3A-4

情報漏洩防止ソリューション(1)
- 全体構成 -

近藤 誠一† 大沼 聡久† 小宮 崇† 中嶋 春光† 樋口 毅† 遠藤 淳‡
三菱電機株式会社† 三菱電機インフォメーションシステムズ株式会社‡

１．はじめに

近年、企業の機密情報や個人情報が外部へ流出する事件が多発しており、社会問題となっている。情報漏洩に対するセキュリティ対策として、紙文書・媒体・機器・建造物といった物の盗難・破壊・侵入の脅威に対する「物理セキュリティ」、計算機上の情報の漏洩・改竄・偽造の脅威に対する「情報セキュリティ」、企業内のネットワークへの不正侵入・攻撃の脅威に対する「ネットワークセキュリティ」がある。従来、物理セキュリティ、情報セキュリティ、ネットワークセキュリティの個々の観点から、対策システムを個別に導入してきたが、さまざまな脅威に対してワンストップで対応していくためには体系的な導入が必要とされつつある。

本稿では、ユーザ認証、アクセス制御、ファイル暗号化等の情報セキュリティと、入退室管理システムなどの物理セキュリティを統合したトータルソリューションである情報漏洩防止ソリューションの全体構成について示す。

２．情報漏洩対策の課題

個々の脅威に対応した対策システムを個別に導入すると、以下に示す新たな課題が生じる。

(1) ユーザ情報、セキュリティポリシーを統一させるための運用管理の効率化
(2) 個別のユーザ認証手段によるセキュリティ強化と利用者の利便性のトレードオフ
(3) 非 PC を含む情報機器構成、広域分散環境でのログ収集・管理

３．機能と構成

本稿で述べる情報漏洩防止ソリューションの体系を図１に示す。

3.1 情報セキュリティコンポーネント

(1) ファイル暗号化システム

特定フォルダ等の一括暗号化・自動暗号化を行う。また、共有サーバ上の機密情報を暗号化して保管し、人事情報に連動したアクセス制御を実現する。

(2) コンテンツ不正流出防止システム

HTML ファイルや画像コンテンツ等の Web コンテンツに対して、暗号化、利用権の設定を施してカプセル化し、利用者に提供する。

(3) デバイス制御ソフトウェア

USB メモリ、DVD 等のリムーバブルメディアへの書込み禁止制御を行う。

(4) デスクトップセキュリティ

IC カード、指紋照合、パスワード、PKI 認証等の多様なユーザ認証手段により PC へのログイン制御を行う。

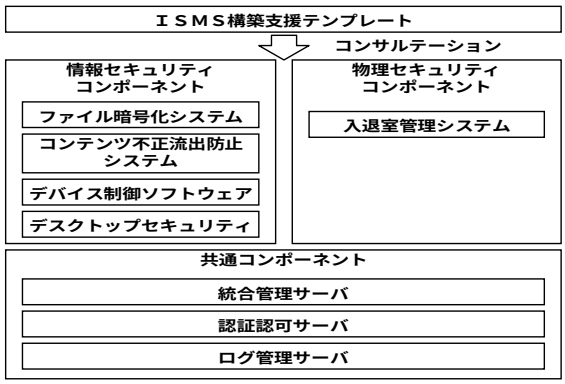

図１．情報漏洩防止ソリューションの体系

3.2 物理セキュリティコンポーネント

(1) 入退室管理システム

ID コントローラがユーザのアクセス制御情報を持ち、IC カード、指紋照合等のユーザ認証により入退室の制御を行う。

3.3 共通コンポーネント

(1) 統合管理サーバ

情報セキュリティコンポーネント及び物理セキュリティコンポーネントのユーザ認証・認可で用いられるユーザ情報、アクセス制御情報を一元管理し、運用管理者向けに統合ツールを提供する。

(2) 認証・認可サーバ

統合管理サーバで管理されるユーザ情報及びアクセス制御情報をもとに、ファイル暗号化システム、コンテンツ不正流出防止システム、デバイス制御ソフトウェア、デスクトップセキュリティに対して、ユーザ認証及び認可決定を行

Information Leak Prevention Solution (1) – System Architecture –
Seiichi Kondo†, Akihisa Oonuma†, Takashi Komiya†, Harumitsu Nakajima†, Tsuyoshi Higuchi† and Jun Endo‡
† Mitsubishi Electric Corporation.
‡ Mitsubishi Electric Information Systems Corporation.

う。また、入退室管理システムに対しては、ユーザ情報、アクセス制御情報を配布する。

(3) ログ管理サーバ

情報漏洩防止ソリューションを構成する各コンポーネントが出力する各種セキュリティログの収集、統合管理を行う。

４．実装方式

4.1 ユーザ情報・アクセス制御情報統合管理

LDAP ディレクトリにて、認証に必要となるユーザ属性情報（パスワード、指紋情報、証明書等）、アクセス制御情報を一元管理し、人事システムと同期を取って、変更管理を行うことにより、運用管理の効率化を実現した。

4.2 ユーザ認証手段の統一

LDAP ディレクトリにて一元管理された認証情報をもとに、認証・認可サーバでの即時認証・認可決定または、認証情報の配布を行う構成をとることにより、ユーザ認証手段の統一を実現した。さらに、認証手段の組み合わせによるステップアップ認証、入室者のみ PC ログインを可能とする機器連携を可能とした。また、相互接続性向上のため、標準認証情報交換プロトコル SAML(Security Assertion Markup Language)[1]の併用を可能とした。

4.3 統合ログ管理

コンポーネント指向ログ収集・統合管理アーキテクチャ、HTTP(S)プロトコルの利用、ログ収集スケジュールの集中管理方式により実現したログ管理システムにて、非 PC を含む情報機器構成、広域分散環境でのログ収集、情報セキュリティマネジメントシステム(ISMS)[2]対応の運用を可能とした。

５．システム適用例

情報漏洩防止ソリューションの広域分散システムへの適用例を図２に示す。

各地に拠点配置された企業では、入退室管理システムや PC のセキュリティ対策は拠点単位となり、全社レベルのセキュリティポリシーの徹底、異動時等の運用管理に課題があった。こうした対策として、広域に分散された拠点での入退室管理、PC のセキュリティ管理、共有ファイルの不正流出防止をデータセンターで集中管理するシステムの構成例（図２）を以下に示す。

①IC カードによる入退室及び PC のユーザ認証：社員証 IC カードのみで入退室、PC へのログオン、共有ファイルへのアクセスを統一的に実現。

②ユーザ情報、アクセス制御情報の一元管理：全従業員のユーザ管理及び入退室・PC ログオン・共有ファイルのアクセス制御情報をデータセンターで一元管理。変更管理及び二重化等の

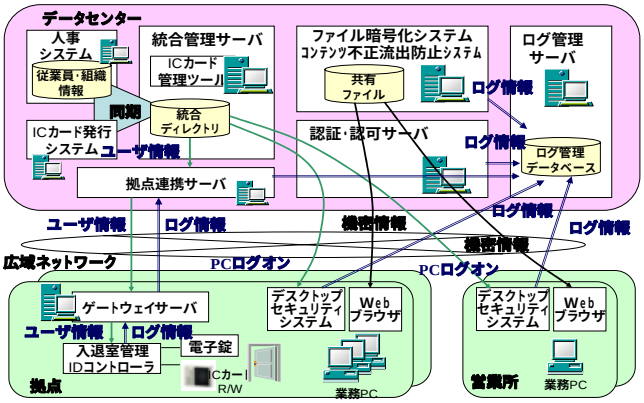

図２．広域分散システムへの適用例

障害・災害対策の運用コスト抑制。

③一括管理された統合ディレクトリと同期した入退室管理：人事異動等に伴う社員証 IC カードの発行・失効・権限変更に連動して、各拠点の入退室管理 ID コントローラに自動反映。

④ログの一元管理：ISMS の運用に必要な入退室、PC 操作といったセキュリティログを広域ネットワーク経由で収集してデータセンターにて統合、集中管理。

６．おわりに

本稿では、以下の特長を持つ物理セキュリティ、情報セキュリティを統合した情報漏洩防止ソリューションの全体構成について示した。

(1) 種々の情報漏洩の脅威に対して網羅的に機能を提供。目的や規模に応じて、大規模なイントラネットシステムから特定用途向きの小規模システムまで迅速・的確に構築可能。

(2) 世界最高水準の暗号 MISTY[3]等の技術を駆使して、ファイル暗号化、ユーザ認証、アクセス制御を実現

(3) １枚の IC カードで、入室、PC ログオン等の種々のユーザ認証を統合可能。セキュリティと利便性の両立を実現。

(4)ユーザ情報及びアクセス制御情報を一元管理。人事異動等に伴う運用管理コストを抑制。

(5) 各コンポーネントのログを収集、統合し、ISMS の運用に必要な統一形式で集中管理。

参考文献

[1] OASIS Security Services(SAML) TC
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[2] 情報セキュリティマネジメントシステム(ISMS)適合性評価制度
http://www.isms.jipdec.jp/

[3] 暗号アルゴリズム MISTY
http://www.mitsubishielectric.co.jp/security/info/misty/about_b.html