パソコン通信における暗号鍵配送方式の考察

6J-1

小林哲二

ＮＴＴ情報通信処理研究所

1. まえがき

パソコン通信で重要なデータを通信するときには，暗号通信が有効である．暗号通信の導入方法には，回線暗号装置による方法があるが，パソコン本体に比べてまだコストが大きい．これに対して，利用者の通信データをソフトウェアにより暗号化を行う方法では，高速な慣用暗号[2]のアルゴリズムを用いれば，低コストな暗号通信を行うことができる．この場合の問題は，二つのパソコンで同じ暗号鍵を共有するための鍵配送である．

2. 鍵配送手順

(1) 鍵の種類と階層

パソコン端末をノードと呼ぶ．鍵配送と暗号通信の概念を図１に示す．この方法により，公開鍵系アルゴリズムの長所(事前に秘密情報を配送する必要がない)を生かし，処理速度が遅い欠点を補うことができる．鍵の階層では，鍵暗号化鍵(マスタ鍵と呼ばれることもある)とデータ鍵を用いる二層形態が知られており，その方法を用いる．鍵の種類は，次のとおりである．

①鍵暗号化鍵（KC_{ab}）：　データ鍵を暗号化するための鍵．公開鍵系の鍵配送アルゴリズムを用いて配送し，ノード間で共有する．

②データ鍵（KD_{ab}）：　通信データを暗号化するための鍵．鍵暗号化鍵で暗号化して配送し，ノード間で共有する．

(2) 鍵暗号化鍵の配送

鍵暗号化鍵KC_{ab}を配送するための公開鍵系の鍵配送アルゴリズムとして，Diffie-Hellman型とＲＳＡ暗号型がよく知られている．注意点は，鍵配送時に，相手ノードの認証も行う必要があることである(回線接続時の端末ＩＤ確認のみでは，不正者が端末になりすますときの攻撃を防止できない)．本稿では，著者の提案による二重暗号型鍵配送方式[1]を用いることとし，その鍵配送方式のパラメータを表１に，鍵暗号化鍵の配送手順を図２に示す．この方式の安全性は，離散対数の計算の困難さに基づいている．

(3) データ鍵の配送

データ鍵の生成と配送は，通信処理単位ごとに行う．なお，Ｅ(Ｘ，Ｙ)は鍵Ｘによるデータの暗号化，Ｄ(Ｘ，Ｙ)は鍵Ｘによるデータの復号化を表す．

Ｓtep １：　ノードＡは，データ鍵KD_{ab}を生成する．次に，鍵暗号化鍵KC_{ab}でKD_{ab}を慣用暗号のＣＢＣモードにより暗号化して，

$$U_1 = E(KC_{ab},\ KD_{ab} \| T_a \| ID_a)$$

を計算し，ノードＢに送信する．T_aは現在の時刻，ID_aは，ノードＡのノード識別子(電話番号等)である．

Ｓtep ２：　ノードＢはU_1を受信すると，鍵暗号化鍵KC_{ab}で復号化して，

$$U_2 = D(KC_{ab},\ U_1) = KD_{ab} \| T_a \| ID_a$$

を求める．次に，ノードＢの現在時刻をT_bとして，

$$|T_a - T_b| < \varepsilon$$

であることにより，T_aの正当性を確認する．更に，ID_aの正当性を確認する．なお，εは，ノードごとに異なる値でよく，任意のノードに関して，受信データ長Ｌ，受信回線の伝送速度Ｇ，受信回線の固有最大遅延時間(交換機の処理，電磁波伝搬等に起因)γ，他ノードとの時計の予測最大偏差δから，

$$\varepsilon = L/G + \gamma + \delta$$

により，決定できる．　□

(4) 鍵確認

鍵確認は，鍵配送時の通信データの改ざんを検出するために行うものであるが，上述の鍵配送方式では，次の理由により，不要である．

①鍵暗号化鍵の配送時：　通信データの改ざんは，表１の秘密情報タイプＩの検証時の異常により，検出できる．

②データ鍵の配送時：　メッセージの改ざんは，ノード識別子が正しく復号化されないことにより，検出できる．

3. 性能

鍵暗号化鍵の配送では，べき乗剰余計算が必要なため，処理時間がかかるが，通信処理単位とは独立に，比較的長期の周期で更新すればよい，通信処理単位ごとの処理には影響ない．

4. 方式比較

現在，鍵配送は，慣用暗号系，ＩＤベース系，公開鍵系に分類でき，それぞれ適用領域がある．①慣用暗号系は，簡単であるが，鍵配送以前に，秘密情報を人手配送することが必要である．②ＩＤベース系では，安全な情報管理センタを設置し，かつ情報管理センタは，鍵配送の以前に，秘密情報を各ノードにＩＣカードなどの物理的な手段で安全に配送しておく必要がある．③公開鍵系は，秘密情報の人手配送が不要であるため，安全性を向上できる(公開情報は，安全に伝達する必要がある)．

以上の状況を考慮すると，対等な利用者間で重要なデータ通信を行うときのパソコン通信に関しては，本稿のように，慣用暗号系と公開鍵系を組み合わせて鍵配送を行う方式が有効である．

5. むすび

パソコン通信において，二重暗号型鍵配送を，二層の鍵構成に適用する鍵配送方式を提案した．

［文献］

(1) 小林："暗号通信における２重暗号型鍵配送方式"，信学論，J71-D，9，pp.1815-1822(1988).

(2) 宮口："慣用暗号－ DES方式とFEAL方式"，最近の情報ネットワークセキュリティとその応用専門講習会(信学会)，pp.16-23(1988).

A Cryptographic Key Distribution Method for Personal Computer Communications

Tetsuji KOBAYASHI

NTT Communications and Information Processing Laboratories

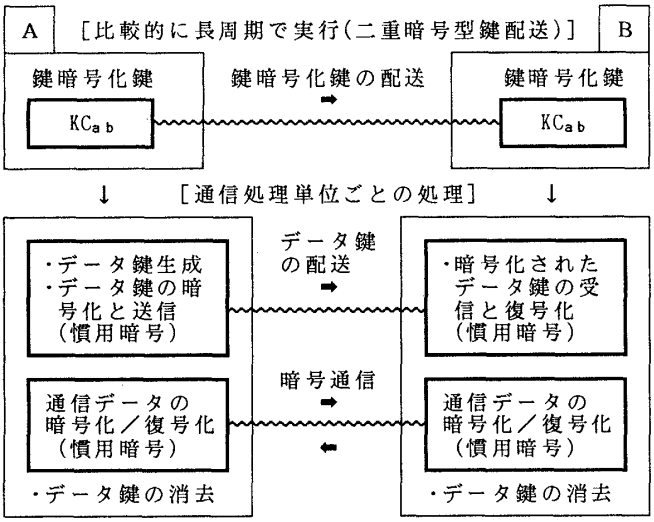

図1　鍵配送と暗号通信の概念

表1　二重暗号型鍵配送方式のパラメータ

情報		ノードA	ノードB
公開情報	共有	f(·):慣用暗号による一方向性関数 p : 素数	
	個別	$f(Q_{ab}(1, M_a))$ $f(Q_{ab}(2, M_a))$ $M_a=0,1,\cdots,J$	$f(Q_{ba}(1, M_b))$ $f(Q_{ba}(2, M_b))$ $M_b=0,1,\cdots,J$
秘密情報	I	$Q_{ab}(1, M_a)$ $Q_{ab}(2, M_a)$ $M_a=0,1,\cdots,J$	$Q_{ba}(1, M_b)$ $Q_{ba}(2, M_b)$ $M_b=0,1,\cdots,J$
	II	K_a (注2) KI_a (K_aの逆元)	K_b (注2) KI_b (K_bの逆元)
	III	RN_c (乱数)	V_b, RN_d (乱数)

備考：各パラメータ等の詳細は，文献(1)参照.

[二重暗号型鍵配送の初期化と実行] ①共有公開情報(f(·), p)の保持，②自ノードの秘密情報タイプIの生成と保持，③自ノードの個別公開情報の計算，④相手ノードの個別公開情報の取得と利用者間の確認(電話等による公開情報の確認)を行う．1回の初期化で，任意の回数の二重暗号型鍵配送の実行が可能.

[二重暗号型鍵配送の実行] 二重暗号型鍵配送を実行し，その結果，各ノードは鍵暗号化鍵KC_{ab}を共有する.

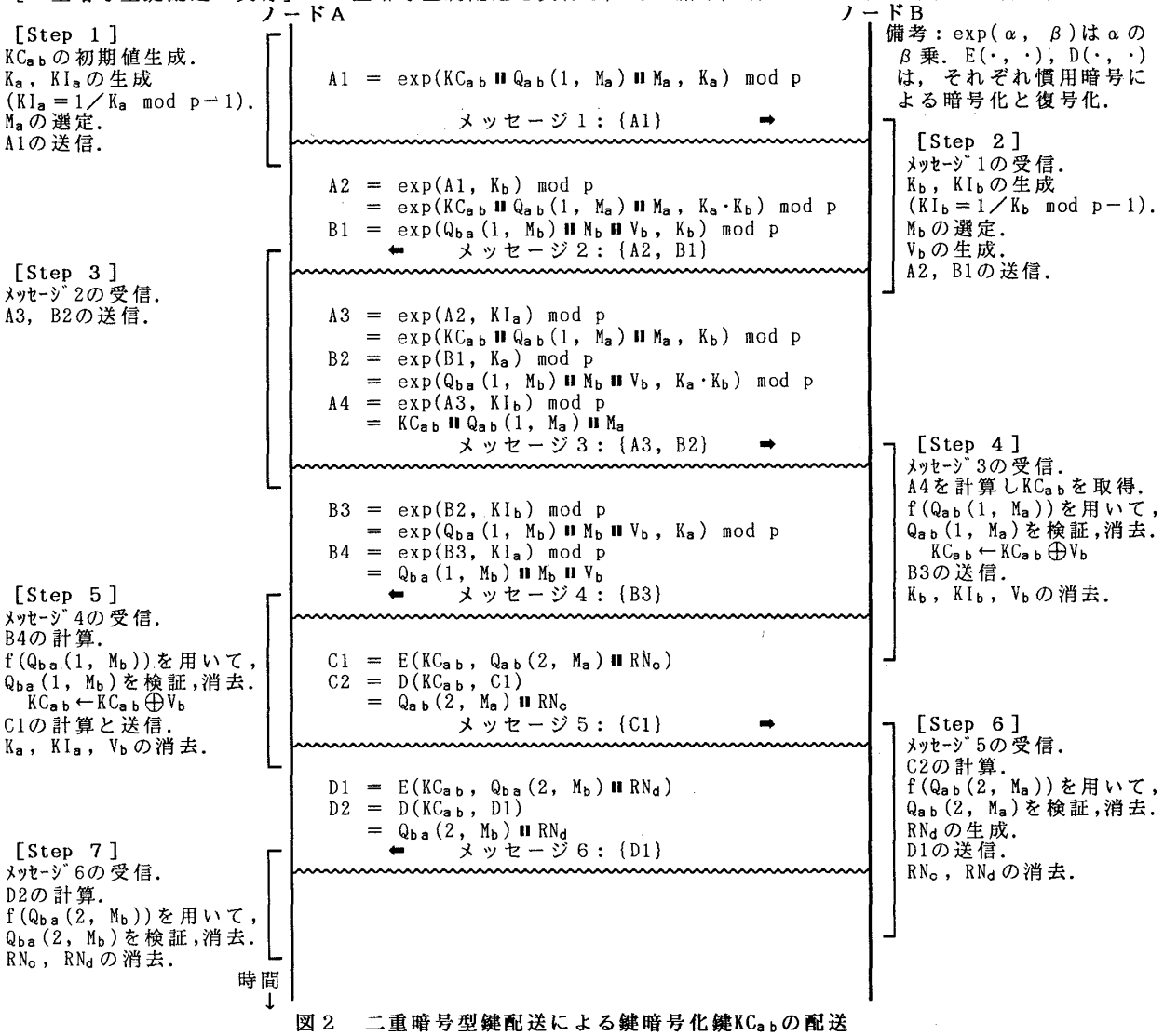

図2　二重暗号型鍵配送による鍵暗号化鍵KC_{ab}の配送