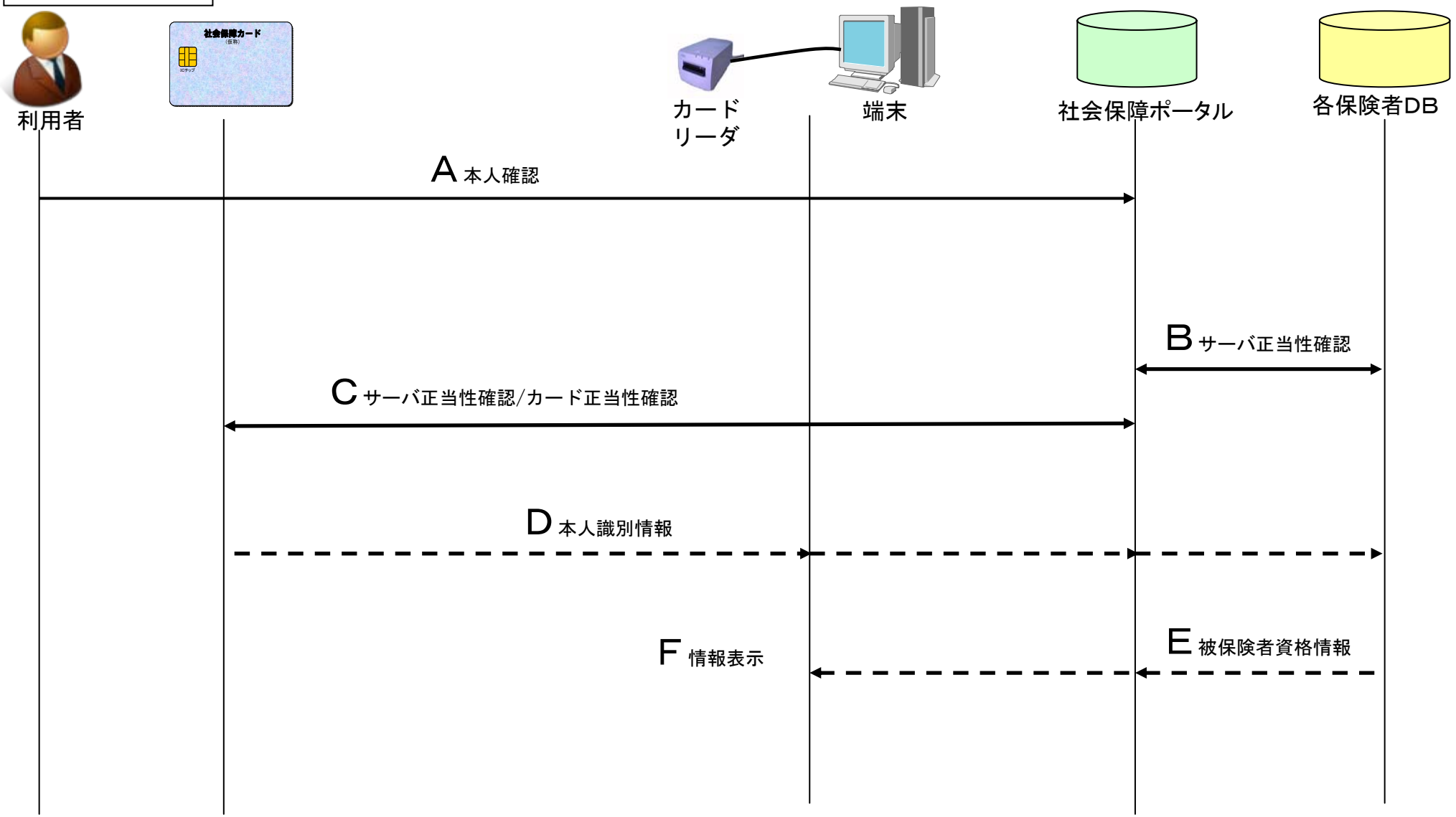
情報閲覧における脅威と対策

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		