2019 年 10 月 31 日

サービス＆セキュリティ株式会社 e-Gate センター

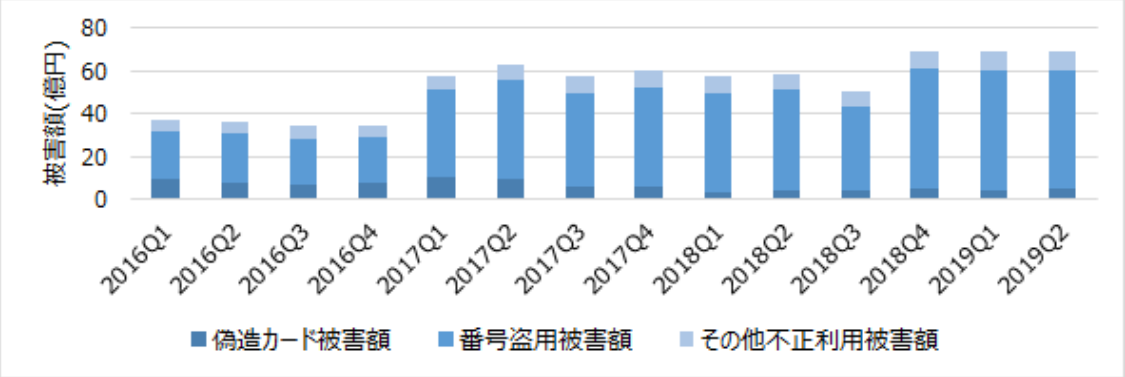
注意喚起：クレジットカード情報の流出インシデント増加中

1. 概要

オンラインショッピングサイトからクレジットカード情報が流出する事件が多く発生して被害額が増加の一途を辿っています。

一般社団法人日本クレジット協会の集計によれば、2019 年第 2 四半期のクレジットカードの不正使用による被害額は 68 億 5 千万円でした。このうち 79.5%は、店頭で偽造カードを使われるのではなく、窃取されたカード情報をインターネット上などの非対面取引で悪用するなりすましです。図 1 のように、被害額は前年同期に比べると 17.5%増加し、本年第 1 四半期に引き続き高い水準の状態が続いています。

直近では 2019 年 10 月に、約 7,000 件のカード番号、有効期限、名義人氏名、セキュリティコードが通信販売サイトから流出し、その一部は不正に使用されたとの報道がありました。



【図 1：クレジットカード不正利用被害の発生状況(日本クレジット協会調べ)】

カード情報の流出とそれによる金銭的被害を防ぐためには、ショッピングサイト利用者と運営者双方での対策が不可欠です。本記事では、ショッピングサイトでのカード情報の取り扱いの現状および最近のカード情報を盗む攻撃手法の特徴と対策方法についてご紹介いたします。セキュリティ対策にご活用ください。

2. 攻撃手法

クレジットカード決済の安全確保のために、カード情報のセキュリティに関する国際的な業界基準「PCI-DSS」が規定されています。クレジット取引セキュリティ対策協議会が策定した指針により、オンラインショッピングサイトの運営者は、PCI-DSS に準拠するセキュリティを備え、審査会社に確認を受けたシステムを運用するか、PCI-DSS に準拠するシステムを持つ他社が提供する決済代行サービスを利用することが求められています。決済代行サービスを利用する場合、ショッピングサイト自身はカード情報を保持せず、カード番号などの情報は決済代行サービスに直接送信します。この方法をカード情報の非保持化と呼びます。カード情報の非保持化により、ショッピングサイトのデータベースやログなどにはカード情報が保存されないため、ショッピングサイトに保存されているカード情報を盗む攻撃方法は成立しにくくなっています。

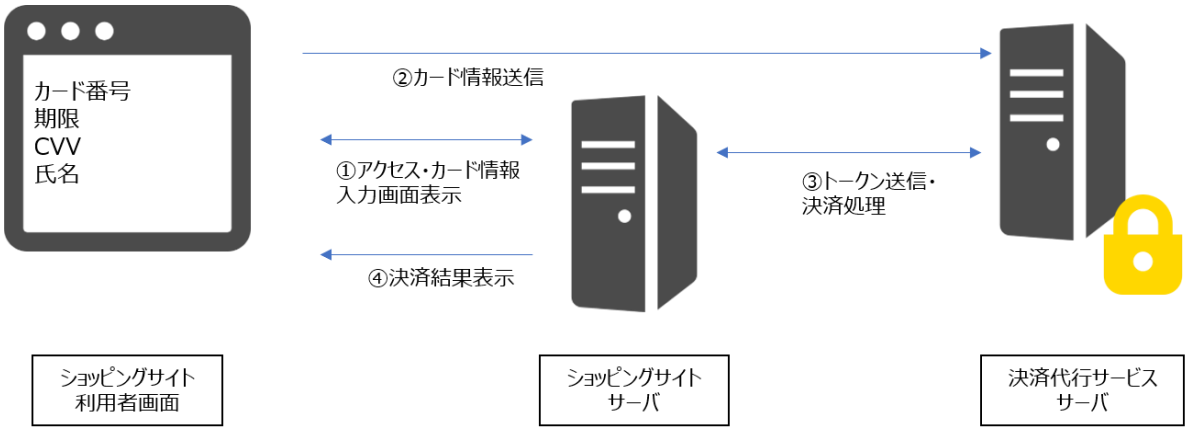
しかし、非保持化を実施しているサイトに対しても、攻撃者は利用者が入力したカード情報を盗むことができ、実際に攻撃が行われています。非保持化の方法と、それに対する攻撃方法を 2 つご説明します。これらの方法によって攻撃者はカー

ド番号、有効期限、名義人氏名、セキュリティコード(CVV)を盗み、不正に使用することができます。

(1) トークン型

トークン型の非保持化方法は、利用者はショッピングサイトのフォームにカード情報を入力し、入力したカード情報はショッピングサイトではなく決済代行サービスのサーバに直接送信される方式です。以下のように、決済代行サービスのサーバからショッピングサイトにカード情報から不可逆的に変換され、カード情報は特定できない「トークン」が送信され、トークンを使って決済処理を行います。

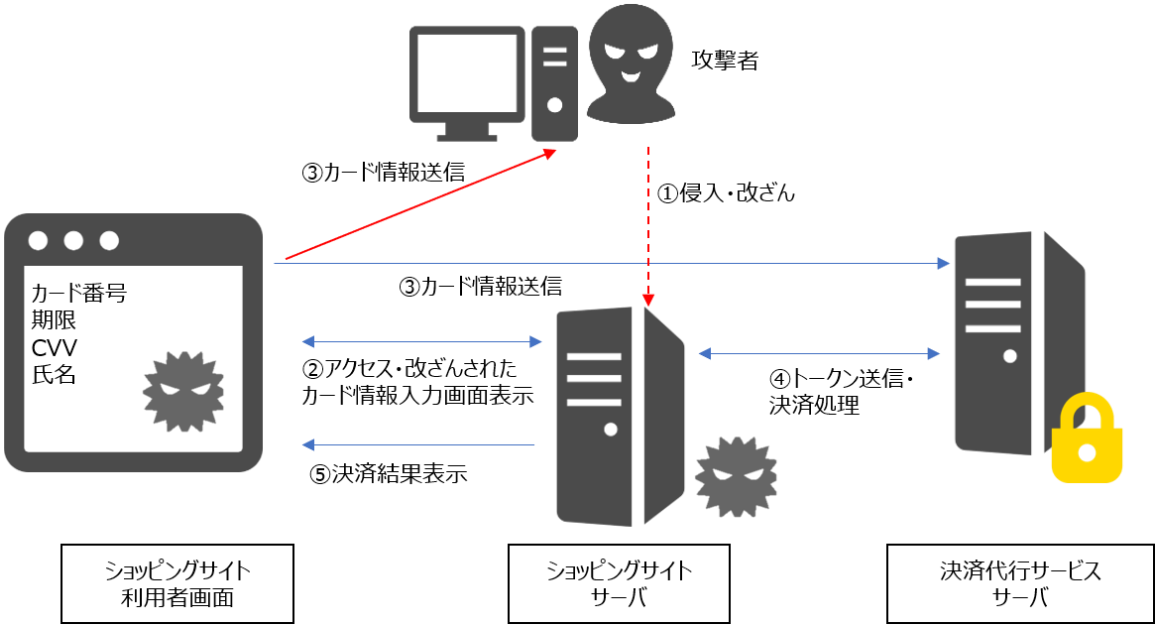
① 利用者がショッピングサイトにアクセスし、注文内容およびカード情報を入力する画面が表示されます。
② 利用者が入力したカード情報は、決済代行サービスに直接送信されます。
③ 決済代行サービスはショッピングサイトにトークンを送信し、ショッピングサイトはトークンを使って決済処理を行います。
④ 決済・購入の結果が利用者に表示されます。



【図 2：トークン型非保持化方法】

この方法に対して、ショッピングサイトのサーバに侵入してカード情報入力フォームの処理を改ざんし、改ざん以後に入力されたカード情報が正規の決済代行サービスに送信されると同時に、攻撃者にも送信されるようになっていた事例があります。利用者での見た目の変化がなく、決済は完了するため、攻撃に気づきにくくなっています。

① 攻撃者はショッピングサイトに侵入し、カード情報送信処理を改ざんします。
② 利用者が改ざんされたショッピングサイトにアクセスし、注文内容およびカード情報を入力する画面が表示されます。
③ 利用者がショッピングサイトに入力したカード情報は、決済代行サービスに送信されると同時に、攻撃者にも送信されます。
④ 決済代行サービスは正常時と同様、ショッピングサイトにトークンを送信し、ショッピングサイトはトークンを使って決済処理を行います。
⑤ 決済・購入の結果が利用者に表示されます。

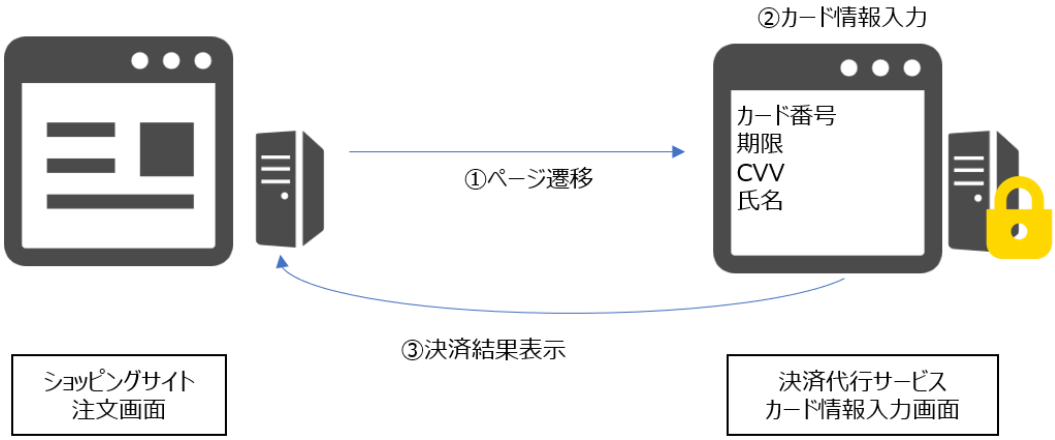


【図 3：トークン型非保持化方法への攻撃】

(2) リダイレクト型

リダイレクト型の非保持化方法は、利用者がショッピングサイトで注文情報を入力した後、決済代行会社のカード情報入力ページに遷移（リダイレクト）し、ショッピングサイト利用者は決済代行会社に直接カード情報を送信する方法です。以下のような手順で、ショッピングサイトは代行会社から決済結果のみを取得します。

① ショッピングサイトから決済代行サービスのカード情報入力画面に遷移します。
② 利用者はカード情報を入力し、入力されたカード情報は決済代行サービスに直接送信されます。
③ ショッピングサイトは決済結果のみを受け取り、結果が利用者に表示されます。

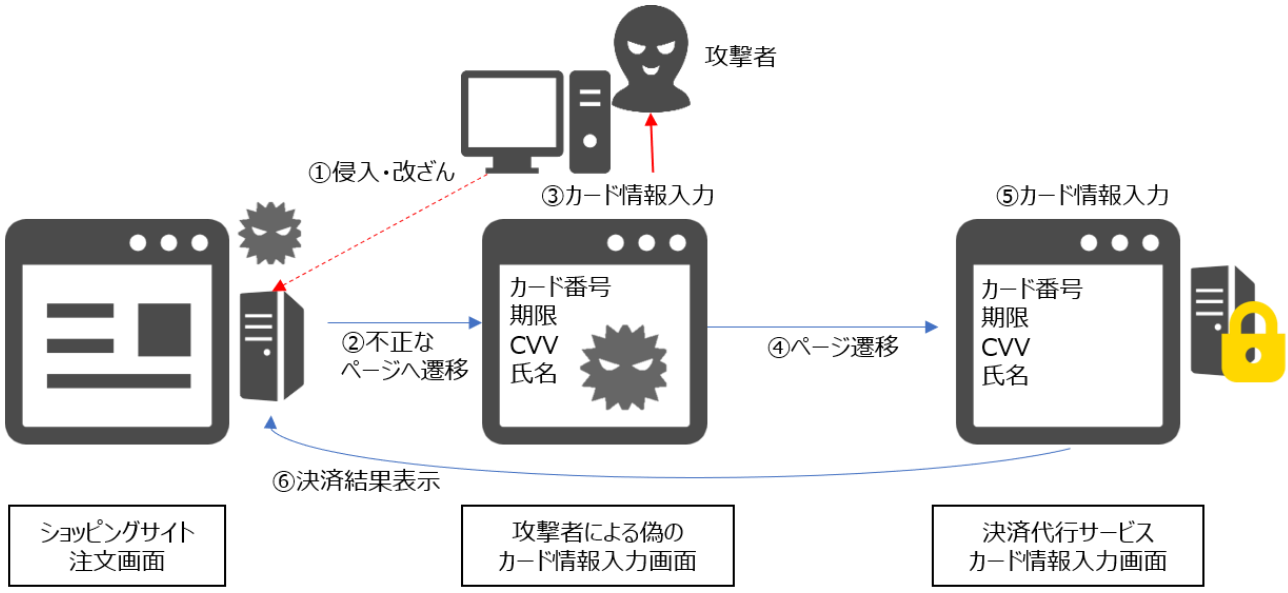


【図 4：リダイレクト型非保持化方法】

この方法に対して、攻撃者は偽のカード情報入力画面を用意し、ショッピングサイトを偽のカード情報入力画面に遷移するよう改ざんすることで、カード情報が盗まれる攻撃が行われた事例があります。利用者が気づかず偽の入力画面に入力されたカード情報は攻撃者に送信されます。その後の動作はさまざまですが、正規の決済代行サービスの入力画面に遷移し、

もう一度カード情報を入力することで、正しく決済されるようになっていた事例があります。

① 攻撃者はショッピングサイトに侵入し、攻撃者が設置した偽のカード情報入力画面に遷移するように改ざんします。
② ショッピングサイトから偽のカード情報入力画面に遷移します。
③ 利用者は偽の入力画面にカード情報を入力し、入力されたカード情報は攻撃者に送信されます。
④ 偽の入力画面から正規の決済代行サービスのカード情報入力画面に遷移します。
⑤ 利用者はカード情報を入力し、入力されたカード情報は決済代行サービスに直接送信されます。
⑥ ショッピングサイトは決済結果を受け取り、結果が利用者に表示されます。



【図 5：リダイレクト型非保持化方法への攻撃】

これら 2 つの攻撃方法に共通する特徴として、一般的なフィッシングのように、精巧な偽のショッピングサイトにアクセスさせるのではなく、正規のショッピングサイトが改ざんされていることが挙げられます。特にトークン型への攻撃では、利用者が見える部分は変化がないため、気づかないうちに攻撃者に情報を送信するようになっています。

3. 対策

ご説明した攻撃に対するショッピングサイト利用者および運営者の対策として以下のような例があります。これらの対策を組み合わせて行うことで、リスクを軽減することができます。

(1) ショッピングサイト利用者の対策

■本人認証サービスの設定

インターネット取引でクレジットカードを使用する際に、あらかじめクレジットカード発行会社の Web サイトで利用者自身が設定したパスワードを決済時に入力する本人認証機能を設定することができます。本人認証機能を設定しておき、決済時にはクレジットカード発行会社の正規の入力画面でのみパスワードを入力するようにすることで、第三者にカードを使用されることを防ぐことができます。また、本人認証にワンタイムパスワードを利用できる場合は、入力情報が流出した場合も悪用できないため、より安全です。

■カード使用履歴の確認

カードの使用履歴を毎月 1 回以上定期的に確認し、不審な使用がないことを確かめます。不審な使用に気づいたらカード会社と警察に連絡し、使用停止や補償などの対応をとることで、支払いを取り消し、さらなる被害拡大を止めることができます。

■使用端末の OS やセキュリティソフトの状態を最新に保つ

端末の OS やセキュリティソフトなどソフトウェアのアップデートやセキュリティパッチを適用することで、マルウェアに感染して画面表示や入力、端末に保存されている情報などから機密情報が流出することを防ぎます。カード情報流出への対策に限らず、セキュリティを向上させる上で重要な対策です。この対策はシステム管理者側にも求められます。

(2) ショッピングサイト運営者の対策

■ソフトウェアのアップデート・パッチ適用・設定確認

脆弱性は日々発見されているため、脆弱性のあるバージョンのソフトウェアを使っていないか定期的に確認し、ソフトウェアのアップデートやセキュリティパッチを適用します。また、初期設定のパスワードを使用している、管理ページがインターネットから参照できるなどの脆弱な設定になっていないかなども確認し、安全な設定状態にしておくことも重要です。

■IPS、WAF などセキュリティ機器の導入・監視

IPS はネットワークやサーバ、エンドポイントへの既知の攻撃パターンに一致する通信の通知や、不正な通信を遮断しシステムを防御します。また、WAF は Web アプリケーションへの攻撃から防御します。Web サイト改ざん検知システムは、Web サイトの内容の不正な改ざんを検知し、復旧します。

このようにセキュリティ機器を導入し、適切に運用することで、サイト改ざん被害につながる不正な通信・攻撃から防御することができます。今回ご紹介した攻撃方法はショッピングサイトのサーバへの侵入によるもので、今後もさまざまな攻撃のために狙われる可能性が高いため、サービス運営者側での対策・監視が特に重要になっています。

4. e-Gate の監視サービスについて

Firewall や IPS をはじめとするセキュリティ機器を導入する場合、それらの機器の運用監視を行うことが重要です。“e-Gate”の 24 時間 365 日有人監視体制のセキュリティ監視サービスをご活用頂きますと、最新の分析システムを活用し精度の高い検知、専任のアナリストによる分析、迅速なセキュリティインシデント対応支援でセキュリティ対策を強化することが可能です。“e-Gate”の MSS の導入をぜひご検討ください。

■総合セキュリティサービス e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた IT 運用のノウハウと、最新のメソッド、次世代 SOC“e-Gate センター”この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”です。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】

https://www.ssk-kan.co.jp/e-gate/

5. 参考情報

- クレジット取引セキュリティ対策協議会 クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画
  https://www.j-credit.or.jp/security/safe/plan.html

- 日本クレジット協会 クレジットカード不正利用被害の集計結果について
  https://www.j-credit.or.jp/information/statistics/

※本資料には弊社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。
リンク先のコンテンツは予告なく、変更、削除される場合があります。
※掲載した会社名、システム名、製品名は一般に各社の登録商標または商標です。

«お問合せ先»
サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp