システムが現在あるいは将来の需要を満たすことができるように、充分なデータ保存容量や処理能力を常に有していることを確認しておくことが重要である。

代表的なものとして、サーバの記憶容量やメモリ容量、及びネットワークの帯域利用率などの容量や能力を常に把握し、管理していくことが挙げられる。

これらを怠ると、新たに更新されたデータは保存されるが、引換えに古い保存データが消失するなどの事故が発生する場合もある。

現在の運用においても、患者の登録者数や A-net に対するアクセス数などを把握し管理しているが、今後も継続し、急激な患者数の増加やアクセス数の増加にも対応できるよう管理していかなければならない。

オ　インシデント管理、問題管理

インシデント管理、問題管理とは、SLA による契約により合意されたサービスに何らかの事象（システムの停止、ネットワークの停止、ハードウェアの故障、セキュリティ上の事故など）が発生した場合に、SLA の内容に則して可能な限り迅速に対応することや、その原因を分析することによって、同じ事象の再発によるサービス中断を最小限に抑えるための管理手法である。

これらを早急に把握できるように、監視装置などによるシステムの死活監視や稼働管理、更にはログや通信フロー状況を取得し、定期的に検証することが重要である。

また、アクセスログの取得などを通じて、患者の情報を守るため予期しない利用者からのアクセスがないか、ルールに反した利用がなされていないかなどを確認することも必要である。

カ　構成管理

構成管理は、サービスを提供するための全ての構成要素を一意に識別して正確な構成情報を管理し、維持することが求められる。

現在の A-net 運用管理においても、どのようなサーバや端末で利用されているか、どのようなネットワーク構成になっているかが把握されており、これに加えて過去に発生した問題点なども集約して管理する必要があり、次期 A-net の運用管理においても継続して取り組むことが求められる。

キ　変更管理、リリース管理

システムを継続的に利用し管理していくためには、システムそのものの機能追加や改修、ハードウェアやソフトウェアの追加、脆弱性などに対応するためのパッチの適用など、様々な変更を繰り返しながら、適切なサービス提供を継続していくこととなる。

これらの全ての変更については、リリース（又は適用）する期日や変更内容、その影響

度などを充分に考慮し、適切に変更が反映されるように管理されなければならない。

例えば、新しく発売された Windows OS のパソコンでは動作が保証できないシステムにおいて、最新の Windows OS を搭載したパソコンを導入することは無用なトラブルの元となるし、メーカから公開された脆弱性に対するパッチや新しい Web ブラウザなどを無条件で適用すると、システムの動作や一部機能に影響を与える可能性も否定できないため、安易な導入や適用は避けるべきである。

また、それらの不具合が発生した際における、元の環境への切り戻しの方法や手順を定めておかなければ、システムの稼働不能や回復不能な事態に陥ることも考えられる。

これらのシステムに係る変更やリリースが、適切な計画に基づいて確実に実施されるように、予めルールを定め管理する必要がある。

変更管理とリリース管理は、本来異なるプロセスであるが、分かりやすいよう簡易的にまとめて記述した。

(4)　サービス提供形態の検討

最近のシステムの利用形態として、ハードウェアやソフトウェアを資産として自ら保有する方式のみならず、ハードウェアをリース契約により借用する方式や、システム開発そのものを委託してしまい、その利用権のみを取得する形態など、様々なサービス提供形態が存在する。

主なサービス形態の比較と特徴を【表 4-2】に示す。

【表 4-2　主なサービス形態の比較】

項番	項目	ハードウェアのリース契約	iDC ハウジング	ASP、SaaS	ASP、SaaS 応用型
1	利用者側が資産として保有する情報資産（買取り又は開発費）				
1.1	サーバ	リース	リース		
1.2	端末	リース	リース	リース	
1.3	ネットワーク設備	リース	リース	リース	
1.4	A-net の電子カルテシステム	○	○		

2	サービス提供者側が資産として保有する情報資産（買取り又は開発費） ※サービス提供者がリースとして借用し、又貸しで提供する場合あり				
2.1	サーバ			△ リース	△ リース
2.2	端末				△ リース
2.3	ネットワーク設備				△ リース
2.4	A-net の電子カルテシステム			○	○
3	利用者側は、利用権としてサービスを受けるもの（使用許諾権）				
3.1	サーバ				
3.2	端末				○
3.3	ネットワーク設備				○
3.4	A-net の電子カルテシステム			○	○
4	主な運用管理の責任主体 ※システム開発者とサービス提供者が異なる場合、開発者が担う場合あり				
4.1	サーバ	利用者	利用者	※ 提供者	※ 提供者
4.2	端末	利用者	利用者	利用者	※ 提供者
4.3	ネットワーク設備	利用者	利用者	利用者	※ 提供者
4.4	A-net の電子カルテシステム	開発者 利用者	開発者 利用者	※ 開発者 提供者	※ 開発者 提供者

ア　ハードウェアのリース契約

近年、IT 技術の進歩は予想以上に早く、最新の情報システムを調達した場合でも、わずか 2～3 年前後には既に陳腐化する場合や、既に市場から姿を消している場合、または最新のシステムと互換性が保たれなくなっているなどの事象もしばしばみられる。

特にセキュリティ分野ではこれらの傾向が顕著であり、現在では予想できない新たなセキュリティ上の脅威に対応するため、日々ハードウェアやソフトウェアの更新が実施されており、それらに対応できなくなった機器については、わずか 1 年程度で販売を終了する製品すら存在する。

次期 A-net においては、一度導入したハードウェアやソフトウェアなどの大切な資産がすぐに陳腐化しないように、また永続的にシステムを利用できるようにするために、ハー

ドウェア等はリースによる賃貸借契約で調達することが望ましい。また、導入時より一定期間経過後には最新のシステムに入れ替えて、システム運用を継続できる環境を整えることを予め想定しておくなど、将来を見据えたシステム構築が必要である。

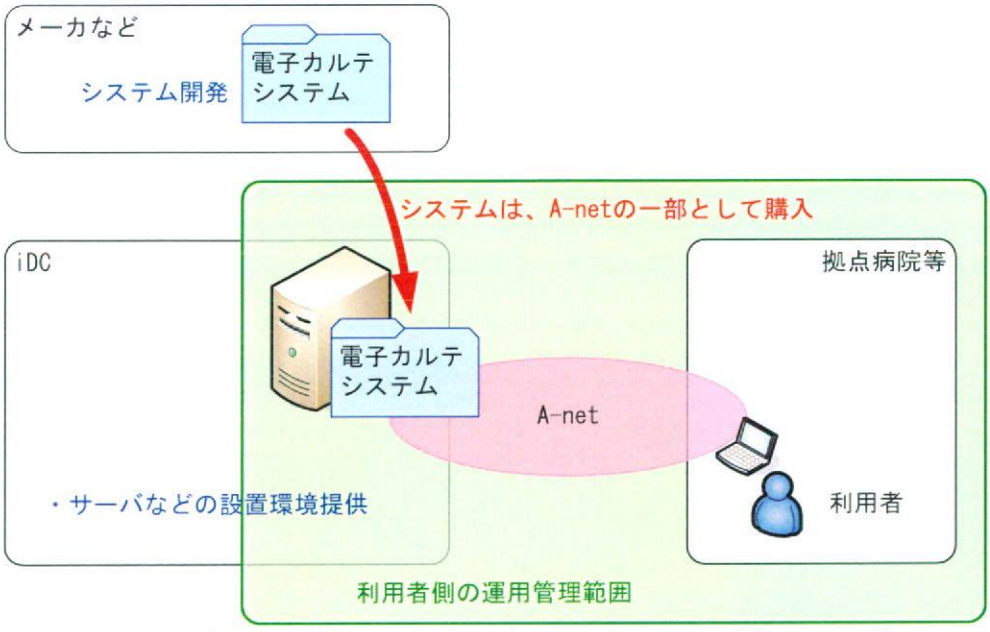
ソフトウェアについても、一定期間はメーカによるサポート期限に係わらず、サービス提供や不具合の改修などを継続して受けられるような契約形態を検討することが重要である。

イ　iDC（インターネットデータセンター）ハウジング

旧来の情報システムは、自らの施設内にサーバやホストなどを設置し、職員や運用管理委託事業者が常駐することによって運用管理を行う方式が主流であった。

しかし、システムの導入コストや運用管理コストの削減、運用管理ノウハウの不足、更にはセキュリティの強化などを目的として、専用の機器設置環境を備えた iDC にサーバを設置したり、また、それらの簡易的な運用管理を委託したりして、自らの施設内にサーバを持たない運用の方法に移行してきている。

iDC は、大規模災害に対する備えも万全であり、また専門の知識を持った技術者が運用管理に従事することで、日頃からのトラブルに迅速かつ適切な対応が可能であるなど利便性も高く、次期システムの導入の際には、これらの運用形態についても検討する価値がある。



【図 4-2　iDC ハウジングによるサービス形態イメージ】

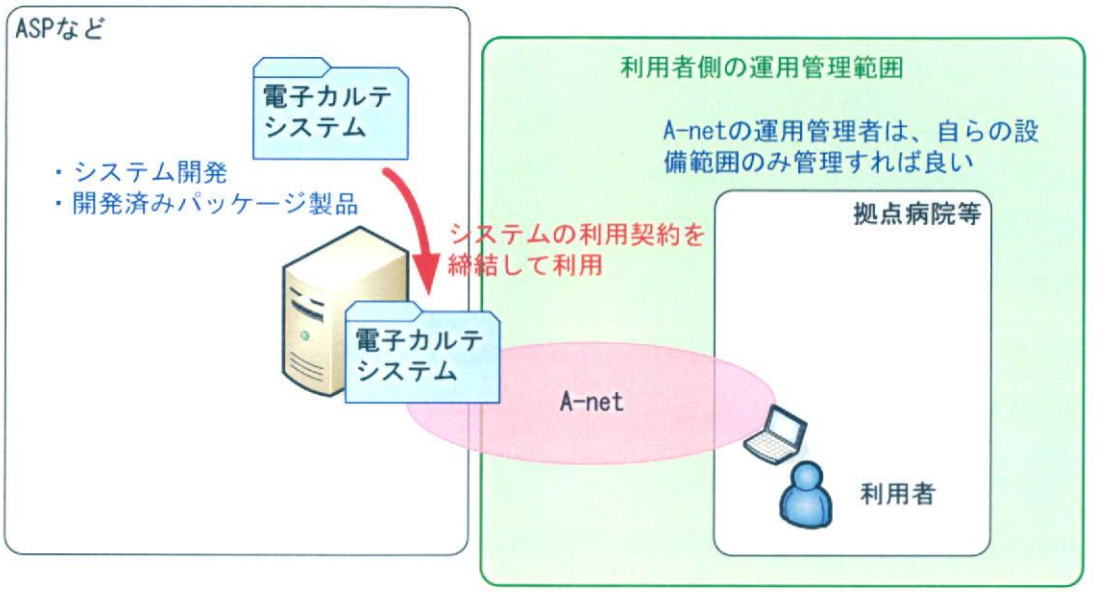
ウ　ASP（アプリケーションサービスプロバイダ）、SaaS（サース）

iDC は、自らの保有資産であるサーバなどのハードウェアの設置場所の供与や簡易的な

運用管理のサービスを供与するものであり、システム開発などは自ら行うか、もしくは別途委託した外部事業者によって実施されるものである。

しかし、最近ではネットワークを経由して「サービスそのものの利用権だけを提供する」ASP や SaaS と呼ばれる仕組みも広がりつつある。これらは、サーバのハードウェアやシステム開発も含めて委託するか、もしくは既にサービス提供事業者によって開発済みのシステムを用いて、それらを資産として保有せずにシステムを利用する権利だけを購入又は契約による取得する形態である。

これらのサービス形態では、利用期間の拘束をされることなく、サービスの利用期間を希望に応じて継続することが可能であり、ハードウェアやソフトウェアの陳腐化といった問題を気にする必要がない。（ただし、最低契約期間の制限がある場合や、一定期間の事前通知によって、サービス提供を停止や終了される場合は想定される。）



【図 4-3　ASP、SaaS によるサービス形態イメージ】

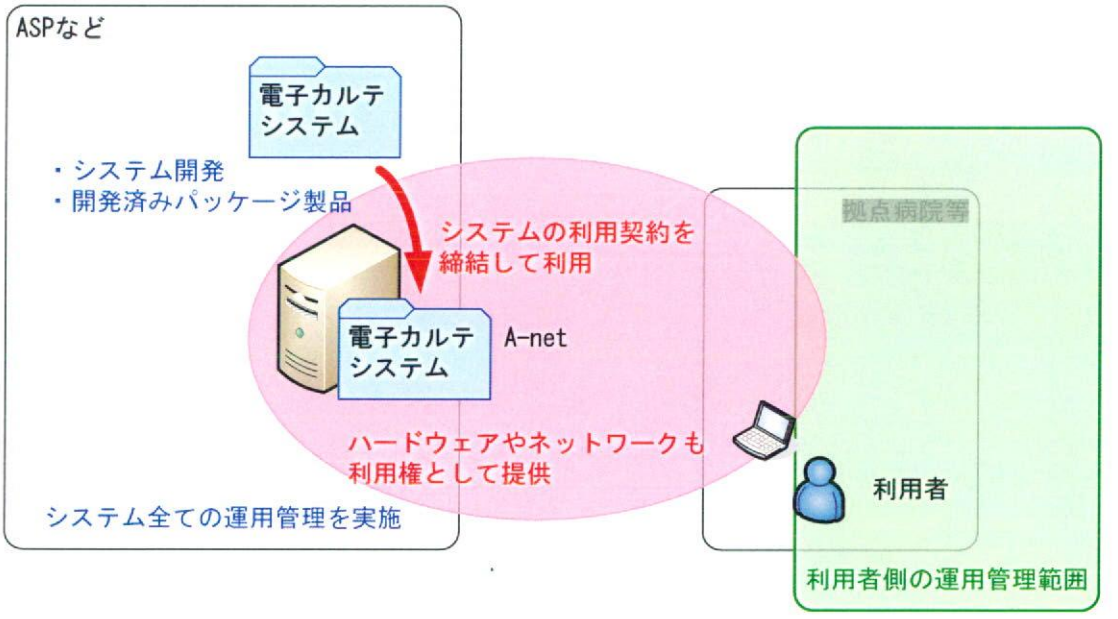
エ　ASP、SaaS 応用型

ASP、SaaS の応用型として、関連するネットワークや利用者端末の提供又はリース契約までも含めて一切の資産を保有せずに、システムを利用する権利だけを提供する契約形態も一部ではみられるようになってきた。

これらのサービスを利用すると、ネットワークインフラやサーバ、端末などのハードウェアの購入やシステム開発、また運用管理に係る費用もほとんど発生せずに、サービス提供そのものに対して対価を支払って利用が可能となる。ハードウェアのサポート期限やソフトウェアの不備に対する改修などをあまり気にすることなく、定められた契約に基づいて継続して利用することができる。

次期システムで実現したい要求が全て満たされ、サービス提供を行うことが可能な事業者が存在することが条件であり、またこれらのサービス形態も逐次発展しているため、ト

ータルコストの比較など慎重な検討が必要ではあるが、次期 A-net の開発委託時には一考の価値があると考える。



【図 4-4　ASP、SaaS 応用型によるサービス形態イメージ】

(5)　まとめ

IT 投資の資源集中や人材不足などの新たな課題も浮き彫りになる中で、次期 A-net のシステム開発時には、今以上にシステム運用管理に係る環境も変化していることが予想される。

次期システム調達時において、最適なサービス提供の形態や運用管理の内容を慎重に検討することが重要である。また、運用管理に係る規格の要求事項などを参考にしながら、費用対効果を検討し、医師や A-net 運用管理者である職員の負担を最大限に減少し、かつ投資も最小になるような調達、構築、運用管理の仕組みを考慮することが必要である。

また、A-net の重要性を鑑み、常に現在のシステムの状況を把握できるようにネットワークやシステムの稼働状況やログなどを一元管理する装置などの活用によって、運用管理性を高めるとともに、運用管理の可視化を行うことも重要である。

採用する運用管理基準や体制によって、人的リソースのみならず、必要となる装置や具備するべき機能（又は技術）なども大きく変わってくるため、慎重な検討が必要である。

システムの開発、構築や運用管理を外部事業者に委託する場合においても、常に関連する医師や職員が現在の状況を把握できるように、運用管理委託事業者などとのコミュニケーションを密に保たなければならない。

5 模擬環境での実証実験

(1) 目的

机上で検討した様々な改善策について、最低限の機能を取り入れた模擬環境を構築し実際に検証することで、机上で検討した改善策の有効性や実用度などの評価を行い、実証実験を通じて現在の A-net と比較した場合の利便性やセキュリティについて検証・考察し、次期 A-net 開発に対する方向付けの参考とすることを目的とする。

(2) 模擬構成

主として下記に示す機器を用いた模擬環境を構築した。

ア　SSL アクセラレータ

シスコシステムズ社　ASA (Adaptive Security Appliance) 5520。

SSL VPN の認証、暗号化、トンネリングなどの機能を提供する機器である。
通常は Web ブラウザを用いて、[https://] で始まる URL を指定してアクセスを行う。
標準では、http、https、ftp、cifs でアクセスするアプリケーションにのみ対応しており、プラグインを用いることによって、rdp、telnet、ssh、VNC (Virtual Network Computing)、ics (Citrix) にも対応することが可能である。
また、その他にも拡張機能を備えており、Cisco AnyConnect VPN クライアントのソフトウェアを端末に自動的にインストールすることによって、Web ブラウザを用いずに通信を行う多くのアプリケーションをサポートできるようになる。
今回は、Cisco AnyConnect VPN クライアントを用いて、Web ブラウザを使用しないシステムである MyProdoc の通信を実現した。
なお、Cisco AnyConnect VPN クライアントを用いた方式では、端末は管理者権限で利用する必要がある。
構成図などでは、「SSL 装置」として記載。

イ　ファイアウォール

シスコシステムズ社　ASA5520 (SSL アクセラレータと兼用)。

インターネットからの SSL による通信以外を拒否する機能を提供する機器である。
今回は、SSL アクセラレータと共存した環境とした。

ステートフルインスペクション型のファイアウォールであり、管理者が定義したアクセス制御ポリシー、詳細なパケット検査、及び全てのネットワーク通信の状態監視を行うことにより、強固なセキュリティ環境を提供する。

また、統合型ファイアウォールとしての設計がなされており、SSL VPN 以外でも IPS やアンチウイルスなどの機能を搭載し共存することも可能である。

構成図などでは、「FW」として記載。

ウ　アンチウイルスゲートウェイ

トレンドマイクロ社　InterScan Gateway Security Appliance。

メール、Web 閲覧から侵入するウイルスをはじめとしたさまざまな脅威に対する検知、駆除する機能を提供する。

ウイルス対策以外にも、スパムメール対策、フィッシング対策、スパイウェア対策、メールコンテンツフィルタリング、URL フィルタリングなどの機能を有している。

構成図等などでは、「アンチウイルス GW」として記載。

エ　認証サーバ

RSA 社　SecurID Appliance。

利用者のアクセスに対する強力な二要素認証（PIN とトークンコード）の機能を提供する。

予め登録しておく PIN と、60 秒ごとに自動的に生成されるトークンコードの組合せによって、強力な認証を実施。

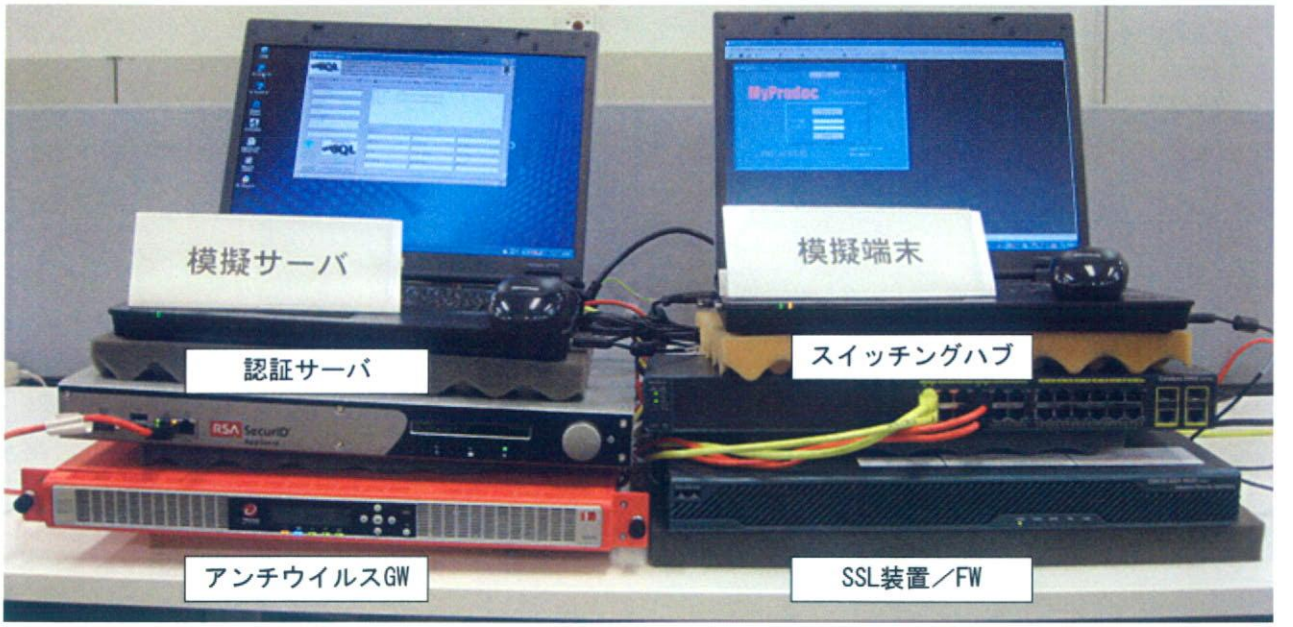
万が一の PIN の漏えいや、ハードウェアトークン（トークンコードを生成する機器）の盗難が発生した場合でも、両方の要素が揃わないと認証が成功しないため、不正利用が困難である。

オ　スイッチングハブ

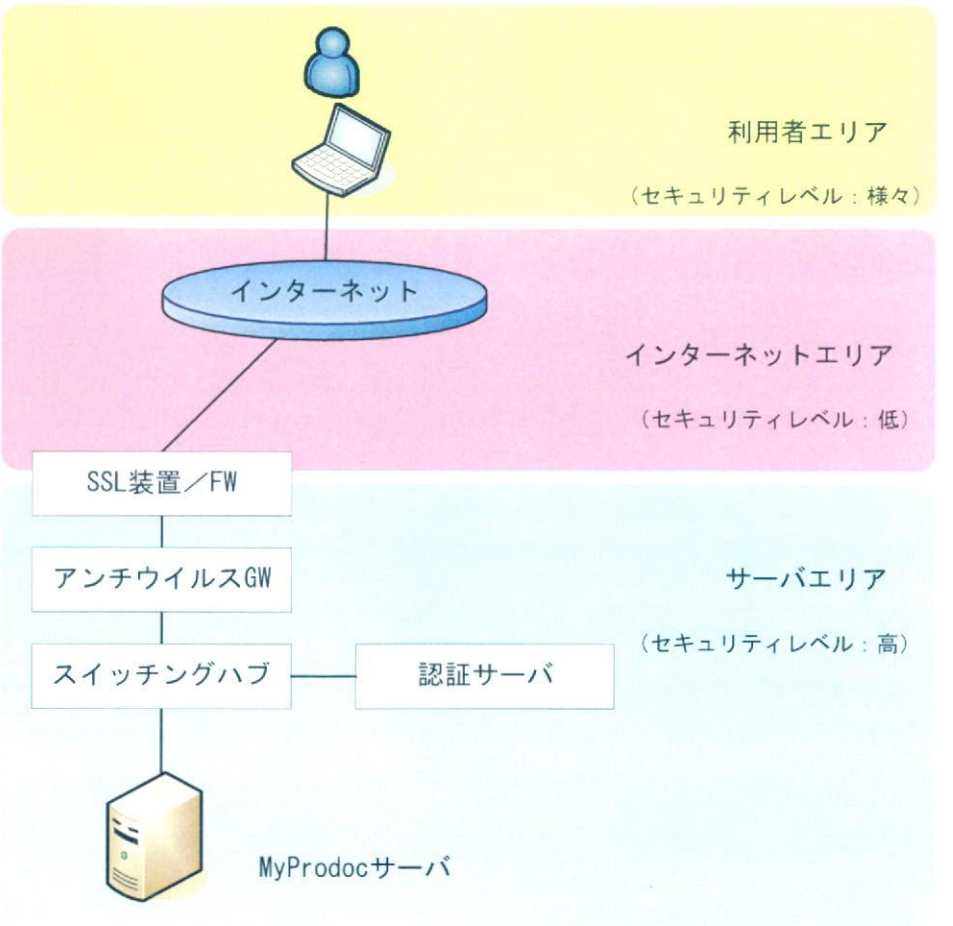
シスコシステムズ社　Catalyst2960-24TC。

カ　電子カルテシステム

ノーバメディコ社　MyProdoc。



【図 5-1　模擬環境構築状況】



【図 5-2　模擬環境構成イメージ】

(3)　検証内容

主に下記の点についての検証を実施する。

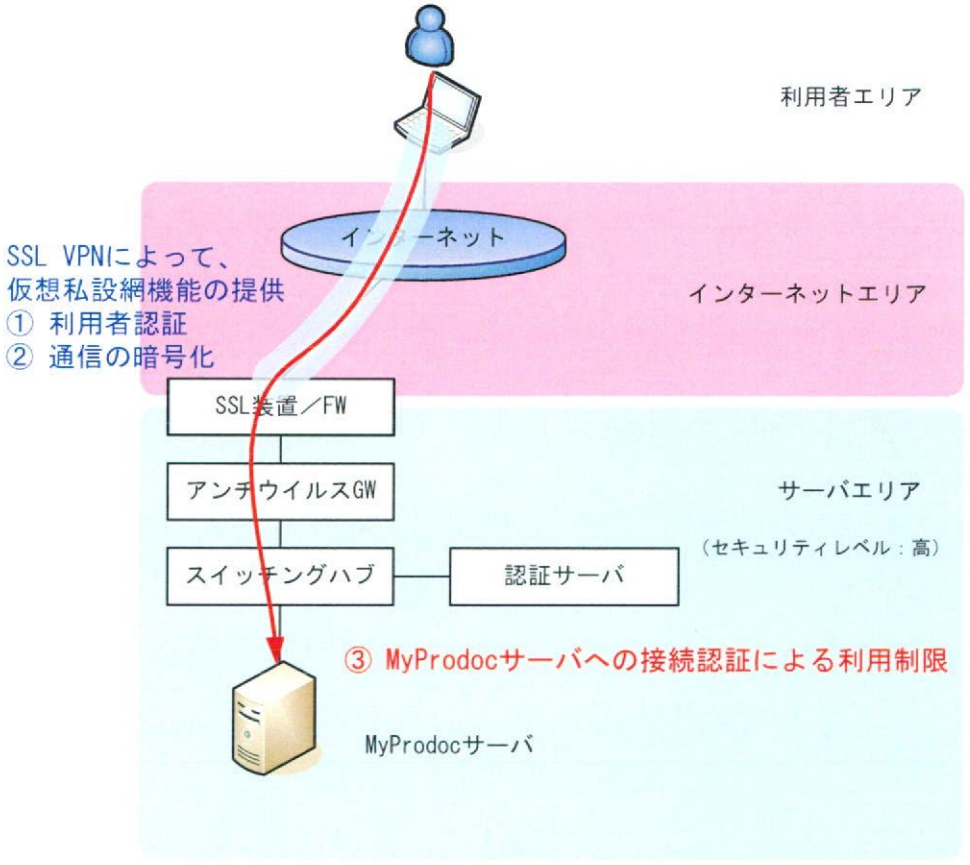
ア　利便性の向上

- 現行の A-net と比較して、端末の使い勝手に改善はみられるか
- 汎用のパソコンで、いつでもどこでも使えるように利便性は高まっているか
- （仮）電子カルテシステムの使い勝手は良いか
- ユーザ ID やパスワードの管理が不便ではないか

イ　セキュリティ対策

- インターネット経由の接続で、セキュリティ上の不安はないか
- ユーザ認証の仕組みにセキュリティ上の問題はないか
- インターネット上の脅威に対する対策に問題はないか

(4)　システム概要

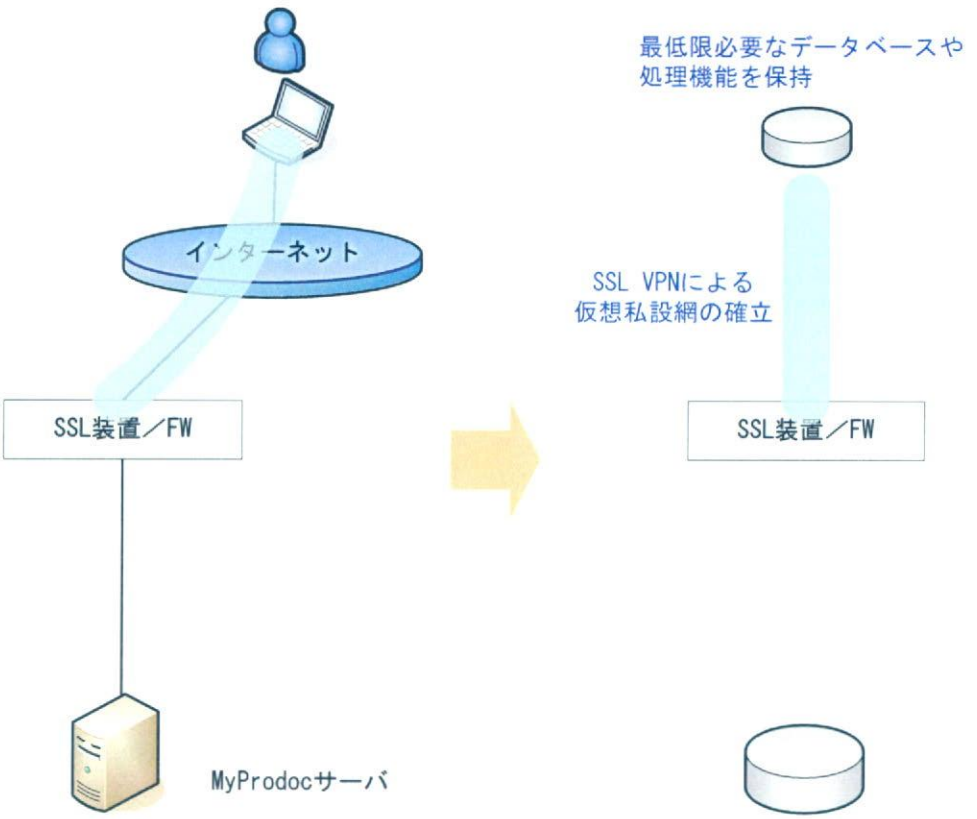


【図 5-3　模擬環境システム概要】

ア　SSL VPN

利便性の向上について検討した結果を基に、SSL VPN 環境を構築する。

セキュリティレベルが低いインターネットからの接続を念頭に、利用者端末と SSL アクセラレータ間で SSL VPN を確立し、利用者認証や通信の暗号化を行い、高セキュリティを担保する。



【図 5-4　SSL VPN 確立システムイメージ】

イ　二要素認証

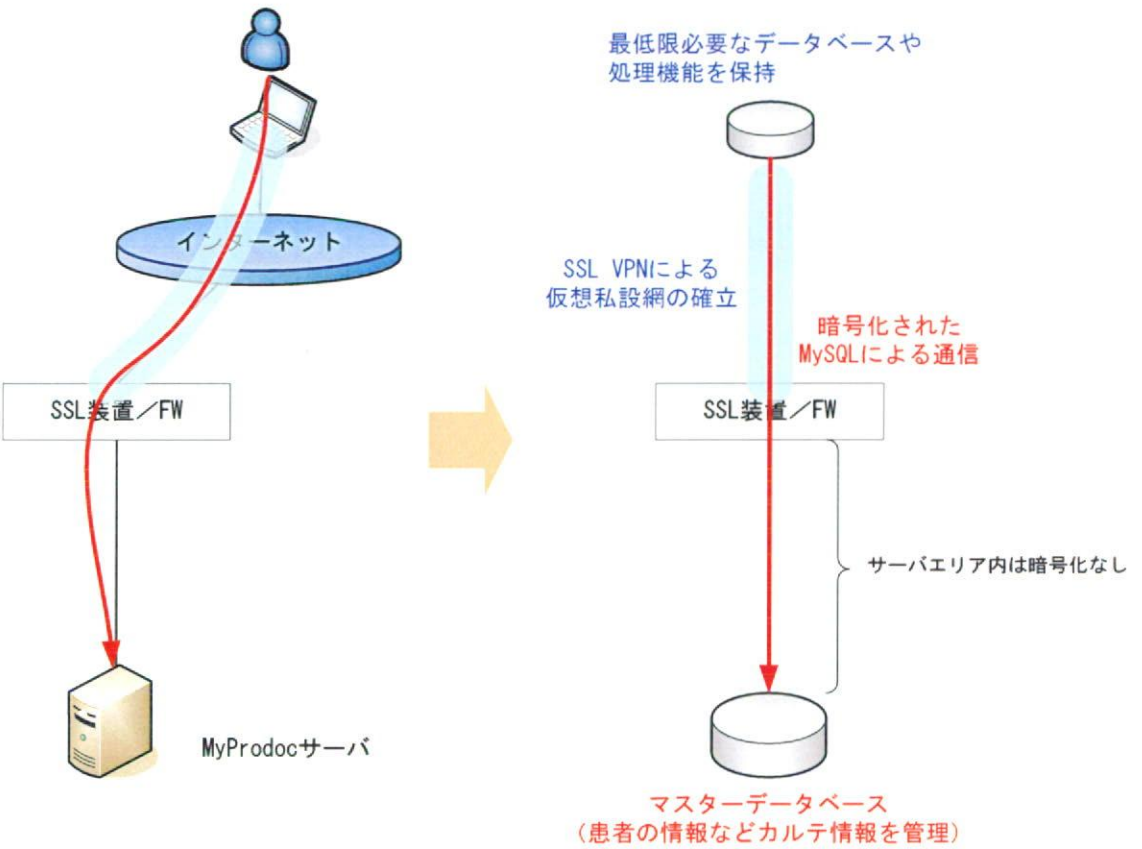
SSL VPN 確立に際しての利用者認証において、固定パスワードだけではなく、ワンタイムパスワードを用いて、PIN とトークンコードによる二要素認証を実施する。

【図 5-5　二要素認証のハードウェアトークン】

ウ　電子カルテシステムでの認証

SSL VPN で確立された仮想私設網の中を通信し、MyProdoc のシステム側でも利用者の認証を行う。

なお、SSL アクセラレータから MyProdoc サーバ間は、セキュリティレベルの高い内部ネットワークであるため、暗号化を行わずに通信を行っている。



【図 5-6　電子カルテシステムの認証通信イメージ】

(5)　システム利用検証

ア　利便性の向上

アクセス環境としてインターネットに接続できる環境があれば、いつでもどこでも利用できる点で、利便性は飛躍的に高まっている。ブロードバンド環境だけでなく、無線 LAN、PHS や携帯電話によるダイヤルアップ接続でも利用が可能である。

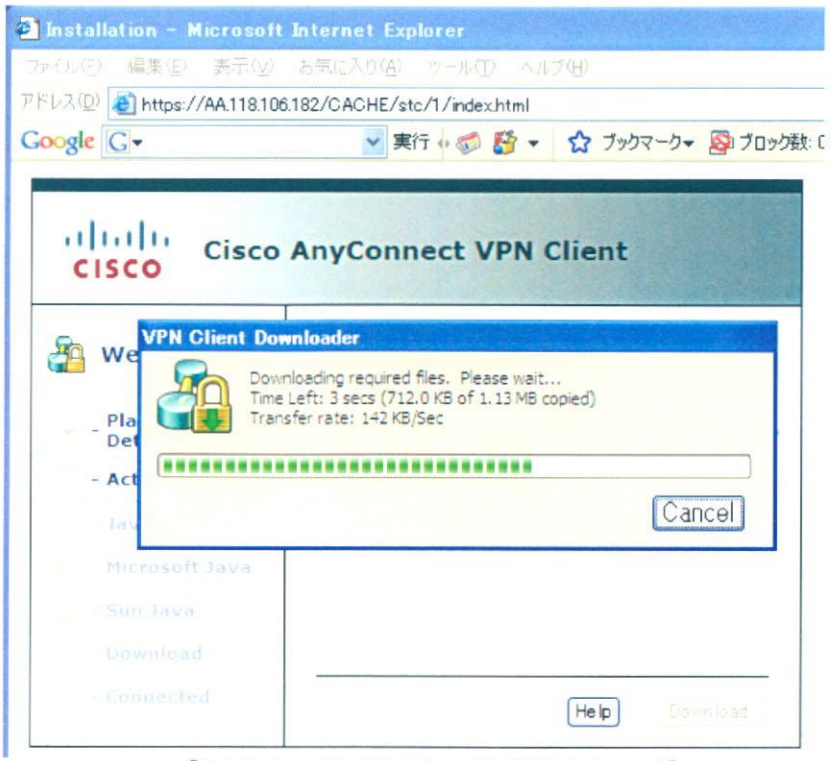
また、日頃使い慣れた Web ブラウザである Internet Explorer などで、指定の URL（この場合は、[https://AA.118.106.182/] ＝グローバル IP アドレスのため、上位 1 オクテ

ットを「AA」で置き換えて表示）を入力するだけで SSL VPN 接続が操作できる点は、IT リテラシーに長けていない患者にとっても利用しやすい環境である。

【図 5-7　SSL VPN 認証画面イメージ】

SSL VPN 接続の際には、必要なソフトウェアを自動的にダウンロードし、インストールが開始される。また、接続解除時には自動的に削除される。

特に利用者の操作を必要とせずに実行される点で、利用しやすいといえる。



【図 5-8　SSL VPN 確立時画面イメージ】

MyProdoc は、Microsoft Access で動作するアプリケーションで、利用者の負担は少ないと考えられる。

MyProdoc の利用についても、ユーザ ID とパスワードでの認証を行う。

二重の認証を行う点でセキュリティが高いといえるが、SSL VPN とは異なり固定のユーザ ID とパスワードを利用する。このため、SSL VPN 接続の認証と、MyProdoc の認証とで、二つのユーザ ID やパスワードを使い分けないといけない。

MyProdoc は開発済みのソフトウェアであるが、次期 A-net の開発時においては、これらの点を考慮し利便性とセキュリティのどちらを優先するのかの判断が必要である。

【図 5-9　MyProdoc 認証画面イメージ】

イ　セキュリティ対策

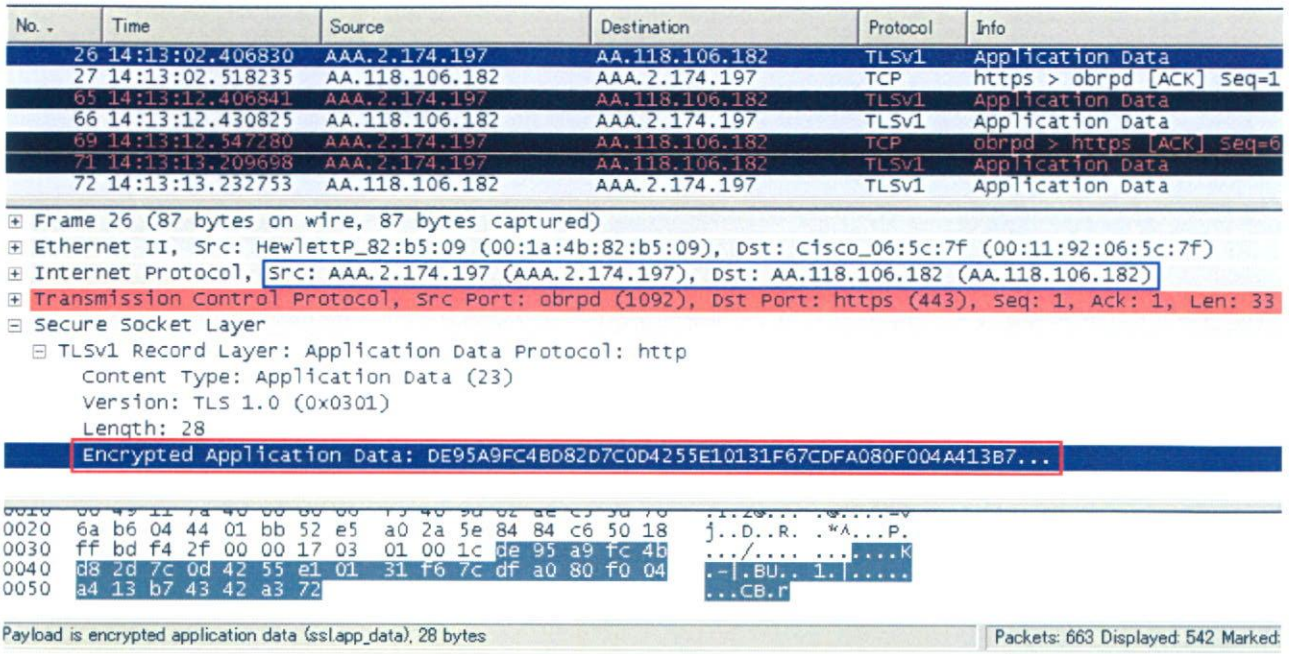
インターネットを経由した通信ではあるが、SSL VPN の確立後は、通信データの暗号化が行われている。

参考として、SSL VPN での通信時のデータの中身を【図 5-10】に示す。

実際には内部ネットワークである、「192.168.0.2」の MyProdoc サーバと通信を行っているが、IP アドレスなども秘匿されており、安全性が確保されているといえる。

常に、「AA.118.106.182」の SSL アクセラレータと通信を行っているように見える（青線）。

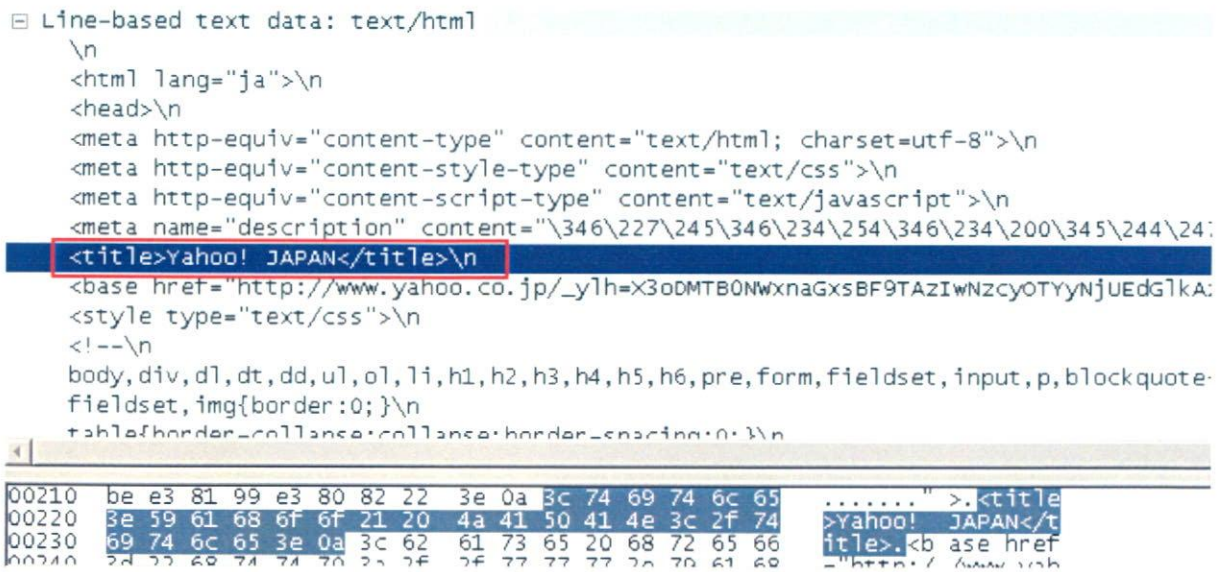
また、通信データの内容も暗号化されていることが分かる（赤線）。



【図 5-10　SSL VPN での暗号化通信データ内容】

参考として、SSL を利用しないで、[Yahoo! JAPAN] を Web 閲覧した場合のデータの中身を【図 5-11】に示す。

平分で通信されており、閲覧したページタイトル「Yahoo! JAPAN」などがそのままの状態で流れていることが分かる。



【図 5-11　通常時の平分での通信データ内容】

SSL VPN 接続の際の利用者認証においては、予め割り当てられた固定のユーザ ID と PIN、及び 60 秒毎に新しいパスワードを生成するトークンコードを使用する。

ユーザ ID と PIN が何らかの事情で漏えいした場合でも、ワンタイムパスワード生成の

ハードウェアトークンがないとログインできず、逆にハードウェアトークンだけを盗まれた場合でも、ユーザ ID と PIN の入手が必須であるため、セキュリティは高い。

また、SSL VPN の経路上は暗号化されているため可能性は低いが、万が一認証に必要な情報が全て盗聴された場合でも、ハードウェアトークンは 60 秒毎に新しいパスワードを自動的に再生成するため、次のログインには盗聴されたパスワードは利用できないため、極めて安全性が高いといえる。

PIN は管理者が予め指定することも可能であるが、利用者が初めて SSL VPN にアクセスした際に、任意のものを設定させることもできる。

管理者が指定した場合には、利用者は覚えにくく、メモなどに記録してしまいがちである。逆に、利用者が設定する場合には、推測されやすい電話番号や生年月日、氏名などの一部、安易なパスワード、他のシステムでも利用しているパスワードと同じものなどを設定しがちである。何れの場合にも、PIN のセキュリティレベルが低くならないような総合的な対策が求められる。

【例】
ユーザ ID：user1
PIN コード：anet2008
トークンコード：904363　［ハードウェアトークンが示した値］

この場合は、anet2008904363［anet2008＋904363］がパスワードとなる。

【図 5-12　ハードウェアトークンを用いたワンタイムパスワードの生成】

(6)　検証結果

ア　考察

検証の結果、現行の A-net と比較して、汎用のパソコンで利用できること、場所を選ばずにインターネットに接続できる環境があれば利用できること、特別な操作やソフトウェアが必要ないことが確認され、利便性は飛躍的に向上されると考えられる。

SSL VPN と電子カルテシステムで認証情報が異なる点は、今回は仮の電子カルテシステ

ムを利用したために問題点が残るが、次期 A-net 開発においてはこの点も考慮して設計することによって、課題は解決できると考えられる。

また、システムへのアクセスという点での利便性は飛躍的に高まるであろうことが実証されたが、これに電子カルテシステムそのものの利便性を高めるための検討や設計を充分に行って開発することで、システム全体としての利便性や有効性が高まると想定される。

一方、セキュリティについても、現行の A-net のセキュリティ対策のレベルを下げることなく、インターネット上からも利用が可能である点が実証された。SSL VPN は広く利用されるようになってきており、ワンタイムパスワードとの組合せは、大手都市銀行やネット銀行などでも利用が進んでおり、それらと同等の安全性が確保できるとすれば、安心して利用できるものと考えられる。

これに加えて、セキュリティの向上について机上で検討した対策を複合的に組み合わせることで、患者にも安心して利用されるシステムが構築できるだろう。

イ　課題

今回の実証実験で明らかになった問題点や課題を列挙する。

実証実験は模擬環境で最低限の設備で実施したため、いくつかの問題点も発生したが、実際のシステム構築の際には、これらの問題の一部は比較的簡単に解決できると考えられる。

- SSL VPN 接続において、指定する URL が一部でも異なると（例えば、最後の［/］スラッシュの入力が抜けていた場合など）、正しい認証情報を用いても認証されない問題点がある。
- Java アプレットで VPN クライアントソフトウェアを自動的にダウンロードするが、低速なアクセス回線を利用している環境の場合、ソフトウェアのダウンロードに非常に時間がかかる問題がある。
- VPN クライアントソフトウェアのダウンロードやインストール時に、まれに動作が止まってしまい、動作しない場合がまれに発生する。
- SSL VPN 接続の一連の動作は、標準では英語での表記であった。
  日本語対応としてのカスタマイズなどが必要と考えられる。
- PIN とトークンコードを組み合わせてパスワードとすることに対して、分かりにくいとの指摘もある。
  検討事項として、ネットバンキングなどでも用いられる乱数表などで代用するか、又は USB キーに VPN 用のソフトウェアやパスワードを格納しておき、USB キーをパソコンに差して PIN 入力や指紋などでの認証が成功すると、自動的にパスワードを送出する方法や自動的に接続される方法などの検討も必要である。
- MyProdoc は、Microsoft Access を用いたシステムのため、利用者端末内部に一部のプログラムやデータを保持しなければならない。

利便性やセキュリティを考慮すると、これらのデータを持たないシステムとする必要がある。

- MyProdoc は、比較的小規模病院向けに作成された電子カルテシステムであるが、様々な患者情報や投薬情報などが管理できる。
  しかし、A-net では必要最小限の情報のみを管理し、利用者の権限（医師と患者の区別など）毎に、表示する情報のレベルを設定するなどの施策が求められる。

6 まとめ

今回の研究において、机上での検討を通じて、利便性の向上、セキュリティの確保、及び運用管理の向上に対する各種対策案が明らかとなった。

また、模擬環境における実証実験によって、セキュリティ対策の技術は進歩しており、利便性の向上を伴いながらも患者の個人情報保護に必要なセキュリティを確保するという要件も、対応が可能であると感じられてきた。実証実験においては、模擬環境における問題点や新たな課題なども明らかになってきており、利便性とセキュリティ確保のバランスを考慮しながら、求められる要件を慎重に検討し、次期 A-net のセキュリティ設計にあたらなければならない。

また、セキュリティ対策は、単純に装置の導入だけでは解決しきれない組織的な問題や物理的な問題、及び人的な問題も多分に存在するため、これらを組み合わせた総合的なセキュリティ対策が重要であると感じる。

更に A-net 本来の目的に照らし合わせると、利便性の向上策についても技術的な対策を実施するだけではなく、多数の患者の臨床情報が今後に役立つようにするためには、利用率の向上を図ることが重要であり、ソフト的な運用面を含めていくつもの課題があると再認識した。拠点病院やその他の利害関係者とも調整が必要な事項も多数存在するため、慎重な検討が必要である。

最後に、運用管理の向上については、資産やサービスの提供形態のみならず、要求される運用管理要素を慎重に検討し、それらを今後の運用管理者への要求事項として求めていかなければならない。