マルチ情報部分暗号化システム

3N−7

岡野　博一　西本　健司　植田　義文
広島電機大学　徳山高専

１．はじめに

コンピュータネットワークが進展し，マルチメディア情報通信システム，グループウエア，電子会議システム等の開発が活発に行われている。これらのシステムのセキュリティは主としてパスワードによるアクセス管理が主体であって、ハッカー等にパスワードを盗聴され、データを盗まれる危険が大きい。一方、暗号化技術はエンドーツーエンドの回線暗号がプレゼンテーション層で用いられているが、それほど普及していない、むしろ、普及はこれからというのが現状である。

本稿では、アプリケーション層で暗号化を行う、マルチ情報部分暗号化システム（ＭＩＰＥＳ）を示す。このシステムはマンーマシン・インタフェースに優れた柔軟な暗号システムであり、暗号技術の普及の一助となると期待される。

２．マルチ情報部分暗号化システム（ＭＩＰＥＳ）

マルチ情報部分暗号化システムで用いるマルチ情報ドキュメントの概念図を図１に示す。テキスト、図形、表、画像などが混在している。さらに、ディジタル署名も同一ドユメントに表示される。もちろん、構造化文書としても良い。

さて、マルチ情報ドキュメントは電子メール、文書データベース等の形でネットワーク上を伝送される。この際、セキュリティが問題となる。ＭＩＰＥＳでは、暗号とディジタル署名を用いて、機密文書の伝送を可能にしている。主な機能を次に示す。1)ドキュメントの真に機密な部分のみを暗号化する。（もちろん全文暗号も可能である。）2)暗号鍵を複数用いて、機密部分のアクセスレベルを複数設定する。3)端末で暗号処理を行うことによって、センター

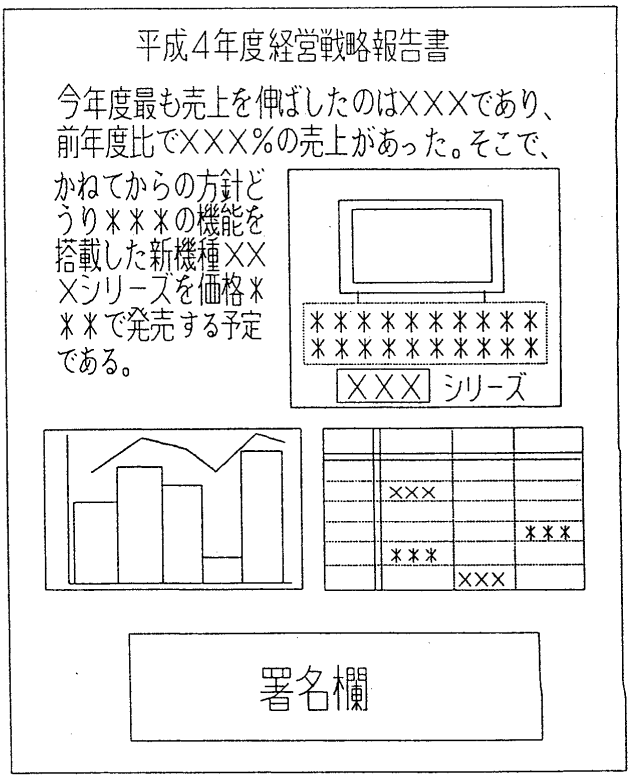

図１．マルチ情報ドキュメント

Multi-Information Partial Encryption System
Hirokazu Okano[1)]　Kenji Nishimoto[1)]　Yoshifumi Ueda[2)]
1)Hiroshima-Denki Institute of Technology　2)Tokuyama Technical College

管理者に機密情報を知らせないで、業務担当者、責任者に最高のセキュリティレベルを与えることができる。4)複数者のディジタル署名を直接ドキュメントに表示し、自由に確認することを可能にする。

したがって、秘書、業務担当者に通常のデータを書き込ませ、社長が最高のセキュリティを持つことを可能とする。図1において、×××および＊＊＊は異なる鍵で暗号化していることを示す。

次に、ディジタル署名の概念図を図2に示す。暗号鍵は秘密にされ、復号鍵は全メンバに公開されている。文書が回覧されると、受信者は印鑑と同様のイメージで自己の署名位置に署名を行い次のメンバに転送する。他者の署名は公開鍵を用いて自由に確認できる。署名の中味は、通常文の一方向性関数値、所属氏名、文書番号、年月日時刻、簡単なコメント等である。ただし、この方式で有効なＲＳＡ暗号はソフトプログラムによるよりもＬＳＩによって高速演算を行う方が良いと思われる。

文書番号 Ａ−１００
１９９２年１０月１０日

（ 通　　信　　文：Ｍ ）

署名者名（契約者名）：発信元（センター）、Ａ、Ｂ

署名者	ディジタル署名
発信元（センター）	＃（8857ad1e2f3514f3c2b8a59ee6f3bc887bc237a568abc36fe3d568df69ab148cbf369afed558）＃
メンバーＡ	¥〔773a2cf258545689afc3b2de3323ad4658〕¥
メンバーＢ	@〈328af18ed3567df74ef1237567189ff12a〉@

図２．デジタル署名

３．ポピュラーなアプリケーションソフトによるＭＩＰＥＳの実現

本格的ＭＩＰＥＳは暗号処理を組み込んだ統合化システムを開発する必要がある。メインフレーム、ワークステーション、パーソナルコンピュータ全てに適用できる。

今回の試作では、一太郎、花子、ロータス1-2-3、およびInformix-SQL（アスキー社）を用いてＭＩＰＥＳの開発を行った。暗号はＮＴＴのFeal-8を使用し、Ｃ言語を用いてシステム開発を行った。これらのデータの全文暗号、部分暗号とも容易に実行でき、さらに、テキスト、図形、画像の混在したファイルの全文暗号も実行できるようにした。Informin-SQLへの暗号の組み込みも容易である。さらに、実用的システムの開発を行っている。なお、本システムのオブジェクト指向型ＤＢへの検討も行いたい。

謝辞　有益な御助言を戴いた、横浜国立大学今井秀樹教授、東京理科大学金子敏信教授、ＮＴＴ情報処理研究所宮口庄司博士、ＫＤＤ田中俊昭氏に深謝します。

参考文献

１）岡野、河本：部分暗号化を用いた文書処理システム、1991年電子情報通信学会春季全国大会予稿集、D-261

２）岡野：部分暗号化を用いたデータベースシステム、1992年電子情報通信学会春季全国大会予稿集、A-338

３）宮口、白石、清水：FEAL-8暗号アルゴリズム、研実報第37巻第4/5、321-327