Joint Security and Privacy Committee

International Medical Informatics

# 医療情報システムにおける
# 有害なロジックに対する防衛

**2003 年 7 月 8 日**

# *SPC 承認用*

# *最終ドラフト*


**www.nema.org/medical/spc**

Secretariat: NEMA (National Electrical Manufacturers Association) www.nema.org
1300 North 17th Street, Suite 1847, Rosslyn, VA 22209 USA tel: 703-841-3200 fax: 703-841-5900
Secretary: Stephen Vastagh tel:703-841-3281 fax:703-841-3381 E-mailto:ste_vastagh@nema.org

# 履歴:

W. Leetz、Siemens Medical Solutions、基本概要、2003 年 1 月 27 日
J. Burke、Toshiba America、範囲に関するコメント、2003 年 1 月 27、28 日
J. Moehrke、GE Medical、範囲に関するコメント、2003 年 1 月 28 日
R. Horn、Agfa、初期ドラフト、2003 年 1 月 29 日
D. Gobuty、Kodak Health Imaging、上記の全テキストからの詳細概要、2003 年 1 月 31 日
W. Leetz、Rob Horn のコメントを含むドキュメントの体裁変更 (内容の変更はなし)
W. Leetz、若干のコメント追加、2003 年 4 月 2 日
W. Leetz、t-con のコメント、2003 年 4 月 4 日
W. Leetz、若干の完全なテキスト、2003 年 4 月 11 日
W. Leetz、Rob Horn と Wolfgang Leetz によって記述された 2 つのテキストの併合、2003 年 4 月 22 日
W. Leetz、若干の簡潔化など
D. Gobuty ほか、Kodak Health Imaging、コメントと提案、2003 年 4 月 29 日
クリーブランドにおける SPC のミーティング、2003 年 4 月 30 日
W. Leetz、4 (「潜在的な脆弱性」) の再調整、2003 年 6 月 12 日
D. Gobuty、Kodak Health Imaging、全体にわたるコメント、提案、修正、2003 年 6 月 24 日
SPC ミーティング、2003 年 6 月 25 日、ロンドン
SPC ミーティング、2003 年 7 月 7、8 日、NEMA

## 1. 目的と範囲

このホワイトペーパーでは、一般にウイルスと呼ばれる有害なロジックに対する医療情報システム (MedIS) の保護に関する概念について検討する。その目的は、このような脅威に対して、患者の安全、ならびに患者の医療データの機密性、完全性、利用可能性を継続的に保護するための、システムの設計方法および対処方法を示すことである。そのため、このホワイトペーパーでは、ベンダーとユーザーの両方に対して、有害な攻撃の可能性に関する情報を提供し、攻撃からシステムを保護するための手段を指摘する。

## 2. はじめに

今日、患者に対する医療の提供は、MedIS にいっそう依存するようになっている。このようなシステムは、最新の IT を利用して、患者のデータを収集、処理、配布、表示、および保管を行う。他の IT システムと同じように、MedIS も、悪意あるロジックによる攻撃を受けやすい。MedIS の所有者および運用者には、悪意ある攻撃からシステムを保護する大きな責任がある。MedIS の適切な運用は MedIS が設置されている企業の責任ではあるが、ベンダーがユーザーを支援することは可能である。このような活動には、製品のライフサイクル全体を通してベンダーとユーザーの両方が考慮する必要のある技術および手順が関係する。
MedIS には、事務用の IT 環境には通常存在しない固有の課題がある。患者の健康を守るために必要な際には、医療データを利用できなければならない。また、MedIS は、安全で効果的でなければならず、システムの安全性と品質に関する規則などの行政命令に準拠しなければならない。

## 3. 有害なロジック

際限のない可能性を考慮すると、MedIS に対しては単なるコンピュータウイルスには収まらない多くのソフトウェア的脅威が存在するので、このホワイトペーパーでは、MedIS に含まれる、または MedIS に投入される不正なソフトウェアを指す場合には、“有害なロジック”または“マルウェア”という用語を使用する。マルウェア攻撃は、医療装置を制御するためのデジタルコンピュータに“感染”して動作する、ベンダーから提供されたものではないソフトウェアによって行われる。コンピュータの本来の機能がマルウェアによって妨害されることがよくある。マルウェアは、通常、MedIS だけを特別に目標とするのではなく、見つかったすべてのコンピュータを攻撃する。マルウェアによって、データや正規のソフトウェアの喪失や損傷が発生することがあり、MedIS のハードウェアコンポーネントが被害を受けることさえある。
システムの正常な動作を阻害して混乱や損害を発生させようとする有害な意図を持つ者により、多くのマルウェアが作成されている。MITRE Corporationが 1994 年に作成したセキュリティに対する脅威の分類[1] では、攻撃の方法に基づいて、有害なロジックのカテゴリが以下のように定義されている。これらのカテゴリはそれ以降変更されていないが、それを実行する技術は急速に変化している。以下の概要では、有害なロジックが原因であるカテゴリだけを選択してあり、その他のカテゴリは除外してある。

### 3.1 偽装者

求められている機能を実現するように偽装して実際には有害な動作を行うマルウェア。

- *トロイの木馬*は、役に立つプログラムのように見えるが、使用すると意図したものとは異なる予想外の機能を実行するマルウェアである。
- *非実行可能データ*は、普通のデータのように見えるが、コンピュータがアクセスすると実行可能なソフトウェアになり、意図しない予想外の機能を実行するマルウェアである。この種のマルウェアの一例は、ワープロファイル中での有害な“マクロ”の使用であり、ワープロアプリケーションがアクセスすると好ましくない動作が発生する。

### 3.2 無力化

このカテゴリのプログラムは、対象のシステムを動作不能にする。

- *時限爆弾*は、有害な機能を隠し持ったプログラムである。重要な意味を持つ時間になったり秘密のメッセージを受信するといった隠れたイベントによって起動されたりするまで、このようなプログラムは意図されている予想通りの機能を実行する。隠れたイベントが発生すると、有害なアクションを実行する。
- *サービス不能 (DoS)* 攻撃: 対象となるシステムの正常な動作を意図的に妨害する環境を作成する (多くの場合は対象システムの外部に) 攻撃である。通常、DoS 攻撃では、対象システムを変更する必要はない。DoS 攻撃は、対象システムに存在することが一般的に知られていて未解決の欠陥を利用して、障害が発生することを攻撃者が認識している特定のデータを送信することで行われる。また、対象システムの正常な動作が利用できなくなるデータ伝送のタイプや頻度を攻撃者が認識している場合は、それを利用して対象システムで大量の処理を発生させ、対象システムを簡単に過負荷状態にすることもできる。

### 3.3 汚染

- *ウイルス:* いったん組み込まれたなら、正規のソフトウェアを改変し、正規のソフトウェアが実行されるとマルウェアが意図する有害な動作も実行されるようにしてしまうマルウェア。ネットワークが広範に利用されるようになる前は、ウイルスがマルウェアの主要な形態であった。

### 3.4 誤用/強奪

- *ワーム:* コンピュータネットワークに接続されたシステムに故意に自分自身をインストールし、発見できる限りのすべての対象に対して自分のインストールを繰り返すマルウェア。ネットワーク上のすべてのシステムにインストールされる可能性がある。いったんインストールされると、ホスト上で有害な動作の実行を試みたり、あるいは単に接続されたコンピュータに繰り返し自分自身のインストールを試みることで DoS を発生させたりすることができる。このようなマルウェアの攻撃では、他の目的で設置された正規のネットワーク設備や、正規のネットワークサービスの欠陥が利用される場合がある。

### 3.5 実現方法

マルウェアは、複数の攻撃方法を利用する複合形式のものが増えている。マルウェアに対するコンピュータシステムの防御技術が向上すると共に、マルウェア自体も防御の裏をかくように変更されている。たとえば、2001 年に出現したコードレッドと呼ばれるワームは、複数のネットワークサービスの弱点を突くいくつかのワーム技法を利用すると共に、一般的な電子メールプログラムの弱点も利用していた。このような攻撃方法のいずれかが成功した場合は、次にウイルス方式の攻撃を使用して自分自身をシステムサービスとしてインストールし、自分をさらに増殖させて、DoS 障害を発生させた。

一部のマルウェアは、他の対象システムを傷つけるために後で使用することが意図されている。上記のいずれかの方法を利用して対象以外のシステムを攻撃して自分自身をインストールするが、これらの非対象システムの動作を妨害することはない。その後、他の対象システムを攻撃するためのコマンドを準備する。

## 4. 潜在的な脆弱性

システムは、攻撃者がアクセスできる環境に置かれると、有害なロジックに対して脆弱になる。製造、通常の動作、サービスなど、現在の MedIS のライフサイクルでは、複数のフェーズにおいてアクセスが可能である。最も堅牢な MedIS は、専用のソフトウェアを使用し、専用の 1 つのアプリケーションだけを実行し、他のシステムから切り離され、完全な物理的アクセス制御を提供し、マルウェアが存在しない工場で開発され、サービスを必要としないものである。このようなあり得ない仮想のシステムからの逸脱はすべて、この節で説明するリスクと脆弱性をもたらす。

### 4.1 MedIS への物理的アクセス

フロッピーディスクドライブや CD-ROM ドライブなどのメディアを含むシステムに物理的にアクセスする方法を知っている攻撃者は、システムをマルウェアで汚染できる場合がある。移動性の高いシステムでは、システムに対する物理的なアクセスを管理する困難さが増す。これにより、不正な使用や変更の危険性が大きくなる。

### 4.2 接続性

MedIS が外界と接触するようになると、脆弱性が現れる。このような脆弱性は、直接的なシリアルポート接続、モデム接続、ネットワーク接続などを通して発生する可能性がある。

#### 4.2.1 スタンドアロンシステム

メディアアクセスのない (つまり、フロッピードライブも、CD-ROM ドライブも、ネットワークもない) スタンドアロンシステムは、攻撃を受けるリスクが最も少ない。それでも、以下のものに対する脆弱性は残る。

- オンサイトで使用される汚染されたサービスツール
- サービス技術者による悪意ある行動または不適切な行動
- 製造の間のベンダーまたはサプライヤによる悪意ある行動または不適切な行動
- ユーザーによる悪意ある行動または不適切な行動

#### 4.2.2 メディアアクセス

以前は、メディアが IT システムを相互に接続する主要な手段であった。マルウェアに汚染されたメディアにより、メディアにアクセスするシステムが汚染される可能性がある。そのため、汚染されたメディアは、有害なロジックでシステムを攻撃する際の一般的な媒介物であった。依然として汚染メディアは問題であるが、MedIS の電子的な相互接続が拡大しているため、汚染メディアの重要性は低下している。

#### 4.2.3 ネットワーク接続されたシステム

ワークフローを改善し、管理コストを低下させるため、スタンドアロンシステムに代わってネットワーク接続された装置が増加している。前記のリスクは、ネットワーク接続されたシステムに対しても同じように発生する。さらに、ネットワークを通してマシンからマシンに移動できるさまざまな有害ロジックにもさらされるので、次のような攻撃を受けやすい。

- 内部型の有害ロジック。システム間で伝搬されることもある。ワームなど。
- 外部型の有害ロジック。MedIS の外部から動作する。DoS を発生させるマルウェアなど。

相互接続された MedIS 間のマルウェアの伝搬には、通常の通信に使われるものと同じ技術メカニズムが使用される。ネットワーク接続されたシステムでは、用途によっては、HTTP、FTP、SSL などの特定のサービスと、それに関係してあらかじめ割り当てられているポートが必要になる場合がある。ネットワーク接続されたシステムの一般的な脆弱性としては、以下のようなものがある。

- データベースのサービスとコンポーネント。SQL サーバーなど。
- Web サービス。IIS や Apache など。
- ディレクトリサービス。LDAP や Active Directory など。
- 電子メールサービス。
- ファイル共有。Samba や FTP など。
- 印刷サービス。Postscript や LPR など。
- リモートコントロールサービス。SNMP など。

攻撃者は、通常、できる限り多くのシステムに影響を与えたいので、サービスの最も一般的な実装に対して、サービス関連の攻撃を行う。システム上に存在するこのようなサービスが多いほど、システムに対する攻撃が成功する可能性が高くなる。同様に、装置の相互接続性が高いほど、攻撃者がアクセスに成功する可能性が高くなる。

潜在的な攻撃者が多いほど、リスクは大きくなる。リスクが最も大きいのは、インターネットに直接接続された装置である。脆弱性の種類が変わるのではなく、攻撃する可能性のある人間の数が多くなるのである。

### 4.3 ソフトウェアに関する脆弱性

#### 4.3.1 一般的なソフトウェアプラットフォームを使用する MedIS

マルウェアによる攻撃は、多くの場合、一般によく使用されているプラットフォームに対して行われる。これは、このようなプラットフォームは、発見しやすく、弱点が知られており、影響が最も大きいためである。したがって、一般的な標準とプロトコルに基づく汎用システムの方が、特殊なシステムより攻撃に弱い。リスクは高くなるが、一般的なソフトウェアプラットフォームの使用は医療機関にとって大きなメリットがある。

#### 4.3.2 装置固有のアプリケーションソフトウェア

特定のタイプまたはモデルの医療装置の専用タスクを実行するために作られたソフトウェアは、装置固有と呼ぶことができる。一般的なプロトコルを利用し、Unix や Windows などの標準的なオペレーティングシステムで動作するように作成されている場合もあるが、この種のソフトウェアは独特なもので、特定の MedIS でのみ機能する。このような装置固有のソフトウェアは、汎用ソフトウェアではなく、ワープロやスプレッドシートなどのオフィスアプリケーションのような他のアプリケーションソフトウェアと比較すると、厳密なライセンス管理とバージョン管理の下で、狭い範囲のユーザーに対して配布される。この種のソフトウェアを攻撃者が手に入れることはあまりないので、ソフトウェアにセキュリティ上の弱点があったとしても、ソフトウェアを使用するベンダーとユーザーの狭いコミュニティの外部に弱点が知られる可能性は低い。

#### 4.3.3 共用システム

共用の汎用 IT システムにインストールされた MedIS は、専用システムに関するすべてのメディアアクセスおよびネットワークアクセスの脅威に対して脆弱である。さらに、ホストシステムの既存または将来のあらゆるマルウェア感染に対して脆弱になる。
ホストシステムに電子メールやインターネットアクセスの機能も備わっていると、MedIS の脆弱性はさらに大きくなる。
実施できる保護手段が制限されるため、さらに面倒な問題が発生する。専用システムの場合は、広範な使用制限を行い、不必要なシステムサービスを削除することができる。共用システムの場合は、さまざまな使用方法のニーズをすべてサポートしなければならないため、あまり多くを変更することはできない。

## 5. MedIS ベンダーのための有害ロジック対策

管理的および技術的な手段を決定するには、まず、想定される使用でのリスクと脅威の分析を行って、リソースを最も有効な場所で利用する必要がある。以下の点を考慮する必要がある。

### 5.1 システムの完全性の保証

完全性の保証により、システムにインストールされているソフトウェアの変更を防止すること、または少なくとも検出することが可能である。ソフトウェアの意図されたものではない変更または予想されない変更は、設計、製造、インストール、サービスのいずれかのプロセスで持ち込まれたマルウェアによるものである可能性がある。以下の節では、システムの完全性を保証するためのいくつかの技術的方法について検討する。

#### 5.1.1 ハードウェア保護

ハードウェアを使用することで、不正な方法でソフトウェアが変更されないことを保証するレベルを高めることができる。ROM (読み出し専用メモリー) や鍵のかかるキャビネットなどがある。

#### 5.1.2 チェックサムの計算

チェックサムを計算して比較することで、ファイルが変更されていないことを保証できる。チェックサムはファイルの内容から計算される値で、ファイルを使用する前にファイルの完全性をチェックするために利用できる。通常はシリアル回線を通したデータ送信に使用される簡単なパリティビットチェックから、MD-5 アルゴリズムを使用すると作成される 128 ビットメッセージまで、広範な実装が可能である。すべての方法は、計算を容易にし、計算された値と予想され

る値の正しい一致が変更されたデータについて発生する可能性が低くなるような、一般的な特性を共有する。

#### 5.1.3 デジタル署名

デジタル署名は、チェックサムを拡張したものである。チェックサムをデジタル署名として付加すると、不正なユーザーまたはプロセスによって元のファイルが変更される可能性をさらに低くすることができる。信頼性の高い署名検証には、複雑な公開鍵基盤 (PKI) が必要である。

#### 5.1.4 システムプロファイル

システムプロファイルは、チェックサムの単純なリストに留まらない高度なチェックサム計算システムである。ファイル属性の検証、ファイルの存在の有無、存在するファイルの全体的な組み合わせに関する他の多くの特性など、完全なディレクトリ構造を検証する。システムプロファイルでは、チェックサムに対応した高度な有害ロジックを検出するため、デジタル署名付きのデータベースが利用されることが多く、オペレーティングシステムの通常の機能をバイパスするファイルシステムチェックが組み込まれることもある。

#### 5.1.5 製造時スキャン

製造プロセスの適切なステージにおいてウイルス検出ソフトウェアを使用することは、システムの完全性を保証するもう 1 つの方法である。市販されているウイルス検出ツールを使ってスキャンを行うことで、提供される製品や更新情報がマルウェアに汚染されていないことを保証できる。ただし、この方法では、それ以降の感染を防ぐことはできない。

### 5.2 システム設計での防御

攻撃経路の多くでは、通常の使用方法では問題が発生しないような、ソフトウェア開発時のありふれたエラーによる欠陥が利用される。このような誤りで最も一般的なものは、“ バッファオーバーフロー ” エラーと呼ばれるもので、すでに多くの悪意ある攻撃によって利用されている。このエラーを利用することで、有害なコードは、割り当てられたバッファをオーバーフローさせ、システムの制御を奪うことができる。
エンジニアリングスタッフが使用する設計方法は、このような欠陥を防止、検出、除去するのに有効なものでなければならない。エンジニアリングスタッフが使用する必要のある具体的なツールと技法のいくつかについて、以下で説明する。

#### 5.2.1 開発ツール

コードを分析して欠陥を検出し、その除去を支援する開発ツールや手法がある。

#### 5.2.2 プログラミング言語

Java や C#のような一部のプログラミング言語には、ある種のマルウェア攻撃を防御するセキュリティ機能が組み込まれている。また、C や C++のような他の言語に対しても、ある種の攻撃に対する脆弱性を低下させるために使用できるサポートライブラリやコンパイラ機能が存在している。

#### 5.2.3 OS およびハードウェアのサービス

一部のオペレーティングシステムやハードウェアには、実行保護ビットや特権リングのようなセキュリティ機能が用意されている。アプリケーションは、可能な範囲内の最も低い特権で動作する必要がある。

#### 5.2.4 ネットワークサービスの制限

多くの MedIS システムは、論理ポートや利用可能なネットワークサービス群などの多くのネットワーク機能が組み込まれた、一般的なコンピュータプラットフォームがベースになっている。必要のない機能、ポート、サービスをすべて削除し、マルウェアによって攻撃される可能性のある箇所を取り除く必要がある。たとえば、電子メールや Web アクセスなどのサービスを必要としない MedIS からは、これらの機能を削除する必要がある。一般的なコンピュータプラットフォームを使い慣れたユーザーにとっては、これらの機能がないことは気になるかもしれないが、IT セキュリティの向上のためには、それが普通のことであり望ましいことを理解してもらう必要がある。

### 5.2.5 セキュリティに焦点を当てたエンジニアリングサービス

ピアレビューやソフトウェアウォークスルーセッションなど、独立した担当者によるソフトウェア監査やインスペクションを行うことで、不注意によるエラーをさらに減らすことができる。これらの技法は、主に、機能的な欠陥の検出に使用される。実施の範囲を、脆弱性の低下まで含むよう拡張する必要がある。

## 5.3 ホストウイルスチェッカー

ウイルスチェッカーまたはウイルススキャニングソフトウェアは、ハードドライブやディスクでそのソフトウェアが認識するウイルスを検索するアプリケーションソフトウェアである。ウイルスチェッカーは、通常、スキャン“エンジン”と呼ばれる実行可能アプリケーションと、スキャンエンジンが既知のウイルスをスキャンするために必要な情報が収められたウイルスパターンのデータファイルで構成される。新しいウイルスの出現は頻繁だが定期的ではないので、パターンファイルの更新情報の配布とインストールも、定期的にではなく、短い間隔で行う必要がある。ウイルスを検出すると、ウイルスチェッカーは、あらかじめ設定されているアクションを実行する。たとえば、ログファイルにエントリを作成したり、ポップアップウィンドウを開いて警告テキストを表示したり、汚染されたファイルの自動修復を試みたりする。

MedIS とウイルススキャナーの併用には重大な難点がある。ウイルススキャナーは、ウイルス検出と除去の万能薬ではない。ウイルススキャナーは大量のリソースを消費する場合がある。また、障害検出に対しては適切に機能しない場合がある。MedIS と共にウイルススキャナーを使用すると、以下のような影響が発生することがよくある。

- ウイルススキャナーが非常に多くのシステムリソースを使用したため、X 線などの医療画像が損傷を受ける。
- ウイルススキャナーが誤ってウイルスと識別したファイルを修復しようとしたため、医療画像ファイルが損傷を受ける。
- システムの動作の異常を検出するように設定されたウイルススキャニングソフトウェアが、医療ソフトウェアの動作を異常なものと誤って判断し、医療ソフトウェアをシャットダウンする。
- ウイルススキャナーのポップアップウィンドウが、医療画像や医療で必要な警告を覆い隠してしまう。

医療分野では、患者の安全と信頼できる運用のためには、適切な構成が非常に重要である。ウイルススキャナーの構成と維持管理においては、ベンダーの推奨に従う必要がある。

## 5.4 行動に関する防御策

前述した技術から選択したものに加えて、ベンダーは次のことを行わなければならない。

- プラットフォームコンポーネントに対するセキュリティ関連のパッチと更新に関する最新の情報を入手し、価値があると考えられる場合には顧客が利用できるようにする。
- 製品に対するマルウェアの感染およびマルウェアが原因の損傷の除去に関して顧客を支援できるようにしておく。

## 5.5 MedIS に対する要件と制限

標準的な事務用 IT と比べて、MedIS で使用される対応策の選択は、医療分野固有の規則および技術による要件からいっそう大きな影響を受ける。

- MedIS は、安全かつ効率よく動作しなければならない。保護メカニズムは、医療に関して意図されている装置の使用を妨げてはならない。
- 障害が発生した場合でも MedIS は患者の治療を続ける必要があるため、通常、MedIS は開いた状態で異常終了する。医療用でない IT 装置は、通常、閉じた状態で異常終了することはない。たとえば、現金自動預払機は、問題が発生した場合にはサービスを停止する。
- MedIS は、リリーステストを含めて、関連する行政規則 (QSR など) に準拠する必要がある。これは、新しい脅威への迅速な対応に対する要求とバランスを取る必要がある。

## 6. MedIS ユーザーのための有害ロジック対策

ベンダーと同様に、ユーザーも、管理的および技術的な手段を決定するには、まず、組織におけるリスクと脅威の分析を行う必要がある。「Identification and Allocation of Basic Security Rules In Healthcare Imaging Systems」[3] を参照すること。このような作業は、最も有効な場所へのリソースの割り当てに役立つ。また、その際には、以下の点を考慮する必要がある。

### 6.1 一般的なネットワークの防御

多くのネットワークルーターおよび他のネットワーク機器は、ある種のマルウェアからネットワークを保護するように構成できる。安全なネットワーク設計において考慮する必要のあるアクションの例を以下に示す。

- オペレーティングシステムおよびルーターレベルでの DoS の検出と改善。
- *接続認証*: 接続を要求するエンティティが提示する ID を確実に認証するセキュリティ技術 (Digital Imaging and Communications in Medicine (DICOM) 規格や IHE Basic Security Integration Profile で規定されているものなど) を使用して、MedIS に対するネットワークアクセスを管理できる。
- *ファイアウォール*は、通常はホスト上またはネットワーク間に設置され、主として内部のサービスに対する外部からのアクセスを防止する。ファイアウォールは、価値のあるセキュリティサービスを実行できる効果的で柔軟なツールだが、そのためには、十分な訓練を受けた要員が適切に管理および構成することが不可欠である。
- *ネットワークウイルススキャナー*は、受信および送信するデータから既知の有害ロジックを検出する。また、スパムや、電子メールまたは電子メールの添付ファイルを偽装する有害なロジックなど、望ましくない電子メールの選別も行う。欠点は、臨床ワークフローの速度が低下したり、障害検出警告に悩まされる可能性があることである。
- *監査ログおよび分析*: MedIS によって提供されるアクティビティログ情報は増加するものと考えられる。ネットワーク運用管理者は、この情報を利用することで、内部だけでなく外部の情報源からも、有害な動作をいっそう迅速に検出できる。OS の監査ログだけでなく、アプリケーションレベルの監査ログもある。両方を頻繁に確認し (リスク分析に基づいて)、組織のセキュリティーポリシーに従って対応する必要がある。
- *侵入検出システム (IDS)*: ハニーポットなどのさまざまな IDS を、医療施設のネットワーク内にインストールできる。IDS は、有害な可能性のあるさまざまな動作を検出できる。IDS が通知した時点では、何らかの損害がすでに発生している場合がある。
- *非武装地帯 (DMZ)* は、通常はプライベートネットワークとインターネットの間に配置される論理的な領域である。着信および発信の接続は、最初に、DMZ 内のコンピュータによって傍受される。プロキシおよび他のセキュリティ保護アプリケーションがトラフィックをスキャンし、セキュリティおよびルーティングに関する決定を行う。トラフィックを停止したり、他のコンピュータにルーティングしたり、プロキシ処理したりすることができる。
- *一元化の排除 - MedIS の分散化*: 有害なロジックは、普通、特定のタイプの IT ファミリーまたは IT プラットフォームの非常に限定された弱点を突く。したがって、IT 製品の一元化を避けることで、このようなシステムを対象とする攻撃によって影響を受けるシステムの数を減らすことができる。

### 6.2 行動に関する防御策

前述した防衛手段に加えて、組織では以下の処理や技術についてさらに考慮する必要がある。

- *ポリシー、手順、ユーザートレーニング*: 組織として、管理面でのセキュリティーポリシーと手順を準備する必要がある、その中では、特に、MedIS のユーザーに求められること、および不注意で、または故意にそれを無視した場合に適用される罰則を記述する。
- *災害時計画*: マルウェアの攻撃が発見された場合に、対応者が、何を行い、どのように対応するかを認識しているよう、損害管理修復計画を用意しておく必要がある。有害な攻撃の後で復元できるよう、重要なデータとソフトウェアをバックアップしておく。

- o 可能な場合は常に、物理的に MedIS を隠したり、ドアを閉じたり、キーボードをロックしたりして、MedIS への*物理的なアクセスを制限する*。さらに、MedIS への論理的なアクセスを、組織およびサービスプロバイダの身元が明らかな要員に制限する必要がある。
- o 他の装置やネットワークに対する MedIS の*すべての接続が必要かどうかを確認し*、絶対に必要な最低限の接続だけに減らす。訓練を受けた IT スタッフがルーターを適切に構成することで、高水準のセキュリティを実現できる。ワイヤレス通信については特に注意する必要がある。
- o SPCのホワイトペーパー「*Remote Service Interface Solution (A): IPSec over the Internet Using Digital Certificates*」[2] で解説されているように、保守サービスを受けるための時間とコストを節約する方法として、サービスに対する安全なリモートアクセスを実際に実現できる。
- o MedIS ベンダーから集中的な支援を受けられるよう、ベンダーとの密接な関係の維持を計画する。

### 6.3 縦深防御

縦深防御という概念は、企業のセキュリティ保護は管理を複数の地点で二重化することにより達成されることを示している。医療施設では、マルウェアおよび MedIS に対する他の脅威のリスクと影響に対し、複数の階層での防衛を確立する必要がある。たとえば、ホスト、部門、および企業のレベルで複数のタイプのファイアウォールを使用する。

## 7. 結論

このホワイトペーパーでは、有害なロジックによってもたらされる問題に対する 1 つの標準化された解決策を提示することはできない。代わりに、基本となる一連の適切な技術的手段について説明した。個別の状況によっては、有害なロジックによって発生する脅威に対する防衛の水準を MedIS を用いて向上させようとする医療提供者に対し、個々の手段の使用が役に立つ可能性がある。一部の手段については、MedIS の安全目的での使用に対する影響を詳しく分析する必要があり、したがって MedIS ベンダーが責任を持って行わなければならない。ほとんどの防衛手段は、適切に設定された一般的な IT ツールであり、医療提供者が適切に構成することが可能である。最善の方法は縦深防御である。

## 8. 参考文献

[1] 「Taxonomy of Threats and Security Services for Information Systems」、Gulachenski、Cost、(研究報告書: Project No.:8353Z、Contract No.:DAAB07-94-C-H601)、MITRE、1994 年

[2] 「Remote Service Interface Solution (A): IPSec over the Internet Using Digital Certificates」、NEMA/COCIR/JIRA 合同セキュリティおよびプライバシー委員会、2002 年

[3] 「Identification and Allocation of Basic Security Rules In Healthcare Imaging Systems」、NEMA/COCIR/JIRA 合同セキュリティおよびプライバシー委員会、2002 年