特集論文

グループ認証基盤の構築

長尾　剛*　日下　武***
下鳥洋平*　増田　博***
木幡康博**

Construction of Group Authentication Platform

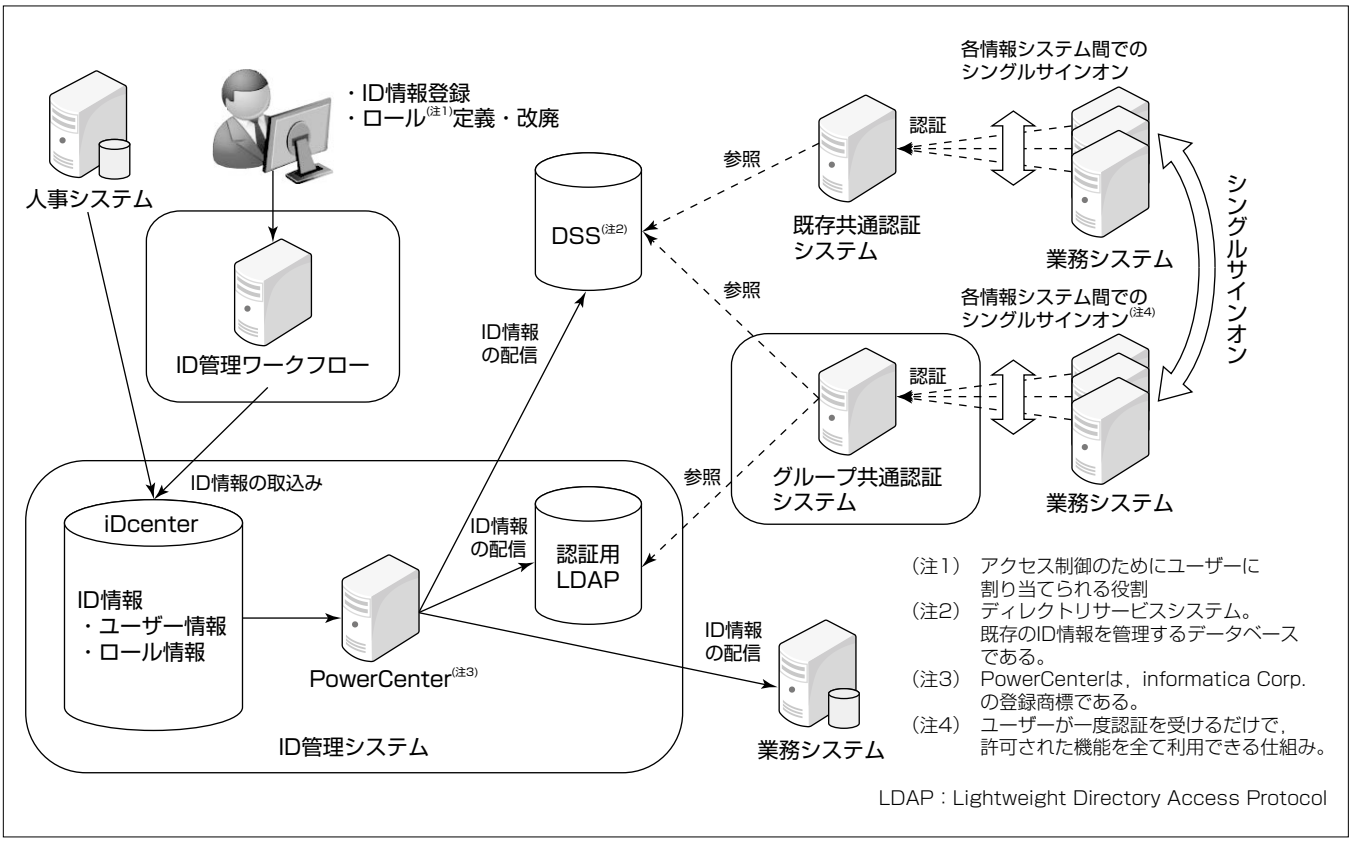
Tsuyoshi Nagao, Yohei Shimotori, Yasuhiro Kowata, Takeshi Hishita, Hiroshi Masuda

要　旨

三菱電機では，従来業務システムの認証を担う認証基盤を構築し運用してきたが，企業機密(営業，設計，製造等の情報)に関する情報システムセキュリティ対策強化や，IT全般統制(2008年4月施行)への対応として，ID改廃の履歴管理や承認機能の強化が必要とされている。一方，事業活動のグローバル化に伴い，国内・海外関係会社，取引先を含め，グローバルにセキュアな情報共有を実現するIT基盤の整備が求められている。三菱電機ではこれらの要件に対応するために，ID管理システム，ID管理ワークフロー，三菱電機グループ(以下“グループ”という。)共通認証システム等のサブシステムで構成するグループ認証基盤を構築した。

構築にあたっては，統合ID管理ソリューション“iDcenter”を導入し，IT全般統制への対応として必要となるID改廃履歴や各業務システムへのアクセス権限の一元管理を実現した。また，ID情報をメンテナンスするワークフローシステムを構築し，ID登録・改廃時の承認機能の強化や予約登録機能を実現した。さらに，各業務システムにおける認証を行うため，一元管理されたID情報を参照して認証を行う機能を実現した。

構築の成果として，IT全般統制に必要となる各種情報の管理が容易となった。また，国内・海外関係会社のみならず，取引先も対象とするID管理及び認証が可能となったことによって，セキュリティ要件を満たすグローバルな情報共有を実現した。



グループ認証基盤のシステム構成

人事システム及びID管理ワークフローからの入力によって，iDcenterにID情報が登録される。登録後，PowerCenterから認証用LDAPや各業務システムにID情報を配信する。また，グループ共通認証システムは，認証用LDAPのID情報を参照することで業務システムの認証を行う。さらには，グループ共通認証システムを利用した業務システム間のシングルサインオン(SSO)や既存共通認証システムとの相互SSOが可能である。

*三菱電機㈱ 情報システム技術センター　**三菱電機インフォメーションテクノロジー㈱　***三菱電機情報ネットワーク㈱

1. まえがき

企業機密(営業，設計，製造等の情報)に関する情報システムセキュリティ対策強化や，IT全般統制(2008年4月施行)への対応として，ID改廃の履歴管理や承認機能の強化が必要とされている。また，事業活動のグローバル化に伴い，国内・海外関係会社，取引先を含め，グローバルにセキュアな情報共有を実現するIT基盤の整備が求められている。そこで三菱電機では，業務システムのセキュリティ強化を目的としてグループ認証基盤を構築した。

本稿ではこのグループ認証基盤について，構成要素である各サブシステムの役割，工夫点を述べる。

2. システム構成

グループ認証基盤は複数のサブシステムで構成しており，また，従来のID情報管理データベースであるDSSや既存の共通認証システムと連携している(**図1**)。この章では各サブシステムの構成と役割について述べる。

(1) ID管理システム

IDの履歴管理やアクセス権限を制御するため，統合ID管理ソリューション“iDcenter”を導入し，ID情報や各業務システムへのアクセス権限の一元管理を行う。また，データ統合ソリューション“PowerCenter”を導入し，iDcenterで管理するID情報を認証用LDAPやDSS，各業務システムに対して配信する。

(2) ID管理ワークフロー

ID管理ワークフローは，ID情報をメンテナンスするシステムであり，IDの個別登録機能，一括登録機能を持つ。その中で，IT全般統制に対応するため，ID登録・改廃時の承認機能を強化するとともに，予約登録を可能とした。

(3) グループ共通認証システム

グループ共通認証システムは，ID管理システムに格納された情報が配信される認証用LDAPの情報を参照し，業務システムにおける認証とシングルサインオンを実現した。

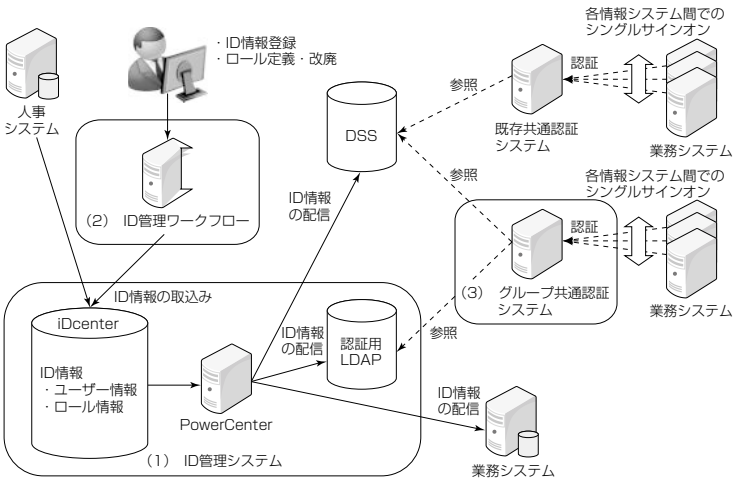


図1. グループ認証基盤のシステム構成

3. ID管理システム[1]

ID管理システムでは，ID情報，アクセス権限の一元管理を行う。ID情報は業務システムでの認証に利用し，アクセス権限は各業務システムでの認可に利用する。ID管理システムの構築にあたっての課題と対応について述べる。

3.1 iDcenter

ID情報の管理を実現する上での課題，対応及びID管理システムとして重要となるアクセス権限について述べる。

3.1.1 ID情報の管理

IT全般統制に対応するため，IDの登録・改廃に関する機能の強化を図った。

(1) 履歴管理による監査機能

iDcenterの情報はID管理ワークフローで更新するが，誰が，いつ，どこで，どのような情報を更新したかを履歴として保管する。またID管理ワークフローから履歴を参照するためのAPI(Application Program Interface) を整備し，IDやロールの登録・改廃の履歴を，ユーザーが参照できるようにした。ここでロールとは，アクセス制御のためにユーザーに割り当てられる役割のことである。

(2) ID管理機能強化

ID登録・改廃機能で，予約登録機能を実現した。反映日を指定した登録を受け付けることで，従来まで困難であった人事異動発令日当日でのID情報，アクセス権限の更新を確実に実施できるようになった。また，IDが悪用された場合などの緊急時を想定し，即時にIDを無効化する機能も実現した。

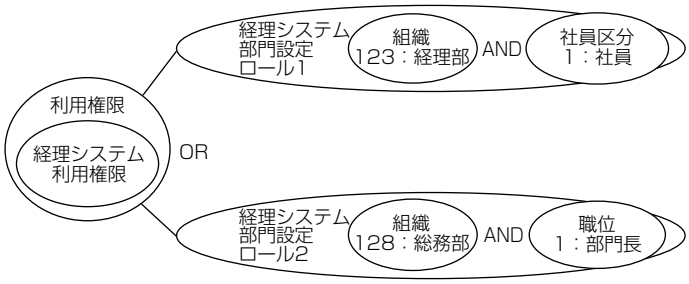
3.1.2 アクセス権限の管理

(1) ロールによるアクセス権限の管理

各業務システムでは，ユーザーに割り当てられたロールに対してアクセス権限を設定することで，効率的なアクセス権限の管理を実現できる。ID管理システムでは，ID管理システムで自動で設定する標準設定ロールと，必要に応じて追加設定する部門設定ロールの2種類のロールの設定を可能とした。

標準設定ロールは，ユーザーの職位(役員，部門長，社員，派遣等)と所属情報から自動で生成されるロールであり，業務システムで職位と所属情報でのアクセス制御を行う際に利用することができる。

部門設定ロールは，用途に応じてメンバーを定義するためのロールであり，メンバーを個人単位に定義する方法と，所属組織，役職情報，社員状況(在籍，休職)，配置状況(本務，兼務，出向)等のユーザー属性を条件として定義する方法がある。所属組織については，組織の直下だけ／指定組織配下を含



例：経理システムを利用できるユーザー＝経理部の社員　OR　総務部の部門長

図2．ロールへのメンバー割り付け

むのどちらの指定も可能とし，多様なアクセス権限への対応を可能とした(**図2**)。

ID管理システムで設定されたロールに対して，各業務システムでアクセス権限を設定することで，対応するロールのメンバーに，同一のアクセス権限を付与することができる。

⑵　人事異動への対応

人事異動があった場合，自動生成される標準設定ロールだけでなく，ユーザー属性を条件として定義した部門設定ロールについても，人事異動に伴って自動的にメンバーの更新を実施する機能を実現した。この機能によって，人事異動と連携したアクセス権限の設定を可能とした。

一方，人事異動によらず特定のメンバーに対して権限を継続的に設定する場合には，部門設定ロールで個人単位のメンバー指定を行うことで実現可能とした。

⑶　組織改編時の権限継承

人事異動時には，先に述べたとおりロールメンバーの自動更新が行われるが，組織の統合や組織名称の変更時など，組織職掌の引き継ぎが必要なケースがある。しかし，組織改編の都度ロール更新を行うことは，運用負荷がかかり，またタイムリーな更新が困難である。そこで，旧組織の情報で設定されていたロールについて，新組織のユーザーが同じアクセス権限を継承できるように，新旧組織のマッピング情報の入力を受け付け，ロールメンバーの自動付け替え機能を実現することで対応した。

3.2　PowerCenter

PowerCenterはiDcenterで管理するID情報，アクセス権限情報を配信する。配信先は，各業務システムで利用されるRDB(Relational Database)やLDAP，AD(Active Directory)[注5]等である。iDcenter上での情報更新をトリガーに，認証用LDAPやDSS，ADに対する個人情報，認証情報，アクセス権限情報の自動配信を実現した。また，配信情報の履歴管理も行っており，いつ，どのような情報が，どのシステムに配信されたのか追跡できるようにした。この機能によって，配信先で障害が発生した場合も，容易にリカバリー配信ができるようになった。

(注5)　Active Directoryは，Microsoft Corp.の登録商標である。

4.　ID管理ワークフロー

ID管理ワークフローは，主にIDや部門設定ロールの登録・改廃における申請・承認機能を実現するためのシステムであり，グループ認証基盤の入力部分を担っている。ワークフロー機能の提供によって，IDとロールの登録・改廃の責任者を明確にし，誰がいつ，どのIDについて申請・承認したかの管理を可能にした。

4.1　機　　能

4.1.1　ワークフロー機能(申請・承認機能)

各権限管理と承認経路管理の機能から成り，申請内容や状況に応じて，承認者を決定する。例えば，ID情報の更新を行う場合，申請はどの部門からでも可能であるが，承認は更新対象者の所属部門長となる。その他，承認依頼メールなどのメール送信，申請状況の確認や過去の申請書の閲覧等，一般的なワークフローに必要な機能を備えている。ID管理ワークフローから実施できる申請は，主にIDと部門設定ロールの登録・改廃である。また，会社単位に組織情報を管理する部門を定義し，対象となる部門では，CSV(Comma Separated Values)アップロードによる，組織情報，ID情報の一括登録機能を利用できる。この機能は，各社でのID管理の実態に応じて管理対象者を選択することができる。例えば派遣社員を会社単位で管理したい会社では，一括登録機能で管理し，部門単位で管理したい会社では，部門管理IDとして各部門で管理することが可能である。

4.1.2　代理承認者機能

ID管理ワークフローで承認を行う責任者は，自身に代わって業務を遂行できる代理承認者を設定することができる。設定方法には個人単位と所属＋職位の2種類を提供した。所属＋職位で設定した場合，人事異動があっても権限を引き継ぐことができる。

4.1.3　その他機能

その他，監査に必要な改廃ログや，ID棚卸しのためのID一覧を，CSV形式でダウンロードする機能，パスワードリセット機能等を実現した。

4.2　iDcenterとの連携

ID管理ワークフローは，iDcenter で管理するID情報やアクセス権限の情報を参照し，更新する必要がある。iDcenterが提供するAPIを利用して，両システム間の連携を実現した。

5.　グループ共通認証システム

グループ共通認証システムは，Webシステムとして構築された業務システムの認証・認可を行う仕組みである。グループ共通認証システムを適用したWebシステム間は，SSOが可能となる。三菱電機社内，国内・海外関係会社，取引先を含め，グローバルにセキュアな情報共有を実現するた

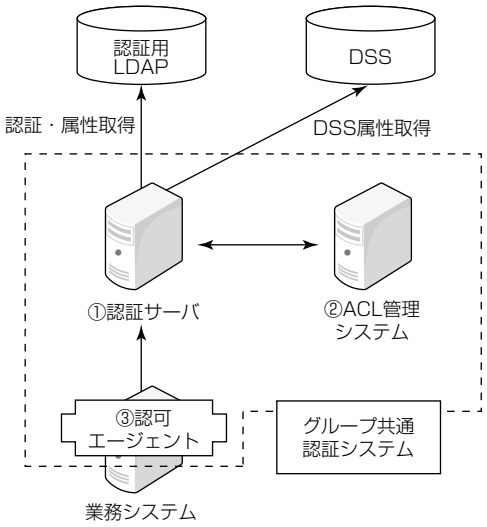


図3．グループ共通認証システムの構成

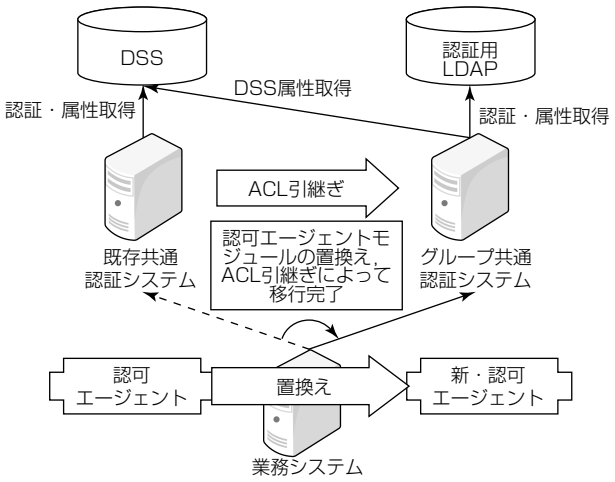


図4．グループ共通認証システムへの移行

めに，既存の共通認証システム（以下“既存共通認証システム”という。）をベースとして，認証処理におけるセキュリティやグローバル対応（多国語化）を強化したシステムである。

5.1　グループ共通認証システムの構成

5.1.1　認証サーバ（図3①）

ログイン画面の表示やID／パスワードのチェック，アクセス権限の有無のチェックを実施する。ACL（Access Control List）サーバの情報を基に生成した業務システム（URL（Uniform Resource Locator）ごと）へのアクセス制御情報，認証用LDAPやDSSから取得したログインユーザーの属性情報を認可エージェントに提供する。

5.1.2　ACL管理システム（図3②）

ACLは，業務システムのURL単位にアクセス可否の条件を定義するアクセス制御リストである。このシステムは，ユーザー属性を使用した認可条件をGUI（Graphical User Interface）画面からメンテナンスする機能を持つACL管理機能と，設定されたアクセス制御リストを管理するACL管理データベースで構成している。ACLには，従来のID情報の管理データベースであるDSSのユーザー属性，認証用LDAPのユーザー属性及びロールを使用した認可条件等の定義が可能である。

(3)　認可エージェント（図3③）

ユーザーのログイン状態をチェックするモジュールで，業務システム側に導入する。認証サーバから提供されるアクセス制御情報に基づいた業務システムへのアクセス可否情報，ログインユーザーの属性情報を業務システムへ提供する機能を持つ。

5.2　グローバル対応

5.2.1　ACL管理システム

日本語に加えて英語のGUI画面を設け，利用者パソコン上のブラウザの言語設定によって，英語・日本語のGUI画面を自動的に切り換え可能とした。

5.2.2　認証サーバと認可エージェント

日本語に加えて英語のログイン画面，エラーメッセージを設け，利用者パソコン上のブラウザの言語設定によって，英語・日本語の画面・メッセージの自動的な切り換えを可能とした。

5.3　既存共通認証システムからの移行への対応

グループ共通認証システムの稼働開始時点では，既存の共通認証システムが多数の業務システムで利用されている状況であり，業務システムごとにグループ共通認証システムへの移行作業を実施していく必要がある。移行にあたって業務システム側での改修を不要とするため，業務システムとのインタフェースの互換性を維持し，認可エージェントモジュールの置き換えだけで，移行ができるように対応した（図4）。また，移行時にはグループ共通認証システム用のACLを再設定する必要があるが，既存共通認証システムのACLを引き継ぐツールを提供し，移行にかかる工数を抑えた。

さらに，移行期間中の利用者の利便性向上のため，既存共通認証システムとグループ共通認証システム間でのSSO機能を実現した。これら2システムでは，暗号化などの処理方式が異なるため認証情報の共有は不可能であるが，相互に相手認証サーバでのログイン状態を確認する方式でSSOを実現している。

6. む　す　び

グループ認証基盤は現在，国内関係会社で活用され，安定したサービスを提供している。今後，海外関係会社への展開を推進していく。

参 考 文 献

(1)　木幡康博，ほか：大規模情報系システムにおける統合ID管理ソリューションの適用，三菱電機技報，**86**，No.7，399～403（2012）