ない。

この様に、人的セキュリティに関する情報をアセスメント対象として受け入れてもらうには、個人の情報から集団の情報へその性質を転換させることが必要であった。ツールでは、ふたつの方法でそれを試みた。直接的には、質問の尋ね方を変え、選択肢を変更した。間接的には、誰がどのように評価しているかを分からなくするために、独立したコンピュータに入れて、回答した結果の個々は意図的に開かない限り見ることができ無い様にした。今後さらに、すでに実施したアセスメントは隠しファイルとなるようにする予定である。

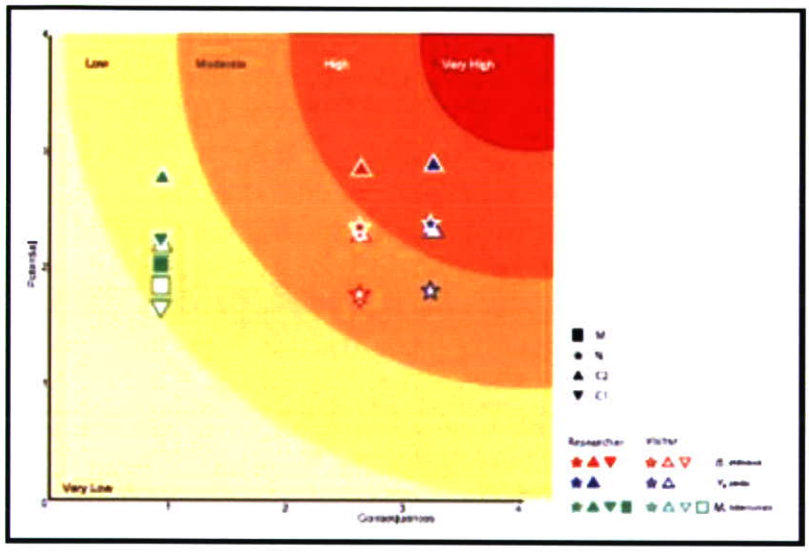

図５．バイオセキュリティリスク・アセスメントの結果表記（グラフ）

意志決定ツールとしてこれを完成させるには、対策効果の再評価の繰り返しを可能にすることが重要である。外部者による監査よりも、関係者自らの手で自己評価し、導入しようと考える対策の効果をも評価でき、変化する状況に伴い、自由に繰り返すことによってそのときに最善の対応ができるならば、利用者も正直に正確な情報を躊躇無く反映できると考える。本年度の試作版ソフトウエアの試行により、紙媒体よりも受け入れが容易であることが確認されたことから、実用晩に向けての調整を続けて行きたいと考える。

国際的には、バイオセーフティに関しても、同様のバイオセーフティリスク・アセスメントのためのツールを、カナダ公衆衛生局を中心に国際連携で作成する動きが始まっている。特に、特筆すべきは、科学的な根拠の必要性を鑑み、専門家の査察の定量化を試みると同時に、不測データについての研究協力を模索するなど、食品のリスクアナリシスにおいて取られてきた体制を、バイオリスクのアセスメントでも開始したことである。バイオセキュリティとバイオセーフティは、多くの必要情報が重複していることから、このグループ活動への参加と相互利益により、将来的にはバイオリスクアセスメントとして、施設運営に日常的に利用してもらえる製品が作成できる。

E．結論

改正感染症法の施行により、バイオセキュリティの概念が日本の法律に導入された。その結果各施設は確立していない概念に戸惑い、指針を提供されていないことから、運用面の検討より先に、ハードウエアの充実を目指すこととなった。バイオセキュリティの確立はその基本であるリスク評価を実践し、それぞれの施設にあった必要なセキュリティを導入し、日常業務と融合することにあり、本成果物は各方面での活用が期待される。

F．健康危険情報

なし

G．研究発表

1. 論文発表

なし

2. 学会発表

1) M. Shigematsu, S. Caskey, J. Gaudioso, S. Ando. Biosecurity self-assessment tool trial run in Japan. 3rd Asia-Pacific biosafety Association Conference. Malaysia, 2008年3月.

2) S. Ando, M. Shigematsu, N. Shimazaki, T. Ikebe, M. Obuchi, J. Terajima, K. Sugiyama and T. Sata. Problem and Confusion of Infectious Substance Transport in Japan. 3rd Asia-Pacific biosafety Association Conference. Malaysia, 2008年3月.

H．知的財産権の出願・登録状況（予定を含む）

なし

別添. バイオセキュリティのリスク評価ツールの原理

参考資料： R. M. Salerno, J. Gaudioso. Appendix B: Example Biosecurity Risk Assessment Methodology, in *Laboratory Biosecurity Handbook*, CRC Press, USA, 2007, pp. 115-131.

暫定日本語訳

付録 B

生物安全保障リスク評価方法例

生物安全保障リスク評価（Biosecurity Risk Assessment）は、リスク管理者が適切な生物安全保障上のリスク低減策を実施する上で役に立つツールである。この目標を達成する方法は多数あるが、本セクションでは、米国ならびに国際的な生物化学施設で優れた実績を上げている方法を取り挙げる。相対的な生物安全保障リスクの系統的評価に用いることのできる、標準的かつ一貫性のある評価基準を策定することがわれわれの狙いである。

この方法は、多基準データ分析（Multiple Criteria Data Analysis）として知られるリスク評価のメカニズムに基づいている。これは評価基準の階層型価値樹（Hierarchical Value Tree）を用いるものであり、「技術的な性能情報を意思決定者から聞き出した決定基準と加重に関連づけ、意思決定プロセスに伴うトレードオフの視覚化と数量化を可能にする」[1]。この方法は、結果的に「スコア（得点）」に結びつく評価基準の質的評価に依拠している。すべての評価基準が均等にリスクの一因となるわけではないことを確認するために、それぞれの評価基準には関連する加重を持たせることができる。各評価基準の相対的重要度（加重）を設定するメカニズムは多数ある。これについては、Expert Choice ™の意思決定支援ソフトウェアツールにインプレメントされているように、階層分析法（AHP: Analytic Hierarchy Process）として知られる、見解聴取（Expert Elicitation）に関して幅広く認められているアプローチを用いる。このアルゴリズムは[2]、多数の利害関係者から情報提供を受けて、複雑な多変量決定を行うために業界では広範に用いられている。AHP は、効用関数と重み関数ではなく、決定基準の対比較に基づく質的比較法を用いる。AHP の重要な仮定条件は、人は絶対的な判断よりも相対的な判断を下すのに、はるかに長けているということである。

加重平均は、Threat Potential（脅威の潜在性）と Consequences（結果）という変数の値に対して計算される。総合的な生物安全保障リスクとは、これら 2 つの変数の相関関係（関数）である（方程式 B.1）。

方程式 **B.1**　生物安全保障リスク

$$\text{生物安全保障リスク} = (T)*(C)$$

T = Threat Potential（脅威の潜在性）

C = Consequences（結果）

こうした尺度（基準）は、生物資産（Biological Asset）を持つ特定の施設に関連した一連のシナリオの相対的リスクに関係している。その上で担当者は、どのシナリオが容認可能なリスクを表し、どのシナリオが容認不能なリスクになるかを判断することができる。

B.1　資産の評価（ステップ 1A）

第 2 章で検討したように、当該施設における病原体と毒素の特定と評価（資産評価）から始めることとする。エージェント（作用物質・生物剤）のベースラインリスクとは、当該エージェントを悪用するタスクの複雑さと、悪用がもたらす最大限説得力のある、起こりうる結果の関数である。

方程式 **B.2**　エージェントリスク

$$\text{エージェントリスク} = (TC)^*(C)$$

TC = Agent task complexity（エージェントタスクの複雑さ）
C = Consequences（結果）

まず、施設の資産を特定しなければならない。これについては、利害関係者のミーティング開催、施設スタッフの面接、施設の視察等のさまざまな段階を通じて行うことができる。資産には、当該施設あるいは敵対者にとって、価値あるものがすべて含まれる。分かりやすくするために、ここでの議論は生物剤（Biological Agents）に限定する。特定化の段階では、見落としが無いことを確実にするために、包括的であることが重要であるが、たとえ小規模な施設でも、特定される資産は膨大な数に上ることが考えられる。資産評価が終了すると、資産の多くは軽微なリスクしかもたらさず、評価対象とし続ける必要は無いと判断されることであろう。

生物剤の評価は、生化学的特性の調査から始まる。生物剤の悪用に伴うタスクの複雑さを特徴づけると、関連するメトリックス（測定基準）を伴った 3 つの評価基準にグループ分けすることができる（方程式 B.3）。スコアが高いほど高リスクを表すように、メトリックスを組み立てた。

方程式 **B.3**　エージェントタスクの複雑さ

$$TC = TC_A w_A + TC_{De} w_{De} + TC_{Di} w_{Di}$$

TC_A = Acquisition task complexity（取得タスクの複雑さ）

TC_{DE} = Development task complexity（開発タスクの複雑さ）
TC_{Di} = Dissemination task complexity（散布タスクの複雑さ）
w_A = Weight of TCA criterion（TC_A 評価基準の加重）
w_{De} = Weight of TC_{De} criterion（TC_{De} 評価基準の加重）
w_{Di} = Weight of TC_{Di} criterion（TC_{Di} 評価基準の加重）

1. TC_A：評価対象の施設に加えて、当該エージェントについて考えられる入手経路がほかにいくつあるかを考慮した、当該エージェントの取得難易度を加味する。エージェントの出所には、毒性株の自然環境からの隔離、合法的施設からの窃盗、デノボ（新規）合成や分子修飾を通じた危険物質の創出が含まれる。

0	あらゆる手段で容易に入手できる、規制されていないか人工的なのもではなく、自然隔離経路が自明である（例：生物学専攻の大学生の技能レベル内）、あるいは適切な自然発生源が世界的に流通している
1	世界的に限定的な規制（めったに規制されていない）、適切な自然発生源が国内で入手可能、合成系と自然隔離が容易（例：経験豊富な技術者、大学院生の技能レベル内）
2	世界的には高度に規制されている、適切な自然発生源または合成系が限定的、自然隔離経路が困難
3	現状では世界中で最大 25 施設のうち 1 施設が当該エージェントを保有、適切な自然発生源が不足しているか人工的、自然隔離経路は高度な技能を必要とする（重要なエージェントについては実現されていないが、関連するエージェントについて実現済み）
4	現状では施設単独またはほとんど単独の発生源、エージェントは自然から根絶されている、合成経路があれば革新的

2. TC_{De}：当該エージェントを最適な散布経路（すなわち、最大限確実な結果に至る経路）に適した形式で、適量に加工する難易度を加味する。これには、要求されるテストと評価レベル、隠密製造の難易度、保存問題等の検討が含まれる）。

0	生物兵器用エージェントとしての検討に先立って広範な研究開発を要する可能性が高い、隠密製造には高度な能力が要求される、極めて不安定な調合品（数日しか保存できず、高度な処理なしには散布圧力に耐えられない）
1	使用前に広範なテストと評価を要する、隠密製造には極めて高度な能力（例：BSL4）が要求される、不安定な調合品（保存が困難－不明のプロセスおよび散布後の生存能力が限定的－1<1 h）
2	テストと評価に中程度な投資を要する、隠密製造には高度な能力（例：BSL3、予防法）が要求される、調合品は比較的不安定（乾式製剤は非常に困難、液状製剤は

	何カ月も保存可能）
3	テストと評価に最小限の投資を要する、隠密製造には一般的な技術力および／またはプロトコル（例：BSL2）が要求される、調合品は安定している（何週間も容易に保存可能で、散布後も数時間から数日にわたり生存可能）
4	確実に作用させる上でテストや評価をほとんど必要としない、隠密製造には最小限あるいは全く技術力もしくはプロトコルが要求されない、調合品は極めて安定している（長期保存が容易、物質は散布後も数週間以上生存可能）

3. TC_{Di}：危害を及ぼす上で当該エージェントを散布する難易度を加味する。これは、選択した散布経路（例：皮膚、吸入、経口、媒介生物）に必要なエージェントの量によって異なる。分析では、最適な散布経路（すなわち、最大限確実な結果に至る経路）の選定が仮定されている。散布後の環境における当該エージェントの安定性も、散布を成功させる上で、難易度に影響する。

0	伝染性または毒性が無いことが知られている、あるいはそのように想定されており、当該エージェントが環境中では非常に不安定であるため、散布に成功することは極めて困難と思われる
1	低い伝染性または毒性（ID50 または LD50 > 50,000、毒素 LD_{50} > 5000μg/70kg）しかない、あるいはそのように想定されており、環境中においては不安定であるため、散布に成功することは困難と思われる
2	中程度の伝染性または毒性しかない、あるいはそのように想定されており、環境中においては多少安定しているに過ぎないことから、散布に成功することは中程度に困難と思われる
3	高い伝染性または毒性（ID50 または LD50 100～1000、毒素 LD50 0.1~100μg/70kg）があり、あるいはそのように想定されており、環境中においては安定しているため、散布に成功することは容易と思われる
4	極めて高い伝染性または毒性（ID50 または LD50 < 100、毒素 LD50 < 0.1μg/70kg）があり、あるいはそのように想定されており、環境中においては極めて安定しているため、散布に成功することは非常に容易と思われる

生物剤の悪用に伴うタスクの複雑さを特徴づけることは、当該エージェント評価の構成要素のひとつに過ぎない。考えられる結果についても、標準化されたメトリックスを用いて評価しなければならない。ここでは三種類の結果を検討する。今回の評価では、敵対者が最大限確実な事象を実現できるものと仮定しており、これは相対的なリスクを比較する上で妥当な仮定である。

方程式 **B.4**　結果

$$C = C_p w_p + C_e w_e + C_{psy} w_{psy} + C_{op} w_{op}$$

C_p = Population impact（住民に対する影響）
C_E = Economic impact（経済的影響）
C_{psy} = Psychological impact（心理学的影響）
C_{op} = Operational impact（運営上の影響）
w_p = Weight of C_p criterion（C_p 評価基準の加重）
w_e = Weight of C_e criterion（C_e 評価基準の加重）
w_{psy} = Weight of C_{psy} criterion（C_{psy} 評価基準の加重）
w_{op} = Weight of C_{op} criterion（C_{op} 評価基準の加重）

1. C_p：住民に対する影響はさらに、伝染性、罹病率、死亡率、事前曝露対策、事後曝露対策にあたる評価基準に細分化することができる（方程式 B.5）。

方程式 **B.5**　住民に対する影響

$$C_p = C_t w_t + C_{morb} w_{morb} + C_{mort} w_{mort} + C_{pre} w_{pre} + C_{post} w_{post}$$

C_t = Transmissibility（伝染性）
C_{mort} = Morbidity（罹病率）
C_{mort} = Mortality（死亡率）
C_{pre} = Preexposure countermeasures（事前曝露対策）
C_{pre} = Postexposure countermeasures（事後曝露対策）
w_t = Weight of C_t criterion（C_t 評価基準の加重）
w_{morb} = Weight of C_{morb} criterion（C_{morb} 評価基準の加重）
w_{mort} = Weight of C_{mort} criterion（C_{mort} 評価基準の加重）
w_{pre} = Weight of C_{pre} criterion（C_{Pre} 評価基準の加重）
w_{post} = Weight of C_{post} criterion（C_{post} 評価基準の加重）

a. C_t：エージェントの伝染性は、病気の伝染性の見通しを示す。

0	伝染の可能性なし
1	伝染は、主に親からのまたは性的曝露による（直接接触）
2	伝染は、主に血液または汚染物による（近接接触）
3	伝染は、大きな液滴による（例：1m 未満の日常的接触）
4	伝染はエアロゾルによる（例：1m以上の遠隔接触

b. C_{morb}：罹病率は、住民が予防接種を受けていないものと仮定し、当該エージェントへの暴露後すぐに病気にかかった割合を表す。

0	罹病率は低い（0～50%）が、治療が必要になる可能性は低い
1	罹病率は低い（0～50%）が、通院治療が必要になる可能性が高い
2	罹病率は低い（0～50%）が、入院が必要になる可能性が高い
3	罹病率は高く（50～100%）、通院治療が必要になる可能性が高い
4	罹病率は高く（50～100%）、入院が必要になる可能性が高い

c. C_{mort}：死亡率は、住民が予防接種や治療を受けていないものと仮定し、兆候的な感染用量または毒性を示した後に死亡した割合を反映するものである。

0	健康な成人を死に至らしめるものではない（予想死亡率 1%未満）
1	致死率は低い（予想死亡率 1～15%）
2	致死率は中程度（予想死亡率 15～50%）
3	致死率は高い（予想死亡率 50～90%）
4	ほとんどが一様に死に至る（予想死亡率 90%以上）

d. C_{pre}：事前曝露対策の評価基準は、当該対策（例：ワクチン）の可用性と有効性を反映するものである。

0	当該エージェントが引き起こす病気への事前曝露対策は、非常に効果的かつ容易に利用できる（95%以上の有効性があり、重大な障害は存在しない）
1	当該エージェントが引き起こす病気への事前曝露対策は、適度に効果的である（90%以上の有効性があるものの、副作用や多少わずらわしい接種手順をはじめとする管理上の障害が存在する）
2	当該エージェントが引き起こす病気への事前曝露対策には、最小限の効果しか無い（90%未満の有効性しかなく、IND ドラッグや危険な副作用、わずらわしい接種手順をはじめとする管理上の重大な障害が存在する）
3	当該エージェントが引き起こす病気への事前曝露対策は存在しないが、開発中である
4	当該エージェントが引き起こす病気への事前曝露対策は存在しない

e. C_{post}：事後曝露対策の評価基準は、当該介入策（例：抗生薬剤）の可用性と有効性を反映するものである。

0	当該エージェントが引き起こす病気への事後曝露対策は、非常に効果的である（病気の進行の最終段階以外は、全体的に非常に効果的である）

1	当該エージェントが引き起こす病気への事後前曝露対策は、適度に効果的である（効果的であるが、病気の進行の初期段階に適用された場合に最善の結果が見られる）
2	当該エージェントが引き起こす病気への事後曝露対策には、最小限の効果しか無い（病気の進行の極めて初期段階で適用された場合であっても、めったに効果が無い）
3	当該エージェントが引き起こす病気への事後曝露対策は開発中である
4	当該エージェントが引き起こす病気への事後曝露対策は存在しない

2. C_e：経済的影響とは、生物剤の悪用に直接関連する国内経済に対する影響の特徴づけを目指すものである。

0	経済的影響なし
1	金融市場または国際貿易における変動なし。景気は数日中に回復し、損失を取り戻すことができる。回復に伴う軽度な財務上の影響
2	金融市場および／または国際貿易における小規模な変動。景気は数週間のうちに回復し、損失を取り戻すことができる。事業を営む上で軽度な継続的コストの増加
3	金融市場および／または国際貿易における中程度の変動。景気の回復には政府の介入を要する恐れあり。政府または業界によって課される安全保障対策が増えるため、事業を営む上で中程度の継続的コストの増加
4	金融市場と国際貿易における世界的ならびに国内における大規模な影響。景気を安定させるには政府の即時介入が要求される。回復に伴う相当なるコスト。事業運営コストが大幅に増加し、さまざまな業種で破産や操業停止が起こる

3. C_{psy}：心理学的影響とは、公衆の挙動または公衆のリスク認識がどのように影響されるかを評価するものである。

0	攻撃による公衆の挙動に対し、重大な影響なし
1	攻撃による影響度は低く、公衆に不安が広まるが、社会的混乱は無い
2	攻撃による影響度は中程度、公衆には全面的に不安が広まるが、社会的混乱は最小限（学校、現地輸送システム、政府事務所等、公共インフラの小規模な閉鎖）
3	攻撃による影響度は高く、公衆には大規模なパニックが発生し、重大な社会的混乱を伴うが、必要不可欠な社会的機能は継続し（学校、地域輸送網等の公共インフラが広範囲にわたって閉鎖され、一部の行政サービスが停止する）、国家安全保障には中程度の脅威が及ぶ
4	攻撃には極度の影響度があり、公衆には大規模なパニックが発生し、極端な社会的混乱が伴い（公共インフラの要素が機能停止）、国家安全保障には重大な脅威が及ぶ

4. C_{op}：運転上の影響は、生物剤の窃盗と悪用に関するシナリオには含まれていない。当該施設が生物テロに用いられる生物剤の出所になる可能性は低く、結果的に施設特有の影響は最小限にとどまることになる。

タスクの複雑さと結果という評価基準に照らしてエージェントを評価することによって、リスク評価者は、エージェントを悪用リスクグループに振り分けることができる。ここでの決定は、施設特有リスク評価の出発点となり、全面的なリスク評価に加えるか否かについて、低リスク生物剤をふるいにかける上で論理的な出発点にもなる。

B.2　脅威の評価（ステップ 1B）

次に、考えられる敵対者とそれらが施設に対して及ぼす脅威を特定し、評価する（脅威評価）。可能な場合、施設としては既知の属性を用いるべきである。ただし、これが不可能な場合がよくある。代替策としては、当該施設に対するもっともらしい敵対者の範囲全体に及ぶ属性を持った概念上の敵対者のセットを作成することである。ここでは概念上の敵対者の一般的セットを定義するが、関連性を高めるためには、リスク評価者としては、現地の脅威環境に関するデータに基づいて、プロフィールを修正する必要がある。施設としては、脅威環境を正確に分析するために、特定の定義済み属性のセットを伴う新たな概念上の敵対者を作成する必要があるかもしれない。現地の警察等（Law Enforcement Community）がこのタスクにとって有益なリソースとなる。以下の概念上の敵対者についての説明書を吟味し、現地の法執行調査票（Law Enforcement Questionnaire）（付録 A にて用意）に記入することが、この検討を進める上で役に立つ。

本セクションにおける概念上の敵対者についての説明書は、許可されたアクセスのレベルに基づいてまとめられている。説明書は、敵対者の属性（動機、手段、機会）のそれぞれについて用いられる仮定セットを定義するものである。こうした敵対者の属性（方程式 B.6）は、潜在的敵対者に関する脅威評価を行うための、一組の標準化された評価基準をもたらすものである。敵対者の説明書は、施設において合法的事業を営む個人のグループ全員が、生物剤やその他の資産を盗もうとするであろうことを黙示するものではない。

方程式 **B.6**　敵対者の属性

$$A = A_{mo}w_{mo} + A_{me}w_{me} + A_{op}w_{op}$$

A = Adversary attributes（敵対者の属性）

A_{mo} = Adversary motive（敵対者の動機）

A_{me} = Adversary means（敵対者の手段）
A_{op} = Adversary opportunity（敵対者の機会）
w_{mo} = Weight of A_{mo} criterion（A_{mo} 評価基準の加重）
w_{me} = Weight of A_{me} criterion（A_{me} 評価基準の加重）
w_{op} = Weight of A_{op} criterion（A_{op} 評価基準の加重）

インサイダーとは、許可されたアクセスを持つ人物である。施設には 1 タイプのインサイダー（全面的アクセスを有するインサイダー）しかいない場合もあれば、盗難の恐れのある資産へのアクセスレベルに基づいて、全面的アクセス（Full Access）を有するインサイダー、建物へのアクセスを有するインサイダー、サイトへのアクセスを有するインサイダー等、多数のタイプのインサイダーがいる場合がある。すべてのインサイダー敵対者にあてはまるものと想定される属性がいくつかある。インサイダーの動機としては、不満、心理的不安定、個人的利益（共謀による）、テロ行為を犯す願望が考えられる。悪意のあるインサイダーは、発覚を避けるために、拙速に窃盗を試みることはないものと考えられる。なぜなら、インサイダーとしては、アクセスを許可されていることから、資産を盗むのにより適したタイミングを待つことができるからである。概して、そうしたインサイダーとは、悪意を持つようになった従業員であり、準軍事的な訓練は受けていないものと考えられる。

全面的アクセスを有するインサイダーとは、研究室の作業員であるか、同伴者を伴わずに資産にアクセスできるその他の人物であることが考えられる。アクセスが許可されていれば、その人物は施設とその運営システムについて、広範な知識を蓄えることができる。また敵対者にも機会がもたらされることになる。生物学的物質への全面的アクセスを有するインサイダーは、ほとんどが高度な技術的訓練を受け、高度な知識を備えた科学者や技術者である。そのため、生物剤を首尾よく入手し、武器として配備し、あらゆる手段を自在に利用できることが多い。サイトがアクセスコントロールを実施している場合、リスク評価者としては、全面的アクセスを有するインサイダーの説明書を変更して、それ以外のインサイダータイプにふさわしい仮定セットを作成することができる。

アウトサイダーとは、サイトへのアクセスが許可されていない人物である。こうした概念的説明書を変更するか、別の説明書を作成するには、サイトとその近辺に特有の情報を用いる必要がある。

テロリストグループである敵対者の動機は、大量の死傷者を出し、経済危機を起こす、あるいは恐怖を広めることであり、政治的な声明を目的にすることも考えられる。このような敵対者は十分な資金力があり、国家や宗教団体、個人、あるいは犯罪組織に支援されていることが考えられる。十分な資金力をバックにしたテロリストグループには、設備も訓練も整っており、攻撃のリハーサルを行うこともできる。テロリストグループには高度な組織力があり、暴力的で死をいとわない。また、かなりの数の爆発物や武器にアクセスでき、それらを活用する技能も有している。アウトサイダーとして、テロリストグループ

にはアクセスや具体的な機会は無い。

単独のテロリストである敵対者には、政治的声明を出す、怒りを表明する、最終的に個人的目標を達成するためにエージェントを盗む、あるいは生物テロ行為を犯す動機があると考えられる。この種の敵対者にはテロリストグループほどの手段は無いが、それでも装備と訓練は整っており、攻撃のリハーサルを行うこともできる。多数の警備員やその他の人々を殺傷する能力があることも考えられる。単独のテロリストは、ほとんどのアクセスコントロールシステムを突破するのに必要なツールを備えており、暴力と武力の行使をいとわない。アウトサイダーとして、単独のテロリストにはアクセスや具体的な機会は無い。

過激派グループである敵対者、政治的声明を出すか、環境、政治、経済、あるいはその他の理由で各種のプログラムに抗議する動機がある。そのため、目的は生物剤を盗むことではなく、所有物を破壊したり、動物を逃がしたりすることが考えられる。ただし、そうした行為は、汚染された動物を逃がすことによって、図らずとも病原体を環境中に漏洩させてしまう恐れがある。過激派グループは、一般的に妨害行為に関連した手段を備えており、これには手工具や放火その他の設備破壊行為用のアイテム、あるいは拳銃の使用が含まれるものと考えられる。こうしたグループは、施設については一般的な情報を有しているが、資産の所在地や施設の防護システムに関する具体的情報は無い。グループのメンバー全員がアウトサイダーであると考えられるため、過激派グループにはアクセスや具体的な機会は無い。推定される動機から、この概念的敵対者は一般的に、生物テロ行為に使用するための病原体や毒素の窃盗にのみ焦点を当てたリスク評価には加味されない。

犯罪者の動機は金銭的利益である。犯罪者とは、武器と手工具を備えていると考えられる単独の敵対者である。組織犯罪が現地の問題になると評価された場合、犯罪組織としての敵対者を適切な方法で定義することができる。犯罪者である敵対者も、アクセスや具体的な機会を持たないアウトサイダーであると推定される。犯罪者である敵対者もまた通常は、生物テロ行為に使用するための病原体や毒素の窃盗にのみ焦点を当てたリスク評価には加味されない。

競争相手は、専有情報や実験用材料の窃盗または破壊を通じて、市場競争上のアドバンテージの各続を目指すものである。競争相手には、知的財産を盗み、資産を入手する意思のある、招かれた同僚やその他の訪問者が含まれるものと考えられる。この種の敵対者には、限定的な手段しか備えていないと考えられるが、直接的あるいは監視付きアクセス（すなわち、同伴アクセス）の機会を得る場合がある。この種の敵対者も、生物テロのリスク評価には関係しない。

心なき破壊者（Vandals）は、個人で活動する場合もあれば、グループで活動する場合もある。動機は損害や破壊をもって不法妨害を行うことである。ツールにはスプレー式ペンキ、ナイフ、手工具が含まれ、標的射手やハンターに対しては、拳銃が含まれる場合もある。自分たちの近辺にある施設を攻撃するが、殺人的傾向は無い。施設に対してはアクセスが許可されておらず、病原体や毒素を盗む機会も無い。生物テロに使われるエージェン

トの窃盗シナリオからは除外することができる。

共謀テロリストグループは、インサイダーとアウトサイダーであるテロリストグループを組み合わせたものである。ただし、より多くの人物を関与させるため、自らを発見される恐れがある。

1. A_{mo}：動機は、敵対者がなぜ病原体や毒素を盗もうとするのかを特徴づける。

0	敵対者は生物剤に関心が無い
1	窃盗は個人的利益のためと思われる（例：経済的または報復）
2	敵対者は政治的声明を出すことに関心がある
3	敵対者は小規模な生物テロ事件を起こそうとしている
4	敵対者は大規模な生物テロ事象、大量殺人、集団ヒステリー、あるいは壊滅的な経済的影響を引き起こすつもりである

2. A_{me}：手段は、敵対者の技術力、運用知識、およびシナリオの実行に必要なツール（生物剤の窃盗と使用）を特徴づけるものである。

0	敵対者はシナリオを実行する手段を備えていない
1	敵対者はシナリオを成功させる上で十分な手段を備えていない
2	敵対者は十分な技術力とツールを備えているが、運用知識がない
3	敵対者は十分な技術力とツール、および不完全ながら運用知識を備えている
4	敵対者は広範な技術力と運用知識、および必要なツールのすべてを備えている

3. A_{op}：機会は、敵対者が隠密に生物剤を盗めるか、あるいは公然と盗まなければならないかを特徴づけるものである。これは当該資産に対する敵対者のアクセスのレベルに基づくものである。

0	敵対者には施設に対する合法的アクセスが無い
1	敵対者には施設サイトに対する合法的サクセスしか無い
2	敵対者は当該資産のある建物に対しては同伴者なしのアクセス、および／または当該資産に対しては同伴者付きのアクセスを有している
3	敵対者は時折、当該資産に対する同伴者なしのアクセスを有している
4	敵対者は当該資産に対して常時同伴者なしのアクセスを有している、および／または年中時間を問わずに当該資産に対するアクセスを得る機会を有している

B.3　シナリオの作成（ステップ 2A）

次のステップは、本格的な評価を正当化するには不十分なリスクしかもたらさない資産をふるいにかけることである。第 2 章では、少なくとも中程度のベースラインリスクを伴わ

ない生物剤を全面的なリスク評価から除外することを検討した。一般的には多くの生物剤が、病原性が無いか、悪用されるリスクが低いため、ふるいにかけられる（表 B.1 参照）。さらに、上述のとおり、一定の敵対者については、生物剤には関心がなかったり、十分な手段を持ち合わせていなかったりするため、一定のシナリオから除外する必要がある。

低リスク資産と生物テロを起こす能力が無い、あるいは関心が無い敵対者を除外することで、全面的なリスク評価の範囲をより管理しやすい規模に絞り込むことができる。その一方で、リスク評価者とリスク管理者にはリスク評価の結果に確信を持たせることができる。

表 B.2 は、生物安全保障リスク評価にほぼ含まれるシナリオを示している。リスク評価者としては当然のことながら、施設の観点から重要と見なされるほかのシナリオを加えることもできる。EMUR に関しては、インサイダー、テロリストグループ、共謀テロリストグループが関与するシナリオを評価するのが適切と思われる。施設によっては、単独のテロリストは EMUR エージェントを盗む手段を備えていないものと考えられる。HMUR に関しては、テロリストグループ（または共謀テロリストグループ）には、当該エージェントの入手に関して評価対象となる特定施設を標的にする動機が不十分であると思われる。

表 **B.1**
生物安全保障リスク評価から除外される生物剤の例

属	種	生物学的安全性リスクグループ	生物安全保障リスク評価から除外される理由	生物安全保障リスクグループ
		バクテリア		
Acinetobacter（アシネトバクター）	*Calcoaceticus*（環境菌）	2	正常フローラ、日和見性病原体	低リスク
Staphylococcus（ブドウ球菌）	*aureus*（アウレウス）	2	環境に遍在する、日和見性病原体	低リスク
		ウィルス		
Parvoviridae（パルボウィルス）	*Canine pavovirus type 2*（イヌパルボウィルス　タイプ2）	2	ヒトの病原体では無い、共通、ワクチン入手可能	非病原性グループ
Picornavirus（ピコルナウィルス）	*Infectious encephalomyelitis*（伝染性脳脊髄炎）	1	ヒトに対して病原性なし	非病原性グループ
		菌類		
Candida（カンジタ）	*albicans*（アルビカンズ）	2	遍在する、軽度のヒトの病気を起こしうる	低リスク
Penicillium（ペニシリウム）	*Sp.*	1	遍在する、免疫システムが弱体化した宿主に感染したという報告はまれ	低リスク

表 **B.2**
本格的生物安全保障リスク評価におけるシナリオ

資産	敵対者	行動
EMUR	インサイダー	病原体または毒素の窃盗
EMUR	テロリストグループ	病原体または毒素の窃盗
EMUR	共謀テロリストグループ	病原体または毒素の窃盗
HMUR	インサイダー	病原体または毒素の窃盗
HMUR	テロリストグループ	病原体または毒素の窃盗
HMUR	共謀テロリストグループ	病原体または毒素の窃盗
HMUR	単独のテロリスト	病原体または毒素の窃盗
MMUR	インサイダー	病原体または毒素の窃盗
MMUR	単独のテロリスト	病原体または毒素の窃盗

B.4　脆弱性の評価（ステップ 2B）

生物安全保障リスク評価というコンテクストにおいて、このステップには必然的に、生物安全保障構成要素、すなわち物理的安全保障、人員安全保障、MC&A、輸送安全保障、情報安全保障、およびプログラム管理に関する既往の実施状況の評価が伴う。付録 A の脆弱性調査票に対する回答は、生物安全保障構成要素のそれぞれについて、0～4 の段階で施設の実施状況を格付けする上で役に立つ。

方程式 **B.7**　脆弱性の評価

$$V = V_{phy}w_{phy} + V_{per}w_{per} + V_{mca}w_{mca} + V_{t}w_{t} + V_{i}w_{i} + V_{pm}w_{pm}$$

V = Site vulnerability（サイトの脆弱性）

V_{phy} = Physical security vulnerability（物理的安全保障の脆弱性）

V_{per} = Personnel security vulnerability（人員安全保障の脆弱性）

V_{mca} = Material control & accountability vulnerability（物質管理とアカウンタビリティの脆弱性）

V_{t} = Transport security vulnerability（輸送安全保障の脆弱性）

V_{i} = Information security vulnerability（情報安全保障の脆弱性）

V_{pm} = Program management vulnerability（プログラム管理の脆弱性）

w_{phy} =　Weight of V_{phy} criterion（V_{phy} 評価基準の加重）

w_{per} =　Weight of V_{per} criterion（V_{phy} 評価基準の加重）

w_{mca} = Weight of V_{mca} criterion（V_{mca} 評価基準の加重）
w_t = Weight of V_t criterion（V_t 評価基準の加重）
w_i = Weight of V_i criterion（V_i 評価基準の加重）
w_{pm} = Weight of V_{pm} criterion（V_{pm} 評価基準の加重）

1. V_{phy}：この評価基準は、施設における現行の物理的安全保障対策の実施状況を捕捉するものである。生物化学研究所にふさわしいさまざまな物理的安全保障対策がある。施設としては、これらを常時、ほとんどの時間、ある程度の時間、もしくはたまに実施している、あるいは全く実施していないことが考えられる。今回の演習においては、次の物理的安全保障要素が施設において現在実施されている状況の検討を推奨する：研究室のアクセスコントロール、建物へのアクセスコントロール、サイトへのアクセスコントロール、施錠保管（例：冷蔵庫、冷凍庫）、建物における適切な夜間照明、建物の入り口が遮られずに見える状態、無許可アクセスを検知し、評価する能力（侵入センサー、警報、警報評価能力）。

0	物理的安全保障対策のすべてが常時またはほとんどの時間実施されている
1	物理的安全保障対策のうち少なくとも 50%は常時またはほとんどの時間実施されており、ほぼすべてが少なくともある程度の時間実施されている
2	物理的安全保障対策のうち少なくとも 50%は少なくともある程度の時間実施されており、ほぼすべてが少なくともたまに実施されている
3	一部の物理的安全保障対策が実施されている
4	物理的安全保障対策は全く実施されていない

2. V_{per}：この評価基準は、施設における現行の人員安全保障対策の実施状況を捕捉するものである。生物化学研究所にふさわしいさまざまな人員安全保障対策がある。施設としては、これらを常時、ほとんどの時間、ある程度の時間、もしくはたまに実施している、あるいは全く実施していないことが考えられる。今回の演習においては、次の人員安全保障要素が施設において現在実施されている状況の検討を推奨する：可能性のある従業員の経歴審査、立ち入り禁止区域における無許可人員に対する付き添い、キー割当て、バッジの使用、写真入り ID バッジの使用、離職する従業員に対する説明。

0	人員安全保障対策のすべてが常時またはほとんどの時間実施されている
1	人員安全保障対策のうち少なくとも 50%は常時またはほとんどの時間実施されており、ほぼすべてが少なくともある程度の時間実施されている
2	人員安全保障対策のうち少なくとも 50%は少なくともある程度の時間実施されており、ほぼすべてが少なくともたまに実施されている
3	一部の人員安全保障対策が実施されている
4	人員安全保障対策は全く実施されていない

3. V_{mca}：この評価基準は、施設における現行の MC&A 対策の実施状況を捕捉するものである。生物化学研究所にふさわしいさまざまな MC&A 対策がある。施設としては、これらを常時、ほとんどの時間、ある程度の時間、もしくはたまに実施している、あるいは全く実施していないことが考えられる。今回の演習においては、次の MC&A 要素が施設において現在実施されている状況の検討を推奨する：各 MMUR、HMUR、または EMUR に対して管理／説明責任のある人物が割り当てられている、必要の無い病原体や毒素は破棄されている、研究室の直接的監督者は研究室で使われる、あるいは保存されているすべての病原体と毒素を認識している、すべての病原体と毒素について最新のインベントリー（棚卸表）が存在している、当該インベントリーは物理的棚卸プロセスを通じて商号確認されている。

0	MC&A 対策のすべてが常時またはほとんどの時間実施されている
1	MC&A 対策のうち少なくとも 50%は常時またはほとんどの時間実施されており、ほぼすべてが少なくともある程度の時間実施されている
2	MC&A 対策のうち少なくとも 50%は少なくともある程度の時間実施されており、ほぼすべてが少なくともたまに実施されている
3	一部の MC&A 対策が実施されている
4	MC&A 対策は全く実施されていない

4. V_t：この評価基準は、施設における現行の輸送安全保障対策の実施状況を捕捉するものである。生物化学研究所にふさわしいさまざまな輸送安全保障対策がある。施設としては、これらを常時、ほとんどの時間、ある程度の時間、もしくはたまに実施している、あるいは全く実施していないことが考えられる。今回の演習においては、次の輸送安全保障要素が施設において現在実施されている状況の検討を推奨する：病原体や毒素の試料共有に先立って適切な許可を得ている、すべての輸送は文書に記録されている、搬出・搬入区域では安全な保管方法が用いられている、受取側研究室の検証が行われている、タイムリーな出荷方法が用いられている、所期の仕向地における確実な受取が確認されている、内部輸送管理手段が整備されている。

0	輸送安全保障対策のすべてが常時またはほとんどの時間実施されている
1	輸送安全保障対策のうち少なくとも 50%は常時またはほとんどの時間実施されており、ほぼすべてが少なくともある程度の時間実施されている
2	輸送安全保障対策のうち少なくとも 50%は少なくともある程度の時間実施されており、ほぼすべてが少なくともたまに実施されている
3	一部の輸送安全保障対策が実施されている
4	輸送安全保障対策は全く実施されていない

5. V_i：この評価基準は、施設における現行の情報安全保障対策の実施状況を捕捉するものである。生物化学研究所にふさわしいさまざまな情報安全保障対策がある。施設としては、これらを常時、ほとんどの時間、ある程度の時間、もしくはたまに実施している、あるいは全く実施していないことが考えられる。今回の演習においては、次の情報安全保障要素が施設において現在実施されている状況の検討を推奨する：コンピュータのパスワードが用いられている、重要文書にはマーキングが行われている、重要文書はうかつに公開されることがないよう保護さている、 評価・承認プロセスが整っている、コンピュータ・ネットワークセキュリティ対策が用いられている、重要文書は処分前に破棄されている。

0	情報安全保障対策のすべてが常時またはほとんどの時間実施されている
1	情報安全保障対策のうち少なくとも 50%は常時またはほとんどの時間実施されており、ほぼすべてが少なくともある程度の時間実施されている
2	情報安全保障対策のうち少なくとも 50%は少なくともある程度の時間実施されており、ほぼすべてが少なくともたまに実施されている
3	一部の情報安全保障対策が実施されている
4	情報安全保障対策は全く実施されていない

6. V_{pm}：この評価基準は、施設における現行の生物安全保障プログラム管理の実施状況を捕捉するものである。生物化学研究所にふさわしいさまざまなプログラム管理対策がある。施設としては、これらを常時、ほとんどの時間、ある程度の時間、もしくはたまに実施している、あるいは全く実施していないことが考えられる。今回の演習においては、次のプログラム管理要素が施設において現在実施されている状況の検討を推奨する：生物安全保障担当役員が指名されている、人員は適切な生物安全保障訓練を受けている、生物安全保障マニュアルが整備されている、SOP には生物安全保障が含まれている、研究所としては生物安全保障を実施する上で十分なリソースを用意している、リスク評価は毎年行われている、自主監査が毎年行われている、演習が毎年行われている、生物安全保障は生物安全性と統合されている、生物安全保障と生物安全性に負の影響を及ぼす恐れのある職員の個人的問題に対する気配りが行き届いている。

0	プログラム管理対策のすべてが常時またはほとんどの時間実施されている
1	プログラム管理対策のうち少なくとも 50%は常時またはほとんどの時間実施されており、ほぼすべてが少なくともある程度の時間実施されている
2	プログラム管理対策のうち少なくとも 50%は少なくともある程度の時間実施されており、ほぼすべてが少なくともたまに実施されている
3	一部のプログラム管理対策が実施されている
4	プログラム管理対策は全く実施されていない

B.5　各シナリオの脅威の潜在性と結果の評価

方程式 B.1 は、生物安全保障リスクが脅威の潜在性と最大限確実な結果の関数であること説明している。ふるいにかけられていないそれぞれのシナリオについて、リスクを特徴づけるには、脅威の潜在性と最大限確実な結果を分析しなければならない。脅威の潜在性とは、エージェントタスクの複雑さ、敵対者の属性、およびサイトの脆弱性の相関関係（関数）である。

方程式 B.8　脅威の潜在性

$$T = TCw_{TC} + Aw_A + Vw_V$$

TC = Agent task complexity（エージェントタスクの複雑さ）
A = Adversary attributes（敵対者の属性）
V = Site vulnerability（サイトの脆弱性）
w_{TC} = Weight of TC criterion（TC 評価基準の加重）
w_A = Weight of A criterion（TC 評価基準の加重）
w_V = Weight of V criterion（TC 評価基準の加重）