acquiring hazardous materials, the key is in preventing insider incidents, the most probable cause of a security breech, is discussed in the Personnel Consideration section.

## Summary

The intent of this chapter is to give a broad overview of the security management considerations for biotechnical/biomedical facilities or institutes. It has not been intended to set policy, replace current SOP's, or become an "off the shelf" standard operating procedure. Rather, it has provided information that can serve as a conservative starting point for those looking to establish or redesign their facility's or institute's security management concept in order to meet current, new, and emerging threats.

Security management, the process of developing a plan to protect assets, ensuring individual employees are protected, maintaining technical countermeasures, and integrating operational security into daily activities may seem to be a concept that could rapidly overtake the business or academic necessities of a facility or institute. However, in the past decade, the world has changed and these aspects of security are more often becoming necessities. Professional activists, bioterrorists, and competitive intelligence agents are rapidly becoming threats in the new century. Only through the development of a staffed endorsed, management supported, integrated security management program can these threats be properly addressed. When the threats are properly addressed, the security program they will be recognized as an asset, not burden.

## APPENDIX

### Table 1

Overview of Security Requirements Analysis. (Hamilton E, 2000).

A. Identify the assets to be protected.
B. Assess the value of the assets.
C. Assess the potential threats.
D. Assess vulnerabilities.
E. Assess risks.
F. Determine countermeasures options and estimate costs.
G. Make risk management decisions.

### Table 2

Explanation of Components Considered in a Security Requirements Analysis (Hamilton E, 2000).

A. Assets to be protected may include:
    - People.
    - Material (biohazardous, chemical, radiologic, etc).
    - Intellectual Property/ Products/ Processes.
    - Equipment/ Facilities.
    - Corporate/ Institutional Reputation and Mission.
    - Records/ Computer Databases/ Personnel Sensitive Information.
B. An institute can then assess the value of its assets by asking the following types of questions:
    - What is the impact of loss, damage, compromise, or interruption of operations?
    - What does the facility stand to lose?
    - What does an adversary stand to gain?

- What is the impact of loss on the institutes mission, or in terms of national threat (i.e., theft of biohazardous material)?
- What is the potential impact on peoples' lives?
- Can the asset be replaced or repaired, and at what cost (not just monetary consideration)?

C. Determine who constitutes the most likely potential threat, this may include more than one type of category:
   - Extremists/ Fanatics (right wing "animal rights" activists)?
   - Criminals/ Vandals?
   - Political Activists (right wing "right to life" activists)?
   - Drug/Alcohol/ Psychologically Impaired?
   - Disgruntled Employees/ Students?
   - Terrorists/ Racists (domestic and international)?

     Keep in mind they may be:

     - Insiders.
     - Outsiders.
     - Both (Collusion).

D. Part of assessing vulnerabilities making an integrated assessment of the following aspects:
   - What weaknesses could be exploited to result in loss, damage, compromise, or disruption of assets at your institute?
   - Location of facility: is it in a high threat area, what is the accessibility of facility, what is the proximity of other buildings and the nearness of response forces, vehicle access roads?
   - How may the adversary gain access or otherwise achieve their goal: forced entry, covert entry (in collusion with insider) authorized entry (insider), extortion of insider, unescorted walk-in, stay behind after hours, arson, diversionary tactics?
   - Determine site specific requirements of the physical security system by assessing:
     - Physical aspects (i.e., perimeter barriers, building construction and layout, facility layout, access roads, response vehicles and equipment),
     - Technical aspects (i.e., existing physical security systems and equipment, communications, power and signal distribution infrastructure, lighting),
     - Operational aspects (i.e., personnel, concept of operations).

E. To assess risks include or consider the following:
   - The motives/goals of your adversaries (greed, revenge, sabotage, societal unrest, vandalism, ego, opportunity, national harm, propaganda, theft, perceived right, no known reason).
   - The adversary's level of knowledge, capability, dedication, skill, and potential that they have "inside" assistance.
   - Prioritize assets according to severity of impact of loss, damage, compromise, or disruption of your mission goals and values.
   - Select most realistic threat to that asset.
   - Select most realistic vulnerability to that asset.
   - Determine the probability of occurrence, probability is a function of vulnerability and threat to the asset.

F. Options for countermeasures:

- Do nothing.
- Upgrade, augment or replace existing security.
- Modify concept of operation.
- Retrain or re-equip personnel.
- Relocate assets to a more secure site.
- Re-evaluate physical security objectives.

## References

"Aids activists vs. PETA" (2001). University of Minnesota School of Public Health. *Biostatistics.* http://www.biostat.umn.edu/~carlton/PETA.html. Online.

Department of Health and Human Services Centers for Disease Control and Prevention (2001). *Biosafety in Microbiological and Biomedical Laboratories (BMBL) 4th Edition.* "42 CFR Part 72." Online. http://www.cdc.gov/od/ohs/biosfty/bmbl4/bmbl4toc.htm.

(DTRA) Defense Threat Reduction Agency (2000). "Enhancing the Security of Dangerous Pathogens Workshop." Albuquerque, NM.

"Fitness for Duty" (2001). Florida State University Employee Assistance Program. http://www.eap.fsu.edu/guidelines.html. Online. 27

Getty, J (1996). "The Tragic Hypocrisy of 'Animal Rights'." *Wall Street Journal.* Online. Americans for Medical Progress Educational Foundation Articles. 13

Gillis, J (2001). "Scientists Accused of Theft." New York Times, A18.

Hamilton, E (2000). "Risk Management In the Approach to Physical Security Planning." Obolensk, Russia.

(ICA) International Crime Prevention Through Environmental Design Assosication. (2001). http://www.cpted.net. Online.

Jopeck, E J (2000). "Five Steps to Risk Reduction." *Security Management.*

Long, J W (2001). "Background Checks Step by Step." *Security Management* 72-78.

Macy, R (1998). "Two Men Arrested with Anthrax." *The Associated Press.* http://archive.nandotimes.com/newsroom/ntn/nation/021998/nationt_20801_noframes.html. Online.

McShane, W J (1999). "Raising Security Awareness." *Security Management*: 29-30.

Myatt, P B (1999). "Going in for Analysis." *Security Management*: 75-79.

Strauchs, J J (2001). "Which Way to Better Controls?" *Security Management*: 93-100.

Verhovek, S Yoon, (2001). "Fires Believed Set as Protest Against Genetic Engineering. *New York*

*Times*. Online. America Online. 23

Webster (1992). New Webster's Dictionary and Thesaurus of the English Language. "Security."

---

Citation:
Chris Royse & Barbara Johnson - *Security Considerations for Microbiological and Biomedical Facilities*, Anthology of Biosafety V - BSL4 Laboratories, Chapter 6 (2002), http://www.absa.org/0200royse.html.

# 微生物学および生物医学施設のセキュリティ問題

Chris Royse & Barbara Johnson 著

## 序文

近年では、病原体を用いて研究し、それを保管しているバイオメディカル（生物医学）研究所および施設における、セキュリティ・プログラム導入の妥当性と必要性についての問題が増加している。懸念の大半が集中しているのは、セレクト・エージェント（特殊病原体）やBSL-4病原体を取扱い、保管している施設である。いくつかの例では、1）動物保護活動家による犯罪行為が見られたこと、2）知的財産権や情報、特許材料や製法、および、業務上の機密情報を保護する必要が生じたこと、3）個人や組織集団が、生物病原体を犯罪やテロに利用する目的で入手しようとする可能性が認識されるようになったことなどの理由から、セキュリティの強化、保護対策、および規則が公表され実施されるようになった。

このような様々な懸念は、次に示すようなバイオテクノロジー産業界の幅広い機関に当てはまる：たとえば、動物飼育・繁殖施設、動物実験を行う研究機関、危険な病原体を用いて研究を行う機関、病原体保管施設、および、製薬企業やバイオテクノロジー企業などである。また、診断検査施設、医療センター、および病原体を用いて研究を行う大学、さらに、病原性物質の取扱い、輸送、あるいはそれを用いて他の形式の作業を行うその他の業種などにも、これらの懸念が当てはまることがある。病原体を取扱う可能性がある組織の多様性を考慮すると、すべてのニーズに対する単一の解決法は存在しないことが明らかになる。病原体を用いて業務を行う準備として、それぞれの施設で生物学的安全性（biological safety）のリスク評価（risk assessment）が行われるのと同様に、セキュリティのリスク評価も実施されるべきである。従って、それぞれの組織が、そのリスク評価、問題と解決法の再評価、任務上の必要性と制約の考慮、および許容できるリスク（acceptable risk）の程度に基づいて、セキュリティ・プログラムを作成し導入することになる。ただし、この章では、許容できるリスクや解決法の要件の定義づけ、あるいは方針の策定を目的とはしていないことを強調しておく。

この章の目的は、セキュリティ・プログラムの要素の候補として挙げられる項目に関する情報と、それぞれの施設におけるセキュリティ上のニーズを特定するための、意志決定マトリックス開発用ツールを読者に提供することである。一連の解決法そのものではなく、幅広い範囲の研究所や施設に共通して適用できるような、意志決定において考慮すべき事項一式の提供を意図している。

暫定訳：バイオセーフティ管理室
2006年3月

成功を収めるような、費用対効果の高い、セキュリティ・プログラムを定義するための、系統的で合理的な方法を開発する試みとして、この章では次のことを検討する：

- セキュリティ管理の概念
- セキュリティ計画の立案
- 人事面の考慮事項
- 技術面の考慮事項
- 運用面の考慮事項

## セキュリティ管理の概念

セキュリティという言葉、つまり「危険や不安からの開放」（Webster, 1992）は、危害を加えようとする側だけでなく、研究所や施設の中で保護サービスを受ける側からも否定的な意味で捉えられることが多い。多くの人にとってセキュリティとは、施設への立ち入り、材料の使用、情報交換、そして時には同僚との接触が、柵、守衛、施錠、立入制限区域、あるいは人を隔離するために考えられた他の手段によって制限されることと同義語として受け止められている。しかし適切なセキュリティ管理は必ずしも、科学者の毎日の活動に過度に干渉しないし、専門的で快適な環境で研究を行うことの妨げとなはならないものである。スタッフと協議し、自らの施設にとって適切な水準のセキュリティを決定し提供すること、そしてそれを監督することは、最終的には研究所や施設の管理者の役割である。

「セキュリティ管理の概念（Security Management Concept）」とは、合理的で費用対効果の高い、物理的セキュリティ・プログラム戦略を開発し、特に重要な施設財産を保護するためにデザインされた系統的過程である。このシステムにおいては、プログラムの資産のうちで実際に測定可能なもの（つまり、職員、製品、特許、機密および職員に関わる個人的情報、および危害物質）と、眼に見えない重要な任務上の機能（研究の自由、協力、および個人の権利）とが考慮されなければならない。この過程の一部として含まれるのが、管理者が受け入れるだろうリスクのレベルに応じた対策（予防的手段）の選択である。

成功するバイオセーフティ・プログラムの主な構成要素の１つが、リスクを特定し、事故／事例（事件）を予防するための措置を取ることであるのと同様に、適切なセキュリティ管理の鍵は、有害な事例（事件）の発生するリスクを特定し、それを軽減することにある。セキュリティに関しては、バイオセーフティと同様、研究施設そのものから「諸経費あるいは間接予算」として資金を提供されることが多い。そのためセキュリティ管理は、資金調達をめぐる避けがたい競争のため、それでなくとも不足している資金という制約の下で実施されるのが一般的である。各種施設や研究所のセキュリティをどのように管理すべきか理解する最良の方法は、連邦、州、地方、および企業レベルにおける既存のセキュリティ要件を明らかにし、保護される

べき施設や研究所の任務を理解することである。生物学的材料が関わるセキュリティに関しては、規則やガイドラインはほとんど確立されていない(http://www.cdc.gov/od/ohs/lrsat/regmat.htm, 2001)。多くの研究所がそれぞれ独自にそれぞれの機関のニーズを正確に反映し、それに対処するセキュリティ計画を策定している。これは、必ずしも悪いことではない。研究施設の種類、任務の目標、資産、およびその他多くの要素は多種多様であるから、それぞれの研究所がニーズに合わせたセキュリティ計画を立てられるということは、おそらく有益なのである。

セキュリティ管理は、一連の技術的な装置や手法を設置するものであると同時に、ある心理状態を確立するものでもある。つまり、有害な事例が起きるまでは、必要なものとして受け入れることが困難な概念であり、事例（事件）が起きてしまった後では往々として、損失を防止あるいは軽減させるための適切な対応を、十分迅速に取るには遅すぎることが多い。セキュリティ管理は費用便益分析である。何を守る必要があるか、何を犠牲にできるかが明確に示される。よく練り上げられたセキュリティ管理概念は、人事、技術、および運用に関する問題を考慮している。また、セキュリティ計画の立案は、施設や研究所に関する意志決定の責任者が、それぞれの施設の資産の状態、脆弱性、リスク因子、現行の予防手段と獲得可能な予防手段、および、損失の可能性（行動した結果、または行動しなかった結果）について理解することを助ける。

## セキュリティ計画

様々な財産物件が危険にさらされることから、セキュリティ・ワーキンググループの設置に関するひとつのモデルでは、主要な関係者の間での相互に影響しあう関係や責任の部分的な重なりを求めている。調和の取れた包括的セキュリティ計画の作成は、その手法において学問的でなければならない。優れた計画に必要なものは、開放的なコミュニケーション、協力する関係者の教育、セキュリティ担当者とその他のスタッフの合同参加、設計と要求の両面の歩み寄り、および継続的な更新であり、これを実行することで、職員とセキュリティ専門家とが共に１つのチームとしてまとまる機会が得られる。主要な関係者に含まれるのは、セキュリティおよびバイオセーフティ担当部門や、緊急対応機関（地域の消防署と警察）、および科学研究主任者やプログラム管理者であるが、それだけに限らない。セキュリティが必須となる項目の優先順位に応じてチームのメンバーを拡大し、労働衛生管理者、産業衛生士、放射線安全管理士、獣医、広報活動担当者などを含むことが考えられる。生物学的材料の保護に関してセキュリティが問題となる場合、その機関のバイオセーフティ・プログラムに適切な構成要素として組み込むまではいかないにせよ、セキュリティ計画と密接に調整しなければならない。チーム参加者の一部は、評価プロセスにおいて、主としてセキュリティを重視した技術的役割と方針的役割を果たし、もう一方の参加者は、現在の能力と任務上の要求に関して技術情報を提供することになる。編成されるチームは、上級管理者の目的と機関の任務によって異なるが、プログラムレベルでの連続性を維持するためにもチームの中核は相当の一貫性を保っていなくてはならな

暫定訳：バイオセーフティ管理室
2006年3月

い。セキュリティ面が活動の中心となるが、実行に関する最終意志の決定においては、上級管理者に対し合意内容と多く聞かれた意見とを提供すべきである。

**セキュリティ管理はセキュリティリスクの管理**

セキュリティ管理とセキュリティリスクの管理は同義であり、生物工学と生物医学の施設や機関において研究あるいは製造の責任を負う人が、有害なセキュリティ事象が起こる可能性を緩和できるようにするコンセプトである。セキュリティとセキュリティリスク管理は、セキュリティリスク分析から始まる。適切なセキュリティリスク分析に関する提案には様々な形式があるが、どれも本質的には同じ要素で構成されている（クイックリファレンス・ガイドは付録の表IおよびII参照）。セキュリティリスク分析概要の良い例は、Jopeckの論文"Five Steps to Risk Reduction"（Jopeck, 2000）に見ることができる。Jopeckの主張では、セキュリティリスク分析は次の諸段階で構成されている（同じく付録の表1参照）。

- 資産評価
- 脅威評価
- 脆弱性評価
- リスク評価
- 対抗手段

*資産評価*

資産には次のものが含まれる。ただし、施設や機関が所有するものだけに限定されない。

- 物理的に存在する土地。
- インフラストラクチャ（空調、電力、水道、下水など）。
- 装置および材料。
- 研究、開発、製造のいずれであれ、情報および知的財産。
- スタッフ。

セキュリティ作業グループは、施設や機関が保有するこれらのものを識別しなければならないが、これらは資産であり、従って潜在的目標である。1つのテクニックは、「プログラム管理者、施設管理者、およびコンピュータシステム管理者」（Jopeck, 2000）と面接することである。資産には、重要度の最も高いものから最も低いものまで優先順位を付けなければならない。重要度は施設や機関の管理者が決定すべきだが、一般的には次の事項を基準にすることができる。

- 時間―その資産の回復または置換にどれだけの時間を要するか。

暫定訳：バイオセーフティ管理室
2006年3月

- 費用—その資産の置換にどれだけの費用を要するか。
- 顧客—その資産の喪失に起因する遅れによって、どれだけの顧客が失われるか。または、それによってどれだけの顧客が獲得できなくなるか。

セレクト・エージェントまたは他の危険な病原体を取り扱う施設の場合、「潜在的な損害—この病原体を故意に使用または放出した場合の影響はどのようなものか」という疑問を追加することも考えられる。

資産を格付けする場合、1つの提案は、施設や機関の業務影響分析（BIA）を顧慮することである。BIAにおいて識別し取り扱うのは、企業が業務の混乱に直面すること、その状態が企業に及ぼす影響、それに対応するために企業が取り得る手順、および、それらの解決法に要する費用である（Myatt, 1999）。BIAを事前に行っていない場合には、資産分析と同時にBIAを作成するのが賢明である。資産評価の結果が、評価された資産とそれらの相互関係を識別し描き出すためのワークシートとなる（Jopeck, 2000）。

*脅威評価*

プログラムのレベルでは、組織および組織の任務と目標に対して認識された脅威を理解し、セキュリティ作業グループに確実に伝達することが、上級管理者（つまり、大学総長、機関管理者、指揮官など）の役割である。前述のように、生物工学・生物医学関連の施設や機関に対する脅威は大きく3種類に分類することができる。

- 動物・環境保護活動家による犯罪行為。
- 競争相手のスパイによる知的財産の侵害。
- 生物病原体を不適切な用途のために入手しようとするバイオテロリストまたは犯罪者。

既知の脅威の能力を評価するためには、「類似組織の資産に対する敵対者の攻撃について、その能力、意図、および歴史」に関する情報を収集しなければならない（Jopeck, 2000）。列挙したグループによる脅威にさらされた施設や機関の例には次のものがある。

- 最近では、地球解放戦線（ELF: Earth Liberation Front）の構成員が、「樹木の遺伝子操作」に抗議するため、ワシントン大学都市園芸センターの研究室に放火したことが疑われている（Verhovek & Yoon, 2001）。カリフォルニアのスタンフォード大学では「動物保護の名目で大学の資産に対して行われた一連の攻撃の結果」AIDS研究者を保護するために研究所を地下に建設することを余儀なくされた（Getty, 1996）。
- クリーブランド・クリニック財団の1組織で、アルツハイマーの研究を専門とするLerner Research Instituteから「細胞と遺伝子物質を盗んだ」として、最近2人の日本の研究者

が起訴された。遺伝子物質を盗んだ後、科学者の1人は自分の研究室で破壊行為を行い、物質が日本に届いた後に辞職し、「数週間後に」日本で働き始めた。「近年では、科学スパイと産業スパイの事例が次第に増加しているが、これは研究の価値の上昇を反映している」（Gillis, 2001）。

- オハイオのLarry Wayne Harrisは「軍事用炭疽菌」を所持していた疑いで1998年に逮捕されたことでよく知られているが、それ以前にも1995年5月に逮捕されており、それは、ロックビル医学研究所が3本のバイアルに入った「腺ペスト」不活性バクテリアをハリス氏の自宅に送ったことによるものである。ハリス氏は「アーリア民族軍のメンバーであることが、FBIによって確認されて」いる（Macy, 1998）。

自然災害（火災や洪水など）は、生物工学・生物医学関連の施設や機関に対する脅威ではあるが、前述の脅威の1つによる攻撃の結果でない限り、通常はセキュリティ計画により被害が軽減されるものではなく、このような脅威のリスクを低下させるためには、「歴史的データと専門家の予測」を分析に含めるべきである。敵対者と自然災害の違いは、自然災害が「意図」を持たないことである（Jopeck, 2000）。

*脆弱性評価*

この段階では、個別の資産について脅威を与える側の観点から考慮する。これは敵対者にとってどんな価値があるか、敵対者がどのようにしてそれを獲得するか（盗むか）、敵対者がどのようにしてそれを破壊するかなどということである。この種の情報を収集する最もよい方法の1つは、資産の責任者（運営者のレベル）に「面接」を行い、「観察」することである（Jopeck, 2000）。観察の焦点となるのは、資産を創造するために使用されるプロセスの手順、または、資産の操作や移転を含むプロセス（つまり、危険な病原体を例に取ると、研究手順のどこでどのように使用されるか、機関の間でどのように移転されるか、保管や増殖のセキュリティ条件はどうかなど）。観察分析を行う目的、あるいはプロセスの擬似リハーサルを行う目的は、窃盗や破壊に対して資産が（最も）脆弱になり得る段階や事例を明らかにすることにある（付録の表2参照）。

一般には、資産を検討するとき、何らかのセキュリティ能力がすでに存在している。つまり「好ましくない事象に対する脆弱性を、既存の対抗手段がどのように低減させるか（進行）」と「設置された対抗手段を無視した後にもう一度それを戻して、資産の脆弱性がどのように低減するかを見る（退行）」という2つの立場から脆弱性を観察することができる（Jopeck, 2000）。

*リスク評価*

この評価は、これまでの評価（資産、脅威、および脆弱性）で得た情報を組み合わせ、施設や機関における現在の運用状態のリスク水準を決定するものである。「リスクを計算するためのテクニックはいくつか存在する。単純な定性的システムから複雑な数学公式を基礎にしたものまであり、その他にこの2つを組み合わせたテクニックもある」（Jopeck, 2000）。しかし著者が目にしたこれらの計算テクニックの大半は、残念ながら生物工学・生物医学関連の施設や機関のモデルとして適切に転換されてはいなかった。使用する計算方法に関わらず理解しておくべき最重要事項は、施設や機関の任務に不可欠な資産の脆弱性が、識別された脅威によってどのように利用されるか、そして、それによって任務を遂行する能力が攪乱されたり破壊されたりする可能性があるか、ということである。

たとえば、「アリゾナ大学の2つの研究室が、動物解放戦線（ALF）に放火され、1,200匹を超えるラット、ウサギ、およびマウスが盗まれ、クリプトスポリジウムの治療法とワクチンの開発に関する数年分の研究成果が破壊された」（http://www.biostat.umn.edu/~carlton/PETA.html, 2001）。振り返ってみると、齧歯類（資産）のリスク分析を考察していれば、この研究における齧歯類は、「喪失によって会社に大きな影響を及ぼす」と判断できることが指摘されたであろう（Jopeck, 2000）。それにより火災や脅威に対して非常に脆弱であるとみなされ、ALFのような組織の過去の活動から判断しても、喪失の影響が大きいとみなされたであろうし、それに基づいて、齧歯類飼育場の周囲のエリアに対してはより厳しい立入制限が保証され、堅牢な消火装置が設けられ、それによって、これら実験動物が生存する可能性は高まったはずである。

**対抗手段評価**

この段階では、脆弱性を低下させ、脅威を寄せ付けずに資産を保護するために、どのような手順を取るべきか決定しなければならない。この方法は、3つのカテゴリーにまとめることができる。

- 「リスク忌避」：目的は、リスクをほぼゼロまで低減させることである（現実的ではないことがある）。
- 「リスク許容」：目的は、セキュリティのニーズと業務上の制約、つまり資金や任務との間で均衡を取ることである。
- 「リスク容認」：コストを削減するために、組織が最大限のリスクを容認する。この方法は、保護が必要な場合には最も望ましくないものである（Jopeck, 2000）。

対抗手段は、人事面の考慮、技術面の考慮、および実施面の考慮、の項目に分類するのが最適である。これらについて、この後のセクションで詳しく説明する。

暫定訳：バイオセーフティ管理室
2006年3月

リスク評価が終わったところで、もし正当ならば、リスクの受け入れとセキュリティ強化の資金供給に権限を持つ管理者に勧告を示すべきである。ここで重要なのは、これが連続的なプロセスであることを忘れないことである。

*人事面の考慮*

生物工学・生物医学関連の施設や機関は、いくつもの外部からの脅威の対象となることがある。概して、資産（特に生物材料）に対して最も現実的に考えられる脅威の大半ならびにあらゆる産業においてセキュリティに対する潜在的に危険な脅威の大半は、「インサイダー（部内者）」つまり従業員によってもたらされるものである（DTRA, 2000）。いくつかの事象によって、従業員が企業、雇用者、または同僚に対し、セキュリティ上と安全上の脅威となることがある。たとえば次のような例があるが、これらに限定するものではない。

- 不満を抱く、「不機嫌」になる。
- 昇進を見送られる。
- 懲戒処分を受ける。
- 心理的問題、あるいは個人的問題が持ち上がる。たとえば、離婚、子供や身内の病気、薬物濫用など。
- 新しいプロジェクトや製品に対して、倫理的・道徳的に同意できない。
- あるエリアに侵入し、別な企業や特別な利害グループのために「スパイ」行為をする仕事に雇用され、受け入れる。

部内者の脅威は最も防御が困難であり、同僚は本質的に信用されることから、様々な理由で最も危険になることがある。部内者の窃盗や不適切な使用から生物材料を保護することに関しては、合理的な、あるいは試験や実証済みの技術的解決法は存在しない（DTRA, 2000）。ほとんどの対策は、人事管理と出入管理に依存している。

学術的環境では不適切であり、ほとんどの企業でも実現不可能であるが、施設や機関の資産を従業員による潜在的脅威から保護する最初の手順は、身元確認を行うことである。「身元確認は、優れた雇用プログラムには不可欠な要素であり、犯罪歴の確認は特に重要である...」(Long, 2001）。身元確認を行わない場合、雇用者は、少なくとも個人の推薦状を点検し、示されている情報が正確であることを確認すべきである。機関が何らかの身元確認を行う場合であっても、個人の問題は、雇用された後まで、場合によっては長期間雇用されていても、表面に現れないことがあると言っておく価値はある。従って、従業員を雇用した後、そのセキュリティ上または人事上の行動調査は、定期的に継続するか、あるいは職務や出入制限に変更があったときに行うべきである。これらの要件とパラメータは、企業や機関の方針レベルで設定し、その実施はセキュリティに組み込むべきである。

暫定訳：バイオセーフティ管理室
2006年3月

従業員のセキュリティ認識レベルを高めることは非常に重要であるが、時には厄介な仕事になる。いくつかの主要な問題として、どのような水準の訓練を行えば関心を維持することができるか、あるいは、どのタイミングで訓練を行えば慌しい研究や製造予定を妨げないかを明らかにすることなどが挙げられる。少なくとも、従業員は次のことを知っている必要がある。

- 人員を識別し、認められたエリアにいるかどうか判断する方法。
- セキュリティ侵害の疑いを報告する方法。
- セキュリティ責任者は同時にあらゆる場所にいることはできないから、全員がセキュリティ担当者である。
- 会社の資産は従業員の資産であり、個人と同僚の安全およびセキュリティはいずれも共有責任である。

誰かが研究所内での火災に気付いた場合、消火活動や火災発生の報告を行わずに火を放置して通り過ぎることは考えにくい。火災が生命、安全、および財産を脅かすということは、小さいときから教えられ訓練されているからである。同様に、セキュリティの侵害や破滅につながる可能性のある個人的問題にも危険な兆候があり、それを観察できるはずである。しかし教育プログラムや訓練プログラムがなく、訓練を経ていない人の目では、これらの兆候やそれが持ち得る意味に気付かない可能性がある。

ほとんどの組織において、セキュリティ意識向上のための訓練をセキュリティ担当以外の者に提供する時間を見つけるのは最も大きな問題である。セキュリティ意識向上のための訓練プログラムには多数のよい例があるが、訓練を複数セッションに分割するときに忘れてならない最も重要なことは、「どのレッスンも、前のレッスンを土台に構築されるように訓練資料を分割し、セキュリティが全員の仕事であるという中心的テーマを強調する」ことである(McShane, 1999)。これは、バイオセーフティ訓練のコンセプトと良く似ており、安全訓練が効果的なのは、それがラインワーカーのレベルで採用され、管理体制の頂点まですべてにおいて支持された場合に限られる。訓練は、対象者の立場とリスクに関連付け、「セキュリティ専門家でない人」にも理解できるように提供し、最大の効果が出るような形式で段階的に実施して、疑問があれば質問できるように担当窓口を設けるべきである。

人は「単なる人間」であるから、克服できない抑圧や問題の蓄積を従業員が感じる可能性は常に存在しており、それが職場での暴力(他者や自己に対して)といった行動に結び付くことや、あるいは材料、独自データ、またはセキュリティ手順情報を部外者に提供(共謀)して報酬を得るといったことが起こり得る。従業員が必要な援助を受けられるようにし、インシデントが起こることを防ぐ最良の方法は、適切な従業員援助プログラム(EAP)を制定することである。

暫定訳：バイオセーフティ管理室
2006年3月

どのEAPでも意図されているのは、生命や生活を脅かす個人的問題を克服するにあたり、従業員が秘密裡に専門家の援助を受けられる方法を提供することである。さらにEAPでは、誰かが問題を抱えていないかどうかをより良く理解するため、同僚や雇用者が気付き得る兆候についても概要を示す。これらの兆候は、「職務適性行動（Fitness for Duty Behavior）」と呼ばれる。多数の企業と州や連邦の機関および組織が、この種のプログラムを通じて、無料の援助を被雇用者に提供している。フロリダ州立大学（FSU）の職員の場合には、大学のEAPがウェブサイトでこれらの兆候について概説している。FSUでは、次のような兆候が挙げられている。

- 奇妙で不適切な考えを口にする。
- 事前の承認や論理的な理由なしで、過度に長期間欠勤する。
- 肉体的外見が変化する。
- 反抗的な態度を取る。
- 作業能力が低下する。
- 職場での人間関係が悪くなる。
- アルコールや薬物の濫用の兆候がある。
- 過剰に不平を訴える。（http://www.eap.fsu.edu/guidelines.html, 2001）

EAPを設ければ、悲劇的な行動や資産の窃盗を防止することができるが、物理的制約の少ないセキュリティ管理では、次のようにそれを発展させることができる。

- 物理的資産を保護する。
- 個人の人格や専門家としての品位を損なわずに、大切な従業員に専門的援助を提供する。

身元や推薦状の確認、セキュリティ意識向上訓練、およびEAPによって、施設や機関は、人事面の考慮に関するセキュリティ管理に向けて、総合的アプローチを開発することができる。

*技術面の考慮*

技術面の考慮に含まれるのは、特定の脅威に対する資産の脆弱性を低下させるために利用できる可能性のある品目または装置である。生物工学・生物医学関連の施設や機関の任務、およびそのリスク分析に応じて、資産の脆弱性を削減するために相応しい装置が市販されている。いくつか例を挙げると、柵、照明、閉回路テレビ（CCTV）、照明またはCCTV付きの動作検知器、自動閉鎖式ドア、ロッキングドア、警報装置、カードキーによるアクセス装置などがある。

出入管理が機関にとって問題になることが多いのは、「どの」エリアにある「どの」材料を使用するための出入許可を「誰が」必要とするかを管理者が決定しなければならないからである。時には通常の業務時間内に限って出入を許可するか、あるいは時間や曜日に関係なく許可を与

暫定訳：バイオセーフティ管理室
2006年3月

えるかという問題も存在する。研究と製造は24時間行われることがあるが、延長スタンドオフ型近接カード、バイオメトリックスおよびリモートアクセスコントロールなどのいくつかの技術が手頃な価格になりつつあり、それを利用すれば、これらの障害を克服することができる（Strauchs, 2001）。滅菌と除染の問題も、労働者や製品の保護として、場合によっては関与することになる。

忘れてならないのは、どのような対抗手段を適切なレベルとして決めたにしても（リスク忌避、リスク許容、またはリスク容認）、技術の利用はプロセスの一部に過ぎないということである。リソース（時間、金、人）を用意して、設計、調達、設置、試験、訓練のための時間を割り当て、その後も再試験と再訓練を継続的に繰り返さなければならない（人事異動のときなど）。

*実施面の考慮*

セキュリティ・プログラムの実施面の構成要素は、現場または地域のセキュリティ組織で構成され、大学警備本部、病院や企業のセキュリティ部署、地域の警察、緊急支援などが含まれる。セキュリティ管理の実施部分は、$D^3RT$（ダート）という頭字語で簡潔に表されるが、これはDeter（抑止）、Detect（感知）、Detain（拘束）、Respond（対応）、およびTrain（訓練）を意味している。適切で有能なセキュリティ組織、セキュリティ手順、およびセキュリティ方針（身元・紹介状確認、セキュリティ意識向上訓練、およびEAP）を維持し、技術装置を設置することで、機関は、ほとんどの脅威を効果的に抑止し感知することができる。セキュリティ組織は大規模である必要はなく、むしろ事前に確定した脅威と脆弱性に対して適切であり、セキュリティ計画に合致したものが求められる。また、これも忘れてはならないが、望ましいレベルの保護を提供するために必要となる人員数を技術によって減らすことはできるものの、人員がインシデントに対応する必要がある場合には、適切な配置を行わなければならない（援助、インターフェース、およびモニタリングを提供するため、別の人員を必要とすることもある）。

脅威の拘留とは、犯罪行為に関するものであれテロ行為に関するものであれ、施設や機関において敵対者が脱出するのを遅らせることを意味する。遅延させることによって、セキュリティ部門では、事象が起きたという通知を受け取り（記録）対応する時間ができる。敵対者を拘束すると共に、安全で審美的に好ましい作業場所を従業員に提供するよい方法は、防犯環境設計（CPTED: Crime Prevention through Environmental Design）を利用することである。CPTEDは、施設や機関の外部および内部を、セキュリティを考慮して設計する慣行である。綿密な設計によって、テロ行為や犯罪行為を行った後に犯人がすぐには出て行けないようにすることができる。例を挙げると、柵や擁壁のすぐ前に来るまでそれに気付かないような修景を施すことや、個人に対する犯罪の発生を最小にするような修景（つまり、明るい照明の付いた開放的な建物への接近エリアに対して、暗い閉じられたエリアのような）、犯罪者がまっすぐ出られる出口

を提供しないために曲がりくねった歩行者通路や廊下を設けることなどが挙げられる（http://www.cpted.net, 2001）。

インシデントの調査においては、科学者などのセキュリティ担当以外の者に対して迅速かつ詳細な説明責任聴取を行うことができなければならず、もはや説明責任がないものについては報告できるようにしなければならない。これに含まれる可能性があるのは、動物や実験用および独自の材料・情報・製品などであるが、セレクト・エージェントやBSL-4病原体を取り扱う施設や機関にとっては特に重要となる。

機関のセキュリティ要員は、あらゆるタイプとレベルの脅威に対して適切に対応する能力を持つ必要がある（悪意による破壊、爆破の脅威、危険な病原体の盗難まで）。ここで推奨されるのは、地域の警察との良好な協力関係を構築し、相互に専門的な交流を持つことや、必要であれば援助を提供することである。施設や機関の物理的な規模に応じて、セキュリティ部門の機動性を考慮すべきであり、エリアを効果的にパトロールし脅威に対して迅速に対応するために、セキュリティ部門は、自動車、オートバイ、自転車、あるいはそれらの組み合わせを必要とすることがある。インシデントに対応するにあたり、セキュリティ要員は、施設内にある材料のうち、バイオハザードやその他の特殊な危険性をもたらす可能性のあるものについて事前に知っておかなければならない（つまり、化学物質、放射性物質、動物など）。セキュリティ要員が、バイオハザードを起こす物質を持っているおそれのある者あるいはそれに汚染されているおそれのある者を安全に取り押さえるためには、適切に開発され実践を経た計画が必要となるが、この計画はバイオセーフティ部門と調整して開発すべきであり、開発を開始する出発点として適しているのは、機関の生物学的緊急対応および支援計画を見直し、起こりうるシナリオに合わせてそれを修正することである。

セキュリティ担当者およびそれ以外の者の訓練は、適切で、整合性があって、継続的に実施されなければならない。適切なセキュリティ訓練は、特に生物工学・生物医学関連施設の場合、存在し得るすべての潜在的脅威について全員に周知させることを含んでいる。そのような脅威としては、産業用化学物質、バイオハザード、放射性危険物質が挙げられ、製造施設においては、低い位置に吊り下げられた物品、滑りやすい床、産業におけるその他の物理的な危険などについても評価しなければならない。また適切な訓練としては、訓練を行う者が研究環境や製造環境で勤務した経験を持っており、教室での指示や現場での監督を通じてその経験を提供できるということも重要である。可能であればこの訓練は、バイオセーフティ担当者、産業衛生士、および、その機関におけるその他の安全専門家が行うべきである。訓練の整合性は質と同義であり、高い水準の基準に維持すべきである。訓練はよく計画すべきであり、実施されたときから新しい要求事項に合わせて変更を開始すべきである。変更が必要になるのは、リスク分析が改訂されたとき、または、場合によっては、新しい事業、プロジェクト、または施設の構

暫定訳：バイオセーフティ管理室
2006年3月

築が考慮されるときである。セキュリティ担当者とそれ以外の者の訓練では、情報を自由に利用できるようにし、全員にすべての手順と方針がよくわかるようにしなければならない。訓練の価値が明らかになるのは、テロ行為や犯罪行為が起きたときであるが、よく訓練された人員とは、従業員をより効果的に保護することができ、情報をセキュリティ部門と管理者にできる限り迅速に報告できるということを意味する。

実施面の考慮において最も重要な部分は、$D^3RT$ 定式のどの部分も、機関や施設の毎日の活動にとって明らかな重荷とならないようにすることである。多くのセキュリティ要員が感じていることだが、管理者や科学者は、セキュリティ手段を、開放的な同僚との協力体制による作業環境を禁止する、非生産的なものとみなしている。これは一般に、以前の兵器施設における風説（または実際の冷戦経験）で育成された誤解である。今日のセキュリティはもっと無害な方法で達成することができ、民間部門では機関管理者の特権である。管理者にとっての推進力となるものは、人員の安全、商業資産の保護、危険な物質の盗難や誤用の防止などが中心となる。安全でセキュリティの完備した施設を維持する一方、セキュリティのために従業員の作業や快適さが妨げられないようにすることも重要であり、これはどのセキュリティ管理システムでも、協力と共同作業を促進するために役に立つ。

**生物病原体のセキュリティにおける技術面と実施面の課題**

実施計画と連携して適用される技術的解決法は、材料が集中型の貯蔵所に保管されている場合のセキュリティ提供にうまく活用することができる。すなわち、細胞系、開発中および試験段階にある製品の薬剤ライブラリー、病原性物質、さらには、人事ファイルや業務上重要な保管文書などがそれである。集中型貯蔵所に保管された病原体を守る1つの方法は、材料の取り扱いにおいて2人制を設けることである。この方法にはいくつかのバリエーションがあり、1人（部門の長や指定者など）に入口ドアの鍵を持たせ、もう1人（バイオセーフティ職員など）に2つ目の鍵または組み合わせ錠の番号を管理させる方法などがある。別な方法としては、日常の在庫管理（材料に関する年間の説明責任）を容易にすることもできるもので、バイアルの内容を名前で示すのではなく、バイアルに添付したバーコードを使用するようになっている。材料を明確に表示しないことが抑止力になるのは、何を盗んでいるのか、それが目的の材料なのか、どのようにして培養するのか、あるいはどのように使用するのかわからないからである。このシステムでは、科学者が材料に対する要求を申請し、管理者と機関のバイオセーフティ職員の承認を受けないと、その材料を貯蔵所から取り出すことはできない。承認済み要求は貯蔵施設職員に示され、貯蔵施設職員が冷凍設備内の当該材料の位置を確認し、科学者かバイオセーフティ職員の立会いの下でその材料を取り出す。この方法は、細胞培養、ハイブリドーマ細胞、BSL-1およびBSL-2（非セレクト・エージェント）材料を取り扱う大規模な組織で使用して成功しており、LANネットワーク機能を利用すれば、材料の要求を短時間で承認することができる。バーコードシステムの利点は、在庫管理を楽にするだけでなく、貯蔵所に残っているサ

暫定訳：バイオセーフティ管理室
2006年3月

ンプルがあらかじめ定めた数量まで減少した場合にプロジェクト管理者か上級研究者に警告が送られるようにしておけば、管理ツールとしても使用できることである（管理者はこれによって補充材料の再発注、培養、またはクローン化を行うことができ、気付かずに最後のバイアルを使い切ってしまうことはない）。

生物病原体のコレクションを保護すると同時に、セレクト・エージェント（BSL-3およびBSL-4）に関するバイオセーフティ要件を満たすための解決法は、コレクションを封じ込めエリアに置くことである。封じ込めエリアが材料の保存に関する安全性から見て道理にかなった場所であるのは、その場所で材料が使用されるからである。封じ込めエリアで貯蔵を行うと、更衣室、シャワー室（BSL-4の場合は、エアロックを通って入場することが必要とされ、このエアロックはエンジニアリングサービスによって監視されるのが一般的）、およびその他の設備への出入りまたは通過を必要とすることになるが、これらの場所は一般に、組み合わせ錠、カードキー、または他の手段で出入りが制限される。職員が貯蔵所に入るドアの前まで来ると、動作検知器起動式CCTVの監視によって、中に入るためにはさらに別の出入管理が設けられていることがある。冷凍庫には標準機能として錠前が付いており、もう1つの抑止機能として働く。このシナリオでは、貯蔵エリアにおける生物材料の保護に関して、運用面と技術面の解決法の組み合わせを提供している。注意すべきこととして、これらの技術は（すべてではないが）ほとんどの侵入者に対して有効であるとはいえ、権限を持った内部の者には効果がない。貯蔵所から材料を取り出す際に2人制を設けることによってこれらの脅威を取り除くことはできるが、その2人が共謀している場合は例外であるだけである（一般に共謀の可能性は非常に低い）。

これも重要であるが、貯蔵所の生物材料はかなりよく保護できるとしても、研究室で培養中の材料に同じレベルのセキュリティを提供するための、妥当な運用面または技術面の手段は事実上存在しない。実際的なセキュリティ・リスク評価では、研究室そのものが最も脆弱なエリアであることが明らかになっている。権限を持つ部内者にとって、自分や同僚が取り扱っている材料のサンプルをフラスコから取り出し持ち出す方がより容易であることは明らかである。このような、フラスコ内の分量の食い違いに気付くことは事実上不可能であるし、失われた材料の追跡はさらに困難である。ほとんどの機関では、BSL-2病原体を取り扱っている研究所のドアは、日常の作業時間中に施錠も閉鎖もされず、誰でも出入りして少量の材料を取り出すことが可能になっている。しかるに、セレクト・エージェントまたはBSL-3やBSL-4病原体を取り扱っている機関では、研究所のドアを自動閉鎖式にし、出入管理装置（錠前、パンチコード、カードキー）を設けて無許可の出入りを抑止すべきである。しかし実際には、少量の生物材料を持ち出そうとしている部内者を合理的な手段を用いて阻止できるような、絶対的な方法は存在しないし、科学者に対して、2人組の相互チェック体制で働くことを期待するのは無理である。そのような体制は煩わしく、少なくとも人件費とPPEコストは2倍になるし、簡単に失敗することは言うまでもない。連続監視用CCTVや「ポータルまたはトラッキング」システム

（現在は未開発で未検証の非常に高価な技術で、生体やメディアなどのラベルの開発に依存するものであり、エリア内での生体の動きを追跡するもの）または、核や化学物質のセキュリティおよび保証プログラムで使用されているその他の技術や方式の使用を試みることも合理的とは言えない。生物材料はリアルタイムで測定できるような固有のサインを「出さない」し（特にバイアルに入っている場合）、微量でも価値がある（増殖できる可能性）ことも、セキュリティの観点からは困難な問題となる。技術面と運用面のセキュリティは部外者が危険な材料を入手できないようにするために非常に役立つが、重要なのはセキュリティ違反の原因として最も可能性の高い部内者によるインシデントを防止することであり、これに関しては人事面の考慮のセクションで説明してある。

## 要旨

この章の目的は、生物工学／生物医学施設または研究所のセキュリティ管理上の考慮事項について、幅広く概要を示すことである。これは、方針を決定することや現行のSOPを変更すること、また、「そのまま利用できる」標準的運用手順を示すことを意図したものではない。むしろ、施設や研究所のセキュリティ管理の概念を確立または再構築し、現在の新しく興ってきた脅威に対処することを目指している人々のために、先ずは出発点として役立つ情報として提供した。

セキュリティ管理は、資産保護計画の立案過程であり、個々の職員保護の保証、技術的対策の維持、および運用面のセキュリティを日常活動に統合することであるが、これは、施設や研究所の業務上または学術上の必然性を、すぐにも超えてしまう可能性がある概念だと思われるかも知れない。しかしながら、過去10年間に世界は変化し、このようなセキュリティの各側面は次第に必要不可欠なものになりつつある。プロの活動家、バイオテロリスト、および競合する情報スパイが、新しい世紀において急速に脅威となりつつある。適切な人材配置と協力を得た、管理者の支持する統合セキュリティ管理プログラムによってのみ、これらの脅威に適切に対処することが可能となる。つまり、脅威に対して適切に対処したときにこそ、セキュリティ・プログラムは、重荷ではなく資産として認識されるのである。

暫定訳：バイオセーフティ管理室
2006年3月

# 付録

## 表1

セキュリティ要件分析の概要（Hamilton E, 2000）

A. 保護すべき資産（assets）を識別する。
B. 資産の価値を評価する。
C. 潜在的脅威を評価する。
D. 脆弱性を評価する。
E. リスクを評価する。
F. 対策の選択肢を決定して経費を予測する。
G. リスク管理の意志決定を行う。

## 表2

セキュリティ要件分析で考慮される構成要素の説明（Hamilton E, 2000）

A. 保護すべき資産には次のものが含まれ得る：
    - 人材
    - 物質（生物学的危険物質、化学物質、放射性物質など）
    - 知的財産／製品／研究方法・製造過程
    - 装置／施設
    - 企業／組織の評判と任務
    - 記録／コンピュータ上のデータベース／個人情報
B. 機関は、以下のように問うことによって、その資産の価値を評価することができる：
    - 損失、損傷、危機、または作業の中断による影響はどのようなものか？
    - 施設の損失は何か？
    - 敵対者は何を獲得することになるか？
    - 研究所の任務に関して、あるいは国家脅威に関して（つまり、生物学的危険物質の盗難）、損失の影響はどのようなものか？
    - 人の生命に対する潜在的影響はどのようなものか？
    - 資産の置換や修復は可能か、そして可能であれば経費はどれくらいか（金銭的な費用に限らない）？
C. 潜在的脅威となる可能性が最も高い者が誰かを特定する。2つ以上のカテゴリーを含むことがある。
    - 過激派／狂信者（「動物愛護」の右翼活動家）？
    - 犯罪者／破壊者？

暫定訳：バイオセーフティ管理室
2006年3月