6．リスクに備える対策（個別）

6－1．個別のリスク&対策一覧

各機関のリスク&対策の一覧を以下に示す．対策がどのセキュリティポリシー、どの共通対策に対応しているかを表している．詳細な内容については次項で個別に記述する．

	ポリシー	共通対策	保険者	医療機関	認証センター
1	NW経路において送受信データの機密性を保つこと	【その1】インターネットVPNを使う	－	⑧保険証認証サービスの導入によって医療機関内の個人情報が流出する可能性はないか	⑧情報漏洩対策
2	NWやサービスへの接続時に本人確認を徹底すること	【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	①業務権限と役割り ②アクセス管理 ③保険証サーバー内のデータの取り扱い方法 ⑧医療機関におけるなりすましに対して、事後確認の方法	①業務権限と役割り ②アクセス管理 ③USBキーを紛失したら ④医療端末内のデータの取り扱い	①業務権限と役割り ②アクセス管理 ⑧改ざん対策
3	情報が必要なときにいつでも使用できること	【その4】想定される処理性能を満たす設備を備える 【その5】その他	④トラブル発生時の対応	⑤トラブル発生時の対応	③バックアップ ⑤トラブル発生時の対応 ⑦DBの保存方法
4	法令その他の規範、規制要求事項を遵守すること	【その5】その他	法令順守に特化した具体的な対策は無いが、ポリシーは基本方針として対策全般に関わっている		
5	＊その他	【その5】その他	⑥保険者側における本来の保険証情報と保険証サーバー内の情報の整合性	⑦院内の情報システムをこのシステムの接続することによって、システムが障害を受ける可能性	④トレーサビリティ ⑥保存するデータの内容

22

6．リスクに備える対策（個別）

6－2．保険者のリスク&対策

6－1項の一覧で示した、保険者特有の想定されるリスクとその対策を以下に示す．

①業務の権限

保険者の業務権限と役割りについて示す．

	保険証サーバのメンテナンス	保険証情報の登録	保険者の申請	ユーザーの申請	その他一般の業務	媒体の管理
運用管理責任者	○	△	－	－	○	－
媒体管理責任者	－	△	－	－	△	○
業務責任者	－	○	○	○	○	－
担当者	－	△	－	－	○	－

②アクセス管理はどうなっているのか

サービスを利用するためには認証センターへの接続時、サービスへのログイン時、認証実行時などいくつかの場面でユーザー認証が行われる．そこで不正なアクセス（IDが違う、権限が無いなど）があった場合は不正アクセスログ情報として認証センターおよび保険者の仮サーバーにログが残る．

23

6．リスクに備える対策（個別）

③保険証サーバー内のデータの取り扱い方法は

保険者に設置する保険証サーバー内のすべて情報（保険証の情報、ログ情報）は、該当の保険者内で定められた基準に沿って取り扱うこと

④トラブル発生時の対応

認証センターのヘルプデスクに速やかに連絡すること

⑤保険者側における本来の保険証情報と保険証サーバー内の情報の整合性は

リアルタイム型保険者でも認証センターのサーバーに保険証情報を蓄積する事前蓄積型保険者（今回の実証実験ではリアルタイム型のみ）でも多かれ少なかれ、データ登録のタイミングのずれはて生じてしまう。実験では参加する医療機関の数や被保険者の数を考慮すると、多少のずれは業務に影響はないと思われるが、認証時に更新情報（更新日時など）を医療機関に通知するなどの検討が必要となるかもしれない。

⑥医療機関におけるなりすましに対して、事後確認の方法はあるのか

不正なアクセス（ＩＤが違う、権限が無いなど）があった場合は不正アクセスログ情報としてサーバーにログ情報が残るが、正しい手順でログインしている場合には、なりすましを防ぐことは困難である。医療機関側で担当者以外が操作できないように離席管理を行い、席を離れる場合は端末をロックする、アプリケーションを閉じる、カメラでの監視を行うなどの対策が必要となる。

24

6．リスクに備える対策（個別）

⑦医療機関側で認証NGとなった場合に、NG理由の正当性を保険者側で保証する必要はあるのか、またその方法とは

保険者の提供する保険証情報で有効性を確認しているので、その時点での認証結果は保険者が保証することとなる。認証NGが正当であるかどうかを確かめたい場合には、医療機関の担当者から保険者に問い合わせて確認してもらう。

⑧個人情報保護法に照らして、認証センターの業務は委託先業務となる。委託先への監督業務は派生しないか。派生する場合、具体的な監督業務はどのように行われるのか。

認証センターの業務は委託先業務となる。よって、委託先への監督業務が派生してくる。監督業務としては月に1度、業務報告書の提出を義務付けるなどの方法があげられる。

25

6．リスクに備える対策（個別）

6－3．医療機関のリスク＆対策

6－1項の一覧で示した、医療機関特有の想定されるリスクとその対策を以下に示す。

①業務の権限

医療機関の業務権限と役割りについて示す。

	医療機関の申請	ユーザーの申請	パスワードの変更	保険証認証業務	認証結果の閲覧業務
業務責任者	○	○	○	○	○
担当者	－	－	○	○	－

②USBキーを紛失したらどうすればいいのか（USBキーを使用する場合）

認証センターへ接続するためにはUSBキーを端末に挿入し、ID、パスワードを入力する必要がある。よってUSBキーを挿入すればすぐに認証センターにアクセスできるわけではないが、情報漏洩の危険が高くなるので速やかに運用責任者から認証センターへの報告しなくてはいけない。

6．リスクに備える対策（個別）

③不正アクセスの管理はしているのか

サービスを利用するためには認証センターへの接続時、サービスへのログイン時、認証実行時などいくつかの場面でユーザー認証が行われる。そこで不正なアクセス（IDが違う、権限が無いなど）があった場合はログインは不可となり、さらにその結果は不正アクセスログ情報として認証センターにログが残る。

④医療端末内のデータはどう取り扱かうのか

一括認証を行った際にその認証結果を保存する機能がある。また、操作者が任意に画面を印刷するなどした場合も同様に、その医療機関内で定められた基準に沿ってデータを取り扱うこと。

⑤トラブル発生時はどうしたらいいのか

認証センターのヘルプデスクに速やかに連絡する。

⑥院内の情報システムと保険証認証サービスを接続することによって、システムが障害を受ける可能性はないか。

実証実験では保険者側に保険証サーバーを別に設置するため、病院内のシステムと直接接続することはない。よってアプリケーションが他システムに障害を及ぼすことはない。また同一ネットワーク上にサーバーが設置される場合も高トラヒック状態になることもない（5項対策その4の計算結果より）ため、他システムへの影響はないと思われる。病院の情報システムに接続した場合でもセンター側から病院システムにログインすることはできないが、互いのネットワークのセキュリティポリシーの整合性については事前に検討する必要がある。

6．リスクに備える対策（個別）

⑦保険証認証サービスの導入によって、医療機関内の個人情報が流出する可能性はないか

ない。理由については⑥を参照。また実証実験では、医療機関側の操作で保険証の認証結果を端末内に保存する仕組みはないので、悪意を持って個人情報を取り出さない限り、流出の危険はないと思われる。

⑧保険証認証サービスで保険証を認証するにあたって、患者の了解を取る必要はないか

ない。診療目的で保険証資格の有効性を確認することは当たり前の行為なので、患者の了解は必要ない。

⑨保険証認証サービスで認証を行っていることを医療機関内に公示したり、インターネット上で公開してもよいか

医療機関内の公示、インターネット上での公開、どちらも行ってかまわない。

⑩保険証認証サービスで認証した結果をレセプトや院外処方箋に表記されることは許されるか

表記してかまわない。システムで認証した結果は、本来、医療機関が保険証資格の有効性を保険者に問い合わせて得られる結果と同一のものである。よって、その結果をレセプトや院外処方箋に表記してかまわない。

28

6．リスクに備える対策（個別）

⑪認証結果情報を医療機関内で蓄積した場合、これは個人情報保護の対象と考えてよいか

認証結果情報には個人情報である保険証情報が含まれる。医療機関内で任意に認証結果情報を蓄積した場合には個人情報保護の対象となり、適切な処置が必要となる。ただし、⑦で記述したように実証実験ではアプリケーションの機能として医療機関内に認証結果情報を蓄積する機能はない。

⑫認証結果情報を保険者などに提供することは、情報の二次利用にあたらないか

あたらない。保険証資格の認証は従来、診療報酬請求の過程で発生している行為で、その際に保険者に資格の有効性を問い合わせて得る結果と、医療機関の窓口で保険証認証サービスを利用して得る結果は同一のものである。よって認証結果情報の二次利用にはあたらない。

29

6．リスクに備える対策（個別）

6－4．認証センターのリスク&対策

6－1項の一覧で示した、認証センター特有の想定されるリスクとその対策を以下に示す。

①業務の権限

認証センターの権限と役割りについて示す。

	システム全体の監視	資格サーバのメンテナンス	媒体の管理	バックアップ	ユーザー情報の登録	一般の業務
システム管理者	○	－	－	○	○	△
運用管理責任者	－	○	－	－	－	△
媒体管理責任者	－	－	○	－	－	△

②不正アクセスの管理はしているのか

サービスを利用するためには認証センターへの接続時、サービスへのログイン時、認証実行時などいくつかの場面でユーザー認証が行われる。そこで不正なアクセス（ＩＤが違う、権限が無いなど）があった場合は不正アクセスログ情報として認証センターにログが残る。

6．リスクに備える対策（個別）

③バックアップ

バックアップの対象範囲を定め、バックアップスケジュールを策定する。バックアップデータを保存する媒体の管理は媒体管理責任者の指示のもとで行うこと。今回は実証実験であるので本格的なバックアップ管理体制は取らないが、バックアップは行う。詳細な内容については別途作成する必要がある。

④トレーサビリティについて

認証を行った結果については、認証を行った時点から将来にわたり、いつ、誰が、何を認証し、どのような認証結果を返したのかトレースを可能とする。個々の認証につて識別番号を用い、依頼元、認証センターのいずれにおいても対象の認証を識別可能とする。具体的には、認証センターで行った認証結果は識別番号を付与し、ログとしてＤＢに記録しておく。それにより、利用者から依頼があれば個々の認証についての内容をトレース可能とする。

⑤トラブル発生時の対応

トラブル発生に備え、各種マニュアルを作成・準備する。トラブル発生時は事前に作成したそれらマニュアルや対応フロー等にしたがってすみやかに障害の回復に努めること。また、回復後はトラブルの原因や対処をマニュアル等にフィードバックし、再発防止に努めることが必要。

6．リスクに備える対策（個別）

⑥認証センターにはどんな情報が保存されるのか

保険者情報、医療機関情報といったユーザー情報と事前蓄積型保険者からの保険証情報、認証結果情報、アクセスログなどが保存される。今回は実験なので、参加する保険者はリアルタイム型保険者のみとなり、保険証情報は認証センターには保存されない（認証結果は保存される）。

⑦認証センターでのデータ保存方法は

サービス共通の対策その5で挙げたように鍵の管理が行われている施錠できる居室にサーバーを設置する。バックアップデータについても媒体に保存する場合には鍵のかかる保管庫に保管する。

⑧認証センターのセキュリティ管理（情報漏洩・改ざん対策）は十分か

このセキュリティ対策資料で記述しているサービス共通の対策について適用する。またこの他に認証センターにおける維持運用管理のガイドラインを作成し、その内容に沿って認証センターの業務を実施する。（「認証センターの維持運用管理」を参照）

32

資料４　認証センターの維持運用管理規則

目的

保険証認証サービスの実証実験を実施するにあたり、情報セキュリティを考慮して、保険証認証センター（以下、認証センター）が遵守すべき維持運用管理の具体的対策を定める。

◆実証実験ではＮＴＴコムウェアで定める情報セキュリティ対策基準ほかＩＳＭＳ関連の規定・要領に準じて作業を実施する。

１．対象範囲

本要領の対象となる端末類および組織を以下に示す。

端末　　：　保険証認証サーバなど同一ネットワーク上に接続されるサーバ類およびアプリケーションにログインするクライアントコンピュータ

組織　　：　認証センター内の全組織

２．管理体制と役割

（１）組織の長（実験においては代表研究者）

認証センター内のサーバ管理、運用において全ての責任と権限を持つ。

（２）運用管理者

運用管理要領を制定し、その要領に基づき各種メンテナンス作業を実施する。

（３）システム管理者

システム管理要領を制定し、その要領に基づき以下の作業を実施する。

・システムの保守

・バックアップ作業の実施

（４）媒体管理者

媒体管理要領を制定し、その要領に基づき作業を実施する。

・　バックアップ媒体の管理

・　保険証情報蓄積用媒体の管理（実証実験では使用しない）

◆実証実験では、主にアプリケーション開発担当者がシステム管理、業務運用管理、媒体管理の認証センター業務全般を行う。

３．アクセス制限

保険証認証サーバへのログインを制限する。

設置されるサーバの重要度により認証方式は異なる。個人情報がサーバ内に保存されるような重要なサーバについては生体認証等の高度な認証方式の導入を検討する。

◆実証実験では共通アカウント、パスワードを入力してログインする。

４．ハードウェアの管理

（１）端末の設置場所

保険証認証サーバは不法侵入、災害、障害等の脅威に対して物理的な管理策を実施する区画に設置する。

・ビルへの入館制限
・入退室管理のできる部屋に設置
　設置される端末の重要度により異なるが、ＩＣカード入室制御装置、暗証番号入力装置、生体認証装置等を設置する。
・鍵のかかるラックに端末を設置する。
・管理責任者を設定し、その管理責任者が鍵の管理を行う
◆実証実験ではＮＴＴ幕張ビル２４Ｆ居室内のサーバ室に認証用のサーバを設置する。ビルの入り口と２４Ｆ居室への入室時に社員証確認（ＩＣカード)、さらに居室内のサーバ室は常に施錠され、入退室管理簿で入退室をチェックする。

（２）媒体の管理
　バックアップ等で媒体を使用する場合には媒体の管理が必要となります。
・施錠できる保管庫に保管する
・鍵の管理は媒体管理者が行う
◆実証実験で媒体を使用する場合はＮＴＴ幕張ビル２４Ｆ居室内のサーバ室に施錠できる保管庫を設置する。

５．業務内容
各管理者は以下の内容で維持運用を行う。
＜運用管理者＞
・ 保険者情報の管理
　保険者から登録申請を受け付け、保険者情報をシステムに登録（新規登録、編集、削除）を行う。
・ 医療機関情報の管理
　医療機関からの登録申請を受け付け、医療機関情報をシステムに登録（新規登録、編集、削除）を行う。
・ ユーザー情報の管理
　各保険者、各医療機関からシステムを利用するユーザーの登録申請を受け付け、ユーザー情報をシステムに登録（新規登録、編集、削除）を行う。
・ サービスログ管理
　認証結果、アクセス結果、不正アクセスログ等の管理を行う。
◆実証実験でも各利用者の申請に基づき、これらのメンテナンス業務を実施する。

＜システム管理者＞
・ ログ管理
　利用者ＩＤ、アクセス日時、アクセスファイル等のログを取得を行う。
・ ＩＤ管理
　組織の長が許可した者に対してＩＤを付与する
　ＩＤは一人に対し、１つのＩＤを付与する。
　ユーザーのアクセス権を定期的にチェックする。
・ サーバ監視

認証サーバ、Ｗｅｂサーバ等の運用状況を監視する。

・ データバックアップ

何らかの原因でデータ復旧作業が発生する場合に備え、認証センターで扱うデータベースは定期的にバックアップする。媒体へバックアップした場合には媒体管理者が媒体の管理を行う。バックアップ対象のファイルには固有の設定情報（ＩＤ情報など）やログ情報も含まれる。

＜その他＞

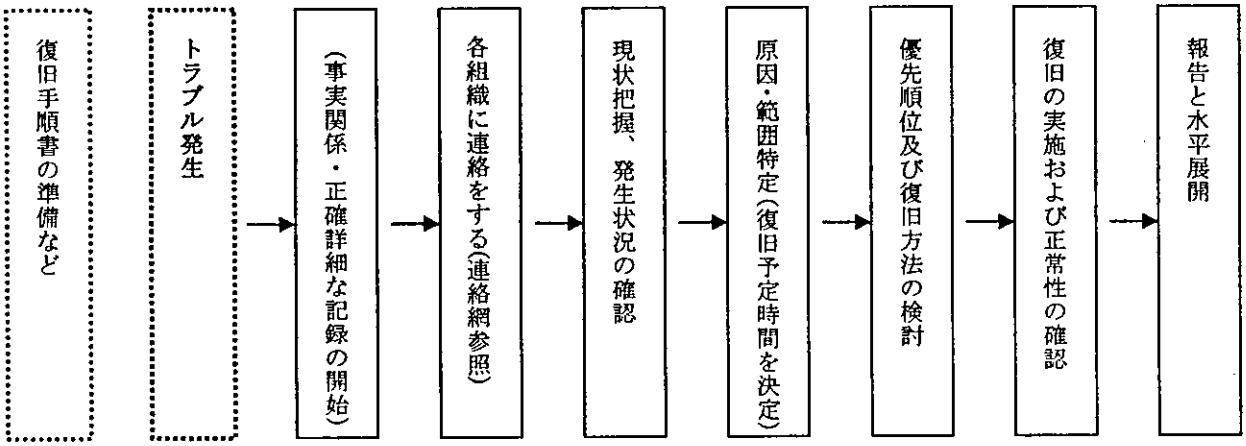
・内部監査の実施

認証センター内に内部監査事務局を設置する。
内部監査事務局はセキュリティ監査を計画及び定期的に実施し、監査結果に基づき組織の長（または情報セキュリティの責任者）に勧告すると共にフォローアップを行う。

◆実証実験では本格的な監査の体制は取りませんが、実験期間中に定期的にセキュリティチェックリスト（ＮＴＴコムウェアのサーバ管理要領に基づき別途作成）に従い、セキュリティ対策が実施されていることを確認します。また、必要に応じて報告様式にとりまとめ、関係機関に報告を行います。

６．トラブル対応

＜対応フロー図＞



（１）トラブル発生前の準備

組織の長は、トラブル事故発生時における報告義務について担当内に定期的に周知させる。また、システム管理者、運用管理者はトラブル発生に備え、必要により各種マニュアルを作成・準備する。

・ 「サーバ起動手順書」
・ 「ＤＢ復旧手順書」など

（２）トラブル発生時の対応

トラブル発生時は事前に定義した手順に従い、迅速なシステム回復を図る事とする。

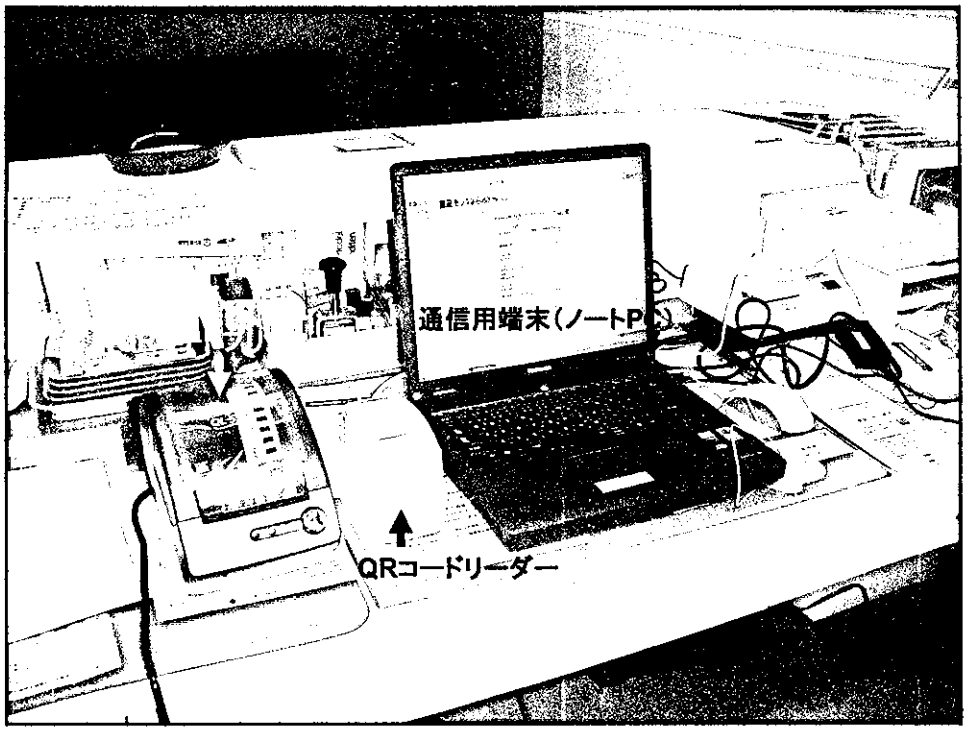
◆実証実験ではＮＴＴコムウェアの定めるＩＳＭＳコミュニケーション要領に従い対応する。

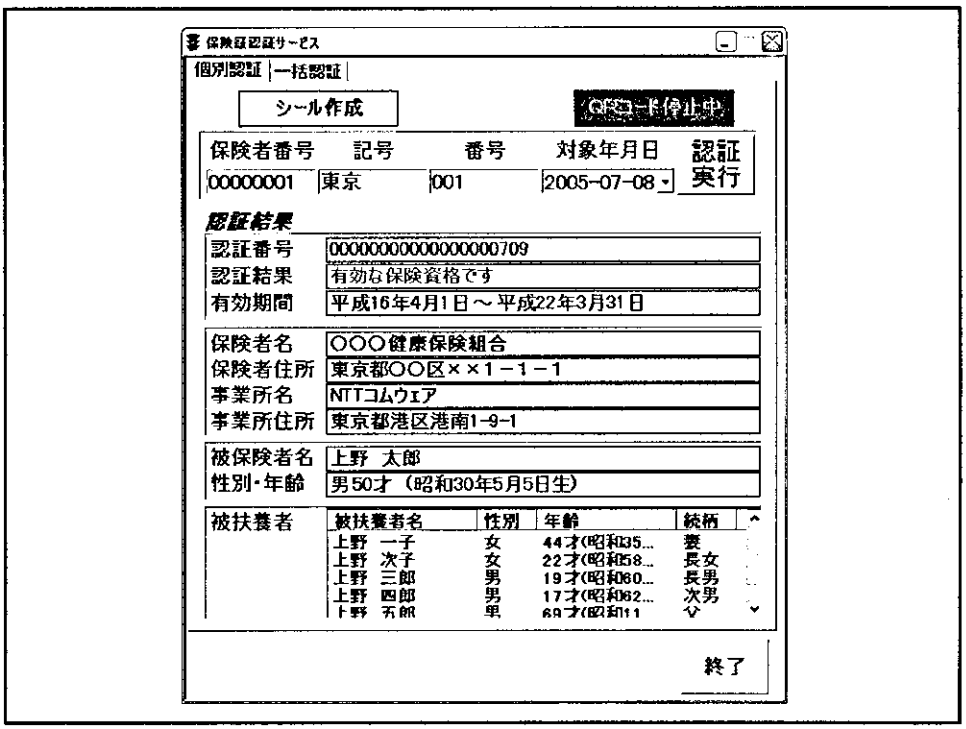
資料5.　認証実験スケジュール（一部　実際は50例を7週間にわたって実施）

5	パターン	被保険者／被扶養者氏名	第1週			第2週			第3週			第4週		
			DB更新	認証1	認証2	DB更新	認証1	認証2	DB更新	認証1	認証2	DB更新	認証1	認証2
#####	「国保」本人（導入後に取得）	認証弐一郎		「国保」なし					資格取得		「国保」あり			
2-2	「国保」家族（導入後に認定）	認証弐二子		「国保」なし								被扶養者認定	「国保」あり	
2-3	「政管」本人（導入後に認定）	認証弐三子			「政管」なし				資格取得		「政管」あり			
2-4	「政管」家族（導入後に認定）	認証弐四郎			「政管」なし							被扶養者認定	「政管」あり	
2-5	「組合」本人（導入後に認定）	認証弐五郎			「組合」なし				資格取得		「組合」あり			
2-6	「組合」家族（導入後に認定）	認証弐六子			「組合」なし							被扶養者認定		「組合」あり
2-7	「共済」本人（導入後に認定）	認証弐七子			「共済」なし				資格取得		「共済」あり			
2-8	「共済」家族（導入後に認定）	認証弐八郎			「共済」なし							被扶養者認定		「共済」あり

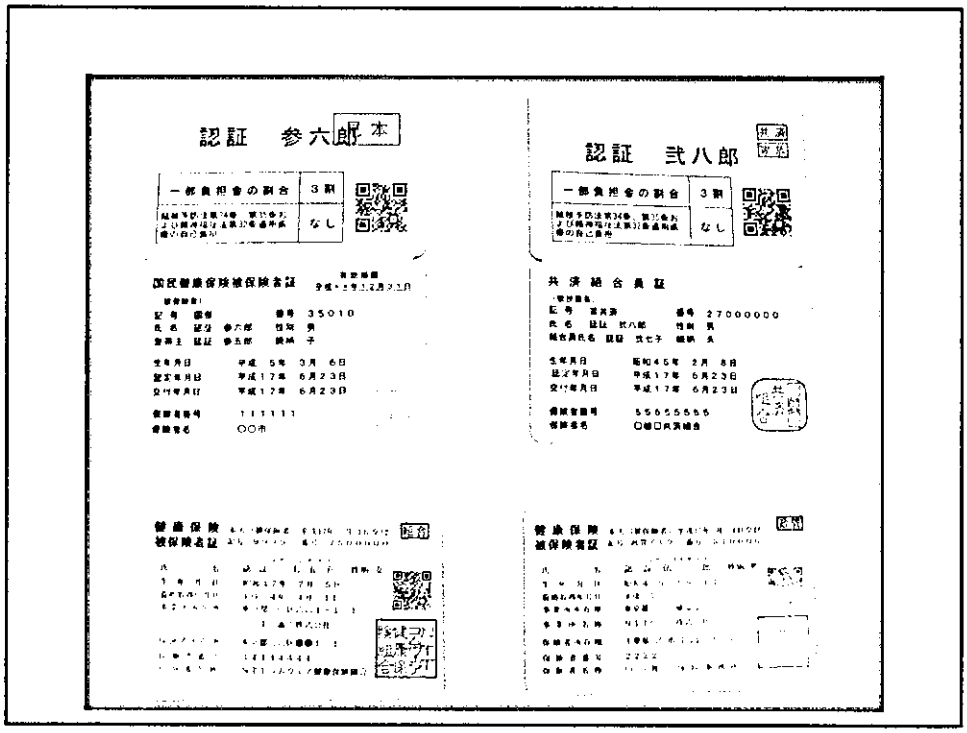
3-1	「国保」本人→「政管」本人	認証参一郎	「国保」資格取得		「国保」あり							1.「国保」資格喪失 2.「政管」資格取得	「国保」なし	「政管」あり
3-2	「国保」家族→「政管」家族	認証参二子	「国保」被扶養者認定		「国保」あり							1.「国保」認定取消 2.「政管」被扶養者認定	「国保」なし	「政管」あり
3-3	「政管」本人→「政管任継」本人	認証参三子	「政管」資格取得		「政管」あり							1.「政管」資格喪失 2.「政管任継」資格取得	「政管」なし	「政管任継」あり
3-4	「政管」家族→「政管任継」家族	認証参四郎	「政管」被扶養者認定		「政管」あり							1.「政管」認定取消 2.「政管任継」被扶養者認定	「政管」なし	「政管任継」あり
3-5	「組合任継」本人→「国保」本人	認証参五郎	1.「組合」資格取得 2.「組合」資格喪失 3.「組合任継」資格取得				「組合任継」あり					1.「組合任継」資格喪失 2.「国保」資格取得	「組合任継」なし	「国保」あり
3-6	「組合任継」家族→「国保」家族	認証三六郎	「組合任継」被扶養者認定				「組合任継」あり					1.「組合任継」認定取消 2.「国保」被扶養者認	「組合任継」なし	「国保」あり
3-7	「共済」本人→「組合」本人	認証参七子	「共済」資格取得				「共済」あり					1.「共済」資格喪失 2.「組合」資格取得		
3-8	「共済」家族→「組合」家族	認証三八子	「共済」被扶養者認定				「共済」あり					1.「共済」資格喪失 2.「組合」被扶養者認定		

資料６．　診療所における認証端末とその画面

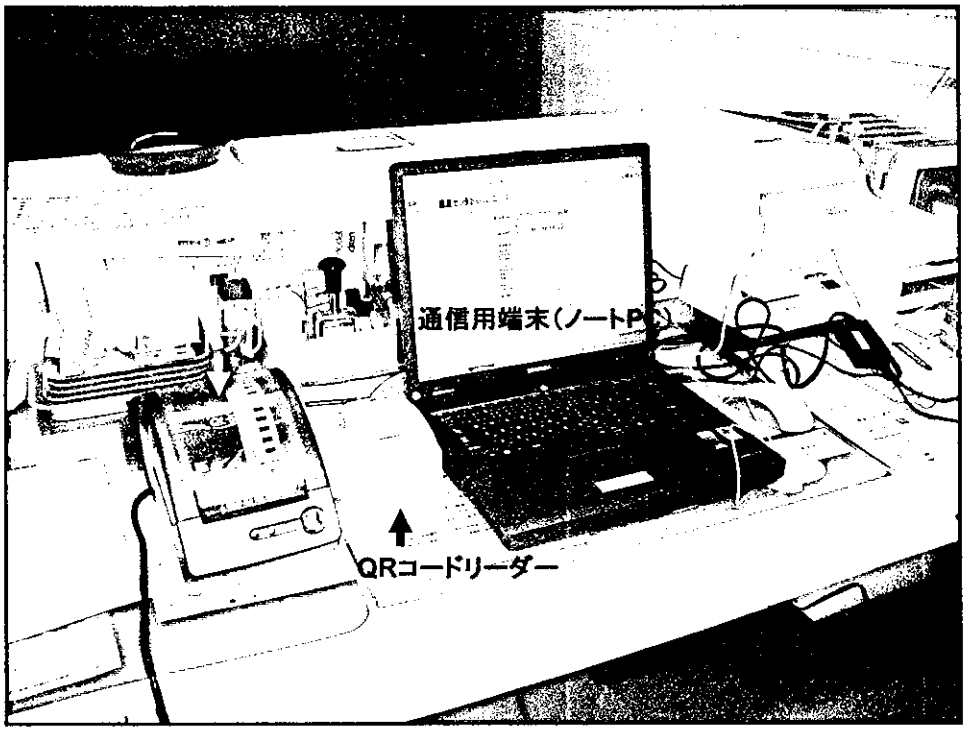


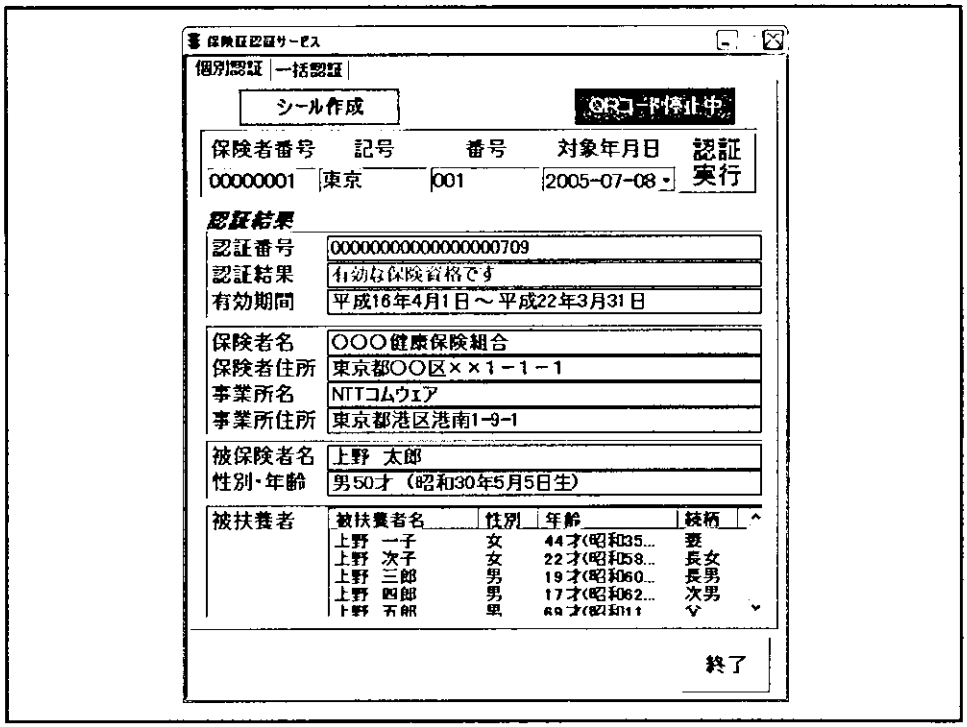


資料７．　実験に使用した仮想保険証



資料６．　診療所における認証端末とその画面





資料9　保険証実証実験・認証アクセス件数一覧

			第1回目	第2回目	第3回目	第4回目	第5回目	第6回目	第7回目	備考	アクセス件数合計
遠藤クリニック	アクセス件数		23	21	32	28	92	26	22	第7回で終了	244
美浜区高瀬	認証結果（内訳再掲）	「有効」	19	19	19	10	82	19	12		(180)
		「有効期限切れ」	0	0	6	13	0	7	10		(36)
		「記号番号なし」	2	0	6	4	10	0	0		(22)
		「保険者番号なし」	2	2	1	1	0	0	0		(6)
若林皮膚科医院	アクセス件数		15	28	34	23	29	48	―	第6回で終了	177
若葉区小倉町	認証結果（内訳再掲）	「有効」	11	22	16	8	19	33			(109)
		「有効期限切れ」	0	0	6	15	8	12			(41)
		「記号番号なし」	2	6	12	0	2	3			(25)
		「保険者番号なし」	2	0	0	0	0	0			(2)
大久保クリニック	アクセス件数		31	25	35	83	30	―	―	第5回で終了	204
緑区あすみが丘	認証結果（内訳再掲）	「有効」	20	17	24	58	18				(137)
		「有効期限切れ」	0	6	8	19	12				(45)
		「記号番号なし」	7	2	1	6	0				(16)
		「保険者番号なし」	4	0	2	0	0				(6)

3医療機関合計		625件
認証結果（内訳再掲）	「有効」	(426)
	「有効期限切れ」	(122)
	「記号番号なし」	(63)
	「保険者番号なし」	(14)