複数計算機でのファイル拡散追跡に関する ログ管理手法の検討

前田　明彦*，高橋　健一，川村　尚生，菅原　一孔
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電子化し計算機で管理する機会が増加している．情報を電子化することで，一度に大量のデータを持ち出すことが可能となった．管理する情報は，個人情報などの機密性の高い情報から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．そこで計算機で情報を管理する機会の増加に伴って情報漏洩事件が多発，深刻化している．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」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．また「誤操作」は，ユーザの不注意による操作ミスである．不注意は計算機操作の確認・制御で防止できると考えられる．そのため，本研究では，「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，機密情報の持ち出し操作が発生した際，操作の確認及び制御を行うことが考えられる．そこで，機密情報の拡散をログとして記録し，拡散経路を特定することで機密情報の持ち出し許可の取得を行い，持ち出し操作の制御を行うシステムを提案する．

2.　機密情報拡散追跡・制御

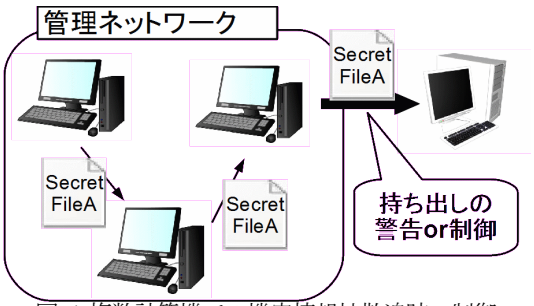

図 1:複数計算機での機密情報拡散追跡・制御

現在，単一計算機での機密情報の拡散追跡・制御[2]するシステムが提案されている．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想定できる．そのような場合，複数計算機で構成されたネットワークのような環境での機密情報拡散追跡・制御システムが必要となる．ここで，機密情報をファイル単位とし，機密情報の拡散追跡・制御機能を持った計算機の集まりを管理ネットワークと呼ぶ．そこで，管理ネットワーク内での機密情報の拡散を追跡し，機密情報が持ち出されようとした時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．システムの概要を図 1 に示す．そこで，複数計算機で機密情報の拡散を追跡するためには，機密情報が拡散する過程をログとして記録する必要がある．蓄積したログによって機密情報の拡散経路の特定が行える．本稿では機密情報の拡散追跡に必要であるログの管理手法について検討する．

3.　ログの管理手法の検討

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，一般家庭のような小規模な環境や企業などの複数のネットワークが存在する環境，また，学校の研究室や企業の部署ごと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での集中管理が適切であるとは限らない．また，サーバが必ずしも準備できるとは限らない．よってネットワーク内に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．そこで，ログの管理手法として集中型と分散型を考える．

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もログ管理手法に影響を与えると考えた．

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：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，サーバの負荷を軽減するため拡散に関係した計算機のインデックスをサーバで管理し，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．また，手法 2，4 はログ発生頻度が高い場合に適切な管理手法である．手法 1，3 は機密情報の拡散経路の検索が発生する頻度が高い場合に適切な管理手法である．以上の各手法の特徴を考察し表 1 に示す．

	利点	欠点
手法1	機密情報の拡散経路の検索が容易	サーバに負荷がかかる，耐障害性が低い
手法2	手法 1 と比較してサーバの負荷を軽減	耐障害性が低い
手法3	拡散経路検索が容易，サーバが不要	性能の高い計算機が必要
手法4	ログを記録するのが容易，サーバが不要	機密情報の拡散経路の検索が難しい

表 1:各手法の特徴

4.　管理手法の評価

4 つの手法を実現するための機能として，ログの取得機能，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．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回数：1 回/1 日(24 時間)

管理手法の評価は，ロギングに関する通信量と拡散経路検索に関する通信量を測定し，それぞれの方法を比較した．比較結果を図 2，図 3 に示す．

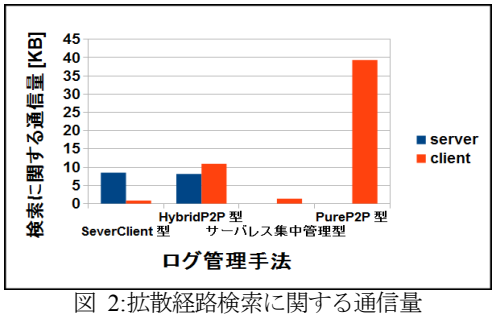

図 2:拡散経路検索に関する通信量

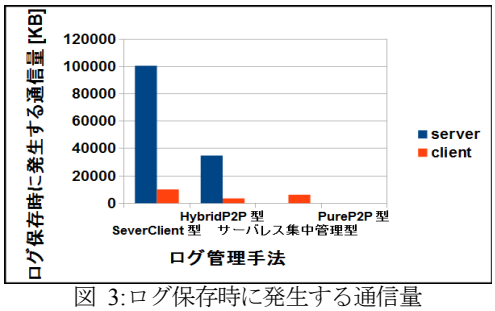

図 3:ログ保存時に発生する通信量

手法 3，手法 4 ではサーバが存在しないため，サーバでの通信量は発生していない．手法 4 ではログ保存時に発生する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より通信量が多く発生している．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，ログ保存時に発生する通信量が多く発生している．よって，検索回数がログ保存回数より少ない環境では手法 4 は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も多い環境に適している．

5.　おわりに

本稿では通信量による各手法の特徴を確認できた．しかし，管理するログのデータ構造や検索アルゴリズムなどによって発生する通信量は変化する．今後はアルゴリズムやログのデータ構造を検討する必要がある．

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．

文　献

(1) 日本ネットワークセキュリティ協会:「2010 年個人情報漏洩インシデント調査結果　Ver．1．3」，http://www．jnsa．org/result/incident/2010．html

(2) 田端利宏，箱守聡，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，Vol．50，No．9 pp．2088-2102，(9，2009)