複数計算機間での機密情報拡散を追跡するためのログ管理手法

Log Management for Tracking Sensitive Information among Multiple Computers

前田 明彦 † 高橋 健一 † 川村 尚生 † 菅原 一孔 †
Akihiko Maeta † Kenichi Takahashi † Takao Kawamura† Kazunori Sugahara †
† 鳥取大学大学院　工学研究科　情報エレクトロニクス専攻

1　はじめに

近年，計算機の性能の向上や普及により今まで紙媒体で管理していた情報を計算機で管理する機会が増大している．また，情報を電子化することで，一度に大量の情報を持ち出すことも可能となった．そこで，管理する情報は機密性の高い情報から機密性が低い情報までさまざまであり，機密性の高い情報は外部に漏れてしまうと企業や個人にとって大きな損失になる．したがって，計算機で情報を管理する機会の増大に伴い，情報漏洩事件が深刻な問題となってきている．個人情報漏洩のインシデント分析結果 [1] によると個人情報漏洩の原因の約 7 割は,「管理ミス」,「誤操作」が占めている.「管理ミス」とは，情報の公開・管理ルールの明確化や遵守が不十分であることが原因である.「誤操作」については，メールの送信先の宛先の間違いや操作ボタンの押し間違いなど，計算機利用者の不注意が原因である．操作確認などで計算機利用者の不注意は防止できると考える．そのため，本研究では，原因のひとつである「誤操作」に論点をおく.「誤操作」を防止するための対策として，機密情報を追跡し，機密情報を送信または USB メモリなどの記憶媒体に書き出す際に警告を出すなどして操作を確認及び制御するシステムを提案する．

2　機密情報拡散追跡・制御

機密情報とは，個人情報などの機密性の高い情報が含まれた情報であり，計算機利用者によって指定され，ファイル単位で扱う．また，機密情報は，読み込まれた後，別のファイルなどに書き出しが行われることで拡散する可能性がある．このため，機密情報を読み込んだ後に情報が書き出されたファイルにも機密性の高い情報が含まれている可能性がある．これらのファイルが外部に持ち出されると漏洩の危険があるので，機密情報の拡散を追跡し，持ち出しの操作を制御する．

現在では，単一計算機での機密情報の拡散追跡・制御 [2] は研究されている．このシステムでは単一計算機を対象としていて個人が利用する計算機を想定している．しかし，企業などの組織では複数の人間で情報を共有して作業することが考えられる．その場合，ネットワークのような複数計算機間での機密情報追跡・制御が必要となる．そのため，単一の計算機内での機密情報の拡散追跡・制御では，ネットワークなどの複数計算機での環境には対応できない．そこで，ネットワーク内での機密情報の拡散を追跡し，機密情報がネットワーク外へ持ち出されようとしたときに警告や持ち出しの制御を行うシステムの実現を目指す．

3　複数計算機での機密情報拡散追跡・制御

システムの概要を図 1 に示す．管理ネットワークとは機密情報の拡散追跡・制御機能を持った計算機の集まりとし，管理ネットワーク内では機密情報が追跡できるとする．複数計算機での機密情報の拡散を追跡す

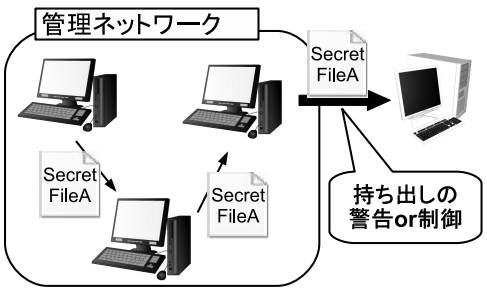

図 1: 提案システムの例

るためには，機密情報が拡散する過程をログとして記録することで，蓄積したログから拡散経路を特定できる．このため，蓄積するログをどのように管理すればシステム全体として効率が良くなるか検討する必要がある．また，機密情報を他の計算機に送信する場合に，送信先の計算機で機密情報の拡散追跡・制御ができなければ，情報漏洩の原因を特定することができない．そこで，送信先の計算機が機密情報の拡散追跡・制御が可能であるかの判断が必要となる．最後に，機密情報を管理ネットワーク外へ持ち出す際に，誤って機密情報が持ち出される可能性がある．そのため，不正な操作や機密情報の誤った持ち出しを防止する必要がある．そこで，機密情報の持ち出しの許可を与える仕組みが必要である．すなわち，複数計算機で機密情報の拡散を追跡・制御するために以下の課題を解決する必要がある．

- ログ管理手法の検討
- 管理ネットワーク内外の判断
- 機密情報の持ち出し許可の取得

よって本研究では，複数計算機間の機密情報追跡を対象としたシステムの実現を目指し，機密情報の拡散情報として記録するログの管理方法の検討を行う．

4 ログの管理手法の検討

ネットワークの種類や環境によって適切なログの管理手法が手法が変わる．現在，ファイルのアクセスログなどの一般的なログ管理手法は，サーバでの集中管理型である．しかし，小規模な環境や複数のネットワークが存在する環境などさまざまなネットワークが考えられる．これらの環境では，コストなどを考えると，サーバが必ずしも準備できるとは限らない，よってログ管理サーバを準備できるかどうかがログ管理に大きな影響を与える．次に，ネットワーク内の計算機の性能に偏りがある場合は性能のよい計算機で集中管理したほうがよい．しかし，偏りがない場合には，分散してログを管理するほうが負荷の偏りが分散され効率的にログを管理することができるかもしれない．さらに，ログの発生頻度や機密情報の拡散経路検索が発生する頻度によっても集中管理と分散管理のどちらが適切な管理手法であるか変わると考え，システムの環境も影響を与えると考える．これらの検討結果より，以下の4つの手法を考えた．

手法 1　サーバ・クライアント型： サーバですべてのログを管理

手法 2　HybridP2P 型： サーバでは拡散に関係した計算機のインデックス情報を管理，ログは各計算機で管理

手法 3　サーバレス集中管理型： 機密指定元の計算機で管理

手法 4　PureP2P 型： 各計算機で分散管理

手法 1，2 はサーバを必要とし，手法 3，4 はサーバを必要としない．手法 1 では，サーバが存在するため，サーバでの集中管理型である．手法 2 は，拡散に関係した計算機のインデックス情報をサーバで管理し，ログ自体は，各計算機で分散管理する．手法 3 では，機密指定元の計算機でログを集中管理する．手法 4 では各計算機でログを分散管理する．

5 管理手法の評価

管理手法の評価は，ファイルの拡散におけるログ保存時に発生する通信量と拡散経路検索に関する通信量を測定し，それぞれの管理手法を評価した．この評価を行うために，ログ取得機能，ログ・インデックス収集機能，拡散経路検索機能を実装した．これらの機能によって，ファイルの拡散を追跡でき，蓄積されたログを参照することで拡散経路の検索が可能となる．評価実験では以下の測定条件を用いた．

- 計算機の台数：10 台
- 1 台の計算機でのログが発生する頻度：1log/6 秒
- 1 台の計算機での検索が発生する回数：1 回/1 日 (24 時間)

図 2，図 3 の結果より，手法 3，4 ではログ管理サーバが存在しないためサーバでの通信量は発生しない．手法 4 ではログ保存時に通信量は発生していない．しかし，検索に関する通信量は，他の手法と比較すると多く発生している．一方，手法 1，3 では，検索に関する通信量はあまり発生せず，ログ保存時の通信量が多く発生している．よって検討した手法を通信量だけで評価すると検索回数がログ保存回数より少ない環境では手法 4 が適切なログ管理手法である．一方，手法 1，3 は検索回数がログ保存回数より多い環境に適している．

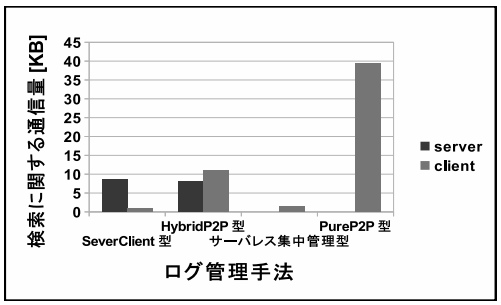

図 2: ログ保存時に発生する通信量

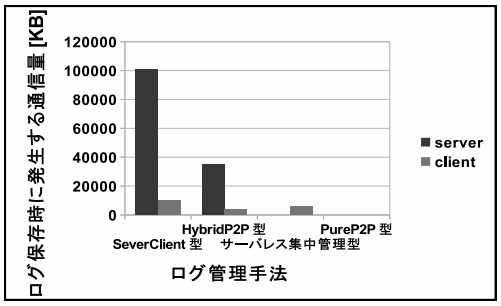

図 3: 拡散経路検索に関する通信量

6 おわりに

本研究では,「誤作動」や「管理ミス」による情報漏洩を防止するシステムを実現するため，ログの管理手法を比較した．今後は，各手法で効率よくログを保存，検索するためにログのデータ構造について検討する．

謝辞

本研究は科学研究費補助金（23700098）の支援を受けて行なった．

参考文献

[1] NPO 日本ネットワークセキュリティ協会，２０１０年情報セキュリティインシデントに関する調査報告書〜個人情報漏洩編〜，http://www．jnsa．org/result/incident/2010．html

[2] 田端 利宏，箱守 聰，大橋 慶，植村 晋一郎，横山 和俊，谷口 秀夫，“機密情報の拡散追跡機能による情報漏えいの防止機構”，情報処理学会論文誌，Vol．50，No．9，pp．2088-2102，(9， 2009)．