一般講演〔１Ｈ会場〕（３月 12 日（火）13：00～15：00）

アプリケーションセキュリティ

座長　村山　優子(岩手県大)

１　PKI 技術を利用したセキュアオンライン人材仲介システムの提案
○米田　健，中川路哲男(三菱)

２　Information Flow Control
○井崎慶之，田中勝也，滝沢　誠(電機大)

３　公開鍵暗号を用いた安全なメッセージ伝達方式の提案
○田中裕之，筒井章博，矢田浩二(ＮＴＴ未来ねっと研)

４　電子チケットの経路非依存配信手法
○仁野裕一，谷　幹也，市山俊治(ＮＥＣインターネットシステム研)

５　グループ鍵生成プロトコールに関する一考察
○陳　志松，山本雅基(デンソークリエイト)
　矢尻えみ子，神保雅一(慶大)，石田　亨(ソフトピアジャパン)

６　ログ管理システムの提案
○中野初美，中川路哲男(三菱)

ログ管理システムの提案

1H－06

中野 初美　中川路 哲男
三菱電機(株) 情報技術総合研究所

1．はじめに

前世紀末に始まったIT革命により、我々は、インターネット社会ともいうべき新しい社会の到来を迎えている。一方、官公庁ホームページへの不正アクセス等に見られるネット犯罪の増加等の新たな問題も本格化しつつあり、情報システムのセキュリティに関する国際基準であるISO15408やISO17799等の策定にも見られるように、情報システムセキュリティを如何に実現するかが危急の課題となっている。情報システムセキュリティ実現における重要な機能の一つとしてセキュリティ監査がある。セキュリティ監査は、システムが正常に(セキュリティ上問題なく)動いていることの証明にもなる。セキュリティ監査では、各アプリケーションやOS等で記録されるログが重要なポイントになる。本稿では、このログに着目し、セキュリティ監査実現に有効なログ管理システムについて提案する。

2．問題点

一般に、官公庁や社会インフラ等の高度なセキュリティを要求されるシステムでは、システムに不正アクセスや不正動作がなく、正常に動作していることを保証する機能が要求される。このためには、安全性の高いログの取得が不可欠である。

現状、この点に関しては

- CD-R等のOne-Time-Write-Onlyな媒体への定期的バックアップ
- システム内でログを重複、分散記述し、マッチングをとることによる不正動作の検証

等が一般的である。

しかし、この状態では、一見してわからないようなログの部分的改竄や削除などが行われた場合、それを検出することができず、ログの完全性が保証できない。このため、システムが正常に動作していることを保証するには不十分であると言える。

一般に、データの完全性保証には、公開鍵暗号を利用したデータ署名が有効である。しかし、署名には公開鍵暗号鍵対の秘密鍵を利用しているため、処理時間は遅い。対象データがログである場合、その出力速度と処理時間を比した場合、データ署名がログ出力のボトルネックになり、返って不正ユーザの攻撃対象になりかねないという危険性がある。

3．提案

このような問題点を解決するために、我々は耐タンパセキュアモジュールとKeyed-Hashを利用した監査証跡管理システムを提案する。本提案のポイントは次の点である。

【Keyed-Hashの利用によるログ処理速度の向上】
ログの完全性保証には、Keyed-Hashを利用する。この時のKeyを秘匿することにより、公開鍵暗号によるデータ署名よりも高速にログ完全性保証が実現できる。

【耐タンパセキュアモジュールを利用した鍵管理】
上のKeyed-Hashで使用する鍵を耐タンパセキュアモジュール内で管理する。モジュール内部で生成、演算、蓄積を行い、外部に公開しないこと、及び、複数の耐タンパセキュアモジュール間でPKI技術を利用した鍵管理を適用することにより、

A Proposal of the LOG management system for audit
Hatsumi Nakano, Tetsuo Nakakawaji
Information Technology R&D Center, Mitsubishi Electric Co.