公表資料

株式会社メタップスペイメントにおける改善策の実施状況

令和４年８月31日　個人情報保護委員会

- 個人情報保護委員会は、株式会社メタップスペイメント（以下「MP社」という。）に対し、令和４年７月13日に指導を行い、同年８月１日を期日とし改善策実施状況について報告を求めていた。
- 今回の改善策の実施状況に関して特に問題は見当たらない。当委員会としては、MP社が前記改善策を確実に実施することを、引続き注視していく。

１．組織的安全管理措置

	事実概要	指導概要	策定した再発防止策及び実施状況
1	MP社では、情報セキュリティ基本規程上、個人データを含む自社が保有する情報資産（以下「情報資産」という。）について棚卸しを実施することになっていたものの、情報資産管理台帳の整備がされていなかったため、棚卸しが適切に実施されず、どのシステムにおいて情報資産を取り扱っているかすら把握していなかった。 また、個人データの取扱状況についての監査・点検も一部実施しておらず、その重要性に見合った取扱いを行っていなかった。 さらに、MP社では、内部監査規程等において規程の外形のみ整備していたものの、それを実行するための適切な人員配置等の実質を伴わず、技術的安全管理措置を含む情報セキュリティに対する内部監査が機能していなかった。	経営層及び従業者は、社内手続を通じるなどして個人データを取り扱っている範囲を把握するとともに、全ての個人データについて、定期的に棚卸しを実施し、個人データの取扱状況についての監査・点検を実施すること。	令和４年８月に、「個人情報管理台帳」、「書類・データ管理台帳」といった情報資産管理台帳を情報セキュリティ事務局が整備し、どのシステムにおいて情報資産を取り扱っているかを把握することとした。以降は、情報セキュリティ実施要領に基づき、情報資産を取り扱っている各部門が年１回以上（具体的には四半期ごと）棚卸しを実施し、これを通じて前記情報セキュリティ事務局が情報資産管理台帳を更新するとともに、情報セキュリティ監査責任者（内部監査室長）が中心となって情報資産の取扱状況の監査・点検を行うこととした。 また、令和４年８月から、経営層（代表取締役）が委員長を務めるコンプライアンス委員会において、個人情報保護管理者（管理部門担当役員）が情報資産を取り扱っている範囲を報告するとともに、情報資産の取扱状況に係る監査・点検の結果判明した課題（情報セキュリティに係る問題を含む。）への対処状況等について検討することとした。 さらに、令和４年８月に、情報セキュリティ基本規程等の関連規程を改定し、情報資産を取り扱っている範囲やコンプライアンス委員会において検討した情報セキュリティに係る問題について、委員長（代表取締役）が概要を取りまとめ、取締役会において報告することとした。 加えて、従業者は、令和４年８月１日付けで全従業者宛に発出された社内規程改定に関する周知事項を確認するとともに、情報セキュリティ事務局から共有された情報資産管理台帳を確認することにより、情報資産を取り扱っている範囲を把握することとした。
		経営層は、技術的安全管理措置を含む情報セキュリティに対する内部監査において、能動的に関与することで、内部監査機能の強化を図ること。	MP社では、従前、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内部監査担当に任命されていたり、システム担当の従業者が情報セキュリティ監査責任者に任命され自己監査を行っていた。 内部監査部門の強化として、令和４年８月に、内部監査室が内部監査を行う部門であることを組織上明確にし、内部監査担当者に情報セキュリティ研修を受講させることとした上で、システム担当の従業者が情報セキュリティ監査責任者として自己監査を行うことを禁止するとともに、内部監査室長を情報セキュリティ監査責任者にすることとした。情報セキュリティ監査責任者は、監査役と連携し、技術的安全管理措置を含む情報セキュリティに対する内部監査を行うこととした。 また、令和４年８月に、内部監査規程を改定し、内部監査室長が取締役会に出席し、取締役会において、内部監査の結果について報告するとともに、十分な質疑を行うことを義務付けることとした。

２．技術的安全管理措置

	事実概要	既に策定した再発防止策	主な改善策の実施状況
1	①決済管理画面について、Web上の公開・非公開を定めるルールを定めていなかった上、接続元IPアドレスの制限を設けていなかった。 ②決済管理画面について、ID・PWでのログインが可能となっており、二段階認証や多要素認証、ログイン試行回数の制限等を設けていなかった。	①情報セキュリティ実施要領を改定し、公開・非公開の基準を定める。また、決済管理画面への接続元IPアドレス制限を実施する。 ②決済管理画面への接続可能時間帯を限定するとともに、決済管理画面のログイン方法を多要素認証に変更する。さらに、ログイン試行回数の制限を設ける。	①令和４年７月27日に、情報セキュリティ実施要領を改定し、決済管理画面の公開・非公開の基準を定めた。また、社内用決済管理画面へのアクセスについて、令和４年１月８日から、VPNによるIPアドレス制限を実施するとともに、システム担当の従業者により、不正アクセスがないかIPアドレスの全件確認を実施している。 ②社内用決済管理画面へのアクセスについては、上記の対応に加えて、接続可能時間帯を午前９時から午前０時までに限定している。また、社外用決済管理画面については、令和４年９月から、OTP認証を採用し、ID・PWのほか、ワンタイムパスワードの入力による多要素認証を導入する。さらに、社内用、社外用決済管理画面のいずれについても、ログイン試行回数の制限を設けるとともに、失敗後にログイン再試行した場合には検知する仕組み（必要に応じてブロックする仕組み）を導入済みである。
2	①アクセスログ等は日次で取得し、システム担当に展開されていたものの、システム担当の従業者が不足していただめ、アクセスログの点検は行われていなかった。 ②セキュリティアラートの内容を検証できる従業者が不足していただめ、セキュリティアラートを受信しても十分な検証を行っていなかった。 ③WAFの導入は検討していたものの、WAFを適切に運用するための従業者が不足していたため、WAFの導入は見送られた。 ④決済システムにおいて、データベーススキーマ（データベースにおける構造）が分離されていなかった。	①日次で取得したアクセスログ等を週次で集計・点検する。具体的には、令和４年４月以降、順次、システム担当の従業者を採用した上で、当該従業者が中心となってログチェックメールを確認し、システム担当の責任者が確認内容を再確認する。 ②外部セキュリティベンダとコンサルティング契約を締結し、令和４年５月20日から、受信したセキュリティアラートについて、外部セキュリティベンダとの間で検証を行う。 ③WAFを導入し、不正な侵入などがないか常時確認する。 ④決済システムのデータベーススキーマの分離を行う。	①令和４年４月に、ログモニタリング業務等に従事するシステム担当の従業者を新たに採用し、当該従業者が中心となって日次で取得したアクセスログを週次で集計・点検している。さらに、情報セキュリティ管理責任者が点検内容を再確認している。 ②令和４年５月20日に、外部セキュリティベンダとの間でコンサルティング契約を締結し、検知したセキュリティアラートの内容を同社に確認できる体制を構築した。令和４年８月に、同社による確認・検証を実施するとともに、今後も、必要に応じて同社に確認を行う。 ③令和４年５月９日からWAFを導入した上で、外部委託先が24時間体制で検知状況を確認している。 ④令和４年１月８日に、決済システムにおいてデータスキーマの分離を行うとともに、不正侵入された場合であっても、不正侵入されたデータベース以外へのアクセスができないよう管理を行っている。また、アプリケーション管理の徹底を行うため、システム担当部署によるアプリケーション一覧の棚卸しを四半期ごとに実施し、維持管理を徹底する。
3	①不正アクセスを受けたアプリは、セキュアコーディング（攻撃者やマルウェア等による攻撃に耐え得る頑丈なプログラムを書くこと。エスケープ処理もそれに含まれる。）の対象から外れていた上、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。）やペネトレーション診断（ネットワークに接続されているシステムに対し、実際に既知の技術を用いて侵入を試みること。システムに脆弱性がないかテストする手法。）も行われていなかった。 ②システム担当の従業者が不足しており、通常の業務量に上乗せして修正業務に対応できる余力がなかった。	①ソースコード・レビューについて、脆弱性ソースコード解析ツールにより検証を行うこととし、改修部分について、改修前・改修後を比較して、脆弱性がないか確認することとした。さらに、当該アプリを含む全ての決済システムについてペネトレーション診断を行うこととした。 ②令和４年４月以降、順次、システム担当の従業者を採用した上で、各種診断レポートについて、システム担当の責任者を含むシステム担当の全員にメールで配信するよう設定を変更し、複数の目で確認する。さらに、自動でレポート結果を受信できるように運用を変更する。	①ソースコード・レビューについて、令和４年８月１日から、脆弱性ソースコード解析ツールを導入した上で、全てのアプリケーションについて、リリース前にソースコード・レビューを実施し、改修部分に脆弱性がないか確認している。さらに、令和４年６月から、全ての決済システムに対してペネトレーション診断等を開始し、順次、脆弱性の修正を行っているところ、同年１２月までに完了する予定である。 ②令和４年４月に、システム担当の従業者を新たに採用するとともに、システム担当の全従業者の業務内容を見直し、システム担当部署として修正等の業務に対応可能な体制に変更した。その上で、毎月実施する内部脆弱性スキャンに係るレポートについては、情報セキュリティ管理責任者を含む複数のシステム担当の従業者に自動配信され、複数の従業者による確認を行うことでレポート内容が変更されないようにしている。さらに、配信されたレポート内容については、毎週実施するミーティングで対応を検討している。