介護関連情報に対する暗号化の適用に関する考察

増渕明彦† 松田隆一†† 斉藤亮‡ 岩田彰‡‡
日本電気(株)† 日本電気(株)†† 日本電気(株)‡ 名古屋工業大学‡‡
通信・放送機構 委嘱研究員‡‡

1. はじめに

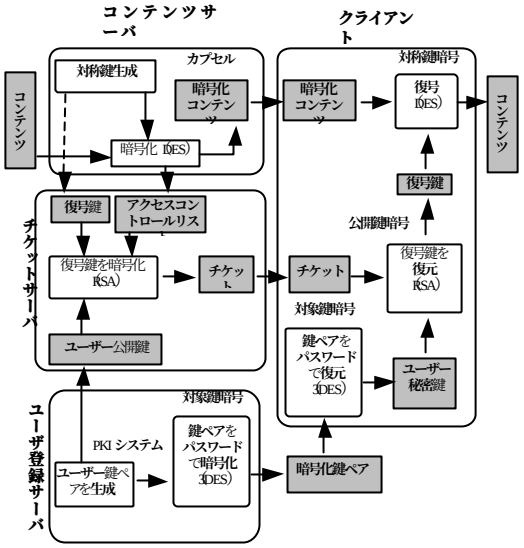
介護関連情報を、インターネットを活用して通信すれば、サービスの向上が期待できるが、情報漏洩に対する高いセキュリティが必須である。

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公開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公開手段の提供を目的とした研究である。

本研究は通信・放送機構の名古屋市福祉支援情報通信システムの開発・展開事業の一環として行っている。

2. カプセル化方式の概要

本システムにおいては、カプセル化方式で、暗号化を行った。カプセル化方式の概要を下図に示す。

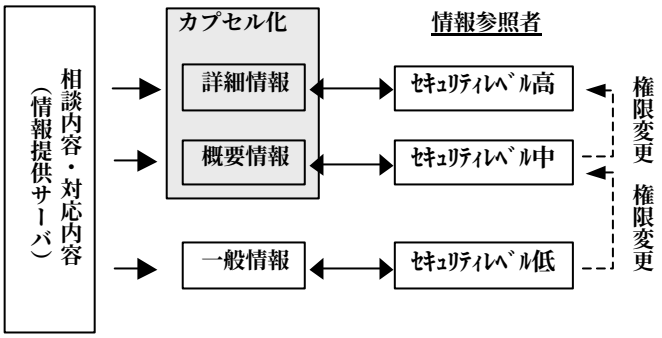


- コンテンツサーバは複数のコンテンツを暗号化してカプセルに格納する。同時に各コンテンツに対する各ユーザーの参照権をアクセスコントロールリストに登録する。
- カプセルは自由にﾀﾞｳﾝﾛｰﾄﾞできる。
- クライアントでは、ユーザーＩＤ、パスワードを入力し暗号ツールを立ち上げる。
- カプセルを参照しようとすると、暗号ツールはチケットサーバにチケットの発行を要求する。チケットは要求ユーザーの公開キーで暗号化され、発行される。
- クライアントでは、チケットからカプセルを復号化するためのキーを復元し、カプセルを復号する。
- サーバはアクセスコントロールリストを随時変更することができる。このため初期値は参照権が無いユーザーに、後から参照権を付加する事ができる。また、その逆も可能である。

また、この方式には次のような特徴がある。

- カプセルは参照しているときを除き、復号された状態とならない。また、復号の都度サーバからﾀﾞｳﾝﾛｰﾄﾞされるチケットが必要である。よって、通信経路のみならず、システム全体で、セキュリティが高い。

3. 本研究における取り組み



介護保険における「ご相談情報」の、公開業務に着目した。名古屋市では、各区において処理された「ご相談」の結果を市役所介護保険課に紙ベースで管理している。貴重な情報であるので、公開したいという要望があった。情報公開により、同一の相談を未然に防ぐ・同一の相談があったとき対応を適切に行えるなどの効果が期待できる。しかし、個人情報を含む内容であるので、セキュリティ上から庁内においても、今まで公開されてはいなかった。

暗号化の観点から見た、ご相談情報の特徴として、「相談内容」、「対応内容」などの項目の文章に、個人情報、事業者名などレベルの違う秘匿すべき内容が含まれていることが挙げられる。そこで我々はセキュリティレベルを一般、概要、詳細の３段階に

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

† Akihiko Masubuchi NEC Corp.
†† Ryuichi Matsuda NEC Corp.
‡ Ryo Saito NEC Corp.
‡‡Akira Iwata Vice President of Nagoya Institute of Technology
Project Leader, Telecommunications Advancement Organization of Japan

分け、それに対応して情報参照者をレベル低、中、高の３段階に分けた。一般情報は誰が参照しても良いレベルであり、詳細情報はすべての情報が記載されているものとした。

また、情報配信後でも権限レベルの変更が容易に出来るカプセル化方式の特徴を生かし、情報参照者の権限は、操作により１ランク上げることが出来るものとした。

情報の秘匿方法であるが、前述のように、「相談内容」などの項目中に秘匿すべき単語が含まれているため、項目ごと秘匿することが出来ない。本ｼｽﾃﾑでは、伏字を使用することにより情報の秘匿を行った。伏字化の詳細は、４　伏字の使用で説明する。

情報公開の方法は、一般情報を検索機能を付けて通常のＷＥＢ画面で表示し、その表示画面に、概要と詳細の両方の情報が入ったカプセルのダウンロードボタンと権限の変更要求のボタンを表示した。

4. 伏字の使用

相談内容、対応内容の秘匿すべき単語を隠すためには、一般情報、概要情報用に別の文章を入力する方式も考えられるが、これは効率が悪い。本方式で使用した伏字化には、次の特徴がある。まず、伏字といえば、単語などを「×」に変換する方法が一般的であるが、複数の単語を同じ「×」に変換したのでは文意が読み取れなくなる可能性が高い。そこで、情報登録者と相談し、単語ごとに別の伏字を割り当てることにした。また、伏字の種別が分かるように接尾語をつけるようにした。具体的には、「○○氏」、「××事業者」のように伏字化を行った。

伏字にすべき単語は相談ごとに異なり、また、同じ氏名、会社名でも相談ごとに適した接尾語が変化する。また、伏字にすべき単語は、相談一件当たりでは数種類に過ぎない。このため辞書機能などは持たせず、相談ごとに入力者が、一般情報と、概要情報に分けて、伏字にする単語入力、伏字の選択、接尾語の選択を行い、一括変換する方式を採用した。

この方式により、効率的かつ、読みやすい文章が表示可能と期待できた。

5. 実験方法と結果

実験は市役所の介護保険業務に携わる職員に閉じて行った。アンケート調査などにより、伏字化に関して次のことが分かった。

- 伏字化した文章でも状況は把握できる。

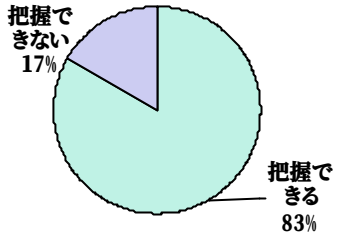
システム全体に関しては

- 操作説明書だけでは、分かりにくく、操作が難しいという印象を与える。
- 一度使えてしまえば、操作は問題なく行える。
- 狭い意味でのシステムとしては、十分実用的なシステムである。

また、一般情報として伏字化した項目に関しては、職員用としては、業者名を隠す必要は無いという意見が多かった。

なお伏字化の見易さの調査結果を下図に示す。

伏字化について



6. 考察

上記結果により、ｾｷｭﾘﾃｨの高い実用的ｼｽﾃﾑが、システム構築を通して仕様としては完成したと考える。

研究・実験全体の結果として、以下に示す成果を得られた。

- 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。
- システムの操作性は実用レベルであること。
- 伏字に関しては、「把握できる」という回答がほとんどであり、有効であると考えられる。

また、実験を通して以下のことが分かった。

- 慣れていない人が多く、システムを操作することに抵抗が大きい。

実験システムには、必要と考えられる機能を一律に組み込んだが、実運用の利便性を考えると、このシステム特有の操作や稀に使用する操作などの観点で層別化し、その部分に関しては、詳細な操作手順書を用意するなどの運用設計を検討しなくてはならないことが明らかになった。

今後の課題として以下の点が挙げられる。

- 提供する情報のレベルに関して検討し、最適なものに近づけていくこと。
- 慣れていない人を想定した、手順書の作成、または画面レイアウトの検討。

7. 今後の取り組み

本システムは、通常業務として継続的に、市の職員に使っていただく予定である。実運用の中で、問題点などの洗い出しと、解決を行っていく予定である。また情報参照者のレベルの分け方、及びそれぞれに提供する情報のレベルは、実運用の中で決める必要があると考えられる。

8. 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