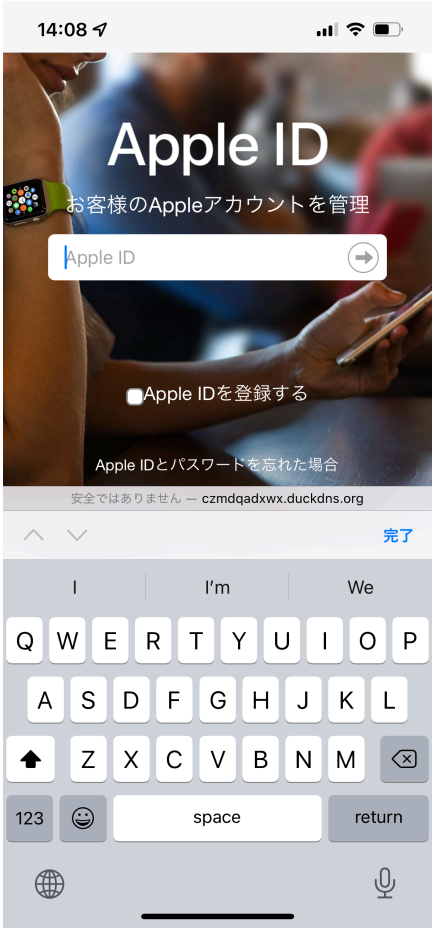
Phishing にご注意を!!

青い鳥こどもクリニック
引田　満

Phishing（フィッシング）とは総務省の web サイトによれば下記のように説明されています。

> フィッシング詐欺とは、送信者を詐称した電子メールを送りつけたり、偽の電子メールから偽のホームページに接続させたりするなどの方法で、クレジットカード番号、アカウント情報（ユーザ ID、パスワードなど）といった重要な個人情報を盗み出す行為のことを言います。なお、フィッシングは phishing という綴りで、魚釣り（fishing）と洗練（sophisticated）から作られた造語であると言われています。



＼やってしまった／

お恥ずかしい話ですが、数ヶ月前にこの Phishinng の被害に合ってしまいました。事の経緯ですが、都内に外出していて、目的の店舗の場所を調べるためにスマホのブラウザ（apple の safari）を開こうとしたところ、左のようなサイトが立ち上がってきました。普段はこんなことはないのですが、約束の時間が迫っており、少しあわてていたため、今思えばひどく不用意に apple の ID とパスワードを入力してしまいました。その後、ブラウザは立ち上がり、用事も済んでほっとしていたのですが、その 30 分後でしょうか、「あなたの apple ID がデバイスのサインインに使用されました」「パスワードが変更されました」「認証用の電話番号が変更されました」との着信がが立て続けにあり、全く身に覚えのないことなので、愕然としましたが後の祭りです。ID（メールアドレス）、パスワード、認証用電話番号を悪意のある第三者に盗まれ、すべて書き換えられてしまったことに気づきました。iPhone を使っているのですが、その直後から apple の提供するすべてのサービスは自分のパスワードを入れてもすべて拒絶され、使用できなくなりました。キャリア通話 (au) は apple と無関係なので使用可能であったのはせめてもの救いでした。

＼さらに困ったことに …／

実は普段常用しているパソコン (mac book) も iPhone と同期（連携）させるために同じ ID とパスワードを使用していたので、クラウド（オンラインストレージ）上の重要なファイルにアクセスできないばかりか、メールも使えず、新型コロナ関連のファイルや情報に接することができなくなり、仕事にも重大な支障が出て、本当に困り果ててしまいました。

＼ 検証してみる ／

帰る道すがら、なぜ？どうして？と自問するうちに気がついたのは、あの HER-SYS（ああ面倒…）でもおなじみの 2 ファクター認証（2段階認証）が機能しなかったことです。自分でも記憶が定かでないのですが、おそらく off にしていたのではないかと思われます。on になっていれば相手が私のアカウントでログインする時に iPhone にパスコードが SMS で通知されるので、それを盗まない限りはログインできない仕組みです。まさに痛恨の極みです。もし2ファクター認証をパスコードなしで技術的に突破していたとすれば恐るべき相手です。

全頁に掲載したのは履歴に残っていた詐欺サイトの画面ですが、そこそこ良くできており、apple の広告の雰囲気に似せているので、その時は特に違和感を覚えず、これにやられてしまいました。不用心な自分にうんざりですが、後から検証すると、当然ながらおかしな点が見つかります。①毎日頻回に開いているブラウザから突然 ID とパスワードをセットで要求されることはそもそもないこと、② URL の表示をよくみると「安全ではありません」との表示があり、セキュリティ保証の目安となる鍵マークもなく、送受信が暗号化されていないことは明白であり、公式の apple のサイトではあり得ないこと、③ドメインが「duckdns org」で終わっており、これも調べてみると誰もが自宅でサーバを構築し、web 上で公開できるシステムで一般的に使われていることがわかり、全てが詐欺サイトというわけではありませんが、悪用される可能性のあるドメインでした。このような不自然な画面が出現した際は、決して入力はせず、すぐに終了することが必要なのです。サイトが要求しているわけではなので、繰り返し情報入力を求められることないでしょう。このような詐欺画面を仕込む仕組みは私にはわかりませんが、その行為自体を抑止する手立てはおそらくないので、現状ではとにかく気をつけるしかありません。実はこの後にも au のサイトを開く際に、同じような画面が出てきたことがありましたので、狙われているような気もして不安な日々でした。

＼ さて、どうする？　苦行のごとく … ／

とにかく金銭的な被害に発展しないようにしなければなりません。各種サブスクリプションや通販の支払いにクレジットカードを使っていたため、早急にクレジットカード会社に連絡し、カードの停止と再発行の手続きを取りました。良くないとわかりつつもパスワードの使い回しをしていましたし、パスワードを記憶するアプリケーション（apple ではキーチェーン）を見られてしまった場合、なりすましで amazon 等の通販サイトにログインされ、大きな買い物をされてしまう可能性があります。クレジットカード番号は下４桁までしか見えないはずですし、３桁のセキュリティーコードはわからないので安全はずなのですが、やはり不安はつきまとうものです。新しいクレジットカードが届くまでは概ね 10 日から２週間程度かかるので、月額サブスクリプションの支払いは滞る可能性がありますが仕方ありません。また、カードを停止するのは電話一本でできますが、各種の支払い継続のために新しいカード番号をひとつひとつ登録し直すのには大変な手間がかかりました。

さらにもう一つ大きな問題があり、私のコントロール下にないデバイス（iPhone と mac

book）自体をどうするかということです。相手は自由に私個人のクラウド上ファイルにアクセスでき、閲覧、改変、削除、流出と、その気になればやりたい放題です。いろいろ調べた結果、奪われた ID を取り戻すことはシステム上、不可能とわかり、できることは相手が書き換えた apple ID と私のデバイスの紐づきを解除するよう、apple に申請することでした。ハードとソフトを同一会社が製造し、同一 ID で一括管理している apple にその権限があり、これは強みといえるかもしれません。マイクロソフト（windows）であれば Surface シリーズが似たような仕組みですね。富士通、SONY、NEC など場合はこうした権限がどこにあるのか難しいところです。この措置を行うとクラウド上のファイルがすべて消去されることになると説明され、大打撃ですがやむを得ません。そのためには各デバイスごとに所有者が私であることを客観的に証明することが必須で、購入証明ができるもの（シリアルナンバー、レシート、保証書、メールなど）をすべてを提出するように指示されました。また、その審査に 1 ～ 2 週間を要すると言われましたが、色々やり取りしているうちに、購入証明にこれほど慎重になるのはのは apple サイドからすれば、私が本当に Phising の被害者なのか、それとも盗品を我が物にしようとする悪意なのかを見極めるためだと想像できました。審査過程は完全にブラックボックスですが幸い、申請が通り、すべての設定が初期化され、新たな ID とパスワードを設定し直して使える様になりましたが、完全に復旧するまで約 1 ヶ月を要しました。

＼ 戦いすんで日が暮れて ／

以上が今回の顛末ですが、同じような経験のある方はいませんでしょうか？ Phishing 詐欺は巧妙かつ高度になる一方で、すぐには見分けがつかない場合も増えてくるでしょう。セキュリティとのイタチごっこが今後も続くと思われます。防止対策のひとつとして、2 ファクター認証が一般的になり、完璧ではないにせよ、現状では有効な手段といえるので可能であれば是非設定しておくことをお勧めします。私は不覚を取りましたが…。また、基本的なことですが、パスワードの使い回しは避けるべきだと改めて実感しました。「増え続けるパスワード問題」が背景にあるわけですが、パスワードを保存するだけではなく、ランダムに生成してくれる機能が標準装備されたパソコンも普及してますし、パスワード管理アプリとして購入することもできますので利用するのも一法です。パスワードのみを求められることは日常的にありますが、ID とセットの場合は、一旦立ち止まって「冷静かつ慎重に」画面を見て判断することが大切です。

自分の認識不足を痛感した出来事でした。これまでの記述に誤認があるようでしたら是非、ご教示頂けれると助かります。ご意見等も医師会宛でも結構ですので、お寄せいただければ幸いです。

追伸

この稿は８月中旬に書いています。KDDI が７月２日に大規模通信障害を起こしたのは記憶に新しいところですが、au ユーザの私も宅配業者にキャリア通話ができず、不便な思いをしました。補償としてすべての利用者（3,589 万人）から通信料 200 円、約款に抵触する 271 万人から基本使用料２日分の割り引きが決定し、８月１６日から順次返金の案内を SMS やメールで送付するそうです。これを利用し、返金に必須な手続きを装った詐欺サイトを仕込んで au の ID、パスワード、暗証番号を盗むフィッシング被害が出ないか、規模が大きいだけに心配なところです。まさに詐欺の手口ですね。

※ au はパスワードと暗証番号を区別しています。