2018 年 12 月 25 日
お客様各位
ディー・エル・マーケット株式会社

不正アクセスによる個人情報流出に関するご報告とお詫び

本年 10 月 22 日に発表しました弊社運営の「DLmarket」（以下、「本件サービス」といいます）における不正アクセスによる情報流出事案について、外部の専門機関 2 社によるフォレンジック調査（※）を実施し、原因ならびに被害状況等の解明をすすめてまいりました。先般の発表時には、「流出した可能性のある情報は、メールアドレス/氏名/会員 ID のみ」とご説明申し上げておりましたが、このたびの調査の結果、当該不正アクセスに関連してお客様のクレジットカード情報の一部が流出した可能性があることが判明いたしました（以下、「本件」といいます）。

お客様をはじめご関係者の皆様には、先般の発表内容に加えて、更なるご迷惑とご不安をお掛けしますこと、心よりお詫び申し上げます。
つきましては、本件の概要および弊社の対応、ならびに再発防止策につきまして、下記のとおりご報告申し上げます。
※PC やサーバなど電子機器に蓄積されるデジタルデータに法的証拠能力を持たせる調査・分析

１.本件の概要

（１）流出の可能性のある対象と情報

①対象の可能性のあるお客様

・2018 年 10 月 17 日 22 時 05 分から 2018 年 11 月 12 日 21 時 50 分
上記期間内に本件サービスにおいて、**クレジットカード決済ページにクレジットカード番号を入力された方**

②流出の可能性のある情報

・クレジットカード番号
・名義
・セキュリティコード（3 もしくは 4 桁の確認番号）
・有効期限
（これら 4 つの情報を以下、「カード情報」といいます）

③決済が成立し、流出の可能性があると判断されたクレジットカード番号（以下、「対象カード番号」といいます）の最大件数： 7,741 件

④③のほか、決済は成立していないが、「偽の決済フォーム」のみに誘導された可能性のある最大件数： 903 件

（2）情報流出の原因

本件サービスのクレジットカード決済ページについて、お客様が本件サービスで商品を購入する際に、本来遷移するはずのクレジット決済代行会社のページではなく、「偽の決済フォーム」に誘導するように弊社サーバが改ざんされたことが発覚しました。これによって「偽の決済フォーム」に入力されたカード情報が不正に取得された可能性があります。

なお、「偽の決済フォーム」を経由する場合、正常な決済は行われず、お客様にはエラーの通知がなされる仕様となっておりました。

正常な決済に進まれず、「偽の決済フォーム」のみに入力されたクレジットカード番号につきましては、フォレンジック調査でも特定できておりませんが、弊社サーバのデータより、「偽の決済フォーム」に誘導された対象者は特定できております。

（3）経緯

・2018 年 10 月 17 日

弊社サーバの不具合を受け、弊社で調査を行った結果、管理画面への不正アクセスによって本件サービスに保管している情報の一部（メールアドレス/氏名/会員 ID）が流出している可能性を認識。

・2018 年 10 月 22 日

不正アクセスによって、個人情報の一部（メールアドレス/氏名/会員 ID）が流出した可能性あるお客様に対してメールでの告知開始。

※この時点ではカード情報流出の事実は認められませんでした。

・2018 年 10 月 23 日

不正アクセスの原因究明のため、外部のセキュリティ専門の調査機関へ、本件に関する情報調査および今後の対応について相談を開始。

・2018 年 11 月 12 日

法人向け決済サービスのクレジット決済代行会社より、弊社サーバを原因としたカード情報流出の懸念があるとの指摘を受け、カード決済およびサイトを停止。

・2018 年 11 月 16 日

不正アクセスによって流出したお客様情報の特定や詳細な原因の究明などについて、クレジットカード情報のセキュリティ専門機関に依頼し、調査を開始。

・2018 年 12 月 6 日

外部のセキュリティ専門の調査機関より最終報告書を受領。

・2018 年 12 月 7 日

クレジットカード情報のセキュリティ専門機関より最終報告書を受領。流出の規模を確定させ、クレジットカード会社へ報告。以降、個人情報保護委員会へ逐次報告するとともにお客様へのご案内と事情説明の体制を整備開始。

・2018 年 12 月 25 日

本件サービスにて、調査報告に基づいた内容・再発防止策について公表。対象となるお客様に対してメールでの告知開始。

２.本件の対応について

（１）お客様対応

本件においてカード情報の漏洩の可能性があるお客様に対し、経緯のご説明、二次被害の注意喚起等を順次メールにて個別にご案内させていただいております。

また、以下のお問い合わせ窓口を設置いたしました。

＜お問い合わせ窓口＞

■専用ダイヤル：0120-790-230

■受付時間：9:30～18:30（土・日・祝祭日を含む）

（２）関係官庁への報告

監督官庁である個人情報保護委員会には不正アクセスの発覚以降、随時報告を行っております。

なお、先般の発表に引き続き、同委員会から不正アクセスに関する調査報告を逐次行うよう指導があり、適宜対応を行っております。

また、所轄警察である渋谷警察署にも 2018 年 12 月 4 日にクレジットカード情報漏洩に関する被害相談をしており、今後の捜査にも全面的に協力してまいります。

（３）クレジットカード会社への報告

カード情報の漏洩の恐れが発覚した 2018 年 11 月 12 日以降、法人向け決済サービスのクレジット決済代行会社に対して、判明した事実を適宜報告し、クレジットカード会社への連絡を行ってまいりました。また、専門機関の最終的な調査結果を 2018 年 12 月 7 日にクレジットカード会社に報告いたしました。

なお、不正利用の防止のため、流出の可能性がある対象カード番号につきましてはモニタリング強化を依頼しました。

３.お客様へのお願い

（１）利用明細のご確認

誠にお手数でございますが、2018 年 10 月 17 日 22 時 05 分から 2018 年 11 月 12 日 21 時 50 分までに本件サービスにおいて決済に利用されたクレジットカード及び「偽の決済フォーム」に入力された可能性のあるクレジットカードにつきまして、身に覚えのない利用履歴がないかどうかご確認ください。万が一、ご不明なお取引があった場合、まずはクレジットカードの裏面に記載のカード発行会社へお問い合わせくださいますようお願いいたします。なお、対象カード番号のクレジットカード再発行に伴う手数料につきましては、お客様にご迷惑がかからないよう、クレジットカード会社に依頼しております。

カード会社にご連絡の際は「DLmarket の個人情報流出の件」とお伝えください。

対象カード番号以外のクレジットカードの再発行をご希望される場合の手数料につきましては、各カード会社により対応は異なりますのでご注意ください。

（２）弊社からの本件に関するメールに、ファイルを添付することはございません。不審なメールについては、メール及び添付ファイルの開封を控えるなど、くれぐれもご注意くださいますよう、お願いいたします。

（３）お客様にお心当たりのない不審な点等がございましたら、弊社までご連絡をお願いいたします。警察機関・官庁と連携し、誠実に対応を進めてまいります。

４.再発防止策ならびに本件サービスの再開について

（１）本件サービスにかかるシステムのセキュリティ強化等

弊社は、被害拡大の防止のために本件サービスの提供を停止するとともに、本件の発生にかかる原因究明及び再発防止策を講じるため、内部調査に加えて専門・中立的な外部の調査会社に依頼して調査を進めております。

当該調査の結果を踏まえ、必要なセキュリティ対策を講じてまいります。

（２）本件サービスの再開

本件サービスの再開につきましては、（１）のセキュリティ対策の完了後とさせていただきます。決定次第改めてサイト上にてお知らせいたします。

５.今後の対応について

弊社は今後におきましても、二次被害防止を最優先事項と捉え、誠実に対応させていただく所存です。

万一、二次被害等が発生した場合におきましては、関係官庁ならびに警察機関との連携を取りながら対応を進めてまいります。

カード情報の漏洩の恐れが発覚した 2018 年 11 月 12 日から、必要な調査及びクレジットカード決済代行会社や関係官庁との連携による二次被害・再発防止に努めてまいりましたが、本日の発表までお時間がかかりましたこと、深くお詫び申し上げます。

正確な状況を把握しない段階でお知らせすることによって多くの混乱を招くことになるとのクレジットカード決済代行会社からの指摘を受け、当該クレジットカード決済代行会社に相談の上、詳細な調査を依頼している第三者機関の最終報告書をもってお知らせすることとさせていただきました。調査結果の精査および関係会社との調整に期間を要しましたことにつき、ご理解を賜れれば幸甚の限りでございます。

お客様におかれましては、ご不安のことと承知しており、また、当該サイトのご利用についてご迷惑をおかけしておりますこと、深くお詫び申し上げます。

６.本件に関するお問い合わせ窓口

＜お問い合わせ窓口＞

■専用ダイヤル：0120-790-230

■受付時間：9:30～18:30（土・日・祝祭日を含む）

※弊社からメールでご連絡させていただいているお客様は件名末尾の管理コードをお手元にご準備の上、お問い合わせください。