		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。

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。