金沢大学統合認証基盤における次世代認証へ向けた取り組み

仲山 悠也 [1)], 松平 拓也 [2)], 東 昭孝 [2)], 高田 良宏 [2)], 笠原 禎也 [1,2)]

1) 金沢大学大学院 自然科学研究科 電子情報科学専攻

2) 金沢大学 総合メディア基盤センター

nakayama@cie.is.t.kanazawa-u.ac.jp

Study on Next Generation Authentication for the Integrated Authentication Infrastructure in Kanazawa University

Yuya Nakayama[1)], Takuya Matsuhira[2)], Akitaka Higashi[2)], Yoshihiro Takata[2)], Yoshiya Kasahara[1,2)]

1) Graduate School of Natural Science and Technology, Kanazawa University

2) Information Media Center, Kanazawa University

概要

金沢大学では, Shibboleth を用いた金沢大学統合認証基盤を運用している. 現在は ID/パスワードによる認証を行っているが, 重要システムとの連携や規模の拡大に伴い, 今後のセキュリティ対策として次世代の認証方式について検討する必要がある. 次世代認証に求められる項目について整理し, 導入へ向けて検討を行った.

1 研究背景

金沢大学 (以下, 本学とする) では, 情報システムの融合化の一環として, 金沢大学統合認証基盤 (Kanazawa University Single Sign On (以下, KU-SSO とする)) を構築し, 平成 22 年 3 月から本格稼働を開始した [1].

それまで, 本学の情報システムは, 認証機構を含め各部署・部局が独自に構築・運用していたため, セキュリティ, コスト, ユーザの利便性の面で問題が指摘されていた. KU-SSO はミドルウェアに Shibboleth[2] を採用し, 一度の認証でユーザに許可された情報システムを全て利用可能とするシングルサインオンおよびユーザの属性情報を情報システム間で安全に共有する仕組みを提供している. これにより, 本学の各情報システムへの入り口として機能する「アカンサスポータル」をはじめとした約 30 の情報システム間をシームレスに利用可能となっている [3]. 現在では, 平日には 10,000 回を超える認証が行われ, 繁忙期には 1 日で 140,000 回を超えるなど, 学生や教職員など本学に関わる多くの人に利用されている [4, 5].

KU-SSO では, 現状 ID/パスワードによる認証を行っている. しかし, 人事給与, 財務, 評価などの重要な情報を扱うサービスも連携対象となっていることから, 今後, セキュリティ強度が高い認証機構の導入が必須である. しかし, むやみにセキュリティ強度を上げると, ユーザの利便性を損なうこととなり望ましくない.

そこで本研究では, 本学のユーザが KU-SSO をどのような環境で利用しているかの動向を調査・分析し, 認証システムのセキュリティ向上を図る上で, ユーザの利便性を損なわない認証方式の導入に向けて検討を行った.

2 次世代認証

本章では, 本学が現在導入を検討している認証方式について紹介する. また, その導入に向けた課題について整理する.

2.1 リスクベース認証

ユーザの環境情報や行動パターンを分析して, リスクを判定した上で認証を課すような認証方式は, リスクベース認証と呼ばれている. 一般的なリスクベース認証は, 次のような流れで行われる.

1. ベースとなる認証を行う
2. リスク判定のためのいくつかのチェック項目をテストする

3. それぞれのチェック項目に設定されているスコアを集計する
4. スコアがリスクのしきい値を下回れば認証成功とし, そうでなければブロック, もしくは追加認証をユーザに課す

リスク判定のためのチェック項目には, 認証の失敗回数や, 過去に利用しているデバイスとの比較, 位置情報や最終ログインからの経過時間を利用するものなどがある. これにより, あからさまに何度も認証に失敗している場合や, 突如遠隔地からのアクセスがあると不正アクセスのリスクが高いと判断される. 逆に, 普段通りにシステムを利用し, 不正アクセスのリスクが低いと判断されれば, ユーザは最初に課されるベースとなる認証を通過するだけで良い.

つまりリスクベース認証は, ユーザの利便性の低下を最小限に押さえて, セキュリティの向上が見込める認証方式であり, 本学の次世代認証方式としてのニーズに合致している. そこで本研究では, KU-SSO にリスクベース認証を導入することを目標とする.

2.2 認証設計の課題

リスクベース認証において, セキュリティ強度の向上だけを目的にリスクの判定基準を定めると, 毎回リスクが大きいと判定され, 追加認証に引っかかってしまうなど, ユーザの利便性の低下につながる. そのためリスクベース認証をユーザの利便性を損なわずに適切に運用するには, ユーザの日常と非日常をうまく判別できる要素を見つける必要がある. そのためには, 個々のユーザの実際の行動履歴を分析し, 大半のユーザに汎用的に適用できる最適な条件やパラメータを決定することが不可欠である. そのために, 本研究では現在運用中の本学の認証サーバのログデータに着目した.

ログデータには, ユーザがアクセスした日時や時間, ID, IP アドレスなどの情報が記録されている. これらの情報を活用し分析を行うことにより, リスクの判定基準を定めることができると考えられる.

2.3 問題点

ログデータの集計は従来から実施されているが, これまでは各々が自前のスクリプトを作成するなどして集計しており, 効率の悪さや, 汎用的な分析ツールが存在しないなどの問題があった. そこで本研究ではまず, 管理者がシステムの日常的な統計情報や, システムの不具合あるいは特定ユーザの認証状況の把握が必要になったとき, 迅速に解析が可能となる分析環境の整備を行った.

3 ログ可視化システムの構築

3.1 目的

日常的な統計情報を分析するプロセスにおいて, 大抵の場合はデータを集計し, グラフ化して考察する手順が踏まれる. また, 今後ユーザの利用状況の分析を行う上で, データ可視化の基盤を構築することは非常に重要である. そこで, 予めよく利用しそうな統計情報を可視化するシステムを構築した.

本研究では, 主に以下の 2 つの目的に焦点を絞った.

- 認証システムの管理者が簡便かつ迅速に, システムの利用状況などを把握できること
- 次世代認証の導入に必要な, ユーザの利用状況などの分析を行う基盤を整備すること

これらの目的から, 利用や情報共有が容易となるように Web システムとして構築を行った.

3.2 ログ可視化システムの概要

ログ可視化システムの構成を図 1 に示す. ログデータには, システムの動作ログなどユーザの行動履歴とは直接関係のない情報が多く含まれている. そこで, ログデータから必要な部分を抽出し, 利用しやすい形に整形, それをデータベースへ格納する処理を実装した.

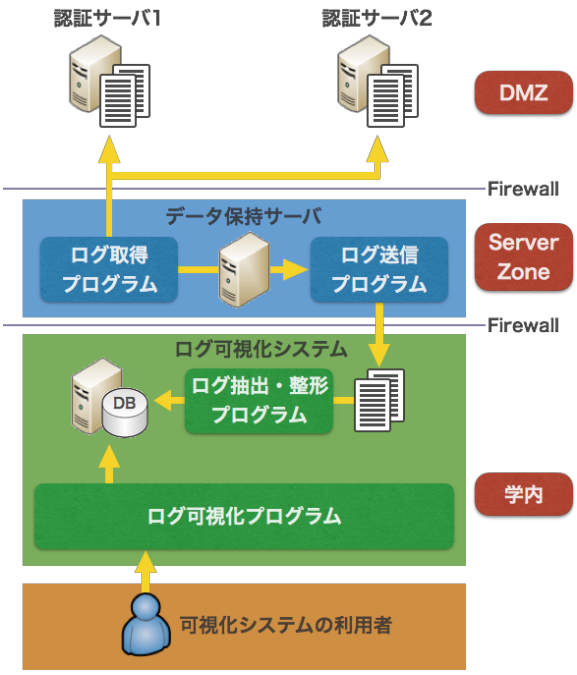

図 1 ログ可視化システム構成図

本学の認証サーバは 2 台で稼働しているため, それぞれのサーバから定期的にログデータを取得し, サーバ負荷の低い時間帯に抽出・整形処理を行い, データベースへ保存する. これにより, 日々生成されるログデータは自動的に加工され, すぐに利用が可能となる.

作成されたデータベースを利用して, 基本的な統計情報の可視化が行われる. 現時点で実装されている可視化機能としては, 以下のようなものが挙げられる.

- 1 日ごとのアクセス数の推移
- 時間帯別のアクセス数
- 各システムの利用割合
- 学内/学外別アクセス数
- VPN によるアクセス数

これらの情報は, システムの利用状況を把握する意味合いが強く, 主にシステム管理者が現在の利用状況把握のために利用することを想定している. 加えて, 「個人分析」という項目を設け, ある特定の個人についてアクセス場所 (学内/学外/VPN) や利用時間帯, アクセス元 IP アドレスの一覧などを表示できるようにした. これらの項目は, ユーザにフォーカスした内容であり, 次世代認証の設計に必要となるユーザの利用状況を可視化するための機能となっている.

月ごとの学内/学外別アクセス数を表示した例を図 2 に示す. このログ可視化システムの構築を行ったことで, Web を介してシステムの利用状況の把握や, 個人の利用状況の分析が可能となった.

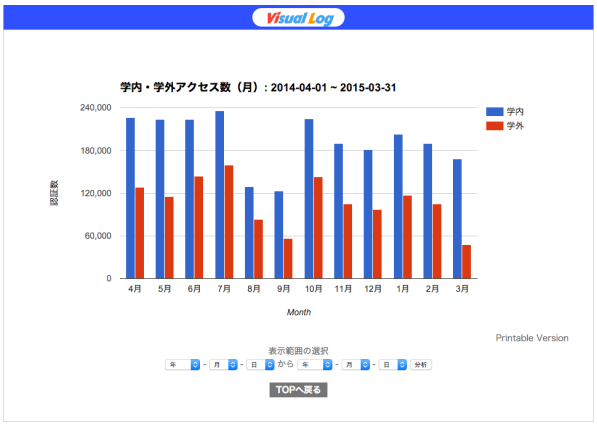

図 2　ログ可視化システム

4　ユーザ分析

本章では, 構築した可視化システムを活用して, 実際にユーザのアクセス履歴をログデータを元に分析した結果について考察する.

4.1　ネットワークに基づいたリスク判定の検討

本研究では, 個人のアクセス履歴に記録されている IP アドレスを, 事業者 (以下, ネットワークとする) ごとに分類することで, 各ユーザが日常的に利用するネットワークからのアクセスと, 例外的なアクセスを識別する方法について検討を行った. IP アドレスをネットワークごとに分類することにより, 初めてのネットワークからのアクセスや, 極端に利用頻度の少ないネットワークからのアクセスがあった場合には不正アクセスの可能性が高いと判断することで, リスクベース認証に取り入れることができると考えられる.

そこで, 本学の認証サーバのログファイルに記録された過去 1 年分の全 IP アドレスに対して whois による問い合わせを行い, 認証サーバへのアクセスがあったネットワーク名に関するデータベースを作成した. このデータベースには, ネットワーク名とそれを保持する組織名, CIDR 表記によるネットワーク情報が格納されている. このデータベースを利用して, 個人のアクセス履歴の IP アドレスを照合してネットワーク名と紐付けることにより, 表 1 のようなネットワーク別のアクセス数を得ることができる.

表 1　あるユーザのネットワーク別アクセス数

NETWORK	COUNT
ネットワーク A	226
Kanazawa University	47
ネットワーク B	32
ネットワーク C	3

4.2　ネットワークに基づいたユーザ分析

ユーザごとのネットワーク別アクセス数を分析すると, 大半のユーザにおいて, アクセス数の多いネットワークとそれほど利用していないネットワークに分けることができる. 例として, ネットワーク別アクセス数に偏りのあるユーザを表 2 に示す. 表 2 から, このユーザが日常的に使用しているネットワークは, ネットワーク D ただ 1 つであることが読み取れる. そのため, この例ではネットワーク D 以外のネットワークからのアクセスを非日常と定義することで, リスク判定に取り入れることが可能になると考えられる.

また, アクセス数上位のネットワークが, そのユーザの全アクセス数の何割を占めているのかという調査を全員に対して行ったところ, 図 3 に示すように, アクセス数上位 3 つのネットワークからのアクセス数の合計

表 2　アクセス数に偏りのあるユーザ

NETWORK	COUNT
ネットワーク D	1357
Kanazawa University	2
ネットワーク E	2
ネットワーク F	1

が, 各個人のアクセス数の 9 割以上であるユーザは全体の 93% に及ぶという結果も得られた. この結果を元に, 上位 3 つに含まれないネットワークに対して高いリスクを設定することで, リスク判定に用いることが可能であると考えられる.

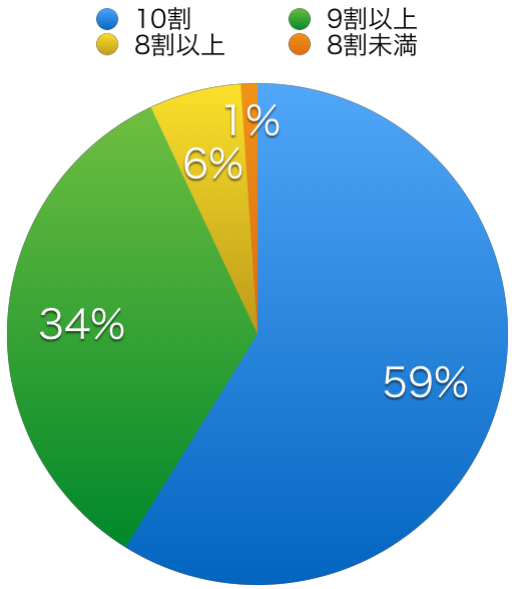

図 3　上位 3 ネットワークが占める割合が各項目に当てはまるユーザの割合

5　まとめ

本研究では, 次世代 KU-SSO にリスクベース認証を導入するために, 認証サーバのログデータを用いてユーザの分析を行った. ログデータの分析を行う上で, 分析の行いやすい環境の整備や, ログ可視化システムの構築も行った. そして, ユーザの IP アドレスを元に, ネットワークに基づいたリスク判定方法についての検討を行った. その結果, ユーザのネットワーク別のアクセス数を集計することで, ネットワークの利用頻度や偏りに応じてリスクのスコアを設定することにより, リスクベース認証を実現できる可能性を示すことができた.

今後はこれらの分析結果に基づき, 実際にリスクベース認証の設計を行う予定である.

参考文献

[1] 松平 拓也, 笠原 禎也, 高田 良宏, 東 昭孝, 二木 恵, 森 祥寛, ”大学における Shibboleth を利用した統合認証基盤の構築”, 情報処理学会論文誌, Vol.52 No.2, pp.703-713, 2011.2

[2] Shibboleth, https://shibboleth.net (accessed 2016.09)

[3] 松平 拓也, 笠原 禎也, 高田 良宏, 東 昭孝, 二木 恵, ”学認との融合化を視野に入れた金沢大学統合認証基盤の構築と運用”, 学術情報処理研究, No.16, pp.41-50, 2012.9

[4] 松平 拓也, 笠原 禎也, 高田 良宏, 東 昭孝, 二木 恵, 藤田 翔也, 金沢大学における統合認証基盤の現状と課題, 大学 ICT 推進協議会 2013 年度年次大会 (AXIES2013) 論文集, W3E-4 (CD-ROM), 18-20 December, 2013.

[5] 藤田 翔也, 松平 拓也, 高田 良宏, 笠原 禎也, 次世代統合認証基盤の構築に向けた大学サービスの利用環境の解析, 第 13 回情報科学技術フォーラム (FIT2014), 2014.9.3-5.