3.8.8. 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。
A.15.1.2	知的財産権（IPR）	4 実施されている。
A.15.1.3	組織の記録の保護	0 A-net では、これに相当するような事象はないと考えるため対象外とする。
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。
A.15.1.5	情報処理施設の不正使用防止	4 実施されている。
A.15.1.6	暗号化機能に対する規制	0 A-net では、これに相当するような事象はないと考えるため対象外とする。
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。
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。
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。

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。

4. 意見区分

A-netの情報セキュリティマネジメントの実施状況の内容を総合的に判断しながら、助言型の監査報告をおこなう。

4.1. 監査結果要約

今回入手した情報を閲覧したり、保守(試験)系のシステムを操作したりした限り、HIV患者の個人情報を取り扱うということで相当に個人情報の保護をはじめセキュリティに対する意識が高いことがうかがい知れた。平成 10 年に試験運用を開始したシステムであることを考えると、その当時からセキュリティ技術、セキュリティ管理に関して先進的な考えを取り入れてきた結果が運用開始以降、これまでセキュリティインシデントが発生しなかった大きな理由であると言える。

製品の販売停止、サポートの停止などの影響でシステムそのものの大きな更新や利用者の増大は、ここ数年間無かったようであるが、保守運用業務仕様に関しては、セキュリティへの関心が高くなった昨今の情勢を反映してか、最近のセキュリティ管理の考え方を取り入れているようであることも評価できる。今後、望まれるのは、個人情報保護法や最新の情報セキュリティマネジメントの要求事項である、JIS Q 27001:2006 などを意識した改善である。

運用でカバーできる範囲は、継続的に改善していることが見受けられ、最近のセキュリティ管理手法と乖離する部分は大きくはないが、物理的環境的側面で見ると、サポート期限の切れたハードウェアやソフトウェアを基幹部分で使っており、新たなセキュリティの脆弱性を突かれる危険性や故障の際の交換部品の入手困難さなどを考えると早急な対処を考えるべきである。

加えて端末側にも現在となってはかなり古いソフトウェア (NetscapeCoominicator4.75)が必須であり、最新の PC で動作させるのには一手間かかり、このことも利用者が増えない障壁となっていると考えられる。

4.2. 検出した不適合事項

次に不適合事項(レベル 4 以外)と判断した項目についてに助言的意見を記述する。ただし、4 以外でも運用上問題が少ないと考えられるものは除外している。

4.2.1. 資産の管理

「資産の管理」に」ついては特に問題がないと判断した。

4.2.2. 物理的及び環境的セキュリティ

A.9 物理的及び環境的セキュリティ		
A.9.1 セキュリティを保つべき領域 目的:組織の施設及び情報に対する認可されていない物理的アクセス,損傷及び妨害を防止するため。		
番号	管理項目	実施状況
A.9.1.3	オフィス,部屋及び施設のセキュリティ	1 明確な記述が見当たらない。 →明確な記述は見当たらないが、A-net 専用ではなくとも国立国際医療センターをはじめ各医療機関でこれに類する記述をした文書があると想定するので、その内容を精査した上で、その記述を引用した文書を作成することが望ましい。
A.9.2 装置のセキュリティ 目的:資産の損失,損傷,盗難又は劣化,及び組織の活動に対する妨害を防止するため。		
番号	管理項目	実施状況
A.9.2.4	装置の保守	1 可用性、完全性を維持するための文書化された手順はあるが、一部、老朽化してベンダの保守期限が切れたものがあり、必要十分とは言えない。 →次の対策をすることが望ましい。 a) サポート可能な機器への入れ替え。
A.9.2.5	構外にある装置のセキュリティ	1 リモート接続による管理策については、装置そのもののセキュリティ対策については、ウィルス対策等しか見当たらず、覗き見(ショルダーハッキング)対策やクリアスクリーン ポリシなどに関する記述が不足しており不十分である。 →次のような記述を含めることが望ましい。 a) アクセス権の無い人物が付近にいることが想定される場所(待合室など)に情報端末等をおかなければならない場合は、ID、パスワードによるアクセス制御を正しくおこない、短時間(数分程度)でスクリーンセーバが動作するような設定にすること。 b) アクセス権の無い人物が付近にいることが想定される場所(待合室など)に情報端末等をおかなければならない場合は、その情報端末自身が重要なデータを保存しないような運用にすること。ま

		た、キャッシュに保存したデータも利用後は端末内に残らないような設定にすること。または、セキュリティワイヤなどで、端末を物理的に保護すること。
		c) アクセス権の無い人物が付近にいることが想定される場所(待合室など)に情報端末等をおかなければならない場合は、同等機器の持込みによる成り済ましを防ぐために通信ケーブルは容易に抜き差しできないような仕組みのものを採用すること。
		d) アクセス権の無い人物が付近にいることが想定される場所(待合室など)に情報端末等をおかなければならない場合は、情報端末自身が盗難にあわないように接続されるケーブル類が容易に抜き差しできないような仕組みのものを採用すること。
		e) 複写機やファクシミリなどは、情報漏洩の道具として使われやすいので。セキュリティの保たれた領域内の適切な場所に設置すること。
		f) デジタルカメラつき携帯電話や小型デジタルカメラの使用による情報漏洩を防ぐためにセキュリティ区画への入室の際には、持ち物を検査し、デジタルカメラ類を預かるような運用を検討すること。
A.9.2.6	装置の安全な処分又は再利用	1 実運用としてはなんらかの安全対策はされているようであるが、明確な文書化された対策は見当たらない。 →下記は一つの例であるが、昨今は廃棄処分したはずの情報機器から情報漏えいが発生することもあるので、利用者の安心感を高めるためにも次のような記述を含めることが望ましい。 a) 装置を廃棄または再利用する場合には、内部の記録装置から完全にデータを削除する必要がある。 PC 端末であれば、NSA 標準(米国国防総省 NSA 規格)に準じたデータの消去方法などを採用することが望ましい。 また、専用装置などで容易に内部のデータが消去できない場合は、外部に処分を委託契約すること。

4.2.3. 通信及び運用管理

A.10 通信及び運用管理		
A.10.4 悪意のあるコード及びモバイルコードからの保護 目的：ソフトウェア及び情報の完全性を保護するため。		
番号	管理項目	実施状況
A.10.4.2	モバイルコードに対する管理策	1 A-net のクライアントソフト自身が、Java のアプレットをダウンロードする仕様である、それ以外のモバイルコードに関する明確な手順、文書の記述が見当たらない。 →モバイルコードはセキュリティ違反を誘発しやすいので、利用者への教育を含めた運用面での管理策や技術的な対策を講じる必要がある。A-net 自身がモバイルコード(Java のアプレットなど)を利用する場合は十分な対策が必要である。
A.10.6 ネットワークセキュリティ管理 目的：ネットワークにおける情報の保護，及びネットワークを支える基盤の保護を確実にするため。		
番号	管理項目	実施状況
A.10.6.2	ネットワークサービスのセキュリティ	1 監視に関する記述はあるが、サービスレベルや管理上の要求事項を特定した記述は見当たらない。 →A-net の運用に必要なレベルで要求事項を定義し、サービスレベルを明確にする必要がある。これは回線業者の選定などに使われることを想定している。
A.10.7 媒体の取扱い 目的：資産の認可されていない開示，改ざん，除去又は破壊，及びビジネス活動の中断を防止するため。		
番号	管理項目	実施状況
A.10.7.1	取外し可能な媒体の管理	1 これに相当する記述は見当たらない。 →最近は小型で大容量で安価な USB メモリによる情報の持ち出し事件などが社会的にも取りざたされるため、必要な管理策を定義することが必要である。
A.10.7.2	媒体の処分	1 これに相当する記述は見当たらない。 →コンピュータ類と同じく、通常のフォーマットや消去ではデータが復活され情報が漏洩される恐れがあるため物理的な破壊を含める処分の手順を定義する必要がある。
A.10.8 情報の交換 目的：組織内部で交換した及び外部と交換した，情報及びソフトウェアのセキュリティを維持するため。		
番号	管理項目	実施状況
A.10.8.1	情報交換の方	4 接続手順、形態にて定義されている。

	針及び手順	→現 A-net では問題ないと思われるが、将来的にさまざまな医療機関と情報交換をおこなうためには、HL7, DICOM や MERIT9 などの規格によるデータ変換を考慮する必要がある。
A.10.8.2	情報交換に関する合意	0 A-net では、これに相当するような事象はないと考えるため対象外とする。 →A10.8.1 と同じく、現 A-net では問題ないと思われるが、将来的にさまざまな医療機関と情報交換をおこなうためには、合意の手順を策定する必要がある。
A.10.10 監視 目的:認可されていない情報処理活動を検知するため。		
番号	管理項目	実施状況
A.10.10.6	クロックの同期	1 これに相当する記述は見当たらない。 →実際にはなんらかの手段で運用されていることと想像するが監査証跡や障害発生時の対応などのために時刻の同期の必要性、手順等に関して記述した文書が必要である。

4.2.4. アクセス制御

A.11 アクセス制御		
A.11.3 利用者の責任 目的: 認可されていない利用者のアクセス，並びに情報及び情報処理設備の損傷又は盗難を防止するため。		
番号	管理項目	実施状況
A.11.3.3	クリアデスク・クリアスクリーン方針	1 端末利用の場合、クリアスクリーン ポリシは必要だと考えるが、これに関する記述は見当たらない。 →利用者教育への資料にあるのかも知れないが、A-net としての管理策を策定するべきである。
A.11.4 ネットワークのアクセス制御 目的: ネットワークを利用したサービスへの認可されていないアクセスを防止するため。		
番号	管理項目	実施状況
A.11.4.4	遠隔診断用及び環境設定用ポートの保護	1 これに相当する記述は見当たらない。 →ベンダの運用手順等にあると想像するが、A-net としての管理策を策定するべきである。
A.11.5 オペレーティングシステムのアクセス制御 目的: オペレーティングシステムへの，認可されていないアクセスを防止するため。		
番号	管理項目	実施状況
A.11.5.3	パスワード管理システム	1 対話式であるかどうか、パスワードを確実にする(長さ、文字種指定など)ことに相当する記述は見当たらない。 →利用者教育への資料にあるのかも知れないが、A-net としての管理策を策定するべきである。
A.11.5.4	システムユーティリティの使用	1 これに相当する記述は見当たらない。 →ベンダの保守マニュアル等にこれに相当する記述があるのかも知れないが、A-net としての管理策を明示するべきである。
A.11.5.5	セッションのタイムアウト	1 これに相当する記述は見当たらない。 →利用者教育への資料にあるのかも知れないが、A-net としての管理策を明示するべきである。
A.11.5.6	接続時間の制限	1 これに相当する記述は見当たらない。 →利用者教育への資料にあるのかも知れないが、A-net としての管理策を明示するべきである。

4.2.5. 情報システムの取得，開発及び保守

A.12 情報システムの取得，開発及び保守		
A.12.1 情報システムのセキュリティ要求事項 目的：セキュリティは情報システムの欠くことのできない部分であることを確実にするため。		
番号	管理項目	実施状況
A.12.1.1	セキュリティ要求事項の分析及び仕様化	3　A-net 設置計画当初から、セキュリティ要求の文書化及び仕様化はおこなわれている。ただし、情報セキュリティに関する状況は、ここ数年で激変しており、その変化には対応しきれていない部分がある。 →老朽化した機器の更改時の前には、最新のセキュリティ要求事項を分析し仕様化する必要がある。
A.12.5 開発及びサポートプロセスにおけるセキュリティ 目的：業務用ソフトウェアシステムのソフトウェア及び情報のセキュリティを維持するため。		
番号	管理項目	実施状況
A.12.5.2	オペレーティングシステム変更後の業務用ソフトウェアの技術的レビュー	3　保守運用業務仕様書により定義され、構成情報の管理が実施されているが、これの管理策としては十分ではない。 →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.12.5.3	パッケージソフトウェアの変更に対する制限	3　保守運用業務仕様書により定義され、構成情報の管理が実施されているが、これの管理策としては十分ではない。 →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.12.6 技術的ぜい弱性管理 目的：公開された技術的ぜい弱性の悪用によって生じるリスクを低減するため。		
番号	管理項目	実施状況
A.12.6.1	技術的ぜい弱性の管理	3 管理策としては手順も文書もあるが、A-net のハードウェアやソフトウェアが老朽化してサポート期限が切れているものもあり、新たな脆弱性に対応できない危険性がある。 →可用性や機密性の観点でサポート期限が切れたものは、なるべく早く更改する必要がある。

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。

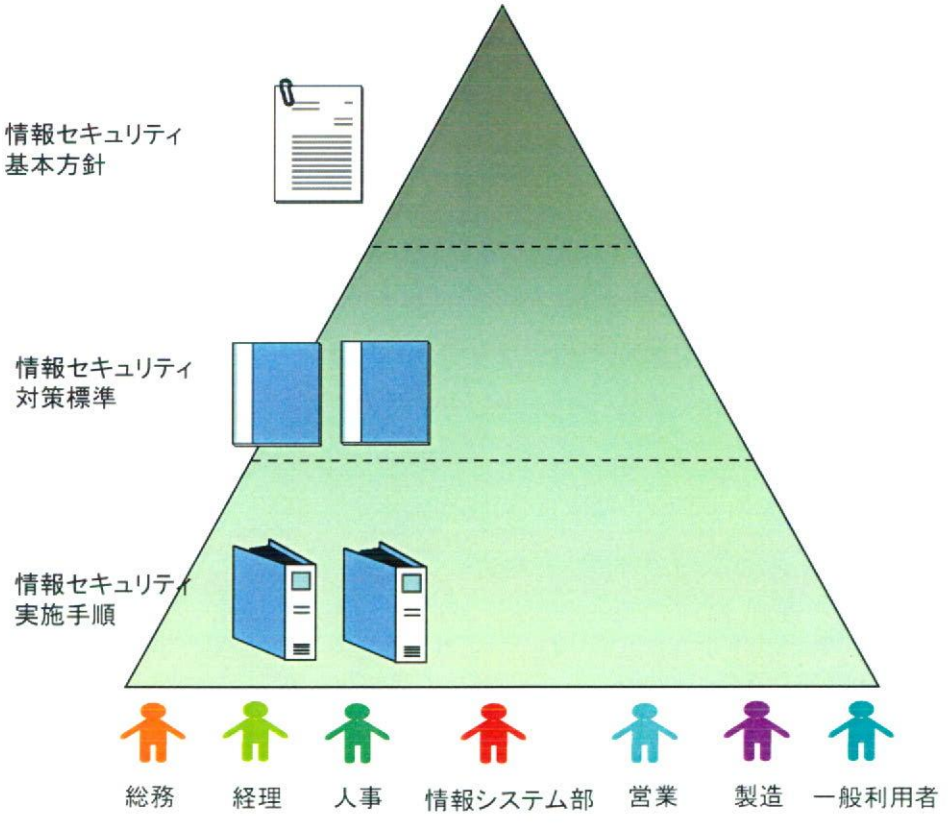


図 5.4.1 情報セキュリティポリシの体系

(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。

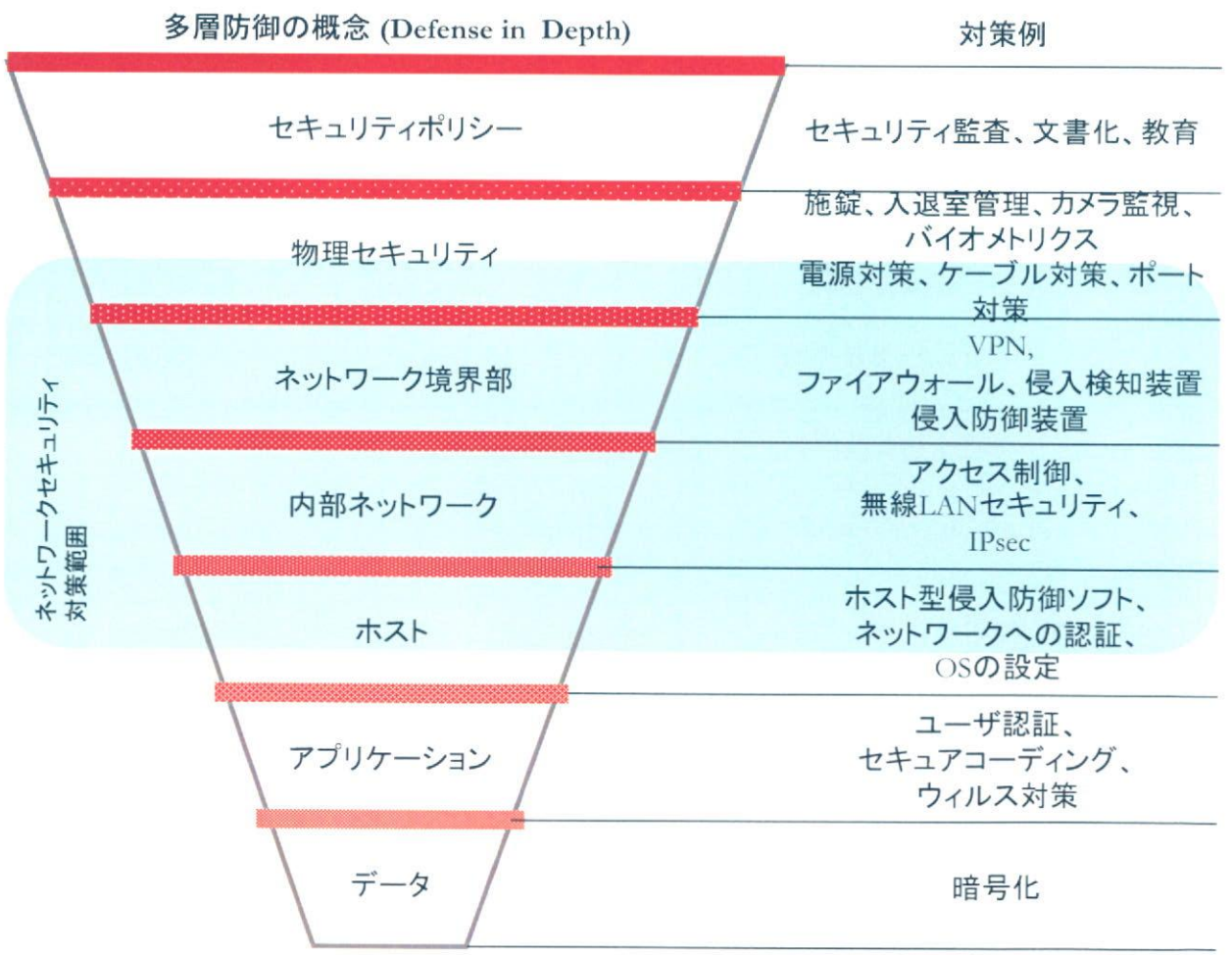


図 5.4.2 多層防御の概念図

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

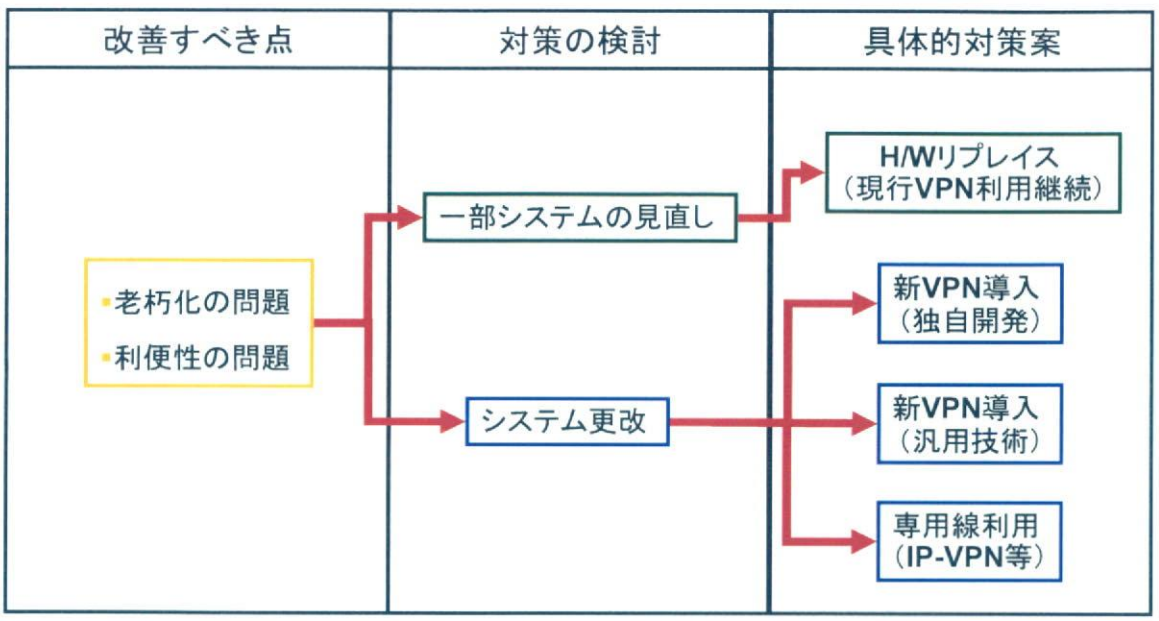
これまでの調査で明らかになった、セキュリティの技術的な問題点に対して最新の技術を実装することによる改善方法を提示する。

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。