

セキュリティコンプライアンス管理 システムの基盤技術

Infrastructure for Security Compliance Management System

あらまし

個人情報保護法が2005年4月から全面施行され、適切な対応が義務付けされた。さらに、日本版SOX法が施行された場合、全般的な情報セキュリティ対策の継続的な監査と改善も上場企業に求められる。

富士通はこれに対応するため、「セキュリティコンプライアンス管理システム」の実現に必要な基盤技術提供に取り組んでいる。「セキュリティコンプライアンス管理システム」を導入することで、情報セキュリティ基準を遵守し、組織のポリシーやルールに従うシステムの構築が可能となる。これにより、企業全体の情報セキュリティガバナンスを強化し、セキュリティコンプライアンス対策運用のTCOを削減することができる。

本稿では、セキュリティコンプライアンス管理システム実現のための基盤技術モデルを示し、基盤技術の要素として、検疫技術、シンクライアント、監査証跡管理について述べる。

Abstract

The Japanese Act on the Protection of Personal Information was enacted in April 2005. In addition, when the Japanese version of the SOX law is enacted, affected companies will have to continuously audit and improve their general information security measures. To help such companies, Fujitsu is developing an infrastructure for the security compliance management system (SCMS). SCMS will enable a company to satisfy company-wide information security criteria based on the company's policies and rules. Therefore, it strengthens the information security governance of a whole company and reduces the TCO of security compliance measures. In this paper, we introduce our infrastructure model for SCMS and explain the computer virus inspection technology, thin client, and security audit trail management as elements of the infrastructure.



畠山卓久
(はたけやま たかひさ)
フロンティアセキュリティ
インフラプロジェクト 所属
現在、セキュリティ製品の
企画に従事。



坂井正徳
(さかい まさのり)
フロンティアユビキタス
プラットフォームプロジェクト
所属
現在、シンクライアント製
品開発に従事。



徳谷 崇
(とくとに たかし)
フロンティアセキュリティ
インフラプロジェクト 所属
現在、セキュリティアーキ
テクトとして、セキュリ
ティ製品の企画に従事。



阿南秀忠
(あなん ひでただ)
フロンティアセキュリティ
インフラプロジェクト 所属
現在、セキュリティアーキ
テクトとして、セキュリ
ティ製品の企画、および
技術開発に従事。

まえがき

個人情報保護法が2005年4月から全面施行され、適切な対応が義務化された。さらに、米SOX法を巡る状況から推し測ると、日本版SOX法が施行された場合、全般的な情報セキュリティ対策の継続的な監査と改善が上場企業に求められる。

本稿では、はじめにITシステムのセキュリティ対策について全般的かつ恒久的に監査・改善を支援する「セキュリティコンプライアンス管理システム」の機能モデルを説明する。続いて、セキュリティコンプライアンス管理システムを構成する様々な要素技術の中から、三つのトピック「検疫システム」、「シンクライアント」、「セキュリティ監査証跡管理」を取り上げ、順に説明する。

セキュリティコンプライアンス管理モデル

情報システムは1箇所でも弱点があると、そこから情報が漏えいし、また改ざんされてしまう。さらに情報セキュリティはクライアントだけでなく、サーバシステムやネットワークなど、情報システム全体に対して施す必要がある。

セキュリティコンプライアンス管理システムは、これらの問題を解決し、システム全体のセキュリティを維持するものである。以下、TRIOLE⁽¹⁾のコンセプトに基づくセキュリティコンプライアンス管理モデル（セキュリティコンプライアンス管理システムの機能モデル）について説明する。

このモデルは、図-1に示すように「ぜい弱性対策」、「侵入対策」、「情報漏えい対策」の三つの対策分野とそれらを統合管理する「セキュリティコンプライアンス管理」機能で構成される。

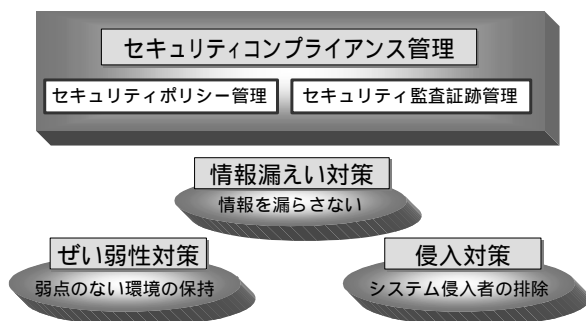


図-1 セキュリティコンプライアンス管理モデル
Fig.1-Security compliance management model.

三つの対策分野

(1) ぜい弱性対策

侵入対策や情報漏えい対策などのセキュリティソフトウェアは弱点のない正しい環境で動作して初めて効果的に動作する。ぜい弱性対策として、クライアントやサーバに対して、セキュリティパッチ管理やウイルス対策を導入し、弱点のない環境を維持することはセキュリティ対策の必須要件である。

(2) 侵入対策

侵入対策は、なりすまし対策や不正アクセス対策を導入し、情報を漏えい・改ざんするシステム侵入者を排除するものである。SOX法対応のなりすまし対策としては、統合ユーザID管理が重要になる。また、富士通では、不正アクセス対策としてIPCOM Sシリーズ⁽²⁾を提供している。

(3) 情報漏えい対策

情報漏えい対策が効果的に働くには、ぜい弱性対策と侵入対策が前提として必要である。その上で、情報漏えいの主たる原因となっている内部不正に対する次の二つの観点での対策が必要となる。

- ・盗難・紛失対策
- ・不正持出し対策

富士通では、帳票ソリューションとしても、情報漏えい対策機能を提供している⁽³⁾

以上(1)～(3)の三つの対策分野にわたって、富士通では、Systemwalker Desktopシリーズ⁽⁴⁾で、対策機能を提供している。

セキュリティコンプライアンス管理

「セキュリティコンプライアンス管理」機能は、情報漏えいや改ざんにかかわる法律などに対応したセキュリティポリシーの遵守を監査し、検出した違反を恒久的に改善するもので、セキュリティポリシー管理機能とセキュリティ監査証跡管理機能から成る。

(1) セキュリティポリシー管理

組織のセキュリティポリシーにのっとり、不正を検出し、改善することで、システム全体のセキュリティレベルを一定以上に維持する。

(2) セキュリティ監査証跡管理

セキュリティ監査証跡管理では、セキュリティポリシーの遵守を監査する。セキュリティ監査証跡（監査ログ）の収集・保管・分析を提供することで、定期監査による安全性の見える化が可能になる。ま

た、漏えい・改ざんの兆候・事故発生後の迅速な原因追求と対策が可能になる。

検疫 - ぜい弱性対策と侵入対策の例

情報漏えい対策の前提となるぜい弱性対策、侵入対策としては、外部からの攻撃を防衛するファイアウォール、IDS (Intrusion Detection System) や、ウイルス対策ソフトなどが従来からあるが、最近ではウイルスの侵入を検疫システムにより防御する技術が注目を集めている。これは、例えば、他事業所からの出張者が、持ってきたノートPCを社内ネットワークにつなげる場合、そのノートPCから社内ネットワークにウイルスが侵入してしまう危険性があるが、このような問題を解決する技術である。

外部から持ち込んだノートPCを社内ネットワークに接続する場合には、そのPCのセキュリティパッチが最新の状態になっていることと、ウイルス対策ソフトの定義ファイルの更新状況などを確認しなければならない。不備があれば接続を許さないようにすればいいのであるが、実際には困難であった。理由は、大きく二つある。一つは、監視する対象が、あらかじめ設定した内部のPCのみであったため、外部からの持ち込みPCに対処できなかった。もう一つは、不備のあるPCを強制的にネットワークから遮断する機構がなかったことである。

これらの問題に対して、富士通は外部のPCを監視・遮断する検疫ソリューションを提供している。Systemwalker Desktop Inspectionは、図-2に示すように認証ゲートウェイ装置IPCOM Lシリーズ⁽⁵⁾

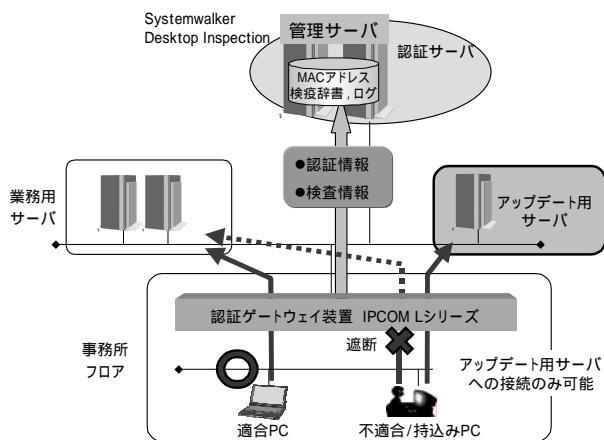


図-2 Systemwalker Desktop Inspectionの検疫の仕組み
Fig.2-Mechanism of Systemwalker Desktop Inspection.

と連携することで、クライアントPCの接続時に、ユーザ認証、MACアドレス認証、セキュリティポリシーを満たしているかどうか(セキュリティパッチの適用状況、ウイルス対策ソフトの定義ファイルが最新かどうかや任意のソフトの導入状況)のチェックをし、業務ネットワークへの接続可否を決定することを可能にする。さらに、セキュリティポリシーを満たしていない場合、アップデート用サーバへの接続のみを許可するように制限することができるため、クライアントPCは、そこでアップデートを行うことで、業務ネットワークに接続することが可能となり、自律的にセキュリティレベルを維持することができる。

シンクライアント - 究極の情報漏えい対策

本章では、究極の情報漏えい対策であるシンクライアントについて述べる。

富士通の取組み

業務システムのTCO (Total Cost of Ownership) 削減のソリューションとして、1996年にOracle社が提唱した「Network Computer構想」から始まったシンクライアントは、2004年以降、個人情報保護法の施行に伴う有力な情報漏えい対策として見直されてきている。

富士通では、1998年に「BT-300 (ディスクレスPC)」, その制御ソフトウェアである「BTS V1」を出荷し、文教市場を中心にビジネスを行ってきた(図-3)。

また、2005年には、情報漏えい対策の高まりに合わせて、新たなディスクレスPC (デスクトップ2機種、省スペースタイプ1機種、モバイルタイプ1機種)、およびCitrix Presentation Server (Citrix社製品: 旧名MetaFrame)、BTSの後継にあたるBT Administration Server V3 (富士通独自製品、ネットワークブートタイプのLinux Desktop) によるシンクライアントソリューションを発表し、新たなシンクライアントビジネスに対応可能な体制を作ってきた。

シンクライアントと情報漏えい対策の接点

前述したように、シンクライアントの当初の目的は、「TCOの削減」にあった。ではなぜ情報漏えい対策の有力候補として注目されてきているのかについて説明する。

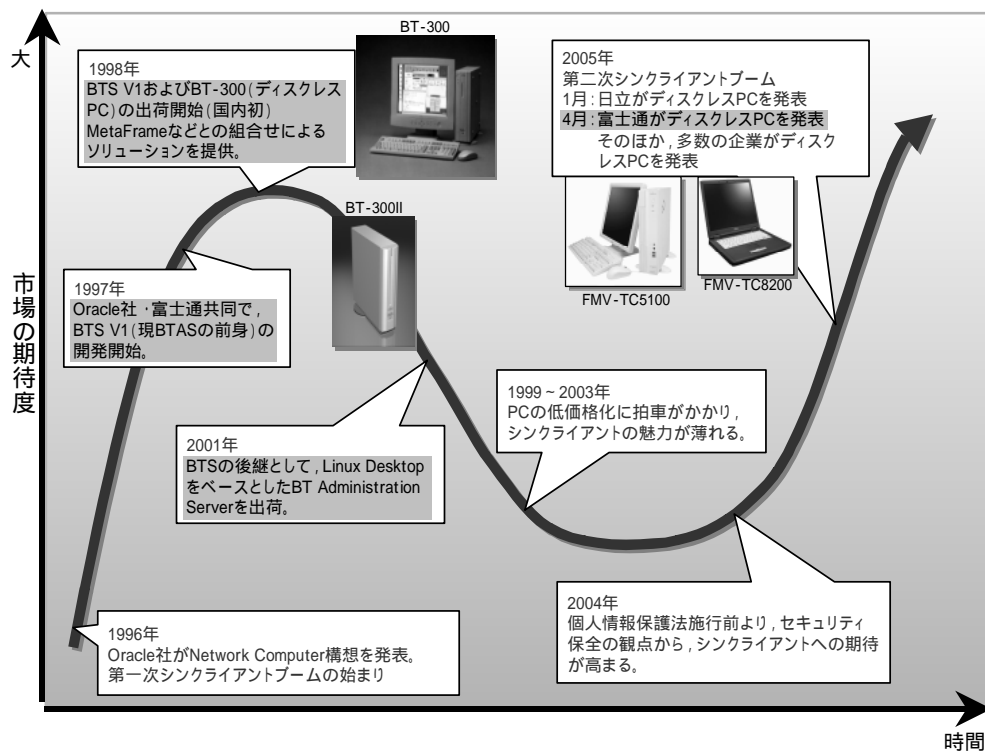


図-3 富士通のシンクライアント技術への取組み
Fig.3-Fujitsu's historical approach on thin client.

【ディスクレスクライアント】

シンクライアントシステムで利用される端末は、基本的にハードディスクを搭載しないディスクレスPCが使われる。

TCOの観点からは、ソフトウェア資源をサーバ側で一括管理するために、管理者は個々のPCを管理する必要がなく、管理コストが削減できるというメリットがある。

この特徴が、「ローカルにソフトウェア資源を格納できないのであれば、PCが紛失した場合でも、なにも残らないため、情報漏えいの可能性がゼロになる」というセキュリティの視点からのメリットとして注目されている。

現状のPCにおいては、情報の流出そのものを皆無にすることは難しく、暗号化などの手法により、流出したとしても「読めない・開けない」などの措置をとることで対応しているが、なくなったPCの中に流出してはならない情報が格納されていた事実までは回避できない。

その点、シンクライアントであれば、「情報は全く格納されていませんし、格納する術もありませんから、情報流出は発生していません」という、単純

明快な説明が可能となる(図-4)。

この点が、シンクライアントの仕組みをモバイルPCに適用する最大のアピールポイントとなり、昨今のシンクライアントブームにつながっている。

【ソフトウェア資源の一括管理】

個々のPCにソフトウェア資源を分散して格納するという事は、企業として情報の散在を広げることだけでなく、情報の管理ができなくなる可能性を意味する。

シンクライアントは、ソフトウェア資源(OS、アプリケーション、データ)を一括して管理することを強要するシステムであり、現状のように散在してしまったソフトウェア資源を、管理しやすくすることが可能となる。

データの一括管理が可能となると、「どのデータを誰に、どこまでアクセス可能とするか」などの情報参照ポリシーを組みやすくなり、より安全なドキュメントサーバの構築を推進していくきっかけとなる。

利用機能制限

シンクライアントでは、TCO削減の観点から、クライアント利用者に操作制限を付加することを可能にしている。これをセキュリティの観点でみると、

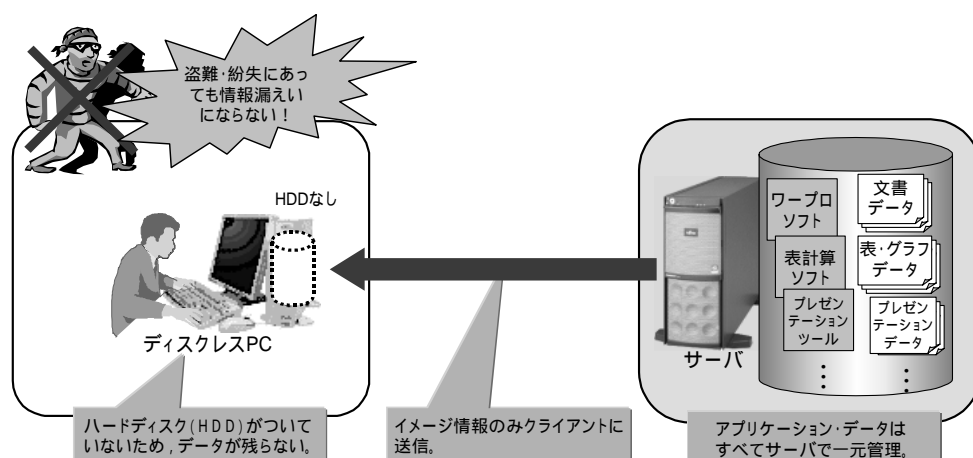


図-4 シンククライアントによる究極の情報漏えい対策
Fig.4-Ultimate countermeasure against information leakage using thin client.

「利用者に対して、利用権限を制限するポリシー」を構築するということになる。

例えば、以下のような措置を取ることが可能となる。

- (1) 可搬媒体（USBメモリなど）へのコピーを制限する。
- (2) アプリケーションからアプリケーションへのコピー＆ペーストを制限する。
- (3) 特定のクライアント・利用者には、印刷できないように制限する。

本章で述べたように、基本的に、現在セキュリティの観点でシンククライアントのメリットとして見られている機能は、もともとシンククライアントが持っていたTCO削減のための様々な仕組みによって提供される。

シンククライアントは、利用者に対して様々な制限を加えるシステムとなり得るため、使い勝手の低下には注意する必要があるが、クライアントPCが盗難・紛失にあっても情報流出にならない究極の情報漏えい対策である。

セキュリティ監査証跡管理 - 安全性の見える化

セキュリティ監査証跡は、監査対象となるシステムにおける一連の動作を追跡するための仕組みと記録（ログ）である。本章では、監査ログを用いてシステム全体の安全性を「見える化」するための課題と、それを解決するための富士通の取組みについて述べる。

システム全体の安全性を見える化するためには、

まず次の二つの機能を実現する必要がある。

- (1) 監査ログの収集
- (2) 監査ログの追跡

追跡が可能になることによってシステム全体のセキュリティポリシーへの違反や、違反の兆候を見える化することができる。

監査ログの収集 - 見える化の前提

監査ログとなるシステムのログはOS、ミドルウェア、ネットワーク機器など様々な場所で採取されている。

しかし、システム全体の安全性の見える化を考えたときに、ある特定の箇所の監査ログだけでは安全性を確認したことにはならない。そこで、システム全体の監査ログを収集し、一元的に管理するシステムが必要になってくる（図-5）。富士通は、Systemwalker Centric Manager®で監査ログの収集・一元管理を実現する機能を提供する。

監査ログの追跡 - 分析の前段・原因の究明

システムの安全性を見える化するためには、監査ログを収集するだけでなく分析することが必要になる。この見える化をシステム全体にまで拡張しようとすると、個々の監査ログの分析だけにとどまらず、システム全体の監査ログを分析して一連の操作を追跡し、システム上でのデータの流れを明らかにしなければならない。操作の追跡のためには、監査ログをひも付ける必要があり、そのキーとして最も適切なものはシステム上でマシンを特定することのできるIPアドレスまたはホスト名、あるいは操作を行った者を特定することのできる「ユーザID」

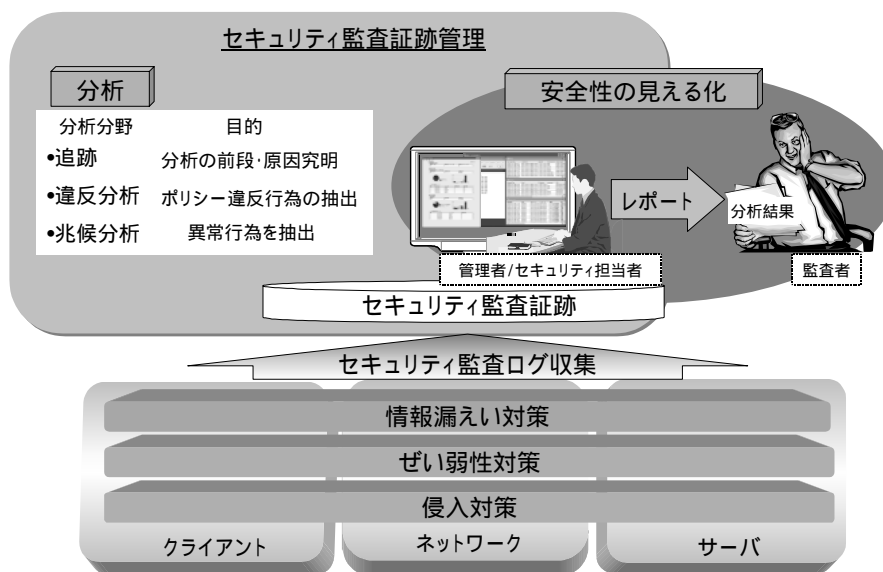


図-5 セキュリティ監査証跡の管理・分析
Fig.5-Management and analysis of security audit trail.

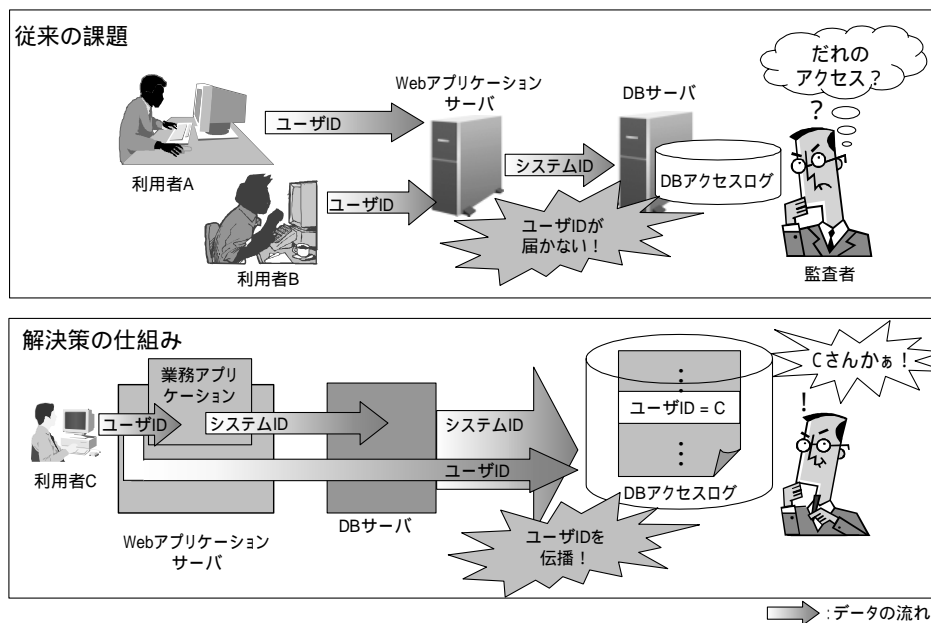


図-6 3階層システムでの課題と解決策
Fig.6-Problem and our solution for three-tier model.

である。

ところが、Webアプリケーションサーバを利用した3階層システムにおいては、一般的にアプリケーションからDB（データベース）へ接続するためのユーザIDが一つのシステムIDに固定されて使われている。これにはDBに1回ログインするだけで、複数ユーザのトランザクション処理ができるというメリットがある。

しかし、DBの監査ログとして記録されるユーザIDがアプリケーションサーバのシステムIDに固定されるため、どのクライアントのアクセスによる監査ログであるのかが分からないという問題をはらむ。

この問題に対して、DBが（Webユーザを特定できる）ユーザIDをセットするインターフェースを提供し、監査ログを残すという方法がある（図-6）。富士通は、DBサーバのSymfoware⁽⁷⁾でこの機能を

今後提供する予定である。さらに、アプリケーションサーバのInterstage Application Server[®]で、これと連携する機能を今後提供する予定である。これにより、Interstageの認証基盤やDBアクセス機能を利用したアプリケーションを作成すると、DBに自動的にユーザIDがセットされるようになる予定である。

上記の方法で採取されたDBの監査ログとアプリケーションサーバのWebアクセスログについて、ユーザIDの一致を見ることでDBの監査ログがどのクライアントのアクセスによるものかが分かる。クライアントPCの操作ログとひも付けることで、クライアント～アプリケーションサーバ～DBの追跡が可能になり、DBのデータがクライアント上で実際にどのように扱われたかが分かるようになる。

違反兆候分析 - 見える化実現へのポイント

ところで、監査ログの分析のポイントとしては、

- ・違反分析

ポリシーに違反した行為（許可されていない行為）を見つけること

- ・兆候分析

普段と異なる行動を見つけること

がある。上記の3階層システムで追跡が実現していれば、あるログインが普段と異なるクライアントログインユーザIDを利用していた場合にDBアクセスのなりすましや情報漏えい、改ざんの兆候として解釈することができる。この後、このユーザに大量の印刷ログや外部媒体持出しログがあった場合には情報漏えいを行っている可能性がより深まる。追跡機能を用いてクライアント～アプリケーションサーバ～DBの監査ログをひも付けた結果、初めてシステム全体での違反・兆候分析が可能になる。

本章で述べたように、システム全体の安全性を「見える化」するためにはシステム全体から監査ログを収集することが前提となる。個々の監査ログからは分析できない部分もそれらをひも付けることで

今まで見えなかったセキュリティリスクへの対策が可能となり、システム全体の安全性を追求することができる。

む す び

以上のような基盤技術を用いて、「セキュリティコンプライアンス管理システム」を導入することで、組織のポリシーやルールに従う情報セキュリティ基準を遵守するシステムを構築することが可能となる。本システムの導入に当たり、組織の情報セキュリティ基準から策定した情報セキュリティポリシーをセキュリティコンプライアンス管理機能に設定することで、システム全体の情報セキュリティガバナンスを強化することが可能になる。

今後も富士通では、システム全体でのセキュリティコンプライアンス管理を実現する製品を提供していく。

参 考 文 献

- (1) 黒柳智司ほか：TRIOLEにおけるセキュリティ . *FUJITSU*, Vol.55, No.1, p.18-30 (2004).
- (2) 富士通：IPCOM Sシリーズ . <http://primeserver.fujitsu.com/ipcom/products/lineup/#ipcoms>
- (3) 山本雅彦ほか：帳票のセキュリティ確保と業務効率の両立 . *FUJITSU*, Vol.57, No.2, p.146-152 (2006).
- (4) 富士通：Systemwalker Desktopシリーズ . <http://systemwalker.fujitsu.com/jp/desktop/>
- (5) 富士通：IPCOM Lシリーズ . http://primeserver.fujitsu.com/ipcom/products/lineup/ipcom_l1400.html
- (6) 富士通：Systemwalker Centric Manager . <http://systemwalker.fujitsu.com/jp/centricmgr/>
- (7) 富士通：Symfoware . <http://software.fujitsu.com/jp/symfoware/>
- (8) 富士通：Interstage Application Server . <http://interstage.fujitsu.com/jp/apserver/>