2022 年 6 月 30 日

クレジットカード番号等取扱業者に対する行政処分を行いました

経済産業省は、本日、割賦販売法に基づくクレジットカード番号等取扱業者である株式会社メタップスペイメント（法人番号 9011101027550）に対し、同法第 35 条の 17 の規定に基づく改善命令を発出しました。

1. 事業者の概要

(1)名称：株式会社メタップスペイメント（以下「同社」という。）
(2)代表者：代表取締役 和田　洋一
(3)所在地：東京都港区港南二丁目 16 番 1 号　品川イーストワンタワー7 階
(4)事業内容：決済代行業等

2. 処分内容

割賦販売法（昭和 36 年法律第 159 号。以下「法」という。）第 35 条の 17 に基づく改善命令

法第 35 条の 16 に規定するクレジットカード番号等の漏えい、滅失又は毀損の防止その他のクレジットカード番号等の適切な管理のために必要な措置として、以下の措置を講じること。

（1）同社が同社とクレジットカード決済に係る契約を締結しているクレジットカード等購入あっせん関係販売業者及びクレジットカード等購入あっせん役務提供事業者（以下「加盟店」という。）に対して提供するクレジットカード番号等による決済を可能とするサービスに係るシステム（以下「クレジットカード決済システム」という。）のうち、同社が保有するシステム（以下「自社システム」という。）について、クレジットカード番号等の漏えい事故の発生を防止するため必要かつ適切な措置として、クレジットカードのデータセキュリティに関する国際的な基準（以下「PCIDSS」という。）を適切に維持し、これを継続的に運用すること、及び、令和 3 年 10 月から令和 4 年 1 月までの間に発生したクレジットカード番号等の漏えい事故と類似の事故の再発を防止するため、第三者機関の検証を踏まえた再発防止策を速やかに策定し、実施すること。

（2）同社のクレジットカード決済システムのうち、PCIDSS 準拠を含むクレジットカード番号等の漏えい事故の発生を防止するため必要かつ適切な措置を講じていないものを確認し、当該措置を講じていなかった原因究明の結果を踏まえ、適切に PCIDSS を準拠及び維持し、これを継続的に運用することを含むクレジットカード番号等の漏えい事故の発生を防止するため必要かつ適切な措置を速やかに講じるこ

と。

(3)経営陣主導の下、システム及びセキュリティ対策に係る内部統制の強化を図り、同社のクレジットカード決済システムにおけるクレジットカード番号等の漏えい、滅失、毀損その他のクレジットカード番号等の管理に係る事故の発生を防止するため必要かつ適切な措置を講ずること。

(4)PCIDSS 監査に際し、監査機関に提出する報告書の改ざん等の不適正な業務の遂行を排除するため、クレジットカード番号等取扱業者としての健全な組織風土を醸成するとともに、内部監査機能の強化や業務の属人化の解消等の抜本的な業務運営体制の再構築を行い、第三者機関による業務運営の適正性の検証及び必要に応じた改善を行うこと。

(5)今般のクレジットカード番号等の漏えい事故の発生原因等を踏まえ、経営責任の所在を明確化するとともに、クレジットカード番号等の適切な管理に必要な経営体制の見直しを行うこと。

3. 処分理由

同社に対して行った法第 40 条の規定に基づく報告徴収命令に対する同社からの報告等から、以下の法第 35 条の 16 第1項に基づくクレジットカード番号等の適切な管理に違反している事実が確認された。

(1)同社は、加盟店に対して、顧客がクレジットカード決済により当該加盟店から購入した商品の代金又は提供を受けた役務の対価に係る立替金の交付を立替払取次業者から受け、当該加盟店に交付している。また、同社は、加盟店において顧客が決済に用いたクレジットカード番号等を立替払取次業者に提供している。したがって、同社は法第 35 条の 16 第 1 項第 4 号及び第7号に規定する事業者に該当する。

(2)同社のクレジットカード決済システム内のアプリケーションの脆弱性を起因とし、第三者による、自社システム内のクレジットカード番号を閲覧するための管理画面への不正ログインのほか、SQL インジェクション攻撃及びバックドアの設置を実施されたことにより、令和 3 年 10 月から令和 4 年 1 月の間、当該クレジットカード決済システム内のデータベースに保存していた暗号化されたクレジットカード番号(マスキングされたクレジットカード番号を含む。)、有効期限、セキュリティコード及びこれらを復号化するための復号鍵が窃取され、また、クレジットカード番号が不正に閲覧されることにより、クレジットカード番号等が漏えいした。漏えいの対象となったクレジットカード番号等が保存されていたデータベースのテーブルは 2 つあり、それぞれ

460,395 件、2,415,750 件の暗号化されたクレジットカード番号等が保存されていた。

(3)同社は、平成 30 年 6 月、同社とコンビニ決済に係る契約を締結していた加盟店にサービスを提供するために開発、運用していたアプリケーション(以下「加盟店向けアプリ」という。)を委託先事業者のシステムから同社のクレジットカード決済システム内に移設している。当該加盟店向けアプリの移設に関しては、代表取締役に稟議が通されており、組織決定されたものではあるが、社内のシステム関係部署及び職員に当該事実について的確に情報共有されていなかった。このため、当該加盟店向けアプリ移設以降に受けた PCIDSS 監査において、同社から PCIDSS 監査機関に対し、クレジットカード決済システム内に当該加盟店向けアプリが移設された事実を伝えておらず、当該加盟店向けアプリは当該監査の対象とはされなかった。
また、同社は、平成 30 年から令和 3 年の間に実施した PCIDSS で求められている WEB アプリケーション(自社システムの管理画面を含む。)の脆弱性診断を診断ツールを用いて自社で実施し、「High」「Medium」レベルの脆弱性が複数検出されていたにもかかわらず、当該脆弱性診断の報告書ではこれらの脆弱性をなかったものに改ざんし、平成 30 年から同社が法第 35 条の 16 第 1 項第 4 号及び第 7 号に規定する事業者に該当することとなった令和 3 年の PCIDSS 監査に際し、改ざんした報告書を監査機関に提示又は提出していた。

さらに、同社は令和 2 年 7 月から令和 3 年 10 月の間に実施した PCIDSS で求められている自社システムのサーバーを対象としたネットワーク脆弱性スキャンをスキャンツールを用いて委託先で実施し、「High」レベルの脆弱性が複数検出されていたにもかかわらず、当該脆弱性スキャンの報告書では、「High」レベルのうちシグネチャ未更新に関する脆弱性をなかったものに改ざんし、令和 2 年及び同社が法第 35 条の 16 第 1 項第 4 号及び第 7 号に規定する事業者に該当することとなった令和 3 年の PCIDSS 監査に際し、改ざんした報告書を監査機関に提出していた。

なお、WEB アプリケーション脆弱性診断の報告書の改ざんについては、担当職員から情報セキュリティ管理担当役員に報告がなされており、ネットワーク脆弱性スキャンの報告書の改ざんに関しては、情報セキュリティ管理担当役員が改ざん前及び改ざん後の報告書の承認をしていた。しかしながら、これらの役員から他の経営陣に対して、これらの脆弱性が検出された事実及び PCIDSS 監査に当たって提出する報告書が改ざんされた事実の報告は行われていなかった。

また、社内の内部監査機能が働くこともなく、当該役員以外の経営陣はこれらについて認識せず、今般のクレジットカード番号等の漏えい事故に係る第三者による原因究明の結果、初めて事実を把握したものである。

このため、同社はクレジットカード決済システムが適確に PCIDSS を準拠するための措置を講じていなかった。なお、今般のクレジットカード番号等の漏えい事故は、当該加盟店向けアプリの脆弱性を原因とした SQL インジェクション攻撃及びバック

ドア設置が一因となっている。

加えて、クレジットカード決済システムにおける不正アクセスの検知や防御対策の不備があったほか、データベースが適切に分離されていない、自社のシステムのアプリケーションやネットワークの脆弱性診断を適切に実施せず、また検出された脆弱性に適切に対応しないなど基本的なセキュリティ対策が実施されておらず、クレジットカード番号等が十分に保護されるよう適切に管理されていなかった。

このため、同社は法第 35 条の 16 第 1 項に規定する割賦販売法施行規則（昭和 36 年通商産業省令第 95 号。以下「省令」という。）第 132 条第第 1 号及び第 4 号に定める基準に従ったクレジットカード番号等の適切な管理のために必要な措置を講じていたとは認められない。

（4）また、同社は、クレジットカード決済システムのうち、少なくとも「会費ペイ」に係るシステムについては、令和 4 年 5 月まで PCIDSS に準拠しておらず、「イベントペイ」に係るシステムについては、PCIDSS に準拠していない。このため、同社は法第 35 条の 16 第 1 項に規定する省令第 132 条第 1 号に定める基準に従ったクレジットカード番号等の適切な管理のために必要な措置を講じていたとは認められない。

（5）同社の自社システムにおいては、システム担当部署で、クレジットカード決済システムの運用に関する状況について関係役職員に的確な情報共有がされず、システム運用に係る業務の遂行状況の記録がされていない状況、及び同社のクレジットカード決済システムの運用監視において、発生したアラートの全件を確認しない状況が継続していた。また、令和 3 年 10 月に加盟店向けアプリの管理画面に SQL インジェクション攻撃があったことを認知したが、速やかにフォレンジック調査等の原因究明を実施しなかった。

このため、同社は、法第 35 条の 16 第 1 項に規定する省令第 132 条第 1 号及び第 2 号に定める基準に従ったクレジットカード番号等の適切な管理のために必要な措置を講じていたとは認められない。

（本発表資料のお問合せ先）
商務・サービスグループ商取引監督課