SE Report

サイバーセキュリティ

プロックスシステムデザイン株式会社
執行役員
川口　賢 *Ken Kawaguchi*

1. はじめに

近年、日本企業や政府機関等への大規模なサイバー攻撃が激しくなり、その攻撃手法も一段と高度になっています。また、国益を保護するため各国のサイバー戦争が激化していく中、日本人のインターネットセキュリティに関する意識は大変低いのが現状です。

セキュリティ意識向上のためには対策の必要性を知り、的確な対策の実践が重要です。

ここでは一般消費者がインターネットを利用するうえでのリスクを再認識し、被害を最小限におさえる対策の一部を紹介します。

2. パスワードクラックについて

従来、個人をターゲットにした攻撃は単なる嫌がらせやイタズラ目的が多かったが、近年では不正取得した個人情報の売買を目的とした攻撃が大変増えています。不正アクセスの手段は多種多様ですが、最も多いのがパスワードクラックです。これはサーバを利用するユーザ名とパスワード情報を不正入手する手法です。一般的なアプローチは、類推攻撃、辞書攻撃、総当たり攻撃の3つです(**表1**)。

「類推攻撃」は、 他人が類推しやすいパスワードを一つ一つ試してみる攻撃です。ユーザ名とパスワードが同じ文字列の場合や、1234などの簡単に予測できる文字列を設定している場合は、比較的短時間でパスワードが破られてしまいます。

「辞書攻撃」は、辞書に掲載されている単語を入力する手法です。Tokyo、dog、catなどの文字列はもちろん、tokyoのスペルを逆さにしたoykotや、キーボードのキー配列の並び順を利用したqwerty なども危険です。また、dog1のようにdogという一般的な名称に1を加える文字列も大変多く存在します。ある有名なソーシャルサイトでは、2/3のユーザが一般的な名称の末尾に"1"を加えていたという調査結果が発表されています。

「総当たり攻撃」は、考え得るすべてのパスワードを試す攻撃手法です。気の遠くなるような話ですが、インターネット上には、総当たり攻撃用のクラッキングツールが存在し、子供でも簡単に「総当たり攻撃」が自動で行えます。クラッカーは様々な手法を用いて攻撃をしかけサーバの侵入に成功すると、次の目的はroot権限の奪取です。

表1　パスワードクラックの主な攻撃手法

類推攻撃	類推されるパスワードでアクセス 例1)　ユーザ名:kawaguchi　パスワード:kawaguchi 例2)　電話番号,誕生日,地番,1234
辞書攻撃	辞書にある単語でアクセス 例1)　tokyo,dog,bridge,windows,baseball 例2)　oykot,dog1,abc123,password,qwerty
総当たり攻撃	考え得る「すべて」のパスワードでアクセス

図1　root奪取による社会的立場の変化

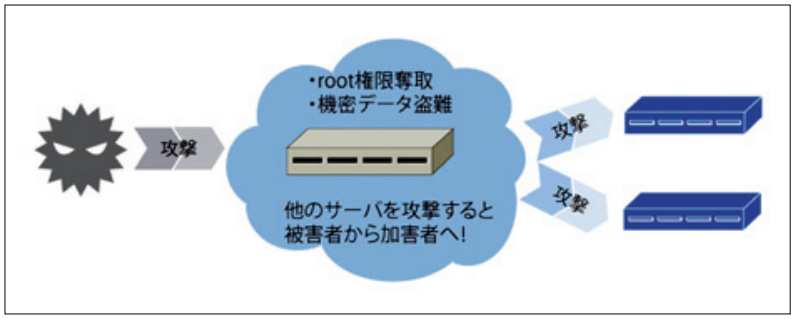
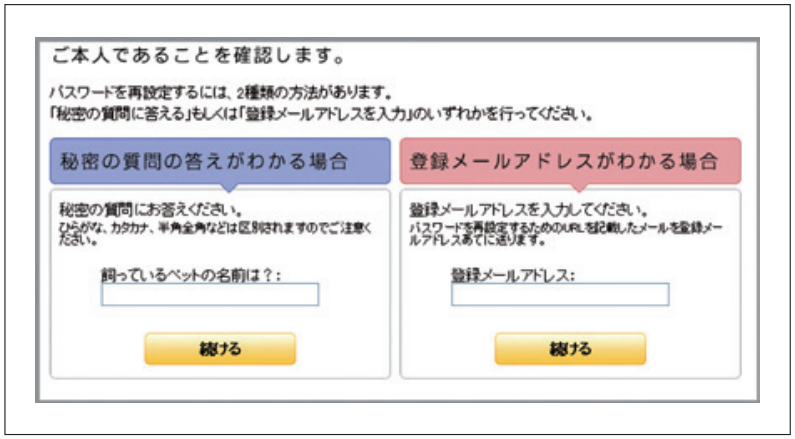


図2　「秘密の質問」の具体例



root権限とはスーパーユーザ特権をあらわし、それを手に入れることでサーバに保存してあるすべてのファイルにアクセスができて各種設定も自由に行えます。専用のハッキングツールを利用すると誰でも簡単にroot権限の奪取が可能で、個人情報を含む機密データの盗難や改ざん、消去という形の被害が発生します。

さらに悪質な場合は、侵入したサーバを踏み台(攻撃拠点)としてほかのサーバを攻撃するなど、重度な犯罪に利用されることも珍しくありません。このようなケースでは、踏み台にされたサーバはクラッキングされた被害者の立場から一転して加害者となり、損害賠償や刑事責任を負うことになるので、不正侵入されないために十分な対策を行うことが必要です(**図1**)。

複雑なパスワードを設定していても油断はできません。実例としてオバマ大統領とサラ・ペイリン氏(元アラスカ州知事・元アメリカ副大統領候補)が遭遇した事件を紹介します。

オバマ氏の場合は、自身が利用するTwitterのパスワード情報が盗まれアカウントが乗っ取られ、サラ・ペイリン氏は利用していたYahooメールが不正アクセスされました。犯人はある方法によりパスワード情報の再設定に成功し、誰でも閲覧できる掲示板にパスワード情報を公開しました。このことによりサラ・ペイリン氏のメールは一般市民にすべてを読まれ、プライベート情報までも公になってしまいました。

なぜパスワード情報が盗まれたのでしょう。多くのインターネットサービスでは、パスワードを忘れてしまった時に備え、自分だけが分かる「秘密の質問」を設定します。この質問に答えることによりパスワードの再設定ができる仕組みになっています(**図2**)。

オバマ氏もペイリン氏も、この「秘密の質問」によりパスワードを再設定されアカウントが乗っ取られてしまいました。「秘密の質問」によく見られるのが「ペットの名前は？」

図3　更新プログラム通知の表示例

「母親の名前は？」「出身地は？」という内容ですが、友人や知人との会話の中でペット自慢をされる方も多いでしょう。母親や出身地のことについて話すこともあるかと思います。このように他人でも知り得る可能性の高い答えを設定した場合、ハッキングされる可能性が確実に高まりますので、質問には必ず架空の名前を設定されることをお薦めします。

パスワード管理を十分に行い、利用するコンピュータのOS（Operating System オペレーティング システム）やソフトウェアが常に最新でセキュリティホール※1のない状態であれば、外部から侵入されるリスクを大幅に軽減できます。

（1）簡単に想像できるパスワードを設定しない。

パスワードは、最低8文字以上の英数字を組み合わせて設定します。なお、パスワードを書いたメモを忘れないようにモニタや机に貼っている人を見かけますが危険な行為です。クラッキングはインターネット経由だけではなく、身近な現実社会から行うソーシャルクラッキングという手法も一般的です。パスワードが書かれた紙を盗む、入力中のキーを盗み見るなどして、 不正アクセスする場合があるので、パスワードの管理は紙で行わず、入力する際は人に見られぬよう細心の注意が必要です。

（2）OSやソフトウェアを最新の状態に保つ。

OSに不具合が発見されると、OS提供元より更新プログラムが公開されます。Windowsでは「Windows update」と呼んでいます（**図3**）。また、各ソフトウェアの更新プログラムについては「アップデートのインストール準備ができました。」というメッセージがデスクトップに表示されることがあります。このようなメッセージを確認した場合は必ず適用してください。ソフトウェアの不具合を解消し、コンピュータを常に最新の状態にすることで不正侵入されにくいセキュア※2な環境を保ちます。

3. フィッシングについて

インターネットの普及により、お店に行かなければできなかった買い物、チケットの予約や銀行への振り込みなどが、手元のPCからできるようになり大変便利になりました。今やインターネットは生活に密着したツールの一つですが、取引相手の顔が見えないことから様々なリスクも同時に存在します。ここでは大別して3つのリスクを挙げ、インターネットを安全に利用するためのポイントを紹介します。

ショッピングサイトを利用する際、個人情報やクレジットカードの情報を入力しますが、通常の通信方法の場合、テキストデータの平文のままデータが送られWebサーバに辿り着きます。Webサーバにデータが送られるまでには様々なネットワーク機器を通過しますが、その経路上でデータを盗み取ることが技術的に可能です。データを盗み見る「傍

※1
セキュリティホール
(security hole)
コンピュータソフトウェアの欠陥。

※2
セキュア（secure）
安全性が確保された状態のこと。

図4　通信方法による安全性の違い

図5　フィッシングサイトへ誘導するメールの実例

****銀行ご利用のお客様へ

**銀行のご利用ありがとうございます。
このお知らせは**銀行をご利用のお客様に発送しています。

この度、****銀行のセキュリティ向上に伴いまして、オンライン上でのご本人確認が必要となります。
この手続きを怠りますと今後のオンライン上での操作に支障をきたす恐れがありますので、
一刻も早いお手続きをお願いいたします。

http://**********.co.jp/

お客様のご協力とご理解をお願いいたします。　　****銀行

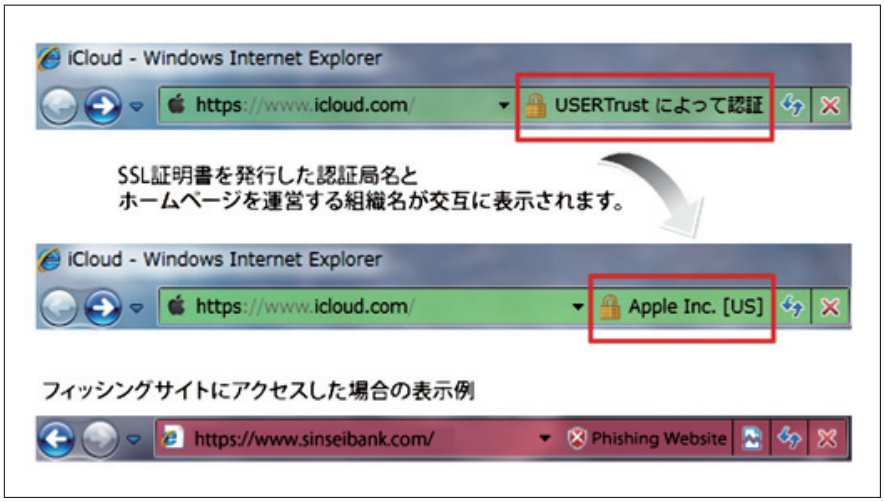
受」、知り得たデータを利用して第三者になりすまし取引を行う「なりすまし」、データの情報内容を書き換える「改ざん」が主なリスクとして挙げられます。これらのリスク回避を目的として一番良く知られているのがSSL※3（Secure Socket Layer）です。SSLは情報を暗号化して送り、Webサーバにデータが到着してから復号することにより大切な個人情報を守っています。もし、経路上でデータを盗まれても複合することが難しいため、オンラインショップやネットバンキングで広く採用されています（**図4**）。

SSLを採用するサイトはWebブラウザのURLと鍵マークで簡単に確認できます。SSL通信を行う場合のURLは通常のhttp://ではなく、https://から始まります。またWebブラウザに鍵マークを表示させることにより、SSL通信であることを分かりやすくしています。オンラインショップに限らず、問い合わせやアンケートフォームなど、大事な個人情報を入力する際は、必ずWebブラウザの鍵マークと、URLバーのhttpsを確認してください。なお、犯罪手法が高度化している現在、SSLを使っていたとしてもそのサイトを全面的には信用できません。

ここで「フィッシング詐欺」について紹介します。情報をつり上げるという意味でこれらのサイトを「フィッシングサイト」と呼びます。犯罪者はあらゆる手段を使ってフィッシングサイトに誘導し、個人情報やパスワード、クレジットカード情報等を入力させて金銭を不法詐取したり、闇マーケットに情報を転売したりします。一般的な誘導方法はメールです。「システムに変更がありました。新たにユーザ登録をお願いします。」「セキュリティの更新が行われたため新たにパスワード情報の入力をお願いします。」という内容を無差別に送りつけ、メール本文に書かれているURLをクリックさせることでフィッシングサイトを閲覧させます。URLは正規サイトの文字列ですがクリックした先のページはフィッシングサイトです（**図5**）。

※3
SSL
(secure sockets layer)
インターネットで、暗号化したデータを送受信するためのプロトコル。
プロトコル：コンピュータ間でデータをやりとりするために定められた手順・規約。

図6　安全と危険を視覚的にアピールするEVSSL



フィッシングサイトでもSSLが利用されるケースがありました。そのサイトのURLは、正規サイトの文字列の一部を変更した非常に紛らわしい文字列で、一見して偽サイトとは分かりません。そこで、フィッシングサイトに有効な新しいタイプのSSLが生み出されました。それが EVSSL（Extended Validation SSL）です。EVSSLではサイト利用者が一目で安全性を確認できる工夫がされています。その一つがブラウザのアドレスバーを緑色に変化させるというものです（**図6**）。例としてアップルの「iCloud※4」にアクセスするとブラウザのアドレスバーが緑色に変化します。そして Webサイトを運営する組織名と、その組織が実在することを確認しSSL証明書を発行した認証局名を交互に表示し安全性をアピールしています。反面、不正なサイトやフィッシングサイトとして報告されている場合はアドレスバーが赤色に変わり危険性を表現します。

EVSSLは金融機関や保険会社、ECサイト（EC：Electronic Commerce　エレクトロニックコマース（電子商取引））など、サイトの信頼性を高め、利用者に安心してWebサービスを安心して提供したい企業のページに使われていますが、一般的なSSLと比較し導入コストが高いためインターネット社会に完全に定着しているとは言えません。その反面、犯罪手法は日々高度になっています。個人情報を入力するさいは十分にサイトを確認し、少しでも不安に感じる要素があれば利用を中止するなど、自衛を心掛けてください。

4. おわりに

私が管理するサーバは個人的な用途でのみ使用しホームページも公開しておりませんが、毎日1000回を超える不正アクセスが確認されます。

マスコミが取り上げるサイバー攻撃は大規模な事件に限られますが、現実には規模を問わずあらゆるデータが標的になっていることが分かります。

インターネットは様々な情報やサービスの利便性を享受する代わりに多くのリスクが伴うことを認識することが重要です。今回紹介したセキュリティ対策は今からでもすぐに実行できることばかりです。インターネットを安全に利用するための参考としていただければ幸いです。

かわぐち●けん
1965年東京都保谷市（現西東京市）に生まれる。ゼネコンにて施工品質および安全管理を主に担当するが、施工性とコスト重視の業界に理念が合わず16年で退社。独学で得た知識を生かし2002年インターネットサーバサービスを基盤事業とするブロックスシステムデザイン(株)に入社。現在に至る。

※4
iCloud
（アイ-クラウド）
米国アップル社が提供するパーソナルクラウドサービス（個人向けサービス）。