L-001

システム運用管理情報と連携した不正アクセス検出方式の検討
Study of unauthorized access detection methods linked to system operation management information

和田 清美† 増田 峰義†
Kiyomi Wada Mineyoshi Masuda

1. はじめに

パブリッククラウドはリソース利用の柔軟性によりシステム構築や更新が頻繁にできるため，悪意のない作業がセキュリティインシデントと誤認される機会が増え，セキュリティチームがシステム運用チームに運用作業によるものか確認する業務負荷が高くなる。

本研究は，システム運用管理者が利用する運用プロセス自動化基盤に，昇格アクセスの正当性を自動判定するフレームワークを提案する。これによりセキュリティリスクの高い操作でも正当な操作はインシデント対応不要にする。

2. 従来方式と課題

2.1 セキュリティ運用ユースケース

セキュリティ基準の標準 ISO27002，業界別の基準 PCI DSS，FISC(金融系)，NIST の CSF(サイバー攻撃対策)など個別に定義されているが，セキュリティ運用項目として共通点が多い。そこで，コンプライアンス・セキュリティ基準を順守するために必要な項目を体系化し，優先度が高いユースケースを特定する。

図 1 は，セキュリティ運用の体系化の方法である。フレームワーク共通で対策すべき項目のベースを米国の CIS(Center for Internet Security)が提供する「CIS Controls v8」とし，これに他のセキュリティフレームワーク(CSF, PCI DSS, ISO27002:2022)をマッピングした。

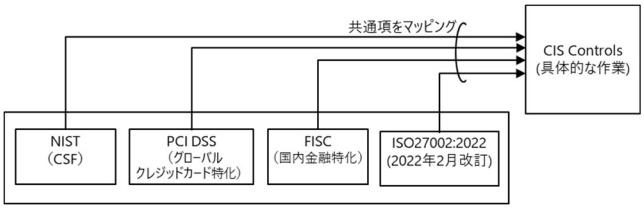

図 1 セキュリティ運用の体系化

表 1 は，CIS Controls の 18 項目のなかで，他のセキュリティフレームワークと共通の保護策，及び CIS Community Defense Mode に基づく脅威に対する防御効果の高い保護策の合計数のランキングである。上位の項目は，アクセス制御管理であり，関連性が高いのはアカウント管理とインシデントレスポンス管理であることから，優先度の高いユースケースとして「昇格アクセス作業」と「不正な昇格アクセス検知とインシデント対応」を検討することにした。

表 1 Control 別要件に対する保護策のランキング

ランキング	CIS Controls		他フレームワークと共通数 (ISO27002, PCI DSS)	脅威に対する防御効果	合計
1	06	アクセス制御管理	4	6	10
5	05	アカウント管理	2	3	5
7	17	インシデントレスポンスと管理	3	0	3

†株式会社 日立製作所，Hitachi, Ltd.

2.2 課題

パブリッククラウド環境のシステムは，あらゆるところから侵入される可能性があるため，システム各所で異常な挙動を検知しアラート通知する。その結果，セキュリティ管理者は大量のアラートに対して，承認済みアカウントによる操作かを確認しなければならないため，アラート処理に時間をとられて本当に見なくてはならないアラートを見過ごしてしまう可能性がある。

そこで，SIEM(Security Information and Event Management)が昇格アクセスと検知したアラートに対して，事前承認済みアカウントによる操作かどうかを自動判定する。従来技術[1]は，作業計画とイベントログを照合する。

ここでの課題は，作業計画に対して実作業で追加の対応や想定外の作業が発生すると，必要なシステム運用作業であってもアラートが不正アクセスと判定されてしまうことと，個々の運用自動化フローを作成する度に，昇格アクセスの正当性判定処理を作らなければならないことである。

3. 提案方式

2.2 節の課題を解決するため，作業計画を遂行するための一時昇格アクセス付与した実作業ログと，SIEM が検出した昇格アクセスとを照合して，昇格アクセスの正当性判定を自動化する。提案方式の運用プロセス自動化基盤は，「昇格アクセス作業データ登録」と「昇格アクセスの正当性判定」のフレームワークと自動化ワークフローからなる。フレームワークが不正な昇格アクセスをチェックしてくれるので，個々の運用自動化ワークフローを作成する人は，昇格アクセスの正当性判定処理を作る必要がない。

3.1 昇格アクセス作業データ登録

図 2 は，フレームワークによる昇格アクセス作業データ登録の流れである。作業者は①運用作業を申請すると，②昇格アクセス権限の要否を判定し，③昇格アクセス要なら昇格アクセス作業 DB に登録し，④承認者に承認要求し，⑤昇格アクセス作業 DB に承認結果を格納する。

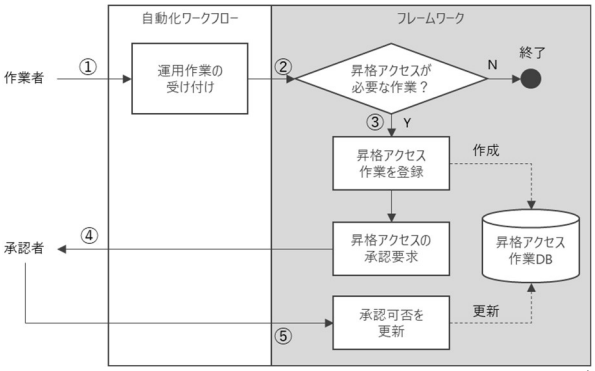

図 2 フレームワークによる昇格アクセス作業データ登録の流れ

3.2 昇格アクセス正当性判定

図 3 は，フレームワークによる昇格アクセスの正当性判定の流れである。昇格アクセス作業 DB に登録された承認済み作業は，①自動的に一時昇格アクセス権限が付与され，②実作業ログは昇格アクセス作業 DB に格納される。不正アクセスと検知されたアラートは，③承認済み昇格アクセス実作業と照合し正当性を判定する。また，不正アクセスであれば，④インシデント登録，初動調査に必要な情報を収集し，⑤セキュリティ管理者に通知する。

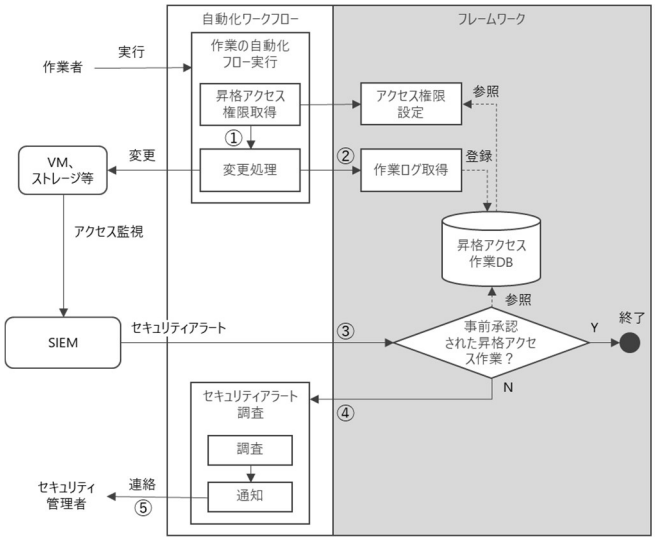

図 3 フレームワークによる昇格アクセスの正当性判定の流れ

図 4 は昇格アクセスの正当性判定処理と使用されるデータである。判定処理は，アラートの発生時間と昇格アクセス作業の時間帯，ユーザ，アクセス元(ソース IP)とアクセス先(リソース名)を照合する。

入力：アラートテーブル

項目	カラム名
イベントID	eventId
発生日時	eventTime
ユーザ名	userName
リソース名	resourceName
ソースIP	sourceIP
アクセス正当性	approved

入力：運用作業テーブル

項目	カラム名
ワークフローID	workflowId
承認	approved
作業時間	requestedDuration
開始日時	startTime
ユーザ名	userName
ソースIP	sourceIP
リソース名	resourceName

判定処理：アラートに対して以下の条件を満たす運用作業を抽出し、あれば正当、なければ不正と判定

```
Select * from 運用作業テーブル where
    【条件1】開始日時 < イベント発生時間 AND
    【条件2】開始日時+作業時間 > イベント発生日時 AND
    【条件3】ユーザ名 = イベントのアクセス元ユーザ AND
    【条件4】ソースIP = イベントのソースIP AND
    【条件5】承認済み作業 = True AND
    【条件6】アクセス先リソース名 && イベントのアクセス先リソース名
```

リソース名は複数あるため、配列型とし、配列要素が一部でも重なる場合は正当と判定する

図 4 昇格アクセス正当性判定方法

4. 実験方法

昇格アクセス作業ワークフローと昇格アクセス正当性判定処理に対する実現性検証を行う。

図 5 は検証システム構成である。Amazon Web Services 環境で「SIEM on Amazon OpenSearch Service」を構築し，操作ログに対するイベント情報などを取得して検証する。

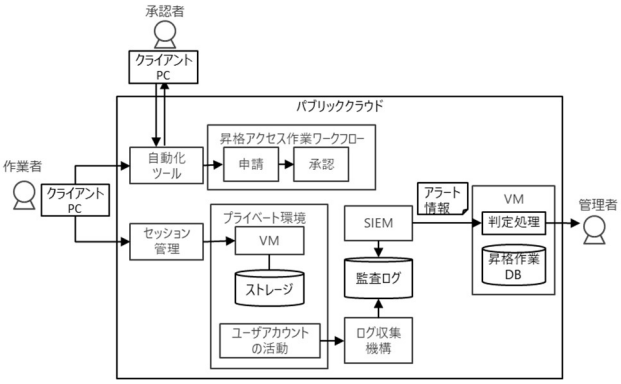

図 5 検証システム構成

5. 結果と考察

昇格アクセス作業ワークフローは，図 5 のワークフローで申請，承認後，自動昇格アクセス権限付与ができることを確認した。昇格アクセス正当性判定処理は，「SIEM on Amazon OpenSearch Service」の操作ログからアラートを生成し，判定できるか確認した。図 6 は判定処理の結果である。アラート発生時，事前承認済み作業と照合し，承認済み作業を検出できた。以上より，昇格アクセス作業ワークフローと昇格アクセス正当性判定のワークフロー別の実現性を検証できた。

入力：operationsテーブル

id	approved	userName	resourceName	sourceIP	startTime	requestedDuration Time	endTime
1111	t	wada	{arn:aws:s3:::example-bucket}	x.x.x.x	2023-02-15 08:30:00	01:00:00	
2222	t	kiyo	{arn:aws:s3:::example-bucket}	x.x.x.x	2023-02-15 08:30:00	01:00:00	

入力：alertsテーブル

id	eventTime	userName	resourceName	sourceIP
1234	2023-02-15 09:00:00	wada	{arn:aws:s3:::example-bucket/exampleFile.txt, arn:aws:s3:::example-bucket}	x.x.x.x

判定処理

```
postgres=# ¥set eventTime ''''2023-02-15T09:00:00''''
postgres=# ¥set eventUserName ''''wada''''
postgres=# ¥set eventResourceName ARRAY[''''arn:aws:s3:::example-bucket/exampleFile.txt'''', ''''arn:aws:s3:::example-bucket'''']
postgres=# ¥set eventSourceIP ''''x.x.x.x''''
postgres=# select * from operations where (startTime < :evetime) AND (startTime+requestedDurationTime > :eventTime) AND
(username = :eventUserName) AND (sourceIP = :eventSourceIP) AND (approved = true) AND
(resourceName && :eventResourceName);
```

出力：operationテーブル(アラートと適合した作業)

id	approved	userName	resourceName	sourceIP	startTime	requestedDuration Time	endTime
1111	t	wada	{arn:aws:s3:::example-bucket}	x.x.x.x	2023-02-15 08:30:00	01:00:00	

図 6 昇格アクセス正当性判定結果

6. おわりに

本報告では，システム運用管理者が利用する運用プロセス自動化基盤に，昇格アクセスの正当性を自動判定するフレームワークを提案し，実環境で SIEM のアラートが昇格アクセス作業かどうか自動判定できることを確認し，セキュリティリスクと業務負荷を低減できる見込みを得た。

商標について

Amazon Web Services は米国およびその他の国における Amazon Technologies, Inc.の登録商標である。

参考文献

[1] 榊原裕之, 岩崎亜衣子, 河内清人, “作業情報等に基づく重要インフラのサイバー攻撃検知について”, IPSJ SIG Technical Report, Vol.2017-CSEC-76, No.29 (2017).