L-028

セキュア・プラットフォームの研究開発(5) システム運用ポリシー遵守チェック
Research and development of Secure Platform (5) Analysis of compliance with system operation policy

寺田 剛陽† 長谷部 高行 † 畠山 卓久† 徳谷 崇†
Takeaki Terada Takayuki Hasebe Takahisa Hatakeyama Takashi Tokutani

1. まえがき

セキュア・プラットフォームの研究開発[1]では、企業のシステム全体のアクセス制御ポリシーの生成、配付を一カ所で統合管理する仕組みを提供することにより、ITセキュリティの強化を実現している。

さらに IT ガバナンスの観点からは、アクセス制御ポリシーが統制ルールに従っているかを適宜確認し、修正していくことが重要である。これらの確認は、通常は人手による確認となり、コスト増大の要因となっている。

本論文では、ポリシー管理者の負担を低減するための機能として、各システムにおけるアクセス制御設定と、統制ルールとの整合性をチェックし、その結果を可視化するポリシー遵守チェック機能を開発したので、これを報告する。

2. 本研究のねらい

ポリシー管理者が配付するポリシー(アクセス制御設定)が、職務分掌や最小権限などのアクセス管理に関する統制ルールに従っているかを定期的にチェックすることで、ポリシーの修正・削除を支援するツールを提供する。

3. 要件

セキュア・プラットフォームの統合アクセス制御情報管理機能（IAM）[2]では、統合 ID 管理機能（IdM）と連携してアクセス制御ポリシーを生成し、各システムのプラットフォームに応じた形式に変換後、配付する。

ここで、システムが職務分掌や最小権限などのアクセス管理に関する統制ルールを遵守した動作をするための 2 つの要件について述べる。

1) システム運用ポリシーの遵守

アクセス制御ポリシーは企業内の組織再編や従業員の異動に合わせて常に更新していく必要がある。しかし、更新後のポリシーが常に適切であるとは限らず、統制ルールにおける職務分掌や最小権限に違反する場合がある。具体的には、ユーザに対するロールの設定ミス、ロールに対する権限の設定ミス、さらにはユーザに対するロールの設定と、ロールに対する権限の設定の連携の不具合などである。

連携の不具合の例を挙げる。顧客 A の情報と顧客 B の情報を同一のユーザが保持してはならないという統制ルールは、IdM のユーザ-ロール設定、IAM のロール-権限設定の連携が正しく行われないと実現できない。

上記の違反を発見するには、IdM のユーザ-ロール管理機能と IAM のロール-リソース管理機能の連携を支援するしくみが必要である。

2) アクセス制御ポリシーの適切な利用

生成時は統制ルールを遵守していたアクセス制御ポリシーも、ビジネス環境の変化に伴うシステム再編後、使用されてない権限が存在するなど、不適切となっている場合がある。このようなポリシーは早急に内容の更新・廃止を行わなければ、最小権限の統制ルールに違反することになり、漏洩事故発生時には業務上把握していなかった機密情報まで流出する危険性がある。したがって、使われていない権限は最小権限の統制ルールの立場から更新・削除する必要がある。

4. 解決手段

前節 1) の解決手段として、本研究では統制ルールをアクセス制御ポリシーのチェックに直接利用できる形式で表現し（以後、システム運用ポリシーとよぶ）、IdM、IAM の設定情報を収集し、ルールを用いてこれらの設定情報のチェックを可能にした。

前節 2) については、アクセス統制管理下の各システムのアクセスログと設定されたアクセス制御ポリシーを照合することで、不要な権限を検出した。

さらに本研究では、上記のチェック結果を既存のグラフ表示ツールなどで利用できるようにするための出力形式を定義した。

4.1 システム構成

上記の解決手段をふまえ、本研究では以下の機能をもつコンポーネントを開発した。

1) システム運用ポリシー遵守チェック機能
   職務分掌などの統制ルールを反映したシステム運用ポリシーを、アクセス制御ポリシーが遵守しているかをチェックする機能。
2) アクセス制御ポリシー利用状況チェック機能
   システムに適用済みのアクセス制御ポリシーの利用状況をチェックする機能。

図 1 に本コンポーネントのシステム構成を示す。ポリシーチェック機能は、定期的に IdM から ID 情報、IAM のポリシー生成・配付機能からアクセス制御ポリシー、統制管理下のサーバシステムからアクセスログを収集してチェック対象情報記憶部に格納する。チェック処理エンジンでは上記 1) 、2) のチェックを行い、結果を既存のグラフ表示ツールなどで利用できるよう、csv などの汎用的な形式で記憶装置に格納する。

次節では 機能 1) と 2) の処理について説明する。

† 富士通株式会社, FUJITSU LIMITED

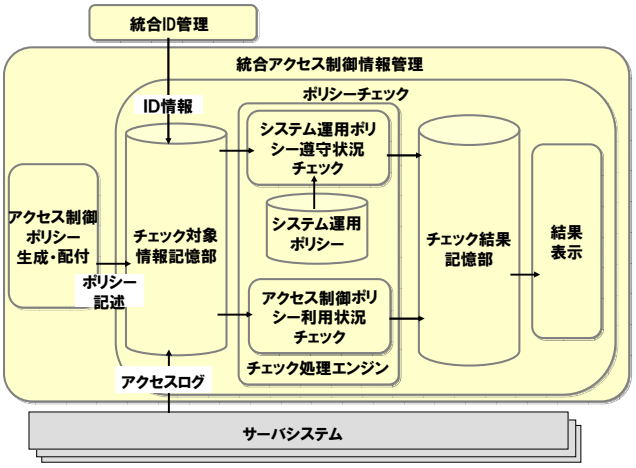

図 1 ポリシーチェック機能のシステム構成

4.2 システム運用ポリシー遵守状況チェック処理

本処理では、以下のステップによりチェックを行う。

・チェック対象情報の正規化処理

本処理では、システム運用ポリシー遵守チェックで必要な情報をチェック対象情報から取り出す。本開発では、システム運用ポリシーのうち、職務分掌に関する統制ルールの 1 つとして、同時付与を禁止するリソースの組合せ を定義した。これは第 3 節の 1) の違反例に相当する。これをチェックするには IAM のアクセス制御ポリシーと IdM の ID 情報を用いる。

・チェックと結果の出力

チェックと結果の出力では、チェック対象情報をシステム運用ポリシーと照合したのち、違反となるアクセス制御ポリシーとそのユーザをチェック結果として出力する。表 1 にシステム運用ポリシーの一種である職務分掌ルールの例を示す。

表 1 職務分掌ルール（1 人のユーザへの権限 1 と権限 2 の同時付与を禁止）の例

職務分掌ルール	権限 1		権限 2	
	アクション	リソース	アクション	リソース
業界 A 顧客コンサル分担	Read	顧客 C 社秘密情報	Read	顧客 D 社秘密情報
システム B の開発と運用の分掌	Any	システム B 開発環境のデータ	Any	システム B 本番環境のデータ
出荷業務と経理業務の分掌	Write	出荷データ	Write	売掛金データ
:	:	:	:	:

4.3 アクセス制御ポリシー利用状況チェック処理

本処理では、以下のステップによりチェックを行う。

・チェック対象情報の正規化処理

本処理では、アクセス制御ポリシー利用状況チェックで必要な情報をチェック対象情報から取り出す。これをチェックするには IAM のアクセス制御ポリシーと IdM の ID 情報に加えて、運用中のシステムのアクセスログを用いる。

・チェックと結果の出力

運用中のシステムのアクセスログと配付中のアクセス制御ポリシーを比較し、利用されていない権限およびアクセス制御ポリシーを検出する。本処理では、前節で述べたチェック対象情報記憶部に含まれているポリシーと、各システムのアクセスログ中のポリシーを、ポリシーID のレベルで照合する前処理を行うことでチェックの高速化を図る。

5. 評価

本機能により IdM・IAM を利用した、確実なアクセス統制を低コストで実現することが可能となる。

本機能の想定利用形態は IAM のポリシー管理者による配付ポリシーの定期チェックである。遵守状況チェックはアクセス制御ポリシーの生成・配付時、利用状況チェックは月に 1 回の頻度でのチェックを想定している。

実測値に基づき、従業員数 3000 人・アクセス制御ポリシー数 100 件、アクセスログ数 100000 件／日の企業モデルで試算を行った。

・システム運用ポリシー遵守チェック機能

チェック処理時間=1200(sec)=20 分

・アクセス制御ポリシー利用状況チェック機能

1 ヶ月分のチェック処理時間=40000(sec)=11.6 時間

上記結果から、冒頭の性能要件を満たす見込みが得られた。よって従来、手作業での確認を強いられていた、ポリシーの統制ルール遵守チェックおよび利用状況のチェックを効率化することが可能になった。

6. おわりに

本研究では、アクセス制御ポリシーの統制ルール遵守状況と、各システムにおける当該ポリシーの利用状況をチェックし、その結果を可視化するポリシー遵守チェック機能を開発し、有意な時間でチェックを実施できることを確認した。

謝辞

本研究の一部は、経済産業省から技術研究組合 超先端電子技術開発機構(ASET)へ委託されている「平成19年度セキュア・プラットフォームプロジェクト」の成果である。

参考文献

[1] 徳谷 崇，畠山 卓久，相澤 泰介，栗田 享佳，五十嵐 功，小川 隆一，小谷野 修，"セキュア・プラットフォームの研究開発 (1) アーキテクチャ", FIT2009, Sep 2009.

[2] 森田 陽一郎，中江 政行，小川 隆一，"セキュア・プラットフォームの研究開発 (2) アクセス制御ポリシー生成・配付", FIT2009, Sep 2009.