

2015年以降のパスワード研究の動向

金岡 晃^{1,a)}

概要：2014年12月に情報処理学会コンピュータセキュリティ研究会において金岡が講演した「パスワード研究の動向」では、主に2010年以降のパスワードに関連する研究の動向が紹介されていた。その後2年が経ち、その間にどういったパスワード関連の研究がされていたかを調べたものが本稿である。2015年以降も引き続き多くの研究がパスワードやその周辺に対して行われており、新たな広まりを見せるなどの特徴が複数見られた。

Trend of password research after 2015

KANAOKA AKIRA^{1,a)}

Abstract: Kanaoka gave a presentation entitled with “Trend of password research” at the Computer Security Study Group of the Information Processing Society of Japan in December 2014. In the presentation, research trends related to passwords since 2010 have been introduced. This paper examined what kind of password related research was done after 2015. A lot of research continues on passwords and their surroundings after 2015, and there were multiple features such as showing a new spread.

1. はじめに

電子認証方式は多種多様に及んでいる。デバイスやハードウェアが新たに開発され製品化されるとともに、それらを利用した電子認証方式が新たに生まれている。一方で、提案されてきた多種多様な電子認証方式において、広く一般的に利用されている手法は数少ない。古来から存在するパスワードが、新たな電子認証方式に対して変わらず強い支配力を保っている。

2012年にBonneauらが調査・調査した分析においても、パスワードが変わらず広く利用されていることや、さまざまな認証方式がパスワードに勝るセキュリティやユーザビリティを持つ一方で広まっていないことが指摘された[6]。Bonneauらの論文では、パスワードが変わらずに広く使われている点はその配置・配備のしやすさ (Deployability) にあると分析していた。

さまざまな電子認証方式の提案がされるのと同時に、パ

スワード自身やその周辺技術に関する研究もいまだ盛んである。2014年12月に情報処理学会のコンピュータセキュリティ研究会において著者は「パスワード研究の動向」と題して研究動向を紹介した[40]。

本稿ではそれからさらに2年を経過した現在において、パスワードに関連する研究がいかに変遷してきたかを調査したものである。

調査は、2015年以降の論文において、セキュリティ関連での有名国際会議やユーザインタフェース関連での有名国際会議をターゲットに、パスワード関連の研究をピックアップした。セキュリティ関連の会議として、IEEE Symposium on Security and Privacy (IEEE S&P) とその併催ワークショップ、USENIX Security Symposium (USENIX Security) とその併催ワークショップ、ACM Conference on Computer and Communications Security (ACM CCS) とその併催ワークショップ、Network and Distributed System Security Symposium (NDSS) とその併催ワークショップを選択した。またユーザインタフェース関連の会議として、ACM Conference on Human Factors in Computing Systems (ACM CHI)、ACM Symposium on User Inter-

¹ 東邦大学
Toho University, Miyama 2-2-1, Funabashi, Chiba 274-8710, Japan

^{a)} akira.kanaoka@is.sci.toho-u.ac.jp

face Software and Technology (UIST)、ACM International Joint Conference on Pervasive and Ubiquitous Computing (Ubicomp) を選択した。さらにユーザインタフェース関連とセキュリティ関連の双方をターゲットにした Symposium on Usable Privacy and Security (SOUPS) も調査対象とした。

その結果、表 1 にあるように各会議から論文が抽出された。

表 1 各国際会議におけるパスワード関連論文の発表件数

会議名	件数	文献
SOUPS 2016	5	[3], [17], [23], [27], [36]
SOUPS 2015	5	[1], [13], [14], [20], [32]
IEEE S&P 2016	1	[9]
IEEE S&P 2015	2	[7], [10]
USENIX Security 2016	3	[18], [25], [37]
USENIX Security 2015	2	[15], [33]
ACM CCS 2016	3	[16], [35], [39]
ACM CCS 2015	3	[8], [12], [21]
NDSS 2017	1	[22]
NDSS 2016	2	[5], [28]
NDSS 2015	0	
ACM CHI 2016	4	[24], [26], [31], [38]
ACM CHI 2015	5	[2], [11], [29], [30], [34]
UIST 2016	0	
UIST 2015	0	
Ubicomp 2016	1	[4]
Ubicomp 2015	0	

これらの論文の内容を見ることで、パスワードに対してそれぞれの論文がどういったアプローチで研究をしているかがわかる。2章では、2014年のCSEC招待講演で発表された内容を基に、2014年時点でのパスワード研究の動向をあらためて俯瞰し、3章以降では2015年以降の論文を概観していく。

2. 2014年以前の動向

2014年の調査では、2010年以降の論文を中心に分析が行われ、43本の論文に対して分類が行われた。そこで示された分類は以下の通りである。

- ユーザ振る舞い調査：11本
- パスワードデータ解析：9本
- グラフィカルパスワード：9本
- パスワードを強化する仕組み：6本
- パスワードデータを守る仕組み：3本
- その他：5本

最も影響が大きいのがWeirらの論文であろう。2009年にRockYouにおいて3200万のアカウント情報の漏えい事件が起き、2010年にWeirらがそれらのデータを分析し、さらにそのデータセットを利用した推測攻撃の効率化を

行った。パスワードに関する研究はこのWeirの論文から新たな展開を迎えたと言っていい。その後、それらデータセットを用いた分析や、Weirらにより高度化した推測攻撃が1つのパスワード強度の評価指標となった。2015年以降の論文でも、多数のパスワードデータセットを持ちた分析や実証をするケースは複数あり、そこではRockYouの漏えいデータが用いられるなど、パスワード研究の分野では広く使われるデータセットとなっている。

その他、ユーザの振る舞い調査としては、スマートフォンのパターンロックにおけるパターンの偏りや、パスワードの変更を求められたときの人間の振る舞いをモデル化するなどのアプローチなどがあつた。

3. 2015年以降の動向

2015年以降を同じく分類してみると、これまでの動向を引き続き継承しているテーマと新たに盛んになってきたテーマが見て取れる。

もっとも特徴的なのは、システムが生成するパスワードに関する研究であろう [9], [14], [17], [18], [32], [38], [39]。アプローチは様々であるが、システムが生成するパスワードをいかに適切に使うかが議論されている。たとえば、ユーザの普段の行動を把握してそれを元にパスワード生成をすることでユーザが記憶しやすいパスワード生成をするアプローチ [11] があつた。またワンタイムパスワード生成において過去のユーザ経験をもとに生成することで記憶しやすさを高めた方式もあつた [38]。これらは2014年以前では盛んな研究テーマではなかつた。

パスワード生成時や利用時のユーザの振る舞いに注目した研究も多い [9], [14], [17], [18], [32], [38], [39]。そこではパスワード生成時のユーザ振る舞いを基に、Decoyを入れることでより強いパスワードを促す仕組みや [28]、ニームニックを用いた生成 [39] など、ユーザの振る舞いを利用した生成手法の提案がある一方で、パスワードの取り扱い [14] や打ち間違い [9] など振る舞い自身の調査もあつた。

2015年以降で盛んになった研究テーマとしては、パスワードの強度測定とそれを利用したフィードバック機構の研究が挙げられる [12], [25], [30], [31], [33], [37]。パスワードの強度を測定しその強度をフィードバックすることでユーザにより強いパスワードを設定させる試みはこれまでもされていたが、2015年以降の特徴としてはその強度計算手法がより本来のパスワードが持つ強度に近づけるための試みが複数あることや [12], [25], [37]、スマートフォンのパターンロックに対して強度をフィードバックする方法の提案 [30] など広がりを見せている。

パターンロックに対して強度をフィードバックするSongらの提案は、これまでのパスワードに対するフィードバック機構（パスワード強度メータ）を発展させたものであり、裾野の広がりを感じさせるものである。同じく裾野の広が

りとしては、ユーザの特性を1つにとどめず、ユーザの特性に合わせたパスワードの在り方についての研究が複数できてきていることに注目したい。視覚障害を持つユーザに対して、Webにおける認証作業の困難性を調査した Dosono らの論文 [13] や、パスワードマネージャを提案した Barbosa らの論文 [4] は、ユーザ母集団を唯一に定義していたこれまでの研究から一歩進んだ研究と言える。

ユーザ行動に関連した論文として興味深いのが Wash らの論文である [36]。パスワードを利用している多くのユーザが実際に行ってしまっている、または、行っているユーザが実際にいるだろうことが容易に想像される「同一パスワードの複数サイトでの使いまわし」について、実際に定量的な調査を行ったものである。同一パスワードの複数サイトでの使いまわしの実態については、論文としては筆者の知る限りこれまでは存在せず、一方でリスト型攻撃といった言葉があるように広く行われていることが予想される状況にあった。Wash らの論文はそれを一端とはいえ詳しくにした論文であると言える。

ここまでに挙げた論文では、ユーザ行動を利用した手法やユーザ行動そのものの観測など、ユーザが関係した論文が多かった。パスワードに関連する研究ではユーザ行動とは関係せずに技術的なアプローチを行う研究も複数存在する。たとえば Garman らの研究では、TLS における RC4 の利用を用いてパスワードの回復攻撃を行っている [15]。Blocki らはパスワード出現頻度リストに着目し、リストから情報が漏れてしまうことを防ぐために、摂動を頻度リストに加えることで情報の保護を行いながらもリストが有効利用できる手法を提案している [5]。Camenisch らはパスワード認証のプロトコルにおいてサーバ側を複数に分散させて認証を行うプロトコル提案をする [8]、Ruoti らによるパスワード入力時のクライアント側での情報保護 [27] などのアプローチが見られた。

その他も、グラフィカルパスワードやニーモニック認証を対象にした研究 [1], [3], [39] や、標的型のオンラインパスワード推測攻撃に関する研究 [35]、スマートフォンのパターンロックに関する研究 [30], [34]、パスワード構成ポリシーの反映状況をフィードバックする機構の研究 [29]、パスワードマネージャに関する研究 [4], [10], [16] などが見られた。

4. まとめ

2015 年以降の 2 年間の間にパスワードに関連する論文は主要な国際会議だけに限定しても 37 本が発表されており引き続き盛んに研究されている様子が分かった。傾向としては、システムが生成するパスワードに対するアプローチや、強度測定とそのフィードバックに焦点を当てたアプローチなどが盛んになっている様子がうかがえた。またパスワードに関連する研究の裾野の広がりが見えるなど、今

後もパスワードの研究は引き続き多くされていくことが予想される結果となった。

参考文献

- [1] Mahdi Nasrullah Al-Ameen, Kanis Fatema, Matthew Wright, and Shannon Scielzo. The impact of cues and user interaction on the memorability of system-assigned recognition-based graphical passwords. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pp. 185–196, Ottawa, 2015. USENIX Association.
- [2] Mahdi Nasrullah Al-Ameen, Matthew Wright, and Shannon Scielzo. Towards making random passwords memorable: Leveraging users' cognitive ability through multiple cues. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, CHI '15*, pp. 2315–2324, New York, NY, USA, 2015. ACM.
- [3] Adam J. Aviv, Markus Dürmuth, and Payas Gupta. Position paper: Measuring the impact of alphabet and culture on graphical passwords. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, Denver, CO, 2016. USENIX Association.
- [4] Natã M. Barbosa, Jordan Hayes, and Yang Wang. Unipass: Design and evaluation of a smart device-based password manager for visually impaired users. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing, UbiComp '16*, pp. 49–60, New York, NY, USA, 2016. ACM.
- [5] Jeremiah Blocki, Anupam Datta, and Joseph Bonneau. Differentially private password frequency lists. In *23rd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21–24, 2016*, 2016.
- [6] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy, SP '12*, pp. 553–567, Washington, DC, USA, 2012. IEEE Computer Society.
- [7] Fangda Cai, Hao Chen, Yuanyi Wu, and Yuan Zhang. Appcracker: Widespread vulnerabilities in user and session authentication in mobile apps. In *IEEE Mobile Security Technologies (MoST)*, San Jose, CA.
- [8] Jan Camenisch, Anja Lehmann, and Gregory Neven. Optimal distributed password verification. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, CCS '15*, pp. 182–194, New York, NY, USA, 2015. ACM.
- [9] R. Chatterjee, A. Athayle, D. Akhawe, A. Juels, and T. Ristenpart. password typos and how to correct them securely. In *2016 IEEE Symposium on Security and Privacy (SP)*, pp. 799–818, May 2016.
- [10] R. Chatterjee, J. Bonneau, A. Juels, and T. Ristenpart. Cracking-resistant password vaults using natural language encoders. In *2015 IEEE Symposium on Security and Privacy*, pp. 481–498, May 2015.
- [11] Sourav Kumar Dandapat, Swadhin Pradhan, Bivas Mitra, Romit Roy Choudhury, and Niloy Ganguly. Activpass: Your daily activity is your password. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, CHI '15*, pp. 2325–2334, New York, NY, USA, 2015. ACM.
- [12] Matteo Dell'Amico and Maurizio Filippone. Monte carlo strength evaluation: Fast and reliable password checking. In *Proceedings of the 22nd ACM SIGSAC Conference*

- on *Computer and Communications Security, CCS '15*, pp. 158–169, New York, NY, USA, 2015. ACM.
- [13] Bryan Dosono, Jordan Hayes, and Yang Wang. “i’m stuck!”: A contextual inquiry of people with visual impairments in authentication. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pp. 151–168, Ottawa, 2015. USENIX Association.
- [14] Paul Dunphy, Vasilis Vlachokyriakos, Anja Thieme, James Nicholson, John McCarthy, and Patrick Olivier. Social media as a resource for understanding security experiences: A qualitative analysis of #password tweets. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pp. 141–150, Ottawa, 2015. USENIX Association.
- [15] Christina Garman, Kenneth G. Paterson, and Thyla Van der Merwe. Attacks only get better: Password recovery attacks against rc4 in tls. In *24th USENIX Security Symposium (USENIX Security 15)*, pp. 113–128, Washington, D.C., 2015. USENIX Association.
- [16] Maximilian Golla, Benedict Beuscher, and Markus Dürmuth. On the security of cracking-resistant password vaults. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16*, pp. 1230–1241, New York, NY, USA, 2016. ACM.
- [17] Thomas Groß, Kovila P.L. Coopamootoo, and Amina Al-Jabri. Effect of cognitive effort on password choice. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, Denver, CO, 2016. USENIX Association.
- [18] Thomas Gross, Kovila Coopamootoo, and Amina Al-Jabri. Effect of cognitive depletion on password choice. In *The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2016)*, pp. 55–66, San Jose, CA, 2016. USENIX Association.
- [19] Christian Holz and Frank R. Bentley. On-demand biometrics: Fast cross-device authentication. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, CHI '16*, pp. 3761–3766, New York, NY, USA, 2016. ACM.
- [20] Jun Ho Huh, Hyounghick Kim, Rakesh B. Bobba, Masooda N. Bashir, and Konstantin Beznosov. On the memorability of system-generated pins: Can chunking help? In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pp. 197–209, Ottawa, 2015. USENIX Association.
- [21] Jun Ho Huh, Seongyeol Oh, Hyounghick Kim, Konstantin Beznosov, Apurva Mohan, and S. Raj Rajagopalan. Surpass: System-initiated user-replaceable passwords. In *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security, CCS '15*, pp. 170–181, New York, NY, USA, 2015. ACM.
- [22] Johannes Kiesel, Benno Stein, and Stefan Lucks. In *Proceedings of the 24th Annual Network and Distributed System Security Symposium (NDSS 17)*.
- [23] Shrirang Mare, Mary Baker, and Jeremy Gummeson. A study of authentication in daily life. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pp. 189–206, Denver, CO, 2016. USENIX Association.
- [24] William Melicher, Darya Kurilova, Sean M. Segreti, Pranshu Kalvani, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Michelle L. Mazurek. Usability and security of text passwords on mobile devices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, CHI '16*, pp. 527–539, New York, NY, USA, 2016. ACM.
- [25] William Melicher, Blase Ur, Sean M. Segreti, Saranga Komanduri, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Fast, lean, and accurate: Modeling password guessability using neural networks. In *25th USENIX Security Symposium (USENIX Security 16)*, pp. 175–191, Austin, TX, 2016. USENIX Association.
- [26] Weizhi Meng, Wenjuan Li, Lijun Jiang, and Liying Meng. On multiple password interference of touch screen patterns and text passwords. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, CHI '16*, pp. 4818–4822, New York, NY, USA, 2016. ACM.
- [27] Scott Ruoti, Jeff Andersen, and Kent Seamons. Strengthening password-based authentication. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, Denver, CO, 2016. USENIX Association.
- [28] Tobias Seitz, Emanuel von Zezschwitz, Stefanie Meitner, and Heinrich Hussmann. Influencing Self-Selected Passwords Through Suggestions and the Decoy Effect. In *Proceedings of the 1st European Workshop on Usable Security (EuroUSEC '16)*. Internet Society, 07 2016.
- [29] Richard Shay, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Alain Forget, Saranga Komanduri, Michelle L. Mazurek, William Melicher, Sean M. Segreti, and Blase Ur. A spoonful of sugar?: The impact of guidance and feedback on password-creation behavior. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, CHI '15*, pp. 2903–2912, New York, NY, USA, 2015. ACM.
- [30] Youngbae Song, Geumhwan Cho, Seongyeol Oh, Hyounghick Kim, and Jun Ho Huh. On the effectiveness of pattern lock strength meters: Measuring the strength of real world pattern locks. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, CHI '15*, pp. 2343–2352, New York, NY, USA, 2015. ACM.
- [31] Blase Ur, Jonathan Bees, Sean M. Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Do users’ perceptions of password security match reality? In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, CHI '16*, pp. 3748–3760, New York, NY, USA, 2016. ACM.
- [32] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. “i added ’!’ at the end to make it secure”: Observing password creation in the lab. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pp. 123–140, Ottawa, 2015. USENIX Association.
- [33] Blase Ur, Sean M. Segreti, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Saranga Komanduri, Darya Kurilova, Michelle L. Mazurek, William Melicher, and Richard Shay. Measuring real-world accuracies and biases in modeling password guessability. In *24th USENIX Security Symposium (USENIX Security 15)*, pp. 463–481, Washington, D.C., 2015. USENIX Association.
- [34] Emanuel von Zezschwitz, Alexander De Luca, Philipp Janssen, and Heinrich Hussmann. Easy to draw, but hard to trace?: On the observability of grid-based (un)lock patterns. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, CHI '15*, pp. 2339–2342, New York, NY, USA, 2015. ACM.
- [35] Ding Wang, Zijian Zhang, Ping Wang, Jeff Yan, and Xinyi Huang. Targeted online password guessing: An un-

- derestimated threat. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16*, pp. 1242–1254, New York, NY, USA, 2016. ACM.
- [36] Rick Wash, Emilee Rader, Ruthie Berman, and Zac Wellmer. Understanding password choices: How frequently entered passwords are re-used across websites. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pp. 175–188, Denver, CO, 2016. USENIX Association.
- [37] Daniel Lowe Wheeler. zxcvbn: Low-budget password strength estimation. In *25th USENIX Security Symposium (USENIX Security 16)*, pp. 157–173, Austin, TX, 2016. USENIX Association.
- [38] Sarah Wiseman, Gustavo Soto Mino, Anna L. Cox, Sandy J.J. Gould, Joanne Moore, and Chris Needham. Use your words: Designing one-time pairing codes to improve user experience. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, CHI '16*, pp. 1385–1389, New York, NY, USA, 2016. ACM.
- [39] Weining Yang, Ninghui Li, Omar Chowdhury, Aiping Xiong, and Robert W. Proctor. An empirical study of mnemonic sentence-based password generation strategies. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16*, pp. 1216–1229, New York, NY, USA, 2016. ACM.
- [40] 晃金岡. パスワード研究の動向. 研究報告コンピュータセキュリティ (CSEC) , Vol. 2014, No. 3, pp. 1–1, nov 2014.