Vol.2011-IOT-15 No.1
2011/10/7

キオスク端末のWebアクセス制限を対象にしたシングルサインオンシステムの運用と課題

佐藤 聡[†1] 高田真吾[†3] 徳田聖子[†2]
平田完[†2] 中山知士[†2]
真中孝行[†2] 新城靖[†3]

我々はキヨスク端末からインターネットのWebコンテンツへのアクセスの認可を制御するための認証部分をシングルサインオンにしたシステムの開発を行った．そのシステムを筑波大学附属図書館のキヨスク端末に対して運用を行う際に，ログアウト処理をどうするかが問題である．その解決策として，ログアウト処理を行うスクリーンセーバを提案し開発した．実際のキオスク端末に設定を行い実運用を行った．その運用の結果について報告する．

Practical Issue of a Single Sign-On System for Web Access Control of Kiosk Terminals.

Akira SATO,[†1] Shingo TAKADA,[†3]
Seiko TOKUDA,[†2] Kan HIRARA,[†2]
Satoshi NAKAYAMA,[†2] Takayuki MANAKA[†2]
and Yasushi SHINJO [†3]

We had developed an web access control system as Single Sign-On. When we operate this system for the kiosk terminal of University Library on University of Tsukuba, the correspondence of a user having forgotten logout processing becomes the important problem. We proposed this solution as a screensaver that worked to logout processing. We applied this screensaver to the kiosk terminal, and operated in real environment. We report a result of this operation and discuss a future work.

1. はじめに

近年，Webを用いたシステムの連携が進んでおり，セキュリティを確保しつつ，利用者の利便性が高まってきている．いくつかのWebにおいて認証連携を行うことにより認証機能を一元的に扱い，それぞれのシステムでは認可だけを行うシングルサインオンの仕組みが普及してきている．国立情報情報学研究所では，Shibboleth[2)]技術を利用してシングルサインオンを可能とするために大学と学術サービスを提供する機関等から構成された連合体である「学術認証フェデレーション (愛称:GakuNin)」の構築と運用を行っている[5)]．また，この連携に参加している大学の中には，学内サービスのシングルサイオンを実現している[3),4)]．

また，ネットワーク認証もShibboleth技術によるシングルサインオンに対応して，利用者の利便性を向上させ，かつ，管理側の認証情報の重複管理を省く方法に関しても研究が行われ，実装されたシステムが稼働している[1),6)]．これらの研究は持ち込みPCのネットワーク認証のシングルサインオン化を実現している．認証されたPCについては全てのプロトコルが許可される．しかしながら，認証を受けていないPCについては，特定のURLの閲覧だけを認めるようなことは実現し難い．

筑波大学においても学認に参加し認証連携を進めてている．附属図書館においては，古くから蔵書検索機能をネットワーク経由で一般にて提供してきた．それ以外において図書館の機能として認証が必要な機能は，Shibboleth対応を行っている．これにより，海外の電子ジャーナルの利用とともにシングルサイオンを実現している．シングルサインオンにて利用できる各機能を始め，認証が不要な蔵書検索機能等を来館者にも提供するために筑波大学附属図書館ではキオスク端末を用意している．これらのキオスク端末から外部のWebサイトの閲覧を認める際には学内のセキュリティポリシにより利用者を認証する必要がある．外部のWebアクセスの認証もシングルサインオンを可能とすることにより利用者の利便性が高り，また，運用側としては別途利用者管理をする必要がなくなりコストを軽減することができる．

我々は，Webアクセスを制御するシステムをShibboleth対応化する方法について提案を

†1 筑波大学 学術情報メディアセンター
Academic Computing and Communications Center, University of Tsukuba
†2 筑波大学 附属図書館
University Library, University of Tsukuba
†3 筑波大学 システム情報工学研究科
Graduate School of Systems and Information Engineering, University of Tsukuba

行った[8]．本稿では，このシステムを筑波大学附属図書館のキオスク端末に導入する際に問題について議論した結果を報告する．さらにその問題の中で最も重要だと思われるログアウト処理についての解決方法について議論を行い，スクリーンセーバにログアウト機能を組み込む方式を提案する．そして，その機能を有するスクリーンセーバを実装し，システムに組み込んで運用を行った．運用の結果について報告し，今後の課題などについて議論を行う．

2. 開発したシステムの概要

我々はシングルサイオン化可能な，HTTP プロクシサーバによる Web アクセス制御システムを開発した[8]．このシステムでは，利用者の認証に Shibboleth の仕組みを利用し，Web アクセス制御は HTTP プロクシサーバである Squid[7] の機能を用いている．本稿では，このシステムを「開発したシステム」と呼ぶことにする．

HTTP プロクシサーバでは，Web ブラウザからのリクエストを受けると，そのリクエストを対象の Web サーバに転送し，そのサーバからの応答をそのままブラウザに返す．開発したシステムでは，Squid の `url_rewrite_program` 機能を用いて，Web ブラウザのアクセスをアクセス制御ルールに基づいて処理を変更することにより，Web アクセス制御を実現している．

開発したシステムにおいて，利用者のブラウザが外部の URL にアクセスするまでの処理の流れを**図 1** に示す．まず，このシステムでは利用者が使っているホストを認証・非認証のいずれかの状態として取り扱う．また，ホストは IP アドレスを用いて識別している．認証前の状態では，明示的に許可された URL を除き，あらゆる URL へのアクセスはプロクシサーバによりログインゲートページへとリダイレクトされる (図 1 (1) 参照)．

ログインゲートページは Shibboleth の SP として動作する CGI スクリプトとなっている．この CGI スクリプトは， Shibboleth の認証情報をチェックする．リクエストに利用者の Shibboleth 認証情報が含まれていない場合，利用者に認証を要求するために，DS にリダイレクトする (図 1 (2) 参照)． DS は，利用者に IdP を選択させる (図 1 (3) 参照)．IdP では，認証後には再びログインゲートページにリダイレクトされる (図 1 (6) 参照)．Shibboleth 認証情報が含まれている場合かつ利用者が用いているホストが非認証状態ならば，あらかじめ設定されたルールに基づいてこのホストに関するプロクシサーバのルールを設定し，利用者が用いているホストを認証状態にして，ログに情報を出力した後，利用者がアクセス要求をした外部の URL にリダイレクトされる． Shibboleth 認証情報が含まれている場合かつ利用者が用いているホストが認証状態ならば，通常のプロクシサーバとして動作する．

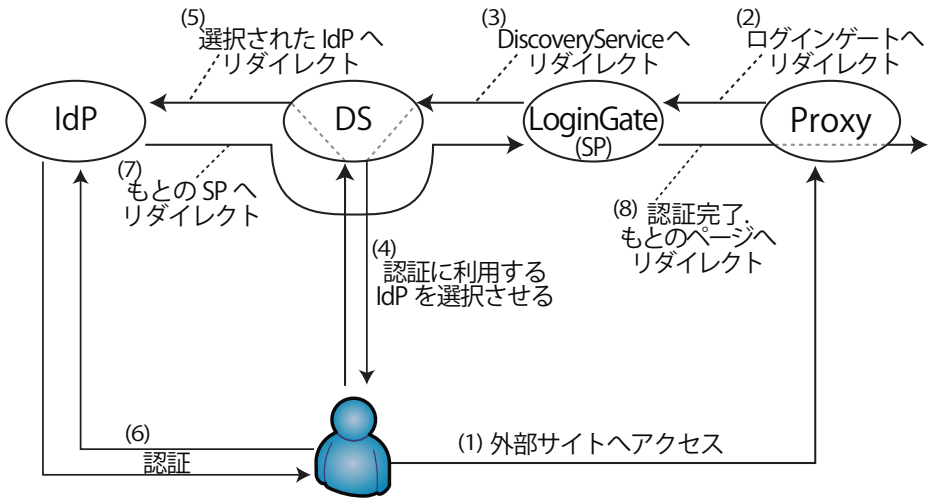

図 1 システムの概要
Fig. 1 Overview of Development System

利用を終了する際には，利用者がログアウトページにアクセスすることにより動作する．利用者が用いているホストが認証状態であるならば，利用者が用いているホストを非認証状態とし，プロキシサーバにおけるこのホストに関するルールを解除し，ログに必要な情報を出力する．

開発したシステムのログアウト処理はログアウトページへのアクセスにより実現しているが，この処理についてはべき等性がある．具体的には，ログアウト処理が行われると，次のログイン処理が行われるまでは，当該ホストからの Web アクセスは拒否するようになるため，何度実行しても同じ結果になる．

3. 運用に際しての問題点と解決方法

第 2 章にて述べたシステムを附属図書館のキオスク端末に設置する際の問題点について検討を行った．以下にその結果を述べる．

(1) Web アクセスルールにはどのように設定を行うとよいのか．具体的には，IdP から受け取る属性はどうするすべきであり，またその属性値により何を許可・拒否するの

かを決定しなければならない．また，認証を行わなくても許可する URL(ホワイトリスト) はどうすべきかも決定しなければならない．

(2) ログアウト処理を用意しても，利用者がログアウト処理を実行し忘れることがある．利用者がログアウト処理をし忘れることにより，次の利用者が意図せずとも前の利用者の認可のまま利用できてしまう．ログアウト処理をシステムが自動的に実施する場合には，利用者の利便性を損ねることがあってはならない．

3.1 附属図書館におけるキオスク端末の管理方法

附属図書館では利用者に Web インタフェースによる蔵書検索機能を提供している．具体的には，利用者は Web ブラウザを用いて附属図書館の Web サイトにアクセスし，フォームから蔵書に関する情報を送信することにより，蔵書の配架や貸出等の情報を受信し，確認することができる．附属図書館では，来館者による持ち込み PC によるネットワークアクセスも提供しているが，PC を持ち込まない来館者に対しても蔵書検索が行えるようにキオスク端末を用意している．本稿では，キオスク端末を利用する来館者のことを利用者と呼ぶことにする．

これらキオスク端末については Microsoft Windows 系の OS を使って運用している．管理方法としては，以下のように行っている．

- 管理コストを軽減するために，グループ・ポリシを用いて一括管理を行い，利用者による設定変更，ソフトウェアのインストール，アンインストールが行えない様にする．
- 蔵書検索機能が使え，かつ，附属図書館からのお知らせが表示できることが目的であるため，ブラウザのみが起動できるように，不要なソフトウェアをアンインストールしてある．

3.2 キオスク端末でのログアウト処理の実現方法

我々はキヨスク端末の利用者が能動的に行うログアウト処理の方法として，ブラウザを終了するという行為をきっかけに行うこととした．これについては，フォーム入力，閲覧履歴などを他の利用者にみられない様にするといった一般的なプライバシ保護のための作業としても受け入れられる行動であると思われる．具体的には，ブラウザの起動時にログアウト処理を行うようにした．これは，利用者がブラウザを終了することにより，次の利用者が利用する際には，必ずブラウザの起動が行われる点を利用した方法である．

また，利用者によるログアウト処理のし忘れへの対応方法としては，スクリーンセーバを利用することとした．スクリーンセーバとは，従来，ディスプレイの焼き付き防止のために利用されているが，現在では，デジタルサイネージ等の情報表示の目的などにも利用している．スクリーンセーバはキーボードおよびマウスの操作が一定時間行われない場合に起動するプログラムである．利用者がログアウトし忘れてキヨスク端末を離れた場合，高確率にてスクリーンセーバが起動する状態となる．したがって，ログアウト処理を行うスクリーンセーバを開発すればよいと考えた．なお，利用者がログアウトし忘れてキヨスク端末を離れてもスクリーンセーバが起動しない場合として考えられるのは，直後に他の利用者がキヨスク端末を使う場合である．このような場合には，他の利用者は利用者の後ろで待機していると思われる．このような場合には，おそらく前述のプライバシ保護の観点から利用者が自主的にブラウザを終了することが期待できる．したがって，他の利用者が待機している状態で，ブラウザを終了し忘れてることにより，他の利用者が意図せずなりすまし利用となる場合はほとんど発生しないと仮定し，対処しないこととした．

ただし，利用者が検索結果のメモをとるなど，一定時間以上キーボードおよびマウス操作を行わない場合も考えられる．そのような，利用中にも関わらずスクリーンセーバが起動する場合については，スクリーンセーバの表示機能を用いて，「このまま使わないとログアウト処理が行われる」といった注意を画面に表示することにより，時間になったら強制的にログアウトされるのではなく，利用者の利便性を確保することが可能な方法を考えた．

以上のように我々はログアウト処理を行うスクリーンセーバを用いる方式がログアウトし忘れに対する対処法として有用であると考え，以下に示すように，ログアウト処理を行うスクリーンセーバの設計を行った．

- ブラウザが起動している場合
  (1) 指定された時間の間，利用者への注意のために指定された文字列を画面に表示する．
  (2) ブラウザを強制的に終了させる．
  (3) ログアウト処理を実行し，指定された他のスクリーンセーバを起動する．
- ブラウザが起動していない場合
  (1) ログアウト処理を実行し，指定された他のスクリーンセーバを起動する．

このスクリーンセーバについては，「注意のためのメッセージを表示する時間」「注意のためのメッセージに用いる文字列」「ログアウト処理後に実行される他のスクリーンセーバ」を設定ファイルにより指定可能となるように実装を行った．これらの設定ファイルは，集中管理により全てのキオスク端末に配布することは容易にできるため，運用を行いながら各種調整が容易に実施できるようになった．運用においては，60 秒間注意のメッセージを表示するようにし，Web ページを表示するスクリーンセーバを他のスクリーンセーバとして設

定することにより，利用者が利用していない時にはキオスク端末をデジタルサイネージとして利用した．

3.3 Web アクセスルール

まず，開発したシステムが動作するために，ホワイトリストとしてには，筑波大学の IdP を加えなければならない．来館者がアクセスを望むサイトでかつ，認証がなく利用しても問題がないサイトを追加する必要がある．まずはじめに，附属図書館の Web ページ，筑波大学の Web ページ等を設定した．それ以外のホワイトリストについては運用を行いながら調整した．また，属性情報として uid を用いることとした．筑波大学では uid は身分によりコード化されている．詳細な身分をあらわす属性については，導入当時には整備されていなかったため，uid の属性値のコード体系を利用して，利用者の身分によりアクセス制限を実現可能とした．導入当初は区分によりアクセスルールを切り替えることはしていないが，一部の区分については利用をかなり制限することを行っている．

3.4 開発したシステムのその他の設定

現在は，我々の開発したシステムが連携している IdP としては筑波大学の IdP だけである．そのため利用者の利便性を考慮して，ログインゲートページにおいて認証情報が含まれていない場合には， DS ではなく筑波大学の IdP に直接リダイレクトする運用をしている．(正確にいえば，筑波大学の IdP ではなくて，このシステムの概要を紹介するページへリダイレクトし，そのページから利用者のクリックにより筑波大学の IdP が表示されるようにしてある) ．ログインゲートページにて認証情報が含まれていない場合にリダイレクトされるリダイレクト先については，開発したシステムの設定ファイルにて指定することができるため，運用の状況に応じて，自在に変更できることが可能である．

また，キヨスク端末では，開発したシステムのプロクシサーバを経由するように，ブラウザの設定を行った．また，上流のルータにより，キオスク端末からの Web アクセスは拒否する設定を行った．

4. 運 用 報 告

筑波大学の附属図書館のキヨスク端末を対象として我々のシステムの導入を行った．初めに，我々のシステムの図書館内部のネットワークに接続されるように設置した．実際には，ログインゲートページ，ログアウトページを提供する Web サーバおよびプロクシサーバを 1 つの仮想計算機上に実装した．また，ログインゲートページを提供するサーバが，筑波大学の IdP と連携できるように申請および設定を行った．平成 23 年 3 月より試験的に運用するために，一部のキヨスク端末が我々のシステムを利用できるようにした．具体的には，ブラウザの設定，スクリーンセーバの設定を変更した．その後，トラフィック量，プロキシサーバのロードなどを監視して問題が無いことを確認しながら運用をつづけ，徐々に我々のシステムを利用するキヨスク端末を増加させた．全てのキヨスク端末 182 台が我々のシステムを利用してもシステムのキャパシティに問題がないことが確認できたため，平成 23 年 4 月より正式に運用を開始した．この論文執筆時まで約半年運用を行ってきたが問題なく運用している．

我々は利用状況の解析を平成 23 年 9 月 1 日 (木曜日) から同年 9 月 8 日 (木曜日) までの期間を対象にして行った．参考までに筑波大学では元来は 9 月 1 日より夏休み後の講義が再開されるが，平成 23 年度については筑波大学が平成 23 年 6 月 23 日に発表した「平成 23 年夏期の節電行動計画」に伴い，休講期間となっている．そのため，附属図書館では上記期間中の平日については，中央図書館，体育・芸術図書館，図書館情報学図書館については 9 時から 17 時まで開館し，医学図書館が 9 時から 20 時まで開館し，大塚図書館が月曜日は 10 時 30 分から 18 時 30 分まで，それ以外は 13 時から 21 時 10 分まで開館している．土曜日，日曜日については，中央図書館，図書館情報学図書館が 10 時から 18 時まで開館し，医学図書館が 9 時から 20 時まで開館し，大塚図書館が土曜日のみ 12 時から 19 時 50 分まで開館し，それ以外の図書館は休館している．

まず，対象期間内のプロクシサーバの転送量を解析した．その結果を**図 2** に示す．横軸が時刻を表し，縦軸が 30 分平均の転送量を表す．全ての日において開館時間帯に転送量があることがわかる．正午以後に転送量のピークがあることから，利用者の利用状況と一致しており，利用者に対してのサービス提供が正常に行われていると判断できる．また，期間中では，9 月 5 日 (月) にピークがあることがわかる．

次に，対象期間内の仮想計算機のロードアベレージを解析した．その結果を**図 3** に示す．横軸が時刻を表し，縦軸がロードアベレージを表す．これについても，全ての日において，日中にロードが高くなっている．また，ピークはそれほど高くなっていないため，今後，キヨスク端末を増やすことは可能ではないかと思われる．

最後に利用者がどれくらいの時間，利用しているかについて，プロキシシステムが出力するログを用いて解析した．我々のシステムでは，利用者が利用開始した時および利用者が利用を終了した時にログを出力している．このログを解析することにより，利用者がどれくらいの時間利用したかを計算することができる．当該期間にて利用者ごとの利用時間を計算し，利用時間に対して頻度を求めた．その結果を図 3 に示す．横軸が利用時間 (対数表記)

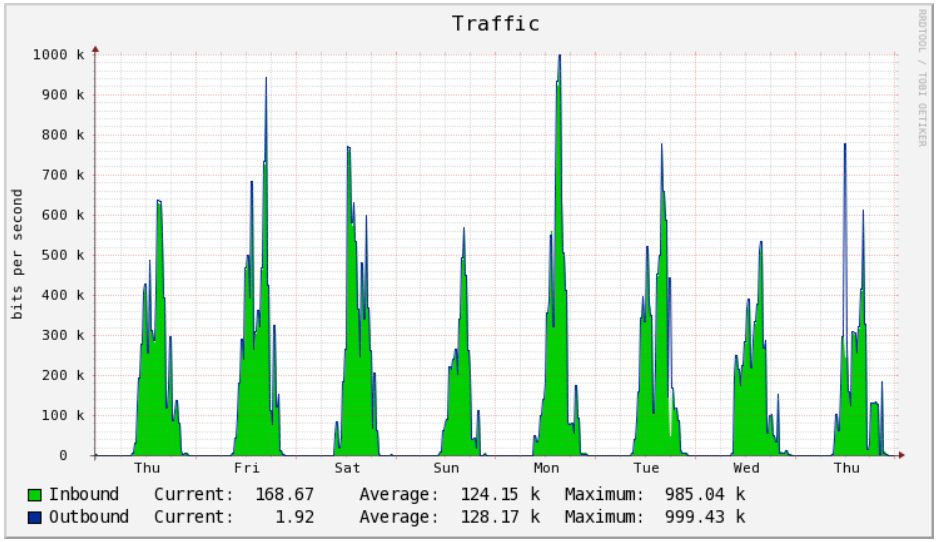

図 2 転送量
Fig. 2 Quantity of transfer

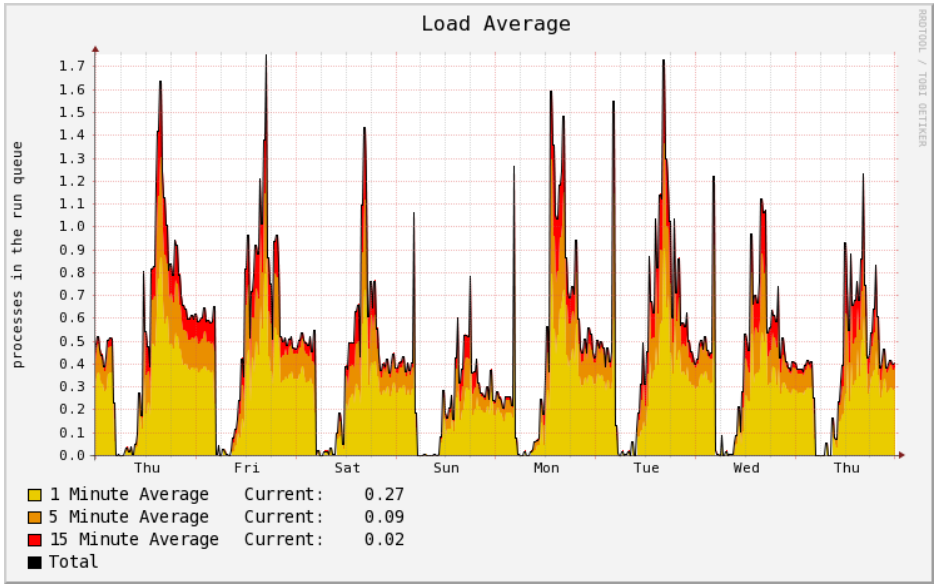

図 3 ロードアベレージ
Fig. 3 Load average

を表し，縦軸は，度数 (左側)，および，累積度数の全体に対する割合 (右側) を表している．度数については赤色の十字記号で表現し，累積度数の全体に対する割合は緑色の線で表現した．

図 3 により，以下のことが分かる．

- 200 秒から 300 秒で利用を終了している利用者が多い．
- 約 50% の利用者は 1000 秒以内に利用を終了している．
- 約 70% の利用者は 2000 秒以内に利用を終了している．
- 約 80% の利用者は 3000 秒 (50 分) 以内に利用を終了している．
- 約 90% の利用者は 3600 秒 (60 分) 以内に利用を終了している．

この結果は，キオスク端末の利用状況を目視で観測したときの感想とほぼ一致している．したがって，ログが正確に記録されていることとスクリーンセーバによるログアウト処理が正常に動作していると言える．

なお，この解析は利用者の認証によるログを使って解析をしている．利用者が認証を受けなくても利用できるサイト (例えば，附属図書館が提供している蔵書検索機能) へのアクセスについては解析を行っていない．具体的には，蔵書検索機能だけを長時間利用していても，この解析のグラフには表現されていない．

5. おわりに

本稿では，筑波大学附属図書館に設置されているキオスク端末の Web アクセスを利用者の利便性を確保しつつ管理するために，既に我々が開発を行ったシングルサインオンを用いた Web アクセス制御システムを運用するための問題点とその解決方法を述べた．また，運用を行った結果について報告を行った．

今後は，このシステムを国立情報情報学研究所が運用しているフェデレーション「学認」と連携することがある．これにより，筑波大学附属図書館を来館した学外者が学認と連携している IdP を用いて認証することにより，キオスク端末を用いてインターネット上の Web 閲覧を許可することが可能となる．本稿で示したデータ等を検討して，学認との連携をした際の問題点を検討し，解決策を考えていきたい．

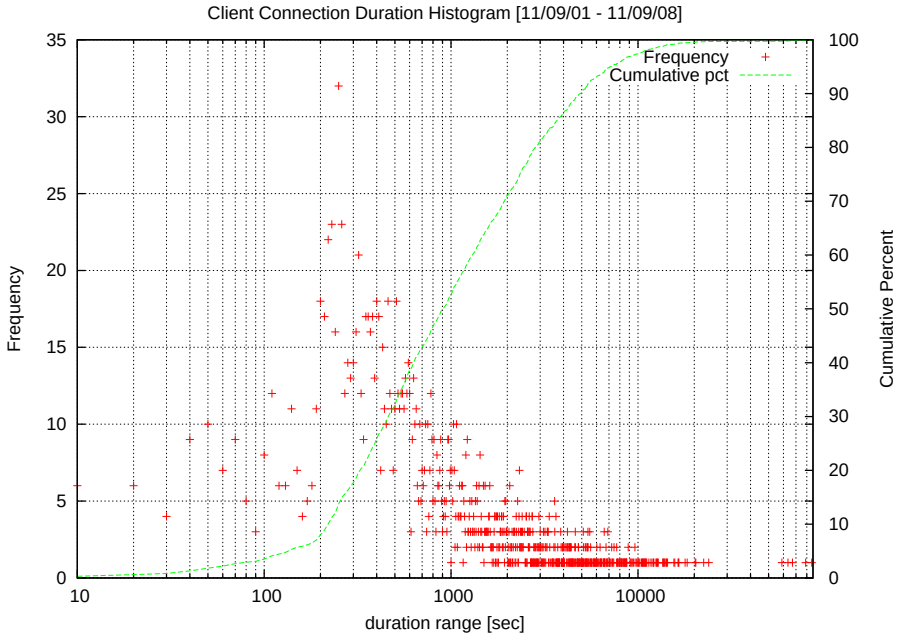

図 4 利用時間
Fig. 4 Client Connection Duration Histogram

参 考 文 献

1) 藤村喬寿，田島浩一，大東俊博，西村浩二，相原玲二：学術認証フェデレーションに基づくキャンパスネットワークの認証機構，情報処理学会研究報告. IOT, [インターネットと運用技術]， Vol.2010, No.37, pp.1–6 (2010-02-22).
2) Internet 2: Shibboleth, `http://shibboleth.internet2.edu/` (Accessed:2011-09-11).
3) 桝田秀夫，村田和義，渋谷　雄，若杉耕一郎，黒江康明：システム統合と運用管理に配慮したサーバの仮想化と統合認証系を有する計算機システム，情報処理学会研究報告. IOT, [インターネットと運用技術]， Vol.2010, No.4, pp.1–6 (2010-07-09).
4) 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 (2011-02-15).
5) 国立情報学研究所：学術認証フェデレーション 学認 GakuNin, `http://www.gakunin.jp/` (Accessed:2011-09-11).
6) 大谷　誠，江藤博文，渡辺健次，只木進一，渡辺義明：シングルサインオンに対応したネットワーク利用者認証システムの開発，情報処理学会論文誌， Vol.51, No.3, pp. 1031–1039 (2010-03-15).
7) squid: Optimising Web Delivery, `http://www.squid-cache.org/` (Accessed:2011-09-11).
8) 高田真吾，金子直矢，齋藤　剛，佐藤　聡，新城　靖，中井　央，板野肯三：UPKI 認証連携基盤を用いた Web アクセス制御，情報処理学会研究報告. IOT, [インターネットと運用技術]， Vol.2010, No.38, pp.1–6 (2010-02-22).