不正アクセスへのセキュリティ対策
―利用者の振る舞いを分析して成り済ましを検知―

不正に入手したID・パスワードのリストを使ったリスト型アカウントハッキングのように、最近は不正アクセスの手法が巧妙化し、被害も後を絶たない。本稿では、Webサイト上の振る舞いを分析することで不正アクセスを検知する手法の有効性と、リスク判断のポイントについて紹介する。

NRIセキュアテクノロジーズ
ソリューション事業本部
ソリューションビジネス一部
上級セキュリティエンジニア
大島（おおしま）　修（おさむ）
専門はIDセキュリティソリューションの企画・開発

NRIセキュアテクノロジーズ
ソリューション事業本部
ソリューションビジネス一部
主任セキュリティコンサルタント
井本（いもと）　武宏（たけひろ）
専門はIDセキュリティソリューションの企画・営業

なくならない不正アクセスとその被害

昨今、Webサイトへの不正アクセスによって企業やサイト利用者が被害に遭う事件が後を絶たない。2016年3月にも、大手インターネットショッピングサイトで、会員のポイントが不正に使用されたり、個人情報が閲覧されたりしたことが公表された。これは、ショッピングサイトとは別のサービスから不正に取得したと思われる会員IDとパスワードを用いてWebサイトにアクセスするという方法によって行われた。

2016年3月24日に公表された警察庁の資料（「平成27年における不正アクセス行為の発生状況等の公表について」）によると、2015年の1月から12月までの不正アクセスの認知件数は2,051件で、前年の3,545件に比べて減少しているものの、依然として高い水準にある。不正アクセスによる不正行為としては、インターネットバンキングでの不正送金が74.6%と圧倒的な割合を占めており、次いで、インターネットショッピングでの不正購入（8.1%）、オンラインゲームやコミュニティーサイトでの不正操作（4.7%）となっている。このことから、Webサイトの利用者に対して直接的な被害を与えるような不正行為が際立っていることが分かる。

資料では、不正アクセスの手口として、サービス利用者のIDとパスワードを他人が不正に使用するものが多く、利用者のID・パスワード管理の甘さにつけ込んだり、インターネット上に流出・公開されたID・パスワードのリストを使ったりすることが多いとされている。

このためWebでサービスを提供する事業者は利用者に対して、推測されにくいパスワードを設定すること、ID・パスワードの使い回しを避けることなどを促している。しかしこれらを利用者に義務付けることは難しいのが実情である。

高度化する攻撃手法

不正アクセスの手法は、Webサイトのアプリケーションやミドルウェアの脆弱（ぜいじゃく）性を

突く攻撃（脆弱性攻撃）と、Webサイト利用者のID・パスワードを推測または盗用し、その人に成り済ましてアクセスするID系攻撃の2つに大きく分類される。

脆弱性攻撃に対しては、サービス提供企業側の対策として、Webサイトのアプリケーションのセキュリティ設計・開発や、ミドルウェアの脆弱性情報の収集と緊急度に応じたセキュリティパッチの適用が求められる。

ID系攻撃には、以前からあるブルートフォース攻撃（ID・パスワードの総当たり攻撃）や辞書攻撃（利用者がパスワードとして利用しがちな単語を辞書として登録しておいてアクセスを試みる）に加え、あらかじめいずれかのサービスから不正に取得したID・パスワードのリストを利用してアクセスを試みるリスト型アカウントハッキングと呼ばれる攻撃手法があり、ID系攻撃の主流となってきている。前述の大手ショッピングサイトに対する不正アクセスでもこの方法が使用された。

リスト型アカウントハッキングは、利用者が複数のWebサイトで同じID・パスワードを使い回す習慣があることを利用した攻撃である。最近は、ボットネット（攻撃用プログラムに感染した大規模コンピュータ群）を利用してIPアドレスが異なる複数の地域から不正アクセスを行う分散型攻撃や、一定の時間をおいて不正アクセスを繰り返す低速型攻撃といった高度な手法が増えてきている。これらは正当な利用者によるアクセスと不正アクセスの見分けがつきにくいため、不正アクセスの認知が遅れ、被害が拡大する危険性が高い。しかしサービスを提供する側では、これを検知するための有効な対策を講じられていないのが実情である。

インターネットバンキングでの不正送金の被害が拡大するなか、金融機関はID・パスワードに加えて、ログインや振り込みなどのたびにワンタイムパスワードの入力を義務付けるといった多要素認証の導入を進めるなど、不正アクセスへのセキュリティ強化を図っている。その一方、サービスを利用するたびにワンタイムパスワードの入力が必要となれば利便性を損ねることにもなるため、顧客の離反を招く懸念もある。

このように、インターネット上のサービスを提供する企業にとって、利用者の利便性の低下を最小限にしつつ、分散型攻撃や低速型攻撃といった高度な手法を取るリスト型アカウントハッキングを防御することは差し迫った課題となっている。

利用者の振る舞い分析による不正検知

上記の課題意識の下で最近注目されているのは、Webサイト上の利用者の振る舞いを分析することで不正アクセスを検知するという考え方である。

同様の考え方に基づく対策は、クレジットカードの不正利用対策として以前から導入されている。クレジットカードの決済では、金額や利用場所、商品属性などの情報を利用者の通常時の取引パターンと照らし合わせ、必要に応じて電話確認などの追加認証を求めたり、不正利用の疑いが強い場合には決済できなくしたりすることが行われている。

表1　振る舞い分析による不正アクセス検知の例

不正検知に利用可能な属性	不正アクセス疑いの判定パターン
端末識別子 （アクセス元端末のOS／ブラウザーのバージョン、言語設定、インストールされているプラグイン、フォント、画面解像度、端末固有IDなどを組み合わせて生成する端末の「指紋」）	・特定端末から大量のログイン試行 ・特定端末から大量のユーザーのログインに成功している ・過去の不正アクセスや他サービスの不正アクセスに使用されたのと同じ端末からのアクセス ・当該ユーザーが通常利用していない端末からのアクセス
IPアドレス	・同一IPアドレスから大量のログイン試行 ・同一IPアドレスから大量のユーザーのログインに成功している ・当該ユーザーが通常利用しないネットワークからのアクセス
地理情報 （IPアドレスから検出できる国／地域情報、あるいは端末GPSなどから取得できる位置情報）	・当該ユーザーが通常は利用しない国／地域からのアクセス ・当該ユーザーの前回アクセス時からの位置の変化で計算される移動速度が異常（例：東京からアクセスのあった1時間後に東欧からログイン）
ページ遷移／入力操作	・人間では不可能な速度でのフォーム入力やページ遷移（ボットによるアクセスの疑い） ・スパイダリング（情報抽出目的の機械巡回）が疑われる画面遷移
曜日／時間帯	・当該ユーザーが通常は利用しない曜日や時間帯におけるアクセス
取引パターン	・当該ユーザーが通常行わない種別の取引の実施 ・当該ユーザーが通常行う金額の範囲を超える取引の実施 ・取引実行前のメール・電話番号などの属性情報変更（本人通知が行われるのを防ぐ疑い） ・取引実行後の即時退会

Webサイトの利用時にも同様の方法が可能である。ログイン時の利用者の属性情報や、ログイン後の挙動を分析することにより不正アクセスのリスクを評価し、必要に応じて追加の本人確認を求めるというものである。これにより、成り済ましログインによる情報漏えいや不正取引のリスクを低減することが可能となる。

クレジットカードの不正検知は、ある時点での店舗でのカード決済という「点」の分析となるのに対し、Webサイトでの振る舞い分析は、利用者の一連のボタン操作やリンクの選択といった「線」での分析になる。このため、利用者に関するより多くの属性情報を活用することで、より正確なリスク判定が可能になる。

米国の調査会社Gartner社は、Webサイト上での不正検知の手法を以下のような5階層のモデルで表している。

①レイヤー1（エンドポイント分析）

アクセス元のPCやモバイル端末固有の属性情報に基づく不正検知手法

②レイヤー2（ナビゲーション分析）

Webサイト上の特定セッションのページ遷移に基づく不正検知手法

③レイヤー3（ユーザー分析）

Webサイト上のユーザーの振る舞いに基づく不正検知手法

④レイヤー4（クロスチャネル分析）

複数のシステムにまたがるユーザーの振る舞いに基づく不正検知手法

⑤レイヤー5（エンティティーリンク分析）

複数のシステム、複数のユーザーにまたがる共謀などによる不正を大規模データ分析により検知する手法

レイヤー1～レイヤー3までが単一Webサイト上での不正アクセス検知の手法で、本稿の対象もこの部分である。それでは、不正アクセスは具体的にどのように検知できるのだろうか。

表1に、レイヤー1～レイヤー3の不正検知に利用できる代表的な属性情報と「不正アクセス疑いパターン」の例を示す。これらは、実際に不正アクセスが行われる際の典型

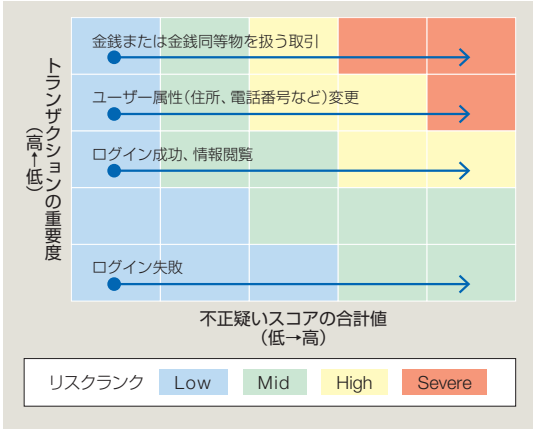
的なパターンを抽出したものである。ただし、アクセスの挙動がこれらのパターンに当てはまったからといって即座にそれが不正なものと断定できるわけではない。そこで、それぞれのパターンに「不正疑いスコア」を割り当て、より多くのパターンに当てはまる（合計スコアが高い）ほど、正規な利用者のものでない不正アクセスの疑いが強いと判断するのである。

次に、「不正疑い」の合計スコアと、アクセスした人が実行しようとしているトランザクション（業務上の処理）の重要度に応じてリスクランクを4段階で判定する（図1参照）。不正アクセスの疑いの強さだけではリスクの高低を決めることができないからである。金銭やその同等物（ポイントなど）を扱うトランザクションは最も重要度が高く、利用者の住所などの変更はその次に重要度が高い。ログインの失敗は重要度の低いトランザクションとする。このようなトランザクションごとの重要度は、あらかじめ数値として定義しておく。

例えば、金銭の取引を目的としたアクセスで「不正疑いスコア」（合計値）が高ければ、当然ながら即時対応の必要性が高い深刻なリスクである。一方、ログインに失敗している限りは、不正アクセスが疑われても、リスクは低いか中程度であり、経過観察や事後的な対応が検討されるべきである。

このようにして不正疑いとリスクランクの判定ができれば、ログインした人が金銭やポイントに関する取引をしようとした場合に、リスクランクに応じて追加認証を要求したり処理を実行不可にしたりするなど、適切な対応が可能になる。

図1　リスクランク判定の例



振る舞いに基づいたリスク判定は、全ての検証がバックエンドで行われるため、利用者には何も意識させないという利点がある。また、リスクランクが高い場合のみ追加認証を要求するなど、利便性を損ねることなくWebサイトのセキュリティを強化することができる。

NRIセキュアテクノロジーズは、以上の考え方に基づいて不正アクセスとリスクランクの判定を行うソリューション「Uni-ID Identity Fraud Detection」を提供している。

継続的な対応が重要

利用者の振る舞いの分析による不正検知を導入する場合、リスクランクに応じた対応方針とその対応の業務フローについても検討しておくことが必要である。また、不正アクセスの手口は巧妙化し続けるため、対策も常に進化させていかなければならない。そのためサービス提供者は、PDCAサイクルを回しながら、リスク対応を高度化できる運用を組織レベルで整備することが重要である。 ■