４．高度安全研究施設の必要性とそのセキュリティー確保に関する研究

分担研究者　森川茂（国立感染症研究所ウイルス第１部第１室室長）
協力研究者　西條政幸、倉根一郎（国立感染症研究所ウイルス第１部）

研究要旨：先進国ではエボラウイルスなどの高病原性病原体(biosafety level-4 病原体，BSL-4 病原体)を扱うことができる高度安全研究施設（BSL4 laboratory，BSL4 研究施設）の建設が進んでいる．BSL4 研究施設のネットワーク会議（International High Security Laboratory Network Meeting；国際高度安全実験室ネットワーク会議）での活動経験およびフランス国リヨン市に設置されている BSL4 研究施設での活動経験を踏まえ，BSL4 施設が稼働しない場合の問題点に関して考察した。さらに、BSL4 研究施設での BSL-4 病原体を用いた研究遂行におけるセキュリティー確保のための以下の提案をする．1）担当責任者による BSL4 研究施設の機能評価（連日），2）BSL4 研究施設の混雑の回避，3）複数の研究者による研究の遂行（一人では，可能な限り BSL4 研究施設には入室しない），4）研究者同士の情報公開(BSL4 研究施設で行われているそれぞれの研究プロジェクトに関する情報の共有化)，5）BSL-4 病原体が保管されている冷凍庫の鍵へのアクセス制限，6）研究者以外の共同作業者(技術専門家，BSL4 施設運営のための事務職員など)の技術・意識向上，等が，BSL4 研究施設安全にかつ効率的に稼働し，感染実験を行う上で大変重要なポイントである．

はじめに

近年，SARS や高病原性トリインフルエンザウイルスによるヒトでの感染症など，新興ウイルス感染症の発生が続いている．また，1960 年代に確認されたマールブルグ出血熱や 1970 年代に確認されたエボラ出血熱の発生頻度が高まっているだけでなく，その発生地域が拡大しつつある．特に 2004 年にアンゴラで発生したマールブルグ出血熱の流行では，約 400 名にのぼる患者が発生し，その多くが死亡した（致死率ほぼ 90％）．また，1970 年代後半に地球上から根絶された天然痘が，天然痘ウイルスが用いられるバイオテロリズムにより再びその流行が発生する危険性が指摘され，わが国を含むいくつかの先進国では痘そうワクチン再生産と備蓄がなされている．このような状況で，世界各国で既存の高度安全研究施設（いわゆる BSL4 研究施設）の機能拡大に加えて，新規の BSL4 研究施設の建設が進んでいる．

このような背景から、G7 にメキシコを加えた８カ国の研究所からなる世界健康安全保障グループラボラトリーネットワーク（Global Health Security Action Group Laboratory Network、GHSAGLN)が平成 14 年に設立された。GHSAGLN の答申を受けて、世界の BSL4 実験施設保有研究所のネットワークである International High Security Laboratory Network Meeting（IHSLNM，国際高度安全実験室ネットワーク会議)が平成 14 年に設立され、米国、英国、カナダ、フランス、ドイツ、オーストラリア、日本、南アフリカ、ロシア、スウェーデンの BSL4 実験室担当者が出席している。国立感染症研究所からは、分担研究者の森川がメンバーとして参加している。IHSLNM は、これまでに平成 14 年、16 年の 2 回開催され、特に BSL4 病原体の診断法の標準化作業に関して、標準標本を用いて RT-PCR，PCR，抗原検出法の各国の試験法の感度、精度の比較検討が行われつつある。

A．研究目的：

わが国においては国立感染症研究所(村山庁舎）にグローブボックスタイプの BSL4 研究施設が 20 年程前に建設され設置されているにも係らず，未だに BSL4 研究施設として稼働されていない．現状では，P3 研究施設として使用

されている.

国立感染症研究所ウイルス第1部では,エボラ出血熱,マールブルグ出血熱,クリミア・コンゴ出血熱,ラッサ熱の診断法の開発を業務のひとつとしているが,上記の理由から感染性のあるエボラウイルス,マールブルグウイルス,クリミア・コンゴ出血熱ウイルス,ラッサウイルスを扱うことができないため,ウイルス性出血熱に関する研究を行うのが困難な状況にある.そのため,2005年春に,協力研究者である西條がフランス国リヨン市に設置されている国立健康医学研究所(National Institute of Health and Medical Research)所属のBSL4研究施設でウイルス性出血熱診断法の開発に関する共同研究を行なった.また,我々は国立感染症研究所(村山庁舎)に設置されているグローブボックス型高度安全研究施設において感染実験を行う経験を積んでいる.両研究施設での経験を踏まえて,BSL4研究施設で高病原性病原体(エボラウイルスなど)を用いた感染実験を遂行する際のセキュリティー確保にする考察を行なう.

B. 研究方法:

1. IHSLNM(国際高度安全実験室ネットワーク会議)のこれまでの経緯と役割に関して明らかにする。

2. フランスの国立健康医学研究所(National Institute of Health and Medical Research)所属のBSL4研究施設でウイルス性出血熱診断法の開発に関する共同研究を行なった経験及び国立感染症研究所(村山庁舎)に設置されているグローブボックス型高度安全研究施設における感染実験の経験を踏まえて,BSL4研究施設で高病原性病原体(エボラウイルスなど)を用いた感染実験を遂行する際のセキュリティー確保に関する考察を行う.

C. 研究成果及び D. 考察

1. IHSLNMでは、これまでカナダのBSL実験室(Canadian science center for human and animal health)が調整したガンマ線不活化エボラウイルスのパネルサンプルを用いて、RT-PCRと抗原検出の各国のシステムの比較検討を行った。その結果、国立感染症研究所のシステムが他の参加国のシステムと比較して充分の感度であることが明らかとなった。しかし、ガンマ線不活化エボラウイルスのパネルサンプルの調整及び配布に要したコストは6,000米ドルであり、今後、他のBSL4病原体のパネルサンプルを用いた評価を行うに当たり、資金源の確保が急務であることが認識された。

一方、シンガポール、台湾、中国でのSARS実験室感染事故、USAMRIIDでのエボラウイルス事故接種の可能性がある事例、ロシアのエボラウイルス実験室感染事故(感染した研究者が死亡している)に関して検討され、実験従事者のトレーニング、GMP、病原体使用記録等の保管を各国とも徹底することの重要性が議論された。また、バイオテロ対策としてレベル4の病原体を扱う研究機関のセキュリティーが強化されている。新興感染症の病原体は米国のCenters for Disease Control and Prevention (CDC)で分離されることが多く、他機関への病原体やそのcDNAの分与は規制が強化されている。すなわち、BSL4が米国のセキュリティー基準を満たして稼働していない場合、新たに分離同定されたレベル4に相当する新興ウイルスに関しては、そのcDNAさえも分与不可能であるとの説明がなされた。他国のBSL4研究施設では、この基準に準拠するような体制を取っているため、ある程度の時間は要しても病原体あるいはその遺伝子を分与され、実験室診断体制を構築できる。国立感染症研究所が現状のままであれば、今後新たなレベル4の新興感染症が発生した場合、その診断系を確立することが不可能になる危惧が極めて高いと言わざるを得ない。

2. 世界各国に設置されているBSL4研究施設でのウイルス性出血熱に関する研究の現状

1967年にウガンダからドイツおよび旧ユーゴスラビアに輸出されたアフリカミドリザルの組織を扱った研究者らが出血熱症状を呈し,これらの患者からマールブルグウイルスが分離されたのがマールブルグ出血熱の存在が確認された初めての出来事であった.マールブルグ出血熱は,その後ケニヤや

ジンバブエでそれぞれ散発的に発生していただけであったが，1999 年にはコンゴ民主共和国で 100 名を，2004 年にはアンゴラでそれぞれ 300 名を超える数におよぶマールブルグ出血熱の大規模な流行が発生した．コンゴ民主共和国およびアンゴラにおける流行では，BSL4 研究施設を有する CDC およびカナダの Canadian science center for human and animal health がその対応にあたった．最近，エボラウイルスの自然宿主がアフリカに生息するコウモリであることが解明された．これも，フランスおよびガボンの BSL4 研究施設で行われた特筆すべき業績である．さらに，カナダ，米国，フランス，ドイツの BSL4 研究施設共同でエボラウイルスやマールブルグウイルスに対する有効なワクチンが開発されている．このように，BSL4 研究施設を有する研究機関では，出血熱ウイルスに関する基礎研究のみならず，公衆衛生上有意義な業績が積み重ねられつつある．

3. BSL4 研究施設での研究テーマの選定

BSL4 研究施設で行われるべきテーマについては，責任ある立場の者からなる委員会で決定され，研究施設使用のための調整がなされるシステムを構築する．

4. BSL4 研究施設で感染実験を行う研究者の資質・条件

BSL4 研究施設では，致死率の高い感染症を起こす病原体［いわゆる biosafety level-4（BSL-4）病原体］が扱われる研究がなされる．そのため，扱われている病原体に研究者が事故・不注意により感染するのを防御することと，病原体が研究施設外に漏れでないような気密性が求められている．そのためには，BSL4 研究施設で研究を遂行する研究者の資質・条件（技術，経験など）が設定されなければならない．1）P2 および P3 レベルの感染実験の経験（合計時間とその研究内容），2）研究者のワクチン接種歴，3）緊急事態（火災など）が発生した場合の対応に関する能力，4）研究者同士そして共同作業者らとの協調性，等が，BSL4 研究施設で感染実験を行う研究者に求められる資質・条件であると考えられる．BSL4 研究施設で感染実験を行う者は，各種病原体に関する十分な知識を有すること，研究を遂行するための十分な技術を習得していることが基本的に求められる．そのため BSL4 研究施設で研究する者には，P2 や P3 レベルの感染実験の経験を十分積んでいるということが当然前提となる．BSL4 研究施設で用いられる病原体が起こす感染症に類似の疾患を起こす病原体の中で，ワクチンが開発されているものについては可能な限りワクチン接種を義務づけることが必要か考えられる．例えば破傷風・ジフテリア・百日咳ワクチン，黄熱ワクチン，痘そうワクチンなどである．また，研究者は心身ともに健康であることが求められる．体調が優れない時には事故が発生しやすいことは自明のことであり，BSL4 研究施設で研究業務に係る者の健康管理には，十分な気を配ることが重要なことであろう．BSL4 研究施設においては，火災や地震などの緊急事態が発生した場合に対する適切な対応が，他の研究施設におけるそれらに比べて，より厳密に求められる．そのためには，火災に対する鎮火作業，地震対策などに適切に対応できるよう，火災訓練や地震災害訓練を受けることを義務化する必要があろう．そして，BSL4 研究施設で研究活動を行う者により重要な資質として求められるものに，研究者間，共同作業者と十分な意思の疎通がはかられるための高い協調性がある．この協調性をなくして安全な BSL4 研究施設での感染実験はありえないと考えるべきである．

5. BSL4 研究施設での感染実験遂行におけるセキュリティー確保のための条件・システム

1） BSL4 研究施設のセキュリティー機能評価．毎日，早朝に（時間を決めて）BSL4 研究施設のセキュリティー機能を，責任担当者（2 名）がチェックし，BSL4 研究施設の機能が正常に稼働していることを確認し，その日の BSL4 研究施設の使用の可否を決定する．重要なことは，セキュリティーチェック担当者が専門的に BSL4 研究施設の機能評価を行い，その責任が研究者に求められることのないようにすることである．あくまでも毎日 BSL4

研究施設の機能状況が責任担当者によりチェックされ，正常に稼働されていることが確認された後に，研究者がBSL4研究施設内に入室できるシステムを構築することが必要であろう．

2) BSL4研究施設での感染実験時間帯．できるだけ多くの研究者や共同作業者が任務にあたっている時間帯に研究を開始し，終了できるような研究計画を立てる．不要に時間外にBSL4研究施設内で研究活動を行うことのないようにする．夜間に研究活動を行っている時に，何らかの事故が発生したとしても，共同研究者や共同作業者と協力して対応にあたることができない．また，夜間の研究活動においては疲労が高まっていること，それに伴い感染事故の頻度が高まることが予想される．可能な限り，日中の時間帯での研究活動が求められる．

3) BSL4研究施設での研究時間．BSL4研究施設での研究活動においては，長時間継続して活動を行うことのないようにする．BSL4研究施設では，防御服を着用した上で研究活動を行う必要があり，P2やP3研究施設で行う研究に比較してより疲労がたまりやすい．疲労が高まれば，それだけ感染事故を起こす可能性が高まる．研究活動は，1日に午前中だけ，または午後だけに限定してできるだけ4時間以上継続して行わない，または，長時間継続して研究活動を行う場合には，2時間ごとに適度に休養を取る，などを義務づける必要があろう．

4) BSL4研究施設が設置されている建物へ入室する時点のチェック．BSL4研究施設が設置されているフロアーに入室するゲート（BSL4研究施設への入室はそのゲートを通った後に可能）には，BSL4研究施設管理室が設置され，BSL4研究施設が設置されているフロアーに入室する者のチェックを行う．フランス国リヨン市に設置されている高度安全研究施設（BSL4 laboratory，BSL4研究施設）では，担当者が管理室でBSL4研究施設に入室する者を直接チェックしている．BSL4研究施設にアクセスするにはこのゲートを通らなければならず，不審者のBSL4研究室への入室は不可能となる．もちろんこのフロアーにアクセスできる者は，ICチップの埋め込まれているIDカードを所持している許可された限られた者またはそのような者と同伴の者しか可能ではない．

5) BSL4研究施設への入室時の手続き．フロアーゲートを通り，BSL4研究施設に入室するにあたり，セキュリティー管理部門に，トランシーバー（この無線トランシーバーを用いてBSL4研究施設内での研究者間または管理部門との会話がなされる）を用いて氏名を伝え，誰がBSL4研究施設に入室するかを明瞭に伝える．このことにより，セキュリティー担当者がBSL4研究施設に入室する者を把握する．入室しようとする研究者は，セキュリティー担当者の了解が得られた段階で初めてBSL4研究施設に入室が可能となる．

6) BSL4研究施設入室にあたって．BSL4研究施設に入室する際には，ゲートに感染実験に用いる病原体を記述しする．この記述によりその日のBSL4研究施設内で感染実験に用いられる病原体の種類が公開される．このことにより，他の研究者や共同作業者が，BSL4研究施設内でどのような研究活動がなされていることかを理解することができ，ひいては，感染事故の危険性を低めることが可能となる．入室時間も明瞭に記載する．

7) BSL4研究施設に入室後．BSL4研究施設に入室したら，次のステップを積んで，実験可能空間に入る．順に着替え室，シャワー室，防御服脱着室，ケミカルシャワー室を経て，実験可能空間に至る．各室では，それぞれ，着替え，防御服の着用（シャワーおよびケミカルシャワーは，入室時には行わない）を終え，BSL4研究室に入室する．トランシーバーを通じて，管理者に自分がどこにいるのかを随時伝える．特にケミカルシャワールームから研究室に入室した時には，その由をセキュリティー担当者に伝える．このような入室する者とセキュリティー管理者との意思の疎通は，退出時にも行われる．

8) 複数の研究者が同時にBSL4研究施設に入室して活動する．決して単独でBSL4研究施設内で研究活動を行わないようにする．これはBSL4研究施設内で突発的な緊急事態が発生した場合にも，適切に対応するために必要

な事項である.

9) 病原体保管冷凍庫の施錠. エボラウイルスをはじめとする BSL-4 病原体を保管している冷凍庫には確実に施錠が施され, その鍵を保管するための保管金庫が設置される必要がある. つまり, BSL-4 病原体にアクセスするためには, 保管されている冷凍庫の鍵が収納されている金庫にアクセスできる立場の者の責任においてなされると言うことである. このようにして, BSL-4 病原体に簡単に誰でもアクセスできないようにして, セキュリティー確保に努める必要がある.

10) 研究活動と消毒. BSL4 研究施設内で感染実験業務を終えた場合には, 適切な消毒剤を用いて汚染されたと考えられる器具・装備等を消毒・滅菌する. 感染事故を防ぐためには重要な事柄である.

11) 感染実験終了時の手続き. 感染実験終了後の退出時の手続きに関して, 以下の事項について提言したい. 研究活動を終えたことを, トランシーバーを通じてセキュリティー管理者に伝える. ケミカルシャワー室に入室した時にもその由をセキュリティー担当者に伝え, 防御服にケミカルシャワーをかけ, 防御服に付着している病原体の消毒を行う. 消毒されない部位が生じないように注意深くケミカルシャワーを浴びるのはもちろんのことである. ケミカルシャワー終了後, 防御服脱着室に入室し, 防御服を脱ぎ, 次いでシャワールームに入室してシャワーを浴びる. このようにして研究作業者に BSL-4 病原体が付着して研究室外に出ることのないようにシステムを構築する. 最後に着替え室で着替えをして, BSL4 研究施設外にでる. この時点でも BSL4 研究施設外に出たことをセキュリティー管理者に伝え, 無事研究活動が終了したことを伝えると同時に, 外出時間を記載する.

6. BSL4 研究施設稼働のための研究者以外の共同作業者 (co-workers) の役割

研究者と BSL4 研究施設維持のための共同作業者との役割分担を明確にし, 研究者に過剰な業務が強いられないようにすることが, 感染事故を防ぐ上で重要なことである. わが国においては往々にして, 研究施設使用者である研究者にセキュリティーの管理まで求められることが多い. しかし, 合理的な研究活動がなされることが最も重要なことであり, それが感染事故を防ぐ上で重要なことであると考えられる. また, 研究者は BSL4 研究施設内でどの様な研究を行っているかを定期的に共同作業者に伝え, また, 意見交換を行うことを通じてお互いの意思の疎通を図ることが, 効率的に, しかも, 安全に研究成果を得る上で重要と考えられる.

7. BSL4 研究施設の機器の保守

フランス国リヨン市に設置されている BSL4 研究施設では, BSL4 研究施設内で使用する機器の保守, 修理などの技術を有するバイオセーフティー・セキュリティー部門のスタッフが, 機器の故障時の対応にあたっている. このような体制は, 機器故障時に実験を停止し, 実験室をホルマリン蒸気滅菌して機器を搬出して修理する方式に比べて, 極めて効率的に実験を遂行することが出来る. 一方, カナダの BSL4 研究施設では, 機器故障時に機器を滅菌して搬出するパスルームが設けられており, 実験を停止することなく機器の修理等が出来るシステムを採用している. 上記のいずれかの体制が BSL4 研究施設には必要である.

E. 結論

IHSLNM での合意に基づいて行われたエボラウイルス検出系の評価により、BSL4 研究施設が稼働していない我が国にとっては非常に有用な情報を得ることができた。しかし、予算の問題などで未だ充分なパネルサンプルが作製できない状況にある。そこで、フランスの国立健康医学研究所との共同研究により、マールブルグ、ラッサウイルスの検出系、抗体検出系の評価を行うことができた。また、この共同研究での BSL4 研究施設での作業経験に基づいて, BSL4 研究施設における感染実験のセキュリティー確保に関して考察した. BSL4 研究施設の構造上のセキュリティーに加えて, BSL4 研究施設の運用上のセキュリティーが感染事故を

防止する上で大変重要であると認識している．研究者のみならず，BSL4 研究施設の運営に係る共同作業者の役割も大変重要である．特に研究活動に係る情報を個々の研究者が保持するのではなく，BSL4 研究施設運営に係る者の間で共有することの重要性を認識した．

バイオテロ対策としてBSL4研究施設のセキュリティーが強化されている。CDC等では、他機関への病原体やそのcDNAの分与は規制が強化され、今後、新たなレベル４病原体が新興した場合、cDNA の入手も困難になると予想される。さらに、新興・再興感染症の発生が続いている今日，現在国立感染症研究所村山庁舎に設置されているBSL4研究施設の稼働や新規BSL4研究施設の建設の必要性が高まっている．より安全なBSL4研究施設においてなされる研究を通じて，今日増加しつつある新興・再興感染症対策にこれまで以上に貢献したいと考えている．

F. 健康危機管理情報

特になし

G. 研究発表

1. 論文発表

1. Mizutani T, Fukushi S, Iizuka D, Inanami O, Kuwabara M, Takashima H, Yanagawa H, Saijo M, Kurane I, Morikawa S. Inhibition of cell proliferation by SARS-CoV infection in Vero E6 cells. FEMS Immunol Med Microbiol. 2006 Mar 1;46(2):236-43.
2. Mizutani T, Fukushi S, Saijo M, Kurane I, Morikawa S. Regulation of p90RSK phosphorylation by SARS-CoV infection in Vero E6 cells. FEBS Lett. 2006 Feb 20;580(5):1417-24. Epub 2006.
3. Tang Q, Zhao XQ, Wang HY, Simayi B, Zhang YZ, Saijo M, Morikawa S, Liang GD, Kurane I. [Molecular epidemiology of Xinjiang hemorrhagic fever viruses] Zhonghua Shi Yan He Lin Chuang Bing Du Xue Za Zhi. 2005 Dec;19(4):312-8. Chinese.
4. Morikawa S, Sakiyama T, Hasegawa H, Saijo M, Maeda A, Kurane I, Maeno G, Kimura J, Hirama C, Yoshida T, Asahi-Ozaki Y, Sata T, Kurata T, Kojima A. An attenuated LC16m8 smallpox vaccine: analysis of full-genome sequence and induction of immune protection. J Virol. 2005 Sep;79(18):11873-91.
5. Matsuyama S, Ujike M, Morikawa S, Tashiro M, Taguchi F. Protease-mediated enhancement of severe acute respiratory syndrome coronavirus infection. Proc Natl Acad Sci U S A. 2005 Aug 30;102(35):12543-7.
6. Fukushi S, Mizutani T, Saijo M, Matsuyama S, Miyajima N, Taguchi F, Itamura S, Kurane I, Morikawa S. Vesicular stomatitis virus pseudotyped with severe acute respiratory syndrome coronavirus spike protein. J Gen Virol. 2005;86(Pt 8):2269-74.
7. Saijo M, Tang Q, Shimayi B, Han L, Zhang Y, Asiguma M, Tianshu D, Maeda A, Kurane I, Morikawa S. Antigen-capture enzyme-linked immunosorbent assay for the diagnosis of crimean-congo hemorrhagic fever using a novel monoclonal antibody. J Med Virol. 2005;77(1):83-8.
8. Mizutani T, Fukushi S, Saijo M, Kurane I, Morikawa S. JNK and PI3k/Akt signaling pathways are required for establishing persistent SARS-CoV infection in Vero E6 cells. Biochim Biophys Acta. 2005;1741(1-2):4-10.
9. Saijo M, Morikawa S, Fukushi S, Mizutani T, Hasegawa H, Nagata N, Iwata N, Kurane I. Inhibitory effect of mizoribine and ribavirin on the replication of severe acute respiratory syndrome (SARS)-associated coronavirus. Antiviral Res. 2005 ;66(2-3):159-63.
10. Ohnishi K, Sakaguchi M, Kaji T, Akagawa K, Taniyama T, Kasai M, Tsunetsugu-Yokota Y, Oshima M, Yamamoto K, Takasuka N, Hashimoto S, Ato M, Fujii

H, Takahashi Y, Morikawa S, Ishii K, Sata T, Takagi H, Itamura S, Odagiri T, Miyamura T, Kurane I, Tashiro M, Kurata T, Yoshikura H, Takemori T. Immunological detection of severe acute respiratory syndrome coronavirus by monoclonal antibodies. Jpn J Infect Dis. 2005;58(2):88-94.

11. Hatakeyama S, Moriya K, Saijo M, Morisawa Y, Kurane I, Koike K, Kimura S, Morikawa S. Persisting humoral antiviral immunity within the Japanese population after the discontinuation in 1976 of routine smallpox vaccinations. Clin Diagn Lab Immunol. 2005;12(4):520-4.
12. Endoh D, Mizutani T, Kirisawa R, Maki Y, Saito H, Kon Y, Morikawa S, Hayashi M. Species-independent detection of RNA virus by representational difference analysis using non-ribosomal hexanucleotides for reverse transcription. Nucleic Acids Res. 2005;33(6):e65.
13. Saijo M, Ogino T, Taguchi F, Fukushi S, Mizutani T, Notomi T, Kanda H, Minekawa H, Matsuyama S, Long HT, Hanh NT, Kurane I, Tashiro M, Morikawa S. Recombinant nucleocapsid protein-based IgG enzyme-linked immunosorbent assay for the serological diagnosis of SARS. J Virol Methods. 2005;125(2):181-6.
14. Saijo M, Niikura M, Maeda A, Sata T, Kurata T, Kurane I, Morikawa S. Characterization of monoclonal antibodies to Marburg virus nucleoprotein (NP) that can be used for NP-capture enzyme-linked immunosorbent assay. J Med Virol. 2005;76(1):111-8.
15. Okada M, Takemoto Y, Okuno Y, Hashimoto S, Yoshida S, Fukunaga Y, Tanaka T, Kita Y, Kuwayama S, Muraki Y, Kanamaru N, Takai H, Okada C, Sakaguchi Y, Furukawa I, Yamada K, Matsumoto M, Kase T, Demello DE, Peiris JS, Chen PJ, Yamamoto N, Yoshinaka Y, Nomura T, Ishida I, Morikawa S, Tashiro M, Sakatani M. The development of vaccines against SARS corona virus in mice and SCID-PBL/hu mice. Vaccine. 2005; 23 (17-18):2269-72.

2．知的財産権の出願・登録（予定を含む）
特許取得：該当なし

3．学会発表

1. Mizutani T, Fusushi S, Saijo M, Kurane I, Morikawa S. Importance of JNK and PI3K/Akt signaling pathways for establishing persistant SARS-CoV infection in Vero E6 cells. Xth International Nidovirus Synposium. 2005年6月, Colorado Springs, CO, USA
2. Nagata N, Iwata N, Hasegawa H, Asahi-Ozaki Y, Sato Y, Harashima A, Morikawa S, Saijo M, Itamura S, Saito T, Odagiri T, Tashiro M, Ami Y, Sata T. Pathological and virological analyses of SARS-CoV infections in experimental animals. Xth International Nidovirus Synposium. 2005年6月, Colorado Springs, CO, USA
3. Fukushi S, Mizutani T, Saijo M, Matsuyama S, Taguchi F, Kurane I, Morikawa S. Pseudotyped vesicular stomatitis virus for functional analysis of SARS-CoV spike protein. Xth International Nidovirus Synposium. 2005年6月, Colorado Springs, CO, USA
4. Saijo M, Ami Y, Nagata N, Hasegawa H, Fukushi S, Mizutani T, Iwata N, Suzaki Y, Sata T, Kurane I, Morikawa S. Highly attenuated vaccinia vaccine, LC16m8, protects monkeys from monkeypox. XIIIth International Congress of Virology. 2005年7月, San Francisco, CA, USA
5. Saijo M, Ami Y, Nagata N, Hasegawa H, Fukushi S, Mizutani T, Iwata N, Suzaki Y, Sata T, Kurane I, Morikawa S. Protection

of non-human primates from monkeypox by highly attenuated vaccinia vaccine, LC16m8, that lacks expression of B5R membrane protein. US-Japan Cooperative Medical Science Program 39th Virology Panel Meeting. 2005年7月, San Francisco, CA, USA

6. 西條政幸, 網康至, 永田典代, 緒方もも子, 福士秀悦, 水谷哲也, 長谷川秀樹, 岩田奈織子, 佐多徹太郎, 倉根一郎, 倉田毅, 森川茂. LC16m8痘そうワクチンによるカニクイザルにおけるサル痘発症予防効果（続報）. 第53回日本ウイルス学会学術集会. 2005年11月, 横浜
7. 水谷哲也, 福士秀悦, 西條政幸, 緒方もも子, 倉根一郎, 森川茂. SARSコロナウイルス感染細胞におけるAktリン酸化の重要性. 第53回日本ウイルス学会学術集会. 2005年11月, 横浜
8. 福士秀悦, 水谷哲也, 西條政幸, 緒方もも子, 倉根一郎, 森川茂. VSVシュードタイプを用いたSARS-CoV感染の解析. 第53回日本ウイルス学会学術集会. 2005年11月, 横浜
9. 永田典代, 岩田奈織子, 長谷川秀樹, 福士秀悦, 西條政幸, 森川茂, 佐藤由子, 佐多徹太郎. マウス, ラットを用いた経代によるSARS-CoVの病原性の変化. 第53回日本ウイルス学会学術集会. 2005年11月, 横浜
10. 福士秀悦, 水谷哲也, 西條政幸, 倉根一郎, 森川茂. SARS-CoVスパイクタンパク質とACE2の相互作用のVSVシュードタイプを用いた解析. 第28回日本分子生物学会年会. 2005年12月, 博多

Ⅲ. 資　料

1

Security Considerations for Microbiological and Biomedical Facilities

by Chris Royse & Barbara Johnson

Introduction

In recent years, increasing questions have arisen regarding the adequacy of and need for the implementation of a security program in biomedical institutes and facilities working with and storing pathogens. Most of the concern has been focused on facilities working with and storing select agents and BSL-4 pathogens. In some instances, increased security, protective measures, and regulations have been promulgated and implemented as a result of 1) criminal activity by animal rights activists, 2) the necessity to protect intellectual rights/information, patent material/processes and business sensitive information, and 3) recognition of the potential for individuals or organized groups to obtain biological pathogens for criminal/terrorist use.

This paper appears in the ABSA publication, **Anthology of Biosafety V - BSL4 Laboratories**

The diversity of these concerns is applicable to a wide range of institutes in the biotech industry that include: animal housing and breeding facilities, research institutes conducting work with animals, institutes conducting research with dangerous pathogens, pathogen repositories, and pharmaceutical and biotechnical companies. The concerns may also apply to other organizations, such as: diagnostic facilities, medical centers and universities conducting work with pathogens, and other businesses that are involved in handling, transportation, or other forms of work with pathogenic material. In considering the diversity of the types of organizations that may work with pathogens, it becomes evident that there is not one solution for all needs. In the same way a biological safety risk assessment is conducted at institutes preparing to work with pathogens, so should a security risk assessment be performed. Hence, each organization will develop and implement a security program based on their risk assessments, evaluation of problems and solutions, consideration of mission requirements and constraints, and level of acceptable risk. The authors would like to stress that it is not the objective of this chapter to define acceptable risk, solution requirements, or develop policy.

The objective of this chapter is to provide the reader with information regarding potential components of a security program, and the tools for developing a decision matrix to determine the security needs of their facility. The intent is to provide a set of decision considerations that can be applied across a vast spectrum of facilities/institutes, not a set of solutions

In an attempt to develop a systematic and rational approach to defining a successful, cost effective security program, this chapter will review:

- Concept of security management,
- Security plan development,

- Personnel considerations,
- Technical considerations,
- Operational considerations.

Concept of Security Management

The word security, "freedom from danger or anxiety". (Webster, 1992) often has a negative connotation not only by those intending to do harm, but also by those who are the recipients of protective services within a facility or institute. To many people, security is equated with limited access to facilities, materials, information exchange, and possibly colleagues, via fences, guards, locks, areas of restricted access, or other measures designed to keep people apart. Competent security management does not have to unduly interfere with the day to day activities of scientific personnel or act as an impediment to conducting research in a pleasant and professional setting. It is ultimately the role of the director of the facility or institute, through consultation with staff, to determine and provide the appropriate level of security and security oversight at their institute.

The Security Management Concept is a systematic process designed to develop rational and cost-effective physical security program strategies in order to protect critical facility assets. This system must take into account the actual, measurable assets of the program (i.e., personnel, products, patents, proprietary and personnel sensitive information, and hazardous materials) as well as the intangible essential mission functions (academic freedom, collaboration, and personal rights). Part of this process involves selecting countermeasures (preventative measures) appropriate to the level of risk that management is willing to accept.

Just as one of the key elements in a successful Biosafety Program is to identify risk and take actions to prevent accidents/incidents, the key to proper Security Management is to identify and reduce the risk of an adverse incident occurring. Security, like Biosafety, is often funded from an institutes "overhead or indirect budget." Therefore, Security Management is typically accomplished within the constraints of already tight financial resources due to inevitable competition for funding. The best way to understand how security at any facility or institute is to be managed is to identify existing security requirements at the Federal, State, local and Corporate levels, and understand the mission of the facility or institute which must be protected. In the case of security involving biological materials, there are scant established rules and guidelines. (http://www.cdc.gov/od/ohs/lrsat/regmat.htm, 2001). Institutes are largely on their own to develop a security plan that accurately reflects and address their needs. This is not necessarily bad. Due to the diverse types of institutes, mission objectives, assets, as well as numerous other factors, it is probably beneficial that each institute be able to develop a security plan that is tailored to its needs.

Security Management is as much an issue of establishing a state of mind as it installing a suite of technical equipment or measures. It is a concept that is hard to accept as a necessity, until an adverse incident occurs. Once an incident occurs, it is often too late to take the appropriate steps rapidly enough to prevent or decrease losses. Security Management is a cost/benefit analysis. It clearly states what is necessary to secure and what is expendable. A well-devised security management concept takes into account personnel, technical, and operational considerations. Also, the development of a security plan will help those charged with making decisions for the facility or institute understand the status of their assets, vulnerabilities, risk factors, current and acquirable preventative measures, and potential for loss (as a function of their actions or lack of action).

The Security Plan

As various equities are at stake, one model for development of a security working group calls for interactive relationships and overlap in responsibility between the principle players. The development of a coordinated and comprehensive security plan should be academic in its approach. A competent plan requires open communication, education of team players, joint participation of the security and other staff, compromise in both design and desires, and continuous updating. This exercise provides an opportunity to bring staff together with their security specialist counterparts as a team. The principals include, but may not be limited to the offices of security, biosafety, emergency response (local fire and police), and the scientific director or program manager. Depending on the prioritization of mandatory secured items, team members may be expanded to include the occupational health staff, industrial hygienist, radiological safety officer, veterinarian, public affairs officer, etc. In cases where security is concerned with safeguarding biological materials, the security plan should be closely coordinated, if not interwoven into the appropriate elements of the institutes biosafety program. Some members of the team will play a predominantly security oriented technical and policy role in the assessment process, while others will be more involved in providing technical information on the current status of capabilities and mission requirements. The team, which is developed, will vary depending on the goals of the senior management and the mission of the institute, but the core team should be fairly consistent at the programmatic level to maintain continuity. While security will lead the effort, the consensus and descending comments should be provided to the senior management for an ultimate decision regarding implementation.

Security Management is the Management of Security Risks

Security Management and the Management of Security Risks are synonymous, i.e., they are concepts which enable those charged with the responsibility for the research or production at a biotechnical/biomedical facility or institute to mitigate the chances of an adverse security event from happening. Security and Security Risk Management begin with a Security Risk Analysis. Suggestions for proper Security Risk Analysis come in many different forms, but all are essentially comprised of the same elements (see Tables I and II in the appendix for a quick reference guide). A good example of a Security Risk Analysis outline can be found in Jopeck's article "Five Steps to Risk Reduction". (Jopeck, 2000). Jopeck contends that a Security Risk Analysis is comprised of these steps (see also Appedix, Table 1):

- Asset assessment,
- Threat assessment,
- Vulnerability assessment,
- Risk assessment,
- Countermeasures.

Asset Assessment

Assets include, but are not limited to the facility's or institute's:

- Land that it physically rests upon,
- Infrastructure (air handling, power, water, sewage, etc.)
- Equipment and materials,
- Information/intellectual property, whether it be research, development or production,

- Staff.

The security working group must identify those things possessed by the facility or institute that are assets and are therefore potential targets. One technique is through interviews "Program Managers, Facilities Managers and Computer Systems Managers". (Jopeck, 2000). The assets must be prioritized from most important to least important. Importance should be determined by the a facility's or institute's director, but can usually be based upon:

- Time - how much time will it take to recover or replace the asset?
- Cost - how much will it cost to replace the asset?
- Customers - how many customers may be lost or not gained do to delays cause by asset loss?

In the case of facilities working with select or other dangerous agents, the question may also be asked, "Potential damage - what is the impact of the intentional use or release of this agent".

When ranking assets, one suggestion is to consult the facility's or institute's Business Impact Analysis (BIA). A BIA identifies and addresses the company's exposure to business disruption, the impact on the company of this exposure, steps the company can take to address it, and how much those solutions cost. (Myatt, 1999). If a BIA has not been conducted before, it would be prudent to complete one during the time the asset analysis is being conducted. The results of the asset assessment is a worksheet that identifies and maps valued assets and their relationships to one another. (Jopeck, 2000).

Threat Assessment

At the programmatic level, it is the role of the senior management (i.e., University Chancellor, Institute Director, Commander, etc.) to ensure that the perceived threats to the institute, as well as the institute's mission and goals are understood and communicated to a security working group. As stated before, there are three major types or groupings of threats to a biotech/biomedical facility or institute:

- Criminal activity by animal/environmental rights activists,
- Intellectual property compromise by competitive intelligence agents,
- Bioterrorists or criminals attempting to obtain biological pathogens for inappropriate use.

In order to evaluate the capabilities of a known threat, information must be gathered on the "capabilities, intent and history of adversaries attacking the assets of similar organizations". (Jopeck, 2000). Examples of facility or institute compromises from the listed threat groups include:

- Recently, members of the Earth Liberation Front (ELF) are suspected of burning the University of Washington Center for Urban Horticulture's research laboratory to protest the "genetic modification of trees". (Verhovek & Yoon, 2001). "Following attacks on university property carried out in the name of animal rights," laboratories had to be built underground in order to protect AIDS researchers at California's Stanford University. (Getty, 1996).
- Two Japanese research scientists were recently charged with "stealing cells and genetic material" from the Lerner Research Institute, a unit of the Cleveland Clinic Foundation specializing in Alzheimer's research. Upon stealing the materials, one of the scientists

sabotaged his own lab, resigned once the materials were in Japan, and began working there a "a few weeks later." "More and more cases of scientific and industrial espionage have come to light in recent years, a reflection of the rising value of research". (Gillis, 2001).

- Prior to his well - publicized arrest in 1998 for suspected possession of "military grade anthrax," Ohio's Larry Wayne Harris was "arrested in May 1995 after a Rockville, Md. Laboratory sent three vials of 'bubonic plague' inactive bacteria to his home." Mr. Harris has been "identified by the FBI as a member of the Aryan Nations". (Macy, 1998).

Though natural disasters (e.g. fire and flood) are threats to biotech/biomedical facilities or institutes, they are not typically mitigated by the security plan unless they result from an attack by one of the aforementioned threats. In order to ensure the risk of such threats are decreased, the analysis should include "historical data and expert predictions." The difference between adversaries and natural disasters is the latter does not posses "intent". (Jopeck, 2000).

Vulnerability Assessment

In this step, individual assets are considered from the perspective of the threat. What value is this to me? How would I take (steal) it? How would I sabotage it? One of the best ways to gather this type of information is to "interview" those responsible for the asset (operator level) and through "observation. (Jopeck, 2000)." Observation may focus on the steps in the processes used to create the asset, or on processes involving manipulation or transfer of the asset (i.e., in the case of dangerous pathogens: how and where are they used in research protocols, how are they transferred with an institute and to other institutes, what are the security conditions under which they are stored or grown, etc). The objective of conducting an observation analysis or mock walk-through of the process is to identify steps or instances where the asset may be (most) vulnerable to theft or sabotage (see Appendix, Table 2).

Typically, some sort of security capability already exists when reviewing assets. This means the vulnerability can be viewed from one of two positions: "how the existing countermeasures reduce vulnerability to the unwanted events (progressive);" ignoring installed countermeasures and plugging them back in later to see how/if they reduce the asset's vulnerability ("regressive"). (Jopeck, 2000).

Risk Assessment

This assessment combines information from the preceding assessments (asset, threat and vulnerability) and determines the level of risk the institute or facility is currently operating under. "Several techniques for calculating risks exist. They range from simple qualitative systems to those based on complex mathematical formulas. Still others are hybrids of the two". (Jopeck, 2000). The majority of these calculation techniques encountered by the authors have not transitioned well to the biotech/biomed facility or institute model. Regardless of the calculation method used, the most important thing to understand is how the vulnerabilities of an asset vital to a facility's or institute's mission may be exploited by an identified threat and therefore disrupts or destroy the ability to complete that mission.

For example, "two laboratories at the University of Arizona were burned and over 1,200 rats, rabbits, and mice were stolen by the Animal Liberation Front (ALF), destroying years of research to develop a treatment and vaccine for Cryptosporidium". (http://www.biostat.umn.edu/~carlton/PETA.html, 2001). In

retrospect, if we could view the risk analysis for the rodents (assets), it would have indicated that the rodents in this study were determined to have a "high loss impact to the company". (Jopeck, 2000). They would have been considered highly vulnerable to fire and the threat, and based on past activities of organizations like ALF, would have been considered a high loss impact. This would have warranted tighter access control to the area(s) surrounding the rodent holdings as well as a robust fire suppression capability that in turn would have increased their animals' chances of survival.

Countermeasures Assessment

In this step, the determination must be made as to what steps will be taken to protect the assets by reducing their vulnerabilities and keeping threats at bay. Approaches can be organized in three categories:

- "Risk Averse": the objective is to have risk reduced to near zero (may not be realistic),
- "Risk Tolerant": the objective is to develop a balance between the needs of security and business constraints, i.e., funding, mission, etc.
- "Risk Acceptance": organization accepts maximum risk, i.e., in order to decrease costs. This approach is least desirable if protection is needed. (Jopeck, 2000).

Countermeasures are best categorized under the headings: personnel considerations, technical considerations, and operational considerations. These will be discussed further in the following sections.

Upon completion of the risk assessment, recommendations should be presented to those members of management with the authority to accept risks and finance security enhancements if warranted. It is important to remember that this is a continuous process.

Personnel Considerations

Biotechnical/biomedical facilities and institutes may be subject to a number of outside threats. Generally speaking, most realistic threats to assets (especially biological materials), and the most potentially dangerous threats to security in any industry, are those posed by "insiders", or employees. (DTRA, 2000). Any number of events may cause an employee to become a security/safety risk for the company, employer, or coworkers. Some examples include, but are not limited to:

- Becoming unhappy or "disgruntled,"
- Being passed over for promotion,
- Being reprimanded,
- Psychological or emerging personal problems, e.g. divorce, sick child/relative, substance abuse, etc,
- Moral/ethical disagreement with new projects or products,
- Recruitment and acceptance of a job to infiltrate an area and "spy" for another company or special interest group.

The insider threat is the hardest to protect against, and due to innate coworker trust, can be the most dangerous for numerous reasons. In terms of protecting biological materials from insider theft or inappropriate use, there are no reasonable, or tested and proven, technical solutions available. (DTRA,

2000). The answer largely depends upon personnel management and access control.

While inappropriate in academic settings, and unaffordable for many corporate entities, the first step in protecting a facility's or institute's assets from potential threats from employees is through the practice of background checks. "Background checks are an essential component of any good hiring program, and the criminal history check is especially critical...". (Long, 2001). In lieu of conducting background checks, an employer should at a minimum check the individuals references, and verify that the information provided is accurate. Even if some form of background check is preformed by the institute, it is worth mentioning that individual problems may not begin to manifest until after someone is hired, possibly even in a long-term employee. Therefore, once employees are hired, security or personnel reviews of their actions should continue on a periodic basis, or upon a change in duties or access. These requirements and parameters should be set at a corporate/institute policy level, and delegated down to security to implement.

Raising the level of security awareness among employees is a very important, but sometimes daunting task. Some of the main problems include identifying the appropriate level of training in order to maintain interest as well as timing the training so as not to interfere with hectic research or production schedules. At a minimum, employees need to know:

- How to identify personnel and determine whether they are in an authorized area.
- How to report suspected breeches of security.
- Security personnel cannot be everywhere at once, therefore, everyone is a security officer.
- The company's assets are their assets, and both personal and coworker safety and security are shared responsibilities.

It would be difficult to imagine an individual noticing, then walking past an uncontrolled fire in a laboratory and not trying to intervene or report the incident. People are taught and trained at an early age that fire poses a threat to life, safety, and property. Similarly there are danger signs which can be observed in terms of security breeches or potentially catastrophic personnel problems. Without teaching or training programs, it is easy for the untrained eye not be aware of these signs or their possible significance.

For many organizations, finding the time to provide security awareness training for non-security personnel is the biggest problem. There are many good examples of security awareness training programs, but the most important thing to remember when breaking training down into sessions is "to segment the training material so that each lesson would build on the previous lesson and reinforce the central theme that security [is] everyone's job". (McShane, 1999). This is not unlike the concept of biosafety training, where safety training is only effective if it is adopted at the line worker level and supported all the way up the management chain. Training should be relevant to the position and risk, provided in a way that is understood to "non-security professionals," provided in format and increments for maximum effectiveness, and a point of contact should be made available for questions.

As people are "only human", there is always the potential for an employee to feel building, insurmountable pressure/problems that may lead them to acts of workplace violence (against others or self), or provide materials, proprietary data, or security procedure information to an outsider (collusion) in exchange for compensation. The best way to ensure employees receive needed help before an

incident occurs is by establishing a good Employee Assistance Program (EAP).

The intent of any EAP is to provide a way for employees to get confidential, professional assistance in overcoming a personal problem that is interfering with their life and livelihood. Additionally, EAPs also outline those signs that fellow employees and employers can look for to better understand if someone is having a problem. These signs are called "Fitness for Duty Behavior." Numerous companies, State and Federal agencies and institutes offer no cost assistance under these types of programs to employees. For employees of The Florida State University (FSU), the University's EAP outlines these signs on their website. At FSU, they are:

- "Expression of bizarre and inappropriate thoughts,
- Excessive absenteeism without prior approval or rationale,
- Degenerating physical appearance,
- Acts of insubordination,
- Poor work performance,
- Poor workplace relationships with others,
- Indications of alcohol/substance abuse,
- Excessive complaining". (http://www.eap.fsu.edu/guidelines.html, 2001)

Instituting an EAP can prevent tragic actions or theft of assets, while a less physically constraining security management system can evolve that:

- Protects physical assets and
- Provides valuable employees professional assistance without jeopardizing their personal or professional integrity.

Through background/reference checks, security awareness training, and an EAP, facilities and institutes can develop a comprehensive approach to security management regarding personnel considerations.

Technical Considerations

Technical considerations include those items or equipment that may be used to decrease vulnerabilities of an asset to a particular threat. Depending on the mission of a biotechnical/biomedical facility or institute, as well as its risk analysis, suitable equipment is commercially available to help reduce the vulnerability of an asset. Some examples include: fences, lights, closed circuit television (CCTV), motion detectors with lights or CCTV, self closing doors, locking doors, alarms, and card key access.

Access control can be a problem for many institutes as Directors must determine "who" requires authorized access to "which" areas or "which" materials. At times there is also a question of whether access is authorized only during regular business hours, or is authorized regardless of time or day. Research and production can be around the clock endeavors. However, there are technologies that are becoming more affordable that may help overcome some of these obstacles like extended standoff proximity cards, biometrics and remote access control. (Strauchs, 2001). Issues of sterilization and decontamination may come into play in some instances, be it worker or product protection.

It is important to remember that whatever is determined to be the appropriate level of countermeasures (risk averse, tolerance or acceptance), installation of the technology is only one part of the process. Resources (time, money and personnel) must be budgeted to account for time to design, procure, install, test, train, and then retest and retrain on a reoccurring basis (e.g. as personnel change).

Operational Considerations

Operational components of a security program are comprised of on-site or local security forces to include campus police, hospital or corporate security personnel, local police, emergency assistance, etc. The operational portion of security management is best remembered through the D^3RT ("dirt") acronym, which stands for Deter, Detect, Detain, Respond and Train. The maintenance of an adequate and competent security force, security procedures and policies (i.e., background/reference checks, security awareness training, and an EAP) and the installation of technical equipment enables the institute to effectively deter and detect most threats. The security force need not be large, rather adequate for the threat and vulnerability previously established and agreed to in the security plan. It is also important to remember that while technology can reduce the number of personnel required to provide the desired level of protection, there must be adequate staffing if personnel need to respond to an incident (other personnel may be required to provide assistance, interface, and monitoring).

Detention of threats refers to delaying the individual(s) egress, be it related to a criminal or terrorist act at the facility or institute. Delay gives the security force time to receive notification (register) that an event has happened, and respond. A good way to detain individuals as well as providing a safe and aesthetically pleasing place to work for employees is through Crime Prevention Through Environmental Design (CPTED). CPTED is the practice of designing the exterior and interior of a facility or institute with security in mind. A thorough design can make it difficult for an individual to rapidly exit after committing a terrorist or criminal act. Some examples include: landscaping so that fences and retaining walls are not noticed until directly upon them, landscaping to minimize instances of crimes against individuals (i.e., well lit, open approach areas to buildings vs. shadowy enclosed areas) and meandering walkways or corridors so as not to provide a straight exit to perpetrators of crime. (http://www.cpted.net, 2001).

During the investigation of an incident, non-security personnel such as scientists must be able to conduct rapid, detailed accountability audits and be prepared to report on anything that is no longer accountable. This may include animals, experimental or proprietary material/information/product, and is especially important for facilities or institutes working with select agents and BSL-4 pathogens.

An institute's security personnel need to be able to respond appropriately to all types and levels of threats (mischievous vandalism to bomb threats to theft of dangerous pathogens). It is recommended that a good working relationship with local law enforcement authorities be cultivated to provide professional interaction, as well as provide assistance if necessary. Depending on the physical size of the facility or institute, mobility of the security force should be considered. The security force may require cars, motorcycles or bicycles, or a combination, in order to effectively patrol areas and rapidly respond to a threat. Before responding to an incident, security personnel must be aware in advance of any potentially biohazardous materials or other unique hazards located in the facilities (i.e., chemical, radiological, animal, etc.). Security personnel will need a well-developed and practiced plan for safely apprehending individuals who may possess, or may be contaminated by, a biohazardous agent. This

plan should be developed in coordination with biosafety personnel. A good place to start is by reviewing the institute's Biological Emergency Response and Assistance Plan, then modifying it for likely scenarios.

Training of security force officers as well as non-security personnel must be competent, consistent, and continuous. Competent security training, especially at biotechnical/biomedical facilities, includes ensuring everyone is aware of all potential threats that may exist. These threats include industrial chemicals, biohazards, radiological hazards; at production facilities, such things as low hanging objects, slippery floors, and other physical industrial hazards must be evaluated. Competency also means that the training is conducted by personnel with experience in working in research or production settings who arfe able to provide that experience through classroom instruction and operational supervision. When applicable, this training should be provided by the biosafety officer, industrial hygienist, and other safety specialists at the institute. Consistency of training is synonymous with quality, and should be maintained at a high level of standard. The training should be well planned, and from the time it is implemented it should change to meet new challenges. Changes will be required when the risk analysis has been revised, or in some instances when new operations, projects or facility construction are considered. Training for security officers and non-security personnel must include open access to information to ensure that everyone is well aware of all procedures and policies. The value of training will be evident in the event a terrorist or criminal acts. A well trained staff means personnel can be more effectively protected and information can be reported to the security force and managers as rapidly as possible.

The most important part of operational considerations is to ensure that no part of the D^3RT formula is an overt burden on the day to day operational activities of the institute or facility. Many security personnel find that administrators and scientists consider security measures prohibitive and counterproductive to an open and collegial work environment. This is generally a misnomer fostered by rumors (or factual cold war experience) at former weapons facilities. Security today can be achieved in a more innocuous manner, and in the civilian sector is a prerogative of the institute Director. The driving forces of the Director may be centered on personnel safety, protecting commercial assets, preventing the theft or misuse of hazardous materials, or other. While maintaining a safe and secure facility, it is also important to prevent security from interfering with the work or comfort of the employees. This will help in fostering cooperation and collaboration in any security management system.

Technical and Operational Challenges in Securing Biological Pathogens

Technical solutions applied in concert with operational plans can be successfully used in providing security to materials when they are stored in a centralized repository, i.e., cell lines, pharmaceutical libraries of products in development and test phases, pathogenic material, and even personnel files or business sensitive archives. An approach to protecting pathogens stored in central repositories is to implement a two-person rule for accessing the materials. There are numerous variations on this approach to include one person (such as a division chief or designate) to have the key to the entry door, while the other person (such as a biosafety officer) to have a key or combination to a second lock. Another variation, which also facilitates routine inventory control (annual accountability for materials), employs the use of bar codes on the vials rather than identifying the contents by name. Not overtly identifying the material is a deterrent since an individual does not know what they are stealing, whether it is the right material, how to grow it, or how to use it. In this system, the scientist files a

request for the material, which is approved by his management and the institution biosafety officer before the material can be removed from storage. The approved request is provided to storage facility personnel who identify the location of the material in the freezer complex and accompanied by the scientist or biosafety officer, retrieve the material. This method is being successfully used in large institutes working with cell cultures, hybridomas, and BSL-1 and BSL-2 (non-select agent) materials. With LAN networking capabilities, requests for materials can be approved in a matter of minutes. The bar code system has the advantage that it not only facilitates inventory control, but can be used as a management tool when it is programmed to alert a project manager or senior scientist when only "X" number of samples remain in storage (the manager can then reorder, grow, or clone replacement material before inadvertently using the last vial).

A solution to protecting a collection of biological pathogens while facilitating biosafety requirements for select agents (BSL-3 and BSL-4) materials is to locate the collection within the containment area. Containment is the logical place from a safety perspective to store the material, since this is where the material will be used. Storage in containment introduces the need to gain access to and traverse change areas, shower areas (in BSL-4 it requires entry through airlocks which are usually monitored by engineering services), and other points which are generally access controlled by combination lock, card key or other means. Once the individual reaches the door to the repository there may be an additional level of access control to enter that area, with monitoring by motion detector activated CCTV. Locks are a standard feature for freezers, and serve as another layer of deterrent. This scenario provides a combination of operational and technical solutions for safeguarding biological materials in storage areas. It is worth noting these techniques are successful against most (if not all) intruders with the exception of the authorized insider. Using the two - person rule for removing material from a storage area would eliminate this threat unless the two people were working in collusion (usually a remote possibility).

It is also important to note that while biological material in the repository can be fairly well secured, there is virtually no reasonable operational or technical way to provide this level of security to materials being grown in the laboratory. A realistic security risk assessment would identify the laboratory itself as the most vulnerable area to protect. It is obviously easier for the authorized insider to obtain a sample of material he or an associate works with from a flask and carry it out. It is virtually impossible to note these types of discrepancies much less track the missing material. In most institutes BSL-2 pathogens are worked with in laboratories where the doors are not locked or closed during routine working hours, allowing anyone to access and remove a small amount of material. In institutes where work is ongoing with select agents or BSL-3 and 4 agents, laboratory doors should be self-closing and should have access control devices (locks, punch codes, card keys) to deter unauthorized access. The truth is, however, that there is no absolute way using rational measures to prevent a motivated insider from obtaining small amounts of biological material. It is not rational to expect scientists to work using a buddy system; it is cumbersome and at a minimum, doubles labor and PPE costs, not to mention that it is easily defeated. Nor is it rational to try to use continuos monitor CCTV, "portal or tracking" systems (currently undeveloped/unproven/very expensive technology dependant upon developing a label for the organism/media/etc. and tracking the movements of organisms through an area), or other technologies and methods employed by nuclear and chemical security and surety programs. Because biological materials do not "give off" a unique signature that can be measured in real time (especially when in vials), and are valuable in minute quantities (growth potential), they pose a difficult problem from a security point of view. While technology and operational security can greatly help deter outsiders from