インターネットでの不正行為 その傾向と対策

今回は、不正アクセスの被害からあなたを守るための基本中の基本であるパスワードについて解説します。インターネットにアクセスする、会社のネットワークにアクセスする、メールを読む…。あまりにも日常的すぎてその重要性を忘れていませんか？ もし、そうだったらこの記事を読んでください。そして、パスワードがどんな意味を持つのかをしっかりと理解してください。

第3回 パスワードについて心がけてほしいこと

JPCERT/CC（コンピュータ緊急対応センター）
URL http://www.jpcert.or.jp/

パスワードとは何か？

まずは、パスワードは何のためにあるのか、最初に立ち戻って考えてみましょう。

パスワードの定義を考えてみます。パスワードを定義するとすれば、「システムの利用を許可されている者であるかどうかを認証するための手段として用いられる文字列」というものになるでしょう。許可されている者のみ知っている情報をシステムに与えることによって、システム側は正しい利用者であるかどうかを判断します。

パスワード認証は、正当なユーザーだけがパスワードを知っているという前提にもとづいています。 したがって、システム側から見れば、まずパスワードの存在が最初にあり、そのパスワードを知っている者が、正当なユーザーであると判断することになります。パスワードとは、このようにシステムに対して、「あなたがあなたであること」を証明するための情報でもあるのです。

パスワードを用いた認証方法は、アリババと40人の盗賊での「ひらけゴマ」で有名なように、昔のアラビアの物語にも現れる、古くから知られている認証方法で、しかも、認証システムのコスト負担が少ない方式です。

パスワード認証は、利用している人間の記憶に（それとシステム中に安全な形で）パスワードが存在しているという前提に立って運用されます。したがって、たとえば、パスワードをメモに書いておき、ディスプレイや壁に張っておくといった行為を行っている場合、パスワード認証における安全性の前提が大きく崩れてしまいます。

間違えた理解

パスワード認証の間違えた理解として、「パスワード入力は利用しようとするシステム機能を起動するためのスイッチのようなものだ」というものがあります。

システム外部から眺めた場合、システムは、最初に利用者の認証を行う必要があるわけですから、“認証を行うこと＝システム機能の起動”のように見えるかもしれません。しかし、「パスワードを使うのは認証のためである」という本質的な理解を最初に持たない限り、パスワードおよびパスワード認証の機能を正しく使用しない、あるいは、誤った利用方法をとっているためセキュリティーホールが発生してしまうといった危険性があります。

パスワードのメカニズム

パスワード認証のメカニズムの枠組みは、先ほど説明したとおり、いたって簡単です。まず、正当なユーザーしか知らない文字列を与え、その文字列がすでにシステムに登録してあるパスワードと比較するだけです。「比較する」いう表現を使っているので、そのままのパスワードと比べるように聞こえますが、通常の安全性の高いシステムは、パスワードそのものを保管しているわけではありません。暗号技術の一種である一方向性ハッシュ関数という関数を用いて、オリジナルのパスワードを変換したものを保管します。

パスワードを認証する際は、毎回、システムが一方向性ハッシュ関数の処理を行い、その値を、システムに保管しているパスワード（変換済み）と比較して判断します。

一方向性ハッシュ関数とは何か？

よく「パスワードは暗号化して保持されている」と説明される場合があります。必ずしも間違いとは言えませんが、この説明は正確ではありません。暗号を定義するとすれば、元のデータを鍵により暗号化でき、また暗号化されたデータを鍵を用いることによって復号化できるというメカニズムであるものです。ところが一方向性ハッシュ関数を用いた変換済みのパスワードは、元のパスワードに逆変換できないのです。

一方向性ハッシュ関数（One Way Hash Function）とは、ある値を入力した時、別の値に変換する関数で、次のような特徴があります。

❶長いデータが入力されても特定データ長に変換される。
❷ 入力が違えば、変換された出力も違う。
❸変換された出力から逆変換して入力を探すことはできない。

このような特徴を持つ一方向性ハッシュ関数を用いて、入力されたオリジナルのパスワードを変換します。

現在では一方向性ハッシュ関数としてMD5やSHAといったアルゴリズムが有名ですが、このような一方向性ハッシュ関数と同等な機能を、既存の暗号アルゴリズムを用いて実現しているものもあります。

入力できるパスワードの長さは、システムにより違います。8文字（8バイト長）のものもあれば、20文字（20バイト長）のものもあります。また、実質的に自由な長さの文字を入れられるものもあります。パスワードとして入力された文字列は、一方向性ハッシュ関数で処理され、そのシステム独自の長さの変換済みパスワードとして保存されるのです。

発見困難性と安全性

パスワードの安全性とは何かを考えてみましょう。パスワードの安全性とは、正しいパスワードを見つけ出すのが困難である、つまりパスワードを発見するのにどれだけの時間が必要となるかがポイントとなります。

多くの場合、パスワードのクラッキング（破る行為）は、専用のクラッキングソフトウェアを使用して自動的に行います。テレビや映画でクラッカー（不正アクセス者）がキーボードにパスワードを推理して打ち込むようなシーンが出ますが、あれはあくまでも芝居だと考えてください。現実には、疲れを知らないコンピュータが黙々と処理します。

パスワードを探す方法は、大きく分けて、2つの方法に分類されます。まず、全件探索（ブルートフォース）と呼ばれる、パスワードとして可能なすべての組み合わせを試していく方法です。原理的には、どんなに強いパスワードでも、いつかは見つけることができます。もう1つは、辞書探索（ディクショナリーアタック）と呼ばれる方法です。これは、英語辞書、百科事典、新聞記事といったものや、ネットニュースやウェブページといったものなど、入手可能なあらゆるテキストデータから単語を抽出し、クラッキングに使用する辞書を作成するというものです。いわゆる「弱いパスワード」は、この辞書探索によって極めて短時間で破られてしまいます。

さて、パスワードのクラッキングを行おうとするとき、クラッカーが、パスワードファイル（アカウント名などの重要な情報が含まれている）を入手しているかどうかで、クラッキングの方法が違ってきます。

パスワードファイルを入手していない場合、アタックするシステムの認証要求に対して、推定したパスワードを直接入力してクラックする方法しかありません。これは、UNIXのログインを繰り返す、あるいはパソコン通信やインターネットプロバイダーに接続を繰り返すといったことにあたります。

パスワードファイルを入手している場合は、高速な計算機上で専用のクラッキングソフトウェアを用いてパスワードを探します。ちなみに処理速度は、60MHzで動作するペンティアムプロセッサーの計算機で1回のパスワードの検証に34ミリセカンド（ミリセカンドは1秒の1000分の1）かかります（筆者注：4.4BSDパスワード生成ルーチンのソースコードのコメントの説明による）。

強いパスワードの安全性

パスワードの認証要求を直接呼び出す場合

を最初に考えてみましょう。ここでは、パスワードの長さは8文字（8バイト長）、認証を1回行うのに1秒かかるとしておきます。この前提で、理想的なパスワードを利用した場合、つまり、完全にランダムな英数字（AからZまでの大文字/小文字、0〜9）からなる入力文字を選んだ場合、どれくらい安全なのでしょうか。ここでは、パスワードとして組み合わせ可能な数の50%を処理する時間を計算します。数式については下にある数式1を参照してください。そうするとこれだけの時間がかかるわけです。

＝109170052792448秒
＝約30325014665時間
＝約1263542278日
＝約3461760年

今度は、システムからパスワードファイルを盗み出し、専用のパスワード検索プログラムを使って、毎秒100万回ほど処理できる場合を考えてみましょう。先に例を挙げたパスワード認証ルーチンの処理能力は、60MHzペンティアムのマシンで毎秒30回弱ですから、ここでの毎秒100万回は、かなり大きな計算機の処理能力を想定しています。

＝約10917006秒
＝約3033時間
＝約127日

注意して欲しいのは、この数字は、パスワードとして可能性のある組み合わせすべての50%を試した時点で正しいパスワードが見つかるという仮定です。実際には、全体の10%を処理した段階で見つかるかもしれませんし、逆に90%処理するまで見つからないかもしれません。あるいは、わずかな確率ではありますが、処理を初めて数秒、あるいは数時間という短い時間で正しいパスワードを見つけてしまう状況も理論上はありえます。

弱いパスワードの安全性

上記のパスワードは、8文字の英数字をランダムに選ぶという条件でした。ところが、多くの人は覚えやすい文字列をパスワードとして使用する傾向があります。もし、なんらかの単語をパスワードに用いてしまった場合、クラッキング辞書を用いて短い時間でパスワードを発見されてしまう危険性があります。その辞書を用いて破られてしまうような弱いパスワードとはどのようなものかを挙げてみます。

❶アカウント名に関連する単語を使う。
❷パスワード（Pass-Word）の名前の由来のとおり、語（Word）を選んでしまう。
❸忘れてしまわないように、単純な組み合わせを付けてしまう。

❶の例で極端なのは、アクセスのためのユーザーアカウントと同じ場合です。パスワードクラッキングのプログラムでは、最初に試すパスワードのパターンです。この場合、処理を開始した次の瞬間にパスワードは破られてしまいます。

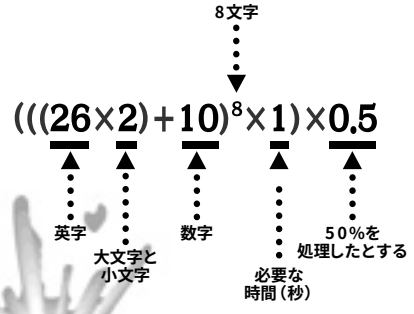
❷の例では、人名であるaliceといった語や、あるいは、triangleといった単語を用いている場合です。辞書に載っている単語や、あるいは一度でも見かけた単語であれば、ほぼ間違いなく短時間で破られます。

実際にクラッキングに使われている辞書の単語数は分かりません。しかし、そのクラッキング辞書の単語数が、数十万となっていても不思議ではありません。また、日本語の単語をローマ字にしても逃げることはできません。なぜなら、日本語の辞書はすでに電子化されて市販されているので、そこから用意してしまえば済むからです。

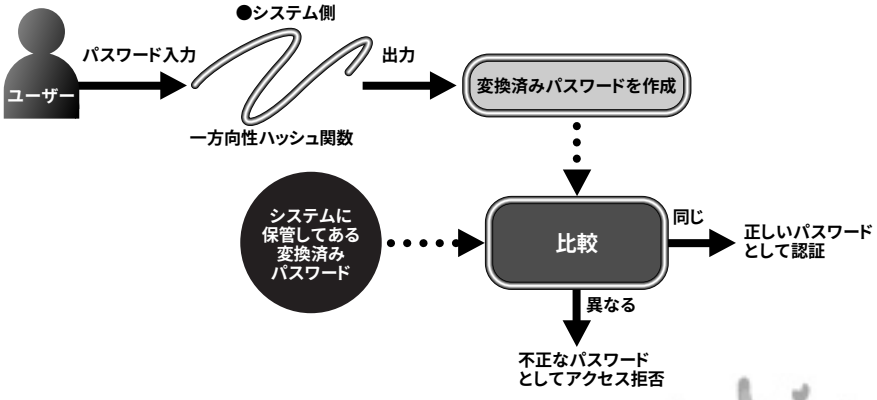
パスワードを探すプログラムを使用した場合、60MHzペンティアムを搭載したパソコンでも毎秒30回程度は処理できます。最新の最高機種のスペックを持ったパソコンを用意すると100回や200回は、処理可能になることでしょう。

たとえば、通常のオンライン英和辞書に載っているような単語をパスワードに使ったと

■数式1



■一方向性ハッシュ関数を使ってパスワードを認証する仕組み



しましょう。オンライン英和辞書に載っている単語を8万語と仮定します。

このオンライン英和辞書に載っているすべての単語をチェックするとしても、だかだか約45分（毎秒30回の場合）で終わってしまいます。

❸の場合は、たとえば、誰かの誕生日とか住所とかIPアドレスやあるいは何かを関連するものです。クラッカーが、侵入される被害者とまったく接触がない場合は一見すると安全なように見えます。なぜなら、被害者に対する個人情報を知り得るチャンスがないように思えるからです。確かに、クラッカーが被害者の個人情報を知らない場合、これは単純な辞書を用いたアタックよりは難しいかも知れません。

ところが、必ずしも安全ではありません。たとえば、コンピュータのファイルシステムにすでに存在している被害者のファイルにアクセスできる場合、そのファイルから得られる文字パターンを使用できます。その昔、コンピュータシステムというのは、数値計算や事務処理といった特定目的のために使われていましたが、今日のコンピュータシステムとは、ノートであり、鉛筆であり、あるいは手紙や書類や、メモを入れてある机の引き出しです。コンピュータを使い込んでいる人であればあるほど、その人の周りで使用する情報のほとんどが詰まっているはずです。

正しいパスワードを選ぶ方法とは

最近のパスワード認証システムは、パスワードを登録する時点で、弱いパスワードは選べない仕組みになっているものが増えてきています。

❶最低6文字以上
❷必ず特殊文字（@や?などの記号）を含むこと
❸辞書にある単語は使わない

などといった条件を、パスワード登録の時点でチェックし、その条件に合わないパスワードは受け付けないような仕様になっているものが、主流になりつつあります。

先のランダムに8文字選ぶという条件に、さらに特殊文字24文字分（いくつかの特殊文字は使えない場合があるので、少なく見積もっています）を加えると、毎秒100万回処理できるとしても、50%の処理が終わるのに約1732日かかるようになります（英数字だけだと約127日だったのを思い出してください）。

また、最近では、長い文を入力として受け付けるパスワードのシステムも出てきました。このようなシステムでは、そのような入力をパスワードと呼ばずパスフレーズと呼ぶようです。なぜなら、「語（ワード）」ではなく、「フレーズ（言い回し）」を入力として与えることができるからです。このようなシステムでは、たとえば、次のようなパスフレーズを与えることができます。

What's different between Elephants and Ants?

さすがにこうなると、単純に辞書ある単語を組み合わせるだけでは、パスフレーズを見つけることができません。また、可能な組み合わせの数も膨大な数になります。

パスワードで注意する点

ここまで説明したことを中心に、個人で管理する際に注意する点を箇条書きにまとめます。

❶弱い（悪い）パスワードは避ける。
❷定期的にパスワードは変更する。
❸過去に一度でも使ったことのあるパスワードは使わない。
❹デフォルトのパスワードはただちに変更する。
❺他人に漏らさない。
❻パスワード入力しているのを他人にのぞかれないようにする。

パスワードの安全性はユーザーの意識にかかっている

1984年、当時AT&Tベル研究所にいたグランプ氏とモリス氏の研究では、8%〜30%のユーザーのパスワードが弱いパスワードだという報告を行っています。しかし、この数字は、アテにはなりません。それは、システムを使っているユーザーのセキュリティー意識がどれだけ徹底しているかという人の問題になるからです。それは限りなく0%に近いかもしれませんし、あるいはほとんどのユーザーが弱いパスワードを使用しているかもしれません。ユーザーの意識という曖昧な要素が大きくからんでくるので、本当の安全性を見積もることができないのです。

ここまで説明してきた古典的なパスワード認証システムでは、徹底してユーザーにパスワード管理の教育を行うことによって、初めて本来のパスワードの安全性を手に入れることができます。最初に述べたとおり、「認証システムのコスト負担が少ない方式」ではありますが、その分、ユーザーの意識や資質にトータルな安全性が左右される根本的な問題を抱えています。

まとめ

ここでは、まず最初にパスワードに対して知っておくべき、ごくごく基本的なことがらに関して述べました。パスワードを使う潜在的な危険性や、さらに安全な認証システムに関しては、別の機会に改めて説明したいと思います。

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp