2004－ＤＰＳ－117　(11)
2004－CSEC－　24　(11)
2004／3／4

情報漏洩防止システムの提案

荒井正人[†]　甲斐賢[†]　永井康彦[†]　冨田理[‡]
[†]（株）日立製作所　システム開発研究所
[‡]（株）日立製作所　情報機器事業部

アブストラクト：個人情報のような機密情報を取り扱うコンピュータシステムでは，情報漏洩の問題が深刻になっている．特に、内部不正による情報漏洩は対策が難しい．機密情報を格納したハードディスクや可搬記憶媒体の持ち出しについてはファイル暗号の適用を義務化することで対処できるが，公開可能な一般情報の取り扱いにも制限を与えることになる．そこで，一般情報と機密情報を区別して、機密情報を含むファイルのみ暗号化し、且つ内部不正によって機密情報が平文のまま一般ファイルに混入しないような強制アクセス制御により情報漏洩を防止可能なシステムを考案したので報告する．

An Access Control System for Protection from Disclosures of Information

Masato ARAI[†]　Satoshi KAI[†]　Yasuhiko NAGAI[†]　Satoru TOMIDA[‡]
[†]Systems Development Lab., Hitachi, Ltd.
[‡]Mechatronics Systems Division, Hitachi, Ltd.

ABSTRACT. Disclosures of information have been a serious issue in computer systems that store classified information such as personal data. Especially, the countermeasure for fraud caused by inside person is difficult. Mandatory file encryption will be able to solve the problem of taking hard disk or removable media includes classified information, but also limit the usage of unclassified information. We propose a system that has capabilities to separate unclassified information from classified information, encrypt classified files only, and prevent intentional plaintext transfer from classified files to unclassified files.

1. はじめに

e-コマースや電子政府といった社会インフラとして，IT システムやインターネットの利用が拡大する一方で, 社内機密情報や個人情報の漏洩といった問題が深刻化している．FBI の調査レポート[1]によると，情報漏洩の件数は，ウィルスや外部からのハッキング行為に比べればごく少数であるが, 発生時の被害額は最も大きいと報告されている．

従来のセキュリティ対策の多くは, 侵入やウィルスといった外部による不正アクセスから情報資産を守ることに対して有効なものであったが，情報漏洩については，機密情報を参照可能な内部の人間によって引き起こされるケースも多い. 例えば可搬記憶媒体や電子メールによる情報流出は, 内部の人間であれば容易にできる. 一般の従業員や職員が操作する PC に機密情報が格納されている場合は, 特に危険が大きいと言える．

本稿では，公開可能な一般情報と，関係者以外に開示してはならない機密情報とが混在するコンピュータシステムにおいて, 機密情報については，可搬記憶媒体，ネットワーク，プログラム間の共有データエリアを用いても, 関係者のみに開示されるよう安全に伝達でき, 機密情報の受け取り側でも, 機密情報として安全に保管可能な情報漏洩防止システム(IT 対策)について述べる．なお本提案のシステムは，行政機関や医療分野のように, 情報の機密性を重要視する IT システムにて，特にクライアントでの情報漏洩防止に利用することを想定している．

2．情報漏洩問題とその対策方針

本章では, 機密情報を取り扱うコンピュータシステムにおける情報漏洩問題と, その対策方針について述べる．

2.1 情報漏洩問題

情報漏洩というセキュリティ問題は, 外部の人間の悪意によって発生するケースと, 内部の人間の悪意または過失によって発生するケースに分けられる. コンピュータウィルスやトロ

イの木馬といった不正なプログラムが外部から混入して活動することによって, 機密情報がネットワークを介して外部へ流出するといった問題は, そのような不正なプログラムを作成した外部の人間の悪意によって生じ得る.

一方, 次に示すような手口による情報漏洩は, 主に内部の人間によって起こりやすいといえる（図 1 参照）.

(1) 電子メールを利用して外部へ送付する
(2) 可搬記憶媒体にコピーして持ち出す
(3) PC やハードディスクごと持ち出す
(4) 共有フォルダに格納して不当に開示する

これらをクライアントーサーバ型のシステムで考えた場合, 管理者しか直接操作できないサーバよりも、一般ユーザが操作するクライアントにおいて多く発生すると考えられる. 次に、このようなクライアントで発生する情報漏洩問題への対策方針を述べる.

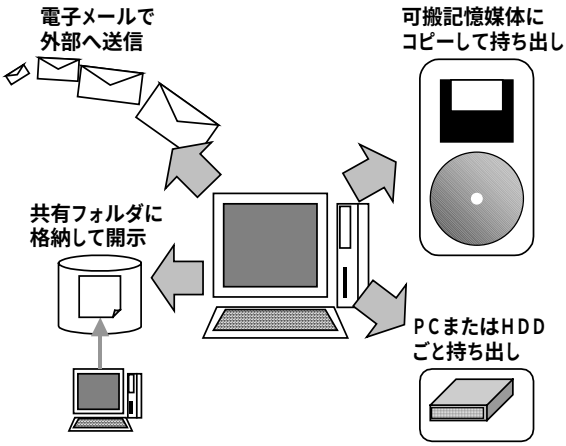

図 1　情報漏洩に使われる主な手口

2.2　対策方針

クライアント側のコンピュータで扱う情報には, 公開可能な一般情報と, 関係者以外に開示してはならない機密情報とが混在することが多い. 情報漏洩を防止するには, 可搬記憶媒体の利用やネットワークを用いたデータ転送を全て禁止すればよいが, 一般情報までデータ転送ができなくなると, 業務上支障をきたす恐れがある.

また, 機密情報が格納されたファイル（以下, 機密ファイル）であっても, 実際にはネットワークや可搬記憶媒体を利用してファイルを交換し, 取り扱い資格をもつ関係者間で参照したり, 編集したりすることもあり, 可搬記憶媒体やネットワークの利用を一律に禁止できない.

更には, 出張等で機密ファイルをモバイル用の PC に格納して持ち歩くこともあり, 据え置き型の PC 筐体だけを保護しても効果は期待できない.

そこで, ネットワークや可搬記憶媒体, およびモバイル PC の利用は禁止しないという前提で, 機密情報については関係者以外に隠蔽可能とすることを対策方針とする.

3.　情報漏洩防止システムの提案

上記方針に基づき考案した情報漏洩防止システムを以下に記す.

3.1　システム概要

図 2 に示すように, 提案の情報漏洩防止システムでは, 機密情報が持ち出されても, 共有フォルダに格納されても関係者以外に対して隠蔽できるように, 機密ファイルは全て暗号化して保存し, 一般ファイルは平文で保存する. これはファイルの格納先がいかなる媒体でも共通とする. 機密ファイルの参照や編集を行う前には, 本システムによるユーザ認証を行い, 機密情報の取り扱い資格をもつユーザであれば, ファイルの暗号復号に必要な鍵の利用を許可する.

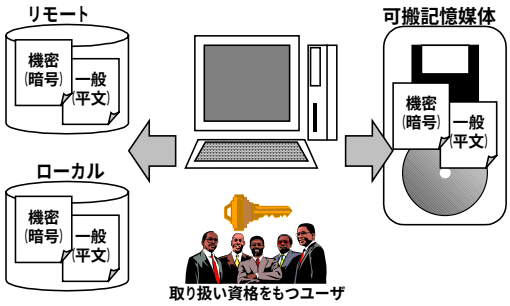

図 2　システム概要

ただし, 上記ファイル暗号が果たす役割は, あくまでも取り扱い資格(鍵)をもたないユーザに対して機密情報を隠蔽することであり, 下記のような取り扱い資格(鍵)をもつユーザの不正行為には対抗できない.

(1) 復号化された機密情報を平文のまま一般ファイルに保存して持ち出す
(2) 復号化された機密情報を平文のままネットワークへ送信する

そこで本情報漏洩防止システムでは, 復号化された機密情報をユーザの悪意や過失から保護する強制アクセス制御方式を, 上記ファイル暗号機能と組み合わせることにした.

3.2 強制アクセス制御方式

上記機密情報の不正な持ち出しや送信ができてしまう理由は, 文書の編集や通信機能など, 多様な機能を備えたアプリケーションプログラム(AP)がクライアントで利用可能なところにある. 本情報漏洩防止システムでは, 機密情報を取り扱うためのプログラムと, 一般情報を取り扱うためのプログラムを区別し, それぞれに必要最小限のアクセス権を与えると共に, 両プログラムの間での不正な情報フローを防止することで強制アクセス制御を実現する. 以下, 各プログラムに与えるアクセス権と, プログラム間の情報フロー制御について具体的に説明する.

3.2.1 ファイルアクセス制御

機密情報を取り扱うためのプログラム(タイプ A)と, 一般情報を取り扱うためのプログラム(タイプ B)に, それぞれ表 1 に示すようなファイル読み出し(R)と書き込み(W)権限を与える.

表 1　ファイルアクセス権

アクセス対象	プログラム タイプ A	プログラム タイプ B
機密ファイル	R(復号) W(暗号)	R
一般ファイル	R	R W
新規ファイル	W(暗号)	W

R(復号)：復号化を伴う読み出し
W(暗号)：暗号化を伴う書き込み

これは, 機密ファイルを復号化する権限を与えられたタイプ A のプログラムには, 一般ファイルへの書き込み権限を与えないことを基本方針としている. また, タイプ A のプログラムによる新規ファイルへの書き込みデータは, 書き込み先の媒体の種類に関わらず, 本情報漏洩防止システムが強制的に暗号化して書き込み, 機密ファイルとして保存する. これにより, タイプ A のプログラムの悪用や誤操作により, 機密情報が平文のままファイルに保存されるといった問題を解決できる. 一方, タイプ B のプログラムには機密ファイルを復号化する権限がないため, 悪用や誤操作によって漏洩が起きることはない. なお, タイプ B のプログラムに復号化を伴わない読み出しを許可する理由については, **3.2.2** で述べる.

本情報漏洩防止システムにおいては, 業務上利用が認められたプログラムには, 上記タイプ A と B のどちらかの権限を予め設定し, 図 3 のようなプログラムテーブルとして管理する. いずれのタイプにも該当しないプログラムによるファイルアクセスは全て禁止する.

プログラム	
パス名	タイプ
C:¥sys¥shell.exe	A
C:¥programs¥editor.exe	A
C:¥sys¥shell.exe	B
C:¥programs¥editor.exe	B
C:¥programs¥internet¥mail.exe	B

図 3　プログラムテーブルの例

3.2.2 ネットワークアクセス制御

上記タイプ A のプログラムが通信機能を備えていると, 機密ファイルの内容が復号化され, ネットワークを通じて平文のままリモートの機器に送信されるという問題が生じる. このとき取り扱い資格のないユーザに開示されないように, 例えば上記ファイル暗号用の鍵を流用して送信データを暗号化することも有効な対策である. しかしながら, 電子メールに機密ファイルを添付することを考えると, 一旦復号化して読み出した機密ファイルを, 再度暗号化して送信するのでは効率が悪い.

表 2　ネットワークアクセス権

アクセス対象	プログラム タイプ A	プログラム タイプ B
ネットワーク	利用禁止	利用許可

そこで本システムでは, 表 2 のようにネットワークの利用をタイプ B のプログラムのみに許可することで, この問題を解決する. つまり, 表 1 に示したようにタイプ B のプログラムであれば, 機密ファイルを暗号データとして読み出すことができるため, そのまま送信すれば暗号データの送信となることから, 上記機密ファイルの復号処理と再暗号処理を省略できる.

3.2.3 プログラム間の情報フロー制御

前記アクセス権設定により, 各タイプのプログラムの悪用や誤操作が引き起こす情報漏洩

の問題は解決できる．しかし，タイプ A と B のプログラム間でのデータ転送によって発生する漏洩問題が残されている．そのようなデータ転送の種類とその対策について以下に記す．

(1) ユーザの操作を伴うデータ転送

ユーザの操作を伴うデータ転送には，ドラッグ＆ドロップによるものと，クリップボードを経由したものがある．ドラッグ＆ドロップ操作は，同一画面に表示されている複数の AP 間でのデータ転送に使える．したがって，上記タイプ A とタイプ B のプログラムが同一画面にあると，タイプ A のプログラムが復号化した機密情報を，タイプ B のプログラムに転送され，機密情報が平文のまま一般ファイルに保存される危険がある．その対策として，本情報漏洩防止システムでは，各 AP のユーザインタフェースを表示するデスクトップ画面を，上記タイプ A 用とタイプ B 用にそれぞれ生成し，タイプの異なるプログラムのユーザインタフェースが同一画面に表示されないようにする．これによりユーザは，扱う情報のレベルに応じて，機密用のデスクトップと一般用のデスクトップを切り替えながら利用することになる．図 4 は，その画面イメージを示したものである．機密用と一般用の各デスクトップ画面には，デスクトップ切り替え用のアイコンを表示しておき，ユーザが当該アイコンを押下して切り替えメニューを選択することで，機密用と一般用のデスクトップを適宜切り替え可能とする．

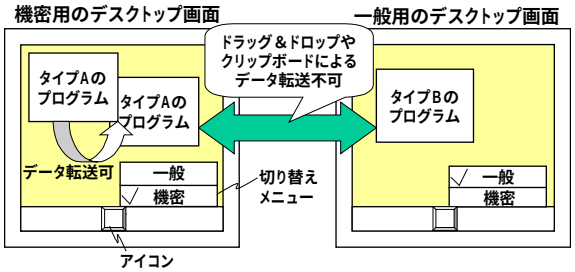

図 4 画面イメージ

一方，クリップボードとは，ユーザが指定した文字列データや画像データ等を一時的に保持し，他のプログラムのデータ領域へ複写するために使われる共有データエリアのことである．クリップボードを悪用すると，タイプ A のプログラムからタイプ B のプログラムへ，機密情報が平文のまま転送できてしまう．そこで本情報漏洩防止システムでは，デスクトップを跨ったクリップボードの共有を防止する機能を提供する．

(2) プロセス間通信を利用したデータ転送

ここでのプロセス間通信とは，例えば名前付きパイプなどを利用して，プログラムが自動で行うデータ転送を指す．上記(1)のデータ転送と異なり，ユーザの操作は介入しない．このようなプロセス間通信は，デスクトップを跨っても可能なことから，タイプ A のプログラムによって復号化された機密情報が，タイプ B のプログラムに渡る恐れがある．ただし，一般的なアプリケーションプログラムには，デスクトップを跨って他のプロセスと通信を行うものは見当たらず，実際にプロセス間通信を悪用して機密情報を流出する可能性は低いと考える．したがって本システムでは，プロセス間通信の悪用を防止する機能は設けないが，敢えて対策するとなれば，プロセス間通信に利用するオブジェクト(名前付きパイプ等)へのアクセスを監視し，タイプの異なるプログラム間でのデータ転送をブロックする機能を追加することも可能である．また，別の手段として，業務上利用が認められていない(図 3 のプログラムテーブルに登録されていない)プログラムの起動を制限する機能を追加してもよい．

4. 実現方式

ここでは，上記情報漏洩防止システムの実現方式の一例を，主要な機能毎に示す．

4.1 ユーザ認証

ユーザは機密ファイルの参照や編集を行う前に，認証を受ける必要がる．ここで述べるユーザ認証は，OS が備えるユーザ認証機能とは異なり，本システムが独自に提供するものである．具体的には，図 5 に示すユーザ認証モジュールが，ユーザに対して ID カードの提示(カードリーダへの差込み)とパスワード入力を要求する．この ID カードは，ファイルの暗号と復号に用いる鍵を保持しており，機密情報の取り扱い資格をもつユーザのみに配布しておく．また，ID カードの紛失に伴う鍵の流出を防ぐために，正当なユーザのみが知り得るパスワードによって鍵を暗号化した状態で ID カードに格納する．ユーザ認証モジュールは，ID カードに格納された鍵を，ユーザが入力したパスワードにより復号化できれば認証成功とみなす．なお，ＩＤカードの代わりにユーザ認証と鍵の生成および配布を行う専用サーバを設ける方法もある．このようなユーザ認証と鍵の配布につ

いては，例えば文献[2][3]にて報告されている方式が利用できる．

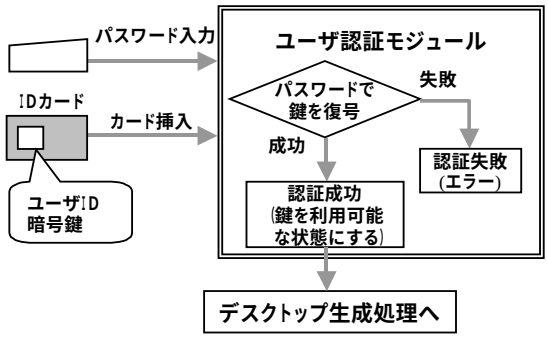

図 5　ユーザ認証処理

4.2 マルチデスクトップ環境の構築

上記ユーザ認証が成功すると，図 6 に示すマルチデスクトップ制御モジュールにより，機密用と一般用のデスクトップを生成する．その結果，１台の機器でデスクトップを形成するプログラムが複数実行されることになる．本システムでは，それらを区別できるように，各デスクトップのプログラムに対して，それぞれ異なるユーザ ID(権限)を割り当てる．具体的には，図 6 に示すように，デスクトップ生成用の２つのユーザ ID(user_A と user_B)を ID カードに予め登録しておき，ユーザが入力したパスワードと合わせて，図 5 のユーザ認証モジュールを経由してマルチデスクトップ制御モジュールへ通知する．マルチデスクトップ制御モジュールでは，受け取ったユーザ ID とパスワードを用いてデスクトップのプログラムを起動する．それらユーザ ID とパスワードを受けて，デスクトップのプログラムは OS へのユーザ認証処理を実行する．その結果，デスクトップのプログラムには，ユーザ認証に使われたユーザ ID(権限)が OS によって割り当てられる．また，各デスクトップから起動される他のプログラムについても，その起動元となったデスクトップと同じユーザ ID(権限)が OS によって割り当てられることになる．これにより，実行中のデスクトップおよびその他プログラムがタイプ A とタイプ B のどちらであるかは，そのユーザ ID から判別可能となる．

デスクトップを生成した後，マルチデスクトップ制御モジュールは，デスクトップの切り替え用のユーザインタフェース(図 4 のアイコン)を提供し，ユーザからの要求に応じてデスクトップの切り替え処理を実行する．デスクトップの切り替えは，プラットフォームとなる OS が，複数のデスクトップを起動可能なものであれば，OS が提供する所定の API を呼び出すだけで切り替え可能である．

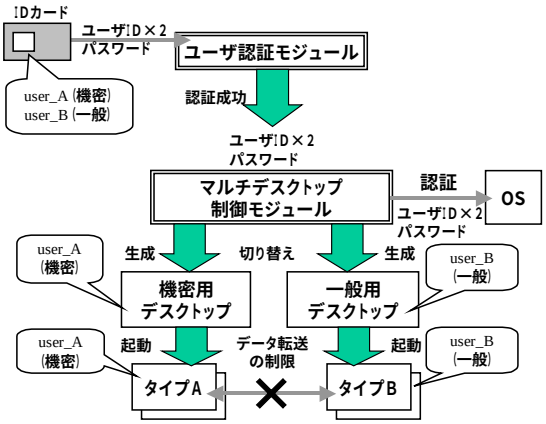

図 6　デスクトップ生成処理

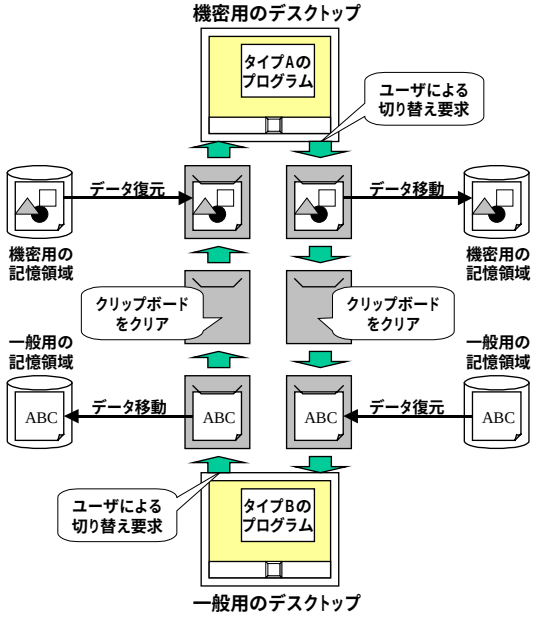

図 7　クリップボードの共有防止策

また，デスクトップを跨ったクリップボードの共有を防止するために，マルチデスクトップ制御モジュールは，デスクトップ毎にクリップボード内のデータを一時的に保管するための記憶領域(メモリまたはディスク中)を管理し，デスクトップの切り替え時にはクリップボード内のデータを移動し，切り替え先のデスクトップで使用していたデータと入れ替える(図 7)．これは，同一デスクトップ内でのクリップボードの利用を制限するものではない．

4.3 ファイルアクセス制御

図 8 に示すファイルアクセス制御モジュールにより, 上位のプログラムからのファイルアクセスをすべて監視する. このとき, アクセス要求元となるプログラムのタイプ(A または B)と, アクセス対象となるファイルの種別(機密ファイルまたは一般ファイル)を判別し, ファイルアクセス権(表 1)に従い制御する.

プログラムのタイプの判別は, そのプログラムが, いずれのデスクトップから起動したものかを確認することで可能となる. 具体的には, そのプログラムに割り当てられたユーザ ID(権限)から判別してもよいし, あるいはプログラムの起動の度に, いずれのデスクトップからの起動であったかを記憶するテーブルを設けて参照する方法もある. ただし, 図 3 で示したプログラムテーブルに登録されていないプログラムであれば, アクセス権がないものと判断する.

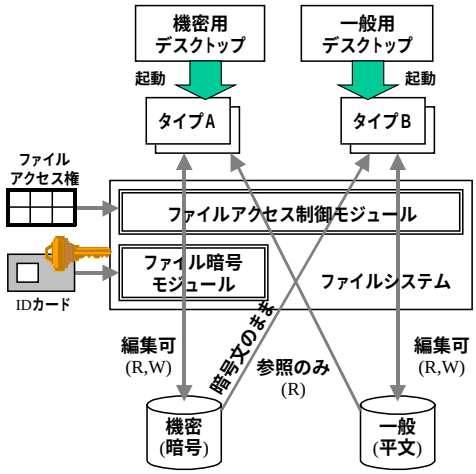

図 8 ファイルアクセス制御

一方, アクセス対象となるファイルの種別については, 暗号化された機密ファイルの先頭部分に特定のコードを埋めておき, 当該コードの有無から判別する.

また, 上記ファイルアクセス権に従い, 正当と判定されたファイルアクセスが, 暗号化・復号化を伴う書き込みや読み出しであれば, ファイルアクセス制御モジュールからファイル暗号モジュールを呼び出す. ファイル暗号モジュールは, 上記 ID カードに登録された暗号鍵を用いて, 機密ファイルの暗号化・復号化処理を実行する.

以上のようなファイルアクセス制御は, 当然ながら一般的な OS が備えるファイルアクセス制御とは異質なものであるが, 例えば文献[4]にて報告しているように, OS が提供するファイルシステムの機能を拡張する形で実装することが可能である.

4.4 ネットワークアクセス制御

図 9 に示すネットワークアクセス制御モジュールにより, 上位のプログラムからのネットワークアクセスをすべて監視する. また, アクセス要求元となるプログラムのタイプ(A または B)を判別し, ネットワークアクセス権(表 2)に従い制御する. プログラムのタイプの判別は, 上記ファイルアクセス制御モジュールと同様に行う.

このようなネットワークアクセス制御は, パーソナルファイアウォールの機能に類似しており, プログラムのタイプに基づいてアクセス制御する点を除けば, 既存技術で実現できる.

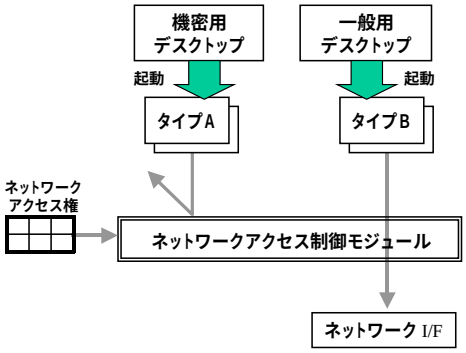

図 9 ネットワークアクセス制御

5. 利用イメージ

提案の情報漏洩防止システムを適用した情報システムの利用イメージを, 図 10 を用いながら説明する. 前提として, 機密文書(機密ファイル)を, 取り扱い資格をもつユーザで共有する鍵を用いて全て暗号化し, ファイルサーバに格納しておく. また, 機密ファイルの参照・編集に必要な鍵を ID カードに格納して, 取り扱い資格をもつユーザへ配布しておく.

クライアント側には, 情報漏洩防止システムを導入し, 機密ファイルの参照・編集用のプログラムはタイプ A とし, 一般ファイルの参照・編集用のプログラムと, ネットワークを利用するメールプログラムはタイプ B と定義する. また, 上記参照・編集用のプログラムは, タイプ A だけでなく, タイプ B として指定してもよい. 以上の作業は, 当該情報システムの管理者が行う.

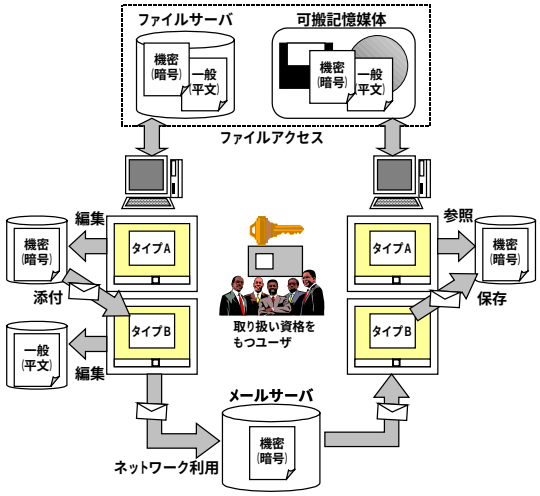

図 10　適用例

機密情報の取り扱い資格をもつユーザは, クライアントにて, 上記暗号化された機密ファイルを, 管理者が指定したタイプ A のプログラムを用いて参照したり, それをもとに新たな機密ファイルを作成したりする. 作成した機密ファイルは, クライアント側に保存するだけでなく, ファイルサーバや可搬記憶媒体に保存することもある. このとき, タイプ A のプログラムを用いて作成したものは, 自動的に暗号ファイルとして保存される.

また, ファイルのコピー操作等に利用するプログラム(一般にシェルと呼ばれる)をタイプ B として利用すれば, タイプ A のプログラムが作成した機密ファイルを, 暗号ファイルのまま(ファイル暗号・復号処理をせずに)ファイルサーバや可搬記憶媒体にコピーできる.

ユーザは更に, 機密ファイルを電子メールに添付して関係者に送付することもある. これには, クライアントのデスクトップを一般用に切り替えて, タイプ B のメールプログラムを用いる. これにより, 機密ファイルを暗号ファイルのまま添付して送付できる.

当該メールの受信側においても, タイプ B のメールプログラムを用いれば, 受信した機密ファイルを暗号ファイルのまま(暗号・復号処理をせずに)ローカルディスクに保存でき, その後はタイプ A のプログラムにより参照・編集可能となる.

6. まとめ

公開可能な一般情報と, 関係者以外に開示してはならない機密情報とが混在するコンピュータシステム, 特にクライアントにおける情報漏洩問題を解決すべく, 情報漏洩防止システムを提案した. 本システムによれば, 一般情報しか含まないファイルは従来通り平文で保存するが, 機密情報を含むファイルは全て強制的に暗号化して保存し, 可搬記憶媒体やネットワークを用いても, 常に暗号ファイルとして関係者に伝達されるようになる. また, 復号鍵を持つ(取り扱い資格のある)ユーザの手により, 機密情報が平文のまま流出しないように, 参照・編集に用いるプログラムと, ネットワークを利用するプログラムとを区別して, 両者の間でのデータ転送を制限できるようにした.

このような情報漏洩防止システムを, 既存技術や製品を活用しながら必要機能を追加することで, 汎用 OS 上に実現すれば, TCSEC[5] B レベルの OS を使わずに, 従来の AP を継承しながら, よりセキュリティの高い情報システムを構築できると考える. また, 機密ファイルが格納されたモバイル PC に本システムを適用すれば, PC 盗難時の機密情報保護にも役立てることができる.

最後に, 本稿で報告した内容は, あくまでも IT セキュリティ面からみた対策の一例である. 情報漏洩対策には, 他にも物理的対策, ユーザ教育など, 幅広い対策が必要である.

参考文献

[1] 米 CSI: 2003 CSI/FBI Computer Crime and Security Survey, 8th annual (2003)

[2] Ito, H., Susaki, S., Arai, M., Koizumi, M. and Takaragi, K.: Group Cipher System for Intranet Security, Trans. IEICE, Vol.E81-A, No.1, pp.28-34 (1998)

[3] 荒井 他：企業情報向けグループ暗号システム, 情報処理学会論文誌, Vol.40, No.12, pp.4378-4387 (1999)

[4] 荒井 他:マルチ OS 環境を利用したアクセス制御システムの実装と性能評価, 情報処理学会論文誌, Vol.44, No.4, pp.1092-1100 (2003)

[5] DoD 5200.28-STD, TCSEC "Department of Defense Trusted Computer System Evaluation Criteria", National Computer Security Center, December 1985.