



NTTデータ先端技術のセキュリティ



**INTELLILINK セキュリティ情報配信サービス  
注目されているセキュリティ事故・事件に関する情報  
<2023年03月版 (第44号)> (選り抜き版)**

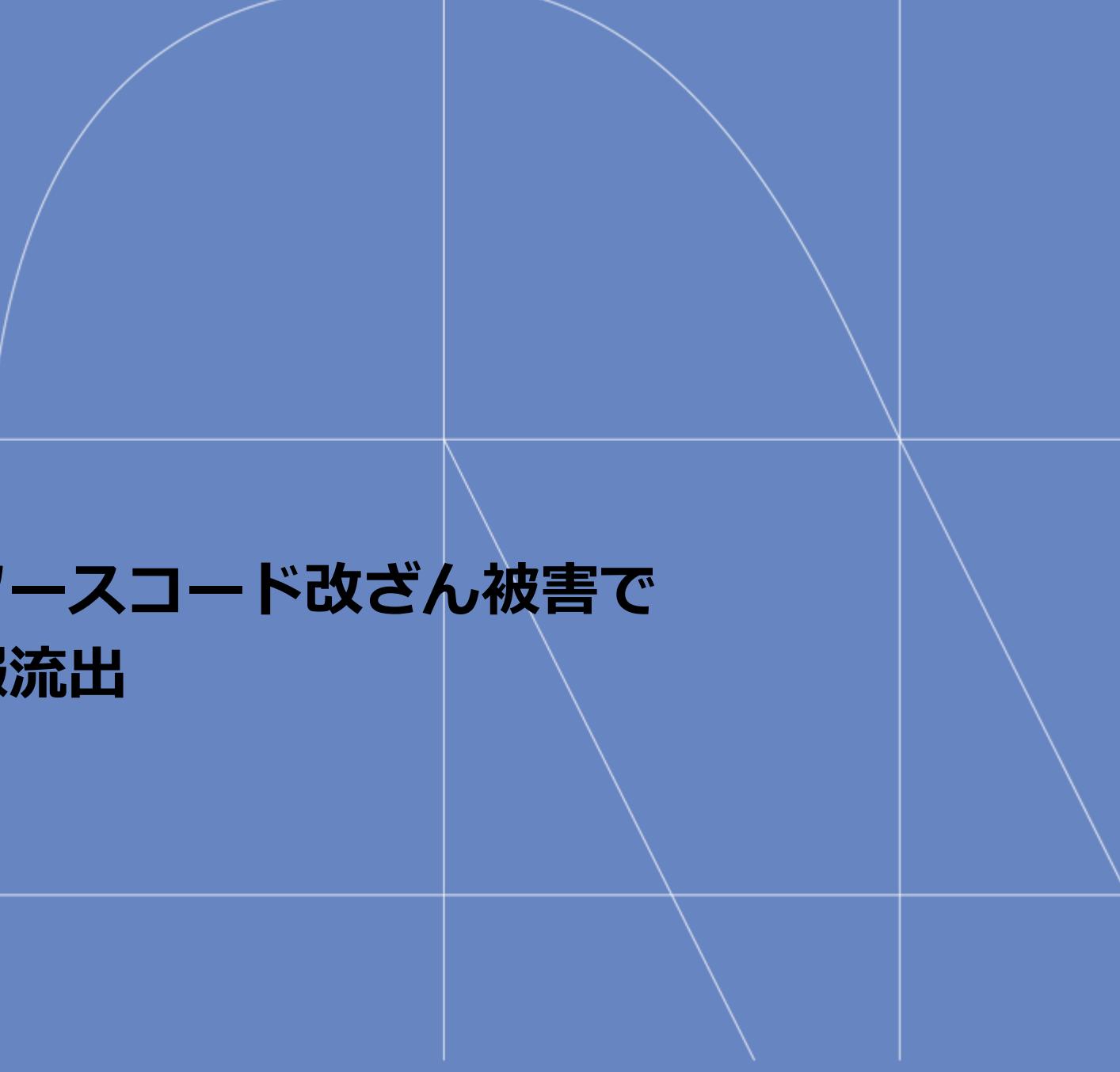
**2023年3月30日**  
**NTTデータ先端技術株式会社**  
**サイバーセキュリティ事業本部**

# 今回のサマリー

## ショーケースのソースコード改ざん被害で利用サイトが情報流出

株式会社ショーケースが提供するウェブサイトの最適化サービスが改ざんの被害を受け、サービスを利用していた複数の通販サイトでクレジットカードなどの情報が流出する被害が発生しました。本記事では、攻撃の仕組みとウェブサイト運営者の対策を解説します。





**ショーケースのソースコード改ざん被害で  
利用サイトが情報流出**

# 1. 事業概要

株式会社ショーケースは2022年10月25日に同社が提供するウェブサイト向けサービスの一部が第三者によって不正に改ざんされたと発表しました。

改ざんによる影響を受けたのはEFO※ツール「フォームアシスト」、マーケティングツール「サイト・パーソナライザ」、サイト表示変換ツール「スマートフォン・コンバータ」としています。ショーケースはこの改ざんの被害によって、サービスを利用していた企業のユーザが入力したクレジットカード番号や個人情報などが外部に流出した可能性があるとしています。

2023年3月10日現在、被害を受けた企業は少なくとも13社におよび、各社が影響を受けたウェブサイトや流出した情報を公開しています。

※Entry Form Optimization ユーザによるフォームへの入力率を高めるためのフォーム最適化

## 2. タイムラインと被害を受けた企業

表1 タイムライン

日付	内容	備考
2022年7月19日～29日	ショーケースが改ざん被害を受けた期間	期間はサービス毎に異なる
2022年7月26日	ショーケースの取引先からフォームアシストのソースコードに不審な記述がある旨の指摘を受け、ショーケース提供のサービスのソースコードを調査	-
2022年7月28日	ショーケースから同社サービスを使用している取引先へ連絡	-
2022年8月04日	出光クレジットが「ウェブステーション」の被害を発表	ショーケースによる影響と明記なし
2022年10月25日	ショーケースが不正アクセス被害を発表	-
2022年10月25日	エービーシーマートが「ABC-MART公式オンラインストア」の被害を発表	発表に件数の情報なし
2022年10月26日	ユーキャンが「生涯学習のユーキャン」の被害を発表	流出は200件
2022年10月26日	出光クレジットが「ウェブステーション」の被害を発表	発表に件数の情報なし
2022年10月26日	富士フイルムイメージングシステムズが「FUJIFILMプリント&ギフト」の被害を発表	流出は851件
2022年10月26日	富士フイルムイメージングシステムズが「フジフィルムモール」の被害を発表	流出は519件
2022年11月1日	カクヤスが「カクヤスネットショッピング」の被害を発表	流出は8,094件
2022年11月10日	エスビー食品が「お届けサイト」の被害を発表	流出は164件
2022年11月15日	本出版販売が「Honya Club.com」の被害を発表	流出は427件
2023年1月10日	カバーマークが「カバーマーク公式オンラインショップ」の被害を発表	流出は2,259件
2023年1月11日	ベストリンクが「e-ca公式サイト」の被害を発表	流出は15件
2023年1月19日	長寿乃里が「あっとよか」の被害を発表	流出は37件
2023年1月24日	シャルレが「CHARLE WEB STORE」の被害を発表	流出は605件

※各ウェブサイトから流出した項目はウェブサイトによって異なりますが、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、生年月日の全てまたは一部となっています。

### 3. 本件の攻撃の仕組みとポイント

本件はウェブサイトへサービスを提供するベンダであるショーケースのサーバを攻撃・侵害したサプライチェーン攻撃です。ウェブサイト自体は攻撃されていないため、ウェブサイト運営者が攻撃や被害の発生に気付けないという特徴があります。ユーザはウェブサイトを通常通り利用するだけで被害を受けます。

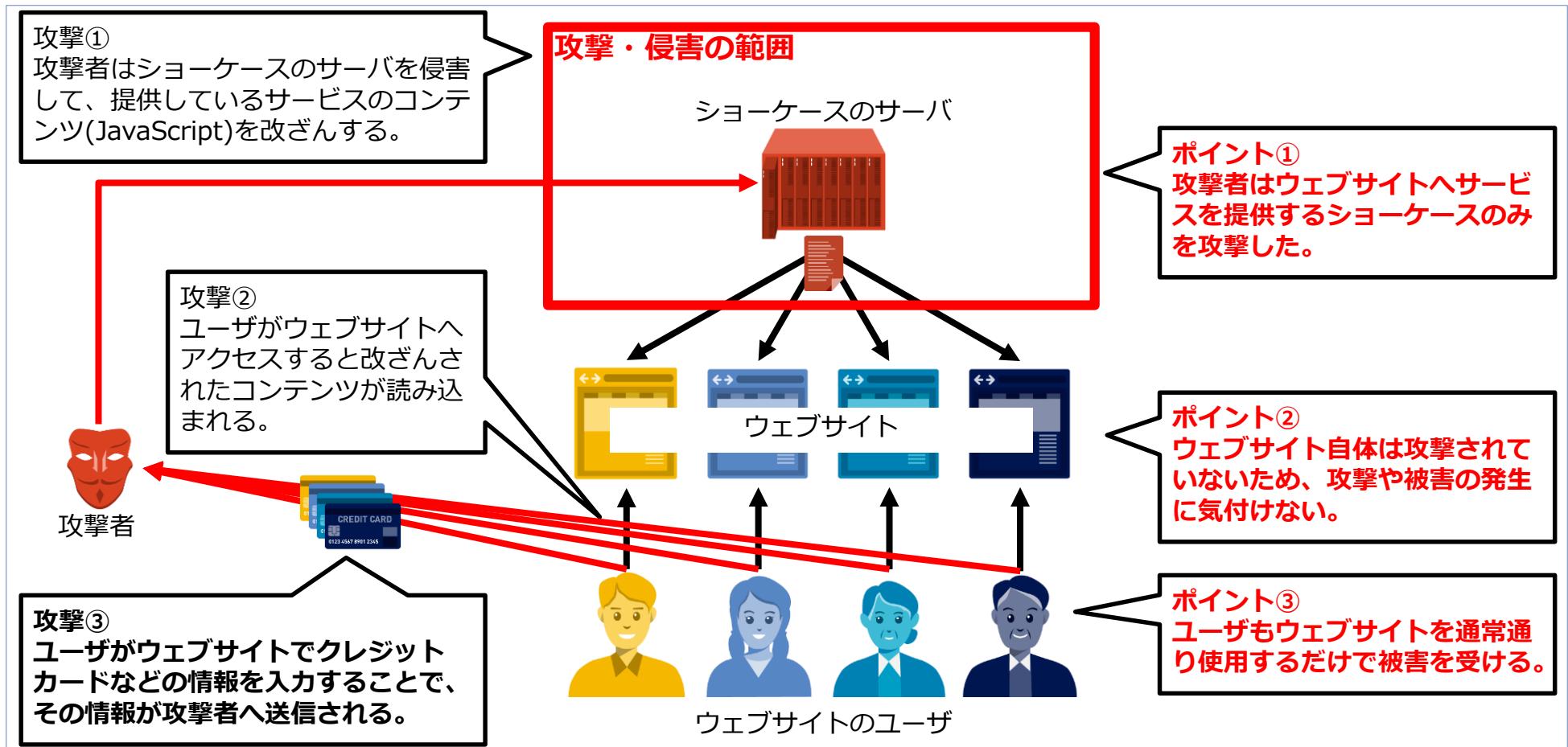


図1 攻撃の仕組みとポイント

## 4. ウェブサイト運営者の対策 (1/2)

技術面では、外部のホストから悪意あるスクリプトが被害者のブラウザ上で実行されること(攻撃②③)を防ぐ必要があります。これには、CSPやSRIなどのウェブ標準のセキュリティ対策技術が有効です※。

ただし、本件ではベンダが管理するスクリプトを設置したホストを信頼する前提のため、**CSPのみではベンダのホストが侵害されるサプライチェーン攻撃を防ぐことはできない**点に注意が必要です。

### CSP(Contents Security Policy)

ウェブページに読み込まれるリソース(画像やスクリプトやスタイルシート)の種類と取得元を制限することで、クロスサイトスクリプティングなどの攻撃を防ぐための仕組みです。ウェブサーバまたはアプリケーションでHTTPレスポンスヘッダ「Content-Security-Policy」またはHTMLの「meta」要素で許可するリソースの情報を指定します。

### SRI(Subresource Integrity)

ウェブページがCDNなどの外部のリソースを読み込む際に、そのリソースが改ざんされていないことを確認するための仕組みです。実際のリソースのハッシュ値と事前に指定したハッシュ値を比較することで、リソースの完全性を確認します。

※CSPとSRIは、運用の際にベンダによるリソースの変更に対応し続ける必要がある点に注意が必要です。CSPはリソースのURLの変更、SRIはリソースの内容(ハッシュ値)の変更に追従する必要があります。いずれも追従できないとウェブサイトの機能を維持できなくなる可能性があります。

## 4. ウェブサイト運営者の対策 (2/2)

ウェブサイトで利用する外部サービスを選定する際には、例えば以下の観点で選定すると良いでしょう。

- ・ ベンダから提供されるリソースを自サイト内に設置でき、外部のホストのリソースの読み込みをしないようにできる
- ・ CSPを使用して外部リソースの種類と取得元を制限できる
- ・ SRIを使用して外部リソースの正当性を検証できる

また、**インシデント対応体制に「利用している外部サービスの侵害」を追加し、**対応できるようにしておく必要があります。対応には、ベンダとの連絡体制の確保や、外部サービス遮断の判断・実施が挙げられます。事前に遮断によってウェブサイトが提供する機能の影響範囲を確認しておき、ウェブサイトの全部または一部の停止を判断・実施できるようにしておくことも重要です。

更に、個人データを扱うウェブサイトの場合は、**個人情報保護法に基づく対応内容も確認しておく**必要があります。2022年4月1日の個人情報保護法改正によって、個人データの流出などによって「個人の権利利益を害するおそれがあるとき※」は速やかに個人情報保護委員会への報告および本人への通知が必要です。本件もサイト運営者によって個人情報保護委員会への報告がされています。

※個人情報保護委員会が挙げている例として、要配慮個人情報が含まれる事態、財産的被害が生じるおそれがある事態、不正の目的をもって行われた漏えい等が発生した事態、1,000人を超える漏えい等が発生した事態があります。

漏えい等報告・本人への通知の義務化について | 個人情報保護委員会 [https://www.ppc.go.jp/news/kaiseihou\\_feature/roubeitouhoukoku\\_gimuka/](https://www.ppc.go.jp/news/kaiseihou_feature/roubeitouhoukoku_gimuka/)

## 5. まとめ

ショーケースが提供するウェブサイト向けサービスが侵害され、ウェブサイトを利用するユーザのクレジットカード情報等が流出する被害が発生しました。

本件はサプライチェーン攻撃であり、ウェブサイト運営者が攻撃や被害の発生に気付けないという特徴があります。ベンダのシステムを信頼する前提のため、CSPだけでは攻撃を防ぐことはできませんが、SRIによって攻撃を防ぐことができます。また、ウェブサイト運営者は、外部サービス侵害を想定したインシデント対応体制の整備や、改正個人情報保護法の内容を確認しておく必要があります。

## 6. 参考URL

- 不正アクセスに関するお知らせとお詫び - 株式会社ショーケース  
<https://www.showcase-tv.com/pressrelease/202210-fa-info/>
- 個人情報漏えいの可能性に関するお詫びとお知らせ | ABC-MART 【公式通販】  
<https://www.abc-mart.net/shop/pages/info-2022.aspx>
- 個人情報漏洩に関するお詫びとお知らせ | ユーキヤン  
<https://www.u-can.co.jp/info/release.html>
- 【重要】個人情報漏洩に関するお詫びとお知らせについて - 重要なお知らせ一覧 - 出光カード  
<https://www.idemitsucard.com/important/information2210-02.html>
- 弊社が運営するECサイト「FUJIFILMプリント&ギフト」への不正アクセスによるクレジットカード情報漏洩に関するお詫びとお知らせ | 富士フィルムイメージングシステムズ株式会社  
<https://www.fujifilm.com/ffis/ja/news/116>
- お詫びとお知らせ: | フジフィルムモール  
<https://mall-jp.fujifilm.com/shop/e/effinfo2022/>
- 株式会社カクヤス 【重要】クレジットカード情報漏洩に関するお詫びとお知らせについて  
<https://www.kakuyasu.co.jp/corporate/topics/20221101.pdf>
- エスビー食品株式会社 クレジットカード情報漏えいに関するお詫びとお知らせ  
[https://www.sbfoods.co.jp/info/2022/jl438m0000003jln-att/221110\\_info.pdf](https://www.sbfoods.co.jp/info/2022/jl438m0000003jln-att/221110_info.pdf)
- 不正アクセスによるクレジットカード情報流出に関するお詫びとお知らせ | 日本出版販売株式会社  
<https://www.nippan.co.jp/info/20221115/>
- カバーマーク株式会社 お客様情報漏洩の可能性に関するお詫びとお知らせ  
<https://www.covermark.co.jp/notice/230110/index.html>
- 弊社が運営する「e – c a 公式サイト」における個人情報漏えいに関するお詫びとおらせ  
<https://www.e-ca.jp/notice>
- クレジットカード情報漏洩に関するお詫びとお知らせについて | 長寿の里【あっとよか】  
[https://www.choju.com/news/2301attention\\_02.html?allocate\\_shopno=3](https://www.choju.com/news/2301attention_02.html?allocate_shopno=3)
- 弊社ウェブサイト「CHARLE WEB STORE (シャルレ ウェブストア)」へのサービス提供会社における個人情報漏えいのおそれに関するお詫びとお知らせ | 重要なお知らせ | 株式会社シャルレ 美と健康のシャルレへ/  
<https://www.charle.co.jp/news/important/p002269.html>

