特集論文

統合ID管理システム“iDcenter”の特長と適用事例

釜坂　等*　　鍋山和也***
池田健一郎*
高橋洋一**

Feature and Application Experience of Total Identification Management System "iDcenter"

Hitoshi Kamasaka, Kenichiro Ikeda, Yoichi Takahashi, Kazunari Nabeyama

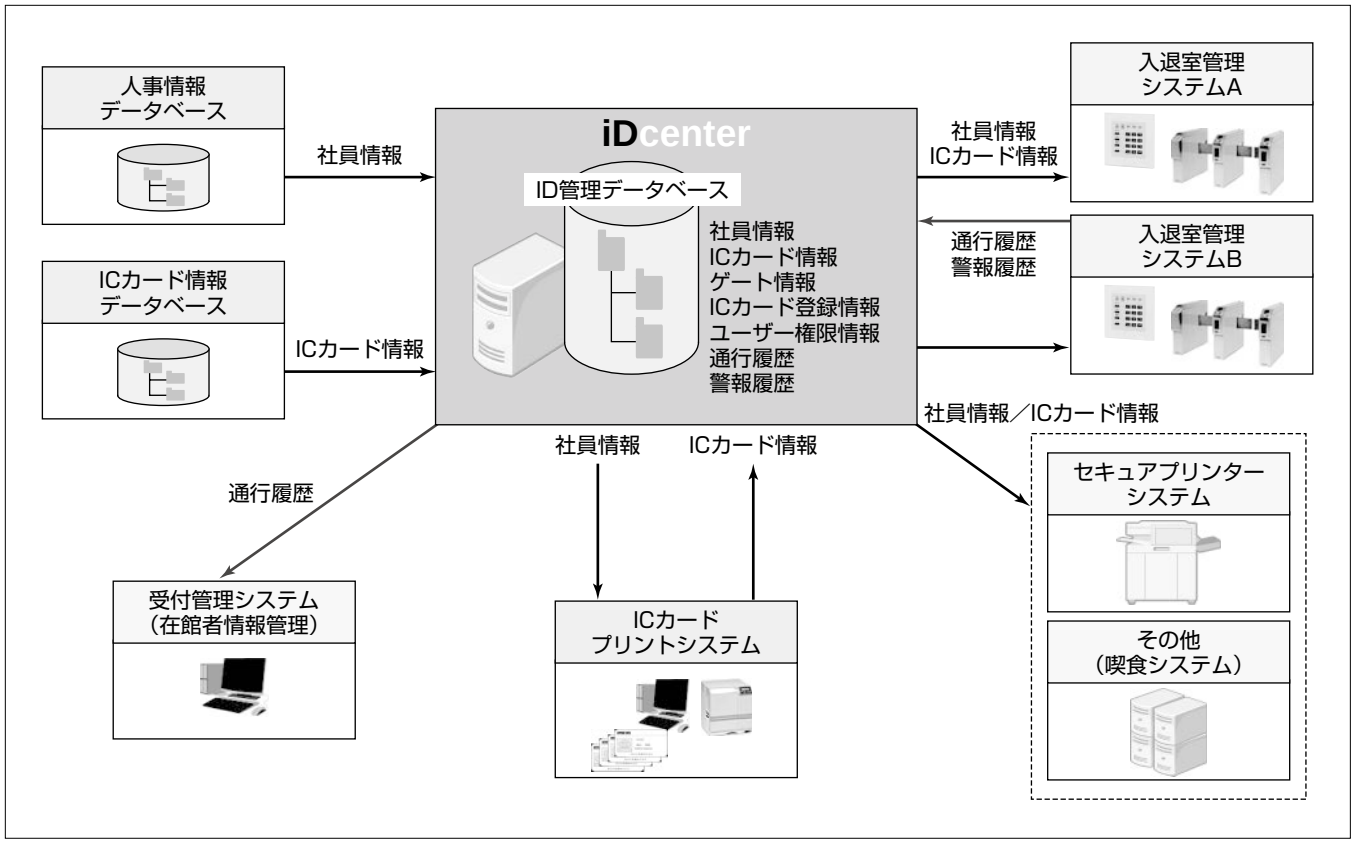
要　旨

近年，様々な脅威に対して，情報セキュリティ対策や物理セキュリティ対策がそれぞれ進められている。本稿では，情報セキュリティと物理セキュリティの両方に対応する統合ID管理システム“iDcenter”の特長を述べるとともに，その適用事例について述べる。

iDcenterは，人事情報データベースと同期して，社員情報などからなるID情報を一元管理し，認証が必要な各種システムに配布する。特に，日本型組織に対応した2つの特長を持つ。1点目は，RBAC（Role Based Access Control）方式による，組織のロール（役割）に応じてセキュリティポリシーを決めるロール管理機能である。2点目は，履歴管理による，人事異動後の仕事の引継ぎなどによって一定期間両方の組織の権限が必要な場合にも対応する猶予設定機能である。

このシステムを東京に本社を置く某製造会社に納入した。適用システムでは，既存の人事情報データベースと同期し，各種システムが管理するID情報の更新・削除などを確実に行う。入退室管理システムへID情報とセキュリティポリシーを配布し，適切な入館・入室を制御する。又，セキュアプリンターシステムなどへも配布し，適切なアクセス制御を実現し，入館履歴を用いた在館者の管理による入退館のセキュリティを強化している。さらに，ほかの地域に設置している入退室管理システムへも同時にID配布を行うため，地域にまたがる異動や社内出張でも，同一のICカードでの入退館・システム利用を可能としている。

今後，iDcenterは，ワークフローとの連携などの機能拡張をしていく予定である。



統合ID管理システム“iDcenter”のシステム構成例

iDcenterは，人事情報データベースから人事異動時に社員情報を入手する。新規社員情報があれば，ICカードプリントシステムで，ICカードの印刷発行を行うとともに，ICカード情報をiDcenterに登録する。iDcenterは，この社員情報やICカード情報を，入退室管理システムやセキュアプリンターなどのシステムへ送付する。又，入退室管理システムからの通行ログは，iDcenterに蓄積され，在館者情報として活用する。

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

1. まえがき

近年，様々なセキュリティ脅威に対して，ユーザー認証，アクセス制御，ログ監査などの情報システムを対象とした情報セキュリティ対策や，人の通行を物理的に制限する入退室管理システムやカメラ監視など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，パスワードなどの個人に関する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など，新たな課題が認識されてきている。

本稿では，これら課題を解決する統合ID管理システムiDcenter[(1)]の特長を述べるとともに，このシステムの某製造会社への適用事例について述べる。

2. iDcenterの特長的な機能

2.1 統合ID管理システム

iDcenterは，人事情報データベースと連携して，ユーザー情報，ICカード情報，利用者権限情報からなるID情報を一元管理し，各種システムに権限情報を配布するシステムである。配布する権限情報は，入退出管理装置や認証・認可などのシステムに応じた形式や情報に加工し，配布することが可能である。

2.2 iDcenterのシステム構成

iDcenterは，ID管理機能と外部連携機能から構成される(**図1**)。ID管理機能は，権限管理データベースと履歴管理データベースで構成している。

次に，人事システムの人事情報データベースと連携し，ICカードを使った入退室管理システムへのID情報を配布するシステムを例にiDcenterの機能を述べる。

iDcenterでは，人事情報システムからユーザー情報などのID情報を,外部連携機能を介して取得する。取得したID情報は，履歴管理データベースで管理する。入退室管理システムへは，履歴管理データベースで管理しているID情報を用い，権限管理データベースに設定したロールに従い生成された権限情報とを，外部連携機能を用い，入退室管理システムに配布する。

2.3 統合ID管理における課題

ID情報を統合的に管理するには，ID情報の配布時の権限情報を生成するためのロールや，変更するID情報の履歴を組織にあった方法で管理することが重要となる。

ロール管理は主に役割に関係し，履歴管理は主に人事異動に関係する。

iDcenterでは，ID管理における次の2つの課題を解決した。

(1) ロール管理は，役割に対する考え方によって，管理方法が異なる点が課題となる。役割の考え方は，個人に役割を付与する考え方と，個人でなく組織に役割を付与する考え方がある。又，組織に役割を付与する場合も，上位組織が下位組織の役割を包含する場合がある。この役割の包含などの，考え方の違いに柔軟に対応する実装をした。

(2) 履歴管理方式は，組織の人事異動に対する考え方によって，管理方法が異なる点が課題となる。人事異動は，必要に応じ採用して少数の異動を随時行う考え方と，4月1日などの特定の日付で大規模に行う考え方がある。特定の日付で大規模に行う場合は，事前に人事情報を登録することも考慮する必要がある。このような事前登録の必要有無に対応する実装をした。

次に，このようなロール管理と履歴管理の課題について，iDcenterの解決策を述べる。

2.4 ロール管理機能

iDcenterのロール管理機能は，RBAC方式を実装した。RBAC方式は，ロールを中心に，人や組織の人事情報を関連付けた情報と，対象システムを関連付けた情報を用いてID情報を管理する(**図2**)。

さらに，iDcenterでは，RBAC方式を下位組織の権限情報を上位組織が包含する方式として実装した。

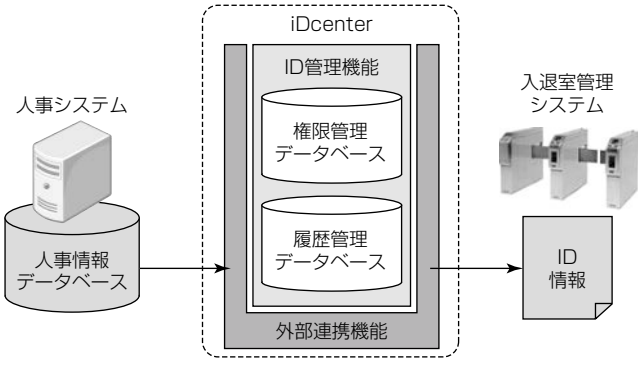


図1．システム構成

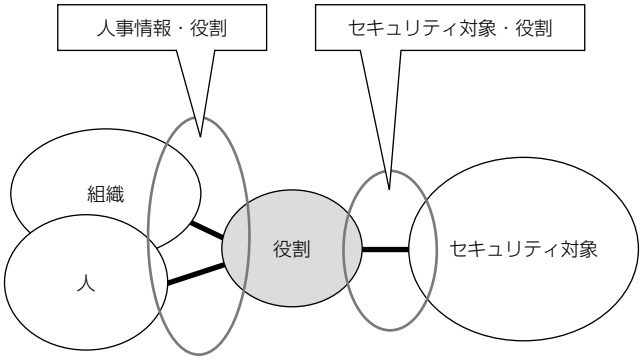


図2．RBAC方式

次に，入退室管理装置への権限配布時の例として，iDcenterが実装した方式を述べる。

iDcenterでは，ロールに組織を関連付ける場合，組織構造を有効に活用するため，上位組織を選択すると下位の組織を含んだ組織を指定したことになる。例えば，**図3**の開発部を選択すると，その部の全課を指定したことにもなる。

例えば，開発部の共通エリア内に，新製品開発課の専用エリアがあり，共通エリアの入り口を入退出管理装置で管理し，更に奥の新製品開発課専用エリア用の入り口を入退出管理装置で管理した場合のエリア例を**図4**に示す。配信する権限情報は，開発部の共通エリアに設置した入退室管理装置へは開発部を指定し，新製品開発課の専用エリアへは新製品開発課のみ指定することで，開発部の全部員に対しては開発部共通エリアへの入退室可能とし，新製品開発課の課員には同専用エリアへの入退室可能とする制御が可能となる。

これによって，対象組織内の組織変更の場合は，組織での役割変更だけで，個別の権限変更を行う必要がない。

2.5　履歴管理機能

iDcenterの履歴管理は，履歴管理データベースを用い，ID情報の現在・過去・未来の状態を管理している。これによって,任意の時点でのID情報の確認が可能となる。

また，ID情報は，組織と関連付けた各ユーザーの有効期限とともに管理する。

例えば，現時点で，ユーザーAは組織B，ユーザーBは組織A，ユーザーCは組織Bに所属しているとする(**図5**)。この場合，過去の定期異動より過去の日付である任意の過去の日を確認すると，ユーザーAは組織A，ユーザーBは組織Aであり，ユーザーCは存在しない。

次に，先に述べた管理のID情報に対し，将来の定期異動の人事情報を事前投入した場合について述べる。定期異動の人事情報を事前投入した場合，現時点の各ユーザーの情報は影響を受けない。しかし，将来の定期異動日以降の任意の未来の日は，各ユーザーの配属情報が更新され，ユーザー情報を参照すると，ユーザーAは組織C，ユーザーBは退職，ユーザーCは組織Bとなる(**図6**)。

そして，各ユーザーの組織の有効期間には，猶予期間を設定できる。例えば,仕事の引継ぎなどによって一定期間両方の組織の権限が必要な場合にも対応できる(**図7**)。

なお，履歴管理機能は，人事異動の情報を連続して管理するため，役割の情報と併せ，不正行為の事後形跡証跡などの解析時の情報としても使用可能である。

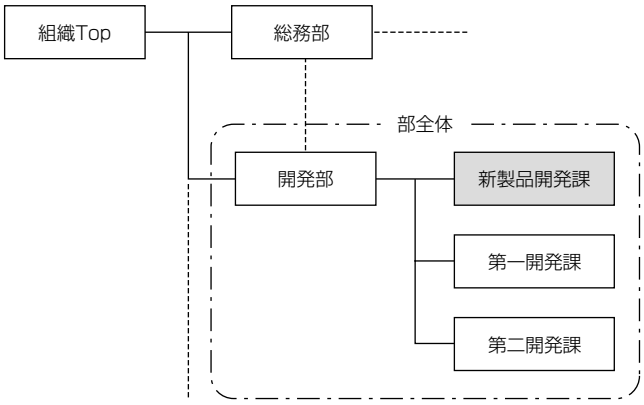


図3．役割に関連つける組織の関係

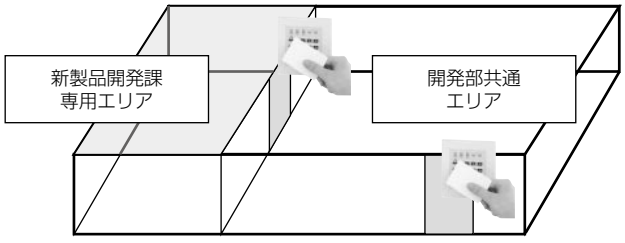


図4．入退室装置によるエリアの管理

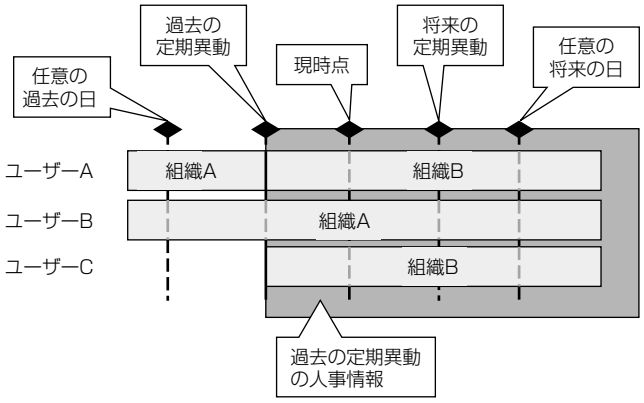


図5．ユーザーの履歴管理方法(1)

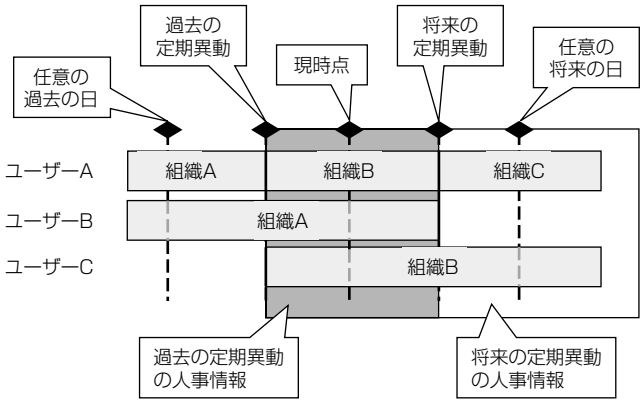


図6．ユーザーの履歴管理方法(2)

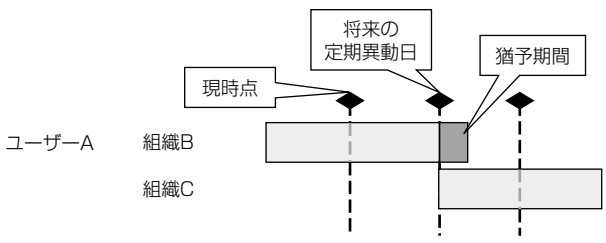


図7．ユーザーの所属の猶予期間

3. 適 用 事 例

iDcenterと入退室管理システムであるMEL-SAFETY-Gとの連携システムとして，東京に本社を置き，全国に工場を持つ某製造会社へ納入した。その納入事例について述べる。

3.1 要 求 仕 様

iDcenterの主な要求仕様を次に述べる。

(1) ビル入退館セキュリティの向上

人事情報データベースからの人事異動情報の入退館システムへの自動反映による適正な入退室制限の実現と通行履歴管理によるセキュリティ監査を実現する。

(2) ICカードによる利便性の確保

ICカードを利用したシステムの構築によって，セキュリティレベルを維持しながら，利用者による認証の利便性を確保する。ICカードの認証キーを用いた認証によって，セキュアプリンター，喫食システム等における運用の利便性の向上を図る。又，全国にある各工場に設置された入退室管理システムに対して1枚のICカードでの相互入館を実現する。

(3) 管理負荷低減

在館者及び人数を確認できる仕組みを取り入れることによって，ビル警備負荷軽減を図る。

3.2 適 用 範 囲

iDcenterは，既存の人事情報データベースや入退室管理システムやセキュア管理システムと連携するように構成した(**図8**)。

iDcenterの主な適用業務を次に述べる。

(1) IDの統合と権限割り付け，及び配信業務の自動化

人事情報データベースからの社員情報とICカード情報の紐(ひも)付けを行い，社員のID情報として統合管理するとともに，各種連携システム(セキュアプリンターシステム，喫食システム)への利用者ID情報の配信を行っている。特にMELSAFETY-Gに対しては，正社員や派遣社員などの属性に応じて，入退室管理の通行権限の割り付け情報も配信している。iDcenterでは，人事情報データベースから入力される属性情報に応じて，ロール管理機能によって自動的に権限の割り付けを行っている。

(2) 社員の人事異動に伴う引継ぎ期間の旧権限維持

人事異動発令後の引継ぎ期間を考慮し，旧組織で設定していた権限(通行権)を一定期間削除せず維持できるように猶予期間を設定しMELSAFETY-Gに自動配信している。

(3) 連携システムへの情報提供(ITシステム連携機能)

ビルオーナーの入退室管理システム，喫食システムで使用するID情報をCSV(Comma Separated Values)ファイル形式で定期的に提供することによって最新の情報でICカードとの認証を実現している。

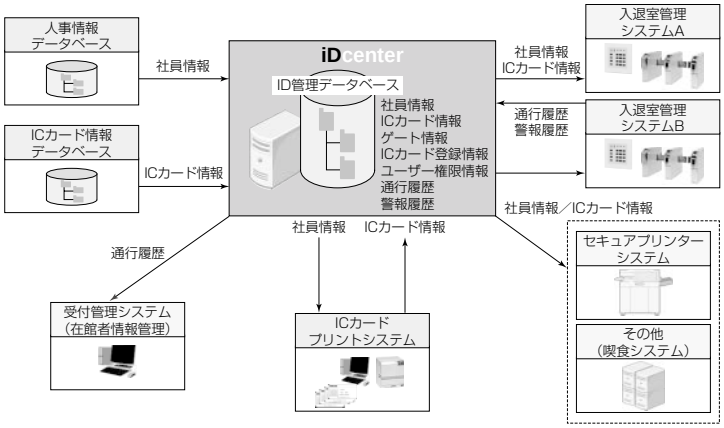


図8．システム構成例

(4) 拠点間相互入館

通行権限の割当て機能によって拠点に設置された入退室管理システムに対して1枚のICカードでの相互入館を実現している。これによって長期出張者は出張先での日々の貸出しカード申請が不要となっている。

(5) 在館人数情報提供業務(ITシステム連携機能)

来訪者管理は，iDcenterとは別システムである顧客受付管理システム側で実施されている。特定ゲートに関する退館情報は統合ID管理システムから顧客受付管理システムに定期的に提供することによって，来訪者の在館人数が，顧客受付管理システム上で確認できるため，警備員による見回りの負荷を軽減している。

3.3 メ リ ッ ト

“IDの統合と権限割り付け，及び配信業務”を自動化したことによって“ID情報の同期の確保”“登録作業ミスの減少”“管理コストの低減”といった効果がでている。今回，iDcenterはMELSAFETY-G，セキュアプリンター，喫食システムとの連携を実現しているが，対象システムを更に拡張することによって上記メリットの拡大が期待できる。又，今後の展開として本社集中による複数管理拠点を追加していくことによって社内セキュリティポリシーの統一化によるセキュリティの安全性向上が期待できる。

4. む す び

iDcenterバージョン3.0として,①情報取込機能，②パスワード管理機能を追加した版をリリースした。以降のバージョンで①ワークフロー連携，②AD(Active Directory)へのデータ投入及び③LDAP(Light weight Directory Access Protocol)連携機能の追加開発を計画している。

参 考 文 献

(1) 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）