Vol.2021-CSEC-94 No.19
Vol.2021-SPT-43 No.19
2021/7/19

パスワード構成ポリシー自動取得技術の開発：Web 上認証サイトのパスワード構成ポリシー表示方法に関する大規模調査

藤田真浩[†1]　山中忠和[†1]　松田規[†1]　金岡晃[†2]

概要：多くの認証システムでは，ユーザーに求めるパスワード構成ポリシーを設定し，そのパスワード構成ポリシーを満たすように生成されたパスワードのみ登録を許可する場合が多い．たとえば，「英数字を混ぜた 8 文字以上」といったポリシーである．本研究では，Web 上のパスワード認証システムのユーザーアカウント登録ページからパスワード構成ポリシーを自動的に取得する技術の実現を研究のゴールとする．本論文は，本研究の初報であり，本技術の必要性や有効性について詳細に論じた．そのうえで本技術の実現のためには，①パスワード構成ポリシーの表示方法の調査，②パスワード構成ポリシー文字列の取得技術の開発が必要となることを示した．その後，①を実施し，パスワード構成ポリシーが掲載されているサイトをクラウドソーシングによって収集し，パスワード構成ポリシーの表示方法について調査した．この結果，クラウドソーシングを通じて計 443 件の認証サイトの収集に成功した．収集したこれらサイトの登録ページを分析した結果，パスワード構成ポリシーの表示方法は 4 パターンに分類できることを明らかにした．

キーワード：パスワード認証，パスワード構成ポリシー，ユーザビリティ

Development of Password Composition Policy Automatic Acquisition System: Comprehensive Survey of Display Methods for Password Composition Policy on Web Authentication Systems

MASAHIRO FUJITA[†1]　TADAKAZU YAMANAKA[†1]
NORI MATSUDA[†1]　AKIRA KANAOKA[†2]

Keywords: Password Authentication, Password Composition Policy, Usability

1. はじめに

1.1 背景

ユーザー認証技術は，認証に用いる要素によって，パスワード認証，持ち物認証，生体認証という三つの認証方式に大別される．これらの要素を複数個組み合わせた多要素認証や複数回組み合わせた多段階認証を採用する認証システムが増えてきており[1]，ユーザーのおかれている環境によって動的に認証方式を変更する認証システムも数多く提案がなされているが[2][3]，依然として，多くの認証システムでは，パスワード認証を採用している．多要素・多段階認証システムや動的に認証方式を変更する認証システムにおいても，要素技術としてパスワード認証が採用される場合が多い．

パスワード認証の安全性を担保するためには，ユーザーが強固なパスワードを登録することが肝要である．これを達成するために，多くの認証システムでは，ユーザーに求めるパスワード構成ポリシーを設定し，そのパスワード構成ポリシーを満たすように生成されたパスワードのみ登録を許可する場合が多い．たとえば，「英数字を混ぜた 8 文字以上」といった構成である．

本研究では，Web 上のパスワード認証システムのユーザーアカウント登録ページ（以下，単に「登録ページ」）からパスワード構成ポリシーを自動的に取得する技術（以下，「パスワード構成ポリシー自動取得技術」）を研究のゴールとする．パスワード構成ポリシーに関しては多くの既存研究や取り組みが存在する．しかし，筆者が知る限り，パスワード構成ポリシー自動取得技術について検討した文献は存在しない．実際，多くのパスワードマネージャーでは，使用するパスワード構成ポリシーをユーザーが手入力で入力したうえで，パスワードを生成しているという現状がある．この作業をパスワード構成ポリシー自動取得技術によ

1 三菱電機株式会社
Mitsubishi Electric Corporation
2 東邦大学
Toho University

Vol.2021-CSEC-94 No.19
Vol.2021-SPT-43 No.19
2021/7/19

って自動化することができれば，パスワードマネージャーの利便性を向上することが可能である．さらに本技術は，パスワード認証画面の利便性向上やパスワード構成ポリシー変換システムの実現へも応用することも可能である．

詳しくは 2 章で説明するが，本技術の実現のためには，①パスワード構成ポリシーの表示方法の調査，②パスワード構成ポリシー文字列取得技術の開発，という 2 つの検討が必要となる．本論文では，①を実施し，パスワード構成ポリシーが掲載されているサイトをクラウドソーシングによって収集し，パスワード構成ポリシーの表示方法について議論する．

1.2 本論文の構成

本論文の構成は次のとおりである．1 章では，本論文の背景を述べた．2 章では，パスワード構成ポリシー自動取得技術の必要性を述べたうえ，パスワード構成ポリシー自動取得技術に必要な 2 つの検討事項を示す．そのうえで，本論文ではその第一段階である「①Web 上の認証システムにおけるパスワード構成ポリシー表示方法の検討」を実施することを示す．その後，3 章で，クラウドソーシングを利用して Web 上のパスワード認証システムの URL を収集する手順を示すとともに，収集した結果を示す．4 章では 3 章で収集した結果を分析することで，パスワード構成ポリシーの表示方法を分類する．5 章で，考察によって，4 章の分類結果に関する考察，既存研究の調査結果の比較，パスワード構成ポリシー自動取得技術の応用先について議論する．6 章では，関連研究や取り組みを説明することで，本研究の位置づけをさらに明確にする．最後に，7 章で本論文の総括と今後の展望を述べる．

2. パスワード構成ポリシー自動取得技術

2.1 パスワード構成ポリシーの利用とパスワードマネージャーの活用

多くの Web サイトでは，パスワード構成ポリシーを導入し，ユーザーのパスワード強度を向上している．ただし，パスワード構成ポリシーはパスワード強度を高める効果を有している一方，ユーザーのパスワード生成・管理する負荷を高めている．複雑なパスワード構成ポリシーに従ったパスワード生成はユーザーにとって面倒な作業である[4]ためである．

この負荷を軽減する有力な手段が，パスワードマネージャーの利用である．パスワードマネージャーの例が，Lastpass[5]や Trendmicro のパスワードマネージャー[6]である．パスワードマネージャーでは，強力なマスターパスワード一つを登録しておくことで，認証システムのパスワードを生成・管理することが可能である．パスワードマネージャーの多くは，パスワードマネージャーへパスワード構成ポリシーを入力することで，その構成ポリシーに準拠したパスワードを自動的に生成する機能を有する場合が多い．したがって本機能は，パスワード構成ポリシーに従ったパスワード生成を容易にすることを支援しているといえる．

一方，現状のパスワードマネージャーには，パスワード構成ポリシーの観点から改善の余地が存在する．現状，パスワードマネージャーでパスワード構成ポリシーに従ってパスワード生成をする際には，ユーザーが登録ページに記載されているパスワード構成ポリシーを視認した後，パスワードマネージャーへそのポリシーを「手動」で入力することが一般的である[7][8]．本作業を「自動」化することができれば，パスワードマネージャーの利便性を向上することが可能であり，ひいては，パスワード認証の利便性を向上することにつながるであろう．そこで，本研究では Web 上の認証システム（以下，「認証サイト」）を対象とし，パスワード構成ポリシー自動取得技術について検討を行う[a]．

2.2 パスワード構成ポリシー自動取得技術の実現に必要な検討

前節に述べた技術を実現するにあたって，多くの認証サイトでは，登録ページ内にパスワード構成ポリシーを記載している．そこで，本研究では，Web 上のパスワード認証システムの登録ページからパスワード構成ポリシーを自動的に取得する技術を研究のゴールとする．

パスワード構成ポリシー取得技術の実現にあたっては，以下の①と②の検討が必要である．

① 認証サイトにおけるパスワード構成ポリシー表示方法の調査

Web 上の認証システムの登録ページにおいて，パスワード構成ポリシー文字列がどのように表示されるかを調査する必要がある．

② パスワード構成ポリシー文字列取得技術の構築

①の調査結果からわかったパスワード構成ポリシーの表示方法によって表示されるパスワード構成ポリシーの文字列を取得するアルゴリズムを構築する．

2.3 本論文の以降の章の位置づけ

以降，本論文は，前節で示した①②の検討のうち，①について検討を行う．パスワード構成ポリシーの表示方法については，文献[9]でも調査は行われているが，2012 年の調査であり，調査対象の範囲も比較的有名な認証サイトに限

a 本章ではパスワードマネージャーへの入力を例に研究のモチベーションを述べたが，本技術は，パスワードマネージャー以外へも応用可能な技術である．詳しくは，5 章の考察で論じる．

定されている．特に，2017 年に NIST Special Publication 800-63B[10]が発表されており，パスワード認証システムに変更が加えられている可能性もある．そこで， Web 上のパスワード認証システムを大規模に収集し，収集した認証システムの登録ページで，パスワード構成ポリシーがどのように表示されているかを調査する．

3. パスワード構成ポリシーの収集

3.1 収集目的と収集方法

認証サイトの登録ページで，パスワード構成ポリシーがどのように表示されているかを調査するために，認証サイトを収集する．認証サイトを収集する手段は種々の方法があるが，今回は，広範囲に多様な認証サイトを収集できる方法として，クラウドソーシングによって収集することとした．具体的には，ユーザーに対して，「知っている認証サイトの URL を回答してもらう」というタスクを依頼することによって収集した．

3.2 収集手順

クラウドソーシングで認証サイトの URL を収集する調査手順の詳細は以下のとおりである．

【募集件数】

延べ 500 件とする．回答 1 件には 1 つの認証サイト URL が含まれ，1 ユーザー5 回答まで許可する．

【手順】

ユーザーが依頼を受諾し，支払いを完了するまでの手順は以下のとおりである．

(1) ユーザーは，クラウドソーシングサイトで本調査の依頼を受諾する．今回は，日本のクラウドソーシングサイトである，ランサーズ[11]を使用した．
(2) クラウドソーシングサイトは，依頼を受諾したユーザーに，収集システムの URL を発行する．
(3) ユーザーは，収集システムの URL へアクセスする．
(4) ユーザーは，収集システムの初期画面で，認証サイトの定義と本調査の注意事項を読む（詳細は，【認証サイトの定義】と【倫理上の配慮】を参照のこと）．
(5) ユーザーは，注意事項に同意する場合，初期画面上で「同意」を押す．すると，アンケートシステムの認証サイト URL 入力画面へ遷移する．
(6) ユーザーは，自身が知っている認証サイトの URL を 1 件入力する．
(7) システムは，入力された認証サイト URL が以下の 2 つの基準を満たす場合のみ有効と判定する．
    (ア) 認証サイトの URL が URL として有効なフォーマットである．
    (イ) 認証サイトの URL がすでに回答された URL でない．今回は，すでに回答された URL であるか否かは，既回答の URL の FQDN と一致しているか否かで判定．
(8) 有効である場合，入力を受け付ける．無効である場合，(6)へ戻り，別の認証サイト URL の入力を求める．
(9) ユーザーは，収集システムでの回答を完了する．
(10) ユーザーは，クラウドソーシングサイトに，依頼の完了報告を行う．
(11) 依頼主（筆者）は，回答された URL へアクセスし，URL が確かに認証サイトの URL であることを確認する．認証サイトであれば，報酬を支払う．認証サイトでない場合，報酬を支払わない．

【報酬】

1 回答あたり 100 円とした．本金額は，【手順】(1)～(9)を筆者らが試行してかかった時間(5 分程度)と 2020 年 12 月時点の東京都の最低賃金(時間給 1,013 円)から算出した金額である．

【認証サイトの定義】

ユーザーに対しては，認証サイトの定義を以下のとおり表示した．

> 1. 認証サイトとは，あなた専用の Web ページにログインするための ID やメールアドレス，パスワードを入力するフォーム（欄）が含まれる Web ページをいいます．
> 2. たとえば，以下のような Web ページをいいます．
> （本論文では，以下省略）

【倫理上の配慮】

本収集において，収集システムに収集する情報は，認証サイトの URL だけであり個人を特定する情報は含まれない．また，回答を行う前に，回答が学術目的や製品開発目的で使用されること，回答完了報告（【手順】(10)）まで実施しなければ報酬を支払わない旨を注意事項としてユーザーへ表示した．この注意事項に同意したうえで，ユーザーは回答を行う必要がある．

【確認環境】

【手順】(10)の確認では，Windows 10 を OS とする PC 上で動作する Google Chrome Ver.86 を用いて確認を行った．

3.3 収集結果

2020 年 12 月 9 日 13:00 頃に収集を開始し，同日 16:30 頃にクラウドソーシングサイトに 500 件の完了報告が集まり，

収集が完了した．このうち，【手順】(11)の確認によって，有効として報酬を支払った依頼が 481 件，無効とした依頼が 19 件である．

ただし，ユーザーの中には，依頼を受諾して収集システムへ回答を入力したにも関わらず，クラウドソーシングサイトへ完了報告をしていないユーザーも存在した[b] ．今回は，収集システムの同意画面で，このような場合は報酬を支払えない旨を明示して，同意をとったうえで回答を収集したことから，このような回答も分析には利用することとした．このような回答は，19 件あり，このうち，認証サイトとして有効な URL は 15 件，無効な URL は 4 件であった．以上の結果，496 件の認証サイトの URL に収集に成功した．

3.4 収集結果のデータクレンジング

収集結果に対して，以下の 2 つのデータクレンジングを施した．

3.4.1 重複サイトの除外

今回の収集においては，【手順】(7)のとおり，収集時に FQDN によって認証サイトの重複を排除している．しかし，認証サイトの中には，http://www.example.com/auth と http://www.example.co.jp/auth のように，同じ企業やサービスの認証サイトでも，異なる FQDN であるため異なる認証サイトと判定されている場合もある．本重複は URL だけでは判定が困難であるため，著者らが目視で認証サイトの内容を確認することで除外した．本重複を排除した結果，認証サイト URL の総数は 448 件となった．

3.4.2 アダルトサイトの除外

収集した結果からは，著者らの組織のポリシーから，アダルトサイトを除外した．アダルトサイトか否かは，該当サイトがアダルトコンテンツを理由に未成年の閲覧を禁止しているかによって判定した．今回の収集結果には，5 件のアダルトが含まれており，この 5 件を除外した結果，認証サイト URL の総数は 443 件となった．

4. パスワード構成ポリシーの表示方法の分析

4.1 目的

収集結果を分析することで，認証サイトの登録ページでパスワード構成ポリシーがどのように表示されているかを明らかにする．なお，分析を行った環境は，3.2 に示した確認環境と同一であり，2021 年 1 月に実施した結果である．

4.2 登録方式分析結果

認証サイトにおいては，ユーザーアカウントの登録にあたって，登録方式が複数存在する．収集した 443 件の認証サイトを分析した結果，ユーザーアカウントの登録方式は以下の 3 つのパターンへ分類できることがわかった．

(1) 事前の手続きなしに登録ができるサイト(241 件)

特段の手続きなしに，ID，パスワード等のアカウント情報を入力し，ユーザーアカウントを登録できる認証サイトである．なお，登録情報入力後にメールで確認が行われる可能性はある．以下，このような形態なサイトを「直接登録方式」と呼ぶ．

(2) 登録の前に電子メールや SMS などで電子的に本人存在確認を行う必要があるサイト(127 件)

ID，パスワード等のアカウント情報を入力する前の作業として，メールアドレスや電話番号を入力する．その後，電子メールや SMS による確認を通じて，メールアドレスや電話番号の所有が確認できた場合にだけ，ID，パスワード等のアカウント情報を入力し，ユーザーアカウントを登録できる認証サイトである．以下，このような形態のサイトを「電子確認方式」と呼ぶ．

(3) 登録のために店舗での申請や郵送などで物理的な本人存在確認を行う必要があるサイト(75 件)

ユーザーアカウント登録前に，店舗での申請や郵送などによって物理的な本人確認が必要である．この本人確認を終えた場合のみ（たとえば，ユーザーアカウント発行に必要な専用番号が発行される），ユーザーアカウントが登録できる認証サイトである．もしくは，店舗での申請や郵送を行った時点で，その場でユーザーアカウントの ID やパスワードが発行される場合もある．以下，このような形態のサイトを「物理確認方式」と呼ぶ．

4.3 表示方法分析結果

調査の簡素化のため，収集した 443 件の認証サイトのうち，直接登録方式を採用する認証サイト 241 件の登録ページのパスワード構成ポリシー表示方法だけを分析することとした．この結果，登録ページのパスワード構成ポリシー表示方法は，図 1 に示すとおり，4 つのパスワード構成ポリシーの表示方法へ分類できることがわかった．以下に，それぞれの表示方法について詳しく説明する．

b ランサーズでは，ユーザーが依頼を受諾後，一定時間，依頼の完了を報告しなかった場合，その依頼受諾は無効化されほかのユーザーに追加依頼がなされる．

Vol.2021-CSEC-94 No.19
Vol.2021-SPT-43 No.19
2021/7/19

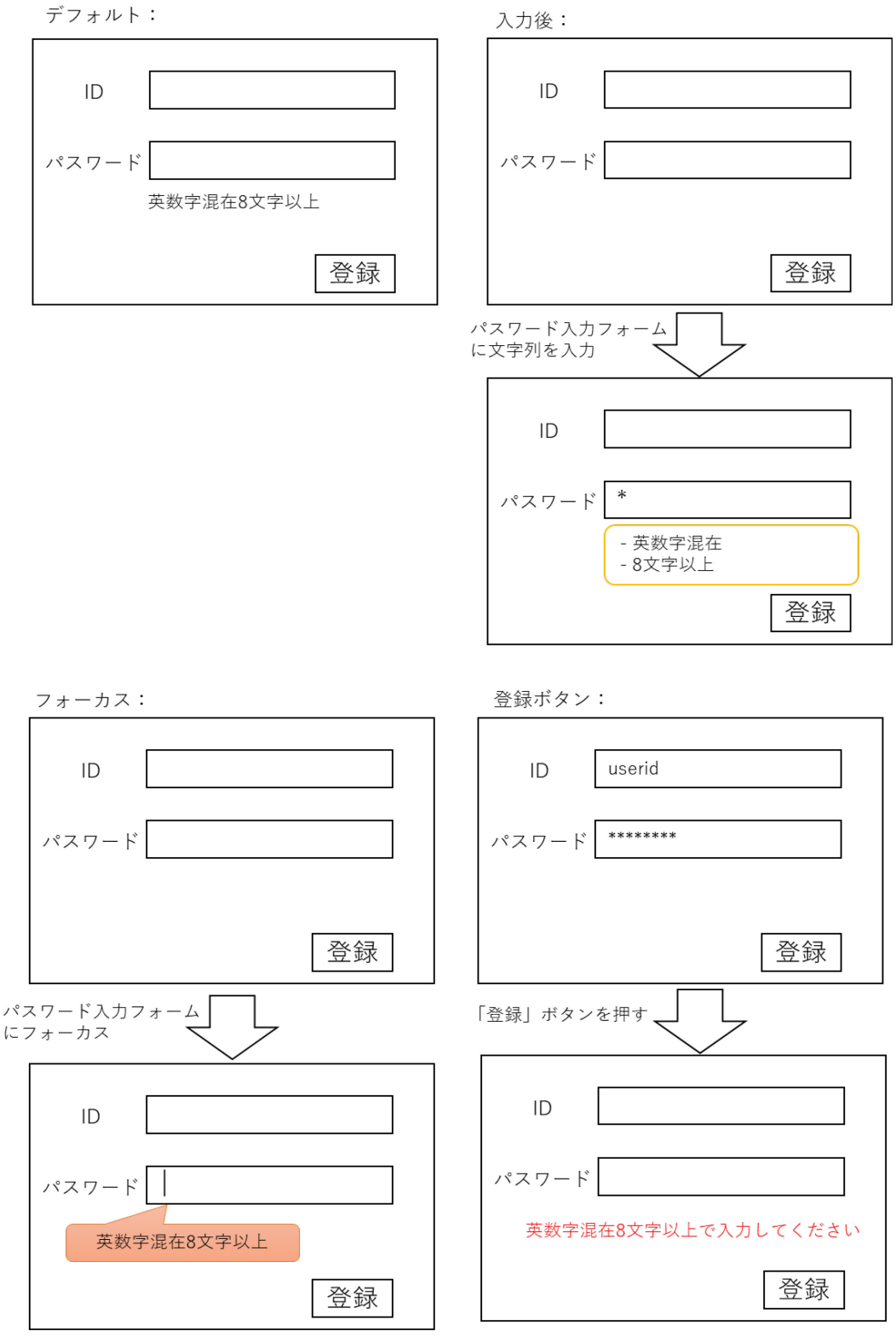

図 1　パスワード構成ポリシーの表示方法の分類

(1)　デフォルト（175 件，図 1 左上）

特にユーザーが登録ページに操作をしなくとも，入力フォーム付近にパスワード構成ポリシーが表示される登録ページである．

(2)　入力後（28 件，図 1 右上）

ユーザーがパスワード入力フォームに何らかの文字列を入力すると，入力フォーム近くにパスワード構成ポリシーが表示される登録ページである．

Vol.2021-CSEC-94 No.19
Vol.2021-SPT-43 No.19
2021/7/19

表 1. パスワード構成ポリシーUI の属性（文献[9]より引用）

Visibility	Language
Static	Tone
Mouse-Over	Clarity
Placement	Font type
Above box	Font size
Below box	Font color
Right next to box	Alignment
Inside box	Consistency
	Graphics

(3) フォーカス（16 件，図 1 左下）

ユーザーがパスワード入力フォームにフォーカスをあてたり，入力フォーム上にマウスポインタを置いたりした場合に，パスワード構成ポリシーがポップアップ等で表示される登録ページである．

(4) 登録ボタン（10 件，図 1 右下）

ユーザーが登録ボタンを押した後に，パスワード構成ポリシーに入力したパスワードがエラーメッセージとしてパスワード構成ルールが表示される登録ページである．

上記の合計は，229 件である．分析対象の総数(241 件)との差(12 件)は，パスワード構成ポリシーが実装されていない登録ページ, 確認環境で正常に動作しなった登録ページ, 収集時には存在したが分析時には削除されていた登録ページである．

5. 考察

5.1 調査結果に関する考察

5.1.1 パスワード構成ポリシー文字列取得技術の検討に向けて

調査の結果，パスワード構成ポリシー文字列を取得するためには，4.3 節で分類した 4 つのパターンで表示されるパスワード構成ポリシー文字列を取得するアルゴリズムを構築する必要があることがわかった． (1)デフォルトであれば，画面中の何処かに文字列が表示されている「静的」な表示形式である．すなわち，画面中を単純なパターンマッチングで探索するだけで発見できる可能性がある．一方，(2)入力後，(3)フォーカス，(4)登録ボタンについては，初期状態では画面中に表示されておらず，画面に対して何らかの操作をしなければ表示されない「動的」な表示方式である．すなわち，単純なパターンマッチングでは取得が困難である．「動的」な表示方式については，何らかの工夫をしてパスワード構成ポリシーを取得する必要があることがわかる．

たとえば，画面に対して何らかの操作を加えるという工夫をし，その後，パターンマッチング等で文字列を取得する工夫が必要である[c]．もしくは，動的な処理を実装している JavasScript のロジックを特定し，ロジックからプログラムの静的解析や動的解析の要領で取得するという工夫も考えられる[d]．これら具体的な検討は今後進めていきたい．

5.1.2 文献[9]との収集結果の比較

文献[9]では，パスワード構成ポリシーの UI について 90 件の Web 認証サイトに調査を行い，パスワード構成ポリシーの UI には，次々項に示す表 1 に記した属性があることが示されている．

本論文の調査結果と比較したとき,「パスワード構成ポリシーの表示方法」は表 1 の「Visibility」に相当する．この Visibility に示された属性と比較して，本論文では以下の知見が得られたことがわかる．

- 表 1 では，パスワード構成ポリシーの表示方法について「Static（本論文でいう，デフォルト）」と「Mouseover（本論文でいう，フォーカス）」が含まれるが，「入力後」と「登録ボタン」が含まれていない．

- 文献[7]では，表 1 のとおり，調査結果の属性分類は示されているが，その内訳件数は記載されていなかった．今回の調査によって，それぞれの内訳件数が明らかになった．

c 取得した文字列は自然言語であるため，単に取得するだけでなく，自然言語を計算機が理解できる形に変換する必要もある．たとえば，取得したパスワード構成ポリシー文字列は，「英数字を混ぜた 8 文字以上」のような自然言語である．パスワードマネージャーが理解するためには，この文字列を解析し，｛利用可の文字種：{英,数}，最低文字長:8，制約:{混在}｝のように，計算機が理解可能な形式に変換する必要がある．

d たとえば，if(password.length <8){ ポリシー表示; }のような実装がなされている場合，パスワード構成ポリシーで 8 文字以上の入力で求められているということがわかる．ただし，コーディングの方法は千差万別であるため，各種認証サイトから一様に取得できる静的解析や動的解析のアルゴリズムを構築することに大きな困難性がある．さらに，JavaScript ではなくサーバ側でロジックが実装されている場合，これら解析を用いることができない．

Vol.2021-CSEC-94 No.19
Vol.2021-SPT-43 No.19
2021/7/19

5.1.3 注意点

今回は，登録方式のうち，直接登録方式を採用する認証サイトのみを対象として調査・分析を行った．登録方式のうち，電子確認方式と物理確認方式を採用する認証サイトに関しても，同様の調査・分析を行う必要がある．ただし，登録方式は，「ユーザーが ID・パスワードを入力する画面にいつアクセスできるか」という点に影響するものであるため，パスワード構成ポリシーの表示方法には影響を与えない蓋然性が高い．241 件というデータの件数に鑑みれば，電子確認方式や物理確認方式をとるサイトでも同じ傾向がみられる可能性は十分にある．

また，今回は，日本のクラウドソーシングを利用してデータの収集を行ったため，ほとんどすべてのデータが日本語で作成されたサイトであった（日本語で作成されたサイトは収集した 443 件のうち，425 件であった）．海外の認証サイトを対象とした場合，今回の結果とは異なる傾向が出る可能性がある．

5.2 パスワード構成ポリシー自動取得技術の他の応用先

本論文では，2 章でパスワードマネージャーにパスワード構成ポリシーを入力することを研究のモチベーションであると述べた．ただし，パスワード構成ポリシー自動取得技術は，ほかにも複数の場面へ応用可能な技術である．

ユーザーの中には，登録時に自身が保有するパスワードを，パスワード構成ルールに合わせて変換する（たとえば，password というパスワードを考えたユーザーが，パスワード構成ポリシーにて数字の混在を求められていた場合，passw0rd と変換して登録する）ユーザーも一定の割合でいると考えられる．このようにパスワードを生成しているユーザーに対しては，認証ページにもパスワード構成ルールを表示することで，手がかり再生[12]によってパスワードの忘却リスクを軽減する効果が期待できる．しかし，多くの認証サイトでは，登録ページにパスワード構成ポリシーが記載されている一方，認証ページにはパスワード構成ポリシーが掲載されていない場合が多い．実際，今回収集した認証サイトでは，認証ページにもパスワード構成ルールを表示しているサイトは 443 件のうち 50 件しかなかった．パスワード構成ポリシー自動取得技術が実現できれば，認証ページにアクセスしたとき，登録ページからパスワード構成ポリシーを自動的に取得し，表示する仕組みも実現可能である．

また，筆者らは認証システムのパスワード構成ポリシーを利便性の高い別のパスワード構成ポリシー変換することで，パスワード認証の負荷を下げる技術（パスワード構成ポリシー変換システム）の検討も別途進めている[13]．当該技術においては，パスワード構成ポリシー自動取得技術が必要であり，本研究成果を応用可能である．

6. 関連研究・取り組み

パスワード構成ポリシーの利便性に関する関連研究・取り組みは多くなされているが，主に二種類へ分類できる．

一つ目の分類は，パスワードの構成ポリシーごとにユーザーの作成するパスワードの強度がどのように変化するかを調査することで，適切なパスワード構成ポリシーを探求する研究である．文献[14],[15]では，各種構成ポリシーを用意し，生成されるパスワードの強度や忘却率に，パスワード構成ポリシが与える影響を調査・検討している．文献[16]では，ユーザーがパスワード構成ポリシーに従ってパスワード生成する時の戦略を調査している．文献[17]のように，PIN に限定してユーザーの PIN 生成における戦略を調査した既存研究も存在する．また文献[18]では，パスワード構成ポリシーの準拠結果を，パスワード入力後，即時に画面表示することによる効果をユーザー実験によって調査している．

二つ目の分類は，パスワード構成ポリシーの実態について調査した研究や取り組みである．文献[19]では，75 のウェブサイトにおけるパスワード構成ポリシーを調査し，サイトのカテゴリごとにどの程度の強度のパスワード構成ポリシーが使用されているかを調査している．文献[20]では，平成 27 年の情報であるが，総務省が日本におけるウェブサービスに関する ID・パスワードの管理・運用実態調査結果を公表しており，その中で事業者が利用しているパスワード構成ポリシーに関するアンケート結果を公開している．文献[21]では，流出したパスワードから，流出したシステムで使われていたパスワード構成ポリシーを推測しようとしている．

著者らが確認した限り，どの研究や取り組みにおいても，本研究がゴールとするパスワード構成ポリシー自動取得技術について言及しているものはなかった．ただし，二つ目の分類であるパスワード構成ポリシーの実態調査の過程では，本研究同様，認証サイトのパスワード構成ポリシーの収集を行っている．しかし，Web ページに表示されているパスワード構成ポリシーを自動で収集した旨は示唆されていなかった（手動で収集したと考えられる）．

7. おわりに

本研究では，Web 上のパスワード認証システムのユーザーアカウント登録ページからパスワード構成ポリシーを自動的に取得する技術（パスワード構成ポリシー自動取得技術）を研究のゴールとした．本技術の実現のためには，①パスワード構成ポリシーの表示方法の調査，②パスワード構成ポリシー文字列の取得技術の開発が必要となることを示した．本論文では，このうち①を扱い，パスワード構成

ポリシーが掲載されている認証サイトをクラウドソーシングによって収集した．この結果，クラウドソーシングを通じて計 443 件の認証サイトの収集に成功した．収集した認証サイトの登録ページを分析した結果，パスワード構成ポリシーの表示方法は 4 パターンに分類できることを明らかにした．さらに，考察によって，既存研究の調査結果の比較やパスワード構成ポリシー自動取得技術の他の応用先について議論することで，本技術の有用性や発展可能性をさらに明確にした．今後は，今回の成果を用いて，②の検討を進めていきたい．

参考文献

[1] THALES: “2019 Thales Access Management Index”, 入手先〈https://cpl.thalesgroup.com/access-management-index〉 (参照 2021-3-1).

[2] P. Arias-cabrios, C. Krupitzer, and C. Becker: A Survey on Adaptive Authentication, ACM Comput. Surv., no. 80 (2019).

[3] Micorosoft: “ゼロトラストセキュリティ”, 入手先〈https://www.microsoft.com/ja-jp/security/business/zero-trust〉 (参照 2021-3-1).

[4] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman: “Of passwords and people: measuring the effect of password-composition policies”, Proc of CHI 2011, pp. 2595-2604, 2011.

[5] LastPass: “Lastpass”, 入手先〈https://www.lastpass.com/〉(参照 2021-2-1).

[6] TrendMicro: “パスワードマネージャー”, 入手先〈https://www.trendmicro.com/ja_jp/forHome/products/pwmgr.html〉(参照 2021-2-1).

[7] TrendMicro, “パスワードマネージャーの各機能の詳細”, 入手先〈https://helpcenter.trendmicro.com/ja-jp/article/tmka-19178〉(参照 2021-2-1).

[8] Lastpass: “Password Generator”, 入手先〈https://www.lastpass.com/password-generator〉(参照 2021-2-1).

[9] S. Moshfeghian, Y. S. Ryu: “A passport to password best practices”, Ergonomics in Design: The Quarterly of Human Factors Applications vol. 20, no. 2, pp. 23-29, 2012.

[10] G. Paul, N. Elaine, F. James, P. Ray, R. Andrew, B. William, R. Richer, L. Naomi, D. Jamie, C. Yee-Yin, G. Kristen, and T. Mary: “NIST 800 63B: Digital Identity Guidelines: Authentication and Lifecycle Management”, 入手元〈https://csrc.nist.gov/publications/detail/sp/800-63b/final〉 (参照 2021-3-1).

[11] Lancers: “Lancers”, 入手先〈http://lancers.jp/〉(参照 2021-2-1).

[12] 中島義明, 安藤清志, 子安増生, 坂野雄二, 繁桝算男, 立花政夫, 箱田裕司 : “心理学辞典”, p.607, 有斐閣（1999）.

[13] 藤田真浩, 山中忠和, 松田規: “パスワード認証システムとユーザー間におけるパスワード構成ポリシーのギャップを緩和するパスワード構成ポリシー変換システムの提案”, SCIS2021 論文集, 2B4-1, 2021.

[14] P. G. Kelley, S. Komanduri, M. L. Mazure, .R. Shay, T. Vidas, L. Bauer, and J. Lopez: “Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms”, Proc. 2012 IEEE symposium on security and privacy, pp. 523-537 (2012).

[15] R. Shay, S. Komanduri, A. L. Durity, P. Huh, M. L. Mazurek, S. M. Segreti, B. Ur, and L. Bauer: “Designing Password Policies for Strength and Usability”, ACM Transaction on Information and System Security, No. 13, 2016.

[16] B. Ur, F. Noma, J. Bees, S. M. Segrei, R. Shay, L. Bauer, N. Christin, and L. F. Cranor, “"I Added '!' at the End to Make It Secure": Observing Password Creation in the Lab”, Proc. of SOUPS2015, pp.123-140, 2015.

[17] J. Bonneau, S. Preibusch, and R. Anderson, “A Birthday Present Every Eleven Wallets? The Security of Customer-Chosen Banking PINs”, Proc. of FC.12, LNCS, vol. 7397, pp. 25-40, 2012.

[18] R. Shay, L. Bauer, N. Christian, L. F. Cranor, A. Forget, S. Komanduri, M. L. Mazurek, W. Melicher, S. M. Segreti, and B. Ur: “A Spoonful of Sugar?: The Impact of Guidance and Feedback on Password-Creation Behavior”, Proc. of CHI 2015, pp. 2903-2912, 2015.

[19] D. Florêncio, C. Herley: “Where do security policies come from?”, Proc. of SOUPS 2010, pp. 1-14, 2010.

[20] 総務省情報セキュリティ対策室: “ウェブサービスに関する ID・パスワードの管理運用実態調査結果(平成 27 年 7 月 30 日)”, 入手先〈https://www.soumu.go.jp/main_content/000370853.pdf〉(参照 2021-2-1)

[21] S.Johnson, J. Ferreira, A. Mendes, and J. Cordry: “Lost in Disclosure: On the Inference of Password Composition Policies”, Proc. of ISSREW 2019, pp. 264-269, 2019.