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。

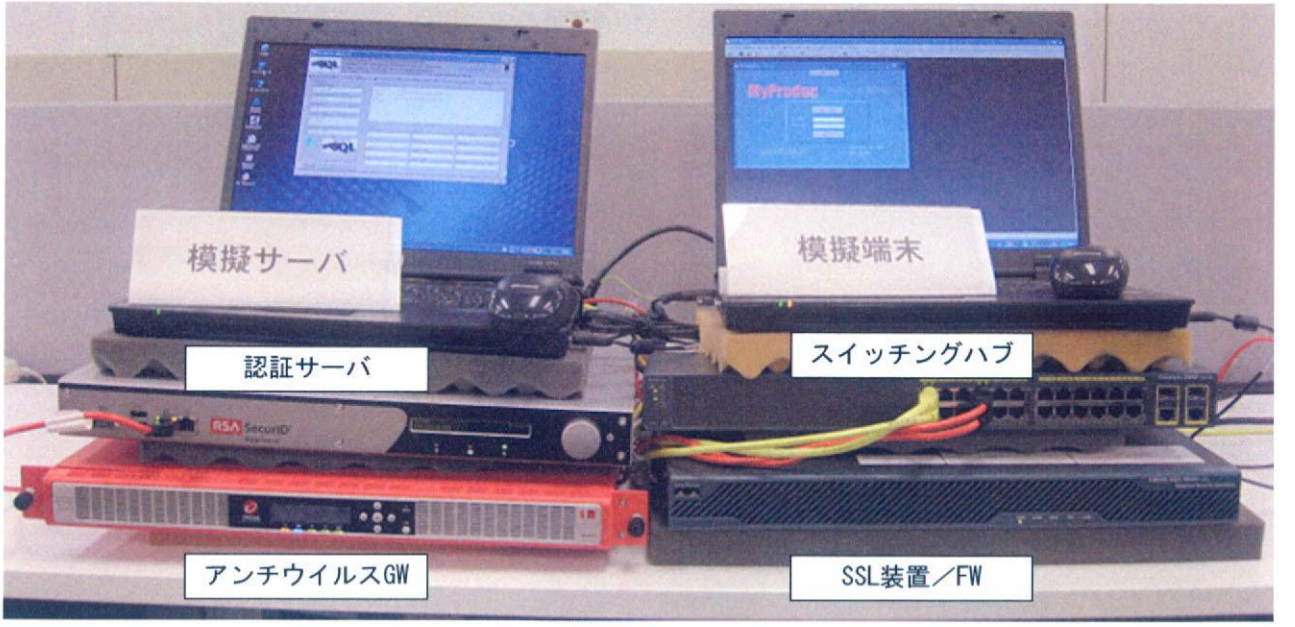
万が一のPINの漏えいや、ハードウェアトークン（トークンコードを生成する機器）の盗難が発生した場合でも、両方の要素が揃わないと認証が成功しないため、不正利用が困難である。

オ　スイッチングハブ

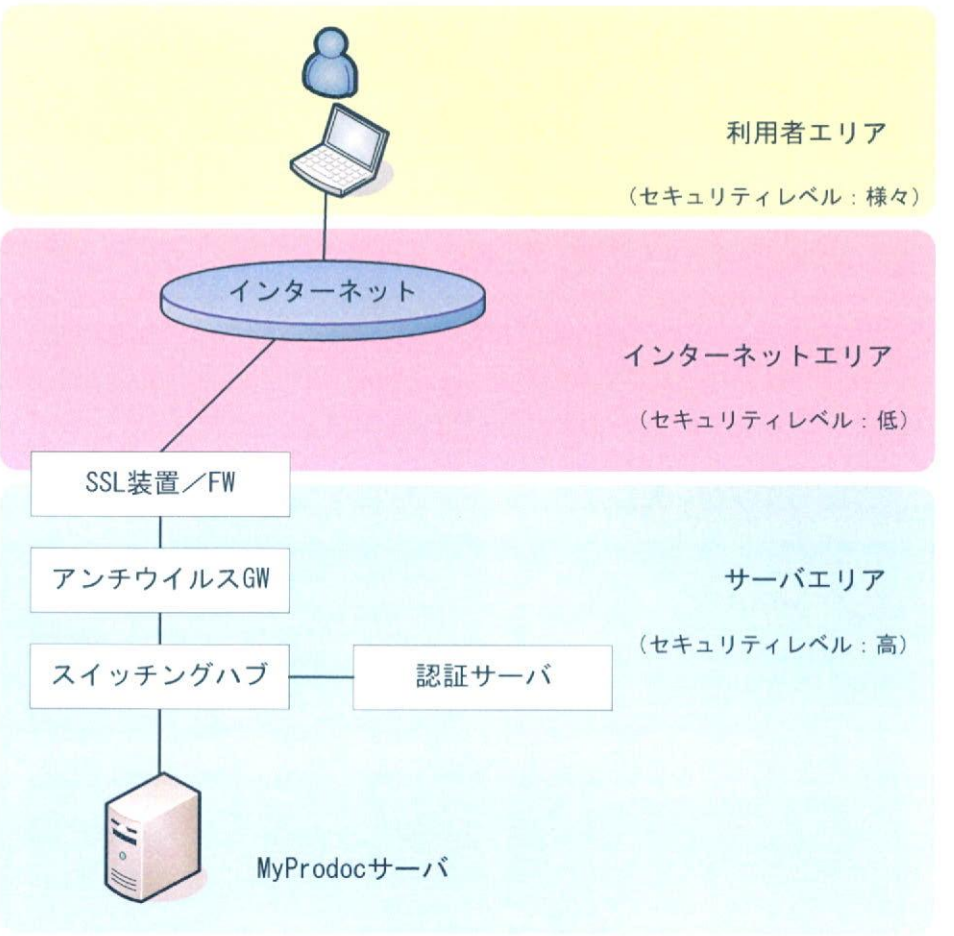
シスコシステムズ社　Catalyst2960-24TC。

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。

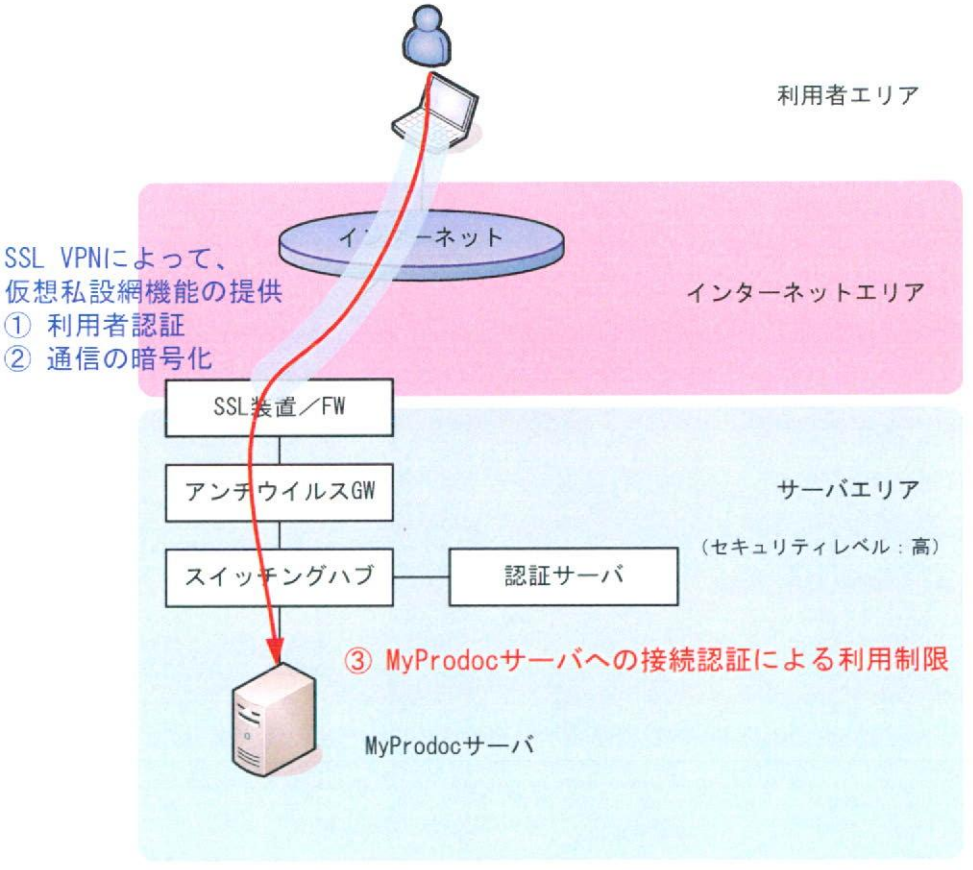
ア　利便性の向上

- 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

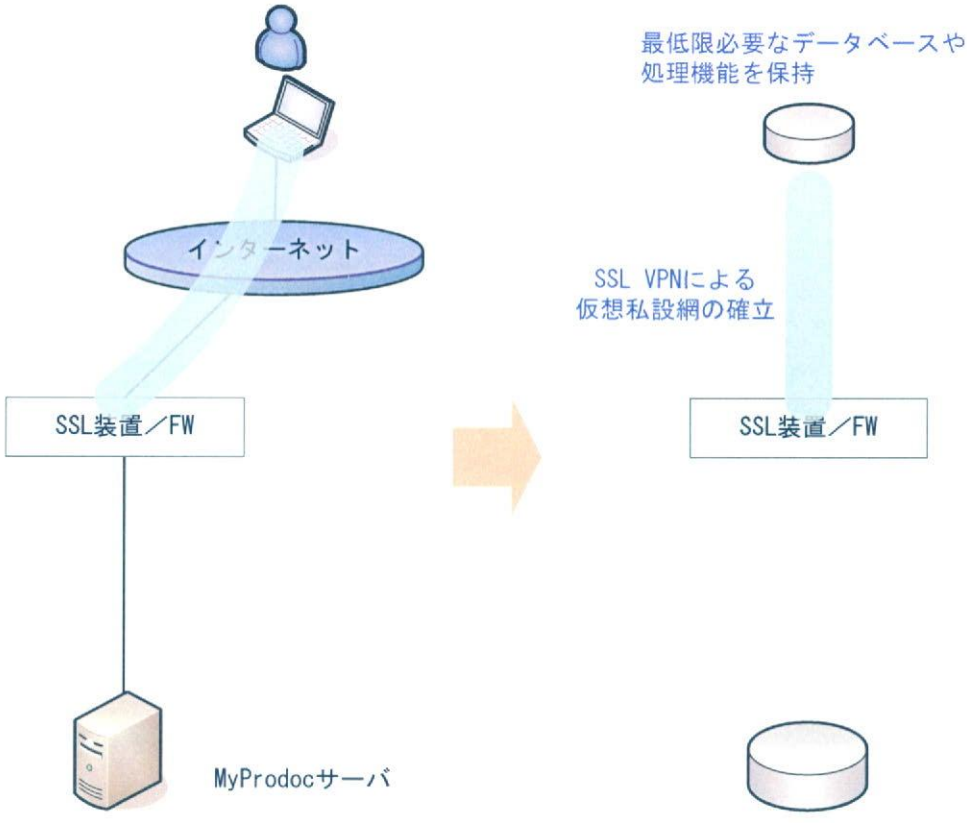


【図 5-3　模擬環境システム概要】

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

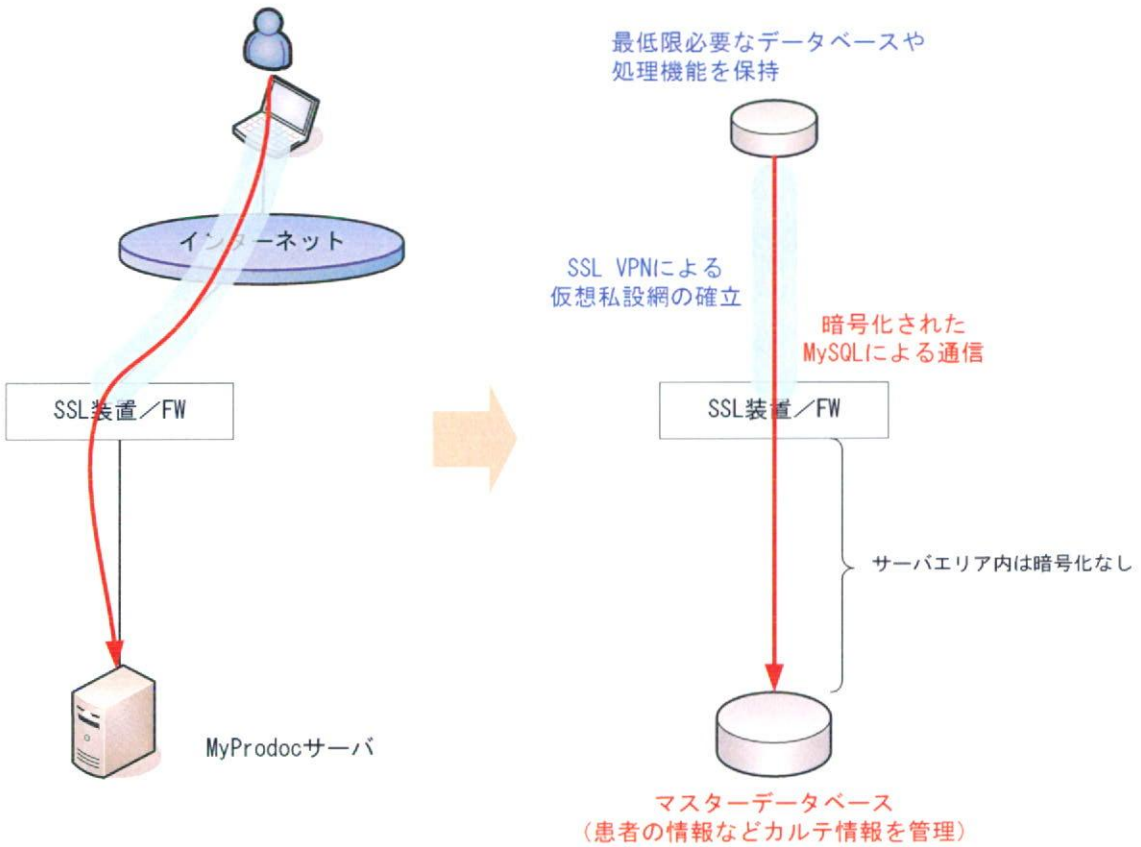
SSL VPN 確立に際しての利用者認証において、固定パスワードだけではなく、ワンタイムパスワードを用いて、PIN とトークンコードによる二要素認証を実施する。

【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】

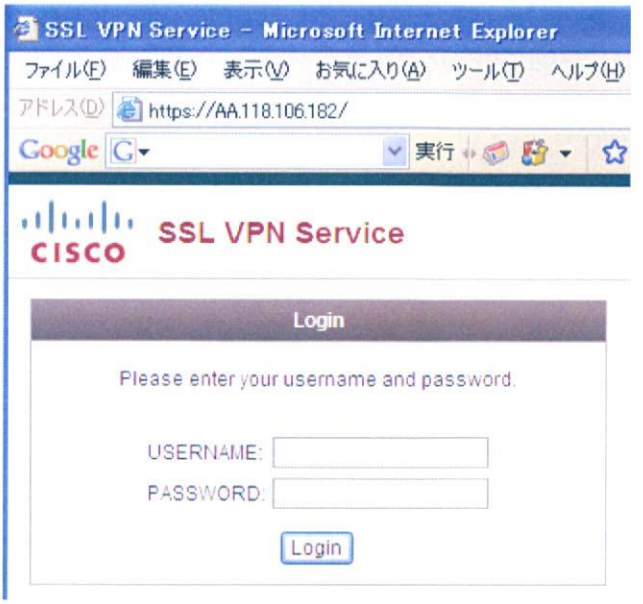
(5)　システム利用検証

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

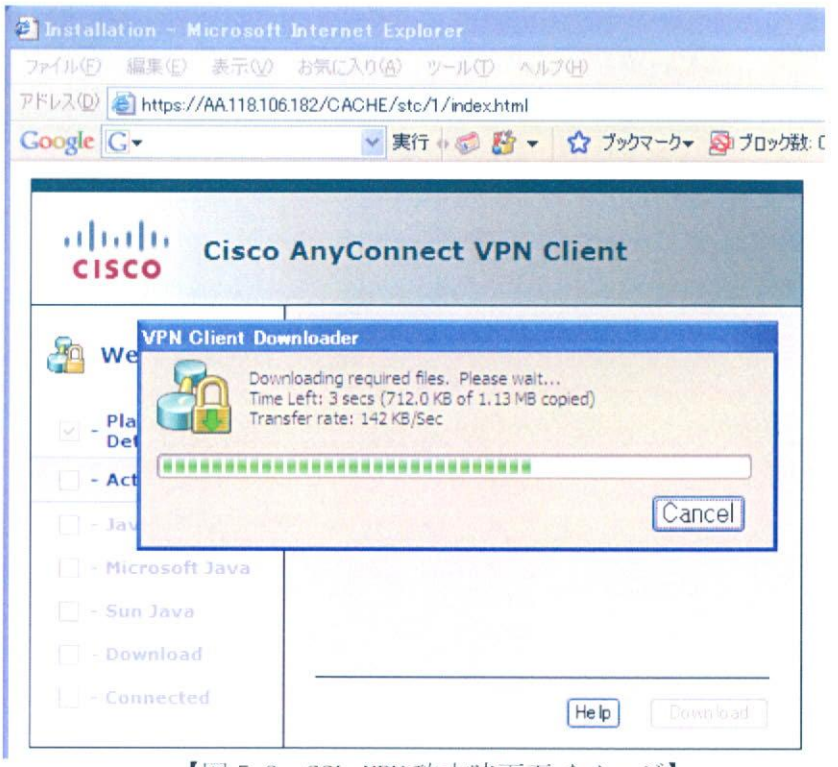
ットを「AA」で置き換えて表示）を入力するだけで SSL VPN 接続が操作できる点は、IT リテラシーに長けていない患者にとっても利用しやすい環境である。



【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。



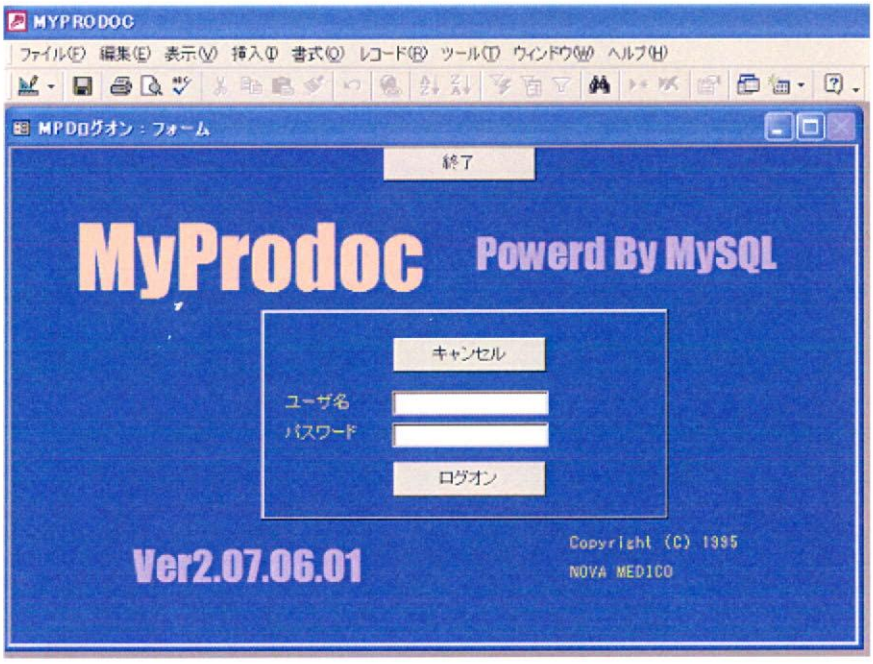
【図 5-8　SSL VPN 確立時画面イメージ】

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

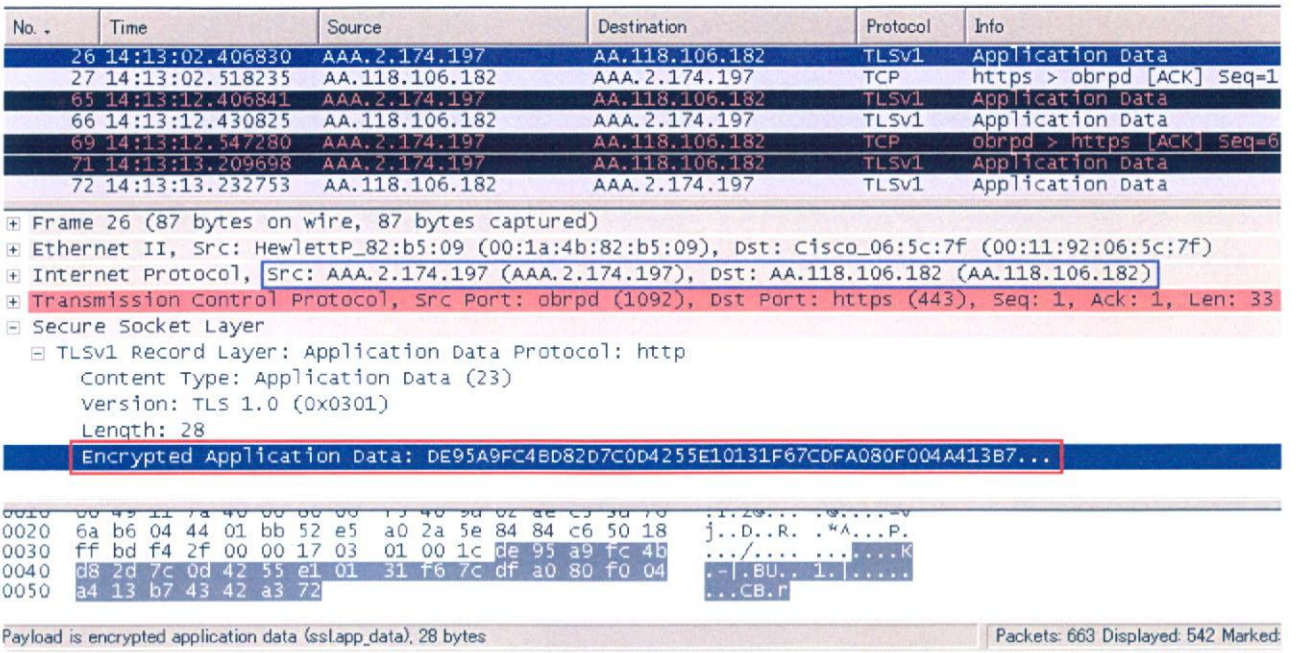
インターネットを経由した通信ではあるが、SSL VPN の確立後は、通信データの暗号化が行われている。

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）。

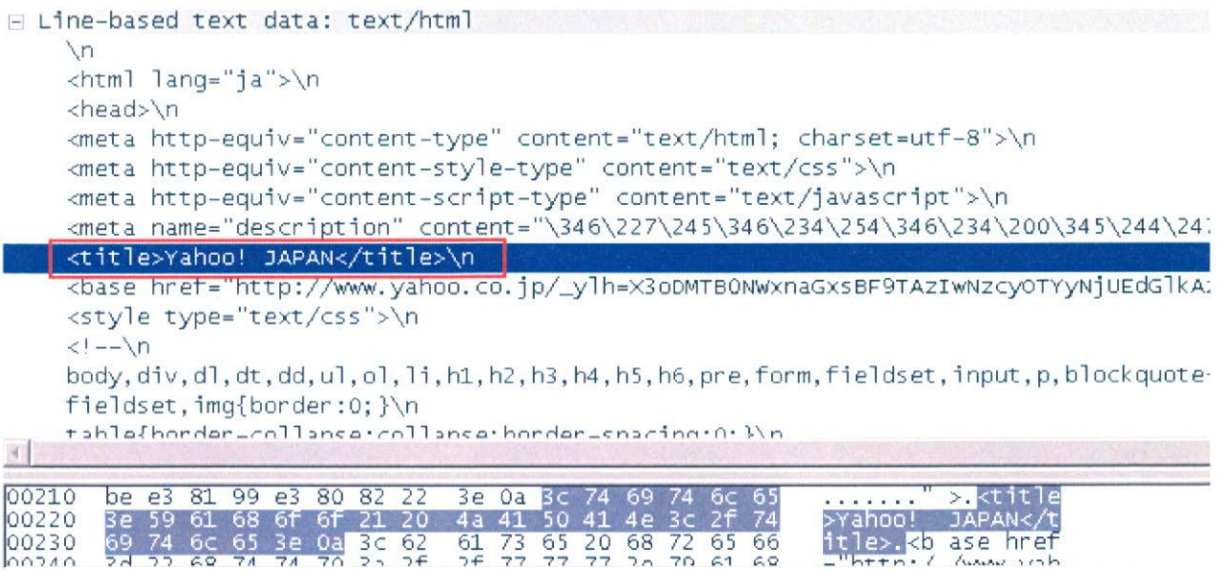
また、通信データの内容も暗号化されていることが分かる（赤線）。



【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。