医療機器及び医療機器を組込んだネットワークのための情報セキュリティリスクマネジメント

Siemens Medical Solution、W.Leetz、アウトライン、2006 年 6 月 9 日（t-con の前に）
N Mankovich によって修正、2006 年 6 月 19 日
Siemens、W.Leetz、2006 年 6 月 22 日
t-con の後の結果（2006 年 6 月 27 日）
GE Healthcare、J. Moehrke（2006 年 6 月 29 日）
Siemens、W.Leetz（2006 年 7 月 27 日）
T-con の結果（2006 年 7 月 28 日）、Cindy A.Levy のコメントを含む（合流）（2006 年 8 月 4 日）
T-con の結果（2006 年 9 月 27 日）
F2F NEMA（2006 年 10 月 11 日）

1. 目的

この文書の目的は、医療において情報技術（IT）セキュリティリスクのマネジメントを行う必要があるとの認識を養成すること、医療においてITセキュリティリスクのマネジメントを行うために用いる特定のステップについて医療機器及びシステムの製造業者を指導することである。もちろん、製造業者のリスク分析は意図する用途で始まり、仮説の医療施設環境を仮定することから、それは最終使用者のリスク分析として考えることはできない。ITセキュリティリスクとは、データ及びシステムへのリスクである。それらは、患者及び／又は使用者に影響する安全性リスクと区別される必要があり、安全性リスクを含んでいない。この文書は脅威のいくつかの代表例を最初に挙げ、安心確実な医療機器及びシステム（以下、システムという[1]）を設計するため使用できるプロセスを記述する。次のような場合、医療施設は、リスクを評価し、低減するために同じ基礎的な方法論の適用が可能であり、またそれを適用することが望ましい。すなわち異なる販売業者の装置を医療提供ネットワークとして組み合わせる場合、新しい装置を既存のネットワークに追加する場合、又は既存のネットワークの構成を大幅に変更する場合である。

2. 序文

リスクは医療の提供に内在するものである。直接的（ネットワーク）及び間接的（媒体）接続性が増加するに伴い医療機器に関連したセキュリティリスクは増加してきた。精巧な装置は、どんな組織さえも完全には除去できないほどのリスクを持っている。したがって、系統的かつ文書化された方法でリスクを割り当てて、リスクを優先順に列記し、それに従って低減し、そして残留リスクを文書化及び受容すること必要性が起きてくる。

[1] ここで一般に使用されるシステムは、医療の提供に直接使用される情報システムをすべて含んでいる。例えば次のようなシステムであるがこれらに限らない：HIS（病院情報システム）、PACS（画像保管通信システム）、画像診断モダリティ、放射線治療システム及び患者監視システム。

医療機器 IT セキュリティ関連リスクのマネジメントを行うプロセスは、長年来の装置安全性プロセスに非常に似ている。医療機器産業は 30 年以上安全性リスク分析を行ってきた。最近、同様の方法が、IT ベースの医療機器及びシステムのセキュリティリスクに適用されたばかりである。これらの方法は、製造業者をサポートして医療サービス提供者を（間接的に）支援し、又は保護された健康情報の機密性、完全性及び利用可能性を維持する医療サービス提供者を直接的にサポートする。

この文書に記述される IT セキュリティリスクマネジメントのプロセスは次のとおりである。

1. 考慮中の資産を列記しそれらの意図する用途を理解すること；
2. 資産に対するセキュリティ関連の要求事項を集めること；
3. 脅威を詳述し、それらをシステムに適用し、作用因子を含む脆弱性、脅威の経路及び起こりうる結果を決定すること；
4. リスクの点数を決めること；
5. 医療領域に適切な脆弱性の低減を提案し実施すること；
6. 継続か中止かの決定を経営者から得るため、医療使命の達成におけるシステムの役割の他に、残留リスクを要約すること；
7. システム開発を進めるための権限をもって経営者が決定すること。

この文書は、セキュリティリスクマネジメントを詳述し、一連の例を示し、医療脅威及び脆弱性に対する洞察能力を提供し、システムの機密性、完全性及び利用可能性のため如何に設計するかの適切なステップを提供し、同時に適切なレベルの（1）安全性、（2）医療の有効性、（3）患者及びスタッフ双方のためのプライバシー、並びに（4） 生産力と緊密にリンクされる相互運用性を維持する。

3. いくつかの攻撃例シナリオ

これらの 5 つのシナリオでは、IT 関連のセキュリティ脅威に対処する場合の、医療提供問題及び悪影響を簡潔に記述している。多くの脅威が、プライバシーの保護に直接影響する。保護しないと規制に違反することになる。例えば米国 HIPAA （Health Insurance Portability and Accountability Act）プライバシー・セキュリティ規則、欧州及び日本のデータ・プライバシー法かどの規制である。

医療システムの保護は、他の多くの IT ベースのビジネスと比較すると、いくつかの違いがある。例えば、ほとんどの銀行又は会社は自然災害又は IT 脅威の場合には閉鎖できるが、医療施設は一般に開けたままにしておく必要がある。悪条件下で操業することが、災害時に現在の患者を診療し、健康及び一般社会を維持し回復させるために必須である。連続性の計画は純粋に運用上のことと時に見なされてはいるが、それは、セキュリティにおいては必須の要素である（セキュリティは、機密性、完全性及び利用可能性をすべて含むことを忘れるな）。

3.1 病院診療の中断

シナリオ： 病院内の局所的な故障によって、緊急処置室（ER）がネットワーク本線に接続できなくなった。したがって、典型的な IT サービスは利用できない（例えばネットワークアドレシング、ルーティング、使用者認証）。しかし、患者は ER に次々と搬送されてきて、クリティカルな診療が必要となる。ER 内の医療システムはクリティカルな診療を提供し続ける必要がある。

可能な設計低減：こうしたシナリオに対して強健であるためには、システムは、作成した健康情報（医療画像、記録）の作成、ローカルな保存が、たとえLANアクセスがない状態でさえ可能でなければならない。

可能な運用上の代替手段：（1） 追加の要員配置、（2）同じ医療施設の他の診療科で利用可能な装置を使用する、又は（3）患者を近くの医療施設へ転送する、（4） 安心確実な無線による解決法を展開させネットワーク本線と接続する。

影響が最小の場合でも、患者はサービス低下を経験する。待ち時間が長くなり、又は別の医療施設へ重態患者を移動させるからである。このため、この代替手段が患者のリスクを低減するのに一般的には適切な場合であっても、患者の容態次第で患者のリスクは増大する。

3.2 広域災害

シナリオ：広域災害の後の医療の提供。そのような災害は、自然によるもの（例えば地震、津波、ハリケーン／台風、火山、野火）又は人為的なもの（テロ、戦争、停電）である。

これらの災害の間に、一般的なインフラストラクチャ（IT ネットワーク、道路、電力、水道）が更に混乱し破壊されるかもしれない。さらに、災害は医療施設自体に損害をもたらすかもしれないし、ローカルな建物の一部又は医療インフラストラクチャを破壊し、「医療システム故障」を引き起こす。この状況は、災害自身が医療施設に来る患者数を増加させるので、更に悪化する。

可能な設計低減：．　システムは、緊急モードを持ち、それによって認証がなくても個人を識別でき、ローカルの医療スタッフを支援できるようにする。この種のアクセスを確実にするため医療サービス提供者が講じる手順については、SPC (Security and Privacy Committee) Break Glass文書を参照。

可能な運用上の代替手段：この種のまれな災害については、リスク低減手段を定義することは困難である。代替できる医療機器がないからである。しかしながら、災害対策は医療使命を継続するために不可欠である。災害対策には、重要な医療データをそのような災害による破壊から保護する手段、及び、可能な場合、バックアップソリューションとして役立つ他の施設からデータがアクセスする手段を含む。

3.3 無差別な悪意のある攻撃

シナリオ：医療機器（例えばX線、ECG、人工呼吸器、CT、MRI、PET）を患者に使用している最中に、悪意のあるソフトウェア攻撃が起こる。これは広いサイバー攻撃の副作用かもしれない。その場合、医療機器は特に攻撃目標ではない。これらの広い、時として低い技能技術の攻撃ツールは、ウイルス、トロイの木馬、虫などという名で知られている。これらの状況下でさえ、システムは患者の安全性及び健康を保護できなければならない。患者データへの攻撃が公衆に向けられた場合、その結果個々の患者及び医療サービス提供者は損害を受ける。

可能な設計低減：日常の稼動中は、システムの適切な使用にとって不可欠なサービス及びネットワーク・プロトコルだけが稼動し許可されるのがよい。認証のメカニズム

が整備され、信用できるノードだけが通信することを許可される。これによって、信用できないノードからの攻撃を禁止する。多くのシステムがありネットワークへのアクセスが故障した場合、システムの機能を縮小し、縮小しても利用できるように設計しておく。例えば、モニタリングシステムがネットワーク接続できない場合、もはや患者情報を中央ステーションで表示できないが、ベッドサイドモニタは作動し表示できる。PACS ワークステーションのようなシステムは、それらの記憶装置へのネットワークアクセスが中断すると機能しない。しかし、ここで運用上の災害対策のフェールセーフが働き、医療スタッフは画像収集装置の所へ直接行き画像を観察するか、又は収集システムから印刷するか、若しくは媒体を収集システムからワークステーションまで手で運ぶことを考慮することができる。

可能な運用上の代替手段：通常の、即時のリスク低減手段は、この装置にネットワークからアクセスできないようにすることであろう。しかし、これは、連続的なネットワークアクセスを要求する装置に適切でないかもしれない。また、それは患者にとって重大な医学的結果になるかもしれない。ネットワーク接続に依存することは増えているけれども、これらのシステムは通常、効率的な作業の流れをサポートしており、生命維持機能を直接提供するものではない。一般に、ネットワークが機能していなくても、生命維持装置は適切な独立運転に戻る。重要なことは、病院がネットワークの不調に対する災害対策を持つことである。例えば長時間のネットワーク障害の場合、スタッフを急いで増員するなどである。

3.4 資金の豊富な攻撃

シナリオ：豊富な資金を持つ悪意のある攻撃者は目標を絞った攻撃ができる（例えば組織犯罪）。典型的には、攻撃者は部外者である。また目標は、医療システムに保存されたＶＩＰ例えばスポーツ選手又は有名人の医療データである。目標としての医療システムは、資金の豊富な攻撃者にとって価値の高い情報を含む他のシステムと異ならないかもしれない。しかし、秘密のパスワードを盗まれて無許可の開示があっても、パスワードを変更すれば一時的な不便で済む。しかし医療情報（例えば癌、エイズウイルスの感染状態）は、一旦開示されると取り返しがつかず、被害者に重大な社会的、金銭的影響を及ぼすことがある。

可能な設計低減：システムに強力な使用者認証及び権限付与の機能を付ける。それはＶＩＰ患者をマークし、その人物の健康情報へのアクセスを制限し、ログインの手順を増すことができなければならない。コミュニケーションの暗号化及び報告書のデジタル署名によって、保存された健康情報の機密性及び完全性が更に増す。

可能な運用上の代替手段：医療施設がこの種の攻撃を防ぐことは困難である。根底に脆弱性がある限り、アクセス権を詳細に管理しても役に立たないかもしれない。悪意のある当事者の動機づけ次第では、金銭的な利益によって、内部の関係者（彼らは通常、患者データへのアクセス権を必要とし、したがってそれを持っている）が、そのような犯罪的攻撃を行うこがある。

3.5 個人的な報復

シナリオ：例示した脅威の最後の種類は、怒って報復したい者（従業員、患者、サービススタッフなど）から発生する。この種の攻撃の大部分は内部関係者（又は元従業

員）から発生する。医療施設の内部の特定目標に対して、又は医療施設全体に対して損害を与えようという不合理な欲求を持っている。

可能な設計低減：システムは、使用者認証及びアクセス管理並びに内部方針からの逸脱を証明する監査ログを含んでいるのがよい。アクセス権の変更は、システムへそれらを入力した直後に有効になる必要がある。

可能な手続的・技術的な低減：報復は短期間攻撃として通常明白なので回避するのは難しい。十分に整備したファイアウォール、適切なアクセス権、分離 VLAN などが適切かもしれない。これらの制御手段は一層厳格にして、内部事情を知っている人、すなわち以前の個人的接触又は職員との親密な関係を介してアクセス方法を知っている人が、攻撃に成功しないようにしなければならない（例えば社会工学的な攻撃）。これらのシナリオが強調していることは、人材育成の重要性、アクセス権を制御する手順の適切な作成及び実施、雇用又は第三者役務契約の終了時に権利を直ちに権利を取り上げるプロセスを持つことである。

3.6 発表された新しい脆弱性が

シナリオ：医療システムプラットフォームコンポーネントが、この分野で調査中の脆弱性を持つことが分かった。

可能な設計低減：医療システムを強固にする：不必要なサービスを閉鎖する、最小特権レベルでサービスを実施する、意図する用途に不必要なサービスへのアクセスを最小にする（例えば電子メール、ブラウザ、など）。詳細については、SPC 白書*医療情報システムの市販ソフトウェアの補修及び悪意のあるソフトウェアに対する医療情報システムの防御*を参照（*www.nema.org/medical/spc*）。

可能な運用上の代替手段：運用ネットワークから絶縁すること、又はそれができなければ、ネットワークに接続しないこと。できればファイアウォールを形成して保護すること。

4. 医療セキュリティリスクマネジメントのプロセス

4.1 概論

セキュリティ関連の医療機器 IT リスクのマネジメントを行うプロセスは、長年来の装置安全性プロセスに非常に似ている。例えば、安全考察に適用される故障モード影響解析（FMEA）のようなツールは、セキュリティ調査にも同様に使用できる。セキュリティが、重要であるけれども、患者及び操作者の安全性に対し従属しなければならない重要な関係に注意する場合以外、我々は、安全性リスクアセスメントを詳述しない。

矛盾及び混乱を回避するために、我々は、セキュリティリスクアセスメントのプロセスを、安全性リスクアセスメントと別々に行うように勧める。なぜなら、全体として、それらは異なる要求事項を持ち、基本的に異なる資産に関係するからである。提案された低減の後でさえ、セキュリティリスクが相当な安全性リスクを持つ場合は常に、安全性リスクアセスメントのプロセスが先行する。一般に、これが意味することは、リスクの主要な議論を安全性チームに移し、それに知識の豊富なセキュリティチーム

のメンバーを同伴させることである。このように、二つのプロセスは、一般に製品生成プロセスの全体にわたり平行して進む。

リスクマネジメントチームのメンバーの技能は、特に詳しく決める必要がある。背景としての一般的な IT 知識を持った者は、多くの場合、医療に特有な問題に気づいていないので、非実用的な手段を提案して終わるかもしれない。セキュリティリスク分析のチームは学際的であり次の属性を持つのがよい：

- システムのビジネスの側面及び技術の側面の両方（IT 知識を含んで）を代表する；
- 臨床プロセス及び製造業者開発プロセスの両方についての明確な理解；
- 医療に特有な要求事項（安全性要求事項はセキュリティ要求事項よりも重要である）についての深い理解；そして
- 製品の安全性リスクマネジメントのプロセスに精通しているメンバーを含める。

さらに、チームは、非常勤の専門家を一時的に参加させて補強されるのがよい。この専門家は、ネットワーク問題、IT セキュリティの深さ、脆弱性ツールのアセスメント及び他の専門的問題であってリスクアセスメントのプロジェクト中に発生する問題に助言できる者である。

次のセクションに記述される IT セキュリティリスクのアセスメントによって、次のような根本的問題に答えが得られるであろう：

- 価値のある資産であって、考慮中の意図する用途に該当する資産は何か。
- 考慮中の資産のセキュリティに関連する要求事項は何か。
- 攻撃をするのは誰か。
- 攻撃者が使用し得るアクセス経路はどんな経路か。
- 攻撃に必要な動機／動機づけ及び手段には何があるか。
- システムにおける既存の技術的なプロセス制御手段には何があるか。
- リスクを低減できるのは、どんな処置によってか。

4.2 資産の一覧表

リスクマネジメントの基礎として、保護を必要とする考慮中の資産及び意図する用途が列記されなければならない。典型的な資産に含まれるのは、医学情報及び種々のデータの処理に使用されるハードウェア及びソフトウェアであるが、これらに限らない：

- 病院の IT インフラストラクチャーの特定のコンポーネント／医学応用システム（例えば画像生成モダリティ、ネットワークコンポーネント）；
- 病院の IT インフラストラクチャーの非特定のコンポーネント／医学応用システム（例えばサービス強制停止の攻撃は全体のネットワーク交通を遮断するかもしれない）；
- 医療アプリケーションソフト自体；
- ハードウェア及びソフトウェアの構成に関するデータ；
- 特定の患者の医療データ；
- 患者の非特定医療データ；そして
- 医療手順のサポート情報。これに含まれるのは使用履歴及び操作者／使用者の詳細である。

資産の一覧表は、十分に詳しいものにして、各々の資産に対する直接の脅威を割り当てることから始めて、適切なリスク低減手段を特定し実施可能にする必要がある。例えば、病院情報システムを一つの資産として列記するだけでは、十分に詳しいとは言えず、現実的な特定の脅威を指摘できない。一般に、ネットワーク図があれば（それが合意された「典型的なネットワーク」であっても）、開発機器の IT アーキテクチャ又は全体の病院ネットワークを系統的に概観できる。ネットワーク図によって、同じ施設の中（又は同じ医療サービス提供者の中）の多数の場所で使用される同一のシステムを特定しやすくできる。それらのシステムは、同じリスクにさらされ、同じリスク低減手段の実施を必要とするシステムである。そのような全面的なネットワークアプローチを適切に使用することによって、製造業者のリスクマネジメントの単独チームは、種々のネットワーク実施の中で使用されるシステムを扱うことができる。

4.3 セキュリティに関連する要求事項の収集

アセスメントチームは、セキュリティに対するシステム要求事項を詳述する資料をすべて集めるのがよい。これに含まれるのは、すべての資産の詳細であって、機密性のレベル、完全性、利用可能性、責任能力（つまり認証、及びログファイル利用可能性／使用）に関する詳細である。この要求事項による収集は、文書を特定して収集するか、又は一組の明示的な参照事項として実現する。後者の場合、参照事項は、「セキュリティ要求事項追跡可能性マトリックス」（サンプルテンプレート用の附属書 SRTM を参照）中で詳述される。入力要求事項は典型的には次のものから由来する：

- 規制要求事項（HIPAA、指令 95/46 EC、など）であって使用者に対する要求事項；
- 顧客要求事項（政府系機関、購買グループ、など）；
- 安心確実なプラットフォームを構成する指針；
- 内部セキュリティ／プライバシー方針文書； そして
- 産業界の模範事例の白書。

4.4 脅威及び脆弱性の詳述

資産の一覧表及びセキュリティ関連の要求事項を使用して、リスクアセスメントチームはブレーンストーミングを行って、各々の資産に対する起こりうる脅威をすべて特定し文書化する。一般的な脅威が特定のシステムに関係する場合、それはシステム脆弱性として知られるようになる。一般に、各々の資産に対する脅威を詳述することは、アクセス経路、作用因子、動機及び結果を連鎖的に特定することである。

4.4.1 起こりうる作用因子

種々の作用因子があり人間と関係するもの、関係しないものがある。脅威に関与する作用因子は、次のように分類できる：

- **認可されている者**：内部関係者であって、有効なアカウントを持つが特定のタスクを行うことを認められない者、例えば、
  - 偶発的な攻撃；
  - 外部イニシエータから支払を受けた内部関係者；そして
  - 個人の利益又は報復によって動機づけられた内部関係者。

- ネットワークのインフラストラクチャにアクセスすることを**認可されていない者**：部外者であって、アカウントを持たないが、医療サービス提供者のインフラストラクチャへアクセス（物理的又は論理的）できる者、例えば、
  - 無法者（スクリプトキディー又はハッカー）：
  - 支払を受けた外部者／組織犯罪；
  - 訪問客及び患者；そして
  - 兵士及び／又はテロリスト。
- **人間と関係しない「作用因子」**：それらは典型的には予測できない状態で起き、直接の人的影響はない。
  - 局所的な故障の継続：緊急処置室がネットワーク本線に接続できない。しかし、何らかの緊急処置を患者にしなければならない。
  - 大規模な産業事故：多数の負傷者を治療しなければならない。同時にその事故によって引き起こされた停電によって医療の提供が困難になっている。
  - 自然災害：それらは、地域社会及び地域インフラストラクチャに損害を与える。停電によって医療機器が操作できない。しかし、多数の負傷者が緊急処置室に同時に押し寄せてくる。

4.4.2 脅威の経路

人為的な攻撃の場合、攻撃者は種々の方法を使用してネットワーク中の目標にアクセスする：

- 医療システムへの**直接の（物理的）アクセス**
  - 医療システムコンソールに座ることは、システムのセキュリティをリスクにさらす手段を提供する。
  - 装置は、適切な物理的セキュリティがないと盗まれる。
  - 物理的なアクセスによって、取り出し可能な媒体（CD、DVD、USB スティック）からの攻撃経路が開く。
- **ネットワークを使用する論理的なアクセス**（例えばIPネットワーク又は経路としての電話接続）
  - 企業の内部から：典型的には、システムに既知の使用者であって、特定の業務を行うよう原則的に許可されている者。例えば X 線画像を CD に患者治療の目的で保存する業務である。この者がこの経路を違法行為に使用するかもしれない。しかしながら、この者は、X 線画像を CD に他の目的、例えば報道関係者にデータを転送する目的で、保存することは許可されていない。
  - 企業の外から：考慮中の装置の使用者名簿が完備されている場合、攻撃者はシステムが認知しないので[illegible]払いになる。従って、意図しているが無許可の業務をする前に、攻撃者は最初にアクセス制御機構を突破しなければならない。

4.4.3 起こりうる影響

可能なシステム脆弱性であって総括的な脅威に由来するものを編集する際に、重要なことは、攻撃が成功した場合の可能な影響を完全に理解することである。影響には種々の場合がある。例えば単一の診断又は監視事象、単一の患者、単一の診断又は監視のシステム、若しくは特定のソフトウェアバージョン番号を持つシステムの展開さ

れた組全体などに対するものである。一般に、影響されるシステムの数が多いほど、重大さは大きい。しかしながら、留意すべき重要なことは、ただ１人の患者プライバシーの問題でさえ非常に重大ということである。個人の健康情報、例えば病気及び容態に関する悪い情報が漏れて、取り返しがつかないと、金銭的な破滅を招くことがある。特に有名人の場合はそうである。

影響を受ける単一システム又は複合システムは、次のような事象から損害を受ける：

- 患者又は操作者の安全性が損なわれる；
- 患者データが無許可で開示され、破壊され又は変更される；
- 監視装置の使用：誰がこの装置を使用しているか、誰が治療されたか；
- 製造業者の仕様書以外のシステムの変更；
- 装置の利用の中断；そして
- 役務又は供給品の窃盗。

リスクマネジメントチームを援助するために、かつできるだけ漏れのない一覧表を作るために、マトリックス表を作ることが時には有用である。利害関係者を一番上に書き、その下に目標資産の行を列記する。手始めに利害関係者は、（a）患者、（b）医療提供者及び（c）製造業者又はサービス機関とする。

4.5 リスクに点数を付ける

4.5.1 リスクの序論

リスクは特定の脆弱性に対して割り当てられるが、これは攻撃が成功する可能性と、資産に生じる衝撃の重大さを組み合わせたものである。セキュリティリスクのアセスメントは、故障モード影響解析（FMEA）の必須の要素を利用する。このステップの目標は、リスクを合理的に分類して、低減活動の優先順位を決めることである。これはきめの細かい数値的な評価を要求しない。一般に、3つのレベルの可能性及び重大さで十分である。しかしながら、地域的な要求事項並びにデータの利用可能性及び質に基づいて、チームは4つ、5つ、又は他の数のレベルを使用してもよい。そうする前に、次のことに留意するのが望ましい：

理論上、チームの使用するレベルの数が多いほど、リスクに付ける点数は詳しくなる。「レベルの数を増すと精密になる」と誤解することが多い。リスクアセスメントチームは、攻撃のあらゆる起こりうるシナリオについて憶測をしないよう注意しなければならない。この憶測はセキュリティ業界では「映画脚本の制作」という。

4.5.2 攻撃成功の可能性

可能性を現実的に評価すれば、「映画脚本の制作」は最小限になるであろう。次の定義が使用される:

可能性とは、脆弱性が、関連する脅威環境の構成の中で生じる確率である。次の要因が考慮されるのがよい：

- 脆弱性が暴露される時間の長さ。
- 脅威の発生源：動機づけ及び作用因子の能力。

脅威の中に、より精密な可能性評価のできる脅威がたとえあったとしても、可能性のレベルは「高い、中程度、低い」の 3 つにしておくことが有用である。これを表 1 に示す。

	脅威の発生源	**制御手段の効果**
高い	動機づけが高く、十分に有能である	脆弱性に対し効果がない。
中程度	動機づけられ、有能である。	効果があり、脆弱性が暴露されるのを抑制する
低い	動機づけも能力も小さい（例えば偶発的な攻撃）	効果があり、脆弱性が暴露されるのを防ぐか又は少なくとも著しく抑制する

表 1　可能性のレベル

人間の関係する攻撃の可能性を評価する場合、攻撃の元になる動機づけが主な要素になる。なぜなら、動機づけの大小によって、適用可能な規則又は法則を破るのに費やす金銭と労力の大小が決まるからである。攻撃者は費用便益評価をして、攻撃の成功の価値に対する攻撃に要するコストを評価する。通常、動機づけが高いほど、費やす金銭と労力が多い。したがって、資産を保護するのに必要な対策は更に精巧なものが必要になる。幸いにも、人間の関係する攻撃は大抵のものが、動機づけが低い。しかし、少数ながら一部の攻撃は、動機づけが極めて高く（例えば金銭又は政治絡みのもの）、医療サービス提供者に重大な損害をもたらすかもしれない。

人間の関係する攻撃の可能性を状況に応じてどのように評価するかを、以下の数例で示す。

- 「無差別な」攻撃（大抵、悪意はなく、特定の意図もない）であって、典型的には不注意によって攻撃が成功する。
  - 明瞭なセキュリティの方針、目的又は活動がない。
  - 研修がなく、手順が順守されていない。
  - 疑わしい除外：セキュリティ機能の使用は、臨床の作業の流れを妨げるものと見られる。
- 意図的な攻撃（大抵、悪意がある）：
  - テロリズム：医療が特定の目標かもしれない。
  - 金銭的な利得：攻撃者の金銭的な利得は数百万ドルにもなり、同様に攻撃を行う努力をする。
    - 窃盗を特定する（ますます普及している）。
    - 報道関係者は重要人物（スポーツ選手又は有名人）の健康情報を取材して記事にするかもしれない。

4.5.3　不満を持った従業員、患者、患者の親族、その他の者による報復。成功した攻撃の重大さ

セキュリティ事故の***重大さ***は、機密性、完全性及び利用可能性がどの程度損失又は低下したかに関して記述できる。優先順位を付けた下記のリストによって、各々のセキ

ュリティの目標、及びその目標が達成できなかったときの結果（又は影響）を簡潔に述べる：

- **完全性の損失**：システム及びデータの完全性とは、情報に不適切な変更を加えないという要求事項である。完全性の損失が起きるのは、無許可の変更がデータ又はシステムに、故意か偶然かで、加えられるときである。システム又はデータの完全性の損失が回復しない場合、被害を受けたシステム又は壊れたデータが引き続き使用され、その結果が不正確、不正行為となり、安全性問題さえ引き起こす。さらに、先ず完全性に対する妨害が手始めとなって、システムの利用可能性又は機密性に対する攻撃が成功するに至る。

- **利用可能性の損失**：最終使用者がシステムを利用できない場合、医療施設の使命が影響されるかもしれない。例えばシステムの機能性の損失及び運用可能性の損失が起きると、例えば安全性に懸念が生じ、診療の量及び／又は質が低下するかもしれない。

- **機密性の損失**：システム及びデータの機密性とは、無許可の開示から情報を保護することである。無許可の、想定外の、又は意図しない開示をすると、製造業者又は医療サービス提供者は地域的な規制、例えば EU 指令 95/46 に違反することになる。又は米国では、製造業者は契約上のビジネス協定に違反（したがって医療サービス提供者は HIPAA 規則に違反）することになる。

結局、大まかな分類（高い、中程度、低いの三つのレベル）が、ほとんどの状況下で十分である（表 2）。重大さレベルの数を幾つにするかは、特定のニーズに依存するかもしれない。（附属書 C も参照。）

重大さ	定義
高い	脆弱性のために、（1）主要な有形資産又は資源の損失が起き、それが非常に高価である；（2）組織の使命、評判又は利益を著しく侵し、損ない、妨げる；又は、（3）人の死亡又は重傷を招くかもしれない。
中程度	脆弱性のために、（1）有形資産又は資源の損失が起き、それが高価である；（2）組織の使命、評判又は利益を侵し、損ない、妨げる；又は、（3）人の負傷を招くかもしれない。
低い	脆弱性のために、（1）一部の有形資産又は資源の損失が起きる；（2）組織の使命、評判又は利益に目立つ影響を与えるかもしれない。

表 2　重大さレベル

4.5.4　リスクの点数

リスクの点数は、攻撃の可能性と重大さとを組み合わせた結果である。それは、リスクの低減手段の格付けを決定する。「どの程度のリスク点数の場合に、リスクを受容できるかまたリスク低減手段を実施する必要があるか」を決める単純で普遍的な合意はない。リスク低減の実際の優先順位は、その装置の運用状態における装置の特定の診療価値、システムの詳細事項及び他のローカルな条件によって異なる。したがって、

リスクマネジメントチーム及び管理者は、各システムの受容できるリスクレベルを定義する必要がある。

可能性と重大さレベルとを表 3 のような表に組み合わせることによって、チームは「高い、中程度、低い」リスク点数を割り当てることができる。医療システムが医療提供の原因をどのように進めるかの仮定によって、表の中の「高い、中程度、低い」点数の割当ては、目標の設置場所又はローカルな条件に適するように、変更できる。

	重大さ		
脅威の可能性	**低い**	**中程度**	**高い**
高い	*低い*	*高い*	*高い*
中程度	*低い*	*中程度*	*高い*
低い	*低い*	*低い*	*中程度*

表 3　可能性と重大さレベルとに由来するサンプルリスクの点数（イタリック書体）

リスクマネジメントチームは、特定のリスクについて議論する前に、継続処置の定義を要求するリスクの点数の相関性について合意するのがよい。上記の例において、リスクチームは、患者安全性を優先させることによって保守的に行動していた。したがって、重大さの「高い」セルの点数は少なくとも「中程度」である。

リスクの点数のサンプル記述は、下の表 4 に示される。それが示すのは、脆弱性があった場合資産が暴露されるリスクの点数、及びそれに対して必要な是正措置である。

リスクの点数	必要な処置
高い	是正措置の必要性が高い。現存システムは作動し続けるかもしれない。しかし、是正処置計画又は他のリスク低減手段をできるだけ早く整備しなければならない。
中程度	是正処置が必要である。また、計画を立ててこれらの処置を妥当な期限内に組み込まなければならない。
低い	システムの所有者は、是正処置が依然として必要かどうかを決定しなければならない。又はリスクを受容することを決心しなければならない。

表 4　リスクの点数及び低減活動の緊急度

もちろん、これらの定義、仮定及び手順はすべて組織的なプロセス文書中で記述される。アセスメントチームが作成した特定の割当て又は仮定は、製品セキュリティリスクマネジメント文書の一部になる。

4.6 リスクを低減する手段

上記のステップを行った後に、製造業者（又は医療サービス提供者）は、関係データを利用して、必要なリスク低減手段を定義する。目標は、特定のシステムに対して、又は特定の医療サービス提供者に対して、受容できる点数まで最大限リスクを低減することである。一旦低減計画が入念に作られたならば、リスクマネジメントマトリックスによって、低減後のリスクを推定でき、最終リスクを明確に決定できる。新しい

リスクが現れるか、又はリスクの点数が十分に低くない場合、このプロセスを繰り返す。

リスク低減が次のものを含むことに注目することは重要である。すなわちシステム内部の技術的制御手段（例えばネットワークポートの閉鎖）、システム外部の技術的な制御手段（例えば適切に形成されたファイアウォール）又は重要なスタッフのためのプロセス記述及び研修である。一般に、低減は技術、プロセス及び人員のすべてに関係する。リスクが設計管理で十分に低減できない場合、リスクを適切に文書化し、運用環境に割り当てられなければならない。外部の（技術的）制御手段は、医療企業によって適用されるのがよい（例えば侵入者の検知など）。

結局、リスクマネジメントチームは、実施されたリスク低減手段及び残留リスクの要約を承認しなければならない。

4.7 残留リスクの文書化及び経営者の承認

リスクアセスメントの最終段階として、経営者から権限を承認された意志決定者は、残留リスク及び （もしあれば）その後の低減計画の要約を受取るのがよい。意思決定者はアセスメントチームの要約を受取り、システムがどのように機能するかの知識と要約とを組み合わせて、診療組織の使命を進め、目標とするシステムを展開するか否かについて、権限のある明確な決断をするのがよい。

5. 結論

ほとんどの国で、患者の安全、スタッフの安全、診療（診断及び治療）、患者のプライバシー（健康情報の保護）について規制が整備されている。セキュリティリスクマネジメントのプロセスをこの白書に記述されたように注意深く実施すれば、これらの目的を満たす助けになる。このプロセスは、製造業者が開発のプロセスにおいて使用してもよいし、医療サービス提供者がネットワークを（再）構成するプロセス、例えば新しいネットワーク化の装置を追加するプロセスにおいて使用してもよい。

セキュリティリスクマネジメントのプロセスは、安全性リスクマネジメントのプロセスとして産業界で知られているものに似ていて、同じツールを使用してもよい。また両方のプロセスが平行して進められてもよい。さらに、安全性と同様に、セキュリティリスクアセスメントも、定期的に又は故障が生じたときに見直しをする。重要なことは、すべての利害関係者（安全性、セキュリティ、作業の流れに関係する者）が良好な連携を保ち、セキュリティリスクを確実に効果的に低減し、医療の使命を促進することである。

附属書 A－要求事項追跡可能性マトリックス

5.1 附属書 A.　要求事項追跡可能性（トレーサビリティ）マトリックス

この文書はシステム・セキュリティ構成を実施するための文書である。次のことに注意すること。「どのように‥‥調査されたか」の略語はインタビュー（I）、文書調査（D）、技術的な試験（T）及び観察（O）であり、どの方法を使用して適合の有無を調べたかを示す。「適合」のコラムでは適合する（Y）か、適合しない（N）かを示す。

セクション及び要求事項の番号	システムを試験するためのセキュリティ要求事項 ‥‥に対して	出所参照	関連した参照	どのように‥‥調査されたか I / D / T / O	適合 Y / N	コメント
XYZORDER 8732.3D に従う要求事項						
セクション 1.0	XYZ 8732.3D；Chapter2 セキュリティ要求事項					

附属書 A－要求事項追跡可能性マトリックス

セクション及び要求事項の番号	システムを試験するためのセキュリティ要求事項 ‥‥に対して	出所参照	関連した参照	どのように‥‥調査されたか I / D / T / O	適合 Y / N	コメント

附属書 B－リスクマネジメントのマトリックス

製品のセキュリティリスクマネジメントのマトリックス　S=脆弱性の重大さ　L=発生の可能性　R=セキュリティリスクの格付け

#	**脆弱性** *（製品のすべての面に上記の脅威マトリックスを適用することを考慮）*	**原因、寄与因子**	**最初のリスク**			**低減/リスクコントロール手段**		**詳細仕様への言及/SW要求仕様**	**検証/妥当性確認報告書への言及**（もし「合格」ならば）	**残留リスク**		
			S	L	リスク	DPMI	1. 設計によって 2. 保護対策又はプロセス制御 （製造、保守） によって 3. 安全性に対する情報によって			S	L	リスク

附属書 B－リスクマネジメントのマトリックス

#	**脆弱性** *（製品のすべての面に上記の脅威マトリックスを適用することを考慮）*	**原因、寄与因子**	**最初のリスク**			**低減/リスクコントロール手段**		**詳細仕様への言及/SW要求仕様**	**検証/妥当性確認報告書への言及**（もし「合格」ならば）	**残留リスク**		
			S	L	リスク	DPMI	1. 設計によって 2. 保護対策又はプロセス制御 （製造、保守） によって 3. 安全性に対する情報によって			S	L	リスク

附属書 B－リスクマネジメントのマトリックス

5.2 附属書 B. リスクマネジメントのためのリソース

IEC 60812 Ed. 1.0：システム信頼性の解析技法－故障モード影響解析（FMEA）の手順

NIST SP 800-30：情報技術システムのためのリスクマネジメントガイド
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

ISO 14971:2000: 医療機器へのリスクマネジメントの適用

ISO 17799（2000） 情報技術 - 情報セキュリティマネジメント実施管理

MIL-STD-1629A、故障モード影響・クリティカリティ解析を実施する手順、1980年11月24日

オーストラリア規格 *AS4360:2004 リスクマネジメント*

運用上重大な脅威、資産及び脆弱性評価（OCTAVE）の枠組み

Wikipedia: リスクマネジメント http://en.wikipedia.org/wiki/Risk_management

OODA: Observe Orient Decide法

IEC 61025　フォールトの木解析

IEC 61882 HAZOP適用ガイド

Carnegie Mellonソフトウェア工学研究所、ソフトウェアリスク評価方法 （バージョン2.0
http://www.sei.cmu.edu/pub/documents/99.reports/pdf/99tr029-body.pdf）

SAE J-1739、設計における潜在的故障モード影響解析、及び生産及び組立工程における潜在的故障モード影響解析、リファレンスマニュアル、2002年8月1日

IHE、IHE プロファイルのセキュリティセクションのクックブック、2006 年 8 月 20 日、

http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_White_Paper_Security_Cookbook_PC_2006_08_30.pdf