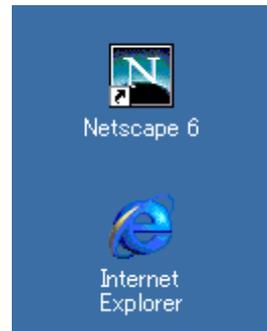


パスワード変更方法

1. Internet Explorer や Netscape Communicator などの Web ブラウザソフトを起動します。



センターシステムの場合は Netscape Communicator 4.7 がインストールされているため、左アイコンとは異なります。

2. 「ファイル」メニューの「開く」に以下の URL を入力し、 をクリックします。
`http://duck.center.kobe-u.ac.jp/password`



`http://duck.center.kobe-u.ac.jp/password`

3. 右の操作画面が表示されたのち、「Login ID」に学籍番号などのユーザー名を入力します。

次に現在使用しているパスワードを「Password」に入力します。

「Authentication Server」では「教育用ユーザー(学生)」か「研究用ユーザー(教職員など)」を選択します。

以後の操作画面を日本語で表示する場合は「Japanese」を、英語の場合は「English」を選択します。

入力・選択し終わったら  をクリックします。



教育用ユーザ: 学生ID用
*** Select ***
教育用ユーザ: 教職員・計算機利用登録者ID用
研究用ユーザ:

4. “3”の操作画面で入力された「Login ID」および「Password」が正しければ、右の操作画面が表示されます。

パスワードを変更するためには**パスワード変更**をクリックします。

パスワードを変更せずに終了するためには**終了**をクリックします。

注) ログインに失敗した場合は右の操作画面が表示されます。**EXIT**をクリックして“3”の操作画面へ戻り、再度「User ID」と「Password」入力しなおして下さい。

注) 以降の操作画面で長時間放置すると「Timeout」のエラーが出ます。**Menu**で“4”の操作画面に戻り、再度入力しなおして下さい。



EXITをクリックして“3”の操作画面へ戻ります。

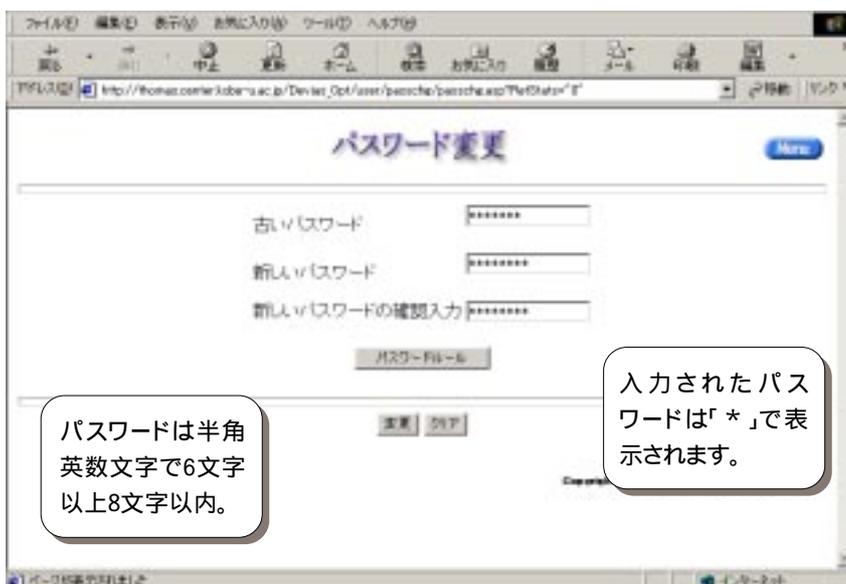


5. 右の画面が表示されたら「古いパスワード」(現在用いているパスワード)と新しく変更したい「新しいパスワード」を入力します。「新しいパスワード」は確認のため2度入力します。

パスワードは6文字以上8文字以内。半角英数文字のみ設定可能です。大文字と小文字も別の文字として認識しますのでご注意ください。

パスワードを変更するためには **変更** をクリックします。

注) 古いパスワードや確認用の新しいパスワードが間違っているとエラーが表示されます。落ち着いて、再度入力して下さい。



注意

パスワードは利用者を特定する唯一の“鍵”です。他人に分かりやすいパスワードは決して用いないでください。クラッカー達がパスワード解析のために使っている辞書には、英単語はもちろんのこと、日本人の名前やアニメキャラクター名まで載っています。覚えやすいから！などと単純なパスワードを使うと、簡単に見破られてしまいます。

悪い例) 名前 電話番号 生年月日
 学籍番号 英単語 動物の名前
 アニメなどのキャラクター名

パスワードの選び方については、次節を参照して下さい。

6. 変更にはしばらく時間がかかります。あわててブラウザを終了しないようにしてください。



7. パスワード変更が無事終了すると右の操作画面が表示されます。

以上でパスワードの変更は終了です。

次に新しいパスワードに変更されているか確認します。



8. **確認** をクリックすると“3”の操作画面に戻ります。

新しいパスワードに変更されているかどうかを確認するためには“3”の操作を行い、“4”の操作画面にログインできるかどうかで判断します。

ログインできるなら“4”の画面で**終了**をクリックして終了します。

Login ID もしくはPasswordが誤りだと右の操作画面が出ます。落ち着いて再入力して下さい。



以上

パスワードの選び方

はじめに

総合情報処理センターの端末、各種サービスを利用するには自分のIDとパスワードが必要になります。

これらは、最初にIDの交付を受けたときの用紙に書かれていますので、そのまま使っている場合もあるでしょう、自分で変更している場合もあるでしょう。しかし、使う時に必要になる面倒なものだと思いませんか？どうでもいいから適当につけたらいいや、とか思っていないですか？こんな風では、到底パスワードの重要性を認識しているとは思えません。

パスワードは非常に重要なものなのです。では、なぜパスワードは重要なのでしょうか？

もし、あなたがクラッカー*だったとしたらどうでしょうか？パスワードを予測して「aaaa, aaaa1, aaaa2と順番に入力していけば何とかなるかもしれない！」と考えるかもしれませんね。一見大変な作業に見えますが、実はそうでもありません。なぜならコンピュータを使えばそれを自動的に行ってくれるからです。最近のパソコンは相当高性能ですから、あなたがコーヒーでも飲んでいる間に解読してしまうかもしれません。もし、1人のユーザーのパスワードでも解読できればしめたものです。そのサーバーに侵入し、別の方法を使ってサーバー自体を乗っ取ることさえも可能になるのです。そうなればそのサーバーから送受信するメールは読み放題、Webページだって改竄し放題になります。おそらくクラッカーであるあなたは、セキュリティ意識の低いサーバーを前にほくそ笑んでいることでしょう。

しかし、この総当たり方法は単純で確実な分、計算に時間がかかります。ですから世の中のクラッカーたちはそんな効率の悪いことはしません。彼らはもっと簡単・素早い方法でパスワードを解読できることを知っているからです。

その効率のよい方法とはどんなものなのでしょうか？セキュリティ専門家の中で「joeアカウント」といわれているものがあります。「joeアカウント」とは、アカウントと同じパスワードをつけているユーザーのことを指します。大規模なサーバーになればそんなユーザーが必ず1人が2人はいるというものです。これならたとえ数万人のアカウントを持つサーバーだとしても、簡単に解読できることでしょう。また、インターネット上には各主要言語の辞書があります。ユーザーがその辞書に載っている言葉をパスワードにしていた場合も同様です。あるいは、もし侵入したいサーバーのある場所に行けるとしたらどうでしょうか？机の中のメモ書きや、キーボードの裏に管理者パスワードが書いてあるかもしれませんね？これらは立派なセキュリティホールです。クラッカーたちはそんなところをねらっているのです。

さて、ここで注目していただきたいことがあります。それはたった一人のパスワードが解読されただけでも、そのサーバーを乗っ取ることが可能になり、他のすべてのユーザーに被害を与える可能性があるということです。もし、あなたのパスワードが解読されたことが原因で、大学、会社やプロバイダーに多大な経済的損失を与えたとすればどうなるでしょうか？莫大な損害賠償請求をされないとも限りません。つまり、あなたのパスワードが極めて重要なものであるということを再認識していただきたいのです。

(A) パスワードの選択

現在の各種の計算機では、パスワードにはアルファベット、数字、特殊記号を含めて8文字使えます。パスワードで使用可能な文字（使用不可のコントロール文字を除く）を用いると、Unix Passwordの場合、43,000,000,000,000,000以上の全く異なるパスワードを作成することが可能です。一方、主要10言語の辞書に載っている語、それを反転させ

* 新聞報道など一般的には侵入者のことを「ハッカー」と呼びますが、本来その言葉はスペシャリストに対する尊敬の言葉として使われるものです。「彼はLinuxのハッカーだ！」という場合は「彼はLinux使いの名手だぜ!!」といった意味になります。コンピューターの世界では侵入、破壊や著作権侵害することを目的にした違法性の高いユーザーを「クラッカー」とし、前者と区別し軽蔑の対象としています。

たもの、その後の最後に数字を1つつけただけのもの、それらに加え、有名人の名前、専門用語などをあわせたとしても5,000,000位しかないと言われてしています。つまり、それらの言葉をパスワード使った場合、総当たりするのに比べて0.0000000012%の努力で解読可能であるということを示しています。

一方(!, ", #, %, \$)などの特殊文字をパスワードに使う人は、全体の1.4%しかいないと調査結果があります。それらを積極的に使うと言うのはどうでしょうか?いくら高速の計算機を使っていたとしても総当たり方式は時間がかかるため、類推しにくいパスワードを付けていれば、解読される危険性もかなり低下します。そこで、

- * 良いパスワード = 類推しにくいパスワード
- * 悪いパスワード = 簡単に分かってしまうパスワード

という関係が成立します。では、良いパスワードとはどんなもので、悪いパスワードとはどんなものなのでしょうか?まず悪いパスワードとはどんなものかを説明しましょう。

(B) 悪いパスワード

悪いパスワードとは次のようなものを指します。

- * ログイン名を変換したもの(逆つづり、大文字化、二重化など) joe アカウント
- * 自分の名前、あるいはそれを変換したもの
- * 自分の両親、子供の名前
- * 自分についての情報:生年月日、ライセンスプレート番号、電話番号、保険証番号、自動車の型番、住所、.....
- * 全部数字、全部同じ文字(11111, aaaaaなど)
- * 英語、日本語、あるいは他の外国語の辞書にある単語
- * 名前などの単語+数字1文字。
- * アイドルタレント、アニメキャラクターなどよく知られた人名
- * 地名や星の名前や動物などの名前
- * 同じ単語の繰り返し
- * キーボードと同じ並び(qwerty, asdfgh など)
- * 8文字より少ないもの

例えば次のようなものです。

- * corona
- * nissan
- * takeshi1
- * wizard

心当たりがありませんか?心当たりのある人は次の良いパスワードとはどんなものかを読んでパスワードを変更して下さい。

(C) 良いパスワード

良いパスワードとは次の様な条件を満たすものです。

- * 8文字であること。

- * 大文字、小文字が混ざっていること。
- * 数字や特殊文字(!"#,% など)が含まれていること。
ただし、特殊文字は計算機のOSによって無かったりする場合もあるので注意して下さい。
- * 簡単には忘れにくく、どこかにメモする必要のないもの。
- * キーボードを見なくてもすばやく打てるもの。

「他人には分かりにくいけど、自分には意味が良く分かるアルファベット2文字以上、数字1文字以上(と特殊文字1文字以上)を含んだ8文字の文字列」が良いパスワードだと言えます。

(D) パスワードの作り方

では、実際にどういう風にパスワードを作れば良いかを説明します。

- * 何か文章を作り、その中から数文字をランダムに抜き出す。
- * 歌や詞の数節を抜き出し、その頭文字をつなげる。
- * 単語の子音1文字と母音1、2文字を入れかえて、へんな単語をつくる。
- * 2つの短い単語を選び、特殊文字でつなげる。

次のようなものです。

- * K06o%nA.
- * niS\$%anN
- * TaKe\$h1i
- * u1ZaA6d0

注:これらはここに載せたのですでに“悪いパスワード”です。

また、例えば、「麦100%ビール」という単語を分解し、

- * 麦 Mugl 6gi
- * 100 1 hundred 1H
- * % %
- * ビール beer br

と変換して繋ぎあわせると「6gi1H%br」というパスワードが出来ます。これであれば、自分には意味が十分に通じるけど、他人には非常に分かりにくくなります。

(C) パスワードの保管場所

いくら良いパスワードを作ったとしても、それをどのように扱えばよいのでしょうか？

理想は記憶することです。作り方に自分なりのルールを持たせたのは、自分には記憶しやすく、他人には記憶しにくいからです。しかし、どうしても覚えられないときはどうすればよいのでしょうか？

まず、悪い例から紹介しましょう。

パスワードを書いたメモ書きをモニターや、キーボードに張ったりしていませんか？賢明な読者のみなさんはキーボードの裏なら大丈夫なんて思わないですよ？もちろん、机の引き出しの中や、予定表の中にしまっておいた！先し
ないですよ？えっ？机の上に置いたままになっているシステム手帳の中に書いてある？こんなところにパスワードを

保管しておくなら、いっそ忘れた方が被害が少ないかもしれません。当然、テキストファイルにしてサーバーの中に保存してあるというのも悪い例です。もし、今現在そうしている人がいたら、すぐに違う方法に改めましょう。

では、どんなところに保管するのが良いのでしょうか？

専門書には、財布の中にしまっておくのがいいと書いてあるものがあります。なぜなら、財布を狙う犯罪者と、計算機を狙う犯罪者は目的が違うからであると言うものです。もっともな話です。しかし、少し注意が必要です。もし、そうする場合でも次の点に注意してください。

- * サーバー名、ユーザー名などとパスワードを一緒に記録しない。
- * パスワードも平文(そのままの文字)ではなく、暗号化する。

つまり、サーバー名やユーザー名が分からなければ、いくらパスワードが分かったとしても、それは意味のない文字の羅列になるからです。また、もし分かったとしても、何文字か入れ替えたり、抜いておいたりと言ったように暗号化してやれば簡単に解読されることは防げます。

おわりに

どんなパスワードが良いパスワードか、またどうやって作ればいいのかご理解いただけたでしょうか？

ただ、いくら良いパスワードを作っても長期に渡って同じパスワードを使い続ける事は、危険な事です。少なくとも1ヵ月1回は違うパスワードに変更してください。また、他人に教えるのはとんでも無いことです。絶対に止めましょう!

参考文献

UNIX & インターネットセキュリティー

Simson garfinkel, Gene Spafford著, 山口 英, 谷口 功 訳 オライリー・ジャパン 1998