株式会社イプサ公式オンラインショップへの
不正アクセスに関する調査報告書

2017 年 1 月 31 日

株式会社資生堂

株式会社イプサ

株式会社資生堂(以下、資生堂)の子会社で、化粧品販売を手掛ける株式会社イプサ(以下、イプサ)の公式オンラインショップ（EC サイト[1]）が外部から不正アクセスを受け、決済いただいたお客さまのクレジットカード情報、ならびに登録いただいた方の個人情報流出の可能性があることが判明しました。

大切な個人情報をお預かりしていたにもかかわらず、このような事態に至り、お客さま及び関係者の皆さまに多大なるご迷惑とご心配をおかけしていることを心よりお詫び申し上げます。

本報告書は、本件の事実関係に関する調査及び再発防止策についてお客さまおよび関係者の皆さまに報告することを目的として作成しました。

概要

2016 年 11 月 4 日、イプサは、インターネット販売を行っているイプサ公式サイトに対して外部から不正アクセスが行われている可能性があることを、クレジットカード決済代行会社からの連絡により認識しました。直ちにインターネット販売機能を停止し、対象となるシステムに関して、社外の専門調査機関による調査（フォレンジック調査[2]）を依頼しました。

11 月 25 日受領したフォレンジック調査の報告書から、下記のことが判明しました。

- イプサ公式サイトの EC サイトにおけるウェブサーバ[3]において、SSI[4]の脆弱性を突かれ、外部から不正アクセスを受けた結果、外部からのコンピューター操作を可能にする「バックドアプログラム[5]」を仕掛けられたこと。
- その結果、EC サイトに登録されていたクレジットカード情報 56,121 件を含むお客さま情報 421,313 件分の個人情報が外部に流出した可能性があること。

上記報告受領の後、直ちに、決済代行会社・クレジットカード会社と公表に向けた準備を進めました。お客さまのお問い合わせに対応する体制を整えた後、12 月 2 日、個人情報流出の可能性があるお客さまにeメールで個別にご連絡するとともに、ホームページや記者会見などで本件を公表いたしました。

---

1 Electronic Commerce（電子商取引）の略で、通信販売機能を有するインターネットウェブページ
2 犯罪の証拠となるファイルの特定、サーバのログから不正アクセスを発見し事象の全貌を調査する活動
3 インターネットウェブページの表示を提供するためのコンピューター機器
4 SSI（Server Side Includes）はウェブサーバの操作を正規に行うためのプログラム技術
5 ユーザーログインなどの正規な手続きを踏まずにサーバ内部に侵入し、不正に遠隔操作を行うためのプログラム

その後、さらに決済代行会社と連携しながら詳細な調査を進めた結果、クレジットカード情報流出の可能性がないとは断定できない 9,699 名に加え、個人情報流出の疑いがある 150 名の存在が判明し、それぞれ個別にご連絡いたしました。

以上のような状況のもと、社外の有識者を交えて原因の解明を行った結果、イプサの EC サイトにいくつかの技術的問題があったこと、ならびにイプサと資生堂グループそれぞれに管理体制を強化する必要があることが明らかとなりました。この事態を真摯に受け止め、今後の再発防止に向けて、イプサにおいては公式サイトの改善と体制強化を、資生堂では国内外のグループサイトの安全性の確認に加え、資生堂情報管理部門主導によるグループ全体で統一した情報セキュリティ維持体制の構築を開始しました。

なお、イプサの EC サイトは現在も閉鎖しておりますが、本年 6 月を目途に、セキュリティ対策を抜本的に強化した全く新しいサイトとして生まれ変わらせるよう準備を進めております。また、イプサ以外の資生堂グループの EC サイトにつきましては、まったく独立した別のシステムで稼働しており、既に 11 月末時点で、外部からの不正アクセス形跡の有無と防止策運用についての緊急調査を行った結果、問題がないことを確認しております。今後も引き続き資生堂グループの EC サイトの安全性向上に努めてまいります。

上記概要につきましての詳細を以下にご報告いたします。

1. 事実関係の整理

(1)経緯

日付	内容
2016 年 11/4(金)	18 時頃: 決済代行会社からイプサ公式サイトへの不正アクセスの可能性について連絡を受領
	18 時半頃: イプサ公式サイトの EC 機能を停止
	19 時頃: イプサに対策本部を設置し、決済代行会社に紹介された社外専門調査機関にフォレンジック調査を依頼
	24 時頃: イプサ公式サイトに一部機能停止のお知らせを掲載
11/7(月)	捜査機関に報告
11/8(火)	監督官庁である経済産業省に第一報を報告
11/9(水)	社外の専門調査機関から第一報を受領、EC サイト内にバックドアプログラムが設置された形跡を確認
	イプサ公式サイトを全面停止
11/10(木)	経済産業省に書面報告
11/18(金)	セキュリティレベルの高い環境に新しいサーバを設置し、商品情報や店舗情報など EC サイトに関連しないイプサ公式サイトを一部復旧
11/25(金)	社外の専門調査機関からフォレンジック調査の最終報告を受領、クレジットカード情報 56,121 件を含む個人情報 421,313 件分が流出した可能性を確認
	決済代行会社・クレジットカード会社と公表に向けた準備を開始
	外部の情報セキュリティ専門企業に対策本部への参画を要請し、本件における詳細調査を継続
12/1(木)	経済産業省に経過報告
	捜査機関に社外の専門調査機関の最終報告を提出
12/2(金)	対象のお客さまに個人情報流出の可能性に関するお知らせ・お詫びのeメールを送信。併せてクレジットカード情報流出可能性のお客さまには郵便でも同様の内容を連絡(～12/13)
	イプサ公式サイトに個人情報流出に関するお知らせ・お詫びを掲載
	専用相談窓口を設置
	記者会見を実施
12/13(火)	詳細調査において認識した、クレジットカード情報流出の可能性がないと断定できないお客さま 9,699 名へ追加でeメールを送信し、郵便でも同様の内容を連絡(詳細後述)
	上記を経済産業省へ報告
12/16(金)	経済産業省へ詳細調査の経過を踏まえた報告書を提出
12/19(月)	対象となった全てのお客さまへお詫び状とお詫びの品(クオカード)を出状
2017 年 1/20(金)	詳細調査の結果、新たに判明した個人情報流出の可能性があるお客さま 150 名にお詫び状・お詫びの品を追加で出状(詳細後述)
1/31(火)	上記について、経済産業省へ追加報告書を提出
	調査報告書をホームページで公開。対象のお客さまに調査報告書に関するお知らせをeメールにて送信

（2）対応

①対象となったお客さまへの対応

12 月 2 日、フォレンジック調査で個人情報流出の可能性が確認された全てのお客さまに対し、eメールで個人情報漏出の可能性があることをご連絡しました。併せて、クレジットカード情報流出の可能性があるお客さまに対しては、郵便で同様の内容をご連絡いたしました。

また、フォレンジック調査の後、追加で行った詳細調査の結果、個人情報およびクレジットカード情報の流出可能性が判明した方には、判明後、直ちにeメールおよび郵便でご連絡いたしました。

12 月 19 日には、その時点で判明していた全てのお客さまに対して、ご迷惑をおかけしたお詫びとして、封書にて、お詫び、経緯、クレジットカード使用停止・切り替え含むお客さま対応方法を記載したお詫び状と、お詫びの品を郵送しました。

なお、クレジットカード情報流出の可能性があるお客さまについては、クレジットカードの交換・再発行費用をイプサが負担するとともに、本事案に起因する不正利用が発覚した際にも、イプサが被害額を負担することとしました。

②イプサ公式サイトの対応

11 月 4 日に決済代行会社から不正アクセスの可能性を指摘され、ただちにイプサ公式サイトを停止し、その旨のお知らせを掲示しました。ただし、11 月 18 日には、イプサ公式サイトで商品情報や店舗情報をご覧いただけない不便を解消するため、セキュリティレベルの高い環境に、全く新たなサーバを設置することで商品情報や店舗情報など一部内容を復旧させました。また、12 月 2 日から、お詫び・経緯・対象・お客さま対応方法の詳細を掲載しました。

なお、1 月末現在、EC サイトは停止しております。

③資生堂グループサイトの安全性確認と対応

2016 年 11 月 4 日、イプサから公式サイトへの不正アクセスの可能性について連絡を受け、直ちに、資生堂グループ全体の ICT（Information and Communication Technology：情報通信技術）統括機能を有する資生堂グローバル ICT 部がグループ各社の EC サイトについて、類似の不正アクセス形跡の有無、及び外部からの不正アクセス検知などの防止策の運用について調査を開始しました。11 月末時点で調査結果をまとめ、イプサ以外に同様の不正アクセスは発生していないことを確認しました。

（3）調査内容と結果

①社外の専門調査機関によるフォレンジック調査の結果

イプサの EC サイトは 2 台のウェブサーバと 1 台のデータベースサーバ[6]によって運営されていました。その全てのサーバでフォレンジック調査を行った結果、以下のことが判明しました。

- 特定の IP アドレス[7]からの不正アクセスが、2015 年 12 月 1 日以降発生していたことを確認しました。
- 2016 年 8 月 27 日と 10 月 31 日、2 台のウェブサーバそれぞれに同じ IP アドレスからの不正アクセスが複数回あり、SSI の脆弱性を利用され、バックドアプログラムが仕掛けられた形跡が確認されました。
- ウェブサーバには 56,121 件のクレジットカード会員データ、データベースサーバには 421,313 件分の個人情報が存在していたため、これらが不正に取得された可能性があることを確認しました。
- EC サイトでお客さまにお買い上げいただいた際の決済処理が行われた旨の記録（ログ[8]）が保存されていた期間は 2011 年 12 月 14 日～2016 年 11 月 4 日であることから、対象となるクレジットカードの利用期間については、最大で同期間と捉えました。

上記の調査の結果から、流出した可能性のある個人情報は以下のとおりです。

（ⅰ）クレジットカード情報

対　象：以下の期間にイプサ公式 EC サイトにおいてクレジットカード決済をされた方
　　2011 年 12 月 14 日～2016 年 11 月 4 日（調査に基づく最大期間）

項　目：カード会員名、カード番号、住所、カード有効期限
　　※パスワード、セキュリティコードは流出しておりません

件　数：最大 56,121 件

（ⅱ）クレジットカード情報以外の個人情報

対　象：2016 年 11 月 4 日時点でイプサ公式 EC サイトにご登録の全てのお客さま

項　目：氏名、性別、生年月日、年齢、職業、電話番号、メールアドレス、住所、購入履歴、ログインパスワード

件　数：421,313 件(上記(i)のお客さまを含む)

---

6 ウェブサーバからの操作要求により商品情報を送信したり、購買情報を保存するためのコンピューター機器

7 インターネットなどに接続されたコンピューターや通信機器に割り当てられた、個別の識別番号

8 コンピューター機器が自動的に活動履歴(利用履歴・実行履歴・データの授受の履歴など)を記録するファイル

②フォレンジック調査後に追加で対策本部が行った詳細調査の結果

社外の専門調査機関によるフォレンジック調査の結果を確認した後、決済代行会社と連携し、外部の情報セキュリティ専門企業の参画のもと、対策本部にてさらに詳細な調査を継続したところ、新たに以下のことが判明しました。

（ｉ）クレジットカード情報

・ 決済代行会社から情報提供を受け、イプサの保有する注文履歴と照合したところ、フォレンジック調査でクレジットカード情報流出の可能性を指摘された方以外に 9,699 名が EC サイトで商品を購入していたことが判明しました。
・ この方々は、イプサの EC サイトにクレジットカード決済のログは残っていないものの、クレジットカード情報流出の可能性がないとは断定できないため、12 月 13 日に対象のお客さまにクレジットカード情報流出懸念をお知らせしました。

（ⅱ）クレジットカード情報以外の個人情報

・ EC サイト未登録で、イプサ商品を店舗にてお買い上げされたお客さまが、ご自身の購入履歴やポイントを参照するために必要な利用登録画面にログインしたまま、本来、実施の必要がない利用登録画面を再度表示させた場合に、個人情報がウェブサーバ内のログに残ることがわかりました。その対象者は 150 名と判明しました。
・ 1 月 20 日に対象のお客さまに個人情報流出の可能性をお知らせいたしました。

2. 原因の分析と今後の対応

（1）原因の分析

外部の情報セキュリティ専門企業の参画のもと行った詳細調査の結果、当事案が発生した直接的な原因として、3 点の技術的な問題があることが判明しました。これらの技術的な問題が発生した要因としては 2 点の管理体制の問題があったと捉えています。

①技術的な問題

（ｉ）SSI に起因する脆弱性に対する認識不足

イプサ公式サイトの開発・運用体制において、SSI 技術の利用に関する脆弱性の認識が甘く、当該技術の利用箇所を限りなく少なくするなどの対策が取られていませんでした。またグローバル ICT 部による定期的なウェブ脆弱性診断で発見された脆弱性のある箇所は改修しましたが、システム全体の総点検をするなどの徹底した対応が取れていませんでした。

（ⅱ）セキュリティ対策不足

対象となる EC サイトにおけるセキュリティ対策がファイアウォール[9]のみという不十分な状態であったものの、他のセキュリティ対策も導入済みであるとイプサが誤認していました。

（ⅲ）クレジットカード情報保持に対する誤認

本来サイト内にクレジットカード情報は保持しない設計であったにもかかわらず、サーバ内に情報が残されていたことが詳細な調査により判明しました。これは、EC サイト立ち上げ準備のために使用していたデバックモード（プログラム上の問題点を見つけるためのテスト仕様のため、クレジットカード情報などの履歴が残る設定）の状態のままで運用状態に入っており、決済処理のログが残る状態となっていたためでした。EC サイト立ち上げを担当したソフトウェア開発会社とは既に取引はなく、その後、保守運用を委託した会社も情報が引き継がれていなかったため、デバックモードのまま運用されていた理由は確認できませんでした。

②管理体制の問題

（ｉ）イプサの管理体制不備

イプサ社内のサイト管理に関する責任部門が不明確であり、また、委託先であるソフトウェア開発会社に対する管理監督や意思疎通が十分ではありませんでした。そのため、技術情報の継承や、正しい状況把握ができていませんでした。

9 インターネットから必要最低限の機器（この場合ウェブサーバ）に接続制限するネットワーク機器

（ⅱ）資生堂の、イプサに対する管理体制・開発における関与不足

イプサ公式サイトの構築時は、開発計画（スケジュール、開発規模など）のみ共有しており、システムの詳細についての確認が行われていませんでした。またシステム稼働後に監査を毎年実施していましたが、口頭・紙面による報告ベースで、詳細な内容確認はできていませんでした。また、グループ各社がECサイトを構築する時に遵守すべきガイドラインや、資生堂グループ全体を通したシステム基準、それぞれのサイトにおける実態を監査する体制が十分ではありませんでした。

（2）イプサの再発防止策

①技術的な対策

EC サイトを含むイプサ公式サイトは、セキュリティレベルの高い新たな環境において全て再構築します。その際には、開発・構築・運用におけるセキュリティ要件を明確にするとともに、EC サイト内ではクレジットカード情報を一切入力せず、決済代行会社のサイトにてクレジットカード情報を入力する決済システム（遷移型決済システム）を採用します。

資生堂グローバルICT部がサポートを行い、不正アクセス監視等の対策を導入する他、セキュリティ要件については、アプリケーションの安全な仕様と、EC サイトの運用基準も含めて包括的に定義し、確実に運用されているかどうかを定期的にチェックしていきます。

②管理体制の見直し

EC サイトを含め、イプサ内のすべてのシステムを一つの部門で一元管理します。また、個人情報等の重要情報を保持しているシステムの安全な管理を推進します。

委託先の管理を強化し、個人情報保護に関する体制や規定などの整備と運用状況の確認、契約書への内容記載の徹底を行うとともに、内部監査の実施状況をはじめとする安全管理状況を把握し、問題が発生すれば速やかに対応できる体制にします。

（3）資生堂グループの再発防止策

①グループ子会社のICT体制強化

グループ子会社のシステムの開発・運用については、これまでは、各社の責任で実施しており、資生堂のグローバルICT部は、大規模開発の場合の開発計画の確認、ウェブサイトの脆弱性診断(毎年実施)、システム監査(毎年実施)に基づき統括していました。

しかしながら、今回抜本的な再発防止策を検討するため、各社のICT体制、管理体制を再点検した結果、子会社によっては、システム専門性が高い人材を必ずしも配置できておらず、

システム開発・運用の品質管理、外部パートナーの管理にも差があることがわかりました。

この状況を受け、17 年 1 月より、国内関係子会社のシステム開発時のグローバル ICT 部の関与度を高め、特に情報システムのセキュリティ対策については、グローバル ICT 部主導で企画推進する体制に変更しました。

②資生堂グループ全体の情報セキュリティ体制強化

グループ全体の情報セキュリティ維持体制を継続的に強化すべく情報セキュリティマネジメントシステム（ISMS）等の外部標準をベースとしたグループ全体の情報セキュリティに関するフレームワークを新たに策定し、この標準に基づき、システムだけでなく文書管理や社内管理プロセス整備等マネジメント面についても強化します。

海外のグループ会社のサイトについても引き続き調査を進め、日々厳しくなる情報セキュリティリスクに対応した一層の強化策を継続的に推進していきます。

（以下余白）

3. 本事案に関する有識者による検証

本事案は、株式会社ラック（本社：東京都千代田区、代表取締役社長：髙梨輝彦）の協力を得て、調査を進めてまいりました。本事案に関する当社対応等についての株式会社ラックによる検証コメントは以下の通りです。

（1）総論

セキュリティ事故として認識された後の対応全般を通じ、対応そのものに問題はなかったと捉えています。ただし、システム面における課題は大きかったと判断しています。

（2）初動対応

外部からの指摘をきっかけに、システムを即日停止し、対策本部の設置、外部への調査依頼、捜査機関への相談・報告を実施した判断には早さがあり、問題はありませんでした。

（3）被害拡大・二次被害防止

システム停止の判断、フォレンジック調査結果からの詳細調査を継続した点、クレジットカード会社との情報連携により、影響を受けた可能性のある個人のお客さまの最大数の割り出し作業を通じ、被害拡大・二次被害防止の観点において、実施可能な事項は網羅されていたと捉えています。

（4）報告

監督官庁・捜査機関との情報連携が継続して実施され、また、記者会見を含め、対外発表においては、二次被害の防止を考慮しながら、資生堂・イプサの関連各部署が連携して対応されており、個人消費者の観点での懸念は拭い切れなかったものの、報告の対応として不備な点はありませんでした。

（5）調査

システム・セキュリティに関する有識者の体制が不足していた点は否めず、「資生堂」「イプサ」というブランドイメージに対して、実際のシステムのセキュリティレベルの低さは大きな課題であったと捉えています。ただし、関係各所において、原因の特定作業の他、影響のあったお客さまの割り出し調査を連日実施されていた経過について、問題は見受けられませんでした。

（6）再発防止

本報告書時点では、再発防止策の詳細は準備段階（システムの新規再構築・体制の再構築）と捉えており、対応方針として問題はなく、今後の経過観察が必要と捉えています。

以上