平成 20 年９月５日

各　　位

本社所在地　大阪市中央区農人橋一丁目１番22号
大江ビル10階
会社名　ミネルヴァ・ホールディングス株式会社
代表者　代表取締役会長兼社長　中島　成浩
（コード番号：３０９０）
問合せ先　取締役　髙橋　要
電話番号　06-6910-0031(代表)
ＵＲＬ　http://minerva-hd.com/

ミネルヴァグループのセキュリティ対策に関するご報告

この度は、弊社子会社であります、ナチュラム・イーコマース株式会社における不正アクセスの件につきましては、お客様ならびに株主の皆様方に多大なご迷惑とご心配をおかけいたしましたこと、改めてお詫び申し上げます。

平成 20 年８月 6 日のプレスリリース発表から今日まで、大勢のお客様や株主の皆様方から、本件に係わる様々なお問い合わせを頂き対応に奔走してまいりましたが、一方では温かい激励のお言葉や応援メッセージを頂くなど、お客様ならびに株主の皆様方に深く感謝いたしております。今後につきましても、お客様に安心してご利用いただけるよう、継続的なセキュリティの強化と改善を行い、信頼の回復に努めてまいる所存でございます。

つきましては、セキュリティ対策と今後の計画を下記の通りご報告させていただきます。

記

1. 情報セキュリティポリシーの策定

今回の不正アクセスの事件は、当社の情報セキュリティに対する考え方、及び取組みにつきまして、新たに見直すきっかけとなりました。

特に、Eコマースを事業の柱として個人情報を取り扱う当社においては、これまで以上にその安全性及び信頼性を確保することは不可欠であると認識しております。

そのための体制の構築、個々の対策を行う上で、明文化された情報セキュリティポリシーが必要と考え、後述の情報セキュリティ委員会にて策定を行いました。

情報セキュリティポリシーについては、以下をご覧下さい。

http://www.minerva-hd.com/security/

また、当社グループは情報セキュリティポリシーを遵守し、高度なセキュリティ管理体制を構築・維持するために、独自のデータセキュリティ基準を設け運用してまいります。

このデータセキュリティ基準は単に当社グループでの運用を目的とするのではなく、Eコマース事業者様や業界の規範となる志を持って策定を行います。

2. 情報セキュリティ委員会の設置

情報セキュリティポリシーの策定に当たり、責任の所在の明確化と今後管理運用し安全対策を推進していくために、専門の組織として、情報セキュリティ委員会を設置いたしました。

情報セキュリティ委員会の具体的な役割は、以下の通りです。

- 情報セキュリティポリシーの策定と維持。
- 当社グループの役員、一般社員への情報セキュリティポリシーの普及と教育。
- 情報セキュリティ監査実施計画の策定。
- 情報セキュリティ監査に基づく情報セキュリティ管理の見直しと改善。
- 当グループでのコンピュータセキュリティインシデント発生時において終息までの全活動の指揮監督。
- 当社グループ独自のデータセキュリティ基準の策定と維持、運用。
- その他、情報セキュリティポリシーを鑑みて必要と思われる事項

情報セキュリティ委員会メンバー

委員長：ミネルヴァ・ＨＤ　代表取締役会長兼社長　中島成浩
情報セキュリティ統括責任者(CISO)：ミネルヴァ・ＨＤ　システム部長　森本武司
委員：ミネルヴァ・ＨＤ　経営戦略室長　山内智和
委員：ジェネシス・ＥＣ　システム開発部長　藤原秀樹
委員：ミネルヴァ・ＨＤ　取締役　譚玉峰（インタセクトコミュニケーションズ株式会社代表取締役社長）

※情報セキュリティ委員会のメンバーについては、ミネルヴァグループの組織編成に応じて変更となる可能性があります。

3.情報セキュリティシステムの計画

(1) 不正アクセス発生の原因と当時のセキュリティ体制

今回の不正アクセスは、SQLインジェクション(※)による攻撃によってメンテナンス用のFTPサーバを悪用され、悪性プログラムを設置されたことが原因であります。昨今のSQLインジェクションによる被害もあって当社でも対策は行われており、セキュリティ専門会社から見ても標準以上のレベルであったと明言をいただいておりました。また当初、セキュリティ専門会社の調査では、SQLインジェクションにエラーを応答しているアクセスログはあっても成功した痕跡は発見されず、詳細な原因は長らく不明なままでした。

調査を積み重ねた結果、最終的にはSQLインジェクション攻撃に対して、当社のシステムがエラーを応答してもなおSQLインジェクションの実行結果を表示する、というセキュリティ専門会社でも初めてみる特殊なSQL文を使われていたとの報告を受けております。

※SQLインジェクション：データベースシステムを不正に操作する攻撃方法の一つ。近年SQLインジェクションによる被害が頻発している。

(2) 情報セキュリティシステム計画

■第一プロセス（不正アクセス発生以降～現在）

・顧客マスター（※）内のクレジットカード番号の暗号化、パスワードの暗号化
・出荷、注文などの個人情報に関わるデータを一定期間で自動的に削除
・SQLインジェクション等、WEBアプリケーションの脆弱性の確認修正
・社内におけるパスワードの一新
・ネットワーク管理専門会社とのアドバイザリー契約
・IPS(不正侵入防止システム)における24時間監視体制の実施等々

※顧客マスター：お客様の個人情報を保管しており、今回不正アクセスがあった場所。

以上につきましては、全て完了しております。実施されました各種対応によって、セキュリティ専門会社より安全性が確認されておりますが、策定した情報セキュリティポリシーに従って今後の高度な情報セキュリティ管理体制の構築のため、以下のプロセスに従って実施いたします。

■第二プロセス（現在実施中、9月末までに完了予定。）

・クレジットカード情報の非保持方式への変更

現在のデータベース内にクレジットカード情報を暗号化して保持する方法から、クレジットカード情報そのものを保持しない方式に変更いたします。
NTTデータが提供する「CAFIS BlueGate」サービスの新商品であるワンクリックダイレクトオプションを導入し実現いたします。これにより、当社からカード情報が漏洩することはあり得なくなります。

現在はNTTデータと開発を進めており9月末に本稼動させる予定でございます。

「CAFIS BlueGate」は、情報セキュリティマネジメントの国際基準規格である「ISMS」の認定、またVISA、JCBが共同で推進するデータセキュリティ保護プログラム「AIS」に準拠しております。

また「CAFIS BlueGate」はPCIDSSへの準拠を予定しており、当社としましてはPCIDSSに準拠したセキュリティレベルで運用できる点を重視し、導入することを決定いたしました。

「CAFIS BlueGate」の詳細はこちらをご覧下さい。

http://solution.cafis.jp/BlueGate/

※PCIDSS（Payment Card Industry Data Security Standard）とは、加盟店様・決済代行事業者様が取り扱うカード会員様のクレジットカード情報・お取り引き情報を安全に守るために、VISA・JCB・MasterCard・American Express・Discoverの国際ペイメントブランド5社が共同で策定した、クレジット業界におけるグローバルセキュリティ基準です。

・オンライントラストマークTradeSafeの導入

ナチュラム・イーコマース㈱が運営する各ショッピングサイトで、安全かつ安心してお買い物ができるショップであることをお客様にご理解いただくために、株式会社TradeSafeが提供しておりますトラストマークサービス、及びADRサービス(ショッピングトラブル解決サポート)の導入を進めております。

現在、TradeSafeの審査を受けております。

TradeSafeが持つADRサービス付きの信頼マークは日本で初めてのサービスとなり、またADRでも解決できないような事態となった場合にはお客様に10万円までのお見舞金が支払われる補償が用意されております。

現在9月中の認証を目指し、準備を進めております。

TradeSafeの詳細はこちらをご覧下さい

http://www.tradesafe.co.jp

■第三プロセス(10月末までに完了予定)

・ネットワークの再構成

第二プロセスに引き続き、高度な情報セキュリティ管理体制を構築するため、セキュリティ専門会社他、外部のアドバイスを取り入れネットワークの再構成を行います。

現在のネットワーク構成のさらなる分離や隔離(DMZ)等の見直しを行うことで、各ネットワークセグメントへのきめ細かいアクセス制御が可能となり、不正アクセス攻撃に対して物理的および論理的なセキュリティレベルの飛躍的向上を図ります。

・Webアプリケーション・ファイアウォールの実装

Webアプリケーション・ファイアウォール(以降、WAF。)は、通常のファイヤーウォールでは防ぐことが難しいアプリケーション層への不正アクセス攻撃に対してブロックを行います。

これまでアプリケーション層への攻撃については24時間有人監視で対応しておりましたが、WAFを導入することで攻撃に対して効率的にブロックすることが可能となります。

またWAFの導入はPCIDSSにも定められた要件項目であります。

■第四プロセス (11月末までに完了予定)

・独自のデータセキュリティ基準の策定

前述しましたCAFIS Bluegateのワンクリックダイレクトオプションの導入により、クレジットカード情報の取り扱いにおいてPCIDSSを準拠した運用が見込めるようになりますが、当社グループが事業を継続し、お客様の個人情報をお預かりするには、Eコマース事業に即した独自のデータセキュリティ基準が不可欠となります。

今回策定しました情報セキュリティポリシーの遵守と高度なセキュリティ管理体制の構築と維持のため、また不正アクセスの一件で得た教訓とノウハウをもって、他のEコマース事業者様や業界の規範となるべく、独自のデータセキュリティ基準(Minerva Data Security Standardと呼称。)を11月末をめどに策定、順次運用を行ってまいります。

以　上