

## 不正アクセスによる情報漏洩のお詫びとご報告

2012年1月20日

株式会社ヴァーナル  
代表取締役 千堂 純子

この度、弊社が運営するウェブサイト「ヴァーナル オンライン (<http://www.vernal.co.jp>)」(以下「本サイト」と申します。)のウェブサーバーに外部からの不正アクセスがあり、第三者機関による調査を行いましたところ、お客様の個人情報(クレジットカード情報)の一部が外部に漏洩したことが確認されました。

お客様をはじめ関係者の皆様に多大なるご迷惑とご心配をおかけいたしましたこと、深くお詫び申し上げます。

調査の結果、判明しました不正アクセスの内容、漏洩した情報等につきましては、以下の通りご報告申し上げます。

弊社では、今回の事態を厳粛に受け止め、二度とこのようなことを起こさぬよう、再発の防止に取り組み、信頼の回復に社員一同、全力で取り組む所存です。

現在、不正アクセスの対策として、本サイトシステムの全面的な変更が終了しておりますので、安心してご利用いただける環境となっております。また、クレジットカード決済につきましても、自社内にクレジットカード情報を持たないシステムで運用しておりますので、弊社からクレジットカード情報が漏洩することは有り得ませんので、ご安心くださいませ。

今後とも「ヴァーナル オンライン」をよろしく願いたします。

※お電話でのご注文におきまして、JCBカード、アメリカンエクスプレス、ダイナースクラブカード、ヴァーナルビューティカード、ヴァーナルカード以外のクレジットカードが今現在ご利用いただけない状況になっております。ご迷惑をおかけいたしました、誠に申し訳なく、深くお詫び申し上げます。今後、クレジットカード決済システムを、よりセキュリティ効果の高いシステムに全面変更し、一日も早いご利用再開を目指す所存ですので、何卒、ご理解いただけますようお願い申し上げます。

本件に関するお問い合わせ先

フリーダイヤル 0120-08-2400（携帯電話からもご利用いただけます）

メール card-info@vernal.co.jp

受付時間 朝9：30～夕方6：00（日・祝日をのぞく）

## 調査結果ご報告

### ■不正アクセスによる情報漏洩の内容

第三者機関による詳細な調査の結果、不正アクセスにより漏洩したと思われる情報は、弊社ウェブサーバー内にありました、オンラインショップの受注データに含まれるクレジットカード情報であることが判明いたしました。

情報項目・件数について

クレジットカード情報（会員名、会員番号、有効期限、商品送付先住所）

1,493件

不正アクセスの日時・攻撃手法

日時：2011年10月14日21：19～11月10日14：26にかけて断続的に

攻撃元：海外（ベトナムとアメリカ合衆国）と日本国内

攻撃手法：弊社のウェブサーバーに対する「SQLインジェクション」（アプリケーションが想定しないSQL文を実行させることにより、データベースシステムを不正に操作する攻撃方法のこと）

### ■お客様への対応について

情報漏洩により、ご迷惑をおかけしたお客様へは、今後、個別にご連絡を差し上げます。また、クレジットカード会社各社へ不審な利用の監視を続け、不正利用を未然に防ぐ体制を依頼しております。

クレジットカードの再発行を希望されるお客様には、再発行に伴う手数料のご負担がないように対応させていただきます。

お客様におかれましては、クレジットカードのご利用明細にお心当たりのない請求が含まれていないか、いま一度ご注意くださいようお願い申し上げます。お心当たりのない請求がございましたら、ご加入のクレジットカード会社までご連絡くださいますよう、併せてお願い申し上げます。

■情報セキュリティ対策について

弊社では、情報漏洩の可能性が指摘されて直ちに、以下の対策を行いました。

2011年11月10日までに行った主な対策

- データベースからクレジットカード情報を削除。
- ウェブサイト上のカード決済システムの一部停止。

2011年11月15日までに行った主な対策

- SQLインジェクション対策、ウェブアプリケーションの脆弱性の修正。

2011年12月20日

- ウェブサイト上のクレジットカード決済システムを、カード情報非保持方式に変更し、全種類のクレジットカード使用を再開。

## 本件の経緯

2011年11月9日 クレジットカード会社より「不正に利用された懸念のあるクレジットカードがある」と連絡を受け、ウェブサイト上での一部のカード決済を「メンテナンス中」として停止。直ちに、弊社システム担当による調査を開始。

2011年11月10日 ウェブサイトのデータベースからクレジットカード情報を削除。

2011年11月11日 SQLインジェクション対策実施。セキュリティ・パッチを適応した新規OSに環境を移設。

2011年11月14日 非対面取引での一部クレジットカードの取り扱いを停止。

2011年11月15日 SQLインジェクションの追加対策実施。

2011年12月2日 クレジットカード会社指定の第三者機関による調査が開始。

2011年12月12日 第三者機関による第一調査報告で、ウェブサイトが不正アクセスによる攻撃を受け、クレジットカード情報が漏洩した可能性があることを確認。

2011年12月20日 ウェブサイト上のクレジットカード決済システムを、カード情報の非保持方式に変更し、クレジットカード全種類の使用再開。

2011年12月24日 第三者機関による第二調査報告で、不正アクセスの内容、漏洩したクレジットカード情報の範囲が判明。漏洩したクレジットカード情報とお客様の特定作業を開始。

2012年1月6日 不正アクセスにより漏洩したクレジットカード情報とその件数、お客様を特定。警察に調査結果を持参し、被害を報告。

2012年1月16日 経済産業省へ「個人情報漏えい等に関する報告」を提出。

## よくいただくご質問と回答

### ■ クレジットカード情報の漏洩について

Q. 流出した情報とは、具体的にどのようなものか

A. ご心配をおかけしております。第三者機関による詳細な調査の結果、クレジットカード会員名、会員番号、有効期限、商品送付先住所が漏洩した可能性があります。

### ■ クレジットカードについて

Q. 自分のクレジットカード情報は大丈夫なのか

A. クレジットカード情報漏洩の可能性のあるお客様については、1月20日にメールにてご連絡させていただいております。お客様が該当されるかどうか、弊社にてお調べすることもできますので、専用お問い合わせ窓口（フリーダイヤル 0120-08-2400 受付時間 朝 9:30~夕方 6:00 日・祝日をのぞく）までご連絡くださいますよう、お願い申し上げます。

Q. クレジットカードが不正利用されていないかを確認したい

A. クレジットカードのご利用状況などに関するお問い合わせにつきましては、個人情報取り扱い上の制限があるため、恐れ入りますが、お客様ご自身からクレジットカード会社にお問い合わせいただきますようお願い申し上げます。

Q. クレジットカード番号を変えてほしい

A. 大変お手数でございますが、発行元のクレジットカード会社にご連絡の上、カード番号変更の旨をお伝えいただければ幸いです。

### ■ クレジットカードの不正利用について

Q. クレジットカードが不正利用された場合どうすればいいのか

A. お客様の不正利用へのご不安を取り除くため、クレジットカード会社のご協力により不審な利用の監視をしていただいております。お客様におかれましては、クレジットカードのご利用明細にお心当たりのない請求が含まれていないか、今一度ご注意をいただきますようお願い申し上げます。もし、お心当たりのない請求がございましたら発行元のクレジットカード会社までご連絡くださいますよう、あわせてお願い申し上げます。

以上