ECサイトのセキュリティ

株式会社セキュアサイクル
代表取締役　服部祐一

プロフィール

名前

服部 祐一

株式会社 セキュアサイクル
代表取締役

所属・役職

- OWASP Fukuoka チャプターリーダー
- SecHack365 研究駆動コーストレーナー
- 北九州情報セキュリティ勉強会「セキュ鉄」代表 等

経歴

九州工業大学卒。在学時はスマートフォンを使った行動認識の研究に携わり、
Microsoft Research AsiaにてResearch Internshipとして行動認識の研究に従事。
その後、ベンチャー企業でチーフエンジニアとして新規Webサービスの開発や脆弱性診断の経験後、
情報セキュリティ専門会社のCTOを経て現在に至る。
各地のセキュリティ関連イベントや、企業、大学等での講演・トレーニング多数。
現在も脆弱新診断や開発時のセキュリティ対策のコンサルなどの実務にも携わる。

会社概要

会社名	株式会社セキュアサイクル (Secure Cycle Inc.)
代表	服部 祐一
従業員	26名（役員・アルバイト含む）
所在地	**本社** 〒808-0138 福岡県北九州市若松区ひびきの北8-1 技術開発交流センター **仙台支社** 〒980-0803 宮城県仙台市青葉区国分町1-4-9 enspace内

設立	2017年06月19日
資本金	1000万円
事業内容	情報セキュリティの各種診断・対応 情報セキュリティのセミナー、コンサルティング 情報システムの設計・開発・研究・運営 システム開発のセミナー、コンサルティング
顧問弁護士	光雲法律事務所　吉井 和明
加盟団体	一般社団法人九州経済連合会 特定非営利活動法人日本ネットワークセキュリティ協会 IOT INNOVATION Base 公益社団法人 福岡貿易会

システム開発におけるセキュリティ対策を当たり前のものに

「システム開発におけるセキュリティ対策を当たり前のもの に」という理念のもとに、自社でのシステム開発、研究開発に おける製品に情報セキュリティ対策を行い安心安全な製品を提 供。情報セキュリティ部門においても開発を経験したエンジニ アが脆弱性診断等に従事しており、

開発者目線での助言などを行っています。また、契約内容に よってはコードレビューや新規機能作成時のセキュリティ面か らの助言といった開発段階での参画も可能です。

セキュリティサービス一覧

名称	概要
Webアプリケーション脆弱性診断	ECサイトや社内システム、コーポレートサイトなどの脆弱性診断
API脆弱性診断	シングルページアプリケーションやスマホアプリで用いるAPIなどの脆弱性診断
プラットフォーム診断	アプリケーションを設置するサーバや社内に設置してある ネットワーク機器などの脆弱性診断
スマホアプリ脆弱性診断	個人情報を取り扱うアプリやクーポン機能などの 悪用されると被害が発生する可能性があるアプリなどの脆弱性診断
セキュリティコンサルティング	ウイルス対策ソフトの選定や企業規模に応じた適切なセキュリティ対策のご提案や、自社開発のアプリケーションの扱うデータの内容等に応じたセキュリティ対策に対するご提案など
研修・講演	脆弱性診断に関する研修や各種セキュリティに関する講演、 情報セキュリティ競技の運営など

システム開発・研究開発

名称	概要
システム開発	工場向け在庫管理システムや営業所向け顧客管理システム、生産管理システム、ベンチャー企業様の独自サービスなどのシステム開発
研究開発	国の研究機関や大学などから委託を受けて行う調査や 研究用途のシステム開発、新規事業の検証用のシステム開発など

ECサイトの
セキュリティ事例

ECサイトのセキュリティ事例

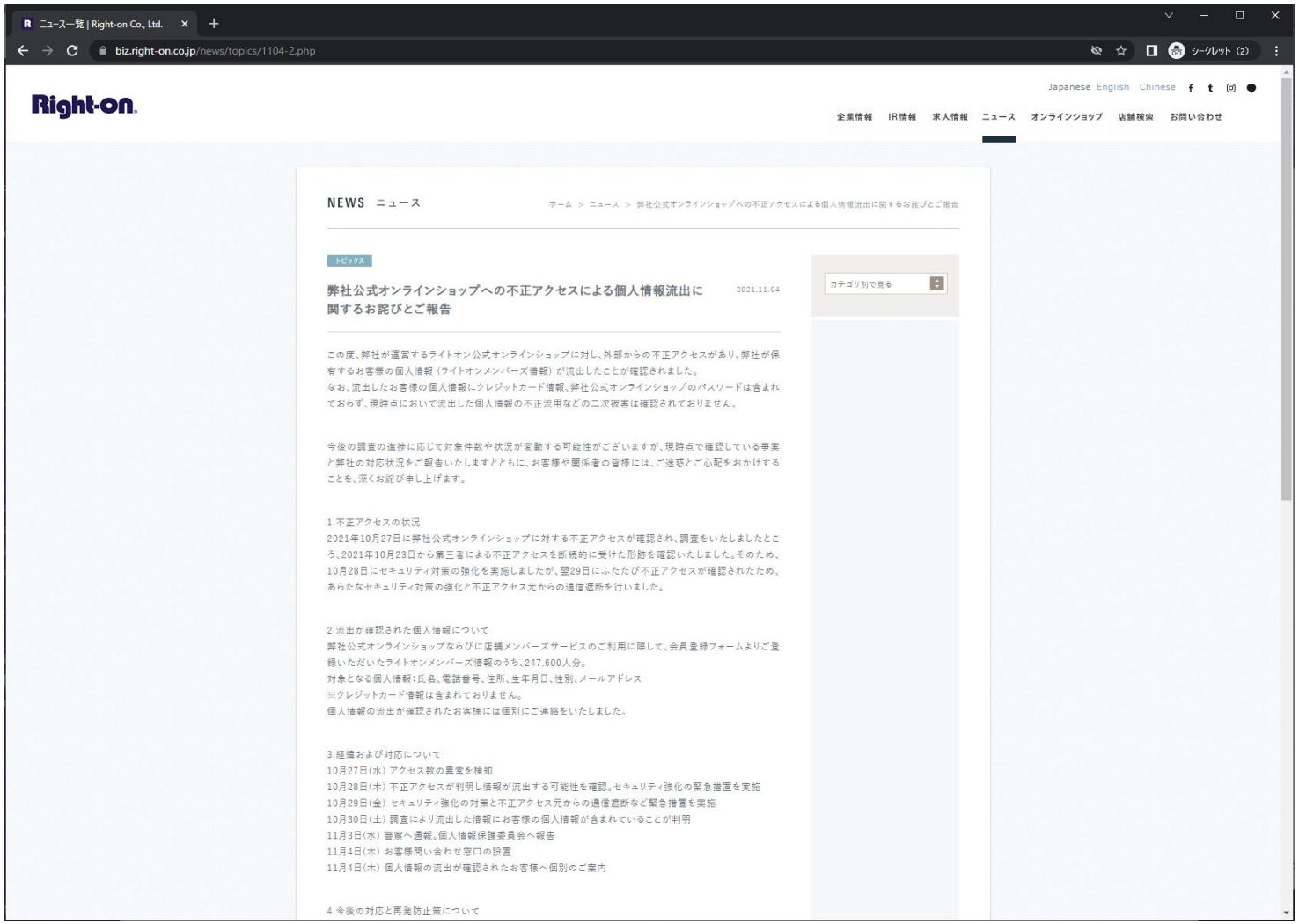
最近、ECサイトからのクレジットカード情報の漏洩や個人情報漏洩は後を絶ちません。
今回はその中のいくつかの事例について説明します。

- ライトオンのECサイトに不正アクセス。氏名、メールアドレスなど個人情報24万件が流出
  - https://netshop.impress.co.jp/node/9219
- ECサイトでまたクレカ情報流出か　建築系ショップから2018年7月～21年1月の間に4000件以上
  - https://www.itmedia.co.jp/news/articles/2107/20/news150.html
- 「エヴァ」公式ECでクレカ情報流出か　セキュリティコード含む1万7828件
  - https://www.itmedia.co.jp/news/articles/2112/01/news107.html
- ユニクロとジーユーのECサイトに不正アクセス、リスト型攻撃で46万件強の顧客情報が閲覧された可能性
  - https://netshop.impress.co.jp/node/6459
- ベイシア通販サイトで個人情報が流出 - ECサービスの不正アクセスで
  - https://www.security-next.com/131254

ライトオンのECサイトに不正アクセス。氏名、メールアドレスなど個人情報24万件が流出

https://netshop.impress.co.jp/node/9219

ライトオンのECサイトへの不正アクセス



https://biz.right-on.co.jp/news/topics/1104-2.php

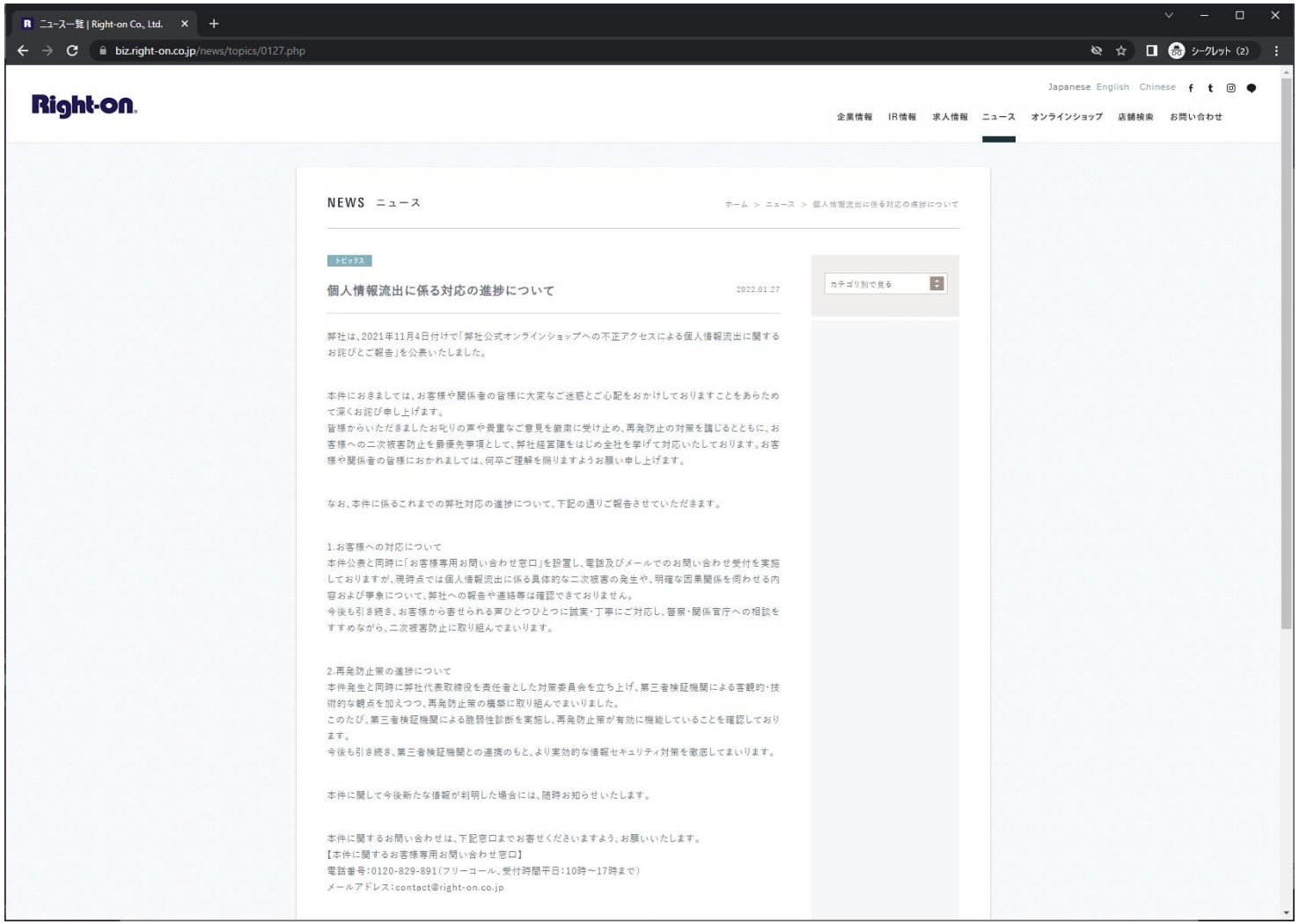
ライトオンのECサイトへの不正アクセス

気づいたきっかけ	アクセス数の異常を検知
期間	2021/10/23-2021/10/29
公表日	2021/11/04
流失した可能性がある数	247,600件
流出した内容	• 氏名 • 電話番号 • 住所 • 生年月日 • 性別 • メールアドレス
クレジットカード情報漏洩の有無	なし
不正アクセスの原因	記載なし
その後の対策	• お客様問い合わせ窓口の設置 • 個人情報の流出が確認されたお客様へ個別のご案内 • 対策委員会を立ち上げ、第三者検証機関による客観的・技術的な観点を加えつつ、再発防止策の構築 • 第三者検証機関による脆弱性診断を実施し、再発防止策の有効性の確認

時系列

- 10/23 第三者による不正アクセスを断続的に受けた形跡
- 10/27 アクセス数の異常を検知
- 10/28 不正アクセスが判明し情報が流出する可能性を確認。セキュリティ強化の緊急措置を実施
- 10/29 セキュリティ強化の対策と不正アクセス元からの通信遮断など緊急措置を実施
- 10/30 調査により流出した情報にお客様の個人情報が含まれていることが判明
- 11/03 警察へ通報。個人情報保護委員会へ報告
- 11/04 お客様問い合わせ窓口の設置
- 11/04 個人情報の流出が確認されたお客様へ個別のご案内
- 11/18 個人情報流出に係る対応状況のご報告
- 01/27 個人情報流出に係る対応の進捗について
    - 第三者検証機関による脆弱性診断を実施し再発防止策が有効に機能していることを確認

個人情報流出に係る対応の進捗について

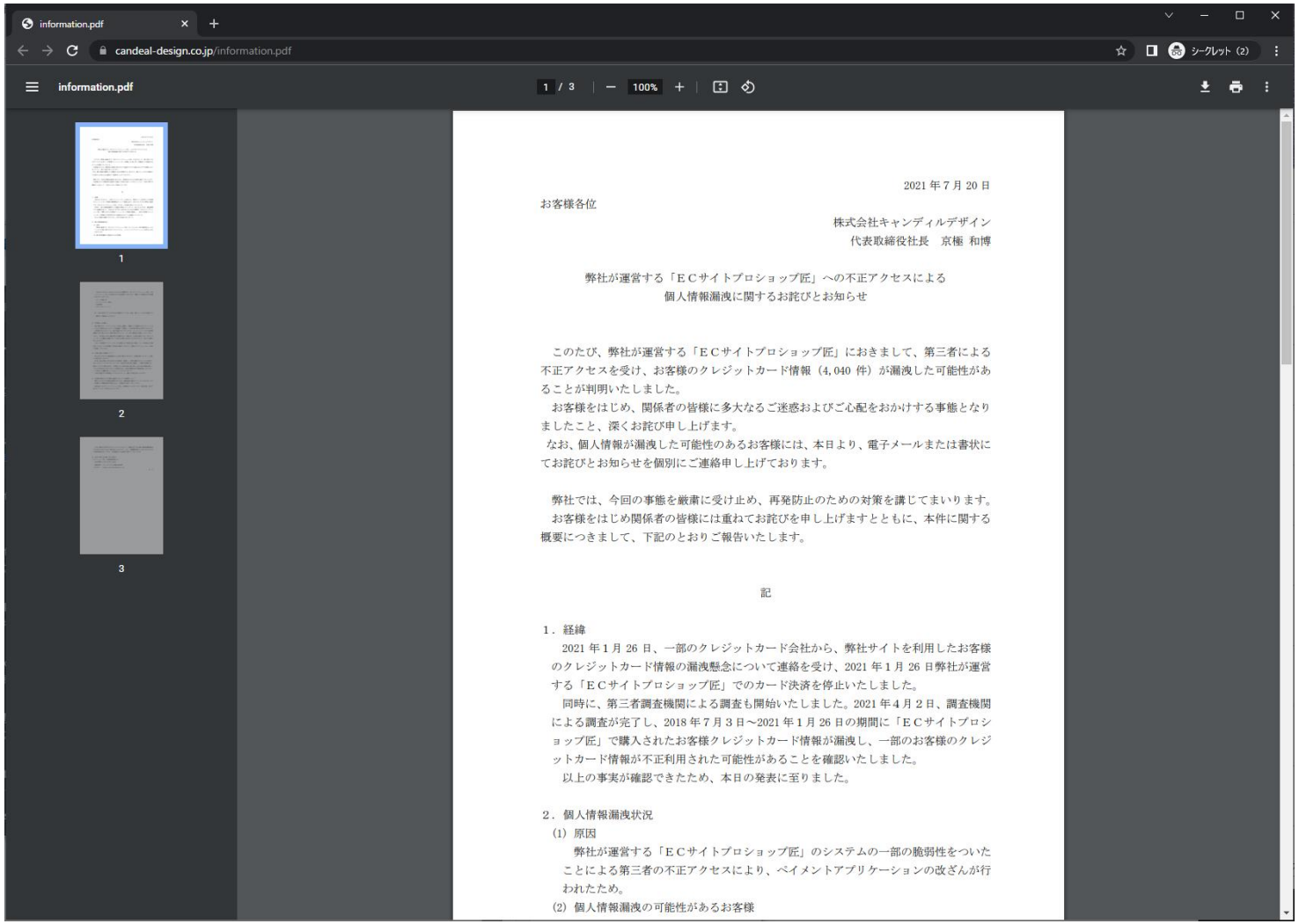


https://biz.right-on.co.jp/news/topics/0127.php

ECサイトでまたクレカ情報流出か　建築系ショップから2018年7月～21年1月の間に4000件以上

https://www.itmedia.co.jp/news/articles/2107/20/news150.html

ＥＣサイトプロショップ匠への不正アクセス



https://www.candeal-design.co.jp/information.pdf

ＥＣサイトプロショップ匠への不正アクセス

気づいたきっかけ	一部クレジットカード会社からの漏洩懸念についての連絡
期間	2018/7/3~2021/1/26
公表日	2021/7/20
流失した可能性がある数	3,357件
流出した内容	・カード名義人名 ・クレジットカード番号 ・有効期限 ・セキュリティコード
クレジットカード情報漏洩の有無	あり
不正アクセスの原因	システムの一部の脆弱性をついたことによる 第三者の不正アクセスにより、ペイメントアプリケーションの改ざん
その後の対策	• 調査結果を踏まえてシステムのセキュリティ対策および監視体制の強化を行い、再発防止を図る • いまだ再開日のお知らせはなし

時系列

- 2018/07/03~2021/01/26 期間中のクレジットカード情報が漏洩
- 2021/01/26 一部クレジットカード会社からクレジットカード情報漏洩の懸念を受けカード決済を停止
- 2021/06/24 所轄警察署に相談
- 2021/06/29 個人情報保護委員会に報告
- 2021/07/20 個人情報漏洩に関するお詫びとお知らせをWebに掲載

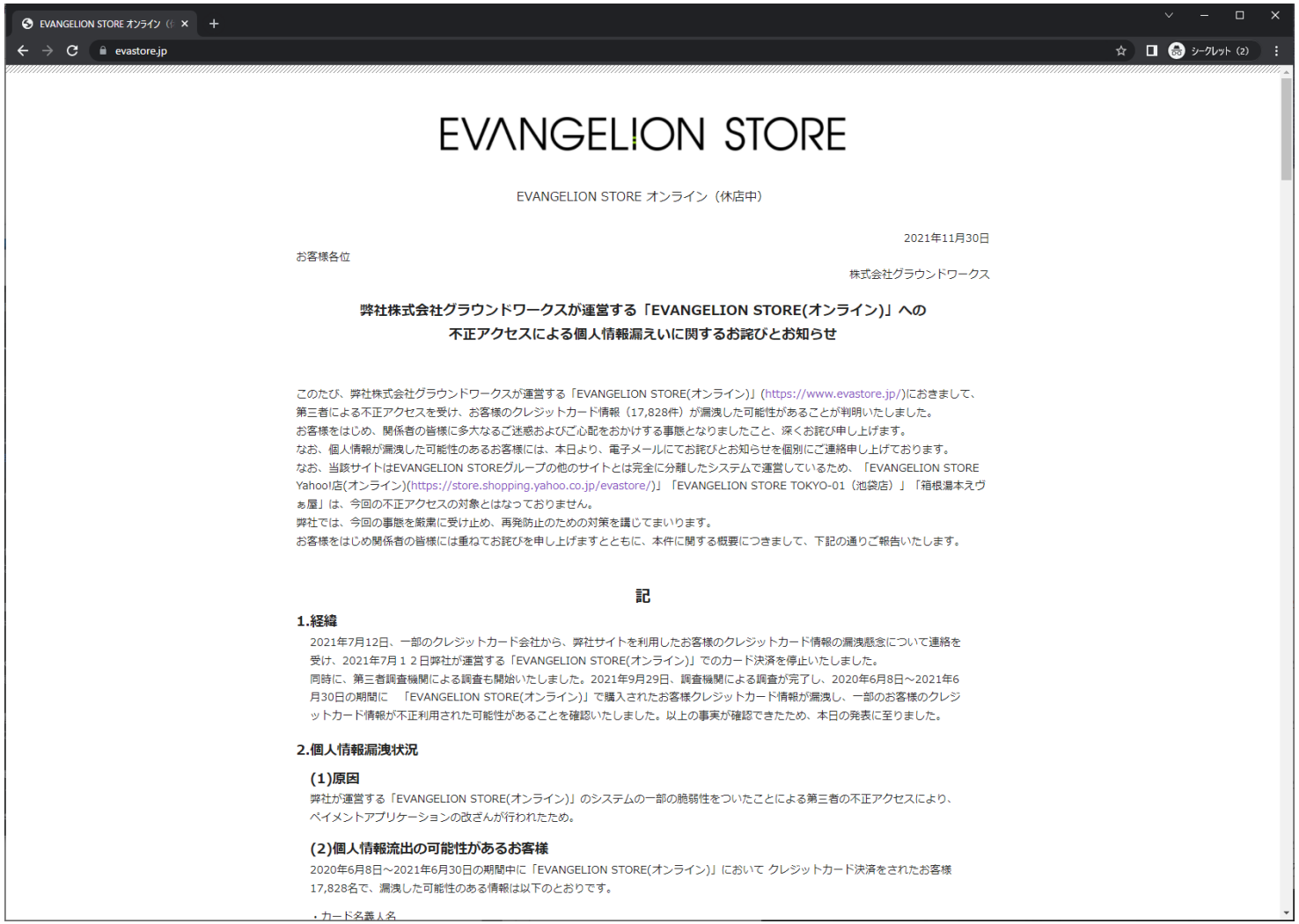
決済代行会社等と協議し、不確定な情報の公開はいたずらに混乱を招き、お客様へのご迷惑を最小限に食い止める対応準備を整えてからの告知が不可欠であるとの説明を受け、発表は調査会社の調査結果、およびカード会社との連携を待ってから行うことにいたしました。

https://www.candeal-design.co.jp/information.pdf

「エヴァ」公式ECでクレカ情報流出か　セキュリティコード含む1万7828件

https://www.itmedia.co.jp/news/articles/2112/01/news107.html

EVANGELION STORE(オンライン)への不正アクセス



EVANGELION STORE

EVANGELION STORE オンライン（休店中）

2021年11月30日

お客様各位

株式会社グラウンドワークス

弊社株式会社グラウンドワークスが運営する「EVANGELION STORE(オンライン)」への
不正アクセスによる個人情報漏えいに関するお詫びとお知らせ

このたび、弊社株式会社グラウンドワークスが運営する「EVANGELION STORE(オンライン)」(https://www.evastore.jp/)におきまして、第三者による不正アクセスを受け、お客様のクレジットカード情報（17,828件）が漏洩した可能性があることが判明いたしました。
お客様をはじめ、関係者の皆様に多大なるご迷惑およびご心配をおかけする事態となりましたこと、深くお詫び申し上げます。
なお、個人情報が漏洩した可能性のあるお客様には、本日より、電子メールにてお詫びとお知らせを個別にご連絡申し上げております。
なお、当該サイトはEVANGELION STOREグループの他のサイトとは完全に分離したシステムで運営しているため、「EVANGELION STORE Yahoo!店(オンライン)(https://store.shopping.yahoo.co.jp/evastore/)」「EVANGELION STORE TOKYO-01（池袋店）」「箱根湯本えヴぁ屋」は、今回の不正アクセスの対象とはなっておりません。
弊社では、今回の事態を厳粛に受け止め、再発防止のための対策を講じてまいります。
お客様をはじめ関係者の皆様には重ねてお詫びを申し上げますとともに、本件に関する概要につきまして、下記の通りご報告いたします。

記

1.経緯

2021年7月12日、一部のクレジットカード会社から、弊社サイトを利用したお客様のクレジットカード情報の漏洩懸念について連絡を受け、2021年7月１２日弊社が運営する「EVANGELION STORE(オンライン)」でのカード決済を停止いたしました。
同時に、第三者調査機関による調査も開始いたしました。2021年9月29日、調査機関による調査が完了し、2020年6月8日～2021年6月30日の期間に　「EVANGELION STORE(オンライン)」で購入されたお客様クレジットカード情報が漏洩し、一部のお客様のクレジットカード情報が不正利用された可能性があることを確認いたしました。以上の事実が確認できたため、本日の発表に至りました。

2.個人情報漏洩状況

(1)原因

弊社が運営する「EVANGELION STORE(オンライン)」のシステムの一部の脆弱性をついたことによる第三者の不正アクセスにより、ペイメントアプリケーションの改ざんが行われたため。

(2)個人情報流出の可能性があるお客様

2020年6月8日～2021年6月30日の期間中に「EVANGELION STORE(オンライン)」において クレジットカード決済をされたお客様17,828名で、漏洩した可能性のある情報は以下のとおりです。

・カード名義人名

https://www.evastore.jp/

EVANGELION STORE(オンライン)への不正アクセス

気づいたきっかけ	一部クレジットカード会社からの漏洩懸念についての連絡
期間	2020/6/8~2021/6/30
公表日	2021/11/30
流失した可能性がある数	17,828件
流出した内容	・カード名義人名 ・クレジットカード番号 ・有効期限 ・セキュリティコード ・ログオンID（EVANGELION STORE(オンライン)会員用メールアドレス） ・パスワード（EVANGELION STORE(オンライン)会員用）
クレジットカード情報漏洩の有無	あり
不正アクセスの原因	システムの一部の脆弱性をついたことによる第三者の不正アクセスにより、ペイメントアプリケーションの改ざんが行われたため。
その後の対策	• 調査結果を踏まえてシステムのセキュリティ対策および監視体制の強化 • いまだ再開日のお知らせはなし

時系列

- 2020/06/08~2021/06/30 期間中のクレジットカード情報が漏洩
- 2021/07/12 一部クレジットカード会社からクレジットカード情報漏洩の懸念を受けカード決済を停止
- 2021/09/29 第三者調査機関による調査完了
  - 2020年6月8日～2021年6月30日の期間に　「EVANGELION STORE(オンライン)」で購入されたお客様クレジットカード情報が漏洩し、一部のお客様のクレジットカード情報が不正利用された可能性があることを確認
- 2021/9/6 個人情報保護委員会に報告
- 2021/10/5 所轄警察署に被害申告
- 2021/11/30 個人情報漏えいに関するお詫びとお知らせをWebに掲載

不確定な情報の公開はいたずらに混乱を招き、お客様へのご迷惑を最小限に食い止める対応準備を整えてからの告知が不可欠であると判断し、発表は調査会社の調査結果、およびカード会社との連携を待ってから行うことに致しました。

https://www.evastore.jp/

ユニクロとジーユーのECサイトに不正アクセス、リスト型攻撃で46万件強の顧客情報が閲覧された可能性

https://netshop.impress.co.jp/node/6459

リスト型攻撃による不正ログイン

https://www.uniqlo.com/jp/ja/contents/corp/press-release/2019/05/19051409_uniqlo.html

リスト型攻撃による不正ログイン

気づいたきっかけ	お客様から「身に覚えのない登録情報変更の通知メールが届いた」というお申し出
期間	2019/4/23~2019/5/10
公表日	2019/5/14
流失した可能性がある数	461,091件
流出した内容	• お客様の氏名（姓名、フリガナ） • お客様の住所（郵便番号、市区郡町村、番地、部屋番号） • 電話番号、携帯電話番号、メールアドレス、性別、生年月日、購入履歴、マイサイズに登録している氏名およびサイズ • 配送先の氏名（姓名、フリガナ）、住所、電話番号 • クレジットカード情報の一部 （カード名義人、有効期限、クレジットカード番号の一部） • クレジットカード番号は、上４桁と下４桁以外は非表示
クレジットカード情報漏洩の有無	クレジットカード情報の一部 、セキュリティコードは漏洩していない
不正アクセスの原因	他社サービスから流出した可能性のあるユーザID・パスワードを利用した「リスト型アカウントハッキング（リスト型攻撃）」と推測
その後の対策	• アクセスについての監視の強化 • 個人情報が閲覧された可能性のある461,091件のユーザIDについては、同年５月13日にパスワードを無効化、再設定のお願いを送付

時系列

- 2019/4/23-2019/5/10 不正ログインが試行される
- 日にち不明 お客様から「身に覚えのない登録情報変更の通知メールが届いた」というお申し出
- 2019/5/10ご本人以外の第三者による不正なログインが発生したことを確認
- 2019/5/13 個人情報が閲覧された可能性のあるユーザのパスワードを無効化し、再設定のお願いを送付
- 2019/5/14 「リスト型アカウントハッキング（リスト型攻撃）」による弊社オンラインストアサイトへの不正ログインの発生とパスワード変更のお願いについて　を　Webに掲載

https://www.uniqlo.com/jp/ja/contents/corp/press-release/2019/05/19051409_uniqlo.html

ベイシア通販サイトで個人情報が流出 - ECサービスの不正アクセスで

https://www.security-next.com/131254

オムニECシステムへの不正アクセス

https://www.grinc.co.jp/information202109.pdf

お客様情報流出に関するお詫びとお知らせ

2021 年 11 月 1 日

「ベイシアネットショッピング」をご利用のみなさまへ

株式会社ベイシア

弊社「ベイシアネットショッピング」委託先への不正アクセスによる
お客様情報流出に関するお詫びとお知らせ

この度、弊社が運営する「ベイシアネットショッピング」の EC サイト（以下「本件 EC サイト」といいます）の制作・運用委託先に対し、第三者による不正なアクセスが確認され、お客様のクレジットカード情報（3,101 件）及び、個人情報（254,207 件）が流出した可能性があることが判明致しました。

ご迷惑をお掛けしているお客様、すべての関係者のみなさまに多大なるご迷惑とご心配をお掛けする事態に至りましたことを、深くお詫び申し上げます。誠に申し訳ございません。
クレジットカード会社からの連絡で、クレジットカードを既に再発行をいただいたお客様には、お手数をお掛け致しましたこと、重ねてお詫び申し上げます。

なお、対象のお客様は 11 月 1 日（月）より、ベイシアネットショッピングに登録していただいているメールアドレスに「ベイシアからの重要なお知らせ」としてご案内メールをお届けしております。
本件流出の可能性が発生した EC サイトは、管理を外部に委託していたもので、弊社ではクレジットカード情報を保有しておりませんでした。また、現在 EC サイトは停止しており、外部からのアクセスは全て遮断する対策を施しております。
なお、ベイシアアプリ、ベイシアポイントカード、タッチ de デリカは、別のシステムを使用しているため、本件との関係は一切ございませんので、ご安心ください。

1. 経緯
2021 年 9 月 1 日に、一部のクレジットカード会社から本件 EC サイトを利用したお客様のクレジットカード情報の流出に関する懸念について連絡があり、確認したところ、不正アクセスのおそれが判明致しました。同日中に本件 EC サイトのサービスを停止し、同時に、第三者調査機関による調査を開始致しました。2021 年 10 月 13 日に調査機関による調査が完了し、その結果、2021 年 4 月 26 日から 2021 年 8 月 19 日までの間に本件 EC サイトで購入された一部のお客様のクレジットカード情報、および過去にご注文をされたお客様の個人情報が流出した可能性があることを確認致しました。その後、クレジットカード会社等と連携し、詳細な事実確認のため本日の発表に至りました。

https://www.beisia.co.jp/wp-content/uploads/2021/11/c9f3e8b196c27d7f25d6e823c664f247-1.pdf

オムニECシステムへの不正アクセス(ベイシアネットショッピング)

気づいたきっかけ	一部のクレジットカード会社から本件 EC サイトを利用したお客様のクレジット カード情報の流出に関する懸念について連絡
期間	2021/4/26-2021/8/19
公表日	2021/11/1
流失した可能性がある数	個人情報（254,207 件）クレジットカ ード情報（3,101 件）
流出した内容	・クレジットカード番号 ・有効期限 ・セキュリティコード ・メールアドレス ・氏名（仮名も含む） ・郵便番号、住所 ・高度に暗号化されたパスワード ・電話番号 ・生年月日 ・初回/最終購入日 累計購入回数/金額 ・注文番号、支払方法、購入金額、受発日、入金日 ・（任意）性別、職業、FAX、注文時のお問い合わせ文
クレジットカード情報漏洩の有無	クレジットカードの番号、有効期限、セキュリティコード
不正アクセスの原因	本件 EC サイト制作・運用委託先（東芝テック株式会社〈東京都品川区〉および株式会社ジーアー ル〈京都市中京区〉）のシステムへの第三者による不正アクセス。
その後の対策	• 調査結果を踏まえてシステムのセキュリティ対策および監視体制を強化し、再発防止 • 今後は外部機関による安全性が確認できてから運用を再開

時系列

- 2021/4/26-2021/8/19 期間中の個人情報及びクレジットカード情報が漏洩
- 2021/9/1 一部のクレジットカード会社から本件 EC サイトを利用したお客様のクレジット カード情報の流出に関する懸念について連絡
- 2021/9/1 ECサイトを停止、第三者調査機関による調査を開始
- 2021/9/3 所轄警察署に状況報告
- 2021/9/22 個人情報保護委員会に報告
- 2021/10/13 調査機関による調査完了

不確定な情報の公表は不要な混乱を招くおそれがあったことから、クレジッ トカード会社等と協議の上、第三者調査会社の調査結果を待ち、クレジットカード会社その他の関 係機関との連携を確保した上で公表することに致しました。

https://www.beisia.co.jp/wp-content/uploads/2021/11/c9f3e8b196c27d7f25d6e823c664f247-1.pdf

複数小売事業者が利用するECシステムに不正アクセス - 個人情報約15万件に影響か

https://www.security-next.com/130145

ECサイトの運用形態

ECサイトの運用形態

- 自社でECサイトを構築する
  - 自社で開発者を雇用しECサイトを構築する
  - システム会社と契約し、自社用のECサイトを構築する
- SaaSを利用する
  - SaaSのサイトに登録し、ECサイトを開設する

ECサイトの運用形態

	自社で構築	SaaSを利用
導入コスト	高い	低い
セキュリティ対策	自社・委託会社で対応	SaaS運営側が対応
サーバの管理	必要	不要
バージョンアップ	自社・委託会社で対応	SaaS運営側が対応
主な料金体制	開発費用+保守費用(月額)	売上に応じた手数料
カスタマイズ性	高い	低い
データの移行	比較的柔軟に対応可能	難しい場合がある

攻撃の仕組みと対策

攻撃の仕組みと対策

- パスワードリスト攻撃
- SQLインジェクションなどによる情報漏洩
- 不正コンテンツを設置されることによる情報漏洩

パスワードリスト攻撃

過去にメールアドレスとパスワードが漏洩した漏洩事故は多々あり、それらが流出した二次被害としてパスワードリスト型攻撃があります。

- 多くのWebサイトはメールアドレスをログインIDに利用している。
- サイトごとにパスワードを変更することはユーザにとっては面倒なため、
  同じメールアドレスと同じパスワードで様々なサイトに登録しているユーザが存在する。

パスワードリスト攻撃の対策(運営側)

パスワードリスト攻撃を防ぐ手段としては下記の対策があります。

- メールアドレス以外のログインIDを利用する
    - 利便性との兼ね合いがあるので要検討
- ２段階認証の導入
- ログイン通知
- ログイン履歴
- 休眠アカウントの廃止

パスワードリスト攻撃の対策(利用者側)

パスワードを使いまわさないことが重要です。

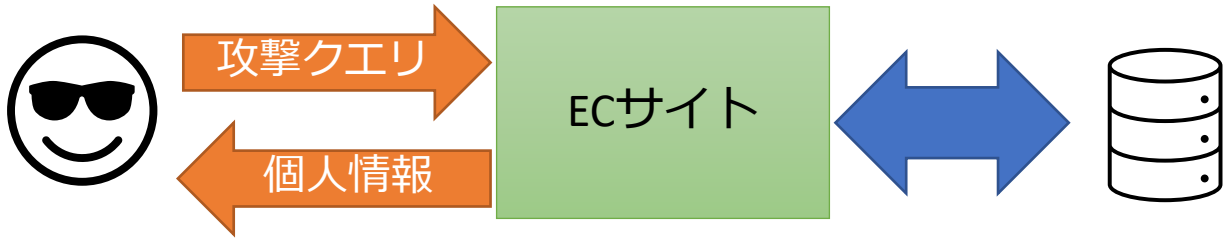
- パスワード管理ツールを利用する。
- 自分なりのルールを決めてサイトごとに違うパスワードを使う。
  - 基本を「1testasdD」として、example.comのパスワードの場合、3文字目にドメインの頭文字を大文字[E]で入れ後ろから2番目にドメインの後ろから二番目の文字[o]を入れるなど「1tEestasdoD」
- 手帳にメモを取って管理する方法もあります。その場合は、紛失するリスクも伴うので、見られてもわからないように工夫することを推奨します。自分しかわからない変換方法を施してメモを取るなど

SQLインジェクションなどによる情報漏洩

ECサイト自体に脆弱性があり、データベースに保存された顧客情報など漏洩するケースは昔から多々ありました。

例えば、WebアプリケーションにSQLインジェクションと呼ばれる脆弱性があり、データベースに保存された顧客データがすべて攻撃者に漏洩してしまうケースです。

ただし、最近では、クレジットカード情報の非保持化が進んでおり、データベースに保存されません。そのため、この手法では、クレジットカード情報が漏洩することは少なくなっています。

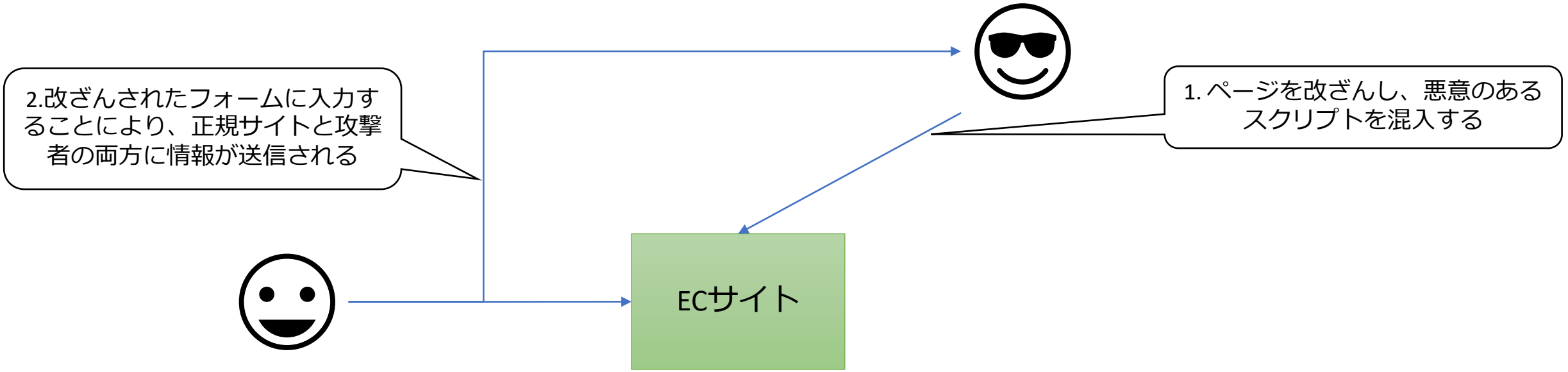


SQLインジェクションなどによる情報漏洩(対策)

- IPAが出している「安全なウェブサイトの作り方」を参考に構築し、セキュリティ実装チェックリストなどを用いてリリース時や更新時に、自己点検を行う。
  - https://www.ipa.go.jp/security/vuln/websecurity.html
- 脆弱性診断を実施し、残存する脆弱性を洗い出し、リスクを評価した上で修正等を行う。

不正コンテンツを設置されることによる情報漏洩

前のページのケースでは、攻撃者が逐次攻撃を行うことにより、顧客データが漏洩していました。しかし、最近のWebアプリケーションでは、クレジットカード情報はデータベースに保持しないため、攻撃者は前のページの手法では、クレジットカード情報を取得することができません。そのため、Webアプリケーションのコンテンツを改ざんし正規のユーザが入力した情報を正常に処理しつつ、攻撃者が用意したサーバにも入力した情報を送信します。



不正コンテンツを設置されることによる情報漏洩(対策)

- IPAが出している「安全なウェブサイトの作り方」を参考に構築し、セキュリティ実装チェックリストなどを用いてリリース時や更新時に、自己点検を行う。
  - https://www.ipa.go.jp/security/vuln/websecurity.html
- 脆弱性診断を実施し、残存する脆弱性を洗い出し、リスクを評価した上で修正等を行う。
- 改ざん検知等の導入を検討し、改ざんされた際に即時検知できる体制を用意する。

番外編(別の漏洩ルート)

ECサイトを運営するうえで、守るべき部分は、ECサイト部分だけでなくそれを利用する環境も守る必要があります。

- 顧客情報等を含むクラウドストレージの公開設定
- 社内に置いたネットワークストレージ等の公開設定
- ECサイトの更新や顧客情報を管理するPCのマルウェア対策
- 店舗のメールアドレスやECサイトの管理ページ等のパスワード管理
- 顧客情報の入ったUSBの紛失
- など

まとめ

- 多くのECサイトが被害にあっている
  - 他社で漏洩したユーザID、パスワードを用いて攻撃されることによってIDパスワードを使いまわしている利用者が不正アクセスされてしまう。
  - サイトを改ざんされることによって気づくまでずっと漏洩し続ける。
    - クレジットカード会社からの不正利用による連絡によって気づく。
- ECサイトを自社で運用するかSaaSのサービスを使うかは事業規模等によってよく検討したほうが良い。
  - SaaSは売上に応じた手数料を取る形が多い。
- ECサイトを運営するうえでは、サイトだけでなくそれを利用する環境についても考慮する必要がある。
  - ネットワークストレージやクラウドストレージの公開設定のミスや
    ランサムウェアへの感染による情報漏洩など。

SECURE CYCLE

システム開発におけるセキュリティ対策を当たり前に

〒808-0138 福岡県北九州市若松区ひびきの北8番1号
技術開発交流センター 314号室
TEL: 093-701-6735 / URL: https://secure-cycle.co.jp/