普通論文

セキュリティ監査システムの開発

Development of Information Security Audit System

石田文治* Fumiharu Ishida　矢野隆利** Takatoshi Yano　渡部政己*** Masaki Watanabe
新井玲子† Reiko Arai　鈴木高之* Takayuki Suzuki

要　旨

情報セキュリティ対策は，もはや対症療法や緊急対応だけでは経営インパクトを避けられません。そこで多くの組織は，情報マネジメント対策やシステム管理対策を，ファイナンシャル課題に次ぐ，重要な経営課題と位置付けています。

本研究は，ITベンチャーから経営コンサルティングまで幅広い会社のナレッジはもとより，それを利用する被監査組織自身が参加できる情報セキュリティ課題に対するDynamic Collaborateの場を提供する，セキュリティ監査システムのプロトタイプを開発し，有効性を実証しました。

The management impact is no longer inevitable information security measure only in an allopathy or an incident response. Many organizations are going to place the information management measure and the security measure for the information system as an important management problem following the financial task.

This research developed and demonstrated as a prototype of security audit system, and it provides the place of dynamic-collaborate for the security problem, which includes the knowledge in the wide-business company from IT venture to management consultant in addition to reaudit organization. The company and organization can participate in that place.

1．まえがき

情報セキュリティの課題にどう向き合うべきでしょうか。「情報セキュリティが，ITによって拡大した自由を損なうことなく，技術，管理運営手法，法律・社会制度，情報モラルを相互に深く連携，協調させて，利便性，効率性と安全性の向上，プライバシーの保護，および監視社会の最小化を同時に達成することを目的とする一体性と完結性を持つ社会的基盤システムを構築するためのダイナミックなプロセスである」との考えに立てば，**図1**のような様々な課題に対し，諸分野を連携させて総合的方策が探求されなければならない[1]ことになります。

プロセスの確立というと，環境マネジメントシステム規格ISO14000やプロセスアプローチを採用している品質マネジメントシステム規格ISO9000を連想される方も多いと思いますが，情報セキュリティに対しても類似スキームで認定を行う安全・安心マーク制度やISMS認証取得制度が既に開始されています。またセキュリティに限らず情報を司るシステム全体に対し，システム監査というスキームも用意されています。ただしこれらの手法や制度は，組織が自力で取り組むには，多少敷居が高いのも事実です。

2．従来の課題

情報セキュリティマネジメントに関する評価は，規格・基準や監査制度を熟知した審査員やコンサルタントが監査

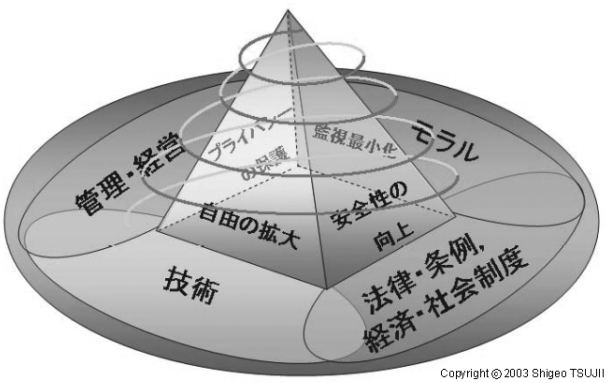


図1　情報セキュリティの理念
Fig.1　Idea of information security.

＊　IT基盤システム開発事業部
IT System Platform Division
＊＊　NECシステムテクノロジー　サーバー基盤事業部
NEC System Technologies, Ltd.
＊＊＊　NECシステムテクノロジー　システムソフトウェア事業部
NEC System Technologies, Ltd.
†　NECソフト　ITソリューション事業部
NEC Soft, Ltd.

対象で，アセスメントや確証の収集とそれらの手作業による集計・分析で実施しています。このため実施できる専門家は限られ，結果報告書や改善対策案の作成作業には多くの時間も要しています。

一方システム診断は，フリーソフトから商用パッケージまで多数のプログラムを活用することで実施されています。これらのプログラムも，安全かつ有効に利用するためには専門知識を要するため，供給ベンダ自身やセキュリティ専業企業に利用が限られています。

ここで課題となるのは，かかるコストはもとより，評価対象範囲や評価結果の格差があることと，とりわけアセスメント側とシステム診断側の評価結果に関して整合性や連携が考慮されていないことです。たとえば，ヒアリングによる質問回答間の矛盾などを指摘し，アセスメント結果に反映するものはあっても，システム診断結果との矛盾などを指摘・反映するものはありません。

3．開発のコンセプト

監査ツールを開発するに当たってのコンセプトは，第一にアセスメントを実施する際に必要となる情報セキュリティマネジメント評価基準や制度の利用を補助する検索機能を持ったデータベースの構築とヒアリングを行うための質問文生成ツールを，審査員やコンサルタントが持っているナレッジを含み提供することでした。

第二は，監査に必要となるシステム診断ツールの機能を洗い出し，その上で既存ツールで不足する機能を新規に開発し，診断内容を網羅的にすることでした。

第三にシステム診断ツールに，専門家でなくても簡単かつ安全に操作できるユーザインタフェースを提供することでした。

第四に本アセスメントツールやシステム診断ツールが，既存のアセスメントツール結果やシステム診断プログラム結果と連携が容易となるように，デファクトとなり得るツールインタフェースを提供することでした。

最後に，アセスメント内容や診断ツールの更新頻度や悪用防止に対応するためのサービス提供手法や，これらのツールコンテンツの提供者と利用者間の課金手法を提供することでした。

4．システムの特徴

4.1　規格・ガイドラインのデータベース機能

国内外の情報セキュリティマネジメントに関する基準の調査を行い，そのなかから一般に適用できるものとして，ISO17799[2]，JIS X 5080[3]，BS7799-2:1999とBS7799-2:2002[4]を選択し，データベース化の対象としました。規格の条文構造は複雑でデータ長だけでなく表示方法もパターン化しにくいこと，規格は定期的な改版が想定されること，規格内だけでなく規格間での引用が多いことが判明しました。そこで条文をスキーマとして管理でき，リンク機能により

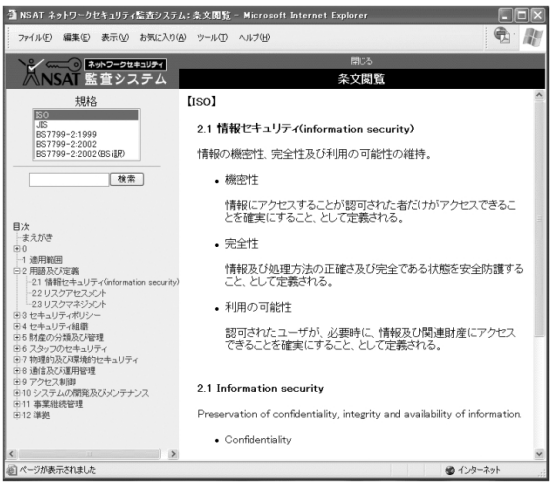


図2　XMLデータベース化された国際規格
Fig.2　ISO standard's notation by XML-DB.

更新前後や他規格などを同時並行的に利用できる点に着目しXML-DBを採用し，**図2**のように仕様化し，評価を行いました。

その結果，規格に関して前提知識のない人が利用する場合は，規格用語などの検索，該当条項を参照するための目次・キーワード検索や，規格原文を参照するための条項の英文・和訳同時表示が必要なことが判明し，仕様変更を行いました。また，規格以外に参照する基準・ガイドラインも検索できるよう，全文検索可能な検索機能も仕様化しました。

4.2　アセスメント機能

監査人によるヒアリングを中心に行われるアセスメントは，様々な質問内容を監査対象組織の条件に合わせ，また日進月歩で変化するIT環境に適応した内容で行う必要があります。その上で同一組織内の異なる部門や同一組織の異なる時期に実施したアセスメント結果が，各バージョンでの結果で比較できるよう，評価基準は，**図3**のように規格条文ごとに設問を任意の個数登録，採点することで得られ

図3　国際規格に沿ったアセスメント内容
Fig.3　Assessment contents following ISO standard.

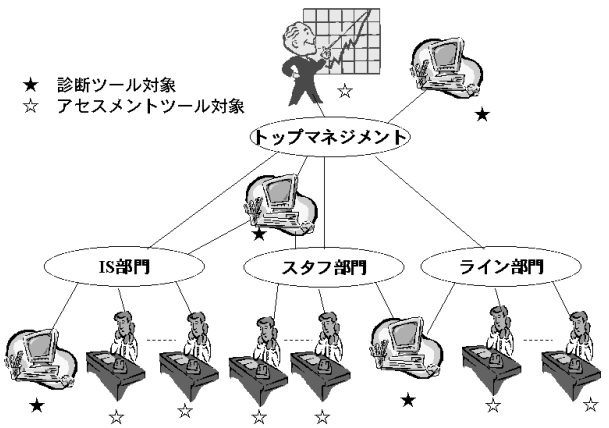


図4　監査対象の組織とシステム構成の関係
Fig.4　Relation between organization and IT system under audit object.

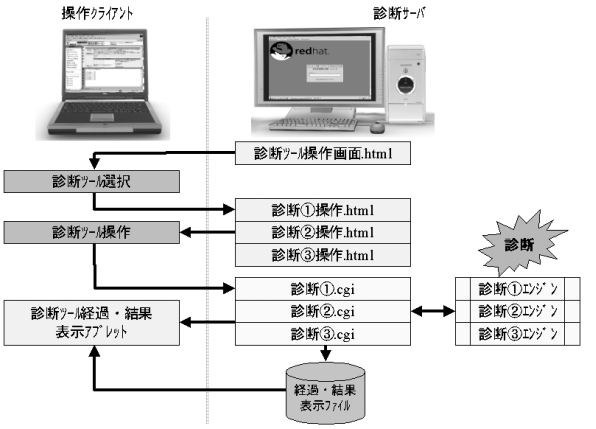


図5　クライアント・サーバ方式でのシステム診断
Fig.5　IT system diagnostic by client-server method.

図6　システム診断の簡易な操作画面
Fig.6　Easy opration screen for IT system diagnostic.

る，規格条文ごとの百分率とし，さらに被監査対象により異なる特性をセキュリティレベルに反映する必要性があることから，アセスメント設問ごとの配点をデフォルト値から任意の値に変更できるようにしました。

また，設問の配点は重要度で分類し，アセスメント時に設問量を選択できるようにし，設問間の依存関係も設定できるので矛盾した回答を回避できます。ただし本ツールに設定したこれらのデフォルト値は，すべてコンサルタントや審査機関のノウハウを反映したものであり，変更作業は基本的には不要です。

さらに**図4**のようにアセスメントを実際の組織で実施する場合，複数の監査人による分担作業が必要となる場合があります。これを前提に，所属監査単位で管理するためのスキームを導入し，監査人相互間のアセスメント結果などをグループ単位で共有できるようにしました。

最後に，既存の他社アセスメントツール結果と連携しアセスメント内容を深めるために，XML形式の結果インタフェースを定義し，データベース登録機能を仕様化しました。

4.3　システム診断機能

システム診断ツールは，コンピュータ・ネットワークの専門家でなくても安全・安心に管理・操作ができるよう，クライアント・サーバ構成（**図5**）としました。

本診断ツールは，**図6**のようにメニューから診断ツールごとまたはISO規格条文ごとの機能分類から診断内容を選択できるようにしました。本診断ツールの操作は，日本語化されていないツールを含み，すべて日本語ベースでの操作で行え，診断項目ごとに解説表示機能を持ち合わせているため，監査対象システムの責任者に説明するために利用できます。

さらに，監査対象システムが日常的に出力しているログを解析・診断したり，ソーシャル・エンジニアリングのシナリオを提供するなど，システム自身に影響を与えず，診断を行う手法も提供します。

また本診断ツールは，その診断結果をアセスメントツールと連携するためのXML形式ログを生成します。アセスメントツール側でアセスメント結果との整合性などの分析が行われます。また，既存の他社システム診断ソフトウェアの結果を本監査ツールにXML形式インタフェースで連携させるためのログコンバータも仕様化しました。

システム診断結果に用いたXMLフォーマットは，アセスメントツールと連携するためだけでなく，各システム診断ツールの特徴を活かせるように設計しました。同時に，XMLスタイルシートを用いて，一般のシステム管理者やSEでも分かりやすい結果表示ができるようにしました。

4.4　監査分析機能

アセスメントとシステム診断から生成されたセキュリティ監査結果は，規格条文に基づいた評価軸ごとの集計値をレーダーチャートまたは棒グラフで即時に表示できます（**図7**）。

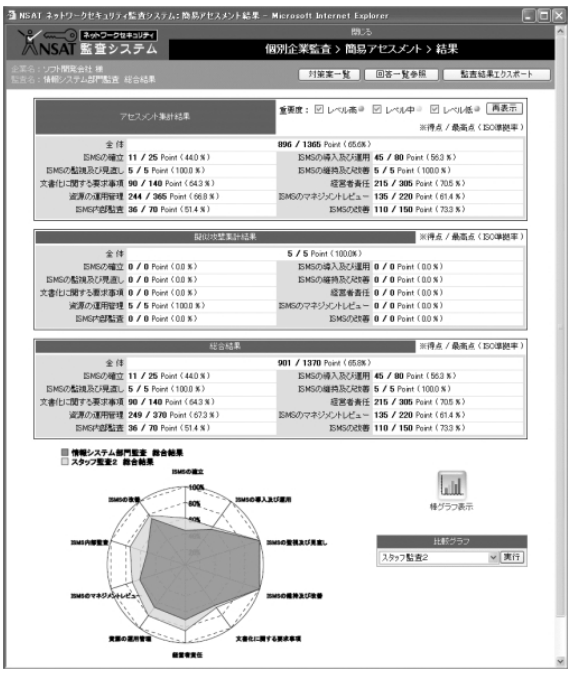


図7　セキュリティ監査システムの結果例
Fig.7　Example of information security audit system.

さらに，異なるバージョンでのアセスメント結果，システム診断結果や，他社ツールのアセスメント結果を重ね合わせることで比較することができ，アセスメント結果に対して対策案を入力することもできます。

5．むすび

本監査システムの商用化のためには，ツールのコンテンツの利用に応じた課金システム，ネットワークを介してやり取りされるデータの暗号化や診断ツールの悪用を防止するためのセキュリティ機能を含むシステム仕様の実装が必要であり，今後システム化を行います。さらに，今回の監査ツールは国際規格をベースに仕様化しましたが，被監査組織のニーズにあった規格・制度や業界ガイドラインなどをベースに同様なコンテンツの増強を行い，さらにそれら評価結果を比較できるようにします。

情報セキュリティ対策は，高度情報化社会に属するあらゆる組織が避けて通ることのできない経営課題です。同時にユビキタス社会のインフラとして安心・安全にITを活用するには，利用者も含め全ての人がこの対策にかかわらなければならないものです。

本セキュリティ監査ツールが実践するダイナミック・コラボレーションを様々な経営課題解決のベストプラクティスに育てるため，今後も多くの行政機関，情報セキュリティベンダ，コンサルタント，監査企業，審査機関などのご協力をいただきながら，まずセキュリティ対策支援インフラとして商用化を狙い，BS15000-1:2002[5] /-2:2003のITサービスマネジメントに代表される他マネジメント規格への適用拡大を図っていく所存です。そして，実証実験を始めとし本研究にご意見やご協力をいただいた皆様からのご要望・ご期待に沿い，コスト対効果を意識した経営課題解決に必要なself consistent-fieldの早期確立に貢献していきたいと考えています。

なお，本研究の一部は，通信・放送機構の委託研究「ネットワークセキュリティ監査技術の研究開発」プロジェクトの成果です。

参考文献

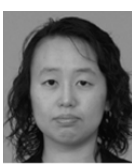
1）辻井重男，電子社会の信頼性向上と情報セキュリティ，電子情報通信学会誌，2003-11
2）ISO/IEC17799 Information technology-code of practice for information security management, 2000-12
3）JIS X 5080 情報技術－情報セキュリティマネジメントの実践のための規範,2002-2
4）BS7799-2:2002 Information security management-Part2: Specification for information security management systems, 2002-9
5）BS15000-1:2002 IT service management-Part1:Specification for Service

筆者紹介

Fumiharu Ishida
石田　文治（いしだ　ふみはる）　1984年，NEC入社。現在，システムソフトウェア事業本部IT基盤システム開発事業部勤務。ISMS主任審査員。日本セキュリティ・マネジメント学会会員。

Takatoshi Yano
矢野　隆利（やの　たかとし）　1985年，四国日本電気ソフトウェア入社。現在，NECシステムテクノロジー サーバー基盤事業部主任。

Masaki Watanabe
渡部　政己（わたなべ　まさき）　1987年，四国日本電気ソフトウェア入社。現在，NECシステムテクノロジー システムソフトウェア事業部セキュリティ技術部主任。



Reiko Arai
新井　玲子（あらい　れいこ）　1991年，日本電気ソフトウェア入社。現在，NECソフト ITソリューション事業部勤務。

Takayuki Suzuki
鈴木　高之（すずき　たかゆき）　1999年，NEC入社。現在，システムソフトウェア事業本部IT基盤システム開発事業部勤務。