管理者はまた、実験室バイオセキュリティシステムの継続的な改善を確保しなければならない。そのために、管理者はシステムの日常的な自己評価を実行すべきである。後の管理見直しはこれらの評価の結果から、重大な弱点を是正する行動をとるべきである。行動は本来、正すもので、予防的なものである。いわゆる、既存の問題を訂正し、生じるかもしれない新たな問題を予測し訂正すべきである。

大多数の施設では、プログラム管理は実験室バイオセキュリティと実験室バイオセーフティの最も重要な要素である。計画、人員配置、資金、訓練などの活動を通して、プログラム管理は実験室バイオセキュリティと実験室バイオセーフティプログラムのすべての要素に取り組んでいる。

次の節では実験室バイオセキュリティプログラムの管理に特定のガイダンスを提供する。

4.1 役割と責任

施設の全職員は効率的で機能的な実験室バイオセキュリティシステムを達成する助けとなる。従って、実験室バイオセキュリティの責任を略述することは管理者にとって重要である。

本節で記述した役割と責任はあるアプローチの実例である。大規模な設備あるいは広範囲に渡る一定の危険な生物剤の研究を行なう特異的な施設が考慮すべきことは目録に従属して付加的な地位を適切に授けるかもしれない。役割と責任は小規模な施設において強化されるかもしれない。

管理者はバイオセキュリティシステムの目的を確立し、適切な利害関係者にこれらの目的を伝達し、必要な施設へ支援と資源を提供しなければならない。施設長は効果的に実験室バイオセキュリティが実施され、緊急対応が適宜実施されることを確保する責任がある。施設長はこれらの役割を委任するために他の管理職員を選別するかもしれない。これは文書にして書き留めるべきである。大規模な施設あるいは材料の濫用／悪用な使用のリスクが高い施設では、施設長は実験室バイオセキュリティ職員を指名すべきである。

実験室バイオセキュリティ職員は実験室バイオセキュリティ計画を展開する。職員は実験室管理者や実験室スタッフと協調する責任があり、実験室は実験室バイオセキュリティの方針を固執している。もし付加的な義務として実験室バイオセキュリティ職員の役割と責任が与えられなかったら、これらの 2 人の職

員は 2 つのプログラムの間で何らかの潜在的な対立を解決するように調整し、補足的なプログラムの目的を達成するための資源を調達する機会を調査しなければならない。実験室バイオセキュリティ職員は施設における物理的そして人事セキュリティの実施を監督し、実験室バイオセキュリティシステムは施設全体のセキュリティの労作に正確に反映されることを確保すべきである。バイオセキュリティプログラムは評価する必要があり、プログラムの成功を測る評価指標は発展させ、追跡する必要がある。従って、この人物は自己評価を実行すべきであり、外部評価との接点となる。実験室バイオセキュリティ職員は確立、発展、維持、そして実験室バイオセキュリティ違反の傾向や実験室バイオセキュリティの目的とゴールを達成するための他の過失(lapses)を明確にし、分析する重要性を更新すべきである。

施設は、人事セキュリティ管理や情報セキュリティなどの様々な管理バイオセキュリティの職務の責任を明示する必要がある。人物は要求された背景となる調査や裁定の調整、バッジの監督、来訪者の必要条件を満たすべきである。同様に、特定の人物は情報セキュリティ問題の重要な関係者として、情報セキュリティ方針を実施し、実験室バイオセキュリティ計画の発展に参加し、地域のコンピューターセキュリティ活動を監視し、コンピューターセキュリティの事態への対応、そしてコンピューターセキュリティの方針と手順の十分な理解を確保すべきである。人物はまた、情報セキュリティの自己評価を調整すべきである。大規模な施設は例として、すでに人事職員や情報セキュリティ管理者がいるため、これら多くの役割や責任はすでに命ぜられているかもしれない。実験室バイオセキュリティ職員あるいは他の管理代表者はバイオセキュリティシステムの適切な局面が一体化されることを確保する既存のシステムを簡単に見直す必要がある。

人物はすべてのバイオセキュリティ文書が適切に維持され、管理されることを確保する責任がある。すべての実験室バイオセキュリティ文書と関連した責任ある人物(リスクの高い病原体の在庫目録の類似品)の中心となる目録を作成することは適切かもしれない。すべての文書を監視する人物はどのくらいの期間文書が保有され、見直しや校正の必要性を説明する必要があるのか予定を明確にすべきである。一定の文書の保有には特定の規制要求事項があるかもしれない。人物は文書がこの予定に従って見直され、校正され、保持されることを確保する必要がある。人物は文書の破壊や一般的な情報セキュリティ問題の適切

な手順を発展する情報セキュリティ専門家との調和が必要であるだろう。バイオセキュリティプログラムの実情や視野に基づいて、実験室バイオセキュリティ職員の付加的な義務かもしれない。

実験室の経営者(例、主要研究者(PI))あるいは他に直接的に監督する研究者、診断者、動物に従事する者、そして実験室バイオセキュリティの中程度そして／あるいは濫用／悪用のリスクの高い材料へアクセスする他の人物の管理には多くの責任がある。実験室バイオセキュリティ職員と調整して、管理者は操作的な実験室バイオセキュリティプログラムを実施しなければならない。管理者は訓練、実施、そして実験室バイオセキュリティの方針やプログラムの監視の資源を提供する必要がある。管理者は全職員が毎年包括的な実験室バイオセキュリティ訓練を含むすべて要求された訓練を受けることを確保すべきである。管理者は新規職員にオリエンテーションを行なうべきである。すべて未解決なバイオセキュリティ問題が取り組まれる(例、鍵となる適切な文書が提出される)ことを確保するために停止過程の期間は退職した職員にも応じるべきである。

実験室で日々関わるため、管理者はまた、公共への情報流出の見直しや承認を行なう訓練をする最高の候補者でもある。最後に、管理者の最も重要な責任は実験室バイオセキュリティの必要条件の存続した問題意識と実験室バイオセキュリティの重要性を植え付け、維持することである。

もし現場に警備隊がいる場合は、入口でアクセスを制限したり、あるいは権限ある搬送車や職員の制限区域への立ち入り制限、駐車区域と不法行為を抑止させるために全敷地の監視、そして許可されていない運搬車あるいは人物が存在しないこと、何らかの電子侵入探知システムによる警報の監視と評価を確保するなどの多くの日常的なセキュリティ機能の責任がある。さらに、警備隊 (あるいは他に現場で対応する職員)は何らかの潜在的な実験室バイオセキュリティ事故へ対応するだろう。

全職員はすべての実験室バイオセキュリティの方針と手順を理解し、遵守する責任がある (Figure 4.2)。

付録 C

バイオセキュリティ計画のサンプルフォーム

この付録では、一例として生物科学研究施設がバイオセキュリティ計画や手引き書を作成する際に有用なサンプルフォームを示します。このサンプルフォームは、本来は実験施設が合衆国の特定病原体基準（42 CFR 73、9 CFR 121、7 CFR 331）を順守する必要性から作成されたフォームですが、この基本的な組み立てや原則はバイオセキュリティ計画を策定しようとする全ての実験施設にとって適用できると思います。

実験施設のバイオセキュリティ計画に含めることが適切であると思われる一般的な事項について以下に述べることとします。それぞれの実験施設に特有の情報に関するガイダンスとして触れなければならない事項はイタリック体で印刷してあります。

C.1 序文

ここでは、このバイオセキュリティ計画では何を最終目的としているかを説明してください。また、このバイオセキュリティ計画は誰に対して適用するのかを説明してください。このバイオセキュリティ計画が42 CFR 73、9 CFR 121、7 CFR 331 のような連邦基準のいずれに対してもその内容を順守していること、および特定病原体（この用語については、このバイオセキュリティ計画でCFR によって規制が行われている全ての病原体や毒素を指す用語であることを説明しておかなければなりません）に関わる盗難や破壊活動に対して段階的な防御を展開するための対策全体に関して述べていることについても、ここで説明してください。本実験施設においては全ての特定病原体に対して共通の単一の手法によって安全を図ろうとするのか、または中等度リスク病原体と高度リスク病原体に対しては別の対策で（全ての連邦規制を順守した上で）対処しようとするのかについても、この序文の中で説明してください。

C.2 役割と責任

この章で述べる役割と責任は、全ての事項に関しての役割と責任を指すのではなく、CFR で求められている要求事項を遂行するに当たって生ずる役割と責任を指しています。

ここでは、一名の人員に対して多数の役割と責任がおわされる可能性があることを説明してください。特に、研究しているプロジェクトの数が少なく、危険度の高い生物剤を用いている実験施設に当てはまります。

C.2.1 施設責任者

施設責任者（RO）は事業が CFR の要求事項に照らして合法的であることを確認する権限が与えられた人員を指します。CFR の要求事項には本バイオセキュリティ計画の策定と実施に関する基準も含まれています。施設責任者はこの計画を年に一度、および何らかのインシデントが発生した際に見直しを行います。

C.2.2 施設責任者代理

施設責任者代理は施設責任者が職務を執行できなくなった際にそれに変わってその職務を執行する権限が与えられた人員を指します。

C.2.3 特定病原体監督者

特定病原体監督者とは研究プロジェクトまたは研究計画の管理監督を行う責任者を指します。各特定病原体の研究プロジェクトや研究計画は特定病原体監督者による監督を受けますが、特定病原体監督者は該当する研究プロジェクトや研究計画に対して科学的および技術的な責任を持ち、特定病原体の使用承認を受けている個々の研究者に対して職務権限を有しています。特定病原体監督者は以下の各項に対して責任があります：

- バイオセキュリティ計画の方法を採用し、監督下にある特定病原体を取り扱う全ての人員が計画内容を理解して年に一度バイオセキュリティ訓練を受けるシステムを確実に実施する。
- 施設責任者に対して特定病原体の輸送、廃棄、および在庫状況の異常について報告する。
- 施設責任者に対して特定病原体の取り扱い許可の変更を求める（4.6.5 参照）。
- 施設責任者の求めに応じて、電子的な記録が行われていない訪問者名簿を提出する。
- 人員のアクセス承認の変更を求める。
- 施設責任者に特定病原体の最新登録パケットを提出する。

C.2.4 管理責任科学者

管理責任科学者は、特定病原体監督者および／または主任研究者が兼任することもできますが、C.6章とC.7章で述べるように特定病原体材料の管理と管理責任ならびに特定病原体材料の輸送に関して責任を持っています。

C.2.5 警備隊

ここでは、警備隊を雇っている場合、雇われている警備隊はどのような責任を持っているのかを説明してください。

C.2.6 地域の警察

ここでは、地域の警察と覚え書きを交わしている場合、地域警察はどのような責任を負っているのかを説明してください。

C.2.7 専門職員

規模の大きな実験施設では専門職員を雇うこともできます。これには安全監視センターに勤務して侵入検出システムを監視するセキュリティ関係の専門職員、建造物の構造セキュリティに関する専門職員、およびスパイ防止活動に関わる専門職員などが含まれます。

これらの専門職員の役割と責任に関しては、セキュリティ計画の中のこの項で詳しく説明しなければなりません。

C.2.8 パーソナルセキュリティ

パーソナルセキュリティに関する部門には必要とされる身元調査を行って人員を監視すること、および適切な時期に監視結果の裁定を行う責任があります。

C.2.9 バッジオフィス

バッジオフィスの人員は通常勤務者および訪問者に対してバッジを発行し、管理する責任があります。

C.2.10 情報セキュリティおよびネットワークセキュリティ

情報セキュリティおよびネットワークセキュリティには次の人員が関わります：

- 主任情報セキュリティ担当者は施設のネットワークと情報のセキュリティ対策に責任を有する。

- 中央および部門別の情報技術担当者は各人のネットワークセグメントと情報保護システムがネットワークと情報のセキュリティ対策通りに作動していることを確認し、職員に対して情報セキュリティおよびネットワークセキュリティに関して適切な訓練を受けさせる責任を有する。

- システム／ネットワーク管理者はシステムセキュリティを維持し、ハードウエアとソフトウエアを最新化し、ネットワークへの侵入に対処する責任を有する。

C.2.11 特定病原体へのアクセス承認を有する人員

特定病原体へのアクセス承認を持つ人員は、各人が有している他の義務に加えて以下に掲げる義務も有しています：

- 特定病原体を保有している間はそれを保護する責任。

- 特定病原体に関する情報を保有、保管している間はそれを口頭および電子的通信手段によって漏出しないように保護する責任。

- 訪問者の受入れや付き添いの方法を含め、特定病原体に関わる全てのセキュリティ関連手段を順守する責任（第5章5.8および5.9参照）。

- セキュリティ系統におけるインシデントおよび／または破壊行為の発生を適切な特定病原体責任者および施設責任者に報告する責任。

C.3 バイオセキュリティプログラムの基本

C.3.1 リスクアセスメント

このセキュリティ計画はリスクマネジメント手順に従って資産と資産に対して及ぶ可能性のある有害行動（危険性）について定義し、その結果発生する好ましくない出来事をセキュリティリスクに基づいて評価しています。リスクアセスメントとは、敵対者がわれわれにとって好ましくない事象を成し遂げ、その結果われわれにとって不利益が発生する可能性に関する評価を行うことです。これによって実験施設が直面する一連のリスクを明らかにしてその順位付けを行い、それによって施設管理の視点からどのリスクに対して防御あるいは軽減対策をとるか、どのリスクに対してはその必要がないかを決定することができることになります。このセキュリティ計画は、このようにして定義したセキュリティリスクの状況に基づいて作成したものであり、セキュリティシステムの枠組みとそれぞれのインシデント対応計画の組み合わせによって施設の保護と被害

の軽減を達成する方法を示すものです。

C.3.2 段階的保護

さまざまな資産は、それぞれ別のレベルの保護、管理責任、および管理を必要とします。最も高いレベルの保護は主要資産に対して行われるもので、その紛失、盗難、損傷、および／または不許可使用によって国家セキュリティ、および／または実験施設人員の健康と安全、および社会、環境、実験施設の業務に対して最も深刻な影響を与えることになります(高度リスク病原体など)。それに比べて、二次的資産に対してはやや軽度の防護措置が講じられますが、二次的資産とは中等度リスクを有する資産または、これが敵対者に利用されたときに重要資産へのアクセスの手段や、その代換えとして利用される恐れのある資産を指します。三次的な資産としては運用上の資産が含まれ、これに対する保護は二次的資産に対する保護よりも軽度の対策が行われます。このように、セキュリティシステムはそのレベルを段階的に変えて、最も高いリスク資産に対しては最高レベルの保護が行われ、想定されるリスクが重要な資産に接近するにしたがって必要なセキュリティレベルが段階的に増加します。

ここでは、施設内で重要資産、二次的資産、および三次的資産とされている資産が何かを示してください。

C.3.3 資産

C.3.3.1 特定病原体

特定病原体とは、CFR で定義されているように人、動物、または植物の健康や動植物製品に対して深刻な被害を及ぼす危険性のある病原体や毒素を指します。

ここでは、実験施設で保有している特定病原体を示してください。

C.3.3.2 機密情報

機密情報とは、その取り扱いがきわめて慎重に行われるべき情報で、公開したり、情報を聞いたり見たり所有したりすることに関して公の目的を持たない（すなわち必知事項ではない）人員に漏らしてはならない情報を指します。機密情報に対しては承認を得ていないアクセスを禁止し、合衆国情報の自由法（FOIA）によって公開が禁止されています。機密情報保護に関する詳細な内容については C.8 を参照してください。

機密情報に含まれるものには、特定病原体に関する情報、セキュリティ関連情報、特定病原体を用いて研究を行っている各個人に関連した人的資源関係の情報が含まれます。

C.3.3.2.1　特定病原体情報

以下に特定病原体に関する機密情報記録の例を示しますが、これらは施設責任者が保管する必要があります。また、機密情報は必ずしもここに示す例に限られるものではありません。

- CFR で説明されている記録に関する特定病原体関連情報として：
  - ・特定病原体にアクセス承認を受けている全ての個人名を示す最新のリスト。
  - ・特定病原体にアクセス承認を受けている人員に対する訓練記録。
  - ・特定病原体の在庫記録（由来と性状に関するデータ、および、何らかの異常があればその記録も含む）。
  - ・使用許可と輸送記録。
  - ・特定病原体保有実験室への訪問者名簿。
- セキュリティ関係および特定病原体情報が入力されているデータベース。
- 実験データの記録、または施設側の判断で審査や承認が必要であるとして制限されていたデータに関する記録。

C.3.3.2.2　セキュリティ関連情報

以下にセキュリティ関連の記録の機密情報の例を示しますが、これらは施設責任者が保管する必要があります。また、機密情報は必ずしもここに示す例に限られるものではありません。

- CFR で説明されている記録に関するセキュリティ関連情報として：
  - ・セキュリティ記録（自動アクセスコントロールシステムのデータ処理、セキュリティシステムの検査および保守記録、訪問者記録など）。
  - ・封じ込めおよびセキュリティに関するインシデント報告。
  - ・バイオセキュリティ計画。
- 施設の説明や設計図に関する詳細情報。特に制限区域や排除区域の設計や防護対策に関わる内容。
- 特定病原体および／または機密情報を取り扱う施設の脆弱性に関する詳細情報。
- 物理的セキュリティに関する詳細情報（セキュリティ関係のハードウエアやソフトウエアシステムの図面や解説など）。
- コンピュータシステムと使用手順の詳細情報。
- セキュリティ手順に関する情報。
- バッジデザインの情報。
- セキュリティシステムの性能試験結果および検査結果。
- インシデント報告と訓練行動。
- 外部の対応機関との契約およびそれら機関の訓練記録。

C.3.3.2.3　人的資源情報

人的資源情報には特定病原体を取り扱っている、または特定病原体へのアクセス承認を有している人員に関する全ての情報が含まれます。これには以下のものがあります：

- 自宅への連絡情報。
- 家族構成。
- 経済状況。
- 身元調査の記録。

C.3.3.3　重要業務資産

重要業務資産とは、もし破壊された場合には業務に著しい遅れが発生する可能性のある資産、破壊された場合に財政上の影響を引き起こす可能性のある資産、および、高度リスク病原体のセキュリティに直接関わる資産を指します。

ここでは、重要業務資産のリストを示し、各資産について簡単に説明をしてください。

C.3.4　脅威の定義

C.3.4.1　インサイダー

インサイダーによる脅威の分類に含まれるものに、施設内へのアクセスが認められている単独の非暴力的な個人によるものがあります。インサイダーとしては、排除区域や制限区域内のいかなる区域へも単独でアクセスすることが承認されている人員が考えられます（これらの区域の詳細に関しては C.4.2 と C.4.3 を参照）。悪意を持ったインサイダーの目的は中等度リスクまたは高度リスク病原体の窃盗、破壊または漏出、もしくは気づかれないうちに［*ここに実験施設名を記入*］において重要な意味を持っている資産の窃盗や破壊を行うことです。インサイダーは発覚を避けるためにはいかなる窃盗行為を働いても途中で中止するものと思われます。施設へのアクセス承認を得たことでこの人物は施設とその運転システムに関してきわめて多くの知識を入手したことになります。インサイダーは犯行を行うために最も適した機会を見極めることができます。

C.3.4.2　アウトサイダー

外部の敵対者であるアウトサイダーはその目的を達するためには武力を用いたり、秘密活動を行ったり、詐欺行為を行うことがあります。武力を用いる場合、敵対者はその行動や意図を隠すことはしません。すなわち敵対者は単純に施設のシステムや人員に対して攻撃を行います。秘密活動を行う場合、敵対者は目的を達成するために実験施設内へ気づかれずに侵入しようとします。

詐欺的な手段を用いる敵対者は偽造証明書やその他の手段によってアクセスが承認されていると見せかけて目的を達成しようとします。知能的で訓練を積んだ敵対者はこれら三種類の戦術を組み合わせて、目的とする資産の窃盗、破壊、漏出を行おうとすることは明らかです。アウトサイダーがアクセスできるのは公開情報のみですが、手工具を装備していたり、武装していたり、暴力的な行為をとる可能性もありますが、自滅的行為はとらないと思われます。

C.3.5 防御戦略

C.3.5.1 インサイダーに対する防御

インサイダーによる敵対行為に対しては、従来から行っている物理的防御対策、パーソナルセキュリティ計画、厳格な付き添いルール、および材料の管理と管理責任を基本的な要素としたセキュリティ戦略によって防御を行います。病原体に関する管理責任が困難だとすれば、ますます重要になることは、職員その他、病原体へのアクセスが承認されている人員に対する信頼です。生物剤に関しては距離を置いてその存在を検知することは技術的に不可能であり、在庫管理システムによっても必ずしも材料の盗難や流用を明らかにすることができない場合があります。そのため、インサイダーによる脅威は生物学研究実験室にとって、対処することがきわめて困難な問題です。

インサイダーによる微生物の窃盗や流用を物理的セキュリティシステムによって防ぐことはきわめて困難です。したがって、生物学研究施設においては危険性の高い病原体や毒素へのアクセスが承認されている人員に対する信用度や信頼性を高めるため、あらゆる可能性を試みるのが最もよい方法となります。

注意しなければならないことは、外国籍の人員に対しては、調査が及ぶ年数の間合衆国に居住するまで、合衆国国民に対して行われるような行き届いた調査を行うことができないことです。この時点までに関しては、本来は身元調査が必要とされる職にある外国籍の職員に関しては、合衆国国民に比べて危険性が高いことになります。外国籍の人員による共謀行為に対しては、他の全てのインサイダーの脅威と同様に防御対策をとります。

C.3.5.2 アウトサイダーに対する防御

アウトサイダーに対する防御戦略は承認を受けていないアクセスの発生を検知すること行われますが、このようなアクセスはバイオセーフティ封じ込め実験室や他の重要資産が置かれている区域へ通ずる経路で行われます。検知活動は適切な時間に行い、対応組織を招集します。これらの対応組織としては、警備隊または地域の法執行機関（LE）があります。地域の法執行機関の活動を容認する場合は、覚え書きを交わして対応時間や法執行機関が現場に到着した後の活動（生物材料の封じ込めを行わなければならない事態が発生する可能性があるため）などに関する条件を

覚え書きに従って実施することが重要です。

適切な時間内にアウトサイダーを検知するためにしばしば用いられる手法は、病原体やその他の重要資産が保管されている物理的な場所のセキュリティ対策を強化し、そのような区域へのアクセスの管理を行うことです。

C.4 物理的セキュリティ

物理的セキュリティのシステムでは、決められたセキュリティ区域へのアクセスに正当な必要性があるとして承認を受けた人員のみにアクセスを制限します。

C.4.1 資産保護区域

資産保護区域は実験施設の最外部境界線の内側です。このセキュリティ区域内で損傷、破壊、施設付属資産の盗難を防ぐ方法を実行します。

ここでは、資産保護区域はどのように区別されているかを示してください（外周のフェンス、など）。もしあれば、資産保護区域へのアクセスにはどのような証明が必要かを示してください。

ここでは、施設内で資産保護区域となっているのはどの区域かを示してください。区域内にある資産は何かを示してください。

C.4.2 制限区域

制限区域は資産保護区域内に設置されたセキュリティ区域で、境界を明確にするための障壁を設けて区域の周りを囲っています。多くは建物の周囲が制限区域の外周となります。

ここでは、制限区域に対してどのような物理的セキュリティ対策を実施しているか、制限区域へのアクセスにはどのような証明が必要かを説明してください。

ここでは、施設内で制限区域となっているのはどの区域かを示してください。区域内にある資産を示してください。

C.4.3 排除区域

排除区域とは制限区域と同様に安全管理区域の一つで、障壁を設置して境界を示し、該当区域を囲みこみ、これによって制限区域を越えてアクセスすることを制限しています。多くの場合、特定病原体の置かれる実験室や保管区域が排除区域とされます。

ここでは、排除区域に対してどのような物理的セキュリティ対策を実施しているか、説明してください。排除区域へのアクセスにはどのような信用証明が必要かを説明して下さい。

ここでは、施設内で排除区域となっているのはどの区域か、区域内にある資産は何かを説明してください。

C.4.4 特定病原体の長期保存

ここでは、特定病原体の保管にあたって施錠した保管容器（フリーザー、冷蔵庫など）を用いる場合に、設置区域に違いはあるかを説明してください。違いがある場合は、ここで設置区域を示してください。

C.4.5 セキュリティ作業

C.4.5.1 入室時間

ここでは、全ての承認人員が24時間のアクセスが承認されているのか、または作業者によってアクセス可能な時間帯が異なるのかを以下の例を参考にして説明してください。例：月曜日～金曜日 午前6時～午後6.時、月曜日～日曜日 午前6時～午後6時または1日24時間、週7日。

C.4.5.2 訪問者名簿

ここでは、訪問者が署名をする場所は、施設内のどこの部屋／区域であるのか、またどのような情報を記入するのかを説明してください。付き添い者の署名も必要とされるか、についても説明してください。

C.4.5.3 車両

ここでは、敷地内への駐車が認められるのは誰かを説明してください。駐車にはその他の制限があるかを説明してください。例えば自家用車は積み下ろし区域への立ち入りが制限されるか、などを説明してください。自家用車には駐車ステッカーまたはプラカードの設置が必要かどうかを説明して下さい。訪問者用駐車場の管理をどのように行っているかを説明してください。

C.4.5.4 追従入場

「追従入場」とはある個人が、電子セキュリティ装置（IC カードなど）によって立ち入り制限が行われている区域に入場する際、自分自身が保有している解錠手段を使用せずに他の人の後に続

いて入場する行為を指します。いかなる制限区域または排除区域でも追従入場は禁止されています。追従入場という用語は訪問者などが正式の入室許可を受けて付き添い者と一緒に入場する場合には適用せず、この場合は別途付き添い／案内役の手続きに従って入場を確認します。

C.4.5.5 アクセスの変更

ある個人のアクセス承認を特定病原体の取り扱いの必要性のない業務に変更して再登録する場合、別の特定病原体へのアクセス承認を必要とする再登録を行う場合、または新しく特定病原体のアクセス承認を必要とする再登録を行う場合には、その人員のアクセス承認に関する管理記録を変更します。特定病原体へのアクセス承認に何らかの変更を行ったときは、施設責任者はCDC/APHIS/特定病原体プログラム（SAP）へ報告します。ある個人の特定病原体へのアクセスを終結させた場合には施設責任者は直ちにCDC/APHIS/SAPへ通報し、CDC SAP/APHISにアクセスを終結した理由についても説明しなければなりません。ある個人がある制限区域へのアクセスの必要性がなくなったときには、この変更についても記録し、電子的アクセス手段を最新化します。

C.4.5.6 荷物の検査

ここでは、CFRによって特定病原体もしくは毒素が用いられていたり保管されている区域内へ持ち込んだり持ち出したりする物品に何らかの疑いがもたれる場合には、事前に全ての荷物を検査する必要があることを説明します。

ここでは、疑わしい荷物の検査に関して、具体的に詳細に記載します。例えば、検査は集配担当部門で行うのか、実験室の入り口で行うのか、何故検査をするのか、漏出か、損傷か、その他か、荷物の検査を行うのは誰かなどです。

職員は次のような郵便物に対しては疑いを持って接しなければなりません。

- 受取を予想していない、もしくは差出人に心当たりがない郵便物
- 宛先がもはやその部署にはいない人である、もしくは古い部署宛ての郵便物
- 差出人の住所がない、もしくは不正と思われる住所の郵便物
- 大きさから考えて重量が異常、重さに片寄りがある、もしくは形が不自然な郵便物
- 「親展」や「部外秘」など条件付きの裏書きがある郵便物
- 針金が突き出ていたり、奇妙な臭いがしたり、シミが付いている郵便物
- 差出人の住所と消印の都市名や州名が一致しない郵便物

もし、何らかの疑わしい郵便物と接触した場合は、その宛先のないまたは疑わしい郵便物を［*ここに施設の名称を記入する*］で発見したのがいつであれ、または自分が疑わしい小包の受取人であった場合でも、それを開いたりしてはなりません。以下のいずれかに電話連絡をしてください。

状況が緊急を要すると思われるときは［*ここに緊急電話番号を記入*］に電話し、状況の緊急度が低いと思われるときは［*ここに非緊急電話番号を記入*］に電話をします。電話では疑わしい郵便物の置かれている場所とその状態を伝えてください。

緊急対応者の到着を待つ間は以下のガイドラインに従ってください：

1. それ以上は問題の小包や物品に触れない。
2. 問題の小包や物品を隔離し、隣接区域から人を避難させる。
3. 問題の小包や物品に接触した人全員が石鹸と冷水で十分に手を洗う。

C.5 パーソナルセキュリティ

C.5.1 職務によるリスク分類

C.5.1.1 低度リスク職

低度リスク職には、実験施設や研究活動に対する重要性が限定的な職、および業務の質や効果が限定的な職が含まれます。

C.5.1.1.1 身元調査

ここでは、この分類に当てはまる人員に対して施設として行っている調査内容について説明してください。

C.5.1.1.2 職務分類

全ての［*ここに施設名を記入*］の職員、請負業者、およびビジター職員で、中等度リスクまたは高度リスクの分類に合致しない人員は低度リスク職にあると考えられます。個人的な、または予定していなかった訪問者にはリスク分類は当てはめません。

ここでは、どの職務分類が当施設では低度リスク職と考えられるか、説明してください。

C.5.1.2 中等度リスク職

中等度リスク職には施設の目的遂行にとって中程度の重要度を持っている職域が含まれ、業務責任の重要な役割が与えられています。中等度リスクの職域リスクレベルには、特定病原体に関連した職域のほとんどが含まれます。

C.5.1.2.1　身元調査

ここでは、中等度リスク職の人員に対しては、通常低度リスク職に比べて、より包括的な身元調査を行うことを説明します。中等度リスク職の分類を特定病原体へのアクセスが必要な人員に限定する場合は、審査は米国司法省リスクアセスメントの追加要求事項に限定されます。これらの職域の人員は定期的な再調査の対象となることを説明します。

ここでは、この分類に当てはまる人員に対して行っている調査内容について説明します。

C.5.1.2.2　職務分類

ここでは、どの職務分類が当施設では中等度リスクと考えられるか、説明してください。

C.5.1.3　高度リスク職

高度リスクの職には広い観点からの責任と権限を有する職務が含まれ、特に当該機関や研究計画にとって重要な職です。

C.5.1.3.1　身元調査

ここでは、高度リスクの職域の人員に対しては、さらに包括的な身元調査および／またはより厳格な権限賦与の審査が行われることを説明します。また、これらの職域の人員も定期的な再調査の対象となることを説明します。

ここでは、この分類に当てはまる人員に対して施設として行っている調査の内容について説明してください。

C.5.1.3.2　職務分類

ここでは、どの職務分類が当施設で高度リスクと考えられるか説明します。

ここでは、ある職員が機密情報にアクセスすることが可能な場合、この職員は高度リスク職にあると考えられることを説明します。ここでは、一般的には、これらの職は職域階級の最高位の職、および万一漏出した場合には施設の脆弱性が明らかになるような情報にアクセスすることのできるセキュリティスタッフまたはIT スタッフで地位の高い者が、高度リスク職と考えられることを説明します。

C.5.2 再調査

施設責任者は、施設内に特定病原体へのアクセスを必要とする人員がいる限り、5年ごとにCDC SAP/APHISのアクセス許可の更新を求めなければなりません。

ここでは、どの職に対して定期的に身元調査を繰り返し行っているのか、もし再調査を行っているなら説明してください。再調査はどの程度の間隔で行っているか、説明してください。

C.5.3 アクセス制限

C.5.3.1 職員

特定病原体へのアクセスを必要とする人員はCDC SAP/APHISのアクセス承認を得ていなければなりません。

ここでは、制限区域または排除区域に対して他に何らかのアクセス制限を実施している場合はそれについて説明してください。例えば、身元調査はある人員がある区域内へ単独で立ち入ることが承認される前に完了させることになっているかどうか説明してください。ある人員がアクセス承認を受ける前に行わなければならない要求事項がある場合、それを説明してください（年ごとの訓練やワクチン接種など）。

C.5.3.2 訪問者

大学関係者、請負業者、学生、特別研究員、客員研究員、実験室訪問者、取引業者、集配業者、その他の訪問者に対しては、区域内への立ち入り期間や作業の性質上、区域内への定期的アクセスは許可しません。訪問者の制限区域内（非公開区域）への立ち入りには、身元調査を完了してアクセス承認を有し、かつ必要事項を熟知した人員による付き添いが常時同行することとします。訪問者は、施設内では訪問者バッジを着用し、全ての訪問者名簿に署名し、付き添い者と同行し、全ての施設の方針と運用事項を順守し、禁止物品には触れないことが求められます。

注：施設／セキュリティ管理者は、訪問者が施設内の通常の人員に必要とされているのと同等の身元調査結果を有し、通常の人員が施設へアクセスする際に必要なCDC SAP/APHIS審査による承認を有し、かつ、区域内で行う作業に合理性が認められる場合には当該訪問者の制限区域内への単独アクセスを許可することが許されます。

C.5.3.2.1　受入れ者の責任

施設内に受入れ者がいなければ訪問者または訪問者グループとして施設を訪れることはできません。受入れ者は標準のバッジ保有者でなければなりません。受入れ者には訪問者に対してアクセス制限、禁止物品その他の施設の方針と運用方法について理解させる責任があります。受入れ者は訪問者に自分自身が付き添うか、または標準バッジを有して訪問区域内の付き添いを認められている他の人員が付き添いをするよう調整することができます。

ここでは、訪問予定者をあらかじめ連絡する必要がある部門または人員（例：建物警備係、受付、駐車係員、その他）、およびその連絡に必要な情報（訪問者名、到着日時、滞在期間など）を示してください。

C.5.3.2.2　付き添い

訪問者の付き添いは標準バッジを有し訪問区域への入室を認められている人員が行わなければなりません。

ここでは、事務部門や実験室など、区域によって訪問者対付き添い者の割合を変えているか説明してください。また、訪問が認められる時間に規定がある場合はそれを説明してください。訪問者に対して付き添いが不要な区域がある場合は、それも説明してください。

C.5.4　外国籍の人

米国国務長官によって国際テロリズムの支援国家と指定された国の国籍を持つ外国人は、付き添いの有無にかかわらず特定病原体取り扱い区域へのアクセスは認められません。

C.5.5　バッジシステム

全ての職員および請負業者に対して「標準」バッジを発行します。訪問者に対しては、これと異なる訪問者バッジが発行されます。バッジには着用者名、使用施設名、着用者の写真（標準バッジのみ）および有効期間が明示されています。

ここでは、標準バッジと訪問者バッジに記入される内容について、記録される情報の内容や電子的アクセスコントロール（通所は標準バッジに行われる）などについて正確に説明してください。また、例えば職員と請負業者に対しては 5 年間、訪問者に対しては訪問期間の限定など、バッジの有効期間についてもここで説明しなければなりません。バッジ着用についての何らかの例外（実験室内やその他の場所などで、バッジを着用することで安全性に問題が発生する可能性がある場合など）があればそれについてもここで説明しなければなりません。また、標準バッジを保有し

ている職員がバッジの持参を忘れた場合、紛失もしくは盗難が発生した場合の対処についてもここで説明しなければなりません。

C.6 材料の管理と管理責任

ここで取り上げる「材料」は特定病原体の保有状況に関する材料です。この「材料」には臨床検体とワーキングストックは含みません。

C.6.1 材料の管理

全ての特定病原体材料はキャンパス［*実験施設に複数のキャンパスがある場合はここにキャンパス名を記入*］、建物番号、階、および部屋番号を明らかにした特別の実験室に保管します。材料の保管は、保管庫（フリーザー、冷蔵庫、金庫室など）に収納して施錠し、アクセス制限を行います。

実験室での在庫検査は在庫記録と実際の材料の状況が一致しているかを確認するため、必要に応じて行います。何らかの不一致が認められた場合は施設責任者に報告します。この在庫検査は実験室のスタッフが自発的に、または施設責任者の要求によって行われます。

実験室における材料保有状況に何らかの変化があった場合は材料の「輸送」と判断され、これは材料安全移動部門への報告対象となります。在庫記録と材料輸送の記録は一致している必要があります。

試験材料、診断材料および臨床検体の管理は材料在庫管理の対象とはなりません。しかしながら、臨床検体や診断材料から得られた分離株が特定病原体であると同定され、かつこれらの分離株を将来の使用に備えて保存した場合には、この分離株は保管と同時に在庫管理対象として追加します。

在庫管理の対象としては取り扱わないが特定病原体を含んでいる可能性のある検体は、必要性がなくなり次第必ず滅菌廃棄します。しかし、在庫調査した材料を滅菌廃棄した場合には在庫記録はそのように書き改め、在庫記録を破棄することはしません。

C.6.2 管理責任

特定病原体を使用したり保管したりしている各実験室内では、管理責任を持つ科学者が材料の在庫記録を管理し、材料の使用状況を監視し、材料へのアクセスを監督します。特定病原体材料に関係したことがらでは、その内容にかかわらず管理責任科学者が施設責任者への連絡窓口となります。管理責任科学者は通常はその材料を用いて作業を行っていることが多い主任研究者または

上級研究科学者が兼任し、特定病原体監督者自身または特定病原体監督者から指名を受けた他の人員が務めます。実験室が複数の特定病原体を用いて研究を行っている場合には、病原体ごとに管理責任科学者をおくことも可能です。管理責任科学者には代替え要員をおくことができますが、それがない場合、管理責任者は 1 名に限られます。管理責任科学者は特定病原体の在庫の変化に関しては、特定病原体監督者および施設責任者に、確実に逐一報告しなければなりません。

同じ実験室の他の人員は材料が保管使用されている区域にアクセスすることが可能ですが、管理責任科学者は材料が保管されているフリーザーや保管庫を施錠してその鍵を所持します。管理責任科学者はその他の人員に鍵を貸し出すことはできますが、使用簿を保管します。保管庫から材料を取り出したり追加したりしたことが報告された場合、管理責任科学者は在庫記録を改めます。

C.6.3 在庫記録

材料の在庫記録は様々な記録様式の中から管理責任科学者が決めた方法によって保管します。記録様式としては電子データベース（MS Access や SQL Server など）、集計表ファイル（MS Excel など）の他、日誌やカード式ファイルを利用した手書きの記録様式を用いることも可能です。この在庫記録には研究目的を記入したり CFR では必要とされていない情報を記入したりすることも可能です。在庫記録には特定病原体以外の生物材料の記録をすることも可能ですが、特定病原体材料の記録は識別して容易に報告できるようにしておきます。重要なことは、在庫記録は一ヶ所にまとめ、それがバイオセキュリティ報告の要求事項および追加目的を満たしていることです。

特定病原体材料の在庫記録は機密情報として扱い、情報セキュリティ部門の規定関連情報と考えられます。

在庫管理の*記録*の中の各記録項目はそれぞれ個別の項目とし、単独の品目の記録（バイアル、アンプルなど）または同一の特定病原体を複数の容器としてあるかなどを記録します。後者の場合、おおよその数量（重量、容量、数など）についても記録します。

各在庫記録（データベースなど）を保存している情報には、最小限、42 CFR 73.15 (b)によって必要とされている情報、および 7 CFR 331.14 (a) (4)と 9 CFR 121.15 (a) (4)と一致する情報として次の項目を盛り込まなければなりません：

- 定病原体の名称と株名
  - 特定病原体の由来：
    - 分離株をいつどのようにして入手したか。ヒト由来株については検体提供者に関する特定の個人情報が必要ではないことは 42 CFR 73 に示されていますが、研究目的で記録に残すことは可能です。