やさしいネットワーク・セキュリティ(4)
パスワード・ハッキングへの対策技術

連載 IT技術

村山　純一
MURAYAMA　Junichi
東海大学大学院情報通信学研究科
情報通信学専攻主任教授

ハッカーに狙われるID・パスワード

これまでに，盗聴，詐称，ウイルスへの対策技術について紹介してきた。これらの対策を重ねることで，インターネット・ショッピングを安心・安全に行える。一方で，ハッカーは常にID・パスワードを狙っている。対策の手を抜くと，直ぐに流出してしまう。金銭被害にも直結するので，充分に気を付けたい。

最近では，顧客側ではなく，店舗サーバ側からID・パスワードがまとめて流出する事件も多発している。一度に約30億件のID・パスワードが流出した事件も記憶に新しい[文献1)]。このような事件に接すると，顧客側でのID・パスワード管理など，無力に感じられることも多いだろう。ところが，現実は逆である。このようなご時世だからこそ，各自での適切な管理が重要なのである。

今回は，このからくりも含めて，パスワード・ハッキングへの対策技術について紹介する。

ログイン情報としてのID・パスワード

インターネットを利用したショッピングでは，商品配送のための住所情報や，料金支払いのためのクレジットカード番号が必要となる。頻繁に利用する店舗サーバには，これらの個人情報を保存しておくと便利である。一方で，他人に勝手に利用されないよう，秘匿しておく必要もある。これを実現するのが，ID・パスワードによる店舗サーバへのログインである。

ログインは，図－1に示すようなホームページを利用して行われる。ここでは，ID（顧客識別子）とパスワードの入力が促される。①IDは，顧客を識別するための情報である。連絡手段も兼ねて，メールアドレスの登録を指定されることが多い。②パスワードは，顧客が本人であることを確認するための情報である。顧客は，店舗サーバ毎に，独自の文字列を登録できる。

ログインページに入力したID・パスワードが，店舗サーバに登録しておいた情報と一致すれば，ログインに成功する。ログイン中のみ，自分自身で登録しておいた個人情報を利用できる。一方で，他の顧客の情報を見ることは一切できない。この仕組みにより，クレジットカード番号が安心・安全に利用されている。

図－1　店舗サーバのログインページ

ハッキングされるのはパスワード

メールを利用していると，迷惑メールが届くことも

ある。店舗サーバにIDとして登録しているメールアドレス宛にも，迷惑メールは届く。つまり，メールアドレスは，オープンな情報である。ハッカーは，他人のメールアドレスを知ると，これをIDとした顧客になりすまし，不正なログインを試みる。

この不正から顧客を守っているのが，パスワードである。秘匿された情報であり，家の鍵のような役割を果たしている。ログインページに入力したIDが正しくても，パスワードが間違っていれば，ログインに失敗する。ログインを成功させるためには，何回もパスワードを再入力する必要がある。すなわちパスワードがハッキング対象となる。

ハッカーは，パスワード検査を行う場合，容易に類推可能な文字列から始めることが多い。辞書にあるような英単語が優先的に検査されることから，辞書攻撃とも呼ばれる。このため，パスワードとして，簡単な英単語や数字列などを登録してはいけない。また，電話番号や誕生日も最優先で検査されることから，充分に気を付けたい。

パスワードを簡単に特定できない場合は，総当たりパターンでの，文字列検査が行われる。このようなハッキングは，ブルートフォース攻撃とも呼ばれる。その本質は暗号解読と同様である。すなわち，ハッキングに必要な時間がパスワードの安全性に影響する。

パスワードの安全性を高めるためには，できる限り複雑な文字列を登録するのが良い。特に，アルファベットの大文字，小文字，数字，記号を全て混ぜた，充分に長い文字列が良い。パスワードの具体的な作り方については，情報処理推進機構（IPA）のホームページでも詳しく紹介されている[文献2)]。ぜひ参考にされたい。

店舗サーバから流出するパスワード

多くの店舗サーバでは，ログインの失敗が続くと，ハッキングと見なし，そのIDでのログインを拒絶する。これにより，不正ログインの成功を防いでいる。ハッカーは，立て続けのログイン失敗を回避するため，別の手段でパスワードの不正入手を試みる。顧客を騙すフィッシング詐欺やファーミング詐欺などは，その一例である。しかし，もっと効率的な手法もある。コンピュータの脆弱性などを利用して，店舗サーバに管理者として不正侵入することである。

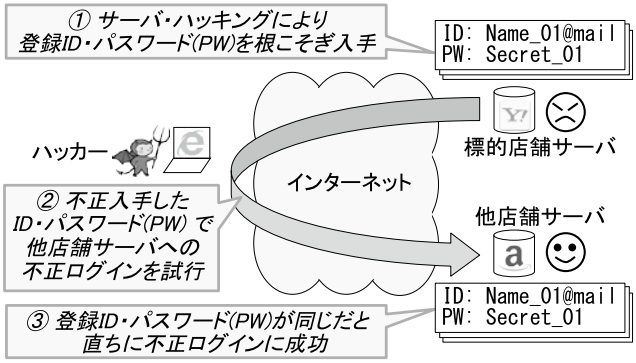
店舗サーバ内のログイン・データベースにアクセスできれば，全顧客のID・パスワードをまるごと持ち出せる。このため，多くのサーバ・ハッキング事件では，莫大な件数のログイン情報が流出しているのである。

「リスト攻撃」による連鎖的な被害

ログイン情報の流出事件は，直ちにニュース報道される。不思議なことに，金銭被害の多くは，標的の店舗サーバではなく，他の店舗サーバで連鎖的に発生している。実は，多くの顧客のパスワード管理に問題が潜んでいる。

顧客の多くは，どの店舗サーバでも，IDとして同じメールアドレスを登録している。さらに，利便性の観点から，パスワードとして同じ文字列を登録していることも多い。図－2に示す通り，このことが問題となる。①ハッカーは，店舗サーバへの侵入に成功すると，メールアドレス（ID）とパスワードを根こそぎ入手する。②また，これらを用いて，他店舗サーバへの不正ログインを試行する。③他店舗サーバでも同じメールアドレス（ID）とパスワードが登録されていると，直ちに不正ログインに成功してしまう。

このような攻撃は，リスト攻撃と呼ばれている。他店舗サーバへの不正ログインに成功したハッカーは，次々と別の店舗サーバへの不正ログインを試みる。これらも成功してしまう確率は高い。結果として，多くの店舗サーバが，芋づる式に不正ログインされる。この不正ログインは，情報流出した顧客数とインターネット上の店舗サーバ数との掛け算で広がっていく恐れがある。



図－2　リスト攻撃による芋づる式の情報流出

顧客による「リスト攻撃」への対策

店舗サーバからのID・パスワード流出を，顧客の努力で防止することはできない。個人でのID・パスワード管理を無力に感じさせる原因でもある。しかし，実際は，個人での対策が大変重要である。基本は，店舗サーバ毎にパスワードを変えておくことである。パスワードを1文字変えておくだけでも，図－2で説明した芋づる式の不正ログインを失敗させることができる。この結果，ハッカーには，新たにパスワード・ハッキングの作業を強いることになる。不正ログインが成功するまでの時間を延ばせるのである。

ID・パスワードを流出させた店舗サーバ側でも，事後対策は行っている。流出を検知すると，そのIDでのログインを拒絶するのである。これにより，クレジットカードの悪用が阻止される。一方，リスト攻撃される店舗サーバ側では，正規のID・パスワードでログインされると，不正アクセスを見抜けない。ID・パスワードを変えておかないと，対策が難しいのである。

パスワードの更新

リスト攻撃に失敗したハッカーは，顧客毎にパスワード・ハッキングを行うことになる。繰り返しの検査に対しては，該当IDのログイン拒絶で対策できる。しかし，これを擦り抜ける総当たり検査の手段も考えられている。一人の顧客を集中的にハッキングするのではなく，次から次へと店舗サーバや顧客を変えて分散的にハッキングしていくのである。

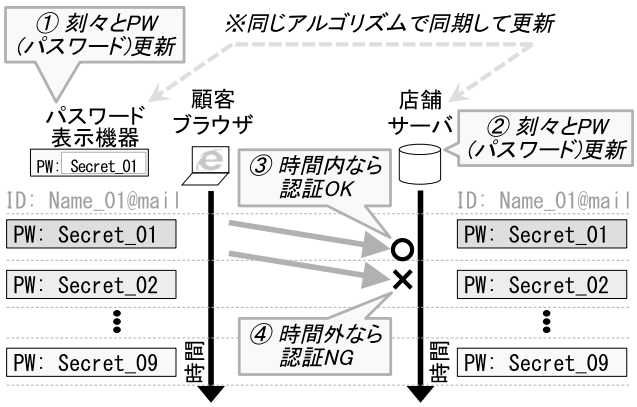
顧客一人あたりへのハッキング頻度が激減すると，ログインの失敗時に，ハッキングか入力ミスかを見分け難くなる。この結果，長い時間をかけてゆっくりとハッキングされ続けることになる。このようなハッキングはパスワードスプレー攻撃とも呼ばれている。

この攻撃への対策として，パスワードの定期的な更新が有効である。この更新は，実質的に，総当たり検査を初めからやり直しさせる効果がある。このような考えで，パスワードの更新を半年毎に促す店舗サーバもある。しかし，これも万能ではない。更新時には，新旧のパスワード情報がインターネット上を流れる。これらが盗聴・解読されるリスクも高いのである。

パスワードの自動更新

究極のパスワード更新は，パスワードを短い時間で次々と変えていくことである。この際，新旧のパスワード情報をインターネット上に流さないことが望ましい。ただし，このような更新を人手で行うことは難しい。そこで，ワンタイムパスワードという自動更新技術が考案されている。

ワンタイムパスワードの仕組みは図－3の通りである。顧客には，予めパスワード表示機器が渡される。この機器は，歩数計に似た小さなハードウェアである。あるいは，スマートフォンのソフトウェアの場合もある。①この機器が表示するパスワードは，短い時間で刻々と更新される。②店舗サーバ側でも，同じアルゴリズムで受付パスワードを刻々と更新する。③一定時間内であれば，パスワード表示機器が表示したパスワードでログインに成功する。④しかし，一定時間が経過すると，このパスワードではログインに失敗してしまう。



図－3　ワンタイムパスワードの仕組み

ワンタイムパスワードでは，顧客側と店舗サーバ側で，時刻を同期させてパスワードを更新する。このため，パスワード更新時に新旧のパスワードがインターネット上を流れることはない。ただし，ワンタイムパスワードも万能ではない。パスワード表示機器の表示を盗み見られたり，機器自体が盗まれたりすると，不正ログインを許す原因となる。充分に気を付けたい。

パスワードとしての生体情報

パスワードとして，文字列情報の代わりに，指紋や

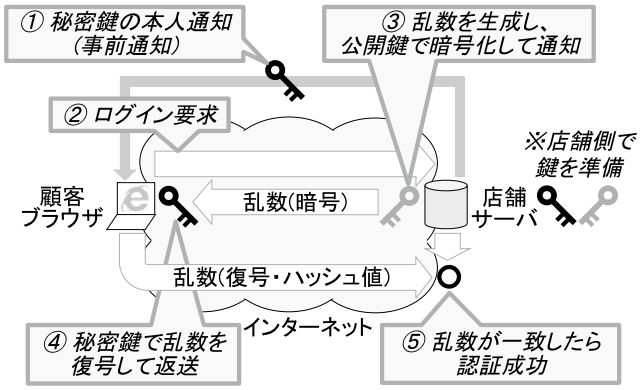
顔形状などの生体情報を利用する技術もある。スマートフォンなどで，よく使われている。利用者がログインする際に，パスワード入力の手間を省くことができ，大変便利な技術である。また，短い文字列情報に比べれば，生体情報は複雑であり安全性も高い。しかし，不正ログインを完全に防げるものでもない。

生体情報は経年変化するため，あまり厳密に照合すると，本人ですら直ぐに認証されなくなる。このため，多少緩く照合する必要がある。このことが偽装を許す原因となる。偽のスマートフォンなどで指紋や顔形状をスキャンできれば，3Dプリンタを利用して，認証可能な模型を製作できるという報告もある[文献3)]。生体認証も万能とは言えない。

パスワードとしての公開鍵・秘密鍵暗号

パスワードとして，公開鍵・秘密鍵暗号を応用する技術もある。一般的な文字列のパスワードに比べて，解読時間の長期化が期待できる。この仕組みは，図－4の通りである。①店舗サーバは，予め顧客本人へ秘密鍵を渡しておく。この秘密鍵は，盗聴されずに，確実に本人に渡される必要がある。②顧客が，必要に応じて，店舗サーバにログイン要求を行う。③店舗サーバは，要求毎に乱数を生成する。また，これを公開鍵で暗号化して顧客へ送る。④顧客は，秘密鍵で乱数を復号し，これを店舗サーバへ返送する。一般的には，返送時の乱数はハッシュ演算で圧縮される。⑤店舗サーバが，乱数あるいはそのハッシュ演算値を比較して一致すれば，顧客の本人確認に成功したことになる。これは，乱数の復号に必要な秘密鍵を，顧客本人のみが保有しているためである。

この仕組みはマイナンバーカードで利用されている。このカードには電子証明書を登録できる[文献4)]。証明書には秘密鍵が含まれる。証明書を登録したカードを利用すれば，インターネット上で行政手続きが行える。確定申告などで利用している方も多いことだろう。ただし，事前のマイナンバーカードの受け取りは大変面倒である。役所で必ず本人確認した上で，手渡しされる。これは，秘密鍵の流出を防ぐ意味もある。



図－4　秘密鍵・公開鍵による顧客認証

パスワードは個人での管理が重要！

現実には，文字列のパスワードを利用する店舗サーバが多い。少なくとも店舗サーバ毎にパスワードは変えるべきである。多くの複雑なパスワードを記憶するのは大変なので，メモなども活用したい。この際，メモが人目に触れないよう充分にご注意戴きたい。パスワード管理ツールなどもあるので，自信のない方は，利用を検討すると良いだろう。

また，混雑した電車の中で，スマートフォンにパスワードを入力するような行為も控えたい。背後から覗かれている可能性も高い。大切な情報は，ちょっとしたことで流出するのである。

「やさしいネットワーク・セキュリティ」は，今回が最終回である。これまで紹介してきた簡単な対策を重ねるだけでも，大きな効果が期待できる。ぜひとも実践して，インターネットに支えられた便利な生活を，安心・安全なものにして戴きたい。

【参考文献】

1）米ヤフーの情報流出，全30億アカウント被害，
https://www.nikkei.com/article/DGXMZO21867310U7A001C1EAF000/
2）パスワードの管理と注意，
https://www.ipa.go.jp/security/fy14/contents/soho/html/chap1/pass.html
3）iPhone Xの顔認証「Face ID」のハッキング競争は続く，
https://wired.jp/2017/11/19/hackers-broke-face-id/
4）公的個人認証サービスによる電子証明書，
http://www.soumu.go.jp/kojinbango_card/kojinninshou-02.html