パスワードマネージャのセキュリティ向上手法

八木佐和子[†1]　田中英彦[†1]

概要：インターネットが社会基盤と化し，ネットサービスの利用が一般化した今日において，ID とパスワードを用いた認証システムは欠かせないものとなっている．だが，相次ぐ不正アクセスの被害によりその評価に変化が生じている．特に問題視されているのは 2013 年頃から多発しているパスワードリスト攻撃だ．
これを防ぐには複数のアカウントに対してそれぞれ異なるパスワードを設けるのが対策に挙げられるが，その為のパスワード管理の煩雑さに辟易して，対策を疎かにしてしまう利用者が後を絶たない．
これの解決策として，パスワード以外の認証システムに移行する流れも目立ちつつあるが，依然として現状は ID/パスワードによる認証システムの方が主流だ．パスワード管理と上手く付き合える方法が今，強く求められている．
そこで本研究ではパスワードマネージャ(PM)と呼ばれる，アカウント毎に設定した異なる ID/PASS の記憶/保管を一手に担うツールに着目し，その有用性と懸念事項を調査し，PM の安全性をより高める新規手法の提案を行う．

キーワード：パスワード，パスワードマネージャ(PM)

Consideration of Security Improvement for Password Manager System

SAWAKO YAGI[†1]　HIDEHIKO TANAKA[†1]

Abstract: Today Internet is social infrastructure and net services are popular. Login system with ID and password is general authentication system to use the net services. But, the assessment of people is weak because it allows victims of unauthorized access. In particular, password-list-attack that has begun in 2013 is big problem.
We should stop using the same password in multiple accounts to prevent this attack. But they are difficult because there are many people who cannot cope with so many service accounts. Solutions of this situation are using other authentication system-for example, fingerprint authentication system, one-time-password system and CAPTCHA, but these systems aren't more popular than passwords system. So, efficient management of passwords is required for people.
In this paper, we focus on password manager (PM). PM is a tool which can store the different passwords for multiple accounts. We survey usability and problem on PM. And, show some improvements as counter methods.

Keywords: Password, Password manager(PM)

1. はじめに

インターネットが普及した現在，企業・行政機関・個人問わず社会全体でネットを利用した情報通信システムが使われている．これを効率良く利用する為に多く用いられている技術がパスワードを用いた認証システムであり，web アプリケーション等の情報通信システムを利用する際には必要不可欠なものとなっている．

だが，近年ではパスワードリスト攻撃等から発生する不正アクセスの被害によってその評価に変化が生じており，それに伴う煩雑なパスワードを管理しなければいけない問題に多くのユーザが悩まされている．

この問題を解決するのに，本研究ではパスワードマネージャ(PM)と呼ばれるパスワードを管理するツール/機能が有用であると考えている．しかし世間の PM に対する評価は低く，その普及率は決して高いとは言えない．

これは PM の機能特徴からセキュリティに関わる複数の問題点が存在する為ではないかと本稿では仮説を立て，このような PM に付随している問題を解決する為の方式を本論文では提案する．

本研究の目的は，PM のセキュリティ問題を解決する方式提案を行う事で PM の安全性を向上させる事である．

PM の安全性が高まる事により PM の有用性と普及率を底上げし，パスワード認証技術に生じている煩雑なパスワード管理問題の解決に繋げていく事が最終目標である．

2. パスワード認証システムの現状

2.1 パスワード認証システムについて

インターネットの普及により情報通信システムが社会基盤と化している今日では，大衆が様々な情報通信システムを利用しており，特に近年ではスマートフォンの普及によりその傾向は増加し続けている．

同じ情報通信システム，またはそれを通じて提供されるサービスシステム等を不特定多数のユーザが使用するとなると，倫理観から個人情報やプライバシーを守る事と，効率化の為に互いの作業を切り分ける事が必要であり，その為に使われているのが認証システムである．

†1 情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2014年に発行されたIPAオンライン本人認証方式の実態調査報告書[1]によれば,認証を行う手段は様々なものがあるが，パスワードを用いた認証システムが最も強く支持されている事が図1から窺い知れる.

同時に不正アクセス行為の犯行手口の内訳を示した図2を見ると，一番の原因として挙げられるのが「利用者のパスワード設定管理の甘さ」で，この点に付け込んだ攻撃の代表格に近年多発しているパスワードリスト攻撃が挙げられる.

	ID・パスワード	第二認証	秘密の質問	CAPTCHA	マトリクス・乱数表	OTP	OTP（スマートフォン）	複数要素OTP
金融	34	17（50%）	1（3%）	0	9（26%）	18（53%）	14（41%）	0
通販・物販購入	26	0	0	2（8%）	0	0	0	0
オンラインゲーム	9	0	1（11%）	2（22%）	0	2（22%）	1（11%）	1（11%）
交通・運輸・旅行	22	0	0	0	0	0	0	0
学習・教育・就職	3	0	0	0	0	0	0	0
ポータルサイト	8	1（13%）	3（39%）	0	0	1（13%）	3（39%）	0
情報通信・提供	25	1（4%）	1（4%）	1（4%）	0	0	1（4%）	0
通信・放送・報道	6	0	0	0	0	0	0	0
	133	19	6	5	9	21	19	1

図1　サービス別ごとの認証方式の比率

手口分類	平成24年		平成25年	
利用権者のパスワードの設定・管理の甘さにつけ込んだもの	122	22.9%	767	79.5%
言葉巧みに利用権者から聞き出した又はのぞき見たもの	229	43.0%	64	6.6%
識別符号を知り得る立場にあった元従業員や知人等によるもの	101	19.0%	56	5.8%
共犯者等から入手したもの	22	4.1%	35	3.6%
スパイウェア等のプログラムを使用して識別符号を入手したもの	29	5.5%	25	2.6%
フィッシングサイトにより入手したもの	18	3.4%	9	0.9%
他人から購入したもの	0	0.0%	7	0.7%
その他	11	2.1%	2	0.2%
合計	532	100.0%	965	100.0%

図2　不正アクセス行為に係る犯行の手口の内訳

2.2 煩雑なパスワード管理問題

パスワードリスト攻撃は ID/パスワードを複数の異なるサイトで使い回しているユーザを狙って行われる攻撃で，2013年から2014年に掛けてmixi，Facebook，LINEなどの有名アプリが攻撃を受けた事でその知名度は急上昇した.

これを受けて多くのユーザが認識を改める一方，パスワードリスト攻撃の対策として挙げられるパスワードの使い回しを辞めようとすると，下記のような悪循環に陥ってしまう場合がある.

・簡単なパスワードを使用する→総当たり，辞書攻撃の餌食になる
・難しいパスワードを使用する→使い回しを狙うパスワードリスト攻撃の餌食になる
・複数個の難しいパスワードを運用する→記憶ではまかない切れなくなる
・記憶ではまかない切れないので何らかの管理方法を考える→管理が煩雑化する

このような煩雑なパスワードの管理に耐えられず，対策を怠ってしまう利用者が多く居る事は度々示唆されており，結果依然として不正アクセスが続いてしまっている事が図3から分かる.

このようなセキュリティの為に煩雑なパスワードを利用し管理しなければいけない「煩雑なパスワード管理問題」が今，パスワード認証システムを利用する上で問題となっており，これを解決するのに本研究ではパスワードマネージャ(PM)が有用なのではないかと仮説を立てている.

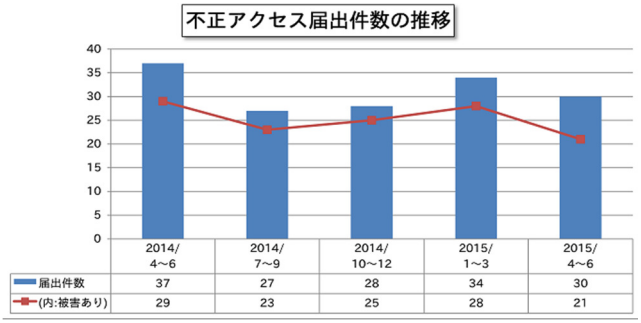

図3　不正アクセス届出件数の推移[2]

3. パスワードマネージャ(PM)について

本章では，調査で判明したパスワードマネージャ(PM)に関する事柄についてまとめあげていく.

3.1 PMの説明

3.1.1 概要

PMは古くから存在するパスワード管理ツール/機能である.ユーザが覚えきれない・管理しきれないIDやパスワードを,ユーザに代わって管理するのがPMの主な目的であり,フリー/シェア問わず様々な組織・個人が異なる形で開発提供をしている.その為，PMのあり方を一概にまとめるのは難しいが，往来より使われているのはユーザが覚えられない複数のパスワードを識別対象であるID，関連キーワード，他要素(ドメイン，URL 等)と紐づけて「記憶」し，これらのデータベース(DB)に記憶した資格情報を「保管」する形態が多くみられる.

3.1.2 PMの種類について

パスワードを逐次生成する逐次生成型と，3.1.1 で先述したDB保存型が存在する.DB保管型を更に分類づけるなら,記憶している資格情報を保管するDBの置き場所によって以下3つのパターンに分けられる.

■DBが専用ハードウェアに保管されるパターン

資格情報 DB を専用ハードウェア内に置く形態.データを蓄えた端末が基本的にはネットワーク接続から隔絶されている事と，小型端末なので簡単に持ち運び出来るのが特

徴に挙げられる.

■DB がローカルコンピュータ内に保管されるパターン

PM をインストールした(ローカル)コンピュータ/ハードディスク内に資格情報 DB が作られる.スタンドアローンアプリ等のように他の機器に依存しない単独コンピュータに関連する資格情報を対象に管理させる場合が多い.

■DB がクラウド/サーバ上に保管されるパターン

資格情報 DB がクラウド上や PM 開発源元のサーバ上に作られる. この形態の PM を使用する場合, web サイトや web アプリケーションの資格情報を管理させる場合が多い. また,この場合には更に PM 自身の形態から以下 2 つに大きく分けられる.

・web ブラウザのプラグインを利用する場合
・同期機能を通じて web ブラウザ上で動作する場合

3.1.3 PM の機能について

PM は記憶, 保管以外にも様々な機能を持っている. これらの機能や特徴は PM により多種多様だが,いずれもセキュリティ・ユーザビリティ・利便性を向上させるのが目的である. 代表的な機能を以下にまとめる.

○セキュリティ面に係る機能

・マスター認証の利用

PM を利用する前に, 利用者が正規ユーザであるか確認する為にユーザが唯一覚えなければいけない「マスターID」「マスターパスワード」確認による認証を行う. この認証の事を「マスター認証」と呼ぶ.

・保管している資格情報の暗号化
・パスワード生成

○利便性・簡便性に係る機能

・リモートアクセス

PM とインターネットを通じて, どのような環境下からでもパスワード DB へアクセス出来る機能. ただし, 使用するコンピュータのプラットフォームや web ブラウザが, 対象 PM のサポート下に入っている事が必須.

・プラットフォーム間の同期

対象 PM がサポートされているプラットフォーム間で「同期」が行える機能. 同期とは, 同じデータを複数の場所で使用している際, 一ヶ所でデータが更新されると他で使用しているデータにも変更が自動的に反映され, 常に同一性が保持される事を指す.

・資格情報の共有

同期されたプラットフォーム間で, PM が保管しているパスワード DB 等の資格情報を共有する機能.

・自動入力

保管している ID/パスワードを, 対応する web アプリケーションのログインフォーム等へ自動的に入力する機能. PM によっては, その後にログインフォームの自動送信も行う. 対象サイトへアクセスしたと同時に行われるケースが多い.

3.2 PM の運用方法について

図 4 は実在する複数の PM がどのような機能特徴を持っているか大まかにまとめたものである. 本稿では実在する PM の中から Lastpass を取り上げて, どういった使い方が出来るかメリット/デメリットを挙げながらまとめていく.

△：有料化によって追加される機能
□：機能を利用するか選択可

	ミルパス	Keepass	Roboform	Lastpass	IE	Firefox	Chrome	Safari (Keychain)
無償提供		○	○	○	○	○	○	○
有料提供	○		△	△				
DB:専用ハードウェア	○							
DB:ローカル保存		○	□		○	○	○	□
DB:クラウドサーバ上保存		□	○	○	□	□	□	○
マスター認証の利用	○	○	○	○			□	○
資格情報の暗号化		○	○	○				
パスワード生成	○	○	○	○				
リモートアクセス		□	○	○	□	□	□	○
プラットフォーム間の同期		□	○	○	□	□	□	○
資格情報の共有		□	○	○	□	□	□	○
自動入力		□	○	○	□	□	□	○

図 4　各 PM の機能をまとめた表

■Lastpass[3]

サードパーティが開発したフリーミアムのソフトウェアで, マルチプラットフォームに対応している. PM をインストールすると, web ブラウザのツールバーに PM アイコンが表示されて,アイコンから PM マスター認証の入力フォームの表示や, DB へのアクセスが可能となる等, web ブラウザを通じて PM の機能が提供されるのが特徴.

web アプリへ資格情報の自動入力を行う機能により, ユーザが逐次パスワード等を DB リストからコピー/ペーストする必要性がなくなった. 他にも DB がクラウド/サーバ上にある為, インターネット接続環境が必須ではあるが, 不特定多数のデバイスから PM を使用する事が出来る. Android スマートフォンや iOS 端末対応のものもある為, 外出先等でも通信を経て資格情報を利用出来る. これらの事から,他 PM よりも利便性面で優れた一面があると言える.

反面, DB が保存されているクラウド/サーバ等に対する攻撃や, ネットワーク接続を利用した攻撃等から保管している資格情報が流出する可能性があり, 情報漏洩の際のリスクは他より大きいとされている.

3.3 PM の研究動向

3.3.1 国内の既存研究

照屋ら[4]の研究ではマスターパスワードの重要性と逐次生成型の PM について触れている.

既存研究が取り上げている逐次生成型 PM はマスターパスワードを用いて対象サイトに応じて都度パスワードを生

成する形態で，例えばwebアプリにログインしようした時には，対象webアプリのネットワークドメイン(URL等)とユーザが入力したマスターパスワードを，PM内のアルゴリズムに則って組み合わせる事で，対象webアプリのパスワードを逐次生成している．その為，マスターパスワードが第三者に知られてしまうと全てのパスワードの漏洩に繋がる恐れがあるとしている．

具体的には，PMを利用しているシステム内にキーロガーが仕込まれていると，マスターパスワードが発覚してしまい，資格情報の漏洩から不正アクセスに繋がってしまう恐れがあると指摘している．

3.3.2 国外の既存研究

Webブラウザのプラグインを利用して稼働するPMの性質とPMの自動入力に焦点を当てている．

Liら[5]の研究では，PMが動作するwebブラウザの脆弱性を突いた攻撃の危険性について触れている．webブラウザのプラグインを利用して動くPMは,現在のwebページのコンテキスト上でJavaScriptが実行される事により稼働する．これは，現在webブラウザが繋がっているwebページの環境によってPMの機能も左右されるという事であり，正規webアプリになりすましたevil.comや脆弱性により改竄されたwebアプリ等とwebブラウザが接続されたりすれば，PMへの攻撃が成り立ってしまう．

それ以外に，Silverら[6]の研究では攻撃者が悪意的に挿入した不可視インラインフレームによる攻撃ページへのリダイレクトによって，PMの自動入力機能が悪用される危険性があると述べており,一度に大量の資格情報がPMから搾取されてしまう可能性があるとしている．

4. PMの有用性と問題点の分析

4.1 PMの有用性検討

2章でパスワード認証システムは情報通信システムを利用する上で重要な一端を担っているが，攻撃の高度化に伴って管理が煩雑化してしまい，その事にユーザが対応しきれない状況にある事が判明した．これを解決するのにPMが有用であるか3章で判明した事柄を元に検討を行う．

PMには複数個のID/パスワード(資格情報)を記憶/保管出来る機能により，人間の記憶だけではまかないきれない不特定多数のパスワード管理を代替可能にすると言える．

また，PMにはランダムなパスワードを生成する機能もついている為，人間が安全性を考慮した難しいパスワードを態々考える必要性がなくなる上に，規則性がなくなる事で攻撃者にパスワードを推測される危険性を減少出来る．

それ以外にもPMのDBがクラウドサーバ上にある場合，webアプリのログインフォームに対して資格情報の自動入力機能が付随している事から，ユーザが情報を入力する手間が省略される.同期機能を用いてデスクトップ/モバイル/タブレット等を通じて,どこからでも資格情報を利用する事が出来る事から，利便性・簡便性の向上にも繋がる．

上述した事柄から，PMは従来パスワード認証システムにつきまとっていた煩雑なパスワード管理問題を解決するのに十分な有用性があると言える．また，それ以外にも安全性と利便性を向上させる機能も備わっている事から，PMは更に有用性のあるシステムであると言える．

4.2 世間のPM評価像

4.1でPMは煩雑なパスワード管理問題に有用である事が分かったが,ではPMはどれほど世間に浸透しているのか考察を行う．

PMに関する調査を行う上で大きく目につくのはPMを取り扱った参考文献の少なさだ．これは，PMが古くから様々な組織・個人が大小異なる統一性のない仕様携帯で開発・提供されている為に，その歴史や概要，特徴，分類等，PMに関する情報をまとめた資料や標準が存在しない事が最たる原因に考えられる．

このようなPMを評価した資料や動向が余りに少なく中途半端な状況を鑑みるに，PMは世間から十分な評価を受けていないと考えられる．

4.3 PMの現状分析

4.2の状況を改善するにはどうすればいいのか，PMの現状を分析する事でPMの問題点を考察するのに繋げる．

4.3.1 情報セキュリティインシデント事例からの考察

PMの評価が伸びない問題点を明示するにあたり，過去に起きたPMのインシデント事例から考察を行う.近年であれば，Lastpassのサーバが攻撃を受けた事でDBから資格情報が漏洩した事件[7]があった．

PMで発生するインシデント事例の代表格は，管理していた資格情報の漏洩であり，この際の情報漏洩は一般的なwebアプリやサーバからの情報漏洩とは規模が違う．PMが有している複数の資格情報が流出するという事は，鼠算式に不正アクセスが発生する事に繋がり，最終的には個人情報の流出や不正送金までの発展も考えられる．その為，インシデント発生時のリスクが非常に大きいのがPMの特徴と言えるだろう．

4.3.2 既存研究の対策案からの考察

照屋らの研究では，マスターパスワードを狙うキーロガー対策として，webアプリログインの際に携帯情報端末と連携を取る逐次生成型パスワード管理システムの構築を提案している．マスターパスワードの入力を携帯情報端末で行わせる事でキーロガーの対策としているが，常時携帯情報端末を用いてログイン認証を行うのは大きな手間となる

他，マスターパスワードが発覚した際の危険性に変化はない．なので，利便性を損ねずにマスターパスワードのセキュリティ負荷を分散させられる方法が必要と考えられる．

Li らの研究では，PM の機能が信頼されていない web ページのコンテキスト上で実行される事が原因の一つに挙げられるので，web ブラウザは隔離された安全な実行環境が保障されるべきだとしてアーキテクチャを提案しているが，頻繁にバージョンアップがなされて仕様が変わる IE や chrome 等の代表的な web ブラウザに対して，隔離された実行環境を作るのは一筋縄ではいかないと考えられる．

Silver らの研究では，ユーザの知らぬ間に自動入力機能が行われる危険性の対策に，自動入力が行われる際は自動入力を行う挙動をユーザに知らせて，決行するか否かをユーザに選択させる事が有効だとしている．またそれ以外にも正規のログインフォームを改竄して情報を搾取しようとする手法もある為，PM は自動入力の前にログインフォームが攻撃者の手により改竄されているか否か確認を取るべきだとしているが，マルウェアや動的スクリプトを読み込む事で起こりうる攻撃の対策については触れられていなかった．これは先述した Li らの既存研究にも言える事であり，web 上で引き起こされる多様な攻撃に上手く対応する必要性があると考えられる．

4.4 PM の問題点

4.3 の考察から，PM の普及率を妨げる弊害になっている問題点は大きく分けて以下の 3 点が挙げられると考える．

■インシデント発生時のリスクが大きい事
■セキュリティ/システム面でマスターパスワードに強く依存している事
■web 上からの多様な攻撃を受ける事

この問題点を改善すれば，PM の有用性を更に広めるのに貢献出来ると仮定し，以降の章ではこれらを解決する為の提案手法の説明を進めていく．

5. PM セキュリティ向上手法

5.1 対象 PM の絞り込み

4.4 で提示された問題点を解決する為の方式提案を行うにあたり，対象として扱う PM について定義する．

PM ランキングレビュー[8]を見ると，現在高い評価を受けているのは DB 型 PM の中でも DB をクラウドサーバに置いているものである．これは一重に昨今の情報通信システムのトレンドにクラウド技術が入っている事も影響として考えられるが，それ以外にも 4.1 で考察した通り，クラウドサーバに DB を置いた PM は利便性に優れた機能を提供出来る為であると思われる．

また，クラウドに DB が存在する PM の多くは web ブラウザと連携して，または web ブラウザそのものが PM として動作する．本研究の提案手法で用いる PM は前者の web ブラウザのプラグインを用いて web ブラウザと連携して稼働する PM を対象とする．これはプラグインを用いた方が実装や導入の観点から融通が利く為である．

5.2 対象 PM の基本的構造

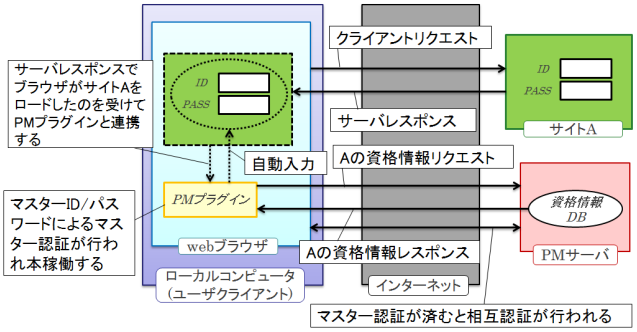

図 5　対象 PM の基本的構造と通信プロセスの概要図

5.1 で対象 PM の種類を絞ったが，具体的にこの PM はどのように稼働して PM サーバや web アプリと通信を行うか，基本的な構造とプロセスを図 5 に図示する．

本研究の提案手法で扱う PM は基本的に web アプリに関連した資格情報を保管しており，web アプリの資格情報をいかに安全且つ簡便に管理/運用補助するかで有用性が変わると想定する．

本研究が提案する手法は，基本的には図 5 の構造とプロセス通信を元に，提案する手法の仕様を追加してく．

5.3 提案手法の概要

5.2 で述べたような構造と通信プロセスを取る PM に対して起こりうる攻撃パターンは，大きく分けて 5 通りが想定される．図 6 は攻撃パターンのイメージを大まかにまとめたものであり，1 つずつ説明を記す．

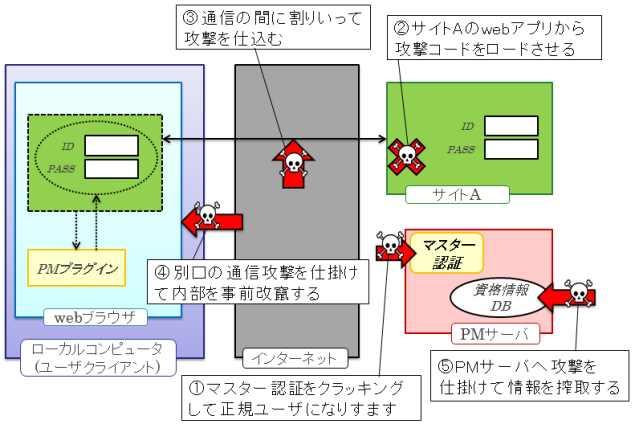

図 6　PM に対して起こりうる攻撃パターンの概要図

①PM マスター認証を突破して PM ユーザになりすまし，資

格情報を搾取する.
②サイト A に攻撃コードを仕込んでおき，web ブラウザがサイト A をロードした際に攻撃コードも一緒に読み込ませる．この際に読み込んだ攻撃コードにより資格情報等が攻撃者に搾取されてしまう.
③web アプリと web ブラウザ間の通信に割り込み，中間者として通信を改竄・取得する過程で資格情報を搾取する.
④事前にユーザクライアントへ攻撃を仕掛ける事で，正常な動作をしていたwebブラウザやPMプラグインを改竄してしまい，後程 PM が稼働した際に異常動作を起こさせる.
⑤PM サーバへ直接攻撃を仕掛けて PM 資格情報を搾取する.

本研究ではこの攻撃が仕掛けられるパターンの内 3 つ，①②③に焦点を当てた方式を提案する．具体的には以下 3 つの方式を提案する.

■リスクベース認証の導入
マスター認証へリスクベース認証の導入を行う．攻撃パターン①に対応.

■通信パケット取得・分析アダプタの追加
web ブラウザと web アプリ間の通信を取得分析するアダプタをローカルコンピュータ内に設けて，web ブラウザが接続しようとしている web アプリが正常であるか判断する．検知の判断材料には過去 web アプリから返されたレスポンスデータを基に行う．攻撃パターン②③に対応.

■PM 利用者の挙動を監視するシステム
PM サーバに設けたシステムが,PM を利用しているユーザが正規ユーザであるか否か，マスター認証後にユーザがサイト A へログインしようとした挙動時刻を過去のアクセス時刻の統計パターンと比較する事で判断する．攻撃パターン①に対応.

本稿では 6.1 でリスクベース認証の導入のみ詳細を記述する．これらの提案手法により 4.4 で提示された問題点が解決されるかの評価については 7.1 で，この提案手法の課題については 7.2 でまとめて表記する.

6. 提案手法の詳細

6.1 リスクベース認証の導入について

PM マスター認証を行う際，リスクベース認証を導入して認証を強化する為の方式/プロセスを提案する.図 7 はリスクベース認証が導入されたマスター認証プロセスを図示したものである.

ユーザが操作するローカルコンピュータには，対象 PM ソフトがインストールされており，通信で取り扱う情報の暗号化と復号化，ハッシュ計算等はローカル内で行えるようになっている.

web ブラウザのプラグインにより機能が提供される PM は，ブラウザツール上に PM マスター認証を行う為のログインフォームが設けられるので,直接 PM サーバへマスター認証情報を送る事が可能になっている.

リスクベース認証を PM マスター認証に導入するにあたり,PM サーバ側には ID/パスワード等の資格情報 DB の他に，過去にマスター認証を行った際のリクエスト通信のデータが貯められている履歴データ貯蓄が置かれており，このリクエスト履歴データを認証に利用するのが従来と異なる点である.

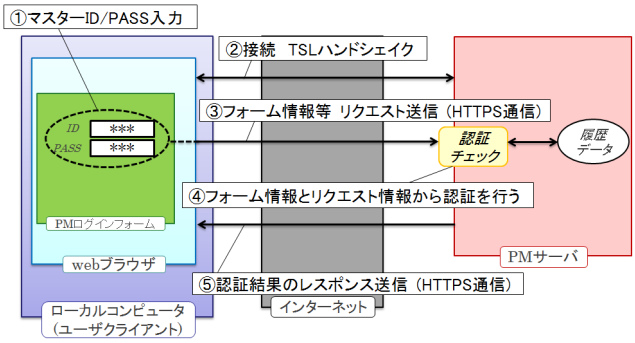

図 7　マスター認証のプロセス図

■リスクベース認証を導入したマスター認証のプロセス
前提としてプロセス開始時から終了時に至るまで，攻撃者やマルウェアの手による介入を受けていない状態である事とする.

まず，PM マスター認証のログインフォームに，ユーザはマスターID/マスターパスワードを入力する．（図 7 の①）ユーザがこれらの情報を送ろうと送信コマンドを行うと，システムはフォーム送信を行う前に，HTTPS 通信を行う為の TSL ハンドシェイクを web ブラウザと PM サーバ間で行い，相互認証した状態にする．（図 7 の②）

それからシステムはフォームに入力されたマスターID と，暗号化されたマスターパスワードまたはハッシュ関数で計算されたハッシュ値を HTTPS 通信で PM サーバへリクエスト送信する．同時に，クライアント IP アドレス，クライアントホスト名，ISP，OS，OS ver，web ブラウザ形式，使用言語，アクセス圏，アクセス時刻，cookie，uuid(ネットワークインターフェイスの MAC アドレス,IP アドレス,web ブラウザ形式とブラウザ情報等を連結したものをハッシュ化等して作られた固有識別子)等の情報をクライアントリクエストとして送付する．（図 7 の③）

PM サーバは図 7 の③で送られてきた情報を元に【認証プロセス】へ移行する．（図 7 の④）

【認証プロセス】【リスクチェック】【追加認証】のプロセスをクリアしてマスター認証が済んだ場合，図 7 の③で送られてきたリクエスト情報は履歴データに日付/時刻と

共に保存される.

【認証プロセス】
①マスターIDとそれに紐づいた資格情報がPMのDB内に存在するか確認する．存在すればマスターPASSの確認へ，存在しなければ「IDが存在しない」とクライアントへレスポンスする．（図7の⑤）
②マスターID に対してマスターPASS が同一であるか確認する.OKなら【リスクチェック】へ,NOなら「マスターPASSが合っていない」とクライアントへレスポンスし，マスター認証の失敗回数を＋1回履歴に残す．（図7の⑤）

【リスクチェック】
PMサーバ側には，過去に送られてきたクライアントリクエスト情報をマスターID 毎に紐づけて貯蓄している履歴データがある．この履歴データの内容と，今回のリクエストの内容とを比較して，通常のアクセスをしてきている正規ユーザであるか否かを判定する為のリスクの点数付けを行う．図8はチェックする項目，チェックする基準，チェックで判別する特徴をまとめたものである.

これらの項目チェックを終えた後，リスク閾値が事前に決めていた基準点を越えなければ通常通りのアクセス(正規ユーザ)であると判断し，PM マスター認証後にクライアントへ渡される情報をクライアントへレスポンスとして返す．（図7の⑤）

リスク閾値が基準を超えた場合は正常ではないリクエストであると判断し，クライアントへ【追加認証】を要求する.

チェック項目	分岐点	判断の内容
・同一クライアントIPアドレスが履歴の中に存在するかチェックする	対象の値が履歴の中に存在すれば通過 存在しなければ、 項目の重要度毎に異なる点数を リスク閾値へ加点する	通常とは異なるネットワーク環境からのアクセスか判断する
・同一クライアントホスト名が履歴の中に存在するかチェックする		
・同一ISPが履歴の中に存在するかチェックする		
・アクセス圏(国)が履歴の中に存在するかチェックする		通常とは異なる位置情報からのアクセスか判断する
・同一uuidが履歴の中に存在するかチェックする		通常とは異なる端末、webブラウザ、ネットワーク環境からのアクセスか判断する
・既知のCookieがリクエスト内に存在し、その数値が正しいものであるかチェックする	対象cookie値が正しければ通過、 誤っていれば項目の重要度毎に 異なる点数をリスク閾値へ加点する	Cookie sessionの接続の有無 Cookieを利用した接続の簡易化
・前回のマスター認証サインアウト後に行われたマスター認証失敗回数が何回であるか履歴からチェックする	失敗回数が任意の回数を超えていればリスク閾値へ加点する	試行錯誤攻撃を受けているかどうか判断する
・アクセス時刻が正規ユーザが利用する時間帯内であるか履歴と比較し、チェックする	履歴に残っている過去のアクセス時間の総分布と比較し、確立の低い所ほどリスク閾値に多く加点する	正規ユーザのアクセスであるか行動パターンから判断する
・クライアントリクエスト内に指定されたヘッダー、及び値を含んでいるかチェックする	事前に指定されたヘッダー、値を含んでいれば通過、 含んでいなければリスク閾値へ加点する	正常な指定条件を満たしているかにより正規ユーザであるか判断する

図8　リスクチェック項目のまとめ

【追加認証】
リスクチェックでクライアントが通常と違うと判断されたので,追加の認証チェックをクライアントに要求する.追加認証で使われる認証手段としては，秘密の質問と対応する答えを確認する，登録したスマートフォンに送信した認証コードや SMS，ワンタイムパスワード等を入力させる事で確認を取る手法等が挙げられる.

この追加認証をクリアすれば正規ユーザと判断されてPM マスター認証後に渡される情報をクライアントへレスポンスとして返し，クリア出来なければ「追加認証が合っていない」とクライアントへレスポンスを返す.(図7の⑤)

■実装方法について
OpenAM[9]と呼ばれるオープンソースソフトウェアを利用すれば実装出来ると考えている．OpenAMとは，シングルサイオン(SSO)を実現する為に開発されたオープンソースソフトウェアで，複数のシステムへのサプライサイドプラットフォーム(SSP)，認証の強化，アクセス制御，フェデレーション（クラウドサービスへの SSO）等の機能を実装しており，用意されている認証モジュールを組み合わせる事で柔軟性のある認証システムを構築出来る.

7. 考察

7.1 提案手法の評価

4.4で提示されたPMの問題点が，提案した手法により解決されているか問題点毎に考察を行う．従来の手法との違いについても記しながら評価を行う.

■マスターパスワードへ依存している点について
6.1 で説明したマスター認証にリスクベース認証を導入する方式によって解決が出来ると考えられる．マスターパスワード以外にも複数の要素を認証で利用する為，マスターパスワードへの依存度は軽減・分散される．また，マスターパスワードだけで認証を行っていた際よりも認証強度も底上げされる為，総じて安全性向上にも繋がっている.

また，運用面においても普段利用しているネットワーク環境からのアクセスであれば追加認証は生じない為，利便性が損なわれる事もない事から，従来のものより安全性・利便性を強化出来たと評価出来る.

■web 上の脆弱性によって起きる多様な攻撃に関して
5.3 で触れた通信パケット取得・分析アダプタの追加により一定の解決が出来ると考えられる．前提として，本研究で提案した手法で全ての異常性(攻撃)に対して完全な検知を行う事は不可能であるが，正常であるか否かの判断確率を高める為の材料を提示したという点では一定の有用性があると評価出来る.

また，この度提案したこの手法はwebの通信を監視するものである為,この方式を用いる事でPMだけでなくリモートコントロール等のような，web 通信全体のセキュリティ向上にも繋げられる.逆を言えばPMのセキュリティを考慮するならば情報通信の安全性そのものを向上させる事が大事であると明示した点が,他研究との違いであると言える.

■インシデント発生時のリスクの大きさについて
5.3で触れたPM利用者の挙動を監視するシステムで一定

の解決が出来ると考えられる．マスター認証後にも利用者の動向を監視する事で，PM を通じた不正アクセスを直前に検知する．その為，特定の場合による情報漏洩は一定の確率で解決出来ると評価出来る．

7.2 提案手法の課題

1.リスクベース認証の導入について

リスクベース認証は普段通りのネットワーク環境からアクセスする分には利便性に差異は生じないが，旅行や出張，外出先や派遣先等から認証を行う際は必ず追加認証が生じてしまうので，その点は課題である．また，マスターパスワードを搾取しようとするキーロガー等を直に防ぐ事は出来ないので,その点に関しても他の工夫が必要である．

2.web アプリケーションとの通信分析アダプタ

実装方法についてと，web アプリを構成するリソースの変動が激しい中で，web 通信上攻撃判断の基準を少しでも増やす為に今回は過去のレスポンスデータを利用する案を取っているが，過去のレスポンスデータを使う事で，どれ程の効果が期待できるか具体的数値を評価していく事が今後必要である．

3.時刻を利用した PM 利用動向の監視

実装方法についてと，PM を利用しているユーザが正規か否か判断を行う判断基準が過去のアクセス時刻の統計データに依存している為，過剰検知が起きる可能性がある．過剰検知が起きる具体的数値を評価する事と，これを和らげる為の対策が必要とされる．

8. まとめ

8.1 研究成果

パスワード認証システムは情報通信システムを利用する上で欠かせない認証技術の一端を担っている．しかし，攻撃の高度化に伴いパスワード強度を上げると管理が煩雑化してしまい，その事にパスワード利用者達が対応しきれない現状が続いている事が調査で判明した．

この現状に対する対策について，本研究では以下のような成果を残せた事を記す．

1.煩雑なパスワード管理問題を解決するのに複数のパスワードを記憶/保管する PM は有用である事
2.PM の有用性を広める為に，セキュリティ向上の手法を幾つか提案した事
3.提案方式に対する考察を行い，評価と課題をまとめた事

8.2 今後の展望

煩雑なパスワードの管理問題を解決するのに本研究では PM が有用であると述べてきたが，FIDO Alliance[10]によるパスワードをなくした認証技術の導入や，OpenID[11]の SSO の浸透によって，パスワードを利用した認証システムの減退化が今後の展望の一つとして考えられる．

特に SSO の浸透によりシステム間が繋がって認証ポイントが収束するという事は，不正アクセス等の攻撃が仕掛けられる機会を減らせる上に，セキュリティ対策も一点に集中強化させられる分,総じて安全性の向上に繋がっていく．(本稿で提案した手法に用いたリスクベース認証は SSO の認証時にも使われている技術である．)

反面，現実的観点から SSO が世界的レベルにまで浸透する事やパスワード認証が完全になくなる事態も想定は出来ない．そういった場合には変わらず煩雑なパスワード管理問題が生じる為，PM のようなパスワード管理ツールは変わらず有用であり続けると考えられる．

参考文献

[1] "IPA オンライン本人認証方式の実態調査報告書". (2014) https://www.ipa.go.jp/files/000040778.pdf
[2] "IPA 不正アクセス届出状況". (2015.07.24) https://www.ipa.go.jp/security/txt/2015/q2outline.html
[3] "LastPass" https://lastpass.com/
[4] 名桜大学 照屋寛直，中村航，天願健，田邊勝義: 神戸大学大学院工学研究科 古本啓祐，森井昌克 「パスワードリスト攻撃に対抗するパスワード管理とシステム構築-マスターパスワードの保護の提案」電子情報通信学会技術研究報告 ICSS2013-70 pp.49-52 (2014)
[5] Zhiwei Li, Warren He, Devdatta Akhawe, Dawn Song, University of California, Berkeley: The emperor's new password manager security analysis of web-based password managers. 23rd USENIX Security Symposium. (2014)
[6] David Silver, Suman Jana, Dan Boneh, Stanford University: Eric Chen, Collin Jackson, Carnegie Mellon University. Password managers: attacks and defenses. 23rd USENIX Security Symposium. (2014)
[7] "ITmedia エンタープライズ 鈴木聖子 「パスワード一元管理の LastPass にハッキング，情報流出も」" (2015.06.16) http://www.itmedia.co.jp/enterprise/articles/1506/16/news050.html
[8] "password manager software reviews". http://password-management-software-review.toptenreviews.com/
[9] "FORGROCK-Products-Access Management-OpenAM". https://www.forgerock.com/products/access-management/
[10] "FIDO Alliance". https://fidoalliance.org/
[11] "OpenID ファウンデーション Japan". http://www.openid.or.jp/