特集論文

企業の安心・便利を支えるクラウドID管理サービス“DIASMILE”

勝山尚彦* 佐藤雅之**
濱田 剛*
大沼聡久*

DIASMILE：Cloud-based ID Management Service to Provide Security and Convenience for Companies

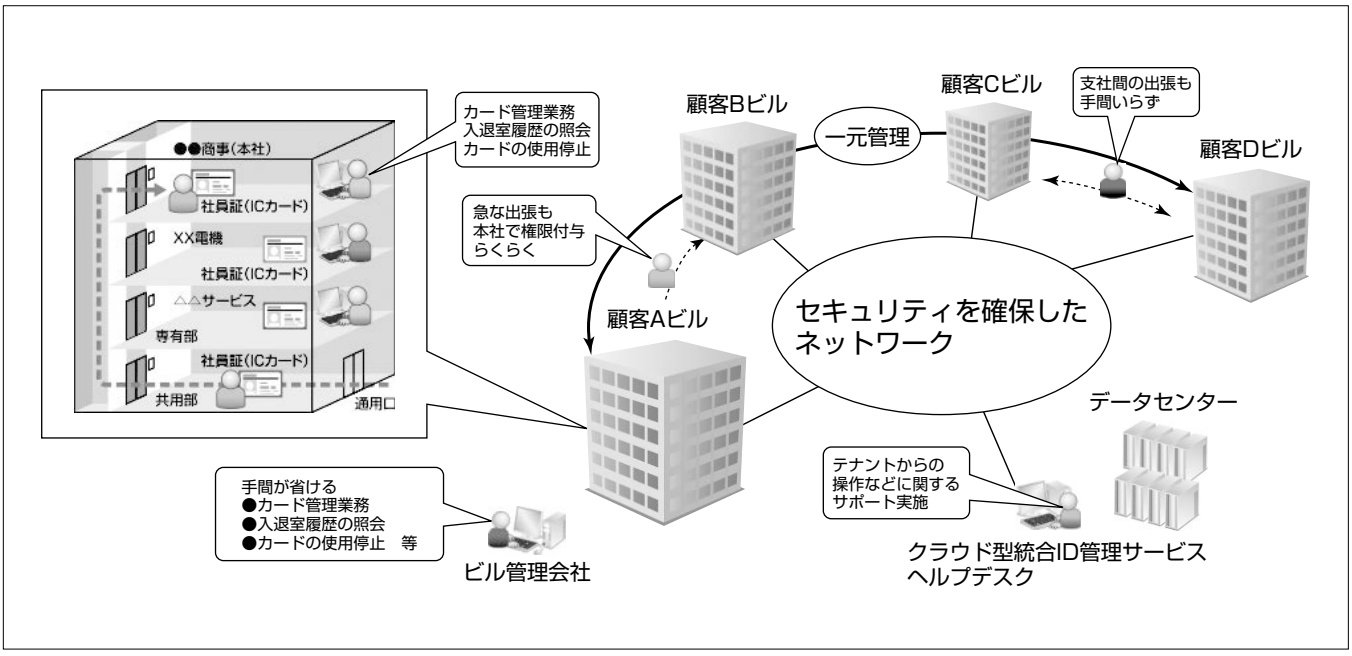
Naohiko Katsuyama, Tsuyoshi Hamada, Akihisa Oonuma, Masayuki Sato

要 旨

不正競争防止法の改定，個人情報保護法，日本版SOX法（米国企業改革法）の施行，サイバー攻撃の激化によって，企業におけるセキュリティ強化のニーズは高まっている。情報システムでは，シングルサインオンなど複数のシステムを統一して認証することによって，利用者の利便性を向上させるとともに，セキュリティの強化を進めてきた。一方入退管理システムやセキュアプリンターを始めとする物理セキュリティシステムについては，機器が拠点ごとに導入されてきた経緯もあり，その管理についても拠点独自で進めているケースが多い。これらの機器の管理者は，組織変更や人事異動による配置転換が発生した場合，それぞれの物理セキュリティシステムに対して，都度メンテナンスを行う必要がある。その結果，管理負荷が増大するとともに，変更漏れなどによるセキュリティリスクも拡大してきている。

クラウドID管理サービス“DIASMILE”（以下“DIASMILE”という。）は，従来ビル管理会社が運用していた入退管理システムのIDカード管理を利用者（テナント）に開放し，利用者が直接行えるようにすることで，利用者の利便性を向上させるサービスである。DIASMILEでは，複数の物理セキュリティシステムを統合的に管理する考え方のもと，入退管理システムなどをインターネット経由で接続する。これによって，従来はビルごとに設置されていた入退管理システムや従来のID管理ソリューションでは対応できなかった専有部と共用部の一元管理や，分散した企業の入退管理を一元的に行うことが可能となった。DIASMILEのベースとなる統合ID管理ソリューション“iDcenter”は，三菱電機グループ11万人が利用する情報システム基盤に導入され，三菱電機グループ内の様々な情報システムに対する統合ID管理としての機能を提供してきた。その大規模システムの実績を踏まえて，DIASMILEでは，各利用者が独自に利用できる基盤を構築可能とし，利用者に開放するサービス提供を実現した。その結果，企業における生産拠点や営業拠点の物理セキュリティシステムを一元的に管理するニーズへの対応が可能となった。

今後は，各拠点にある様々な物理セキュリティシステムと接続可能とするように機能を拡充し，利便性，安全性の向上を図っていく。



クラウドID管理サービス“DIASMILE”の全体イメージ

利用者（テナント）は，ビルの共用部，及び自社の専有部を通行する自社社員の個人情報，カード情報，通行権限などに対する管理業務を自席から行うことが可能である。また，他ビルに入居する支社などに関する管理業務も一元的に行うことが可能である。これによって，複数のビルに跨（またが）った場合でもカードの一枚化やセキュリティポリシの統一が可能となり，セキュリティリスクの低減や管理業務の負荷低減，利便性を向上させることができる。

*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

不当競争防止法の改定や，個人情報保護法，日本版SOX法の施行によって，企業は，営業機密，個人情報，財務情報の漏洩(ろうえい)による損害賠償や社会的な責任を問われるようになった。また，サイバー攻撃の激化によって情報漏洩のリスクが高まっている。そこで，企業は情報を保護するため，セキュリティポリシーの強化・徹底，建物への不正侵入を防止する物理セキュリティ対策と情報システムへのネットワーク経由の不正侵入を防止する情報セキュリティの対策を強化している。

物理セキュリティの主要な対策である入退管理システムについては，機器が拠点ごとに導入されてきた経緯もあり，そのID管理も拠点ごとに行われているケースが多い。組織変更や人事異動が発生した場合に，それぞれの入退管理システムに対するメンテナンスを行う必要があり，ビル管理会社や企業の管理部門の管理負荷が増大するとともに，変更漏れによるセキュリティリスクも拡大してきている。

クラウドID管理サービス“DIASMILE”は，ビル管理会社などが運用していたID管理を利用者(テナント)が直接行えるようにしてビルの専有部と共用部の一元管理を可能にすると共に，企業が各拠点に分散していたID管理を一元的に行うことを可能にする。

本稿では，入退管理システムの課題，課題解決に必要な機能，及びそれらの機能を備えたDIASMILEについて述べる。

2. 入退管理システムの運用の現状と課題

従来の入退管理システムは，ビルごとで導入及び管理が行われてきた。そのため，施設管理部門や管理部門から委託を受けたビル管理会社が管理を担当していた。近年，通行権限の設定や通行履歴の閲覧等，利用者(テナント)自身による実施が利用者にとってのメリットとなるような運用は，利用者で実施できるようにすることで，ビル管理会社の運用負荷を軽減することが求められてきた。しかしながら，利用者自身が運用を行う場合は，利用者の情報をほかの利用者から秘匿するなどセキュリティの確保が課題となる。

一方，従来の入退管理システムは企業内ネットワークに接続されていないため，本社と複数の拠点(支店や工場等)を持つ企業では，それぞれの拠点の入退管理システムは，個別に通行権限が管理されていた。入退管理システムを拠点ごとに運用しているため，複数の拠点間で異動が発生した場合に，通行権限の設定変更の負荷が高く，設定ミスが発生する要因の一つとなる。また，複数の拠点の組織を兼務する人や複数の拠点の組織を横断するプロジェクトに属する人の通行権限の設定も各拠点で個別に行う必要があり，組織やプロジェクトの情報を活用した効率的で安全な通行権限設定も困難となる。企業で統一的なセキュリティポリシーを策定した場合でも，各拠点で個別に適用する必要があり，セキュリティポリシーが適切に拠点に適用されているかを確認する負荷も大きい。

次に，IDカードの運用・管理について考える。複数のテナントが入居するテナントビルでは，一般的にビルに導入されている入退管理システムはビル所有者が所有する。その場合，利用者はビル所有者から提供されたIDカードで入退管理システムを利用する。このような環境では，テナントビル内に支店などの拠点を持つ企業が社員証といった全社統一のIDカードをビルの入退管理システムで利用することができない。利用者は，社員証とビルの入退管理システム用のIDカードを管理する必要があり，IDカードの紛失といったセキュリティ事故の発生，事故発生時におけるIDカードの識別番号による個人の特定が困難といったセキュリティ上のリスクが存在している。また，異なる拠点に出張した場合，同じ会社にも関わらず，社員証で入館できず，利便性が損なわれる。

これまで述べたように，入退管理システムの現状の運用における課題は次の4点に集約される。

(1) ビル管理会社の入退管理システム設定作業の負荷軽減
(2) 複数のIDカード利用による利便性の欠如と紛失等によるセキュリティリスクの増大
(3) 拠点間を跨ぐ組織や異動及び出張における通行権限設定の運用負荷の増大
(4) 運用が各拠点単位で実施されていて，セキュリティポリシーの統一的な適用や適用の確認が困難なことによる，セキュリティリスクの増大

3. クラウドID管理に必要な機能

3.1 運用形態に対するニーズ

1章で述べた入退管理システムに対する課題を解決するためには，“テナント開放”“複数拠点の一元管理”といった運用形態に対するニーズを満たす必要がある。

(1) テナント開放

テナント開放とは，テナントビルのような入退管理システムの利用者(テナント)と所有者が異なる場合で，利用エリアの通行権限設定や利用カードの管理を利用者自身が行う運用形態である。これによって，**2章**で示した課題(1)，課題(2)に対応することが可能となる。

(2) 複数拠点の一元管理

複数拠点の一元管理とは，複数の拠点(支店や工場等)を利用する企業で，セキュリティ管理部門が策定したセキュリティポリシーに基づき，全ての拠点で設置されている入退管理システムの設定を行う運用形態である。これによって，課題(3)，課題(4)に対応することが可能となる。

3.2 機能要件

3.1節で述べたニーズを満たすために必要とされる機能について述べる。

3.2.1 テナント開放を実現するための機能

⑴ 管理権限付与

管理権限付与機能は，テナント開放の中核を成す。この機能によって，テナントビルに入居している各利用者(テナント)に対して，入退管理システムに対する管理者権限を与えることができる。管理者権限が与えられた利用者は，入退管理システムに対して通行権限設定や通行履歴の閲覧，利用するカード情報の登録が可能になる。このとき，利用者は社員証といった自社保有IDカードを登録でき，ビルから貸与されるカードや他拠点のカードとの2枚持ちから開放され，共通カードの利用が可能になる。この機能によって，入退管理システムへの登録作業の時間短縮やカードの1枚化による利便性の向上，又はカード紛失といったセキュリティ事故に対するリスク軽減が可能になる。

⑵ アクセス制限

アクセス制限機能は，任意の利用者(テナント)が管理する情報に関して，ほかの利用者からのアクセスに対する保護・秘匿を行う。この機能によって，それぞれの管理情報に対する利用者間の相互アクセスを禁止し，不正な通行権限設定による侵入や機密情報の漏洩といったセキュリティ事故を防ぐことができる。

3.2.2 複数拠点の一元管理を実現するための機能

⑴ 役割による通行権限設定

通行権限設定機能は，組織，資格といったある役割によって指定されたグループに対して通行権限設定を行う。企業内で機密情報に対するアクセス制御を実施する場合には，組織や資格等の役割によってアクセス制御を行う方が，個人単位でアクセス制御を行うより，セキュリティポリシーを適切に反映でき，異動に伴う設定変更も少なくすることができる。入退管理システムにおける通行権限設定も同様であり，機密情報を管理する部屋に入室するための通行権限は，組織や資格等の役割で設計・管理・運用する必要がある。この機能によって，個人単位での入退管理システムの通行権限の設定が不要となり，設定ミスの防止や運用負荷の軽減ができる。

⑵ 設定の自動化

設定自動化機能は，通行権限の設定変更や入退管理システムへの反映を自動的に行う。⑴の“役割による通行権限設定”で，組織構成の変更によって組織の役割が変わった場合や組織に所属する社員に異動や変更があった場合，入退管理システムに対して通行権限の変更情報を自動反映する。この機能によって，従来手動で変更していた通行権限設定が自動的に行われるため，設定ミスの防止や運用負荷の軽減が実現される。

4. クラウドID管理サービスDIASMILE

3章に示した課題を解決するための機能を備えたシステムがクラウドID管理サービスDIASMILEである。

4.1 DIASMILEとは

DIASMILEは，テナントビルに入居する利用者(テナント)自らが入退管理システムの通行権限管理，通行履歴管理，カード管理等運用を行える機能を提供するサービスである。利用者は，クラウド上に設置されたID管理システムに対してセキュリティを確保したネットワークに接続された端末からアクセスして管理業務を行うことができる。サービスヘルプデスクを用意し，サービス利用者に対して利用方法等に関するサポートも行う。**図1**にDIASMILEのイメージを示す。

4.2 システム構成

DIASMILEのシステム構成を**図2**に示す。

サービスの利用者(テナント)は，インターネットに接続された自席の端末から，サービスにアクセスが可能である。一方，入退管理システムは，このサービスを提供するサーバとセキュリティを確保したネットワークで接続されており，入退室の権限情報や通行履歴情報を送受信する。現状，このサービスでは，連携する入退管理システムとして，三菱統合ビルセキュリティシステム“MELSAFETY-G”を対象としているが，今後対象範囲を拡大していく。

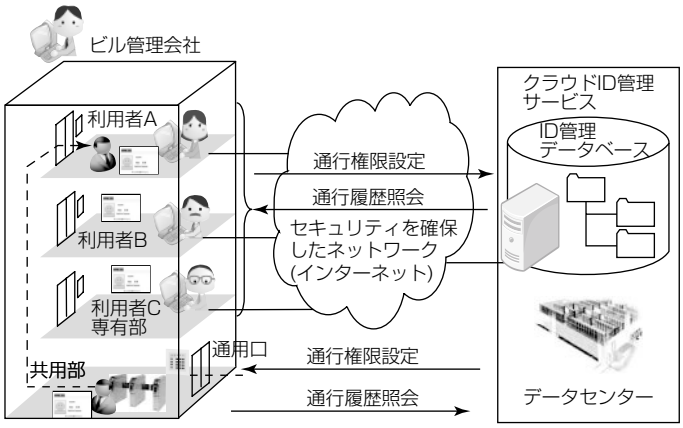


図1．DIASMILEのイメージ

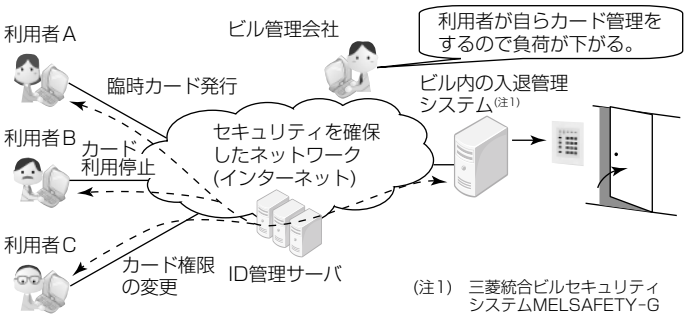


図2．DIASMILEのシステム構成

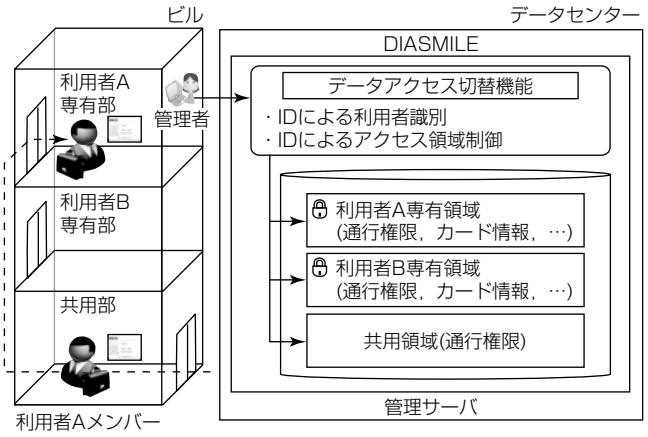


図 3．管理権限の付与及びアクセス制御機能

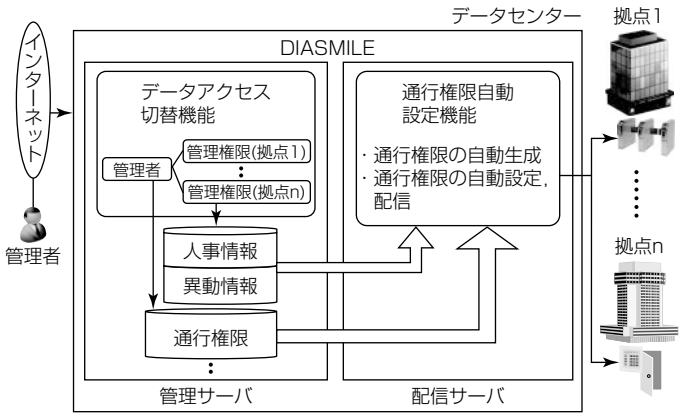


図 4．通行権限管理の集約と自動化の機能

4.3 特　　長

DIASMILEの特長は，次のとおりである。

⑴ 利用者への入退管理システム操作の開放

DIASMILEは，利用者への入退管理システム操作の開放に当たって，管理権限の付与とアクセス制御を行う機能を実現した。この機能は，IDによって利用者を識別し，システム上でアクセス可能なデータ領域を制御する。システムで扱うデータを格納するデータ領域には，共用領域と専有領域があり，前者では共用部の通行権限を管理し，後者では利用者ごとの人事情報やカード情報，専有部の通行権限を管理する。また専有領域では，共用部の通行権限と人事情報との関連付け情報も管理しており，この関連付け情報によって，共用部の通行権限を参照可能としている。

図 3 に，管理権限の付与及びアクセス制御機能について示す。

⑵ 役割による通行権限の設定

役割に対する通行権限設定を行うため，ロールによる通行権限の設定機能を実装した。ロールとは組織やプロジェクト，資格といったある役割で指定されるグループを指す。これによって，従来は個人ごとに行っていた通行権限設定を組織などに対して設定することが可能となるため，設定作業や通行権限の棚卸し作業の省力化ができるとともに，設定ミスや設定漏れを解消することができる。また，通行権限の設定は従来と同様に個人に割り当てることも可能であり，組織と個人を混在して割り当てることもできるため，柔軟な通行権限の設定ができる。例えば情報システムエリアについては，情報システム課に所属しているメンバーと，各部門のOA管理者を入室可能にさせるといった設定ができる。

⑶ 設定と配信の自動化

DIASMILEは，データセンタ上の管理サーバに，異動情報を含む人事情報，通行権限の情報を集約，一元管理している。管理者がインターネットに接続された自席の端末から異動情報などを入力すると，組織などに割り当てられた通行権限設定を自動的に個人単位の設定に分解し，各拠点の入退管理システムへ自動的に反映する。これによって，企業では，設定のミスや漏れが解消され，手作業による負荷削減，システム管理コストの削減が可能となるとともに，セキュリティポリシーの統一が可能となる。**図 4** に通行権限管理の集約と自動化，及びそれらを実現可能とする機能について示す。

5. む　す　び

DIASMILEのベースとなる統合ID管理ソリューション“iDcenter”は，三菱電機グループ11万人が利用する情報システム基盤に導入され，三菱電機グループ内の様々な情報システムに対する統合ID管理としての機能を提供してきた。その大規模システムでの実績を踏まえて，DIASMILEでは，各利用者が安全に，それぞれが独自に利用できる基盤の構築を可能としたサービス提供を実現した。その結果，企業における生産拠点や営業拠点など，離れた拠点間の物理セキュリティシステムを一元的に管理するニーズへの対応が可能となった。今後は，各拠点にある様々な物理セキュリティ機器と接続可能とするようにオプションを拡大していくことで，利便性，安全性の向上を図っていく。

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）

⑵ 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）