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							

A. 15. 3. 1	情報システムの監査に対する管理策							
A. 15. 3. 2	情報システムの監査ツールの保護	△						

(3)　外部セキュリティ対策の要素

インターネットやHOSPnetといった、A-netからみると外部のネットワークからの脅威に対応するため、内部ネットワークとの接続境界において実装を検討するべきセキュリティ対策についてまとめる。

また、利便性を高めるために、インターネットやHOSPnetを経由した医師及び患者からのA-netへのアクセスを考慮し、外部ネットワーク上でのデータ通信の安全性確保についても検討する。

ア　ファイアウォール

ファイアウォールは、外部に公開されるネットワークと組織内部のネットワークとを分離する役割を果たす。

一定のルールに沿って、組織内部のネットワークに対して外部から侵入されることを防ぎ、内部ネットワークからの情報漏洩も一定レベルで防止する効果がある。

一般的には、ネットワークのレイヤ3（ネットワーク層）情報やレイヤ4（トランスポート層）情報である宛先や送信元のIPアドレスやポート番号などを監視し、予め設定された条件に適合するとその通信を許可又は拒否する仕組みである。これは「パケットフィルタ型」や「ステートフルインスペクション型」と呼ばれ、仕組みが単純なため高速に動作可能となる。

しかし、予め設定されたIPアドレスやポート番号であればその通信を許可するため、不正なアクセスを防ぎきれない場合がある。

一方で、レイヤ7（アプリケーション層）情報のHTTPやFTPなどのアプリケーションプロトコルのレベルで通信を制御する方式を「アプリケーションゲートウェイ型」と呼ぶ。アプリケーションゲートウェイは、一般的にはProxy（又は中継）サーバと同じで、一旦通信のセッションを分断し代替して通信を行う。セッションを分断した際に、RFCで規定されている標準プロトコルフォーマットに従っているか、許可されたアプリケーションの正しい動作かなどを確認するため、前者に比べて安全性は高まる。

しかし、パケットを書き換える必要があるため、高速なネットワーク環境で利用すると処理に時間がかかるなどの欠点がある。

イ　IDS/IPS（不正侵入検知システム／不正侵入防御システム）

IDSは侵入検知システムと呼ばれ、ファイアウォールでは制御しきれなかった外部ネッ

トワークからの攻撃や不正アクセスを検知する役割を果たす。

一方の IPS は、侵入防御システムと呼ばれ、IDS と同様に攻撃や不正アクセスを検知し、更に検知したその通信を拒否（破棄）する仕組みを備えている。

一般的に、IDS/IPS にはネットワーク型とホスト型の二つの仕組みがあり、ネットワーク型は、外部ネットワークとの境界付近に設置され、ネットワークセグメントを流れる全てのトラヒックを収集しそのデータを解析する。不正な通信を検知した場合には、管理者に通知（IDS の動作）し、また、その通信の破棄（IPS の動作）を行う。

しかし、不正な通信を検知した段階では、既に当該通信は終了し攻撃や侵入が完了している場合もあり、完全な侵入防御を果たすことはできない。

一方、ホスト型は、端末にソフトウェアをインストールし、端末自身に対する攻撃を検知する。検知方法は各社の実装において様々であるが、定義ファイルに頼らないアノマリー検知（特定パターンにマッチしなくても異常を検知する方法）や DDoS 攻撃に対応した製品も登場しており、ファイアウォールなどと併用することによって強固なネットワーク環境を構築することが可能となる。

しかし、ホスト型は端末に予めソフトウェアをインストールする必要があるため、ライセンス費用が高価となることや、特に個人として利用する患者などにとっては負荷となるため、導入には慎重な検討を要する。

ウ　ウイルス対策

コンピュータウイルスはコンピュータに被害をもたらす不正なプログラムの一種であり、最もよく知られたセキュリティ上の脅威である。

Web サイトの閲覧だけでなく、メール、ソフトウェアのマクロ、外部記憶媒体、及び P2P ソフトなどを通じて感染することがあり、コンピュータの誤作動やファイルの削除、他のコンピュータへの攻撃や感染活用、更には利用者が気付かない間にコンピュータに保存された情報を盗み出すような情報漏洩にまで発展する可能性がある。

A-net をインターネット経由で接続することを想定すると、ウイルス対策に関心のない患者や、IT リテラシーの低い患者、更には意図的なウイルスを拡散しようとする悪意のある者の前に晒されることとなる。これらの脅威を排除するために、個人に頼らずにウイルスによる脅威を排除するための仕組みづくりが必要となる。

これらを実現するためには、ゲートウェイ型のウイルス対策装置によって、流れる全てのデータを収集し、ウイルスに感染していないかの確認を行うと効果的である。しかし、全てのデータの収集によって、ある程度パフォーマンスが劣化することと、暗号化やパスワードで保護されたデータに対しては基本的には無効であるため、導入する際にはその役割を明確にし、設置場所にも配慮する必要がある。

また、A-net 内部を考えた場合でも利用者任せのコンピュータウイルス対策では脅威を完全に払拭することが困難となってきており、自動的に全ての端末で定期的なウイルス検査や定義ファイルのアップデートを実施するような機能を実装したウイルス対策機器を

導入することが求められる。

エ　ネットワーク上での認証

公開 Web サーバのような、不特定多数の者のアクセスを許可するサービスとは異なり、A-net は限られた医師や患者のみにアクセスを限定するべきシステムである。

このようなセキュアなシステムにおいては、通常の外部ネットワークとの境界において、アクセスを許可するべき利用者を認証し、不正な利用者によるアクセスを排除する仕組みを講じなければならない。

ネットワーク上での利用者認証の仕組みとしては、VPN 技術として通信の暗号化などとともに技術が確立しているため、VPN の項で詳述する。

オ　通信の暗号化

インターネットや HOSPnet などの外部のネットワークを通じてデータ通信を行う際に、通信途中で第三者にデータを盗み見られたり改ざんされたりしないように、データを暗号化し、通信を行う必要がある。

送信元では平文を暗号文にデータ変換（暗号化）して送信し、受信側では暗号文を平文にデータ変換（復号化）する操作を行う。このデータ変換に係る一定のルール（暗号アルゴリズム）と、暗号及び復号に使用する鍵が必要になる。

暗号の方式は、暗号化に用いる暗号鍵と復号化に用いる復号鍵で同じ鍵を利用する方式である共通鍵暗号方式（秘密鍵暗号方式）と、一対になった異なる鍵を利用し一方の鍵を公開する方式である公開鍵暗号方式に大別される。

【表 3-2】に共通鍵暗号方式と公開鍵暗号方式の特徴を比較する。

【表 3-2　共通鍵暗号方式と公開鍵暗号方式の比較】

	共通鍵暗号方式	公開鍵暗号方式
暗号鍵／復号鍵	共通	異なる
鍵の公開	公開しない（秘密）	一方を公開する
鍵の受渡し	必要	不要
処理速度	高速	低速
主な用途	認証	デジタル署名 片方向認証
主な暗号アルゴリズム	DES、3DES IDEA RC5	RSA ElGamal 楕円曲線暗号

このように、共通鍵暗号方式は処理速度も比較的速く認証用途に適した暗号方式である

が、秘密鍵の受渡しに大きな問題がある。一方で、公開鍵暗号方式は相手へ容易に鍵を受け渡すことができる暗号方式であるが、処理速度が遅いなどの問題がある。

これらを上手く組み合わせたハイブリッド方式と呼ばれる暗号方式などによって、安全で高速に処理される鍵交換の仕組みなどが実現されている。

ネットワーク上での通信の暗号化の仕組みとしては、VPN技術としてネットワーク上での認証などとともに技術が確立しているため、VPNの項で詳述する。

カ　VPN（仮想私設網）

インターネットのような公のネットワーク上で、セキュアなデータ通信を行う場合には、認証・暗号化・カプセル化などの技術によって、仮想的にプライベートなネットワークであるVPNを構築することによって、安全にデータのやりとりが可能となる。

VPNは、利用者の認証や通信の暗号化、データ改ざんの検出などを行っており安全性の高い技術である。

VPNの技術には様々なものが確立されているが、一般に広く普及しているIPsecとSSLについて【表3-3】で検討する。

【表3-3　IPsecとSSLの比較】

	IPsec	SSL
動作する階層	ネットワーク層	トランスポート層以上
必要なソフトウェア	IPsec 用クライアントソフトウェア	一般的なWebブラウザ（Windows OS標準搭載のもので可能）
ソフトウェアのインストール	事前にインストールや設定が必要	不要（クライアントレス）
対応するアプリケーション	IP で通信する全てのアプリケーション	主に、Webブラウザを用いて通信するもの ・Web ・FTP ・Webメール　など
アクセス制御	IP アドレスやユーザ毎に制御を行う	IPアドレスなどに依存せず、ユーザ毎に利用できるアプリケーションを限定するなど柔軟な制御が可能
制約	IP レベルでの技術のため、ファイアウォールや NAT の影響を受ける	一般に、Webブラウザを用いて通信しないメールや専用システムなどは利用できない

主な用途	・拠点間通信 ・特定のパソコンからの通信	インターネット上のパソコンからの通信

このように、IPSec VPN（ネットワーク層での VPN）は、主に拠点間の固定通信を行うために適しているといえる。また、組織で管理されたパソコンについては、事前に必要なソフトウェアをインストールし設定を行うことで、リモートアクセスとしての利用が可能である。

一方、SSL VPN（トランスポート層以上での VPN）は、Windows OS 標準の Web ブラウザなどを用いて通信を行うため、事前にパソコンにソフトウェアをインストールする必要がなく、インターネット上の管理されていないパソコンからの利用に適しているといえる。

また、SSL VPN は、より上位の層で動作を行うため、利用する場所やパソコンに依存せずにきめ細かいアクセス制御が可能であるというメリットもある。

これらのことから、ある程度管理された医師が利用するパソコンからのアクセスや、拠点間通信となる HOSPnet との接続には、IPsec を用いることが最適であり、患者がインターネット上のパソコンから利用する接続に対しては、SSL VPN を用いることが望ましいといえる。

しかしながら、SSL VPN を用いた場合には、Web ブラウザを用いないアプリケーションの利用ができない欠点がある。この欠点を補うために、SSL VPN の機能を提供する各社においてこれを拡張し、必要なソフトウェアを接続時に自動的にダウンロードしパソコンにインストールすることで、IPsec と同様の利便性をうたう技術を実装してきている。これらの実装には、Java アプレットや ActiveX などが用いられており、インストールされたソフトウェアは、SSL VPN の切断時には削除されるのが一般的である。

このように、同じ VPN でも用いる技術によって特徴が異なることから、それぞれの用途に応じて最適な技術を適用することが求められる。

(4)　内部セキュリティ対策の要素

A-net の内部ネットワーク上でのセキュリティを確保するための各種技術について検討する。

ア　端末認証

ネットワーク上のスイッチングハブなどの認証機能を利用して、予め内部ネットワークにアクセスが可能な端末の MAC アドレスや端末固有の情報を登録しておき、該当する端末からのアクセスがあった場合にのみ通信を許可することでアクセス制御を実現する。

MAC アドレスによる認証方式では、末端のスイッチングハブを認証対応のものに変更するか、又はサーバなどの重要なセグメントと端末セグメントの間にゲートウェイを設置す

る必要がある。コスト的にはゲートウェイ型のほうが優れているが、シングルポイントとなり故障時の影響が大きくなるといった問題点もある。

これらの方式は、ユーザ認証と比較すると端末への専用ソフトウェアのインストールや設定変更が不要であるため、導入コストを比較的安く済ませられるメリットがある。

また、MAC アドレスで認証を行うため、利用者が認証情報の入力などの特別な操作を行う必要がなく、運用上、利用者に与える影響やコストも最小限に抑えることができる。

一方で、MAC アドレスは詐称することが可能なことや、端末の故障による入れ替えなどにより、認証情報の登録変更が必要になるなど、運用管理者の負荷が高くなるなどの問題がある。

イ　ユーザ認証

標準規格である IEEE 802.1X に対応した認証スイッチや独自に実装された Web 認証などに対応したスイッチングハブを導入し、利用者による識別を行う方式である。

IEEE 802.1X による認証では、認証が成功しないとスイッチングハブのインターフェースをシャットダウンすることが可能であり、端末からの一切の通信ができなくなるなど、他の方式に比べて高度なセキュリティレベルを保つことが可能となる。

しかし、端末が IEEE 802.1X 認証に対応している必要があり、標準では、Windows2000 SP4 以上、Windows XP SP1 以上などの条件がある。このため、他の OS がインストールされた端末では、サプリカントと呼ばれる有償の対応ソフトウェアのインストールが必要となる。また、一般的に端末直前まで IEEE 802.1X 認証に対応した認証スイッチを配備する必要があるなど、導入における技術的な要求水準や経済的負担が大きくなるなどの課題がある。

一方、Web 認証などの方式では Web 認証に対応したスイッチングハブにアクセスし、認証情報の入力などを行うことで認証を行う。Web 認証方式では、端末は通常の Web ブラウザで認証が可能なため、端末への変更を最小限に抑えることが可能であり採用が進んでいる。

ユーザ認証においては、より高度な認証や識別が必要な場合には、パスワードに代わる認証手段として、複製が不可能といわれる秘密鍵を IC カードなどに格納し、本人しか持ち得ない秘密鍵を利用した PKI（公開鍵基盤）を併用した認証方式なども注目を集めている。その他の方式として、本人しか持ち得ない生体認証（指紋、彩紋、光彩など）を用いて認証を行う仕組みについても徐々に普及しつつある。

ウ　検疫

これらの端末認証やユーザ認証を応用した仕組みとして、OS のパッチの適用状況やウイルスパターンファイルの適用状況などの端末のソフトウェア環境をチェックし、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も導入が進んでいる。

ウイルス対策などを利用者任せにしないための施策として普及しつつあるが、端末を起動した際に直ちにシステムを利用できないなどの問題もあるため、導入に際しては充分な検討が必要である。

エ　アクセス制限

不正な利用者からのアクセスを防止するため、一定回数以上認証を失敗した場合には、その利用者の ID を無効にするなどの機能を実装することが望ましい。

また、一度に複数の患者情報などに触れることのできる医師については、業務や研究などに支障のない範囲内でその利用時間を制限したり、一定時間経過後には接続を切断するなどの対策を施すことが望ましい。

更には、利用する端末の IP アドレスやその他の固有の情報によって、ネットワーク自体へのアクセス許可や拒否の制御を実施することや、利用者の権限レベルによって、データのアクセス件（読み取り専用、書込可能、削除可能など）を、データのカテゴリ毎に適切に設定する必要がある。

これらのアクセス制御は比較的容易に実装が可能であれ、これらを適切に組み合わせることで、より強固なセキュリティ対策が実現できる。

オ　保存データの暗号化

患者の個人情報などを取り扱うにあたっては、サーバなどに蓄積されたデータも暗号化する必要がある。

通信経路上での情報の搾取よりも、より短時間で大量のデータを得ることができるサーバやデータベースについては、その影響度は計り知れないため、万が一の事故が発生した場合でもその情報が漏えいしないような対策が求められる。

また、バックアップなどでデータを持ち出す必要がある場合には、それらのデータについても暗号化を施す必要がある。

カ　端末へのデータ保存の禁止

Web ブラウザを用いたシステムにおいては、一般的にサーバと端末間においてデータ転送が行われ、一旦その情報が端末内に保存される。

患者の個人情報などを取り扱うにあたっては、できるだけ端末にデータを保存しない仕組みが求められる。特にインターネットカフェなどの公の端末からの利用を想定すると、端末にソフトウェアを予めインストールすることなく実現できるような仕組みが望ましい。

また、院内の端末などについては、端末に保存されるデータも暗号化することで、この

代替対策とすることも可能であるが、USB メモリなどの外部媒体へのデータの保存や大量印刷によるデータの持ち出しについても、制限する仕組みの検討が必要である。

キ　ログの記録

各ネットワーク機器やサーバ等においては、通信ログ、アクセスログ、エラーログ、トラヒック状況などを全て収集しておく必要がある。

これは有事の際、誰が、いつ、どこにアクセスしたかが分かれば、情報漏洩の範囲や影響度など素早い状況把握が可能になるための措置である。また、障害発生時においては、エラーログより障害原因の解析を実施するという重要な役割を担う。

また、利用者がログインした際には、前回のログイン日時やアクセス履歴を表示し利用者に知らせるような仕組みを講じることにも活用できる。こうした仕組みを講じることで、利用者に対して管理されていることを意識されると同時に、身に覚えのない利用履歴が表示されている場合には、運用管理者に問い合わせるなど、セキュリティ事故の兆候をいち早く感じ取ることにも有効に機能する。

ク　脆弱性検査

ネットワーク基盤やサーバを高いセキュリティで設計した場合でも、その構築段階において、設定ミスや重大なセキュリティホールをそのままにしてしまう危険性がある。これを確認するためにシステムの脆弱性検査を実施することが望ましい。

また、構築段階では脆弱性がないと思われていたものも、その後、重大な脆弱性が発見され、その脆弱性が存在したままである場合も考えられる。そのため、脆弱性検査を定期的に行い、セキュリティホールを検出することが望ましい。

脆弱性検査は、脆弱性を検出するだけであり、検出された脆弱性に対しての是正処置についても適切に検討し、実施する必要がある。

(5)　人的なセキュリティ対策の要素

ア　ID 管理

ID は、利用者を識別するための重要な情報である。

ID の管理については、医師や患者などの利用者自身にも貸し借りをしたり漏えいしたりすることのないように、厳格な管理を徹底する必要がある。

運用管理者においては、予め定められた手順に基づいて適切に ID の付与を行う必要がある。また、不必要となった ID が登録されていないか、本来の権限を超越した権利が与えられていないか、共有 ID を登録していないかなどを定期的に確認することが求められ

る。

特に、院内での組織変更や医師の転勤などの何らかの変更があった際には、必ず見直しを行うことが望ましい。

また、管理者用の特権 ID については、その付与や利用については厳格に管理しなければならない。

イ　パスワード管理

パスワードは、ID とともに利用して、利用者を認証するための重要な情報である。

パスワードの管理については、ID と同様に医師や患者などの利用者自身にも貸し借りをしたり漏えいしたりすることのないように、厳格な管理を徹底する必要がある。

特に、パスワードは忘れがちなため、メモにとってパソコンに貼り付けたり、誰でも推測が可能な簡易なパスワードを設定したりする行為を目にするが、これらの行為は禁止しなければならない。

また、パスワードを定期的に変更するような仕組みを導入したり、使い捨てのワンタイムパスワードによる認証方式を導入し利用者のパスワード管理負荷を軽減したりするなど、利用者の利便性にも配慮しつつ、厳格なパスワード管理が求められる。

特に、管理者用の特権 ID のパスワードについては、運用管理者が変更になった際などは、必ずパスワードを変更するなどの管理策を講じる必要がある。

ウ　クリアスクリーン

A-net の利用場所が拡大するにしたがって、本来アクセスを許可されていない第三者からの情報の盗み見やシステムの利用といった脅威に対面することとなる。

特に、院内だけでなく外出先などの公共スペースからのアクセスが可能となった場合には、これらの脅威が増大する。

利用者は、離席時においては画面に表示された情報が見られないようにスクリーンセーバを動作させるなどの対策、またパソコンの操作ができないようにキーロックをかけておくなどの基本的な対策が重要となる。

(6)　まとめ

さまざまなところに存在するセキュリティ上の脅威に対し、完璧な対策を行うことは事実上不可能であるといえる。

A-net 全ての安全性を確保するために、いかに効果的な対策を可能な限り安価で実施するかが重要である。

ここで分類した、外部セキュリティ対策、内部セキュリティ対策、人的なセキュリティ

対策、及びその他の物理的な対策や管理上の対策などのそれぞれのカテゴリにおいて、どの程度の脅威がありどの程度の対策が必要であるかを充分に吟味し、各々において適切なレベルのセキュリティ対策を実施することが求められる。

これらのセキュリティ対策を複合的に組み合わせることによって、より強固なセキュリティ対策が施された A-net のシステムが出来上がる。

4 運用管理の向上

(1) A-net の現状

現在、A-net では、システムの運用管理を外部事業者（運用管理を委託された外部事業者を「運用管理委託事業者」とする）に委託している。

A-net に関連する情報資産については把握し管理されており、また、運用管理委託事業者からは逐次アクセス数やデータ量などについての報告を受けており、一定レベルの運用管理体制が確立されているといえる。

しかし、サービスレベル（システム運用を提供する時間や内容、水準などを定めた基準）などの運用管理上の要求事項が明確に定義されていないなどの問題点も散見される。

加えて、システムを構成するハードウェアやソフトウェアを資産として購入しているため、既にサポートが受けられなくなったハードウェアやソフトウェアを継続して利用しているなど、重大な問題も抱えている。

これらの状況で、ひとたび重大なインシデントが発生した際には、原因の分析や復旧の対応までに非常に多くの時間を要する可能性がある。また、システムの運用継続ができなくなる可能性だけでなく、管理しているデータの喪失などの危険性もはらんでいる。

(2) 運用管理の変貌

IT が進歩し複雑化してくるにつれて、情報システムの運用管理工数は何倍にも膨れあがってきている。また IT 資産のライフサイクルは年々短くなってきており、それに伴ってハードウェアの入替えなど、システムの運用管理を担う管理者に求められる業務負荷が高まり、その内容も変わりつつある。

旧来の管理業務は稼働監視や資産管理といった受動的なものが主であったが、最近はより能動的な対応・対策が求められている。これは、システムの高度化、複雑化によってインシデントが発生した場合の影響範囲が拡大しており、その影響度が非常に大きいためであり、これに対処するためには不具合の迅速な解決のみならず、未然の防止が強く求められている。

特に情報セキュリティ事故は、組織にとって事故の処理に莫大な労力と時間を費やすこととなり、取り返しのつかない信用失墜や患者の個人情報の流出などの結果を招く可能性があり、事前の防止策が重要視されている。

人的なリソースには限界があるため、昨今では、旧来の業務はツールや外部事業者の提供するサービスを積極的に活用して省力化し、内部の職員は傾向分析や対策、改善、及び IT 戦略の企画や推進といった、より高度な業務に注力するという考え方が主流となってきている。

特に IT サービスにおける成功事例を集めた ITIL（Information Technology

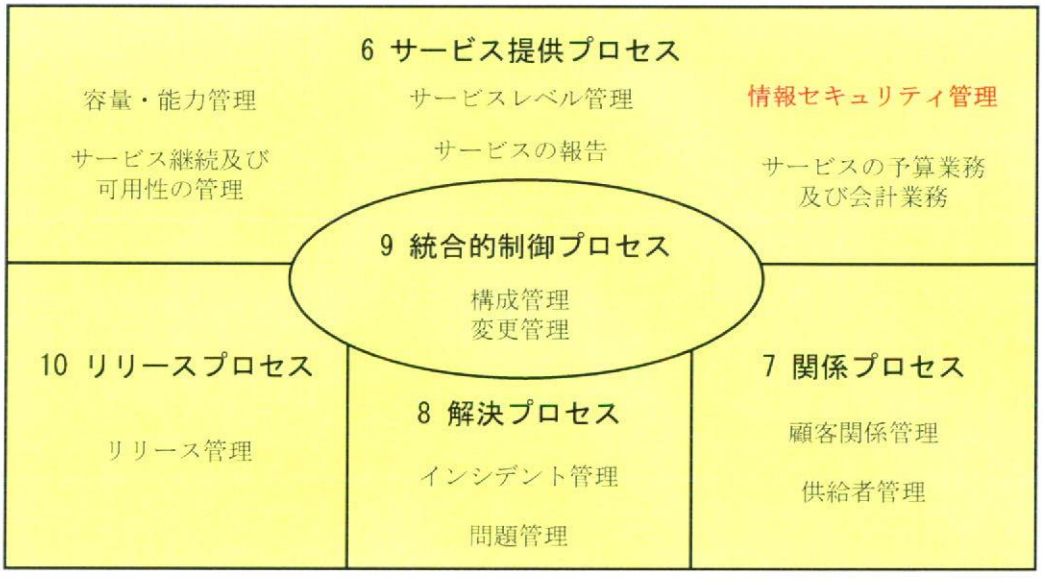
Infrastructure Library）が世界的に導入されるようになってきており、システム運用管理に係る中長期的なコストの削減に注目されるようになってきている。

本項では、これらの運用管理に係る要素や要件などを、ITIL や ITSMS（Information Technology Service Management Systems）の認証規格である「JIS Q 20000」の概念を踏まえて整理するとともに、次期 A-net の運用管理を考える上で、考慮するべき事項の検討を行う。

(3)　運用管理の要素

日頃のシステムの運用管理を考える上で、ITIL や ITSMS の観点を踏まえ、あるべき運用管理の姿を検討すると、以下の５つの管理項目が必要であると考えられる。

- サービス提供プロセス
- 関係プロセス
- 解決プロセス
- 統合的制御プロセス
- リリースプロセス



【図 4-1　JIS Q 20000 における運用管理の各プロセス】

運用管理における各管理項目は、情報セキュリティ管理の「JIS Q 27001」規格とも密接に関連しているため、これらを併せて考えると効率的である。

本項では、【表 4-1】において運用管理に係る規格である「JIS Q 20000」に基づく検討を行い、情報セキュリティ管理に係る規格である「JIS Q 27001」に定義された事項と関連する項目については、その関連性を明確にする。

なお、本項での検討対象となるものは、主として「技術的対策」欄に○が記載された、技術的な検討事項の項目とする。また、情報セキュリティ管理は、別項で検討しているため省略する。

【表 4-1　JIS Q 20000 における運用管理の各項目の検討】

項番	項目	技術的対策	JIS Q 27001 関連項番
6	サービス提供プロセス		
6.1	サービスレベル管理	○	A. 10. 2. 1
6.2	サービスの報告	○	A. 10. 2. 2
6.3	サービス継続及び可用性の管理	○	A. 14. 1 全般
6.4	サービスの予算業務及び会計業務	－	－
6.5	容量・能力管理	○	A. 10. 3. 1
6.6	情報セキュリティ管理	－	－
7	関係プロセス		
7.2	顧客関係管理	－	A. 6. 1. 6 A. 6. 1. 7
7.3	供給者管理	－	A. 10. 2. 1 A. 10. 2. 2 A. 10. 2. 3
8	解決プロセス		
8.2	インシデント管理	○	A. 13. 1. 1 A. 13. 1. 2 A. 13. 2. 1
8.3	問題管理	○	A. 13. 2. 2 A. 13. 2. 3
9	統合的制御プロセス		
9.1	構成管理	○	A. 7. 1. 1
9.2	変更管理	○	A. 10. 1. 2 A. 10. 2. 3 A. 12. 5. 1
10	リリースプロセス		
10.1	リリース管理	○	A. 12. 5. 2 A. 12. 5. 3

ア　サービスレベル管理

客観的にサービス品質を把握し、適正にシステムを運用管理するための値として、サービスレベルの設定が必要である。

システム管理を委託する運用管理委託事業者との間で、サービスを提供する時刻やその内容、障害が発生した場合の回復目標時刻などのサービスレベルを予め合意し、SLA（Service Level Agreement）を定義する必要がある。

SLA とは、運用管理委託事業者等が一定の基準値を守って医師や患者に対して A-net のサービスを提供することを保証する契約であり、この SLA を取り交すことによって、運用管理開始後のサービス品質を保つことができる。

契約期間中はメーカによるサポート期限が切れた製品についても、運用管理委託事業者の責任の範囲でサポートを継続するよう求めることも可能であり、これらの条件の取り交わしについても、対応可否を検討する。

イ　サービスの報告

運用管理委託事業者が SLA に基づくサービスを実行していることを確認するためには、定期的に適切なサービスの報告を受けることが重要である。

現在においても、A-net の運用管理に係る報告を運用管理委託事業者から定期的に受けているが、今後も SLA に基づく正確な報告を受けることができるように、サービス報告書を受取、管理することが求められる。

ウ　サービス継続及び可用性の管理

より多くの医師や患者に利用してもらうためには、使いたいときに使える可用性を有したシステムでなければならない。

サービス提供時間がごく短時間に限定される運用が行われていたり、予期せぬ時間帯にメンテナンスが行われていたり、利用率が増えると停止や待ち時間が発生するようなシステムであっては、徐々に利用頻度が少なくなることが想定される。

また、不測の事態が発生した場合などに備えて、必ずバックアップデータを取得しておく必要があるが、大規模災害ではバックアップデータも同時に破壊される可能性が高いため、影響を受けないような遠隔地に保管するなどの対策を検討する必要がある。

特に、患者の個人情報や重要な研究情報を取り扱う本システムにおいては、これらの事態が発生した場合でも、情報漏洩が発生しないようにセキュリティ面でも充分な対策が求められる。

エ　容量・能力管理