階層型ユーザに対応した部分暗号方式の検討*

4M－8

藤岡 秀樹†
日立ソフトウェアエンジニアリング（株）‡

1　はじめに

オフィス内の情報の電子化が進む中、ネットワークを利用したコンピューティング環境が広がり、情報の処理形態に変化が起きてきている。従来、情報処理センタのような専門の部署が汎用計算機を使用してデータベース化していたものを、ＷＳやＰＣを端末として検索・利用する形態へと変化してきている。これに伴い、ネットワーク上を流れる情報も、業務関連・社内文書・プログラムなど多様化しており、今後は、情報の保護や認証がなされることを前提に、秘密文書の流通も進むものと考えられる。

オフィス内の情報は、従業員に関するもの、営業・開発などの部門に関するものや全社内に関するものなどであり、それぞれの情報を参照可能な人間が異なる場合が多い。例えば、各部に所属する従業員の情報は部長が参照でき、各課の従業員の情報は課長が参照できるといったように、社内の職制に対応した形で参照する側のユーザが階層化される場合が考えられる。また、それぞれの情報には一般に公開しても良い情報と、参照可能なユーザを制限しなければならない秘密情報が含まれることも多い。例えば、人事情報などでは、入社年度や所属部署などは公開しても構わないが、給与や病歴など、職場の上長人事課員だけが参照可能でなければならない情報も存在する。

これらの情報を、ネットワークを利用して社員に公開する場合、秘密情報の保護が不可欠であり、そのために社内の職制などの階層に応じて、情報の一部分を暗号化して参照可能なユーザに制限を持たせる方式の検討を行なった。

2　情報参照制限へのアプローチ

公開された情報に対して参照可能なユーザを制限する方式として、共有情報を参照する際に、組織内の階層構造に対応してユーザに権限を持たせる方式[1]が提案されているが、ユーザは自分が属している階層やグループに対応している鍵を全て管理しなければならない。また、情報の部分暗号の方式として機密情報自身にアクセスレベルを設定しそれぞれに異なる鍵を設定する方式[2]が提案されているが、これも同様に、アクセスレベル毎の鍵をユーザが全て管理しなければならず、ユーザに負担をかけることになる。

そこで、今回ユーザは１つの鍵だけを管理し、その鍵を所有しているユーザがどの情報を参照可能かを階層情報で表現し、この階層情報を変更するだけで容易にユーザの参照可能なレベルを追加・変更できる方式を考案した。

3　公開情報の構成

情報の参照を制限するに当たってはデータベースの利用が最も容易であるが、社内でのLAN利用時だけでなく、営業員が社外で営業活動時等でも利用可能にするために、情報は通常のテキストファイルで構成し、市販の表計算ソフトウェアで参照可能な形で実現することにした。ユーザの階層の表現と、部分暗号を実現するために以下に説明する３つのファイルを使用する。

3.1　鍵階層構成ファイル

各ユーザには秘密情報へのアクセス権を示す鍵が唯一与えられる。この鍵を階層に対応させてテキスト形式で１行ずつファイルに格納する。各行は、一番左の鍵を持つユーザは、それ以外の鍵を持つユーザが参照可能なデータは全て参照可能であることを示す。木構造を構成した時に階層の最下層にあたる鍵には、暗号化された秘密情報を参照可能かチェックするためのコードを設定する。

[本部長]　[部長１]　[部長２]
[部長１]　[課長１]　[課長２]
[部長２]　[課長３]
[課長１]　課コード１
[課長２]　課コード２
[課長３]　課コード３
＜凡例＞　[ユーザ]: ユーザの鍵

図１．　鍵階層構成ファイルの例

*Examination of Partial Encryption Method for Classified Users
†Hideki Fujioka
‡Hitachi Software Engineering Co.,Ltd.

3.2 部分暗号設定ファイル

部分暗号設定ファイルは、3.3章に示す公開情報ファイルの構造を定義するもので、ファイル内の情報の内、どの情報が暗号化されているか、暗号化された情報を参照できるかどうかをチェックするコードは何かを設定する。

```
(AAA<6><3>) 従業員番号 <9> 部課コード <3> 従業員氏名 ?
(SHL<6>&<3>) 昇格歴 {%<5> %?}20
(KYO<6><3>) 教育歴 {<5> 講座名 ?}10

<凡例> (N)      N文字データ
       ?        可変長文字列
       %        暗号データ
       &        暗号チェックコード
       {}N      繰り返し最大数
       文字列   挿入文字列
       (文字列) 行の種別
```

図2. 部分暗号設定ファイルの例

図2の例では、"SHL"で始まる行のデータが暗号化されており、先頭から10文字めからの3文字がチェックのコードになることを示している。

3.3 公開情報ファイル

公開情報ファイルは、部分暗号設定ファイルに記載されたフォーマットで作成されたテキストファイルである。それぞれの行の先頭には、行の種別を表すコードが格納されており、これを利用して暗号化する情報を判断する。

```
AAA999001FFO 7S9999001 FFO 山田 太郎
SHL999001FFO 88-04 企画職2級 90-04 企画職1級
KYO999001FFO 94-10 セキュリティ 94-12 ネットワーク概論
```

図3. 公開情報ファイルの例

4 情報の暗号・復号化

情報を暗号化する際には、鍵階層ファイルと部分暗号設定ファイルを暗号化・復号化プログラムが持つ秘密鍵で暗号化し、公開情報ファイルのなかの部分暗号設定ファイルに設定された暗号化する情報を暗号化したものを順に並べて一つのファイルに格納する。

情報参照時には、ユーザが入力したパスワードを鍵階層から探して、そのパスワードで参照可能なコードの行に含まれた暗号化されている部分は復号して表示する。試作システムでは、ユーザインタフェースにMS-Excelを使用するため、一旦復号化した情報をファイルに格納しそれを読み込む。

4.1 処理性能

試作システムでは、暗号化プログラムはHP9000/750 (HP-UX8.05)、復号化プログラムはIBM-PC/AT互換機(486DX 33MHz)で開発した。

表1: 暗号化時間

情報数	秘密情報数	CPU時間(秒)	処理時間(秒)*1
2000行	100行	0.6	2.8
2000行	2000行	3.6	11.6

*1) ファイルの読み書き時間を含めたターンアラウンドタイム

表2: 復号化時間

情報数	秘密情報数	処理時間(秒)*1	読込時間(秒)*2
2000行	100行	11.6	42.4
2000行	2000行	76.5	25.6

*1) ファイルの読み書き時間を含めたターンアラウンドタイム
*2)MS-Excelでの読み込み時間

5 今後の課題

1. 復号速度の向上
   計測したデータは、約80名分であり中規模な会社の部単位程度の情報であるが、画面表示までの時間は54秒と運用に耐えない速度である。ただし、このうち、実際の復号処理の時間は3秒程度であるので、専用の表示プログラムを用意することで10秒以内に調整可能と思われる。

2. データ破壊への対応
   暗号化された情報は、パソコン上に通常のファイルとして格納される。そのため、MS-DOS,Windowsなどを利用するとアクセス制御は不可能であり、暗号化された情報が変更されてしまう可能性がある。

3. チェックコード
   復号化可能なユーザのチェックに利用するコードは、1箇所にしか記述することができない。1行に記述された情報に対し、ユーザごとに異なる場所を暗号化できる必要があるものと考えられる。

参考文献

[1] 大田幸由, 清水明宏: "暗号を用いた共有情報参照制御方式の検討", 電子情報通信学会技術研究報告 オフィスシステム, 93, 31, (1993).

[2] 岡野博一, 水津寿夫: "マルチ情報部分暗号化システム", 電子情報通信学会技術研究報告 情報セキュリティ, 93, 69, (1993).