2022 年 6 月 29 日

株式会社メタップスペイメント　御中

# 第三者委員会

# 調査報告書

# （公表版）

委員　　右　崎　大　輔

委員　　大河内　貴　之

（注）本書においては、セキュリティリスクを含む各種リスクを踏まえて、固有名詞や具体的な事実関係に係る記載を省略している部分がある。

目次

# 第１章　当委員会及び本調査の概要

## 第１　当委員会の設立経緯等

MP のホームページで公表されている 2022 年 2 月 28 日付け「不正アクセスによる情報流出に関するご報告とお詫び」に記載のとおり、MP が運営する決済システムにおいて第三者による不正アクセスが確認され、カード情報及び個人情報が流出した。

MP は、本件事象への対処を目的として、2022 年 2 月 25 日、役員に外部の専門家アドバイザーを加えたメンバーで構成される再発防止委員会を設置した。再発防止委員会においても、本件事象に係る事実関係の調査を行っているが、最終的な原因究明に至っていない。

このような状況を踏まえ、再発防止委員会において、本件事象に係る事実関係の調査等のためには、客観的かつ専門的で、公正性及び透明性を有した機関による調査が必要との判断がなされ、当委員会の設立に至ったものである。

当委員会は、MP 及び同社内の再発防止委員会とは独立しており、客観的かつ専門的で、公正性及び透明性がある調査等を行うための第三者機関である。

なお、本報告書において使用される用語の意味は、別途定義する場合を除き、末尾用語一覧による。

## 第２　当委員会の目的

当委員会は、本件事象に係る事実関係を解明することを第一の目的とし、次いで判明した事実関係を基に原因を追及することを第二の目的とする。

さらに、事実関係及び原因に照らして、MP における再発を防止するための方策を提言することを第三の目的とする。

## 第３　調査事項

当委員会が MP より委嘱を受けた本件事象に係る調査事項は、以下のとおりである。

１　事実関係の調査

２　原因の究明

３　再発防止策の提言

４　調査報告書の作成及び当該調査報告書の MP への提出

## 第４　当委員会の委員

当委員会の構成は、以下のとおりである。

| | | |
|---|---|---|
| 委　員 | 右　崎　大　輔 | 片岡総合法律事務所（弁護士） |
| 委　員 | 大河内　貴　之 | Secure･Pro 株式会社　代表取締役 |

当委員会は、本調査を実施するに際して、以下の５名を調査補助者として任命し、本調査の補助に当たらせた。

| | |
|---|---|
| 片岡総合法律事務所 | 弁護士　福　田　隆　行<br>弁護士　柳　原　悠　輝<br>弁護士　小　柏　光　毅<br>弁護士　廣　見　光二郎<br>弁護士　近　岡　裕　輔 |

**第５　調査期間**

2022 年 4 月 7 日から同年 5 月 31 日まで

**第６　調査方法**

１　当委員会は、本報告書の作成にあたり、次の方法に基づいて調査を実施し、上記調査期間内で開示された情報の範囲内で、その情報の真正及び正確性を前提とした。

⑴　役職員（MP 退職者を含む。）に対するヒアリングによる調査

⑵　関係資料（規程類、議事録、稟議書、監査資料、報告書、slack でのやり取りを含む。）の精査

２　なお、本件事象は、決済システムに対する第三者による不正アクセスに関連するものであり、MP におけるシステム環境の脆弱性等を前提にした事象であったことから、「システム環境の観点」からの事実関係の調査、原因の究明、再発防止策の検討（以下、まとめて「調査等」という。）が必要であり、この観点からの調査等については、主として、Secure･Pro 株式会社　代表取締役である大河内委員が担当した。

また、本件事象は、MP におけるシステム環境の脆弱性の発生を未然に検知又は防止できる体制が欠如していた疑いや、本件事象発生時における対応が不適切であった疑いがあり、人的環境面（体制整備面）での問題も疑われたため、「人的環境の観点（体制整備上の観点）」からの調査等も必要であり、この観点からの調査等については、主として、片岡総合法律事務所所属弁護士である右崎委員及び同事務所所属の調査補助者が担当した。

このように２つの観点からの調査を行ったことを受けて、本報告書の一部においては、「システム環境の観点」からの調査等と「人的環境の観点（体制整備上の観点）」からの調査等とを区別して記載している。

## 第２章　MP の事業概要等

当委員会が本調査の前提とした MP の事業概要等は、以下のとおりである。

### 第１　事業内容

| 大分類 | 小分類 | 概要 |
|---|---|---|
| 決済事業 | Web 決済 | EC 市場における各種決済サービス |
| | リアル店舗決済 | 実店舗における各種決済サービス |
| | 不動産決済 | 賃貸不動産市場における各種決済サービス |
| パッケージソリューション事業 | 会費ペイ | フィットネスジム・スクール等の会員管理・決済サービス |
| | イベントペイ | セミナー・学会・オンラインイベント等のチケット販売・管理サービス |
| | チケットペイ | 音楽・舞台・スポーツ・エンタメ等のチケット販売・管理サービス |
| トラスト事業 | CRIA（クリア） | 求人応募数や定着率向上を支援する給与即時払いサービス |

### 第２　システム概要

MP は、その提供する加盟店向けパッケージサービスに関して、①クレジットカード決済、コンビニ決済、電子マネー決済等の各種決済を行う「決済システム」と、②イベントペイやチケットペイ、会費ペイなど、決済自体は行わずにサービスのパッケージとして提供する「フロントシステム」の二つのシステムを保有している。

「決済システム」は、実際にカード会員のカード情報を取り扱うことから、PCI DSS に準拠したデータベース（東京 DC）内に格納されているのに対し、後者の「フロントシステム」は、クラウドサービス（2018 年までは$\alpha$クラウド、同年以降は$\beta$クラウド）に格納されており、データベースの分離が図られている。

### 第３　役職員数

2022 年 3 月 1 日時点における MP の役職員数は、合計 88 名（役員 4 名、従業員 83 名、業務委託 1 名）である。

## 第３章　本件事象に係る時系列

当委員会が本調査により確認した本件事象に係る時系列の詳細は、別紙時系列表のとおりである。

## 第４章　システム環境の観点からの事実認定

### 第１　情報漏えいの要因

PCF レポート及び MP が経済産業省向けに作成した各種報告書記載の時系列及びヒア

リング結果やその際に提供されたキャプチャー画面等の資料からすれば、情報漏えいの経緯は別紙時系列表のとおりであるが、その大きな要因としては、おおよそ以下の5つがあると考えられる。

**１　K管理画面のアカウント情報の取得及び不正アクセス（別紙時系列表①）**

攻撃者は、K管理画面のクロスサイト・スクリプティングに関する脆弱性を悪用し、データベース内に格納されていた管理者のアカウント情報（UserID、パスワード等）を取得し、K管理画面内の不正操作を行っていたと考えられる。

具体的な管理者のアカウント情報の取得方法については、別紙時系列表に記載のとおりの可能性が考えられる。

「X氏」のアカウント情報を用いたK管理画面内の不正操作については、フル桁のカード番号の参照可能な画面に到達しているログが無いことからすれば、カード情報の漏えいがあったとは認められず、そうだとすると、不正操作によって、K管理画面の構造などを調べていたと考えられる。

なお、UserID「X氏」に係る従業員は、2021年9月末から10月初旬にアカウント情報に係るパスワードの変更を行っており、それ以降、UserID「X氏」を利用した不審なIPアドレスからのアクセスは、「history log」を精査したが不見当であったため、UserID「X氏」を利用したアクセスは、2021年10月初旬以降はないと考えてよい。

その後、同様の手口を用いて「Y氏」のアカウント情報を得て、2021年10月6日以降に不正アクセスを行ったと考えらえる。

**２　SQLインジェクション攻撃（別紙時系列表②）**

攻撃者は、2021年10月14日から2021年10月27日に渡り、A社アプリに対するSQLインジェクション攻撃により、暗号化されたカード番号、マスクされたカード番号及びA社管理画面の管理者アカウント情報をそれぞれ不正取得した。

**３　バックドアプログラムの設置及び攻撃（別紙時系列表③）**

攻撃者は、2021年10月15日、A社管理画面に一度不正アクセスしているが、更に2021年11月11日、A社管理画面に不正アクセスを行い、A社アプリの管理機能の一つであるファイルアップロード機能を悪用し、バックドアプログラムを設置した。

そして、不正ファイル経由で、データベース内から、暗号化されたカード情報を含む当時格納されていた全ての情報を不正取得したと考えられる。

**４　K管理画面への再度の不正アクセス及びカード番号照会開始（別紙時系列表④）**

攻撃者は、2021年10月25日から同年12月14日までに渡り、UserID「Y氏」の情報等を用いて、再度、K管理画面に不正アクセスを行った。

そして、この頃までに、攻撃者は、上記 SQL インジェクション攻撃及びバックドアプログラムにより、既にデータベースからマスクされたカード番号を不正取得しており、K 管理画面上で不正取得したマスクされたカード番号を検索照会することによって、平文のフル桁のカード番号を閲覧することができたと考えられる。

**５　バックドアプログラム経由での攻撃の収束（別紙時系列表⑤）**

上記のとおり、不正ファイルを経由してデータベース内の暗号化されたデータやアプリケーションログからデータが不正取得されたものの、2022 年 1 月 25 日、バックドアとなる対象プログラムを全部削除した。

## 第５章　人的環境の観点（組織体制上の観点）からの前提となる事実認定

システム環境以外の直接的な原因及び間接的な要因（背景要因）を認定するに際して前提とした MP の組織体制は、概要以下のとおりである。

### 第１　一般的な組織体制

**１　沿革**

| | |
|---|---|
| 1999 年 3 月 | 株式会社デジタルチェックとして設立 |
| 2005 年 4 月 | ISMS（Ver2.0）認証取得 |
| 2006 年 4 月 | プライバシーマーク取得 |
| 2008 年 3 月 | PCI DSS 1.1 準拠（以下、PCI DSS のバージョンアップに伴う準拠の途中経過は省略する。） |
| 2014 年 1 月 | 商号をペイデザイン株式会社に変更 |
| 2014 年 12 月 | ISMS（ISO/IEC 27001:2013 / JIS Q 27001:2014）移行完了 |
| 2016 年 4 月 | 株式会社メタップスの完全子会社化 |
| 2017 年 12 月 | 商号を株式会社メタップスペイメントに変更 |
| 2018 年 12 月 | PCI DSS 3.2.1 準拠 |

**２　システム部・IT 推進部**

2015 年 4 月以前から決済システムの企画・構築・運用・保守・改善・改修を所管する部署として「システム部」（部長：甲氏）があり、同部は、開発グループ、商用インフラグループ、運用グループ及びシステム管理グループの 4 グループによって構成されていた。なお、上記のうちシステム管理グループは、2017 年 6 月に総務部（部長：地井良太氏）に移管されている。

2019 年 9 月にシステム部門の組織強化・効率化等を目的として、システム部と営業企画部（部長：増沢将秀氏）のシステムグループを統合して「IT 推進部」とした。なお、それ以降、同部は、決済システムグループとサービス開発グループの 2 グループによって構成されている。

**３　内部管理部門**

2015 年 4 月以前から管理本部（本部長：地井良太氏）があり、同本部は、総務部、

経理財務部、法務部及び営業管理部の 4 部によって構成されていた。

2018 年 9 月に管理部門は「本部」から「部」に変更され、管理部は、総務グループ、経理財務グループ、営業管理グループ、カスタマーサポートグループの 4 グループによって構成されることとなった。なお、上記のうちカスタマーサポートグループは、2021 年 1 月に営業本部（本部長：増沢将秀氏）に移管されている。

**4　内部監査担当**

2010 年 3 月から内部監査制度の確立・運営・改善を所管する社長直属の機関として内部監査担当（1 名）がおり、2016 年 8 月以降は親会社である株式会社メタップスの内部管理部の部長が内部監査担当を兼務している。

**5　監査役**

2015 年 4 月以前から監査役会設置会社であったが、株式会社メタップスの完全子会社となって同社の内部統制に服することを踏まえて、2016 年 6 月に監査役会を廃止した。

**6　取締役及び代表取締役**

本報告書の関係で明らかにする必要がある取締役の主要な経歴等は、以下のとおりである（敬称略）。

| 氏名 | 役職 | 期間 |
|---|---|---|
| 和田　洋一 | 代表取締役 | 2017 年 10 月　～　現在 |
| 増沢　将秀 | 取締役 | 2016 年 10 月　～　現在 |
| | 営業本部長／事業本部長 | 2014 年 2 月　～　現在 |
| | 情報セキュリティ管理体制上の代表者 | 2017 年 11 月　～　現在 |
| 甲 | 取締役（※） | 2008 年 6 月　～　2020 年 9 月 |
| | システム本部長／システム部長／IT 推進部長 | 2008 年 2 月　～　2020 年 7 月 |
| | 情報セキュリティ管理体制上の IS 責任者 | 2014 年 8 月　～　2020 年 7 月 |
| 地井　良太 | 取締役 | 2016 年 10 月　～　現在 |
| | 管理本部長／管理部長 | 2015 年 4 月　～　現在 |
| | 情報セキュリティ管理体制上の IS 監査責任者 | 2018 年 11 月　～　2020 年 6 月 |
| | 情報セキュリティ管理体制上の IS 責任者 | 2020 年 7 月　～　現在 |

※　2008 年 10 月からは CIO（情報統括役員）

## 第２　情報セキュリティ及びリスク管理に関連する組織体制

本件事象に関連する 2021 年 8 月から 2022 年 1 月までの期間における MP の情報セキュリティ及びリスク管理に関連する組織体制は、概要、以下のとおりである。

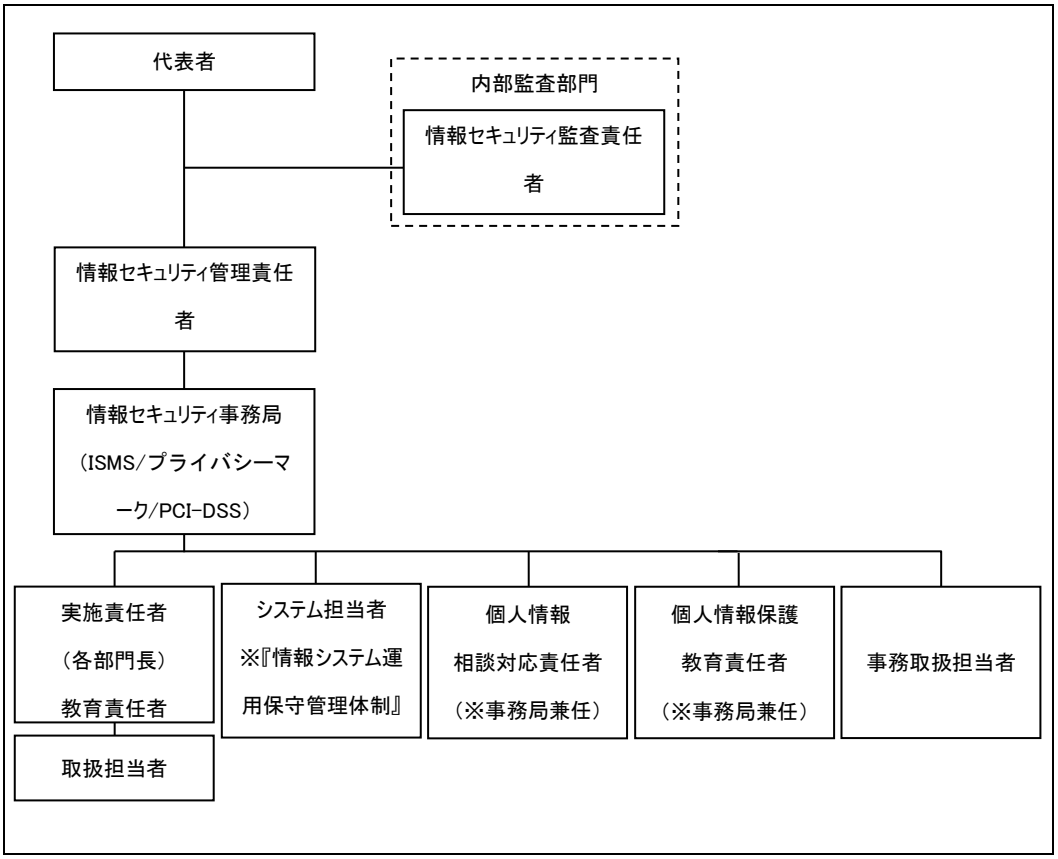
### １　関連する社内規定類

MP では、情報セキュリティ及びリスク管理に関連する社内規程として、「リスクマネジメント基本規程」、「情報セキュリティ基本規程」、「情報セキュリティ実施要領」、「コンプライアンス基本規程」等が整備されている。

### ２　リスク管理

まず、MP における一般的なリスク管理に関する事項は、リスクマネジメント基本規程により規律されており、そこでは、各部門において把握されたリスクについてコンプライアンス委員会が内容を検討し、対処を指示することとされている。そして、MP において想定され得る各種リスクの中でも、とりわけ、決済システムの正常な運用やセキュリティ保持を阻害するリスク（以下、「情報セキュリティリスク」という。）については、特に重要なリスクとして認識されており、当該リスクについては、「情報セキュリティ基本規程」等に基づく管理体制を構築し、決済システムの予期せぬ停止や、漏えい、滅失、毀損等の情報管理に関わる事故の発生を防止することとされている。

これを受けて、情報セキュリティ基本規程により、情報セキュリティ体制として以下の体制が構築されており、それぞれの責任及び権限が定められている。




## ３　コンプライアンスとの関係

また、コンプライアンス基本規程上は、MP におけるコンプライアンスの維持・向上を推進するためにコンプライアンス委員会を設置することとされており、そこでコンプライアンス上の問題に対応することとされているところ、情報セキュリティに関する重要な問題は、コンプライアンスに関わる問題として取り扱うこととされている。このことから、結局、コンプライアンス委員会は、社内規程上は、コンプライアンス及びリスク管理の二つの側面から情報セキュリティに関わる問題を主管するものとして位置付けられているものと理解される。

## ４　情報セキュリティに係る監査

MP においては、内部監査規程に基づく内部監査担当による監査の定めのほか、ISMS や PMS の観点からの、情報セキュリティ監査責任者による個人情報保護マネジメントシステム（JISQ15001）、情報セキュリティマネジメントシステム（JISQ27001）及び PCI DSS 要件に基づく内部監査に関する規律が定められている。

## ５　小括

MP の社内規程上は、以上のとおり、情報セキュリティリスクの管理及び監査に関して一定の管理体制が構築されていたといえる。

もっとも、MP における実際の業務運営においては必ずしも実態が伴っていない部分が見受けられ、以下第 7 章において詳述するとおり、ルールの形骸化や体制の機能

不全等の各種問題が認められた。

## 第６章　システム環境の観点からの直接的な原因

### 第１　ログの日次点検の不実施

PCI DSS 要件では、「ネットワークの定期的な監視及びテスト」として、ネットワークリソース及び会員データの全てのアクセスを追跡及び監視することが求められており、具体的にはログの日時点検を実施すべきである。

しかし、これらの点検が行われていなかった。

### 第２　セキュアコーディングの不備

カード情報を扱うサービスプロバイダーにおいては、たとえ PCI DSS に準拠していたとしても、インターネット経由でアクセス可能なサイトには強固なセキュリティ対策が求められる。特に本件では、同一サーバ内で同等のセキュリティ対策が求められる。本件では、SQL インジェクション攻撃に対する脆弱性の他にも PCI DSS 要件に記載されている脆弱性（クロスサイト・スクリプティングなど）のアプリケーション構築レベルでのセキュリティ対策に不備があった。

### 第３　ペネトレーション診断の不備

MP のウェブサーバにおいては、決済システム直下に A 社アプリが存在するため、ペネトレーション診断の対象であるとされている。

もっとも、上記にもかかわらず、A 社アプリについては、2017 年以降 5 年間にもわたり診断の対象とされていなかったと認められる。ペネトレーション診断に係る報告書では、一定の診断を実施した旨の報告がなされているが、どの遷移を診断したのか、また、どの様に診断対象を特定していたかなど、診断を実施する前提条件が明らかではなく、実施担当者を含む関係者においても明確に意識されていなかったと考えられる。

### 第４　WAF の未導入

本来は、多重的重層的にファイアウォール、IPS 又は WAF の導入等をして、全体的なセキュリティレベルを相互補完する構造とすることが一般的である。たとえ本章第 2 のセキュアコーディングの不備や本章第 3 のペネトレーション診断の不備等の問題があったとしても、WAF が導入されていたとすれば、これによる検知ないし防御がなされ、既知の脆弱性を利用した不正アクセスのリアルタイム検知ないし防御ができていた可能性がある。

### 第５　データベーススキーマの未分離

SQL インジェクション攻撃に対する脆弱性を利用されてデータベースに攻撃を仕掛

けられ、A 社アプリから A 社管理画面内の ID 及びパスワードを不正取得されたとしても、それ以後にデータが不正取得される範囲は、A 社アプリのデータベース内のデータにとどまるはずであった。

しかしながら、本件事象に係るウェブサーバにおいては、データベーススキーマが分離されていなかったため、A 社アプリのデータベース内のデータにとどまらず、暗号化されたカード番号が格納されたデータベースへの不正アクセスをも許し、当該暗号化されたカード番号を不正取得されるに至った。

### 第６　様々なセキュリティアラートに対する検証などの運用要員不足と影響範囲の調査不備

本章第 2 から第 4 までの不備があったとしても、セキュリティアラートの検証等の方法により、攻撃経緯と影響範囲の調査が出来ていれば、不正侵入を未然に防止する可能性があった。

PCI DSS では、様々なセキュリティ商材の導入等が要件とされており、MP においてもセキュリティアラートが導入されていたが、セキュリティアラートの検証等の方法により、攻撃経緯と影響範囲の調査がなされていなかった。

### 第７　インターネット経由で K 管理画面へのアクセス制限とログイン認証の不備

上記のとおり、本件においては、SQL インジェクション攻撃に対する脆弱性を悪用されて、A 社管理画面の ID とパスワードを不正取得され、K 管理画面より不正アクセスされた事実が認められるが、不正ファイルのアップロードがなされたのは 2021 年 11 月 11 日のアクセスのときである。

したがって、仮に SQL インジェクション攻撃に対する脆弱性を確認した時点（2021 年 10 月 25 日）で影響範囲を特定できていれば、不正アクセスされないようにアクセス制限の実施や不正取得された ID に対するパスワードの変更等の対応を実施することができた。

### 第８　侵入された場合の対策の不備

本来、ファイル整合性監視などの侵入検知サービスは、外部や内部攻撃者から不正侵入がされた後にアプリケーションの改ざんや不正ファイルをアップロードされた場合に、初めてサービス利用者に対して「気づき」を与える仕組みである。

上記のとおり、MP においては、セキュリティアラートの導入自体は実施されていたと認められるが、当該セキュリティアラートが適切に作動し、適時のタイミングで適切なアラートが発信されていなかった可能性がある。

また、仮に当該セキュリティアラートが適切に作動していたとしても、担当者において、当該アラートを日常的に確認することはなく、またそもそも当該アラートを受信す

る者の範囲も不明確であるなど、セキュリティアラートを検知し適切な対応をする人的な環境も整っていなかった。

### 第９　サーバ内のアプリケーションの管理の不備

本章第 2 から第 7 のそれぞれの原因に有機的かつ複合的に関連し、うち本章第 5 のデータベーススキーマの未分離に強く関連するが、Web2 系に暗号化されたカード情報に係る復号化サーバが配置されていた。Web2 系には、決済システムも配置されており、そこで暗号化されたカード情報も管理されていた。

### 第 10　影響範囲の特定の不備

本件事象が発生した決済システムは、PCI DSS 準拠対象範囲内であるものの、その構成上、情報漏えいなどの事象が起こった際にその影響範囲が特定できるシステムが未導入であった。

### 第 11　推測しやすいＡ社管理画面のファイルパスやアップロード機能の設定不備など

本件においては、A 社管理画面は推測されやすい管理画面のファイルパスであり、また、アップロード機能を有していた為、管理画面が推測される可能性はもともとあったと考えられ、管理画面内に不正アクセスされるとファイルにアップロード機能の設定の不備により、想定以外のファイルをアップロード可能だった為、バックドアプログラムを設置されていた。

## 第７章　人的環境の観点（組織体制上の観点）からの直接的な原因

### 第１　クロスサイト・スクリプティングの脆弱性についての意図的な変更

MP においては、「γツール」という診断ツールを用いて K 管理画面を対象とした脆弱性診断を実施しているところ、当委員会の調査において確認できた限りでも、少なくとも 2018 年から 2021 年まで当該脆弱性診断に係るレポートに対し意図的な変更が加えられていた。

真正なレポートにおいては、「High」や「Medium」レベルの脆弱性が検出されていたところ、変更後のレポートにおいては、それら脆弱性が検出されていないかのような記載に修正され、当該変更後のレポートが真正なものとして取り扱われていた。特に、2020 年及び 2021 年に実施された脆弱性診断では、クロスサイト・スクリプティングに対する脆弱性が検出されていたが、当該脆弱性も検出されていないかのようにレポートの記載が変更されていた。

MP の従業員によれば、2018 年 10 月 25 日に開催されたシステム部の部会において、

上記変更を行っていた同部の担当者が上記レポート変更の事実及びシステムの脆弱性について当時の部長であった甲氏を含む部員に報告したものの、同部会においては、具体的な改善が命じられることもなく、結果的に上記対応が容認されることとなったとのことである。この点について、同部の部長であった甲氏は、当該事実につき認識がないと否定するものの、変更の期間が少なくとも 2018 年以降からと長期にわたること及び当時のシステム部の所属人数からすれば同人の認識がないというのは不自然であり、仮に真に認識がないとしても取締役としての重大な任務懈怠があると考えられる。

上記のような取扱いがなされた理由については、上記脆弱性診断の対象である K 管理画面は PCI DSS の準拠対象とされており、K 管理画面について脆弱性が存在する場合には、MP の決済事業のために必須な PCI DSS の認証が維持できなくなる一方で、脆弱性を修正するための人的リソースの不足や過剰なコスト削減の意識などから、上記脆弱性を修正するのではなく、脆弱性自体をなかったことにすることにより PCI DSS の認証を維持しようと考え、上記のようなレポートの意図的な変更が行われていたものと推測される。

その後、2019 年以降も担当者から他の部員に対して上記脆弱性を解消するために必要なシステムのアップデート等を行うよう要請はなされていたものの、時間やコストを理由に必要な対応はなされなかった。

以上のとおり、本件事象が発生する 1 年以上前より、本件事象のきっかけとなったクロスサイト・スクリプティングに対する脆弱性が検出されていた。MP においてクロスサイト・スクリプティングの脆弱性についての変更がなされず、IT 推進部（システム部）として当該脆弱性の存在を受け止め、事前に脆弱性の修正がなされていれば、本件事象の発生を防ぐことができた可能性が高いと考えられる。

## 第２　A 社アプリの東京 DC への移管

第 2 章第 2 で述べたとおり、MP が保有するシステムは、「決済システム」と「フロントシステム」に分けられるところ、本件事象の発生原因の一つとなった脆弱性を有する A 社アプリは、機能的にフロントシステムに係るアプリケーション（以下「フロント系アプリ」という。）に位置付けられるものであるため、2018 年までは、αクラウドにおいて格納されていた。

しかしながら、以下での述べるとおり、MP は、2018 年に A 社アプリをαクラウドから切り離し、決済システムが格納されている東京 DC への移管を実行した。

### １　A 社アプリの東京 DC への移管の経緯及び理由等

αクラウドにおいては、2017 年ころから定期的にシステムの不具合やサービス障害が生じていた。そこで、これらの問題の改善その他の必要性に迫られて、A 社アプリをαクラウド及び他のフロント系アプリから切り離すことになったという経緯があり、その判断自体は特に不合理な点は見当たらない。

問題は、αクラウドから切り離したA社アプリの移管先として東京DCを選び、実行した点である。すなわち、本来、フロント系アプリのA社アプリを、カード会員のカード情報を取り扱う決済システムと同じデータベースに格納することは、情報セキュリティリスクの観点からは有り得べからざる対応であり、実際、本件事象による情報漏えいも、東京DC内のA社アプリの脆弱性が突かれたことを発端の一つとしている。

この点に関し、A社アプリの移管先を東京DCと定め、実行したのは、当時システム部の部長であり、システム関係を所管する取締役でもあった甲氏とされている。同氏へのヒアリング結果によれば、αクラウドから切り離す必要が生じたA社アプリの移管先については、本来それ専用の独立した環境を構築することが最善ではあったものの、インフラ運営費用の問題で現実的には難しかったため、差し当たりの「一時的」な対応としてどこか既存のデータベースに入れ込む必要があったとのことである。また、その際に東京DCが選ばれた主要な理由としては、東京DCがA社アプリと同じJavaで構築されているため、サービスの安定性を考慮した場合にそれが現実的であろうと判断されたためとのことである。

なお、甲氏のもともとの想定では、随意のタイミングで他のフロント系アプリと同じβクラウドに移す予定であったとのことであるが、実際は、A社アプリは、本件事象発生時に至っても、そのまま東京DC内で運用され続けていた。

## ２　A社アプリの東京DCへの移管に係る問題点等

上記のとおり、2018年のA社アプリの東京DCへの移管に関しては、主に費用面の理由やサービス安定性の観点から東京DCが選ばれたとのことであり、その際に、本来であれば第一に目を向けるべき情報セキュリティリスクがMPのシステム関連所管部門や経営陣等において具体的に検討され、又は対策等が採られた形跡は見当たらない。

また、仮にA社アプリにおいてSQLインジェクション攻撃を許すような脆弱性が存在していなければ、本件事象の発生は防げた可能性も残るが、第8章第1で述べるように、A社アプリに関してはその開発時のみならず、2018年の東京DCへの移管時も、ソースコード・レビュー等による安全性の確認措置は採られていない。

さらに、当初は東京DCへの移管が「一時的」なものとの想定であったという点に関しても、甲氏以外の役職員がこれを明確に認識していた様子はなく、むしろ実態としては、本件事象が起こるまで、2018年以降A社アプリが東京DC内に格納されていたこと自体把握していなかったという役職員が大半であったこともあり、MP内において、実際にA社アプリの再移転に関する検討等が進められた様子もない。

以上の一連の事象は、PSI DSS準拠やISMS認証を取得した上で、その業務においてクレジットカード会員のカード情報を大量に取り扱うPSP事業者としての判断ないし対応としては、杜撰なものであったと言わざるを得ず、第8章で触れるような、

MP の情報セキュリティリスクに対する体制上の牽制不備や、役職員のリスク認識の低さを指し示す事象の一つであるといえる。

## 第３　本件事象が発生した後の被害防止対応の不十分性

本件事象が発生した後、これによる情報漏えいの発生、あるいはその被害の拡大を防止し得たタイミングとして、

① SQL インジェクション攻撃を受けていることを MP が認識した 2021 年 10 月、

② 各カード会社からの報告によりカード情報の不正利用が生じている可能性が発覚した同年 12 月、

③ 決済システムからの情報漏えいの事実を認識した 2022 年 1 月

の 3 つの時点を挙げることができる。

しかしながら、MP においては、以下で述べるとおり、各時点において必要十分な対応が採られておらず、そのことが程度の差こそあれ、本件事象による情報漏えいないしその被害の拡大に繋がったものと考えられる。

### １　2021 年 10 月の対応不十分

⑴ 別紙時系列表のとおり、本件事象の発端として、2021 年 10 月 14 日に A 社アプリに対する SQL インジェクション攻撃が開始されたことが判明しているが、MP では、同月 25 日に対象システムの定期メンテナンスを実施した際に、たまたまではあるものの、担当者が当該 SQL インジェクション攻撃に気が付き、上長に報告を上げている。また、その際には、当該攻撃に係る情報量が日常的に発生する不正アクセスに比べて大きかったため、情報漏えいの有無を判断すべく、ログ調査を外部に依頼した方が良いのではとの意見も現場から出されていた。

実際、この時点で外部にログ調査を依頼していれば、それにより情報漏えいの事実ないしリスク等を発見できていた可能性があり、その後の本件事象の発生あるいは被害の拡大を防止できた可能性がある。

⑵ しかしながら、担当者から SQL インジェクション攻撃の報告を受けた当時の IT 推進部の副部長は、いわゆる 500 エラー（プログラム自体へのアクセスはなされているが、実行できず処理が完了しない場合に発生するエラー）の発生を確認したことで、これを根拠に外部への情報漏えいはないと考えた。そのため、外部にログ調査を依頼することまでは不要と考え、ただ用心として、攻撃者の IP アドレスをファイアウォールでブロックした上で、同月 27 日に SQL インジェクション攻撃についての解析結果に基づき文字列処理ロジックを強化し、更新プログラムをリリースすることにより脆弱性を修正することで対応としては十分だと判断した。なお、MP において、不正アクセスを探知した際の対応として、特定の IP アドレスをファイアウォールでブロックしたのはこれが初めてだったとのことである。

また、経営陣は、SQL インジェクション攻撃を受けていたことやその対策方針等

について、同副部長から報告を受けていたが、当該報告を受けた際にSQLインジェクション攻撃の対象が決済システムに係るデータベースが保管されている東京DCであることを踏まえた問題意識を有した形跡はないし、その時点及びその後直近の経営会議や取締役会の場においても、攻撃の対象が東京DCであったことを踏まえて、上記対応の十分性やリスクについての追加の確認その他の実質的な検討等がなされた形跡はない。

すなわち、2021年10月のSQLインジェクション攻撃の存在が判明した時点における経営陣の対応としては、同副部長からの報告をそのまま了承し、是認するにとどまっており、本来経営陣はじめ全社的に対応に当たるべき情報セキュリティリスク顕在時の対応に関しては、社内の一部門に過ぎないシステム部門に全面的に依拠しており、経営陣自らが問題意識をもった取組みが行われていない実態が伺われる。

⑶ これらのSQLインジェクション攻撃の発覚時点におけるMPとしての一連の判断が結果として、その後の情報漏えいの発生ないし被害の拡大に繋がったことは否定し難い。

この点、上記のとおり、MPが2021年10月25日に認識した本件事象に係るSQLインジェクション攻撃は、対象が決済システムに係るデータベースが保管されている東京DCを対象としたものである点や、当該攻撃に係る情報量が多く、MPとして初めてIPアドレスのブロックという対応を採ろうとの判断に至ったという点において日常的に発生する不正アクセスとはリスク度合いや様相を異にする側面があったことに鑑みれば、その時点において、MPにて外部機関に対するログ調査依頼を含めたより注意深い対応を期待することは不合理とはいえない。

しかしながら、実際にはMPにおいてそのような観点から必要とされる情報セキュリティリスク上の対応が十分に図られたとはいえず、そのことが本件事象及びこれに基づくカード情報等の漏えい発生に繋がった直接的な要因の一つとして挙げられる。

## 2 2021年12月の対応不十分

⑴ 別紙時系列表のとおり、MPは、2021年12月14日に、フロントシステムの「イベントペイ」に係るアクワイアラであるE社から、カード情報の漏えい懸念がある旨の連絡を受け、翌日にかけての社内調査でも同様の事実が確認されたため、同月16日に自主的に「イベントペイ」のクレジット決済を停止した。その上で、外部の調査会社であるPCFに対して、「イベントペイ」サービスに対するフォレンジック調査を依頼した。

その後MPは、同月20日から21日かけて、今度は、「会費ペイ」及び「Web決済（トークン方式）」で複数の不正利用発生疑いの情報に接した。議事録等の客観的資料によれば、MPは、その時点で、「決済センター（すなわち、東京DC）側での事

故である可能性が極めて高い状況」であること、また最大リスクとして、カード会社側から「『クレジット決済停止』を求められる可能性があること」を認識していた事実が認められるものの、MP は、自主的なクレジットカード決済の停止には踏み切らず、実際に採った対応としては、PCF に依頼しているフォレンジック調査の対象を、念のためフロントシステムのみならず決済システムにまで拡大するというものにとどまった。

⑵　この点、一般社団法人日本クレジット協会がクレジットカード取扱加盟店宛てに発出している「クレジットカード情報の漏えい時及び漏えい懸念時の対応要領」（以下「JCA 漏えい時対応要領」という。）においては、「情報漏えいの被害を最小限に抑え、顧客（カード会員）を保護すること」を目的として、「発見・連絡」、「状況把握・事前確認」、「初動対応」、「調査」、「通知・公表・報告等」及び「再発防止対応」の流れに沿った各段階において求められる対応が示されている。

その中で、カード情報の漏えいの懸念が生じた時点の「初動対応」における「情報漏えいの被害を最小限に抑える」ための優先対応事項の一つとして、「新規のカード決済（カード情報の登録を含む）を停止」することが挙げられており、その上で、次の段階として専門技術によるフォレンジック調査を実施することを求めている。

⑶　確かに、上記の JCA 漏えい時対応要領は、クレジットカード取扱加盟店を名宛人とするものであり、PSP である MP は、直接的にはその適用対象と明示されているわけではない。

しかしながら、JCA 漏えい時対応要領は、カード番号等のカード情報が漏えいした場合又はその懸念が生じた場合にカード会員の被害を最小限に抑える観点からの対応ポイントをまとめたものであり、その要請趣旨は、加盟店のみならず、カード情報を取り扱う PSP に対しても同様に妥当する。

そうだとすれば、本件においても、MP がその決済システムにおける情報漏えい事故の可能性が極めて高い状況にあることを把握し、カード会社側から「クレジット決済停止」を求められる可能性があることも認識していた 2021 年 12 月 21 日の時点で、JCA 漏えい時対応要領に基づき又はこれに準じて、クレジットカード決済を止めるべきだったとの考えもあり得るところであるし、少なくとも、クレジットカード決済の停止について速やかな検討を行うべきであったといえる。

実際、事後的に判明した情報漏えいの発生推移等の事実関係に照らすと、少なくとも PCF レポートによれば、カード情報は 2022 年 1 月 18 日までバックドア経由でのアクセスがあったことからすれば、同日まで窃取され続けていた可能性があるため、仮に MP がこのタイミングでクレジットカード決済を停止する対応を採っていれば、少なくともその時点以降のカード情報の漏えい発生は防ぐことができたといえる。

このことから、2021 年 12 月 21 日以降のカード情報の漏えいに関していえば、同日時点において、JCA 漏えい時対応要領でも示されているようなクレジットカード決済の停止措置を採らなかったこと（少なくとも、クレジットカード決済の停止について検討を行うべきであったのに、当該検討すら行っていなかったこと）がその発生要因の一つとして認められる。

### ３　2022 年１月の対応不十分

⑴　別紙時系列表のとおり、MP は、2022 年 1 月 7 日に F 社（カード会社）から、クレジットカードの不正利用の報告を受けた。実際、上記のとおり客観的には、その時点では本件事象のシステム上の原因について完全な対策は未だ完了していない状況にあり、同月 18 日までカード情報が窃取され続けていた可能性が皆無ではない。

したがって、本章第 3 の 2 と同様に、F 社からの不正利用の報告を受けた 2022 年 1 月 7 日時点でクレジットカード決済の停止に踏み切っていれば、それ以降の情報漏えいの防止に繋げられた可能性があり、MP がそのような判断に至らなかった点は、情報漏えい被害の拡大に寄与した要因であると指摘できる。

⑵　しかしながら、同時に MP は、それまでにフォレンジック調査の実施を進めていた PCF から、本件事象の原因となったシステム上の問題については、2022 年 1 月 8 日に A 社アプリの脆弱性対策を実施したことにより対策が完了している旨の途中報告を受けていた。

実際、2022 年 1 月 13 日付けの PCF レポートにおいても、「収束日」の項目に、「2022 年 1 月 8 日までに封じ込め対応の措置が完了している」との記載が見受けられる。

⑶　以上の点を考慮すると、結果的には、2022 年 1 月 8 日に対策が完了していたとする当時の PCF の調査結果に正確ではなかった部分があったとしても、当時の具体的状況を踏まえれば、MP の経営陣が PCF の報告を根拠として、既にシステム上の問題は解決済みであると考えてその旨をカード会社に説明し、クレジットカード決済のサービス提供を継続したことについては、強く責められるものではないと考える。

## 第８章　間接的な要因（背景要因）

第 6 章で指摘した「システム環境の観点からの直接的な原因」及び第 7 章で指摘した「人的環境の観点（組織体制上の観点）からの直接的な原因」に加えて、本件事象に係る要因として、以下で述べる間接的なものも認められた。

## 第１　A 社アプリの脆弱性の不検証

MP の社内規程においては、「『クレジットカード会員情報を伝送、処理、保管するシステム』にて、カスタムコードのレビューが正確、かつ、セキュリティを保った形で実施されることを目的」として、「決済サービスに関わる、カード会員番号を扱うプログラムやスクリプトのカスタムコード」等に対して、内製、委託先開発に関わらず、ソースコード・レビューを実施する旨が定められていた。

また、社内チェックシートにおいても、その項目として SQL インジェクション攻撃への対策は明記されていた。

しかし、SQL インジェクション攻撃の対象となった A 社アプリには、以下のとおりソースコード・レビューが行われていなかったため、その脆弱性が看過されていた。

### １　開発時等

上記ソースコード・レビューに関する社内規程が作成されたのは、2012 年 10 月であるところ、A 社アプリが委託先である B 社によって開発されたのは、2007 年頃であるため、当時は、社内的にも同アプリに対して SQL インジェクション攻撃への対策としてソースコード・レビューを実施することは必須とされていなかった。

また、MP においては、以前より「決済システム以外は脆弱性対策をする必要がない」との認識があったため、同規定の作成時において、当時フロントシステムにあった A 社アプリが見直し的にソースコード・レビューの対象となることもなかった。

### ２　変更時

ソースコード・レビューは、開発時のみならず、変更時においても実施することとされており、A 社アプリは、2014 年以降、軽微な変更も含めて合計 9 回の変更が行われている（うち 1 回は、後述の 2018 年 7 月の移管後に行われている。）。

しかしながら、MP においては、以前より「決済システム以外は脆弱性対策をする必要がない」との認識があったため、当時フロントシステムにあった A 社アプリの変更時においても、ソースコード・レビューの対象となることはなかった。また、後述のとおり、東京 DC への移管によって他の決済システムと同様に脆弱性対策の対象に含まれるという意識も欠如していたため、移管後の変更時においても、ソースコード・レビューの対象となることはなかった。

### ３　東京 DC 移管時

MP においては、「決済システムは脆弱性対策をする必要あり、それ以外のシステムはその対策をする必要がない」という認識がされていた一方で、あるアプリをフロントシステムから決済システムに移管する際などのルールは存在しなかった。

また、2018 年に A 社アプリを東京 DC に移管する際にも、セキュリティ上の問題点などについてシステム部（当時）や取締役会において事前に議論された形跡はない（したがって、ソースコード・レビューが実施されることはなかった。）。

## 第２　情報セキュリティ体制の不全（コンプライアンス）

### １　現場のセキュリティ意識の不足（事業部門による自律的管理不十分）

情報セキュリティ体制においては、情報の取扱いを行う現場でPDCAサイクルを適切に機能させることが必要であるところ、IT 推進部ではセキュリティ意識の不足によりPDCAサイクルが十分に機能していなかった。

具体的には、以下のような脆弱性スキャンツールの未更新などの事実が認められた。

⑴　内部脆弱性スキャンツール「δツール」のシグネチャ未更新

ア　MPにおける「δツール」による内部脆弱性スキャンの概要

PCI DSS の要件では四半期ごとの内部脆弱性スキャンを行うことが求められているところ、MPでは、少なくとも2020年4月から2022年3月までの間、社内においてサーバを対象としてスキャンを行いOSやミドルウェアの脆弱性の有無及び程度を検証するためのツールである「δツール」を用いて上記内部脆弱性スキャンを実施していた。また、当該スキャンの結果が記載されたレポート（以下「第1次レポート」という。）を基に、PCI DSS準拠のために監査会社へ提出するための内部脆弱性のスキャン結果に関する報告書（以下「第2次レポート」という。）が作成されており、少なくとも2020年4月以降分の第2次レポートの作成は、MP元従業員がMPから委託を受けて行っていた。

イ　「δツール」のシグネチャ更新対応の不備

2020年7月に実施された「δツール」による内部脆弱性スキャンに係る第1次レポートにおいて、「High」レベルの脆弱性として、当該「δツール」のシグネチャ更新が未了である旨の指摘が検出されるようになり、それ以降、2022年4月に脆弱性スキャンに用いるツールを別のツールに変更するまでの間における各脆弱性スキャンにおいて、同様の脆弱性が継続して検出され続けていた。

当該第1次レポートは、MP社内においてIT推進部の副部長及び地井良太氏が内容を確認し承認することとなっていた。

MPでは上記「δツール」を利用しており、「δツール」のシグネチャ更新が可能となると、上記サービスの提供事業者からMPに対しシグネチャ更新に係る通知がなされていた。

このように、MP において「δツール」のシグネチャ更新が未了であることを認識し得る状況にあったと考えられるが、本件では、別のスキャンツールへ変更するまでの間、結果的に脆弱性スキャンツールのバージョン更新という情報セキュリティ対策において重要な対応がなされないままとなっていた。このような状況となった理由に関して、MP において当該通知を受けた場合に更新作業の担当者が明確に定まっていなかったことなどが影響しているものと推認される。

ウ　第2次レポートにおける脆弱性の不記載

また、第 1 次レポートにおいて検出された上記シグネチャ未更新に関する脆弱性については、第 2 次レポートにおいても当然に記載されるべきものであるところ、MP 元従業員が作成した、上記実施された各内部脆弱性スキャンに対応する各第2次レポートにおいては、上記「δツール」のシグネチャ未更新に関する脆弱性について何ら記載がなされていなかった。

かかる対応がなされていた理由や経緯等について、MP 元従業員に対するヒアリング調査が実施できていないこともあり、本調査においては必ずしも明らかとはならなかったものの、複数回にわたりかかる取扱いがなされていることからすれば、少なくとも MP 元従業員による意図的な対応であったと推認される。

この点、MP においては、第2次レポートについても第1次レポートと併せて IT 推進部の副部長及び地井良太氏が確認及び承認を行っており、各レポートの内容を読むことにより、MP 元従業員による上記取扱いを認識し得たものと考えられるが、結果的に当該手続の中では判明することはなかった。

⑵ ウィルス対策ソフトのパターンファイル更新未確認

PCI DSS の要件ではウイルス対策ソフトが常に最新の状態へ自動更新されようになっていることが求められているところ、MP においては、月次で決済センターにおけるウイルス対策ソフトの定義データベースの更新が問題なく行われているか等の項目について、当該項目部分の担当者が確認を実施し、報告を行うこととされている。

かかる月次チェック報告に関し、2021年4月に実施された分の報告書において、ウイルス対策ソフトの定義データベースの更新ができていない旨の指摘が記載されていたところ、翌 5 月実施分の報告書においては、当該指摘が記載されておらず、代わりに問題ない旨の記載がなされており、それ以降の期間における報告書においても同様の記載が続いている。

しかしながら、MP の従業員によれば、上記 2021 年 4 月から 5 月にかけてウイルス対策ソフトの定義データベースの更新は実施されていないとのことであり、これが事実であれば、ウイルス対策ソフトの定義データベースの更新という情報セキュリティ対策において重要な対応が行われることなく、加えて上記報告書において実態と異なる内容が記載されていたということとなる。もっとも、上記期間におけるウイルス対策ソフトの定義データベースの更新未了の事実について客観的な証跡は存在していないため、本調査においてはあくまで上記のような実態が存在した可能性を指摘するにとどめることとする。

⑶ 小括

脆弱性スキャンツールやウイルス対策ソフトを常に最新の状態に維持しておくことは、情報セキュリティ対策における基本的な対応の一つであり、当該対応がなされているか否かを自律的に管理することは、情報セキュリティの維持管理を担

当するIT推進部などの現場において、本来求められるべきセキュリティ意識であるといえる。しかしながら、上記のような実態に鑑みれば、MPにおいては現場のセキュリティ意識が不十分な状況であった可能性が高い。

**２　内部管理部署が不明確で機能していないこと（管理部門による牽制不十分）**

企業のリスク管理等に係る内部統制の在り方については、商品や役務の提供を行う営業部門（いわゆる第一線）、これを管理及び支援する管理部門（いわゆる第二線）及び独立した立場で内部監査を行う監査部門（いわゆる第三線）の3つの役割の観点から整理及び構築する、いわゆる3ラインモデルが有効であるとされている。

この点、MPにおいて、情報セキュリティリスクに関していわゆる第二線として監視、助言等を担当する部署が明確には存在していない。また、上記のとおり、システムに関してはブラックボックス化されていたこともあり、IT推進部における判断等について内部管理部署において適切な牽制を効かせることができていない状況であった。

**３　情報セキュリティ対する内部監査の機能不全（内部監査部門による検証不十分）**

MPにおいては、内部監査担当が設けられており、MPにおける業務監査などの内部監査に関する業務を行うこととされている。そして、当該監査事項の中には情報管理に関する事項が含まれている。

また、内部監査担当とは別に、情報セキュリティマネジメントシステム（ISMS）やPCI DSS、プライバシーマーク等の認証との関係から、情報セキュリティに関する監査を専門的に行う情報セキュリティ監査責任者も配置されていた。

しかしながら、内部監査担当には情報セキュリティに関する知見が必ずしも十分ではない者が任命され、ISMSやPCI DSSに係る規程の整備状況などに対する監査については、それら認証に準拠していることを所与の前提として監査を行われており、また情報セキュリティ監査責任者による監査報告についても内容について精査を行うことはなく、情報セキュリティ監査の実施の事実を確認する程度にとどまっていた。また、情報セキュリティ監査責任者にはIT推進部所属の者が任命される場合もあり、その場合には同部の担当するシステム業務に対する監査については自己監査に該当することとなるため、情報セキュリティ事務局員を補助者とした間接的な監査の実施にとどまるものであった。

以上のとおり、MPにおいていわゆる第三線としての情報セキュリティに関する監査は必ずしも実効的に機能していたとはいえない。後記のとおり、ルールの形骸化等の問題が存在していたのであり、情報セキュリティに関するに内部監査が機能していたならば、MPにおいて情報セキュリティに関するルールに従った適切な取扱いがなされ、本件事象の発生を未然に防ぐことができた可能性がある。

## 第３　システム担当部署における業務の属人化

### １　システム部門のブラックボックス化

MP のシステム関係については、IT 推進部（当時のシステム部）の部長であった甲氏やその部下の担当者に任されており、システム上のリスクや脆弱性の洗い出しは行なわれていなかった。また、人事面においても固定化されていたため、システム管理に関する権限は、上記のように一部の者にのみ集中している状況であり、システム部門は社内においてブラックボックス化している状態であった。

このような状況の下で、MP の経営陣もシステム部門に対する管理監督を十分行うことができず、その結果、MP における情報セキュリティ対策がおざなりとなっていた可能性がある。

### ２　業務引継体制の不整備

IT 推進部が担当する業務に関しては、同部に所属する個々の従業員の専門性などに応じて、ある業務について特定の従業員のみが担当し、他の従業員が当該業務の分担や引継ぎをすることができるような体制構築はなされていなかった。特に甲氏がシステム部の部長として在籍していた期間においては、同部の従業員が不在となり業務の引継ぎが生じる場合には、具体的な業務説明等の引継ぎがなされることなく他の従業員に割り振られるような状況であったとのヒアリング結果もある。

そのため、退社等により従業員が IT 推進部を離れると、当該従業員が担当していた業務の引継ぎがなされず、当該業務の担当者が不在のままとなることもあり、そのことが不十分な情報セキュリティ対策状況の原因となった可能性がある。

### ３　能力ある人材の不足

これまでも、IT 推進部などの現場から人材不足であるとの指摘がなされ、システム関係の知見・経験を有する人材の採用について繰り返し要望が上がっていた。しかしながら、今日に至るまで人材不足の問題は解消されていない。

このような慢性的な人材不足により、IT 推進部の従業員は自らが担当する業務に追われ、アラームの運用見直しなど必要な情報セキュリティ対策のために人員を割くことが難しい状況となっている。

また、IT 推進部における人材不足は、上記で指摘した業務の属人化をより一層強める要因にもなっていたものと推測される。

## 第４　ルールの形骸化

### １　ソースコード・レビュー規程の適用範囲の不浸透

MP では、ソースコード・レビュー規程が策定されており、同規程によれば、その適用範囲は、決済サービスに関わるカード会員情報を扱うプログラムやスクリプトのカスタムコードとされるが、カード会員情報を扱わないカスタムコードであっても、特性等を鑑み、同規程によるレビューが必要とプロジェクトリーダー又は上長が

判断した場合には、同規程の適用範囲となる。

ソースコード・レビュー規程の記載によれば、決済サービスに関わるカード会員情報を扱うプログラム等でなければ、プロジェクトリーダー又は上長が同規程によるレビューが必要であると判断していない限り、ソースコード・レビュー規程に従う必要がないとも解されるが、システム部内部では、決済システム以外は同規程に基づく脆弱性対策はする必要がないと認識する従業員がいる一方で、決済システム以外であっても、ソースコード・レビュー規程に従った脆弱性対策を行う必要があると認識する従業員が認められた。

ソースコード・レビュー規程に従った脆弱性対策の内容として、SQL インジェクション攻撃への対策、クロスサイト・スクリプティング対策などを行うこととなっており、また、MP では、アプリ開発時のチェックリストやシステム変更時の妥当性確認フローに関する文書等が完備されていたが、ソースコード・レビュー規程に従った脆弱性対策を行うことの要否について従業員間の認識の齟齬があり、かかる認識の齟齬は、A 社アプリのように決済サービスに関わるカード会員情報を扱わないプログラムについても SQL インジェクション攻撃への対策等の必要なセキュリティ対策を行っているはずであるという認識に至らしめた可能性は否定できず、A 社アプリを含むシステム全体の脆弱性が見過ごされた遠因として考えられる。

**２　外注業者選定基準の形骸化**

MP では、A 社アプリの開発を含む一定のアプリケーションの開発等を B 社に委託しており、また、ペネトレーション診断対応や ASV 対応（脆弱性スキャン）を MP 元従業員に委託していた。

そして、2008 年 7 月 15 日に外注管理規程が施行され、2017 年 10 月 1 日に同規程が全面改定され、同規程において外注業者選定基準等が定められており、同規程に基づき、外注先選定手順も定められていた。

しかしながら、B 社との間の委託契約は 2007 年頃以前に締結しており、当時、外注管理規程が存在しておらず、MP において B 社が外注先選定基準を満たしていないことが判明して以降も、同基準を満たすためだけに、中間業者として C 社を介在させ、他方で、アプリケーション開発等の実作業は引き続き C 社の下請け的な立場で B 社に行わせるなどの同基準の潜脱が行われていた。

また、MP 元従業員に対する委託に関しても、外注業者選定基準等を満たしていなかったことがうかがわれたが、上層部判断により、同元従業員に上記業務の委託されることとなったとのことであった。

上記のとおり、MP において、外注業者選定基準の形骸化が認められ、事前ないし事後的に外注管理規程に従った外注業者の妥当性の確認なども行われていなかった。

なお、B 社が外注先選定基準を満たしていなかったにもかかわらず、引き続きアプリケーション開発等に携わっていた一因として、アプリケーション関係の文書が十

分に整っておらず、外注先を変更しても、変更先に置いて引き継ぐことが困難であったという事情が認められるが、このような文書不整備は、外注先担当者と外注先の属人的な関係が築かれていたことも背景にあったと認められる（本章第 2 の 2 参照）。

### ３　リスクアセスメントの形骸化・不徹底

MP では、情報セキュリティ基本規程や、情報セキュリティ実施要領が策定されており、保有する情報資産について機密性、完全性、可用性の観点から脅威、脆弱性を洗出し、内在するリスクを把握し、また、定期的かつ重大な変化に応じてリスクアセスメントを再実施するとされ、少なくとも年 1 回、資産の洗い出しや、資産に対するリスクアセスメントを行うとされ、サーバやシステムの脆弱性管理や、ネットワーク機器への内部脆弱性スキャンやペネトレーション診断を行うこととされている。

しかしながら、資産の洗い出しに用いる文書として指定されている決済サービス概要構成（改定日:2021 年 11 月 15 日）においても、たとえば A 社アプリが東京 DC 内に格納されていたか否かは判然とされていないなど、最新化かつ適正化された資産管理台帳の維持、整備ができておらず、社内における提供サービスの洗い出しや、リスクアセスメントが適切に実施されていたとは認められなかった。このような資産の洗い出しが不十分な状況が、連鎖的に不十分な自己点検やリスク分析を招くこととなったと認められる。

### ４　セキュリティアラートに対する検証などの運用人員不足

MP では、情報セキュリティ実施要領において、セキュリティのパフォーマンスを維持するために、可能な範囲で監視体制・要員を整備し、障害発生時の連絡体制を整備することとされており、重要セキュリティ・エラー対応手順書において、一定のセキュリティアラートを検知した場合における手順が定められていた。

しかしながら、従業員のヒアリング結果によれば、実際はセキュリティアラートにする検証ができる人材が不足しており、また、必要な範囲でセキュリティアラートを発信するようにするためのシステム面での調整（チューニング）が出来ていないことも相まって、MP の従業員は、セキュリティアラートが発信されても、特段気にして監視していなかったとのことであり、十分な検証がなされていなかったことが認められた。

本件事象について、セキュリティアラートの検証により攻撃経緯と影響範囲が適切に調査されていれば、被害を最小化又は未然に防止できる可能性もあったところであり、運用上、セキュリティアラートの検証体制について定める規程が形骸化していたことは、本件事象を発生させた要因になる。

## 第５　ガバナンスの不備

前記第 3（「システム担当部署における業務の属人化」）のとおり、MP のシステム関係については、IT 推進部（当時のシステム部）の部長やその部下の担当者に任されてお

り、情報セキュリティに関するシステム部門の判断を無批判に受け入れることが常態化しており、経営陣による踏み込んだ監督はなされていなかった。

もっとも、MP は、システム部内で閉鎖的に判断される構造を問題視し、2019 年、D 社との間で、MP の基盤改革の一環として必要なシステム整備・体制づくりを実施する目的で、システムコンサル委託契約を締結し、システム部の運営体制や外部委託先への業務委託状況に関し、問題点を抽出した上で、D 社に指摘を受けた事項を踏まえて、システム部門への改善を図ってもおり、本件事象は、改善の過渡期における事象であった事実も認められた。

具体的には、セキュリティ人材の獲得の必要性等が指摘されたことを踏まえ、人材獲得に向けた採用活動を行っていたことがうかがわれ、また、システム部部長のタスクとして「セキュリティ担当者の稼働」を明確に指示し、同部長に改善命令を出すなど適切なシステム部門の運営体制を構築することを企図していたこともうかがわれるのであって、2019 年から本件事象当時にかけてはガバナンスの機能強化についての一定の対応を講じていることが認められる。

## 第６　効率優先の意識

１　MP が主な事業とする決済代行事業は、加盟店とアクワイアラの間に立って、加盟店に対し多様な決済手段を提供することを主な内容とするビジネスである。

決済代行事業はいわゆる手数料ビジネスであり、その収益源は加盟店から支払われる手数料に大きく依存している。すなわち、決済代行業者の手元に残るのは、当該手数料から、イシュア、アクワイアラ、ブランド等が収受する手数料分を控除した金額に限られているため、コスト削減を図れば、収益が増加するという構造にある。

上記のような収益構造に加えて、業界シェア率において最大手にあったわけではないという MP の業界における位置付けも相まって、MP においては、コスト削減を必要以上に優先しようとする傾向があったと認められる。

２　このようなコスト削減優先の傾向は、①MP の 2019 年 1 月時点における中期経営目標を示す資料において、当時の喫緊の課題として、決済代行ビジネスにつき「極限まで効率性向上」が挙げられており、その解決策として 2020 年を目途に「決済ビジネスの固定費を大幅圧縮」することや、②2019 年 7 月頃の D 社による報告書においても、上記と同様の課題が示され、今後の方針として「決済システムの維持保守はトラブルが起きない程度に省力化・効率化し、空いたリソースは営業本部と融合するなどして活用すること」が示されていること、にも表れている。

さらに言えば、決済システムにおけるセキュリティ保持の観点で、WAF の導入は必須であるにもかかわらず、過剰な人的コストを要することを理由に導入が見送られていること等の事実もその表れの一つである。

３　以上の事実に照らせば、MP においては、少なくとも 2019 年ごろの時点では、コス

ト削減を必要以上に優先するという意識が認められ、セキュリティ上必要な箇所についてはコストをかけなければならないという点については、本件事象に至るまで重要視されなかったものと思われる。

この点については、経営陣もその事実を認識し、改善を図る動きをしていたものの、本件事象発生まで最終的な改善には至らなかったものであり、本件事象の遠因になったものと考えられる。

## 第７　セキュリティ意識の低さ・従業員教育の不備

１　MP におけるコンプライアンス基本規程では「必要に応じて教育研修を行う」ことが規定され、コンプライアンス行動原則でも、「役職員に対するコンプライアンスに関する研修を充実させ」ることが示されている。

また、情報セキュリティ基本規程では「定期的に、かつ必要に応じて教育を実施」することとされ、これを受けた情報セキュリティ実施要領でも一定の従業員教育を実施するものとされている。また、「長期休暇等の理由により教育プログラムを受講できない従業者については、休暇明けに確実な教育を実施」すること、「教育責任者は、教育内容の理解度確認のため、受講者に対し、質問・アンケートおよび小テスト等で理解度の確認を行う」こと、及び「理解度の合格基準を 70%以上とし、70%未満の受講者には再教育を実施する」ことが規定されている。

このように、MP の社内規程においては、情報セキュリティ分野に関して、適切な教育を行うことが規定されている。

実際にも、例えば、2021 年度には、全従業員に対して「情報セキュリティ管理体制の確認」、「業務 PC への SW インストール方法の確認」、「個人情報保護方針の理解度について」、「PMS（個人情報マネジメントシステム）適合性の重要性について」等の項目につき教育が実施されており、上記規程に従って、一定の運用はされていたものと認められる。

２　しかしながら、役職員に対するヒアリングによれば、情報セキュリティに関する知識の不足及び意識の低さを指摘する声が散見された。

この点に関し、前述したクロスサイト・スクリプティングの脆弱性に係るレポートについての意図的な変更や、内部脆弱性スキャンツール「δツール」のシグネチャ未更新などの事象は、情報セキュリティに関する知識の不足及び意識の低さが露呈した具体的な事象であると解される。

また、一部の役職員の間には、自社内のシステムについて PCI DSS 又は ISMS に準拠していることに対する過剰な信頼が認められ、これらの基準への準拠が情報セキュリティにおける最終目標となっていた傾向が認められた。

そのため、これらの基準に係る準拠が認められ、一定の認証等を得た後においては、情報セキュリティの観点から改めて業務内容を見直し、改善が図られるようなこと

もなく、仮に不適切な取り扱いがなされていたとしても、特段疑問を抱く声が上がることはなかった。

3　以上のとおり、MP においては、形式的には規程に従った教育は実施されていたものの、情報セキュリティに関する意識の低さが改善されるような内容ではなく、全社的な情報セキュリティに対する意識の向上は図られなかった。このような点も、本件事象の遠因になったものと考えられる。

## 第９章　再発防止策の策定への提言

当委員会は、第 6 章から第 8 章までに記載した本件事象の要因を踏まえ、以下のとおり、再発防止策を提言する。

### 第１　システム環境の観点からの再発防止策

まず、システム環境の観点からの再発防止策は、以下のとおりであり、多層的、複層的再発防止策を講じ、セキュリティの向上を図るべきである。

①　日時のログの点検

②　セキュアコーディングを行ったアプリケーション開発とソースコード・レビューの実施

③　ペネトレーション診断又は脆弱性診断と診断結果を踏まえた脆弱性等の修正

④　WAF の導入

⑤　セキュリティアラートの発信後に、何故アラートが発信したのか、その原因となった「障害」又は「侵害」を検証すること

⑥　社内及び加盟店の業務向けのログイン画面へのアクセス制限

⑦　社内及び加盟店の業務向けのログイン画面の二要素認証、二段階認証の導入

⑧　ファイル整合性監視の範囲の見直しとアラートに対する検証手順の整備

⑨　ログの取得方法の見直し

⑩　クレジット取引セキュリティ対策協議会の作成資料の内容を踏まえた、決済サービスに関するシステム以外のシステムに係る全面的な検証、見直し

⑪　フロントシステム側に関するセキュリティ対策の強化

## 第２　人的環境の観点（体制整備上の観点）からの再発防止策

### １　業務上の不正、業務懈怠等の発見のための措置

⑴　各部署レベル

①　不正常な業務を防止するシステム、仕組みの検討、構築

情報の処理、取扱いなどを行う各部署において、不正常な業務を防止するためのシステム、仕組みを検討し、構築することが必要である。具体的には、以下のような措置が考えられる。

ア　業務上行われる各種検証等の結果を改ざん、変更等できないようなシステムや、複数の担当者に各種検証結果が連携され、相互の牽制が働くようなシステムなどを導入すること

なお、この場合には、各部署における現場の状況を踏まえた、業務上の不正、業務形態等を確実に発見できる仕組みを検討し、構築することが必要である。

イ　定期的な人事ローテーション等を行い、引継ぎによる担当者の変更に伴う、不正発見を促進することや、人事ローテーションを定期的にすることにより、事前の抑制効果、担当者相互の牽制効果を生じさせること

②　不祥事や不正アクセス等を発見しやすくするための業務システムの構築

システム環境の観点からの再発防止策においても指摘しているところであるが、各部署における業務上の行為について、可能な限り、ログの証跡の保存などを行い、仮に不祥事や、不正アクセス等が生じた場合に、事後的に確実に検証ができるシステム、仕組みを構築することが必要である。

③　決裁・業務手続に係る手順、マニュアル、規程の改訂、整備

既存の決裁や業務上の手続に関して、業務上の不正や業務懈怠（委託先の管理懈怠を含む。）等を発見できる仕組みになっているか否かという観点から、従前の手順、マニュアル、規程を検証し、必要に応じた改善や、これらの新設を行うことが必要である。

また、部署間の相互牽制を図るために、必要に応じて、レポートラインの再検証及び再構築を行うことも検討すべきである。

⑵　全社レベル

①　内部管理部門の新設

前述のとおり、MP においては、いわゆる第二線として監視、助言等を担当する部署が明確には存在しておらず、IT 推進部における判断等について内部管理部署において適切な牽制を効かせることができていない状況であった。

そのため、早急に、内部管理（第二線）を担う部門を明確に設置し、当該部署について、役割の明確化、必要な人員の配置を行うべきである。

また、当該部署を通じて、業務に対するチェック機能の強化を図るべきである。

②　内部監査部門の強化

MP においては、内部管理部門は存在したものの、前述のとおり、必ずしも実効的に機能していたとはいえない。

そのため、以下の方策を講じることにより、内部監査部門の強化を図る必要がある。

ア　情報セキュリティ分野（ISMS）と全社分野の内部監査機能の統一化

現時点での内部監査部門は、情報セキュリティ分野（ISMS）と全社分野とで、各々別の部署とされているが、これを統一化し、横断的かつ実効的な内部監査を可能とすべきである。

イ　内部監査部門の人員の拡充、業務に対するチェック機能の強化

内部監査部門の人員を拡充するだけでなく、情報セキュリティに関する必要な人材を確保し、業務に対するチェック機能を強化すべきである。

ウ　内部監査部門の能力（特にセキュリティ分野）の強化

前述のとおり、情報セキュリティに関する必要な人材を確保することで、セキュリティ分野に係る内部監査の実効性を確保する必要がある。

エ　取締役会との連携、監査役との連携

内部監査部門によるチェック機能を強化し、実効化を図ることは、重要な経営課題であり、取締役会や監査役としても、内部監査部門との十分な連携を図るべきである。

オ　外部専門家の活用、連携の検討

人材確保が困難であるなどの事情により、以上のような内部監査部門の強化が直ちに図れない場合も想定されるが、このような場合には、外部専門家を活用し、これらと連携することにより、内部監査部門に代わるチェック機能を確保すべきである。

③　取締役会の機能強化

情報セキュリティに関するシステム部門の判断を、深い検討を行うことなく、

受け入れることが常態化していた点にも表れているとおり、MP においては、経営陣による踏み込んだ監督はなされていなかった。

そのため、取締役の権限分掌を、相互牽制機能の強化の観点から改めて見直し、検討を行うことが必要である。

また、相互牽制機能の強化のためには、取締役においてサイバーセキュリティの重要性を再度確認し、必要な知識を有しておくことが求められる。このような観点から、経営陣におけるセキュリティに関する意識改革を図ることも必要であり、役員に対するサイバーセキュリティに係る教育を定期的に行うことが考えられる。

④　内部通報制度の充実化

前述のとおり、MP においては、脆弱性診断に係るレポートに対し意図的な変更が加えられ、取締役の一部はこれを認識していたか、認識すべき状況にあったことが認められる。

このような業務上の不適切行為については、内部通報制度が充実化していれば、早期発見につながるはずであり、また牽制効果により、未然に防止することも可能であった。

この点、MP においては、既に内部通報制度は整備されているものの、直近 5 年間での利用は 0 件であり、有効に機能していたとは言い難い。そのため、以下の点に留意し、内部通報制度の充実化を図るべきである。

ア　通報者保護の徹底

イ　通報制度の周知徹底、利用の促進

ウ　運営状況の確認

エ　リニエンシー（不正者が自ら申し出を行った場合の社内処分の減免）の導入

## ２　業務の属人化防止のための措置

前述のとおり、MP のシステム関係については、IT 推進部（当時のシステム部）の一部の役職員に任されており、システム上のリスクや脆弱性の洗い出しは行なわれていなかった。また、人事面においても固定化されていたため、システム管理に関する権限は、上記のように一部の者にのみ集中している状況であり、システム関係の業務について、業務の属人化が認められる。

そのため、以下の措置を講じることにより、このような状態を早急に解消し、業務の適正化を図るべきである。

①　定期的な人事ローテーションによる各自の業務内容の見える化

②　既存人材の配置の見直し

③　他部門との人材交流

④　専門的知見・経験を有する人材の新規採用、活用

### ３　社内ルールの形骸化防止のための措置

MP においては、様々な社内ルールがあるものの、これらの社内ルールの内容や趣旨が全社に浸透しておらず、その結果、様々な側面において、ルールの形骸化が認められた。そのため、以下の措置を講じる必要がある。

①　既存の社内規程の整備・見直し

この整備、見直しに際しては、従業者が遵守すべき規範をスムーズに理解できるかという観点から、従前の社内規程を、内容面だけではなく、体系面も含めて検証し、必要に応じた改善や、これらの新設を行うことが肝要である。

また、特に、PCI DSS 準拠用、ISMS 準拠用などいう目的に応じて社内規程を整備するという観点を徹底的に排除し、規程の一元化、平易化を図ることが重要である。

②　社内への周知徹底

整備、見直しを行った社内規程については、適切に社内に周知徹底を図るべきである。

その際には、形式的に規程の内容を周知するのではなく、当該規程の目的や趣旨を含めた周知を心掛ける必要がある。

③　定着化のための不断の努力

後述する従業者への教育とも共通するが、社内規程の定着化のために、社内教育の継続や、業務部署毎の定着化のためのミーティング、社内イントラを通じた各種の理解測定の実施など、経営陣が率先して不断の努力を行うべきである。

### ４　委託先管理

前述のとおり、MP では、外注業者選定基準の形骸化が認められ、事前ないし事後的に外注管理規程に従った外注業者の妥当性の確認なども行われていなかった。

そのため、以下の措置を講じ、委託先の管理の徹底、強化を図るべきである。

①　委託先の管理体制の再整備

特に、委託先に対する取引開始時の審査や、定期的・継続的な監視・監督がなされていなかったことを踏まえ、これらの管理体制について、改めて整備することが必要である。

また、委託先に関する情報についても、適切に収集、管理を行い、上記の審査、監視、監督の際に利用できるような体制とすべきである。

②　委託先管理に係る社内決済プロセス・社内規程等の整備・徹底

上記①に併せて、委託先の管理に係る社内決済プロセス・社内規程等の整備・徹底も行うべきである。

具体的には、委託先審査のプロセスにおいて必要となる情報項目や審査方法について確実にルール化するとともに、この運用を徹底することが必要である。

また、委託先の審査基準をクリアできない事業者を、業務上の必要性を踏まえて、委託先として選定することが想定されるのであれば、この場合の例外的な手続を予め明確化しておくことが必要であり、恣意的な運用を認めるべきではない。

③　委託先の多様性、多元化確保

委託している業務について、属人化を排し、他の委託先においても実施が可能な状態とした上で、委託先の多様化、多元性を確保すべきである。

④　委託先管理の担当者に関する措置

担当者の変更・流動性を確保することにより、担当者及び委託先間の馴れ合いを防止し、牽制強化を図るべきである。

また、同様の目的により、必要に応じて、委託先の管理に関する担当部署や担当者の権限分掌の見直しも行うべきである。

## ５　「サイバーセキュリティ経営ガイドライン」（脚注1）を踏まえた体制整備

MP においては、自社の中核的なサービスが決済代行サービスであり、顧客の個人情報、カード番号等の重要な情報の取扱いを伴うこと、当該取扱いの対象となる情報については、サイバー攻撃の対象となることを十分に認識し、サイバーセキュリティを最重要の経営課題と認識した体制整備が必要である。

そのため、前述した点に加えて、「サイバーセキュリティ経営ガイドライン」を踏まえた、以下の体制整備も必要となると考える。

⑴　経営者が理解すべき「3 原則」の認識徹底

MP の経営陣は、システム担当部署に一任するのではなく、自らリーダーシップを発揮して、同ガイドラインに示された以下の 3 原則を踏まえた対応を実施すべきである。

①　経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要

②　自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーン

1 https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf

に対するセキュリティ対策が必要

③　平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要

⑵　重要 10 項目の改めての徹底

また、MP 経営陣は、同ガイドラインで示された以下の重要 10 項目について、自社の実態を踏まえた実効的な体制構築を再考すべきである。

なお、これらの体制構築については、当然ながら、これまでの形式的には遵守してきた事項と思われるものであるところ、真に実効的な体制となっているかという観点からの再度の確認及び徹底が必要である。

①　サイバーセキュリティリスクの認識、組織全体での対応方針の策定

この点に関しては、形式的に CISO を選任するだけではなく、実効的な役割を果たさせるために必要な措置を講じることが重要である。

②　サイバーセキュリティリスク管理体制の構築

特に、システム担当部署に一任するのではなく、取締役、監査役としても当該体制の構築、運営状況を適切にチェックする必要がある。

③　サイバーセキュリティ対策のための資源（予算、人材等）確保

コスト削減優先ではなく、必要な対策について十分な資源を確保することが必要である。

④　サイバーセキュリティリスクの把握とリスク対応に関する計画の策定

⑤　サイバーセキュリティリスクに対応するための仕組みの構築

⑥　サイバーセキュリティ対策における PDCA サイクルの実施

⑦　インシデント発生時の緊急対応体制の整備

特に、決済代行ビジネスは、関係する当事者が多数想定されることから、被害拡大防止の観点から関係当事者への円滑な連携手順や、関係省庁への報告手順など、各手順を検討、確立しておくことが必要である。

⑧　インシデントによる被害に備えた復旧体制の整備

復旧体制の整備に際しては、迅速な復旧手順を検討、確立するだけではなく、

直ちに、被害拡大を防止する観点からサービスの一時停止手順等も含めた、事前検討を行うことが必要である。

⑨　ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握

⑩　情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供

MP では、従前は、同業他社との情報交換、交流等を積極的に行ってきた様子はうかがえない。今後は、積極的に、業界団体や同業他社との情報交換を図り、有益な情報取得を図ることが重要である。

### ６　企業風土の改善、従業員教育

当委員会の調査によれば、MP においては、必要以上にコスト削減を優先すべきとする傾向（効率優先の意識）や、情報セキュリティに関する知識の不足及び意識の低さが伺われた。

これらを一朝一夕に解決することは困難であり、経営陣が継続的かつ積極的に関与した以下の取り組みが必要である。

①　効率優先の意識の改善に向けた以下の取り組み

ア　代表者自らがトップメッセージを発し、これに前提に経営陣の意識改革を図ること

イ　各方面でのコミュニケーションを確保し、これを通じて、経営陣の改善意識を浸透させ、意識改善を図ること

・各部署の現場担当者と経営陣の間のコミュニケーション
・従業員間のコミュニケーション
・上記を促進するための改善・改革に関する組織・プロジェクトの設置の検討
・業界団体や、同業他社とのコミュニケーション

②　情報セキュリティに関する知識の不足及び意識の低さの改善に向けた取り組み

社内教育の継続や、業務部署毎の定着化のためのミーティング、社内イントラを通じた各種の理解測定の実施などの実効的な社内教育の実施

## 第 10 章　結語

1　MP は、ISMS や PCI DSS に準拠した情報セキュリティ体制を有する会社であり、外形的には、一定のセキュリティ水準を有しているはずの会社であった。

2　しかしながら、社内の状況をみると、ISMS や PCI　DSS の準拠という結果に対する過剰な信頼が認められ、極論すれば「準拠が認められ、認証が得られれば良い」という考えの下で、社内ルールが形骸化し、業務が属人化し、チェック機能が十分に働かないなど、必要な情報セキュリティ体制が確保されていなかった。

具体的な事例として、社内ルール上必要とされる脆弱性診断の意図的な変更や、脆弱性診断に必要となるツールの未更新、システムから発せられるアラートへの検証不足など、様々な事実が認められた。

ISMS や PCI　DSS は、あくまで一つの基準であって、これに基づく認証を得ることは単なる過程に過ぎず、最終的な目標は、カード番号を含む顧客情報を安全かつ適切に管理するために必要な情報セキュリティの確保である。

そのため、認証を得た後も、社内の実態を踏まえた実効的な態勢整備が必要である。

また、必要となるセキュリティの水準は、技術の変化によって、日々変わり得るのであるから、継続的な取り組みによって、セキュリティ水準を高めていくという意識も必要である。

MP については、このいずれもが欠けていたといわざるを得ない。

3　また、MP の中核業務は、決済業務であり、決済システムには、一般消費者である顧客の個人情報だけでなく、カード番号などの漏えいにより財産的被害が生じるおそれのある情報が多数保有されている。そのため、⑴個人情報保護法に基づき個人情報取扱事業者として、⑵割賦販売法に基づきクレジットカード番号取扱事業者として、これらの情報についての安全管理措置を講じることは当然であるが、万一、不正アクセス等による漏えい事故が発生した場合には、一般消費者である顧客の利益保護の観点から、被害拡大を防止するために最大限必要な措置を講じる必要がある。

本件事象発生後の MP においては、一般消費者の利益保護という観点からの検討や、取り組みが必ずしも十分ではなかったものと認められる。

4　当委員会は、調査期間が許す限りの調査を行い、本報告書記載の事実認定及び再発防止策の提言を行った。

MP の従業員の大部分は、当委員会のインタビューに非常に協力的であり、日々の業務において問題と感じる点を率直に情報提供していただいたものと感じている。今回の調査をきっかけに会社を改善していきたいという想いがあったものと推察される。

MP の経営陣は、このような想いを、これからの改善に生かすべきである。

今後、MP においては、本報告書を受けて、関係するクレジットカード会社の協力

を得た上で、漏えいした可能性のあるカード番号等とカード会社が把握している不正利用されたカード番号等を照合する手法による調査などを行い、最終的な事実関係を確定させることも検討すべきである。

また、上記の事実関係の確定にかかわらず、当委員会が提言した再発防止策については、速やかに措置を講じ、一刻も早く、必要な情報セキュリティ態勢を構築し、信頼回復を図るべきである。

本報告書がその一助になれば幸いである。

以上

用語一覧

| 用語 | 説明 |
| --- | --- |
| ASV 対応（脆弱性スキャン） | PCI DSS によって年間に 4 回実施することが義務付けられている認定スキャニングベンダー（ASV（Approved Scanning Vendor））による脆弱性診断をいう。 |
| β Security Hub | セキュリティのベストプラクティスのチェックを行い、アラートを集約し、自動修復を可能にするクラウドセキュリティ体制管理サービスをいい、以下の各サービスの一元管理が可能となる。 |
| βクラウド | 某社が提供するクラウドサービスであって、MP がフロントシステムのために利用していたものをいう。 |
| BASIC 認証 | HTTP で定義される認証方式（HTTP 認証）の一つであり、ユーザ名とパスワードにより認証を行うことをいう。IP アドレスによるアクセス制限ができない場合に用いられる。 |
| CISO | Chief Information Security Officer<br>（最高情報セキュリティ責任者）の略称であり、企業における情報セキュリティを統括する責任者をいう。 |
| CVSS | Common Vulnerability Scoring System（共通脆弱性評価システム）の略称であり、情報システムの脆弱性の深刻度を数値化して評価する手法をいう。 |
| K 管理画面 | 社内用決済管理画面をいう。 |
| ICMS | International Certificate authority of Management System Co.,Ltd.の略称であり、PCI DSS 準拠の訪問審査を行う、PCI SSC が認定した審査機関(QSA)をいう。 |
| αクラウド | 某社が提供するクラウドサービスであって、MP がフロントシステムのために利用していたものをいう。 |
| IPS | Intrusion Prevention System（不正侵入防止システム）の略称であり、ネットワークやサーバを監視し、不正なアクセスを検知して管理者に通知する役割を担うシステムをいう。 |

| | |
|---|---|
| IP アドレス | Internet Protocol Address（インターネットプロトコルアドレス）の略称であり、インターネット上で特定のコンピュータ（ホスト）を一意に識別する数値コードをいう。 |
| ISMS | Information Security Management System（情報セキュリティマネジメントシステム）の略称であり、情報資産のセキュリティを適切に管理するための仕組みをいう。 |
| A 社 | 一般社団法人 A をいう。 |
| A 社管理画面 | A 社アプリに係る管理画面をいう。 |
| A 社アプリ | A 社会員向け申込フォームとして稼働するアプリケーションをいう。 |
| Lanscope | IT 資産管理から情報漏洩対策、ウィルス対策までまとめて管理できるソフトウェアをいう。 |
| Logstorage | サーバやネットワーク機器等の情報システムから出力される大量のログデータを収集し、多様な目的にログデータを利用可能とする統合ログ管理システムをいう。 |
| MP | 株式会社メタップスペイメントをいう。 |
| PCF | P.C.F.FRONTEO 株式会社をいう。 |
| PCF レポート | PCF が MP からの委嘱を受けて行ったフォレンジック調査に関する報告書であり、2022 年 1 月 13 日付け初期調査報告書、同月 30 日付け調査結果報告書、同年 2 月 8 日付け最終調査報告書を個別に又は総称していう。 |

| | |
|---|---|
| PCI DSS | Payment Card Industry Data Security Standard の略称であり、カード情報を取り扱う全ての事業者に対してカード会員情報を安全に取り扱うことを目的として、国際ブランドが共同で策定したデータセキュリティの国際基準をいう。 |
| PMS | Personal information protection Management Systems（個人情報保護マネジメントシステム）の略称であり、JIS Q 15001 に規定された、個人情報を保護する体制を整備し、定められた通り実行、定期的な確認、継続的に改善するための管理の仕組みをいう。 |
| PSP | Payment Service Provider の略称であり、インターネット上の取引において EC 加盟店にクレジットカード決済スキームを提供し、カード情報を処理する事業者をいう。 |
| プライバシーマーク | 個人情報について、日本産業規格「JIS Q 15001 個人情報保護マネジメントシステムー要求事項」に適合する適切な保護措置を講ずる体制を整備している事業者等を評価して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認める制度をいう。 |
| SQL インジェクション攻撃 | プログラムに対し、セキュリティを無効化するような不正なコマンドや文字列を混入し、データベースに不正にアクセスする攻撃をいう。通常想定しない SQL（データベースを操作するために使用される代表的なプログラミング言語）文を実行させることによりデータベースに不正にアクセスする方法をとる。 |
| WAF | Web Application Firewall の略称であり、ファイアウォールの一種として、アプリケーションの通信の内部まで監視し、不正な通信の監視・遮断を行うソフトウェアや機器をいう。 |
| アクワイアラ | 加盟店に対しクレジットカード番号等を取り扱うことを認める契約を締結する事業者をいう。 |
| アプリケーションログ | アプリケーションの動作状況についてアプリケーション自身がファイルに残した記録をいう。 |
| 暗号化 | データを第三者に盗み見られることや、改ざんを防ぐために、一定の規則・法則に従ってデータを変換することをいう。 |
| イシュア | クレジットカードの発行会社をいう。 |

| | |
|---|---|
| カード会員情報 | クレジットカード会員に係る氏名、住所、電話番号、メールアドレス及びカード情報等を総称していう。 |
| カード情報 | カード番号、有効期限、セキュリティコードを総称していう。 |
| カード番号 | クレジットカードに係るカード番号をいう。 |
| クエリ―ログ | MySQL サーバが実行した全ての SQL クエリ（データベース管理システムに対する命令文）を出力するログをいう。 |
| クレジットマスター | カードの規則性を利用して他人のカード番号を割り出し不正に取得する行為をいう。 |
| クロスサイト・スクリプティング | 攻撃対象の Web サイトの脆弱性を突き、攻撃者がそこに悪質なサイトへ誘導するスクリプトを仕掛けることで、サイトに訪れるユーザの個人情報などを詐取する攻撃のことをいう。 |
| 決済システム | MP においてクレジットカード決済、コンビニ決済、電子マネー決済等の各種決済を行うシステムをいう。 |
| 再発防止委員会 | MP 社内において組織された本件事象の根本的な原因を究明し再発防止策を検討することを目的とする再発防止委員会（2022 年 2 月 25 日設置）をいう。 |
| 情報セキュリティ委員会 | MP の情報セキュリティ管理規程に基づき、情報セキュリティの管理、実施を行うために社内に設置した委員会をいう。 |
| 情報セキュリティ監査責任者／IS 監査責任者 | MP の情報セキュリティ管理規程に基づき、情報セキュリティに関する監査を行うために社内に設置された役職をいう。 |
| 情報セキュリティ責任者／IS 責任者 | MP の情報セキュリティ管理規程に基づき、情報セキュリティの確保及び維持の活動を行うために社内に設置された役職をいう。 |
| セキュアコーディング | 悪意のある攻撃者やマルウェア等による攻撃に耐え得る、堅牢なプログラムを書くことをいい、エスケープ処理（※）を含む。<br>（※）プログラミング言語やソフトウェアで文字列を扱う際に、特定の記号文字などに続けて記された文字（の並び）に、その文字本来の意味とは異なる特別な意味や機能を与えることをいう。<br>本報告書では、SQL インジェクション攻撃を回避するアプリケ |

| | |
|---|---|
| | ーションを構築されていることを意味する。 |
| データベーススキーマ | データベースにおける構造をいう。 |
| ソースコード・レビュー | ソフトウェア開発工程で見過ごされた誤りを検出・修正することを目的としてソースコードの体系的な検査を行う作業のことをいう。 |
| ディレクトリトラバーサル | コンピュータシステムへの攻撃手法の一つで、ファイル名を扱うようなプログラムに対して特殊な文字列を送信することにより、通常はアクセスできないファイルやディレクトリ（フォルダ）の内容を取得する手法をいう。 |
| テーブル／TBL | データベースを構成する基本要素として、データを表として整理したものをいう。 |
| 当委員会 | MP の委嘱を受けて本調査を行った第三者委員会（委員：右崎大輔、大河内貴之。2022 年 4 月 7 日設置）をいう。 |
| 東京 DC | MP における決済システムに係るデータベースが保管されている東京データセンターをいう。 |
| 二段階認証 | 認証を二段階で行うことをいい、異なる要素を組み合わせる二要素認証・多要素認証とは異なる。 |
| 二要素認証 | 記憶、所有物、生体情報の各要素のうち、複数の認証情報を組み合わせることで、利用者本人であることを確認する当人認証方法のこと |
| バックドアプログラム | システムに正規の手続きを経ることなくアクセスできる裏口を作るプログラムのことをいう。 |
| 平文 | 暗号化されていないデータをいう。 |
| ファイアウォール | 内部のネットワークと外部の境界で、通信の監視・遮断等の制御を行うソフトウェアや機器のことをいう。 |
| ファイル整合性監視 | サーバ上の重要なファイルの不正な変更や改竄を検知することをいう。 |

| | |
|---|---|
| フォレンジック調査 | 不正アクセス等の後に当該システムに残された証跡やログを解析し、事実を明らかにする調査のことをいう。 |
| 復号 | 暗号化されたデータを平文に戻すことをいう。 |
| フロントシステム | MP において決済自体は行わず、サービスのパッケージとして顧客に提供するシステムをいう。 |
| ペネトレーション診断 | ネットワークに接続されているコンピュータシステムに対し、実際に既知の技術を用いて侵入を試みることにより、システムに脆弱性がないかどうかテストする手法をいう。 |
| 本件事象 | 別紙時系列表①に記載される K 管理画面のアカウント情報の取得及び不正アクセスに係る事象、別紙時系列表②に記載される SQL インジェクション攻撃に係る事象並びに別紙時系列表③に記載されるバックドアプログラムの設置及び攻撃に係る事象を個別に又は総称していう。 |
| 本調査 | 当委員会による本件事象に関する調査をいう。 |
| 本報告書 | 本調査の結果に係る第三者委員会調査報告書をいう。 |

別紙

時系列表

以下では、客観的な外部からの攻撃に対応する時系列を①から⑤にまとめ、これらに係るMPの認識及び対応をaからeにまとめている。

**（注）以下の時系列表については、セキュリティリスクを踏まえ、具体的な記載をマスキングしている部分がある。**

| イベント | 日時 | 事象 |
|---|---|---|
| K管理画面のアカウント情報の取得及び不正アクセス（①） | | |
| | 2021年8月31日21:51 | 不正と考えられるIPアドレスからK管理画面へのログイン成功が確認された。利用されたUserIDは「X氏」であり、正常時は事業本部従業員が当該アカウントを使用していた。 |
| | 2021年9月末から2021年10月初旬までの間 | 事業本部従業員が、UserID「X氏」のパスワードを変更したため、攻撃者が「X氏」でK管理画面にアクセスができなくなる。 |
| | 2021年10月6日11:22:38から2021年10月14日16:07:20 | UserID「Y氏」を利用して、K管理画面に対して不正アクセスが開始される。<br>なお、当該UserIDは、正常時は事業本部従業員が使用していた。 |
| SQLインジェクション攻撃（②） | 2021年10月14日23:10:40 | A社アプリにSQLインジェクション攻撃を受ける。 |
| | 2021年10月15日05：09 | SQLインジェクション攻撃により、データベースにアクセスが行われ、不正ログインが可能となるIDとパスワードが窃取された。 |
| | 2021年10月15日05：12 | 不正ログインが行われた。 |

| | | |
|---|---|---|
| | 2021年10月19日<br>から<br>2021年10月27日<br>までの間 | 複数のIPアドレスからカード番号等が格納されたデータベースへのアクセスが行われ、テーブルの情報が約2万5千件窃取された。 |
| SQLインジェクション攻撃の認識及び対応（a） | 2021年10月25日<br>01:30から<br>同日06:30 | IT推進部従業員において定期メンテナンスを実施したところ、不正アクセスの存在に気付く。当時のIT推進部副部長に報告し、同副部長が、攻撃者のIPアドレスをファイアウォールでブロックするように指示し、情報セキュリティ監査担当者がIPアドレスのブロックを実施した。 |
| | 2021年10月25日<br>09:50から<br>同日15:24 | ①当時のIT推進部副部長は、和田洋一氏、増沢将秀氏、地井良太氏に対し、Slack上で、「SQLインジェクションのアクセスを確認したと報告を受けた」旨の報告をし、対応策の方針の確認等を行った。<br>②その際、IT推進部副部長より、SQLインジェクション攻撃と思われるアクセスは全てエラーとなっていること（情報漏えいはないこと）の報告があった。なお、IT推進部従業員間で、バケットキャプチャーを見て情報が取られているかどうかを確認し、情報は取られていないという結論になったとのことであったが、攻撃の全容を解明すべく、外部のセキュリティ業者に依頼した方が良いとする提言もあった。 |
| | 2021年10月27日 | SQLインジェクション攻撃を解析し、文字列処理ロジックを強化し、更新プログラムをリリースし、SQLインジェクション攻撃に対する脆弱性対策を施した。 |
| K管理画面への再度の不正 | 2021年10月25日<br>17：09から<br>2021年10月26日<br>07:14 | 海外のIPアドレスよりUserID「Y氏」を利用してカード番号の検索が行われ、閲覧用パスワードを入力後、平文のフル桁のカード番号の検索結果が表示された（上記ログはその事を示している。）。 |

| | | |
|---|---|---|
| アクセス及びカード番号照会開始（④） | 2021年10月26日以降<br>2021年11月18日までのアクセス状況 | 多数の不正アクセスが認められた。 |
| | 2021年10月27日<br>00:25から00:34 | 海外IPアドレスによりUserID「Y氏」を利用してカード番号の検索が行われ、不正取得した閲覧用パスワード入力後、平文のフル桁のカード番号の検索結果が表示された。 |
| | 2021年11月18日<br>17:18から18:23 | 海外IPアドレスによりUserID「Y氏」を利用してカード番号の検索が行われ、不正取得した閲覧用パスワード入力後、平文のフル桁のカード番号の検索結果が表示された。<br>なお、この間、平文のフル桁のカード番号を確認可能なURLに対し、約2万回不審な連続アクセスが確認された。 |
| | 2021年12月14日<br>18:08:09 | 海外IPアドレスによるアクセスが確認された。このアクセス以降、日本、海外問わず、不審なIPアドレスからのK管理画面へのアクセスは無い。 |
| | 上記のURLに到達されたログは2万回程度あったとされている。 | |
| バックドアプログラムの設置及び攻撃（③） | 2021年11月11日<br>15:43以降 | ファイルアップロード機能のURLに連続アクセスを開始した。 |
| | 2021年11月11日<br>15:52 | バックドアファイルをアップロードした。 |
| | 2021年11月11日<br>15:57 | バックドアファイルを利用しサーバ上での不正操作を開始した。 |
| | 2021年11月12日<br>6:40 | 不正ファイルへのアクセスが開始された。 |
| | 2021年11月12日<br>6:42 | 不正ファイルへのアクセスが開始された。 |

| | | |
|---|---|---|
| 情報漏えい懸念の認識及び対応（b） | 2021年12月14日 | MPは、イベントペイのアクワイアラであるE社よりカード番号の漏えい懸念の連絡を受ける。 |
| | 2021年12月15日 | MPは、E社よりカード番号漏えい懸念のあるカード情報を入手し、社内調査によりイベントペイの不特定多数の加盟店での情報漏えい懸念を確認したため、イベントペイ加盟店に対し、カード決済の提供停止をメールにより通知する。 |
| | 2021年12月16日 10:00 | MPは、自主判断により、イベントペイを停止した。 |
| | 2021年12月17日 | 増沢将秀氏が、経営会議において、概要、下記のとおり報告した。<br>＜イベントペイ、情報漏えいについて＞<br>①12/14よりE社及びクレジット協会より疑義連絡あり<br>②E社では対象が確認できず、G社（カード会社）で10件程度確認<br>③G社からの資料では、傾向の確認ができない<br>④12/15に12/16より決済停止を案内　16日停止<br>⑤フォレンジック調査開始　見積もりの上20日から調査を開始（最長1か月） |
| | 2021年12月17日 | MPは、G社より、イベントペイ不正利用に関し、追加の被害発生情報を入手する。 |
| | 2021年12月17日 | MPは、PCFに「イベントペイ」のフォレンジック調査を依頼する。 |
| | 2021年12月20日 | MPは、「会費ペイ」で複数の不正利用発生情報を加盟店より受領する。 |
| | 2021年12月21日 | MPは、G社より情報漏えい懸念のある加盟店66加盟店を入手した。確定情報ではないリストの中に、Web決済（トークン方式）の情報漏えい懸念も含まれていた。 |
| | 2021年12月21日 | 地井良太氏から株式会社メタップスに対し、概要、以下のとおり報告した。<br>・MP決済に関するカード情報漏えい懸念について、「会費ペイ」「WEB 決済」での不正利用疑いが判明し、決済システム側での事故である可能性が極めて高い状況である。 |

| | | |
|---|---|---|
| | | ・現在フォレンジック調査の結果までに 1 か月はかかる。<br>・最大リスクとして、現時点、疑いがある情報の精査により、カード会社側の判断で「クレジット決済停止」を求められる可能性がある。 |
| | 2021 年 12 月 23 日 | PCF に調査対象を決済システムに拡大を依頼する。 |
| | 2021 年 12 月 27 日 | 地井良太氏より、取締役会において、12 月 17 日経営会議報告事項に加え、報告事項として、カード漏えい懸念の報告が行われた。<br>①12/23 E 社より、イベントペイを対象にフォレンジック調査指示。12/23 に調査範囲を「決済サーバー&決済管理画面」に拡大する旨の追加発注。<br>②12/24 E 社より、会費ペイ及びレットに対する停止及び調査実行の追加指示。<br>③現時点で社内調査において、情報漏えいの検討がついていない状況。 |
| | 2021 年 12 月 28 日 10:17 | MP は、F 社より、アップリンク・ラボの停止指示を受ける。 |
| | 2021 年 12 月 28 日 23:59 | MP は、アップリンク・ラボ（トークン方式）を停止する。 |
| | 2021 年 12 月 29 日 12:00 | MP は、レット（トークン方式）を停止する。 |
| | 2021 年 12 月 29 日 | MP は、トーク決済利用加盟店に注意喚起をメール通知する。 |
| | 2022 年 1 月 5 日 | MP は、会費ペイを停止する。 |
| K 管理画面に対する不正アクセスの認識及び対応(c) | 2022 年 1 月 5 日 | MP は、上記フォレンジック調査の過程で、K 管理画面に対する不正アクセスを初めて確認する。 |
| | 2022 年 1 月 6 日 | 管理用サイトに Basic 認証を追加。 |
| | 2022 年 1 月 6 日 | 経済産業省　商務・サービスグループ商取引監督課より連絡があり、経済産業省に対し、状況報告を行う。 |
| SQL インジェクションの影響範囲の認識及び対応(d) | 2022 年 1 月 6 日 18:20 | MP は、PCF より、SQL インジェクション攻撃により、A 社アプリから DB 格納データの情報を窃取できることを確認した旨の報告を受けた。 |
| | 2022 年 1 月 7 日 | 当時の IT 推進部副部長が、経営会議において、下記のとおり報告した。 |

| | | |
|---|---|---|
| | | ＜情報漏えい懸念報告＞<br>①1/6（木）18:20　PCF より<br>・A 社アプリから SQL インジェクション攻撃による DB 格納データを窃取できることを確認<br>・別手段を含め対象範囲について調査継続中<br>②現状の脆弱性に対応する必要がある。<br>・管理画面サーバから確認用サイト、A 社アプリの分離<br>・A 社用 DB と PaymentDB の分離<br>→A 社アプリに 1 時間程度の停止が必要 |
| | 2022 年 1 月 8 日 | MP は、A 社アプリのサーバの分離を実施 |
| | 2022 年 1 月 11 日 | MP は、カード会社複数社に対し、1 月 8 日までの会社対応を報告（報告の際、1/13 付け PCF レポートの方向性も共有）した。なお、F 社から既存加盟店の決済停止は不要との回答を得る。 |
| バックドアプログラム経由での攻撃の収束<br>（⑤） | 2022 年 1 月 7 日<br>20:24 | 最後に不正ファイルへのアクセスが確認された時刻。 |
| | 2022 年 1 月 18 日<br>9:59 | 最後に不正ファイルへのアクセスが確認された時刻。 |
| | 2022 年 1 月 18 日 | IT 推進部従業員がサーバ内のアプリケーションを分離、細分化を行ったことにより、バックドアプログラムが入っていたサーバにアクセスできなくなった。 |
| | 2022 年 1 月 19 日 | アプリケーション機能分離を実施(管理用サイトのサーバ分離)。 |
| | 2022 年 1 月 20 日 | MP は､A 社アプリのアップロードプログラムを削除（アップロード機能の停止）する。 |
| | 2022 年 1 月 21 日 | MP は、K 社（カード会社）から 1 月 8 日以降も情報漏えいの懸念がある旨の報告を受けた。 |
| | 2022 年 1 月 22 日 | MP は、2022 年 1 月 21 日に受領した K 社 12 件のログの社内検証結果として、判明している原因（K 管理画面に対する不正アクセスや SQL インジェクション攻撃)以外でクレジットカード情報が窃取されていると判断した（1 月 8 日までの対策のみでは情報漏えいを防ぎきれていないことを認識した。)。 |

| | | |
|---|---|---|
| | 2022年1月23日 | トークン方式の停止を自主判断した。 |
| | 2022年1月24日 | 和田洋一氏が、取締役会において、概要、下記の通り報告した。<br>・クレジットカード決済の一部「トークン方式」について停止を行う。<br>・サービス再開についての対応については、決済代行業者を監督する立場にある各アクワイアラでの許可に加えて、クレジットカードインフラ事業者の所管である経済産業省への報告が必須の状況である。<br>・トークン決済を止めることの影響が大きいためそれを公表するという説明を経済産業省にした。経済産業省には全件を止めることは出来ないと説明した。 |
| | 2022年1月24日<br>21:00 | MPは、前記フォレンジック調査の過程で、バックドアプログラムファイルを確認した。 |
| | 2022年1月25日<br>02:20 | MPは、バックドアとなる対象プログラムを全部削除した。 |
| その後の対応(e) | 2022年1月28日 | MPは、トークン決済を全停止した。 |
| | 2022年1月28日 | A社アプリセクション管理の脆弱性の対応（Basic認証も追加)。 |
| | | 管理用サイトのクロスサイト･スクリプティングに対応（Basic認証も追加)。 |
| | | 復号APIのディレクトリトラバーサルに対応。 |
| | 2022年1月28日 | 増沢将秀氏が、経営会議において、概要、下記のとおり、報告。<br>＜リンク方式停止の件＞<br>①9日以降の問題については原因判明。止血も完了して現状は最終確認に入っている。<br>②31日にK社へレポート提出し、先方の判断を仰ぐ予定。 |

| | | |
|---|---|---|
| | 2022年1月29日 | プロダクト名・バージョン情報の非表示対応及び改ざん検知設定を修正。 |
| | 2022年1月30日 | アプリケーションサーバのバージョンアップを実施した。 |
| | 2022年1月31日頃 | K社に対し、1/25付けPCFレポート、1/30付けPCFレポートをそれぞれ提出し、止血が出来ているということを説明し判断を仰いだところ、決済全体を止める必要がない旨の回答を得る。 |
| | 2022年2月4日 | 増沢将秀氏が、経営会議において、概要、下記のとおり、報告した。<br>＜情報流出懸念について＞<br>①原因追及、止血については調査会社確認の元で完了している停止範囲の拡大等には至ってはいない状況である。<br>②範囲について、リンク方式・コンビニを含めた全体に及ぼしている可能性がある。該当のデータベースに不正アクセスされていた形跡がある、現在調査中であり特定作業が重要な局面、優先してIT推進部のリソースを用いる。 |