4.2.6. 情報セキュリティインシデントの管理

A.13 情報セキュリティインシデントの管理		
A.13.2 情報セキュリティインシデントの管理及びその改善 目的：情報セキュリティインシデントの管理に，一貫性のある効果的な取組み方法を用いることを確実にするため。		
番号	管理項目	実施状況
A.13.2.2	情報セキュリティインシデントからの学習	3　不十分ではあるが、これに近い手順が文書化され実施されている。 →ベンダの保守マニュアル等にあるのかも知れないが、A-netとしての管理策を充実させるべきである。
A.13.2.3	証拠の収集	3 通常のログ収集手順の範囲で手順が文書化され実施されている。ただし、証拠保全、提出を前提とするには不十分である。 →ベンダの保守マニュアル等にあるのかも知れないが、A-netとしての統一した証拠収集のための管理策を充実させるべきである。

4.2.7. 事業継続性管理

A-net の場合は、一般的な企業がおこなう事業とは性格を異にするので、全体として大規模災害時の A-net 運用や可用性についてのみ検討し、管理策の個々の項目について検討したわけではない。

大規模災害のみを想定しているようであるが、コンピュータウィルスの大規模な蔓延時や DDoS 攻撃による運用が可能な場合も想定した方が良い。

また、縮退運用や代替センタ（国立大阪病院）への移転等は、本来の運用へ戻す方法、個々の災害（障害）ごとの復旧目標時間なども考慮しておくべきである。

なお、これらの詳細な計画について公に公開する必要は無い。

また、今回閲覧した文書以外にこれらの指摘事項を明記した文書がある可能性もある。

4.2.8. 順守

A.15 順守		
A.15.1 法的要求事項の順守 目的：法令，規制又は契約上のあらゆる義務，及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。一般的にコンプライアンスと呼ばれることである。		
番号	管理項目	実施状況
A.15.1.1	適用法令の識別	1 明確な記述は見当たらない。 →順守している法令について記述するべきである。
A.15.1.4	個人データ及び個人情報の保護	3 管理策としては、かなり厳しい対策が立てられているが、最新の関連法令に準拠したものではないと考える。 →個人情報保護法など最新の法令に準拠した管理策を策定すべきである。
A.15.2 セキュリティ方針及び標準の順守，並びに技術的順守 目的：組織のセキュリティ方針及び標準類へのシステムの順守を確実にするため。		
番号	管理項目	実施状況
A.15.2.1	セキュリティ方針及び標準の順守	3 これに相当する文書化された手順があるが、最新の標準類に準拠したものではないと考える。 →JIS Q 27001:2006 など最新のセキュリティ標準に準拠した管理策を策定すべきである。
A.15.2.2	技術的順守の点検	3 これに相当する文書化された手順があるが、最新の標準類に準拠したものではないと考える。 →上記と同じく、JIS Q 27001:2006 や JIS Q 27002:2006 など最新のセキュリティ標準の要求事項を考慮し最新のセキュリティ技術を考慮した管理策を策定すべきである。
A.15.3 情報システムの監査に対する考慮事項 目的：情報システムに対する監査手続の有効性を最大限にするため，及びシステムの監査プロセスへの干渉及び／又はシステムの監査プロセスからの干渉を最小限にするため。		
番号	管理項目	実施状況
A.15.3.1	情報システムの監査に対する管理策	1 これに相当する管理策が無い。 →今回の監査では、この管理策が無いために実システムに対する脆弱性検査や設計文書の閲覧ができなかったと考えるので、これらを考慮した管理策を策定すべきである。
A.15.3.2	情報システムの監査ツールの保護	1 これに相当する管理策が無い。 →A.15.3.1 の策定に合わせた管理策の策定が必要である。

5. A-net の今後のあるべき姿

この章では、次のことを目的とする。

(1) 前章のセキュリティ監査結果を踏まえて、現状のA-netの問題点を洗い出すこと。

(2) 洗い出された問題点を解決し、かつ新たな価値を付加するような、新しいA-netの方向性について検討する。

5.1. A-net の発足時の理念

A-net の現状の問題点について洗い出す前に、A-net の目的の確認ということで、A-net 発足時（平成 9 年頃）の理念を提示する。

(1) セキュリティを確保した病院間ネットワーク
・利用者の講習会と簡易テスト
・サーバルームの管理とバックアップシステム
・端末設置場所の確認
(2) HIV 診療の標準化（地域格差のない医療の提供）
・共通カルテによる最低限必要な医療情報の提供
(3) 医療情報の研究利用への応用
・すべての患者からの同意書
(4)患者参加型の医療のモデル
・運用ルール作りに患者も参加

5.2. A-net の現状の問題点

5.2.1. A-netの技術面の問題点

項目	問題点の内容
アプリケーションサーバ	・ハードウェアのサポート停止予定。（一部のハードウェアは既に停止。） ・ソフトウェアのサポートの停止。
VPN 機器	・平成 12 年度で現 IBM のトンネリング方式の VPN ソフトウェアの販売が終了となり、平成 13 年度と平成 14 年度は、IBM の例外処理によりライセンスを供給されたが平成 15 年度以降は、新規参加施設募集を休止し現在に至る。 ・ハードウェアのサポート停止予定。 ・ソフトウェアのサポートの停止。
クライアント側の Web ブラウザ	・Netscape Communicator4.75 という平成 12 年（2000 年）に公開された Web ブラウザが必要であり、Internet Exploler 6 が業界標準の現在では操作や新規参加の障壁となっている。
セキュリティ標準への準拠	・当初のコンセプトは先進であったが、開発から 10 年が経ち、現在のセキュリティ技術標準、セキュリティ管理標準から遅れ始めている。
技術の古さ	・物理的な機器と基本ソフトウェアがともに今の水準からすると古く、新しいコンセプトを受け入れ開発できる余地が無い。
性能問題	・上記に関わる問題でもあるが、ハードウェア機器のパフォーマンスが現在の水準からすると良くない。

5.2.2. A-netの運用面の問題点

問題点の内容
限定された施設でしか、自動取り込みができない。
自動取り込みができない施設では、入力に手間がかかる。その手間が嫌がられて使われないという悪循環に陥っている。
端末買い上げによって、技術の進歩やセキュリティ標準の変化に容易に対応できない。
登録には患者の同意が必要であり、全数登録が難しい。
入力項目、内容の妥当性。
アクセスできる環境が限られる。

5.3. 次期 A-net の方向性

5.3.1. 重点検討項目

次期 A-net の方向性を検討する場合の重点検討項目は次のものになると考える。

(1) コスト削減
(2) システムそのものの利用価値の向上
(3) セキュリティの確保
(4) 運用管理のしやすさ
(5) 利便性の向上

これらの項目は相互に背反、矛盾するものもあるが、それぞれの要件を検討し次期 A-net へは費用対効果、適材適所への適用を考えて実装方法を決めていくものである。

本書の前半でセキュリティ監査をおこなっている関係もあるが、以降、「セキュリティの確保」を軸に各重点項目について検討する。その理由について次に記す。

例えば、「セキュリティを確保」するための投資を誤ると「コスト」が増す場合が多い。これは、「セキュリティを確保」するための手段の投資を増大すると製品やその運用「コスト」が増すということだけではなく、その反対に「セキュリティを確保」するための手段の投資が少ない場合でもシステムの可用性が低くなったり、情報漏えいなどの情報セキュリティインシデント発生時の処理(賠償、訴訟費用など)にかかる「コスト」が増したりすることがあるからである。

また、「セキュリティの確保」無しには、「システムの利用価値の向上」の意義はほとんどなく、逆に「運用管理のしやすさ」や「利便性の向上」などは「セキュリティの確保」とは背反する場合が多い。

これらが「セキュリティの確保」を軸に検討する理由である。

5.4. セキュリティの確保の考え方

5.4.1. 情報セキュリティポリシの概念

実際にセキュリティの確保を考える場合は、いわゆる「情報セキュリティポリシ」の概念に沿って進めると網羅性が良く、漏れが少なくなる。ISMS 認証の取得は別にしても、患者様や医療機関の関係者を説得し納得いただくためにも社会的に認知度の高い情報セキュリティマネジメントシステムに則って進めるべきである。

「情報セキュリティポリシ」は、組織の情報資産を利用・管理するすべての者に対し、故意、偶然および事故などという区別に関係なく、情報資産の改ざん、破壊、漏洩等から保護されるような管理策を体系的にまとめたものである。

次に一般的な企業における「情報セキュリティポリシ」の概念を記す。

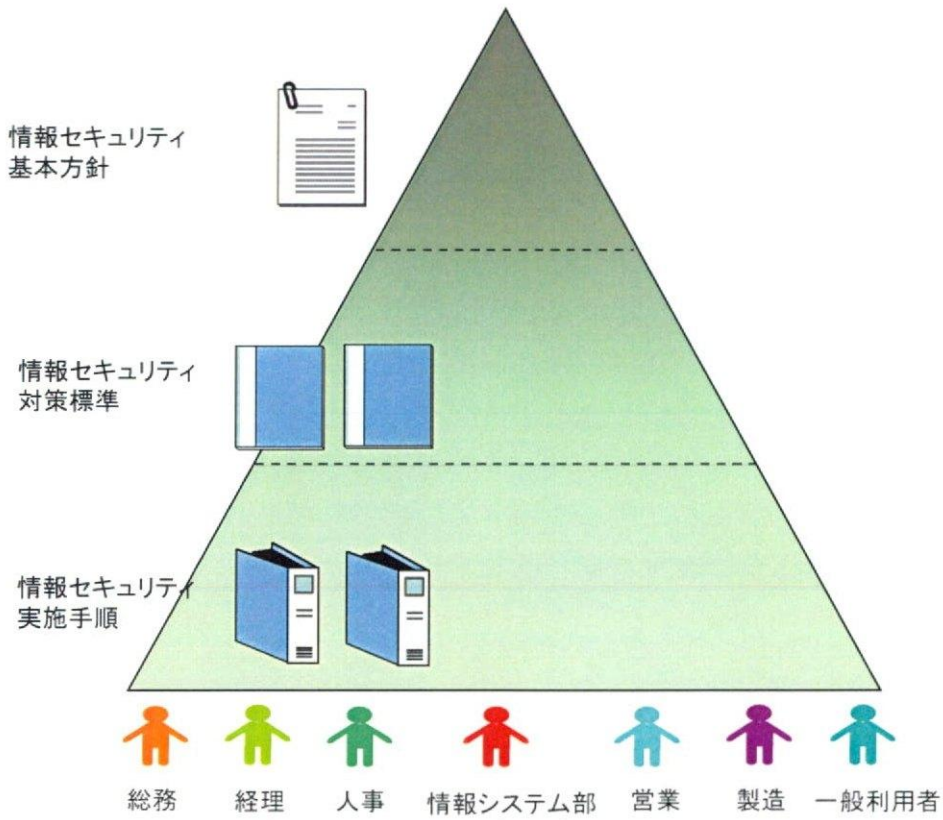


図 5.4.1 情報セキュリティポリシの体系

(1) 「情報セキュリティポリシ」の適用範囲

「情報セキュリティポリシ」の適用範囲は、組織の情報資産に関連する人的・物理的・環境的リソースを含むものとする。

(2) 「情報セキュリティポリシ」の適用者

「情報セキュリティポリシ」の適用者は、組織の情報資産を利用するすべての者である。

情報セキュリティの三要素である「機密性」、「完全性」、「可用性」を確保し維持するためにこれらの文書体系は構築されなければならない。

機密性・・情報資産の機密に基づく重要性
完全性・・情報資産の完全性・正確性に関する重要性
可用性・・情報資産の利用可能性・継続性に関する重要性

(3) 情報セキュリティポリシ対策標準のカテゴリ

情報セキュリティポリシ対策標準のカテゴリは、次のJIS Q 27001:2006の付属書Aにある管理策のカテゴリに沿って、漏れのないように情報セキュリティ対策標準としてまとめるべきである。

1) セキュリティ基本方針
2) 情報セキュリティのための組織
3) 資産の管理
4) 人的資源のセキュリティ
5) 物理的および環境的セキュリティ
6) 通信及び運用管理
7) アクセス制御
8) 情報システムの取得、開発及び保守
9) 情報セキュリティインシデントの管理
10) 事業継続管理
11) 順守

(4) 作成すべき情報セキュリティ対策標準の例

(3)で述べた、JIS Q 27001:2006の付属書Aにある管理策の中から、情報技術分野に特化したセキュリティ対策標準の一般的な例を次の表に記載する。

表 5.4.1 セキュリティ対策標準の例

対策カテゴリ	作成する対策標準
人的対策	人による誤りや設備誤用のリスクを軽減するための管理策。 (1) アカウント管理 (2) ユーザ認証 (3) 委託時の契約 (4) プライバシー (5) セキュリティ教育
物理的対策	業務施設及び業務情報に対する認可されていない物理的なアクセス、損傷及び妨害を防止するための管理策。 (1) サーバルーム (2) 職場環境

	(3) 職場設備
ネットワーク対策	ネットワーク及び関連する機器類に関わるリスクを軽減するための管理策。 (1) ネットワーク構築 (2) LANにおけるPC設置・変更・撤去 (3) 社内ネットワーク利用 (4) リモートアクセスサービス利用 (5) 専用線及びVPN
サーバ対策	サーバに関わるリスクを軽減するための管理策。 (1) ソフトウェア・ハードウェアの購入及び導入 (2) 外部公開サーバ (3) サーバ等におけるセキュリティ
クライアント対策	クライアントに関わるリスクを軽減するための管理策。 (1) クライアント等におけるセキュリティ (2) ウィルス対策
運用的対策	情報システムの運用面に関わるリスクを軽減するための管理策。 (1) システム維持 (2) システム監視 (3) 電子メールサービス利用 (4) 全社ネットワーク利用 (5) Web サービス利用 (6) 媒体の取り扱い (7) 文書改正 (8) 監査 (9) セキュリティインシデント報告・対応
事業継続管理対策	重大な障害または災害の影響が与えるリスクを軽減するための管理策。 (1) 事業継続計画

A-net は公的な医療機関のシステムであり、利用者も一般的な企業とは異なるため、上記の例が必ずしも当てはまるわけではない。

実際に、A-net を対象とした情報セキュリティポリシの対策標準や実施手順を策定する場合は、下記の文書を参考にすると良い。

1. JIS Q 27002:2006 情報技術—セキュリティ技術—情報セキュリティマネジメントの実践のための規範
2. 「医療情報システムの安全管理に関するガイドライン 第 2 版(案)」

また、医療機関のセキュリティに詳しいコンサルティング会社や医療系のセキュリティコンサルティング経験のある IT ベンダなどに依頼することも一つの方法である。

5.4.2. セキュリティのアーキテクチャ

セキュリティのアーキテクチャの考え方は、多層防御 (Defense in Depth) の概念を採用すると良いと考える。情報セキュリティポリシの策定から設計、実装に至るまで、この考え方で進めておけば漏れが少なくなると判断する。次に、その概念について述べる。

システム内では、単一のセキュリティ対策に頼ってアクセス制御をした場合、そのセキュリティ対策に不備があり、攻撃者がその単一のセキュリティ対策を突破した場合、システムへの脅威は一気に高まる。システムの複雑化による潜在的な技術的脆弱性(セキュリティホール)の増大やクラッキング技術の進歩などによっても、システムへの脅威は日々変化する。

そこで、シングルポイント(単一のセキュリティ対策)の突破によるセキュリティの脅威を軽減するためにネットワークシステムの中でのセキュリティ対策は、同様の機能を持つセキュリティ対策をネットワークトポロジの異なった場所で実装し、2重、3重の防御体制を取ることを検討すべきである。

次に多層防御 (Defense in Depth) の概念図を示す。

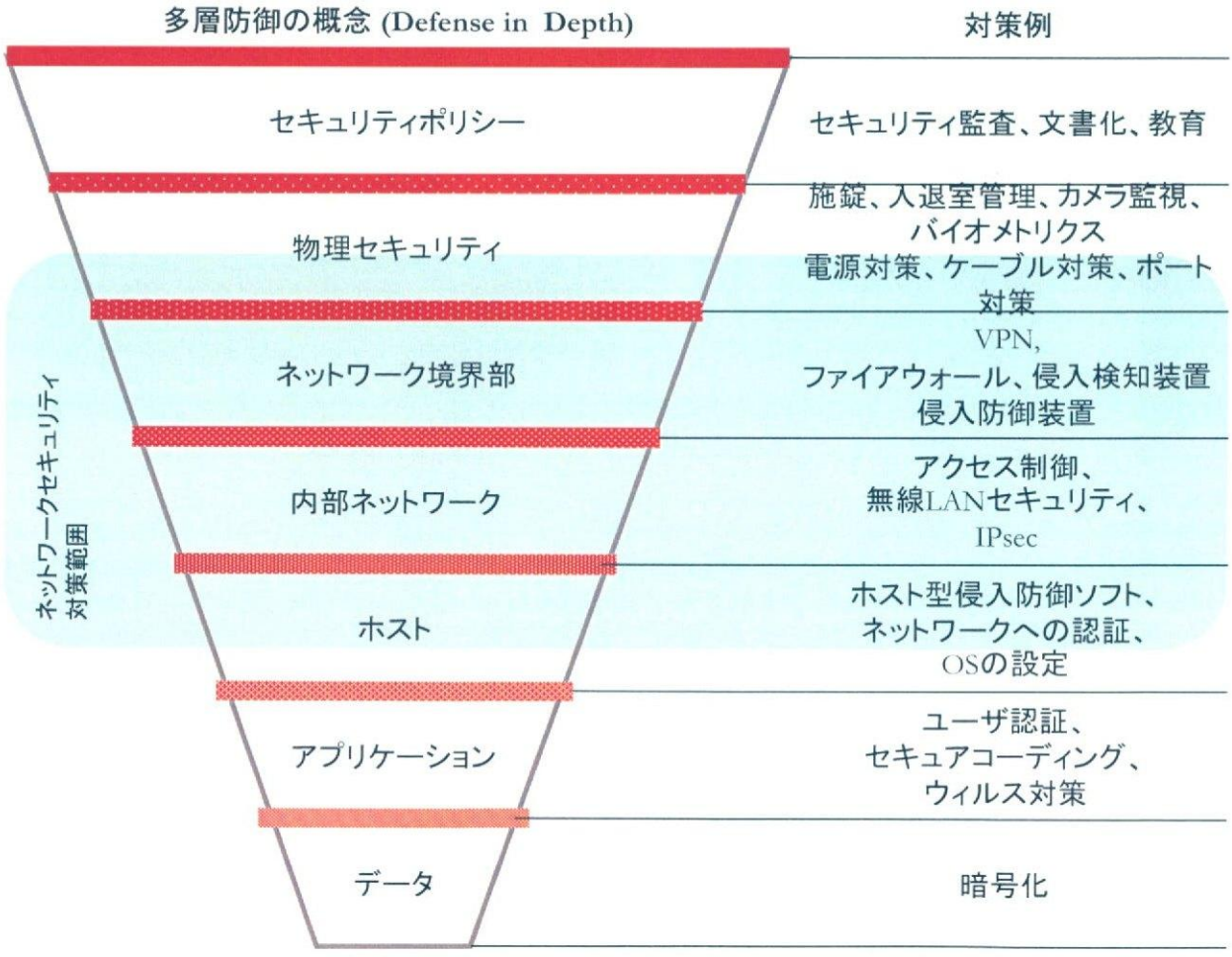


図 5.4.2 多層防御の概念図

概念図の中で、「ワームによる脅威」の対策を例にとって考えると、多層防御の上の層から

1) セキュリティポリシ層の教育(情報)による、正しいワーム対策の周知。
2) ネットワーク境界部層に置いたセキュリティゲートウェイ(ファイアウォール、侵入検知装置、侵入防御装置など)によるワームの遮断。
3) 内部ネットワーク層における Layer2, Layer3 デバイスでのワームの遮断。
4) ホスト層の、PC におけるホスト型侵入防御ソフト、アンチウィルスソフトによるワームの遮断
5) アプリケーション層のセキュアコーディングによるワームの無力化

という対策をとることができる。ワームによる攻撃の実行者はデータの破壊、漏洩に行き着くには何段かのセキュリティ対策を突破しなければならない。

2 重、3 重の防御体制を取る場合、システム全体の中でセキュリティ脅威の軽減の観点で最も有効なセキュリティソリューションの設定位置を精査し、守るべき情報資産の重要性や運用管理コストを含めた費用対効果を検討した上で実装の可否を決定すべきである。

5.5. セキュリティの実装

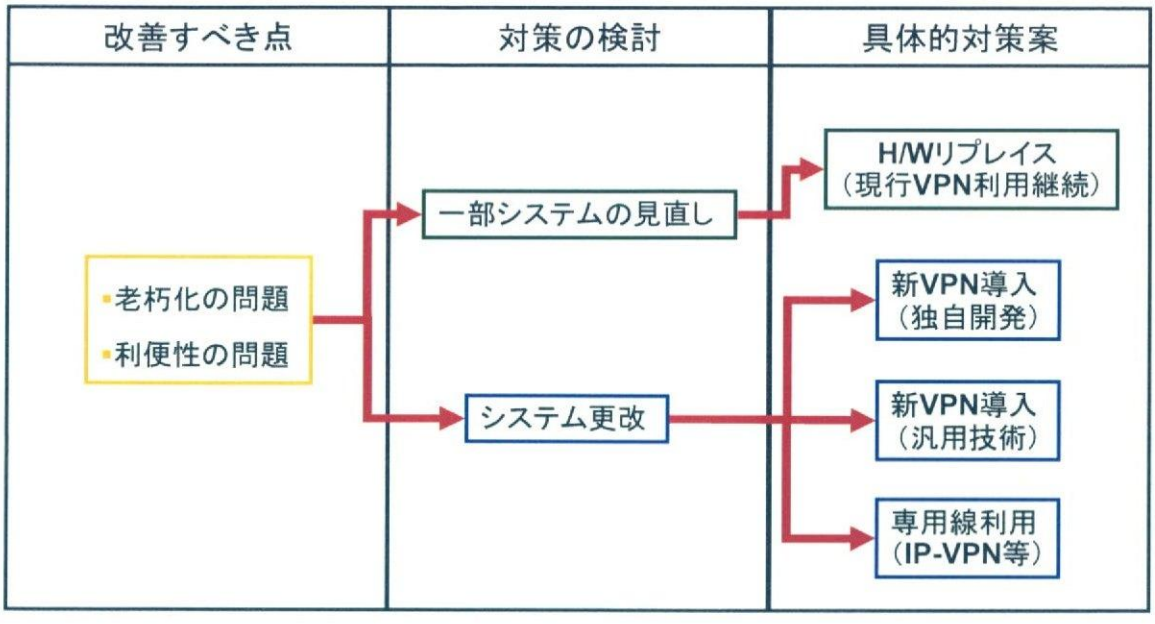
これまでの調査で明らかになった、セキュリティの技術的な問題点に対して最新の技術を実装することによる改善方法を提示する。

5.5.1. VPN

本セキュリティ監査の中で明らかになったのは、対象 VPN 機器の販売停止、サポートの停止である。

現在の VPN は老朽化と利便性の問題があり、これらの検討と具体的な対策案は次のようになる。

図 5.5.1 VPN の対策検討



次に、それぞれの具体的対策案に関して検討する。

表 5.5.1 対策案の比較

		セキュリティ	利便性	運用	コスト
インターネット回線	現行 VPN	△現在の水準に合わない	×専用端末が必要であり新拠点の追加ができない	△独自技術のため専門の技術者が必要となる	○運用できる人が限られため運用コストが高い。
	新 VPN（独自技術）	◎独自に開発をおこなうため強固である	○独自の技術のため互換性がない	△独自技術のため専門の技術者が必要となる	△開発、運用に多額の費用がかかる。
	新 VPN（汎用技術）	○現在の水準をみたしている	◎汎用性があり、接続形態に自由度がある	○一般的な技術のため運用の標準化が可能	◎一般的な技術のため運用の標準化が可能
専用線（IP-VPN 網等）		◎閉域網のためセキュリティーレベルは高い	△専用線を利用するため提供出来るエリアが限られる	○一般的な技術のため運用の標準化が可能	△拠点全てに専用線を引き込む必要があるため高コスト

対策案の比較検討の結果、汎用技術を実装した新 VPN である SSL-VPN を最優先で検討することが望まれる。

SSL はオンラインバンキングや電子商取引でも使用されており実績がある。PC に通常搭載されているブラウザには、SSL-VPN のクライアント機能があり新たにソフトウェアを導入する必要が無い。

SSL-VPN は A-net のセンター側で VPN(暗号化)装置を設置すれば、拠点側で VPN 装置を設置する必要がなく保守運用性やコスト面でも優れている。

5.5.2. エンドポイントセキュリティ

本項では、A-net のネットワークの終端(エンドポイント=End Point)に接続されるものとして、エンドポイントデバイスのセキュリティ対策についてまとめる。この対策を実装するには、あらかじめ「PC 端末利用手順」や「PC サーバ利用手順」等のエンドポイントデバイスに関連するセキュリティポリシを策定しセキュリティに対する要件を定義する必要がある。

(1) 想定される脅威

A-net のネットワークのエンドポイントに配置されネットワークプロトコルを介して接続される PC 端末、PC サーバには、機密性、完全性を要する重要なデータがおかれ、システムの内側から外側に向かって見ると、システム管理者にとっては最前線の防御点である。

また、反対にエンドポイントからシステムの内側を見ると、USB などのポートに接続されたデバイスを経由した情報漏洩、および悪意のあるソフトウェアの侵入という脅威がエンドポイントから発生することを想定する必要がある。悪意のあるソフトウェアは一般的なアンチウィルスソフトを利用することによってあるていどリスクを回避できるが、アンチウィルスの定義ファイルが更新されていない時期に発生する、ゼロディアタックには対処できない。

加えて、正当な利用者が使っている、正当な端末であるかという認証や、その端末がセキュリティポリシを順守しているかどうかという認証も必要な場合がある。ある程度セキュリティの確保された場所で病院関係者だけが操作していることが保証されている場合は、比較的安全であると言えるが、将来的に患者様が自宅から自分自身で操作する場合には、このような認証方法も検討すべきである。

(2) 対策

a) ゼロディアタックへの対策は、エンドポイントへの悪意のある動作やセキュリティポリシ関連の動作(悪意は無くとも状況により危険性がある動作)を判断し抑止するためのソフトウェアを使用することにより対策できる。ふるまいによる危険な動作を抑止するソフトウェアはアンチウィルスソフトウェアと同時に動作して最大の効果を発揮する。

これらのふるまい関連の危険な動作は次のようなものを想定している。

表 5.5.2 エンドポイントへの脅威と分類

脅威の分類	脅威
悪意のある動作	➢ オペレーティングシステムに対する不正な改ざん ➢ 意図しないファイルの削除、新規ファイルの作成 ➢ 意図しないプログラムのインストール ➢ バックドアを仕掛けるプログラムのインストール ➢ バッファオーバーフロー攻撃 ➢ DoS アタック ➢ メールソフト管理下のファイル(アドレス帳)への不自然、不合理なアクセス ➢ ネットワークリソースへの不自然、不合理なアクセス(ポートスキャン、DoS 攻撃など) ➢ P2P 関連(Winny など)のファイル交換ソフトウェアのインストール

ポリシー関連の動作 （悪意がない場合でも危険性がある。）	➢ ウェブブラウザなどからファイルをダウンロードさせるかどうか。 ➢ ダウンロードしたファイルを実行させるかどうか。 ➢ メールの添付ファイルを開封させるかどうか。添付ファイルの危険性を考慮する。 ➢ 着脱可能な記憶装置を使用許可とするか。着脱可能な記憶装置（USB メモリなど）経由での悪意のあるファイルの侵入や情報漏洩。読み出しと書き込みの許可、不許可の区別。 ➢ PCに内蔵されている、記憶装置を使うか。読み出しと書き込みの許可、不許可の区別。 ➢ メッセンジャーソフトを使用する際、プログラムをダウンロードさせるか。 ➢ 新規にプログラムをインストールさせるか。 ➢ 既にインストールされている、特定のアプリケーションを利用させるか。

b) ユーザ認証、端末認証に関しては、802.1x のような現在、標準的で実績のある認証方式の採用を検討する。

[802.1x 概要]

- LAN および MAN 向けに標準化された IEEE Standard （標準化終了：2001 年 10 月）
- Port-Based Network Access Control
  - ✓ ネットワークの入口（Switch Port, Wireless AP）でのユーザ認証とアクセス制御手段を提供
- LAN 環境でのユーザ識別によるセキュリティ確保を目的
  - ✓ 認証されていないクライアントからの通信を（認証要求を除いて）すべて遮断し、認証されたユーザにのみ通信を許可する
- 認証は RFC の EAP を使用 -（EAP – Extensible Authentication Protocol）
  - ✓ 802.1x は認証時の通信経路の暗号化を行わないため、別途 RFC に定義された EAP と言う技術を用いて通信経路の暗号化をおこなう。
  - ✓ 認証システムには RADIUS を使用 （RADIUS 側が EAP タイプを認識する必要がある）
- 802.1x 認証を標準でサポートする OS の登場
  - ✓ WindowsXP で採用

c) 802.1x 認証での「端末認証」と「ユーザ認証」による認証方式は、端末のセキュリティポリシ（「PC 端末利用基準」など）への準拠度合いは判断できない。

A-net のネットワークへ接続を試みようとする PC 端末に実装されているセキュリティ対策（アンチウィルスソフトウェアのインストールの有無や定義ファイルの更新の日付など）をセキュリティポリシに照らし合わせて検査し、その結果をもって、A-net のネットワークに接続させるか、させないかを判断する方が、802.1x 認証よりもセキュリティ強度が高くなる。

このセキュリティポリシへの準拠度合いの検査を、802.1x でおこなう「端末認証」と「ユーザ認証」に対して「状態認証」と定義する。

IT ベンダの何社かは、これに相当する機能を提供する製品を販売している。費用対効果を考えて実装の可否を検討することが望ましい。

5.5.3. アプリケーション指向のネットワーク

A-net のシステムに保存されているデータは、治療目的に限定すると個人情報と診療情報の連結は必須である。しかし研究目的に限って考えると、個人が特定できる個人情報ではなく、研究に必要な範囲にかぎり匿名情報で十分な場合があると考えられる。たとえば、名前や生年月日や住所を特定せずに、名前の変わりに識別番号を振って次のようなデータ構造を仮定する。

番号	性別	年齢範囲	居住地域	感染歴	発症歴	その他(個人を特定できない属性情報)
00001	男性	20-25	関東	4 年	2 年	

このような情報であれば、これまでA-netに登録することに対して同意が得られなかった患者様にも理解されやすくなるかもしれない。あるいは、もっと縮小された情報でも十分に目的を達することができる場合もあることも想定できる。

注) 個人情報の匿名的な取り扱いについては、データの内容が機密性の高いものだけに事前に、患者様との合意や法律や医療、技術関係の識者達との意見交換が必要であると考える。

このようなことを実現するには、A-netのセンターのデータベースサーバから患者様の情報を取り扱う場合は、患者様情報をネットワークに送り出す時点で匿名化された情報に変換する方法があれば良い。連携機関へは必要な情報のみ匿名化して送る、すなわち、サーバではなくネットワーク機器自身がアプリケーションを理解しデータの中身を精査し変換するようなソリューションである。
IT ベンダの何社かは、これに相当する機能を提供する製品を販売している。費用対効果を考えて実装の可否を検討することが望ましい。

5.5.4. ネットワーク境界部のセキュリティソリューション

A-net のセンターでは現在、ネットワーク境界部のセキュリティソリューションとして、ファイアウォールと VPN のみを利用しているが、現在のネットワークセキュリティの脅威から考えてファイアウォールだけでなく侵入検知装置や進入防御装置の導入の検討が必要になるかも知れない。

その場合、何台もネットワーク境界部のセキュリティソリューション製品を購入すると、導入コストも運用コストも非常に高いものとなる。

現在ではこれらの機能を複合化した製品があるので、セキュリティ要件を精査した上で、このような製品を A-net のセンターへの導入を検討することが望ましい。

以上