ビルネットワークにおけるセキュリティ連携システムの開発(2)
－物理・情報連携システムの構築－

原田 篤史†　近藤 誠一†　大沼 聡久†　三浦 健次郎†　金子 洋介†
三菱電機株式会社 情報技術総合研究所†

1. 物理・情報連携システムの必要性

入退室管理をはじめとする物理セキュリティシステムと，計算機システム上の業務データの保護を目的とする情報セキュリティシステムは，それぞれ個別に管理されているのが通例である．しかし，近年では組織内部者による情報漏洩事件が頻発するなど，物理・情報システムにおいて個別に対応することは現実的では無くなってきた．企業や組織に求められる内部統制の面からも，物理・情報システムを相互に結びつけて体系的に管理したいという要求が高まっている．

しかし，物理・情報システムはこれまで管理の独立性が高く，各システムで個別の ID 体系や，イベント形式，ログ形式が使用されていることで，統合が難しかった．そこで著者らは，ビルネットワークにおけるセキュリティ連携システムを構築するプラットフォーム[1]上に，物理・情報システムの統合 ID 管理とログ監査を実現する連携システムを開発した．

本稿では上記の一例として，入退室管理・出張申請ワークフローの連携について述べる．

2. 入退室管理とワークフロー・ID 管理の連携

人事系情報システムと入退室管理システムが連携していない環境では，出張来客時など入退室管理システムに一時的なアカウントが必要な場合は，事前に登録された臨時の入退場 ID カードを貸与のうえ記帳管理することが一般的である．しかしこの方法では，出張者は携帯している自拠点用の ID カードを利用することができず，利便性が低い．また，臨時カードの準備・貸与に伴う手続きの管理コストの問題と，人為的ミスの危険がある．ログ管理の面では，出張先では別 ID で入退室を行うため，自拠点 ID と整合がとれず，拠点間のログ監査を困難にしている．

そこで本開発では，ワークフローによる出張申請から，入退室管理システムへの通行権限設定まで，統一した ID で管理し，拠点をまたぐログ監査を容易にする連携システムを開発した．

2.1. システム構成

図 1に，本システムのシステム構成を示す．

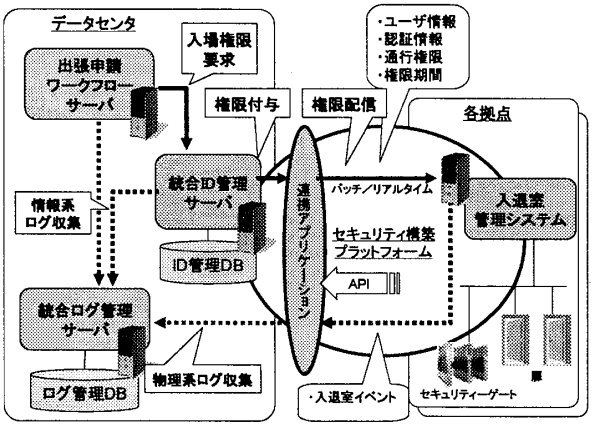

図 1　システム構成

(1)出張申請ワークフローサーバ

社員の出張申請を受付け，規定の承認ルートに沿った Web ベースの稟議システムを提供する．最終承認後，統合 ID 管理サーバに，出張先への入場権限（いつ，誰が，どこへ）を要求する．

(2)統合 ID 管理サーバ

人事情報をマスタとして，社員の ID 情報，すなわち個人情報・認証情報・権限情報を，物理・情報システムを含めて一元管理する．ワークフローからの権限要求の内容や対象者の役職をもとに，規定のルールに従って通行権限と権限期間を確定し，パスワード・IC カード情報・指紋情報などの認証情報とともに対象拠点の入退室管理システムに配信する．

(3)統合ログ管理サーバ

各拠点の物理・情報システムで発生するログ情報を収集管理する．統合 ID 管理サーバによって管理される ID で統一されたログ情報を集中管理することで，物理・情報システムを含めた全社的なログ監査を容易にする．

(4)セキュリティ構築プラットフォーム

物理・情報システムに対して，統一したインターフェース(API)を提供する構築基盤であり，入退室管理システムの機種やログ形式の差を吸収し，システム間の連携を容易にする．

"The Integrated Security System on Building Network (2)—Physical - Information Security System"
Atsushi HARADA†, Seiichi KONDO†, Akihisa OONUMA†, Kenjiro MIURA† and Yosuke KANEKO†
†Mitsubishi Electric Corporation

(5)連携アプリケーション

セキュリティ構築プラットフォームが提供する入退室管理 API を用いて，対象拠点の入退室管理システムに対して，認証情報・権限情報の事前配信および事後削除と，入退室イベントの収集の処理を行う．

(6) 入退室管理システム

各拠点において，社員の入退室を，IC カード等規定の認証方法によって制御する．

2.2. 統合 ID 管理サーバによる権限管理

統合 ID 管理サーバにおける権限管理について述べる．

(1)運用ルールに基づく権限付与

統合 ID 管理サーバは，ロールベースアクセス制御方式[2]に基づいて社員の権限管理を行う．所属・役職などの属性情報を入力とし，会社規則等のポリシーで定められたルールに従って，社員に割り当てるロール（役割）を決定し，適切なアクセス権限を付与する機能を持つ．本システムにおいては，統合 ID 管理サーバは所属や役職などの静的な属性から割り当てられる本務としての権限に加えて，「出張」に相当する動的な属性をもとに他拠点への一時的な入退室権限を管理する．ワークフローの申請内容である出張者・行先・出張期間等の情報をもとに，対象エリアへのアクセス権限が割り当てられる．

(2)権限のライフサイクル管理

出張などで権限が変更される場合，変更以前の権限の内容を履歴として保存し，新たに変更後の権限を有効期限つきで追加するという処理を行う．これにより，有効期限に応じて権限情報を事前配信・事後削除することや，過去の特定時点に遡って，所属拠点および出張先拠点における権限を監査することが可能である．

2.3. 利用イメージ

本システムの利用イメージを，図 2に示す．

1. 拠点 A に所属する社員 U が，出張申請ワークフローを用いて拠点 B への出張を申請する（図中①）．その後，社員 U の所属上長，拠点 B の受入責任者ら規定の承認ルートにおいて社員 U の出張が承認される．
2. 社員 U は出張開始日に，出張先の拠点 B へ移動する（図中②）．社員 U の社員証カード情報と通行権限は，当日早朝に事前配信されている．
3. 社員 U が拠点 B に到着すると，社員 U は自身の社員証を入場 ID カードとして利用して，目的の部屋まで入室できる（図中③）．
4. 出張終了日時を過ぎると，社員 U の認証情報と通行権限は拠点 B から自動削除される．

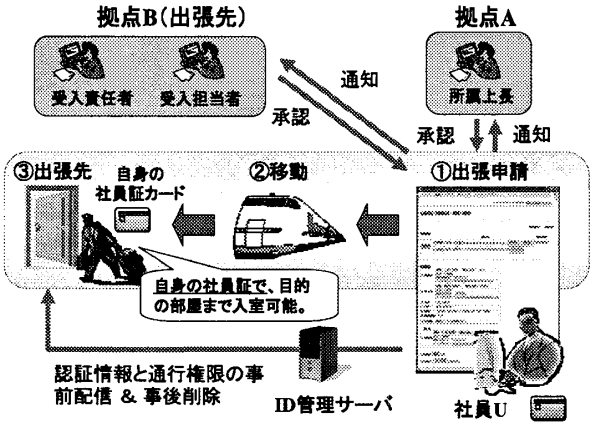

図 2 利用イメージ

3. 考察

本システムにより，以下の効果が得られる．

(1)利用者の利便性

利用者（一般社員）の観点からは，出張先拠点における臨時カードの受け取り，携帯，返却といった一連の手続きを行う必要が無くなり，利便性が向上する．

(2)来客管理の容易化と，手続きの迅速化

本システムを利用することにより，臨時カードの発行・貸与の手続きを減少させ，来客管理の容易化と処理手続きの迅速化が可能である．

(3)全社的なログ監査

所属拠点だけでなく，出張先拠点における入退室履歴も統一した ID で管理できるため，全社的なログ監査が可能である．ワークフロー申請・承認，ある時点の権限情報，出張先での実際の入退室まで，一連の行動と権限を紐づけて参照可能であり，厳密な監査を実施できる．

4. まとめと今後

物理・情報セキュリティ連携システム開発の一例として，入退室管理と出張申請ワークフローシステムの連携について述べた．現在，本システムを某所に適用し，1000 人規模の 2 拠点間において運用を開始した段階であり，今後，拠点数を増やしてゆき，3節で記述した効果についてサーバ負荷・性能等を含めた評価を進める．

参考文献

[1] 三浦健次郎 他：ビルネットワークにおけるセキュリティ連携システムの開発(1) －セキュリティ構築プラットフォームの開発－，第 70 回情報処理学会全国大会講演論文集（予定），2008 年 3 月．

[2] D.F. FERRAIOLO et al, NIST Standard for Role-Based Access Control, ACM Transactions on Information and System Security, Vol. 4, No. 3, Pages 224-274, August 2001.