

目 次

1	はじめに	- 3 -
(1)	背景	- 3 -
(2)	基本的な考え方	- 3 -
	ア 利便性の向上	- 4 -
	イ セキュリティの確保	- 4 -
	ウ 運用管理の向上	- 4 -
(3)	現状の問題点	- 4 -
	ア 技術上の問題点	- 4 -
	イ 運用上の問題点	- 5 -
(4)	問題点の解決に向けて	- 5 -
	ア 利便性の向上	- 6 -
	イ セキュリティの確保	- 6 -
	ウ 運用管理の向上	- 6 -
2	利便性の向上	- 7 -
(1)	市場動向	- 7 -
(2)	対策	- 7 -
	ア インターネット経由での利用	- 7 -
	イ 汎用パソコンでの利用	- 8 -
	ウ リアルタイム処理	- 8 -
	エ 臨床情報の自動収集	- 9 -
	オ 管理する情報	- 10 -
(3)	まとめ	- 10 -
3	セキュリティの向上	- 12 -
(1)	市場動向	- 12 -
(2)	セキュリティ対策の整理	- 12 -
(3)	外部セキュリティ対策の要素	- 19 -
	ア ファイアウォール	- 19 -
	イ IDS/IPS (不正侵入検知システム/不正侵入防御システム)	- 19 -
	ウ ウイルス対策	- 20 -
	エ ネットワーク上での認証	- 21 -
	オ 通信の暗号化	- 21 -
	カ VPN (仮想私設網)	- 22 -
(4)	内部セキュリティ対策の要素	- 23 -
	ア 端末認証	- 23 -

イ ユーザ認証	- 24 -
ウ 検疫	- 24 -
エ アクセス制限	- 25 -
オ 保存データの暗号化	- 25 -
カ 端末へのデータ保存の禁止	- 25 -
キ ログの記録	- 26 -
ク 脆弱性検査	- 26 -
(5) 人的なセキュリティ対策の要素	- 26 -
ア ID 管理	- 26 -
イ パスワード管理	- 27 -
ウ クリアスクリーン	- 27 -
(6) まとめ	- 27 -
4 運用管理の向上	- 29 -
(1) A-net の現状	- 29 -
(2) 運用管理の変貌	- 29 -
(3) 運用管理の要素	- 30 -
ア サービスレベル管理	- 32 -
イ サービスの報告	- 32 -
ウ サービス継続及び可用性の管理	- 32 -
エ 容量・能力管理	- 32 -
オ インシデント管理、問題管理	- 33 -
カ 構成管理	- 33 -
キ 変更管理、リリース管理	- 33 -
(4) サービス提供形態の検討	- 34 -
ア ハードウェアのリース契約	- 35 -
イ iDC (インターネットデータセンター) ハウジング	- 36 -
ウ ASP (アプリケーションサービスプロバイダ)、SaaS (ソース)	- 36 -
エ ASP、SaaS 応用型	- 37 -
(5) まとめ	- 38 -
5 模擬環境での実証実験	- 39 -
(1) 目的	- 39 -
(2) 模擬構成	- 39 -
ア SSL アクセラレータ	- 39 -
イ ファイアウォール	- 39 -
ウ アンチウイルスゲートウェイ	- 40 -
エ 認証サーバ	- 40 -

オ	スイッチングハブ	- 40 -
カ	電子カルテシステム	- 40 -
(3)	検証内容	- 42 -
ア	利便性の向上	- 42 -
イ	セキュリティ対策	- 42 -
(4)	システム概要	- 42 -
ア	SSL VPN	- 43 -
イ	二要素認証	- 43 -
ウ	電子カルテシステムでの認証	- 44 -
(5)	システム利用検証	- 44 -
ア	利便性の向上	- 44 -
イ	セキュリティ対策	- 46 -
(6)	検証結果	- 48 -
ア	考察	- 48 -
イ	課題	- 49 -
6	まとめ	- 51 -

1 はじめに

(1) 背景

『HIV 診療支援ネットワークシステム（以下、「A-net」とする）』は、患者さんのプライバシー保護を図りながら、患者さんの診療情報の一部をエイズ治療・研究開発センター（以下、「ACC」とする）のホストコンピュータに入力し、エイズ治療・研究開発センターとエイズ治療ブロック拠点病院、拠点病院をネットワークで結ぶことにより、患者さんが受診される病院相互で診療情報を共有し、HIV 診療を円滑にし、かつ患者さんの地元で質の高い診療を可能にすることを目的としています。[HIV 診療支援ネットワークシステム（A-net）の説明文書より引用]

しかしながら、A-net は平成 10 年に試験運用を開始したシステムであり、システムを構成するハードウェアやソフトウェアの老朽化に加え、サポート期限の切れたハードウェアやソフトウェアも散見されるようになってきている。このような状況下で、万が一大幅なトラブルが発生した場合には、システムの復旧や継続運用が不可能な状況に陥る可能性も考えられ、大きな問題を抱えている。

また、当時は最新のセキュリティ対策を講じていたものが、年月の経過とともに近年のセキュリティ管理手法とは乖離したものとなりつつあり、更には現在一般的に用いられる汎用技術ではなく、あまり使われなくなった独自技術を採用していることが、今後のシステム改修や継続運用にあたっては大きな障害となっている。

更に、患者の個人情報の取扱いやプライバシー保護をめぐる、強固なセキュリティの確保に努めたため、利便性という観点からみると満足のものではなく、蓄積されたデータ量とその内容からシステムそのものの利用価値も高いとはいえ、アクセス数も伸び悩んでいる状況である。

よって、現在の A-net に代わる次期 A-net の開発に向けて、現状の課題の整理を行うとともに、医師及び患者からも積極的に利用されるシステムの構築を目指して、その解決策や目指すべき方向について検討することとする。

(2) 基本的な考え方

情報システムは、人々の利便性や作業効率を高め、我々の生活の一助となるべき活躍を担うものである。よって、A-net についても、HIV の治療や研究開発に努める医師や患者にとって利便性や研究効率を高め、その成果によって治療負担の軽減や治癒率の向上、更には今後の治療や予防活動全般における研究に役立つことを期待されている。

患者のプライバシー保護は最重要課題ではあるが、高度なセキュリティ対策を施し見栄えの良いシステムを構築したとしても、それが利用されなければ研究への活用度が低くなる。

本研究においては、昨年度実施した、A-net セキュリティ監査の結果を基に記された「A-net セキュリティ監査報告書」で指摘された A-net の現状の問題点や次期 A-net の方向性の助言意見を踏まえ、次期 A-net のシステム開発において重点的に検討が必要と思われる「利便性の向上」、「セキュリティの確保」、「運用管理の向上」について、詳細に検討することとする。

また、A-net 自体の利便性の向上、利用価値の向上について検討するため、机上での検討に加えて、サンプル的な電子カルテシステムとして、株式会社ノーバメディコ製「MyProdoc」を用いた検証環境を構築し、現在の課題に対する対応策について検討する。

ア 利便性の向上

使いやすいシステム、使う価値があるシステムの開発を目指して、具体的な利便性向上策の検討を行う。

イ セキュリティの確保

A-net の最重要課題であるセキュリティの確保について、様々な面から対策内容の検討を行う。

ウ 運用管理の向上

A-net のシステム全体の運用管理方針や効率的な管理のための各種手法の検討を行う。

(3) 現状の問題点

ア 技術上の問題点

昨年度実施した、A-net セキュリティ監査の結果、明らかになった技術上の問題点を【表 1-1】に記す。

【表 1-1 技術上の問題】

項目	現在の問題点
アプリケーションサーバ	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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

	<p>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。</p> <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 Explorer 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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。

イ 運用上の問題点

昨年度実施した、A-net セキュリティ監査の結果、明らかになった運用上の問題点を【表 1-2】に記す。

【表 1-2 運用上の問題】

現在の問題点
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。

(4) 問題点の解決に向けて

現状の問題点を踏まえて、具体的な解決案についてそれぞれのカテゴリ毎に検討する。

ア 利便性の向上

- ・ 場所を選ばず、どこからでも同じような環境で利用できる方法の検討
- ・ 標準の Web ブラウザでアクセスが可能なシステムの検討
- ・ 情報の連携による利便性向上策の検討
- ・ 患者の個人情報など、システムとして管理すべき必要がある情報の精査

イ セキュリティの確保

- ・ 様々なセキュリティ対策について、効率的な適用についての検討
- ・ 最新かつ汎用的な VPN 方式の検討

ウ 運用管理の向上

- ・ 今後の運用として、ハードウェアなどのサポート切れによる影響が少ない運用形態の検討
- ・ 標準技術、汎用技術を採用し、今後永続的に利用できるシステムの検討
- ・ 職員の負担が少ないながらも、システムの現状が把握できる運用管理形態の検討

2 利便性の向上

(1) 市場動向

現在一般に普及している電子カルテシステムは、特定の端末からサーバへアクセスする「クライアント・サーバ型システム」か、端末内部に情報を保持する「スタンドアロン型システム」が大勢を占めている。また、これらは独自の院内ネットワークにのみ接続されており、他の医療機関との情報連携やデータ交換などは積極的に行われていない。

頻繁に新制度の発足や制度変更が行われる医療分野においては、これらの電子カルテシステム自体も最新の医療事情に対応するためには、頻繁に開発や改修を実施し、これを継続的に繰り返す必要があった。そのため、これらの開発や改修に合わせて、サーバだけでなく、利用する端末に対しても必要なソフトウェアの導入や設定変更などの作業が発生する場合もあり、運用負荷が高くなっている。

しかし、現在の情報システムの世界では、各端末に標準で導入されている Web ブラウザを用いてサーバにアクセスする「Web 型システム」が一般的になってきている。我々の身近なところでも、航空機や新幹線のオンライン予約システム、銀行や証券会社のオンラインバンキングやオンライントレードなどが例としてあげられる。

Web 型システムでは、サーバで集中管理を行うため、端末の新規導入やシステムの仕様変更のために、複雑な再構築や設定などの展開作業を必要としない。

また、様々なセキュリティ技術と併用することによって、インターネットに接続された世界中のどの端末からでも、セキュリティに配慮しながら、システムへのアクセスが実現している。

更には、一つのシステムで更新した情報が他のシステムにまで連携して反映されるなど、情報連携によって飛躍的に利便性が向上し、システムの利用範囲が拡大している。

これらの現状を踏まえて、より使い勝手が良く、医師の負荷を軽減するようなシステム、患者にも積極的に利用してもらえそうなシステムの方向性を検討する。

(2) 対策

ア インターネット経由での利用

現在のシステムでは、アクセスできる環境に限られる（ACC や拠点病院などの限られた場所でのみしか利用ができない）という制約がある。セキュリティを考慮すると、A-net 稼働当時としては的を射た方法であったと推測されるが、インターネットや様々なセキュリティ技術が普及した現在においては、利用者にとって不便なシステムになっていると言わざるを得ない。

これらを解消するために、インターネット経由で、どこからでもどのパソコンからでも利用が出来るような環境作りが必要であるといえる。これにより、場所と時間を選ばずにシステムにアクセスできるため、利便性そのものは飛躍的に高まると期待できる。

しかしながら、インターネットは全世界とつながる公の場である。患者の情報など秘匿性の高いものを取り扱う本システムにおいては、様々な脅威に対する十分なセキュリティ対策を施す必要がある。必要と考えられるセキュリティ対策については、別項にて検討する。

イ 汎用パソコンでの利用

現在のシステムでは、専用のソフトウェア（Netscape Communicator）がインストールされた端末でしか利用できないなどの問題点がある。また、現在ではあまり利用されていないため、操作性の問題が指摘され、また A-net の開発や改修に対する障害の一因にもなっている。

しかし、現在では、一般的な Windows OS に代表されるパソコンが各家庭に普及してきており、街中にはインターネットカフェをはじめとして手軽にインターネットを利用できる環境が整備されてきている。

このような状況下で、特定の端末からの利用に限定することは、セキュリティ対策としては有効に機能するものの、それらのソフトウェアの配布などに係る手間と費用が発生し、効率的ではなく、また利便性を損なっている。

よって、一般家庭に広く普及しているパソコンから簡単に利用できるシステム、利用料が発生せず、かつ長期的なサポートが受けられるソフトウェアで利用できるシステムなどを開発する必要がある。

現在では、オンライン予約やインターネットバンキングをはじめとする様々なシステムにおいて、Windows OS 標準の Web ブラウザ（Internet Explorer）などの利用を想定したシステムが数多く開発・提供されており、次期システムにおいては一般に広く普及している Web ブラウザなどの利用を想定したシステム開発を検討するべきである。

ウ リアルタイム処理

ホストを利用した旧来のシステムなどは、日中時間帯において利用者に対してサービスを提供し、夜間に『バッチ処理（又は、「一括処理」とも言う）』を実施して、更新されたデータの集計や反映及びデータ転送などを行うシステムが主流であった。

しかし、最近では利用者が入力した時点で直ちに情報が反映され（「リアルタイム処理」と言う）、また必要な複数のサーバ等に対してそのデータが転送されるような仕組みが一般的である。

次期システムにおいては、リアルタイム処理を前提として、常に最新の情報に触れることができるようなシステムを検討する必要がある。

また、リアルタイム処理を検討する上では、データ容量が大きくなる動画や画像データの取扱いについても慎重に検討し、必要最低限のサーバにのみ保持する仕組み作りや、必要時にのみ取り出すような仕組みを検討する必要がある。

エ 臨床情報の自動収集

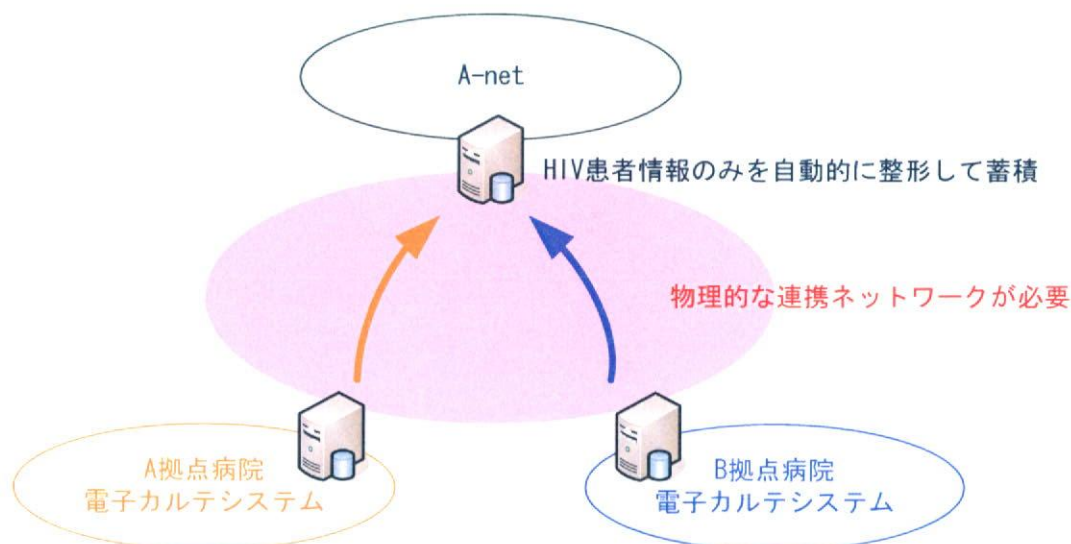
現在の A-net では、患者が来院（又は、受診）した際の診療情報や臨床情報などは、主に ACC や各拠点病院など（以下、「各拠点病院」とする）の独自の電子カルテシステムなどを用いて管理されている。それらの情報の中から、HIV 患者の必要情報だけを抽出し A-net に反映させる仕組みが十分に講じられておらず、医師による手入力が必要となっている。

このように A-net へのデータ入力の手間がかかるため、データ蓄積が円滑に進まず利用する価値が低くなり、よって手間を惜しんでデータ入力を行わなくなるという悪循環に陥っている。

次期システムにおいては、電子カルテシステムなどから該当する患者の診療情報や臨床情報などを自動的に抽出し、A-net 側のデータベースに反映する仕組みが欠かせない。

現在、データフォーマットに関する標準仕様が定められていないため、複数の電子カルテシステム間において、データ互換性の問題が発生する。これらのデータフォーマットの標準化や、どのメーカー製の電子カルテシステムを利用していても、A-net に情報を反映できる仕組みを検討する必要がある。

更に、各拠点病院独自の電子カルテシステムは、セキュリティの観点からも閉ざされた院内ネットワークにのみ接続されており、他の医療機関やインターネットへの接続を行っていないケースが多く、自動でのデータ連携には課題がある。そこで、各拠点病院間を閉域に接続する新ネットワークの構築や、そのネットワークと各拠点病院独自の電子カルテシステムとの接続についても検討する必要がある。しかしながら、これには各拠点病院内のセキュリティポリシーやネットワーク構成の変更を伴う場合もあるため、各拠点病院を巻き込み、早急に検討する必要がある。



【図 2-1 A-net と電子カルテシステムとの情報連携イメージ】

オ 管理する情報

現在は、個人情報保護法や各種ガイドラインなどによると、臨床研究への活用が目的であったとしても、原則として患者の同意の上で個人情報を管理する必要がある。この臨床研究における患者に対するインフォームド・コンセント（臨床研究の意義、目的、実施方法、個人情報保護の方法などの説明や同意の確認などの行為）が不十分であったりするため、提供される情報が少なく、利用者が低迷する要因ともなっている。

個人を特定できない情報の利用にあたっては、個人情報保護法の適用を受けないが、生年月日や性別、血液型などを組み合わせると個人を特定される場合も考えられるため、同法の適用除外に該当する可能性は極めて低いと言える。

そこで、臨床目的に限り、患者を容易に特定可能な個人情報（例えば、氏名、住所、電話番号など）を用いない場合に限っては、個人情報保護法の適用除外とするなど、関連機関との調整を行い、一定のルールに従って柔軟に利用できるように検討するべきである。

また、患者団体の代表者と研究責任者が代表で同意文書を交わすなど、今までの概念だけに囚われずに代替的な対応策を検討することが重要である。

更に別の手段としては、各拠点病院での初診時に、カルテ作成に係る個人情報の提供を依頼する際に、これらの個人情報について臨床目的にも利用することを明記（利用目的や、その範囲、苦情申出先などを周知）し、予め同意を得ておく方法などを広く模索する必要がある。

これらは現行法令やガイドラインだけでは対応できないケースも想定されることから、関連省庁を巻き込んだ対策が不可欠である。

一方、患者本人に対するデータ提供については、患者本人の過去の受信履歴や検査結果が一目で確認できることや、それらの詳細なデータの提供が求められる。また、同じような症状を持つ他の患者の状況を集約された統計データや臨床情報などとして、分析して分かりやすく加工したデータの提供が望まれる。

医師に対するデータ提供においても、通常の医療機関による外来・入院患者に対して管理する情報とは異なる情報の管理が必要である。膨大な不要な情報に埋もれて、目的の情報が即座に取り出せないのでは、本来の目的を達しているとはいえないため、A-net の本来の目的に立ち返り、必要最低限でかつ有益な情報を管理し利用できるように、そのデータの管理範囲をもう一度確認し、見直す必要がある。

今後のシステム開発においては、厳重に管理すべき必要がある情報の種類や、その重要度、利用範囲、開示区分なども合わせて検討する必要がある。

(3) まとめ

A-net の利便性を向上させるため、このようにいくつかの施策が考えられるが、現状の A-net の環境と比較するとセキュリティレベルを落とさざるを得ない事項、他の拠点病院を巻き込んで検討する必要のある事項、また、関係省庁などを含めて慎重に検討する必要がある事項などに分類される。

システム開発や改修などが伴う技術的な対策については、現行の A-net のシステム改修が困難なことから、次期 A-net の開発までの実現は期待できないが、他の調整事項についてはいち早く検討を進める必要がある。

これらの諸施策の実施によって、利便性の向上、利用価値の向上が図られ、A-net そのものの存在意義が高まることを期待する。

3 セキュリティの向上

(1) 市場動向

近年、情報セキュリティへの意識の高まりを受けて、多くの民間企業や中央省庁、及び各種団体において、情報資産を保護するためのセキュリティ対策が実施されている。

特にインターネットなどの外部ネットワークとの接続点においては、強固なファイアウォールを設け、不正アクセス、DoS 攻撃（又はサービス妨害）及びクラッキングなどの外部からの脅威に対する対策を積極的に講じている。

一方で、近年では自宅などから持ち込んだ私有パソコンによるウイルスの蔓延や、Winny に代表される P2P ソフトによる情報漏洩など、内部の要因による事故や事件が全体の 7 割以上を占めると言われるようになってきた。

これらに対処するために、内部ネットワークで利用者や使用する端末の認証を行うことで許可された利用者や端末に対してのみ、ネットワークやシステムの利用を許可するといった認証システムが注目を集めており、利用者の認証によるネットワークアクセス権限の制御や、端末へのパッチの適用状況などの環境をチェックし、一定のセキュリティレベルに達した端末のみを内部システムにアクセスできるようにする検疫システムなどの技術が、多くのメーカーから提供されている。

また、技術的に強固なセキュリティ対策を施したとしても、それを利用する利用者の意識が低ければ、セキュリティ事故を完全に防止することはできない。よって、利用者に対する教育や注意喚起にはじまり、最低限順守すべき ID やパスワードの管理などの対策事項を明確にし、順守させる必要がある。

このような、インターネットなどの外部からの通信に対する外部セキュリティ対策、院内やサーバ設置箇所などイントラネット内部通信に対する内部セキュリティ対策、利用者に対する教育などを含む人的なセキュリティ対策などの要素を組み合わせ、多層的にセキュリティ対策を実施することで、大きなセキュリティ事故を防止する必要がある。

本項では、これらの外部からの脅威に対する対策方法、認証などの内部アクセス制御の技術、及び包括的なセキュリティ対策の主な実現方式や課題点、適用条件の検討を行う。

(2) セキュリティ対策の整理

A-net におけるセキュリティ対策について、まず、昨年度の A-net セキュリティ監査でも評価基準に用いた ISMS (Information Security Management Systems) の認証基準である「JIS Q 27001」の各項目に基づいて、主に誰が、どの装置がその対策の対象となるのかを【表 3-1】で整理する。

各項目は、「JIS Q 27001」の附属書 A「管理目的及び管理策」に準じる。

なお、対象となる○や△が記載のない項目については、各拠点病院を統括する組織管理

者やセキュリティマネジメントシステムの管理者が対象となるものであり、△と記載のあるものは、それらの管理者の方針に基づいて実際に実施を担当する事項などを示す。

【表 3-1 JIS Q 27001 に基づくセキュリティ対策の対象】

項番	項目	対象者			対象装置			
		システム運用管理者	利用者(医師)	利用者(患者)	ネットワーク	サーバ	院内の端末	自宅などの端末
A. 5	セキュリティ基本方針							
A. 5. 1	情報セキュリティ基本方針							
A. 5. 1. 1	情報セキュリティ基本方針文書	△	△	△				
A. 5. 1. 2	情報セキュリティ基本方針のレビュー							
A. 6	情報セキュリティのための組織							
A. 6. 1	内部組織							
A. 6. 1. 1	情報セキュリティに対する経営陣の責任							
A. 6. 1. 2	情報セキュリティの調整	△	△	△				
A. 6. 1. 3	情報セキュリティ責任の割当て							
A. 6. 1. 4	情報処理設備の認可プロセス	○						
A. 6. 1. 5	秘密保持契約	○						
A. 6. 1. 6	関係当局との連絡							
A. 6. 1. 7	専門組織との連絡							
A. 6. 1. 8	情報セキュリティの独立したレビュー							
A. 6. 2	外部組織							
A. 6. 2. 1	外部組織に関係したリスクの識別	○						
A. 6. 2. 2	顧客対応におけるセキュリティ	○						
A. 6. 2. 3	第三者との契約におけるセキュリティ	○		○				
A. 7	資産の管理							

A. 7. 1	資産に対する責任								
A. 7. 1. 1	資産目録	○	○						
A. 7. 1. 2	資産の管理責任者	○	○						
A. 7. 1. 3	資産利用の許容範囲								
A. 7. 2	情報の分類目的								
A. 7. 2. 1	分類の指針	○							
A. 7. 2. 2	情報のラベル付け及び取扱い	○							
A. 8	人的資源のセキュリティ								
A. 8. 1	雇用前								
A. 8. 1. 1	役割及び責任								
A. 8. 1. 2	選考								
A. 8. 1. 3	雇用条件	○	○	△					
A. 8. 2	雇用期間中								
A. 8. 2. 1	経営陣の責任								
A. 8. 2. 2	情報セキュリティの意識向上, 教育 及び訓練	○	○	△					
A. 8. 2. 3	懲戒手続								
A. 8. 3	雇用の終了又は変更								
A. 8. 3. 1	雇用の終了又は変更に関する責任								
A. 8. 3. 2	資産の返却	○	○	○					
A. 8. 3. 3	アクセス権の削除	○							
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								
A. 9. 1. 1	物理的セキュリティ境界								
A. 9. 1. 2	物理的入退管理策								
A. 9. 1. 3	オフィス, 部屋及び施設のセキュリ ティ								
A. 9. 1. 4	外部及び環境の脅威からの保護								
A. 9. 1. 5	セキュリティを保つべき領域での作 業								
A. 9. 1. 6	一般の人の立寄り場所及び受渡場所								
A. 9. 2	装置のセキュリティ								
A. 9. 2. 1	装置の設置及び保護	○	○			○	○		
A. 9. 2. 2	サポートユーティリティ	○				○	○		
A. 9. 2. 3	ケーブル配線のセキュリティ	○	○		○				
A. 9. 2. 4	装置の保守	○	○		○	○	○		
A. 9. 2. 5	構外にある装置のセキュリティ	○	○	○		○	○	○	

A. 9. 2. 6	装置の安全な処分又は再利用	○	○	○		○	○	○
A. 9. 2. 7	資産の移動	○	○			○	○	
A. 10	通信及び運用管理							
A. 10. 1	運用の手順及び責任							
A. 10. 1. 1	操作手順書	○						
A. 10. 1. 2	変更管理	○						
A. 10. 1. 3	職務の分割	○						
A. 10. 1. 4	開発施設, 試験施設及び運用施設の分離							
A. 10. 2	第三者が提供するサービス							
A. 10. 2. 1	第三者が提供するサービス	○						
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	○						
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	○						
A. 10. 3	システムの計画作成及び受入れ							
A. 10. 3. 1	容量・能力の管理	○						
A. 10. 3. 2	システムの受入れ	○						
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							
A. 10. 4. 1	悪意のあるコードに対する管理策	○	△	△		○	○	○
A. 10. 4. 2	モバイルコードに対する管理策	○	△	△		○	○	○
A. 10. 5	バックアップ							
A. 10. 5. 1	情報のバックアップ	○				○	○	
A. 10. 6	ネットワークセキュリティ管理							
A. 10. 6. 1	ネットワーク管理策	○				○		
A. 10. 6. 2	ネットワークサービスのセキュリティ	○				○		
A. 10. 7	媒体の取扱い							
A. 10. 7. 1	取外し可能な媒体の管理	○	○	○				
A. 10. 7. 2	媒体の処分	○	○	○		○	○	○
A. 10. 7. 3	情報の取扱手順	○	○			○	△	△
A. 10. 7. 4	システム文書のセキュリティ	○						
A. 10. 8	情報の交換							
A. 10. 8. 1	情報交換の方針及び手順	○				○	○	
A. 10. 8. 2	情報交換に関する合意							
A. 10. 8. 3	配送中の物理的媒体	○	○	○				
A. 10. 8. 4	電子的メッセージ通信	○	○	○		○	○	○

A. 10. 8. 5	業務用情報システム	○	○	○	○	○	○	
A. 10. 9	電子商取引サービス							
A. 10. 9. 1	電子商取引	○	○	○	○	○	○	○
A. 10. 9. 2	オンライン取引	○	○	○	○	○	○	○
A. 10. 9. 3	公開情報	○				○		
A. 10. 10	監視							
A. 10. 10. 1	監査ログ取得	○			○	○	△	△
A. 10. 10. 2	システム使用状況の監視	○			○	○	△	
A. 10. 10. 3	ログ情報の保護	○			○	○		
A. 10. 10. 4	実務管理者及び運用担当者の作業ログ	○			○	○		
A. 10. 10. 5	障害のログ取得	○			○	○	△	
A. 10. 10. 6	クロックの同期	○	○	○	○	○	△	△
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							
A. 11. 1. 1	アクセス制御方針							
A. 11. 2	利用者アクセスの管理							
A. 11. 2. 1	利用者登録	○				○		
A. 11. 2. 2	特権管理	○			○	○		
A. 11. 2. 3	利用者パスワードの管理	○	○	○	○	○	○	○
A. 11. 2. 4	利用者アクセス権のレビュー	○			○	○		
A. 11. 3	利用者アクセスの管理							
A. 11. 3. 1	パスワードの利用	△	△	△	○	○	○	○
A. 11. 3. 2	無人状態にある利用者装置	○	○	○		○	○	○
A. 11. 3. 3	クリアデスク・クリアスクリーン方針	○	○	○		○	○	○
A. 11. 4	ネットワークのアクセス制御							
A. 11. 4. 1	ネットワークサ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	○	○	○	○	○		
A. 11. 4. 3	ネットワークにおける装置の識別	○	○	○	○	○	○	○
A. 11. 4. 4	遠隔診断用及び環境設定用ポートの保護	○			○	○		
A. 11. 4. 5	ネットワークの領域分割	○			○			
A. 11. 4. 6	ネットワークの接続制御	○			○			
A. 11. 4. 7	ネットワークルーティング制御	○			○			
A. 11. 5	オペレーティングシステムのアクセス制御							

A. 11. 5. 1	セキュリティに配慮したログオン手順	○	○	○	○	○	○	○
A. 11. 5. 2	利用者の識別及び認証	○	○	○		○	○	○
A. 11. 5. 3	パスワード管理システム	○	○	○		○	○	○
A. 11. 5. 4	システムユーティリティの使用	○	○	○		○	○	○
A. 11. 5. 5	セッションのタイムアウト	○	△	△	○	○		
A. 11. 5. 6	接続時間の制限	○	△	△	○	○		
A. 11. 6	業務用ソフトウェア及び情報のアクセス制御							
A. 11. 6. 1	情報へのアクセス制限	○	○	○	○	○		
A. 11. 6. 2	取扱いに慎重を要するシステムの隔離	○	○		○	○	○	
A. 11. 7	モバイルコンピューティング及びテレワーキング							
A. 11. 7. 1	モバイルのコンピューティング及び通信	○	○	○	○		○	○
A. 11. 7. 2	テレワーキング	△	△	△	○		○	○
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							
A. 12. 1. 1	セキュリティ要求事項の分析及び仕様化	○						
A. 12. 2	業務用ソフトウェアでの正確な処理							
A. 12. 2. 1	入力データの妥当性確認	○				○		
A. 12. 2. 2	内部処理の管理	○				○		
A. 12. 2. 3	メッセージの完全性	○				○	△	△
A. 12. 2. 4	出力データの妥当性確認	○				○	△	△
A. 12. 3	暗号による管理策							
A. 12. 3. 1	暗号による管理策の利用方針	△	△	△		○	○	○
A. 12. 3. 2	かぎ（鍵）管理					○	△	△
A. 12. 4	システムファイルのセキュリティ							
A. 12. 4. 1	運用ソフトウェアの管理	○	△	△		○	△	△
A. 12. 4. 2	システム試験データの保護	○						
A. 12. 4. 3	プログラムソースコードへのアクセス制御	○				○		
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							
A. 12. 5. 1	変更管理手順	○				○		
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	○	○	○	○	○	○	○

A. 12. 5. 3	パッケージソフトウェアの変更に対する制限	○	○	○		○	○	○
A. 12. 5. 4	情報の漏えい	○			○	○		
A. 12. 5. 5	外部委託によるソフトウェア開発							
A. 12. 6	技術的ぜい弱性管理							
A. 12. 6. 1	技術的ぜい弱性の管理	○	○	○	○	○	○	○
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							
A. 13. 1. 1	情報セキュリティ事象の報告	○	○	○				
A. 13. 1. 2	セキュリティ弱点の報告	○	○	○				
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							
A. 13. 2. 1	責任及び手順							
A. 13. 2. 2	情報セキュリティインシデントからの学習							
A. 13. 2. 3	証拠の収集							
A. 14	事業継続管理							
A. 14. 1	事業継続管理における情報セキュリティの側面							
A. 14. 1. 1	事業継続管理手続への情報セキュリティの組み込み							
A. 14. 1. 2	事業継続及びリスクアセスメント							
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	△						
A. 14. 1. 4	事業継続計画策定の枠組み							
A. 14. 1. 5	事業継続計画の試験, 維持及び再評価	○						
A. 15	順守							
A. 15. 1	法的要求事項の順守							
A. 15. 1. 1	適用法令の識別							
A. 15. 1. 2	知的財産権 (IPR)							
A. 15. 1. 3	組織の記録の保護						△	
A. 15. 1. 4	個人データ及び個人情報の保護						○	
A. 15. 1. 5	情報処理施設の誤用防止							
A. 15. 1. 6	暗号化機能に対する規則							
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							
A. 15. 2. 1	セキュリティ方針及び標準の順守							
A. 15. 2. 2	技術的順守の点検	○			○	○	○	
A. 15. 3	情報システムの監査に対する考慮事項							