平成 29 年 5 月 1 日

各　　位

会 社 名　GMO ペイメントゲートウェイ株式会社
代表者名　代表取締役社長　相浦　一成
（コード：3769　東証第一部）
問合せ先　取締役副社長　村松　竜
（ＴＥＬ．０３-３４６４-０１８２）

再発防止委員会の調査報告等に関するお知らせ

当社は、平成 29 年 3 月 10 日付け「不正アクセスに関するご報告と情報流出のお詫び」及び平成 29 年 3 月 14 日付け「「再発防止委員会」の設置について」にて開示しましたとおり、当社において運営受託しております東京都の都税クレジットカードお支払サイト（以下、都税支払サイト）及び独立行政法人住宅金融支援機構の団体信用生命保険特約料クレジットカード支払いサイト（以下、保険特約料支払いサイト）において、第三者による不正アクセスが確認され、両サイト利用者のクレジットカード情報及び個人情報が流出したことに関し、当社は本件の事実関係の調査、原因究明、再発防止策については、客観的かつ専門的で、より公正性、透明性を有した調査、検討及び判断が必要であると判断し、外部の専門家を交えて構成される再発防止委員会を平成 29 年 3 月 14 日付で設置し、平成 29 年 4 月 30 日まで調査及び再発防止策の検討・実施をしてまいりました。
この度、再発防止委員会の「不正アクセスによる情報流出に関する調査報告書」が取りまとめられ、当社取締役会に対し提出されましたので、下記の通りお知らせいたします。
なお、現時点では不正に取得されたクレジットカード情報の不正利用は確認されておりません。

お取引先様、株主様、投資家及び市場関係者の皆様をはじめ関係各位に、ご迷惑とご心配をおかけしておりますことを心よりお詫び申しあげます。

記

１．再発防止委員会の調査報告書の内容

調査報告書の概要は、以下のとおりです。詳細については、添付資料「不正アクセスによる情報流出に関する調査報告書」をご覧ください。

（１）　本件事故の概要

平成 29 年 3 月 8 日から 9 日にかけ、当社が運営受託している都税支払サイト及び保険特約料支払いサイトにおいて、アプリケーション・フレームワークである Apache Struts 2 の脆弱性(リモートから任意のコマンドを実行可能である脆弱性(S2-045))を利用してサーバ内部にバックドアプログラムを設置され、バックドアプログラム経由で暗号化された会員カードデータ等と個人情報を攻撃者により不正に取得されました。

（２）　再発防止策

再発防止委員会は、短期及び中長期の技術的な防止策と、情報セキュリティマネジメントに関する防止策を実施することを決定いたしました。詳細については、添付資料「不正アクセスによる情報流出に関する調査報告書」第 7　再発防止策をご覧ください。

（３）　再発防止策の実施

当社は再発防止委員会で決定した再発防止策に基づき、平成 29 年 4 月 14 日までに、以下の防止策を実施いたしました。

①技術的な防止策における短期的対策

②セキュリティインシデント対応

③システム開発に関する短期的対策

さらに、都税支払サイトの再開のために、同サイト及び保険特約料支払いサイトを対象として、再発防止の観点から Payment Card Forensics 株式会社による PCI DSS アセスメントを実施いたしました。その結果、同月 14 日時点で PCI DSS 要件を満たしたことが確認されました。

２．経営責任について

本件は、再発防止委員会の調査報告書に述べられているとおり、情報セキュリティに関するマネジメント体制とその運用が要因であり、当社は今回の事態の重要性を厳粛に受け止め、その経営責任を明らかにするため、以下の処分を行うことといたしました。

代表取締役社長	相浦　一成	月次報酬の 30％を３ヶ月減額
取締役副社長	礒崎　覚	月次報酬の 30％を３ヶ月減額
取締役	杉山　真一	月次報酬の 10％を１ヶ月減額

以 上

不正アクセスによる情報流出に関する調査報告書

２０１７年4月３０日

GMO ペイメントゲートウェイ株式会社

再発防止委員会

目次

用語定義 3
第１　調査の概要 5
１　再発防止委員会設置の経緯 5
２　調査の目的 6
３　受任事項 6
４　調査期間 6
５　調査方法 6
第２　本件事故の概要及び経緯 7
１　本件事故の総括 7
２　本件事故の対象となった事業に係る認証取得状況 7
３　本件事故の概要 8
４　検知から初動対応までの時系列 8
第３　本件事故への対応 10
１　脆弱性情報の収集に関する評価 10
２　本件事故への対応に対する評価 10
第４　フォレンジック調査結果 12
１　フォレンジック調査最終報告書の提出 12
第５　情報セキュリティに関するマネジメント体制 13
１　情報セキュリティインシデント管理 13
２　システム開発プロセス 13
第６　リスク全般のガバナンス体制及びコーポレートカルチャー 15
１　全社的リスク管理の課題 15
２　属人的なリスク判断に伴うリスク管理の偏重 15
３　教育・啓蒙活動の鈍化 16
第７　再発防止策 17
１　技術的な防止策 17
２　情報セキュリティマネジメントに関する防止策 17
３　リスク全般のガバナンス体制及びコーポレートカルチャーに関する防止策 19
４　再発防止策の実施 20

用語定義

本書で使用する用語・略語について説明する。

索引	用語	説明
G	GMO-PG	GMO ペイメントゲートウェイ株式会社
I	IPA	Information-technology Promotion Agency 独立行政法人情報処理推進機構
	ISMS	Information Security Management System: 情報セキュリティマネジメントシステム､情報資産を適切に管理し守るための包括的な枠組み
J	JPCERT	Japan Computer Emergency Response Team: コンピュータセキュリティ情報の収集と情報発信､インシデント対応支援等を行う一般社団法人
P	PCF 社	Payment Card Forensics 株式会社
	PCI DSS	Payment Card Industry Data Security Standard: クレジットカード情報を安全に守るために､国際クレジットカードブランドが共同で策定したグローバルセキュリティ基準
W	WAF	Web Application Firewall: ファイアウォールの一種。 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・遮断を行なうソフトウェアや機器
あ	アプリケーション･フレームワーク	ある領域のアプリケーションに必要とされる機能や処理を部品としてまとめたソフトウェア群
さ	再発防止委員会	本件事故の事実関係・原因の調査、再発防止策の提言を目的に外部の専門家を交えて構成された委員会
し	情報セキュリティ委員会	GMO-PG の情報セキュリティ管理規定に基づき、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
は	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
ふ	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・遮断等の制御を行なうソフトウェアや機器
	フォレンジック調査	不正アクセス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
	プライバシーマーク	個人情報について適切な管理措置･体制を備えている事業者等を認定する制度

ほ	本部	GMO-PG の事業を運営する組織体 https://corp.gmo-pg.com/company/figure/
り	リスク管理委員会	GMO-PG のリスク管理規定に基づき、全社リスクを管理するために社内に設置した委員会

第１　調査の概要

１　再発防止委員会設置の経緯

GMO-PG は、2017 年 3 月 9 日、IPA（独立行政法人情報処理推進機構）の「Apache Struts 2 の脆弱性対策について(CVE-2017-5638)(S2-045)」並びに JPCERT の「Apache Struts 2 の脆弱性（S2-045）に関する注意喚起」の情報に基づき、GMO-PG システムへの影響調査を開始したところ、GMO-PG において運営受託している東京都税クレジットカード支払サイト（以下「**都税支払サイト**」という。）及び独立行政法人住宅金融支援機構の団体信用生命保険特約料クレジットカード支払いサイト（以下「**保険特約料支払いサイト**」という。）において、第三者による不正アクセスが確認され、両サイト利用者の個人情報が流出するという事故（以下「**本件事故**」という。）の発生が確認された。

GMO-PG は、本件事故の事実関係の調査、本件事故の原因究明、責任の所在の明確化、再発防止策については、客観的かつ専門的で、より公正性、透明性を有した調査、検討及び判断が必要であると判断し、外部の専門家を交えて構成される再発防止委員会を 2017 年 3 月 14 日付で設置した。

再発防止委員会の委員は、以下のとおりである。

役職	氏名	所属
委員長	相浦　一成	代表取締役社長
委員	村松　竜	取締役副社長
委員	礒崎　覚	取締役副社長
委員	久田　雄一	専務取締役
委員	木村　泰彦	取締役
委員	杉山　真一	取締役
委員	吉岡　優	取締役
委員	中村　好伸	中村好伸法律事務所 弁護士
専門家アドバイザー	大井　哲也	TMI 総合法律事務所 弁護士
専門家アドバイザー	白井　邦芳	社会情報大学院大学 広報・情報研究科 教授
専門家アドバイザー	大河内　貴之	PCF 社 フォレンジック・ シニアコンサルタント

2　調査の目的

本報告書は、2017 年 4 月 30 日までの調査に基づき、次項記載の受任事項に関して、本報告書提出時における再発防止委員会の見解を報告することを目的としたものである。

なお、本報告書は、GMO-PG が再発防止委員会を構成した目的に照らして、あくまで客観的な見地から、当該受任事項について再発防止委員会の見解を述べるものである。

3　受任事項

再発防止委員会の受任事項は、以下のとおりである。

（1）本件事故の事実関係の調査
（2）本件事故の原因調査
（3）再発防止策の提言

4　調査期間

2017 年 3 月 14 日から同年 4 月 30 日まで

5　調査方法

再発防止委員会は、本報告書を作成するに当たり、次の方法に基づいて調査を実施し、上記調査期間内に開示等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て本報告書を作成した。

（1）インタビューによる調査
（2）社内規程等のドキュメントのレビュー
（3）各種ログの調査
（4）実地による技術調査

以降、第２から第６までは、再発防止委員会の外部の専門家アドバイザーからの報告によるものであるが、セキュリティリスクとなり得る情報については、記載していない。

第２　本件事故の概要及び経緯

１　本件事故の総括

GMO-PG では、2008 年 12 月に最初の PCI DSS 認証を取得し、年次での再認証監査を 8 回経た上で、2016 年 12 月に最新の認証を取得しており、クレジットカード情報を取扱う事業者として要求されるべき一定レベルの情報セキュリティ体制を具備していたものの、本件ではそのような体制が Apache Struts 2 の未知の脆弱性を突いたゼロデイ攻撃に対しては、奏功しなかったという事案である。

また、GMO-PG では、Apache Struts 2 の脆弱性リスクの重大性に鑑み、2016 年 4 月に Apache Struts 2 の使用を停止する「脱 Struts 宣言」をし、以降新規のシステムにおいては、Apache Struts 2 の使用を取りやめている。

他方で、既存の一部のシステムについては、システム変更の影響と顧客業務への影響が大きいことから、Apache Struts 2 の都度アップデート等個別対応に留めており、その最中に攻撃を受けてしまったという不運な面も否定できない。

もっとも、脆弱性情報の早期収集体制の改善、不正検知能力の向上、データ隠蔽対策の改善、セキュリティに配慮したシステム構築のプロセスの改善等、より堅牢な情報セキュリティシステムを構築するための不断の努力をすべきことには変わりなく、再発防止委員会では、本件事故の原因究明のみならず、GMO-PG の全般的な情報セキュリティ体制を改めて見直すことにより、再発防止を徹底するために実装すべき多層的なセキュリティ施策を提示した。

２　本件事故の対象となった事業に係る認証取得状況

GMO-PG では、2006 年 4 月に最初の ISMS 認証を取得し、その後、3 年ごとの再認証監査を 3 回経た上で、2014 年 12 月に最新の認証を取得した。なお、ISMS は認証期間が 3 年である一方で、年次でサーベイランス監査という外部監査を受ける必要があるところ、GMO-PG は同監査についても受けている。

また、GMO-PG では、2008 年 12 月に最初の PCI DSS 認証を取得し、年次での再認証監査を 8 回経た上で、2016 年 12 月に最新の認証を取得した。

さらに、GMO-PG では、2009 年 9 月に最初のプライバシーマークを取得し、2 年ごとの監査を 3 回得た上で、2015 年 9 月に最新のプライバシーマークを取得した。

3　本件事故の概要

2017 年 3 月 8 日から 9 日にかけ、GMO-PG が運営受託している都税支払サイト及び保険特約料支払いサイトにおいて、アプリケーション・フレームワークである Apache Struts 2 の脆弱性(リモートから任意のコマンドを実行可能である脆弱性(S2-045))を利用してサーバ内部にバックドアプログラムを設置され、バックドアプログラム経由で暗号化された会員カードデータ等と個人情報を攻撃者により不正に取得された。

4　検知から初動対応までの時系列

日付	時刻	イベント	GMO-PG 担当者
3/6	22:14	US Apache Site で脆弱性(S2-045)を公表。公表時点は、Max Security Level は、High、その後は、3/20 5:59 に Critical に変更された。	
3/7	15:21	Github で攻撃コード公開	
3/8	04:54	保険特約料支払いサイトへ攻撃開始	
	04:57	保険特約料支払いサイトにバックドアプログラムが置かれる。	
	10:43	JPCERT 早期警戒情報発信	(注)この時点では、未加入
	15:25		外部のセキュリティ情報提供サービスより、本件脆弱性情報をメールで受信
	16:51	都税支払サイトへ攻撃開始	
	17:14	都税支払サイトにバックドアプログラムが置かれる。	
	17:40	都税支払サイト DB に不正アクセス開始	
	18:20	都税支払サイトにてアプリケーション例外が発生していることを検知	不正アタックと判断し、ファイアウォールにて攻撃元 IP を遮断
	23:53	都税支払サイト DB に不正アクセス終了	

日付	時刻	イベント	GMO-PG 担当者
3/9	02:30	保険特約料支払いサイト DB に不正アクセス開始	
	04:59	保険特約料支払いサイト DB に不正アクセス終了	
	18:00	本件脆弱性に関する IPA の注意喚起を把握	本件脆弱性情報を認識
	21:56		本件に関連する攻撃について、WAF による遮断を実施
	22:40		緊急対策本部を設置
	23:53		Apache Struts 2 が稼動しているシステムを全て停止し、ネットワーク未接続状態にあったバックアップシステムへの切替
3/10	00:30		上記バックアップシステムへ Apache Struts2 パッチ適用(パーサ変更)
	02:15		都税支払サイト、保険特約料支払いサイトで不正侵入の痕跡と DB への不正アクセスを確認
	08:05		関係各所へ連絡、対応協議開始
	09:20		PCF 社へフォレンジック調査依頼
	11:15	都税支払サイトのサービス停止	
	11:30	保険特約料支払いサイトのサービス停止	
	14:00		二次被害防止のため関連カード会社に流出した可能性のあるカード情報の連携を開始（19:30 に終了）
	17:00		臨時コールセンターをオープン
	18:22		本事案の HP 公表と適時開示

第３　本件事故への対応

１　脆弱性情報の収集に関する評価

（１）本件脆弱性情報に関する外部契約先からの情報共有

GMO-PG は、外部のセキュリティ情報提供サービスから本件脆弱性情報について、3 月 8 日 15 時 25 分にメール（以下「**本件メール**」という。）にて情報を取得していたが、セキュリティ担当者が内容を確認しておらず、本件脆弱性情報の重要性を即座に認識できなかった。

（２）本件における脆弱性情報の収集の評価

Apache Struts 2 の脆弱性「S2-045、CVE-2017-5638」は、リモートから任意のコードが実行可能な脆弱性であった。そのため、悪意のある第三者がこの脆弱性を利用するとインターネット経由でバックドアプログラムの設置又は削除が可能であった。GMO-PG の脆弱性情報の収集に関しては、3 月 8 日 15 時 25 分に本件脆弱性情報が本件メールとして通知されているものの、本件メールには危険度を示す表示はなかった。また、GMO-PG のログ解析の結果によれば、3 月 8 日 4 時 57 分に最初のバックドアプログラムが設置されていることが判明しているが、この時点でも危険度が不明であった。さらに、本件メールによる通知は、Apache Struts 2 の開発元である Apache Software Foundation の脆弱性情報発信から 2 日間の遅れがあった。

GMO-PG は、特にオープンソースソフトウェアである Apache Struts 2 を使用する場合には、開発元の提供している情報を収集して、その情報をもとに自社内でセキュリティ対策を行うべきだった。

２　本件事故への対応に対する評価

（１）本件事故の発覚前後のアクション

GMO-PG は、3 月 8 日の 18 時 20 分、アプリケーション例外が発生していることを検知し、これについては不正アタックと判断し、直ちにファイアウォールにおいて攻撃元の IP アドレスからの通信を遮断した。しかしながら、かかる不正アクセス自体は同日の 23 時 53 分まで続いた。

その後、セキュリティ担当者が Apache Struts 2 の脆弱性の詳細情報を認識したのは、3 月 9 日の 18 時であり、かかる情報を受けて、GMO-PG は、調査を開始し、同日 20 時に情報流出の可能性を認識した。そして、GMO-PG は、同日 21 時 56 分に、緊急対策として WAF による遮断を実施した。

このように、GMO-PG では、実務に応じた対応マニュアルに従った一応の初動対応はなされていた。

（2）緊急対策本部の設置とその後の緊急対策指示

3 月 9 日 22 時 40 分には緊急対策本部が本社に設置された。

Apache Struts 2 の脆弱性の脅威を考慮すれば、速やかに緊急対策本部を設置したことは、GMO-PG 内の指揮系統を一つとし、トップダウンによる優先事項への対応を徹底するために重要な判断であったと評価できる。

（3）関係者への報告及び公表までのプロセス

GMO-PG は、3 月 10 日までには、関係省庁を含む多数の関係者への報告を完了するとともに、渋谷警察署への通報も実施した。さらに、GMO-PG は、本件事故の被害の抑止を目的として、同日 11 時 15 分には、都税支払サイトを、また、同日 11 時 30 分には、保険特約料支払いサイトを停止した。

また、GMO-PG は、不正利用による二次被害防止のために同日 14 時 00 分から関連のカード会社に流出した可能性のあるカード情報の連携を開始し、同日 17 時、本件事故に対応するためコールセンターを開設した。

なお、同日 18 時 22 分には、本件事故に関する適時開示とホームページ上での公表を行っている。

以上のような、緊急対策本部の設置から関係者への報告、公表までのプロセスについて、時間的な遅滞はなかったと評価できる。

第４　フォレンジック調査結果

１　フォレンジック調査最終報告書の提出

GMO-PG は、2017 年 3 月 31 日に PCF 社よりフォレンジック調査の最終報告書（以下「**最終報告書**」という。）を受領した。GMO-PG としては、即時に最終報告書において推奨されている各施策を含めた再発防止策を推し進めた。

第５　情報セキュリティに関するマネジメント体制

１　情報セキュリティインシデント管理

（１）脆弱性についての情報収集と脆弱性に関する対応体制の不備

GMO-PG では、セキュリティインシデントに関する社内規定として対応手順を定めており、脆弱性が見つかった場合には、情報セキュリティ委員会事務局にかかる事実に関する報告が上がり、その後の対応が指示されていくこととなるとされている。

もっとも、GMO-PG が脆弱性に関する情報を収集する手段としては、外部のセキュリティ情報提供サービス等からの情報受領に限られていた。また、収集した脆弱性情報について、規程として対応手順が存在していたが、対応手順を具体化するためのチェックリスト、フロー及び連絡先一覧のように、情報をエスカレーションするための手続については、実務担当者が依拠できる詳細かつ具体的なマニュアルが存在していなかった。

２　システム開発プロセス

（１）本件事故に係るシステム開発について

ア　Apache Struts 2 の使用に対するリスク認識

GMO-PG では、2010 年頃、ある自治体の自動車税支払サイトにおいて、初めて Apache Struts 2 が使用されることになった。その後、自動車税以外の税目に係るクレジットカード支払サイトシステムの構築も受託したが、同システム構築は上記自動車税支払サイトと同様の手法で行われたため、都税支払サイトにおいても Apache Struts 2 が使用されることとなった。

一方で、保険特約料支払いサイトは、都税支払サイトと比較すると、画面遷移等の点において異なる点が多く、一からシステムを構築しなければならない箇所が多かったものの、そのシステム構築にあたっては、Apache Struts 2 が使用された。

2013 年から 2014 年頃にかけて、Apache Struts 2 の脆弱性をついた不正アクセスによる事故が各地で多数発生していたものの、GMO-PG では、Apache Struts 2 の脆弱性情報が出される都度対応し、不正アクセスを防止してきたという実績から、積極的に Apache Struts 2 の使用を停止し、他のソフトウェアを採用するには至らなかった。その後、2014 年秋頃から、GMO-PG のセキュリティ担当者と開発担当者の間では、Apache Struts 2 の脆弱性によるリスクの重大性から、Apache Struts 2 の使用を停止することについて検討し、議論が行われるようになった。もっとも、Apache Struts 2 の使用を取りやめ、既存のシステムの変更を行うことになると、顧客等の関係者に与

える影響が大きいため、既存システムにおける Apache Struts 2 の使用のリスクが経営層にエスカレーションされることはなかった。

近年、脆弱性に対する攻撃の手法は多様化かつ高度化しており、その対策が十分に功を奏さない場合もある上、前述のとおり、仮に攻撃を受け、不正アクセスが行われた場合に生じる影響は甚大である。それにもかかわらず、GMO-PG における Apache Struts 2 の脆弱性に関するリスクの認識は不十分であり、この点について、社内におけるより慎重な議論が必要であった。

しかしながら、2016 年 4 月には Apache Struts 2 の使用を停止する「脱 Struts 宣言」をし、以降新規のシステムにおいては、Apache Struts 2 に依存しないシステム構築が行われるようになったが、既存の Apache Struts2 使用システムの再構築には至らなかった。

イ　保険特約料支払いサイトにおけるセキュリティコードの出力

通常、コードレビューは、コーディングを担当していないメンバーで実施されるところ、保険特約料支払いサイトの開発では、オンライン部分の構築を担当していたメンバーがコーディングをしつつ、自らコードレビューも行っていた。また、保険特約料支払いサイトにおいては、コードレビュー後に、検証が十分に行えていなかったこともあり、結果的にセキュリティコードが出力されることになった。

セキュリティに配慮したシステム開発を実現するためには、セキュリティ担当者がセキュアコーディングの基準を策定し、それが開発担当者に遵守されているかを確認するなど、セキュリティ担当者と開発担当者が密に連携をとり、開発現場における課題の共有、課題の評価、そして課題解決のための方策の検討・実施という問題解決のプロセスが実行されなければならない。

GMO-PG では、月次の会議において、個別のアプリケーションやシステムの脆弱性に関する情報共有がなされているものの、セキュリティに配慮したシステム開発に関するセキュリティ担当者と開発担当者の連携が少なく、上記の問題解決のプロセスの実行が不十分であった。

第６　リスク全般のガバナンス体制及びコーポレートカルチャー

１　全社的リスク管理の課題

（１）リスクの抽出及び重大リスクの選定プロセス

本来、経営リスク管理プロセスにおいては、経営管理の上流で全社的なリスクを抽出し、評価すべきであるが、GMO-PG では、各本部におけるリスク評価結果をリスク管理委員会が追認するというプロセスがとられており、リスク管理委員会としての俯瞰的なリスクの検証が適切に行われていない状況であった。また、リスク管理委員会が毎年一度しか開催されておらず、平時からのリスクモニタリングやリスク量の変動に伴う速やかな対応がなされていない状況であった。

個別のリスクに対する評価は、各本部自身がそれぞれ影響度・頻度を定性的に評価しているに過ぎず、リスク量の変動等については客観性に乏しい結果となっていた。本件事故の原因とも言える「大規模の脆弱性発覚」のリスクは、本来、看過できない重大なリスクであったと考えられるものであるが、経営管理の上流での検討が十分になされないまま、現場サイドの判断によって重大リスクから漏れてしまっていた。

（２）重大リスクの選定後の管理不備

リスク管理委員会は、重大リスクを選定後、その概ねのコントロール手法を確認し、方向付けをした後、各本部に関係するリスクに対する四半期ごとのリスク量の見直しと、検証結果の報告を指示していたが、実際に各本部に振り分けられたリスクへの対応に関する活動について議論の場は開催されていなかった。

２　属人的なリスク判断に伴うリスク管理の偏重

GMO-PG では、リスク管理委員会委員長が、情報セキュリティ委員会委員長、さらにシステム本部本部長を兼任していた。リスク管理は、本来マトリックス的に様々な視点からダブルチェックされるべきであるが、その牽制機能が働きにくい状況にあった。

また、GMO-PG のコーポレートカルチャーとして、個人の能力を高く評価し、一定の判断裁量や決定権限を与えているが、これは現場における意思決定のスピードを速めるメリットもあるものの、現場担当者等による一次的な初期判断の失敗が最終的に経営リスクに及ぶ事態を惹起させる可能性がある。

さらに、リスク管理規程では、個別の重大リスクを監視、コントロールする目的で小委員会を設置することを認めているが、リスク管理委員会、システム本部、情報セキュリティ委員会の役割、責任分担が不明瞭であったため、本来あるべきマトリックス的な牽制機能が働いていなかった。

3　教育・啓蒙活動の鈍化

システム開発に伴う開発体力不足や納入日・サービス開始日までの遅延リスク等、会社の目前の利益に直結するリスクに関心が集中し、長期的な視点でのセキュリティ教育、啓蒙活動が疎かになった結果、会社が有する多様かつ不変なリスクへの対応が不十分となっていた可能性がある。

第７　再発防止策

再発防止委員会は、前述の第２から第６の報告を受け、以下に列挙する再発防止策を実施することを決定した。

なお、技術的な再発防止策については、セキュリティリスクになり得るため、最小限の記述に留めている。

１　技術的な防止策

（１）短期的対策

ア　不正リクエストの遮断（入口対策）の改善対応

イ　不正プログラムの配置抑止の改善対応

ウ　データ隠蔽対策（重要情報のマスク化等による非保持化）の改善対応

エ　データ持ち出し抑止(出口対策) の改善対応

（２）中長期的対策

ア　既存の Struts2 廃止対応

代替フレームワークの選定にあたっては、過去の脆弱性数等リスク低減の観点や、サポートの観点から比較検討を実施する。

イ　SQL レベルの不正アクセス検知の改善対応

ウ　GMO-PG の全システムを対象とした PCI DSS 再監査の実施

２　情報セキュリティマネジメントに関する防止策

（１）セキュリティグループにおける人的リソースの確保

セキュリティグループに、情報セキュリティに関する専門的知識を有する人員を補充すべきである。その上で当該人員の専門的知識を活用し、リスク管理担当者、コンプライアンス担当者等の意見も踏まえ、システムの開発及び運用を含めた全体的な情報セキュリティマネジメントを再度見直し、社内規程の改訂、運用体制の見直しを進める。

（２）リスクアセスメント

ア　外部の専門家の参加

情報セキュリティ委員会に、情報セキュリティに関するノウハウを有する人員（外部専門家が望ましい。）を参加させ、リスクアセスメントのリスク項目に漏れがないかのチェックや、資産価値、脅威、脆弱性の評価の妥当性の検証等、リスクアセスメントを実効的に行えるようにする。

イ　情報セキュリティ委員会の役割の明確化

リスクアセスメントにおけるリスク管理委員会と情報セキュリティ委員会との役割分担や委員会としての実施事項の明確化を図るべく、社内規程や組織体制の見直しが必要である。

例えば、情報セキュリティ委員会をリスク管理委員会の下部組織として位置付け、システム関連のリスクアセスメントについては情報セキュリティ委員会において実施し、リスク管理委員会に上程する体制をとることなどが考えられる。

（3）セキュリティインシデント対応

ア　脆弱性情報の早期入手

脆弱性情報入手方法の改善として各種の情報ソースを活用し、脆弱性情報を社内関係者に共有できる仕組みを確立する。

イ　脆弱性情報等に関する情報のエスカレーションプロセスの策定

チェックリスト・フロー・連絡先一覧のように、情報をエスカレーションするためのマニュアルを策定（追記）することにより、エスカレーションプロセスを明確化することが必要である。その際、情報セキュリティ委員会及びシステム本部の両方の関係者が情報共有出来るようにする。

（4）システム開発

ア　ソフトウェアの選定基準を明確にすること

GMO-PG としては、システム開発において使用するソフトウェアに関して、どのような内容及び頻度で脆弱性が発現されてきたか、脆弱性が公表されてからセキュリティパッチの提供開始までのタイムラグがどの程度あるか、当該ソフトウェアに関し、外部の業者からシステムセキュリティのサポートを受けることができるか否かといった点等を考慮要素とした上で、ソフトウェアの選定基準を明確にすべきである。また、当該選定基準に照らして使用することが不適切であると評価されるソフトウェアが既存システムに使用されている場合には、速やかに当該ソフトウェアの使用停止を検討する。

イ　セキュリティに関する社内規程等をより具体化すること

GMO-PG としては、要件定義、設計、構築、試験といったシステム開発の各工程において遵守すべきセキュリティ基準をより具体的にするという観点から、システムセキュリティ基準やシステム開発標準化基準の内容を明確化する。

ウ　セキュリティグループと開発グループとがより連携を図ること

（1）で挙げたセキュリティグループの権限強化、人員補充をもとに、セキュリティグループが個々のシステムのセキュリティに関する理解を深めることを前提として、セキュリティグループと開発グループとが、それぞれのセキュリティに関する課題（特に、個々のシステムのセキュリティに関する課題）を共有し合うべきである。その上で、両グループが当該課題を評価し、解消するための具体的な方策を検討・実施していくために、より緊密に連携を図っていく。

（5）情報セキュリティに関する教育活動

教材の改訂、外部講師による教育等により、重大な脅威や、不正検知等、他の攻撃方法についての知識を得られるように改善する。

3　リスク全般のガバナンス体制及びコーポレートカルチャーに関する防止策

（1）全社的リスク管理の課題

ア　リスクの抽出及び重大リスクの選定プロセスへの対応

個別リスクの評価については、担当する部署内での限定的評価ではなく、社内での一定の役職者以上の全員で評価することが望ましい。また、重大リスクの選定に関しては、内部統制上の脆弱性判断基準を背景にコントロール手法を確立することが重要である。

前述の脆弱性判断を行った上で、個別リスクの残存リスクを判定し、リスクコントロール対応について決定する。

イ　重大リスクの選定後の管理不備への対応

現在のリスク管理規程は、リスク管理委員会の開催の回数について年１回以上としているが、PDCA の観点を考慮する場合、少なくとも四半期ごとに開催し、重大リスクの管理状況をリスク管理委員会において確認する。

（2）少数責任管理制度下でのリスクの増幅への対応

会社全体に影響を与えるリスク判断を現場の特定の社員に限定して行わせることは、相当かつ過大なリスクを伴う。従って、そのような場合は、少なくともその判断の過程で取締役会か業務担当取締役への報告及び承認を経ることとする。

（3）教育・啓蒙活動の鈍化への対応

本件事故に伴い、多くの改善すべき課題が確認された。課題解決にはシステム対応のような技術的対応も多く含まれるが、人的・組織的な改善行為の多くは、教育・啓蒙活動が中心となる。一過性の対応ではなく、今回のような事故を二度と起こさないよう年度ごとに教育・啓蒙活動を計画としてスケジュール化し、しっかりと改善活動が組織内に根付くよう運用管理していくことが重要である。

4　再発防止策の実施

GMO-PG では、再発防止委員会で決定した上記 1 から 3 の再発防止策に基づき、2017 年 4 月 14 日までに、以下の防止策を実施した。

・技術的な防止策における短期的対策
・セキュリティインシデント対応
・システム開発に関する短期的対策

さらに、都税支払サイトの再開のために、同サイト及び保険特約料支払いサイトを対象として、再発防止の観点から PCF 社による PCI DSS アセスメントを実施した。その結果、同月 14 日時点で PCI DSS 要件を満たしたことが確認された。

以上