3.2. セキュリティ監査の範囲

JIS Q 27001:2006(情報セキュリティマネジメントシステム-要求事項)の付属書Aに記載されている情報セキュリティの管理策は次の 11 分野に分類される。A-5, A-6 などとあるのは、付属書 A の管理番号である。

① セキュリティ基本方針 (A5)

② 組織のセキュリティ (A6)

③ 資産の分類および管理 (A7)

④ 人的セキュリティ (A8)

⑤ 物理的および環境的セキュリティ (A9)

⑥ 通信および運用管理 (A10)

⑦ アクセス制御 (A11)

⑧ 情報システムの取得、開発および保守 (A12)

⑨ 情報セキュリティインシデント管理 (A13)

⑩ 事業継続管理 (A14)

⑪ 順守 (A15)

上記の11分野の中の「情報セキュリティ基本方針」そのものや「組織のセキュリティ」や人の雇用等に関係する「人的セキュリティ」は本セキュリティ監査の範囲外とし、他の分野のネットワーク セキュリティとシステム セキュリティに関連する項目に重点をおいた。すなわち、

- 資産の分類および管理 (A7)
- 物理的および環境的セキュリティ (A9)
- 通信および運用管理 (A10)
- アクセス制御 (A11)
- 情報システムの取得、開発および保守 (A12)
- 情報セキュリティインシデント管理 (A13)
- 事業継続管理 (A14)
- 順守 (A15)

について監査をおこなった。

3.3. 対象システムのセキュリティ標準への準拠状況

A-net試験運用開始時が平成10年(1998年)であったせいか、公開されている資料を閲覧する限り、現在の社会的認知度の高い標準に準拠したセキュリティ技術やセキュリティ管理手法を適用しているわけではないようである。

ただし、厚生省保健医療局国立病院部政策医療課様より、web にて公開されている情報である、「HIV診療支援ネットワークシステム(A－net)について」(http://www1.mhlw.go.jp/topics/a-net/tp0114-1_12.html) を読む限り、「個人情報の保護」、「コンピュータウィルス対策」、「システムの無停止運用」、「大規模災害時の対策」など、情報セキュリティの3要素である、機密性、可用性、完全性に加えて真正性、責任追跡性、信頼性などの考え方を取り入れており当時のセキュリティに対する一般社会の意識から類推すると先進的な考え方を取り入れていると言える。

また、当該webサイトに、そのような記述があるわけではないが、通商産業省(平成10年当時)により制定されていた「情報システム安全対策基準」平成9年9月24日最終改正版の内容は反映されているようである。

3.4. 情報資産

3.4.1. 情報資産の洗い出し

セキュリティ監査をするためには、「何」を「どんな」脅威から守るにあたり、その対策（管理策）の有無を調べ、次にその対策（管理策）が存在した場合でも、その対策内容が必要十分に有効であるか、必要十分に機能しているかどうかを検討しなければならない。このためには、守られるべき情報資産を洗い出して特定する必要がある。

3.4.2. 情報資産区分

A-netの情報資産を大きく分類すると次のようになる。

[情報資産区分]

1. パソコン、サーバ、ネットワーク機器などの物理的な情報資産。
2. パソコン、サーバに保管されるデータやソフトウエアなどの電子的（光学的、磁気的なものも含む）な情報資産。ネットワークに流れるデータも含む。
3. 紙や媒体などに含まれる情報資産。
4. 人的情報資産

本セキュリティ監査では、1.の「物理的な資産」、2.「電子的な情報資産」と3.の「媒体などに含まれる情報資産」も2.の「電子的な情報資産」と便宜上同じ範疇で考える。

3.4.3. A-netが取り扱う物理的な情報資産

A-net のサーバルームに置かれている物理的な情報資産は次のようなものがある。

情報資産の内容	各種サーバ類
	各種クライアント類
	ネットワーク機器
	媒体そのもの
	ケーブル類
	電源関係（2 重化電源、無停電電源装置など）

3.4.4. A-netが取り扱う電子的な情報資産

サーバ内、クライアント内、ネットワーク上に関わらず、次のような電子的な情報資産がある。

情報資産の内容	操作者の情報
	患者情報（氏名、生年月日、保険種類、住所、投薬情報、副作用情報、アレルギー情報など患者個人に付随する情報）
	コンピュータ基本ソフトウェア
	アプリケーションソフトウェア

3.5. 脅威と脆弱性

3.5.1. 脅威の分析

A-net の情報資産に対する脅威(リスク)は、完全性、機密性、可用性の観点で次のものを想定する。

表 3.5.1 脅威の分析

人為的脅威 意図的、計画的脅威	偶発的脅威	環境的脅威
不正侵入	送信エラー(送信先間違い)	地震
ウィルス、ワーム、スパイウェアなど	悪意のあるソフトウェア	火災
悪意のあるソフトウェア	ソフトウェアエラー(バグなど)	ちり、ほこり
成りすまし	要員不足	湿気
盗難	要員のスキル不足	ハードウェアの物理的な故障
ソフトウェアエラー(意図的なバグ)	湿気	ハードウェアのサポートがなくなる
操作ミス	停電	ソフトウェアのサポートがなくなる
湿気	火災	
火災		

3.5.2. 脆弱性の分析

A-net の情報資産に対する脆弱性を検討した。ここで検討した「脆弱性」の定義は、脅威の発生を起因する可能性のある情報資産固有の弱点を想定している。

脆弱性自体は、それだけでは障害とはならないが、脅威を顕在化させ、損害や障害を発生させてしまう可能性がある。

表 3.5.2 脆弱性の分析

脆弱性の分類	脆弱性の例	脅威の例
物理的、環境的	入退室設備の不備	盗難
	電源設備の不備	停電、誤作動
	災害を受けやすい環境（例：地盤、川や海に近いなど）	洪水、地震、台風
ハードウェア	極端な温度、湿度	故障、誤作動
	記憶メディアの不良	故障、情報漏洩
	老朽化	故障、代替部品の入手
ソフトウェア	不完全な仕様	ソフトウェアバグ、誤作動
	アクセス制御が不完全	成りすまし、改ざん、情報漏洩
	パスワードの不備	不正アクセス、改ざん、情報漏洩
	監査証跡（ログ）が取れない	不正アクセス
	バックアップの不備	障害発生時の復旧不能
	ドキュメントの不備	操作ミス
	サポート期間の終了した基本ソフトウェアやアプリケーションソフトウェア	放置されたセキュリティホール、最新の標準との不整合による不具合
通信	保護されていない通信経路	盗聴、情報漏洩
	ケーブル接続、配線の不備	通信傍受、通信不能
	暗号化されていない通信	盗聴、情報漏洩

3.6. 情報資産の評価

洗い出した「情報資産」について、情報資産の価値を評価する場合は、次のような手順になる。

表 3.6.1 情報資産の評価

機密性(Confidentiality)区分	個人情報
	関係者外秘情報（部門外秘情報）
	システム関係の情報
	公開情報
完全性(Integrity)区分	データの誤りや情報の落ちがどのレベルまで許されるか
可用性(Availability)区分	どのくらいシステムが使えなくても耐えられるか

機密性、完全性、可用性の分野で、上記の表の観点でポイント化するが、A-netという重要な「個人情報」を扱う場所での「情報資産」の保護という観点で、公開情報を除き、すべての個人に付随する「情報資産」は最重要「資産」分類として守られるべきものとしてセキュリティ監査をおこなった。

3.7. セキュリティ監査の実施方法

本セキュリティ監査の実施方法であるが、A-netそのものが非常にセキュアなシステムのため、実システムを対象にしたポートスキャンやペネトレーション攻撃をおこなうことによる脆弱性検査をおこなうことができなかった。

また同じ理由でA-netそのものの、詳細なシステム仕様書、設計書、プログラムのソースコードを閲覧することによる精査もできなかった。加えてA-netの実環境におけるサーバやネットワーク機器などの設定情報を閲覧することによる調査ができたわけでもない。

このような背景から、本セキュリティ監査の入力情報は主に次にあげるものである。

表 3.7.1 セキュリティ監査の入力情報

文書関係	HIV診療支援ネットワークシステム(A－net)について 厚生省保健医療局国立病院部政策医療課より、web にて公開 http://www1.mhlw.go.jp/topics/a-net/tp0114-1_12.html (平成 11 年 11 月 8 日 最終更新)
	平成 18 年度 HIV 診療支援ネットワークシステム保守運用業務仕様書 (IBM 様より受理)
	A-net 構成概要図 (IBM様より受理)
	A-net 2006部会用資料 (国立国際医療センターエイズ治療研究開発センター様より受理)
聞き取り調査	医療関係者、A-netシステム開発ベンダ担当者への聞き取り
操作関係	A-netの保守(試験)系システムへの操作見学と実操作

ここに記した情報と日本規格協会発行の、JIS Q 27001:2006 (情報セキュリティマネジメントシステム-要求事項)の附属書A(規定)管理目的及び管理策の項番に沿って可能な限りで助言型のセキュリティ監査をおこなった。

3.8. セキュリティ監査

JIS Q 27001:2006(情報セキュリティマネジメントシステム-要求事項)の付属書 A に従ってセキュリティ監査をおこなった。A-7, A-8 などとあるのは、付属書 A の管理番号である。管理策の全文は著作権法の関係で記載していない。

それぞれの項目について実施状況を下記の区分でコメント記入した。

レベル	判断基準
0	該当しない。範囲外。
1	整備していない。
2	整備している。
3	運用している。
4	継続的に改善している。

3.8.1. 資産の管理

A.7 資産の管理		
A.7.1 資産に対する責任 目的:組織の資産を適切に保護し, 維持するため。		
番号	管理項目	実施状況
A.7.1.1	資産目録	4 A-net のハードウェア資産、ソフトウェア資産は台帳等により目録が作られ管理されている。(保守運用業務仕様書に記載。)
A.7.1.2	資産の管理責任者	4 管理責任者は指定されている。(保守運用業務仕様書に記載。)
A.7.1.3	資産利用の許容範囲	4 A-net のハードウェア資産、ソフトウェア資産およびそれらに含まれる電子的な情報資産は利用範囲について明確に文書化され実施されている。
A.7.2 資産の分類 目的:情報の適切なレベルでの保護を確実にするため。		
番号	管理項目	実施状況
A.7.2.1	分類の指針	4 分類されている。(保守運用業務仕様書に記載。)
A.7.2.2	情報のラベル付け及び取扱い	4 A-net の目的に従い、ハードウェア資産、ソフトウェア資産、電子的な情報資産は型番、シリアル番号などにより分類され管理されている。(保守運用業務仕様書に記載。)

3.8.2. 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.9.1.1	物理的セキュリティ境界	4 サーバ類、ネットワーク機器のある区画(以下、センターと略)は、物理的に保護されている。(保守運用業務仕様書に記載。)
A.9.1.2	物理的入退管理策	4 適切な入退室管理が行われている。(保守運用業務仕様書に記載。)
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。
A.9.1.4	外部及び環境の脅威からの保護	4 センターに関しては、火災、地震対策など環境の脅威からの保護策はある。(聞き取り調査による。)
A.9.1.5	セキュリティを保つべき領域での作業	4 機密管理についての内部教育や機密文書の取り扱い規定などにより担保されていると考える。(保守運用業務仕様書に記載。)
A.9.1.6	一般の人の立寄り場所及び受渡場所	4 センターは物理的に隔離されており、入退室管理策も策定されており問題ないと考える。(保守運用業務仕様書の記載内容より判断。)
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.9.2.1	装置の設置及び保護	4 保護されている。(聞き取り調査による。)
A.9.2.2	サポートユーティリティ	4 保護されている。(聞き取り調査による。)
A.9.2.3	ケーブル配線のセキュリティ	4 保護されている。(聞き取り調査による。)
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。
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。
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。
A.9.2.7	資産の移動	4 ハードウェア資産、ソフトウェア資産の移動に関しては A-net の目的からして範囲外である。電子的な情報資産の研究目的のための持ち出し(二次利用)に関しては別途規則がある。

3.8.3. 通信及び運用管理

A.10 通信及び運用管理		
A.10.1 運用の手順及び責任 目的:情報処理設備の正確，かつ，セキュリティを保った運用を確実にするため。		
番号	管理項目	実施状況
A.10.1.1	運用の手順及び責任	4 操作手順等に関しては、保守運用業務仕様書により定義され、文書化され維持されている。
A.10.1.2	変更管理	4 変更管理は、保守運用業務仕様書により定義され、「変更管理規定」によりシステムの変更は管理されている。
A.10.1.3	職務の分割	4 保守運用業務仕様書により定義され、役割分担及び管理されている。
A.10.1.4	開発施設，試験施設及び運用施設の分離	4 A-net の実運用システムの保守(試験)系のシステムは分離されている。
A.10.2 第三者が提供するサービスの管理 目的:第三者の提供するサービスに関する合意に沿った，情報セキュリティ及びサービスの適切なレベルを実現し，維持するため。		
番号	管理項目	実施状況
A.10.2.1	第三者が提供するサービス	4 一般的な SLA ではないが、サービスの提供内容は文書化され運用されている。(保守運用業務仕様書に記載。)
A.10.2.2	第三者が提供するサービスの監視及びレビュー	4 報告及び記録のレビューは実施されている。(保守運用業務仕様書に記載。)
A.10.2.3	第三者が提供するサービスの変更に対する管理	4 管理されている。(保守運用業務仕様書に記載。)
A.10.3 システムの計画作成及び受入れ 目的: システム故障のリスクを最小限に抑えるため。		
番号	管理項目	実施状況
A.10.3.1	容量・能力の管理	4 保守運用業務仕様書により定義され、「性能管理業務」として実施されている。
A.10.3.2	システムの受入れ	1 これに相当する明確な手順、文書は見当たらない。ただし、その必要がある場合は、保守(試験)系のシステムで実施している。(聞き取り調査による。)

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.10.4.1	悪意のあるコードに対する管理策	1 ウィルス対策の一環として定義されている。
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。
A.10.5 バックアップ 目的：情報及び情報処理設備の完全性及び可用性を維持するため。		
番号	管理項目	監査結果
A.10.5.1	情報のバックアップ	4 データベースのバックアップなど、保守運用業務仕様書により定義され、実施されている。
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.10.6.1	ネットワーク管理策	4 ネットワークに関しては適切に管理されている。（保守運用業務仕様書に記載。）
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.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。
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。
A.10.7.3	情報の取扱手順	4 機密文書の取り扱い規定がある。（保守運用業務仕様書に記載。）
A.10.7.4	システム文書のセキュリティ	4 システム関係の機密文書は保護されている。
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	情報交換の方針及び手順	4 接続手順、形態にて定義されている。

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。
A.10.8.3	配送中の物理的媒体	0 A-net では、これに相当するような事象は恒常的には発生していないと考えるため対象外とする。
A.10.8.4	電子的メッセージ通信	0 利用者教育の中で、メールに関する記述がある。
A.10.8.5	業務用情報システム	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.10.9 電子商取引サービス 目的: 電子商取引サービスのセキュリティ, 及びそれらサービスのセキュリティを保った利用を確実にするため。		
番号	管理項目	実施状況
A.10.9.1	電子商取引	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.10.9.2	オンライン取引	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.10.9.3	公開情報	0 A-net では、電子取引に関わる公開情報はないと考えるため対象外とする。
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.10.10.1	監査ログ取得	4 保守運用業務仕様書により定義され、実施されている。
A.10.10.2	システム使用状況の監視	4 保守運用業務仕様書により定義され、実施されている。
A.10.10.3	ログ情報の保護	4 保守運用業務仕様書により定義され、実施されている。
A.10.10.4	実務管理者及び運用担当者の作業ログ	4 保守運用業務仕様書により定義され、実施されている。
A.10.10.5	障害のログ取得	4 保守運用業務仕様書により定義され、実施されている。
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。

3.8.4. アクセス制御

A.11 アクセス制御		
A.11.1 アクセス制御に対する業務上の要求事項 目的:情報へのアクセスを制御するため。		
番号	管理項目	実施状況
A.11.1.1	アクセス制御方針	4　保守運用業務仕様書により定義され、実施されている。
A.11.1.2	利用者アクセスの管理	4　保守運用業務仕様書により定義され、実施されている。
A.11.2 利用者アクセスの管理 目的:情報システムへの，認可された利用者のアクセスを確実にし，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.11.2.1	利用者登録	4　保守運用業務仕様書により定義され、実施されている。
A.11.2.2	特権管理	4　特権に関する記述は見当たらない。
A.11.2.3	利用者パスワードの管理	4 保守運用業務仕様書により定義され、実施されている。
A.11.2.4	利用者アクセス権のレビュー	4 保守運用業務仕様書により定義され、実施されている。
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.11.3.1	パスワードの利用	4 保守運用業務仕様書により定義され、実施されている。
A.11.3.2	無人状態にある利用者装置	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.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。
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.11.4.1	ネットワークサ	4　保守運用業務仕様書により定義され、実施されている。

	ービスの利用についての方針	
A.11.4.2	外部から接続する利用者の認証	4　保守運用業務仕様書により定義され、実施されている。
A.11.4.3	ネットワークにおける装置の識別	4　利用端末を識別する手順がある。
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。
A.11.4.5	ネットワークの領域分割	4　必要に応じて行われている。
A.11.4.6	ネットワークの接続制御	4　必要に応じて行われている。
A.11.4.7	ネットワークルーティング制御	4　必要に応じて行われている。
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.11.5.1	セキュリティに配慮したログオン手順	4　保守運用業務仕様書により定義され、実施されている。
A.11.5.2	利用者の識別及び認証	4　保守運用業務仕様書により定義され、実施されている。
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。
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。
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。
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。
A.11.6 業務用ソフトウェア及び情報のアクセス制御		

目的：業務用ソフトウェアシステムが保有する情報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.11.6.1	情報へのアクセス制限	4 保守運用業務仕様書により定義され、実施されている。
A.11.6.2	取扱いに慎重を要するシステムの隔離	4 A-net の基幹部分そのものが、取り扱いに慎重を要するシステムであり物理的に隔離されている。

3.8.5. 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。
A.12.2 業務用ソフトウェアでの正確な処理 目的：業務用ソフトウェアにおける情報の誤り，消失，認可されていない変更又は不正使用を防止するため。		
番号	管理項目	実施状況
A.12.2.1	入力データの妥当性	4 実施されている。保守（試験）系のシステムで確認。
A.12.2.2	内部処理の管理	4 実施されている。保守（試験）系のシステムで確認。
A.12.2.3	メッセージの完全性	4 実施されている。保守（試験）系のシステムで確認。
A.12.2.4	出力データの妥当性	4 実施されている。保守（試験）系のシステムで確認。
A.12.3 暗号による管理策 目的： 暗号手段によって，情報の機密性，真正性又は完全性を保護するため。		
番号	管理項目	実施状況
A.12.3.1	暗号による管理策の利用方針	4 リモート接続の際に暗号化通信が使用される場合がある。
A.12.3.2	かぎ（鍵）管理	4 実施されている。
A.12.4 システムファイルのセキュリティ 目的： システムファイルのセキュリティを確実にするため。		
番号	管理項目	実施状況
A.12.4.1	運用ソフトウェアの管理	4 保守運用業務仕様書にこれに相当する記述があるり実施されている。
A.12.4.2	システム試験データの保護	4 実施されている。
A.12.4.3	プログラムソースコードへ	4 実施されている。

	のアクセス制御	
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.12.5.1	変更管理手順	4 保守運用業務仕様書により定義され、「変更管理業務」として実施されている。
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。
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。
A.12.5.4	情報の漏えい	4 実施されている。
A.12.5.5	外部委託によるソフトウェア開発	4 実施されている。
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。

3.8.6. 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.13.1 情報セキュリティの事象及び弱点の報告 目的：情報システムに関連する情報セキュリティの事象及び弱点を，時機を失しない是正処置をとることができるやり方で連絡することを確実にするため。		
番号	管理項目	実施状況
A.13.1.1	情報セキュリティ事象の報告	4　手順が文書化され実施されている。
A.13.1.2	セキュリティ弱点の報告	4　手順が文書化され実施されている。
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.13.2.1	責任及び手順	4　手順が文書化され実施されている。
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。
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。

3.8.7. 事業継続性管理

A-net に関係する運営や活動は、営利目的ではなく、一般的な企業がおこなう事業とは性格を異にするが、本項目では、大規模災害時の運用や可用性についてのみ監査することによる。

A.14 通信及び運用管理		
A.14.1 事業継続管理における情報セキュリティの側面 目的:情報システムの重大な故障又は災害の影響からの事業活動の中断に対処するとともに，それらから重要な業務プロセスを保護し，また，事業活動及び重要な業務プロセスの時機を失しない再開を確実にするため。		
番号	管理項目	実施状況
A.14.1.1	事業継続管理手続への情報セキュリティの組込み	2 縮退運用に関する記述がある。
A.14.1.2	事業継続及びリスクアセスメント	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.14.1.3	情報セキュリティを組み込んだ事業継続計画の策定及び実施	2 代替センター(国立大阪病院)に移す旨の記述がある。
A.14.1.4	事業継続計画策定の枠組み	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.14.1.5	事業継続計画の試験，維持及び再評価	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。