リスト型アカウントハッキングによる
不正ログインへの対応方策について

（サイト管理者などインターネットサービス提供事業者向け対策集）

平成 25 年 12 月

総務省

目次

１．はじめに

昨今、国内大手ポータルサイトや会員制Webサイトに対する不正アクセス事案が多発しています。事案の多くは、何らかの手段により他者のID・パスワードを入手した第三者が、これらのID・パスワードをリストのように用いて様々なサイトにログインを試みる、いわゆる「リスト型アカウントハッキング攻撃（リスト型攻撃）」によるものとみられています。

リスト型攻撃によるものとみられる不正アクセスが増加している背景には、インターネットバンキングやフリーメールサービス、動画投稿サイト、ソーシャル・ネットワーキング・サービス（SNS）などのインターネットを用いたサービスが拡大し、多くの人がサービス利用に当たって自らのアカウントを所有するようになり、ID・パスワードによりアカウントにログインすれば、Web サイトから、氏名・住所などの個人情報やクレジットカードなどの信用情報など多様な情報が得られるようになったことがあると考えられます。トレンドマイクロ社の調査[1]によれば、ID・パスワードによるログインが必要となる Web サイトの利用について、一人あたり約 14 の Web サイトを利用しているとのことであり、利用者のうち約7割が 3 種類以下のパスワードを複数の Web サイトで使い回しをしているということです。リスト型攻撃は、このような現状を悪用したサイバー攻撃であると言えます。

このようなリスト型攻撃から個人情報や信用情報などを守るためには、利用者において、自身のID・パスワードの管理に際して対策を実施していただく必要があることは言うまでもありません。しかし、リスト型攻撃による不正アクセスの発生やそれに伴う個人情報の漏洩は、企業のコンプライアンス上問題となり、企業の信用を損ねる恐れがある他、内部調査及び復旧のためにサービスを停止する事態になれば、多くの機会損失が発生することになるなど、サービスを提供する事業者自身の問題とも言えます。このため、サービスを提供する事業者において、ビジネス的観点やインターネット利用の安全・安心を確保する観点から、サービスの運営に際して適切な対策を実施していただくことが重要です。

本対策集では、今後のリスト型攻撃による被害の拡大を防ぐため、ID・パスワードを利用者に振り出してサービスを提供する事業者、特に利用者がID・パスワードを

[1] Web サイトのパスワード利用実態調査（トレンドマイクロ社、2012 年 12 月 14 日プレスリリース）
（http://jp.trendmicro.com/jp/about/news/pr/article/20121213002352.html）

自ら設定する形態をとっている事業者において、実施していただくことが好ましい対応方策について整理しました。事業者の皆様におかれましては、これを参考にしていただき、名前や住所などの個人情報やクレジットカード情報などの信用情報に至るまで、管理されている情報資産の価値に応じた、適切なレベルの対策を選択していただければ幸いです。

２．これまでのリスト型攻撃による被害の特徴

企業のニュースリリースなどの公表資料から、最近発生した主なリスト型攻撃事案を分析すると、攻撃について以下の特徴を挙げることができます。

- ○ ある程度の期間にわたって攻撃が行われているものがあり、攻撃が検知されるまでに時間を要するものがあること
- ○ 数万単位での不正ログインが検出されていること
- ○ 利用者からのログインができないといった通報、大量のアクセスエラーの発生、特定のIPアドレスからの不正なログインの検知、社内の調査によって攻撃が検知されていること
- ○ 氏名、性別、生年月日、住所などの個人情報が閲覧されている可能性があること

これらの特徴も参考にして、リスト型攻撃に対して考えられる対応策について以下の章で述べます。

３．攻撃を予防する対策

リスト型攻撃は、リスト化されたＩＤ・パスワードが第三者によって入手され、これらを用いて行われるものです。「１．はじめに」の章でも言及した通り、インターネット利用者の約７割の人が３種類以下のパスワードを複数の Web サイトで使い回しているとの調査結果があり、攻撃者もこのパスワードの使い回しに着目して不正アクセスを行っています。このため、攻撃の予防として、下記の対策を講じることが有効と考えられます。

① ＩＤ・パスワードの使い回しをしないなどの注意喚起を行う
② パスワードを定期的に更新し、リストを陳腐化する
③ ＩＤ・パスワード以外の認証要素を追加する
④ ＩＤ・パスワードの保管を徹底し、リスト化を防ぐ
⑤ 一定期間利用の無いアカウントを廃止し、不正ログイン後の悪用を防ぐ
⑥ 推測が容易なパスワードの設定を受け付けない

本章では、上記の点から具体的な対応方策について記載します。

（１）ID・パスワードの使い回しなどに関する注意喚起の実施

ID・パスワードの使い回しを悪用するリスト型攻撃に対しては、サービス毎に異なるパスワードを設定することが本質的な対策となります。このため、利用者の登録時やパスワードの変更時などあらゆる機会を活用して、ID・パスワードの使い回しから想定される被害も紹介しつつ、使い回しの注意喚起やパスワードの強度（最低文字数や記号の使用など複雑性の程度）の紹介などを行うことが効果的と考えられます。このような注意喚起は、事業者によるコスト負担があまり生じず、一定の効果が得られると考えられます。

また、多少のコスト負担は生じますが、ID・パスワードの両方の使い回しが攻撃の主要因であることを踏まえれば、事業者においてIDを設定し、利用者ではパスワードのみを設定するような形態にすれば、リスト型攻撃による被害を大きく減らすことが可能になります。なお、その際においても、メールアドレスは攻撃者がID・パスワードのリストとともに把握していることが多いことから、IDにメールアドレスは利用しないことを推奨します。

参考1　パスワード管理の便利なツール（パスワードマネージャソフト）

利用者にとってサービス毎に異なるパスワードを設定するのは大きな負担となるのも現実です。そこで、その負担を減らすためのツールとして「パスワードマネージャ（パスワード管理）ソフト」を紹介します。具体的には、利用しているサービスのID・パスワードとマスターとなるパスワードをソフトに登録することで、マスターとなるパスワードのみで複数のサービスの認証が行われるようになるソフトです。このソフトを使うことにより利用者はマスターのパスワードのみ管理すれば良くなり、パスワード管理の手間が省けます。ソフトの中には無料で公開されているものもありますので、ID・パスワードの使い回しに関する注意喚起と合わせて、このようなソフトについて周知していただくことも一案ではないかと思います。[2]

（２）パスワードの有効期間設定

何らかの方法で作成されたID・パスワードのリストをもとに不正アクセスを行うリスト型攻撃に対しては、定期的にパスワードを変更することでリストを古いものにし、リストを役立たないものにすることが有効です。具体的には、サービスを運営する事業者において、利用者へのアカウントの振り出しに際し、利用者のパスワードに一定の有効期間を設定し、利用者に定期的にパスワードを変更してもらうことが効果的です。

また、不正アクセスによりID・パスワードが窃取された場合、攻撃者が不正に入手したID・パスワードを使ってアカウント上にある情報を窃取するほか、パスワードを変更して正規の利用者がアカウントを使用できないようにするといった実害が発生する場合も考えられます。そのため、パスワードが既に流出している又は近い将来流出する可能性がある場合において、パスワードの定期的な変更を行うことは、攻撃の予防だけでなく、このような被害の拡大防止にも一定の効果があります。

ただし、パスワードの有効期限を短くして利用者に頻繁に変更を求めすぎると、利用者が、他人に推測されやすい簡単なパスワードを設定する傾向に陥りやすく、窃取される危険性を高めることもあるので注意を要します。また、有効期間も一年、半年にするなど、事業者で管理している情報の価値に応じて設定することも一案です。

---

[2] 現実的には、複数のサイトの利用が想定される状況で、このサイトの数だけのＩＤ・パスワードを持つことは難しいという発想から、パスワードマネージャソフトの他にも、最近は認証連携の推奨がされています。認証連携は利便性を維持しつつ、一定の強度が担保できることから、この可能性について検討されているところです。

（３）パスワードの履歴の保存

上記（2）の措置をとっている場合でも、パスワードの変更時期が来た際に、利用者が前回まで使用していたパスワードに戻してしまうなど、更新時期が来るたびに2つのパスワードが使い回しされては、攻撃者が保有するリストが再度有効なものになってしまい、意味がありません。そのため、上記（2）のパスワードの定期的な変更と合わせて、パスワードの更新履歴を保存し、変更時に過去のパスワードと照合して、数世代前に使用したパスワードへの変更を認めないようにすることも考えられます。

なお、数世代前のパスワードの履歴の保存においては、暗号化など適切な管理が必要となります。（下記（5）を参照ください。）暗号化はパスワード全体を1つの塊として行われるため、過去のパスワードとの照合は、一部一致ではなく、全文一致で判定することを推奨します。

（４）二要素認証の導入

インターネット上のサービスの利用にあたっては、利用者が正当な権限のもとに利用していることを確認するために認証を行います。認証の方式については大きく分けて以下の3種類に分けられます。

- 対象者の知識を利用したもの（ID/パスワード、暗証番号、事前に登録した質問事項への回答など）
- 対象者の持ち物を利用したもの（セキュリティトークン[3]、ICカードなど）
- 対象者の身体の特徴を利用したもの（指紋認証、静脈認証など）

一般に、認証はこれらのうちいずれか一つを利用しますが、複数の種類の認証方式を組み合わせることを「多要素認証」（二つの認証方式の組み合わせの場合は「二要素認証」）といいます[4]。攻撃者はID・パスワードの対をもとに攻撃を行うため、新たな認証要素を追加することでリストを無効化することができます。しかし、事前

[3] セキュリティトークンは、権限のある利用者に対して正規のログインを補助するために与えられるデバイスであり、セキュリティトークンを通じて認証に必要な情報が生成されます。トークンには、表示部を持った携帯用機器のハードトークンと PDA（携帯情報端末）や携帯電話にインストールするソフトウェアタイプのソフトトークンがあります。

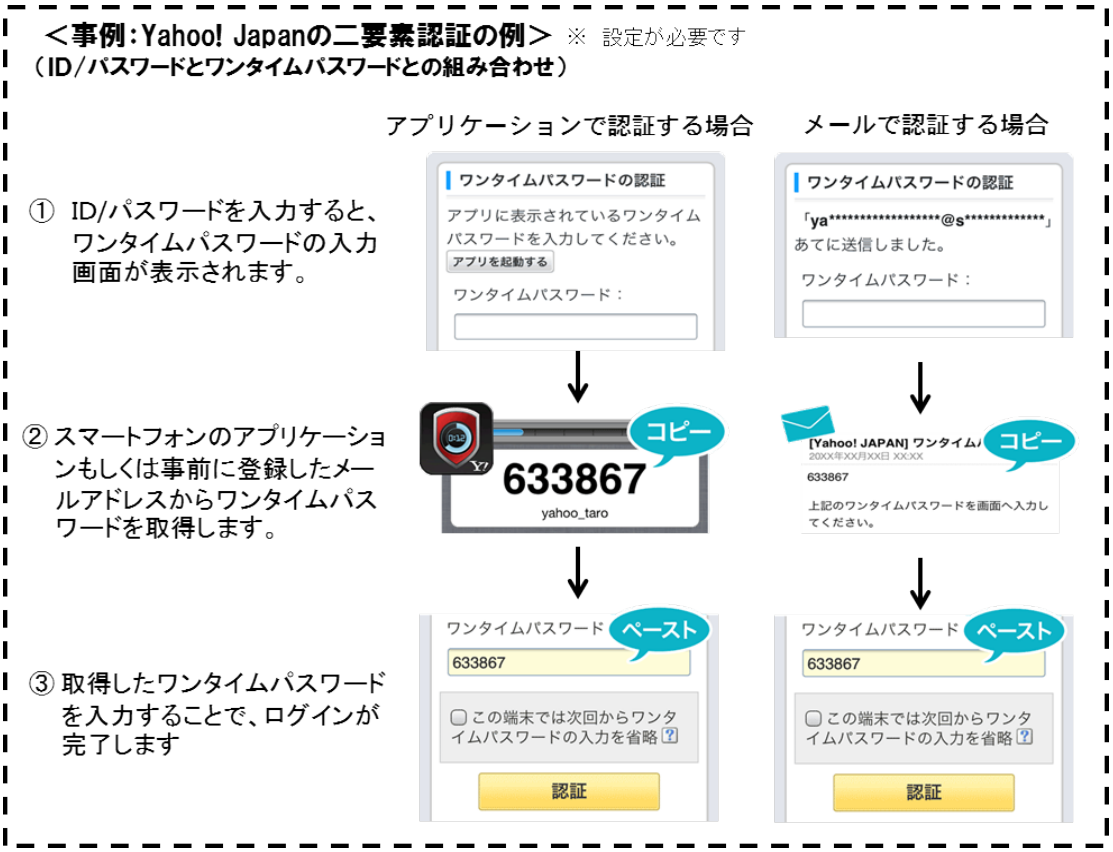
[4] 一般的に、多要素認証は、「知識」・「持ち物」・「身体の特徴」の認証要素のうち、異なる種類を組み合わせることを指し、ＩＤ・パスワードと第２パスワードのように、同じ種類を組み合わせたものは、多要素認証とは言いません。
また、多要素認証・二要素認証については、それぞれ多段階認証・二段階認証と呼ぶこともあります。

に登録した質問事項への回答についても、利用者が使い回しをしている可能性が考えられるため、定期的な変更が必要です。なお、最近では Zbot などのマルウェアによる Man in the Browser 攻撃[5]がワンタイムパスワードを突破している例もあり、二要素認証を導入していれば必ずしも安全というわけではないケースもあります。本対策集に記載している対策を複数組み合わせて実施していただくことが重要です。

＜多要素認証の例＞

- ○ ID/パスワードに加えてセキュリティトークンにより生成されたワンタイムパスワード[6]を入力させる
- ○ 暗証番号に加えてICカードを利用する など

＜事例：Yahoo! Japanの二要素認証の例＞ ※ 設定が必要です
（ID/パスワードとワンタイムパスワードとの組み合わせ）



引用元：http://id.yahoo.co.jp/security/otp.html

5 送受信する通信内容を改ざんする機能を持つマルウェアに感染させることで、利用者が入力した認証情報を窃取したり、利用者の意図とは異なる通信を行ったりする攻撃であり、ネットバンキングを用いた不正送金などに悪用されています。

6 短時間のみ有効な使い捨ての暗証番号のこと。通常のパスワードに追加することで不正ログインを防ぐことができます。

（５）ID・パスワードの適切な保管

リスト型攻撃については、はじめに何らかの手段で利用者のID・パスワードが窃取されていることが前提となります。そのため、サービスを運営する事業者において、適切に利用者のID・パスワードを保管し、必要な不正アクセス対策を実施することが重要です。具体的には、①不正アクセスが行われた際に、ID・パスワードなどの利用者情報に直接アクセスできないよう、Webサーバと認証サーバを分離するなどの物理的なサーバ構築を行うこと、②ID・パスワードに関しては、窃取された場合に容易に内容を読み取られないよう、平文での管理を行わず、暗号化（ハッシュ化）して管理すること、③ID・パスワードを記録したファイル自体にパスワードを設定し、そのパスワードを暗号化して管理すること、④窃取された際のリスクを軽減するため、IDとパスワード、両者を紐づける対応表のそれぞれを別のファイルにて管理すること、⑤退職や部署異動の際には該当者のID・パスワードを停止し、退職後の不正なシステムの使用によるID・パスワードの流出を防ぐことなどが考えられます。

ハッシュ化については、攻撃者においてハッシュ化されたパスワードを復元することもあるので、ハッシュ化を行えば問題はない、とまでは言い切れません。しかし、ID・パスワードのハッシュ化に当たり、ソルト[7]の追加やキーストレッチング[8]を行うことで、ID・パスワードの解析が困難になり、パスワードの解析に時間を要するようになります。リスト型攻撃と見られる不正ログインを検知した際には、その時間的猶予を利用して、すぐに利用者に注意喚起を行い、パスワードの変更を促すなどの対策を行うことにより、被害の拡大を防ぐことが可能となります。

---

7 ソルト（ＳＡＬＴ）：ハッシュ化の際にパスワードの前後に付け加えるランダムな文字列のことで、ソルトをつけた上でハッシュ化することにより、同一のパスワードであっても異なるハッシュ値が生成され、ハッシュ値の同一性からパスワードが割り出される危険性がなくなり、攻撃者によるパスワードの解析が困難になります。

8 キーストレッチング：パスワードを複数回ハッシュ化する方法のことであり、ストレッチングを行うことで、短時間での元のパスワードの割り出しを困難にします。

参考2　情報漏えいが発生した際の対応について

リスト型攻撃により情報漏えいが発生した際には、事業者において以下の対策を取り、被害の拡大防止を図ることが重要です。

○ 発見・報告

通報を行った発見者にヒアリングをし、発見の事実確認をするとともに、責任者への報告を行い、初動対応に移行するか判断します。

○ 初動対応

報告のあった情報を元に、具体的調査の実施・被害情報の公表・被害の拡大防止策の実施などの具体的な対応を行うかを判断します。

○ 調査

①いつ、②どんな情報が、③どのくらいの件数、④どこから、⑤どこに漏えいしたのかの観点から、具体的な情報漏えいの状況を調査するとともに、事実関係を裏付ける情報や証拠を確保します。

○ 通知・報告・公表など

情報漏えいに関する事実関係を、漏えい情報の主体である本人に通知し、各利害関係者[9]に開示し、監督官庁に報告を行います。

○ 抑制措置と復旧

情報漏えいの原因となった脆弱性の修復や通信の遮断などを行うことで、被害の拡大を防止するとともに、可能な限り被害情報の回収に努めます。

○ 事後対応

情報漏えいの再発防止に向けて、再発防止策の立案と実行、継続的な調査、情報漏えいに対する責任の追求を行います。

参考：独立行政法人情報処理推進機構「情報漏えい発生時の対応ポイント集」
（http://www.ipa.go.jp/security/awareness/johorouei/rouei_taiou.pdf）、
同「情報漏えいインシデント対応方策に関する調査報告書」（http://www.ipa.go.jp/files/000002223.pdf）

（６）休眠アカウントの廃止

無料でアカウントを取得できるサービスについては、手軽にID・パスワードが取得できることから、利用者自身も忘れてしまっているものや、いわゆる「捨てアカウント」として一時的な利用のために取得され、わずかな回数しか使用されずそのままになっているものなど、長く休眠状態にあるアカウントが多く存在していると考えられます。

このような休眠アカウントは、アカウントが乗っ取られたとしても利用者が気付きに

[9] 利害関係者としては、顧客、マスメディア、株主、セキュリティインシデントに関する対応・調整を行う機関（JPCERT コーディネーションセンターなど）が考えられます。

くいことから、第三者に悪用されることも考えられます。このため、一定期間利用実績のないアカウントについては、アカウントの廃止[10]措置を取る方法も考えられます。

長期間利用のないアカウントを廃止することで、利用者の管理が及んでいないところから個人情報が流出するリスクを減らすことができます。しかし、利用者がアカウントに重要な情報を保管している場合も考えられ、廃止に伴う各種データの消失に対して利用者から苦情が寄せられる可能性も考えられます。そのため、一定期間利用実績がない場合はデータも含めてアカウントを削除する旨利用規約に事前に記載する、休眠状態のアカウントについては停止にとどめて復活の手続きを定める、あるいは、廃止にあたってはあらかじめ登録されたメールアドレスに連絡してどのような情報が保管されているか提示しながら廃止か利用継続かを利用者に選択してもらうなど、善後策を講じておくことが好ましいと思われます。

参考3　休眠アカウントの停止・廃止に関する利用規約について

サービスの利用規約などにおいて、その他の停止・廃止に関する規定とともに、休眠アカウントの取扱いについて定めを置いているものがいくつかあります（Gmail、Twitter など[11]）。具体的な規定の内容はサービス毎に異なりますが、停止・廃止により発生する利用者の不利益を考慮すれば、どのくらいの期間の利用実績が無ければ停止・廃止措置を取るかについて明記し、停止・廃止にあたって事前に通知を行うことが求められると考えられます。

（７）推測が容易なパスワードの利用拒否

攻撃者はリストに登録されているパスワードの他にも、利用者の個人情報やキーボード配列などから推測されるパスワードを使って不正ログインを試みることがあるため、容易に推測が可能なパスワード[12]は第三者による不正ログインが行われる危

10 ここでは、利用者の求めによってもアカウントやデータの復活が不可能な状態にすることを「廃止」とし、利用者の求めに応じてアカウントやデータを元に戻すことを可能にし、アカウントや各種データの管理を継続しているものを「停止」として区別しています。

11 Gmail プログラムポリシー（http://mail.google.com/mail/help/intl/ja/program_policies.html）
Twitter ルール（http://support.twitter.com/articles/253501-twitter）

12 推測が容易なパスワードとしては、辞書に登録されている単語やアルファベットのみもしくは数字のみを組み合わせた単純なもの、5 文字以下のもの、メールアドレスをそのまま流用したもの、ＩＤと同一のものなどが考えられます。また、一般ユーザが実施することが推奨される情報セキュリティ対策として、「サイバーセキュリティトップティップス」（「ＡＰＥＣサイバーセキュリティ意識啓発の日」の取組として作成・公開）が作成されており、その１つにおいてパスワードは最低でも８文字以上とし、数字や記号を混ぜるようにするよう記載されています。
（http://www.soumu.go.jp/menu_news/s-news/02ryutsu03_02000012.html）

険性を高めます。このため、推測が容易な、強度が弱い[13]パスワードを受け付けないなどのパスワード・ポリシーを予め定めておき、利用者が申請するパスワードがポリシーに反する弱いものである場合には、より強いパスワードを求めるという方策が考えられます。

参考4　危険なパスワードの例

（1）自分や家族の名前、ペットの名前

- yamada、tanaka、taro、hanako（名前）
- 19960628、h020315（生年月日）
- tokyo、kasumigaseki（住所）
- 3470、1297（車のナンバー）
- ruby、koro（ペットの名前）

（2）辞書に載っているような一般的な英単語

- password、baseball、soccer、monkey、dragon

（3）同じ文字の繰り返しやわかりやすい並びの文字列

- aaaa、0000（同じ文字の組み合わせ）
- asdf、qwerty（キーボードの配列）
- abcd、123456、200、abc123（安易な数字や英文字の並び）

（4）短すぎる文字列

- gf、ps

出典：総務省「国民のための情報セキュリティサイト」
（http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.html）

4．攻撃による被害の拡大を防ぐ対策

リスト型攻撃は、保有するリストにある全てのＩＤ・パスワードを網羅的に照合してログインを試みているとされるため、過剰なログインの試行回数と認証エラー回数が発生するとともに、通常の利用の場合と異なるＩＰアドレスからのアクセスが生じることが考えられます。このため、攻撃を受けた際、下記の対策を講じることが有効と考えられます。

①　複数回認証を失敗したアカウントを停止し、以後の攻撃を防ぐ
②　攻撃が行われているＩＰアドレスからの通信を遮断する
③　ログイン履歴を表示するなど、攻撃を検知しやすくする

本章では、上記の点から具体的な対応方策について記載します。

13 パスワードの強度を高めるには、使用する文字の種類（大文字、小文字、数字、記号）や文字数を多くすることが重要です。使用するパスワードの強度を確かめる方法として、パスワードの解析に要する時間の目安を表示するツール（インテル「How Strong is Your Password?」https://www-ssl.intel.com/content/www/us/en/forms/passwordwin.html）や、パスワードの強度を段階に分けて判定してくれるツール（マイクロソフト「パスワードチェッカー」https://www.microsoft.com/ja-jp/security/pc-security/password-checker.aspx）があります。

（１）アカウントロックアウト

リスト型攻撃が行われる場合には、必ずしも参照されるリストのID・パスワードの全てがログインに成功するわけではないため、ある程度のログインの認証エラーが発生します。これまでのリスト型攻撃に関する被害報告によれば、リスト型攻撃は成立件数以上の試行が行われているため（参考5参照）、認証エラーのログを監視し、同一のIDに対して一定の閾値以上の認証エラーが発生した場合に、そのアカウントを一時停止する措置を講じることも有効です。

一時停止の措置を受けたアカウントは、リスト型攻撃に再び利用される可能性があるため、正規の利用者の求めによりアカウントを復活させる際、パスワード変更の注意喚起を促すなど、今後の攻撃に対する予防措置を講ずることも考えられます。この場合には、アカウントが停止され、一時的にサービスが利用不能になることについて、予め利用者の了解を得ておくなど、適切な配慮を行うことが好ましいと考えられます。

参考5　不正ログインの成立率

被害企業	試行件数（A）	成立件数（B）	成立率※（B／A）
A社	約 24,000	77	0.32%
B社	約 26,000	97	0.37%
C社	約 1,110,000	約 15,000	1.35%
D社	約 240,000	682	0.28%
E社	5,202,002	8,289	0.16%
F社	11,031	126	1.14%
G社	15,457,485	23,926	0.15%
H社	3,945,927	35,252	0.89%

※「成立率」は、企業が公表した数値を基に独立行政法人情報処理推進機構（ＩＰＡ）が算出したもの

出典：ＩＰＡ「『全てのインターネットサービスで異なるパスワードを！』
～多くのパスワードを安全に管理するための具体策～」
（https://www.ipa.go.jp/security/txt/2013/08outline.html）

（２）特定のIPアドレスからの通信の遮断

上記（１）で記載したように、リスト型攻撃においてはある程度の認証エラーが発生しますが、攻撃の中には、１つのIDに対するパスワードの試行回数が１、２回にとどまるものもあり、必ずしも一つのIDにおける認証エラーの閾値を超えない攻撃も存在します（参考6参照）。そのような攻撃に対しては、別の方法による対策が必要です。

リスト型攻撃は、リストにある全てのID・パスワードを網羅的に照合して行われるものですので、攻撃が行われる際には、大量のアクセスが発生します。１人の利用者が１つのサービスにおいて何十、何百ものアカウントを保有し、それらのアカウントに対して短時間で大量のログインを行うことは一般的に想定されていないため、同一の通信元からの大量アクセスが発生した場合、リスト型攻撃が行われていると判断して、その通信元からの通信を遮断する方法が対策として考えられます。

一般に、インターネットによる通信を行う際には、データを送受信する機器（パソコン、ルータなど）を識別するための番号として、インターネット・サービス・プロバイダ（ISP）からIPアドレス[14]が割り当てられます。IPアドレスはいわば住所や電話番号のようなもので、IPアドレスにより通信の相手方が一意に識別されることで通信が成立し、また通信を確実に成立させるため、基本的に異なる機器には異なるIPアドレスが割り当てられます。リスト型攻撃による大量のログインが試行される場合には、通常、特定の機器から行われるため、同一のIPアドレスから大量の通信が発生することになります。このため、一定の閾値を設定し、特定のIPアドレスから閾値以上のアカウントへのログイン要求の通信が発生した場合には、当該IPアドレスからのアクセスを遮断する方法が考えられます。

本対応策は、膨大な量のログインを試みるというリスト型攻撃特有の性質に着目し、当該通信を行うIPアドレスからの通信を遮断するものであり、リスト型攻撃に対する対応策としては非常に有効な対策と言えます[15]。なお、IPアドレスは、個々のネットワーク接続に対して異なるものが割り当てられる[16]ので、攻撃を行ってきた特定のIPアドレスのみを遮断するだけでは、攻撃者がネットワーク接続を切り替えて別のIPアドレスから攻撃を再開することも考えられます。このため、大量の不正ログインが行われている発信元のIPアドレスについて、サービスを運営する事業者間において共有し、リアルタイムで対策を講じることも有効な対策と考えられます。一方で、

---

14 ＩＰアドレスには大きく分けて、インターネットの接続用に使用されるグローバルＩＰアドレスと家庭内や企業内など組織内のみで使用できるローカルＩＰアドレス（プライベートＩＰアドレス）の２つがありますが、ここでは、グローバルＩＰアドレスのことを指してＩＰアドレスと呼びます。

15 攻撃の中にはマルウェアに感染させた無数の機器を遠隔で操作して行うものもあり、その場合それぞれ異なるＩＰアドレスから攻撃が行われ、検知が困難になる場合もあります。

16 一方で、複数の機器に同一のＩＰアドレスを割り当てて共有する技術（キャリアグレードＮＡＴ）により、個々のネットワーク接続に対して異なるＩＰアドレスが割り当てられるとは限らない場合もあります。この場合、特定のＩＰアドレスからの通信を遮断すると、攻撃者以外の善良な利用者の通信も遮断してしまう可能性があるため、注意が必要です。

個別の通信におけるIPアドレス情報は、通信の秘密（電気通信事業法[17]第４条）として保護されるものであるため、本対応を行う場合には、留意する必要があります。この点は、下記の対応(3)についても同様です[18]。

参考6　eBookJapan サイトに対して行われたリスト型攻撃において、1 つのログイン ＩＤに対して試行されたパスワード数

【ログイン成立分】

IDあたり PW試行回数	該当ID数
1	386
2	347
3	37
4	4
5	5

【ログイン失敗分】

IDあたり PW試行回数	該当ID数
1	1,327
2	72
3	20
4	7
5	3
6	1
9	1

出典：イーブックイニシアティブジャパン「【重要なお知らせ】不正ログイン被害のご報告とパスワード再設定のお願い」（http://www.ebookjapan.jp/ebj/information/20130405_access.asp）

（３）普段とは異なるIPアドレスからの通信の遮断

上記（２）で記載したように、利用者の端末には、契約しているISPからIPアドレスが割り当てられます。また、一般的に、ISPは一定のレンジのIPアドレスを保有しており、これを利用者に動的に割り当てているため、利用者がISPから割り当てられたIPアドレスにより通常使用している端末からアクセスを行った場合には、比較的近似のIPアドレスからの通信が行われることになります。このため、通常ログインされているIPアドレスから大きくレンジの外れたIPアドレスからのログインがあった場合には、正規の利用者ではなく、第三者からの不正なアクセスである可能性があります。これに着目し、通常のIPアドレスから大きくレンジの外れたIPアドレスからのアクセスがあった場合に警告を発すると共に通信を遮断する方法が対策として考えられます。普段使用されているIPアドレスとの相違に着目し、通信を遮断する本対策に

17　昭和 59 年 12 月 25 日法律第 86 号

18　「通信の秘密」の範囲は、通信の内容のほか、通信の日時、場所、通信当事者の識別符号などこれらの事項を知られることによって通信の意味内容が推知されるような事項すべてを含むことから、ログイン時に使用された発信元の IP アドレスについても通信の秘密に含まれます。
このため、ログインに係る通信の当事者ではない ISP などが、ログイン時に４の(2)ないし(3)記載の対策を講ずる場合には、当該ログインに係る通信の当事者であるサービスを提供する事業者の同意に基づく必要があります。

ついては、リスト型攻撃に限らず、広く不正アクセスの防止に効果があります。

ただし、出張時などにおいて、出張先などのインターネットカフェや公衆無線LANスポットを利用して通信を行うことも考えられるため、通常のIPアドレスから大きくレンジの外れた通信が必ずしも不正なアクセスによるものとは言い切れません。そのため、攻撃のあったIPアドレスからの通信を遮断するという手段の他にも、そのような通信が発生した際に、3.（4）で説明した二要素認証を用い、利用者が予め登録しているメールアドレス（ID・パスワードが流出している可能性を考慮して、フリーメールのアドレスの登録の回避を推奨します。）にワンタイムパスワードを送付し、認証要素を追加する対策も考えられます。

（4）ログイン履歴の表示

リスト型攻撃は、大量のログインや認証エラーが発生する場合などには、検知も容易ですが、ごくわずかな件数にとどまる場合など、サービスを運営する事業者による検知が困難な場合もあります。そのため、利用者が不正に使われた形跡の有無を確認できるようにし、不正利用に関する届出窓口を整備するなど、利用者からの不正アクセスに関する通報の仕組みを整える対策も考えられます。具体的には、利用者がログインを行う度に、あらかじめ登録しているメールアドレスにメールを送付して通知を行う、また、ログイン履歴を保存し、ログイン後の画面に前回のログイン日時を表示するなど、利用者にアカウント利用実績を認識することができるように設定する方法が考えられます。

本対策は、あくまでも被害を受けた後の実態把握に役立つものであり、被害の防止対策ではありませんが、利用者において、これまで検知が困難であったリスト型攻撃についての発生状況の把握が容易となり、サービスを運営する事業者においても、利用者から報告を受ければ、パスワード変更などの被害の拡大防止策の検討に役立たせることができます。

５．おわりに

これまで述べたリスト型攻撃への対応方策をまとめると、以下の通りとなります。

① 利用者にID・パスワードの使い回しをしないなどの注意喚起を行う

② そもそもID・パスワードのリスト化を防止するため、推測困難なものを設定するとともに、ID・パスワードの管理を徹底する

③ 何らかの手段によりID・パスワードがリスト化された場合でも、パスワードの定期的な更新、認証要素の追加などによりリストを陳腐化させる

④ 攻撃が行われた際、認証に複数回失敗したアカウントをロックする、攻撃を行うIPアドレスからの通信を遮断するなど、被害の拡大を防止する

⑤ ログイン履歴を表示するなど、攻撃の実態を把握し、利用者対応などの善後策を講じる

	リスト型攻撃への対策	
	攻撃を予防する対策	攻撃による被害の拡大を防ぐ対策
具体的内容	○ ID・パスワードの使い回しに関する注意喚起 [3. (1)] ○ パスワードの有効期間設定 [3. (2)] ○ パスワード履歴保存 [3. (3)] ○ 二要素認証の導入 [3. (4)] ○ ID・パスワードの管理徹底 [3. (5)] ○ 休眠アカウントの廃止 [3. (6)] ○ 推測困難なパスワードの設定 [3. (7)]	○ 認証エラーに対するアカウントロックアウト [4. (1)] ○ 特定のIPアドレスからの通信遮断 [4. (2)] ○ 普段と異なるIPアドレスからの通信遮断 [4. (3)] ○ ログイン履歴の表示 [4. (4)]

図：対策の目的に着目した分類

	リスト型攻撃への対策				
	ID・パスワードの使い回し防止	リストの陳腐化	ID・パスワードのリスト化防止	攻撃検知・悪用防止	攻撃時の被害拡大防止
具体的内容	○ 使い回しに関する注意喚起の実施 [3. (1)]	○ パスワードの有効期間設定 [3. (2)] ○パスワード履歴保存 [3. (3)] ○二要素認証の導入 [3. (4)]	○ ID・パスワードの管理徹底 [3. (5)] ○ 推測困難なパスワードの設定 [3. (7)]	○ 休眠アカウントの廃止 [3. (6)] ○ ログイン履歴の表示 [4. (4)]	○ 認証エラーに対するアカウントロックアウト [4. (1)] ○ 特定のIPアドレスからの通信遮断 [4. (2)] ○ 普段と異なるIPアドレスからの通信遮断 [4. (3)]

図：対策の内容に着目した分類

また、これまで検討した対応方策については、コストや利用者の利便性などの観点からメリット・デメリットが考えられますので、検討の参考として以下の通り整理します。それぞれの事業者において対策を講じられる際には、下記のメリット・デメリットのように、コスト負担の発生程度、利用者の利便性への影響、保有している個人情報の内容（金銭の有無など）などを踏まえ、検討してください。

ID・パスワードの使い回しに関する注意喚起	◎ リスト型攻撃の要因であるID・パスワードの使い回しを比較的少ないコストで防ぐことが可能。 × 注意喚起のためのページ作成やメール配信に若干のコストが生じる。
パスワードの有効期間設定	◎ リスト化されたID・パスワードを陳腐化するという点において、シンプルかつ有効な手段。 × 定期的にパスワードを更新することで利用者の利便性が落ちる。
パスワード履歴の保存	◎ リスト化されたID・パスワードを数世代分にわたり陳腐化する点において有効。 × 数世代分のパスワードを保存するためのシステム改修が必要となり、コストが生じる。
二要素認証の導入	◎ 攻撃者がリスト化したID・パスワードによるログインを不可能にし、リスト型攻撃を無効化できる。 × 認証要素を追加するためのシステム改修、利用者への周知などの導入コストが大きくかかる。
ID・パスワードの管理徹底	◎ ID・パスワードが漏洩した場合のリスクを軽減することができ、攻撃の端緒となるID・パスワードのリスト化を防ぐことができる。 × ID・パスワードの暗号化や管理に若干のコストが生じる。
休眠アカウントの廃止	◎ 正規の利用者の管理の範囲外にある休眠アカウントが、攻撃者に悪用されるリスクを軽減することが可能。 × 利用者において定期的なログインが必要となるなど利用者の利便性を損ねる。
推測困難なパスワードの設定	◎ 攻撃者のパスワード推測による不正アクセスの可能性を低くすることができ、ID・パスワードのリスト化を防ぐことができる。 × 推測が困難なパスワードは利用者も覚えることが困難であり、利用者の利便性が落ちる。
認証エラーに対するアカウントロックアウト	◎ 攻撃の対象となったアカウントを一時停止することで、別の者による二次的、三次的な攻撃を防ぐことが可能。 × アカウントロックアウトに関するシステム改修や利用者の同意取得などのコストが生じる。
特定のIPアドレスからの通信遮断	◎ 攻撃の事実を元に、攻撃が行われている通信を断つことで攻撃を防ぐものであり、非常に有効。 × 攻撃者の通信以外にも善良な利用者の通信を遮断する可能性があり利用者の利便性が落ちる。
普段と異なるIPアドレスからの通信遮断	◎ リスト型攻撃に限らず、不正なログインに対して広く有効。 × 正規の利用者の外出先からのアクセスを遮断する場合があり、利用者の利便性を損ねる。
ログイン履歴の表示	◎ これまで検知が困難であった小規模のリスト型攻撃についても検知できる可能性がある。 × ログイン履歴の表示に関するシステム改修にコストが生じる。

図：対応方策のメリット・デメリット（◎はメリット、×はデメリット）

これまで挙げた対応方策についてはあくまでも一例であり、攻撃者においても新たな攻撃手法を日々生み出していることから、本書で掲げた対策が必ずしも長期的に有効とは限りません。このため、サービスを運営する事業者において、常に有効な対応方策に自主的に取り組んでいただくことが肝要です。