3E-8

文書解析と設定検証に基づく情報漏えい脅威分析方式 (３)設定検証を用いた不正アクセス経路発見

榊　啓　　矢野尾　一男　小川　隆一　細見　格

NEC インターネットシステム研究所

１．はじめに

機密情報の漏洩防止は、情報セキュリティ上の大きな課題となっている。多様なプラットホームから構成される現在のオープンシステムでは、情報漏洩対策として情報セキュリティ管理システム(ISMS)のセキュリティサイクルを導入する必要があるが、監査・運用・保守のプロセスの多くを人手に頼っているのが現状である[1]。

本稿では、情報漏洩を防止するための監査・保守のプロセスを支援する情報漏洩パス検証方式(LPAS)を提案する。本方式は、対象とするシステムが、与えられたアクセスポリシー通りに設定されているかどうかを検証し、情報漏洩につながる設定の不備を指摘することで、監査・保守に必要な負担を削減することを目的とする。

２．設定検証の必要性と課題

情報漏洩を防止するためには、アクセス制御機構などの防止対策がアクセスポリシーを満たしているかどうかを監査し、保守することが必要である。アクセス制御機構とは、文書や、ネットワークへのアクセスの可否を判定する手段であり、OS のファイルアクセス制御、ファイアウォールによるフィルタリング、アプリケーション独自のファイルアクセス制御やフィルタリング等をさす。アクセスポリシーとは、誰がどのような条件でどの文書にアクセスしてよいかを記述したセキュリティ要件である。ここで、条件とは「ネットワークアクセスには暗号化プロトコルを使用する」というようなアクセス方法の条件である。

一般的なシステムは、複数のアクセス制御機構から構成され、異なるアクセス制御機構の下では、同一の文書やユーザが異なる名前で管理されることもある。このようなアクセス制御機構の設定が、すべて正しいかどうかを人手で監査するには工数がかかり、間違いが生じやすい。

そこで、全ての監査対象のアクセス制御機構の設定を集め、アクセスポリシーを満たしているかどうかを検証する手段が必要であり、これを実現するために、次の課題を解決する必要がある。

１．複数のアクセス権設定やフィルタリング設定を統一して取り扱うモデルの実現

２．暗号化経路などの条件を指定したアクセスポリシーと、複数の設定を比較検証するアルゴリズムの実現

これらの課題を解決するために、複数の設定を基に文章が流通する経路を表現したモデル(LPAS モデル)を作成し(課題１)、LPAS モデルがアクセスポリシーを満たすかどうかを検証する(課題２)情報漏洩パス検証方式を提案する。

３．情報漏えいパス検証方式(LPAS)

LPAS は、図１に示すように、対象とするシステムの設定情報から LPAS モデルを生成するモデル生成部、アクセスポリシーと構成情報から設定検証ポリシーを生成する設定検証ポリシー生成部、生成されたモデルが設定検証ポリシーを満たすかどうかを判定する情報漏洩パス検証部から構成される。

設定検証ポリシーとは、アクセスポリシーと LPAS モデルとを比較検証するために、アクセスポリシーを対象システムの構成情報を用いて具体化したものである。構成情報とは、文書や、ユーザ、サービスといったシステムの構成要素に、その属性(文書分類、ユーザの役職、暗号化の有無等)を対応付けたものである。

検証の結果、モデルがポリシーを満たさない場合、情報漏洩パス検証部は、修正案を提示する。これにより、ユーザは、簡単に設定不備を修正できる。

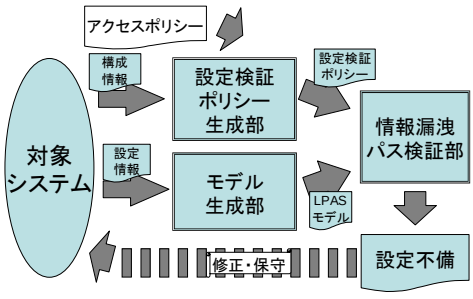

図 1　LPAS の概要

３．1. LPAS モデルの生成

モデル生成部では、複数の設定を統一的に扱うために、対象システムの設定を収集し LPAS モデルを生成する。LPAS モデルは、ファイアウォールや、サーバ・クライアントの設定によって起こりうる文書の流通経路を表わす有向グラフである(図２)。

An Information Leakage Risk Evaluation Method Based on Sensitive Document Detection and Security Configuration Validation: (3) Security Configuration Validation

Hiroshi SAKAKI, Kazuo YANOO, Ryuichi OGAWA, Itaru HOSOMI

Internet Systems Research Laboratories, NEC Corporation

図２を参照すると、LPAS モデルは、ユーザ ID を表わすユーザノード(U)、文書の格納場所(パス、URL)を表わすファイルノード（F）、ネットワークストリームや、フィルタ設定を表わすネットワークノード(N)と、それらをつなぐアークからなる。

モデル生成部では、アクセス制御機構ごと(図２の破線囲み部)にノードとアークを作成する。

アークには、情報伝達アークと別名定義アークがある。情報伝達アークは、アクセス制御機構によって許可される文書の流れを表し、アクセス権設定のうち read 権限と write 権限をアークの向きで表わす。別名定義アークは、複数のアクセス制御機構により異なる名前で管理されるファイルや、ユーザを対応付ける。例えばウェブサーバの設定により、ファイル「/secret/index.htm」（図２の F1)とファイル「http://example.com/secret/index.htm」（図２の F2)とが同一の文書をさし示しているとき、この 2 つのノードを別名定義アークで結ぶ。また、アプリケーションの認証ユーザ「sakaki」（図２の U2)が OS では、ユーザ「apache」（図２の U1)として扱われるときには、U1 と U2 を別名定義アークで連結する。これにより、F1 へアクセスができるかどうかを判定するためには、F1, U1 および、F2, U2 の間の情報伝達アークを調べる必要があることが分かる(図２の角丸四角部)。

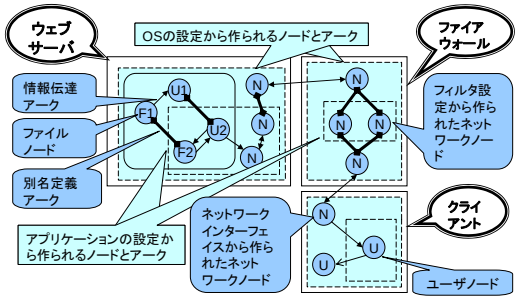

図 2　LPAS モデルの具体例

３．２．設定検証ポリシー

設定検証ポリシーとは、アクセスポリシーを検証対象システムの構成情報を用いて具体化したものであり、あってはならない文書の流れをアクセス先のファイル、アクセス元のユーザ、アクセス経路によって記述する。ここで、アクセス経路は、文章が通る経路上のノード列を、正規表現を用いて定義したものである。例えば「機密ファイルは、クライアントのユーザが、暗号化された経路以外を用いて、読んではいけない」という意味のアクセスポリシーが与えられた場合は、構成情報の「"/secret/index.htm"が、機密ファイルである」と、「ウェブサーバは 80 番ポートを利用して暗号化されていない通信を行う」とを用いて、「ファイルノード"/secret/index.htm"から 80 番ポートを表わすネットワークノードを経由して、クライアントのユーザノードにいたる経路」を表わすノード列を設定検証ポリシーとして作成する。

３．３．情報漏洩パスの検出

情報漏洩パス検証部では、LPAS モデルと、正規表現で書かれた設定検証ポリシーとのマッチングをとり、情報漏洩の可能性のある経路を検出する。初めに、別名定義に従って文書へのアクセスの可否を判定し、複数のアクセス制御機構によるグラフを情報伝達アークだけから構成されるグラフで置き換える。次に、有向グラフ上で、正規表現で書かれた経路を探索するアルゴリズムを用いて、LPAS モデルから設定検証ポリシーで書かれた経路を探索する。正規表現にマッチする経路がある場合には、経路に含まれるネットワークノードのフィルタリング情報を用いて、経路が遮断されているかどうかを判定する。遮断されていない場合は、その経路を情報漏洩パスと判定する。

４．実験

LPAS のプロトタイプを実装した。まず検証対象機器に LPAS エージェントを配置し、OS やサーバの設定情報から LPAS モデルを生成する。次に検証サーバで、画面上で入力されるアクセスポリシーを、文書解析[2]で作成した構成情報を用いて設定検証ポリシーに変換し、生成した LPAS モデルとのマッチングをとる。情報漏洩パスが検出された場合、漏洩対象ファイルと、設定不備の可能性のある設定ファイルとその対策を画面に表示する(図３)。

図 3　検証結果

５．まとめ

LPAS の方式概要と試作について報告した。本方式により、複数の設定がアクセスポリシーを満たしているかの検証や、不備のある設定の発見・修正が簡単に実施でき、情報漏洩防止のための監査・保守コスト削減が期待できる。

参考文献

[1]小川 他, 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の概要、第67回情報処理学会全国大会, 3E-6, 2005

[2]細見 他, 文書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