UUIを利用した鍵配送システム

5H－4

田中清人　小柳津育郎
NTTヒューマンインタフェース研究所

1.はじめに

・通信の高度利用に伴い、企業秘密やプライバシ保護のためのデータ・セキュリティの必要性が要求されてきている。この要求を満たす有力な手段に暗号がある。暗号方式は秘密鍵暗号と公開鍵暗号に大別される。現状では暗号化／復号速度の点より、ISDNを利用したマルチメディア通信のデータ暗号化にはDES[1]、FEAL[2]に代表される秘密鍵暗号が用いられる[3]。端末が秘密鍵暗号を用いて互いに他と秘密の通信を行うには、互いに通信する端末数に等しい暗号鍵が必要である。端末数が増えれば鍵の数が膨大になり、鍵の管理が重要な課題になる。本課題を解決する方法として、我々はISDNのDチャネルのUUIを利用し、慣用暗号を用いて認証と鍵共有を行うセンタ鍵管理方式を提案するとともに、あわせてその方式の実装と評価を報告する。

2.鍵配送手順

2.1　設置時の手続き

端末Tiを設置する時にあらかじめ処理する手続である。IDにもとづくの個別鍵生成法[4]を適用し、端末個別鍵を生成する。端末Tiの鍵Kiを式(1)により生成し、端末Tiの鍵管理テーブルに通信とは別の手段を用いてIDi、Giと鍵Kiを書き込む。記法を図1に示す。

P1,P2：秘密パラメータ(秘密値)。
Ki：端末Tiの暗号鍵(秘密値)。
IDi：端末Tiの加入者番号(公開可能)。
Gi：端末Tiの鍵修飾パラメータ(公開可能)。
Ri：端末Tiが生成する乱数。
Ks：セッション鍵。
F(K,d)：鍵生成関数。鍵Kを用いて、データdをCBCモードで暗号化した結果の最後のブロック。
eK(p)：平文pを鍵Kで暗号化した暗号文。
dK(c)：暗号文cを鍵Kで復号した平文。
mac(K,d)：MAC(Message Authentication Code)。鍵Kを用いて、データdをCBCモードで暗号化した結果の最後のブロックの上位4バイト。
⊕：ビット対応の排他的論理和。
‖：連結(concatenation)。
各データ長は、MACが4バイトである他はすべて8バイト。

図1　鍵配送手順における記法

$$Ki = F(P1 \oplus Gi, IDi \,\|\, Gi \,\|\, P2) \qquad (1)$$

2.2　通信時の手続き

端末Tiが端末Tjを呼び出して暗号通信するときの

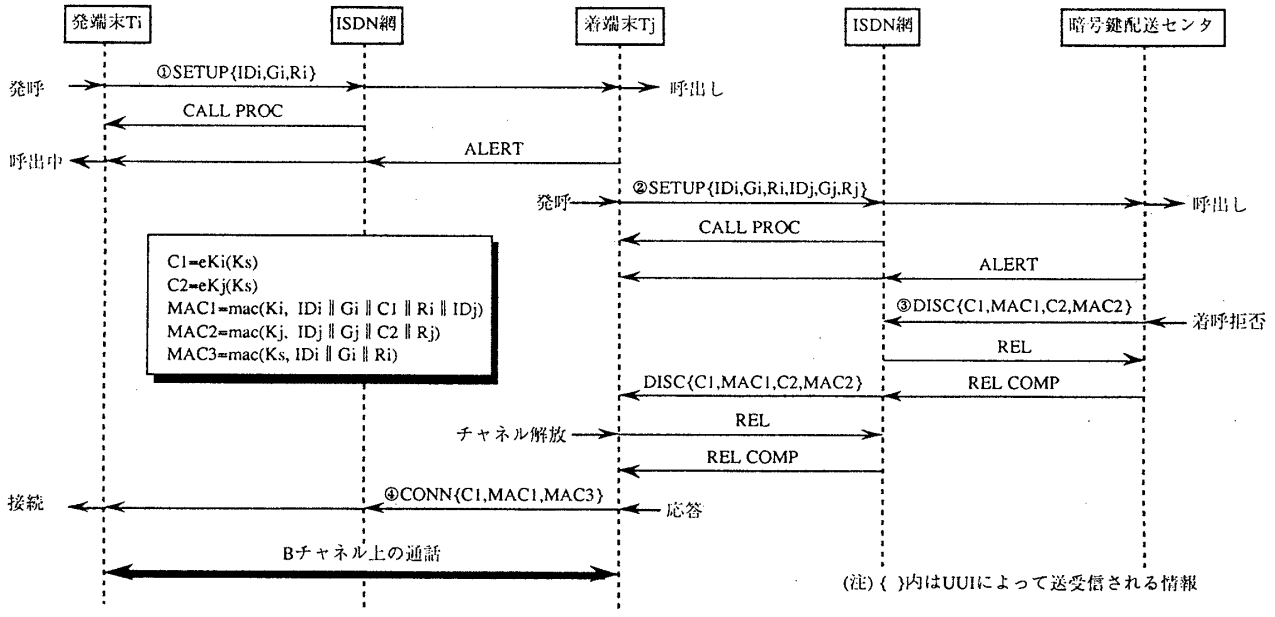

図2　鍵配送シーケンス

セッション鍵を共有する手続きである。図2に示す。本鍵配送手順では着端末からの鍵配送要求に対し鍵配送センタは着呼拒否で応答し、4回のUUIで鍵配送を行うため、全国一律4×0.4=1.6円で鍵配送を実現で

Key Distribution System using ISDN User-to-user Signalings
Kiyoto Tanaka, Ikuro Oyaizu
NTT Human Interface Laboratories
1-2356,Take,Yokosuka-shi,Kanagawa-ken,238-03,Japan

きる。

3.暗号鍵配送システム

鍵配送機能付き電話機はディジタル電話機に暗号用LSI[3]を追加するとともにファームウェアを改造することで実現した。また、暗号鍵配送センタはPC9801パソコンにMS-DOS配下で動作するISDN暗号通信用拡張ボード[5]を実装し、APを作成することで実現した。

4.評価

4.1 鍵配送時間

図3に鍵配送時間の測定結果を示す。図3から明らかなとおり、暗号鍵配送センタから着端末へのセッション鍵配送を1秒以下で完了している。従って、マンマシンインタフェース上問題なく、暗号鍵配送のサービスを実現できる。

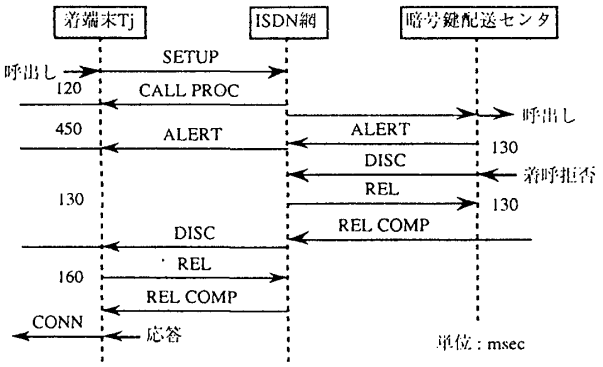

図3 鍵配送に要する時間

4.2 鍵配送センタの処理能力

(1)評価モデル

暗号鍵配送センタの処理能力を待ち行列モデルを用いて評価する。PC9801パソコンには複数枚のISDN暗号通信用拡張ボードを実装できるため、同時に最大(回線数×2)個の呼を受付け可能である。一方、OSはシングルタスク構成であるため、呼を一個ずつ処理する。従って、本待ち行列は待合せ放棄のある待時式完全線群のM/D/1(m)モデルとなるが、解析簡単化のためM/M/1(m)モデルで解析する。

(2)トラヒック条件

・呼損率 : 0.01以下
・呼量 : 0.225アーラン／回線
・平均保留時間 : 80秒

(3)評価結果の例

呼損率が0.01以下という条件において、許容待ち個数と接続可能電話機台数およびそのときの増加待ち時間の関係を図4に示す。暗号鍵配送センタが鍵配送のために収容する回線数をKとすると、K=(m+1)／2となる。従って、図4より暗号鍵配送センタが高々2回線を収容すれば、約500台の秘話機能付き電話機をサポートできる。このときの鍵配送時間の増加分は130msecとなる。

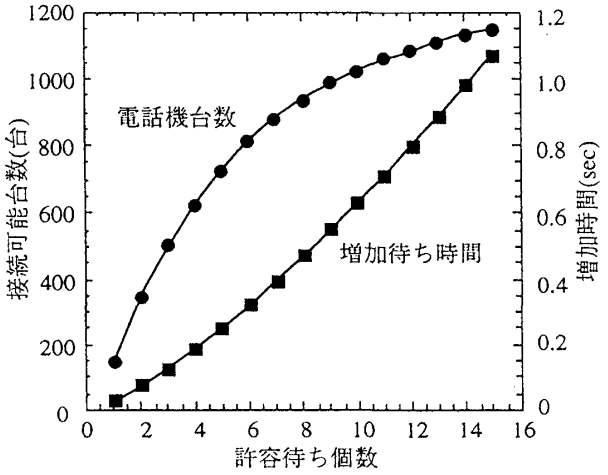

図4 接続可能電話機台数と増加待ち時間

5.おわりに

ISDNのUUIを利用し、慣用暗号を用いて認証と鍵配送を行うセンタ鍵管理方式を提案し、パソコンを使用した暗号鍵配送センタと鍵配送機能付き電話機で構成して評価した。1.6円で鍵配送が可能であり、鍵配送に要する時間も通常の呼接続時間に対し約1秒の増加で済む。また、企業内の数100回線で使用されるものであれば暗号鍵配送センタもパソコン程度の処理能力で十分であることを示した。

謝辞 ご指導いただいた情報通信網研究所宮口庄司主幹研究員をはじめとする宮口研究グループの皆様に深く感謝します。

参考文献

[1]FIPS pub.46 : Data Encryption Standard, NBS, (1977).
[2]宮口, 白石, 清水 : FEAL-8暗号アルゴリズム, 研実報, Vol.37, No.4/5, pp.321-327 (1988).
[3]小柳津, 松本, 石井 : ISDNマルチメディア通信用ワンチップ暗号プロセッサ, 情処論誌, Vol.33, No.2, pp.91-99 (1992).
[4]宮口, 岩田 : ICカードの個別鍵管理方式, 信学技報, ISEC88-37 (1988).
[5]田中, 松本, 小柳津 : ISDNマルチメディア暗号通信用PC拡張ボード, 信学技報, OFS91-64 (1992).