200401082A

平成１６年度　厚生労働科学研究費補助金

医療技術評価総合研究事業

保険証認証情報の通信に関する実証的研究

平成１６年度　総括研究報告書

主任研究者　里村洋一

平成１７（２００５）年　４月

目　　次

厚生労働科学研究費補助金（医療技術評価総合研究事業）

保険証認証情報の通信に関する実証的研究

主任研究者　里村　洋一　　千葉大学名誉教授

共同研究者
本多正幸　長崎大学医学部教授
山本隆一　東京大学情報学環助教授
佐藤清司　NTTコムウエアー研究開発部研究員

保険証認証システムの実証実験のための諸問題を検討した。特に、システムのセキュリティーに関して、ポリシーの設定から、医療機関および保険者の運用周りにたるまでの、セキュリティー仕様とその実施要綱を検討した。また、個人情報保護の観点から、本システムの位置づけ、および個人情報の取り扱いについて検討し、実施要綱を作成した。また、保険証認証システムへの保険者の参加の条件を調査した。３箇所の診療所に保険証認証用端末を設置し、これらと認証センターおよび仮想の保険者の被保険者ＤＢを、ＶＰＮで結び、50件の仮想被保険者について複数回の認証実験を行った。

A. 研究目的

健康保険証書は、有価証券の一種であるにも関わらず、被保険者の受診時にその有効性を即時に認証する方法がない。そのため、保険証番号の誤記や、無効となった保険証による受診がトラブルの原因となっている。その数は、社会保険診療報酬支払い基金の平成１５年度報告で、全レセプト件数 48000 万のうち 336 万件（0.71%）、金額でも 797 億円（0.78%）とされている。これを全ての健康保険に当てはめると、年間約 600 万件を越すトラブルがあり、そのために失われている労力は1000億円を超えると推定される。こうした状況を改善するには、クレジットカードの様にリアルタイムにその有効性をチェックすることが必要である。われわれは、昨年までの研究によって、保険証認証のための通信規格やDBの設計を終え、実験用システムを構築した。また、ピアツウピアでこのシステムが設計通りに働くのを確認した。しかし、目的とする大規模なシステムを運用するためには、システムの設計ばかりでなく、実際の保険者（健康保険組合など）と医療機関（診療所や病院）における対応措置や実装上の問題点を洗い出し、システム運用のための課金方法を含めて、その解決の手法を検討しなければならない。そこで、少数の医療機関と保険者の協力を得た上で、実際の被保険者情報を利用して実験を行おうとした。

資料１　保険証認証システム構成
資料２　保険証認証情報交換規約

B．研究方法

B.1　情報の安全性について

本システムの実用的な運用のためには、インターネット上でのデータセキュリティーを確保する手法や、医療機関ならびに認証センターにおける情報システムの安全管理、さらに被保険者のデータ提供を安全に遂行するための運営手法が確立されなければならない。そこで、研究者らは、まず、次の３点に関して検討した。

1）　医療機関における被保険者データの安全管理と個人情報保護

2）　認証センターにおける被保険者データの安全管理と個人情報保護

3）　保険者のデータベースからの被保険者情報の漏洩防止

はじめに、機密性、完全性、可用性を考慮したセキュリティーポリシーを策定し、本システムにおけるリスクの分析を行った。①不正利用、改ざん、②アプリケーションの障害、③ホストハードウエアの処理能力不足、④ネットワークからの侵入、⑤自然災害による障害、などのリスクが考えられることから、それぞれの防護対策を設定した。すなわち、暗号化、ウイルス対策、システムロバシティーの強化、侵入検知、ＶＰＮ検疫制御、などのシステムやネットワーク上の安全管理に加えて、サーバー設置場所の警備、施錠、キーファイル管理、さらにユーザー教育までを必要な対策としてあげた。また、システムアベイラビリティーを向上させるためにシステムの冗長性確保、運転監視体制などを条件として設定した。具体的には、インターネットＶＰＮの使用、ユーザーの業務管理マニュアルの作成、キーカードによるユーザー認証などを行うこととした。保険者における管理としては、業務権限管理の厳格な運用、移送メディアのデータ廃棄、保険者情報の迅速な更新などを必要条件とした。医療機関では、業務権限管理、キーカードの管理などを条件とした。これらの検討の結果を整理して、認証センターの管理運用規則を作成した。

資料３　保険証認証サービス実証実験におけるセキュリティの検討

資料４　認証センターの維持運用管理規則

B2.　実証実験の実施

保険者認証サーバーおよび医療機関における認証端末を設置した上で、次のような作業を行うこととした。

1. 医療機関は被保険者が受診した際に、認証端末から被保険者の記号・番号を入力する。
2. 認証端末はＶＰＮ通信回線により、一旦、医療機関に与えられた機関認証情報を、認証センターに送り、医療機関が正当な参加者であることの認証を受けた上で、被保険者の記号番号を認証センターに送信する。
3. 被保険者の記号番号を受け取った認証センターは、これを保険証サーバーに送信する。
4. 認証センターから被保険者情報を受け取った保険証サーバーは、サーバーで管理されている被保険者情報を検索して、認証に必要な被保険者情報を、認証センターに送信する。
5. 認証センターは保険証サーバーから送られてきた被保険者情報に基づき、認証判定を行う。認証センターは認証判定結果を医療機関内の認証端末に送信する。
6. 保険者は、保険証サーバーの被保険者情報の更新を許される限り早いタイミングで行う。
7. 研究班は保険者と医療機関の通信が良好な状態に確保されるよう、常に双方から受診した情報をモニタリングし、その内容を記録する。

千葉市医師会に所属する医師が診療をしている診療所３箇所に認証端末を設置して、上記の要領で試験的な認証をおこなった。実験には実際の被保険者情報が使えなかったので。それぞれに異なった保険者に属し、保険情報の変更履歴を有する仮想被保険者５０例を設定して、認証サーバーに記録し、協力を受けた診療所において２ヶ月にわたって操り返し認証の作業を行った。

資料５　認証実験スケジュール

Ｂ３．医療機関のセットアップ

このシステムが対象とする医療機関は多様である。一般の診療所や歯科診療所に始まり、すべての規模の病院、調剤薬局など本格的な運用が始めれば、３０万に近い医療関連機関が参加することになろう。それだけに医療機関における認証機器のあり方も一様ではない。各種のいわゆるレセコンに組み込む場合、病院情報システムの一機能として導入することなどが想定される。また、医療機関がなんらのＩＴ機器を持っていない場合もあり、独立した認証端末が必要である。これらのすべてに対応するのは実験段階では困難であるので、今回の実験には、ノートＰＣを利用した認証端末を用意した。これに二次元バーコードの読み取り装置とＱＲコードプリンターを加えて各診療所の窓口に設置した。

資料６　診療所における認証端末とその画面

Ｂ４．ＱＲコードの利用

保険証情報（記号、番号）の入力手法には多様性が求められる。保険証は従来からの家族単位の印刷物の場合から、個人別のプラスチックカード、ＩＣカード、磁気カードなどさまざまであるからである。記号番号の入力をＰＣのキーボードによって入力する場合の他に、磁気カードリーダー、ＩＣカードリーダー、ＯＣＲなどの利用が考えられる。しかし、多様な保険証の記録方式に対応して、すべての入力機器を準備するのは経済的にも操作の面からも好ましくない。保険証の様式の統一が望まれるところであるが、実現は容易でなかろう。そこで、システムを利用する医療機関の場で、簡便な入力を実現するため、マトリックス方二次元シンボルのひとつとして普及しつつあるＱＲコードを使うこととした。ＱＲコードは情報量によって最小３ｍｍ角まで小さくすることができ、保険証のような小さな紙面にも貼付可能である。また、保険証に貼らずとも、診察券や診療録の表紙などに貼って使用することも可能で、本システムの脇役として好適だと思われる。

資料７　実験に使用した仮想保険証（ＱＲコードつき）

Ｂ５．課金モデルについて

本システムを全国規模で運用するには、医療機関の端末や保険者のサーバーの経費の他に、年間30億円程度の認証センター運用経費や通信料が必要となる。これらをまかなう方法はさまざま考えられるが、システムの独立した運用を前提とするならば、アクセス数に応じた課金制度も有望な手法である。そこで、被保険者一件あたりのアクセス料を設定した場合のモデルを作成した。

資料８　課金モデル

Ｃ．結果

Ｃ１．情報の安全性について

ＶＰＮによる通信が実験期間中に障害を受けたり、情報の漏洩を起こした形跡は見られなかった。ただし、意図的な侵入は試みていない。

Ｃ２．　認証の精度

３箇所の診療所において、それぞれ、２４４、１７７，２０４件、合計６２５件の認証を６回に分けて行った。内、有効４２６、期限切れ１２２、記号番号誤り６３、保険者誤り１４件を設定してあったが、いずれも正しく回

答された。これらのうち、それぞれの診療所で４１、７２、２０件を一括認証（一旦、ＰＣに収録した記号番号のリストに従って一括送信し、一回の通信でまとめて回答を得る方式）した。システム設計上や実装上のエラーは検出されなかった。

Ｃ３．ユーザーからの要望

認証結果は意図されたシナリオの内容を正しく反映したものであったが、いくつかの運用上の問題点が明瞭になった。

１．診療所の受付に専用端末を置くスペースが足りない。
２．画面の認証ウインドウが小さくて見にくい。（対応済み）
３．毎回手入力での認証はわずらわしい。
４．認証の履歴を見たい場合がある。
５．医療機関側で保険証にＱＲコードを貼り付けてもよいのか。

しかし、ＱＲコードの使用によって利便性が高く、おおむね好評であった。ＱＲコードは、保険証のほかにも診察券やカルテの表紙に貼り付けることで、保険証を持参しない場合でも認証が楽にできること、どのような保険証にも対応できることなどの点で、評価が高かった。

Ｃ４．保険者の協力

実験の目的は、実際の被保険者情報を使うことであったので、実験に先立って以下のような作業について保険者の協力を求めた。

１） 研究グループは、保険者が指定する場所に保険証サーバーを設置し、通信環境を構築する保険者に対して、保険証サーバーに被保険者情報を移送するためのフォーマットを提示する。
２） 保険者は上記フォーマットにしたがって記録された被保険者情報を、保険証サーバーに読み込み、データベースに記録するプログラムを開発する。
３） 保険者側の責任者立会いの下、被保険者情報の抽出と保険証サーバーへの初期ロードを行う認証センターの管理と、それによるデータの集計・解析を行う。
４） 上記解析結果を解析し、システムの問題点、運営上の課題などを検討する。
５） 個人情報保護法の諸規定に準拠し、さらに厚生労働省による「医療・介護関係事業者における個人情報の適切な取り扱いに関するガイドライン」に従った認証センターのセキュリティー管理を行う。
６） 研究者側は、システムの運用に問題が生じたときに直ちに対応できる体勢をとる。

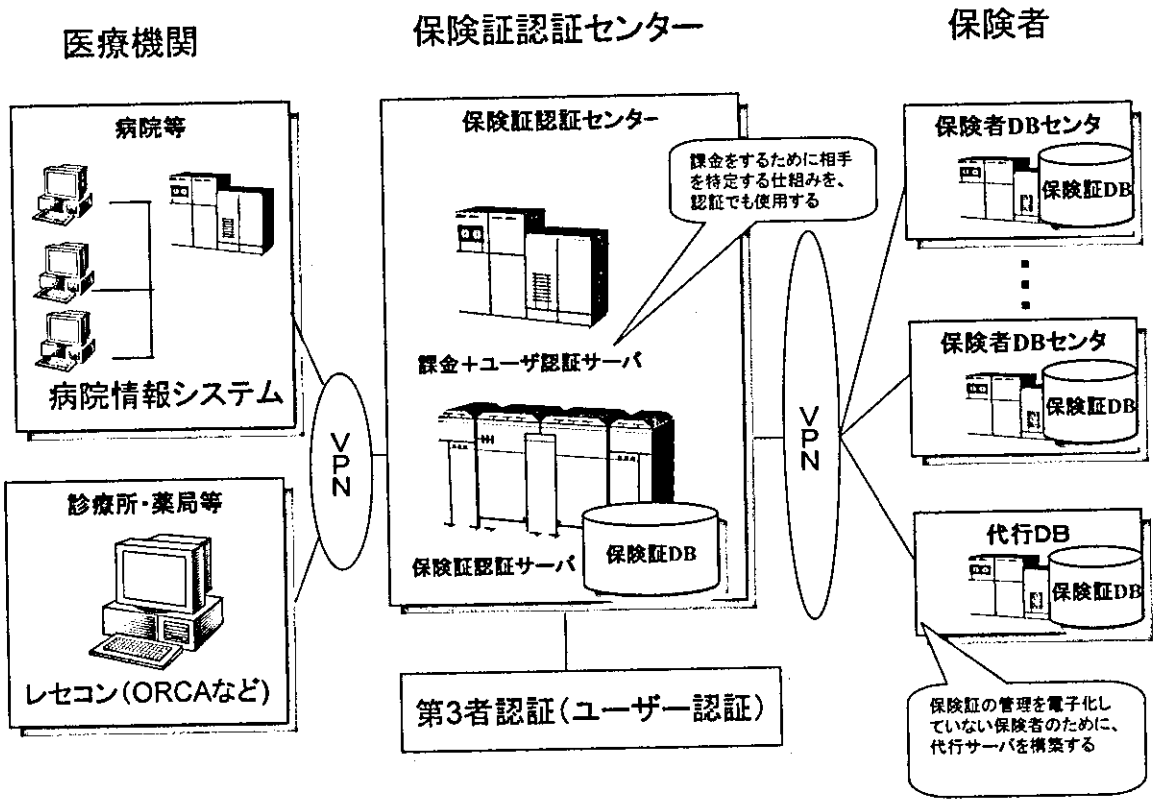
実験の計画に当たって、いくつかの保険組合と交渉し、実験の意義について理解が得られたが、最終的には、本年度の研究期間に被保険者情報を提供してもらえなかった。理由は以下のようなものである。

１）被保険者情報の更新が、必ずしもリアルタイムに認証できるようなタイミングで行われていないので、結果に責任が持てない。
２）一部の保険者（特に国保）は被保険者の情報把握を能動的に行っていない（被保険者の申告による）ため、正確な情報が提供できない。
３）個人情報保護法が施行されて、情報の漏洩に関心が高まっている状態で危険は冒せない。
４）実験とはいえ組織を挙げての協力体制が必要であり、社内の説得が容易でない。

Ｄ．結論

システムの完全性はかなり高いことが証明された。しかしながら、全国の２０万を超える医療機関や薬局を対象とする場合には、ＶＰＮのような固定したユーザー間を想定した方式には疑問もあり、ＰＫＩの採用が必要となるかもしれない。

当初の目的であった。医療機関における実用的な認証の実験は成就しなかった。保険者団体の協力を得るには、前記の問題点を解決しなければならないが、研究班の私的な活動では限りがあり、何らかの公的な支援が必要であることを痛感した。また、個人情報保護法の施行に伴って、保険者の個人情報保護に関する意識が高まっており、受診時に必要とされる被保険者情報の医療機関への提供に関しても、過敏となっている嫌いがある。
平成１４年１２月に保険局から出された各健康保険組合宛の通知文書「健康保険組合における個人情報保護の徹底について」においても、保険組合における個人情報の管理の徹底を指示しているが、情報提供の範囲に関してはなんら言及していない。このことが本研究のような情報提供を核とするシステムへの協力を躊躇させていることは想像に難くない。
今後、実用的なシステムの導入に際しては、行政上の何らかの措置が必要であると思われる。



資料1　保険証認証システム構成

資料2.　J－MIXによる保険証情報構成

					用区間(凡例 ●:必須エレメント ○:任意エレメント －:不要エレメン					
XMLエレメント名	説明	データ型	参照表	繰り返し	個別(一括)認証要	個別(一括)認証結	RT保険者要求	RT保険者結果	事前蓄積要求	事前蓄積結果
<jmixHic:CertificationModuleTop>	保険証認証グループトップレベル				●	●	●	●	●	●
<jmixHic:CertificationModule>	保険証認証情報グループ				●	●	●	●	●	●
(attr)sn	Moduleを繰り返す場合の通番(整数)	数値型			○	○	○	○	●	●
<jmixHic:HealthInsuredProvider.Symbol>	保険者の保険者番号	文字列型			●	●	●	●	●	●
<jmixHic:HealthInsuredProvider.Name>	保険者の名称	文字列型			－	●	－	●	●	－
<jmixHic:InsuranceProvider.WholeAddress>	保険者の完全な住所表記	文字列型			－	●	－	●	●	－
<jmixHic:HealthInsuredProvider.PhoneNumber>	保険者の電話番号。半角数字と半角ハイフンだけから構成する	文字列型			－	●	－	●	●	－
<jmixHic:HealthInsuredPerson.Symbol>	被保険者の記号	文字列型			●	●	●	●	●	●
<jmixHic:HealthInsuredPerson.Number>	被保険者の番号	文字列型			●	●	●	●	●	●
<jmixHic:HealthInsuranceCertificate.IssuedDate>	保険証交付日付	日時型			－	●	－	●	●	●
<jmixHic:HealthInsuranceCertificate.ExpirationD>	保険証の有効期限(日付)	日時型			－	●	－	●	●	●
<jmixHic:HealthInsuredPerson.WholeName>	被保険者の氏名の完全表記	文字列型			－	●	－	●	●	－
<jmixHic:HealthInsuredPerson.WholeAddress>	被保険者の完全な住所表記	文字列型			－	●	－	●	●	－
<jmixHic:HealthInsuredPerson.Sex>	被保険者の性別	区分型	T0001		－	●	－	●	●	－
<jmixHic:HealthInsuredPerson.Birthday>	被保険者の生年月日	日時型			－	●	－	●	●	－
<jmixHic:HealthInsuredPerson.PhoneNumber>	被保険者の連絡先電話番号。半角数字と半角ハイフンだけから構成する	文字列型			－	●	－	●	●	－
<jmixHic:WorkInfo.Name>	事業所の名称	文字列型			－	●	－	●	●	－
<jmixHic:WorkInfo.WholeAddress>	事業所の完全な住所表記で空白を含まない文字列。英数字は半角	文字列型			－	●	－	●	●	－
<jmixHic:WorkInfo.PhoneNumber>	事業所の電話番号。半角数字と半角ハイフンだけから構成する。	文字列型			－	●	－	●	●	－
<jmixHic:HealthInsuredFamilyInfo>	被扶養者情報グループ				－	○	－	○	○	－
<jmixHic:HealthInsuredFamily.WholeName>	被扶養者の姓と名を全角空白1文字でつないだ氏名の完全表記	文字列型			－	○	－	○	○	－
<jmixHic:HealthInsuredFamily.Sex>	被扶養者の性別	区分型	T0001		－	○	－	○	○	－
<jmixHic:HealthInsuredFamily.Birthday>	被扶養者の生年月日	日時型			－	○	－	○	○	－
<jmixHic:HealthInsuredFamily.Relationship>	被扶養者(家族等)の続柄(夫、長男、隣家知人等)	文字列型			－	○	－	○	○	－
<jmixHic:CertificationId>	個々の認証を識別する番号	文字列型			－	●	－	－	－	－
<jmixHic:CertificationCode>	認証結果コード	文字列型			－	●	－	－	－	－
<jmixHic:CertificationMessage>	認証結果を説明する文章	文字列型			－	●	－	－	－	－
<jmixHic:CertificationTargetDate>	認証対象年月日	日時型			●	●	●	－	－	－
<jmixHic:HealthInsuredField>	保険分野(予備)。民間保険や海外保険などに拡張した場合に識別に使用	文字列型			－	－	－	－	－	－
<jmixHic:Individuality>	個人識別情報(予備)。一人1カード化などの場合に個人を特定する情報に	文字列型			－	－	－	－	－	－
<jmixHic:StoreDataIssuedDate>	事前蓄積情報効力発生日	日時型			－	－	－	－	●	●
<jmixHic:StoreResultCode>	保険者から認証センタへ保険証情報を事前蓄積依頼した結果	文字列型			－	－	－	－	－	●

資料３

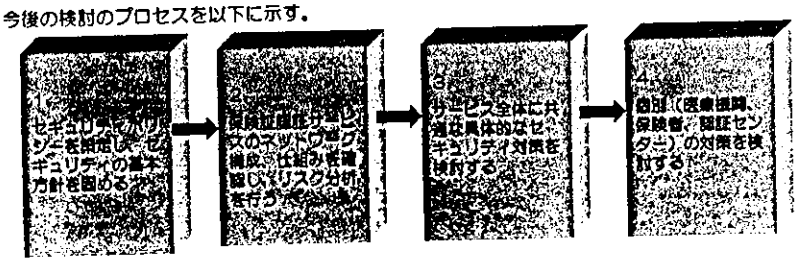
保険証認証サービス実証実験における セキュリティの検討

セキュリティ検討の方針とプロセス

保険証認証サービスの実証実験（以降、実証実験）を行うにあたり、考慮すべきセキュリティについて検討する。

実証実験で取り扱う健康保険証の記載事項には、氏名、住所など多くの個人情報が含まれ、漏洩等の問題が起きた場合の社会的影響は大きい。よって実証実験では高レベルのセキュリティ対策が必要であることは明白である。そこで実証実験の安全な運用のためにセキュリティ対策の原則である機密性、完全性、可用性を考慮したセキュリティポリシーを策定する。そのポリシーを以降のセキュリティ対策検討の基本的な方針とする。

今後の検討のプロセスを以下に示す。



目次

1．セキュリティポリシーの策定

1－1．セキュリティポリシーの策定

機密性、完全性、可用性を考慮し、保険証認証サービス実証実験のセキュリティポリシーを、以下に定める。これらのセキュリティポリシーを基本方針として具体的なセキュリティ対策を立てる。

ポリシーの対象範囲

保険証認証サービスを利用する全員、保険証認証サービスに関わるすべての情報

守るべき情報資産

保険証認証サービスに関わるすべての情報資産

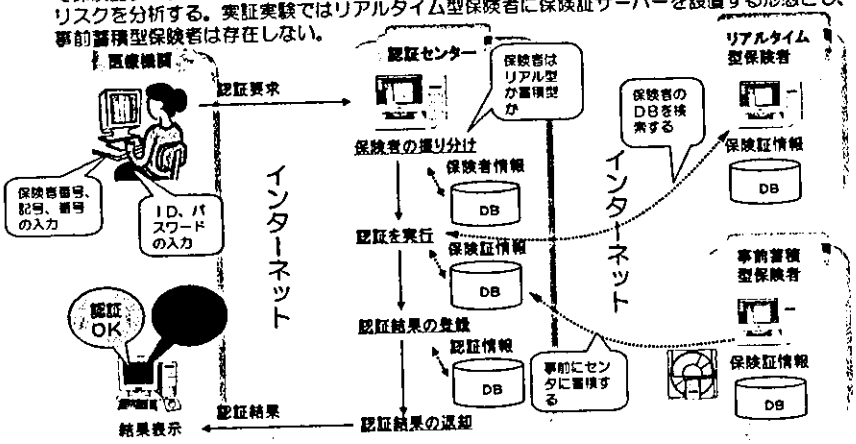
基本方針

1．*ネットワーク経路において送受信データの機密性を保つこと*
2．*ネットワークやサービスへの接続時に本人確認を徹底すること*
3．*情報が必要なときにいつでも使用できること*
4．*セキュリティ関連の法令その他の規範、規制要求事項を遵守すること*

2．保険証認証サービスの構成

2－1．保険証認証業務の流れ

医療機関が保険証認証を行って結果が画面に表示されるまでの流れは以下のとおりである。保険証認証サービスはＷｅｂサービスを用いるアプリケーションであり、インターネット回線を使って保険証データを医療機関、認証センター、保険者の間でやり取りしている。この仕組みに潜むリスクを分析する。実証実験ではリアルタイム型保険者に保険証サーバーを設置する形態とし、事前蓄積型保険者は存在しない。



4

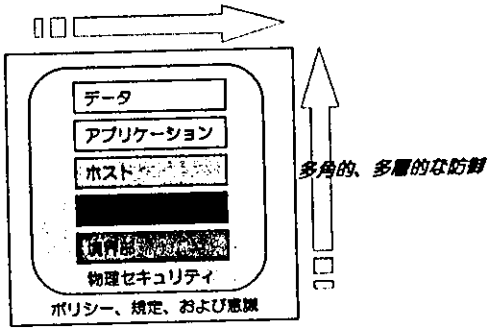
3．リスクの分析

3－1．マルチレイヤ・アプローチ（多層防御）によるリスクの分析

保険証認証サービスのシステム構成からサービス全体に共通のリスクをマルチレイヤ・アプローチの考え方を参考にして分析する。

マルチレイヤ・アプローチ（多層防御）はウィルスソフトやファイアウォールだけでシステムを防御するのではなく、マクロな視点でデータやアプリケーション、ホスト、物理セキュリティなど、さまざまな層でセキュリティ対策を施す防御方法である。1つの層の対策は、その前の層の対策が破られたことを前提として構築、多角的、多層的な防御を行うという考えで構築される。

完全無欠のセキュリティ技術は無いが、より安全な情報システムのセキュリティには、マルチレイヤ・アプローチによる包括的なセキュリティ対策を採用することがベストだと言われている。

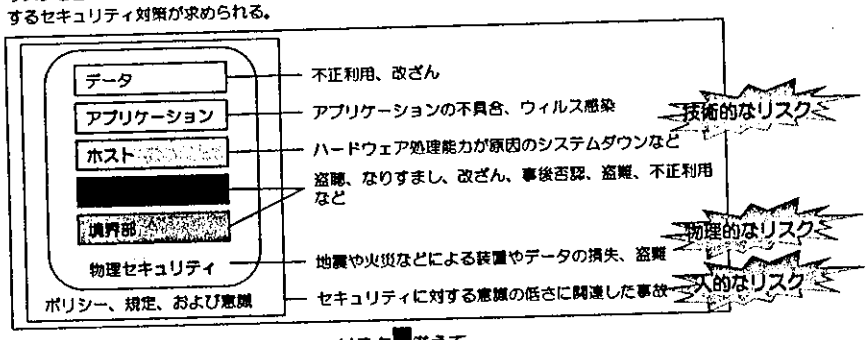


5

3．リスクの分析

3－1－1．実証実験のリスクを分析

実証実験のシステム構成から、ネットワークおよびサービスを利用する保険者、医療機関、認証センターに共通なリスクを各レイヤごとに抽出する。各レイヤで想定されるリスクは以下のとおりである。まずはこれらのリスクに対するセキュリティ対策が求められる。



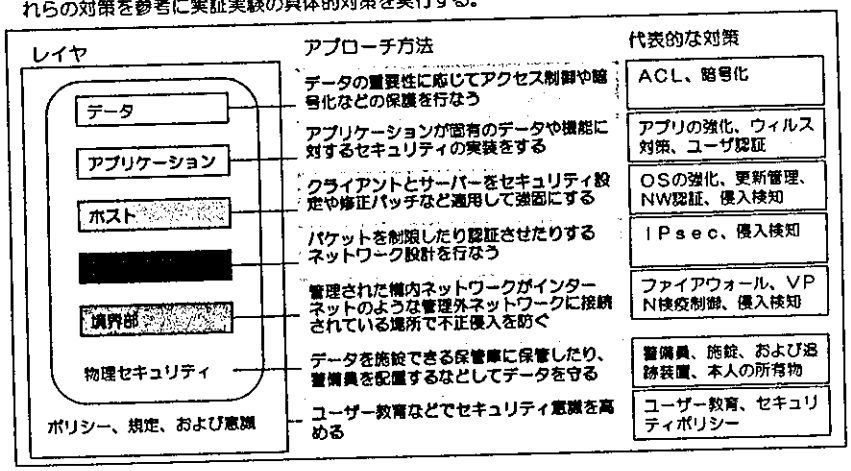
リスクに備えて

サービス内容に即したセキュリティ対策が必要

3．リスクの分析

3－1－2．対策へのアプローチ

一般的なシステムで実施・検討されている代表的なセキュリティ対策をレイヤごとに示す。これらの対策を参考に実証実験の具体的対策を実行する。



3．リスクの分析

3－2．アベイラビリティの向上

アベイラビリティ（＝可用性）はシステムのこわれにくさ、障害の発生しにくさを意味し、滅多に障害が発生せずいつでも安心して使えるシステムがアベイラビリティの高いシステムとなる。保険証認証サービスも信頼性を高めるために、システムダウン等の障害に備え、アベイラビリティの高いサービスを目指す。

3－2－1．アベイラビリティの阻害要因

実証実験のシステム構成から想定される、ネットワークおよびサービスを利用する保険者、医療機関、認証センターに共通なアベイラビリティ向上の阻害要因抽出する。

	阻害要因
1	認証サーバーの処理能力が低く、システムダウンやタイムアウトを起こしてしまう
2	ネットワークの容量が足りないために応答に時間がかかる
3	何らかの原因でデータが失われてしまう
4	何らかの原因で設備故障を起こしてしまう
5	悪意ある攻撃（DoS、ワームなど）によりシステムダウンを起こしてしまう
6	ネットワーク経路が切断されてしまう

8

3．リスクの分析

3－2－2．アベイラビリティ向上のための代表的な対策と効果の確認

アベイラビリティ向上のための対策を列挙する。（3－2－1項で抽出した阻害要因に対応した対策が網羅されていることがわかる）これらの対策を参考に実証実験の具体的対策を実行する。

	代表的なアベイラビリティ向上対策
1	高負荷（高トラヒック）状態でも正常に動作できるスペックの設備を整える
2	データ、サーバ、ネットワークなどを対象に万一の事故に対してバックアップを行う
3	万一の事故に備え、冗長構成をとる
4	バックアップデータやバックアップのシステムなどもリハーサルを実施して緊急時には正常に動作することを確認しておく
5	サーバやルータなどでファームウェアのバージョンアップやセキュリティパッチの適用が今後発生する可能性の高い機器は、バックアップ用の機器で動作検証をしてから適用する
6	DoS攻撃や突発的に増加するワームなどへの対策
7	火災や地震といった大規模な災害の発生に備えるディザスタ・リカバリ対策を行う
8	システム全体の監視、管理体制を整える

	阻害要因
1	実証実験のトラヒック量に対して、認証センターの処理能力が低く（スペックが低い）、システムダウンやタイムアウトを起こしてしまう
2	ネットワークの容量が足りないために応答に時間がかかる
3	何らかの原因でデータが失われてしまう
4	何らかの原因で設備故障を起こしてしまう
5	悪意ある攻撃によるシステムダウン
6	ネットワーク経路が切断されてしまう

これらの対策の中から実証実験で必須な対策を実施

9

4．リスクに備えた対策を立てる

4－1．対策の立案

セキュリティポリシーを前提として、リスクに備えた保険証認証サービス実証実験のセキュリティ対策を以下のように立てる。

≪リスクに備える対策≫

【その1】インターネットVPNを使う
【その2】ユーザーの業務権限の範囲を決める
【その3】ログイン時に本人認証を行う
【その4】想定される処理性能を満たす設備を整える
【その5】その他

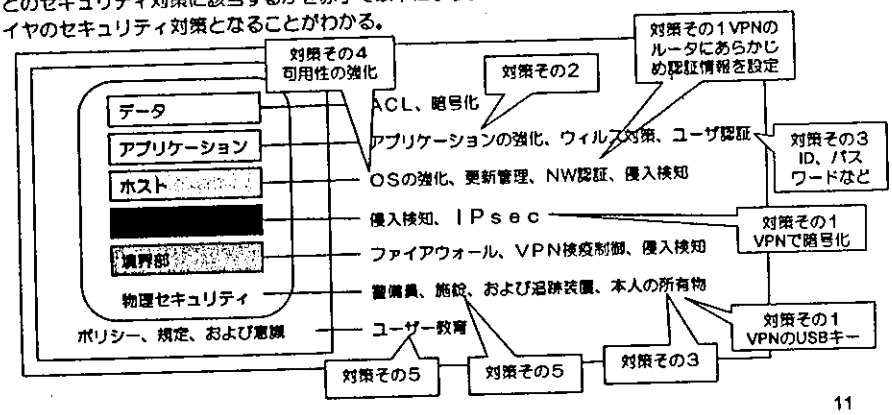
（＊）医療機関、保険者、保険証認証センター個々の立場に立ったリスク分析とセキュリティ対策については6項で考察する。

10

4．リスクに備えた対策を立てる

4－2．効果の確認

＜参考＞
4－1項で立てた保険証認証サービス実証実験のセキュリティ対策が、3－1－2項のどのレイヤのどのセキュリティ対策に該当するかを赤字で以下に示す。インターネットVPNを使用することで複数レイヤのセキュリティ対策となることがわかる。

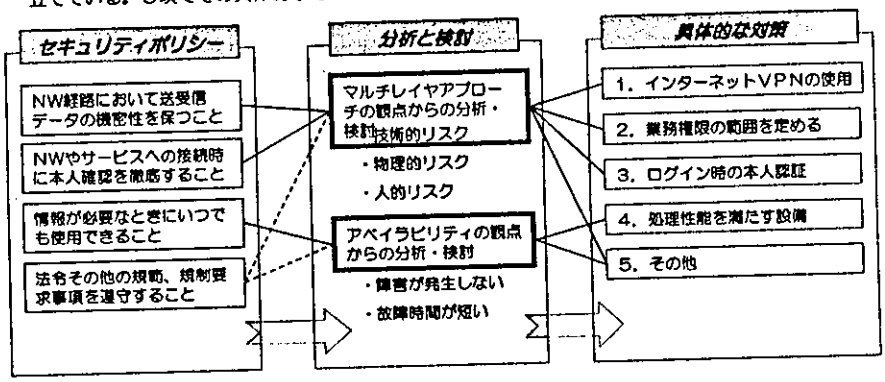


11

4．リスクに備えた対策を立てる

4－3．対策立案までのまとめ

具体的対策立案までの内容をまとめると以下の通りである。最初に策定したセキュリティポリシーを基本方針として実証実験のリスクを分析し、対策の検討を行い、実証実験における具体的な対策を立てている。5項でその具体的な対策の効果を検討する。



12

5．リスクに備える対策（共通対策）

5．リスクに備える対策（共通対策）

対策その１　インターネットVPNを使う

（１）VPNの仕組み
①接続する２点間に暗号化や認証機能を持つ論理的な仮想トンネル（ＩＰパケットの内容をVPN用のプロトコルでカプセル化）を構築する。
②データを仮想トンネル内に流すことでセキュリティを確保する。
③VPN通信機器間は暗号化してデータを送信する。

★対策の効果
・データが途中で盗聴されても盗聴者は暗号を解読しない限りデータの中身を見ることができない。
・暗号化の際に認証を行うため第３者によるなりすましも防ぐことができる。
・接続拠点／経路が特定されるとともに利用者も特定される
・USBキーは本人認証の手段としても利用できる

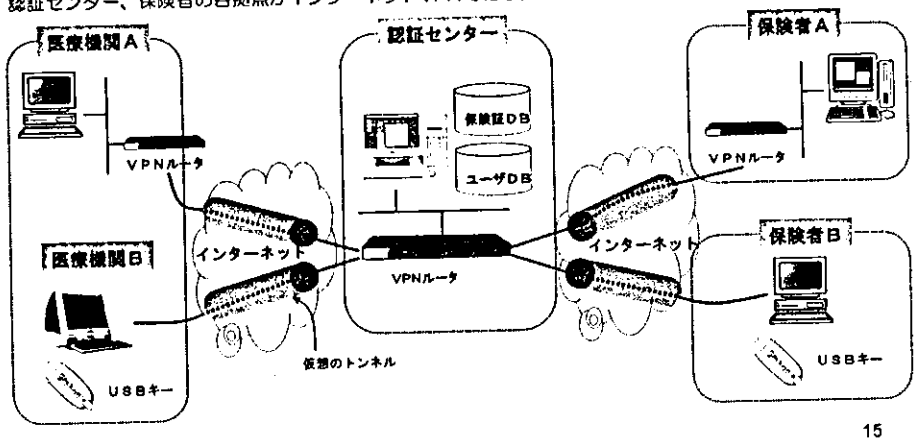
（参考）構内環境での実験はＮＴＴ東日本のインターネットVPNサービスである「Ephelio-VPN」のIPsecVPNイージーキットを使用し、動作を確認した。

14

5．リスクに備える対策（共通対策）

対策その１　インターネットVPNを使用したネットワーク構成

インターネットVPNを使用した保険証認証サービスのネットワーク構成を以下に示す。医療機関、認証センター、保険者の各拠点がインターネットVPNで結ばれる。



15

5．リスクに備える対策（共通対策）

対策その2　ユーザーの業務権限の範囲を決める

（1）アクセスするユーザーの役割りを以下に示す。

業務	分類	役割り
システム	システム管理者	ＩＤ管理など各種メンテナンス作業やバックアップ作業を行う
業務	業務責任者	業務運用管理を行う
運用	運用管理責任者	サーバーの監視などサービス運用管理を行う
	媒体管理責任者	保険証情報蓄積用媒体、バックアップ媒体、ドキュメント類などの管理を行う

（2）ユーザーの役割りによって、それぞれの実施可能な業務を限定する
ユーザーＩＤにより、実施可能な業務を管理する。
（詳細は個別のセキュリティで記述）

★対策の効果
利用する権利の枠を超えたデータの不正利用を防ぐ手段となる。

16

5．リスクに備える対策（共通対策）

対策その3　本人認証を行う

（1）認証センターへの接続時やアプリケーション起動時など、いくつかの場面でユーザー認証を行う。

	認証を行う場面	セキュリティ対策
（1）	端末へのログイン	・USBキーやＩＣカードなど、本人を特定できる所有物を使用する ・VPNを利用することで操作可能な端末を限定する
（2）	センターへの接続	・VPNを利用することで認証センターへの接続を制限する
（3）	保険証認証サービスへのログイン	・ユーザーＩＤ、パスワードを認証センターで管理する ・ユーザーＩＤの業務権限により業務メニューを出し分け、操作するユーザーを限定する
（4）	認証業務へのログイン	・ユーザーＩＤ、パスワードを認証センターで管理する ・業務権限をもつユーザーだけが業務を実施できる

★対策の効果
なりすましやデータの改ざんを防ぐ手段となる。

17

5．リスクに備える対策（共通対策）

対策その４　想定される処理性能を満たす設備を整える

（１）１日のトラヒック量やピーク時のトラヒック量を計算し、十分に稼動を維持できる設備を備える。全医療機関がこのサービスを利用した場合の試算結果（H16.3試算済み）を参考に実証実験で想定されるトラヒック量と必要な処理能力について試算する。

■全医療機関（約218,000）が参加した場合を想定

受診件数	12.7億受診／年
	508万件／日＊１
ピーク時	254万件／時間＊３
処理能力（絶対量）	706件／秒
処理能力（必要量）	1412件／秒*4
サーバ通信量	12Mbyte／秒＊５
下位プロセス・暗号化を考慮した通信容量	22Mbyte／秒＊６

※１　１レセプトあたり１受診として
※２　１年あたり250診療日として
※３　ピーク時１時間に１日の受診の1/2が集中するとして
※４　処理能力必要量は絶対量の2倍として
※５　保険証情報（被扶養者2名を想定）を記述し、1件の照会に対して通信を行った場合の概算通信量・・・8Kbite／件より
※６　サーバ通信量の2倍を見込む

■実証実験における試算

参加する医療機関数：10ヶ所　保険者数：2

ピーク時　10件程度／時間

サーバ通信量や下位プロセス・暗号化を考慮した通信容量は上記と変わらない。

★実証実験では想定量に従った設備を整える

18

5．リスクに備える対策（共通対策）

対策その４（つづき）

３－２－２項で列挙したアベイラビリティ向上のための対策について、実証実験でどこまで実現できるかを検討する。

	アベイラビリティ向上のための対策	*実証実験での対応・実現性*
1	高負荷（高トラヒック）状態でも正常に動作できるスペックの設備を整える	対策その４（１）のとおり
2	データ、サーバ、ネットワークなどを対象に万一の事故に対してバックアップ を行う	認証センターのデータベースについてバックアップを実施する。スケジュールや方法については別途
3	万一の事故に備え、冗長構成をとる	冗長構成はとらない
4	バックアップデータやバックアップのシステムなどもリハーサルを実施して緊急時には正常に動作するのを確認しておくこと	実証実験ではデータベースのバックアップのみなので事前の動作確認までは行わない
5	サーバやルータなどでファームウェアのバージョンアップやセキュリティパッチの適用が今後発生する可能性の高い機器は、バックアップ用の機器で動作検証をしてから適用する	実証実験の途中でバージョンアップやセキュリティパッチが発行されても、よほどの重大な問題でない限り適用しない
6	DoS攻撃や突発的に増加するワームなどへの対策を行う	ウィルス対策ソフトで対応する
7	火災や地震といった大規模な災害の発生に備えるディザスタ・リカバリ対策を行う	実験では災害対策はとらない
8	システム全体の監視、管理体制を整える	限られた条件の中でできる範囲の体制をとる

19

5．リスクに備える対策（共通対策）

対策その５　その他

（１）ハードウェアの管理徹底
・施錠できる部屋に設置する
・鍵のかかるラックに端末を設置する
・鍵の管理は運用管理責任者が行う
　（参考）実証実験を行う場合はＮＴＴ幕張ビル２４Ｆ居室内のサーバー室に認証センターのサーバーを設置（居室はＩＣカード管理、サーバー室は施錠管理）する
★対策の効果
盗難や破壊を防ぐ手段となる

（２）媒体の管理徹底
・施錠できる保管庫に保管する
・鍵の管理は媒体管理責任者が行う
　（参考）ＮＴＴ幕張ビル２４Ｆ居室内のサーバー室に保管庫を設置する。
　　保管庫は施錠可能。
★対策の効果
盗難を防ぐ手段となる

（３）ユーザー教育、規定の策定
・保険証認証サービスのセキュリティポリシーを制定し、ユーザーに徹底する
・運用マニュアル類の整備

20

6．リスクに備える対策（個別）