3E-6

文書解析と設定検証に基づく情報漏洩脅威分析方式 (1) コンセプトとシステム概要

小川　隆一　榊　啓　矢野尾　一男　細見　格
NEC インターネットシステム研究所

１．はじめに

コンピュータシステムの運用不備や文書管理不備による情報漏洩事故の防止はセキュリティ管理にとって最重要課題のひとつである。最近、PC や媒体の持ち出し制御などの漏洩対策が急速に普及しているが、これはあくまで「最終ラインの水際防御」である。根本的な施策としては、文書への適正なアクセス権設定と運用を実施するため、誰がどの文書にアクセスしてよいかに関するアクセスポリシーを正しく定義し、それに反した運用がなされないようシステムをチェックすること、すなわち ISMS フレームワークの活用が必要となる。しかし実際にはこの作業は管理者の負担が大きく、現実的でない。本稿ではこの問題に対処するため、「重要文書の洗い出し」と「その文書が適正なアクセスポリシーのもとで管理されているか」を文書解析技術と設定検証技術に基づき確認する情報漏洩脅威分析方式を提案し、その概要を述べる。

２．アクセスポリシー実施と検証の必要性

誰がどのような条件でどの文書にアクセスしてよいか、に関するアクセスポリシーを定義し、これに基づき正しいアクセス権を設定（ポリシー実施）すれば、例えば単一の DRM (Digital Rights Management System)システムにおけるアクセスポリシー実施などの分野では十分な安全性が得られるだろう。

しかし、実運用される多くのシステムでは、アクセスポリシー実施において、OS のアクセス権、ファイアウォール、サーバソフトウェア固有のアクセス権等の設定実施が複合的に絡み合うことが普通であり、これらの設定を正しく維持管理していくことは至難である。

従って、情報漏洩を起こさないシステム運用のためには、適正なポリシー実施（アクセス権設定・アクセス制御）の支援とともに、設定が今どうなっているか、漏洩につながる不正アクセスがおこらないか、の検証・監査支援が必須である。次節でこれを詳細に検討する。

３．セキュリティサイクルと漏洩対策

図 1 に ISMS のセキュリティサイクル（PDCA サイクル）を示す[1]。これは状況把握、対策、監査、運用保守の４つのプロセスのループであり、システム全体のセキュリティを維持し、情報漏洩を防止する管理サイクルである。

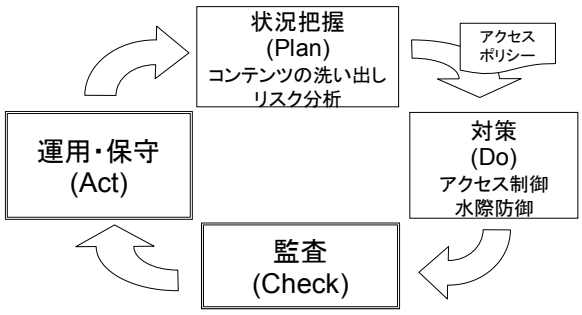

図 1　PDCA サイクル

情報漏洩対策を各プロセスに当てはめると、以下のように詳細化される。

1．状況把握：システムが保持する機密文書を洗い出し、リスク分析を行う。システムの構成や脆弱性を考慮し、文書に対する正しいアクセスポリシーを定義する。関連する既存技術として、キーワードによる文書分類、脆弱性検査ツールなどがある。

２．対策：アクセスポリシーを実施するための対策を実施する。既存技術として、ファイルのアクセス制御、ネットワークフィルタリング、DRM、コンテンツフィルタリングなどがある。

３．監査：アクセスポリシーを正しく実施しているか監査する。既存技術として、ログ監査ツールなどがある。

４．運用・保守：前記３つを繰り返し実行しながら状況の変化に対応する。既存技術として、セキュリティ運用管理ツールがある。

既存の情報漏洩対策技術は主に対策プロセスに集中しているのがわかる。一方で、状況把握

An Information Leakage Risk Evaluation Method Based on Sensitive Document Detection and Security Configuration Validation: (1) Concept and System Architecture
Ryuichi OGAWA, Hiroshi SAKAKI, Kazuo YANOO, Itaru HOSOMI
Internet Systems Research Laboratories, NEC Corporation

や、監査、運用・保守に関する技術は少なく、情報漏洩対策について PDCA プロセスを実施するのは現時点では容易ではない。特に重要な課題として、以下が未解決である。

課題１．状況把握：高い精度で機密文書を検索・分類する技術。

課題２．監査・運用：アクセスポリシーと複数の対策（設定情報）を比較し、アクセスポリシーが正しく適用されているか検証する技術。

課題３．保守：不備のある設定を探索し、修正を促す技術。

４．情報漏えい脅威分析方式のコンセプト

PDCA サイクルのプロセスのうち、状況把握と監査の自動化、および運用・保守の支援を行う情報漏洩脅威分析方式を提案する。本方式は、文書解析と設定検証を組み合わせ、機密文書洗い出しからポリシー実施状態のチェック、不備発見時の対処までの一連の流れを支援し、上記３つの課題を解決することを目的としている。本方式は、文書内容解析部、設定検証ポリシー生成、設定検証の３つの機能ブロックで構成される（図２参照）。

（１）文書内容解析

システム内に格納された文書を探索、内容解析を行い、文書の特徴に応じて「個人情報」や「機密情報」などの機密カテゴリに分類する。文書のレイアウト情報を用いた分類アルゴリズム[2]により、課題１を解決する。

（２）設定検証ポリシー生成

文書内容解析部で分類した結果をもとに、アクセスポリシーから設定検証ポリシーを生成する。設定検証ポリシーとは、機密文書の分類カテゴリに応じて定義される抽象的なアクセスポリシーを、実システムへ適用できるよう個々のファイル名・ユーザ名でおきかえたものである。例えば、「機密文書は、暗号化された通信路を用いた場合のみ、ユーザ sakaki が読める」と定義されたアクセスポリシーがある場合、文書内容解析部で機密に分類されたファイル「secret.doc」と、サービスの暗号化の知識を用いて「ファイル secret.doc は、https を用いてユーザ sakaki が読める」という設定検証ポリシーに変換する。これにより、システム構成と独立に定義されたアクセスポリシーを、実際の設定と比較検証可能な形式に変換できる。

（３）設定検証

システム内の複数の設定情報を収集し、それらが全体として設定検証ポリシーを満たすかどうか、をモデルベースで検証する。このために、設定情報とシステム構成から、文書の流通・伝達経路を表わす情報漏洩パス検証モデル(LPAS-モデル)を作成する。LPAS モデルと設定検証ポリシーとのマッチングにより、元になったアクセスポリシーが正しく適用されているかを判定する[3]。これにより、課題２を解決する。

また設定検証部は、設定がアクセスポリシーを満たしていない場合にその原因となっている設定情報を特定し、保守を促す。これにより、課題３を解決する。

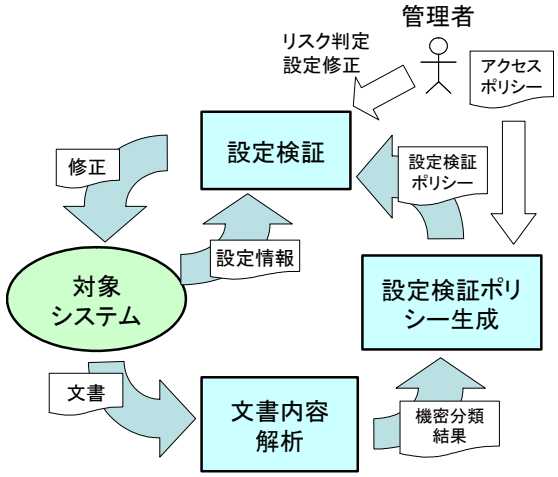

図 2　情報漏えい脅威分析方式

５．まとめ

本方式により、従来セキュリティ管理者に多大な負担を強いていた（１）機密情報の洗い出し（状況把握）、（２）機密文書がアクセスポリシーにあわせ管理されているかの検証（監査、状況把握）、（３）不備が発見された場合の対策検討（保守）、のコストが大幅に削減され、PDCA サイクルの実施が容易になる。セキュリティ脅威分析、情報漏洩監査、文書管理支援等への適用が有望と考えられる。今後、本方式の試作・性能実証を進めていく。

６．参考文献

[1] ISMS 適合性評価制度, http://www.isms.jipdec.jp/

[2]細見他，文書内容解析と設定検証に基づく情報漏洩脅威分析方式 (2)文書内容と構造解析を用いた機密情報分類、第 67 回情報処理学会全国大会，3E-7，2005

[3]榊 他，文書解析と設定検証に基づく情報漏洩脅威分析方式 (3)設定検証を用いた不正アクセス経路発見，第 67 回情報処理学会全国大会，3E-8，2005