

ユーザー以外のログインを未然に検知する、最新不正ログイン対策ツール「リスクベース認証」

CAPYリスクベース認証

人間の手による不正ログインにも効果を発揮

capy

製品概要

Capyリスクベース認証

Web サービスを利用するユーザーのログイン履歴をデータとして蓄積し、「その人らしさ」をベースにログイン行動がそのユーザーによってなされたものであるかを識別。不正な第三者がなりすましてログインするのを未然に検知し、不正ログインをしっかりと防ぎます。



製品ポイント

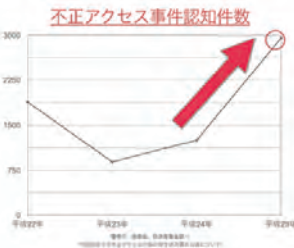
Capyリスクベースの4つのポイント

<p>人間の手によるなりすましログインに効く</p> <p>キャプチャだけでは防げなかった、人間の手によるなりすましログインにも対応。</p>	<p>30分以内の簡単導入</p> <p>ASP方式でのご提供となるため、すぐにWebサイトにご導入頂けるうえ、面倒なメンテナンスも必要ありません。</p>	<p>「その人らしさ」をもとにした不正ログイン判定</p> <p>学習期間をへて、各ユーザーの「その人らしい」ログイン習慣を学習。不審なログインを見逃しません。</p>	<p>初期コストゼロ。業界常識をくつがえす低価格</p> <p>今まで非常に高価な認証技術として考えられてきたリスクベース認証を、すべてのWeb事業者様にご導入頂ける低価格にてご提供致します。</p>
--	---	---	---

導入推奨ポイント

年間80万件にもおよぶ被害の実態

不正ログイン行為の発生件数は、警察庁へ報告がなされたものだけでも2013年の1年間において80万件ほどに達し、1日あたり2,000件以上発生している計算になります。そのためWebサービス運営事業者やインターネットユーザーにとって非常に大きな脅威となっています。大手企業にもその被害は広がっており、大手のクレジットカードサイト、SNSサイト、運輸サイト、通信キャリアサイト、ゲームサイトをはじめ、公表されているものだけでも25社から30件の被害報告がありました。



急増する不正ログイン

警察庁によって毎年発表される「不正アクセス行為の発生状況等の公表について」では、平成25年に不正アクセス事件の認知件数は約3,000件にもなることが明らかに。この数字は前年の1,200件と比較すると2.5倍にも上り、過去最高となっています。不正アクセスには、1) サーバ・ネットワークなどの脆弱性を突く攻撃 2) 内部の関係者からの流出 3) 個人になりすました不正ログインが含まれるのですが、特に、中でも3つ目の「個人になりすました不正ログイン」が急増しています。検挙された約1,000件のうち、およそ80%近くも事件が利用権者のパスワードの設定・管理の甘さにつけ込んだ不正ログインであることが判明しました。

不正ログイン激増の理由とは

警察庁によって毎年発表される「不正アクセス行為の発生状況等の公表について」では、平成25年に不正アクセス事件の認知件数は約3,000件にもなることが明らかに。この数字は前年の1,200件と比較すると2.5倍にも上り、過去最高となっています。不正アクセスには、1) サーバ・ネットワークなどの脆弱性を突く攻撃 2) 内部の関係者からの流出 3) 個人になりすました不正ログインが含まれるのですが、特に、中でも3つ目の「個人になりすました不正ログイン」が急増しています。検挙された約1,000件のうち、およそ80%近くも事件が利用権者のパスワードの設定・管理の甘さにつけ込んだ不正ログインであることが判明しました。

ハッカーの手口の変化

不正ログイン被害拡大の背景には、上記の理由に加えて攻撃者であるハッカーの手口にも変化がみられることが考えられます。これまで不正アクセスの手口と言うと、サーバーなどデータベースへのハッキングや、組織内部の人間による犯行が主流でした。しかし現在では、不正アクセス被害の大多数が不正ログイン、いわゆる「なりすまし」による不正アクセスなのです。サーバーや組織のコンプライアンス強化による情報漏洩対策はもちろんのこと、今後はユーザーがWebサービスを利用するためにまず最初にアクセスをするログインページのセキュリティもさらに強化することが求められているのです。

販売価格

個別見積

商品番号 1000632

リスクベース認証