M-95 介護情報に対する暗号化の適用に関する考察

The Consideration about The Application of The Encryption to The Care Information

松田隆一※ 増渕明彦※ 斉藤亮※ 岩田彰※※
Ryuichi Matsuda Akihiko Masubuchi Ryou Saito Akira Iwata

1. はじめに

介護関連情報を、インターネットを活用して通信すれば、サービスの向上が期待できるが、情報漏洩に対する高いセキュリティが必須である。

本研究は、福祉サービスの向上手段の一つとして、暗号化技術により情報伝達の効率化と情報に対する高いセキュリティとが両立した情報伝達手段の提供を目的とした研究である。

2. セキュリティの課題

情報漏洩にはさまざまなﾊﾟﾀｰﾝがある。実用レベルの効率を持つ今までのシステムでは、ＳＳＬなどを使用しているが、セキュリティに関して次の様な課題がある。

- センタのオペレータによる漏洩の危険。
- 情報参照端末を設置するオフィスを訪れた部外者の不正操作による漏洩の危険。
- 盗難等により情報参照端末が外部に渡った場合など、その端末に対し相当な時間をかけてアタックされたときの情報漏洩の危険。

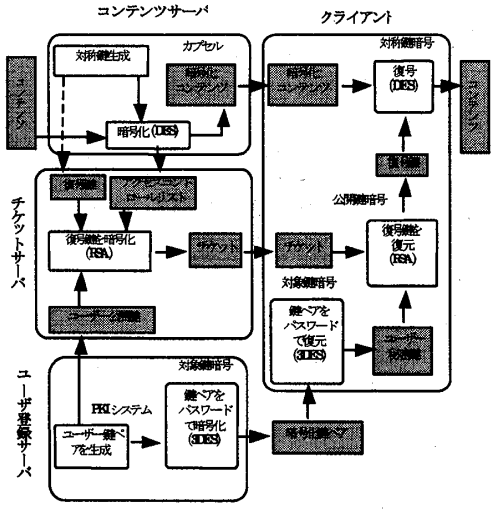
この解決方法としてカプセル化技術による暗号方式を採用し、同方式を組み込んだ実験システムを構築し、実証実験を行い評価した。カプセル化技術による暗号方式は課題を次のように解決している。

- カプセル（暗号化済）をダウンロードするため、通信経路からの漏洩が無い。
- サーバに格納されている情報はカプセル化されているため、アタックに強い。
- サーバ上では復号化の手段を持たないため、ｾﾝﾀｵﾍﾟﾚｰﾀｰでもデータ参照は出来ない。
- 情報参照には端末からその端末に合ったユーザーＩＤ、パスワードを入れる必要があり、部外者は容易に情報参照できない。
- 復号済みの情報は端末に残らない。また、復号化には復号化の都度サーバからダウンロードされるチケットが必要であり、このため配信済みの情報に対してもセンタから容易に復号化の権限を取り消しできる。

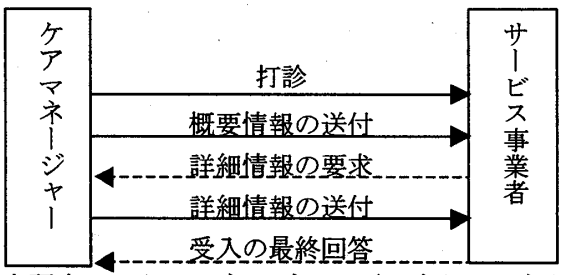
3. カプセル化方式の概要

カプセル化方式の概要を下図に示す。

- コンテンツサーバは複数のコンテンツを暗号化してカプセルに格納する。同時に各コンテンツに対する各ユーザーの参照権をアクセスコントロールリストに登録する。
- カプセルは自由にダウンロードできる。
- クライアントでは、ユーザーＩＤ、パスワードを入力し暗号ツールを立ち上げる。
- カプセルを参照しようとすると、暗号ツールはチケットサーバにチケットの発行を要求する。チケットは要求ユーザーの公開キーで暗号化され、発行される。
- 情報参照端末では、チケットからカプセルを復号化するためのキーを復元し、カプセルを復号する。
- サーバはアクセスコントロールリストを随時変更することができる。



4. 本研究における取り組み

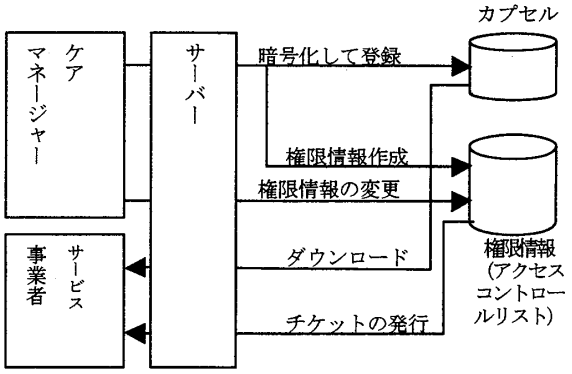


本研究ではケアマネージャー（以降ケアマネと略す）が事業者を決定する業務に着目した。サー

※ 日本電気株式会社
※※名古屋工業大学工学部教授
通信・放送機構 委嘱研究員

ビス事業者（以降事業者と略す）が、要介護者にサービスを提供可能かを判断するために必須の情報である要介護者情報は、上図のように、打診（簡単な説明）、概要情報の送付、詳細情報の送付（実線部分）の形で通信される。この部分に関するシステム化を行った。

5. システムの構成



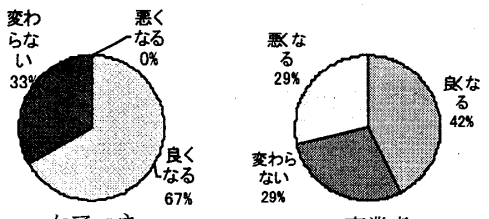
要介護者情報の処理を説明する。

- ケアマネが情報を登録すると、カプセル化を行い、同時に情報を送信する事業者に対する概要情報閲覧の権限情報を作成する。また情報が登録されたことを事業者にﾒｰﾙを使用して通知する。
- 事業者は、情報をダウンロードして、復号する。概要情報を見て受入可能であれば、ケアマネに回答する。
- ケアマネは回答のあった事業者に対する権限を概要から詳細に変更する。システムは権限変更し、対象事業者に通知する。
- 事業者は詳細情報の復号化を行い、受入が決定する。

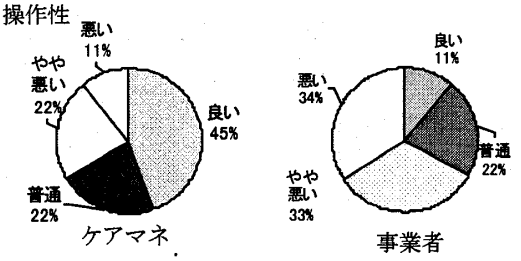
6. 結果

モニタに対するアンケート調査により、効率化の検証を行った。結果を下図に示す。

効率



操作性



7. 考察

上記結果により、「2.ｾｷｭﾘﾃｨの課題」に提起されたすべての課題をｸﾘｱするｾｷｭﾘﾃｨの高いｼｽﾃﾑとして、実用的な効率、操作性が実現できたと考える。

研究・実験全体の結果として、以下に示す成果が実証できた。

- 情報漏洩に対する課題をｸﾘｱするシステムが構築できたこと。
- 業務の効率は実用レベルであること。
  実験の結果から「良くなる」が、「悪くなる」を明らかに超えており、効率に関して問題がないと考えられる。
- 操作性は実用範囲内であること。
  受信に関しての操作性は、暗号ツールを立ち上げるなどの操作が入るため、当初からやや悪いという評価を予想していた。結果としてほぼ予想通りとなった。送信の操作性において、内容を確認したところ、「概要から詳細への権限変更時、権限の変更要求者を指定するときに、概要を送付した全事業者から選択しなくてはならない。」という点に、マイナスの評価が集中していることが分かった。
  操作性に関しては改善すべきではあるが、「良い」、「普通」がほぼ半数をしめており、実用レベルと考える。

また、課題として以下の点が挙げられる。

- 事業者からの応答をシステムに取り込み、権限変更の操作性を上げる必要がある。
- 受信系に関しては、操作性改善を検討する必要である。

8. 今後の取り組み

今回の実験では複数の事業者に対し、初期状態では同じ内容が参照できるケースを扱った。今後は、異なるセキュリティレベルを持つ複数のユーザーに対し、セキュリティレベルに対応した異なる情報提供のケースを検討する。このケースに有効な、情報参照の形式、登録の方法、各情報に対する、ユーザーのセキュリティレベルの変更方法について、研究・実験を行う。

9. 参考文献

[1]細見、中江、市山、「カプセル化コンテンツ流通基盤(1)－全体構成と利用状況適応機能－」、第 57 回情処全国大会、1998

[2] 中江、細見、市山、「カプセル化コンテンツ流通基盤(2)－チケットによる利用制御方式－」、第 57 回情処全国大会、1998