ACOS－6MVXセキュリティについて

日本電気株式会社基本ソフトウェア開発本部

海老野 征雄　橋本 敏昭

コンピュータシステムの大規模化に伴い、一つのシステムで多種多様な業務が同時に動作するようになり、またネットワークの広域化により接続形態も多様化しています。このため、コンピュータのハードウェア、ソフトウェア、およびデータなどコンピュータ資源に対する破壊、漏洩、不正アクセスを防ぐ、すなわち脅威を未然に防止し、影響の極小化を図る必要があります。
一般に、コンピュータセキュリティに関する対策の一つである技術的対策を支援するソフトウェア機能としては、HW故障対策のRAS機能、データ破壊に対する復旧支援機能などの高信頼性対策と、データ保護の機能に大別されますが、ここでは後者について説明します。機密保護機能は、プロセッサ使用／機能実行、主記憶、ファイル等のOS制御の対象になるシステム資源をいろいろな脅威から防御するため、それら資源へのアクセス要求に関して、資源へアクセスしようとする利用者ごとにアクセス権を有するか否かのチェックを行う確認機能・保護機能、および不正なアクセスを検出する機能に分類されます。

ACOS—6/MVXオペレーティングシステムでは、FMS(File Manegment Supervisor)によるファイル機密保護と利用者の認証機能を従来からOSの基本機能として提供していますが、利用者ごとの管理を行うべく利用者管理拡張機能(UAF-AF：User Administration Facility Advanced Functions)を開発し、FMSでのファイル機密保護との組合わせによって、以下に述べるセキュリティ機能を提供しています。

1. 利用者の確認と管理

利用者はセンターやリモートからジョブを申し込んでシステムを利用したり、端末からTSSを使うことによりシステムを利用します。いずれの形態でシステムを利用する場合でも、無資格者の使用による不正接続・利用を防止するためには、確認機能としての認識を行い、利用者属性に基づいた利用者の認証を行います。

従って、登録されていない利用者によるシステムの無断使用や、使用が許されていないTSSなどの個別システムの利用などが禁止されます。

このことをTSSの利用者に関連した場合について述べると、次のようになります。つまり、

端末からの接続に対して

◦利用者識別名および課金番号が登録されているか。

◦パスワードは登録されているものと一致するか。

◦タイムシェアリングシステムの利用が許されているか

などの妥当性を確認します。利用者識別名はＦＭＳのファイル体系（図－４）のシステムマスタカタログ（ＳＭＣ）を使用しますが、ＴＳＳの利用者認証はファイルへのアクセス権を確認することによって実現しています。またパスワードもＳＭＣに登録されているものを使用します。もし妥当性がない場合には、ＴＳＳ-ＡＦセッションの開設を拒否します。

また、ＵＡＦ-ＡＦではＴＳＳ-ＡＦセッション開設時の利用者の妥当性チェックについて以下の条件によって不正接続を防止する機能があります。

◦利用者名とグループ名による確認

◦利用者ごとの使用期間制限（曜日、時間帯など）

◦利用可能端末の管理

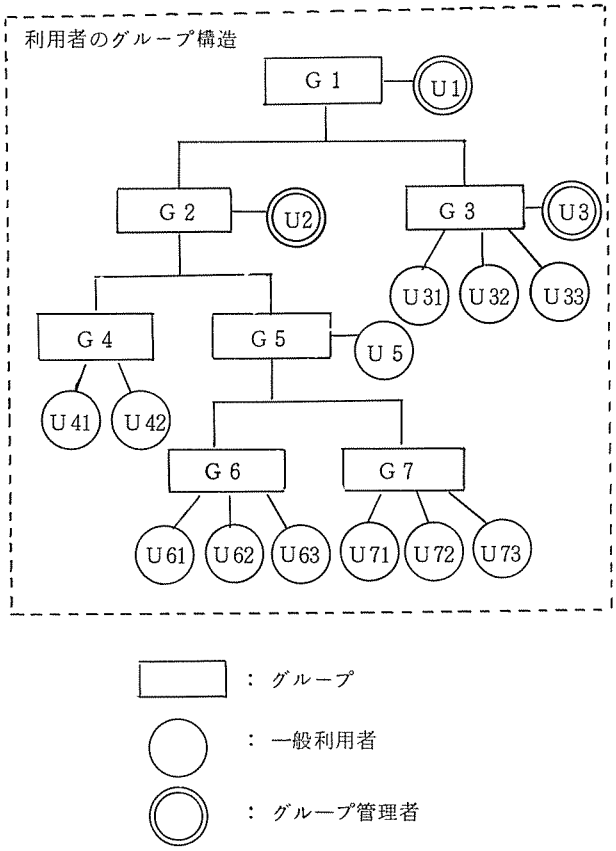
◦パスワード管理

(1) グループ名と利用者名による認証

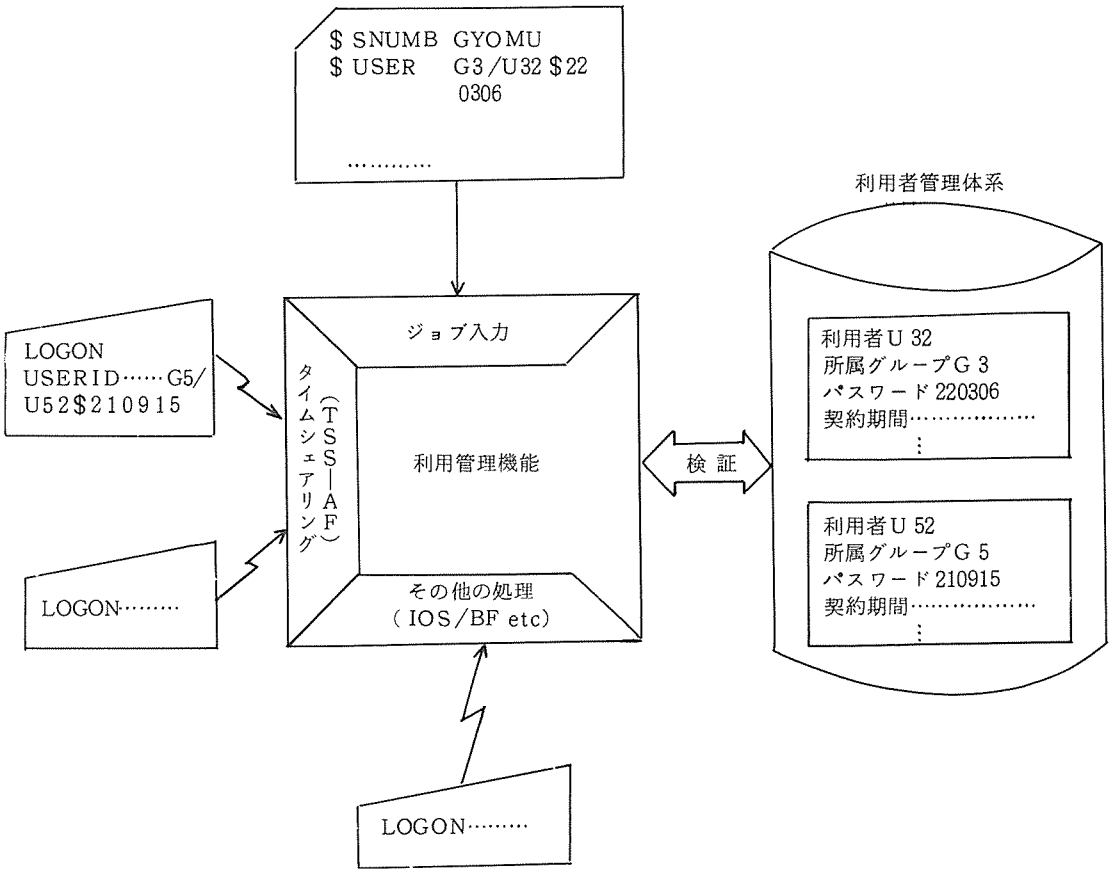
コンピュータの利用者はグループと呼ばれる利用者の集合に所属して管理されかつグループは図１に示すような階層化された構造になっています。例えば、ＴＳＳに接続してセッションを開設する場合には、図－２のようにグループ名と利用者名、およびパスワードが登録されていなければなりません。この階層構造を成す管理体系によって利用者の集中管理を行います。

(2) 使用期間、使用時間帯による制限

ＴＳＳを利用できる契約期間の設定、あるいは使用できる時間帯を曜日毎に設定することによって利用者の使用できる期間、時間帯を制限して不正接続を排除することができます。また、ＴＳＳの一



図－１　利用者管理構造



図－2　システム利用時の検証

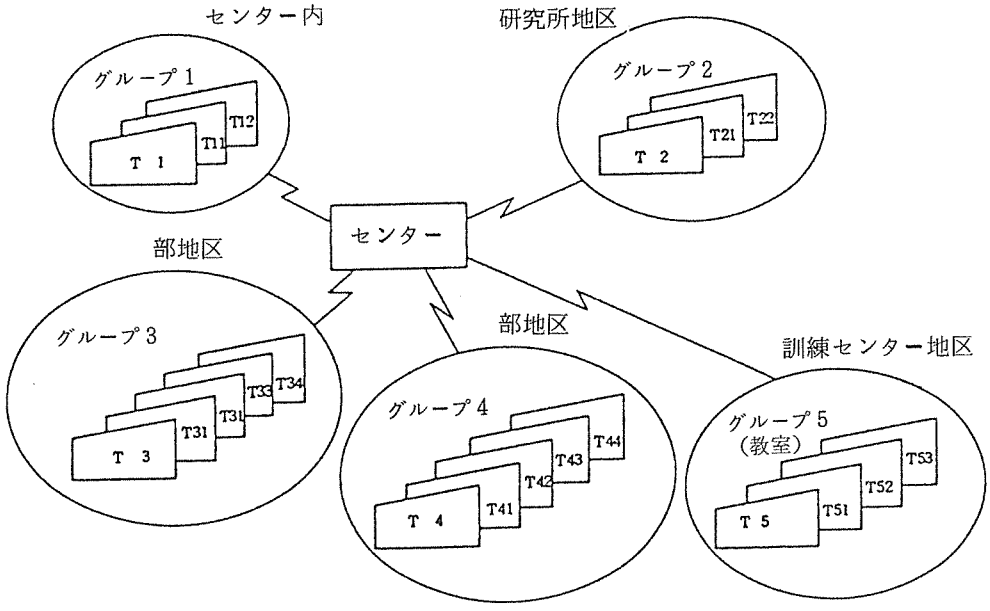
つのセッション当たりの利用時間の制限を行え、この使用時間の制限を行うことにより、一人の利用者が長時間にわたって資源を専有する弊害を防止することもできます。

(3) 利用可能端末の制限

UAF-AFでは利用者が使用できる端末のグループ（図－3：端末のグループ化を示す）を設定できる機能を提供して、該当端末からの接続要求でなければセッションは開設しません。端末からのシステム利用が多くなってきているので、特定の端末からのアクセスしか認めない利用端末の制限が必要になっており、この端末管理機能によって、悪意の利用者の排除を使用可能端末の方面から実現しています。

(4) パスワード管理

UAF-AFではパスワードの認証の時点で不正パスワードと判断した場合、パスワード失敗回



図－３　端末のグループ化

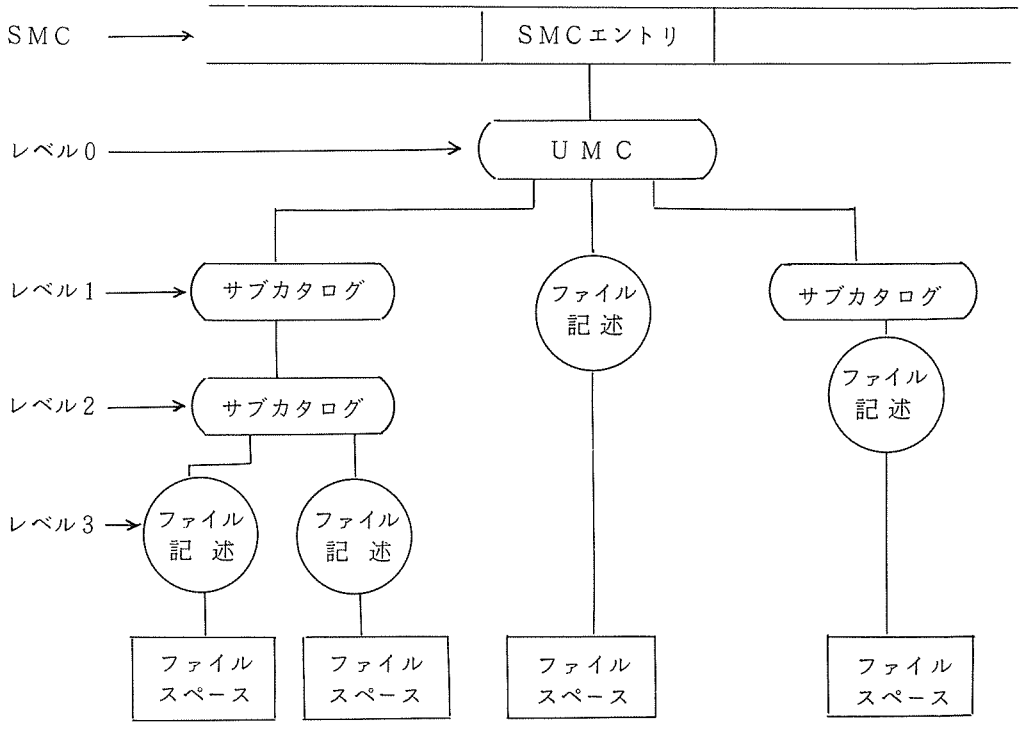
数を体系内に累積します。そしてこの累積値がある一定値に到達している場合には、システムの利用を拒否します。利用者の認証に用いる、このパスワードは管理体系内のグループ／利用者名に対応する一つの属性として管理しています。累積値を超えることによるセッションの開設拒否状態はUAF−AFの管理者が処置を取るまで続き、このことによって悪意の利用者によるパスワードの検索、盗用を排除することができます。

2. ファイルの機密保護

利用者が使用する全てのパーマネントファイルはＦＭＳの管理下で体系的、集中的に取り扱うことにより、システム全体としてのファイルシステムの機密保護を実現しています。

利用者ごとにファイル体系（SMCからのカタログツリー構造図）を作りあげて、すべてのカタログ／ファイルに対しては、その作成者を所有者とし、所有者は当該カタログ／ファイルの全権限を保有させます。これが、ACOS−6/MVXのファイル保護の基本的な考え方です。

この所有者の考え方により、他人からの体系へのアクセスを防止しています。さらに、カタログ構造内のサブカタログ、ファイルごとのパスワードを指定することによって一層ファイルへの不正アクセスを保護できます。またファイルを作成者以外の利用者に対しても使用できるようにサブカタログ／ファイルにパーミッションを付加することもできます。



図－4　ファイル体系とカタログ構造

(1) パスワード

ファイルへのアクセスを保護するため、二種類のパスワードがあります。

◦利用者パスワード

ファイル体系が他利用者からアクセスされることを保護するためにシステムマスタカタログ（SMC）に付いているパスワードです。FMS管理下のパーマネントファイルをアクセスしたり、TSSのログオン時の利用者名を宣言する時に同時に指定するパスワードと同じであり、TSSセッション開設のための利用者確認に使用されています。システムとの接続を行うには、利用者が宣言する利用者識別名がSMCに登録されていなければなりません。この登録はシステム運用者が行います。

◦カタログ／ファイルのパスワード

このパスワードは、重要な保護すべきデータやプログラムを格納しているならばファイルに、またはそのファイルの上位のカタログに利用者によって選択的に指定することができます。このパスワードが付いているカタログやファイルへのアクセスには、パスワードの提示が必要になります。名前にパスワードは、次のようにカタログやファイルの名前の後に＄、続いてパスワードを示します。

```
名前＄パスワード
```

パスワードは、名前と同様に、12文字以内のアルファベット、数字、ハイフン、ピリオドからなる。

このようにファイルやカタログにパスワードを指定する目的は、ファイルやカタログ名をなんらかの手段により知った人が、カタログやファイルを勝手に利用すること、およびファイル内容の破壊などを防ぐことにあります。例えば、カタログ名やファイル名は、その上位カタログをリストすることにより知ることができますが、その中にはパスワードは表示されません。このように、パスワードは通常の手段では外部にもれることはないので、ファイル名やカタログ名を知ったとしても、通常それらに対し参照、更新などの操作は行えません。

また、パスワードを変更することによりファイルの使用を、その時点から使用が許される利用者のみに限定すること、つまり、パスワード変更の通知を受けた利用者のみファイルの使用を続けられます。これは、ファイル名を変えることにより同じ効果を得ることもできますが、変更されたファイル名は、カタログをリストすることにより知ることが可能であるし、ファイルをその名前で参照しているプログラムリストを入手することによっても知ることができ、パスワードの変更は機密保護に有効な方法となります。

(2) 使用時間帯パスワード

カタログやファイルに対するパスワードで、１日のうちの時間を区切り、各区間内でのみ有効なパスワードを時限パスワードといいます。この時限パスワードを使っている場合、パスワードは、１日のうちのそのパスワードに割り当てられた時間内に使用しなければなりません。

したがって、時限パスワードは、ファイルやカタログにアクセスする時間を限定するために使用でき、この使い方ではパスワードをほんの短い間（例えば15分だけ有効にする）、あるいは端末が監視下におかれている間（例えば、勤務時間中）のみ有効にすることによって使用時間外でのファイル／カタログへの操作要求は受け付けられなくなります。但し、割り当て中のファイルは制限時刻がきても継続して使用できます。

時限パスワードの指定のしかたは、ＬＩＬＳＹＳディレクティブで次のように、各パスワードを指定し、開始時刻、および終了時刻を指定します。

```
ＰＡＳＳＷＯＲＤ／パスワード：開始時刻＊終了時刻、
                  ……，
                  パスワード：開始時刻＊終了時刻／
```

(3) パーミッション

ファイルの所有者は、カタログ構造上の各ノード（サブカタログ、ファイル）にアクセス権を

付加することによって、他利用者にカタログ／ファイル操作や、ファイルアクセスのための権限を委譲することができます。この権限の委譲をパーミッションと呼びます。

ファイルやカタログあるいはその下位に属するファイルやカタログに対して、誰にどのような操作を許可するかということは“パーミッション”で指定することができます。パーミッションには、実行権（EXECUTE）、読込権（READ）、書込権（WRITE）、他、全部で８種類が用意されています。また、誰に権限を委譲するかによって、任意の人を対象とする一般パーミッションと、特定の名前の利用者を対象とする特定パーミッションがあります。このパーミッションはファイルやカタログを作成したり変更したりするときに指定できます。

パーミッションをカタログに対して指定したとき、その効果は下位のカタログやファイルにも適用され、つまり、下位に多くのレベルが存在する場合には、各レベルのパーミッションの効果が累積されます。ただし、特定パーミッションが指定された利用者は、そのカタログおよび下位のカタログまたはファイルにおいて、一般パーミッションの対象から外されます。

① パーミッションで許可される操作

パーミッションで許可される操作について主なものを表に示します。ファイルだけに適用されるパーミッションもあり、このパーミッションが、カタログに対して指定された場合、その下位にあるファイルに対する操作のパーミッションを意味する。他の操作は、ファイルとカタログの両方に適用される。ただし、CREATEは、カタログに対してだけ指定できる。

表　パーミッションの意味

パーミッション指定	意　　味
READ	ファイルからデータを読み込むことの許可。書き込みは許可しない
WRITE	ファイルからデータを読み込みおよび書き込むことの許可
EXECUTE	プログラムファイルの実行の許可
PURGE	ファイルやカタログを削除することの許可
CREATE	カタログに従属するカタログやファイルの作成の許可
MODIFY	カタログやファイル記述の変更許可。全てのパーミッションの許可

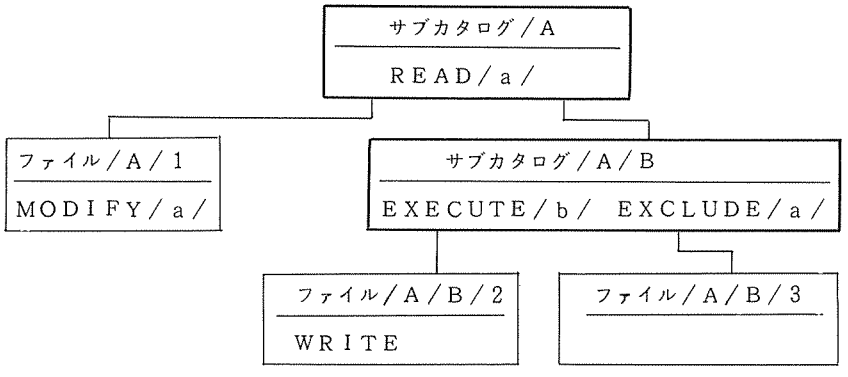
なお、各パーミッションはお互いに包含関係を持っています。すなわち、READはEXECUTEを包含し、WRITEはREADを包含し、さらにMODIFYは全ての権現を持ちます。

② パーミッション効果（一般、特定、EXCLUDEパーミッション）

パーミッションの形態は、そのカタログ／ファイル操作やファイルアクセスの権限を許す対象者を指定するか否かにより、特定パーミッション（specific permission）と一般パーミッション（general permission）に分けられています。一般パーミッションの対象者は全利用者ですが、特定パーミッションは特定利用者に対するものであり、指定された利用者は特別扱いされ、以後一般パーミッションの対象から外されます。

このパーミッションの効果はそれが指定されたノードおよびその下位のノード群に対し有効でパーミッションの包含関係により累積されます。パーミッションの効果を制御するために、一般および特定パーミッションのほかにEXCLUDEパーミッションが導入されています。EXCLUDEパーミッションに指定された利用者は、以後一般パーミッションの対象から外されるだけでなく、今までその利用者に累積された特定パーミッション効果も打ち消されます。

ある利用者の所有するカタログ／ファイルに対して、利用者ａと利用者ｂに対するパーミッションが図５のようなパーミッション指定しているときに、利用者Ａと利用者ｂの各ファイルの最終的なアクセス権は図－６のようになります。



図－５　パーミッションの指定例

	利用者ａのアクセス権	利用者ｂのアクセス権
ファイル／A／1	MODIFYパーミッション	パーミッションなし
ファイル／A／B／2	パーミッションなし	WRITEパーミッション
ファイル／A／B／3	パーミッションなし	EXECUTEパーミッション

図－６　パーミッション効果の例

③ ＵＡＦ－ＡＦでの特定パーミッッション

特定パーミッッションは、利用者＝ＳＭＣ名（ＴＳＳでの利用者識別名）をその対象とするものと、人を示す利用者をパーミッションの対象とする“利用者管理”の考えに基づくものとがあります。「誰に、どんな操作を許可するか」というパーミッションを利用者自身に与えることによって、ファイルの機密保護を“人”対応に行おうとする考え方であり、パーミッションの対象としては、「利用者名」と、複数の利用者を含む「グループ名」とがあります。

カタログやファイルにアクセスする場合、そのプロセスが利用者管理モード下で実行されるならば、グループ名や利用者名およびＳＭＣ名対応のパーミッション効果が累積されます。

グループ名と利用者名、ＳＭＣ名は同等に扱われる為、そのうちのどれか１つにＥＸＣＬＵＤＥパーミッションは付加されている場合、そのグループ名、利用者名、ＳＭＣ名に今まで累積された特定パーミッション効果は、全て打ち消されます。

パーミッションのグループ名と利用者名の指定形式

“ＧＮＡＭＥ＝”オプションをグループ名の前に付加し、利用者名はコロン（：）で区切ってその後に指定します。

```
／ＧＮＡＭＥ＝グループ名１：利用者名１：利用者名２／，
```

(4) ロック機能

ファイルへのアクセスを禁止するライトプロテクトロック（ＷＬＯＣＫ）があります。このＷＬＯＣＫはファイルの更新をファイルの所有者自身を含めて禁止するものです。

このロックをかければ、ファイル更新の誤り、悪意の利用者によるファイル内容の破壊を防ぐことが可能になります。

(5) オーディットオプション（実績記録）

ファイルの機密保護に関係して、カタログとファイルに対する操作の履歴と不正アクセスの履歴を収集・記録できます。

- スペースアカウンティング、システムマスタカタログ、バックマスタカタログの問い合せ
- システムマスタカタログ、バックマスタカタログの作成、更新、削除
- カタログおよびファイル記述の作成、更新、削除

◦必要なパーミッションまたはパスワードがないため拒否されたファイル割り当て要求。または受け付けられた要求、拒否された要求の両方

◦許可されていない操作を行おうとしたこと。例えば、READのみで割り当て要求を出し認められていたのに、書き出しを行おうとしたアクセス

これらの履歴について、サイトでの運用環境に適した項目を選択して収集することにより、カタログ、ファイルへの不正アクセスを検出することができます。

4. 情報の保護

(1) ドメイン保護

プログラムの実行時には、手続きがアクセスする可能性のあるセグメントは全てアクセス可能とする必要がありますが、逆に、誤って、または、故意に必要以上のセグメントをアクセスさせない保護機能として、ACOS−6/MVXではドメイン保護があります。

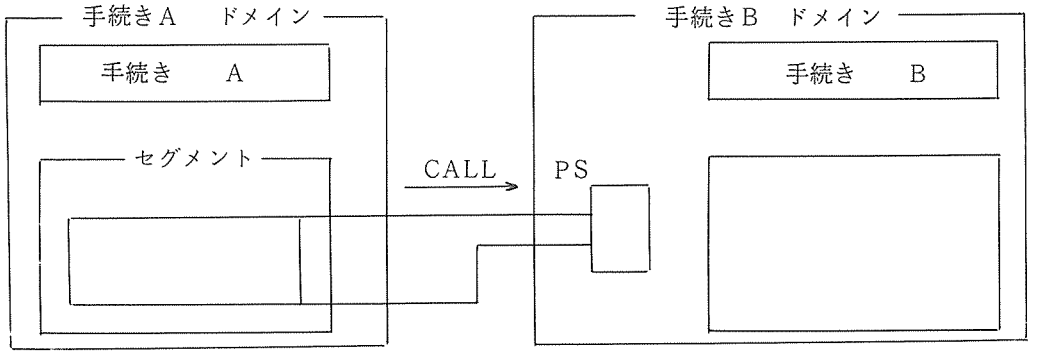
プログラム間の手続きの移行時に、対応するリンケージセグメントを動的に切り換え（ドメインの切り換え)、各手続き内で参照、あるいは更新可能な、他ドメインの情報を必要最小限に制約しています。このように、ドメインによりアクセス可能な範囲に制限を加える主記憶の機密保護方式をドメイン保護と呼んでいます。

ドメイン保護には、明示して参照可能にしたデータ以外は他のドメインの情報を見れない静的保護機能と、他のドメインに情報を見せる場合にも、参照可能な範囲を動的に限定する動的保護機能があります。この動的保護機能では、ある手続きAのドメインから、別の手続きBを呼呼び出す時、手続きA内のセグメント領域を示す記述子をパラメータとして渡しますが、この時、

◦セグメントサイズの縮小

◦アクセス権の縮小（READ/WRITEをREADに）

を動的に行います。手続きBでは、手続きAから渡された記述子をパラメータスタック（PS）内から入手して、目的とするデータ領域をアクセスします。このようにして、目的とするデータ以外をアクセスさせないことによって、プログラム情報の保護を実現しています。



(2) 確認情報の不可視化

システムの機密保護として端末接続時の確認機能と、カタログ、ファイルの不正アクセスからの保護機能がありますが、この確認機能で利用者の提示する利用者名、パスワードなどは他人に知られないことが大切です。例えば、ＴＳＳを使用する時、端末に表示されている情報が漏れることによって不正アクセスが生じることも考えられるため、確認と保護に関係している情報の不可視化として、次のような対策を行っています。

- ＴＳＳへの接続時の利用者識別名、または利用者名とグループ名の非表示
- ログオンパスワードの非表示
- ファイル名出力時のＵＭＣ（ユーザマスタカタログ）の非表示
- カタログ／ファイルパスワードの非表示

ＴＳＳ－ＡＦ使用においては、接続時の利用者名、パスワードなどの認証情報について端末画面制御のシークレット表示機能を使用して、入力文字が表示されないようにしています。これに対してバッチジョブでは、実行レポート上のパスワード部分はスペースが出力され、他人からの判読を防止しています。

ＴＳＳでは、修飾名が表示されると、そのファイルがどのノードにカタログされているか、または、どの利用者識別名を使用しているかが漏れるため、ＦＬＩＳＴコマンドでは修飾名表示時にＵＭＣ部を非表示とすることができます。

パスワードの表示／非表示について、ＦＩＬＳＹＳでは要求が特権ディレクティブである場合にのみ実行レポート上にパスワードを表示します。従って、システム管理者は特権ディレクティブを用いてパスワードを知り、ある利用者のＵＭＣやその下位のカタログおよびファイルを退避、抹消、リストすることができますが、サイト機能としてパスワード非表示機能を組入れれば特権ディレクティブによる要求に対してもパスワードの表示を抑えることができます。

また、一般利用者でも、カタログ／ファイルの退避結果またはリスト結果を入手する際に、出力レポート上にパスワード表示しない機能があるので、必要ならばパスワードの出力表示を抑えることによってファイルの保護を行うことができます。

このように、パスワードの表示／非表示を選択することによって、システムサイトの機密保持要求の度合いにより情報の保護を行うことができます。なお、パックシリアルＮＯの非表示機能、ファイル内容のパージ機能、ボリュームセット機能を使用することでさらに細かく情報の保護を行うことができます。

5. おわりに

ACOS−6/MVXのセキュリティについて概要を紹介しました。詳細については、下記のマニュアルを参照してください。

1）ファイルマネジメントスーパバイザ説明書＜ＦＭＳ＞　ＦＦＢ２１

2）利用者管理説明書　ＦＤＢ３０

3）ＴＳＳ−ＡＦシステム説明書　ＦＥＦ２２