不正アクセス発信源追跡システムにおける暗号通信方式及び鍵管理方式の検討*

1G－6

田中　美穂
東日本電信電話株式会社　法人営業本部マルチメディア推進部
永吉　孝行
東日本電信電話株式会社　研究開発センタ

1.はじめに

不正アクセス発信源追跡システム（以下、追跡システム）の研究開発の一環として、前年度行った鍵管理方式の検討結果を踏まえ[1]、通信データの原本性保証及びデータの隠蔽を効率的に実現する鍵管理方式及び性能の検討を行い、通信箇所毎の暗号・認証技術の適用法について決定した。

2．システムの特徴

追跡システムの特徴を以下に示す。

① AMNはインターネット上に多数散在しており、追跡依頼は隣接・非隣接に関わらず追跡依頼元から直接行われる。

② AMN内各構成要素は追跡マネージャとのみ通信を行い、個々のAMNは閉じた管理空間とみなすことができる。

3．課題、評価の観点

暗号・認証技術の決定には、鍵の生成・配送・保持・世代管理・削除・リカバリと言った一連の鍵管理も考慮することが重要である。ここでは、暗号・認証技術として、以下の組合せについて特に重要となる鍵管理の課題及び追跡時の性能について（表1参照）検討する。

方式1：公開鍵暗号方式・デジタル署名
方式2：共通鍵暗号方式・メッセージ認証
方式3：共通鍵暗号方式・デジタル署名

検討は、通信箇所ごとの特徴にかんがみ、AMN内・AMN間に分けて行う。

ここで、暗号・認証技術は鍵配送に兼用する。暗号・認証用の鍵は、通信でしか使わないため、削除鍵を管理しない。リカバリは構成要素の削除と追加の組合せ処理を行うとし、鍵保持で検討する構成要素の追加・削除と同様とする。

表1　課題と評価の観点

課題		評価の観点
鍵管理	鍵更新 ・　鍵生成 ・　鍵配送 ・　世代管理	生成時の安全性 鍵生成の負荷 世代管理にかかるコスト 秘密情報の配送
	鍵保持	信頼性の担保 構成要素の追加・削除の影響範囲
性能		追跡可能時間

4.比較検討

4-1 鍵管理

（1）鍵更新

AMN内：方式1では、各構成要素で鍵を生成し、公開鍵のみの配送を行い、前世代の鍵によるデジタル署名を添付することによって、生成の安全性及び負荷、秘密情報の配送の危険性について解決できる。鍵更新のタイミング・世代管理の手法については[1]参照のこと。方式2では、Diffie-Hellman鍵配送方式（以下、DH法）にて共通鍵をセッション単位に共有することで、課題を解決できる。方式3では、方式1と方式2を併用。

AMN間：後述のように、鍵管理機構の追加があるが、AMN内と同様。

（2）鍵保持

AMN内：いずれの方式でも特徴②より通信相手が特定しているため、あらかじめ各構成要素に鍵生成情報を個別に保持することにより、信頼性の担保

---

* A discussion of encrypted data transmission methods for unauthorized access tracing system: Miho Tanaka and Takayuki Nagayoshi, NTT East Corp.

ができる。

AMN 間：特徴①より通信相手が追跡発生時まで確定しない。方式１では、追跡マネージャ間に新たに鍵管理機構を設け、認証を補完し課題を解決する。運用方法は、[1]参照。方式２では、鍵生成情報を全体で一つのものを使うのは信頼性が低い、しかし個別に管理するのは構成要素の追加・削除処理など管理面を考慮すると好ましくないことから、課題解決とならない。方式３は、方式２と異なり共通鍵の鍵生成情報を全体で共有しても、認証用の公開鍵を併用（方式１と同様）することにより課題を解決できる。

（３）鍵管理評価

鍵管理における評価結果を表 ２に示す。

本検討結果より、AMN 内では世代管理が必要ではない方式２が若干優位ではあるが、方式を限定するまでの要因ではない。AMN 間では、鍵管理面で方式２は不可とする。

表 ２ 鍵管理評価

	AMN 内			AMN 間		
方式	方式１	方式２	方式３	方式１	方式２	方式３
鍵保持	○	○	○	○	×	○
鍵更新	△	○	△	△	○	△
評価	○	○	○	○	×	○

4-2 性能

（１）モデル

追跡基本モデル（NH=40, NA=3, M=32, [2]参照）における、追跡処理時間(14.3 秒)に、暗号・認証にかかる時間を加えた性能を見積った。本モデルでは、追跡処理の大部分を AMN 内の処理が占めるため、AMN 内の処理時間が全体の追跡時間に大きく影響する。

ここでは暗号・認証にかかる時間を加えた場合の追跡時間が、追跡可能時間（25.6 秒、[2]参照）より小さければ追跡可能であり、性能要件を満たしているとする。

（２）考察

計算結果及び性能評価結果を表 ３に示す。

AMN 内において方式１を用いる場合は、追跡可能時間を超過しているため、不可とする。

その他の組合せについては、追跡可能時間内となり性能要件を満たしている。なお追跡処理時間が長くなることは、それだけ必要情報の蓄積及び処理能力などシステムコストがかかるため、全体の処理時間が最も短くなる方式とする。

表 ３ 性能評価

AMN 内 / AMN 間	方式１		方式２		方式３	
方式１	35.9	×	17.9	○	19	○
方式３	34.5	×	16.5	○	17.6	○

単位(s)

5. 結論

評価の観点からみて最も優れた組合せである、AMN 内:方式２、AMN 間:方式３を適用する。

AMN 内は、暗号・認証ともに同一の共通鍵で行う。鍵生成情報を事前に通信者間毎に個別に保持した上で、DH 法にて、セッション鍵を共有する。

AMN 間は、暗号に共通鍵暗号方式、認証に公開鍵暗号方式を用いる。認証を補完する目的で鍵管理機構を介在させ、マネージャは AMN 間追跡の都度、相手の公開鍵を鍵管理機構から取得し認証に用いる。また共通鍵は、鍵生成情報は共通とするが、AMN 内と同様に DH 法にてセッション鍵を共有する。

謝辞

本研究は、通信・放送機構(TAO)の委託研究テーマ「不正アクセス発信源追跡技術に関する研究開発」の一環として行われているものである。

参考文献

[1]永吉他：“不正アクセス発信源追跡システムの通信データ防御に関する鍵管理方式の検討”，情処 62 全大講演論文集 (3)，pp.287-298, Mar. 2001.

[2] 池田他，“不正アクセス発信源追跡システムのアーキテクチャの有効性検証”，情処 62 全大講演論文集(3)，pp.284-285, Mar. 2001.