5B-05

情報システムのアクセス制御における通行履歴の活用

○小宮 崇†

三菱電機株式会社　情報技術総合研究所 †

1. はじめに

近年の情報社会化に伴い、多くの企業では業務システムやファイルサーバ等の情報コンテンツに対して利用者の権限に応じたアクセス制御等を行うことにより、業務内容に合わせたコンテンツの活用と不正利用の防止を実現している。

本論文では、そのアクセス制御方式の 1 つとして、入退室管理システムが提供する通行履歴を用いたアクセス制御方式について提案する。

2. 背景・課題

従来の情報コンテンツへのアクセス制御では、業務システムへのアクセスやファイルサーバ上のファイル読み書き等を、利用者の業務内容に合わせて制限する設定を行っている[1]。

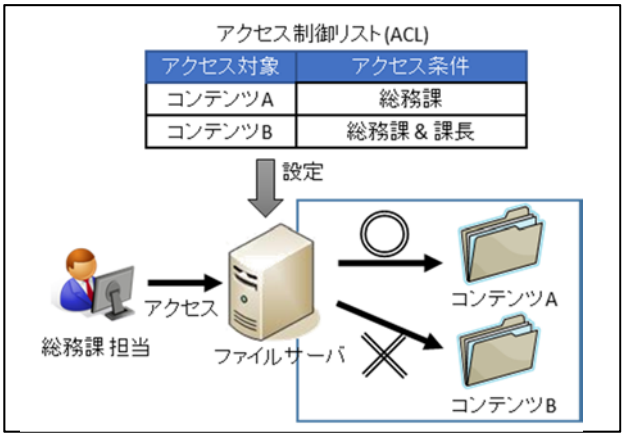

図 1　情報システムのアクセス制御

図 1 は従来のアクセス制御について図示したものであり、総務課の担当者がファイルサーバへアクセスした場合に、アクセス制御リスト(ACL)に記述された条件に従いアクセス制御を行った結果、コンテンツ A へのアクセスは許可されるが、コンテンツ B へのアクセスは拒否されることを示したものである。

更なるセキュリティを確保するための手法として、アクセス条件に使用 PC やアクセス元の部屋等の物理的な情報を追加するにより利用形態を限定することで正しい利用方法を強制する方式や、再度ユーザ認証を要求したり他の認証方式を要求したりすることで認証レベルを引き上げ、利用者本人であることを特定して成りすましを防止する方式も用いられている。

しかし、これらの方式では、その時点での利用者本人の情報のみだけを使用するものであるため、アクセス制御の内容が固定的という問題があり、その解決のためには状況に合わせた柔軟な設定の実現が課題となっていた。

3. 通行履歴の活用

課題の解決策の 1 つとして、入退室管理システムが提供する通行履歴の活用を提案する。従来でも情報システムと入退室管理システムの連携したソリューションは存在し、入退室管理システムが提供する通行履歴から得た現在位置によるアクセス制御を実現しているものがある[2]。

通行履歴は、どこを誰がいつどのような方法で通過したかを示す情報である。1 つの情報ではその時点の 1 人の行動しか特定できないが、これを蓄積することにより、その入退室管理システムが適用されている範囲における全ての利用者に対して、現在の居場所だけでなく、その場所に入ってからの経過時間や以前入ったことがある場所等の情報も取得可能である。本提案は、この利用者の現在地以外の情報についてもアクセス制御に活用するものである。以降、通行履歴から特定した利用者の過去から現在までの居場所の情報を在場情報と呼称する。

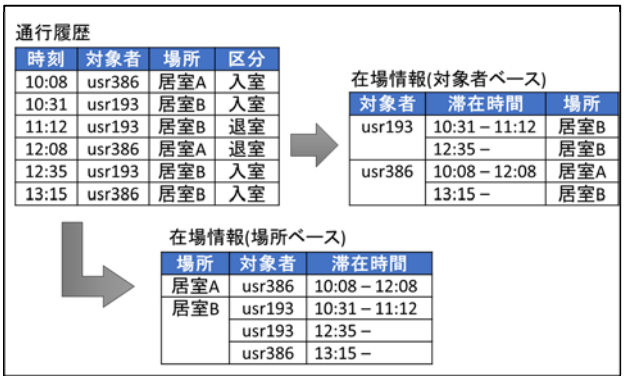

図 2　通行履歴からの在場情報生成

図 2 は通行履歴から在場情報を得る例を図示したものであり、通行内容を示す通行履歴から、利用者がどこに居ついたかを示す対象者ベースの在場情報と、その部屋にいつ誰が居たかを示す場所ベースの在場情報の例を示している。

また、通行履歴を利用する利点として、場所が確実に特定できる点がある。GPS の普及により、これを用いて場所を特定する機会が多くな

Access Control Method of Information System Using Passage History
†Takashi Komiya,
Information Technology R&D Center, Mitsubishi Electric Corporation

っているが、利用可能な範囲は GPS の電波が受けられる場所に限定されるため、電波の入りづらい屋内や地下では利用できない。その点、通行履歴は入退室時に必ず出力されるため、確実に利用者の場所を特定可能である。

4. 情報システムのアクセス制御への適用

情報システムのアクセス制御への、在場情報の適用方法について例を挙げる。

本例では、情報システムのアクセス制御を判定する認可サーバから独立した形で、入退室管理システムから提供される通行履歴を用いて在場情報を作成し、それの管理と提供を行う在場情報管理サービスを構築する形式とした。在場情報として取得可能な情報には、特定の利用者の現在と過去の居場所と入退室時間、特定の部屋の現在と過去の在室者と入退室時間の情報を想定している。

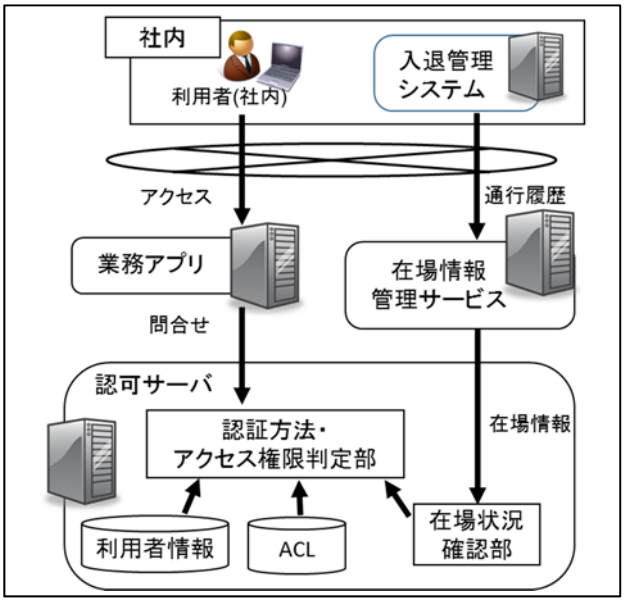

図 3　通行履歴を活用したアクセス制御

図 3 は通行履歴を活用したアクセス制御の構成例を示したものであり、認可サーバが業務アプリ上のコンテンツへのアクセス権限判定を行う際に、該当のアクセス制御リスト(ACL)に在場情報が設定されている場合には在場情報管理サービスから在場情報を取得して判定を行うことを想定している。

判定の結果、合格した ACL が複数ある場合に、より大きな権限を適用する、低い方の認証レベルを採用する等により、在場情報によって適用される権限の変更することも可能である。

在場情報を活用することにより可能となるアクセス制御の例を挙げる。

- 設定例 1：入室したまま 3 時間以上経過した場合には、再度認証を要求する。
  - 定期的に再認証させることで成りすましを防止。
- 設定例 2：退室後 10 分以内に戻ってきた場合には、簡易な認証で利用可能とする。
  - トイレ休憩等を想定。
- 設定例 3：同じ部屋に課長以上の役職者が現在居る場合にコンテンツへの書き込みを許可する。
  - 役職者によるダブルチェックを必要とする、機密の高いコンテンツを想定。

このようなアクセス制御が可能となる。これらの設定例を表 1 に挙げる。

表 1　在場条件を設定したアクセス制御リスト

対象	ID	認証レベル	適用権限	利用者条件	在場条件	過去在場条件
設定1	01	レベル1	読み書き	組織＝総務課		本人：入室から3時間以内
設定2	01	レベル2	読み書き	組織＝総務課	本人：居室A	(無し)
	02	レベル1	読み書き	組織＝総務課	本人：居室A	本人：10分以内に再入室
設定3	01	レベル2	読み	組織＝総務課	本人：居室B	(無し)
	02	レベル2	読み書き	組織＝総務課	本人：居室B & (組織＝総務課 &役職=課長) ：居室B	(無し)

以下に、設定内容について説明する。

- 設定 1 は、過去条件に、入室時間が 3 時間を超えた場合には再認証を促すように設定している。
- 設定 2 は、2 つの ACL を使用し、過去条件の「10 分以内に再入室」を満たせた場合には認証レベルが低い、ID が 02 の ACL を選択させることで、10 分以内に戻った場合には認証レベルを落とすように設定している。
- 設定 3 は、在場条件に役職者を設定することで、役職者が同室する場合のみ書き込みを許可するという条件を設定している。

このように通行履歴から作成した在室情報を活用することにより、現在よりも高度な情報コンテンツへのアクセス制御を実現可能となる。

5. おわりに

今後は、実際に適用した実験により、利用シーンの再確認や性能評価を行い、改善を重ねる予定である。

参考文献

[1] 情報処理推進機構,「アクセス制御に関するセキュリティポリシーモデルの調査」, https://www.ipa.go.jp/security/fy16/reports/access_control/policy_model.html,2005

[2] 勝山,濱田,大沼,佐藤,「“企業の安心・便利を支えるクラウド ID 管理サービス“DIASMILE”」,2013,三菱電機技術報告,2013 年 07 月号,p27