

エージェントを用いた セキュアウェブアプリケーション

能登研究室

野崎正臣 (200046075)

1 はじめに

近年、電子ネットワークの普及に伴い、Web シラバスなどの Web アプリケーションも普及している。同様に注目を集めているエージェントとは、仮想的な主体によって人間の情報処理を代行させるための技術の総称であり、近年のノート PC、携帯電話を始めとする携帯情報機器やネットワークインフラの充実によってその応用範囲と可能性が拡大している。

本研究では既存の Web シラバスに、エージェントを用いて利用者の個人情報扱うことで、履修登録や授業情報の掲示などの機能を追加した学業支援システムを提案するが、このシステムには、個人情報という守るべき情報を利用することからセキュリティが必要となる。これらから Web アプリケーションの安全性向上を目的とし、エージェントの構造的特徴とセキュリティの考え方を基に、学業支援システムのセキュリティ強化を行った。

2 セキュリティ

セキュリティの基礎概念として、暗号化、証明書、認証、デジタル署名が挙げられる。個々のソフトウェアの開発者がソフトウェアの持つすべての機能をプログラミングするのは困難で無駄が多いため、多くのソフトウェアが共通して利用する機能は、OS やミドルウェアなどの形でまとめて提供されている。個々の開発者は規約に従ってその機能を「呼び出す」だけで、自分でプログラミングすることなくその機能を利用したソフトウェアを作成することができる反面、セキュリティの類似・同一化と構造解析の危険性が存在する。

これらを考慮し、本研究のセキュリティ強化は、主に認証の基礎概念を用いてエージェントにセキュリティルールを与えることにより、エージェントの自律性を利用した構造解析回避を行い、ルール定義の幅広い適応性を利用することで類似・同一化を防ぐことにした。

不正利用可能となりうる要因を以下に示す。

- ファイル名と拡張子が漏れた場合、特別な処理がされていなければプログラムソースなどが閲覧可能である。
- プログラムソース内にデータベースを利用するための情報が記載されている。
- データ（レポート）転送システムのデータ保存先が外部アクセス可能である。

不正利用・解析の対策を以下に示す。

- ファイル名なども、ID やパスワードと同様に外部に漏らさないようにする。
- 外部アクセス可能なデータに特殊な処理（暗号化や否オープンソース化など）が施されるようにする。

本研究では、対策の一つ目に対して、ホスト管理者が気をつける以外に無いので、対策の二つ目を試みた。

3 提案システム

提案する学業支援システムの構造を図 1 に、特徴を以下に示す。

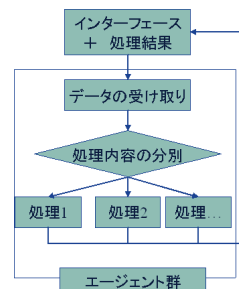


図 1: 基本システムフローチャート

- 履修登録や授業情報の確認が Web 上のどこからでもできる。
- データ転送システムが有り、閲覧及びダウンロードが可能である。

エージェントを用いたセキュリティシステムの特徴を以下に示す。

- 処理に一貫性を与えることで、プログラムの修正・追加が容易に可能である。
- エージェントにセキュリティルールを付けることで解析・不正利用を抑止できる。
- エージェントが稼働条件を満たしていれば、当システムの不正利用はできない。

本システムのセキュリティルールを以下に示す。

- エージェントに内部 ID を持たせ、その認証を行う。
- データ転送システムで用いられるデータに拡張子（及びファイル名）署名型チェックを行い、安全性を得る。

4 システムの考察

本システムを実際に用いて、外部 Web ブラウザ上からの解析について、従来のシステムとの比較結果を以下に示す。

- ソース及びファイルの不正閲覧が不可能になった。
- レポートデータの不正閲覧が不可能になった。

これらから重要情報（データベース関連情報及び、転送情報）の守秘に成功したといえる。また、従来のセキュリティ方法は汎用化するため、API を用いて機能を「呼び出す」ことで製作されている。それゆえ、構造解析による打破という可能性があるのに対し、本システムは外部からの構造解析ができないことから、セキュリティ構造解析の回避ができた。

5 おわりに

本研究による、エージェントを用いたセキュリティ解析の回避は有効であり、エージェントルールによる多重セキュリティの簡易作成ができ、セキュリティの類似・同一化も防ぐことができた。