4E-4

インテリジェント暗号を利用した情報マスキング方式の考察

工藤 史堯† 川邊 秀樹† 山本 隆広†
NTT セキュアプラットフォーム研究所†

1. はじめに

近年、企業や団体が保持する個人情報の流出事件が多発しており、中でもインターネットなどのネットワークを通じて文書や画像といったデジタルデータをやり取りする際には、第三者に盗み見られたり、改ざんされたりする危険性は非常に高くなる。そこで、特に情報の連携先が複数になる場合や開示先を複雑に指定する場合は必要な情報を必要な機関にだけ開示するための適切な開示先のコントロールが必要になる。

個人情報の連携先が複雑になるユースケースとして、必要な複数の申請を一度に行えるワンストップ申請［1］（図１）がある。ワンストップサービスは既に行政手続きや民間サービスの手続きで実現しているが、今後行政機関と民間企業の間で個人情報を連携させることになると、より個人情報の扱いに注意しなければならない。本稿では、個人情報を漏えいさせることなく、安全にワンストップ申請を実現するための方式について議論した上で、暗号化によって個人情報の開示制御を行うワンストップ申請方式の運用コストを、インテリジェント暗号を用いることで低減する方式を提案する。

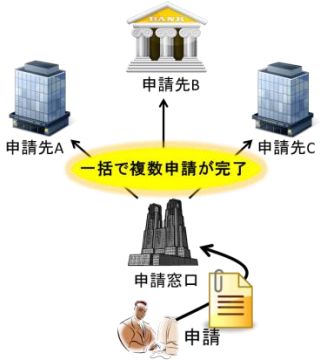

図１．ワンストップ申請概念図

2. ワンストップ申請の課題

前述のようにワンストップ申請では、申請窓口に一括で入力を受けた個人情報の中から、必要な情報のみが各申請先に開示されるよう配慮されていなければならない。不要な情報の開示を回避することができるワンストップ申請の実現方式としては、申請先ごとに必要な情報のみを記載した申請書を作成して送付する方式（申請書分割送付方式）と１枚の申請書をフィールドごとに暗号化（マスキング）した上でそのコピーを各申請先に送付する方式（一括申請書送付方式）の大きく２方式が考えられる。（図２）申請書分割送付方式を採用した場合には、申請者は申請書の真正性を担保するために、申請先の数だけ電子署名しなければならず、利用者の手間が増大するという課題がある。一方で一括申請書送付方式を採用すると、申請者の利便性は保たれるが、ワンストップ申請窓口と各申請先が暗号化・復号化に用いる鍵管理の手間に代表される、運用コストが増大するという課題がある。

本研究では、ワンストップ申請最大のメリットである利用者の利便性を優先して、一括申請書送付方式を採用することとし、その運用コスト改善に取り組む。

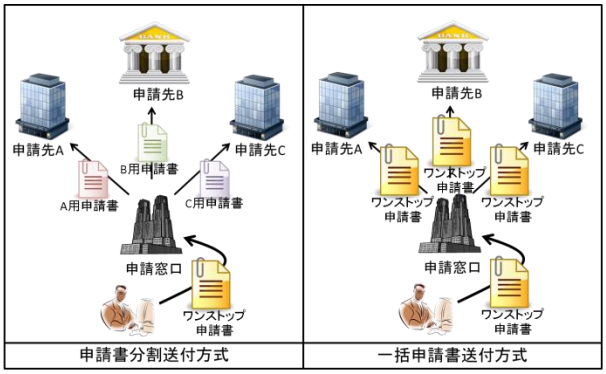

図２．ワンストップ申請実現方式分類

3. 提案方式

本研究では、前述の申請書回覧方式の運用コストを低減するために、申請書のマスキングにインテリジェント暗号［2］を適用した方式を提案する。（図３）インテリジェント暗号は、暗号・復号のメカニズムの中に高度なロジック（論理）を組み込むことが可能な ID ベース暗号の一種であり、それぞれの属性情報が入った属性鍵を配布すれば、この書類は「部長または人事部の課長だけが閲覧できる」といった開示制御ができる。このインテリジェント暗号を用いて、申請書の各フィールドを開示が必要な機関のみ復号できる条件式で暗号化を行えば（例：フィールド１は申請先 A と申請先 B のみ復号可能）、従来

A Study on the masking system of information using intelligent encryption

Fumiaki Kudoh† Hideki Kawabe† Takahiro Yamamoto†
NTT Secure Platform Laboratories†

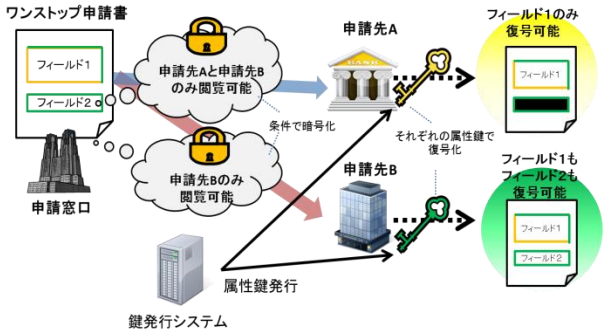

図３．提案方式

の暗号化方式を利用するよりも、鍵管理コストの低減が期待できる。ここで、鍵管理コストとは、暗号鍵へのアクセス制限、暗号鍵の暗号化、暗号鍵の定期更新を想定している。

4. 方式評価

本稿では、行政機関と民間企業の間で個人情報を連携させることになる、引っ越しワンストップサービスを具体例として、従来のハイブリッド暗号（共通鍵暗号＋公開鍵暗号）を利用した場合と今回提案するインテリジェント暗号＋公開鍵暗号を利用した場合について管理すべき鍵の数を比較した。鍵の数が少ないほど、上述した３つの鍵管理コストの低減につながるためである。また比較においては、引っ越し時に転出元、転出先の役所と銀行の計３機関にワンストップで申請を行うシナリオを設定し、それぞれの機関に提出する転出・転入届、住所変更届の実際の申請項目を利用した。（子細な申請項目については本稿では省略する）また、暗号化によるアクセス制御は組織単位（例：○○市役所△△課）で行うものとした。

両暗号方式での使用する鍵数の比較結果（表１）から、申請先側で管理する鍵の数はインテリジェント暗号を用いた方式の方が少なくて済むことが分かった。これは、ハイブリッド暗号が暗号化ブロックのパターンごとに各申請先に共通鍵を配布しなければならないのに対して、インテリジェント暗号では暗号化のパターン（条件式）に関わらず一つの申請先に対して属性鍵は一つで済むためである。（表１申請先が管理する鍵の数参照）そのため、ユースケースが複雑になればなるほどまた取り扱う申請サービス数そのもの増加すればするほど表１の両者の差は大きくなっていくことになる。また比較結果から、ハイブリッド暗号とインテリジェント暗号両者で管理する鍵の数に差が出る支配項は、申請先の数と暗号化ブロックのパターン（開示先の組み合わせ）数であることが分かった。

上記支配項より、インテリジェント暗号を利用した本提案方式は、申請先（個人情報の開示先）が多く、暗号化ブロックのパターンが多くなる（例えば、

表１．比較結果概要

	ハイブリッド暗号方式	インテリジェント暗号方式
申請窓口が管理する鍵の数	8 ・共通鍵５個 （暗号化ブロックパターンが5つ） ・各申請先の公開鍵３個	8 ・暗号鍵５個 （暗号化ブロックパターンが5つ） ・各申請先の公開鍵３個
申請先が管理する鍵の数（3機関合計）	11 ・各申請先の秘密鍵３個 ・共通鍵（転出先3個、転入先3個、銀行2個） →申請先数と暗号化ブロックパターン数に応じて増大	6 ・各申請先の秘密鍵３個 ・属性鍵（転出先1個、転入先1個、銀行1個） →申請先数と同数
申請窓口が配布する鍵の数	8 ・共通鍵８個 →申請先数と暗号化ブロックパターン数に応じて増大	3 ・属性鍵３個 →申請先数と同数

ワンストップサービスの種類が多数あるなど）ケースにおいて運用上非常に有効であると言える。ただし、システム構築にあたっては、鍵発行システムの運用などについて合わせて検討が必要である。

5. おわりに

本稿では、官民に渡ってのワンストップ申請を利用者の利便性を保ったまま安全に実現するために、一括申請書のコピーをフィールドごとに暗号化した上で各申請先に送付する方式を採用した際に課題となる鍵管理コストの増大を、インテリジェント暗号を用いて低減する方法を提案した。具体的な引っ越し時のワンストップ申請シナリオに基づいて提案方式を評価した結果、ワンストップ申請の実装方式選定における基礎情報として以下の２点を提供することができた。

・インテリジェント暗号が鍵管理コストの低減に有効であること
・鍵管理コストを決定づける支配項

しかし、インテリジェント暗号の実用化にあたっては、属性鍵生成時の認証や属性鍵の配布・管理方法など ID ベース暗号の一般的な課題 [3] が存在するため、今後これらの課題を踏まえた、実システムへの適用を検討していく必要がある。

6. 参考文献

[1] “引越手続ワンストップサービス調査報告書”. 経済産業省
http://www.meti.go.jp/policy/it_policy/report/report_04/01_02_honbun.pdf
[2] “インテリジェント暗号”. NTT 研究開発マガジン
http://www.ntt.co.jp/RD/OFIS/keyword/vol9.html
[3] “ID ベース暗号に関する調査報告”. CRYPTREC
http://www.cryptrec.go.jp/report/c08_idb2008.pdf