【研究ノート】

パスワード管理方法教育の必要性と具体的な方法について
－紙のメモと表計算ソフトを併用した方法の提案とその実用性についての検討－

京都光華女子大学　　臼井　義比古

1 はじめに

現代ではコンピュータの利用は必要不可欠であるが、個人でコンピュータが提供するサービスを利用する場合、利用資格の認証が必要となることがほとんどである。これらのうちログインパスワードによる認証は一般的に利用されており、利用者に理解されやすいことから、今後も使われていくと考えられる。一方で、ログインパスワードを用いた利用者認証には、ログインパスワードの管理の難しさや使い回しによるログインパスワードの流出などの問題もある。たとえば、電子的な方法でログインパスワードを記録すれば、ネットワーク経由での流出の可能性が増え、紙を用いた管理ではつねにメモを持ち運ぶ必要があるなど利便性が損なわれてしまう。さらに、学校で、生徒や学生(情報が非専門)などへの教育の場合は、生徒や学生が高度な情報技術を理解できることを前提とする、あるいは、金庫を用意できるような前提はとれない。今回、すべての場合には適用できないが、Microsoft 社のアプリケーションである Office 製品を準備できる場合での、学校で教育可能なログインパスワードの管理方法の一つについて提案を行う。

2 問題点

本稿では、インターネットのサイトを利用する際に正当な利用者であることを確認するための、サイトと利用者の間の符丁として用いられる文字列をログインパスワードと呼ぶ。

ログインパスワードは、文字列の設定で利用できるようになることから、一般的に用いられている仕組みであり、今後も正当な利用者の確認に用いられる方法であると考えられる。

ログインパスワードはログイン先への登録で流出する可能性があり、使いまわすべきではない。しかしながら、TRENDMICRO 社が 2020 年に行ったアンケートで、85.2%の回答者がログインパスワードを使いまわしていると報告されている。ログインパスワードを使いまわす理由としては、『「異なるパスワードを設定すると忘れてしまう」（71.4%）、「異なるパスワードを考えるのが面倒」（49.4%）』(TRENDMICRO、2020)という結果であった。つまり、ログインパスワードを忘れてしまう不安やログインパスワード設定を急ぐあまり、使いまわしが発生しているということになる。

ログインパスワードは忘れないように記録する必要があるが、ただ記憶すれば良いというわけではなく、記録が流失しないように管理する必要があり、具体的な管理方法を決めるのが難しい。管理方法に不安があると、使いまわしを助長すると考えられる。

内閣サイバーセキュリティセンター(NISC)は「インターネットの安全・安心ハンドブック」(ハンドブック)を発行し、一般的に利用可能なログインパスワードの管理方法が記載されて有益であるが、一

方で、金庫が必要な方法も記載されており、教育内容としてはそのまま採用できない(NISC、2020、p61)。また、NISC のハンドブックでは、スマートフォンアプリケーションを用いたログインパスワードの管理方法を推奨しているが、これらのアプリケーションは必ずしも信頼できるものではない。あるいは、アプリケーションを選択して利用する必要があるが、この選択が難しい。学校教育で推奨する方法として、これらの問題についても配慮する必要がある。

また、管理方法の改善だけでは不十分なことも考えられ、本稿では、管理方法だけでなく、ログインパスワードの準備教育の必要性についても第４章で言及する。

2−1 ログインパスワードの問題点

ログインパスワードの問題点としては、類推されやすいログインパスワードを利用者が設定してしまうと、他者に試されすぐに知られてしまう事や、類推し難いログインパスワードであっても、何度でも試すことが可能であれば、すべての組み合わせを試すことで、ログインパスワードが知られてしまうことがあげられる。ただし後者については、何度も試せないような防御機能(アカウントロック)や反応遅延が設定されているのが一般的である。

他の問題点としては、あるサイトでログインパスワードを設定すると、そのサイトの管理者にログインパスワードを知られてしまう可能性があるため、すべてのサイトに対して異なるログインパスワードを設定する必要があり、ログインパスワードが覚えられないほど増えてしまう可能性があることがあげられる。また、増えたログインパスワードを記録する方法によっては、ログインパスワードが漏れてしまう可能性が高くなることがあげられる。

ログインパスワードが類推されてしまう問題点の解決方法は、利用者の理解を求めて利用者が設定しないように働きかけることや、類推されやすいログインパスワードのリストを作り、それらをログインパスワードとして受け付けないようにすることがあげられる。前者については日本の高校教育用の教科書に述べられており、一定の対応はなされていると判断できる(坂村、2020)(萩谷、2022)。さらなる改善策としては、本稿の第４章で提案する方法での改善が期待されると考えている。

ログインパスワードの試行を繰り返され、知られてしまう問題点は、一般的にログインをさせる側で試行回数制限による防御機能(アカウントロック)が働いて、ログインパスワードが守られていると考えてよい。ただし、短いログインパスワードは見つけられやすいため、アカウントロックの内容に応じたログインパスワード文字列の最低限長が必要になる。NIST では、1分に3回しか試行できなくすれば、ランダムな文字列で 6 文字、利用者が作成する文字列で 8 文字程度の文字列で問題がないと報告している(NIST、2004、付録 A)。NIST の文献は 2004 年のものだが、当時の計算機能力を想定して導出されたものではなく、アカウントロックの制限から情報エントロピを計算したもので、現在の議論の根拠として問題はない。また、NISC ではアカウントロックの有無には触れていないが、ログインパスワードは 10 文字以上としており、アカウントロックがなされていなくても、インターネットを経由することによる遅延などだけを考慮しているものと考えられる(NISC、2022)。

過剰な最低文字の制限はかえって問題を生むことがあるが、日本で行う教育では、NISC のハンドブックに従って、10 文字以上とするのが適切であると考えられる。ただし、これは、汎用的な場合であって、サービス提供側からの指示があれば調整が可能であることは、教育として説明するべきである。

また、アカウントロックの内容がサービス側から提供されている場合は、その内容に応じて変更することも可能であると説明するのが望ましいが、高校までの教育や大学の情報系非専門の学生の教育に取り込むことは難しいと考えられる。

2−2 ログインパスワードの記憶方法の検討

ログインパスワードはサイトごとに変更する必要があり、一人の人が利用するサイトが多くなれば、覚えるべきログインパスワード数も多くなる。これらの記憶方法については、紙のメモやスマートフォンアプリケーションなどが考えられるが、スマートフォンアプリケーションなどの電子的な記録方法の利用については否定的なところもある。例えば、滋賀大学では「しがだいＩＤやパスワードをコンピュータ上に記憶させていると、コンピュータウイルスや不正なプログラムにより情報が流出し、データ消失・情報漏えい等の被害を拡大させる危険性が高くなります。」とそのホームページに記載している(滋賀大学情報機構)。

また NISC ではスマートフォンでの保存方法は推奨としながらも、クラウド上の保存については推奨せず、スタンドアロンで使えるものを優先するように記載している。これはクラウドサービスのセキュリティレベルの実態を利用者が知り得ないためであると書いている(NISC、2020、p61)。

さらに付け加えて言えば、スマートフォンアプリケーションは悪意を持って作られたものかどうかを利用者が知り難い。学校で教育の一環として行う場合は、スマートフォンアプリケーションを安易には信用しないように説明したほうがよいことに配慮すると、その選択は非常に難しい。より安全な作成元の開発したソフトウエアがあればそれらを優先するべきである。

紙のメモによるログインパスワードの管理は NISC などで推奨されている。たしかに、上述の電子的な管理方法の問題点は回避できるが、不便さや、紙での管理方法などの問題が発生すると思われる。例えば紙のメモあるいはノートの場合は紛失時に備える必要があり、NISC のハンドブックでは 2 つ作成し、金庫などでの管理が必要と記載されているが、学校教育でなくても金庫の準備は難しい。

今回は一部の環境に限定されるが、Microsoft 社の Word や Excel や PowerPoint などの製品が利用可能な場合のログインパスワード管理の改善方法について提案し、評価をおこなう。

２－３ 今回利用する暗号化の暗号キーについて

暗号キーとは電子システムで情報を暗号化するときに使う文字列である。暗号キーで暗号化した情報は、暗号キーを知っているものだけが読みとることができる。ファイルの暗号化を行うときにも使われ、一部のシステムでは、ログインパスワードと同じく「パスワード」と呼ばれているが、本稿では、「暗号キー」と記述して「ログインパスワード」と区別する。

暗号キーの問題点としては、暗号キーの試行回数が制限できないため、暗号化された情報(ファイル)を入手されてしまうと、暗号キーを何度も試されてしまい、情報自体が漏れてしまうことである。

ただし、暗号キーの文字数を増やすと、暗号キーをすべて試すための回数を文字数のべき乗で増やすことができるため、暗号化された情報が漏れても、情報自体を読みとられにくいようにすることが可能である。

また、ファイルが漏れても、十分に長い暗号キーを用いていればファイルからは暗号キーが漏れない

ため、異なる情報を収めたファイルの暗号化に同じ暗号キーを用いることもできるし、一度作った暗号化ファイルをそのままコピーすることもできる。

暗号キーとして必要な長さは NISC のハンドブックによれば 15 文字である(NISC、2022、p58)。暗号キーを一つ覚える程度であれば、十分実現可能であると判断できる長さである。

3 パスワード記憶方法の提案

Microsoft 社のオンライン版でない(アプリ版と呼ぶ)Word や Excel や PowerPoint(Office 製品)を利用できる場合に限定されるが、これらのソフトウエアを用いて、ログインパスワードを記録し、十分長い暗号キー(製品内では「パスワード」と表現されている)を設定する方法を、学校教育で行える一方法として提案する。アプリ版の Office 製品が使えない環境については第 5 章のまとめでコメントする。

Office 製品で、「完全にランダムで英大文字小文字＋数字＋記号混じりで 15 文字以上」(NISC、2022、p58)の暗号キーで暗号化すると、暗号化されたファイルを入手されても、試すべき暗号キーが多いため、暗号化された情報を読まれる可能性が極めて少ない。ファイルをクラウドに置いてファイル自体が流出しても、内容も暗号キーも漏れないため、コピーが可能である。同様に、暗号キーを使いまわすことも可能である。

このため、暗号キーを一つ覚えれば十分であるし、その一つを覚えきれない場合は紙にメモして管理が可能である。

3−1 提案の配慮点

先に問題点としてあげた、ソフトウエアの開発会社としての信頼性に関しても、Microsoft 社は Windows OS を作成し、同 OS は広く使われていることから、一定のレベルで信頼できると判断できる。Microsoft 社がパスワードの入手を目的としてこれらの Office 製品を作っているという疑いをもつのなら、OS レベルでおこなっている可能性から疑いをもつべきである。同社の OS を利用するならアプリケーションも同列で判断するのが妥当であると考えてよい。ただし、以上は企業としての信頼性であって、クラウドの安全性については、会社と管理業務を行う人を区別して考え、信頼できるかどうかの判断が難しいと考える人も多いと思われる。

3−2 暗号キーに対する風評について

Office 製品にはパスワード解析ソフトウエアが存在しているとインターネット上では書かれているが、これらの解析ソフトウエアは類推とパスワードの総当たりを行うソフトウエアであり、例えば NISC が言う 15 文字以上のような十分な長さを持つ暗号キーを用いると、解読できない。

以上のことから、Office 製品を用いてログインパスワードの暗号化を行えば、クラウドの安全性を検討することなく、比較的慣れた操作で、便利にログインパスワード管理ができることがわかる。

4 事前準備の提案

ログインパスワードを決定する必要が急に起こることがある。しかし、急いで決めると、記録、記憶できないし、ログインパスワードを忘れる不安から、類推しやすいログインパスワードやすでに覚えて

いるログインパスワードを使い回すことが多くなると推察できる。

そこで本稿では、たとえば 3 で提案した Office 製品を管理ツールとして用い、ランダムなログインパスワードを事前に準備し、準備したログインパスワードを、あらかじめ管理ツール(Office 製品など)にサイト名や ID がからのまま記録しておき、インターネットサイトのログインパスワード設定時に、ID やサイト名を入力する方法を提案する。

このようにすることで、ログインパスワードなどを忘れてしまう不安を減らし、毎回同じ手順を取ることで、ログインパスワード入力の作業の安定性を増し、推察可能なログインパスワードや短いログインパスワードやログインパスワードの使い回しを防ぐことにつなげられないかという提案である。

5 まとめ

ログインパスワードの安全な管理方法として、Office 製品を利用し、15 文字以上の暗号キーをかけた暗号化ファイルに保存する方法を、学校で教育可能なログインパスワード管理方法として提案した。NISC によれば、15 文字以上の暗号キーがかかった Office 製品のファイルはファイルの保存場所によらず安全である。クラウド上に置いても、内容を総当りで読まれてしまう可能性が極めて低く、NISC の推奨基準をクリアする。NISC はデータをクラウドに置かないスマートフォンアプリケーションか紙での管理を推奨し、クラウドの利用に慎重になるようにアドバイスしているが、15 文字以上の暗号キーが解読されにくいという前提にたてば、保存場所は関係がないと考えられる。

上記はアイデア的な方法に依存しないという利点がある。アイデア的な方法には全員がアイデアを採用すれば、偏りが生じ、安全性が崩れることがあるという問題がある。たとえば「password」をログインパスワードにするというアイデアも、他に誰も思いつかなければ、記憶しやすいログインパスワードの作り方の良いアイデアであったかもしれないが、結局はだれもが思いついたため、採用できないアイデアになってしまった。

また、ログインパスワードの使い回しを減らす目的で、事前にログインパスワードを準備しておく方法も、学校でのログインパスワード管理方法の教育内容として提案を行った。

作為的な攻撃を行う可能性が低い OS ベンダーに対するアプリケーション提供元としての信頼度はやはり高いため、Microsoft 社や Google 社が、標準添付のテキスト編集アプリケーションでの暗号化保存ツールを作成することを期待したい。詳しく調べる必要はあるが、Apple 社は「メモ」で 15 文字以上のパスワードをかけると同様のことができるようである。また Google 社の「Keep メモ」はクラウドの安全性を信用して使うことになる。

学校教育だけでなく、長い暗号キーの利用とログインパスワードの事前準備がひろがれば、より安全なログインパスワード社会の構築が可能になると考える。

参考文献

TRENDMICRO(2020)「－ログインパスワードの利用実態調査 2020－新型コロナウイルス拡大前後で約 2 割がネット上で機微情報の取り扱いが増加」https://www.trendmicro.com/ja_jp/about/press-

release/2020/pr-20200929-01.html (2022/11/23 確認)
NISC(2022)「パスワード・Wi-Fi・ウェブ・メールのセキュリティを理解して、インターネットを安全に使おう」『インターネットの安全・安全ハンドブック』内閣サイバーセキュリティセンター、Ver. 4.20、https://www.nisc.go.jp/security-site/handbook/index.html (2022/11/23 確認)
坂村健、越塚登、重定如彦、清水謙多郎、加納寛子、大橋真也、志賀潔、武沢護、骨川敬章、松本吉生、数研出版株式会社編集部(2022)「改訂版高等学校情報の科学」数研出版
萩谷昌己、渡辺美智子(編修)、西村和則、厚地一弘、糸井和弘、大石智弘、岡本尚志、佐藤万寿美、高瀬敏樹、布施泉、実教出版株式会社、岡本敏夫(監修)(2022)「最新情報 I」実教出版
NIST(2006)「Digital Identity Guidelines」『NIST Special Publication 800-63 Version 1.0.2』(IPA 及び NRI による翻訳版の URL：https://www.ipa.go.jp/files/000025342.pdf)(2023/1/14 確認)
滋賀大学情報機構「パスワードの重要性とその設定方法」https://itc.shiga-u.ac.jp/itc/?page_id=50 (2023/1/14 確認)

The Necessity for Password Management Training and Specific Methods of Management:

A Proposal for a Method Using Paper Memos and Spreadsheet Software, and Consideration of Its Practicality

Yoshihiko USUI

Login passwords are likely to be one of the authentication methods used on Internet sites for some time to come, but there are problems. For example, frequently used login passwords such as "password" can be easily guessed, and short login passwords can be discovered even if account locking is enabled on the server side. Also, if you use the same login password at other sites, leakage is likely to occur. In order to prevent these problems, cooperation among users is required. However, looking at the results of a certain questionnaire, it turned out that considerable reuse is being carried out among Internet users. The reason for this is thought to be that the methods of managing login passwords which has been recommended so far was difficult to use for many users. Therefore, we would like to propose a safer and more feasible login password management method that can be used in school education. Specifically, it is a method of using OS vendor application software for encryption and using an encryption key of 15 characters or more in accordance with NISC recommendations. By using a sufficiently long encryption key, a brute force attack can be avoided and the encryption key will not be leaked. Since the encryption key is not leaked, one encryption key can be reused many times. If there are a few encryption keys, they are easy to remember and easy to manage even if they are written down on paper. We believe that teaching this method in schools will reduce the reuse of Internet users' login passwords. In this paper, we would also like to propose preparing alternative passwords in advance as a method to avoid the reuse of login passwords.