Vol.2019-IOT-46 No.4
2019/6/14

既設ファイアウォールシステムを活用した認証シャッターの実装方式

佐藤 聡[1,a)]　三宮 秀次[1]　片岸 一起[1]　中井 央[1]　亀山 啓輔[1]

概要：アカウント情報の漏洩による不正アクセスの事例は頻繁に発生している．その対策の一手法として「認証シャッター」という概念が提案されている．また，概念を具体化したシステムも提案されている．著者らは，既存のファイアウォールシステムに認証シャッターの機能を実装する方式を提案する．提案方式の特徴は，現有のサービスシステムに対して，ネットワーク構成を全く変更することなく認証シャッターの機能を導入できる点にある．

キーワード：認証シャッター，アクセス制御，アカウント管理

Implementation scheme of authentication shutter utilizing existing firewall system

Abstract: As a countermeasure against frequent fraudulent accesses using leaked credentials, an authentication shutter concept and its implementation have already been studied. In this paper, an implementation scheme for realizing the authentication shutter into an existing network firewall system is proposed. The advantage of the proposed scheme is that the authentication shutter function can be installed without any configuration changes of existing network service systems in operation.

Keywords: Authentication shutter, access contorol, account management

1. はじめに

アカウント情報の漏洩による不正アクセスの事例は頻繁に発生している．その対策の一手法として「認証シャッター」という概念が提案されている [3], [5]．また，この概念を具体化したシステムも提案されている [4], [6]．これらのシステムは既存のシステムに改変を行わずに実現できるが，既存のシステムの物理的ネットワーク構成を変更する必要がある．

一般的な組織であれば，サービスサーバとそのサーバを運用している組織の外部とのネットワークの間にはファイアウォールが設置されている．著者らは，既存のファイアウォールシステムに認証シャッターの機能を実装する方式を提案する．認証シャッターは「シャッターが降りている間は個人認証を通過できなくするもの」と定義されている [5]．本研究で提案するシステムは，「個人認証を通過できなくする」手段として既存のファイアウォールによる通信制限を用いる．すなわち，シャッターが開いている時は当該サービスサーバへの通信を許可し，シャッターが閉じている時は通信を拒否する．

提案方式の特徴は，現有のサービスシステムに対して，ネットワーク構成を全く変更することなく認証シャッターの機能を導入できる点にある．

提案方式では，認証シャッターを，既存のファイアウォール，新たに導入するシャッター認証管理サーバ，ならびに，新たに導入するシャッター制御サーバの３つによって実現する．新たに導入するシャッター認証管理サーバは，大学等の来訪者のネットワーク利用のためのネットワークアカウントを発行する機能を使って実装することができる．また，ファイアウォールについては，ユーザ認証機能を持っているものであれば，シャッター制御サーバとファイアウォールが連携するように実装すれば，ファイアウォール

[1] 筑波大学
University of Tsukuba, Tsukuba, Ibaraki, 305–8577, Japan
[a)] akira@cc.tsukuba.ac.jp

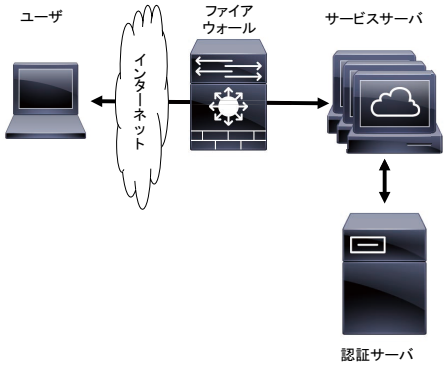

図 1 現有サービスシステムの概要
Fig. 1 Configuration of existing network service systems

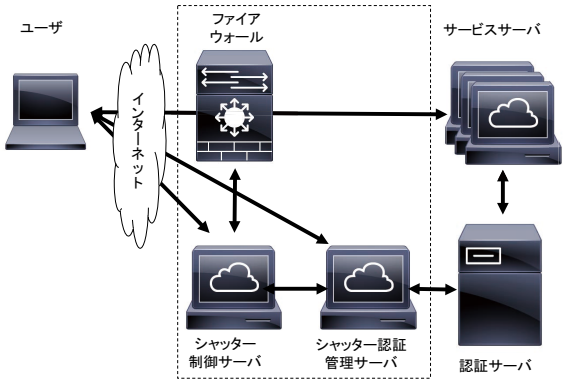

図 2 提案システムの概要
Fig. 2 Proposed configuration for implementing authentication shutter

の設定変更項目を最小限現にすることも可能である．

本論文では，さらに実装手法の提案を行い，実際に実装を行なったプロトタイプにより，提案方式の有効性を示す．

2. 提案方式

2.1 概要

高田は，漏洩した認証情報を用いた不正なログインを防ぐ仕組みとして，**認証シャッター**を提案しており [3], [5]，参考文献 [5] の中で「認証シャッター」を以下のように定義している．

> シャッターが降りている間はアカウント名と正しいパスワードを知っていたとしても個人認証を通過できなくするものである。

我々は個人認証を通過できなくすることを，そもそもの通信を通過できなくすることにより実現するシステムを設計した．すなわち，普段はシャッターを閉めて通信を拒否しておき，利用者が利用を宣言した時から一定期間はシャッターを開けて通信を許可する。

2.2 想定するサービスの概要

認証シャッターシステムが導入されていない状況でのサービスシステム全体の構成の概要を**図 1** に示す．

このサービスシステムは，サービスを利用したい**ユーザ** (正確にはユーザが使う計算機ではあるが，本論文ではそれを単にユーザと呼ぶ)，ユーザの認証情報を管理している**認証サーバ**，ユーザのパスワード認証のためにその認証サーバを利用している**サービスサーバ**，および， ユーザとサービスサーバとの間のアクセス制限を実現している**ファイアウォール** から構成されている．

2.2.1 ユーザ

ユーザはインターネットに接続されている．すなわち，ユーザには IP アドレスが割り当てられている．ユーザが Web メールサービスを利用して 1 日分のメールの読み書きを行うなど，サービスを利用して一連の作業をしている間は IP アドレスが変わらないものとする．

2.2.2 認証サーバ

認証サーバはサービスを利用する全てのユーザの認証情報を集中的に管理していることを想定している．なお，サービスサーバから LDAP 等のプロトコルを用いて直接認証サーバに問い合わせをする構成，もしくは，認証サーバがサービスサーバ内の認証機能に対してプロビジョニングを行なっている構成を想定している．

2.2.3 サービスサーバ

認証サーバを利用して認証を行なっているサービスサーバは複数あることを想定している．これらのサービスシステムが使用しているプロトコルは，Web，SSH などの様々な種類であることを想定している．

2.2.4 ファイアウォール

ファイアウォールは，外部のネットワークからサービスサーバへの通信を制御できるように 1 拠点に集中的に配置されていることを想定している．

2.3 提案システムの概要

我々は，前節にて述べた環境に対して，ネットワーク構成，IP アドレスの変更，DNS 設定の変更等を一切行わずに認証シャッター機能を導入する方法を提案する．

提案するシステム全体の構成の概要を**図 2** に示す．提案方式における認証シャッター機能は，図 2 中の点線にて示した **シャッター認証管理サーバ**，**シャッター制御サーバ**および **ファイアウォール** により実現する．

このうち，ファイアウォールについては，現有のシステムにおいて導入されているものを用いることを想定している．

2.3.1 シャッター認証管理サーバ

シャッター認証管理サーバは，後述するシャッター制御

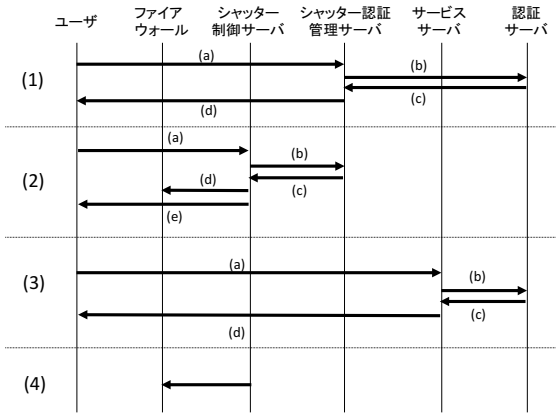

図 3 提案システムに置けるサービスシステムの利用の流れ
Fig. 3 Utilization procedure of service systems in proposed configuration

サーバの認証用サーバとして利用する．

提案手法では，シャッターを開けたいユーザには，まず，シャッターを開ける作業をするための専用のアカウント(以後，シャッター用アカウントと呼ぶ）を発行してもらう必要がある．このシャッター用アカウントの管理をするのがシャッター認証管理サーバである．

シャッター認証管理サーバは，認証シャッターの利用を希望するユーザに対してのシャッター用アカウントの新規発行，削除，および有効なシャッター用アカウントの一覧を表示する機能を実現する．これら機能を利用する際のユーザ認証には，認証サーバを用いる．

シャッター認証管理サーバは，各ユーザごとに，申請によって発行したシャッター用アカウントの情報（ID とパスワード）を管理している．発行に際しては，ユーザごとに発行できるシャッター用アカウント数の上限値を設定できるものとする．また，発行するシャッター用アカウントの有効期限の最大値を設定できるものとする．

2.3.2 シャッター制御サーバ

シャッター制御サーバは，シャッター認証管理サーバと連携して，シャッター用アカウントを用いたログイン認証を実現する．シャッター用アカウントによる認証が成功した場合には，アクセス元の IP アドレスの情報を用いて，あらかじめ定めていた時間だけ，ファイアウォールのルールを変更する． 具体的には，事前に，外部からサービスシステムへのアクセスは拒否する設定にしておき， 認証に成功した場合には，アクセス元 IP アドレスからサービスシステムへのアクセスを許可するように変更する．また，指定された時間が経過したのちに設定を戻す．

2.3.3 サービスサーバの利用の流れ

提案方式におけるサービスシステムの利用の流れの概要を**図 3** に示す．

(1) ユーザはあらかじめシャッター認証管理サーバにてシャッター用アカウント情報を入手しておく．具体的には，ユーザはシャッター認証管理システムにログインする (図 3 中 (1) の (a))．シャッター認証管理サーバは入力された認証情報を認証サーバ に送る (図 3 中 (1) の (b))．認証サーバは，送られてきた認証情報について認証を行い，結果をシャッター認証管理サーバに送る (図 3 中 (1) の (c))．シャッター認証管理サーバは認証が成功した場合には，ユーザの申請に応じてシャッター用アカウント情報（ID とパスワード）をユーザに送る (図 3 中 (1) の (d))．

(2) ユーザは，サービスシステムの利用に先立って，シャッター制御サーバにてシャッターを開ける作業を行う．具体的には，ユーザはシャッター用アカウントを用いてシャッター制御サーバにログインを行う．(図 3 中 (2) の (a))．シャッター制御サーバは，受けとったシャッター用アカウント情報をシャッター認証管理サーバに送る (図 3 中 (2) の (b))．シャッター認証管理サーバは，受け取ったシャッター用アカウント情報により認証を行い，その結果をシャッター制御サーバに送る (図 3 中 (2) の (c))．シャッター制御サーバは，認証が成功している場合には，ユーザのアクセス元 IP アドレスを用いて，ファイアウォールの設定を変更する (図 3 中 (2) の (d))．シャッター制御サーバは，ユーザにシャッターを開けたことを報告する (図 3 中 (2) の (e))．

(3) 導入以前と同様の方法でサービスサーバにアクセスしサービスを受ける．
具体的には，ユーザはサービスサーバにログインをする (図 3 中 (3) の (a))．サービスサーバは入力された認証情報を認証サーバに送る (図 3 中 (3) の (b))．認証サーバは，送られてきた認証情報について認証を行い，結果をサービスサーバに送る (図 3 中 (3) の (c))．サービスサーバは認証が成功した場合には，サービスをユーザに提供する (図 3 中 (3) の (d))．

(4) シャッター制御サーバへのログイン成功後，指定された時間が経過したのちにファイアウォールの設定が元に戻る．

上記 (4) の後に再度サービスシステムを利用する場合には，(1) にて発行されてたシャッター用アカウントの有効期限内であれば，(2) 以降の手順を行うことでサービスシステムを利用することができる．また，(1) にて発行されたシャッター用アカウントの有効期限が経過してしまった場合には，(1) から行うことで，サービスシステムを利用することができる．

上記 (2) の (d) から (4) までの間，ユーザは同じ IP アドレスを使っている限りはサービスシステムにアクセスすることが可能となる．しかし，ユーザが使う IP アドレスが変更した場合には，アクセスすることができない．さらに．

(2) の (d) よりも前，もしくは (4) より後は，ユーザはサービスシステムにアクセスすることはできない．

2.4 提案方式の特徴および問題点

提案方式の最大の特徴は，現有のサービスシステムのネットワーク構成を一切変更せずに導入できる点にある．変更しなくてすむものは，物理的なネットワーク構成だけでなく，IP アドレスや DNS の設定も一切変更する必要がない．これはサービスを運用している管理者にとっては非常に導入しやすい．また，ファイアウォールによりネットワークアクセス制御を受けている全てのサービスサーバに対して容易に導入することが可能である．大学のような組織の場合には，ファイアウォールによりネットワークアクセス制限を受けているサーバのうち，認証サーバを使わずに認証を行なっているサービスも多数ある．これらに対してもこのシステムは適用可能である．

問題としては以下の点があげられる．

- シャッター制御サーバにアクセスする際の IP アドレスと，サービスサーバにアクセスする際の IP アドレスが異なっている場合には正常に動作しない．
  たとえば，ユーザ側でプロトコルごとに透過的なプロキシーが存在しており，IP アドレスが書き換えられるなどの処理がなされる場合には使えない．
- シャッター制御サーバを利用するためのシャッター用アカウント情報への攻撃耐性が低い．
  シャッター制御サーバは，全てのユーザからアクセス可能である必要があるため，自身をシャッターにより保護できない．したがって，攻撃への耐性を高める必要がある．それに対しては提案方式では，このシャッター用アカウント情報を ID とパスワードの組としたので，攻撃耐性が高いとは言い難い．その対策方法としては，シャッター制御サーバへの認証方式をクライアント証明書認証等に切り替える方法が考えられる．一方，シャッター用アカウント情報は，ユーザに割り当てられた認証サーバの ID とは異なっており，かつ，シャッター制御サーバ専用の ID であるため，有効期限を短くし，期限が切れた際には今までに発行されたものとは全く異なる新しい ID を発行するなどの方法により攻撃耐性を高めることが可能である．

3. 提案システムの実装方式

著者らが所属する筑波大学のキャンパスネットワークにて，プロトタイプの実装を行なった．筑波大学のキャンパスネットワークのファイアウォールには パロアルトネットワークス社製 PA-7050 (バージョン 7.1) を用いている．また，大学来訪者のネットワーク利用のためのいわゆるゲストアカウントも含めたネットワークアカウントを管理するために，エイチ・シー・ネットワークス製 Account@Adapter+ を用いている．これらの２つを使った実装例ついて説明する．

3.1 シャッター認証管理サーバ

シャッター認証管理サーバとして，筑波大学のキャンパスネットワークで運用している Account@Adapter+ を用いた．

Account@Adapter+ は，認証サーバに登録されているユーザであれば，ゲストアカウントを発行できる機能を有している．その際に，ユーザごとに発行できるゲストアカウント数の上限値や，ゲストアカウントの有効期限の最大値を設定できる．Account@Adapter+ にログインしたユーザはゲストアカウントの発行以外に，すでに発行したゲストアカウントの削除や，ゲストアカウント情報の確認を行うことができる．さらに Account@Adapter+ は，発行したゲストアカウントの RADIUS サーバ [2] として動作することができる．

また，Account@Adapter+ は，Shibboleth SP [1] として動作させることができる．すなわち，ユーザはシングルサインオン (SSO) により本サーバを利用することも可能となっている．

提案システムのプロトタイプ実装においては，Account@Adapter+ に設定を追加することにより，SSO によりログインしたユーザに対して，発行したゲストアカウントをシャッター制御サーバでしか使えないアカウントとする機能を追加した．その際に作成できるアカウント数の上限値，有効期限の最大値を設定した．

3.2 ファイアウォール

ファイアフォールは，筑波大学のキャンパスネットワークで運用している PA-7050 を用いた．PA-7050 はユーザ識別の機能を有している．具体的には，特定の IP アドレスが割り当てられている機器へのログイン時にそのユーザの ID と割り当てられている IP アドレスの組を， API を通じて PA-7050 に登録することができる．この時，パラメータにより，この組み合わせを一定期間のみ登録したり，無期限に登録したりすることができる．

本学では，この機能を用いて無線 LAN システムでのログインの情報を PA-7050 に登録している．これにより，PA-7050 はファイアウォールセッションログに IP アドレスだけでなく無線 LAN システムに接続した際のユーザの ID も同時に記録しており，トラブル発生時の証跡作業を効率化することができている．

また，PA-7050 は，登録されているユーザの ID を用いたネットワークアクセス制御ポリシーを設定可能である．たとえば，登録されていないユーザには通信を拒否するポリシーを設定することができる．

これらの機能を組み合わせることで認証シャッターの機

能を低コストに実現できる．筑波大学のキャンパスネットワークのファイアウォールでは，サービスサーバへのネットワークアクセス制御ポリシーは次の優先順位で設定されている．

(1) サービスサーバあての特定のプロトコルを許可
(2) サービスサーバあての全ての通信を拒否

認証シャッターの実装においては，これらのさらに上位に次のポリシーを設定する．

(0) サービスサーバあてかつ発信元のユーザの ID が登録されていない場合は拒否する．

これにより IP アドレスとシャッター用アカウントの ID の組が登録されていない場合には，サービスサーバにアクセスできない，すなわちシャッターが閉じている状態となる．それに対して，IP アドレスとシャッター用アカウントの ID の組が登録されると，サービスサーバにアクセスすることができる．すなわちシャッターを開けている状態となる．

また，IP アドレスとシャッター用アカウントの ID の組を API にて登録する時に制限時間を設定することにより，PA-7050 が制限時間が経過した時に自動的にその組の登録を削除する．すなわち，図 3 中の (4) の作業については，PA-7050 自身が行うこととなり，シャッター制御サーバは行う必要がなくなる．

3.3 シャッター制御サーバ

提案する実装方式では，シャッター制御サーバのみを新たに構築する．シャッター制御サーバは PHP を用いた Web アプリケーションとして実装した．シャッター制御サーバのログインページのスナップショットを**図 4** に示す．

フォーム入力により，ユーザからシャッター用アカウント情報（ ID とパスワード）を受け取り，シャッター認証管理サーバとなっている Account@Adaptor+ に RADIUS 接続し認証を行う．成功した場合には，アクセス元の IP アドレスとシャッター用アカウントの ID の 組を規定された時間だけ登録するように PA-7050 の API を操作する．

この実装方式では，シャッター制御サーバはログイン状態やユーザの情報を保持する必要がない．

3.4 サービスサーバ

今回のプロトタイプシステムはあるサーバ (以後，サーバ A と呼ぶ）の SSH サービスを対象として実験を行なった．このサーバ A に認証シャッターを提供した．学外のインターネットに接続したユーザの端末から，このサーバにアクセスできないことを確認した．その後，シャッター制御サーバにあらかじめ取得したシャッター用アカウントでログインした後に，サーバ A にアクセスしログインができることを確認した．その後，一定時間を経過した後，サーバ A にアクセスできないことを確認した．これにより，認証シャッターは正しく動作していると言える．

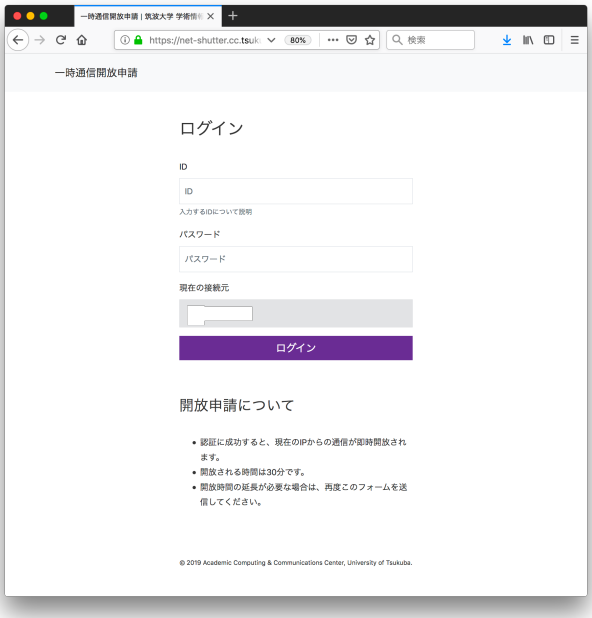

図 4 シャッター制御サーバのログイン画面
Fig. 4 Login page of shutter control server

4. おわりに

本論文では，大学等の組織にすでに導入されているファイアウォールやゲストアカウント発行管理機能を利用して，認証シャッターを実現する設計方式および実装方法についての提案を行なった． 提案方式の特徴は，現有のサービスシステムについて，ネットワーク構成を全く変更せずに認証シャッターの機能を導入できる点にある．

実装方法では，著者らが所属する筑波大学のキャンパスネットワークにすでに導入されているパロアルトネットワークス社製の PA-7050，および，エイチ・シー・ネットワーク社製 Account@Adaptor+ を用いた．これらの機能を使うことにより，認証シャッターの導入には， Web サーバとなるシャッター制御サーバのみを新たに構築するのみでよいことを示した．非常に低コストで導入できることを示した．また，プロトタイプシステムを用いて，実際に運用しているサービスサーバに対して認証シャッター機能を適用して，動作していることを確認し，提案方式の有効性を示した．

今後の課題としては，認証シャッター機能を学内の様々なサービスサーバに適用し，安定的に運用できることを検証する必要がある．

謝辞

本研究を進めるにあたり，筑波大学学術情報メディアセンターには，様々な支援を頂いた．また，パロアルトネットワーク社，および，エイチ・シー・ネットワークスス社には製品の設定に関しての様々な技術情報の提供を頂いた．ここに感謝の意を表する．

参考文献

[1] Shibboleth Consortium & Privacy Preserving Identity Management, https://www.shibboleth.net/.
[2] Rigney, C., Willens, S., Rubens, A. and Simpson, W.: Remote Authentication Dial In User Service (RADIUS), RFC 2865 (Draft Standard) (2000). Updated by RFCs 2868, 3575, 5080, 6929.
[3] Takada, T.: Authentication Shutter: Alternative Countermeasure against Password Reuse Attack by Availability Control, pp. 1–9 (online), DOI: 10.1145/3098954.3103153 (2017).
[4] 多田　充：パスワード認証の強化策，学術情報処理研究，Vol. 19, No. 1, pp. 40–49 (2015).
[5] 高田哲司：Authentication Shutter:個人認証に対する攻撃を遮断可能する対策の提案，コンピュータセキュリティシンポジウム 2014 論文集，Vol. 2014, No. 2, pp. 883–890 (2014).
[6] 本村真一, 川村尚生：既存のサービスシステムの変更を不要とする認証シャッターの提案，学術情報処理研究，Vol. 20, No. 1, pp. 112–118 (2016).