Computer Security Symposium 2021
26 - 29 October 2021

日本における認証サイトパスワード構成ポリシーの大規模実態調査

藤田 真浩[1]　山中 忠和[1]　松田 規[1]　金岡 晃[2]

概要：本論文では，日本における認証サイトで使用されているパスワード構成ポリシーの大規模な実態調査を行う．具体的には，各認証サイトで利用されているポリシーの最小文字数，最大文字数，使用できる文字種，文字種の構成要件について傾向の分析を行う．その後，分析した傾向と既存研究で得られた傾向とを比較し，本調査で新たに得られた知見を明確にする．さらに，各種規格やガイドラインで求められているパスワード要件も踏まえながら，どうして各認証サイトがその構成ポリシーを使用しているかの考察も行う．

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

Comprehensive Survey of Password Composition Policy on Japanese Authentication Websites

Masahiro Fujita[1]　Tadakazu Yamanaka[1]　Nori Matsuda[1]　Akira Kanaoka[2]

Abstract: In this paper, a comprehensive survey of password composition policy on Japanese authentication websites was conducted. Specifically, the following four factors of the policy was analyzed: (i) minimum password length, (ii) maximum password length, (iii) character types that users can use for a password, (iv) character-type composition requirements. Compared the result with that obtained by previous works, some new findings were shown. In addition, based on the result and some references (i.e. password standards and guidelines), the following research question was discussed: “why developers of the websites selected the password composition policy?”.

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．

本論文では，日本における認証サイトで使用されているパスワード構成ポリシーの実態（パスワード構成ポリシーとして，どのような要件のポリシーが採用されているか）の大規模実態調査を行う．具体的には，213 件の Web 上認証サイトで利用されているパスワード構成ポリシーについて，最小文字数，最大文字数，利用できる文字種，文字種の構成要件の観点で実態調査を行う．その後，調査結果から各認証サイトで用いられているパスワード構成ポリシーの傾向をまとめ，関連研究との差分を議論する．さらに，まとめた傾向と各種規格・ガイドラインで求められている要件との比較を行い，得られた傾向が産出された理由についての考察を行う．

1.2 本論文の構成

本論文の構成は以下のとおりである．1 章ではパスワード認証やパスワード構成ポリシーの背景を述べたうえで，本論文で取り扱う実態調査の内容を概説した．2 章では，関連研究・調査を紹介したのち，関連研究・調査と本論文

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

の関係性を議論することで，本論文の位置づけを明確にする．3 章では， 日本における認証サイトのパスワード構成ポリシーの大規模実態調査を行う．4 章は，調査結果から傾向をまとめたうえで，考察を行う．5 章ではまとめと今後の研究課題を述べる．

2. 本論文の位置づけ

2.1 関連研究・調査

パスワード構成ポリシーの利便性に関する関連研究・調査については，①パスワード構成ポリシーの実態について調査した研究・調査[4][5] [6] [7][8]，②パスワード構成ポリシーに応じて利用者のパスワード強度がどのように変化するかを調査した研究・調査[9][10][11][12][13]の二種類の研究に大別される[14]．本論文はこのうち①について取り扱うものであるため，以下では，①に関する関連研究・調査について詳述する．

文献[4]は，著者が知る限り，①に関するもっとも初期(2007 年)の研究論文であり，10 の著名な Web サイトに関してパスワード構成ポリシーを調査した論文である．文献[5]は，2010 年に実施された調査であり，75 の Web サイトに対して，それぞれのサイトで用いられているパスワード構成ポリシーを調査した論文である．その結果，パスワード構成ポリシーの要件は，サイトで取り扱う情報の重要度に依存しているではなく，サイトの利便性に依存しているという傾向を明らかにしている．これら論文と主旨は少し異なるが，文献[6]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．

これらは海外における調査研究であるが，日本でも同様の調査が報告書レベルで行われている．文献[7]では，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（28 社）を公表している．その中では，約 9 割のサービスで 3 種類以上の文字種をパスワードとして利用できる，パスワードの最大桁数が 12 桁未満のサービスが約 4 分の 1 存在する，などの傾向を得ている．文献[8]は，2020 年の記事であり， 31 の Web サイトに関してパスワード構成ポリシーを調査している．調査の結果，最小文字数は 6,8 文字に集中している一方，ほかの観点については一定の傾向が見られなかったことを説明している．

2.2 本論文が取り扱う課題

本論文は日本におけるパスワード構成ポリシーの実態を調査し傾向をまとめ，考察するものである．前節に示したとおり，日本においてもパスワード構成ポリシーの実態調査すでには行われているが，サンプル数が少ない（文献[7]では 28 件，文献[8]では 31 件）という課題がある．そこで本論文では，大規模に収集した認証サイトに対して，パスワード構成ポリシーで求められている要件の実態調査を行い，その傾向を把握する．さらに，得られた傾向について，以下の二つの観点で考察する．

1. 文献[8]で得られた傾向と比較して，新たに得られた傾向は何か[a]
2. 得られた傾向となっている理由は何か（各種規格・ガイドラインで求められている要件を踏まえて考察する）

3. 調査

3.1 調査目的

大規模に収集した日本語で実装された認証サイトに対して，各認証サイトに実装されたパスワード構成ポリシーで求められている要件を実態調査する．

3.2 調査観点

パスワード構成ポリシーの要件としては多くの観点が考えられるが，今回は調査の第一報であり，紙面のスペースも限られていることから，以下の 4 つの観点に絞って調査を行い，傾向を把握することとする．各観点については，パスワード構成ポリシーの文章から読み取ることとする（システムに対して，各種パスワードを実際に入力して取得したものではない）．

1. 最小文字数
2. 最大文字数
3. 使用できる文字種（例：英数字だけ，英数字記号だけ，任意の文字）
4. 文字種の構成要件（例：英数字混在，英数記号混在）

たとえば，

> 半角英字・半角数字混在の 8～64 文字
> ※パスワードには，半角英字・半角数字・半角記号が利用できます

というパスワード構成ポリシーがあった場合，

1. 最小文字数：8 文字
2. 最大文字数：64 文字
3. 使用できる文字種：半角英字・半角数字・半角記号
4. 文字種の構成要件：半角英字・半角数字（の混在）

である．

a 文献[7]は，事業者に対するアンケートによって調査を行っており，本論文のアプローチ（実際に認証サイトのパスワード構成ポリシーを確認する）と異なるため比較対象としないこととした．

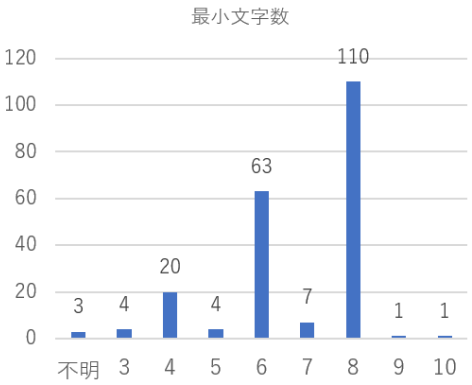

図 1　最小文字数分析結果

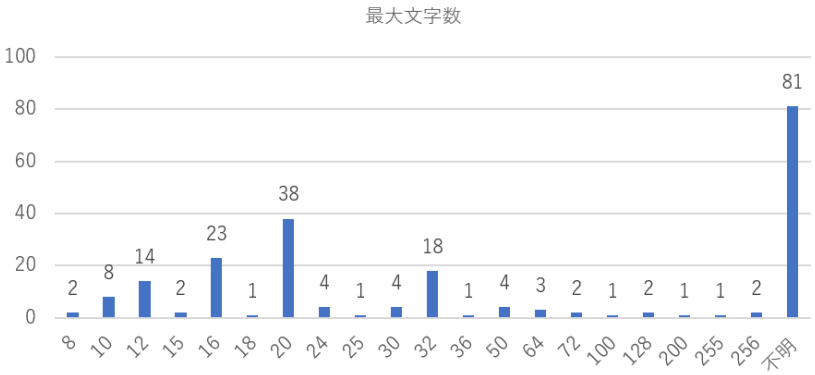

図 2　最大文字数分析結果

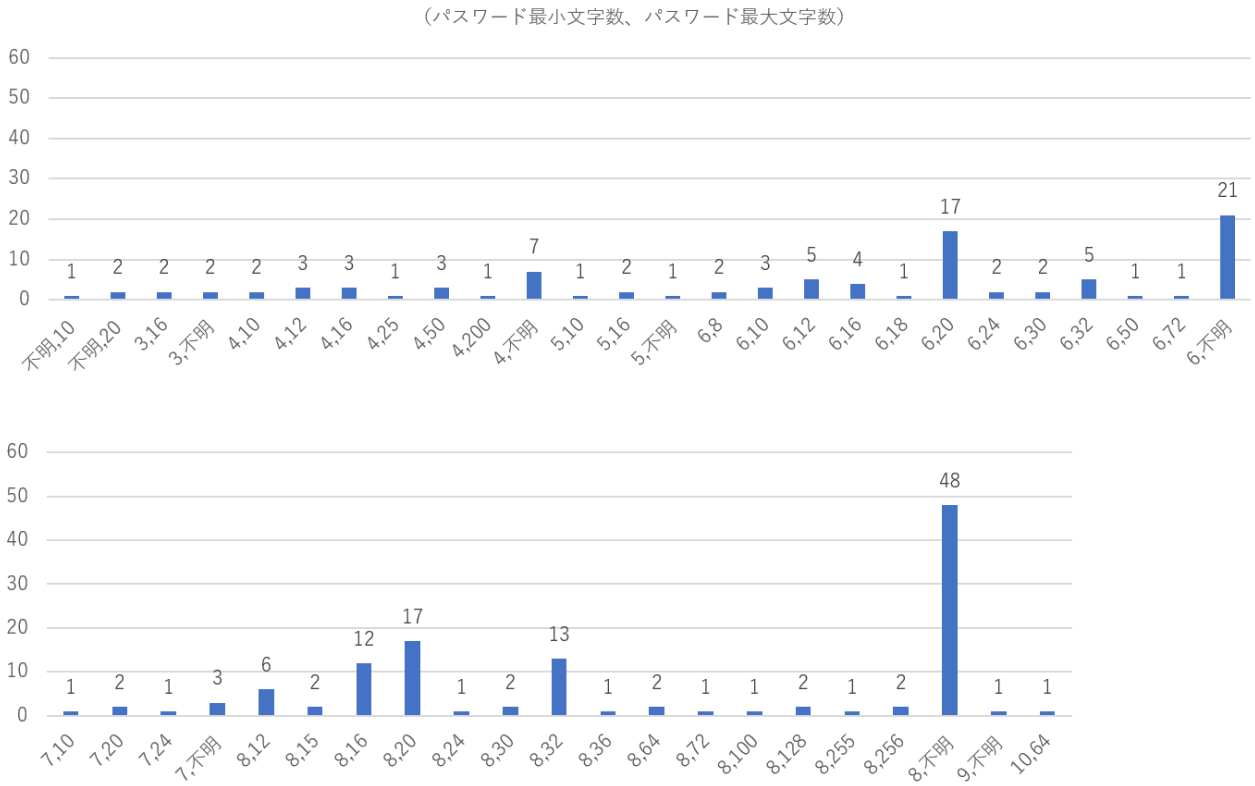

図 3　最小文字数,最大文字数の組み合わせ分析結果

3.3　調査対象データ

分析の対象とする認証サイトのソースは，文献[14]で収集した認証サイト 229 件である．以下，文献[14]における収集方法の要点をまとめる．詳細は，文献[14]の 3 章及び 4.2 節を参照されたい．

- クラウドソーシングサービス「ランサーズ」[15]を使用して，2020 年 12 月 9 日に収集
- ランサーズにおいて，回答者（ランサー）に「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して収集

ただし，文献[14]で収集した認証サイトには，以下の二つの理由から，今回の調査において適切でない認証サイトが含まれていた．

- 実態調査実施時点（2021 年 4 月）において，削除されている認証サイト
- 英語で実装された認証サイト

これら認証サイトを除外した結果である 213 件の認証サイトに対して，3.2 節の観点で実態調査を行った．

3.4　調査結果

調査を行った結果を図 1～図 5 に示す．これら図の中で用いているいくつかの表記について，以下で説明する．

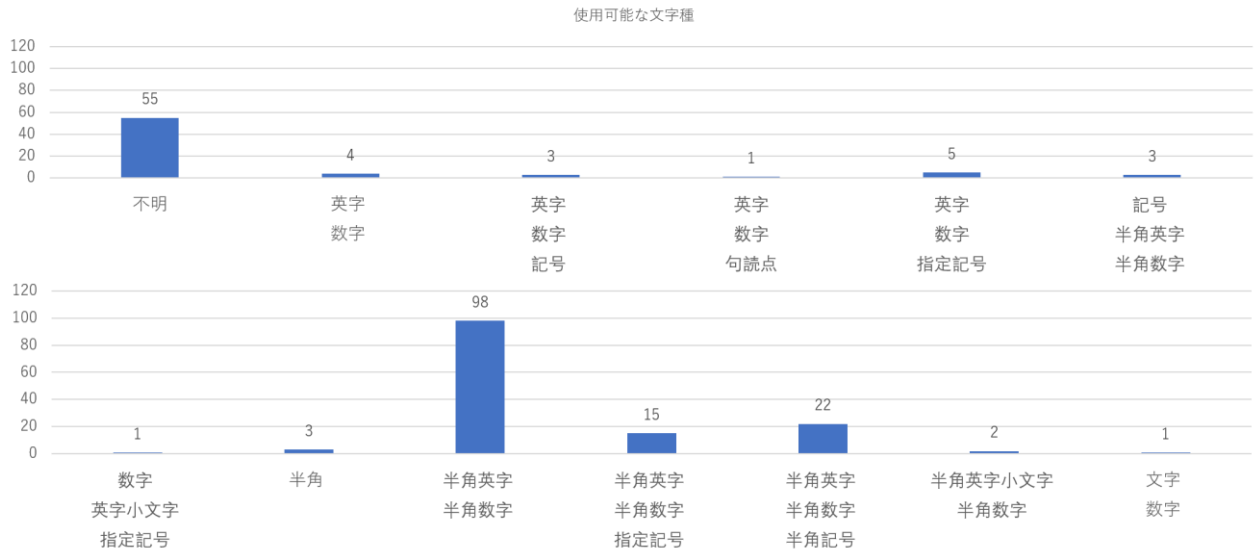

図 4 使用可能な文字種

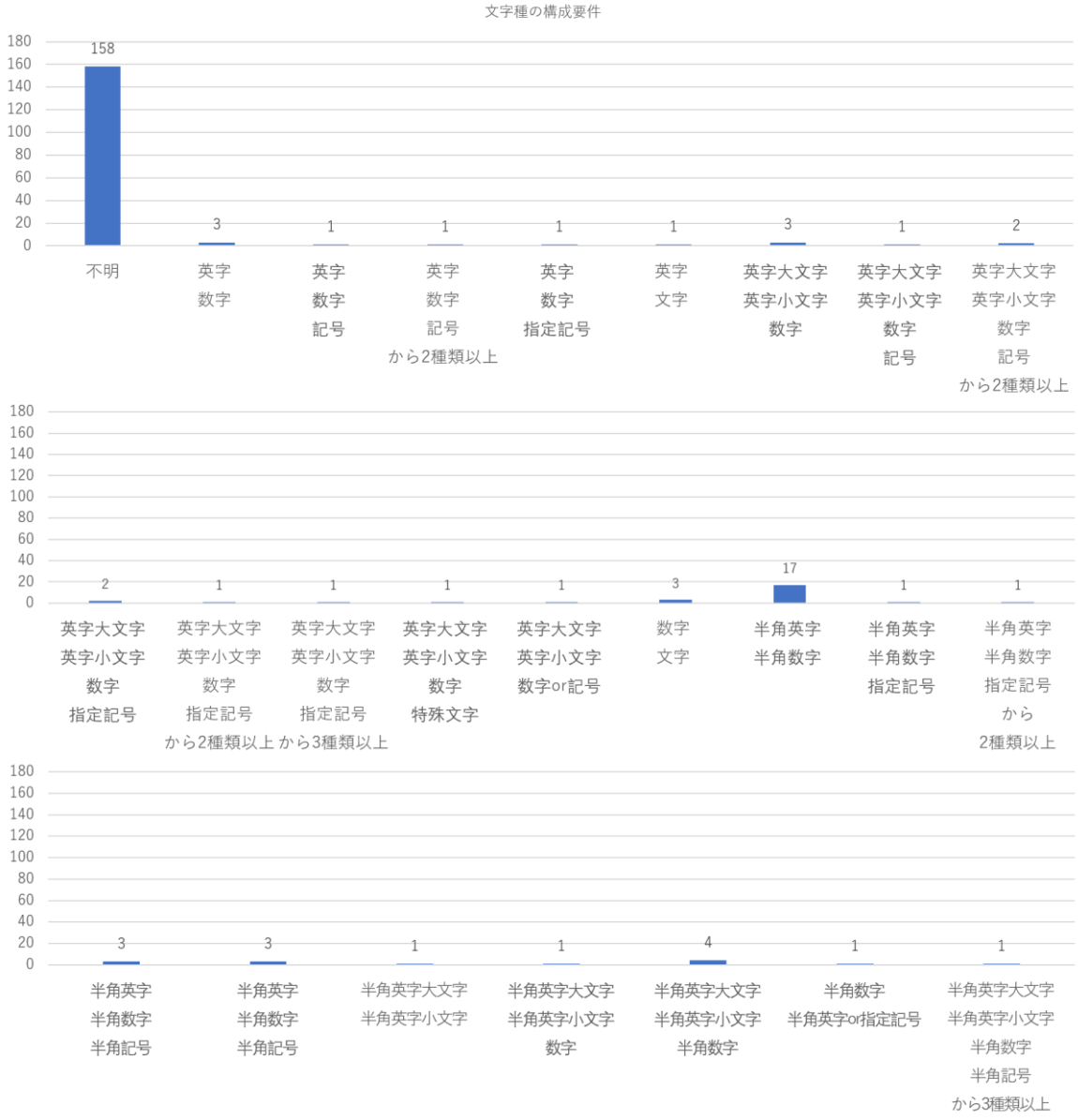

図 5　文字種の構成要件

表 1　関連研究・調査との傾向と比較結果

項目	傾向		傾向を比較した考察
	本論文	文献[8]	
最小文字数	・8 文字（110 件 [51.6%]） ・6 文字（ 63 件 [29.6%]） ・4 文字（ 20 件 [9.4%]）	・6 文字（12 件 [38.7%]） ・8 文字（12 件 [38.7%]） ※「6・8 文字に集中していてばらつきはあまりない」と結論	・8 文字や 6 文字が多い傾向にあるのは同じであるが，8 文字（110 件）は 6 文字（12 件）の 2 倍程度の総数がある． ・4 文字を利用しているサイトも 20 件（1 割程度）いる．
最大文字数	・不明　（81 件 [38.0%]） ・20 文字（38 件 [17.8%]） ・32 文字（18 件 [15.0%]） ・16 文字（23 件 [7.5%]） ・12 文字（14 券 [6.6%]）	・不明　（13 件 [41.9%]） ・20 文字（4 件 [12.9%]） ・16 文字（4 件 [12.9%]） ※「かなりばらつきがある」と結論	・総数を増やしてもおおよそ傾向は同じであるが，32 文字を利用しているサイトも 18 件（2 割弱）いる．
文字数組み合わせ	・8,不明（48 件 [22.5%]） ・6,不明（21 件 [9.9%]） ・6,20　（17 件 [8.0%]） ・8,20　（17 件 [8.0%]） ・8,13　（13 件 [6.1%]） ・8,16　（12 件 [5.6%]）	記載なし	・不明を取り除いた部分（144 件）で評価すると，最小文字数を 6 または 8，最大文字数を 16～20 と設定している認証サイト 59 件（4 割程度）を占める． ・加えて，不明を「十分な上限値であるために取り立てた記載はしていない」と好意的に解釈した場合，最小文字数が 6 または 8 に設定され，最大文字数を十分な上限値で設定しているサイトは 69 件（全体の 3 割程度）いることとなる．
使用可能な文字種	・半角英字・半角数字（98 件 [46.0%]） ・不明　（55 件 [25.8%]） ・半角英字・半角数字・半角記号（22 件 [10.3%]） ・半角英字・半角数字・指定記号（22 件 [10.3%]）	・英字・数字　（7 件 [22.6%]） ・不明　（6 件 [19.4%]） ・英字大文字・英字小文字・記号　（5 件 [19.4%]） ・英字・数字・記号　（5 件 [16.1%]） ・その他　（4 件 [12.9%]） ・英字大文字・英字小文字・数字　（4 件 [12.9%]） ※「あまりばらつきはない」と結論	・不明を取り除いた部分（158 件）で評価すると，「半角英数字」「半角英数字に記号を加えたもの」で 142 件（9 割）を占める． ・加えて，不明を「すべての文字種が利用できるために取り立てた記載はしていない」と好意的に解釈した場合，すべての文字列を受け付けているサイトも全体の 55 件（2 割 5 分程度）いる．
文字種の構成要件	・不明　（158 件 [74.2%]） ・半角英字・半角数字（17 件　[8.0%]）		・158 件（7 割 5 分）のサイトが不明である．不明を「複雑さの要件を求めていない」と好意的に解釈した場合，これら 7 割 5 分のサイトで複雑さの要件を求めていないこととなる．

・　「不明」は，パスワード構成ポリシーの文章表記にその要件が書かれていないことを表す．パスワード構成ポリシーの表記だけは，設定されていないのか，設定されているのに記載されていないのかの判断がつかないため，「不明」としたことに注意されたい．

・　文字種「指定記号」は，任意の記号が用いることができず，一部の記号だけ使用できる場合をいう（たとえば，「半角英数字（$#_も利用可能）」というパスワード構成ポリシーの場合，「$,#,_」が指定記号を意味する）

・　「英字」「半角英字」などの表記は，パスワード構成ポリシー原文に書かれた表記をそのまま採用している．（たとえば，「英字」という表示が「半角英字」を意味している可能性がある）

4. 考察

4.1 調査結果から得られる傾向

3 章に示した各図の各要件の傾向（多くの認証サイトで利用されている要件）について，表 1「傾向」「本論文」列へまとめる．ここで，「多くのサイトで利用されている」というのは，

・ 総数が最大値の 10%以上を有する
（図 1 であれば，8 の 110 件が最大値であるため，その 10%以上である 11 件以上）
・ 総数が 10 件を超える

という二つの条件を満たす要件とした[b]．列中[ ]で示した数値は，データの総数 213 件を母数としたときの割合である．

4.2 傾向に関する考察

4.2.1 前提

前節で得られた傾向について，2.2 節で述べた，以下の二つの観点から議論を行う．

1. 文献[8]で得られた傾向と比較して，新たに得られた傾向は何か
2. 得られた傾向となっている理由は何か（各種規格・ガイドラインで求められている要件を踏まえて考察する）

なお，本章で述べる議論は，あくまでパスワード構成ポリシーの実態がどのような傾向を有しており，その傾向はどうして産出されているかを議論するものである．**各認証サイトに実装されたパスワード構成ポリシーの要件の適切さや良し悪しを議論する主旨ではないことに注意されたい**．

4.2.2 文献[8]で得られた傾向と比較して，新たに得られた傾向は何か

文献[8]で得られた傾向を，表 1「傾向」「文献[8]」列にまとめる．なお，文献[8]はサンプル数が少ない（31 件）ため，「最大値の 10%以上を有すること，かつ，4 件を超える[c]こと」を目安に記載することとした．また，筆者らで確認したところ，文献[8]においては「使用可能な文字種」と「文字種の構成要件」を明確に分けていない（混在して記載している）よう見受けられた．そこで，これらの行については結合して一つの結果として示している．

本論文によって，大規模に調査した結果と文献[8]の結果を比較した際の違いを考察した．可読性を重視し，考察した結果は，表 1「傾向比較結果」列に記すため参照されたい．

4.2.3 得られた傾向となっている理由は何か

本項では，前述のような傾向となっている理由（システム設計者・開発者が，調査結果のようなパスワード構成ポリシーを採用している理由）を考察する．理想的な方法は，各認証サイトの設計者・管理者にその理由を問うことである．しかし，この方法は大きなコストがかかるため容易でない．そこで，本論文では各種規格やガイドラインを参考に，その理由を考察することとする．

本考察を実施するために，パスワード構成ポリシーの設計について言及されている規格やガイドライン[d]を収集した．具体的には，2021 年 7 月 22 日に，Google 検索によって「password requirements guidelines」「パスワード 要件 ガイドライン」と検索し，それぞれ上位 50 件，計 100 件の検索結果を取得した．この検索結果に含まれている，上記規格やガイドラインをリスト化した．ここで，「含まれている」というのは，その検索結果が目的とする規格やガイドラインそのものであるほか，検索結果の Web ページ内で言及されている規格やガイドラインも含んでいる．リスト化した結果を表 2 に示す[e]．

以下，最小文字数，最大文字数，使用可能な文字種，文字種の構成要件（最小文字数，最大文字数の組み合わせについては，これらの組み合わせであることから省略する）の四つの観点で，本論文にて得られた傾向と表 2 を比較する．

最小文字数

多くの規格やガイドラインで最小文字数「8」が推奨されている．8 文字が多い傾向は，これら規格やガイドラインに影響を受けている可能性がある．一方，4 文字や 6 文字について言及している規格・ガイドラインはなく，4 文字や 6 文字に設定している理由は，規格・ガイドラインからは不明である．ただし，4 文字については，キャッシュカードやクレジットカードの PIN として利用されている文字長として一般的であるため，この PIN 長に影響を受けている可能性はある．

最大文字数

最大文字数について，各種規格・ガイドラインでは特定の値が言及されていない．4 割（81 件）の認証サイトが「不明」としているのは，これら規格やガイドラインに影響を

b 「多くのサイトで利用されている」という明確な評価指標は存在しない．本論文では，相対的な評価指標として，「最大値を基準として 10%以上」，および，絶対的な評価指標として，「データ数 213 を基準として 5%(10.65)以上」＝「10 件を超える」という指標を置くこととした．
c データ数 31 を基準としてこの 10%以上とした．
d ここで収集した規格・ガイドラインは「システム視点」であるもののみ抽出した．すなわち，ユーザーに強固なパスワードを作るための示唆（例：○文字以上のパスワードを作りましょう）を行うガイドラインや教育資料といった，「ユーザー視点」の文献は除外した．
e 著者が，各種規格やガイドラインに書かれた内容を要約や解釈したうえでまとめた結果である．すなわち，本結果は著者の理解や解釈が含まれたものである．さらに，これら規格・ガイドラインには Web 上の認証システムへ要求する要件として書かれたものでないものも含まれる．これらの理由から，**本情報を利用するときは，原本の規格やガイドラインも必ず参照されたい．**

表 2　各種規格・ガイドラインで求められるパスワード構成ポリシーの要件

規格・ガイドライン名	出版年月日	補足	最小文字長	最大文字長	使用可能な文字種	文字種の構成要件
NIST 800-63B	2017/6	ユーザが作成	8	少なくとも64	すべて	課すべきでない
Microsoft Password Guidance	2021/7	管理者	8	記載なし	すべて	求めない
		ユーザ	記載なし	記載なし	記載なし	記載なし
NCSC	2018/11		設定すべき（具体値なし）	設定すべきでない	記載なし	課すべきでない
PCI DSS v3.2.1	2018/5		7	記載なし	記載なし	数字と英文字の両方
ISO27002	2013/10		十分な最短文字数（具体値なし）	記載なし	記載なし	同一文字を連ねただけ、数字だけ、英字だけはNG
CIS Password Guidelines	2020/7	単要素	14	設定すべきでない	すべての文字種	少なくとも1文字は英文字以外を含める
		多要素	8	設定すべきでない	すべての文字種	記載なし
NERC CIP 007-6	2014/1		8(条件あり)	記載なし	記載なし	3種類以上の文字
HITRUST共通セキュリティフレームワーク v9.4	2020/11	通常アカウント	8	記載なし	記載なし	記載なし
		特権アカウント	15	記載なし	記載なし	1文字以上の数字または特殊文字、1文字以上の英文字大文字、小文字
CNIL パスワードに関する勧告	2017/1	単要素	12	記載なし	記載なし	大文字、小文字、数字、特殊文字を含む
		パスワード＋試行制限	8	記載なし	記載なし	大文字、小文字、数字、特殊文字から3種類以上
		多要素認証	5	記載なし	記載なし	記載なし
CMMC v1.02	2020/3	Level2	最低限のパスワードの複雑性を担保すべきと書かれているが具体的な記載なし			
政府機関等の対策基準策定のためのガイドライン	2021/*		強固なパスワードに必要な桁数や複雑さが必要だが、一律に定めることは困難と記載			
医療情報システムの安全管理に関するガイドライン	2021/1	最低限ガイドライン：（条件なし）	13	記載なし	記載なし	英数字、記号を混在
		最低限のガイドライン：（定期変更）	8	記載なし	記載なし	記載なし
		最低限のガイドライン：（2要素認証）	8	記載なし	記載なし	記載なし
国民のための情報セキュリティサイト	2013/*		適切な長さの文字列であると書かれているが具体的な記載はなし			
Google cloud	不明(2019年以降)		8文字以上	非常に長い文字列	UTF-8のような可能な限り大きな文字集合	記載なし

受けている可能性がある．一方，残りの 6 割（132 件）が値を設定している理由は，規格・ガイドラインからは不明である．一つの可能性として，実装上の制約である可能性はある．

使用可能な文字種

使用可能な文字種について，各種規格・ガイドラインで言及されている場合，すべての文字種を受け付けるべきと記載しているものが多い．一方，今回の結果では，「半角英数字」「半角英数字に記号を加えたもの」で 142 件（7 割弱）を占めていた．したがって，使用可能な文字種の理由については，規格・ガイドラインからは不明である．一つの可能性として，実装上の制約である可能性はある．

文字種の構成要件

文字種の構成要件については，規格・ガイドラインごとに大きく異なっている．ただし，リスト化にあたって参照した Google 検索結果に表れた 100 件の Web ページ中で何らかの規格・ガイドラインに言及していた Web ページの総数は，63 件であった．このうち，NIST SP 800-63B に言及していた Web ページの総数は，46 件（約 7 割）であった．すなわち，パスワード要件の規格・ガイドラインとしては，NIST SP 800-63B が参照されやすいと規格・ガイドラインであるといえるであろう．この点，158 件（7 割 5 分）の認証サイトが「不明」となっているのは，NIST SP 800-63B の使用可能な文字種「すべて」に影響を受けている可能性はある．

5. おわりに

5.1 総括

本論文では，日本における認証サイトで使用されているパスワード構成ポリシーの実態の大規模調査を行った. 213 の認証サイトに対して，各認証サイトで利用されているポリシーの最小文字数，最大文字数，利用できる文字種，文字種の構成要件の観点で実態調査を行った．本結果の傾向をまとめることで，既存の調査結果では知られていなかった，これら要件に関する新たな知見を多く得た（表 1）．さらに, このような傾向となっている理由を考察するために，14 件の規格・ガイドラインに記された，これら要件に関する記述をリスト化した（表 2）．最後に，規格・ガイドラインのリストを踏まえ，実態調査で得られた傾向はどうして産出されているかを議論した. その結果, 最小文字数「8 文字」や使用可能な文字種「不明」が多いことは説明がつく可能性がある一方，規格・ガイドラインだけでは説明がつかない傾向も多くあることを示した.

5.2 今後の研究課題

本論文で得られた実態調査結果・考察を踏まえて，今後のパスワード構成ポリシーの研究課題を二点述べる. 今後，各研究課題について深堀を行っていく予定である.

- 今回の考察（規格・ガイドラインに基づく考察）では，認証システム設計者・開発者が，最小文字数を 4,6 と設定する理由など, 多くの不明点が残った. すなわち，**認証システム設計者・開発者は，どのようにパスワード構成ポリシーの要件を決めているのか？**

- 今回はシステム視点の規格・ガイドラインの調査結果である．一方，脚注[d]に記したとおり，強固なパスワードを生成するという観点で「ユーザー視点」のガイドラインや教育資料も多く存在することがわかった. **システム視点とユーザー視点の文献間では矛盾が発生していないか？**

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. Furnell: An assessment of website password practices, Computer & Security, Vol. 26, Issue. 7-8, pp. 445-451, 2007.

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

[6] 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.

[7] 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)

[8] 宮崎駿：“パスワードの要件をガイドラインと実態調査から考える”, 入手先〈https://jpn.nec.com/cybersecurity/blog/200918/index.html〉(参照 2021-8-4)

[9] 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).

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 藤田真浩，山中忠和，松田規，金岡晃：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, 情報処理学会研究報告セキュリティ心理学とトラスト(SPT)，Vol. 2021-SPT-43，No. 19，pp. 1-8，2021.

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