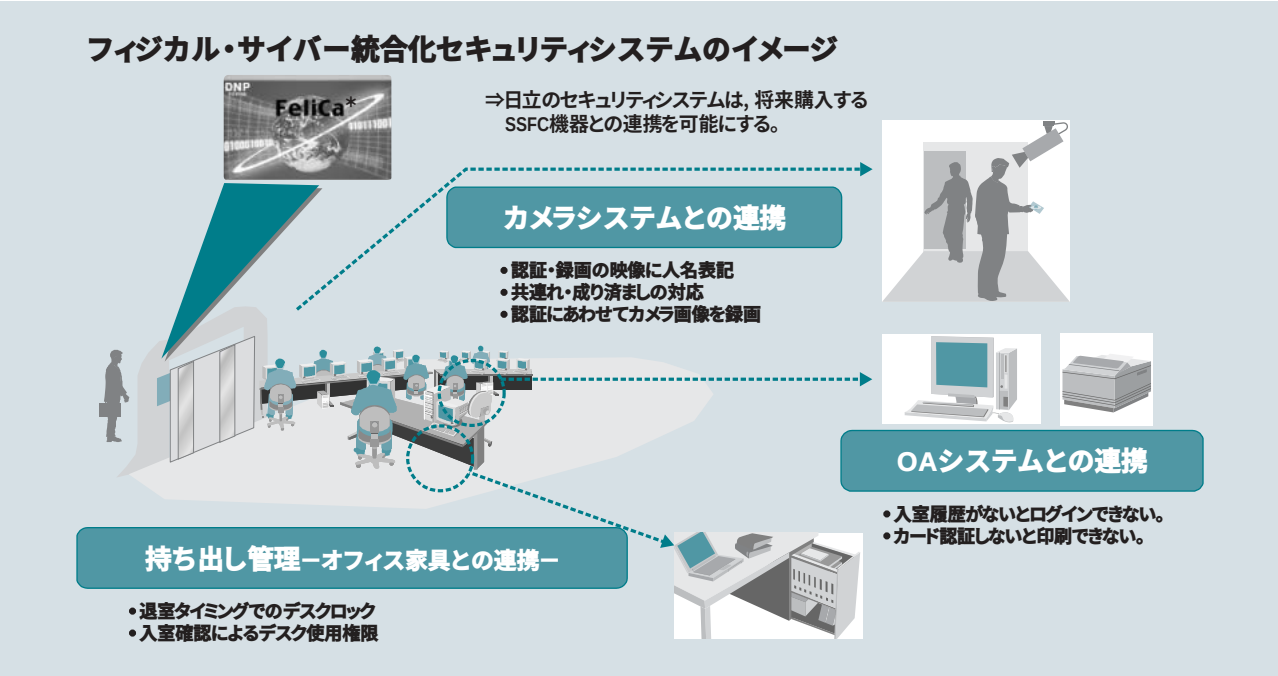
ビルセキュリティの動向とJ-SOX法への対応

Trend of Building Security and Correspondence to J-SOX Act

萩谷 茂 Shigeru Hagiya
澤村 伸一 Shinichi Sawamura
木村 正彦 Masahiko Kimura
正嶋 博 Hiroshi Shojima
甲斐 賢 Satoshi Kai



注:略語説明ほか SSFC(Shared Security Formats Cooperation)，OA(Office Automation)
*FeliCaは，ソニー株式会社の登録商標である。

図1 フィジカル・サイバー統合化セキュリティシステム
入退出管理システムとオフィス機器，カメラが1枚のカードによってシステム連携することで，オフィスのセキュリティ強化とユーザビリティの実現を図っている。

1. はじめに

オフィスの形態により，導入するセキュリティシステムの形は異なってしかるべきである。小規模テナントとしてフロアの一部分にオフィスを構えるのであれば，最小投資で導入し，運用も保守もアウトソーシングできる「インターネット型入退出管理システム」が適している。一方で，大型のシステムを望む大規模のオフィスにおいては，J-SOX法(Japanese Sarbanes-Oxley Act:日本版企業改革法)，内部統制の対応が急務となっている。日本での特徴となっているIT統制の成熟を実現するためには，IT側のアクセス管理，ログ管理だけでなく，同時にフィジカル系の管理も重要となり，システムの統合化が望まれている。また，システムを継続運営する場面において，クリアすべき課題が新たに発生してきている。

ここでは，ビルセキュリティの動向と，J-SOX法，および日立のフィジカル・サイバー統合化セキュリティシステムについて述べる(図1参照)。

2. オフィスセキュリティのニーズと対応

オフィスにおけるセキュリティシステムのニーズは多様化してきている。企業は今，J-SOX法対応で頭を痛め，小規模テナントとしてオフィスを構える企業も，何らかのセキュリティ対策を規模に応じた予算で構築する必要に迫られている。

日立では，小規模オフィス向けに，非接触ICカードでの入退出管理を1ドア単位で始められ，運用・管理は日立カスタマーセンターが代行する「インターネット型入退出管理システム」を提供している(図2参照)。小規模テナントでは，システムを導入してもカードの新規発行，登録データの更新，ログ管理，ドア立てつけなどの異常動作についての対応といった運

**オフィスにおけるセキュリティシステムは，メーカーを問わずに基本形ができるほど成熟してきた。
守るべき対象や規模に合わせたセキュリティ性，利便性，
そしてコストをバランスさせて，ユーザーがシステムを選択する時代になってきている。
日立グループは，小規模テナント向けから大規模システムまで，顧客ニーズに合わせたシステムを提供してきた。
一方，企業に課せられた大きな課題としてJ-SOX法への対応がある。
アクセス制御などを考えた場合，その監査用の証跡にはIT側とフィジカルセキュリティ側の統合されたログが有効となり，
したがってシステムも統合化された形が望まれるようになってきた。効率的で強固なセキュリティ性を確保し，
さらに運用者の負担を軽減することのできる，ログ解析とともに成長性のあるシステムに注目が集まっている。**

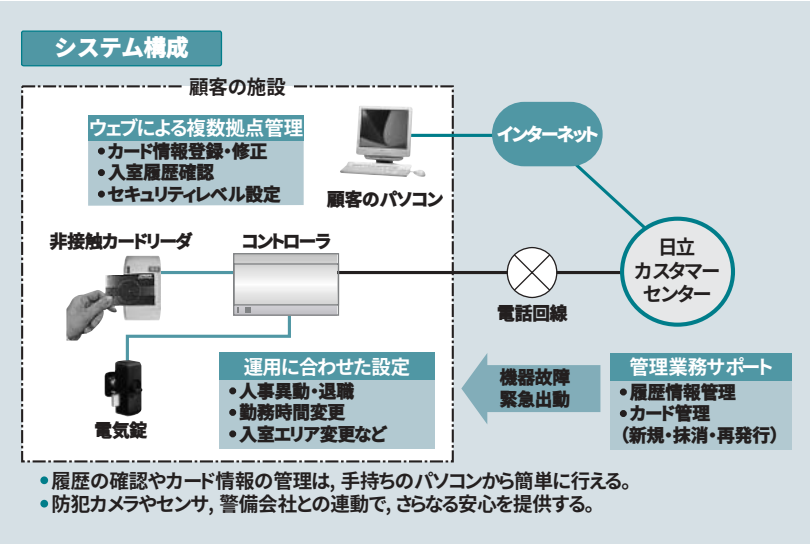


図2　インターネット型入退出管理システム
日立カスタマーセンターを利用したASP（Application Service Provider）方式の入退出管理システムの概要を示す。

用や，専門的な知識が必要なサーバ管理などに従事する担当者がいないという状況が考えられる。また，電気錠を設置するにも，ドアごとの交換と復元が必要となってしまうことで，予想外の出費が発生するなど，導入から維持管理までを含めた場合，思うほど簡単にはいかない。

そういったニーズに対応するのが，日立の「インターネット型入退出管理システム」である。まず，システムの運用・データ管理をカスタマーセンターが代行することで，専用サーバや管理者が不要となる。非接触ICカードによる入退出管理を行うことができ，入退出履歴の収集，検索をはじめ，時間単位でのセキュリティレベルの設定など，ユーザーの要求に合わせた管理が可能となり，遠隔監視ができるので異常時には全国の拠点から緊急で出動，対応する体制を備えている。

一方，企業の内部統制に関しては，アクセス制御，セキュリティ基盤をどのように作り上げるかがポイントになってくる。いつ，誰が，ほんとうにその操作をしたかという点において，フィジカルセキュリティシステムを連携していくことにより，大きなメリットが生まれる。その具体的な規格がSSFC（Shared Security Formats Cooperation，事務局：大日本印刷株式会社）である。SSFCについては後述する。

ITとの統合，そして監視画像デジタル化による大容量データのハンドリング，大規模デジタルネットワーク構築の必要性など，システムの拡大，統合に合わせて生まれてくる課題も煩雑である。現状の監視員，システム管理者の枠を超えたスキルが要求される部分を，システムがどのようにカバーしていくかが大きな課題となってきている。

3．J-SOX法対応のシステムとして，SSFCベースのサイバー・フィジカルセキュリティ紹介

3.1 J-SOX法対応におけるサイバー統制とフィジカル統制との位置づけ

J-SOX法対応では，財務報告に影響する業務フローの正常な履行を行うにあたり，各業務部門における手作業による統制（コントロール）の実装に加え，情報システム部門が行う自動化によるコントロールの実装を併用する（図3参照）。

業務フローを正しく遂行するには，紙文書・電子ファイルなど各種の媒体や，PCからの業務アプリケーションなどへ，権限を与えられた者が権限の範囲内でアクセスすることが重要となる。そのため，自動化によるコントロール要素としては，電子証明書を利用した業務アプリケーションのアクセスコントロールやファイルアクセスコントロール，エラーデータコントロールなど，主にサイバー系のコントロール環境が挙げられる。一方，手作業によるコントロール要素としては，書庫の施錠管理や入退室管理などによる入力原票のコントロール，プリンタ出力など紙文書のアクセスコントロールが挙げられ，主にフィジカル系のコントロール環境を整備する必要がある。

また，正しく業務フローが遂行されているか，内部統制のテスト・評価を実施するには，監査用に証跡を残すことが今後必須となる。現状のサイバー系ではPCログイン管理，データベースなどへのアクセス管理によるログ収集，フォレンジック

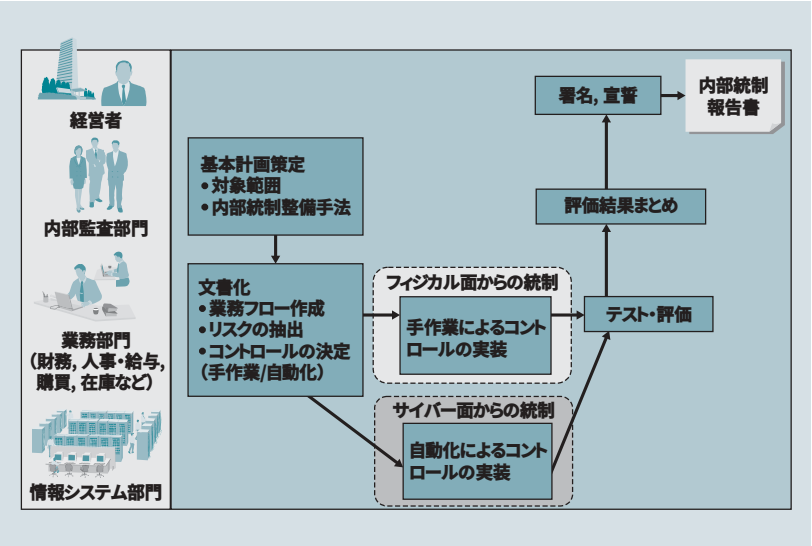


図3 J-SOX法対応の流れ
財務報告に影響する業務の内部統制を，手作業によるコントロールと自動化によるコントロールを併用して整備する。

ツールなどを利用し，フィジカル系では入退履歴，カメラを用いた画像ログを利用する。

3.2 SSFCベースのセキュアオフィスシステム

従来，入退室管理などのフィジカル系コントロールと，情報を管理するサイバー系のコントロールとは個別に検討・導入されることが多かった。しかし，業務に対するコントロールを確実に行い，テスト・評価を効率よく行うには，フィジカル系のコントロールとサイバー系のコントロールは整合が取れていることが望ましい。

これを実現するシステムとして，日立ではセキュアオフィスシステムを提案中である（図4参照）。入退室管理と情報アクセスの連携により，例えば，オフィスへの入室履歴がなければPCへのログインができないといった連携を実現する。また，書庫をはじめとするオフィスファニチャの施錠管理やプリンタへの出力制限と連携することにより，手作業によるコントロールのサポートを行うことが可能となる。

さらに，このシステムで業務を行った際のアクセスログ，入退履歴はサイバー・フィジカル両面からの正当性を持つことになり，客観性，証拠性を向上させることができる。

セキュアオフィスシステムの1実装方式として，SSFC規格を用いたシステム構成を図5に示す。各オフィス機器との連携を行うための通信規格はSSFCのフレームワークにのっとり，対応した機器のフィジカル系イベントを取得することで上位ACS（Access Control System）側から機器間連動制御を行う。

これにより，手作業によるコントロールと自動化コントロールの双方を統合的に扱うID/アクセス管理環境が構築できる。また，機器間連動として，例えばカメラへの録画指示を行うと，「書庫を開けた」，「プリンタへ出力」などのイベント情報とその時点での録画記録を業務実行履歴としてとることができる。

SSFC規格では各機器間の連携組み合わせ手法などは範囲外となっている。そのため，実際にシステムをオフィスへ導入する際には，どの部屋の入退情報がどの機器と連携するのか，どのフィジカルイベントをどのカメラで記録するのかといったSI（System Integration）が必要となる。また，最初からすべての機器を前提としてシステムを構築するのでは初期費用が大きくなるため，必要としている部分から導入できないかといった課題もある。

日立では，もともとインターネットを活用した「インターネット型入退出管理システム」で特定の個所，順次導入の形でシステムを構築しているが，今後はこうした既存SI体制にSSFCフレームワークを取り込む形でセキュアオフィスを実現していく。

上述の機器間連携の設定や機器の順次導入を含め，これからのJ-SOX法対応オフィスとして，業務フローの正常な履行をよりセキュアにサポートし，リスクマトリックスの分析，コントロールへと導き，改善していくスパイラルを描くサイバーシステムと連携するシステムをめざしている。

4. 新たな課題と解決するための技術

現在のシステムは何をやるにもカード提示（認証手続き）が

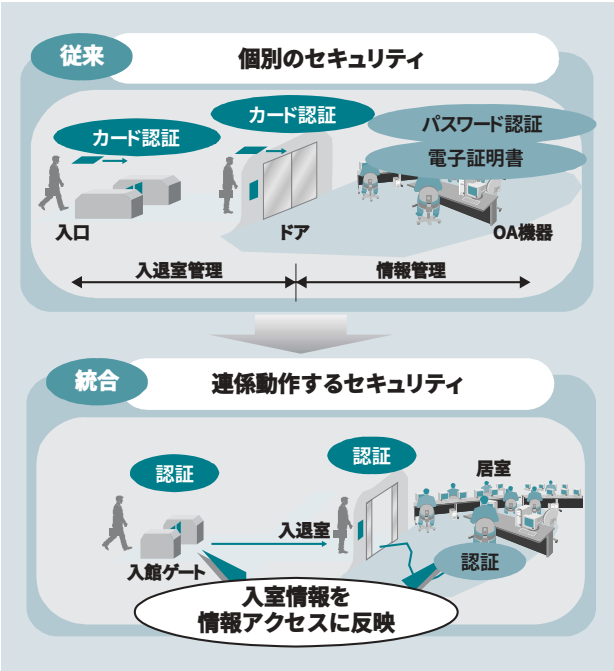
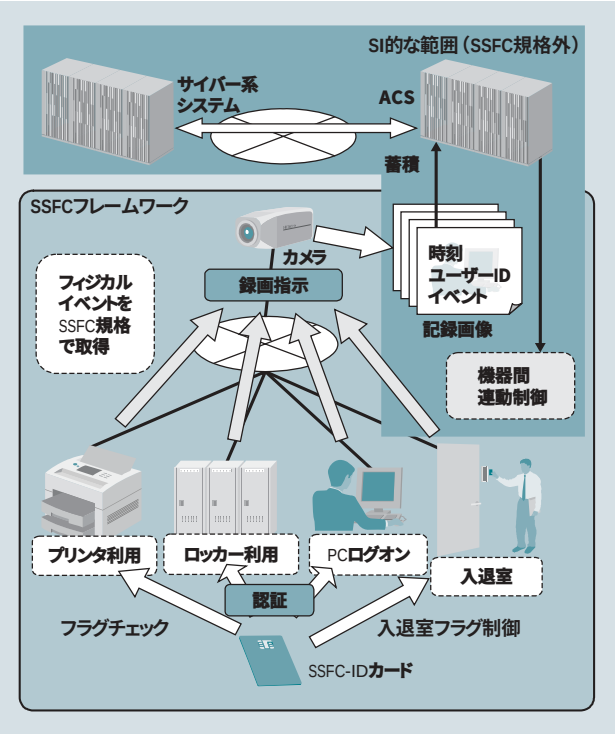


図4 セキュアオフィス
入退室管理と情報管理の連携により，不正アクセスを排除し，ログ機能の証拠性を向上する。



注：略語説明　SI（System Integration），ACS（Access Control System）

図5　SSFCベースフィジカル・サイバー統合セキュリティ
オフィス機器のフィジカルイベントを取得し，カメラ画像にひも付けしたログ情報を記録する。

必要であり，今後はセキュリティレベルを維持しつつ，手続きを軽量化する技術が必要である。

退室時はSSFCのデータリードのため，必ずカード提示が必須であり，これは現状では削減できない。書庫を含むすべての事務室内設備がネット接続されるのを待つしかない。

入室時のカード提示は，画像処理を用いたアンコンシャスセキュリティ技術の実現によって軽減される。これは，入館時・退室時の認証結果を継承し，顔認証とのマルチモーダル認証で入室時のカード提示削減をめざすものである。

また，社外からの人的な生産性妨害に対処するため，共連れ部外者の検知技術が必要となる。これは，通常のオフィスで起きる「善意」の共連れが，従来の認証数と物理的な人数との不一致による検知では，すべて異常と判定され実用的ではないため，「悪意」の共連れのみを検出することをめざすものである。

さらに，専門家がいなくても，別の担当者でも，所定の対応が可能な知的業務支援技術が必要となる。上記機能と連携し，少なくとも業務の中において，固定プロセスで対応可能なものについては，ルールのデータベース化と半自動化により，適切な指示を出力する。未経験者では対応不可能な手続きは，専門家に緊急メールが送信されることになる。このような大量異常発生時の早期正常復旧支援機能は，破滅的な事態が発生した場合の業務のトリアジ技術（現状リソースで最大効果を上げるための業務の選択）とも言える。企業運営続行を目的関数として，最短最小コストで対応すべき事象を選別し，その対応を指示しつつ，取り下げた事象へのわび状送信を行うが，現場の社員からすればサービスレベルの低下は免がれない。別の手段として，専門家集団へのアウトソーシングがある。この場合は，自社の業務プロセスに合った管理サービスのカスタマイズの柔軟性技術が委託の鍵となる。

5．おわりに

ここでは，ビルセキュリティの動向と，J-SOX法，日立のフィジカル・サイバー統合化セキュリティシステム，および新たな課題と実現するための技術について述べた。

今後も，日立は，システムおよびサービス提供者として，どのような立場を取るべきかを模索するとともに，社内で培った業務プロセスノウハウをコアに，顧客の業態にフィットさせてアウトソーシングを請ける「丸ごとバックオフィスビジネス」を，ここで述べた期待技術の構築を優位化要因として実現していきたいと考えている。

執筆者紹介

萩谷 茂
1979年日立製作所入社，都市開発システムグループ
ユビキタスソリューション部 所属
現在，セキュリティシステムの事業化に従事

正嶋 博
1981年日立製作所入社，日立研究所 情報制御第二研究部 所属
現在，都市開発ソリューション技術開発に従事
情報処理学会会員

澤村 伸一
1995年日立製作所入社，システム開発研究所 第六部 所属
現在，セキュアオフィス，フィジカル・サイバー統合型セキュリティシステムの研究開発に従事
情報処理学会会員

甲斐 賢
1998年日立製作所入社，システム開発研究所 第七部 所属
現在，デジタルフォレンジックの研究開発に従事
情報処理学会会員

木村 正彦
1984年株式会社日立ビルシステム入社，ビル事業部 システムソリューション部 所属
現在，セキュリティ関連事業化に従事