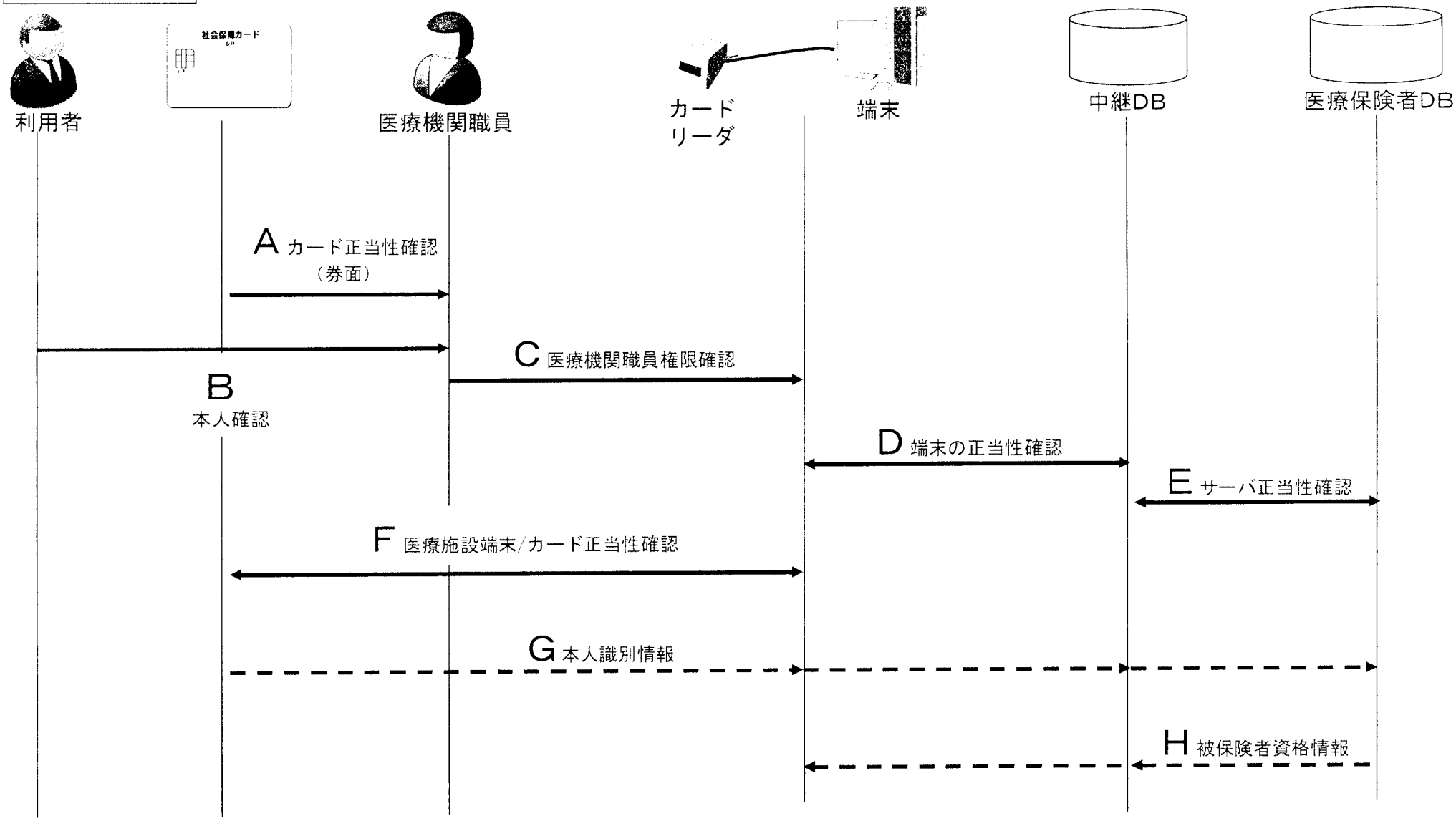
資格確認における脅威と対策

参考資料１

関係図



資格確認における脅威と対策（１）

（１）正しいカードが正しい持参者によって利用されることを担保できること

要件	想定される脅威	対策	分類	残余リスク	備考
①正しい持参者であることの確認	借りたカード、拾ったカード、盗んだカードを使用し、他人に成りすまして、受診される。 B	暗証番号（PIN）の入力	技術	・暗証番号（PIN）を忘れる場合がある。	・受付に時間がかかり、窓口業務に支障を来す可能性。 ・本人が意識不明等の場合には、暗証番号（PIN）を入力させることができない。
		指紋や静脈等の生体情報による認証	技術	・100%の認識率ではないので、誤認識を行う場合がある。	・生体情報をICチップに収録することとなるので、これに抵抗感を持つ人もいる。 ・専用の読取機が必要。
		券面情報との照合による本人確認	運用	・券面が偽造される可能性 ・券面情報が減ると本人確認の確信度が減少	
②正しいカードであることの確認	券面が偽造されたカードによって受診される。 A	ホログラム等の券面特殊加工を施す。	技術	偽造技術の向上により、特殊加工までも偽造される可能性がある。	・券面の特殊加工によりカード価格が高くなる。
	ICチップが偽造されたカードによって受診される。 F	医療機関のカード読み取り端末がカードが正当なものかどうかを認証する。	技術	カード発行時にカード内の鍵情報が流出するリスク（※）	※ＩＣカード発行機関が適切な安全管理のもとにＩＣカード発行を行っていれば、本残余リスクは限りなく小さくなる。
	ICチップの中の情報が偽造されたカードで受診される。 F・G	情報に電子署名を付す。	技術	カード発行時（情報収録前）の情報流出リスク（※）	※ＩＣカード発行機関が適切な安全管理のもとにＩＣカード発行を行っていれば、本残余リスクは限りなく小さくなる。
③持参者が正当な資格を持つことの確認	正当なカード所有者だが、不当な権利主張 G	IDと資格情報の正当性確認	技術		・オンライン認証により本人確認をした後、資格確認を行う。

資格確認における脅威と対策（２）

（２）正しい資格情報が確認できること					
要件	**想定される脅威**	**対策**	**分類**	**残余リスク**	**備考**
①資格情報の完全性が確保されること	保険者のデータベースが何者かによって、不正に書き換えられる。 G・H	情報登録・更新などの正当性を確保	技術	・保険者による登録誤り。	
②資格情報の機密性が確保されること	保険者のデータベースが何者かによって不正にアクセスされる。 D・E	・アクセスできる医療機関の端末を中継DBが認証する。	技術		アクセスできる医療機関をどのように認定するか。
		・アクセス履歴を一定期間保存する。 等	技術		

資格確認における脅威と対策（３）

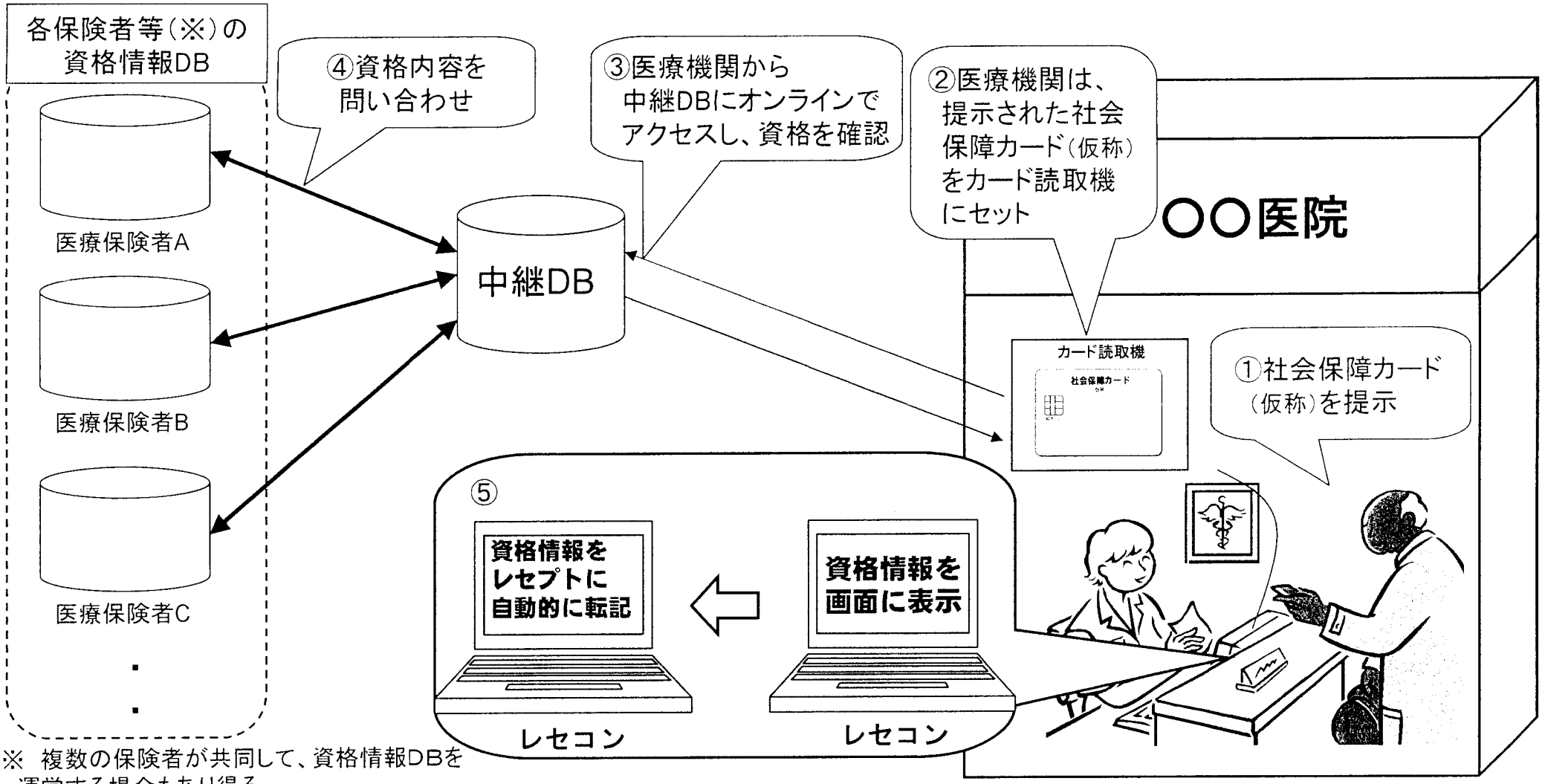
（３）悪意のある者や不正な機器からの攻撃に耐えられること

要件	想定される脅威	対策	分類	残余リスク	備考
①カード内情報が改ざんされないこと	カードに不正にアクセスし、カード内情報が改ざんされる。 F	・書換不要な情報は書換不可とする ・耐タンパ性が確保された媒体を採用 ・カードが外部機器を認証	技術	端末、中継DBからの鍵情報の流出により、端末や中継DBのなりすましが行われる可能性。	
	カードから読み出したデータが改ざんされる。 G	カード内情報に電子署名を付す。	技術		
	医療機関の端末がウイルスに汚染される、ソフトウェアのバグ等によりカード内情報が改ざんされる。 F・G	・セキュリティパッチの適用 ・ウイルス対策ソフトの導入 ・不正ソフトをインストールしないよう指導	運用 技術		全ての医療機関で統一的な運用が確保されるか。
		中継DB側でカード内情報の電子署名を検証	技術		
②カード内情報が漏洩しないこと	カードに不正にアクセスされ、カード内情報が漏洩する。 F	・耐タンパ性が確保された媒体を採用 ・カードが外部機器を認証	技術	端末、中継DBからの鍵情報の流出により、端末や中継DBのなりすましが行われる可能性。	
	カードから読み出したデータが漏洩する。 F・G	通信の暗号化	技術	端末、中継DBからの鍵情報の流出により、端末や中継DBのなりすましが行われる可能性。	
	医療機関職員がカード内情報を他者に告知する等して漏洩する。 C	・漏洩時の罰則規定を設ける ・医療機関の職員権限管理 ・アクセス履歴の保存（抑止効果）	制度 技術 運用		
	医療機関の端末がウイルスに汚染される、ソフトウェアのバグ等によりカード内情報が改ざんされる F・G	・セキュリティパッチの適用 ・ウイルス対策ソフトの導入 ・不正ソフトをインストールしないよう指導	運用 技術		全ての医療機関で統一的な運用が確保されるか。

レセプトへの自動転記の仕組みのイメージ

参考資料２

○　資格確認の仕組みと基本的に同じ仕組み。
○　資格確認用にレセコン（レセプトを作成するためのコンピュータ）画面上に表示した資格情報がレセプトに自動的に転記される。



※　複数の保険者が共同して、資格情報DBを運営する場合もあり得る。

レセプトに自動転記される項目

参考資料３

【医科入院レセプトの場合】

① 氏名

② 性別

③ 生年月日

④ 保険者番号

⑤ 被保険者証記号・番号

⑥ 保険種別１（１：社・国、２：公費、３：後期、４：退職）

⑦ 保険種別２（１：単独、２：２併、３：３併）

⑧ 本人・家族（１：本入、２：六入、３：家入、７：高一、９：高入７）

⑨ 給付割合（１０、９、８、７、（　））

⑩
- 公費負担者番号①／公費負担者番号②
- 公費負担医療の受給者番号①／公費負担医療の受給者番号②

参考資料４

カードが利用できない状況下や現行の被保険者証等からカードへの移行期間の対応について

資格確認ができない場合の対応①

分類	ケース	対策	対策分類
被保険者	①カードを持ってこない（未受領・紛失・忘却・緊急時など）、有効期限切れ	現行の健康保険証での運用と同様の対応。	運用
	②カードの故障	医療保険の資格情報を記載した別紙を交付しておく。	運用
		カードに、本人を識別でき、資格確認が可能な情報を記載しておく。	制度
		その他、カードの耐久性の向上等	予防
医療機関	①カードを読み出す設備がない（未整備、往診等）	医療保険の資格情報を記載した別紙を交付しておく。	運用
		カードに、本人を識別でき、資格確認が可能な情報を記載しておく。	制度
		代替手段として携帯電話等の携帯端末での読み出し	システム
	②カードを読み出す設備がない（移行期）	医療保険の資格情報を記載した別紙を交付しておく。	運用
		カードに、本人を識別でき、資格確認が可能な情報を記載しておく。	制度
	③カード読み出しシステムの停止	医療保険の資格情報を記載した別紙を交付しておく。	運用
		カードに、本人を識別でき、資格確認が可能な情報を記載しておく。	制度
		システムの冗長化（予備システムによるバックアップ）。	予防
	④オペレーションミス	医療機関側での研修や、ミスをチェックできる仕組みを構築。	予防

※　これらの対策をとった場合のデメリット等も踏まえ、今後、具体的な対応策を更に検討

資格確認ができない場合の対応②

分類	ケース	対策	対策分類
ネットワーク （医療機関と中継ＤＢ間）	ネットワーク停止	医療保険の資格情報を記載した別紙を交付しておく。 カードに、本人を識別でき、資格確認が可能な情報を記載しておく。 システムの冗長化（予備システムによるバックアップ）。	運用 制度 予防
中継ＤＢ	システムの停止		
ネットワーク （中継ＤＢと保険者間）	ネットワーク停止		
保険者	①資格データ反映までのタイムラグ	事後的に、現行と同様のフローで正しい保険者に再請求する。	制度・運用
	②誤操作による間違ったデータ反映	操作者の研修やミスをチェックできる仕組みを構築。	運用・予防
		誤った保険者に請求した場合は、現行と同様のフローで処理する。	運用
	③システムの停止	医療保険の資格情報を記載した別紙を交付しておく。	運用
		カードに、本人を識別でき、資格確認が可能な情報を記載しておく。	制度
		システムの冗長化（予備システムによるバックアップ）。	予防
	④保険者システムの未整備	代替システム提供（代行サービス提供等）	運用
		医療保険の資格情報を記載した別紙を交付しておく。	運用
		カードに、本人を識別でき、資格確認が可能な情報を記載しておく。	制度

※　これらの対策をとった場合のデメリット等も踏まえ、今後、具体的な対応策を更に検討

現行の介護保険被保険者証に記載されている情報

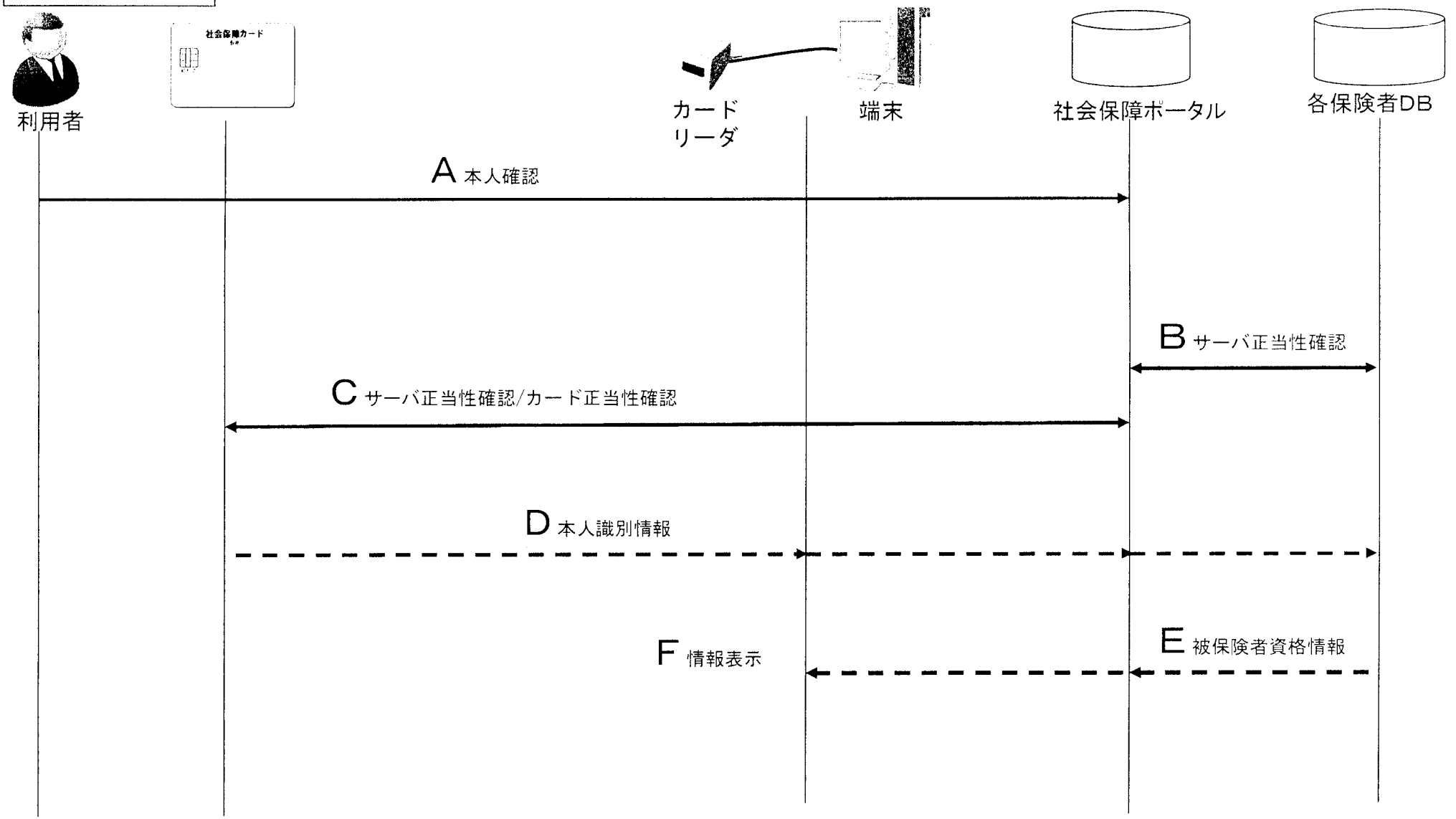
参考資料５

①被保険者の番号
②住所、氏名のフリガナ、氏名、生年月日、性別
③交付年月日
④保険者番号、保険者名称及び印
⑤要介護状態区分等
⑥認定年月日
⑦認定の有効期間
⑧居宅サービス等の区分支給限度基準額及び期間
⑨(うち種類支給限度基準額)サービスの種類及び種類支給限度基準額
⑩認定審査会の意見及びサービスの種類の指定
⑪給付制限の内容及び期間
⑫居宅介護支援事業者又は介護予防支援事業者及びその事業所の名称、届出年月日
⑬介護保険施設等の種類、名称、入所等年月日、退所等年月日
※労災保険の介護補償給付受給者についてはその旨及び常時介護・随時介護の別
※バウチャーを発行する市町村については、支給限度基準額の欄に「うちバウチャー切り分け欄」を設ける。

情報閲覧における脅威と対策

参考資料６

関係図



確認される側 ——→ 確認する側

情報の流れ ------→

※利用端末がセキュリティ技術上の信頼点として必ずしも保障されない場合の一例

情報閲覧における脅威と対策（１）

（１）正しいカードが正しい所有者によって利用されることを担保できること

要件	想定される脅威	対策	分類	残余リスク	備考
①正しい所有者であることの確認	借りたカード、拾ったカード、盗んだカードを使用し、他人の情報を閲覧する。 A	暗証番号（PIN）の入力	技術	・暗証番号（PIN）を忘れる場合がある。	暗証番号（PIN）を忘れた場合に思い出すためのヒントの登録などのサポートが必要。
		指紋や静脈等の生体情報による認証	技術	・100%の認識率ではないので、誤認識を行う場合がある。	・生体情報をICチップに収録することとなるので、これに抵抗感を持つ人もいる。 ・専用の読取機が必要。
②正しいカードであることの確認	ICチップが偽造されたカードを利用される。 C	端末システムもしくは閲覧システムがカードを正当なものかどうかを認証する。	技術	カード発行時にカード内の鍵情報が流出するリスク（※）	※ＩＣカード発行機関が適切な安全管理のもとにＩＣカード発行を行っていれば、本残余リスクは限りなく小さくなる。
	ICチップの中の情報が偽造されたカードを利用される。 C・D	情報に電子署名を付す。	技術	カード発行時（情報収録前）の情報流出リスク（※）	※ＩＣカード発行機関が適切な安全管理のもとにＩＣカード発行を行っていれば、本残余リスクは限りなく小さくなる。
③所有者が正当な資格を持つことの確認	正当なカード所有者だが、不当な権利主張（加入していない制度の情報閲覧等） D	IDと資格情報の正当性確認	技術		・オンライン認証により本人確認をした後、情報閲覧を認める。

情報閲覧における脅威と対策（２）

（２）正しい閲覧情報が確認できること					
要件	**想定される脅威**	**対策**	**分類**	**残余リスク**	**備考**
①閲覧情報の完全性が確保されること	保険者のデータベースが何者かによって、不正に書き換えられる。 D・E	情報登録・更新などの正当性を確保	技術	・保険者による登録誤り。	
②閲覧情報へのアクセスの正当性が確保されること	閲覧情報に不正にアクセスされる。 B	・オンライン認証、アクセス制限、履歴証拠保存 等	技術		

情報閲覧における脅威と対策（３）

（３）悪意のある者や不正な機器からの攻撃に耐えられること

要件	想定される脅威	対策	分類	残余リスク	備考
①カード内情報が改ざんされないこと	カードに不正にアクセスし、カード内情報が改ざんされる。 C	・耐タンパ性が確保された媒体を採用 ・カードが外部機器を認証する。	技術	端末、中継DBからの鍵情報の流出により、端末や中継DBのなりすましが行われる可能性。	
	カードから読み出したデータが改ざんされる。 D	カード内情報に電子署名を付す。	技術		
	自宅端末がウイルスに汚染される、ソフトウェアのバグ等によりカード内情報が改ざんされる。 C・D	・セキュリティパッチの適用 ・ウイルス対策ソフトの導入 ・不正ソフトをインストールしないよう指導	運用 技術		全ての利用者で統一的な運用が確保されるか。
		中継DB側で電子署名を検証	技術		
②カード内情報が漏洩しないこと	カードに不正にアクセスされ、カード内情報が漏洩する。 C	・耐タンパ性が確保された媒体を採用 ・カードが外部機器を認証する。	技術	端末、中継DBからの鍵情報の流出により、端末や中継DBのなりすましが行われる可能性。	
	カードから読み出したデータが漏洩する。 C・D	通信の暗号化	技術	端末、中継DBからの鍵情報の流出により、端末や中継DBのなりすましが行われる可能性。	
	自宅端末がウイルスに汚染される、ソフトウェアのバグ等によりカード内情報が改ざんされる C・D	・セキュリティパッチの適用 ・ウイルス対策ソフトの導入 ・不正ソフトをインストールしないよう指導	運用 技術		全ての利用者で統一的な運用が確保されるか。

情報閲覧における脅威と対策（３）－２

（３）悪意のある者や不正な機器からの攻撃に耐えられること					
要件	**想定される脅威**	**対策**	**分類**	**残余リスク**	**備考**
③PINが漏洩しないこと	情報端末において認証するための鍵情報が漏洩する。 A	専用入力装置を利用する。	技術		
④表示された後の情報が漏洩しないこと	残存する閲覧情報への不正アクセス F	・一時ファイル（キャッシュ）の削除 ・一時ファイル（キャッシュ）の暗号化	運用 技術		情報端末の場合は、全ての利用者で統一的な運用が確保されるか。 自宅での閲覧の場合はこの脅威をリスクと感じる場合には対策を実施する。
⑤閲覧情報の機密性を確保すること	閲覧情報そのものが漏洩する E・F	閲覧情報の適切な暗号化	技術		