2022.09.15

サイバーセキュリティニュース ＜2022 No.001＞

パスワードに頼り切らない認証方法とは～多要素認証のススメ～

【要旨】
■ アクセス管理に用いられるID・パスワードを狙う攻撃は様々あり、その設定にはいくつかの推奨事項があるが、適切に設定されないといったIT統制上の課題がある。
■ 多要素認証とは、知識認証、所有物認証、生体認証のいずれか複数の認証を行い、定められた全ての要素が揃うことで認証に成功する仕組みである。
■ 本稿では、アクセス管理の一要素である識別・認証・認可の役割と、よりセキュアな認証を実現する多要素認証について説明する。

１．ＩＤ・パスワード管理の課題

インターネットを介したサイバー空間は、世界中の誰でも・どこからでも利用できる公共財の一つであり、いつでも・どこからでも欲しい情報にアクセスできる利便性をもたらす一方で、秘匿にしておきたい機密情報や個人情報などといった重要情報が想定しない第三者から閲覧される可能性がある。

秘匿にしておきたい重要情報へのアクセス管理の役割を担っているのがIDとパスワードであるが、ひとたびパスワード情報が悪意ある攻撃者に知られると、重要情報を盗取するといったサイバー攻撃の起点とされるおそれがある。

例えば、リスト型攻撃[1]や辞書攻撃[2]、総当たり攻撃[3]など、パスワードの盗取を目的とした攻撃手法は様々存在しており、複数の異なるサービス間において使い回されているパスワードや、誕生日や氏名で構成される推測が容易なパスワードはかかる攻撃によって攻撃者に盗取される可能性が高い。

従前より企業の情報システム担当やサービス提供事業者は、利用者に対して以下のようなパスワード設定を促している。

・サービス毎に固有のパスワードを設定する
・大文字、小文字、数字、記号を織り交ぜて設定する
・同じ文字の繰り返し(aaaaa)や順番(abcde…)のパスワードを利用しない

一方で、複雑なパスワードは利用者の管理負荷を増大させるため、上記の要求項目が形骸化してしまい、社内のIT統制が正しく機能せず、セキュアな状態の確保が難しくなっている。

本稿では、アクセス管理の一要素である識別・認証・認可の役割と、よりセキュアな認証を実現する多要素認証について説明する。

２．識別・認証・認可とは

サイバー空間において、利用者を限定して特定の利用者のみがアクセスできる仕組みの一つに識別・認証・認可のプロセスがあり、情報セキュリティにおける機密性・完全性・可用性[4]を守るために不可欠な要素となっている。

---

1 何らかの手段により不正に入手した他者のＩＤ・パスワードをリストのように用いて様々なサイトにログインを試みることで、個人情報の閲覧等を行うサイバー攻撃。

2 辞書に登録されている単語や人物名などを組み合わせたものをパスワードに使用して、システムなどへのログインを試みるサイバー攻撃。

3 パスワードを解読するため、考えられる全てのパターンを試す方法。

4 「機密性」は特定の人だけが情報にアクセスできるように制限をかけること、「完全性」は情報が不正に改ざんされないこと、「可用性」はシステムを継続的に利用できることを指し、情報セキュリティ三要素と総称される。

（１） 識別(Identification)

識別とは、サイバー空間にアクセスする利用者に対して固有の識別子を与える仕組みであり、現実空間における免許証や社員証、学生証のような仕組みである。サイバー空間では自分自身の身元証明として ID がユーザーごとに付与される。例えば、A さんがメール機能や動画視聴、マップ機能が利用できるシステム X を新たに利用する場合、A さんの個人情報(氏名・メールアドレス等)を登録することで、システム X を利用する際の固有の識別子(＝ID)が付与される。

（２） 認証(Authentication)

認証とは、識別において付与された ID の正当性を検証するプロセスである。現実空間では免許証等に付与されている顔写真と、免許証を保有している人物の顔が同一であると判断できるかどうかを通じて本人性を確認している。サイバー空間において自分自身を証明する仕組みとして、本人だけが知り得る情報を元に本人の特定を行う。例えば、A さんがシステム X にログインを試みる場合、ID と A さんのみが知っている情報(パスワード)を組み合わせることで、システムにアクセスをしようとしている A さんの本人性を確認することができる。

（３） 認可(Authorization)

認可とは、識別と認証によりアクセスを試みる利用者の本人性が確認できた後に、当該利用者がどの機能・サービスを利用できるかを決定する仕組みである。例えば、A さんがシステム X においてメール機能のみ利用できる権限が付与されている場合、その機能のみにアクセス権限を付与することが認可である。認可の仕組みが存在しない場合、識別・認証のプロセスにおいてアクセスする利用者の身元が特定できたとしても、システム内のすべての情報に自由にアクセスできることになり、秘匿としたい情報を秘匿のままにすることが出来なくなる可能性がある。

【図１】識別・認証・認可の概念図

識別・認証・認可の３要素の中でも、特に「認証」はアクセスする本人の本人性確認として重要な機能を果たしている。これまでは「本人のみが知り得る情報」を「パスワードのみに依存」して認証をしてきたが、推測が容易なパスワードや使い回しをしているパスワードは容易に盗取される可能性があることは前述のとおりである。

３．多要素認証とは

多要素認証とは、「本人のみが知り得る情報による認証(知識認証)」、「本人のみが所有している物による認証(所有物認証)」、「本人の身体的特徴による認証(生体認証)」のいずれか複数もしくは全てを組み合わせることで認証の強度を高める方法である。

多要素認証では、仮にパスワード情報が漏えいしたとしても、システムにアクセスする際にパスワード以外の追加要素が必要になるので不正アクセスの成功率を低減させることができる。例えば、インターネットバンキングで現金を振り込みする際は、パスワード(＝本人のみが知り得る情報）に加えて本人が持つ乱数表(＝本人のみが持ち得る所有物)に記載された特定の数字の両方が必要となるケースがあり、身近な多要素認証の一つである。悪意のある攻撃者はパスワードだけを入手したとしても、乱数表が手元になければ不正送金をすることはできない。

【表１】　認証の三要素とその具体例

要素	メリット	デメリット	具体例
知識認証 (Something you Know)	・導入が容易	・忘れてしまう可能性がある ・突破方法がいくつか存在する	・暗証番号 ・パスワード
所有物認証 (Something you Have)	・忘れる可能性がない	・認証機器を保有する必要がある ・紛失/盗難のリスクがある	・ICカード ・スマートフォン ・乱数表
生体認証 (Something you Are)	・忘れる可能性がない ・本人自身が鍵となるので偽装が難しい	・利用者の抵抗感を考慮する必要がある ・本人拒否率/他人受入率について考慮する必要がある	・指紋認証 ・声帯認証 ・顔認証

続いて、認証の三要素(知識認証・所有物認証・生体認証)それぞれの概要と利用時に注意するポイントについて説明する。

（１）知識認証(Something you Know)

知識認証とは、パスワードや暗証番号による認証のことを指す。

NIST(米国国立標準技術研究所)から発行されている認証に関するガイドライン「NIST SP800-63B」において、パスワードは最低 8 文字、最大 64 文字、スペースを受け入れるべきという推奨事項があり、これは「パスワード」から「パスフレーズ」への移行を促している。

「パスフレーズ」とは、いくつかの単語を組み合わせて「I have lived in Tokyo for 5 years」や「I want to be a cybersecurity expert」のようにランダムな文字列ではなくフレーズとなっているものを指す。パスワードは長く複雑であればあるほど強度が高くなる一方で、利用者が忘れてしまう、また第三者が閲覧できる形でメモを残してしまう可能性も高くなり、パスワード漏えいのリスクが大きくなる。フレーズであれば利用者も覚えやすく、文字数も長くなるためパスワードの強度を高めることができる。また、スペースを受け入れる設定が有効になっていることでフレーズのパターン数が増加するので、理論的にありうるパターン全てを試す総当たり攻撃への耐性も高くなる。

一方、「ThankyouThankyou」のような単純なフレーズは、辞書に載っている単語や人物名を組み合わせてログインを試す辞書攻撃により突破されてしまう可能性が高い点に留意する必要がある。

NIST SP800-63Bの推奨事項

・パスワードは最低8文字(Shall)・最大64文字まで受け入れ、スペースを受け入れる(Should)
・過去に漏えいしたパスワード、辞書に含まれる言葉、繰り返し(例：aaaaa)、
もしくは連続的な文字(例：abcd1234)がパスワードに含まれる場合は、
異なるパスワードを設定することを要求し(Shall)、その理由をユーザーに知らせる(Shall)
・ユーザーが設定するパスワードの強度メーターを表示して強力なパスワードの設定を促す(Should)
・ユーザーに対して定期的なパスワード変更を要求するべきではない(Should Not)
ただしパスワードの漏えいが発覚した場合は変更を強制する(Shall)
・パスワードマネージャーの利用を促すために、パスワード入力の際にペースト機能を有効にする(Should)
・パスワードを入力する際、＊表示ではなく入力している文字を表示する(Should)

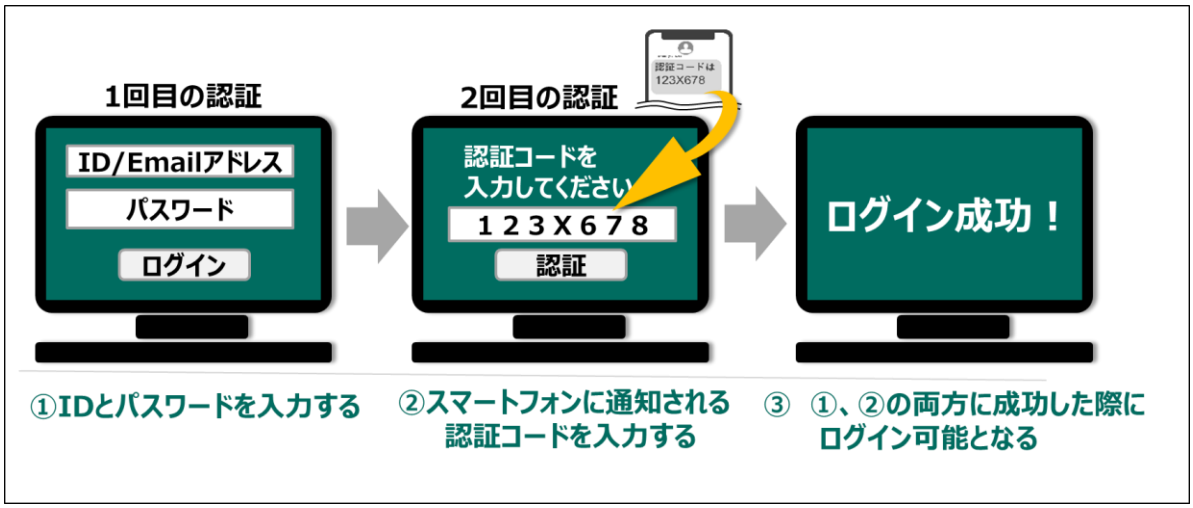
【図２】　NIST SP800-63B のパスワード設定に関する推奨事項

また、利用者に対して定期的にパスワード変更を求めることは避けるべきという推奨事項もある。理由として、利用者側が覚えやすい簡単なパスワードを設定したり、既存パスワードの一部のみを順番に変更する(xxxxx1 から xxxxx2、xxxxx3. . .)原因となることが挙げられる。ただし、パスワード情報が漏えいしていると分かった際は利用者に変更を強制するべきであり、「どんなことがあっても利用者にパスワード変更を要求してはならない」と誤認しないよう留意されたい。

（２）所有物認証(Something you Have)

所有物認証とは、IC カードやスマートフォン、乱数表など本人のみが所有している物を通じて認証を行う仕組みである。個人で保有するスマートフォンを所有物認証に使う際は、Google 社や Microsoft 社が提供している認証アプリを利用する方法と SMS[5]を利用する方法等が挙げられる。

所有物認証を利用した多要素認証は【図３】のように進み、①と②の両方の要素を満たすことでログイン可能となる。



【図３】　所有物認証を用いた多要素認証の例

5 携帯電話の電話番号を使ってメッセージを送受信するサービスである、Short Message Service の略

なお、NIST SP800-63B において、SMS はセキュリティを考慮したサービスではなく、送受信内容が傍受されるリスクがあるので所有物認証の際に用いることは避けるべきと示されている。今後、SMS を利用した所有物認証はサポートされなくなる可能性があり、今後の動向に注視する必要がある。

（３）生体認証(Something you Have)

生体認証とは、本人の身体的特徴を認証に用いる手法で、スマートフォンの指紋認証や、国際空港の出国審査に活用されている顔認証などが挙げられる。

生体認証は、知識認証で懸念されるパスワードの失念や所有物認証で懸念される紛失による機能停止は起こり得ないが、生体認証を用いてアクセス管理をする際の注意点を 2 点紹介する。

1 点目は、生体認証の精度の問題である。生体認証は完全に誤りなく本人と他人を識別できるわけではなく、登録された本人ではない他人が認証される他人受入率と、登録された本人であるにも関わらず認証が拒否される本人拒否率が、機能の確保と利便性に大きく影響する。オフィス等のエントランスの顔認証ゲートにおいて、他人受入率が高いと、正当な権限を持たない者の入室を許可してしまう可能性が高まる。一方、本人拒否率が高いと、オフィスの関係者であり正当な権限を持つにも関わらず、オフィスへの入場が出来ず、利便性を損ねてしまう。そのため、生体認証を利用する際は他人受入率と本人受入率の精度を調整することが肝要である。

2 点目は、生体認証は本人の身体的特徴という個人情報を登録するため、登録する本人の感情についても考慮する必要があるということである。例えば、生体情報として DNA 情報の提供を求められた場合、DNA 情報の改ざんや漏えいを懸念して、強い心理的抵抗感を持つ可能性がある。また、生体認証を登録する際、何らかの身体的マイノリティを持つ方は生体データの登録自体ができないことも想定できる。認証サービスとして生体認証を利用する際は、代替手段として生体認証以外の認証方法を用意する配慮が不可欠である。

４.「認証」の展望

米国サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA)は 2021 年 8 月、リモート環境から国の重要なインフラを支えるシステムにアクセスする際、パスワードのみを用いた単要素認証は「Badpractice」、つまり、やってはいけないことであると発表した。対象はインフラ企業であるが、コロナ禍においてその他の企業も社内ネットワークへリモートアクセスする機会は増加しており、業種や事業規模を問わず、サイバー攻撃の脅威から自社を守るために、パスワードのみに依存した認証のリスクを正しく認識して多要素認証の利用を積極的に検討することが求められている。

また、「FIDO 認証[6]」や「WebAuthn[7]」などパスワードを使わない認証技術をはじめとした新たな認証方法やガイドラインが発表されている。2022 年 5 月には、Apple 社、Google 社、Microsoft 社が共同で、FIDO 認証の機能を拡充し、異なるプラットフォーム間であっても、シームレスに FIDO 認証の技術を利用できるパスワードレス環境を拡充していく計画を発表した[8]。この取り組みにより、利用者をパスワード利用の煩雑さから解放し、利便性と安全性が保たれた認証方法の普及を期待できる。

セキュリティ対策には、資産管理やアクセス管理、脆弱性管理など、多くの要求事項があり、その中でも認証はアクセス管理の重要な要素の一つとなっている。本稿が認証に関する考え方のアップデー

---

[6] FIDO(Fast IDentity Online)認証とは、パスワードを利用せず、生体認証を用いた認証技術の一つである。現在、FIDO Alliance によって規格の標準化が進められている。

[7] WebAuthn(Web Authentication)とは、ブラウザ上で FIDO 認証を実現する仕組みであり、Google Chrome や Microsoft Edge、Mozilla Firefox 等のブラウザでサポートされている。

[8]FIDO Alliance「Apple、Google、Microsoft が FIDO 標準のサポート拡大にコミット、パスワードレス認証の訴求を促進」
https://fidoalliance.org/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard-to-accelerate-availability-of-passwordless-sign-ins-jp/?lang=ja (2022 年 7 月 14 日閲覧)

トの参考となり、サイバーセキュリティ対策強化の一助となれば幸いである。

ＭＳ＆ＡＤインターリスク総研株式会社
リスクマネジメント第三部 サイバーリスクグループ
コンサルタント　辻本　竜一

ＭＳ＆ＡＤインターリスク総研株式会社は、MS&AD インシュアランスグループに属する、リスクマネジメントについての調査研究及びコンサルティングに関する専門会社です。
情報セキュリティに関するコンサルティング・セミナー等を実施しております。
コンサルティングに関するお問い合わせ・お申込み等は、下記の弊社お問合せ先、またはあいおいニッセイ同和損保、三井住友海上の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
ＭＳ＆ＡＤインターリスク総研㈱
リスクマネジメント第三部 サイバーリスクグループ
東京都千代田区神田淡路町2-105　**TEL.03-5296-8932**
http://www.irric.co.jp/

本誌は、マスコミ報道など公開されている情報に基づいて作成しております。
また、本誌は、読者の方々に対して企業のリスクマネジメント活動等に役立てていただくことを目的としたものであり、事案そのものに対する批評その他を意図しているものではありません。