特集論文

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

木幡康博* 森田康之*
及川和彦* 山足光義**
小宮 崇* 小杉 優**

Applying the Integrated Identification Management Solution to Very Large Information System

Yasuhiro Kowata, Kazuhiko Oikawa, Takashi Komiya, Yasuyuki Morita, Mitsuyoshi Yamatari, Yu Kosugi

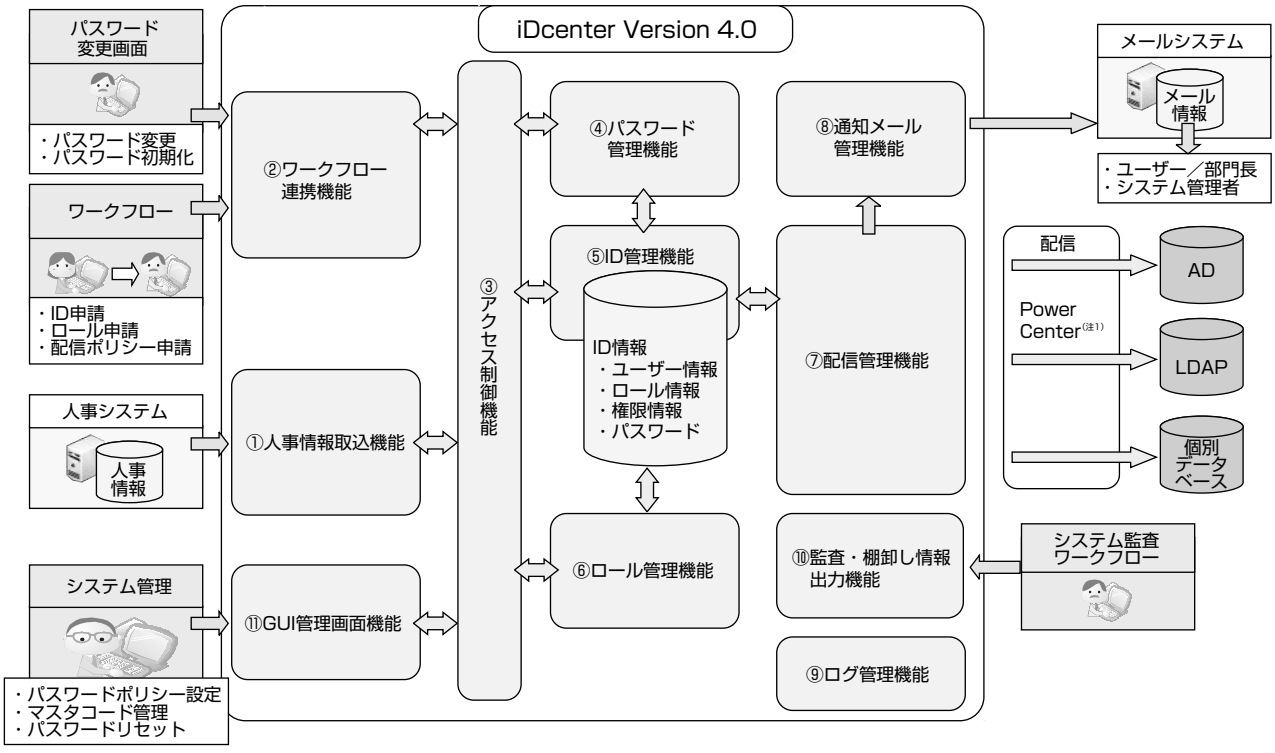
要 旨

企業には，従業員の個人識別情報を使った情報システム，入退出管理や機密情報管理等の複数のセキュリティシステムが導入されているが，それぞれのシステムがID情報を個別に持ち，ID情報の変更管理も個々に行われてきた。このため，組織変更や人事異動によるシステムへのアクセス権限や通行権限の管理負荷が増大し，変更ミスなどによるセキュリティリスクも拡大している。

統合ID管理ソリューション“iDcenter（アイディーセンター）”は，複数のシステムに対して，組織変更や人事異動によるアクセス権限の変更情報を自動配信することで，業務の効率化，セキュリティの強化を実現する。ID情報の“過去・現在・未来”にわたる世代管理によって，予約登録や情報の履歴管理による内部統制の強化が可能である。また，各種情報システムと入退室管理システムを連携し，来訪者管理，在場管理，パソコンログイン連携，勤怠管理等の様々な機能を提供する。

iDcenterを三菱電機グループ全体のユーザー11万人が利用する大規模情報系システムに適用し，次の機能を提供した。人事システムとワークフローシステムとの連携によるユーザーID情報管理機能，各種システムでの認証情報となるパスワード管理機能，各種システムに対するユーザーの利用権限の管理機能，ユーザーの所属情報や職位情報等を利用した利用権限自動割り付け機能，これらのユーザー情報，認証情報，各種システムの利用権限を自動的に各種システムに配信する機能，内部統制のためのログ管理，監査・棚卸し情報出力機能である。

これらの機能について，大規模情報系システムのID管理で必要とされる課題とその対応策を述べる。



AD：Active Directory，LDAP：Lightweight Directory Access Protocol，ID：IDentification，GUI：Graphical User Interface

（注1） Power Centerは，Informatica Corp. の登録商標である。

統合ID管理ソリューション“iDcenter”の情報系システム構成例

iDcenterは，人事システムとワークフローからユーザー情報を取り込む。また，パスワード情報と，各種システムに対する権限情報の管理と権限自動割り付けを管理する。ユーザー情報と認証のためのパスワードと各種システムでの権限情報を一元管理し，各種業務システムにID情報を配信する。また，ID情報の履歴を管理し監査ログとして提供する。

*三菱電機インフォメーションテクノロジー㈱ **三菱電機㈱ 情報技術総合研究所

1. まえがき

近年，様々なセキュリティ脅威が増大する中，ユーザー認証，アクセス制御，ログ監査等の情報セキュリティ，人の通行を物理的に制限する入退室管理システムや監視カメラ等の物理セキュリティの導入が進められている。

これらのセキュリティシステムが有効に機能するためには，氏名，社員番号，ICカード情報，役職，パスワード等の個人に関する情報（ID情報）が正しく登録され，運用されることが不可欠である。一方，システムの高度化・多様化に伴い，ID情報管理も複雑化し，ID情報の管理運用の負荷増大，登録・変更ミスや漏れによるセキュリティリスクの発生，企業におけるIT全般統制としての基盤構築の必要性等，新たな課題が認識されてきている。

本稿では，これらの課題を解決するために，統合ID管理ソリューション“iDcenter”を三菱電機グループの大規模情報系システムのID管理に適用したので，その事例を基に述べる。

2. iDcenterの特長

iDcenterの特長を次に示す。

⑴ ID世代管理による予約登録と内部統制への対応

現在の個人情報，組織情報を管理するだけでなく，過去の個人情報，組織情報を世代管理し，未来の個人情報となる予約登録（例：4月1日付けの新入社員を含む人事異動情報を3月20日に事前登録）を可能とする（**図1**）。また，情報の世代管理によって，いつ，誰が何を変更したかの履歴を参照でき，内部統制に対応できる。

⑵ 各種システムへの利用権限自動割り付けと自動配信

人事システムから取り込まれる人事異動の情報やユーザーの役職情報等によって，各システムに対しての利用権限を設定することで，人事異動による利用権限の変更が自動的に行われ，変更情報を自動配信する。

⑶ 日本企業に適したID管理

日本企業では，組織の階層例として事業本部，統括本部，部，課，係，班と言った階層構造が深いツリー状の組織体系を持つ。iDcenterでは，このような深い組織階層構造でも対応できる内部データ構造を持ち，配下を含めた部全体や統括本部全体に対して各種システムの利用権限を管理できるなど，日本企業に適した統合ID管理を実現する。

3. 認証システムとiDcenterの役割

今回開発した大規模情報系システムに対するiDcenterのID管理機能は，三菱電機グループ全体の認証システムの一部として利用するために，機能強化が行われた。この認証システムの概要とそこで利用されているiDcenterの役割について述べる。

⑴ 認証システム

三菱電機の社内，国内外関係会社及び社外取引先の会社を含めて，グループ全体で11万人のユーザーが使用する各種システムに対する認証機能を提供する。

⑵ iDcenterの役割

図2に示すように，iDcenterでは，①人事システムと連携しCSV（Comma Separated Values）形式でユーザー情報を一括で登録する機能と，②API（Application Programming Interface）によって画面から個別にユーザーを登録する機能の2つの方法が利用できる。③権限管理では，人事情報だけでなく各種システムへのユーザーの利用権限情報をiDcenterに取り込む。④パスワード管理では，APIによって，認証情報となるパスワードを取り込み，変更，初期化を管理する。⑤配信機能では，こうして取り込んだユーザー情報，認証情報，各種システムへの利用権限情報を認証システムであるLDAPや各種ADシステム，各種業務システムへ配信する。各種システムは，iDcenterから渡された情報で認証を行う。⑥内部統制のためのID情報，権限情報の履歴管理を提供する。

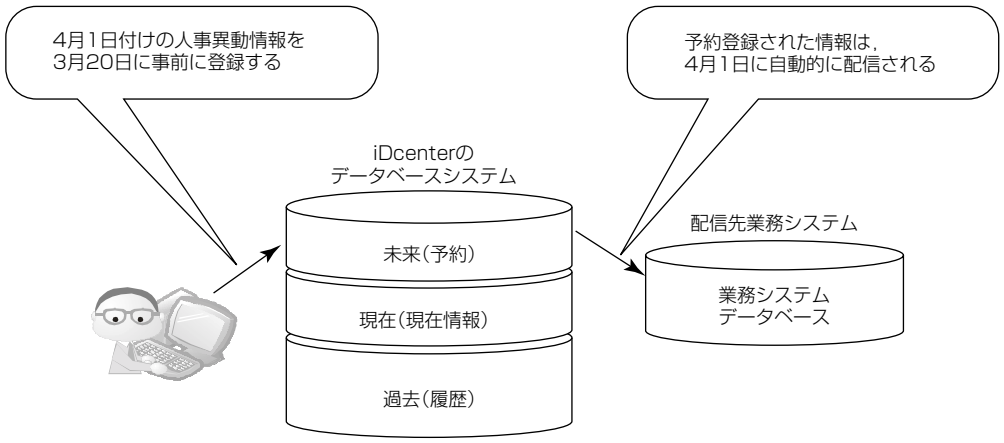


図1．予約登録

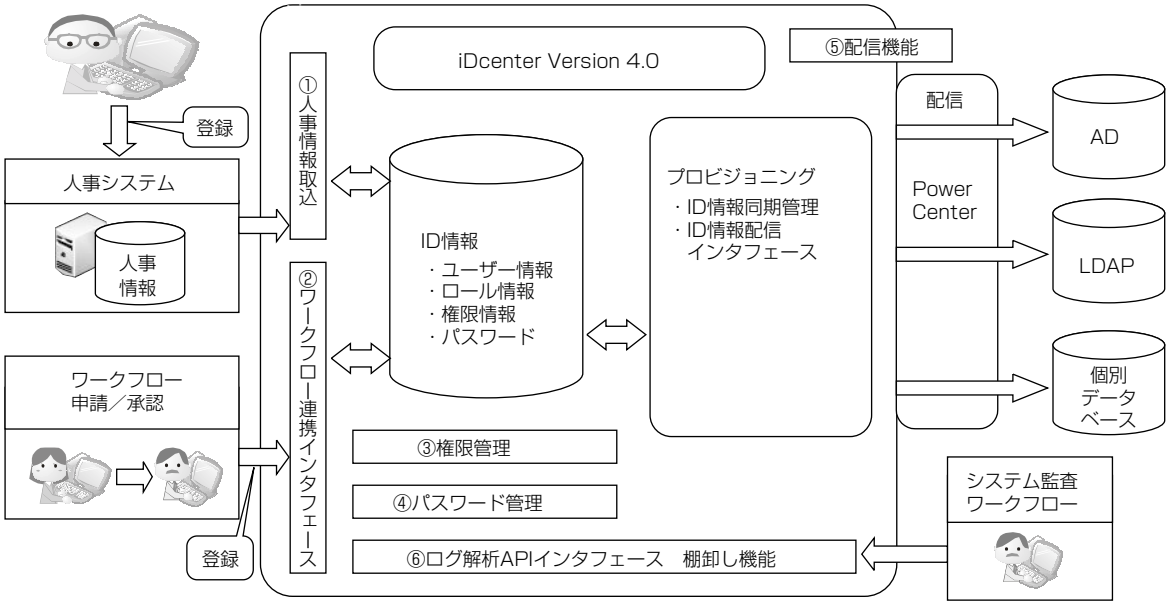


図２．iDcenterの役割範囲

4. 大規模情報系システムのID管理に関する課題と対応

iDcenterは，人事システムデータからID情報を生成し，認証のためのパスワード管理を行い，各種システムの権限を一元管理して，それらの情報を各種システムに配信することで，ID管理を自動化し管理コストを低減する。ここでは，主な追加開発機能である①データ入力，②権限管理自動化，③配信制御，④配信先連携レパートリーの強化，⑤内部統制のための監査機能の課題とこの開発における対応について述べる。

4.1　データ入力での課題と対応

iDcenterは，人事システムとワークフローから渡される人事情報，各種システムへの認証情報となるパスワード及び各種システムへの権限情報を管理する。人事情報については，人事システムと連携してユーザー情報を一括で取り込む機能に加えて，ワークフローから個別にユーザー情報を取り込むためのAPIの機能が求められた。また，ユーザー情報だけでなく，ユーザーにシステム利用の権限を割り付けるためのAPIも必要となる。さらに，このシステムは海外関係会社を含むため，グローバルな対応が必要となった。

⑴　APIによるワークフロー機能への対応

企業が持つワークフローに対して，人事情報の取り込みAPI，承認・代理承認のためのAPI，認証情報であるパスワード更新・初期化のためのAPI，各種システムに対する利用権限割り付けのためのAPIを提供することで，各種ワークフローによる情報をiDcenterに直接取り込み，人事情報，認証情報，権限情報を一元管理できるようにした。これらのAPIによって，各企業が既に使用しているワークフローエンジンを利用して，企業固有のワークフローを構築できる。

⑵　UNICODEによるグローバル対応

適用システムでは，世界中に工場や支社，取引先企業があることから，グローバルなユーザー登録が必要となる。データ入出力をUNICODEにすることで対応した。

4.2　権限管理自動化のための課題と対応

ID管理では，各種システムへのユーザーの利用権限割り付け機能をどれだけ自動化できるかが，システム導入の際の重要なポイントの一つとなる。この課題については，ロールによる権限付け替え自動化機能を強化することで対応した。

ロールは，複数の人や部門を同一の権限グループとして扱うために利用するものである。iDcenterでは，ユーザーの権限管理としてロールを利用する。同じロールに割り付けられたメンバーは，対応の業務に対して，同じ利用権限を持つ。複数の組織をロールAに割り付け，このロールAの属性情報とロールAに割り付けられたメンバー情報を業務システムAに配信することで，ロールAに割り付けられた組織の人は，業務システムAに対して，同じ利用権限が与えられる。ロールに対して，どのようにユーザーを割り付けできるかが，システム自動化の決め手となる。ロールに対して個人を割り付けると，人事異動によって権限がなくなった時に，ロールから削除する必要があり，管理が煩雑となる。企業の中での各種システムの利用権限は，所属と部長・課長等の職位などによって，与えられることが多い。ロールに割り付ける方法として，組織とユーザーの職位を条件として割り付けを行うことで，権限割り付けの自動化が図れる。

ロール割り付けの条件として，組織の直下のユーザーを対象としたり，指定組織配下のユーザーを対象としたりできる。さらに，会社単位，事業部単位といった部門単位や，

ユーザー区分等の他のユーザー属性を条件として，ロール割り付け設定を行うことができる。これによって，柔軟な権限割り付けの自動化を実現できた。**図3**にロールへのメンバー割り付けの例を示す。

4.3 配信制御での課題と対応

iDcenterの配信制御は，夜間に取り込んだ人事情報データを，これまでに配信した情報との差分を取って，各種システムに一括配信する機能を基本としているが，APIで入力された情報を即時配信する機能も開発した。また，人事異動や組織変更に伴う混乱を回避するため，引継ぎのための猶予期間を設けた配信にも対応した。

(1) 一括配信制御

iDcenterの配信制御は，データ取り込み済みの入力データテーブルと各種システムへの配信済みデータを保持する配信データテーブルによって管理される。入力データテーブルと配信データテーブルには，過去に入力されたデータと過去に配信されたデータが配信履歴情報として管理されているので，IDの世代管理を行うことができる。

図4に一括配信制御の概要を示す。通常は，夜間に人事システムからバッチでデータを一括で取り込み，一括配信する。

(2) 即時配信制御

ワークフローからAPIを用いて入力されるデータは，ユーザーごとに即時で各システムに配信することが求められることから，性能面を考慮した配信制御を実現した。即時配信では，**図5**に示すように，ワークフローから入力されたユーザー情報を配信データテーブル中の対応するユーザーデータと比較し，この差分データを配信する。これによって，配信性能の向上を図った。

(3) 猶予期間を考慮した配信

iDcenterは，各種システムに対してユーザー情報，利用権限情報，認証情報を配信する時には，原則として，配信日のユーザーの利用権限を配信する。しかし，所属で利用権限が決められている業務システムなどでは，人事異動などで誰も利用できなくなると困るシステムがある。こうしたシステムに対しては，引継ぎのための猶予期間を与えて利用権限を配信することを可能にしている。

4.4 PowerCenter連携による配信先連携レパートリー強化

配信先システムとしては，CSVファイルによる連携だけでなく，LDAPシステムやADシステム，データベースシステムに対して，直接連携できる機能が求められる。

iDcenterは，ETL(Extract Transform and Loading)機

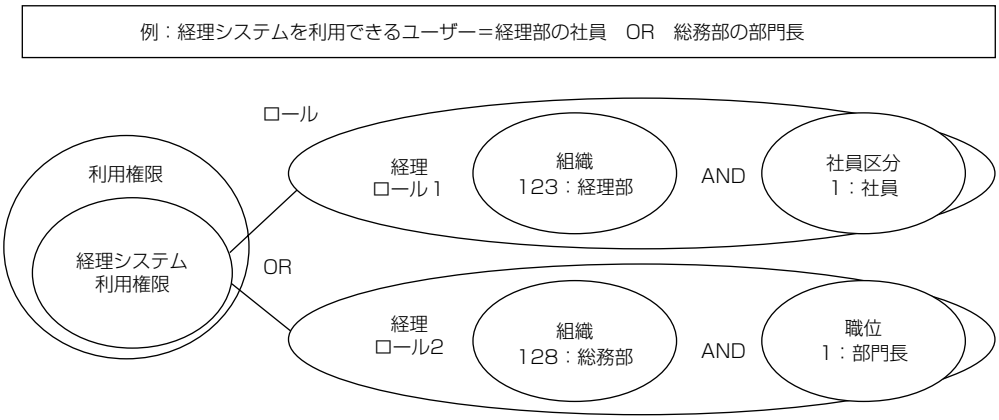


図3．ロールへのメンバー割り付け例

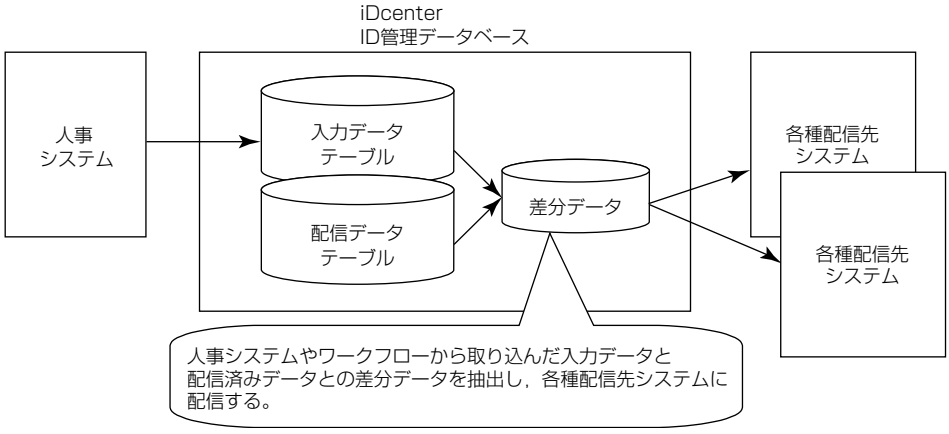


図4．一括配信制御

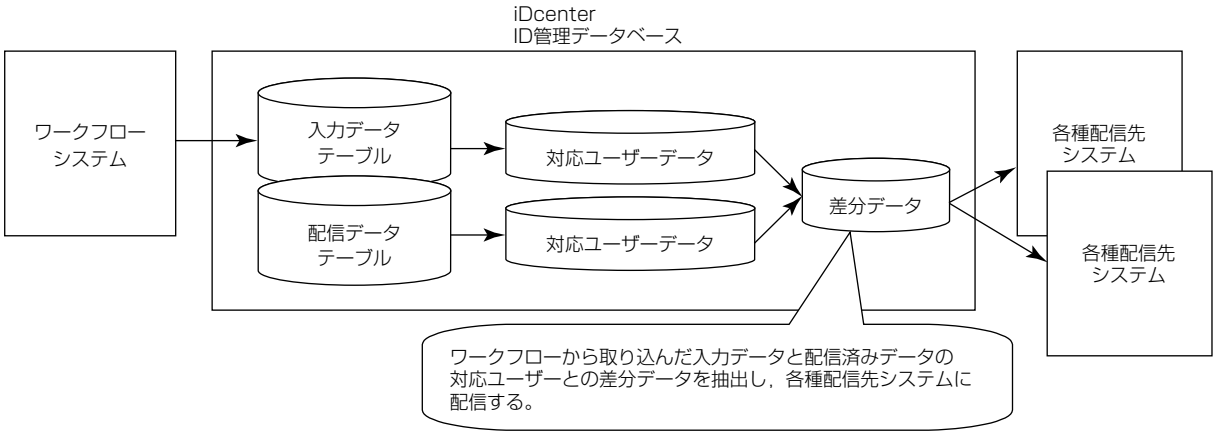


図５．即時配信制御

能搭載のデータ統合ソリューションInformatica Power Center（以下“PowerCenter”という。）と連携し，人事システムからiDcenterに取り込んだ全社のID情報を情報系システムの認証基盤となるLDAP／ADへPowerCenterを通して自動配信する。また，PowerCenterとの連携によって，ORACLE(注2)，SQL Server(注3)，DB2(注4)等のデータベースとの連携も可能となった。

（注２） ORACLEは，Oracle Corp. の登録商標である。
（注３） SQL Serverは，Microsoft Corp. の登録商標である。
（注４） DB2は，International Business Machines Corp. の商標である。

4.5 ログ・監査機能強化

内部統制に対応するため，入力された情報に対して，履歴を追跡できる必要があり，ID情報の履歴管理強化によって対応した。

⑴ 操作ログ機能強化

所属長が承認して登録されたID情報に関しては，誰が，いつ，どこで，どのような情報を登録したかについてログを残し，履歴を参照可能とするためのAPIを提供した。これによって，ワークフローで登録された派遣社員の情報や，各種システムへの権限情報の割り付けについての履歴を参照できるようにした。

⑵ 情報の世代管理による監査機能

iDcenterでは，入力された情報の全てが履歴として管理されており，いつどのような情報が入力されたかについてデータベースを確認することで追跡できる。また，配信情報についても世代管理されており，いつどのような情報が，どのシステムに配信されたのかをデータベースを確認することで追跡できる。

5. むすび

iDcenterの特長であるID情報の世代管理による予約登録や猶予期間を考慮した配信への対応，ロールによる権限の自動割り付け機能強化等によって，三菱電機グループの大規模情報系システムにおけるID管理業務負荷の軽減，セキュリティの強化，ID情報の履歴管理による内部統制への対応等を実現することができた。

今回，iDcenterに対する機能強化として，API機能，ロール管理機能強化，配信先システム連携強化としてのLDAP連携，AD連携，各種データベース連携機能等の開発を行ったが，これらの機能を取り込んで，“iDcenter Version4.0”として製品化する予定である。また，今後は，オンデマンドITサービス対応の強化を図り，適用範囲を拡大していく。

参考文献

⑴ 木幡康博，ほか：確実なセキュリティ運用を実現する統合ID管理システム“iDcenter”，三菱電機技報，**83**，No.9，559～562（2009）