている。この脚注は、述べられた理由のため、次のような状況で適用可能である。

- (a) 一般的なプルトニウム系燃料、混合酸化物燃料及び高速炉燃料は、一般的に、それぞれ約 7%及び約 30%のプルトニウムを含んでいる。原子炉の中での照射はプルトニウムの含有量のある程度下げるが、照射済燃料の中のプルトニウムの全体的な重量含有量を大幅に下げないだろう。そのような燃料は通常は大量に貯蔵されるので、代表的な貯蔵場所での照射済燃料の中のプルトニウムの量は、そのような燃料を区分 I と位置付けるのに十分であろう。この燃料は、その高い放射線レベルが敵対者に燃料を魅力的でないようにするので、表 1 の脚注 e に従って、区分 II に 1 区分下げてもよい。
- (b) 高濃縮ウラン燃料（すなわち ^{235}U 濃縮度 20%以上のウランを含む燃料）の原子炉の中の照射は、 ^{235}U の含有量を数パーセント下げるであろう。しかしながら、この低減は、一般的に濃縮レベルを 20%未満に下げないだろう。したがって、照射済燃料は、主に 20%以上に濃縮されたウランからなることを続けるだろう。結果として、表 1 の脚注 e に従って、照射前に合計で 5 kg 以上の ^{235}U を含有していて 1 か所に収容された照射済高濃縮ウラン燃料は、区分 I から区分 II に下げてもよく、また、照射前に 1 kg を超え 5 kg 未満の ^{235}U を含有していた高濃縮ウラン燃料は、区分 II から区分 III に下げてもよい。この区分の引き下げは、物質の照射レベルのせいとその魅力度の低下を反映している。

(c) 同様に、当初は ^{235}U を少なくとも 10%以上 20%未満に濃縮したウランを含んでいた燃料（例えば、一般に照射前に ^{235}U が約 19.5%に濃縮された研究炉燃料）の原子炉の中での照射は、一般的に、 ^{235}U の濃縮レベルを 10%未満に下げることはないだろう。これらのレベルに濃縮された燃料の照射は、研究炉で使用される燃料の量は比較的少ないため、区分 III のしきい値を超える量のプルトニウムを作らない。この理由で、一度照射された、この燃料の区分は、量と濃縮レベルによって主に決定される。したがって、もし、1つの場所で収容されたこの燃料の総量が照射前に 10 kg 以上の ^{235}U を含有していた場合、それが 1 度、照射済燃料になったら、それは区分 II から区分 III に下げてもよい。

3.79. 照射済燃料に表 1（脚注 d）に示された物理的防護の区分と異なる区分を指定するための国に対する選択肢は、当初は区分 I 又は区分 II の量のプルトニウム又は 10%以上に濃縮されたウランを含有した照射済燃料に必ずしも適用しない。すべての種類の照射済燃料の放射線レベルが時間と共に下がることは、表 1 の脚注 e 及び第 4 行に基づいて一区分下げられた物質の区分の再検討を必要とするかもしれない。

3.80. 上記のように、国は、表 1 の脚注 e に基づき、もし、不法移転に対して防護される核物質が、間の遮蔽なしで接触可能表面から 1 m の距離で 1 時間当たり 1 グレイを超える総外部線量率である場合、その物理的防護措置を 1 区分下げる選択肢を持つ。この基準は、核物質に触れようとする者がその線量率で、1 時間未満の放射線被ばくによって重篤な確定的健康影響に苦しみ始める線量率である。単純な盗取シナリオの下で、このレベルでの放射線量率は、もともと、放射性物質の盗取への有効な抑止として役目を果たすと仮定された。しかしながら、現代の一部の敵対者は、自分の使命を果たすためには死のリスクいとわぬ気持ちを持っており、したがって、照射済燃料を取り扱うことによる放射線被ばくの影響によって抑止されないかもしれない。したがって、国は、脚注 e の規定が、国の物理的防護要件の決定において受容可能な変更であるかどうかを慎重に検討すべきである。

物質の形態又は希釈に基づいた等級別の防護要件の設定における検討

3.81. 多くの国は、歴史的に、不法移転に対する適切な物理的防護を適用する目的のために、未照射の核物質を分類するための 3 つの要因による方法を使用してきた。この方法の下で、核物質について、核分裂性元素（プルトニウム又はウラン）、同位体組成及び量が、不法移転に対する防護に要求される物理的防護のレベルの決定において考慮される 3 つの要因である。この方法は、実施するのが容易であるが、場合によっては、防護されている物質について過度の防護要件をもたらすことがある。したがって、潜在的な盗取シナリオで敵対者へのさらなる阻害要因を与えるかもしれない物質のその他の特性を国が検討

することが推奨される。これらの阻害要因としては、核物質の希釈、又は、核物質を大きく空けて分離させておくことがある可能性がある。

3.82. 参考文献[1]の勧告は、次のように、他の要因の検討の必要性を認識している。

(a) 一般に、核物質については、参考文献[1]による区分は、

「核物質(例えば、プルトニウム及びウラン)の種類、同位体組成(つまり、核分裂性同位体の含有量)、物理的形態及び化学的形態、希釈度、放射線レベル及び数量によっており、この区分は、核爆発装置に使用され得る核物質の不法移転に対する防護に関する等級別手法の基礎である。」(参考文献[1]の Paragraph 4.5)

(b) 廃棄物については、「もはやいかなる原子力事業の使用に適さない形態であり、環境への飛散が最小化され、及び實際上、回収不可能である核物質は、慎重な管理慣行に従って、不法移転に対して防護される。」(参考文献[1]の Paragraph 4.7)

(c) 照射済燃料については、表1の脚注eは、放射線レベルに基づいて区分を下げることを可能にしている。

3.83. 希薄な状態で核物質が存在することにより、敵対者は有意量の核物質を得るために、かなり多い総量の物質を取得することを余儀なくさせられる。敵対者は、また、核物質の回収がより困難になり、核物質を核爆発装置の製造に利用可能な形態に転換するためにより多くの処理ステップを実施することが必要になる。敵対者に対して与えられたこれらの追加的な難題を考慮すると、国は、核物質の区分分けをする時に、希釈度を考慮しようとする場合がある。区分分けのために追加の可能性のあるパラメータは、核物質の濃度及び、物質中の濃度の均一性であろう。これは、敵対者にとって魅力のない形態での核物質の処理及び貯蔵を奨励し得る。

3.84. 物質自体が敵対者にとっての魅力度を低下させる固有の要因又は、適切な防護を決定する上で考慮するその他の特性を有していると考えられる場合、これらの要因の期待できる効果の評価が、区分分けの3つの要因による方法によって示された物理的防護措置を修正するためにそのような要因を使用する前に、実施され、文書化されるべきである。

核物質の積算に基づく追加的検討事項

「4.8. 複数の建物で構成される施設の物理的防護のレベルを決定する際、事業者は、国の所管当局との合意の下で、異なる区分の核物質を含んでいて、それ故に原子力施設の他の部分とは異なるレベルで防護される原子力施設の一部を特定することが

ある。逆に、多くの建物に含まれる核物質の積算総量を、この建物群の適切な防護措置を決定するために考慮する必要があることがある。」 [1]

3.85. 核物質の不法移転に対して、原子力施設、建物グループ又は部屋グループについての物理的防護レベルを割り当てる際に、検討が、施設、建物グループ又は部屋グループの中の核物質の総量を集計（合計）することについて必要なことがある。核物質の集計のために使用される方法は、要求される物理的防護のレベルを決定する上で、及び必要ならば、そのレベルを上げる上で重要な要素である。

3.86. 参考文献[1]の параграф 4.8 は、大量の核物質が、1回の攻撃中にいくつかの場所又は建物から敵対者によって持ち去られる可能性について示している。

3.87. 施設によっては、同じ種類の核物質（例えば、 ^{235}U の濃縮度が 20%を超えるウラン）が、様々な目的のため、又は処理の様々な段階において、いくつかの異なる建物に置かれる場合がある。例えば、ある建物の中にそのような物質が 4 kg あり、同じ **Protected area** 内の別の建物の中に同様の物質が 4 kg あるとする。個々に検討すると、物質のそれぞれの量は区分 II とされるであろう。しかしながら、8 kg 全部が、1回の攻撃中に敵対者によって取られ得るならば、物質は区分 I として指定されるべきであり、物理的防護システムは、それに対応して堅固であるべきである。

3.88. 様々な種類の核物質（例えば、プルトニウム、 ^{233}U 、 ^{235}U の様々な濃縮度のウラン）が、同じ原子力施設内に一緒に配置されているばあいがある。施設の中の核物質の総量が、施設内の特定の場所にある核物質の区分を決定する際に、また、したがって、核物質に適用する適切な物理的防護措置を同定する際に、考慮されるべきである。様々な核物質の集計量についての区分を判断するための、いくつかの実用可能な計算式があり、国は、使用される手法を決定すべきである。様々な種類の核物質を積算するための 1つの手法は、表 1 から導き出される一連の計算式を使用する：この手法は付録 III で説明している。

3.89. 原子力施設内の様々な場所からの不法移転に対する強化された防護は、もし、所管当局が、単独の敵対者に様々な場所からの別々の量の物質の不法移転が次の理由で、ありそうもないとする事業者の決定を承認するならば、要求されない。

- (a) 別々の場所は、別々の物理的防護システムによって防護されており、また、警備員及び／又は対抗部隊は、すべての場所において敵対者の攻撃に有効に対抗することができる。
- (b) 別々の場所は、異なる従業員グループによって管理され、その管理下にあり、そのため、内部者からの脅威をそれらの場所のうちの 1つに限定している。

3.90. 事業者は、集計された量について適切と考えられる物理的防護のレベルの決定を伝えるために、規定された時間内に敵対者が得ることができるであろう核物質の量も検討することもある。事業者は次に、

- (a) 核物質を集計する敵対者の能力を下げるための適切な物理的防護措置を計画する、又は、
- (b) 核物質の集計がより高い区分をもたらすなら、適切な物理的防護措置を適用する。

妨害破壊行為の影響に基づく物理的防護の等級別レベル

「3.44. . . . 妨害破壊行為に対する防護について、国は現在の原子力安全及び放射線防護を考慮に入れて、物理的防護の適切なレベルを決定するために、受容できない放射線影響のしきい値を策定すべきである。」 [1]

3.91. 核物質の不法移転についての表 1 に記載された区分とは異なって、妨害破壊行為の攻撃対象についての単純な区分の分類表はない：不法移転のリスクに基づいて核物質に割り当てられる区分は、物質又は物質が中にある施設の妨害破壊行為の潜在的な影響の有用な指標ではない。例えば、高濃縮ウランの新燃料（区分 I）は、可能性のある盗取に関しての重大な関心事であるが、妨害破壊行為の視点からは、物質からの放射線レベル及び物質の放出する潜在的な放射線影響が低いので、ほとんど問題はない。しかしながら、原子炉内で照射された高濃縮ウラン燃料は、核分裂及び放射化生成物からの高い放射線レベルが盗取を困難で危険なものにするため、盗取に関してはほとんど問題がないかもしれないが、そのような燃料は、核分裂及び放射化生成物の放出による潜在的な放射線影響のために、妨害破壊行為にとって、より魅力度の高い攻撃対象である場合がある。

3.92. 国は、妨害破壊行為に対する物理的防護の規制上の基礎を確立すべきであり、これは、国が規定している受容できない放射線影響のしきい値を含めるべきである。この基礎は次に、妨害破壊行為に対する物理的防護措置を策定するために事業者によって使用されるべきである。パラグラフ 3.93～3.95 に述べるように、国はまた、参考文献[1]のパラグラフ 5.20～5.42 で説明するように、上回ると、枢要区域が同定されて、より高いレベルで防護されることが推奨される、重大な放射線影響についてのしきい値も規定すべきである。

受容できない放射線影響及び重大な放射線影響

3.93. 妨害破壊行為の潜在的な影響が、それを上回ると受容できない放射線影響であると国によって規定されるレベルに関して検討される。受容できない放射線影響の定義は定量的又は定性的である。受容できない放射線影響は、国によって規定され、放射性核種の放出についての基準（例えば、総放射能放出又は同定されたあるレベルを超える特定の放射性核種の放出）、線量基準（例えば、規定された場所での個人への規定された限度を超える放射線線量につながるのに十分な放出）及び設計限度（例えば、原子炉内での著しい炉

心損傷をもたらす妨害破壊行為) とする場合がある。同じ受容できない放射線影響は、原子力施設でのすべての放射性物質についての妨害破壊行為の潜在的な放射線影響に適用すべきである。受容できない放射線影響の国の定義は、次に、そのような影響につながり得る、したがって防護されるべき、妨害破壊行為の攻撃対象の同定を可能にするであろう。受容できない放射線影響(及び重大な放射線影響(下記参照)) であると考えられる影響を規定することは、安全上の検討を含むであろう、また、安全当局と緊密な協議を行って決定されるべきである。例えば、受容できない放射線影響及び重大な放射線影響の定義は、緊急事態準備及び対応について使用される基準に関連づけられている[10、11]。

3.94. 受容できない放射線影響のしきい値は、原子力施設内の限定化された区域の中の、放射性核種の比較的少量の放出に相当するレベルで設定されることがある。潜在的にこのようなより小さい影響だけを引き起こす攻撃対象は、それに対応して低いレベルの防護を求める。その一方で、原子力施設の境界を越えて、人及び環境に大きく影響するかなりの放射線放出を潜在的にもたらし得る妨害破壊行為の攻撃対象は、最高レベルの防護を必要とする。そのような重大な事案は、参考文献[1]で、重大な放射線影響があるとされている。

3.95. したがって、国は、重大な放射線影響についてのしきい値も規定すべきである。もし、妨害破壊行為の潜在的な放射線影響が重大な放射線影響のしきい値以上と評価されたら、枢要区域が、参考文献[1]の paragraph 5.9~5.19 に示されている設計を用いて、参考文献[1]の paragraph 5.20~5.42 に勧告されているように、同定されて、防護される必要がある。もし、放射線影響が、受容できない放射線影響と重大な放射線影響のしきい値の中間に位置するならば、国は、潜在的な放射線影響に基づいて等級別の防護要件を規定し、防護は、参考文献[1]の paragraph 5.9~5.19 に示された設計手順を用いて備えられるべきである。もし、潜在的な放射線影響が受容できない放射線影響のしきい値を下回るならば、事業者はそれでも、参考文献[1]の paragraph 5.7 で勧告されているように、安全関連の機器及び装置へのアクセスを制限し、それらを守ることによって、それらを防護すべきである。受容できない放射線影響及び重大な放射線影響と防護レベルとの間の関係を図 1 に示す。

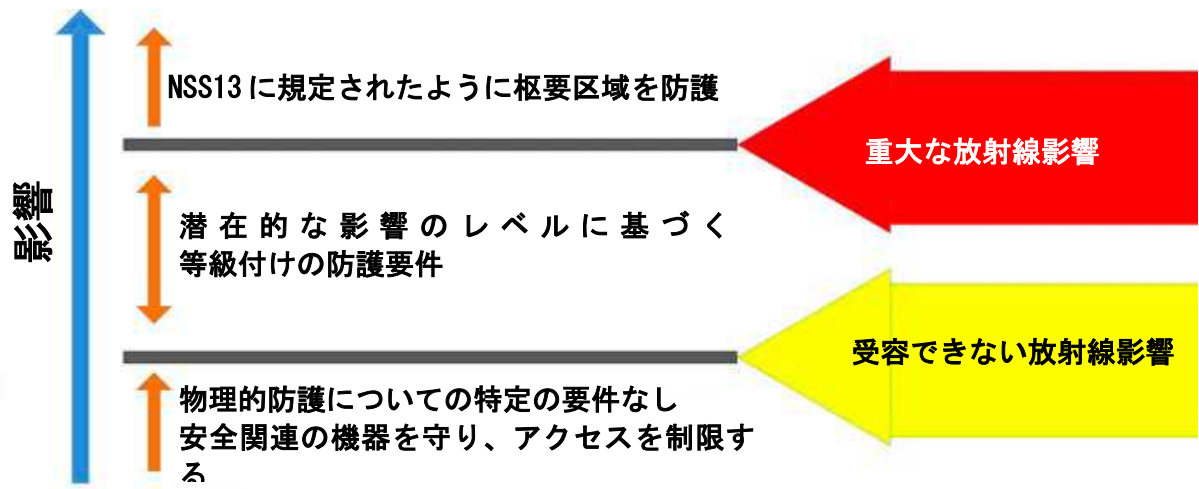


図1. 受容できない放射線影響及び重大な放射線影響と防護の等級別のレベルとの関係
(NSS13 : IAEA 核セキュリティ・シリーズNo. 13)

妨害破壊行為の潜在的な放射線影響の範囲

3.96. 潜在的な敵対者の妨害破壊行為の攻撃対象の魅力度の評価は、受容できない放射線影響及び重大な放射線影響についての国のしきい値に基づいていて、不法移転の脅威に基づいて規定された核物質の区分とは無関係である。妨害破壊行為から生じる潜在的な放射線影響は、放射性物質の在庫量及び物質の拡散の容易さに依存するであろう（次に、容易さは、妨害破壊行為から生じることが予想される拡散のメカニズム及び物質の形態に依存するであろう）。妨害破壊行為から生じる潜在的な放射線影響は、重大度のいくつかの範囲を反映するために、それに対応して防護の等級別レベルを要求している各範囲に等級付けされる場合がある。

3.97. 妨害破壊行為の事案が、原子力施設において受容できない放射線影響をもたらす可能性は、施設の特徴（例えば、施設のタイプ、並びに施設の使用、設計、建設、運転及び配置）及び、妨害破壊行為自体に依存する。施設において受容できない放射線影響の可能性があるかどうかを決定する時に、考慮に入れるべき要因としては、（該当する場合）以下に述べる特徴がある。

- (a) 原子力施設における放射性物質の量、種類、物理的形態及び状態（例えば、固体又は液体形態、処理中又は貯蔵中）
- (b) 原子力施設で通常行われる物理的処理及び化学的処理に関連する固有のリスク（例えば、臨界のリスク）
- (c) 攻撃の中で不安定になる処理の特性又は工学的機能
- (d) 施設の熱出力容量及び（原子炉用の）核燃料の照射履歴

- (e) 様々なタイプの事業のための原子力施設の構成
- (f) 原子力施設の中の放射性物質の空間的分布。例えば、研究炉施設で、放射性物質の在庫量の大部分は、一般に原子炉及び燃料貯蔵プールの中にある；処理及び貯蔵施設で、放射性物質の在庫量はサイトのいたる所に分布させられている。
- (g) 大気中及び水圏への放射性核種の拡散の影響に関係する原子力施設の特徴（例えば、施設の大きさ、設計及び建設、又は地域の人口構成及び土地と水の特徴）
- (h) 施設内と比べての施設外の放射能汚染の可能性（放射能汚染は、サイト境界と放射性物質のある場所との位置関係にある程度、依存する）

3.98. 妨害破壊行為に対する防護のための等級別手法を規定している 1 つの方法は、妨害破壊行為の事案の中で、受容できない及び深刻なレベルでの放射性影響を生じさせる得る放射性物質に適用する物理的防護に求められている相当する性能レベルとともに、受容できない放射線影響及び重大な放射線影響のしきい値として、原子力施設の境界における放射線被ばくのレベルを規定している国を必要とする。次に事業者は、各攻撃対象について、放射性物質の関連する在庫量の拡散がこれらの規定されたレベルを超える放射線影響を引き起こし得るかどうかを決定するために、すべての可能性のある妨害破壊行為の攻撃対象の評価を実施することが要求される。この評価の結果は、敵対者の能力を考慮に入れて、施設の様々な区域について必要とされる防護のレベルを同定するために使用される。

3.99. 表 2 は、様々な潜在的な放射線影響の範囲について等級別の物理的防護レベルがどのように設定されるかのもう 1 つの例を示している。このそれほど高度でない手法は、原子力又は放射線緊急事態についての対応準備に関する IAEA 安全基準文書[10~12]に述べられている、施設及び事業に対する推奨される緊急事態対応準備の区分に対応している影響レベルに基づいて、妨害破壊行為に対する物理的防護システムを策定するための出発点を提供している。この表は、原子炉の熱出力レベルが大きくなるにつれて、妨害破壊行為の攻撃の間に放出される放射性物質の在庫量が多くなるという仮定に基づいている。この手法は、規制の規範的な手法により適している。

3.100 表 2 は、施設を等級付けするための手法の一例として、妨害破壊行為の潜在的な放射線影響についての 3 つのしきい値の概要を述べている。この表を使用して、国は、影響レベル A での、原子力発電所の妨害破壊行為の潜在的な放射線影響が重大な放射線影響であり、枢要区域の同定を要求することを決定することがある[13]。影響レベル B 及び C は、重要であるが、重大な放射線影響よりも懸念の少ない、受容できない放射線影響を意味し、これらのレベルの潜在的影響についての物理的防護システムは **Protected area** を含む場合がある。原子力発電所についての妨害破壊行為の潜在的な放射線影響を決定する方法についての追加的な情報は、参考文献[14]に示されている。参考文献[14]に示されている方法は、他のタイプの原子力施設に適用されることがある。

表 2. 妨害破壊行為の防護要件への等級別手法の例

影響レベル A	影響レベル B	影響レベル C*
<p>妨害破壊行為が、オフサイトに重大な確定的健康影響を生じさせ得る。例えば：</p> <ul style="list-style-type: none"> - オフサイトの重大な確定的影響をもたらすのに十分な、分散性の放射性物質の在庫量を有する施設 - 100 MW(th)を超える出力レベルの原子炉（例えば、原子力発電所、原子力船、研究施設） - 最近の取出燃料及び合計で約 0.1 EBq（3,000 MW(th)の原子炉の中の在庫量と同等）を超える Cs-137 を収納することがある使用済燃料プール（E:エクサ 10¹⁸） 	<p>妨害破壊行為が、オフサイトの緊急の防護活動を必要とするオフサイトの人への線量をもたらし得る。例えば：</p> <ul style="list-style-type: none"> - オフサイトの緊急の防護活動を必要とする線量をもたらすのに十分な、分散性の放射性物質の在庫量を有する施設 - 2 MW(th)を超え、100 MW(th)以下の出力レベルの原子炉 - 能動冷却を必要とする使用済燃料プール - サイト境界の0.5 km以内に、制御されない臨界の可能性のある施設 	<p>妨害破壊行為が、オンサイトの緊急の防護活動を必要とする線量又は汚染をもたらし得る。例えば：</p> <ul style="list-style-type: none"> - オンサイトの緊急の防護活動を必要とする線量をもたらすのに十分な、放射性物質の在庫量を有する施設 - 遮蔽が失われた場合、1 m の距離で 100 mGy/h を超える直接の外部（シャイン）線量率の可能性のある施設 - オフサイト境界から 0.5 km を超えて、制御されない臨界の可能性のある施設 - 2 MW(th)以下の出力レベルの原子炉

* レベル C に満たない潜在的な影響は、少なくとも、慎重な管理慣行に従った防護を要求する。

3.101. 参考文献[8]は、核物質及び原子力施設の物理的防護は受容できない放射線影響を防止するために適切であるという、より大きな保証を国が必要とする時はいつも、設計基礎脅威が規定され、実施されることを推奨している。上記の例で、設計基礎脅威は、参考文献[1]のパラグラフ 3.37 で勧告されているように、重大な放射線影響が発生する影響レベル A の攻撃対象についての防護を策定する時に使用されるべきである。設計基礎脅威はまた、影響レベル B の攻撃対象、及び影響レベル C の攻撃対象についても、国の裁量で使用され得る。

多層防護 (defence in depth) ³

「国の物理的防護の要件は、敵対者対者の目的達成のために敵対者対者によって打ち負かされ又は迂回されなければならない防護の複数の層及び方法（構造的、その他の技術的、人的、及び組織的な）の概念を反映すべきである。」（基本原則 I：多層防護 (defence in depth)）

「3.45. 物理的防護の国の要件は、多層防護 (defence in depth) の概念に基づくべきである。物理的防護の概念は、ハードウェア（防護機器）、手順（警備員の組織及びその職務の遂行を含む）及び施設設計（レイアウトを含む）の計画的な混合を必要とするものである。」 [1]

3.102. 国は、多層防護 (defence in depth) の手法が、検知、遅延及び対応の各機能についての物理的防護システムの設計において実践されることを要求すべきである。各機能について、システムは、それぞれ独立した能力で設計され、1 つの能力の不具合がその機能の喪失にならないようにすべきである。例えば、検知は、要員による観察及び／又は電子的な方法の使用に頼っている。遅延は、攻撃対象へのアクセスを得るために打ち負かされなければならない、複数の独立で多様な物理的障壁（例えば、フェンス、バリケード及び強化された建物など）によって提供される。対応は、施設内の警備員及びその地域の警察、並びに施設内及び施設外外の対抗部隊によって提供される。

3.103. 等級別手法を多層防護 (defence in depth) の適用と組み合わせることは、上位区分の盗取の攻撃対象及び、より重大な潜在的な影響を有する妨害破壊行為の攻撃対象についての物理的防護措置（検知、遅延及び対応）に対して、より多くの層及び、より有効な構成要素の使用を要求するであろう。

物理的防護体制の持続

3.104. 核セキュリティ体制の持続は、IAEA 核セキュリティ・シリーズ No. 20、「国の核セキュリティ体制の目的及び基幹的な要素」[4]に提示している基幹的な要素の 1 つである。持続可能性

³ 「多層防護 (defence in depth)」という用語は、本書においては、参考文献[1]で核セキュリティの分野で定義されているように、物理的防護が損なわれる前に打ち負かされ又は迂回されなければならないシステム及び措置の多層の組み合わせを意味して用いられる。この定義は、安全における「深層防護」のそれと原則的に似ている概念を説明しているが、具体的な定義は IAEA 安全基準シリーズで使用されているものと同じではないということが注意されるべきである。

は、永続的で有効な核セキュリティ体制に寄与するそれらの機能に依存する。参考文献[1]は、次のように、物理的防護を持続することに特に寄与する4つの要素を認識している。

- (a) 核セキュリティ文化：核セキュリティ文化の定義は、「核セキュリティの持続」という語句を明確に含んでいる。
- (b) 品質保証：物理的防護の要件が継続的に満たされているという確信を与える作業。
- (c) 秘密保持：物理的防護を損ない得る機微情報の開示の防止。
- (d) 持続可能性プログラム：有効な物理的防護に必要とされる、保守、資源及び基盤（財政的、人的及び技術的）を具体的に扱うプログラム

核セキュリティ文化

「物理的防護の実施に関係するすべての組織は、セキュリティ文化並びに、組織全体でのその有効な実施を確実にするために必要なその醸成及び維持に対して相応の優先権を与えるべきである。」（基本原則 F：セキュリティ文化） [1]

3.105. 核セキュリティ文化に関する手引きは、参考文献[15]で提供されており、その中で、核セキュリティ文化は、「核セキュリティを支援し強化するための手段として機能する、個人、組織及び機関の特性、姿勢及び行動の集合」として定義されている。

3.106. 強力な核セキュリティ文化の醸成は、有効であるために協働を必要とする、多様な分野及び組織の個人を必要とする。すべての組織は、国の立法上及び規制上の枠組みと調和して策定される、国の核セキュリティ方針を適用する必要がある。組織は、適切な管理構造を策定し、十分な資源を割り当て、また、適切な管理システムを整備する必要がある。これらの組織の管理者は、自身のリーダーシップ及び管理慣行によって、文化に影響を与える上で鍵となる役割を持ち、これには、職員を動機付けすること及び、継続的な改善を捜し求めることがある。有効な核セキュリティ文化の結果は、すべての個人が、物理的防護への厳格で慎重な手法を採用し、用心深く、疑問を持つ姿勢を持ち、また、そうする必要が生じた場合は、迅速かつ正確に対応するというようにあるべきである。

品質保証

「物理的防護に重要なすべての活動についての規定された要件が満たされているとの確信を与える観点で、品質保証方針及び品質保証計画が策定され、実施されるべきである。」
（基本原則 J：品質保証）

「3.52. 物理的防護に関する品質保証方針及び品質保証計画は、物理的防護システムが、脅威評価又は設計基礎脅威に有効に対応できる状態に設計、実施、運転及び維持されること及び、その規範的要件及び/又は性能基準要件を含め、国の規則に適合することを確実にすべきである。」 [1]

3.107. 品質保証プログラムは、作業又はシステムを通してデータを得ること、得たデータを体系的に基準と比較すること及び、作業又はシステムをモニタリングすることについての、メ方法

を提供する。このプログラムの目標は、誤り及び不作為を低減することである。品質保証は統合された管理システムの1つの要素である。

3.108. 確立された物理的防護システムの継続的な有効性を確実にするために、所管当局及び事業者が次の事項を行うことが推奨される。

- (a) 不法移転及び妨害破壊行為に対する核物質及び原子力施設の物理的防護に適用され得る管理方針及びプログラムの品質保証の側面を維持する。
- (b) 品質保証への自らのコミットメントを示すために、品質保証に関する自らの責任を方針声明で発表して、理解してもらい、また必要に応じて、品質に関する組織の目標を設定する担当者にガイドラインを提供する。
- (c) 組織の最高管理層に品質保証に関する直接の報告を提供するような方法の、管理プログラムを設計する。
- (d) 不具合の同定及び評価、並びに是正措置計画の作成及び進捗管理を要求する自らのそれぞれの組織の管理プログラムを開発する。

3.109. 事業者が、性能ベースの要件を満たすために設計された物理的防護システムがその有効性を実証するための適切な裏付け文書を有していることを確実にする管理プログラムを持つことが推奨される。この情報は、補う措置を確立し、是正措置を実施する際に特に重要である。そのようなプログラムはまた、核セキュリティ事案が適時に所管当局に報告されることを確実にすべきである（パラグラフ 3.47 及び 3.48 参照）。

3.110. 管理プログラムがすべてのセキュリティに関連した活動（技術的、手順的及び管理的）を網羅していること並びに、定期的にレビュー及び更新されることも推奨される。管理プログラムは、物理的防護システムの継続性を確実にするために、物理的防護システムの構成管理において重要な役割を果たし、また、変更を行うという決定についての論拠を提供する。

秘密保持

「国は、その不正な開示が核物質及び原子力施設の物理的防護を損ない得る情報の秘密を保護することについての要件を策定すべきである。」（基本原則 L：秘密保持）

「3.53. 国は、その不正な開示が核物質及び原子力施設の物理的防護を損ない得る具体的な又は詳細な情報の適切な保護を確実にするための対策を講じるべきである。どの情報が保護される必要があるのか、及びそれがどのように保護されるべきかを、等級別手法を用いて規定すべきである。」 [1]

3.111. 情報セキュリティに関する国についての手引きは参考文献[16] で提供されている。この手引きは次のように述べている。

「2.5. 機微情報は、その無許可の開示（又は、修正、改変、破壊又は使用拒否）が核セキュリティを損ない得る、又は、原子力施設、組織若しくは輸送に対する悪意ある行為の

実施を支援し得る情報である。そのような情報は、例えば、施設における核セキュリティの取り決め、施設におけるシステム、構造物及び構成要素、核物質若しくはその他の放射性物質の輸送の場所と詳細、又は、組織の要員の詳細を指す。」

3.112. 国は、事業者が満たすための情報セキュリティの要件を設定する；これらの要件は国のセキュリティ当局からの手引き及び方針に基づく。国は、何が機微情報となるかを規定し、また、等級別手法を用いて、そのような機微情報の保有者のための関係する情報セキュリティの要件を規定する。核セキュリティ情報についての区分の分類表の例が、参考文献[16] で提供されている。

3.113. 情報の機密性、可用性及び完全性の保護は、機微情報が無許可の個人又は組織によって入手又は改変されないことを確実にするために、機微情報にセキュリティ措置を適用することに依存する。情報セキュリティとしては、いかなる形態の情報の保護を確実にするシステム、プログラム及び一連の規則がある。情報セキュリティとしては、最低限として、以下のものがある。

- (a) 物理的媒体及び電子媒体上の情報セキュリティ
- (b) コンピュータ・ベースのシステムのセキュリティ（コンピュータ・セキュリティ）
- (c) 通信システム及びネットワークのセキュリティ
- (d) 施設の従業員及び第三者（例えば、請負業者、供給業者）についての情報セキュリティ
- (e) 無形の情報（例えば、上記に関する知識）のセキュリティ

3.114. 機微情報を有する組織は、国の情報セキュリティ方針が施行されていること、及び、すべての従業員がセキュリティについての要求を十分に認識し、かつ、組織の規則に従っていることを確実にすべきである。

3.115. 各組織は、国の情報セキュリティ方針を遵守して、それぞれの機微情報の機密性、完全性及び可用性を保護することについての、その組織の内部方針、計画及び手順を確立する必要がある。

3.116. 参考文献[1]の параграф 3.54 は、次のように述べている。

「物理的防護システムの管理者は機微情報へのアクセスを、機微情報について個人の信頼性が適切であると確認され、かつ、本人の職務の遂行のためにそれを知る必要のある者だけに制限すべきである。物理的防護システムの脆弱性を示している情報は、高度に保護されるべきである。」

保護される情報としては、妨害破壊行為及び盗取の攻撃対象の場所と特徴、物理的防護システムの設計と運転に関する情報（防護システムであり得る脆弱性及び核物質の計量及び管理の側面を含む）及び、対抗部隊の戦術と活動の危機管理計画の詳細がある場合がある。

3.117. 国は、物理的防護システムに関係する情報の機密保持を確実にする上で、事業者が実践すべき規定を明確に規定すべきである。これらの規定は、保護される必要のある情報を、及び、情報の機微性と情報の紛失の影響にふさわしい、要求される保護のレベルを同定すべきである。これらの規定を満たすための事業者の措置は、事業者のセキュリティ計画の中で文書化されるべきであり、事業者と所管当局によって定期的に評価されるべきである。

3.118. 参考文献[1]の paragraph 3.55 は、次のように述べている。「守秘義務違反者に対する制裁は、国の法律又は規制制度の一部であるべきである。」守秘義務違反者に対する制裁についての情報は、機微情報へのアクセスを許可される者に伝えられるべきであり、また、そのような行為に対する抑止として作用するために十分厳しいものであるべきである。国は、そのような違反を、その違反の潜在的な深刻さを考慮に入れた適切な罰をもって処するべきである。

持続可能性プログラム

3.119. 国は、核セキュリティ体制の一環として、物理的防護の基盤、システム及び措置の持続可能性を立法上及び規制上の枠組みが支援することを確実にすべきである。2つの良好事例は、国が、国と事業者の両方の物理的防護要員の訓練のための基盤を提供すること、及び、実務の場合には常に、物理的防護の機器の試験及び評価のための施設を提供することである。そのような試験は、国及び事業者に、必要な性能レベルで物理的防護の措置及び機器を維持するための実務について情報を与えることができる。

核セキュリティ事案についての計画、準備及び事案への対応

「核物質の不法移転、又は原子力施設若しくは核物質への妨害破壊行為、又はその企てに対応するための危機管理(緊急時)計画は、すべての許可保有者及び関係する所管当局によって準備され、また適切に演習されるべきである。」(基本原則 K : 危機管理計画) [1]

3.120. この基本原則は、危機管理計画が緊急事態計画と同じものであることを暗に意味している。実際には、これらの用語の定義と使用に、国の間で違いがある。参考文献[1]では、危機管理計画は全体的な核セキュリティ計画の一部であり、悪意ある行為を含む核セキュリティ事案への物理的防護の要員の対応に関連している。IAEA 安全基準シリーズ No. GSR Part 7、「原子力又は放射線緊急事態への備えと対応」[10]で、緊急事態計画は、緊急事態が事故によって引き起こされるか悪意ある行為によってかを問わず、原子力又は放射線緊急事態への対応に関連している。しかしながら、危機管理計画及び緊急事態計画の実施は、物理的防護、核物質の計量及び管理、並びに安全の要員による協調的対応を要求するであろう。

3.121. 核セキュリティ事案への対応の間、事案の対応に関係するすべての組織が、地方及び国レベルで適切に対応する準備ができていることが最も重要である。核セキュリティ事案について、計画及び準備し、事案に対応するために国が取るべき措置が、参考文献[4]に述べられている。国及び事業者は、行方不明の核物質を捜し出して回収するために、並びに、妨害破壊行為の影響を緩和及び最小化するために、核セキュリティ事案のために計画及び準備すること及びこれに対応することについて、共有で相補的な責任を有する。盗取後の核物質を捜し出して回収する

ための活動について、事業者は原子力施設の外での権限が限られる場合があり、したがって国が、事案へのオフサイトの対応の第一の責任を有することが期待できる。これに関して、責任が、事業者とその他の政府組織との間で明確に割り当てられる必要がある。

3.122. 危機管理の計画立案の目標は、原子力施設に関係する、又は原子力施設に向けられた悪意ある行為を含む、核セキュリティ事案へのすべてのレベルでの適時で有効な対応を確実にすること、及び、例えば放射性核種の放出に関係している事故、医療的緊急事態又は自然災害など、他の事象の間の物理的防護を維持することである。正しい措置がとられること及び、事案に適切に対応して状況を解決するために適切な時間になされる決定を必要とする。原子力又は放射線緊急事態の場合に、緊急事態計画の実施の間の物理的防護システムの継続的な有効性を確実にするために措置がなされるべきである。

3.123. 国及び所管当局は、事業者のセキュリティ計画に含まれている危機管理計画が国レベルで策定されたそれと整合性のあることを確実にすべきである。この整合性は、対応に係る政府機関と事業者との間の協定（書面による記録、例えば覚書やその他の協定書など）の作成の助けを借りる場合がある；これらの協定は、例えば、各組織の役割及び責任を明確に同定するであろう。必要な協調のレベルは、例えば、練習シナリオ及び適切な危機管理計画を用いた合同訓練及び演習を実施することによって達成され得るであろう。

3.124. 国、適切な所管当局及び事業者は、様々なタイプの核セキュリティ事案に対処する包括的な一連の危機管理計画を有しているべきである。危機管理計画を要求するそのような事案の例は、付録 I に提供されている。

3.125. 国は、全体的な核セキュリティ体制の枠組みの中で危機管理計画の有効性の検証を促進するために、演習が定期的実施されることを確実にすべきである。これらの演習としては、脅威評価又は設計基礎脅威の範囲である不法移転と妨害破壊行為の両方についてのシナリオがあるべきである。

3.126. （例えば、盗取の結果として）規制の管理外にある核物質の捜し出しと回収のための適切な対応に関する追加の手引きは参考文献[7]で提供されている。

4. 原子力施設のための統合された物理的防護システムの 策定、実施及び維持

4.1. このセクションは、不法移転及び妨害破壊行為に対する、核物質及び原子力施設の物理的防護について、事業者に対して示された勧告[1]を実施することに関する手引きを提供する。これらの勧告は大体、参考文献[1]の параграф 3.23～3.30 並びにセクション 4 及び 5 にある。

4.2. 参考文献[1]は、物理的防護システムが核物質の不法移転と妨害破壊行為の両方の脅威に対して有効な単独のシステムであるべきであるということを暗に意味していて、その両方に対して防護するための物理的防護の要件を一体的に実施することを勧告している。さらに、参考文献[1]は、不法移転又は妨害破壊行為のリスクのどちらが、より嚴重な物理的防護の要件を要求するにしても、リスクに対する有効性を確実にする方法で物理的防護システムを設計することを勧告している（参考文献[1]の параграф 4.4、5.3 及び 5.17）。

4.3. このセクションは、不法移転及び妨害破壊行為の両方の脅威に対して有効な単独の物理的防護システムの設計に推奨される手法を提供している。このセクションで示されている設計のための段階的手法は、参考文献[1]で詳細にカバーされていないシステムエンジニアリングの原則（物理的防護の要件の同定、これらの要件を満たすためのシステムの設計、及び、その結果の物理的防護システムの有効性の評価）を物理的防護に適用している。物理的防護についての体系的なエンジニアリング手法の要素を明示するための他の方法があるかもしれないが、このセクションで示される手順は、IAEA によって奨励されている手法と整合性があり、また、利用者の物理的防護システムを設計し、実施するための基本的枠組みを利用者に提供することを目的としている。

事業者の全般的な責任

「国内の物理的防護の様々な要素の実施に対する責任は、明確に特定されるべきである。国は、核物質の又は原子力施設の物理的防護の実施に対する第 1 の責任が関連する許可の又はその他の認可文書の保有者(例えば事業者又は荷送人)にあることを確実にすべきである。(基本原則 E : 許可保有者の責任)」

.....

「3.25. 事業者、荷送人及び運搬人は、物理的防護に責任を有する、例えばオフサイトの対抗部隊など、その他のすべての国の組織と協力して協調すべきである。」 [1]

4.4. これらの責任を履行する際に、事業者は、国の立法上及び規制上の枠組みの規定に完全に適合すべきである。これらの規定は、その地域の法執行機関、国の警察、軍、並びに、例えば地方及び国の緊急事態対応者、諜報及びその他の国内のセキュリティ組織などのその他の組織と協定（例えば覚書、協定又はその他のタイプの書面による記録など）を締結することを事業者に要求する場合がある。

4.5. 事業者は、事業者の施設での核物質についての物理的防護システムの策定及び実施の第一の責任を有する。事業者は、施設固有のセキュリティ計画を作成すべきである（パラグラフ 4.154～4.161 参照）。付録 I は、提案するセキュリティ計画の書式を提供している。

4.6. 参考文献[1]のパラグラフ 3.30 は、次のように述べている。

「物理的防護システムが要求される防護レベルを提供することができないと判断されたときはいつも、事業者、荷送人及び/又は運搬人は、十分な防護を提供するための補う措置を直ちに実施すべきである。事業者及び/又は荷送人は次に（同意された期間内に）、所管当局によってレビューされて、承認されるために、是正措置を計画し、実施すべきである。」

補う措置は、劣化した又は動作不能なセキュリティに関連した構造物、システム及び構成要素を補うために、それらが修理又は交換され得るまでとられる短期的な措置である。補う措置を提供することの 1 つの手法は、不備が同定されたらできる限り早く不備を補うために予備の警備員及び/又は対抗部隊を追加することである。補う措置は文書化され、承認されること、並びに、措置が実施される前に、国、所管当局、事業者及び対抗部隊の間で、必要な協調についての取決めが合意されることが推奨される。

4.7. 参考文献[1]のパラグラフ 3.28 は、次のように述べている。

「新規の原子力施設に関して、立地選定及び設計は、物理的防護をできるだけ早い時期に考慮に入れるべきであり、さらに、物理的防護、安全並びに核物質の計量及び管理の不一致を避けるために、並びに、3つの要素が互いに支え合うことを確実にするために3つのインターフェイスにも取り組むべきである。」

注意深い考慮が、原子力施設の立地の核セキュリティに対する影響について払われる必要がある。その地域の基盤、サイトの配置及びその地域のその他の条件はすべて、核セキュリティに影響を与える。特に、複数の原子力設備を持つ原子力施設のサイトの配置は、適切な多層防護（defence in depth）を提供するために物理的防護措置の必要空間について考慮する必要がある場合がある。

4.8. 新規の原子力施設の設計は、核セキュリティの要求を考慮すべきである。これらの目的を達成するための設計手法は、「セキュリティ・バイ・デザイン」と呼ばれている。そのような手法を実施することは、原子力施設の存続期間に亘って物理的防護のコストを低減することにつながる場合があり、また、存続期間に亘って有効な物理的防護システムを維持するという職務を平易にする場合もある。

4.9. セキュリティ・バイ・デザインの目的は、要求されるセキュリティのレベルが、運転、安全並びに核物質の計量及び管理と両立できる費用効果の高い方法で提供されるように新規の原子力施設を設計することである。セキュリティ・バイ・デザインは、国の核セキュリティの目的が

考慮され、かつ、施設の計画に始まり、設計、建設、運転及び廃止措置フェーズまでを含めて続く、施設の存続期間全体についての設計の決定において十分に考慮されるような構造化された手法によって最良に実施される。

4.10. 良好事例は、物理的防護システムの策定作業のできるだけ早期に、原子力施設の全体的な設計の中へ、物理的防護システムの設計を統合することを開始することである。早期の検討としては、施設の立地及び配置に関する決定が物理的防護システムの設計と有効性にどう影響を及ぼすかを考慮に入れて、それらの決定を行うことがある。例えば、適切な工学技術によって潜在的な脆弱性を排除することにより、相補的で相乗的な設計の機会を利用しながら、その他の設計要件との不一致を最小化することが重要である。

4.11. 事業者の最高管理者レベルは、施設の活動の中への物理的防護措置の統合を認識し、承認する必要がある。参考文献[15]に記載され、また、パラグラフ 3.105 及び 3.106 で簡略に論じているように、管理者が、強力な核セキュリティ文化を奨励することも同様に重要である。

4.12. 物理的防護の実施の統合された手法について、原子力施設の事業者は不法移転及び妨害破壊行為に関するすべての潜在的な攻撃対象を同定し、国の規制の手法に基づいた等級別の方法ですべての要求される防護措置を実施する。原子力施設のタイプに応じて、妨害破壊行為又は不法移転のいずれかの攻撃対象は、より高い防護のレベルを必要とする場合があるが、すべての場合に、防護の適切なレベルが、すべての攻撃対象に対して実施されるべきである。この手法は、参考文献[1]のパラグラフ 4.4 及び 5.3 の「より厳しい該当する要件」を適用するという勧告が目的とするものである。

4.13. 原子力施設の建設における核セキュリティの検討は、勧告文書[1]では具体的に示されていない。しかしながら、良好事例は、建設前に、事業者（又は申請者）がすべての建設フェーズの間に物理的防護がどのように実施されるかを同定すべきであるということを手助けしている。もし新規の施設が建設されることになっているサイトに隣接して、原子力施設がある場合、既存の運転中の施設を防護するための追加の物理的防護措置が、建設が始まる以前に、密接に連携して両方の事業者によって、同定され、実施されるべきである。（同様にもし、既存の原子力施設を拡張又は変更するための建設作業が行われる場合は、その施設の既存部分を防護するために、追加の物理的防護措置がとられるべきである）。安全及び品質保証の監査は、例えば欠点や偽装された装置の意図的な導入など、将来の妨害破壊行為を手助けすることを意図する行為を検知することによって、妨害破壊行為に対して防護するためにも使用されるかもしれない。建設フェーズの終わりに、最終評価が、試運転御開始前に物理的防護の措置の有効性を確認するために推奨される。

防護組織

4.14. セキュリティについての任務と責任は、統合された管理システムの枠組みの中で確立されるべきであり、次の3つの相補的ユニットに分けられる場合がある。

- (a) 物理的防護の全体的責任を有し、また、所管当局及び施設管理者（人的資源管理者を含む）とインターフェイスをとる管理者、セキュリティ計画の策定と維持に責任がある計画立案者、所管当局の要件を満たすための物理的防護システムの設計又は更新に責任がある設計者、及び、設計要件に対する物理的防護システムの性能を評価することに評価に責任がある分析者を含んでいるセキュリティ管理ユニット。安全とセキュリティ間のインターフェイスについての責任の割り当ても、セキュリティ管理の一部である（パラグラフ 4.147～4.153 参照）。
- (b) 要員と訪問者に関係するセキュリティ（個人の信頼性及び立入許可）、情報セキュリティ、コンピュータ・セキュリティ、並びに、出入管理及び付添、中央警報ステーションの業務、巡視及び核セキュリティ事案への対応を含む業務に当たる警備員及び（国によって指定された責任に従う）対抗部隊についての責任があるセキュリティ業務ユニット。
- (c) 設置及び高度化、（必要に応じてセキュリティ業務担当者による支援を受ける）性能試験、予防保守、臨時の修理及び交換を実施する技術担当者を含んでいて、また、必要に応じてセキュリティ管理ユニット及びセキュリティ業務ユニットに支援とインプットを提供する技術的セキュリティユニット。

物理的防護システムの策定及び実施の手順

4.15. このセクションは、新規の原子力施設の建設（及び、既存の原子力施設への新規の設備の建設）のための物理的防護システムの設計、策定及び実施について、既存の物理的防護システムの高度化について、並びに既存の物理的防護システムの有効性のレビューについての手法の概要を述べる。

物理的防護システムの策定のための手法

4.16. 物理的防護システムの策定は、3つのフェーズからなる体系的な手法を用いて最適に達成される。これらの3つのフェーズは次のとおりである。

- (1) 物理的防護システムの目的及び要件を同定。
- (2) フェーズ1で同定された目的及び要件を満たすために物理的防護システムを設計。
- (3) フェーズ1で同定された目的及び要件を満たしている、フェーズ2で設計された物理的防護システムの有効性を分析及び評価。

これらの3つのフェーズの順序付けと各フェーズの下での活動の大まかな概要を図2に示す。

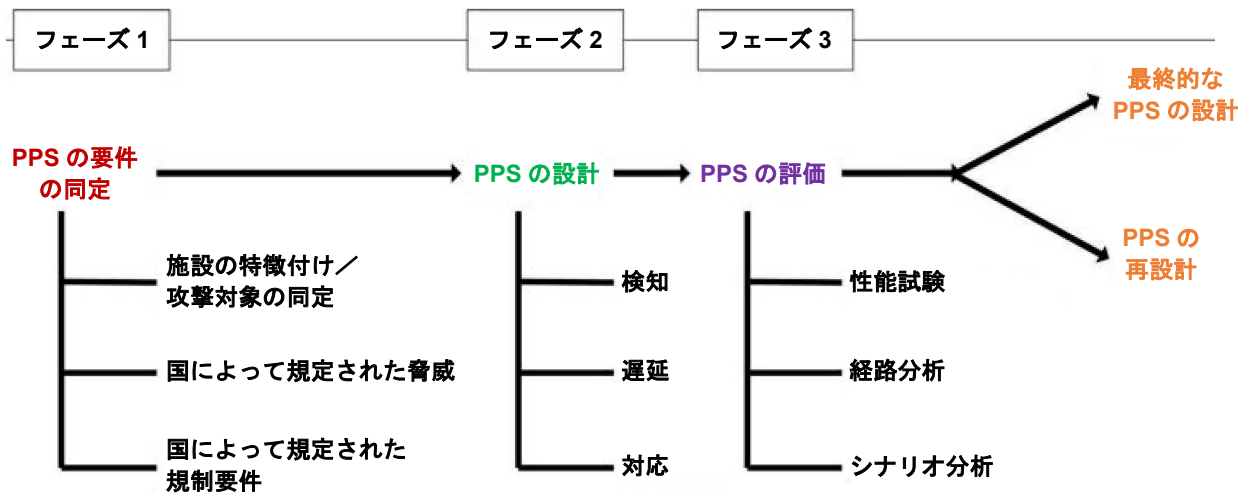


図2. 物理的防護システムの設計と評価の手順 (PPS：物理的防護システム)

4.17. 以下の詳細で及びパラグラフ 4.23～4.59 で説明している、これらの3つのフェーズを適用することは、核物質の不法移転及び妨害破壊行為の脅威に対して防護するための、また、適用することがあるその他の施設固有の目的を満たすための物理的防護システムの設計をもたらすであろう。

物理的防護システムのライフサイクル

4.18. 物理的防護システムが、この策定手順を用いて設計及び評価された後、物理的防護システムのライフサイクルでの次のステップは、設計を実施すること；その結果の物理的防護システムを運用、維持及び持続すること；及び、脅威、施設の配置、運転又は潜在的な攻撃対象の変化に基づいた、又は性能監視に基づいた物理的防護システムの適切な再設計を計画することである。これらのライフサイクルのステップを図3に示す。

物理的防護システムの持続

「3.57. 事業者・・・は、物理的防護システムについての持続可能性プログラムを策定すべきである。持続可能性プログラムは、次のものを網羅すべきである。

- 業務手順(指示書)
- 人材管理及び訓練
- 設備の更新、維持、修理及び較正
- 性能試験及び運用監視
- 構成管理(施設の物理的防護システム(コンピュータ・システム及びソフトウェアを含む)の特徴の同定及び文書化の処置、並びにこれらの特徴の変更が適切に策定、評価、承認、発行、実施、検証、記録され、施設の文書化体系に組み込まれることを確実にする処置)
- 資源の割当て及び運用コストの分析」 [1]

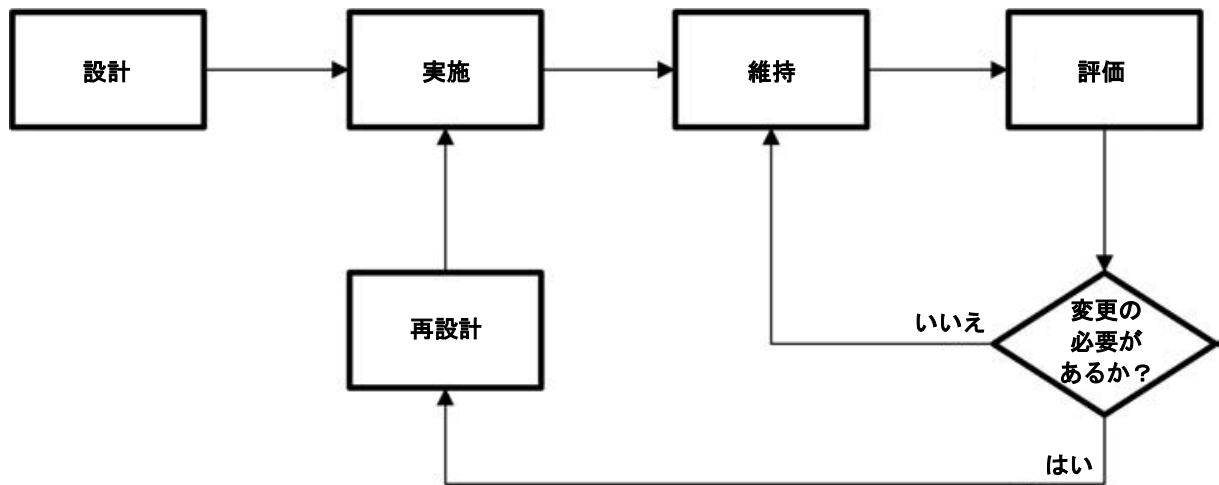


図3. 物理的防護システムのライフサイクル

4.19. 核セキュリティ体制を持続するための国の手法を考慮に入れて、事業者は、必要な資源（訓練を受けた知識豊富な要員、信頼性のある機器、関係する基盤、品質保証及び財源）が、持続可能性プログラムの一環として事業者の物理的防護システムを維持するために提供されることを確実にすべきである。

国の要件の適合

4.20. 図2に示す3つのフェーズの作業を開始する前に、事業者又は申請者は、セクション3で網羅されているような、国の核セキュリティ体制の関連関係する側面を理解すべきである。特に関係しているのは、事業者又は申請者が物理的防護システムを設計すること、及び設計の承認について国に申請することに影響を与えるいくつかの側面である。そのような側面としては、以下のものがある。

- (a) パラグラフ 3.12～3.26 に明示されるように、脅威に対処するための要件を指定するために、国によって選択される規制手法を含む、国の立法上及び規制上の枠組み、並びに、国の個人の信頼性の方針の実施
- (b) パラグラフ 3.70～3.73 で述べられているように、等級別手法に基づいて国によって規定される要件
- (c) パラグラフ 3.33～3.37 で述べられているように、新規の許可証及び既存の許可証の更新又は変更についての申請を承認するための許認可の作業

4.21. 国によって採用される規制手法（パラグラフ 3.18～3.26 で述べられているような、）性能ベースの手法、規範的な手法及び複合手法）に応じて、要件を満たすための事業者又は申請者の手法は異なるであろう。

4.22. 図 4 は、事業者又は申請者が規制手法に応じて実施すべき作業を示している。複合手法について、必要に応じて両方のフローに従う必要があるであろう。図 3 は、設計がどのように策定され、評価されるを示している；図 4 は、事業者又は申請者が実施するその他の活動、及び国が付与する承認を示している。

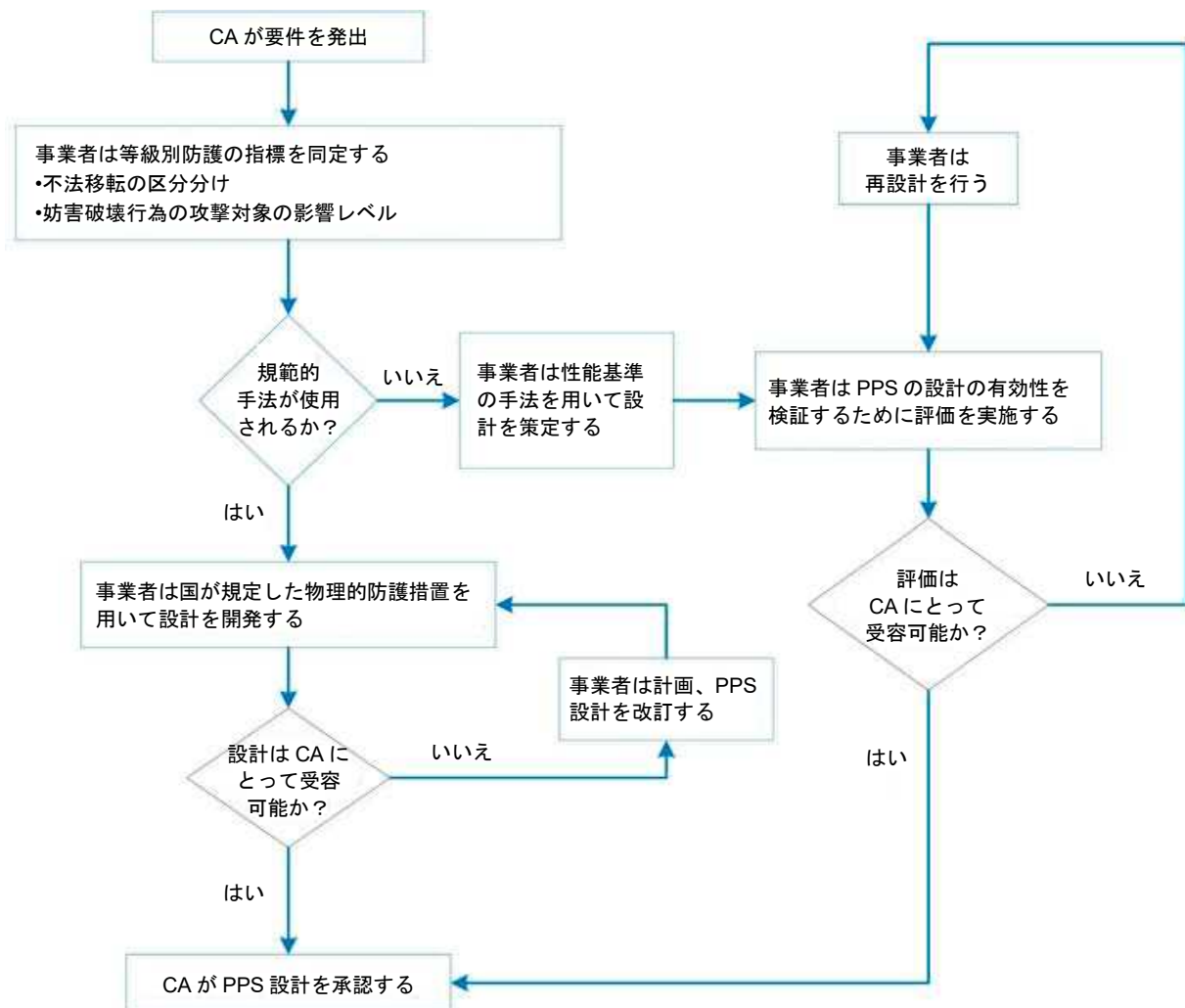


図 4. 物理的防護システムの設計手順
(CA：所管当局、PPS：物理的防護システム)

物理的防護システムの要件の同定（フェーズ 1）

4.23. 事業者又は申請者による物理的防護システムの設計の策定及び評価におけるフェーズ 1 は、具体的なサイト、原子力施設及び物理的防護システムに適用する、物理的防護についての国の要件を決定することである。事業者又は申請者は、この決定において、次のように、いくつかのステップを実施する必要がある。

- (a) 施設の業務と状態の特徴付け。このステップは、施設内の作業及び業務を記述すること；（施設の境界及び建物場所、平面図、構造物の立面図及びアクセスポイントを含む、）施設の詳細な説明を展開すること；及び、既存の施設又は設計について、物理的防護システムの要素として使用される場合の既存の機能又はシステムを同定することを含む。施設についての情報は、例えば施設図面及び作業記述書など、既存の文書を含む、すべての関係する情報源から、及び、施設の観察及び担当者との面談から集められ得る。物理的防護システムの設計者は、この情報、及び、設計中に直面する可能性がある施設固有の制限事項（例えば安全上の制限事項など）の詳細な知識を必要とするであろう。
- (b) 設計の基礎として役立つために、事業者又は申請者に国によって提供される脅威に関する情報の解釈（パラグラフ 3.55～3.63 参照）。このステップは、性能ベースの手法又は複合手法に徳化している（規範的な手法でにおいて、国は通常、事業者に脅威情報を提供しない）。
- (c) 核物質の国の区分及び／又は妨害破壊行為の潜在的な影響に基づいて国によって規定されるような敵対者から防護される必要のある、攻撃対象及び施設内でのそれらの場所の同定（パラグラフ 3.74～3.101 参照）。

4.24. 国によって明示される敵対者の能力は、物理的防護システムによって対抗される必要があり、したがって、事業者又は申請者によって検討される必要がある。これらの能力としては次のようなものがある。

- (a) 物理的防護システムに関する知識
- (b) 攻撃に役立つ技能
- (c) 攻撃に使用され得る工具及び武器

攻撃対象の同定

4.25. 攻撃対象の同定は、どの物質及び／又は機器が敵対者から防護される必要があるかを決定する。攻撃対象の同定の作業における4つのステップは次のとおりである。

- (a) 物理的防護の目的を理解する。
- (b) 不法移転及び／又は妨害破壊行為から防護される必要のある、核物質及びその他の放射性物質の種類、並びに、（コンピュータ・ベースのシステム及び情報を含む）安全上重要なシステムを同定する。
- (c) 核物質の適切な区分及び／又は、各攻撃対象に適用する妨害破壊行為の潜在的な影響を同定する。
- (d) 施設についての、防護されるべき各攻撃対象の説明、その区分及び場所を含んでいる、攻撃対象リストを策定する。攻撃対象リストは、機微情報として保護されるべきである。

4.26. 核物質の各区分のについて推奨される防護措置が、参考文献[1]のパラグラフ 4.9～4.49 に述べられている。

4.27. 妨害破壊行為の攻撃対象の同定のために、国は先ず、受容できない放射線影響及び重大な放射線影響として規定するために適切と考える、潜在的な放射線影響のしきい値のレベルを決定すべきである（パラグラフ 3.91～3.101 参照）。

4.28. 参考文献[1]のパラグラフ 5.4 は、次のように述べている。

「各原子力施設について、放射性物質の在庫量が、国によって決められた受容できない放射線影響を生じる潜在力を有しているかどうかを判定するために、所管当局によって有効性が実証された解析が、物理的防護措置又は緩和措置の効果を無視して、妨害破壊行為が成功裡に完遂されることを仮定して、実施されるべきである。」

この分析は、参考文献[14]で論られているように、受容できない放射線影響につながる可能性がある、2つのタイプの妨害破壊行為、すなわち、直接的及び間接的な妨害破壊行為に取り組む。直接的な妨害破壊行為は、核物質又はその他の放射性物質を拡散するために、例えば従来型の爆発物など、外部からエネルギーを持ち込む；間接的な妨害破壊行為は、例えば炉心冷却系に損傷を与えることによって、核物質又はその他の放射性物質内の過程からのエネルギー（例えば、核分裂又は放射性崩壊からの熱）を使用する。

4.29. 保守的な分析が、施設において同定された妨害破壊行為の攻撃対象のそれぞれの中の核物質又はその他の放射性物質の在庫量の全部の放出から生じる得る潜在的な放射線影響を決定するために、実施されるべきである。核物質の間接的な妨害破壊行為について、この在庫量としては、核連鎖反応によって生じる核分裂生成物があることがある。

4.30. 原子力施設は、その運転が安全であることを示すために、大規模な安全解析の対象となる。安全解析報告書の中の情報は、妨害破壊行為に対して防護される必要のある構造物、システム及び構成要素を同定するのに役立つ場合がある。悪意ある行為による不具合のその他の可能性のある原因を検討することも、重要である。

4.31. 妨害破壊行為の攻撃対象について評価された潜在的な放射線影響は、次に、それらの攻撃対象についての物理的防護の要件を決定するために、次のように使用される。

- (a) もし、潜在的な放射線影響が、重大な放射線影響のしきい値を超える場合、枢要区域が同定され、防護されるべきである。
- (b) もし、潜在的な放射線影響が、受容できない放射線影響と重大な放射線影響のしきい値の中間に位置する場合、国は、潜在的な影響のレベルに基づいて等級別の防護要件を規定するであろう。
- (c) もし、放射線影響が、受容できない放射線影響のしきい値を下回る場合、物理的防護の具体的な要件はないかもしれないが、事業者はそれでも、安全に関連する機器及び装置を守り、アクセスを管理すべきである。

脅威の明確化

4.32. 物理的防護システムについての目的と要件の同定の一環として、施設への脅威が、脅威評価、又は設計基礎脅威の策定による脅威のいずれかを通して、国によって明示されるべきである。関連する情報は、この情報を物理的防護システムの設計と評価についての基礎として使用すべき事業者提供されるべきである。

物理的防護システムの設計及び評価

4.33. 物理的防護システムの目的及び要件が同定されると（フェーズ1）、事業者又は申請者は物理的防護システムの目的が分かる；何を防護すべきか（攻撃対象）、何に対してか（脅威）、及び、どれほど良くか（要件）。次のステップ（フェーズ2）は、システムの目的を満たすのに十分である検知、遅延及び対応についての物理的防護措置を提供するために、新規のシステムを設計すること、又は既存のシステムを再設計することである。物理的防護システムが設計又は特徴付けされると、物理的防護の要件を満たすことを確実にするために、物理的防護システムが分析及び評価されるべきである（フェーズ3）。評価は、防護を確実にするために様々な措置が連携した有効性によって示されような、システムの全体的な有効性に基づくべきである。

設計フェーズ（フェーズ2）

全般的な設計検討

4.34. このフェーズの間、設計者は、例えばフェンス、貯蔵庫、センサ、手順、通信機器及び対抗部隊など、物理的防護の措置を、防護要件を満たすようにいかに最適に物理的防護システムに統合するかを決定する。この決定は、物理的防護と安全の目的が満たされるように、安全と運転上の検討事項を考慮に入れる。全体の目的は、物理的防護システムが、検知、遅延及び対応の機能間の適切な調和を提供することによって、防護要件を満たすことを確実にすることである。

4.35. 図5は、設計の原則を示しており、また、明確にされた物理的防護システムについて、敵対者が指定された悪意ある行為を完遂するために必要な作業のすべてを実施する前に、対応するために十分早期に確実に通知を受けるかどうかを判定するために使用されるタイムラインを示している。最上段は、敵対者の攻撃の時系列及び、敵対者の存在を感知するための物理的防護システムについて、攻撃対象への敵対者の経路に沿って、機会を表している。「物理的防護システムの対応時間」は、この図の下部のタイムラインに描かれている；このタイムラインは、時間 t_0 において敵対者の活動について最初に成功した感知（パラグラフ 4.62~4.67 参照）から、時間 t_1 において敵対者が阻止され得るまでの時間を測る。この図で、感知は、敵対者が攻撃をうまく完遂する時間 t_c よりも前に、敵対者が対抗部隊によって阻止されることを可能にするために、十分早く気付いている。

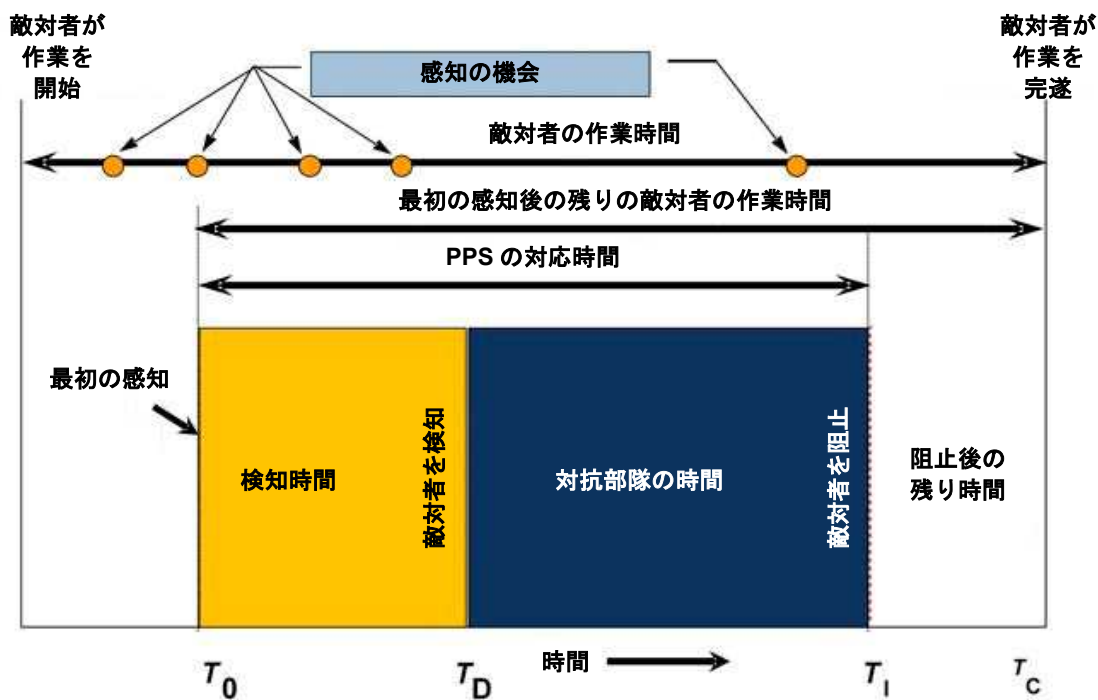


図5. 敵対者のタイムラインと対応のタイムラインの比較
(PPS：物理的防護システム)

4.36. 物理的防護措置の設計における良好事例としては、次のような対策がある。

- (a) 多層防護 (defence in depth) 例えば、敵対者が、成功するために、順に、いくつかの防護措置を欺く、避ける、又は打破する必要があるようなこと。多層防護 (defence in depth) は一般に、攻撃対象の周りに一連の防護の層を置くこと (物理的な措置 (例えば、区域への立入の管理。パラグラフ 4.86~4.89 参照) と管理的な措置 (例えば、機微情報の保護及び個人の信頼性の方針の実施) の組み合わせとする場合がある)、によって実施される。この手法は、物理的防護の各構成要素の長所を利用すること、及びその強みを補完する又は互いの限界を補う組み合わせで機器を使用することを含む場合がある。
- (b) 調和のとれた防護 例えば、敵対者が、いつでも、どこでも、又はどのように悪意ある行為が企てられても、物理的防護システムの同じ程度に有効な措置に直面するようなこと。
- (c) 堅牢性 物理的防護システムが、さまざまなタイプの敵対者の攻撃の際に、有効に機能する高い確率を有することを意味しており、一般に、設計に冗長性と多様性を取り入れることによって成し遂げられる。

4.37. 敵対者の目標を達成するために敵対者に必要な時間は「敵対者の作業時間」である (図 5 参照)。障壁の第一の役割は、敵対者が選ぶかもしれない経路に沿って障害物を導入することにより、敵対者の作業時間を増加させることである。敵対者は、特定の攻撃対象に接近する前に、いくつかの別々の障壁を突き抜ける又は迂回しなければならない。これらの障壁のそれぞれを突き抜ける又は迂回するのに必要とする時間は、必ずしも同じである必要はないが、障壁は、敵対者が経路に沿って移動している時に、それぞれの障壁が、別々で異なる行為を必要とするよう

に、選ばれるべきである。多層防護（defence in depth）を提供するために設計される物理的防護システムによって敵対者にもたらされる影響は次のようなものとなるであろう。

- (a) 物理的防護システムについて敵対者が感じる不確かさを増加させる。
- (b) 物理的防護システムを攻撃する前に、追加の工具及びより大規模な準備を必要とする。
- (c) 敵対者に攻撃を失敗させる、又は攻撃を断念させる、追加のステップを設ける。

4.38. 検知及び評価のシステムについて、堅牢性は、複数の相補的なセンサ及び人による監視の組み合わせによって達成され得る。相補的であるために、特定の層又は障壁のセンサは、1つのセンサを打破するための企てが、別のセンサによって検知可能であるように、また、異なるセンサが同じ迷惑警報源に反応しないように選ばれる。人によるランダム又は継続的な監視を追加することは、物理的防護システムについて敵対者が感じる不確かさを増加させ、攻撃を計画して成功裏に実施することをより困難にさせる。

4.39. 物理的防護システムの設計は、安全のために重要な施設の運転システムと両立できる必要があり、また担当者が安全で厳重な方法で担当者の任務を実施することを可能にする必要がある。もし、担当者にとって、担当者の作業を完了することを困難にする物理的防護措置があれば、担当者は、それらの防護措置の実行を避ける方法を見つける場合がある。物理的防護システムの設計の間に応用される、原子力施設の運転に関する詳細な理解は、物理的防護の要求と安全及び運転の要求のバランスを取ることを促進するであろう。

4.40. 上述の設計手法は、外部の敵対者に対して防護するために開発されており、また、防護するために適用される。追加の及び／又は別の要素が、内部脅威に対する物理的防護システムを設計する際に考慮される必要がある。

内部脅威についての追加的な設計検討

4.41. 内部者は、不法移転若しくは妨害破壊行為を企て得る、又は、そうする外部敵対者の助けとなり得る、原子力施設又は関連する機微情報へのアクセス権を有する1人又は複数の者と定義される。内部脅威はそのような行為を実施する意図を持つ内部者である。内部者としては、管理者、常勤従業員、請負業者及びサービス提供者、検査官、及び訪問者である場合がある。したがって、内部者は、施設におけるいかなる立場の場合もあり、また、管理区域又は物質へのアクセス権を持つ場合がある。

4.42. 内部者の能力は、一般的に次の3つの特性によって明示される。

- (a) アクセス権の範囲：内部者が様々な施設の状態（例えば、通常業務、非稼働の期間、保守停止期間）の間に、又は、セキュリティ事案若しくは安全事案の間に、施設のどの区域に立ちることができるか、又はできないか。
- (b) 他の人々又は一定の作業及び機器に対する権限のレベル
- (c) 攻撃対象、施設配置、物理的防護システム、及び／又は、施設に在る特殊な工具及び機器を入手し操作するための方法の知識

4.43. 内部脅威は、不法移転又は妨害破壊行為に及ぶため、又は手助けするために技術的及び管理的な物理的防護の措置を迂回するために、これらの内部者の特性を利用し得るので、外部敵対者と異なる問題を提起する。内部者はまた、検知の可能性を下げ、したがって、成功の可能性を高める長期間に亘る、別々になった一連の行為によって、悪意ある行為への寄与を完遂することもできる。内部者はまた、悪意ある行為を遂行するために、最も脆弱な攻撃対象及び絶好の機会を選ぶための、より多くの知識及び／又は機会を有している場合がある。

4.44. 国の脅威評価又は設計基礎脅威と整合性のある悪意ある行為に対して攻撃対象を防護するために、物理的防護システム的设计としては、攻撃対象への無許可の者又は機器によるアクセスを拒否するための、及び悪意ある行為に及ぶためにそのようなアクセスができる内部者の機会を最小化するための機能があるべきである。例えば、障壁の存在は、実働の対抗部隊と組み合わせると、攻撃対象への外部の敵対者のアクセスを拒否することを果たす。一方、攻撃対象に関連する一部の機器を施錠することは、攻撃対象の在る区域へのアクセス権を持つ内部者に対して遅延を引き起こすことでもある。また、もし、区域が連続的な監視下にある場合は特に有効である。

4.45. 参考文献[9]は、悪意ある行為を始める又は支援する内部者の機会を最小化するための予防措置、及び内部者によって犯される行為の検知、遅延、対応及びその緩和のための防護措置を含んで、内部脅威に対して防護するための体系的な手法を提示している。

4.46. 内部脅威の攻撃シナリオに対抗するための防護措置は、物理的防護措置、プロセス制御、安全警報、施設の核物質の計量及び管理システムによって発せられる警報、並びに同僚若しくは監督者による監視を含む、1つ又は複数の利用できる情報源による、攻撃の検知から始まる。

評価フェーズ（フェーズ3）

「3.29. 事業者は、物理的防護システムの、性能試験を含む評価及び維持の方法並びに手順を策定し、実施すべきである。」 [1]

4.47. フェーズ3の間に、フェーズ2からの物理的防護システム的设计が、新規のシステムであるか既存のシステムであるかにかかわらず、フェーズ1で同定された要件をそれが満たしているかどうかを決定するために評価される。物理的防護システムを評価する理由としては、次のようなものがある。

- (a) 設計された、又は（既存のシステムについて）特徴付けられた物理的防護システムが、物理的防護の要件を満たすことを検証すること。
- (b) システムの要件を満たすために対処される必要のある設計上又は実施上のシステムの不備を同定すること。
- (c) 同定された不備に対処し、システムの性能を改善するために必要である、可能性のある高度化を分析すること（脅威の変化のために必要となる高度化を含む）。
- (d) 攻撃対象又は施設の変更を考慮するために、年に1回、又はその他の定期的に物理的防護システムの有効性の評価を繰り返すこと。

4.48. 物理的防護システムは、構造的要素、技術的要素及び人的要素によって、検知、遅延及び対応の機能を備える。これらの要素と、機器及び手順との相互関係は、物理的防護システムの有効性の評価を難しい作業にする。

4.49. 評価フェーズで、データが、物理的防護システムの措置の性能について収集され、物理的防護システムの全体的な有効性を評価するために使用される。

事業者による物理的防護の評価及び性能試験

4.50. 参考文献[1]は、物理的防護システムの評価及び試験を強調している；例えば、次のとおりである。

- (a) 事業者は、「性能試験を含む評価及び維持の方法及び手順を策定し、実施すべきである。」（参考文献[1]の параграф 3.29）。
- (b) 区分 I 及び II の核物質について：「物理的防護措置の及び物理的防護システムの、性能試験を含む評価が、警備員及び対抗部隊の適時な対応を含めて、定期的実施されるべきである。」（参考文献[1]の параграф 4.35）。
- (c) 区分 I の核物質について：「少なくとも年に一回、物理的防護システムの性能試験は、適切な演習（例えば武力対抗演習）を含めるべきである。・・・」（参考文献[1]の параграф 4.49）。
- (d) 重大な放射線影響をもたらす可能性のある攻撃対象の妨害破壊行為について；

「物理的防護措置の及び物理的防護システムの、性能試験を含む評価が、警備員及び対抗部隊の適時な対応を含めて、定期的実施されるべきである。・・・物理的防護システムの性能試験は、適切な演習（例えば、武力対抗演習）を含めるべきである。・・・」（参考文献[1]の параграф 5.41）。

4.51. これらは、事業者が規制要件を満たすために設計された方法で、物理的防護システムの評価及び性能試験を計画、実施及び文書化することを推奨している。この評価及び試験の適切な部分は、原子力施設の存続期間の全体に亘って（すなわち、設計、建設、許認可、運転、変更又は高度化、及び廃止措置、並びに放射性廃棄物及び使用済燃料の管理）検討されるべきである。

4.52. 事業者は、区分 I の核物質についての、及び重大な放射線影響を引き起こす可能性のある妨害破壊行為についての、事業者のシステムの評価及び性能試験をレビューするために独立の専門家の利用を検討すべきである。

システム評価の方法

4.53. いくつかの性能ベースの手法が、内部者及び外部敵対者対者に対する物理的防護システムの有効性を評価するために利用できる。性能ベースの評価方法としては、次のようなものがある。

- (a) 経路分析。この評価方法は、敵対者が攻撃対象に到達することを企てる、信憑性のある様々な経路について、図 5 に示すような、タイムラインを組み上げることを含む。タイムラインに基づいて、分析は、敵対者を阻止する対抗部隊のために、敵対者の残りの作業時間が十分である間に攻撃が検知されることの高い確証があるかどうかを決定する。一般に、作業時間と対応時間は定量的に測定又は推定され、検知機能の有効性の程度は性能試験に基づく確率論的推定値である。
- (b) シミュレーション。この評価方法としては、物理的防護システムのコンピュータ・ベースのシミュレーション、並びに敵対者及び施設の対抗部隊による模擬決定に直面しての対応の基礎としてのセキュリティ計画及び危機管理計画の有効性の検討を可能にする机上演習がある。これらの手法は一般に、すべての措置を考慮に入れて、模擬敵対者を検知すること、阻止すること、及び無力化することにおける物理的防護システムの全体的な性能を評価するために使用される。シミュレーションはまた、例えば敵対者を無力化する（すなわち、検知及び阻止の後で、敵対者がその行為を完遂することを防ぐ）対抗部隊の有効性など、特定の側面に焦点を合わせるためにも使用される場合がある。
- (c) 演習。この評価方法は、例えば警報への対応など、物理的防護システムの特定の要素の限られた演習から、模擬敵対者の攻撃に対する全体の物理的防護システムの有効性を示す武力対抗演習へと多岐にわたる。シミュレーションは、対応の重要な実践的な側面を反映することができない場合があり、また、攻撃シナリオの重要な側面を外すことがある。シミュレーションはしたがって、現場の施設の要員及び対抗部隊の関係している演習に十分に取って代わることはできない。

4.54. シミュレーション及び演習は、一般に、想定される様々な攻撃（シナリオ）が同定されるシナリオ分析の一環として実施され、次に各シナリオにおいて物理的防護システムがいかにか有効的に機能するかを判定するために、演習の基礎としてシミュレート又は使用される。シナリオ分析は一般に、敵対者がセンサ、障壁及び通信システムを打破するために、並びに対抗部隊の一部をかわす又は打ち破るために使用する、具体的な方法を検討することによる経路分析に基づいている。一般に、対象分野の専門家がシナリオを策定し、次に、演習及び／又はシミュレーションがシステムの有効性を定量的又は定性的に判定するために使用される。シナリオ分析は、経路分析の間に作成される経路のタイムラインについての情報を使用する場合がある。

4.55. シナリオ分析としては、そのようなシナリオが設計基礎脅威又は脅威評価の範囲に含まれる範囲で、外部敵対者対者との内部者の共謀が必要とされているシナリオの場合がある。外部脅威に対する評価としては、例えば攻撃者の人数、彼らの機器装備（武器及び爆発物を含む）及び、物理的防護措置を打破することを助ける彼らの技能など、敵対者の属性の検討がある。一般に、特別な手法の使用が経路分析に含まれる。

4.56. システムの有効性は、定量的又は定性的のいずれかで評価され得る。国は、様々なタイプの攻撃対象、脅威及びシナリオについて、どちらの手法が使用されるべきかを決定すべきである。全体的な物理的防護システムの有効性の要求されるレベルは、すべての信憑性のある敵対者

の経路及びシナリオが考慮された時に、それでも規制目標を満たすような物理的防護システムの定量的又は定性的な有効性の最低レベルとして保守的に規定されることが推奨される。

4.57. 大まかに 2 種類のシナリオが、2 つの脅威；不法移転及び妨害破壊行為、に対処する。不法移転について、敵対者は攻撃対象の物質の場所へ侵入し、次に、その核物質をオフサイトの場所へ持ち去る必要がある。区分 I の核物質の場合は、有効な対抗戦略は、核物質へのアクセスを拒否することであろう、又は、アクセスが達成される場合は、核物質がサイトを出る前に敵対者を阻止することであろう。妨害破壊行為について、敵対者は攻撃対象の物質及び／又は枢要区域へ侵入し、次に、その物質に直接的に妨害破壊行為を行う、又は、機器に妨害破壊行為を行うことによって間接的に放射性核種の放出を引き起こす必要がある。この場合、対抗戦略は、少なくとも、妨害破壊行為を完遂するために必要となると思われる時間の間、物質又は機器へのアクセスを拒否することであろう。

内部脅威についての追加的な評価検討

4.58. 評価としては、内部脅威への物理的防護システムの脆弱性の分析もあるべきである。そのような評価を実施するための手引きが、参考文献[9] で提供されている。分析するために、内部脅威は、内部者が受動的（例えば、機微情報の収集のみ）であるか、能動的であるかによって、また、内部者が能動的であれば、内部者が攻撃対象又は人に対して武力を行使することをいとわないかどうかによって、区分される。脅威評価又は設計基礎脅威を考慮に入れて、評価としては、他の内部者又は外部の敵対者対者と共謀する内部者の可能性の検討があることがある。

4.59. 内部脅威による一連の行動を含んでいるシナリオは、内部脅威に対する施設の防護の有効性を判定するために使用されることがある。敵対者の経路のタイムラインは、外部脅威と同様の方法で評価できる、連続的な一連の行動を含んでいる内部脅威の攻撃シナリオの評価をすることについてのみ適切である。能動的な内部者についての経路のタイムラインは、外部の敵対者についてのタイムライン（図 5 参照）に類似した連続的な一連の作業、又は作業によっては大きな時間間隔で別々になっている、及び／又は様々な場所で実施される、不連続の一連の作業を示す場合がある。連続的なタイムラインのシナリオの一例は、内部者が連続した一連の行動で核物質の盗取を完遂することを企てるという唐突な盗取である。不連続の内部脅威の攻撃シナリオの一例は、内部者が、数日又は数週間の期間にわたって一連の少量の別々の盗取によってかなりの量の核物質を得ることを企てるという長期にわたる盗取である。

物理的防護システムの主要な機能

4.60. 物理的防護システムは、抑止、並びに検知、遅延及び対応の組み合わせによって、物理的防護要件を満たし、物理的防護の目標を成し遂げる。参考文献[17]は、物理的防護システムのこれらの主要な機能の、追加の、より詳細な手引きを提供している。

抑止

4.61. 抑止は、潜在的な敵対者が、成功の確率は低すぎる（又は、敵対者自身にとっての潜在的なマイナスの影響を高すぎる）と推測することによって、魅力のない攻撃対象であるとして施設

をみなし、攻撃しないと決定する場合に達成される。抑止を促進させるために、事業者は、例えば施設を巡視している警備員の一目瞭然の存在、夜間の明るい照明、窓の鉄格子、及び車両障害物など、目につく防護措置を使用する場合がある。抑止は、攻撃を思いとどまらせることに役立つかもしれないが、抑止の有効性は測ることが、不可能ではないにしても、困難である。さらに、物理的防護の措置及び要員を一目瞭然にしておくことは、敵対者の行動に対するそれらの措置及び要員の脆弱性を増加させる場合がある。

検知

4.62. 検知は、潜在的な悪意ある行為で若しくは無許可の行為で、又は感知されている敵対者の存在で、並びに警報が発せられることで開始する物理的防護システムでの過程である。過程は、警報の原因が評価されたときに完了する。

4.63. 図 6 は、検知に関連する一連の事象を示しており、検知は単独の瞬間的な事象ではないことを示している。潜在的な敵対者による行動は、この連鎖でのすべての措置が生じた場合にのみ、検知されたとみなされる。警報の正確な評価のために必要である情報としては、例えば、誰が（又は、何が）警報のきっかけとなったか、どんな特定の活動がその警報のきっかけとなったか、活動がどこで行われたのか、また、何名の者が含まれているかなど、詳細がある。図 6 の最初の 3 ステップ（センサの作動、警報信号の開始及び警報報知）は、「感知」を構成している；最後の警報評価が検知の過程を完了させる。

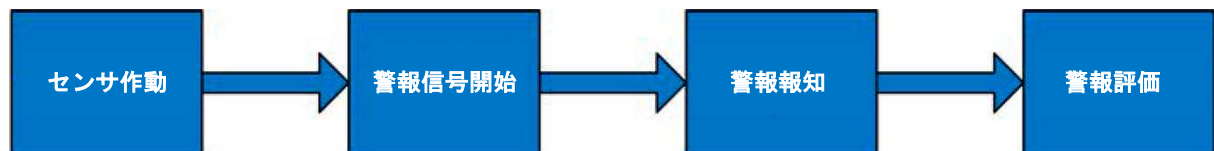


図 6. 物理的防護システムにおける検知機能

4.64. 検知の連鎖は、何らかの種類 of センサが何らかの原因によって作動したときに始まる。センサの作動は、物理的防護システムでのハードウェアセンサ（例えば、放射線モニター又は人感センサ）のきっかけになること、又は例えば警備員などの人による何らかの疑わしいものの報告を意味する。

4.65. 検知機能を遂行することでの物理的防護システムの有効性は、センサ、警報信号の作動、警報報知及び警報評価についてのシステムの性能、並びに、中央警報ステーションの担当者、及び検知での役割を有する警備員又は対抗部隊のメンバーの能力に依存する。技術は、検知の過程のすべての段階の効率を増加し得る。技術が使用される場合、検知システムは、感知と評価にデータを提供するためにセンサ及びビデオシステムを使用すべきである。

4.66. 検知の有効性は、検知確率と、検知の完了に必要な時間の両方の関数である。検知確率は、行動が感知される確率、警報が発せられて報知される確率、及びそのときに警報が正しく評価される確率で構成される。検知時間 ($T_0 \sim T_D$; 図5参照) は、図6での4つの措置が生じるのにかかる時間の総計である。より短い検知時間は、警報の原因が評価されやすくなり、また、必要に応じて、敵対者を阻止するのに間に合うように警備員が配置されやすくなる。

4.67. 検知はまた、例えば、企てられた、人、車両又は禁制品の無許可の入域、又は企てられた、核物質の不法移転の場合、出入管理の措置によってきっかけとされる。

遅延

4.68. 遅延は、攻撃対象への敵対者の前進を遅くし、それによって有効な対応のためのより多くの時間を提供しようとする物理的防護システムの機能である。遅延は、横切られなければならない距離及び面積によって、並びに、例えばフェンス、ゲート、ゲート（ポータル）、ドア、施錠、ケージ及び可動の遅延システムなど、打破されるか迂回されることが必要である障壁によって簡単に成し遂げられ得る。障壁は、もし敵対者が障壁を突き抜けられなければ、敵対者を抑止する又は挫折させる。それぞれのタイプの障壁は、敵対者が付け抜ける又は打破するのに時間がかかる。これらの遅延時間は、物理的防護システムを設計する時に検討される要素である。警備員又は対抗部隊は、もし、適切に、適切な場所に配置され、武装及び防護される場合、さらなる遅延を提供する。

4.69. 物理的防護システムでの遅延要素の有効性の一番の目安は、検知後、遅延を提供している措置を打破するために敵対者が必要とする時間である。検知の前に敵対者が直面する遅延は、そのような遅延が敵対者に、対応するための追加の時間を提供しないので、物理的防護システムの有効性にとって価値がない。(外部障壁は、例えばスタンドオフ攻撃の抑止又は影響の緩和など、その他の目的も果たす場合がある)。遅延は、対抗部隊が日常的にすぐ近くに配置されていなくて、悪意ある行為の完遂を防ぐために十分な遅延が対抗部隊に提供されることが必要である場合に、特に重要な機能である。

対応

4.70. 対応は、悪意ある行為の完遂の前に敵対者を阻止して無力化しようとする物理的防護システムの機能である。警備員は、出入りの管理、人への付添、中央警報ステーションでの警報のモニタリング及び評価、巡視、及び／又は潜在的な敵対者の検知への初動対応についての責任が割り当てられている。これらの警備員は、武装対抗をすることが準備される又は許可される場合もあり、されない場合もある。対抗部隊は、武装し、適切に装備されていて、また、不法移転又は妨害破壊行為を企てている敵対者を阻止し、無力化するために訓練を受けている、施設内の又は施設外の者で構成される。

行方不明又は盗取された核物質の捜し出し及び回収

4.71. 事業者は、国の立法上及び規制上の枠組みに応じて、行方不明又は盗取された核物質を捜し出して回収するための措置を支援して、次のように、参考文献[1] で詳細に述べられている多くの措置を実施すべきである。

「4.57. 事業者は、核物質の行方不明又は盗取が、核物質の計量及び管理システムや物理的防護システムのような手段(例えば定期的な棚卸、点検、出入管理での検査、放射線検知検査など)によって、適時な方法で検知されることを確実にすべきである。」

「4.58. 事業者は、国によって規定された期間内にできるだけ早く、迅速な緊急棚卸の措置によって、行方不明の又は盗取された核物質を確認すべきである。核物質の計量及び管理のためのシステムは、核セキュリティ事案の直後に、施設内の行方不明の可能性のある核物質についての正確な情報を提供すべきである。」

「4.59. 事業者は、国によって規定されているように、行方不明の又は盗取された核物質の所管当局及びその他の関連する国の機関に通報すべきである。」

「4.60. 行方不明の又は盗取された核物質を捜し出して回収するための事業者の措置は、事業者の危機管理計画に含まれるべきであり、定期的に試験されて評価されるべきである。適切な合同演習が所管当局及びその他の国の機関と行われるべきである。」

「4.61. 事業者は、行方不明又は盗取されたと発表された、施設内の及び場合によりオフサイト（緊急追跡において）の核物質を、法制及び規制の枠組み並びに危機管理計画に従って、できる限り速やかに、捜し出すために、適切なあらゆる措置を取るべきである。」

「4.62. 行方不明の又は盗取された核物質が捜し出され同定された後できるだけ速やかに、事業者は、危機管理計画に従って、その場でこの物質を守り、その後、所管当局の相応の許可で適切な原子力施設にそれを戻すべきである。」

「4.63. 事業者は、核物質を捜し出して回収するために、国の機関に対して、その他の必要な支援を提供すべきであり、かつ、その後の捜査及び訴追の間に協力すべきである。」

4.72. 行方不明及び／又は盗取された核物質の捜し出しと回収のための最初の措置は、核物質がそれについて許可された場所がないことを検知することである。例えば、

- (a) 物理的防護システムは、核物質を盗むことを企てている敵対者を検知することができ、もし物理的防護システムがこの行為を防ぐことに成功しない場合は、そのときに、核物質は施設から持ち去られる。
- (b) 核物質の計量及び管理システムは、核物質が行方不明であることを、運転、棚卸又は検査の間に検知する。
- (c) 出入管理地点での検査、又は汚染検査は、核物質が無許可の方法で持ち出されていることを検知する。

(d) 施設の要員は、誰かが核物質を持ち出すことを企てていることを観察して検知する。

4.73. 核物質がそれについて許可された場所がないことが検知された後、事業者は、できる限り早く、行方不明の核物質の量及び種類を確認するための措置を取るべきである。事業者は、核物質がそれについて許可された場所に、もはやないことを確認した後、国内の関係する所管当局に速やかに通知すべきである。危機管理計画に従って、事業者は次に、物質の施設内の捜索を続け、また、必要に応じて、関係所管当局と協調して、施設外での捜索も開始する。場合によっては、これらの捜索は、緊急時計画の発動を必要とする[10、12]。行方不明の又は盗取された物質が以前に置かれていた区域は、可能性のある犯罪現場として厳重に守られ、扱われるべきである。他の核物質の継続的な物理的防護も検証されるべきである。

4.74. すべての対応措置は、危機管理計画に従って実施されるべきであり、また、適切な所管当局と協調されるべきである。核物質が捜し出しされると、事業者又は別の適切な団体は、物質を守り、適切な場所に物質を戻すべきである。物質を守って戻すことは、特に、犯罪捜査が開始されている、又は開始される可能性が高い場合に、法執行機関を含む、すべての関係する所管当局と密接な協議を行って実施される必要がある。

4.75. 回収の業務の協調についての取り決め及び協定が、危機管理計画の中で詳細に設定されるべきであり、必要に応じて、緊急時計画と調整されるべきである。フォローアップレビューが、核物質の紛失の後に実施されること、及び対応から学んだ教訓が危機管理計画の変更の中に取り入れられることが推奨される。

妨害破壊行為の放射線影響の緩和又は最小化

4.76. 妨害破壊行為の事案への対応は、緊急事態が事故によるものか妨害破壊行為によるものかにかかわらず、場合によっては、原子力緊急事態又は放射線緊急事態への対応についての責任がある所管当局を含め、多くの所管当局が関係する。有効であるために、妨害破壊行為の事案への対応は、結果として生じる緊急事態への対応と適切に統合されて、協調されるべきである[10]。

4.77. 事業者は、参考文献[1]に提示しているように、妨害破壊行為の放射線影響を緩和又は最小化するための措置を支援する、次の責任を有する。

「5.54. 事業者は、危機管理計画を策定すべきである。

「5.55. 事業者は、危機管理計画の実施について、警備員、対抗部隊、法執行機関及び安全対応チームと一体となって行動するために施設の要員に用意をさせるべきである。

「5.56. 事業者は、悪意ある行為を検知したら、この行為が放射線影響につながる可能性があるかどうかを評価すべきである。

「5.57. 事業者は、危機管理計画で規定されているように、妨害破壊行為又は妨害破壊行為の企てについて、所管当局、対抗部隊及びその他の関連する国の機関へ、適時に通報すべきである。

「5.58. 妨害破壊行為の直後に、事業者は、更なる損傷を防止するため、原子力施設を守るため、並びに非常用設備及び緊急時要員を防護するための措置を取るべきである。」

4.78. 妨害破壊行為への対応者は、原子力施設内に存在する安全上のハザード（例えば、放射線被ばく）について、及びこれらのハザードが妨害破壊行為によってどのような影響を受けるかについてよく知っている必要がある。対応者は関係するすべての安全措置にも従う必要がある。

4.79. 危機管理計画は、妨害破壊行為への対応に関係するすべての関係当局の役割及び責任を同定し、例えば次のような規定を含める必要がある。

- (a) 施設内の対応は、ただちに開始され、運転上の安全及び物理的防護の機能の継続的な性能を損なうことなく管理される。
- (b) 施設外の対応は、有効に管理され、施設内の対応と協調される。
- (c) 資源の割り当ての決定を行うために必要な情報は、事案の全体に亘って評価される。

4.80. 事業者は、事業者の危機管理計画に、攻撃対象及び施設のその他の部分への追加的なダメージを防ぐこと、原子力施設を守ること、並びに緊急時用の機器及び要員を防護することに焦点を合わせた措置を含めるべきである。

4.81. 危機管理計画は、妨害破壊行為攻撃の影響の制限に役立つために策定され、展開されるべきである。妨害破壊行為への対応及び結果として生じる緊急事態への対応は、同じ場所で同時であっても、異なった目標の活動を含むことがある。したがって、危機管理計画及び緊急事態計画について、相補的であり、それらの有効性と両立性を確実にすることを促進するために定期的に合同演習が行われる必要がある。対抗部隊の活動が安全に悪影響を及ぼさないこと、及び物理的防護が安全上の措置の実施の間に悪影響を及ぼさないことを検証するために、注意が払われる必要がある。危機管理計画の一例が付録 II に含まれている。

4.82. 原子力施設での緊急事態への施設内の対応及び施設外の対応の両方を調整し管理するために設置された緊急事態対応施設も、その起因事象にかかわらず[10]、物理的防護の対応機能の指揮及び統制の要素のために使用される場合がある。

物理的防護措置

4.83. 原子力施設で実施される物理的防護システムは、セキュリティ計画に従うべきであり、セキュリティ計画の中で詳細に述べられるべきである。この計画は、物理的防護システムの設計にある物理的防護措置のすべての側面を含む。物理的防護措置の実施に関するより詳細な情報は参考文献[17]にある。

4.84. 物理的防護措置は、パラグラフ 4.60～4.70 で述べたように、それらが遂行する機能によって分類される。表 3 は、物理的防護措置の各タイプについての参考文献[1]のセクション 4 及び 5 の勧告を、不法移転についての核物質の区分、及び妨害破壊行為の潜在的影響レベルに関連付けている。この表はまた、各防護層について、評価及び性能試験の要件も記載している。

4.85. 参考文献[1]での物理的防護措置についての勧告は、等級別手法を用いて体系化されている。区分 II の核物質について勧告された措置は、区分 III についての措置も含んでおり、また、区分 I の核物質についての措置は区分 II 及び区分 III についての措置も含んでいる。

防護の区域及び層

4.86. 図 7 は、参考文献[1]のパラグラフ 4.14、4.22～4.28、4.37～4.40、4.42～4.46 及び 5.20～5.35 での勧告に基づいて、多層防護（defence in depth）が提供される必要のある核物質及び妨害破壊行為の攻撃対象に応じて、原子力施設で見られる場合のある様々なタイプの区域の概念図を提示している。これらの防護の区域は、それぞれが有しているそれ自身の防護の層によって物理的に分離されている。最も内部の区域で始まり、各区域の防護層についての要件が、区域の場所、アクセス、検知、遅延及び対応の勧告という観点で以下に述べる。

立入制限区域

4.87. 立入制限区域は、そこへの立ち入りが物理的防護の目的のために制限及び管理される、原子力施設及び核物質を包含している指定された区域である。この区域に収容される区分 III の核物質は、表 3 に記載された措置の実施によって防護されるべきである（国の方針によって、原子力施設の境界の外の土地も管理される区域である場合がある）。

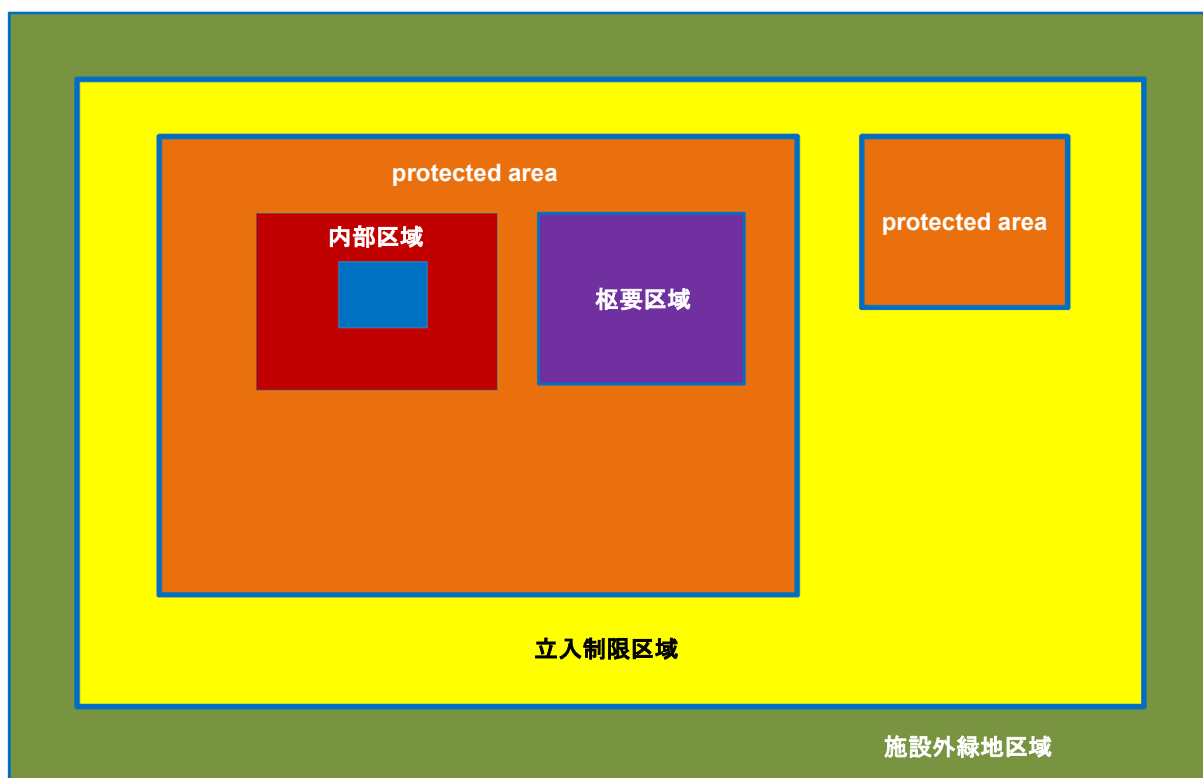
Protected area

4.88. 区分 II の核物質は **Protected area** 内で守られるべきである。等級別防護の一環として、国は、**Protected area** 内の、受容できない放射線影響から重大な放射線影響に及ぶ潜在的な影響を有する、妨害破壊行為の攻撃対象を守ることを検討する場合がある。すべての **Protected area** は立入制限区域内にあるべきであり、表 3 に記載された措置の実施によって防護されるべきである。物理的障壁が、**Protected area** の境界で特に推奨される。

表3. 施設の物理的防護措置：参考文献[1]のパラグラフとの相互参照

使用中及び貯蔵中の核物質の重大な影響を有する施設の不法移転（物質区分別）		妨害破壊行為			
	区分 III (立入制限区域)	区分 II (Protected area)	区分 I (内部区域)	Protected area	枢要区域
物理的防護措置					
検知	4. 14、4. 15、 4. 16	4. 14、4. 15、 4. 16、4. 23、 4. 30、4. 31	4. 14、4. 15、 4. 16、4. 23、 4. 30、4. 31、 4. 38、4. 40、 4. 46、4. 47、 4. 48	5. 14、5. 21、 5. 22、5. 36、 5. 37	5. 14、5. 26、 5. 29、5. 33、 5. 36、5. 37
警報評価	N/A ^a	4. 23、4. 30、 4. 31	4. 23、4. 30、 4. 31、4. 47	5. 21、5. 36	5. 36
立入制限	4. 14、4. 17	4. 12、4. 17、 4. 24、4. 25、 4. 26、4. 27、 4. 28、4. 30	4. 12、4. 17、 4. 24、4. 25、 4. 26、4. 27、 4. 28、4. 30、 4. 38、4. 40、 4. 42、4. 44、 4. 45	5. 14、5. 22、 5. 23、5. 24、 5. 25、5. 36	5. 14、5. 26、 5. 28、5. 31、 5. 32、5. 34、 5. 35、5. 36
禁制品の検知	N/A ^a	4. 25	4. 25、4. 43	5. 14、5. 23	5. 14
中央警報 ステーション	N/A ^a	4. 30、4. 31、 4. 32、4. 33	4. 30、4. 31、 4. 32、4. 33、 4. 47	5. 36、5. 37、 5. 38	5. 36、5. 37、 5. 38
遅延	N/A ^a	4. 23	4. 23、4. 38、 4. 39、4. 41、 4. 46	5. 14、5. 21	5. 14、5. 26、 5. 27、5. 30
対応	4. 15、4. 19、 4. 20	4. 15、4. 19、 4. 20、4. 30、 4. 32、4. 33、 4. 34	4. 15、4. 19、 4. 20、4. 30、 4. 32、4. 33、 4. 34、4. 49	5. 14、5. 21、 5. 36、5. 38、 5. 39、5. 40、 5. 42	5. 14、5. 36、 5. 38、5. 39、 5. 40、5. 42
評価					
性能試験	4. 20	4. 20、4. 35	4. 20、4. 35、 4. 49	5. 15、5. 16、 5. 41	5. 15、5. 16、 5. 34、5. 41

^a N/A：該当なし



- 原子力施設のその他すべての区域であり、その一部は区分Ⅲの核物質を収容していることがある。外側の青線は原子力施設の外周を表す。
- 区分Ⅰの核物質を収容する。区分Ⅰの核物質はこの内部区域内の強化された部屋又は強化されたエンクロージャー内に保管される。
- 強化された部屋又はエンクロージャー
- 区分Ⅱの核物質、URC と HRC の間の影響を有する攻撃対象及び／又は枢要区域を包含する。外側の青線は protected area の外周を表す。
- その妨害破壊行為が HRC につながるかもしれない攻撃対象を収容する。

図 7. 原子力施設の配置

(URC : 受容できない放射線影響、HRC : 重大な放射線影響)

内部区域及び枢要区域

4.89. 内部区域は、区分Ⅰの核物質を収容している区域であり、また、枢要区域は、妨害破壊行為が重大な放射線影響につながり得る、機器及び／又は放射性物質を収容している区域である。内部区域は、不法移転と妨害破壊行為の両方についての措置が実施されるべき場合に、枢要区域でもある。内部区域内で、区分Ⅰの核物質は、強化された部屋又は強化されたエンクロージャーの中で保管されるべきである。すべての内部区域及び枢要区域は **Protected area** 内にあるべきであり、表 3 に記載された措置の実施によって防護されるべきである。

中央警報ステーション

4.90. 中央警報ステーションは、区分Ⅰ及びⅡの核物質を保持する、及び／又は重大な放射線影響のしきい値を超える潜在的影響のある妨害破壊行為の攻撃対象を有する原子力施設について推奨される。

4.91. 以下の勧告は、区分 I 及び II の核物質の防護に関係している。

「4.30. 常時に要員が配置されている中央警報ステーションが、警報のモニタリング及び評価、対応の発動、並びに警備員、対抗部隊及び施設管理者との通信連絡のために備えられるべきである。中央警報ステーションで取得された情報は、厳重な方法で保管されるべきである。中央警報ステーションは、一般的に **Protected area** の中に設置されるべきであり、脅威に臨んでその機能が継続できるよう防護（例えば、堅固化）されるべきである。中央警報ステーションへのアクセスは、厳格に最小限に抑えられ、管理されるべきである。」 [1]

4.92. 重大な放射線影響のしきい値を超える潜在的影響を有する妨害破壊行為の攻撃対象について、参考文献[1]の paragraph 4.30 及び 4.47 の勧告を基本的に組み合わせた勧告が同文書にある：

「5.36. 常時に要員が配置されている中央警報ステーションが、警報のモニタリング及び評価、対応の発動、並びに警備員、対抗部隊及び施設管理者との通信連絡のために備えられるべきである。中央警報ステーションで取得された情報は、厳重な方法で保管されるべきである。中央警報ステーションは、一般的には **Protected area** の中に設置されるべきであり、脅威に臨んでその機能が継続できるよう、防護（例えば、堅固化）されるべきである。中央警報ステーションへのアクセスは、厳格に最小限に抑えられ、管理されるべきである。警報のモニタリング及び評価、対応の発動及び通信連絡に関する中央警報ステーションの機能が緊急事態の間に継続できることを確実にするために、冗長性の措置を含む、対策がなされるべきである(例えば、バックアップ警報ステーション)。」

4.93. 警報の通信及び表示システムは、中央警報ステーションの主たる構成要素である。このシステムは、中央警報ステーションにおける警報のモニタリング及び評価を円滑にする。最小限として、システムの機能は次のとおりである：

- (a) センサ及びカメラからの警報及びビデオ信号を中央警報ステーションに送信する；
- (b) 決定及び措置の基礎として使用されるために、この情報を中央警報ステーションの要員に表示しする；
- (c) 警報を評価するために、中央警報ステーションの要員を支援する。

4.94. 良好事例は、警報のための通信経路を、それらが冗長で（すなわち、2 つ以上の別々の通信システム）かつ多様性のある（例えば、別々のシステムが異なる物理的経路を使用する）ように設計することである。冗長性は、より信頼性のある通信システムに役立ち（もし1つの通信経路が機能することを止めても、他の経路がその機能を引き継ぐことができる）、また、敵対者が、1 つでなく少なくとも 2 つの通信経路を打破するか、又は無効化するか侵害する必要があるため、より確実である。

4.95. 参考文献[1]からの以下の勧告は、区分 I 及び II の核物質の防護に関係している。

「4.31. 警報機器、警報の通信経路及び中央警報ステーションは、無停電電源が備えられ、無許可の通信傍受、操作及び改竄に対して防護されるべきである。

「4.32. 中央警報ステーションと対抗部隊との間の双方向の音声通信用に、専用の、冗長性があり、秘話の、多様性のある通信システムが検知、評価及び対応に必要とする活動のために備えられるべきである。専用の、盗秘話の、双方向の音声通信が警備員と中央警報ステーションとの間に備えられるべきである。」

重大な放射線影響のしきい値を超える潜在的影響を有する妨害破壊行為の攻撃対象について、参考文献[1]の параграф 5.37 及び 5.38 に同様な 2 つの勧告がある。

4.96. 物理的防護措置は、核セキュリティの事案の間に、(設備へのアクセスを拒否し、情報へのアクセスを拒否及び検知する) 警報の通信・表示システムの健全性を維持するために設計され、運転され得る。中継器箱や機器のキャビネットの中の改ざん兆候検知センサは物理的防護への追加的な貢献をする場合がある。

4.97. 中央警報ステーションの要員は、警報を評価して、核セキュリティ事案への適切な対応を開始する責任がある。この極めて重要な機能のため、中央警報ステーションは、一般的に、**Protected area** 内にあるべきである。中央警報ステーションは、検知機能と対応機能との間のインターフェイスであるため、中央警報ステーションの要員は、危機管理計画の十分な知識及び理解を有しているべきであるので、理想的には警備員及び/又は対抗部隊のメンバーであるべきである。中央警報ステーションの機能は、通常の利用中に定期的に演習され、より稀な運用条件について試験されることが推奨される。

4.98. 重大な放射線影響のしきい値を超える潜在的影響を有する、区分 I の核物質に関する追加的な勧告が参考文献[1]の параграф 4.47 に含まれている：

「警報のモニタリング及び評価、対応の発動及び通信連絡に関する中央警報ステーションの機能が緊急事態の間に継続できることを確実にするために、冗長性の措置を含む、対策がされるべきである(例えば、バックアップ警報ステーション)。」

重大な放射線影響のしきい値を超える潜在的影響を有する、妨害破壊行為の攻撃対象についての同様の規定が、参考文献[1]の параграф 5.36 にある。

4.99. 中央警報ステーションの最も重要な機能は、危険にさらされている、侵害されている又は安全上の理由で退避させられているときに、維持されるべきである。バックアップ警報ステーションはそのような状況において、最も重要な中央警報ステーションの機能についての運用の継続を提供する。バックアップ・ステーションは、中央警報ステーションの最も重要な機能の継続的な運用を可能にする場所に、中央警報ステーションから離れて位置する必要がある。中央警報ステーションだけでなく、バックアップ警報ステーションも有する物理的防護システムは次のような利点がある。

- (a) 2つのステーションの間の設備の冗長性は、ハードウェアのより大きな信頼性を提供する。
- (b) 中央警報ステーションを、バックアップ・ステーションからの監督監視のある、基本のシステムとして使用され得る。
- (c) バックアップ・ステーションは、中央警報ステーションでハードウェア又は要員の不具合の場合には、又は中央警報ステーションへの攻撃の場合には、物理的防護の機能を引き継ぐことができる。

物理的障壁

4.100. 物理的障壁は、敵対者が、それを打破する又は迂回する必要性によって遅延させられ、それによって悪意ある行為の完遂の前に、対抗部隊に敵対者を阻止する十分な時間を与えるように、設置されるべきである。調和のとれた設計としては、敵対者の様々な経路及びシナリオについての調和のとれた遅延があり、また、物理的障壁は、特定の場所に適切であるように慎重に計画され、敵対者の経路の適切な場所に配置される。遅延の程度は、使用される障壁の種類に依存する。脅威評価又は設計基礎脅威と整合性のある、可能性のあるすべての敵対者の経路に沿った様々なタイプの物理的障壁の複数の層が、(時間の増加に加えて、) 様々な工具及び技能の使用を必要としていることによって、敵対者の前進を難しくし、したがって遅延させる方法として推奨される。警報の評価の助けとなるため、及び予測可能な場所で敵対者を阻止する機会を提供するために、攻撃が感知された直後に敵対者が障壁に直面するように、物理的障壁と検知システムを互いに隣接して設置するための検討がなされるべきである。この措置は、検知の地点において敵対者を遅延させ、攻撃の検知の確率を増加させる。物理的障壁への攻撃又は細工を検知するために、侵入検知システムでカバーされていない障壁は、ランダムに巡視される、又は別の形態の監視の対象となることが推奨される。

4.101. 車両が、多くのタイプのフェンス又は閉じたゲートを突破するために運転され得る。車両障壁が、枢要区域及び内部区域から適切な距離に、設置されることが、参考文献[1]で勧告されている。守られた区域が突破される確率を最小化するために、車両障壁は、設計され、陸上及び水上の適切な場所に設置され得る。車両ゲート及びその進入路の向きは、それに対して走らされている車両によってゲートが突破される確率を低減するために設計され得る。ゲートのそれぞれの側に一連の急カーブのある進入路は、ゲートに近づく車両の速度を低下させ、それによって、車両障壁の有効性を増加させている。すべての場合に、車両障壁は、設計基礎脅威又は脅威評価に記載された車両を止めることができるように設計され、使用されるべきである。車両障壁の細工を検知するために、車両障壁が監視の適切な形態を持つことは良好事例である。

出入管理システム

4.102. 出入管理システムは、立入許可を照合するため、並びに各区域を出入りする人及び物質の動きを管理するために使用される、設備、人、及び手順を含む。出入管理システムは、立ち入りが許可される者、それらの者が立ち入ることが許可される時、及び、立ち入りできる場所を管理するため、並びに許可された立ち入りについての条件を適用するために使用される。出入管理

に関連する情報は機微情報であり、したがって、出入管理システムは適切に保護される必要がある。

4.103. 出入管理システムは、通常経路にを通過しての、許可された者、物質及び機器の円滑で頻繁な出入、並びに無許可の者及び禁制品の移動を検知すること及び遅延させることを支援するために設計され得る。出入管理システムの目標は、許可された者及び車両のみに出入りを許すこと；区域に入る若しくは区域から出ていく物質、情報又は機器の不法な移動を検知及び防止すること；評価及び対応を円滑にするために警備部隊に情報を提供すること；並びに核セキュリティ事案の間及び緊急事態の間について人々の行動が把握されていることを判定することである。

4.104. 出入管理システムは、各地点で出入りする必要がある者の数及び、出入りの時を考慮して、原子力施設の様々な区域への立ち入りを管理するために設置される必要がある。物理的防護システムは防護の層を有しているため、立入制限区域から **Protected area** へ、内部区域及び／又は枢要区域への経路上に、様々なタイプの、次第に厳格になる検知手段を備える。立ち入りを許可される者の数は、一連の各立入地点でより少なくなり、また、この限られたアクセスは、出入管理の設備及び手順の選択に影響を与えることがある。

警備員及び対抗部隊

4.105. 対応をすることについての事業者の責任は、通常は、武力の合法的使用及び被疑者を逮捕する権限に関する国の法令の違いから、国によって異なる。国によっては、立法上及び規制上の枠組みに整合して、事業者は、対抗部隊を備える主たる責任を有さず、これらの能力を備えることを国に依存する。また他の国によっては、事業者は、自社の担当者及び／又は請負業者の一員として警備員と対抗部隊の両方を備える。そのような場合、事業者は、直接雇用か又は契約雇用かにかかわらず、自社によって雇用された警備員及び施設内の対抗部隊が、事業者の管理者によって指示されるように、また、セキュリティ計画に提示されたように、それぞれの責務を履行することを確実にすることについての全責任を保持する。

4.106. 事業者が自社の警備員及び対抗部隊を有している場合でも、特に、重大な核セキュリティ事案の場合に、地方又は国の法執行機関に属する施設外の対抗部隊も対応する。そのような場合、取り決めが、事業者と対抗部隊を備えている外部の組織との間での文書化される必要がある；これらの取り決めは、体系的、協調的及び有効な対応を提供するために、すべての団体による対応についてのための活動の目標、方針及び概念を提示する。これらの文書化された取り決めは、事業者の危機管理計画が外部の対抗部隊の危機管理計画と十分に整合しており、調整されていることを確実にすることを促進する。核セキュリティ事案の間の警備員と対抗部隊の間の協調は、定期的に演習されるべきである。この協調は、区分 I 及び II の核物質、並びに妨害破壊行為が重大な放射線影響につながり得る原子力施設の場合、事業者と対抗部隊との間の全面的な協力で実施されるべきである。

4.107. 誰が対抗部隊を備える場合であっても、対抗部隊は、脅威評価又は設計基礎脅威に記載された方策及び能力を有している敵対者を阻止して無力化することができる必要がある。阻止

は、潜在的な敵対者が検知されたことの対抗部隊への連絡で開始し、訓練を受け装備を整えた十分な人数の対抗部隊のメンバーが、悪意ある行為を完遂する敵対者を止めるのに間に合うように、適切な場所に到着する時に完了する。無力化は、阻止の直後に、敵対者の目標が成し遂げられる前に敵対者を掌握する、又は敵対者に企てを断念させる行為である。有効な無力化を達成することが信頼できるために、対抗部隊は、人数、装備及び／又は訓練という観点で、敵対者よりも優れている必要がある。

4.108. 対抗部隊への有効な連絡は、敵対者の行動と特性に関する情報（観察された人数、並びに工具、機器、武器、及び車両についての利用できる情報を含む）、及び対抗部隊の配備についての指示に関する情報を提供する。対抗部隊との連絡の有効性は、正確な連絡の確率、及び対抗部隊と正確に連絡をするために必要な時間によって測られ得る。

4.109. 物理的防護システムとしては、対応活動の協調を支援するための通信計画がある場合がある。対抗部隊によって使用される通信システムは、脅迫状態信号をこっそり送るための性能を対抗者のために備えることが推奨される。通信システムは、設計基礎脅威又は脅威評価に記載されているような脅威への有効な対応のために、通信が信頼できるように適切なままであることを確実にするために、十分な冗長性と多様性を有すべきである。

4.110. 有効な対応のために厳格な訓練プログラムが最も重要である。すべての警備員、中央警報ステーションの担当者及び対抗部隊は、その職位と責任に適切で、頻繁に実施される訓練に参加する必要がある。

4.111. 核セキュリティ事案に対処するための警備員及び対抗部隊の両方についての参考文献[1]からの勧告は次のとおりである。

「3.60. 核セキュリティ事案時の、警備員と対抗部隊の間の協調が、定期的に演習されるべきである。さらに、その他の施設の要員は、計画の実施のために、警備員、対抗部隊、及びその他の対応チームと一体となって、行動するために訓練を受け、準備が出来ているべきである。」

4.112. 区分 I、II 及び III の核物質の不法移転に対する対応のための能力に関する参考文献[1]からの具体的な勧告は次のとおりである。

「4.15. 対策が、核セキュリティ事案に対処するために、無許可の侵入を検知するため並びに十分な警備員及び／又は対抗部隊による適切な活動のために、なされるべきである。

.....

「4.20. 国は、対抗部隊が、サイト及び核物質の在る場所に精通していること、並びに対応活動の安全への潜在的な影響を考慮しながら、必要な対応活動を行う十分な準備ができ

ることを確実にするために、放射線防護に関する十分な知識を有していることを確実にすべきである。」

4.113. 区分 I 及び II の核物質の不法移転に対抗するための参考文献[1]の勧告としては、次のものがある。

「4.33. 24 時間体制の警備業務及び対抗部隊が、不法移転の企てに対して有効に対抗するために備えられるべきである。・・・警備員及び対抗部隊は、国の法律と規則に従って、彼らの職務について訓練を受け、十分に装備されるべきである。

「4.34. 警備員は、**Protected area** のランダムな巡視を実施すべきである。巡視の主要な機能は、次のとおりであるべきである。

- 敵対者対者を抑止すること；
- 侵入を検知すること；
- 物理的防護の構成要素を目視で検査すること；
- 現在の物理的防護措置を補完すること；
- 初期の対応をすること。」

参考文献[1]の Paragraph 4.34 からの勧告も、妨害破壊行為に対して防護するために、**Protected area** 内の警備員の機能に関して適用する（参考文献[1]の Paragraph 5.40 参照）。

4.114. 巡視を、施設を観察している敵対者が予測できないように、ランダムな時間に、各当直の間に数回、境界全体をカバーして行うことは良好事例である。この間、巡視はまた、フェンスの健全性、照明が機能していること、並びにすべてのゲート及びドアが適切に守られていることをチェックする場合もある。その他の良好事例は、**Protected area** の境界のセンサの動作を試験するために警備員を使用すること、他の場所の検知システムの機能を検証すること、及び、必要な時に、例えば故障したセンサが修理又は交換されるまで、補う措置をすることである。

4.115. Paragraph 3.27~3.32 及び 4.50~4.52 は、それぞれ国及び事業者について、区分 I 及び II の核物質の不法移転及び妨害破壊行為に対する対抗部隊の評価及び性能試験に関する勧告を示している。

4.116. 警備員及び対抗部隊の訓練としては、危機管理計画の演習、性能試験、机上演習、モデル化及びシミュレーション、対抗部隊の演習及び／又は武力対抗演習がある場合がある。

スタンドオフの妨害破壊行為攻撃に対する防護措置

4.117. 事業者は、設計基礎脅威に含まれているスタンドオフ攻撃のタイプに対して防護する責任を有する（Paragraph 3.55~3.63 参照）。

4.118. スタンドオフ攻撃に対する防護を備えることでの事業者の最初のステップは、スタンドオフ攻撃に対する攻撃対象の区域並びにそれらの区域内の物質、設備及び系統の潜在的な脆弱性を同定することである。この過程としては、脅威評価又は設計基礎脅威に明示された特性に基づ

いた妨害破壊行為シナリオの策定、並びにそれらのシナリオにおける攻撃対象への影響及び物理的防護システムの評価がある。安全の担当要員と物理的防護の担当要員との緊密な協力関係が必要である。

4.119. 事業者は、スタンドオフ攻撃に対する防護措置を設計すること、及び、それらが所管当局によって承認されたときには、それらの措置を実施することについての責任がある。スタンドオフ攻撃に対して防護する、又はスタンドオフ攻撃の影響を緩和する防護措置としては、次のものがある。

- (a) 敵対者が使用する武器の射程距離を超えるように、スタンドオフ攻撃が企てられ得る施設からの距離を増加させること。
- (b) そこからスタンドオフ攻撃が企てられる区域から攻撃対象への照準線を見えなくすること。
- (c) 施設外の巡視及び監視によって、検知及び抑止を増加させること。
- (d) 飛来物を途中で止める、又は爆風若しくは破片を吸収する能力のある障壁を使用すること。
- (e) 機微な攻撃対象を防護するために施設の配置を変更すること。
- (f) そのような攻撃に耐えるために施設を堅牢にする

空から及び水上からの攻撃についての防護措置

4.120. 脅威評価又は設計基礎脅威は、盗取又は妨害破壊行為シナリオにおいて、輸送に航空機及び／又は水上船舶を使用する敵対者を含む場合がある（空中のスタンドオフ妨害破壊行為攻撃と混同されないこと）。これらの場合、敵対者は、航空機又は船舶でサイトに到着する、及び／又はサイトから退去する。事業者は一般に、このような攻撃モードに対して防護する何らかの責任を有する。

4.121. レーダー、音響及び振動センサはすべて、空からの攻撃に対して何らかの検知能力を備え得るが、迷惑警報のほとんどない良好な受信可能範囲を提供するために慎重に設置される必要がある。一部のタイプの航空機は、施設の小面積及び／又は密集地域のために、原子力施設の敷地での着陸が妨げられる。この効果は、ポール又はその他の物理的障壁の戦略的な配置によって強化される。

4.122. 設計基礎脅威及び国の要件に基づいて、事業者は、そのような攻撃を検知するための設備及び装置を設置し、運転する場合がある。

核物質の輸送

4.123. 原子力施設の事業者は、荷送人又は荷受人として、施設に輸送される、又は施設から輸送される核物質の物理的防護について一定の責任を有する。これらの責任は、計画された発送の事前通知をすること、輸送手段を検査すること、輸送情報の機密性を保護すること、到着次第に荷物の健全性をチェックすること及びその到着を荷送人に通知すること、並びに物理的防護の責任の移管に関して運搬人と事前の取り決めを行うことを含む場合がある。さらに、事業者は、原

子力施設における2つの Protected area 間の区分 I 及び II の核物質の施設内の移動が、施設の外側のそのような核物質の輸送に関する国の要件に従って防護されることを確実にすべきである。輸送中の核物質のセキュリティに関する追加的な手引きは、参考文献[2] で提供されている。

核セキュリティのための核物質の計量及び管理⁴

4.124. 参考文献[1]は、次のように、核セキュリティに関係する核物質の計量及び管理に関するいくつかの勧告を提供している。

「3.26. 事業者は、常に、原子力施設のすべての核物質の管理を確実にし、軽量することが出来るべきである。事業者は、所管当局によって規定されたように、確認された計量上の不一致を適時な方法で報告すべきである。」

.....

「3.36. 脅威を検討する場合、相応の注意が内部者に払われるべきである。内部者は、専用の物理的防護の要素又は例えば安全上の手順など、その他の対策を回避するために、自身の権限及び知識によって補完された、アクセス権を悪用し得る。物理的防護システムは、内部者による核物質の長期にわたる盗取を抑止及び検知するために、核物質の計量及び管理の措置によって支援されるべきである。」

.....

「3.47. 多層防護 (defence in depth) は、内部者及び外部脅威に対して防護するために、物理的防護システム並びに核物質の計量及び管理システムの性能を考慮に入れるべきである。」

.....

「4.57. 事業者は、核物質の行方不明又は盗取が、核物質の計量及び管理システムや物理的防護システムのような手段(例えば定期的な棚卸、点検、出入管理での検査、放射線検知検査など)によって、適時な方法で検知されることを確実にすべきである。」

「4.58. 事業者は、国によって規定された期間内にできるだけ早く、迅速な緊急棚卸の措置によって、行方不明の又は盗取された核物質を確認すべきである。核物質の計量及び管理のためのシステムは、核セキュリティ事案の直後に、施設内の行方不明の可能性のある核物質についての正確な情報を提供すべきである。」

⁴ 参考文献[1]は、「核物質の計量及び管理 (nuclear material accountancy and control)」という用語を使用し、参考文献[17]は「核物質の計量及び管理 (nuclear material accounting and control)」という用語を使用している。参考文献[1]から直接引用している場合を除き、本文書においては後者の用語が使用されているが、これら 2 つの用語は互いに置き換え可能であるとみなされる。

4.125. 核物質の計量及び管理システムは、施設にあるすべての核物質の量、種類、場所、使用、移動及び転換に関する情報を維持するために設計される。核物質の計量機能は、すべての核物質の在庫量及びその場所を維持することによって、核物質の不法移転に対する抑止及び不法移転の検知を備えている。核物質の管理機能は、内部者による悪意ある行為を検知する場合がある、封じ込め及び監視の手段を備えている。どちらかの又は両方の機能は、もし、それらの機能が、核物質が無許可で持ち去られた、又は無許可の方法で使用されたことを検知した場合に、対応を始めるための根拠を提供する。有効な核物質の計量及び管理システムは、内部者の活動を検知するための、及び内部者又は外部敵対者対者によって始められたかにかかわらず、核物質に関係する不規則な事を正確に評価するための事業者の能力を強化させる。もし核物質が施設から持ち去られた場合、核物質の計量及び管理システムは、持ち去られた核物質の量と特性を同定することができるべきである。

4.126. 物理的防護に関する核物質の計量及び管理システムの目的は次のとおりである。

- (a) 核物質への無許可のアクセス又はその持ち去りを検知し、評価する。
- (b) 核物質の場所、特性及び量についての情報を提供する。

4.127. これらの目的を実現することは、事業者に以下のことを可能とする。

- (a) 核物質の不法移転があったことを関係している所管当局に連絡する。
- (b) 許可された場所でない、物質の捜し出しを支援するために、正確で適時の情報を提供する。
- (c) 物理的防護及び核物質管理の措置と協調して、核物質の区分に応じた適切な防護と管理が核物質に適用されるという保証を備える。

4.128. 核物質の監視とモニタリングが、核物質の移動を検知するため、並びに核物質の計量及び管理の設備と核物質の状態についての連続的な情報を提供するために、事業者によって使用される場合がある。核物質の監視とモニタリングとしては、運転要員による目視監視、及び物理的防護要員による目視及び遠隔モニタリング、並びに、例えば重量センサ、熱センサ、レーザーモニター、放射線モニター、無線タグ（RFタグ）及び人感センサなどのその他の技術的手法がある場合がある。

4.129. 有効である目視による監視について、観察を行う者は、無許可の活動を認識すること、状況を正しく評価すること、及び不法移転を防ぐのに間に合うように適切な対応要員にその活動を報告することのできる必要がある。もし、2人ルールが、そのような監視に適用される場合、2人の許可された者は、ともに適切な訓練を受けていること、並びに遮られることなく物質及びお互いが見え、無許可又は不正な手順を検知できる必要がある。

4.130. 物質の封じ込め手法及び改ざん兆候センサが、核物質に関する情報の連続性の確保を支援するため、及び無許可のアクセスを表示するために使用され得る。様々なレベルの封じ込め手法—例えば缶、グローブボックス、貯蔵キャビネット及び保管室など—の使用は、有効な改ざん

兆候センサや監視と併せて、核物質が行方不明かどうか、また、もしそうであればどの物質か、また、緊急棚卸又は臨時棚卸が必要かどうかを決定するために必要とされる時間を短縮するであろう。

4.131. 核物質の計量、核物質の管理及び物理的防護という別々の機能についての責任を別々の個人又はグループに割り当てることは良好事例であるとみなされる。

4.132. すべての場合において、適時の検知が重要である。事業者は、様々な検知手段についての累積時間が所管当局によって定められた要求事項を満たしているかどうかを判定するために、さまざまな場合の累積時間を見積もって、核物質が行方不明、盗取又は不法な手順で持ち去られたことを検知することのあらゆる可能な手段をレビューすることが推奨される。このトピックに関する追加的な手引きは参考文献[18]で見られる。

機微情報のセキュリティ

4.133. 核物質又は原子力施設に関係している悪意ある行為を計画又は実施したいと思っている敵対者は、機微情報へのアクセスから便益を得るかもしれない。そのような情報は、それ故に、適切な方法で同定され、分類され、及び守られるべきである。

4.134. 機微情報は、いかなる形態（ソフトウェアを含む）であれ、その無許可の開示、修正、変更、破壊又は使用拒否が核セキュリティを侵害し得る情報である。

4.135. 参考文献[16]の Paragraph 1.2 は、次のように述べている。「機密性は、情報が無許可の者、団体又は作業に利用できないようにする、又は開示されないようにする属性である。」機微情報の機密性を保護することと同様、情報セキュリティは、情報の正確さ及び完全性（その健全性）、並びに、必要な時の情報の入手可能性又は有用性（その可用性）を守る。

4.136. 情報セキュリティは、核セキュリティについての分野横断的な要件であり、国の核セキュリティ体制の重要な要素である。国は、所管当局によって、国のセキュリティの所管当局からの手引き及び方針を考慮して、事業者及びその他の関連組織についての情報セキュリティの要件を設定する。

4.137. 事業者は、国のセキュリティ方針並びに関連国内法及び要件に従って、事業者が保有する又は扱う機微情報の機密性、健全性及び可用性を保護することについての内部方針及び手順を策定する必要がある。これらの手順は、セキュリティ計画に取り入れられる必要がある。事業者はまた、施設内又は施設外にかかわらず、事業者の請負業者が、事業者から伝えられた情報の秘密度を意識させられること、及びそのような情報を適切に保護するための手順に関して説明を受けることを確実にすることも必要である。事業者は、請負業者がこれらの手順に従うことを確実にするためのチェックを実施すること、及び機微情報が契約の終結時に事業者に戻されることを確実にすることについての責任がある場合がある。

4.138. 情報セキュリティプログラムの頻繁なレビュー及び定期的な監査は、プログラムが意図されたように機能しているかどうかを判断すること、及び同定された不具合を強化又は是正することの役に立つ場合がある。調査及び是正措置を可能にするために、情報セキュリティの侵害は、国の要件に従って適切な所管当局に報告されるべきである。

4.139. 機微情報を同定する上で、国及び事業者を支援するための分類例の手引きを含む、情報セキュリティに関する追加的な手引きは、参考文献[16]で見られる。

コンピュータ・ベースのシステムの防護

「物理的防護、原子力安全並びに核物質の計量及び管理のために使用されるコンピュータ・ベースのシステムは、脅威評価又は設計基礎脅威と整合性のある侵害(例えば、サイバー攻撃、不正操作又は改竄)に対して防護されるべきである。」(参考文献[1]のパラグラフ 4.10 及び 5.19)

4.140. 国は、コンピュータ・セキュリティに関する要求事項を規定すること、並びに事業者がコンピュータ及びコンピュータ・ベースのシステムがサイバー攻撃に対して適切に防護されるとい保証を備えていることを確実にすることの責任を有する。事業者は、これらの要求事項に従って、コンピュータ・セキュリティ・プログラムを実施することについての責任を有する。

4.141. 核物質及び原子力施設の物理的防護におけるコンピュータ・セキュリティの全体の目標は、核物質の不法移転又は妨害破壊行為を手助けすることを目的とする攻撃に対してコンピュータ・システムを防護することである。事業者は、敵対者の攻撃の成功を防ぐことを助けるように、侵害に対する防護を必要とするそれらのコンピュータ・ベースのシステムを同定することについての責任を有する。事業者は次に、コンピュータ・セキュリティ方針及びその実施計画を策定する必要がある。

4.142. 脅威及び敵対者の攻撃のベクトルは多次元的である。敵対者は以下の様であり得る。

- (a) 外部の敵対者
- (b) 内部者
- (c) 1人又は多数の個人

4.143. 攻撃は次のようなものであり得る。

- (a) 機器の損傷又はセキュリティ機能の低下を生じる、即時の影響を持つ、
- (b) 例えば隠密の情報収集など、継続的である、
- (c) 時限的な影響又は個別に引き起こされる影響を生じる遅延を含む、
- (d) 物理的攻撃を含む、その他の敵対者の活動と同期する。

4.144. 攻撃のタイプとしては、以下がある場合がある。

- (a) サービスの拒絶又は機能の喪失。このタイプの攻撃は、システムダウンを遅くすることによって、変化するシステム状態を観察するための、及び／又はそれに対応するための事業者の能力を阻害することを意図する。
- (b) 横取り（「中間者の」）。コンピュータのノード間のデータの流れを横取りして改変することにより、そのような攻撃は、情報の供給又は機器への命令信号を改変することを意図する。
- (c) 秘密裏のシステムモニタリング及びデータ収集。無許可のファイルアクセス及びデータ記録、メッセージ（情報）傍受及びデータ抜き取りは、攻撃の計画と実施における予備調査を提供し得る。
- (d) 誤動作につながる要員に対する欺瞞。無許可の又は誤りのあるデータの流れの挿入により、攻撃は、正しくない措置を取ることを要員に仕向ける、正しくないシステム表示をオペレーターに提供することを意図する。
- (e) コンピュータ及び制御システムの直接操作。敵対者は、作業及び装置の独自の管理を担当することを意図する。
- (f) 重要なシステムの運転特性の改変。システムのロジック、機器の構成、設定点又はデータの改変によって、攻撃は、システムの運転特性を異常な挙動につながるように、変えることを意図する。重要なシステムのこの改変は、攻撃の主たる目的であり得るし、又は別の目的を支援し得る。

4.145. そのような攻撃に対する防御は、技術的、管理的及び物理的なセキュリティ管理を利用する多層防護（defence in depth）に基づいた手法を実践する必要がある。したがって、コンピュータ・セキュリティは、セキュリティ計画の全体的な枠組みの中に統合される必要がある。

4.146. 原子力施設での有効なコンピュータ・セキュリティプログラムの策定についての詳細な手引きは、参考文献[6]で提供されている。

安全とセキュリティとのインターフェイス

「4.11. 事業者は、安全並びに核物質の計量及び管理の活動との核物質防護のインターフェイスを、それらが相互に悪影響を及ぼさないこと及び、可能な限り、それらが相互に支え合うことを確実にするための方法で、評価し、管理すべきである。」 [1]

4.147 安全とセキュリティとのインターフェイスを有効に管理することは、両方のプログラムの重要な要素であり、また、核物質及び原子力施設の適切な物理的防護を備えること、並びに作業員及び公衆の健康と安全を守ることにあって最も重要である。

4.148. 事業者は、原子力施設の安全について、及び施設における物理的防護措置についての第一の責任を有する。事業者が、安全又は物理的防護に関連する理由で計画された変更が他の分野での措置の意図せぬ劣化をもたらさないことを確実にするために、事業者の統合された管理システムによって、計画された変更が実施される前にその変更をレビューする統合及び協調された手

法を採用することが推奨される。不利な相互作用の可能性が同定された場合、事業者は、組織内の適切な要員にそれを伝え、補う措置を検討するか、又は、補う措置及び／又は緩和措置を取る必要がある。

4.149. 事業者は、安全とセキュリティとのインターフェイスの問題を認識し、設計、建設及び通常運転中、並びに核セキュリティ事案及び緊急事態の間、さらに廃止措置の間に、それらの問題を適切に管理する必要がある。これらインターフェイスの問題は、例えば安全又はセキュリティレビュー委員会、作業の計画及び管理、並びに構成管理など、既存の管理統制によって対処される。

4.150. 核セキュリティ事案及び緊急事態の間のそのような問題の例としては、次のようなものがある。

- (a) 核セキュリティ事案への物理的防護の対応を、その事案から生じている緊急事態への安全上の対応と調整すること。
- (b) 物理的防護の対抗部隊が、核物質、及び安全上の重要な機器／システムの在る場所を含む、原子力施設に精通していること、及び放射線防護の要件の適切な知識を有していることを確実にすること。
- (c) 妨害破壊行為攻撃の間に、対抗部隊が汚染区域に立ち入り及び通過するので、対抗部隊の放射線防護を確実にすること。
- (d) 核セキュリティ事案の間に、安全上の対応者及び施設の要員が、対抗部隊が活動している区域に立ち入る又は通過する必要がある場合、それらの者を防護すること。
- (e) 物理的防護の障壁は、例えばドアやゲートに内側の迅速な解錠を設置するなどによって、火災、臨界、又は放射性核種の放出の場合には、警報に伴って、要員が区域を迅速に退避できることを損なうことなく、物理的防護の目的を満たすことを確実にすること。特別の物理的防護の措置が、まだ要員が原子力施設から出る前に検査の対象となることを確実にしている緊急時に、**Protected area** から要員が迅速に退避することを可能にするために必要とされる。
- (f) 医療的緊急事態又はその他の緊急事態時に支援するために迅速に立ち入る施設外の緊急時対応者及び車両についての潜在的な必要性を十分考慮せずに、**Protected area** への立ち入り前に詳細な検査（と探査）を要求すること。

4.151. 緊急事態計画と危機管理計画との間のインターフェイスに関する情報は、両方の計画のタイプを演習することが協調を互いに改善するという手引きを含め、パラグラフ 4.76～4.82 で提供されている。

4.152. 安全とセキュリティとのインターフェイスを管理することの重要な側面は、物理的防護の要員が、原子力施設の物理的配置の特性；施設、構造物、系統及び機器の構成；及び施設の運転又は緊急事態計画への変更について通知されることを確実にすることである。これらの分野における変更が実施される前に、よく知っている要員にそれらの変更をレビューさせることも役立つ。

つ。同様の通知及びレビューの処置は、物理的防護措置に関連する変更の観点から、安全対策のレビューへのインプットとして役立つ。特に、安全の専門知識が、受容できない放射線影響のしきい値の新しい定義、又は運転若しくは脅威における変化を反映するためのしきい値の変更をレビューするために必要である（これは次に、妨害破壊行為の既存の又は新たな攻撃対象に適用される物理的防護の必要なレベルを決定するための根拠を提供する）。

4.153. 安全と物理的防護との間のインターフェースの有効な管理としては、安全及び物理的防護が相互に支え合うような方法で、それらを実施することがある。例えば、安全に関係するインシデント又は事故を防止するための安全の手順は、内部者による悪意ある行為に対する物理的防護の手順を支援する上でも有効である。安全上重要な構造物、系統及び機器は、それらが防護すべき妨害破壊行為の一連の攻撃対象の指定、及び出入管理のための原子力施設の区画化を平易にするような方法で設計され、原子力施設内に配置される場合がある。例えば、冗長性を提供するために安全設備の適切な物理的分離を確実にすることは、この設備のすべてが1回の妨害破壊行為によって損傷を受ける可能性を低減することにもなる。核物質の在庫量の低減及びその他のハザードの低減措置は、安全のリスクと核セキュリティのリスクの両方を低減する。

セキュリティ計画

「3.27. 事業者は、許可を得るための申請の一環としてセキュリティ計画を作成すべきである。セキュリティ計画は、脅威評価又は設計基礎脅威に基づくべきであり、物理的防護システムの設計、評価、実施及び維持に関する章、並びに危機管理計画を含むべきである。所管当局は、以後のその実施が許可条件の一部であるべきセキュリティ計画をレビューし承認すべきである。事業者は、承認されたセキュリティ計画を実施すべきである。事業者は、セキュリティ計画が、現在の運転状態及び物理的防護システムについて最新であることを確実にするために、それを定期的にレビューすべきである。事業者は、承認されたセキュリティ計画の中に詳述される措置に、一時的な変更を含め、重大な修正を行なう前に、所管当局による事前承認のためにセキュリティ計画の改訂版を提出すべきである。所管当局は、セキュリティ計画についての事業者の遵守を検証すべきである。」 [1]

4.154. セキュリティ計画は、国による原子力施設の許認可のための根拠を提供している。また、セキュリティ計画の実施は、原子力施設において事業を行うための許可の条件である。したがって、セキュリティ計画は、原子力施設における物理的防護システムのすべての側面を詳細に述べるべきである。セキュリティ計画は、施設における攻撃対象が不法移転及び／又は妨害破壊行為に対する懸念があるかどうかをそれぞれのケースで示している攻撃対象のリストを含むことが推奨される。セキュリティ計画はまた、区分 I 及び区分 II の核物質の、2つの **Protected area** の間の施設内の移動についての物理的防護の措置、並びに原子力施設を出入りする核物質の受領及び発送についての措置を含めることが推奨される。

4.155. セキュリティ計画は、国の物理的防護の目的及び要求事項を満たすための措置を記述する。したがって、セキュリティ計画は、詳細な分析に基づけられる必要があり、また、計画が遂

行されるときに、物理的防護の要件が満たされることを確認するための適切な情報によって裏付けられる必要がある。セキュリティ計画は、物理的防護システムが、脅威評価又は設計基礎脅威に含まれた脅威に対処していることの保証を提供する。

4.156. セキュリティ計画の構成及び推奨される内容の例が付録 I で提供されている。

策定、レビュー及び更新

4.157. 事業者は、セキュリティ計画が原子力施設の現状及び現在の脅威を反映するように、セキュリティ計画を最新のものに保つべきである。したがって、事業者は、事業者の統合された管理システムの中で、セキュリティ計画及び関連する手順の策定、実施、監督及び更新を備えるためのセキュリティ管理システムを整備する必要がある。実施手順は、セキュリティ組織の構造、例えば技術や手順などのセキュリティ措置の利用、セキュリティ要員の訓練及び資格認定、及び危機管理計画を文書化する場合がある。セキュリティ計画は、必要に応じて、計画の各部分の実施についてのスケジュールを記載する場合があるし、また、施設の改修に関する活動を扱う場合がある。

4.158. セキュリティ計画が所管当局によって承認された後、セキュリティ計画は、原子力施設についての許認可の根拠の一部になる。所管当局は、セキュリティ計画の変更を承認し、また、事業者は、変更が物理的防護システムの有効性を低下させない場合を除いて、所管当局による承認なしに、変更案をセキュリティ計画について実施することが許可されない。物理的防護システムの有効性を低下させない軽微な変更について、事業者は、合意された期間内に、変更の所管当局に通知すべきである。

4.159. セキュリティ計画は、計画が現状を反映し続けることを確実にするために、所管当局によって規定された間隔でレビューされるべきである。セキュリティ計画はまた、物理的防護に潜在的に悪影響を与え得る、物理的防護の要員、手順、設備又はシステムにおける変更の実施前にレビューされる必要がある。核物質の新たな量又はタイプの持ち込み、妨害破壊行為の攻撃対象における変更及び物理的防護システムのその他の大きな変更は、セキュリティ計画の変更を必要とする可能性が高いであろう。その結果の行動計画を含む、そのようなレビューの結果が文書化され、保持されることは良好事例であるとみなされる。

機微情報の秘密保持

4.160. セキュリティ計画における一部の情報は機微情報であろう、また、その無許可の公表は原子力施設の物理的防護を損ない得る。したがって、事業者は、無許可の開示に対してセキュリティ計画を保護する必要がある。国の要件に従って、機微情報へのアクセスは、個人の信頼性が確認されていて、かつ、職務遂行のために知る必要のある者にのみ許されるべきである。

4.161. セキュリティ計画は、必要に応じて、各セクションが、知る必要のある者で、かつ、適切なレベルの個人の信頼性を有する者と共有され得るように、秘密度の異なるレベルのセクションに分けられることがある。

付録 I

セキュリティ計画

I.1. セキュリティ計画についての可能性のある構成の例を囲み 1 に示す。この骨子の後に、各セクションの推奨される内容を簡略に述べている。国及びその所管当局は、この構成案をレビューし、それぞれの要求事項及び特定のニーズに合うように修正すべきである。

囲み 1: セキュリティ計画の構成例

1. 管理上の情報

- 1.1. 序論及び実施スケジュール
- 1.2. 施設の説明（業務及び配置）
 - 1.2.1. 全般的な施設の説明、使命及び活動
 - 1.2.2. 施設の配置
- 1.3. セキュリティ方針
 - 1.3.1. 管理方針
 - 1.3.2. 核セキュリティ文化
 - 1.3.3. 品質保証
 - 1.3.4. 個人の信頼性の方針
 - 1.3.5. 持続可能性プログラム
- 1.4. セキュリティ組織
 - 1.4.1. セキュリティ組織の構成
 - 1.4.2. セキュリティ管理及び責任の割り当て
 - 1.4.3. セキュリティ要員の資格要件
 - 1.4.4. セキュリティ要員の訓練
 - 1.4.5. 警備員／対抗部隊の武装及び装備
- 1.5. 原子力情報のセキュリティ
- 1.6. コンピュータ・セキュリティ

2. 物理的防護システムの明確化

- 2.1. 物理的防護システムの目的及び要件
- 2.2. 攻撃対象の同定
- 2.3. 脅威の明確化
- 2.4. 法執行機関との連絡

3. 物理的防護システム

- 3.1. 物理的防護システムの詳細な説明
- 3.2. 内部脅威の緩和プログラム
- 3.3. 核物質の輸送
- 3.4. 物理的防護システムの試験、評価及び保守
 - 3.4.1. 試験及び評価のタイプ
 - 3.4.2. 試験及び評価の頻度
 - 3.4.3. 保守
 - 3.4.4. 拡大及び高度化

3.5. 補う措置

4. 対応計画

- 4.1. 組織及び責任
- 4.2. セキュリティ部隊
 - 4.2.1. 警備員
 - 4.2.2. 施設内の対抗部隊
 - 4.2.3. 施設外の対抗部隊
 - 4.2.4. 中央警報ステーションの職員
- 4.3. 危機管理計画
- 4.4. インシデント通信の指揮及び統制
- 4.5. 高脅威状態への対応

5. 方針及び運用手順

- 5.1. 文書化された方針及び運用手順
- 5.2. セキュリティ計画のレビュー、評価、監査及び更新
- 5.3. 脅威又はインシデントの報告

参考文献

略語及び用語集

管理上の情報

I.2. このセクションは、原子力施設の防護について、法のもとで責任を有する組織の完全な正式名称及び住所に関する情報を含む。セキュリティ計画の承認を申請する者の適切な電話番号及びファックス番号、並びにEメールアドレスは送付状に含まれる場合がある。

序論及び実施スケジュール

I.3. このセクションは、施設の使命及び業務の簡単な説明、施設の地図、並びに施設のマップに主要な活動の場所を示すためのその他の情報を含む。地図は、地形、輸送経路、近隣の町、又は危険物の施設、及び、対応活動に影響を及ぼし得るその他の区域を表す場合がある。地図はまた、法執行機関又はその他の施設外の対応者のための、主経路及び代替経路を示す場合がある。

施設の説明（業務及び配置）

I.4. このセクションは、施設において行われる原子力業務の詳細を規定する。

全般的な施設の説明、使命及び業務

I.5. このセクションは、施設で行われる原子力事業のタイプ、並びにこれらの事業によって使用又は生成される核物質及びその他の放射性物質についての全般的な説明をする。

施設の配置

I.6. 主要な建物及び同定された活動を示したマップ、略図又は画像が、このセクションで提示される場合がある。様々な業務のブロック図が、施設の活動を説明するには有用である場合がある。

セキュリティ方針

I.7. このセクションは、施設の書面でのセキュリティ方針を含む。

管理方針

I.8. このセクションは、物理的防護の手順の策定、改訂、実施及び監督することがシステムの目的である、施設の物理的防護の監督をする管理システムを説明する。このセクションはまた、安全と物理的防護との間のインターフェイスにどのように取り組むかについても扱い得る。

核セキュリティ文化

I.9. このセクションは、管理者、従業員及び請負業者にセキュリティ方針を伝える上での重要な部分として、核セキュリティ文化を事業者がどのように促進させるかを述べる。

品質保証

I.10. このセクションは、物理的防護に該当する管理方針及びプログラムの品質保証の側面を述べる。

個人の信頼性の方針

I.11. このセクションは、施設内の特定の区域（例えば、**Protected area**、内部区域、枢要区域）への、核物質への、及び機微情報へのアクセスについて、原子力施設における従業員及び請負業者に適用される個人の信頼性のレベル及び要求事項、並びに、継続的な個人の信頼性を確実にするために講じられる措置を述べる。

持続可能性プログラム

I.12. このセクションは、物理的防護システムについての持続可能性プログラムを述べる。

セキュリティ組織

I.13. セキュリティの責任を有するすべての者は、それぞれの職務と責任の簡略な説明で同定される場合がある。このセクションは、核物質及び原子力施設の防護することについての責任を有する者の選定、訓練、装備、試験及び資格認定についての要件を含む場合がある。事業者が割り当てた責任及び能力に応じて、このセクションは、セキュリティ組織のどの部分が社内担当者によって提供され、どの部分が外部の請負業者によって提供されるかを述べる必要がある。請負業者について、このセクションは、施設を防護するための要件を請負業者がどう満たしていくかを説明した、事業者と請負業者との間の書面による合意を簡単に述べる場合がある。セキュリティ計画に含まれる詳細のレベルは、施設によって異なることがあるが、このセクションは、セキュリティ計画を読む者に対して、施設のセキュリティ部隊の

能力を理解するのに十分な情報を提示する必要がある。提示される情報は、セキュリティ組織が、物理的防護を実施するために計画、人員配置、訓練、資格認定及び装備されることを確認しようとする。

セキュリティ組織の構成

I.14. このセクションは、管理者、警備員及び施設内の対抗部隊、技術的なセキュリティ要員、並びに物理的防護に関連する機能に責任を有するその他の者を含んでいるセキュリティ組織の構造を述べる。このセクションはまた、責任、及び、権限の系統が施設及び企業の管理者までどのように及んでいるかを含めている、各監督的及び管理的職位の説明も含む場合がある。

セキュリティ管理及び責任の割り当て

I.15. このセクションは、施設のセキュリティ組織に割り当てられる具体的な物理的防護の責任を述べる。

セキュリティ要員の資格要件

I.16. 説明は、セキュリティの職務及び責任を割り当てられる者の当初の及び継続的な適性についての要件が提示される場合がある。このセクションはまた、これらの要員が要求された業務を提供するために資格付与され続けることを確実にするための手順も述べる場合がある。このセクションはまた、警備員及び施設内の対抗部隊のメンバーについての、銃火器の使用資格認定及び再資格認定の要件の説明も含む。

セキュリティ要員の訓練

I.17. このセクションは、警備員及び施設内の対抗部隊についての訓練プログラムを述べる。また、警備員及び施設内の対抗部隊が割り当てられた職務又は責任を実施する能力をどのように示すかについても述べる。対抗部隊について、対抗戦術の訓練プログラムの説明が含まれる場合がある。

警備員／対抗部隊の武装及び装備

I.18. このセクションは、警備員及び施設内の対抗部隊のメンバーに割り当てられる武装について、職位別に述べる。有効な対応能力を提供することができるように警備員及び対抗部隊に利用可能なその他の装備の説明が述べられる場合がある。

原子力情報のセキュリティ

I.19. このセクションは、機微情報の機密性、健全性及び可用性を維持するために講じられる措置を明示する。情報管理の手順はまた、機微情報の配布が、知る必要性に基づいて、個人の信頼性が適切に判定された、適切な者にどのように限定されるかを述べる必要がある。機微情報に適用される管理は、機微情報の受領、場所、送達及び破棄の記録を含む場合がある。

コンピュータ・セキュリティ

I.20. このセクションは、コンピュータ及びコンピュータ・ベースのシステムに保持されている機微情報の機密性、健全性及び利用可能性、並びに、計装制御システムの健全性及び可用性を確実にするアクセス管理の手順、通信規約及び物理的防護の措置について述べる。

物理的防護システムの明確化

物理的防護システムの目的及び要件

I.21. このセクションは、攻撃対象の秘密度のレベルに従ったグループに分けた、様々なタイプの攻撃対象の防護についての目的を、記述する。

攻撃対象の同定

I.22. このセクションは、潜在的な盗取又は妨害破壊行為の攻撃対象及びそれらの場所を記載する。また、その侵害が、悪意ある行為を円滑にすることを促進し得る、物理的防護、安全並びに核物質の計量及び管理にとって重要なコンピュータ・システムも記載する。

脅威の明確化

I.23. このセクションは、物理的防護システムが、それに対して防護するように設計されていて、国によって明示された脅威評価又は設計基礎脅威を参照している脅威のタイプを、大まかに記述する。

法執行機関との連絡

I.24. 潜在的なセキュリティ事案の早期警報を確実にするために、法執行機関との日常の連絡がどのように維持されるかの詳細が規定されることがある。

物理的防護システム

I.25. このセクションは、施設における物理的防護システムについての説明である。

物理的防護システムの詳細な説明

I.26. このセクションで、例えば人員・車両の出入管理地点など、層の境界及び防護措置を示している施設の地図が提示されることがある。防護措置の説明が、次のように、示される必要がある。

- (a) 出入管理。各出入管理地点での、人、車両及び物質の管理及び検査の説明が示される必要がある。この説明は、緊急事態の間又は緊急事態につながり得る状況の間に、アクセス許可及び出入管理システムが、許可された者及び車両の迅速な出入りにどのように便宜を図るかについても含めることがある。注意が、立入制限区域、**Protected area**、内部区域、枢要区域及び物理的防護機器へのアクセスを管理するために使用される、すべての鍵、錠、組み合わせ数字、パスワード及び関連する装置の管理に払われる。

- (b) 中央警報ステーション。このセクションは、中央警報ステーション及びバックアップ監視ステーションの場所を説明する。また、中央警報ステーションの警報の通信及び表示システム、通信機器及び出入管理の設備、並びに中央警報ステーションが攻撃及び無許可のアクセスに対してどのように防護されるかの詳細についても述べる。
- (c) 通信。中央警報ステーションと警備員及び対抗部隊との間の通信と同様に、警備員及び施設内の対抗部隊についての通信能力が述べられる必要がある。このセクションは、継続的な通信能力が、通常時及び緊急事態の間に、施設内及び施設外の対抗部隊との有効な指揮及び統制を確実にするために、どのように維持されるかを述べる。もし、通信が制限される施設の区域があれば、これらの区域が同定される必要がある。
- (d) 検知及び監視。このセクションは、検知システム、及び、警報がどのように中央警報ステーションに伝えられて評価されるかを述べる。このセクションはまた、改竄の兆候がある状況に対処する手順も述べる場合がある。侵入者を検知するため、並びに物理的障壁、又はその他の構成要素及び物理的防護システムの機能の健全性を確実にするために、施設区域を継続的に調査、観察、及び監視する方法を述べる場合がある。
- (e) 照明。このセクションは、例えば警報後の評価など、事業者が、選定された用途のための最小限の照明のレベルをどのように維持するかを述べる。
- (f) 物理的障壁。このセクションは、施設内の様々なセキュリティ区域内の障壁（例えば、建物、地形、フェンス、壁、ドアなど）を説明する。また、車両障壁、その配置及び運用、並びにそれに関連する監視の措置の説明を含む場合がある。
- (g) セキュリティ区域／層。このセクションは、施設に存在する物理的な防護の区域（又は層）を同定する。

内部脅威の緩和プログラム

I.27. このセクションは、内部脅威に対して防護するための方法を述べるべきである。

核物質の輸送

I.28. このセクションは、それぞれ異なる区分の核物質の施設内の輸送についての手順、及び施設を出入りする核物質の受領及び発送について施設内でなされる措置を述べる。

物理的防護システムの試験、評価及び保守

I.29. このセクションは、物理的防護システムの評価及び試験についての手順を同定する。

試験及び評価のタイプ

I.30. このセクションは、既存の試験及び評価プログラム、及びそれらが、施設の物理的防護システムの有効性を評価するためにどのように使用されるかを述べる。

試験及び評価の頻度

I.31. 試験及び評価プログラムが実施される頻度の詳細が述べられる必要がある。

保守

I.32. このセクションは、すべての物理的防護機器についての保守および較正プログラムを述べる。

拡大及び高度化

I.33. このセクションは、新規の建設若しくは既存の建造物の大きな物理的改修、又は機器の設置に係る物理的防護措置を実施することについての予測されるスケジュールを述べるために利用できる。

補う措置

I.34. このセクションは、定期的な試験又は保守の間を含む、物理的防護障壁が劣化した場合、又は機器が動作不可能になった場合に適用されるすべての補う物理的防護措置を同定する。特に、すべてのタイプの物理的防護の機器への予備電源の提供が述べられる必要がある。

対応計画

組織及び責任

I.35. このセクションは、施設における様々な攻撃対象についての有効な対抗戦略を維持するための、施設及び施設外の対抗部隊の組織と責任の詳細を提示する。

セキュリティ部隊

I.36. このセクションは、協調的対応の戦略を行うために利用可能な対抗部隊の概説を提示する。

警備員

I.37. このセクションは、警備部隊の武器、装備及び輸送の詳細を含む、それらの人数、場所及び任務を述べる。

施設内の対抗部隊

I.38. このセクションは、施設内の対抗部隊が使用される場合には、核セキュリティ事案に適時に対応するためのその能力及び性能を述べる。

施設外の対抗部隊

I.39. このセクションは、推定される対応時間を含む、核セキュリティ事案に対応するための、施設外の対抗部隊の能力及び性能を述べる。施設外の対応を提供することについての合意の文書化と維持の手順が含まれる場合がある。

中央警報ステーションの職員

I.40. このセクションは、中央警報ステーションで使われる担当者の最低限の人数、任務、責任及びローテーション・スケジュールを述べる。

危機管理計画

I.41. このセクションは、核セキュリティ事案に対する、及び物理的防護の対応を必要とするその他の事案に対する危機管理計画を述べる。核セキュリティ事案が発生した場合に危機管理計画を実施する責任と権限を有する具体的な人々及び／又は職位を同定する。危機管理計画がどのように、また、いつレビューされ、演習されるかの詳細を述べる。

I.42. 下記のリストは、危機管理計画において考慮し、対処される様々なタイプのシナリオの例を推奨している。

- (a) 行方不明の核物質の捜し出し及び回収（緊急棚卸を含む）
- (b) 妨害破壊行為の放射線影響の最小化及び緩和
- (c) 内部脅威の発見
- (d) 原子力施設への無許可の侵入
- (e) 外部脅威（例えば、爆破予告）
- (f) スタンドオフ攻撃
- (g) 空からの攻撃
- (h) 水上からの攻撃
- (i) サイバー攻撃
- (j) 機微情報の侵害

I.43. 危機管理計画は機微情報を含むので、要求される保護のレベルを示すために適切な標示が付けらる必要がある。また、緊急事態計画との協調のための措置も扱う必要がある。危機管理計画の例が付録 II に示されている。

インシデント通信の指揮及び統制

I.44. セキュリティ計画は、関係する機関による核セキュリティ事案への対応において有効な指揮及び統制がどのように実施されるか、施設内及び施設外のインシデント指揮及び統制センターがどこに置かれるか、及びこれらの場所でどのような通信施設が利用可能かを述べる。

高脅威状態への対応

I.45. リストは、国内で脅威の全体的なレベルが上がった場合に実施される物理的防護の手順への計画された強化が提示されるべきである。

方針及び運用手順

文書化された方針及び運用手順

I.46. このセクションは、例えば安全システムや核物質の計量及び管理システムなど、物理的防護システムを補完するシステムとインターフェイスをとるための手順を含む、施設における物理的防護を運用する、文書化された方針及び運用手順を記載する。

セキュリティ計画のレビュー、評価、監査及び更新

I.47. セキュリティ計画が最新であることを確実にするために使用される手順及びレビューの処置（その頻度を含む）の詳細が、必要なすべての修正は、その実施前に承認のために所管当局に提出されるという保証と一緒に、示される必要がある。

脅威又はインシデントの報告

I.48. 指定された出来事を施設のセキュリティ組織に報告する、施設の従業員及び請負業者のための手順、及び、必要に応じて、所管当局に以後の報告をすることについての手順が、このセクションで述べられる。

付録 II

危機管理計画の例

目的

II.1. このセクションは、特定の危機管理計画の目的を述べる。目的は、さらなる対応に備えること、又は敵対者の行為の影響を低減することである場合がある。

インシデントの対応手順

交戦規定

II.2. このセクションは、法のもとでどのような種類の武力が許可されるか、及びそのような武力がいつどこで使用され得るかを明示する交戦規定を述べる。

対応手順

II.3. このセクションは、どのように対応が組織され、協調されるかを述べる。この危機管理計画の下での対応の開始を示すために使用される標識を同定する。このセクションは、以下の内容を含む場合がある。

- (a) 盗取及び妨害破壊行為シナリオに対する対抗部隊のすべての所定の行動、責任分野及び配置についてのタイムライン
- (b) あり得る攻撃に対応要員をさらすことを制限する手順
- (c) 施設外の対抗部隊に通知するときに使用されるタイムライン
- (d) 対抗者の最少人数

奪回及び回収

II.4. このセクションは、盗取シナリオにおいて敵対者が施設を去った時に、対応がどのように組織されるかを述べる。様々な対応チーム、指揮系統、及び責任の変更を調整するために使用される手続きを含む。

最小化及び緩和

II.5. このセクションは、物理的防護の対応が、妨害破壊行為の攻撃の影響を最小化及び緩和する緊急事態の対応者を支援するためにどのように体系化されるかを述べる。

指揮、統制、連絡

II.6. このセクションは、外部の対応組織との間で合意された協定に文書化された取り決めについて述べる。どの機関が作戦の指揮権を持つのか、また、この指揮権が別の機関に移る状況について詳細に述べる。そのときの状況並びにインシデント統制センターの戦略的及び戦術的な責任を考慮して、使用されるすべての通信回線、及び事案の様々な段階において使用されるインシデント統制センターの場所の詳細を述べる。

危機管理計画の演習

II.7. このセクションは、危機管理計画の実施を試験及び訓練するために行われる演習のタイプと頻度を述べる。情報は、危機管理計画と緊急事態計画の両方が実施される合同演習によって両方の計画の間の協調を試験することを含む。このセクションはまた、危機管理計画をさらに改善するために、これらの演習から学んだ教訓がどのように得られ、使用されるかも述べる。

付録 III

核物質の加算又は集計

手法 1

III.1. この例は、表 1 が、集計された核物質を分類するために使用される方法の 1 つを示している。同じ施設内にある核物質は、次の概要のように分類されるべきである。

(a) 次の場合は、区分 I

$$\frac{\text{Pu} + {}^{233}\text{U}}{2000} + \frac{{}^{235}\text{U}(\geq 20\%) }{5000} \geq 1 \quad (1)$$

(b) 次の場合は、区分 II

$$\begin{aligned} \frac{\text{Pu} + {}^{233}\text{U}}{500} + \frac{{}^{235}\text{U}(\geq 20\%) }{1000} + \frac{{}^{235}\text{U}(\geq 10\% \text{ and } < 20\%) }{10000} &\geq 1 \\ &> \frac{\text{Pu} + {}^{233}\text{U}}{2000} + \frac{{}^{235}\text{U}(\geq 20\%) }{5000} \end{aligned} \quad (2)$$

(c) 次の場合は、区分 III

$$\begin{aligned} \frac{\text{Pu} + {}^{233}\text{U}}{15} + \frac{{}^{235}\text{U}(\geq 20\%) }{15} + \frac{{}^{235}\text{U}(\geq 10\% \text{ and } < 20\%) }{1000} \\ + \frac{{}^{235}\text{U}(> \text{U}_{\text{nat}} \text{ and } < 10\%) }{10000} &\geq 1 > \frac{\text{Pu} + {}^{233}\text{U}}{500} + \frac{{}^{235}\text{U}(\geq 20\%) }{1000} \\ + \frac{{}^{235}\text{U}(\geq 10\% \text{ and } < 20\%) }{10000} \end{aligned} \quad (3)$$

(d) 次の場合、又は、物質が天然ウラン、劣化ウラン若しくはトリウムのみで構成される場合は、区分 III 満

$$\begin{aligned} 1 > \frac{\text{Pu} + {}^{233}\text{U}}{15} + \frac{{}^{235}\text{U}(\geq 20\%) }{15} \\ + \frac{{}^{235}\text{U}(\geq 10\% \text{ and } < 20\%) }{1000} + \frac{{}^{235}\text{U}(> \text{U}_{\text{nat}} \text{ and } < 10\%) }{10000} \end{aligned} \quad (4)$$

ここで、

Pu	${}^{238}\text{Pu}$ の同位体組成が 80% を超えるものを除く、すべてのプルトニウムのグラム単位の質量
${}^{233}\text{U}$	${}^{233}\text{U}$ のグラム単位の質量

$^{235}\text{U} (\geq 20\%)$	^{235}U の濃縮度が 20%以上の形態で存在する ^{235}U のグラム単位の質量
$^{235}\text{U} (\geq 10\% \text{ and } < 20\%)$	^{235}U の濃縮度が 10%以上、20%未満の形態で存在する ^{235}U のグラム単位の質量
$^{235}\text{U} (> U_{\text{nat}} \text{ and } < 10\%)$	^{235}U の濃縮度が天然ウランを超え、10%未満の形態で存在する ^{235}U のグラム単位の質量

また、分母はグラム単位の質量である。

III.2. これらの数式は、原子炉内で照射去れていない物質、又は、原子炉内で照射されているが、遮蔽なしで、1メートル離れた地点で1グレイ/時（100ラド/時）以下の放射線レベルの物質に関するものである。

手法 2

III.3. 集計した核物質の区分を決定するための別の手法は、次の数式を使用する。

$$\frac{1}{S} = \sum_i \frac{f_i}{S_i} \quad (5)$$

ここで、

- f_i (無次元) 混合物のタイプ i の物質の質量分率（存在する各種類の物質の質量を存在する物質の合計質量で除したもの）
- S_i (kg 又は g) 表 1 に記載された、検討対象の区分についての種類 i の物質の質量しきい値

また、 S (kg 又は g) は、表 1 に記載された、検討対象の区分についての物質の集計した質量しきい値である。

III.4. 以下は、区分 I の質量しきい値である。

- (a) すべての同位体を合わせて、2 kg のプルトニウム
- (b) ^{235}U の濃縮度が 20%以上の形態で存在する 5 kg の ^{235}U
- (c) 2 kg の ^{233}U

III.5. 以下は、区分 II の質量しきい値である。

- (a) すべての同位体を合わせて、500 g のプルトニウム
- (b) ^{235}U の濃縮度が 20%以上の形態で存在する 1 kg の ^{235}U
- (c) ^{235}U の濃縮度が 10%以上、20%未満の形態で存在する 10 kg の ^{235}U
- (d) 500 g の ^{233}U

III.6. 以下の量は、区分Ⅲの質量しきい値である。

- (a) すべての同位体を合わせて、15 g のプルトニウム
- (b) ^{235}U の濃縮度が 20%以上の形態で存在する 15 g の ^{235}U
- (c) ^{235}U の濃縮度が 10%以上、20%未満の形態で存在する 1 kg の ^{235}U
- (d) ^{235}U の濃縮度が 10%未満の形態で存在する 10 kg の ^{235}U
- (e) 15 g の ^{233}U

III.7. ^{238}Pu の同位体濃度が 80%を超えるものを除く、すべてのプルトニウムが考慮される。

III.8. これらのしきい値は、原子炉内で照射されていない物質、又は、原子炉内で照射されているが、遮蔽なしで、1メートル離れた地点で 1 グレイ/時 (100 ラド/時) 以下の放射線レベルの物質に関するものである。

III.9. 該当する区分を決定するために、まず、集計された物質が区分Ⅰであるかどうかを決定する (ステップ 1)。物質又は混合物は、合計質量が、物質又は混合物について計算された区分Ⅰの質量しきい値以上であれば、区分Ⅰである。もし、区分Ⅰでなければ、ステップ 2 に進む。

III.10. 集計された物質が区分Ⅰでない場合は、それが区分Ⅱであるかどうかを決定する (ステップ 2)。物質又は混合物は、合計質量が、物質又は混合物について計算された区分Ⅱの質量しきい値以上であれば、区分Ⅱである。もし、区分Ⅱでなければ、ステップ 3 に進む。

III.11. 集計された物質が区分Ⅰ又はⅡでない場合は、区分Ⅲであるかどうかを決定する (ステップ 3)。物質又は混合物は、合計質量が、物質又は混合物について計算された区分Ⅲの質量しきい値以上であれば、区分Ⅲである。

III.12. 物質又は混合物の質量が区分Ⅲの質量しきい値を下回る場合は、区分Ⅲ未満である。

例 1

III.13. 核物質は、濃縮度が 20%を超えるウランに含まれた 4 kg の ^{235}U 、及び 1 kg のプルトニウムからなり、 ^{235}U とプルトニウムの合計は 5 kg である。濃縮度が 20%を超えるウランの質量分率は 4/5 であり、プルトニウムについては 1/5 である。

ステップ 1: この物質についての区分Ⅰの質量しきい値は次式で与えられる。

$$\frac{1}{S} = \frac{4/5}{S_{\text{U-235}}} + \frac{1/5}{S_{\text{Pu}}} = \frac{4/5}{5 \text{ kg}} + \frac{1/5}{2 \text{ kg}} = 0.26$$

したがって、 $S = 3.85 \text{ kg}$ である。この物質の質量 (5 kg) は、 S (3.85 kg) よりも大きいため、この混合物についての区分 I のしきい値を超える。

この物質は、したがって、区分 I の量である。

例 2

III.14. 核物質は、濃縮度が 20%を超えるウランに含まれた 2.5 kg の ^{235}U 、及び 500 g のプルトニウムからなり、 ^{235}U とプルトニウムの合計は 3 kg である。濃縮度が 20%を超えるウランの質量分率は $2.5/3$ (又は $5/6$) であり、プルトニウムについては $0.5/3$ (又は $1/6$) である。

ステップ 1: この物質についての区分 I の質量しきい値は次式で与えられる。

$$\frac{1}{S} = \frac{5/6}{S_{\text{U-235}}} + \frac{1/6}{S_{\text{Pu}}} = \frac{5/6}{5 \text{ kg}} + \frac{1/6}{2 \text{ kg}} = 0.25$$

したがって、 $S = 4 \text{ kg}$ である。合計質量は、区分 I についての混合物の質量しきい値を下回る、 3 kg である。

ステップ 2: この物質についての区分 II の質量しきい値は次式で与えられる。

$$\frac{1}{S} = \frac{5/6}{S_{\text{U-235}}} + \frac{1/6}{S_{\text{Pu}}} = \frac{5/6}{1 \text{ kg}} + \frac{1/6}{0.5 \text{ kg}}$$

したがって、 $S = 0.86 \text{ kg}$ である。合計質量は、区分 II についての混合物の質量しきい値を上回る、 3 kg である。したがって、この混合物は区分 II である。

付録 IV

勧告文書との相互参照

表 4 は、参考文献[1]の параグラフと本文書の関連した параグラフとの間の相互参照を示している。

表 4. 勧告文書[1]との相互参照

勧告文書[1]の параグラフ	本文書の関連した параグラフ
はじめに	セクション 1
背景 (1. 1～1. 8)	
目的 (1. 9～1. 11)	
範囲 (1. 12～1. 18)	
構成 (1. 19～1. 24)	
国の物理的防護体制の目的 (2. 1～2. 3)	セクション 2
核物質及び原子力施設についての国の物理的防護体制の要素	
国の責任 (3. 1、3. 2)	3. 5～3. 7
国際輸送 (3. 3～3. 7)	参考文献[2]でカバーされている
物理的防護の責任の割り当て (3. 8)	3. 8～3. 11
立法上及び規制上の枠組み	
立法上及び規制上の枠組み (3. 9～3. 17)	3. 12～3. 32
所管当局 (3. 18～3. 22)	3. 39～3. 48
許可保有者の責任 (3. 23～3. 30)	3. 49、4. 4～4. 13、4. 154～4. 161

表 4. 勧告文書[1]との相互参照（続き）

勧告文書[1]の параграф	本指針の関連した параграф
国際協力及び支援 (3. 31～3. 33)	3. 50～3. 54
脅威の同定及び評価 (3. 34～3. 40)	3. 55～3. 63
リスクベースの物理的防護システム及び措置	
リスク管理 (3. 41、3. 42)	3. 64～3. 103
等級別手法 (3. 43、3. 44)	3. 70～3. 101
多層防護 (defence in depth) (3. 45～3. 47)	3. 102、3. 103
物理的防護体制の持続	
セキュリティ文化 (3. 48～3. 51)	3. 105、3. 106
品質保証 (3. 52)	3. 107～3. 110
秘密保持 (3. 53～3. 55)	3. 111～3. 115
持続可能性プログラム (3. 56、3. 57)	3. 119
核セキュリティ事案への計画及び準備並びに対応 (3. 58～3. 62)	3. 120～3. 126
使用中及び貯蔵中の核物質の不法移転に対する措置の要件	4. 4～4. 14、4. 23～4. 59、 4. 71～4. 75、4. 124～4. 139
総則	
関連基礎事項 (4. 1～4. 4)	
区分 (4. 5～4. 8)	3. 74～3. 90
使用中及び貯蔵中の不法移転に対する物理的防護の要件	
総則 (4. 9～4. 12)	4. 83～4. 123、4. 133～4. 146

表 4. 勧告文書[1]との相互参照（続き）

勧告文書[1]の параграф	本指針の関連 параграф
区分 I、II 及び III 核物質についての要件（4. 13～4. 20）	4. 33～4. 59、4. 83～4. 123
区分 I 及び II 核物質についての要件（4. 21～4. 35）	4. 33～4. 59、4. 83～4. 123
区分 I 核物質についての要件（4. 36～4. 49）	4. 33～4. 59、4. 83～4. 123
行方不明の又は盗取された核物質を捜し出して回収するための措置の要件	4. 71～4. 75
国に対する要件（4. 50～4. 56）	
事業者に対する要件（4. 57～4. 63）	
原子力施設並びに使用中及び貯蔵中の核物質の妨害破壊行為に対する措置の要件	4. 4 ～ 4. 14、4. 23 ～ 4. 59、 4. 76～4. 82、4. 133～4. 146
総則（5. 1～5. 3）	
妨害破壊行為に対する物理的防護に関する等級別手法の基礎（5. 4～5. 8）	3. 91～3. 101
妨害破壊行為に対する物理的防護システムを設計する作業についての要件（5. 9～5. 19）	4. 140～4. 153
原子力施設での妨害破壊行為に対する物理的防護の要件	4. 33～4. 59、4. 83～4. 123
原子力発電所を含む高影響施設に対する要件（5. 20～5. 42）	4. 33～4. 59、4. 83～4. 123
その他の原子力施設及び核物質に対する要件（5. 43）	5. 20～5. 42

表 4. 勧告文書[1]との相互参照（続き）

勧告文書[1]の параграф	本指針の関連 параграф
妨害破壊行為の放射線影響を緩和又は最小化するための関連措置も対する要件	4. 76～4. 82
範囲及び境界（5. 44）	
国に対する要件（5. 45～5. 53）	
事業者に対する要件（5. 54～5. 58）	

参考文献

- [1] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Material in Transport, IAEA Nuclear Security Series No. 26-G, IAEA, Vienna (2015).
- [3] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).
- [5] INTERNATIONAL ATOMIC ENERGY AGENCY, Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme, IAEA Nuclear Security Series No. 19, IAEA, Vienna (2013).
- [6] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).
- [7] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, UNITED NATIONS OFFICE ON DRUGS AND CRIME, WORLD CUSTOMS ORGANIZATION, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).
- [8] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).
- [9] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).
- [10] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, INTERPOL, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, PREPARATORY COMMISSION FOR THE COMPREHENSIVE NUCLEAR-TEST-BAN TREATY ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, WORLD METEOROLOGICAL ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (2015).

- [11] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR OFFICE, PAN AMERICAN HEALTH ORGANIZATION, WORLD HEALTH ORGANIZATION, Criteria for Use in Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSG-2, IAEA, Vienna (2011).
- [12] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR OFFICE, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, Arrangements for Preparedness for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-G-2.1, IAEA, Vienna (2007).
- [13] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, IAEA Nuclear Security Series No. 16, IAEA, Vienna (2012).
- [14] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, IAEA Nuclear Security Series No. 4, IAEA, Vienna (2007).
- [15] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).
- [16] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).
- [17] INTERNATIONAL ATOMIC ENERGY AGENCY, Handbook on the Physical Protection of Nuclear Materials and Facilities, IAEA-TECDOC-1276, IAEA, Vienna (2002).
- [18] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities, IAEA Nuclear Security Series No. 25-G, IAEA, Vienna (2015).

本書は、IAEA核セキュリティ・シリーズNo.13「核物質及び原子力施設の物理的防護に関する核セキュリティ勧告（INFCIRC/225/ Revision 5）」を実施する上での、一連の手引きの中の主要な「実施指針」である。

本書は、不法移転に対する核物質の及び妨害破壊行為に対する原子力施設の防護に焦点を合わせている。本書は、国及びその所管当局に国内の物理的防護体制をどのように確立、強化及び持続するかについて、並びに事業者の物理的防護システムを含む、関連するシステム及び措置をどのように実施するかについての手引きを提供する。

国際原子力機関

ウィーン

ISBN 978-92-0-111516-4

ISSN 1816-9317