3A-2

情報漏えい対策システム InfoCage のアクセス制御方式

矢野尾　一男†　　川北　将‡　　小川　隆一†

NEC インターネットシステム研究所†

NEC システム基盤ソフトウェア開発本部‡

1. はじめに

近年、顧客情報の漏えい事件などが相次いでおり、情報システムからの機密情報の漏えいを防止するシステムへの要望が高まっている。

強制アクセス制御による機密情報の保護技術は古くから存在するが、操作性が悪いため、一般のオフィス業務ではあまり利用されていない。

本稿では、情報漏えい対策システム InfoCage[1]のアクセス制御方式について報告する。本方式は、機密情報の局所化などによって、強制アクセス制御の欠点である操作性の悪さを軽減している点に特長がある。

2. 研究の背景

本研究では、一般のオフィス業務における機密情報の漏えい防止を目的としている。例えば、人事業務の場合はファイルサーバ上の人事データ、企業内ポータルでは社外秘情報が記載された Web ページなどが漏えい防止の対象となる。

機密情報は、アクセス制限されたサーバ上で管理されることが一般的である。しかし、サーバが保護されていても、サーバへのアクセス権限を持ったユーザが、クライアント PC 経由で機密情報を閲覧・編集する際に、出来心や操作ミスによって、機密情報を外部メディアにコピーできてしまうという課題がある。

3. BLP モデルによる強制アクセス制御

機密性を保障するセキュリティモデルとして、Bell-LaPadula(BLP)モデルが良く知られている。BLP モデルの簡単な定義を以下に示す。

(1) サブジェクト(アクセスの主体、プロセス等)とオブジェクト(アクセスの対象、ファイル等)に機密度が割り振られる。機密度には半順序関係が定義される

(2) 機密度の低いサブジェクトは、機密度の高いオブジェクトを読むことはできない

(3) 機密度の高いサブジェクトは、機密度の低いオブジェクトに書くことはできない

BLP モデルによる強制アクセス制御をクライアント PC 上で実現し、サーバ側ではそれらのクライアント PC からの接続のみ許可することによって、サーバ上の機密ファイルのクライアント経由の持ち出し防止を実現できる。

例えば、サーバ上の機密ファイルの機密度を、外部メディアの機密度よりも高く設定すれば、機密度の低いプロセスはサーバ上の機密ファイルを読めず、機密度の高いプロセスはサーバ上の機密ファイルを読めても、外部メディアに書き込めないため、機密ファイルのクライアント PC 外への持ち出しを防止できる(図１)。

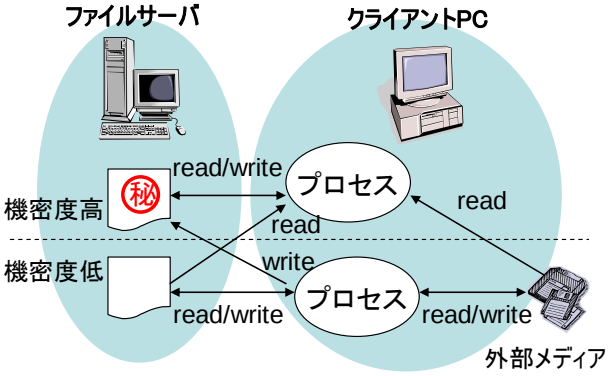

図 1 BLP モデルによる持ち出し制御

BLP モデルに基づいた強制アクセス制御は、トラステッド OS[2]で一般的に用いられている。

しかし、これを一般の業務システムに適用する場合、強制アクセス制御になじみのないユーザにとって使いにくいという問題がある。以下に、その主要な課題を３点挙げる。

(課題 1) 機密度の設定 … 機密ファイルに適切な機密度を設定することが煩雑であり、かつ、間違いを起こしやすい

(課題 2) 機密度の昇格 … ユーザの不注意によって、機密でないファイルの機密度が昇格してしまい、持ち出せなくなってしまう

(課題 3) 操作の煩雑化 … プロセス起動時にプロセスの機密度を指定する必要があるなど、操作が煩雑になり使いにくくなる

4. 提案するアクセス制御方式

本アクセス制御方式では、サブジェクトはプロセス、オブジェクトはファイルであり、それぞれ「機密」と「通常」の２段階の機密度を定

Access Control Model for Information Leakage Protection System “InfoCage”
† Kazuo YANOO, Ryuichi OGAWA, Internet Systems Research Laboratories, NEC
‡ Masaru KAWAKITA, System Platform Software Development Division, NEC

義する。そして、以下の２つの制約を設けることによって、上記の課題 1, 課題 2 に対処する。なお、課題 3 は実装によって対処する(後述)。

（A）機密ファイルの局所化

ユーザから見て、機密ファイルは特定のサーバ(機密サーバと呼ぶ)上にのみ存在し、クライアント上には保存できない

（B）機密度の昇格の制限

通常プロセスが機密ファイルを読み込もうとした場合、プロセスの機密度を昇格させるのではなく、読み込みをブロックする

機密サーバ上に配置されたファイルが機密ファイルとみなされるので課題 1 は解決できる。また、機密ファイルが局所化されるため、ユーザが機密ファイルと通常ファイルを混同することがなくなり、不注意によるプロセスの機密度の昇格も生じないため、課題 2 も解決できる。

しかし、制約(A)は一般には実現困難である。例えば、一時ファイルの書き出しをブロックしてしまうと、そのアプリケーションは正常に動作しなくなる。

そこで、本アクセス制御方式では、クライアント PC 上の特定のディレクトリを「機密」とし、機密プロセスによるクライアントへのファイル書き出しはそのディレクトリ内のパスに変換して書き出す(UNIX の chroot システムコールや、トラステッド OS で用いられる Multi-Level Directory の処理に類似)ことによってこれを解決している。

ここで、パス変換するファイル書き出しは、アプリケーション毎に決められた定義ファイル(プロファイル)によって決定し、プロファイルに合致しないファイル書き出しは単にブロックする(図２)。これにより、ユーザの過失によって、機密ファイルがクライアント PC 上に作成されてしまうこと（機密度の昇格問題を生じさせる）を最小限に抑えることができる。

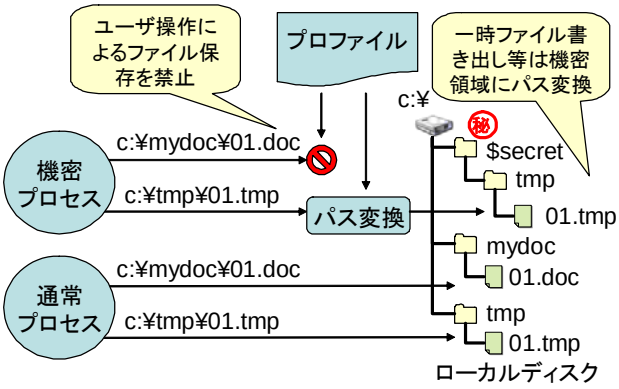

図２ プロファイルによる書き出し制御

5. 実装方式

本アクセス制御方式を実装したミドルウェア(InfoCage クライアント)について簡単に述べる。

InfoCage クライアントは、Windows 2000, XP 上で動作し、ユーザプロセスから OS に対する操作を仲介して、以下の処理を行う(図３)。

1. ファイル等のリソースアクセスに対して、上述したアクセス制御を行う
2. クリップボードや COM/OLE 等のプロセス間通信による、機密プロセスから通常プロセスへのデータの移動を防止する
3. シェル操作等を仲介して、操作性を向上させる。例えば、エクスプローラで機密ファイルをダブルクリックすると、該当する機密プロセスが起動する処理を行う

上記 1, 2 により、機密プロセスが保持する情報が通常プロセスに漏えいしたり、外部メディアに出力されたりすることを防止する。また、3.により、前述した課題 3 を解決できる。

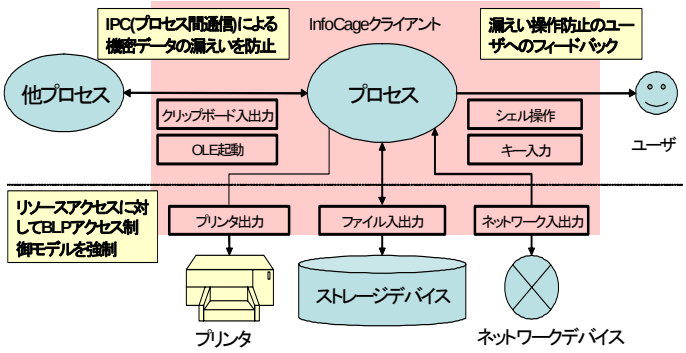

図３ InfoCage クライアントの処理

6. 従来技術との比較とまとめ

現在、商用の情報漏えい防止システムでは、(1)端末からの外部メディアへのアクセスを一律に禁止する、(2)メールゲートウェイなどでファイルの内容を元にフィルタする、(3)DRM 技術を用いたファイル暗号化、といった対策が一般的である。本方式は、(1)と比較して外部メディアへのアクセスを選択的に防止するため柔軟性が高く、(3)と比較してアプリケーション側の変更が不要なため適用範囲が広いという利点がある。

一方、他の技術との組み合わせも有望であり、今後その方式を開発していく予定である。

参考文献

[1]M. Kawakita et al., “InfoCage - Information leakage protection software”, NEC Journal of Advanced Technology, Vol.2, No.1, 2005

[2]IPA/ISEC, オペレーティングシステムのセキュリティ機能拡張の調査, 2002, http://www.ipa.go.jp/security/fy13/report/secure_os/secure_os.html