

外付けによるワンタイムパスワード認証システムの開発

小林 聖梧¹⁾, 三河 賢治²⁾

1) 前橋工科大学大学院 工学研究科

2) 前橋工科大学 工学部

mikawa@maebashi-it.ac.jp

Development of Attachable One-Time Password Authentication System

Seigo Kobayashi¹⁾, Kenji Mikawa²⁾

1) Graduate School of Engineering, Maebashi Institute of Technology

2) Faculty of Engineering, Maebashi Institute of Technology

概要

従来のユーザ ID とパスワード文字列による認証は不正アクセスのリスクが高く、多くの情報システムでセキュリティ向上のためにワンタイムパスワード認証等の多要素認証を導入している。多要素認証の導入により多くのサイバー攻撃を防ぐことができるため、情報システムの構築にあたり多要素認証を導入することが望ましい。しかしながら、既設の情報システムに多要素認証を導入する場合、認証に関わるソフトウェアを改変するか、それが難しければ情報システムを買い替える等、莫大な時間と費用が必要となる。そこで、本論文では既設の情報システムを改変することなく外付けで多要素認証を実現する認証システムを提案し、その実装と評価について述べる。

1 はじめに

インターネットサービスが広く普及し、多くの人々がログインやサインイン等の認証作業を日常的に行っている。認証作業は本人を識別する重要な作業であるため、非常に高い安全性が要求される。しかしながら、現在においてもユーザ ID とパスワード文字列のみを認証作業に利用しているサービスが一般的であり、内部犯罪や不正アクセス、ブルートフォース攻撃等による認証情報の漏えいからなりすましや更なる不正アクセスの被害につながり、認証に関わるセキュリティの問題は後を絶たない。

近年、認証技術の進歩が目覚ましく、新しい認証技術を利用した情報システムのセキュリティは飛躍的に向上している。ユーザ ID とパスワード文字列等の知識情報だけでなく、指紋や静脈、虹彩等の生体情報、職員証やスマートフォン等の所持情報を認証に取り入れた多要素認証の導入が進められている。知識情報、生体情報、所持情報から 2 つ以上の情報を組み合わせた認証方式を多要素認証とよぶ。SMS（ショートメッセージサービス）認証やワンタイムパスワード認証は、本人所有のスマートフォンに送信された時限付き情報を認証に利用するため所持情報に分類されるが、知識

情報に分類されることもある。多要素認証が社会に認知されるきっかけとなった出来事は、2019 年に発生した 7pay に対する不正アクセス事案である。7pay は、2019 年 7 月 1 日に決済サービスを開始したが、その翌日には不正利用が発覚し、同年 9 月末日をもってサービスを廃止する事態となった。7pay のユーザ認証システムでは多要素認証を導入しておらず、不正アクセスの手口は、攻撃者が不正に入手したユーザ ID とパスワード文字列のリストを使用して不正アクセスを試みる“パスワードリスト攻撃”である可能性が高いと報告されている [1]。仮に多要素認証を導入していれば、パスワードリスト攻撃による被害を未然に防ぐことができたため、この事案が“多要素認証”という認証技術を世間に知らしめた。Google によると、ユーザ ID とパスワード文字列のみで認証する情報システムに対し SMS 認証を追加するだけで、自動ボットからの攻撃を最大 100%、フィッシングによる攻撃を最大 96%、標的型攻撃を最大 76% 防御できることが示された [2]。

ユーザ認証を必要とする情報システムを構築する場合、セキュリティの観点から多要素認証を導入することが好ましい。しかしながら、多要素認証に対応していない既設の情報システムに多要素認証の機能を組

み入れる場合、ユーザ認証に関わるソフトウェアを改変するか、それが難しければ情報システム本体を買い替える必要があるかもしれない。ソフトウェアの改変や情報システム本体の更新は、予算の獲得からその運用までを考慮すると時間も費用も必要であり、簡単に解決するものではない。そこで本研究は、多要素認証として広く普及しているワンタイムパスワードに注目し、既設の情報システムのソフトウェアを改変することなく、その情報システムでワンタイムパスワードを使用した多要素認証を実現する外付けの認証システムを提案する。

2 認証コードを利用する方式

認証コードを利用する一般的な方式として、メールアドレスに認証コードを送信するもの、スマートフォン等の SMS を利用して認証コードを送信するもの、スマートフォン等のアプリを利用して時間同期による認証コードを生成するもの等が知られている。これらの方式のうち、時間同期によるワンタイムパスワード方式 (Time-based One-Time Password, TOTP) は RFC6238 [3] で定義されており、そのアプリケーションが GitHub [4] に公開されている。

TOTP は、認証機能を提供するサーバとクライアント端末で秘密鍵を共有し、現在時刻からカウンタを生成して、これら 2 つの情報から認証コードを生成する。サーバとクライアント端末で現在時刻が正しく同期されていれば、同一の認証コードを生成できるため、これをワンタイムパスワードとして利用する。実際、Google や Microsoft の TOTP では、80 ビットの秘密鍵に対応する QR (Quick Response) コードをクライアント端末の TOTP アプリケーションに読み込ませることで秘密鍵を共有し、サーバでは、Base32 で秘密鍵を 16 桁の英数字に符号化して保存する。秘密鍵と現在時刻から 30 秒毎に値が変更されるカウンタを生成するアルゴリズムを使用して同一の認証コードを生成する。例として、Google の TOTP アプリケーションで表示される認証コードを図 1 に示す。認証コードの右欄にある円グラフで次の認証コードに更新されるまでの残り時間を表している。

通常、メールアドレスや SMS で認証コードを送信する方式では、ユーザの認証作業が完了するまでその認証コードを有効とする場合が多く、ブルートフォース攻撃に弱いとされる。一方、TOTP では、アプリケーションを実装する方針によるが、例えば Google や Microsoft の TOTP は認証コードに 30 秒の有効期



図 1: Google Authenticator による認証コードの表示画面

限を設定し、ブルートフォース攻撃に対する耐性を向上させている。認証コードは 30 秒毎に更新され、本人所有のスマートフォンでのみ確認可能な情報であるため、一般に TOTP による認証コードは所持情報に分類される。また、メールアドレスや SMS で認証コードを送信する方式と比較して、TOTP では、サーバとクライアント端末でそれぞれ独自に認証コードを生成し、相互に直接通信する必要がないため、ネットワークに接続していない環境においても認証コードを利用できる。したがって、TOTP は、認証コードを利用する方式の中では、ブルートフォース攻撃や盗聴等のサイバー攻撃に対する耐性が高く、通信障害の影響を受けない方法といえる。本研究で提案する認証システムでは、ワンタイムパスワードとしてこのような利点を有する TOTP を使用する。

2.1 RADIUS サーバによる TOTP 認証の実現

標準的な RADIUS サーバでは、認証情報として 2 つの項目 (例えば、ユーザ認証ではユーザ ID とパスワード文字列、ネットワークアクセス認証では Mac アドレスと共通パスワード文字列等) を認証に利用することができるが、Google Authenticator [5] で提供されているモジュールを追加することにより、RADIUS サーバで TOTP 認証を利用できるようになる。認証情報として、ユーザ ID とパスワード文字列の他、ユーザ ID とワンタイムパスワード文字列の 2 種類、ユーザ ID、パスワード文字列、ワンタイムパスワード文字列の 3 種類を組み合わせる利用することができる。

具体的には、認証情報の後半の項目であるパスワード文字列にワンタイムパスワードを連結した文字列を照合し、ワンタイムパスワードによる認証を実現している。ワンタイムパスワードを認証情報として利用する場合、認証情報の前半の項目であるユーザ ID は

RADIUS のデータベースに登録せず、RADIUS サーバ上のユーザとして作成する。ユーザのホームディレクトリに TOTP 認証に必要な秘密鍵と設定情報を記述したファイルを置き、モジュールはそれらのファイルを確認して TOTP 認証を行う。以下に RADIUS による TOTP 認証の手順を示す。

- ① クライアント（認証情報を入力する機器）から認証情報を含むリクエストを RADIUS サーバに送信する。
- ② モジュールが呼び出されて、リクエストのユーザ ID とパスワード文字列からユーザの TOTP 設定情報を確認する。
- ③ ユーザの秘密鍵から TOTP を生成し、クライアントから送信された TOTP と照合する。
- ④ TOTP による認証が成功した後、RADIUS サーバ上のパスワード認証が行われる。
- ⑤ RADIUS サーバからクライアントに認証の可否を返信する。

本論文で提案する認証システムでは、Google Authenticator のモジュールを利用し、RADIUS サーバ上で TOTP 認証を実現している。

3 認証システムの構成

本研究の目標は、情報システムに手を入れず、ワンタイムパスワードを使用した多要素認証を実現する認証システムの構築である。このような認証システムの場合、クライアント端末と情報システムを論理的に接続するネットワーク経路上のいずれかの地点に認証システムを設置することになるが、認証システムの管理のしやすさの観点から、クライアント端末が所属する組織のネットワーク内に設置するか、情報システムが所属する組織のネットワーク内に設置することになる。クライアント端末が所属する組織のネットワーク内に設置するような場合、ネットワークの入り口（もしくは出口）となる L2 スイッチや無線 LAN アクセスポイント等に認証処理を組み込む構成が一般的である。情報システムが所属する組織のネットワーク内に設置する場合、情報システムの直前に配置されるリバースプロキシや WAF (Web Application Firewall) 等に認証処理を組み込む構成が考えられる。提案システムでは、後述の情報システムが所属するネットワーク内に設置する方式を採用するが、提案システムの概要を明確にするため、両方の設置形態の認証システムについて説明する。

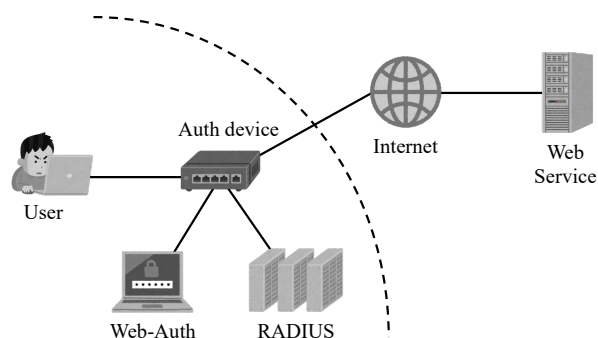


図 2: クライアント端末のネットワーク内に認証システムを設置する場合の機器の構成図

3.1 クライアント端末のネットワーク内に設置

クライアント端末が所属する組織のネットワーク内に認証システムを設置する場合、L2 スイッチや無線 LAN アクセスポイント等に認証処理を組み込む構成が一般的であり、多くの組織で実現している [6]。このような構成では、クライアント端末のブリッジやゲートウェイとなる L2 スイッチや無線 LAN アクセスポイント、認証情報を入力するための認証 Web サーバ、認証データを提供するための RADIUS サーバ等の機器が必要である。認証 Web サーバと RADIUS サーバの機能を L2 スイッチや無線 LAN アクセスポイントに内包する単体の機器も存在する。

組織ネットワーク内に設置する場合の機器の構成を図 2 に示す。認証スイッチは、情報システムへのアクセスを試みるクライアント端末からの通信を遮断、認証 Web サーバへリダイレクト、認証情報を RADIUS サーバへ送信する等の役割をもつ。クライアント端末から情報システムへの通信を Captive Portal 等の技術により認証 Web サーバにリダイレクトし、認証が許可された後、情報システムへのアクセス制限を解除する。以下にクライアント端末から情報システムにアクセスできるまでの手順を示す（図 3 参照）。

- ① 端末から情報システムにアクセスする。
- ② 認証スイッチが端末からの通信を検知し、認証 Web サーバに通信をリダイレクトする。
- ③ ユーザは認証 Web ページで認証情報を入力する。
- ④ 認証用 Web サーバは認証情報を認証スイッチに送信し、認証スイッチは認証情報を RADIUS サーバに送信する。
- ⑤ RADIUS サーバで認証処理（マッチング）を行い、認証の可否を認証スイッチに返信する。
- ⑥ 認証スイッチは認証可の場合に認証スイッチの通信制御を更新し、端末から情報システムにアクセ

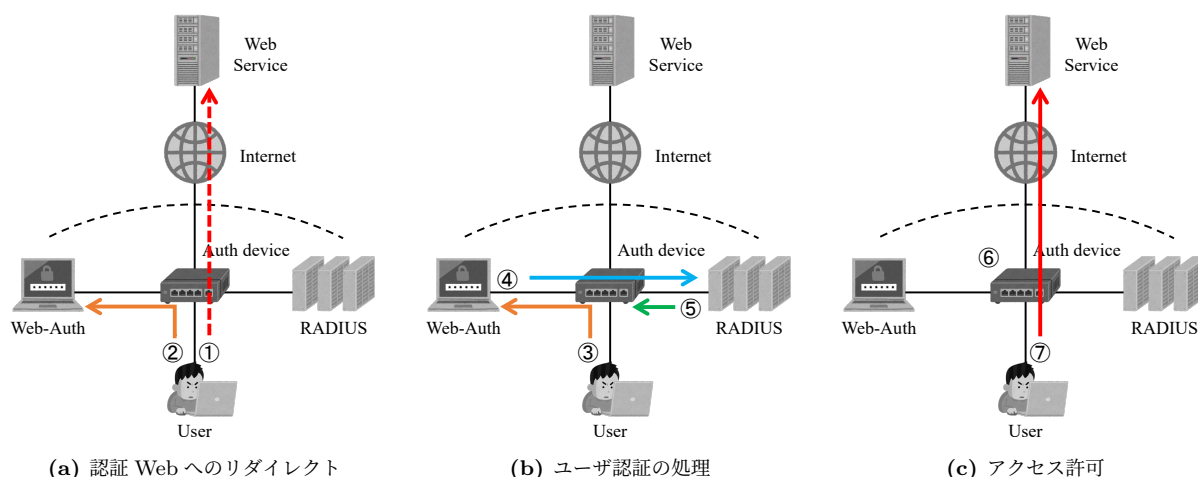


図 3: クライアント端末のネットワーク内に認証システムを設置する場合の認証フロー

スできるよう変更する。

⑦ 端末から情報システムにアクセス可能となる。

手順⑥において、認証スイッチでフィルタリングによるアクセス制御の他、認証の可否に基づき VLAN を動的に切り替える方式もある。

クライアント端末が所属する組織のネットワーク内に認証システムを設置するような構成は、許可されたユーザのみに組織のネットワークを利用させる、という環境の実現に適したものである。一方このような構成では、情報システムは依然としてインターネット上からのパスワードリスト攻撃等には無力であり、安全性の高い構成が求められる。

3.2 情報システムのネットワーク内に設置

情報システムが所属する組織のネットワーク内に認証システムを設置する場合、情報システムの直前に配置されるリバースプロキシや WAF 等に認証処理を組み込む構成が考えられる。提案システムは、既存の情報システムのネットワーク構成を変更しないブリッジ接続、すなわちネットワーク透過である認証システムを提案する。このような構成も、提案する認証システムを実現するための認証スイッチの他、前小節の構成と同様、認証 Web サーバ、RADIUS サーバ等の機器が必要である。

情報システムが所属する組織ネットワーク内に設置する場合の機器の構成を図 4 に示す。提案システムの核となる認証スイッチは、デュアルポートの NIC を搭載する PC サーバをブリッジ化して構築している。クライアント端末からのアクセス制御は iptables を使用し、認証が許可された端末の IP アドレスをアクセス制限を解除する方式を採用する。以下にクライアント

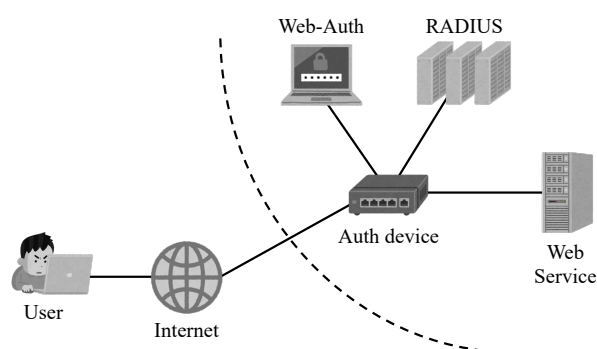


図 4: 情報システムのネットワーク内に認証システムを設置する場合の機器の構成図

端末から情報システムにアクセスできるまでの手順を示す（図 5 参照）。

- ① 端末から情報システムにアクセスする。
- ② 認証スイッチが端末からの通信を検知し、認証 Web サーバに通信をリダイレクトする。
- ③ ユーザは認証 Web ページで認証情報を入力する。
- ④ 認証用 Web サーバは認証情報を認証スイッチに送信し、認証スイッチは認証情報を RADIUS サーバに送信する。
- ⑤ RADIUS サーバで認証処理（マッチング）を行い、認証の可否を認証スイッチに返信する。
- ⑥ 認証スイッチは認証可の場合に認証スイッチの通信制御を更新し、端末から情報システムにアクセスできるよう変更する。
- ⑦ 端末から情報システムにアクセス可能となる。

認証スイッチは、初期設定としてすべての IP アドレスから情報システムへの通信を拒否する設定を登録しておく。手順②について、HTTP 通信であれば認

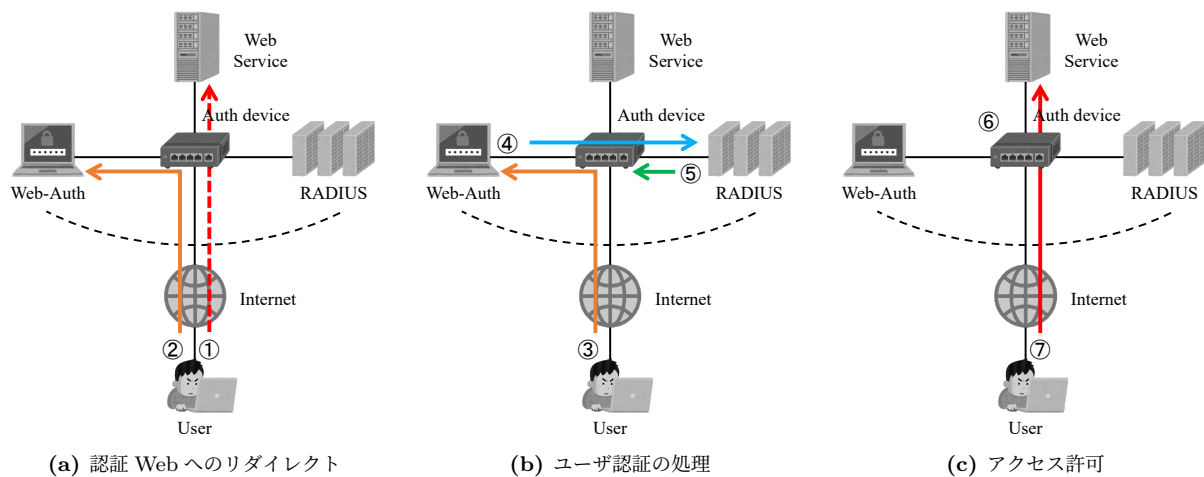


図 5: 情報システムのネットワーク内に認証システムを設置する場合の認証フロー

証 Web サーバにリダイレクトすることができるが、HTTPS 通信をリダイレクトすることはできない。また、端末からの通信はインターネットを経由して情報システムに届くため、Captive Portal 等の技術を利用することもできない。したがって、運用上はユーザに対してあらかじめ認証 Web サーバの URL を周知しておき、ユーザ自身で認証 Web サーバにアクセスする必要がある。提案システムでは、手順③でユーザ ID、パスワード文字列、ワンタイムパスワードの 3 種類を認証情報として利用したが、前節で述べたとおり、ユーザ ID とワンタイムパスワードの組合せでも利用可能である。手順⑥では、認証が許可された IP アドレスを iptables に設定する。

提案システムの構成では、認証情報としてワンタイムパスワードを利用することによって、情報システムはインターネット上からのパスワードリスト攻撃等に対して一定の耐性をもつと考える。多要素認証を実装し、認証が許可された端末の IP アドレスからのアクセス制限を解除するため、インターネット上からの不特定多数の IP アドレスからの攻撃を防御することが期待できる。

4 提案システムの評価

提案システムの利点と欠点を述べる。はじめに利点について、本研究の目的でもあるが、多要素認証の導入により、情報システムへのサイバー攻撃に対するセキュリティが向上する。また、提案システムを情報システムのネットワーク内にブリッジ接続して設置するため、クライアント機器、情報システムの双方を改変する必要がなく、これらの機器が所属するネットワークの設定を変更する必要もない。提案システムは、情

報システムの認証の安全性を強化することを目的として構築したものであるが、その仕組み上、多要素認証付きの簡易ファイアウォールとしても利用可能であると考えられる。例えば VPN 接続は、拠点となるネットワークに VPN 機器を設置し、クライアント機器に専用ソフトウェアを導入することで実現するが、提案システムも同様に拠点のネットワークに提案システムを設置すれば、クライアント機器に専用ソフトウェアを導入することなく、認証が許可された端末のみ拠点のネットワークにアクセス可能となる。通信の暗号化に関しては、別途 HTTPS や SSH 等でアクセスすればよい。

一方、欠点について、提案システムは IP アドレスのみでアクセス制限しているため、NAT 機器の配下のある端末で認証が許可された場合、同じ NAT 機器配下のすべての端末が認証状態を共有してしまう。これは提案システムに限った欠点ではなく、IP アドレスのみでアクセス制限する機器全般の問題である。

5 まとめと今後の課題

本研究は、既設の情報システムのソフトウェアを改変することなく、その情報システムでワンタイムパスワードを使用した多要素認証を実現する外付けの認証システムを提案した。提案システムの仕組み上、多要素認証付きの簡易ファイアウォールとして利用することもでき、多様な用途に転用できると思われる。しかしながら、提案システムを実際のネットワーク環境で運用しておらず、利用者の利便性に関する評価や運用上の評価は不十分のままである。これらの評価について、今後の課題としたい。

参考文献

- [1] 株式会社セブン&アイ・ホールディングス, 「7pay (セブンペイ)」サービス廃止のお知らせとこれまでの経緯, 今後の対応に関する説明について, 2019. <https://www.sej.co.jp/company/important/201908011502.html>
- [2] K. Thomas, A. Moscicki, New research: How effective is basic account hygiene at preventing hijacking, 2019. <https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html>
- [3] RFC6238, TOTP: Time-Based One-Time Password Algorithm, 2011. <https://datatracker.ietf.org/doc/html/rfc6238>
- [4] M. Kliewe, Google Authenticator PHP class, 2019. <https://github.com/PHPGangsta/GoogleAuthenticator>
- [5] Google, Google Authenticator PAM module, 2024. <https://github.com/google/google-authenticator-libpam>
- [6] 山本一幸, 青山茂義, 三河賢治, 動的 VLAN を利用した新潟大学無線 LAN システムの設計と運用, 学術情報処理研究, vol.18, no.1, pp.43–52, 2014.