



平成 25 年 7 月 23 日

各 位

会 社 名 株 式 会 社 イ ー ブ ッ ク
イ ニ シ ア テ ィ ブ ジ ャ パ ン
代 表 者 名 代 表 取 締 役 社 長 小 出 齊
(コード番号：3658 東証マザーズ)
問 い 合 わ せ 先 取 締 役 管 理 部 長 磯 江 英 子
(TEL. 03-3518-9544)

不正アクセスによる「なりすまし」ログインについての調査結果ご報告（最終報告）

平成 25 年 4 月 6 日および 9 日付けにてご報告申し上げました不正アクセスによる「なりすまし」ログインにつきまして、クレジットカード情報漏洩事故の調査を行う第三者機関である Payment Card Forensics 株式会社に調査を依頼し、「サーバーへの不正侵入及び情報漏洩の懸念を示す形跡はなかった」との調査結果を受領しましたのでご報告申し上げます。なお、再発を防止する対策を導入以降は本件は発生しておらず、今回の不正アクセス対策は完了したと判断いたしましたことを併せてご報告申し上げます。

記

1. 不正アクセスの内容（自社調査の結果）

- eBookJapan サイトにおきまして、平成 25 年 4 月 5 日（金）午前 10 時 30 分頃、サーバーの高負荷が検知されたことから詳しい調査を行ったところ、4 月 2 日から 4 月 5 日にかけて、779 アカウントに対して不正の疑われる IP アドレスからログインが行われました。
 - 前のご報告からのアカウント数の変更はございません。
 - 調査対象を 2013 年 4 月だけでなく、1 月から 3 月まで広げましたが、3 月以前分には該当する不正ログインは発見されませんでした。
- 本件は「なりすまし」ログイン行為、即ち、不正の疑われる複数の IP アドレスからログインページに対して、予め持っていたログイン ID とパスワードの適用可否を試行する大量アクセス行為であることが判明いたしました。
 - つまり、大量アクセス行為を仕掛けてきた者は、当社以外の他のサービスなどで他のサービスのログイン ID とパスワードを不正に入手し、ユーザーがログイン ID とパスワードを共通に設定している可能性を狙って当社サービスに不正にログインしようとし、上記件数についてはログインに成功してしまっただけのことです。
 - そのように判断した根拠は、一つのログイン ID（メールアドレス）について試行するパスワードの数の少なさです。

○ ログイン成立分

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

(注) 1 つのログイン ID について PW を試行した回数は最大 5 回までであり、1 回しか試行していないのに正当したアカウントが半数近くを占めている。

○ ログイン失敗分

<u>ID あたり PW 試行回数</u>	<u>該当 ID 数</u>
-----------------------	----------------

1	1327
2	72
3	20
4	7
5	3
6	1
9	1

(注) 1つのログイン ID について PW を試行した回数は最大 9 回までであり、1 回だけで断念しているアカウントが 9 割を占めている。

- なお、当社サーバーからログイン ID、パスワード、カード番号などの個人情報または決済情報が直接漏洩した形跡はございません。
2. 第三者機関による調査結果
- クレジットカード情報漏洩事故の調査を行う第三者機関である Payment Card Forensics 株式会社の調査報告書に於いても以下のように総括されており、上記の判断が裏付けられました。
 - 「サーバーソフトウェアおよび Web アプリケーションの脆弱性を利用した不正侵入および情報漏洩の懸念を示す形跡はありませんでした。また、カード会員データを「伝送・処理・保存」していないため、当該加盟店（当社注：当社を指します）よりカード会員データの漏洩リスクの可能性は殆どないと考えられます。」

3. 被害について

事故発生から現時点に至るまで、今回の「なりすまし」ログインによる eBookJapan サイト内における金銭的な被害は発生しておりません。なお、「なりすまし」ログインされた方のパスワードは既に変更して、ご連絡しております。

その他の詳細は以下の通りです。

- eBookJapan サイトへの「なりすまし」ログイン
 - 2013 年 4 月 1 日から 4 月 5 日にかけて、779 アカウントに対し不正の疑われる IP アドレスからログインが行われました。
 - うち、eBookJapan サイト内のマイページにおいて、会員情報（お客様の「メールアドレス」「パスワード」「氏名」「生年月日」「性別」「住所（都道府県）」などが登録されているページ）が表示された件数が、549 アカウント（同一ユーザーの IP アドレス重複分を含む）ありました。
 - また、「ワンタッチ銀行引落」という名称で実施している銀行決済に関して、eBookJapan サイト内のマイページにおいて口座番号情報が表示されており、該当する件数が、16 アカウントありました。
 - また、「ワンタッチクレジット決済」という名称で実施しているクレジットカード決済に関して、当社が指定した仕様により eBookJapan サイト内のマイページから決済代行会社の運営するページに遷移し、クレジットカード番号および有効期限が表示された件数が、47 アカウントありました。
- ※ なお、当社ではクレジットカード情報は保管しておりません。
- 不正利用
 - eBookJapan サイトにおける不正利用の形跡はありません。

4. 対応内容

- 従前からの防御内容
 - 総当たり攻撃を防ぐためのアカウントロック
同一のログイン ID に対して、一定期間内に、一定回数以上パスワードを間違えると、一定期間ロックされます。
これにより、機械的にパスワードを総当たりすることでログインしようとする不正を防ぐことが出来ます。
- 今回追加した防御内容

- 同一 IP アドレスからのログイン制限
同一の IP アドレスからログインフォームへのアクセスに制限をかけました。
この結果、適法に同一 IP アドレスから同時に多くのユーザーがログインしようとする場合にも制限をかけてしまう悪影響が生じる可能性があります。当面はセキュリティ確保を優先いたします。
- マイページ内のワンタッチ銀行引落に登録している方の口座番号の非表示化
- マイページから遷移可能な決済代行会社の運営するページにおける、クレジットカード番号および有効期限の非表示化
- 不正の疑われる IP アドレスをブロック
- 不正の疑われる IP アドレスからログインされたアカウントのパスワード初期化
 - ◇ 該当のお客様にはパスワード再設定のお願いをメールにて送付
- パスワードを他のサービスと共有しないことのおお願い
 - ◇ 重要なお知らせページ
 - ◇ ログイン画面
 - ◇ マイページ
 - ◇ 会員情報変更画面
 - ◇ パスワード再設定画面
 - ◇ 新規会員登録画面

※ 上記の対策により、4月6日以降は不正ログインは発生しておりません。

5. 今後の対応

このたびの事件について必要な対策を講じたものと判断し、収束させていただきます。

なお、今後本件に起因してお客様に金銭的被害が発生したことが判明した場合は、お客様の負担とならぬよう関係機関と連携を図りながら対処して参ります。

本件に関するご質問は、下記窓口にお問い合わせ下さい。

【投資家様・株主様からのお問い合わせ先】

管理部

お問い合わせフォーム：<https://corp.ebookjapan.jp/contact/ir/>

電話：03-3518-9544

【お客様からのお問い合わせ先】

eBookJapan サポートセンター（月-金の10-18時）

お問い合わせフォーム：<http://www.ebookjapan.jp/ebj/support/>

電話：03-3518-9744

（お問い合わせいただく際には、必ず対象の eBookJapan 会員メールアドレスをご用意ください）

以上