保護資産領域分割によるユーザ管理方法の提案

岡原 弘典† 伊東 輝顕† 三浦 昭浩†
三菱電機(株) 情報技術総合研究所‡

1．はじめに

工場の生産ラインや各種製造装置など，シーケンサを用いた産業用システムでは，構成機器は主にシーケンスプログラムや各種機器へ格納されるパラメータによって制御されている．これらはパソコン上で動作する開発環境を使用して作成され，シーケンサへダウンロードされるのが一般的である．

生産ラインの効率性や生産される製品の品質などは，プログラムやパラメータに大きく依存する．これらには装置メーカやエンドユーザの技術や長年培ってきたノウハウが詰まっており，各社にとって重要なソフトウェア保護資産となっている．

しかし現在，シーケンサに書きこまれたプログラムは短いパスワードによって保護される程度に留まっている．近年，納入先で製造装置が分解，パスワード解析，プログラムのコピーが行われ，製造装置の安価なコピー製品が販売されるといった問題が発生している．

これら保護資産の流出や不正コピーを防止するため，強固で産業用システムに適合したユーザ管理とアクセス制御の仕組みが求められている．

2．産業用システム開発の特徴

産業用システムは，生産自体に関わるシステムのため，装置メーカやエンドユーザは時と場合によって立場が入れ替わる．

装置メーカがエンドユーザから制御プログラム資産を守りたいのと同様に，エンドユーザは装置メーカからパラメータ資産を守りたい，といった相互の関係がある（図1）．

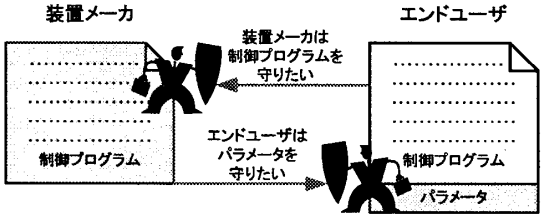

図1　保護資産の相互関係

一方，エンドユーザの生産ラインは一品一葉である．通常，装置メーカの納入した製造装置がそのまま使用されることは少なく，納入先に合った装置にカスタマイズされる．

プログラムでの例を挙げると，機器メーカが開発したライブラリを用いて，装置メーカが制御プログラムを開発し，エンドユーザは納入された制御プログラムに，製造する製品に特化したパラメータを追加するといった具合である（図2）．

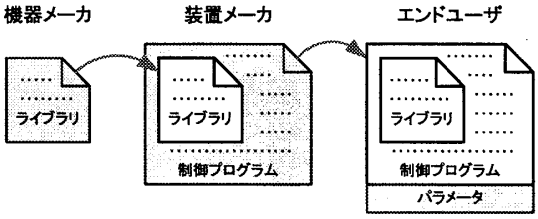

図2　プログラムのマルチベンダ開発

3．本論文で解決する課題

このような環境で保護資産の流出や不正コピー防止を確実に行うために，以下の課題がある．

1つ目の課題として，自組織以外の全ての組織からの不正アクセスを防止する仕組み（機密性の確保）が必要である．

一般的な情報システムのユーザ管理・アクセス制御方法では，システム内の全ての保護資産にアクセスできる絶対的権限を保有するシステム管理者（Administrator）がユーザ階層の頂点に存在する．

このようなユーザ管理体系を産業用システムに適用しようとすると，管理者の所属する一つの組織が他組織の保護資産に対して自由にアクセスできてしまうという問題が発生する．

2つ目の課題として，自組織以外の組織からの正当なアクセスを許可する仕組み（可用性の確保）が必要である．

従来技術であるNTドメインでは，組織ごとに保護資産を分けてドメイン間に信頼関係を持たせることで，自組織以外からのアクセスを認めている．この方法では各ドメイン管理者が常に存在している必要があり，組織から組織へ時系列で製品が納入されていく産業用システムにはそぐわない．

4．複数組織による資産管理モデル

そこで，各組織に対応した独立した領域と，全ての組織で共通の領域を定義し，保護資産を分割して管理することで，平等に保護資産を管理できるユーザ管理・アクセス制御体系を提案する．

図3は，A，B，Cの3つの組織での資産管理を表したモデルである．このモデルでは，システムの保護資産を，他組織からのアクセスを許可しないものと，複数組織にアクセスを許可するものに分けている．前者は，他組織からの不正アクセス

User management method by multiple asset domains
† Hironori Okahara, Teruaki Ito, Akihiro Miura
‡ Information Technology R&D Center,
Mitsubishi Electric Corporation

を防ぐため，組織固有の保護資産として各組織内で個別に管理する．後者は，組織を超えた共通資産と考え，他組織からアクセスできるように，共有部分で管理する．

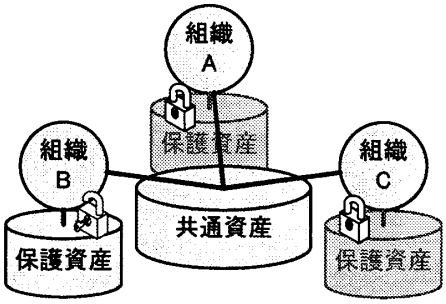

図３　複数組織による資産管理のモデル

５．具体的方法の提案

以降に図３のモデルの具体化方法を記す．

まず，各組織が管理する保護資産の範囲である「ドメイン（保護資産領域）」を定義する．ドメインには各組織に対応したものと，システム全体を通して共通な「共通ドメイン」がある． 保護資産も，そこへアクセスするユーザも共にドメインによって独立して管理される．

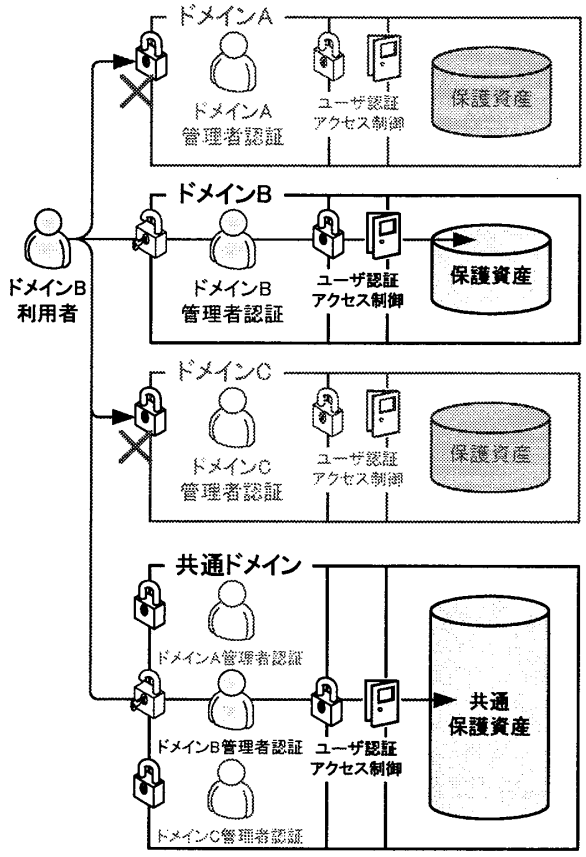

図４　ドメイン別のアクセス制御と共通ドメイン

各ドメインには「ドメイン管理者」が存在する．ドメイン管理者は，自身のドメイン内では絶対的権限を持ち，新規に他ドメインも作成できる．

ドメインでは，他組織からのアクセスを排除するため，システムを納入するタイミングで，納入元組織のドメイン管理者が自分のドメインをロックし，納入先組織のドメイン管理者が自分のドメインのロック状態を解除する．

共通ドメインでは，共通資産へのアクセスが許可された全てのユーザが管理されており，いずれかのドメイン管理者の認証をもって内部の共通資産へのアクセスが可能となる．

納入元組織のドメイン管理者は，作成した保護資産に対して，納入先組織からのアクセス制御を設定する．通常のドメインと同じく，納入時に自分のドメインをロックし，納入先ドメイン管理者がロック状態を解除する（図４）．

例えば表１では，ドメイン B 利用者は，ドメイン B 内の保護資産に関しては，アクセス制御に従って保護資産にアクセスが可能である．また，共通資産についても，アクセス対象保護資産を作成したドメインのドメイン管理者が定めたアクセス制御に従って，アクセスすることが可能である．

表１　アクセス可能な保護資産

ユーザ	アクセス対象					
	組織個別の保護資産			共通の保護資産		
	A管理	B管理	C管理	A作成	B作成	C作成
ドメイン A	○※1,A	×	×	○※1,A	○※1,B	○※1,C
ドメイン B	×	○※B	×	○※A	○※B	○※C
ドメイン C	×	×	○※2,C	○※2,A	○※2,B	○※2,C

※1:ドメインA管理者がロック解除すれば可能
※2:ドメインC管理者がロック解除すれば可能
※A:ドメインAユーザが設定したアクセス権限内であれば可能
※B:ドメインBユーザが設定したアクセス権限内であれば可能
※C:ドメインCユーザが設定したアクセス権限内であれば可能

６．まとめ

ドメイン別のユーザ管理とアクセス制御を行うことで，ドメイン内の保護資産に対するドメイン外からのアクセスを防ぐことができ，マルチベンダ開発環境においても，各組織が平等にセキュリティを確保することが可能となる．

また，共通ドメインを用意しているため，同一資産に対して複数の組織がアクセスするケースでも，作成したドメイン管理者の制御範囲内で，他組織がアクセスすることが可能となる．

今後はこの管理方法のプロトタイプを作成し，特に共通ドメインの動作について検証を行っていく予定である．