特集論文

物理セキュリティにおける管理強化と効率化

清原　聡*

Enhanced Management and Efficiency in Physical Security Control

Satoshi Kiyohara

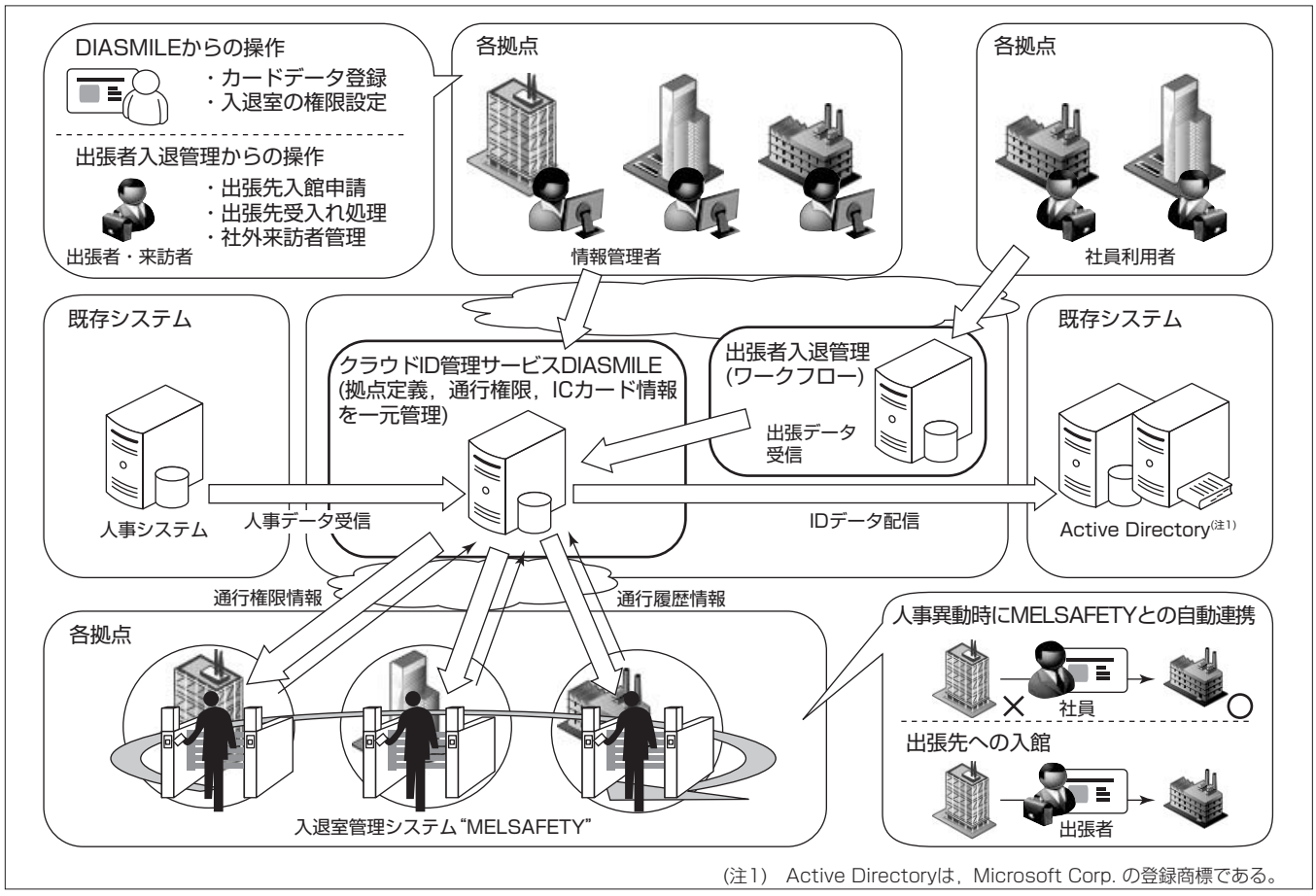
要　旨

物理セキュリティ強化を目的とした三菱電機のセキュリティ施策として，2009年度までに当社各拠点に統一仕様の社員証(ICカード)を利用した入退室管理システム“MELSAFETY”を導入した[1]。しかし，人事異動や出張者受入れに伴う入退室を管理する作業負担は増加し，作業ミスによるセキュリティリスクが新たな課題であった。

これに対して，クラウドID管理サービス“DIASMILE”を導入し，当社国内拠点の拠点定義情報，ICカード情報，入退室の権限情報(通行権限)，出張者情報を集中管理する基盤を確立した[2]。これに社内情報システム部門のノウハウを活用した2つの機能(①人事異動に伴う通行権限自動更新機能，②出張者本人の社員証による当社国内拠点相互入館機能)を実現し，更なるセキュリティガバナンスの強化と，業務効率の向上を実現した。

セキュリティシステムを運用する管理部門では，社員の人事異動に伴う通行権限の更新作業が原則不要となり，人手の作業による入力ミスなどのリスクが解消される。出張者は，事前登録をしておくことで，本人の社員証で当社国内拠点での通行ができ，利便性が向上する。

今回実現した2つの機能は，当社の企業向けのSI(System Integration)事業で社内展開の実績を踏まえて製品化する。製品仕様に社内情報システム部門のノウハウを組み込むことの有効性を確認した。



クラウドID管理サービスDIASMILEによる当社物理セキュリティ施策の実現構成

各拠点で独立運用していたMELSAFETYを，プライベートクラウド環境に配置したDIASMILEに接続することで，人事システムからの人事異動情報や出張者情報に基づく通行権限情報の配信，各拠点の通行履歴情報の一元管理が可能となった。現在，全国の拠点に順次展開を進めている。

*IT戦略室

1. まえがき

2009年度までに実施した当社の物理セキュリティ施策では，物理セキュリティ上の安全面，管理面を考慮して，氏名，社員番号，ICカード番号等のID情報や，通行権限(通行可能な扉，時間帯を定義したもの)などの物理セキュリティ情報を，各拠点の総務部門で管理する運用とした。しかし，入退室管理が多様化することで，各拠点総務部門の管理運用作業の負担は増大し，また，作業ミス，連絡ミスによるセキュリティリスクの増加が新たな課題になってきた。

これらの課題を解決するため，複数拠点の入退室権限情報，異動発令情報など関連する情報を集中管理する基盤を構築した。構築に当たっては，社内情報システム部門が持つ社内運用特性を熟知した情報活用技術や，ワークフローシステム等の社内既存資産を活用し，設計・運用品質の向上とコスト抑制を行った。

本稿では，今回実現した①人事異動に伴う通行権限自動更新機能と，②出張者本人の社員証による当社国内拠点相互入館機能の2つの機能とその考慮点について述べる。

2. 現状の課題と対応

2.1 セキュリティリスクの課題

国内拠点の通行権限の新規登録・削除件数は年間約30,000件であるが，管理を担当する各拠点の総務担当が専用端末を利用して手作業で通行権限設定の変更操作を行うため，人事異動発令情報の連絡漏れ，作業漏れ，作業ミスによって，本来入室が禁止されている人が入室できる等のセキュリティリスクが内在していた。

2.2 作業生産性の課題

社員の採用・退職に伴う社員証の発行・回収や，入退室情報の登録・更新への対応のほか，他拠点からの兼務者・長期出張者の受入れ，拠点間異動者の引継ぎ期間対応などで発行するゲストカード及び入構証の管理やグループ企業社員・構内外注への個別の管理など，業務は多様化してきた。これに伴い，適切に通行権限を見直してセキュリティを維持する総務担当者の負担は増加していた。

また，年間の社員出張者は延べ358,000人であり，各拠点では，出張者は受付で社員証を提示し，その場で入構証の発行を受ける運用であった。各拠点の受付では，カード発行待ちや，社外の来客者の入館に支障を来すといった課題も確認されてきた。

2.3 課題への対応

これに対して，人事異動に伴う通行権限設定業務を自動化し，通行権限設定ミスを排除することでセキュリティガバナンスを向上させる。また，国内拠点を対象とした出張者の相互入館を可能にすることで作業効率を向上させる。

3. 実現する機能

3.1 人事異動に伴う通行権限自動更新機能

社員の採用，退職，拠点内異動，拠点間異動，出向・出向復帰，休職・休職復帰などの異動情報を入退室管理拠点に対応して独自に識別し，人事異動に伴う通行権限の変更を自動的に行い，総務部門が担当している権限変更作業を不要とする。また，異動者に対する受付窓口での臨時の入構証の発行を不要とする。通行権限には有効期限を設け，異動元の通行は，発令日当日から通行不可とする。

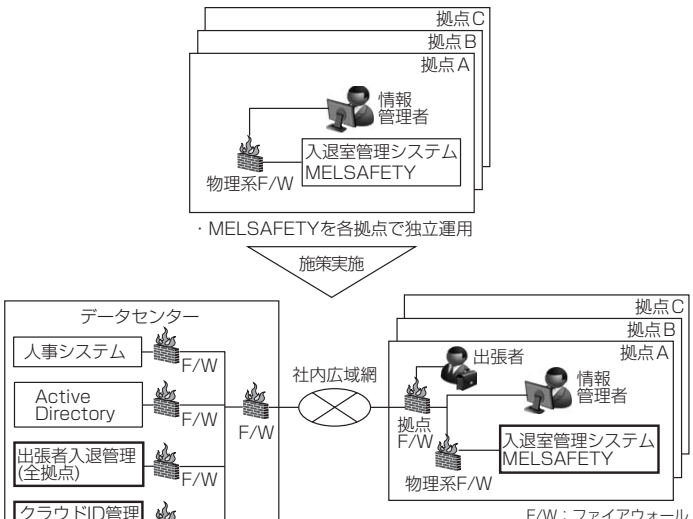
3.2 当社国内拠点の相互入館機能

事前に出張申請をしていれば，出張者が本人の社員証で出張先の居室内まで通行可能とする。申請登録は，出張者側・受入れ側の双方から可能とする。承認は受入れ側の上長が実施し，出張の目的と通行権限付与の期間や範囲の妥当性を確認する。

4. システム構成

4.1 システムの構成

各拠点で独立運用していたMELSAFETYを，プライベートクラウド環境に配置したDIASMILEに社内広域網を介して接続することで，セキュリティ・ゲートや物理エリア(部屋)の通行権限情報を集中管理に切換えた。そして，人事異動情報，IDカード情報，出張者情報などの社内情報と連携することで**3章**で述べた2つの機能を実現した。情報管理を担当する総務部門担当者は，本人の端末からDIASMILEへアクセスして業務を行う。社内広域網との接続はファイアウォールを用いており，社内広域網外からのアクセスを拒絶する(**図1**)。



・DIASMILEをプライベートクラウド環境に配置して集中管理
・社内広域網を介し，DIASMILEとMELSAFETY及び情報系システム(人事システム，出張者入退管理システム)を連携

図1．物理セキュリティ施策実施前後のシステム構成比較

4.2　サブシステム構成

サブシステムの機能構成と今回実現した2つの機能を**図2**に示す。

4.2.1　入退室管理システムMELSAFETY

入退室管理システムは，各拠点に導入した入退室管理装置で構成した物理セキュリティ管理の中核となるシステムである。DIASMILEから配信される社員情報と通行権限情報を使用する。

4.2.2　クラウドID管理サービスDIASMILE

DIASMILEは，社員情報・ICカード情報・通行権限情報を集中管理する。この製品が持つ人事情報連携機能，出張情報連携機能を活用し，人事異動に伴う通行権限自動更新，当社国内拠点相互入館を実現する。ICカード情報は，拠点の情報管理者がこのサブシステムに直接登録し，結果をICカード情報配信機能によってActive Directoryへ配信する。

社員情報，ICカード情報，通行権限情報とそれらを組み合わせた情報を有効期間付きで管理し，通行権限が有効期間に入った時点又は有効期間が切れた時点で，その情報を対応する拠点の入退室管理システムへ配信する。

4.2.3　社員情報変換システム

社員情報は，人事システムと連携してDIASMILEへ取り込む。DIASMILEデータベースは，拠点ごとに情報を分割管理するため，人事情報を拠点ごとに分割する社員情報変換システムをDIASMILEと人事システムとの間を取り持つブリッジシステムとして設けた。

4.2.4　出張者入退管理システム

当社国内拠点を対象に，出張者の自拠点以外への通行を申請するワークフローシステムである。出張者又は出張受入れ者から通行申請を受け付け，出張受入れ部門長の承認を得て通行を許可する。その結果をDIASMILEへ配信する。

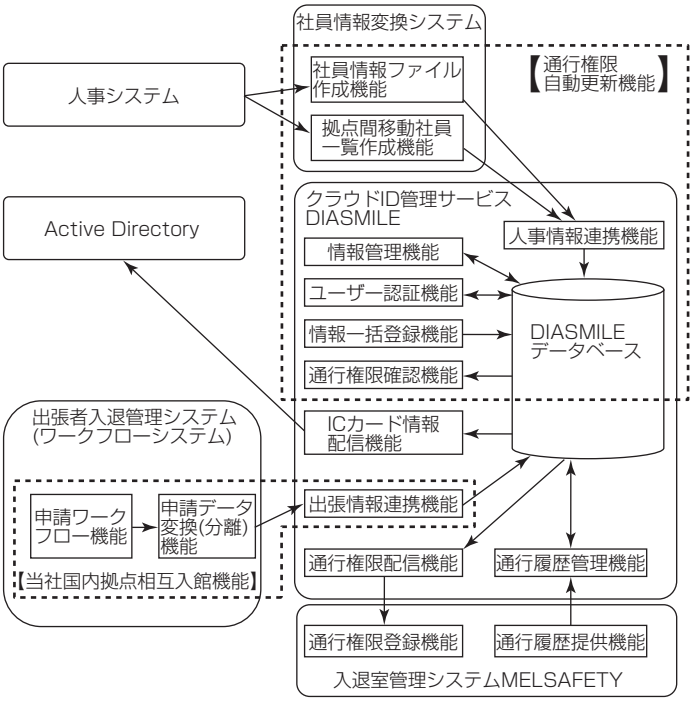


図2．サブシステム構成

5.　導入機能の考慮点

5.1　人事異動に伴う通行権限自動更新機能の考慮点

5.1.1　人事情報取得元と自動化対象範囲の決定

人事異動を正確に把握し，発令日前に権限設定作業を完了させるため，人事情報を人事システムから直接連携する。一方，構内外注などの社員外従業員は自動更新の対象外となる。社員外従業員は，拠点の裁量で一人ずつ管理画面から更新を行う。このため，更新作業の生産性を考慮し，拠点で持つ個人情報を一括登録する外部ファイル取り込み機能を社員外従業員専用機能として実装した。

5.1.2　通行権限割当てモデル

通常，同一組織の社員は同じ通行権限を持つこと，組織と物理エリア(部屋)はおおむね対応関係が整理されていることを考慮し，基本的には組織に通行権限を設定することにした。組織改正があった場合は，管理画面から総務担当者が組織に権限を設定するため，下位組織は上位組織の権限を継承するモデルとして，拠点内の権限設定の作業負担を抑えた。

一方，サーバルームなどセキュリティレベルが高いエリアは，権限を付与する個人を特定する必要がある。これは人事情報からは把握できないため，個人に通行権限を設定する。

設定する通行権限には，有効期間を設置して予約入力，期限到来時の削除を可能とし，入力忘れ防止に対応した。

5.1.3　通行権限包含確認機能

新棟設立など拠点のレイアウト変更に伴って組織に割り当てた通行権限を見直す際，通行権限割当てモデルに則して下位組織に割り当てる権限は上位の組織が通行可能なエリアに包含されている必要があるため，影響範囲を把握し網羅的に変更を行えるように補助機能を実装した。通行権限を指定し，その権限が割り当てられた組織を一覧にして外部ファイルに出力する。

また，入退室管理システムに配信する前に総務担当者が個人に割り当てた権限を確認できるよう，管理画面から組織を指定し，その組織下の社員の通行権限を一覧にして外部ファイルに出力する機能を実装した。入退室管理システムでは，一人に割り当てる通行権限数に上限を設けているため，このシステムで上限を超える割当てがあった場合に，どの権限が配信されるかを事前に確認できる。また，社員外従業員に割り当てた権限の棚卸しにも活用する。

5.1.4　業務引継ぎ期間のルール制定

他拠点へ異動になった場合に，業務連続性確保の観点から，業務引継ぎ期間(異動発令日から着任日までの期間)へ

の対応を考慮し，異動元の通行を可能とする。就業規則に則し，業務引継ぎ期間を設定して運用を統制した。業務引継ぎ期間経過後に通行を不可とする。

5.1.5 定期入場者の社員証ID登録

他拠点からの兼務者や長期出張者などの定期入場者は，人事情報では勤務拠点を把握できない。このため，社員外従業員と同様に拠点の管理画面から登録するが，本人の社員証で登録できるようにした。これによって，社員一人に発行する通行証は社員証１枚だけとする。社員は長期出張先でも社員証で通行するので，他拠点の通行記録も本人の通行記録として蓄積される。

5.2 当社国内拠点の相互入館機能の考慮点

5.2.1 申請画面の利便性

大量の通行権限情報から出張者が入場可能な通行権限だけを抽出する機能を実装し，申請者の利便性を考慮した。拠点の従業員用の通行権限は除外し，出張者用の通行権限だけを選択画面に表示する。

MELSAFETYで作成してDIASMILEデータベースに収集された通行権限を，DIASMILEが提供するAPI（Application Programming Interface）を介して取得する。

5.2.2 申請データ変換(分離)機能

物理セキュリティを担保するため，DIASMILE及びMELSAFETYでは，予約登録（未来日の登録）の制限や，１拠点に対して付与可能な通行権限数の制限を設けている。これに対応するため，申請情報を正規化し，出張者，出張日，通行権限に分割する管理機能を実装した。出張者を拠点ごとに管理し，出張期間は複数日にわたる申請を日単位に分割管理し，申請された権限数が上限を超えた場合にエラーを返し，システム運営管理部門が登録状況を一元管理できる機能とした。

5.2.3 運用を考慮した拠点管理コードの選定

管理者及び管理ルールが明確な人事システムの拠点管理コードをこのシステムでの基本コードとした。物理的な入退室管理での拠点管理コードとは一致していないため，入退室管理単位を整理し，拠点情報の対比表を実装した。職制改正等による対比の乖離（かいり）を回避するため，変更管理を総務部門で行う運用とした。

6. 導 入 効 果

このシステムは，2014年11月からモデル拠点の運用を開始した。導入後の効果を，2015年4月の人事異動対応後にモデル拠点へ聞き取り調査を実施した結果，“権限設定変更の手間が削減された”“異動者の入館手続きでは異動者，受入れ側の双方に効果があった”との評価を得た。出張申請では，申請ログから，月当たりの平均出張者が過去実績比97%に達しており，利用は定着していると判断した。

今回の社内展開で実現した２つの機能は，当社の企業向けのSI事業で社内展開の実績を踏まえて製品化する。製品仕様に社内情報システム部門のノウハウを組み込むことの有効性を確認できた。

7. む す び

DIASMILEは，企業内システムと連携し，物理セキュリティの確保と管理コスト削減を実現する。企業内システムとの連携では，企業内情報システム部門が持つ業務を止めないノウハウが必要不可欠であり，今回整理した考慮点は，今後のSI事業展開にも活用できる。

また，MELSAFETYに蓄積される通行履歴や，情報連携エラーログを集中管理する仕組みを確立した。DIASMILEのクラウド型サービスの展開で，収集した情報を活用した保守・管理サービス事業のソリューション検証モデルとして役立てたい。

参 考 文 献

(1) 奥西幸喜，ほか：出張者用事前カード登録システムと入退室管理システムの連携，三菱電機技報，**83**，No. 9，555～558（2009）
(2) 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）