キャッシュレス セキュリティ レポート 2022

2022年7月31日

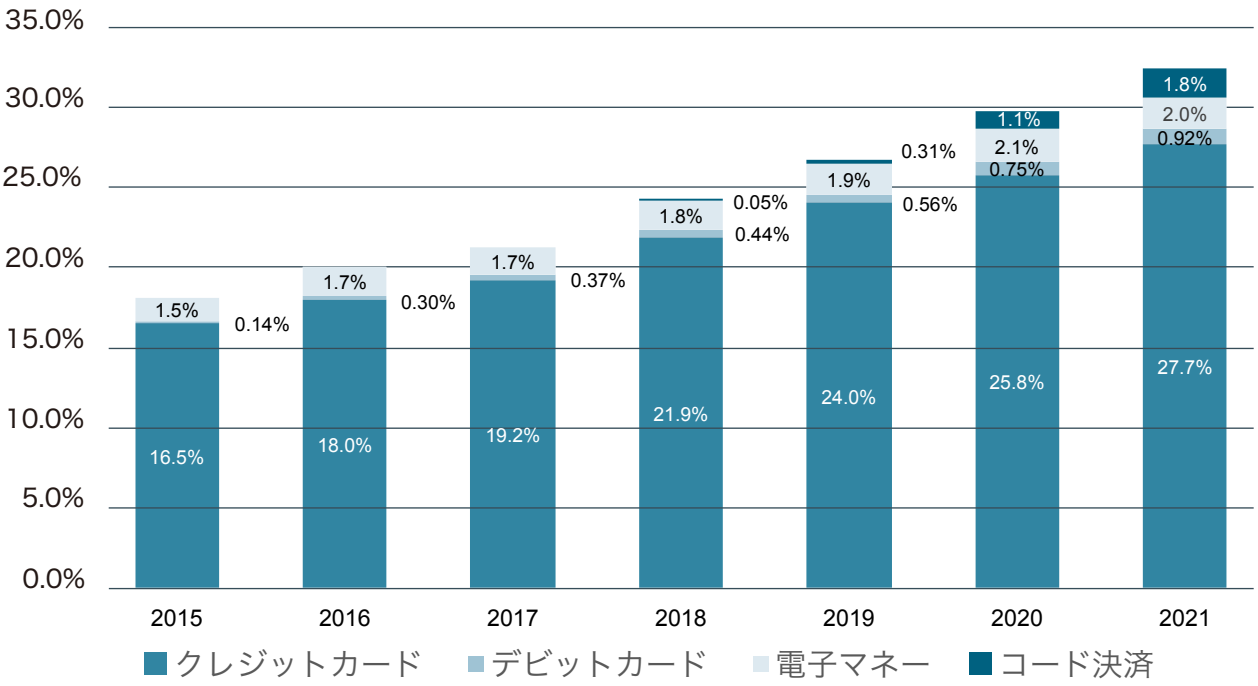
fjconsulting, INC.

はじめに

政府が公表した『キャッシュレス・ビジョン 2018』では、「2025 年に民間消費支出に占めるキャッシュレス決済比率 40%」の目標を掲げている。2022 年 6 月に経済産業省が公表したデータによれば、2021 年のキャッシュレス決済比率は 32.5%にまで迫っており、全年に比べて 2.8%の増加となった。

決済手段別に見るとコード決済が2020年の1.1%から2021年は1.8%と1年間で約60%増加した。

2022年1–3月期には、電子マネーの決済金額が1兆4,185億円に対し、コード決済の決済金額（クレジットカードで支払われた金額を除く）は 1 兆6,353億円と逆転した。クレジットカード決済は2020年の25.8%から2021年は27.7%と着実に増加しており、日本のキャッシュレスの 8 割以上はクレジットカードが占めている。（図）



キャッシュレス決済比率の推移
出所：経済産業省ニュースリリース『2021年のキャッシュレス決済比率を算出しました』（経済産業省商務・サービスグループ キャッシュレス推進室 2022年6月1日）

キャッシュレス比率が着実に増えている要因としては、昨年に引き続き新型コロナウィルス感染拡大による消費行動の変化や店頭でのキャッシュレス決済利用意向の高まりがある。また、2021 年に開催された東京オリンピック・パラリンピックをターゲットにしたクレジットカードの NFC 決済対応もキャッシュレス比率増加を後押ししたといえるだろう。Visa によれば 2021 年 9 月時点での NFC 決済対応カードの発行枚数は 5,700 万枚に達し、対応する決済端末台数も 100 万台を超えたという。コード決済、電子マネーに加えて、クレジットカードも少額決済で使いやすい NFC 対応が進むことで、『キャッシュレス・ビジョン 2018』が掲げるキャッシュレス比率 40%の前倒し達成も視野に入ってきている。

一方で、クレジットカードなどのカード情報を狙った攻撃やキャッシュレス決済の不正利用の被害が激増している。2021年は国内におけるカード情報流出事件数、クレジットカード不正利用金額がそれぞれ調査開始以来過去最悪となった。

キャッシュレス決済の普及と共に、キャッシュレス・セキュリティの重要性は増している。そこでｆｊコンサルティングでは、国内のキャッシュレス不正被害の現状と対策についてとりまとめた年次レポートを発行した。本レポートが安全安心なキャッシュレス社会実現に貢献できれば幸いである。

目次

1．2021年のキャッシュレス不正被害状況

■1-1．2021年のカード情報流出事件

クレジットカードやブランドデビットカードなどのペイメントカード情報（以下、カード情報）流出事件に関しては業界団体や官公庁などによる統計が存在しない。ｆｊコンサルティングでは各社の報道発表や報道など公開情報を2013年から独自に収集し、カード情報流出事件の事件数、事件発生社数、カード情報流出件数を集計している。2021年の事件数、事件発生社数については次の通り定義している。

▶**事件数**：2021年中に発表主体により、カード情報流出事件が公表されたサイトの数を集計（同時に複数サイトからの流出が、流出件数の内訳を明示されない形で公表された場合は「1件」として集計）

▶**事件発生社数**：2021年中に発表主体により、カード情報流出事件が公表された法人数を集計（同時期に同一法人により公表された事件については「1社」として集計）

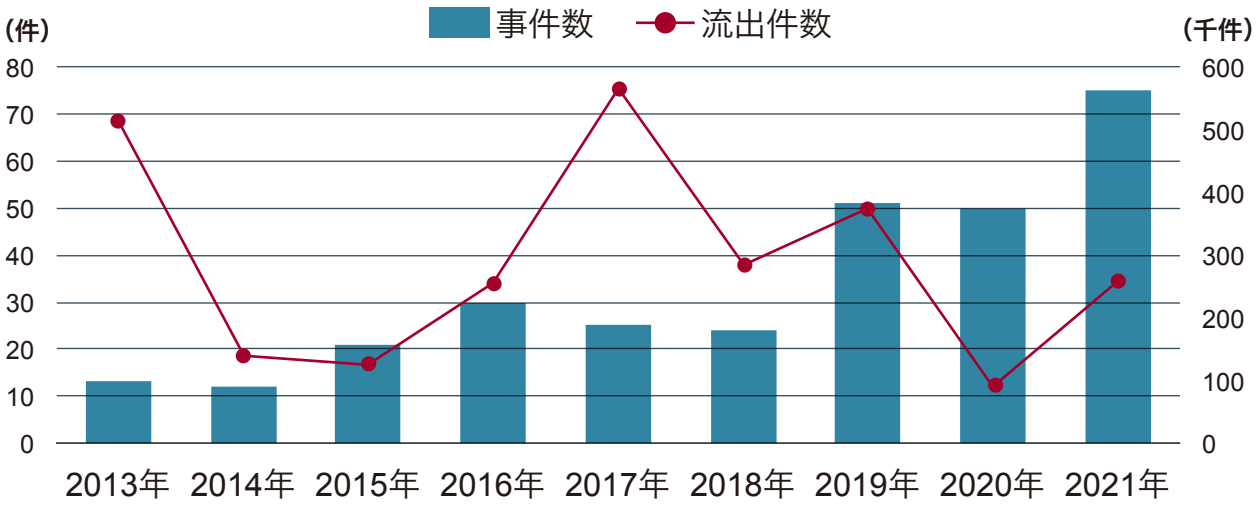
▶**カード情報流出件数**：発表主体により公表された流出カード情報の件数で、クレジットカード、ブランドデビットカード、ブランドプリペイドカードが含まれる。公開された流出カード情報件数のうち最新の情報を正として集計

以下本節では特に断りがない限り、データは当社独自の調査による。

1-1-1. 調査開始以来最多の事件数

2021年1月から12月に公表された事件数は75件と、調査開始（2013年）以来最多となった。カード情報流出件数は256,822件となり、2020年に比べると約3倍となっている。1事件あたりのカード情報流出件数は3,424件となり、2020年の1,793件に比べると2倍近くに増えている。流出規模別の事件数を見ると、カード情報流出件数500未満の事件が26件（36%）、500～999の事件が10件（14%）となっている。合計すると1,000未満の事件が約5割を占めており、全体の傾向としては事件の規模は縮小しつつあるといえるだろう。一方で、2021年はカード情報流出件数が1万を超える大規模流出事件が5件公表されており、これがカード情報流出件数と1事件あたりの平均を押し上げている。

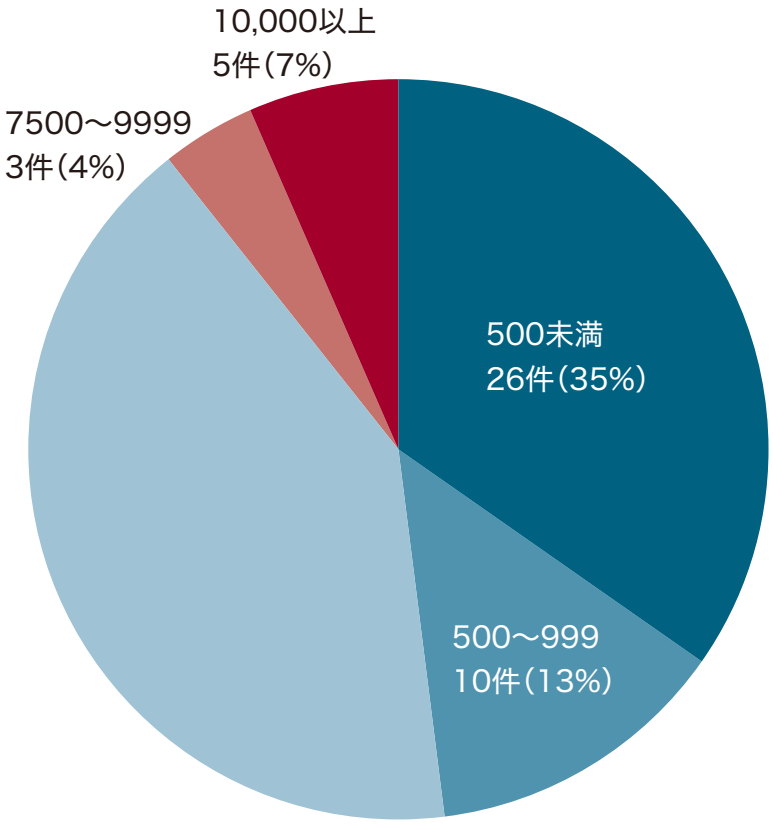
▼図1-1 国内のカード情報流出事件発生状況



【年別の推移】

公表年	2013年	2014年	2015年	2016年	2017年	2018年	2019年	2020年	2021年
事件発生社数	13	12	21	30	25	24	51	47	70
事件数	13	12	21	30	26	24	51	50	75
カード情報流出件数	514,369	138,717	123,527	255,689	564,844	283,374	375,479	89, 628	256,822
1件あたり平均件数	42,864	12,611	7,266	9,132	21,725	12,321	7,362	1,793	3,424

▼図1-2 2021年のカード情報流出件数規模別時件数



流出件数規模	事件	割合
500未満	26	35%
500～999	10	13%
1000～1499	6	8%
1500～1999	4	5%
2000～2499	5	7%
2500～2999	4	5%
3000～3499	3	4%
3500～3999	2	3%
4000～4499	3	4%
4500～4999	3	4%
5000～7499	1	1%
7500～9999	3	4%
10,000以上	5	7%

▼図1－3 カード情報流出件数の多かった事件（2021年）

サイト名(運営企業)	流出件数	流出期間	原因
宅配クリーニングサービス A社	58,813	(開始日不明)～2020/11/16	SQLインジェクション
ドラッグストア B社	25,484	2020/2/7～2021/4/22	オンラインスキミング(可能性高)
寝具販売 C社	19,197	2019/12/3～2020/12/7	オンラインスキミング(可能性高)
キャラクターグッズ販売 D社	17,828	2020/6/8～2021/6/30	オンラインスキミング
輸入食品販売 E社	10,219	2019/6/24～2020/7/28	オンラインスキミング(可能性高)
女性向けアパレル販売サイト F社	9,656	2020/2/24～2021/4/20	オンラインスキミング(可能性高)
健康食品販売 G社	9,515	2020/11/6～2021/2/24	オンラインスキミング(可能性高)
健康食品販売 H社	8,644	2019/10/4～2020/10/8	オンラインスキミング(可能性高)
女性向けファッションモール I社	6,485	2020/4/27～2021/3/24	オンラインスキミング(可能性高)
雑誌公式オンラインショップ J社	4,544	2020/1/9～2020/5/29	オンラインスキミング(可能性高)

1-1-2. 手口は「オンラインスキミング」が主流

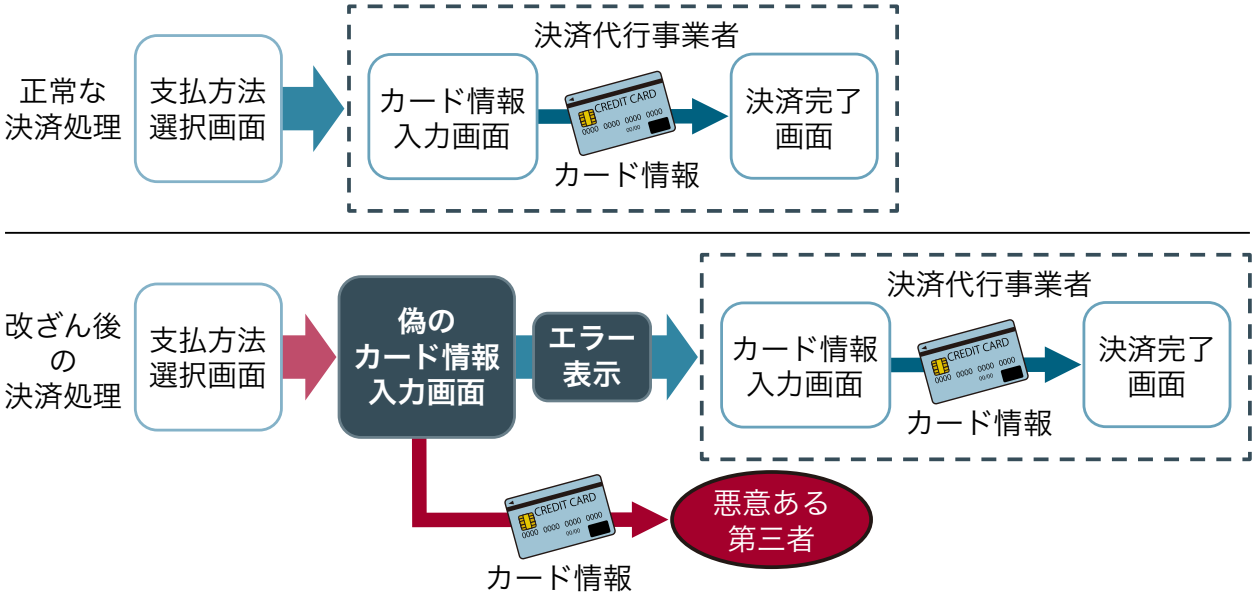
カード情報窃取の手口としては、2018年頃から、ECサイトを改ざんし、消費者が入力したカード情報を直接消費者のブラウザから窃取する手法が増えている。対面加盟店でカードを読み取るときに不正な装置を用いて券面の磁気ストライプ情報を盗み取る手法を「スキミング」と言うが、そのオンライン版ということで「オンラインスキミング」と呼ばれる。

具体的には、ECサイトの決済ページへのリンクを改ざんして偽の決済ページを挿入したり、決済ページに不正なJavaScriptを挿入することで、カード情報を正規の決済代行事業者以外に、第三者にも送信する。オンラインスキミングでは、ウェブブラウザに表示された決済ページに消費者が入力した情報がそのまま流出するため、ほとんどの場合セキュリティコードも一緒に流出する。

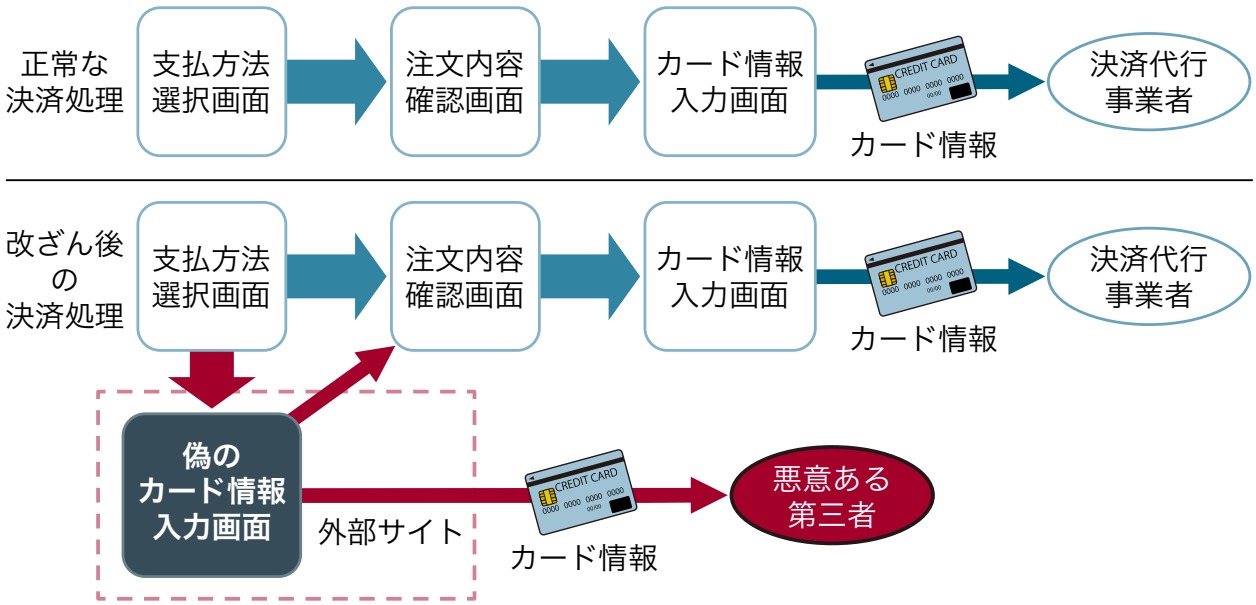
図1-4の例は、クレジットカード情報を入力するページが決済代行事業者のサイトに設置されている「リンク型決済」でオンラインスキミングが行われている。正常な決済処理（上段）であれば、消費者が支払い方法を選択した後、決済代行事業者のサイトに設置されたカード情報入力画面が表示され、カード情報を入力して決済を完了する。改ざんされたサイト（下段）では、支払方法選択画面からサイト内に設置された偽のカード情報入力画面が呼び出される。ここでカード情報を入力すると、悪意ある第三者にカード情報が窃取されるが、同時に「通信エラー」などのエラー画面が表示される。エラー画面で「次へ」等のボタンをクリックすると、決済代行事業者の正規のカード情報入力画面が表示される。そのまま手続きを進めると決済が正常に完了する。

図1-5の例は、ECサイト内にある決済画面にJava

▼図1-4　オンラインスキミングの例（リンク型決済）



▼図1-5　オンラインスキミングの例（JavaScript型決済）



Scriptを埋め込むことで決済代行事業者にカード情報を送信している「JavaScript型決済」でオンラインスキミングが行われている。正常な決済処理（上段）であれば、支払方法を選択後に注文内容を確認し、カード情報を入力するという順序になるが、改ざんされたサイト（下段）では支払方法選択画面から一度外部にある偽のカード情報入力画面が呼び出され、ここで入力したカード情報が第三者に窃取される。その後、正常な注文プロセスに戻り再度カード情報の入力が求められる。ここで消費者が気づかずカード情報を再度入力すると決済が完了して注文が正常に完了する。二度カード情報を入力することで異常に気づいたとしても、その時には既にカード情報は流出した後となる。

JavaScript型決済の決済画面そのものに不正なコードを埋め込む手法も存在する。2020年に報告された米国のtupperware.com（家庭用品販売サイト）のケースでは、決済画面に埋め込まれた画像に不正なJavaScriptコードを埋め込み、ユーザーのブラウザ上で実行して偽のカード情報入力フォームをiframeで表示する「ステガノグラフィ攻撃」による改ざんが行われた（図1-6）。決済画面のソースコードを改ざんして攻撃コードを書きこんだり、外部JavaScriptの攻撃コードを読み込ませる手法に比べ、より巧妙に隠蔽され分かりにくくなっている。

では実際に、国内のカード情報流出事件のうちオンラインスキミングがどのくらいの割合を占めているのだろうか。事件公表時の公式発表の多くは、流出の原因として「第三者によるペイメントモジュールの改ざん」等の表現をとっており、オンラインスキミングであるとはっきり分かるような書き方をしているものは多くない。そのためｆｊコンサルティングでは、2021年に発生した75件のカード情報流出事件の原因がオンラインスキミングである可能性を公表内容から以下の観点で推定し、その割合を集計した。

①オンラインスキミング：公式発表で「決済画面が2枚あった」「画面に入力したカード情報が第三者に送信された」等のオンラインスキミングであることがわかる記載がある

②オンラインスキミングの可能性高：公式発表でオンラインスキミングであることがわかる記載はないが、セキュリティコードが流出している

③オンラインスキミングの可能性低：公式発表で原因が明確にわかる記載がないが、セキュリティコードが流出していない

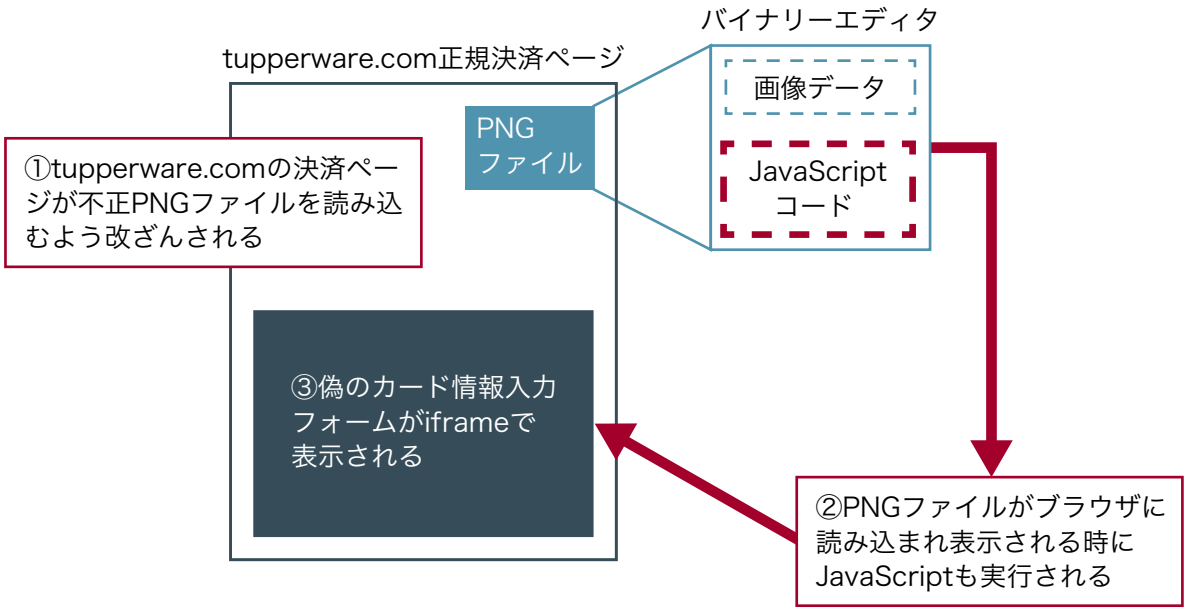
④オンラインスキミングではない：公式発表でSQLインジェクション等、オンラインスキミング以外の原因が明記されている

事件数でみると、2021年に発生したカード情報流出事件75件のうち、オンラインスキミングが20件（27%）、オンラインスキミングの可能性が高いものが51件（68%）となり、合計すると71件、9割以上がオンラインスキミングであると推測される（図1-7）。なお、ここで「オンラインスキミングではない」としている2件は、公式発表で原因はSQLインジェクションであることが明記された事件、「オンラインスキミングの可能性が低い」とした2件は原因が特定できる記載は無いがセキュリティコードは流出していない事件である。カード情報流出件数ベースでもオンラインスキミングによる被害は8割近くを占めると推測される。

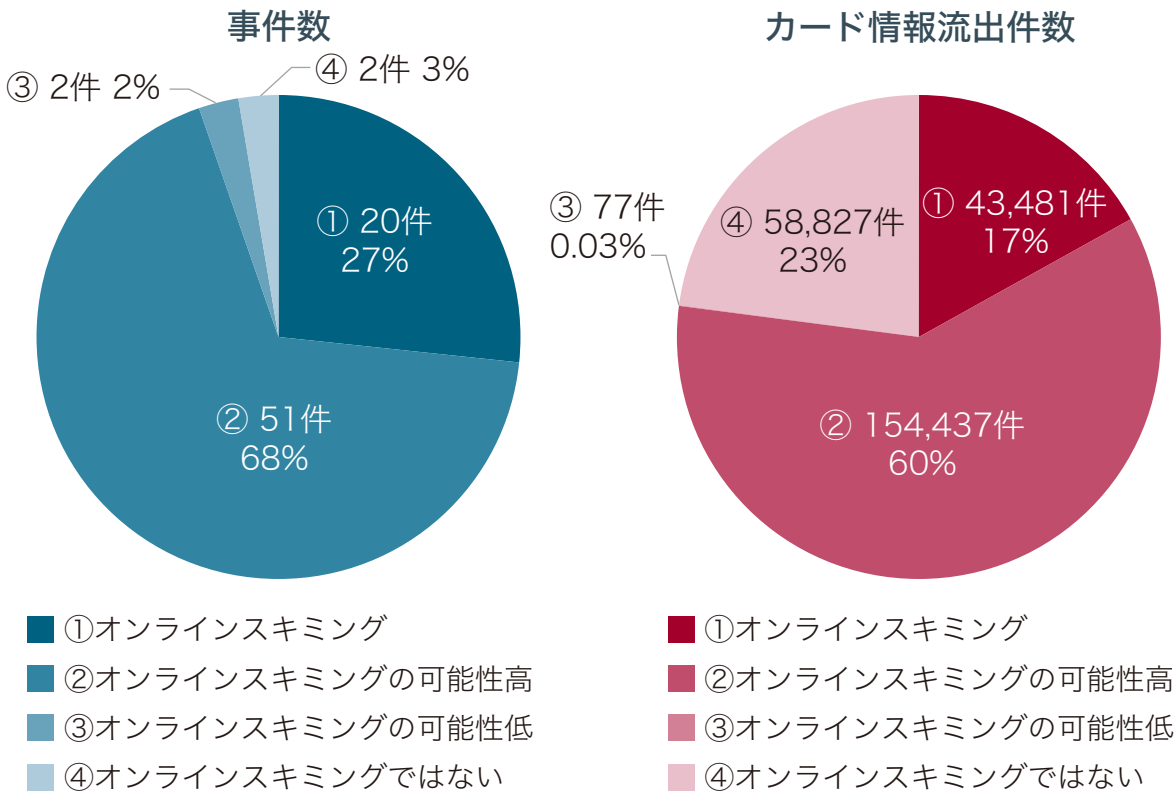
1-1-3. 具体的な決済画面やコードの改ざんの原因

オンラインスキミングを行うための決済画面の改ざんやコードの原因をいくつか挙げる。

▼図1-6　ステガノグラフィ攻撃によるオンラインスキミング



▼図1-7　2021年のカード情報流出事件に占めるオンラインスキミングの割合



1）管理画面への不正アクセス

EC-CUBEなど多くのECショップが使用するECプラットフォーム構築パッケージソフトウェアでは、管理画面のURLや管理者アカウントの初期設定値が広く知られている。これらを変更しないまま使用しており、かつ管理画面アクセスの接続元IPアドレス制限や多要素認証などによるアクセス制限を行っていない場合、よく使用されるパスワードを総当たりで入力する「パスワードリスト攻撃」により認証が突破され、管理画面に不正アクセスされる。またEC-CUBEの提供元を騙るフィッシングメールにより、偽の管理画面に誘導して管理者のIDとパスワードを入力させ窃取する手口も確認されている。管理者画面にいったん不正ログインされると、サイトの改ざんは容易である。

2）クロスサイトスクリプティング（XSS）脆弱性の悪用

2021年4月、トレンドマイクロからECサイトのXSS脆弱性を悪用した攻撃手法である「Water Pamola」が報告されている。2021年7月には、JPCERT/CCにより同様の攻撃を確認したとして、手法が公開されている（図1-8）。

①攻撃者は、注文フォームから不正なスクリプトを含んだ文字列を入力し、購入処理を行う。

②ECサイトの購入処理にXSS脆弱性が存在する場合は、管理者がECサイトの管理画面を閲覧することで不正なスクリプトが実行される。

③管理者ログイン情報の窃取が行われる。

④盗んだログイン情報で管理者ログインした犯人は、簡易WebShellを設置し、不正ファイル、不正JavaScript、多機能なWebShellなどの設置などを行う。

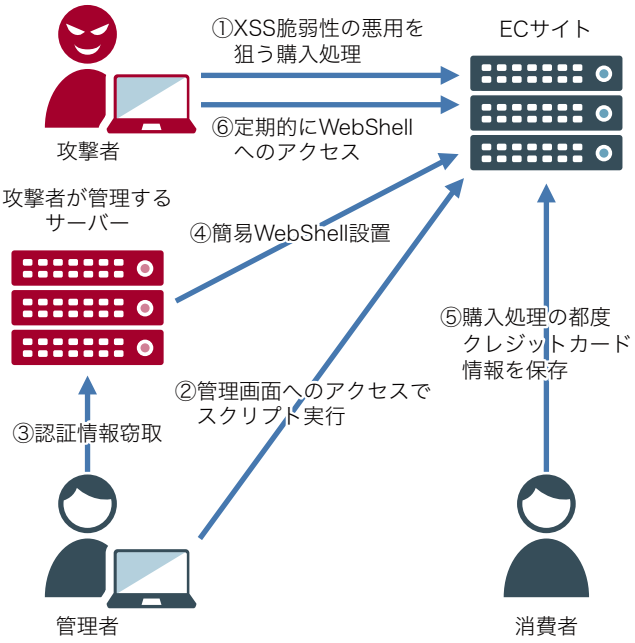
⑤不正なスクリプトが設置された後は、消費者が購入処理時にクレジットカード情報を送信する都度不正JavaScriptが実行される。カード情報は正規の決済代行事業者等に送信されると同時にECサイト上に設置された不正ファイルにも保存される。

⑥犯人は定期的にWebShellにアクセスし、サーバー上の不正ファイルをダウンロードしてカード情報を窃取する。

いったん不正なスクリプトが設置されると、消費者によるカード情報の「送信」ボタンのクリックをトリガーとして、入力された情報がECサイト内に作成した情報保存ファイルに保存される。このファイルを犯人がサーバーに定期的にアクセスして取得することで、ログイン情報やカード情報を不正に窃取していたと推測されている。

また、JPCERT/CCが確認した手法では、攻撃時にデータベース操作ツールの「Adminer」が設置されていたという。Adminerはデータベースの中身をGUI環境で確認するツールである。攻撃者は、このツールを使用して、データベース内の個人情報などの情報窃取も行っていたと推測される。

▼図1-8 オンラインスキミング攻撃手法の例（クロスサイトスクリプティング脆弱性を悪用した攻撃）
出所：『ECサイトのクロスサイトスクリプティング脆弱性を悪用した攻撃』
（JPCERT/CC Eyes 2021年7月6日）を元に作成



設置されたファイル	内容
WebShell	・多機能なWebShell（中国語をベースとしており、ツール名は不明）
データベース操作ツール	・Adminer version 4.2.4
情報窃取JavaScript	・ボタンをクリックした際にクレジットカード情報などを送信する ・ログインページや決済ページでロードされる
情報保存JavaScript	・“情報窃取JavaScript”からの情報送信先 ・受信したデータを“情報保存ファイル”に保存する
情報保存ファイル	・クレジットカード番号、有効年月、セキュリティコード、メールアドレス、パスワードなどが保存されている
簡易WebShell	・アップロードされたPHPファイルを実行する

3）サードパーティのJavaScriptを改ざん

広告配信サービスなど、ECサイトに読み込んでいる外部サービスの提供元で改ざんが行われた結果、カード情報が流出する手口である。2019年にフランスのオンライン広告配信サービス「Adverline」の広告配信用ライブラリが改ざんされスキミングコードが注入された事件では、当該コードをサイトに読み込んで広告を表示していた277店のECサイトでカード情報が同時に流出する状態となっていた（図1-9）。複数の加盟店が利用するサービスが攻撃を受けることで、加盟店のサイトが直接攻撃されていないにもかかわらず、カード情報が流出するサプライチェーン攻撃の一種である。サプライチェーン攻撃については、この後にも事例を紹介する。

2018年施行の改正割賦販売法により、加盟店にはカード情報を自社システムに保存、処理、通過しない「非保持化」もしくはPCI DSS準拠が義務付けられた。2021年時点ではほとんどのEC加盟店は「非保持化」を選択しており、自社サーバー内にはカード情報を保存していないと考えられる。実際に、一度に大量のカード情報が流出する事件は減少しているが、非保持化対策済みの加盟店でオンラインスキミングの被害が増え続けている。

非保持化には、大型の事件を防ぐ一定の効果があったが、EC加盟店には追加のセキュリティ対策が必要である。非保持化済みの加盟店であっても、従業員に対するセキュリティ教育や脆弱性対策、ウイルス対策、管理者権限の管理、デバイス管理等の基本的なセキュリティ対策が求められる。

1-1-4. EC-CUBEは3系へと被害広がる

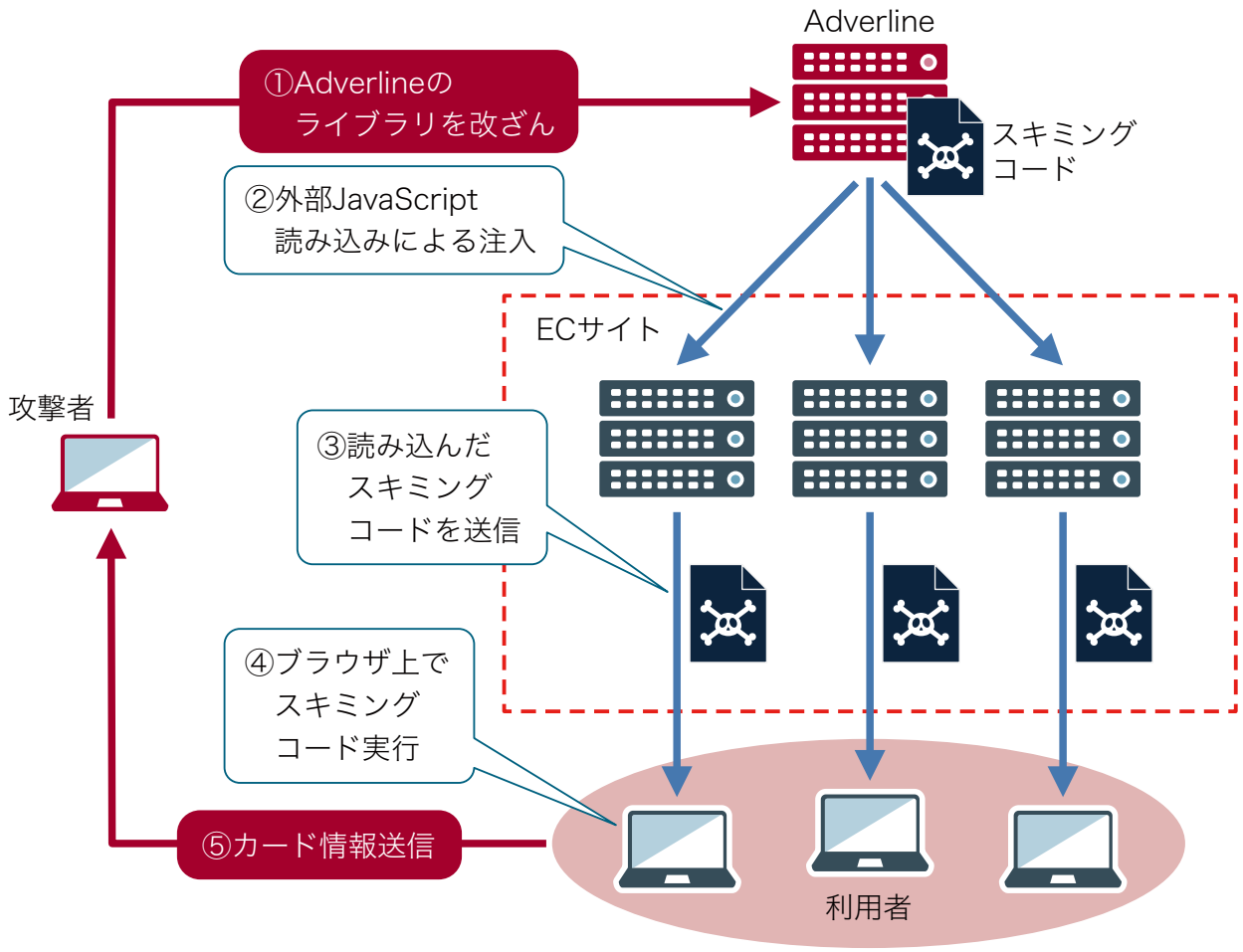
オープンソースのECプラットフォームとして国内でNo.1のシェアを占めるEC-CUBEは、利用する企業が多く、また被害も多発している。2019年12月には経済産業省から注意喚起の文書が公表されている。

その文書によれば、2019年時点でEC-CUBEを利用しているECサイトから14万件のカード情報が流出しているとされていた。セキュリティ情報サイト「フォックスエスタ」では、独自にカード情報流出を公表したサイトを調査し、使用されているプラットフォームを推定している。同サイトの調査結果をもとに2021年に発生したカード情報流出事件のうちEC-CUBEが占める割合を推計したところ、事件数で59件（79%）、流出件数で155,364件（60%）にのぼる。中にはEC-CUBEのプラグインやWordpressなど別のCMSが原因となっている可能性も否定できないものの、EC-CUBEを利用するECサイトでの被害は依然拡大し続けていることがうかがえる。

2019年12月の経産省の注意喚起と同時期に株式会社イーシーキューブから公表された「お知らせ」では、特に2系を利用するユーザーに向けて、インストール時の不備、既知の脆弱性への対応不備、管理画面のアクセス制御不備などにより攻撃を受けることが多いとしている。さらに、2021年5月から6月にかけ、EC-CUBE　3系、4系で相次いで管理画面にクロスサイトスクリプティング（XSS）脆弱性があることが公表された。

実際に、EC-CUBE 3系の被害が増え始めている。2020年に発生したカード情報流出事件で、EC-CUBEを利用しているサイト（32件）のうち、バージョンが推定できるものは全てEC-CUBE2系（29件）であった。2021年にはEC-CUBE利用サイトの流出事件数（59件）のおよそ4分の1（15件）をEC-CUBE3系が占めるようになっており、実際にXSS脆弱性による攻

▼図1-9.外部サイトの広告配信用JavaScript改ざんにより複数の加盟店サイトを攻撃する手口



撃を受けたことを公表しているサイトもある。今後は3系、4系の被害も増えることが予想される。オープンソースソフトウェアを利用する際は、自らの責任でセキュリティパッチを迅速に適用し、既知の脆弱性に対応する必要がある。

1-1-5.　サプライチェーン攻撃による複数加盟店の被害が発生

加盟店そのものを攻撃するのではなく、加盟店が利用するプラットフォームやサービスを攻撃することで、一度に複数の加盟店から情報を窃取する「サプライチェーン攻撃」が国内でも発生している。

1）ECシステム提供会社Q社

2021年9月、ECシステム提供会社Q社の運営するECプラットフォームに対し、外部から不正アクセスが発生し、個人情報流出の痕跡があることが公表された。当該プラットフォームは、店頭のシステムとECサイトを連携するオムニチャネルを実現するツール群で、POSシステムとも連携する。サーバーおよびシステムはQ社が管理するSaaS型サービスである。Q社の公式発表によれば、当該プラットフォームの2台のサーバーに不正アクセスされ、個人情報が流出した可能性を示す痕跡を確認したとしている。

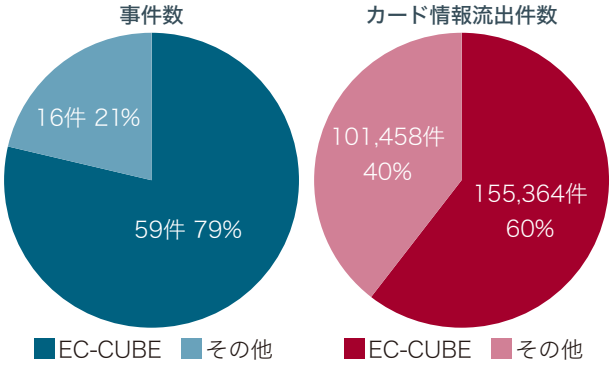
2022年4月時点で当該プラットフォームを利用しておりカード情報流出を公表しているのは以下の６社（6サイト）で、計6,141件のカード情報が流出している。カード情報以外に顧客の氏名、メールアドレスなどの個人情報が全てのサイトで合わせて流出している。これ以外に、カード情報は流出していないが個人情報が流出したことを公表しているのが、５社（5サイト）存在する。

6社の発表内容を見ると、園芸・農業資材販売M社とネットスーパーL社が原因について少し踏み込んだ発表をしている。

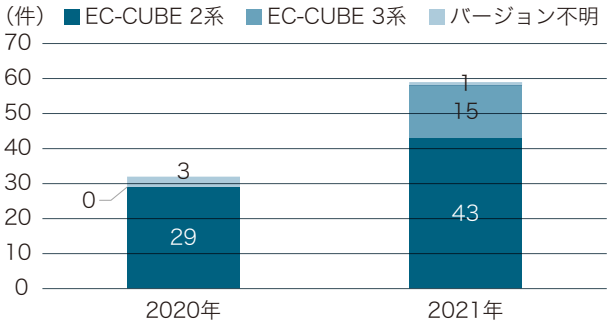
＜園芸・農業資材販売M社＞
・当該プラットフォームのXSS脆弱性をついたことによる第三者の不正アクセスにより、不正ファイルの設置およびペイメントアプリケーションの改ざんが行われた。

＜ネットスーパーL社＞
・当該サイトの脆弱性を悪用するための不正な注文情報が登録され、それを足掛かりとして不正アクセスが発生してデータベース内に不正侵入された。
・攻撃者は断続的に当該サイトのデータベースにアクセスしていた。
・あわせてペイメントアプリケーションの改ざんが行われ、改ざんからサイト停止までの間に決済されたカード情報が漏えい可能性の対象となっている。

▼図1-10. 2021年のカード情報流出事件に占めるEC-CUBEの割合
出所：『フォックスエスタ』調査結果を元に作成



▼図1-11. カード情報流出事件サイトで使用されていたEC-CUBEのバージョン
出所：『フォックスエスタ』調査結果を元に作成



また、ホームセンターO社と持ち帰り寿司予約サイトP社が「第三者の不正アクセスを受け悪性ファイルが設置された」という記載をしている。

以上より、当該プラットフォームを利用するサイトへの一連の攻撃では、前述のJPCERT/CCが公開したXSS脆弱性を悪用した手法と同様の手口で、各サイトの管理画面への侵入、不正ファイルの設置による個人情報やカード情報の窃取、データベースに保存された個人情報の窃取が行われたと推測される。

攻撃を受けたサイトではEC-CUBE 3系が使用されていたと推測される。前述の通り、このバージョンには、まさに攻撃を受けたXSS脆弱性が存在しており、株式会社イーシーキューブからは3系のXSS脆弱性情報と修正パッチが2021年6月22日に公開されている。一方で、被害にあったサイトではカード情報が流出していた期間を一様に8月19日までとしている。また、当該プラットフォームを利用するECサイトからの問い合わせにより、Q社がカード情報流出の可能性を認識したとして公表したのは9月に入ってからである。

仮に攻撃されたのがEC-CUBE 3系のXSS脆弱性だったとすると、攻撃が開始されたのは2021年3月～4月頃と脆弱性情報の公開前であり、未然に防ぐことは困難だった可能性が高い。しかし、EC-CUBEによる脆弱性の公表後、Q社がEC-CUBEへの最新のパッチ適用などの対応を迅速に行っていれば、6月の時点でカード情報の流出被害を減らせた可能性はある。

本件はECシステム提供会社のセキュリティ脆弱性を狙われて多数の加盟店に被害が及んだサプライチェーン攻撃であり、複数のカード加盟店に決済サービスを提供するサービスプロバイダーのセキュリティ対策が重要であることがあらためて浮き彫りとなった。2021年4月施行の改正割賦販売法では、ECシステム提供業者に対してもクレジットカード情報保護対策を義務付けており、Q社のような事業者にはPCI DSS準拠が求められている。

2）PCI DSS準拠済みの決済代行事業者R社

2022年1月には、決済代行事業者のR社が、第三者の不正アクセスを受けてカード情報が流出した可能性を公表した。国内の決済代行事業者にはPCI DSS準拠が義務付けられており、R社もPCI DSS準拠していた。PCI DSS準拠済みの決済代行事業者からカード情報が流出したのは、国内では2017年3月にも発生したS社以来となる。

2月に公表された情報によれば、同社の運用するトークン方式クレジットカード決済情報データベース（以下トークン方式DB）から、カード番号、有効期限、セキュリティコードを含むカード情報が最大で460,395件流出した。さらに、決済情報データベースからは、格納されたクレジットカード決済情報2,415,750件のうち434件のカード番号と有効期限が流出したという。トークン方式DBは同社の運営する複数の決済サービスで使用されている。

直接的な原因は、①一部アプリケーションへのSQLインジェクション、②社内用決済管理システムへの不正ログインおよびカード番号の参照、③バックドアの設置であるという。

国内のEC加盟店の大多数はクレジットカード決済については決済代行事業者のシステムを利用しているため、決済代行事業者が攻撃を受けカード情報が流出した場合、その影響範囲は複数の加盟店に及ぶ。2022年7月時点で、R社への攻撃を理由としてカード情報流出のお詫びを発表している加盟店は90社以上に上っている。2022年6月、R社は経済産業省より行政処分（改善命令）を受けた。

▼図1-12. Q社ECプラットフォームへの攻撃によるカード情報流出事件

サイト名（運営企業）	流出件数	流出期間
ネットスーパー K社	3,101	2021/4/26～2021/8/19
ネットスーパー L社	322	2021/3/25～2021/8/19
園芸・農業資材販売 M社	349	2021/4/7～2021/8/19
持ち帰り寿司予約サイト　N社	1,607	2021/3/26～2021/8/19
ホームセンター O社	110	2021/3/26～2021/8/19
持ち帰り寿司予約サイト　P社	652	2021/3/26～2021/8/19

■1-2. クレジットカード不正利用被害の推移

クレジットカード不正利用については、日本クレジット協会が四半期毎に「クレジット不正利用被害の発生状況」として不正利用被害金額の統計を発表している。

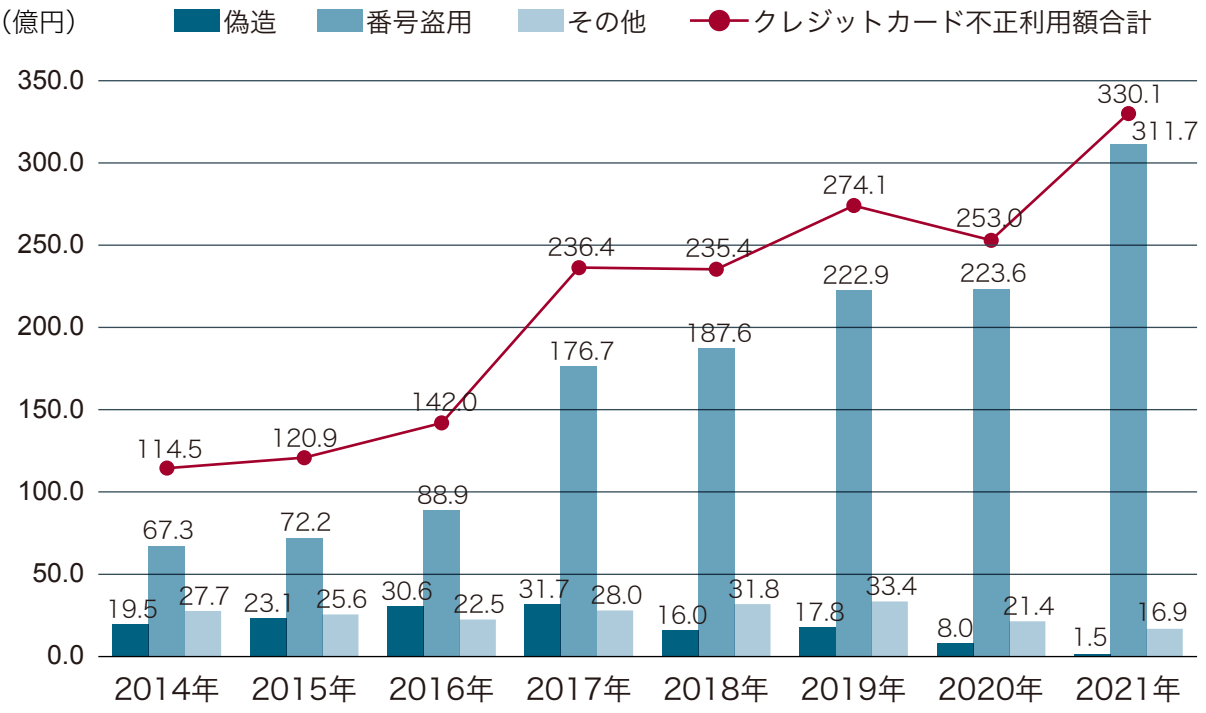
1-2-1. 調査開始以来最悪の不正利用被害

ここ数年、年間250億円前後で推移していたクレジットカード不正利用被害は、2021年に入り再び増加に転じている。2021年の被害額はでは330.1億円と、日本クレジット協会による調査が開始された1997年以降最大の被害額だった2000年（308.7億円）を超え過去最大となった。

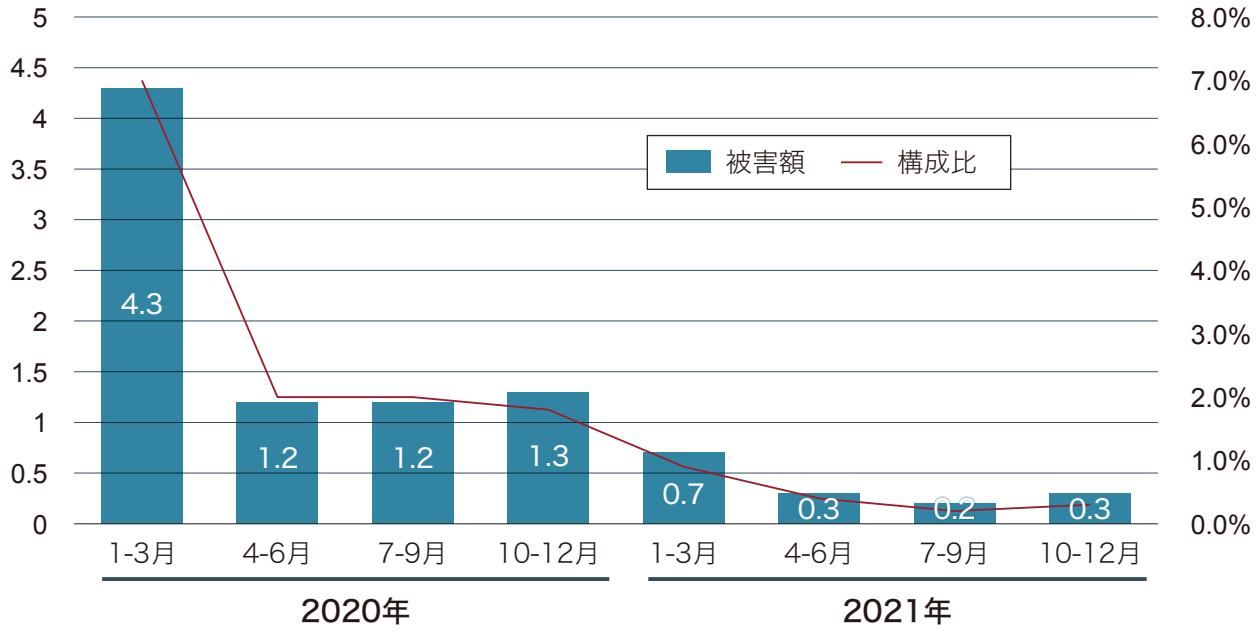
その内訳をみると、まず、クレジットカード偽造被害は1.5億円と全体の0.5%にまで減少している。その理由は2018年施行改正割賦販売法の実務上の指針である『クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画』（以下『実行計画』）で2020年3月を期限として義務付けられた対面加盟店のIC対応がほぼ完了していることが挙げられる。実際に2020年、2021年の四半期毎の偽造カード被害は、2020年3月の期限を超えて急減した後も金額、構成比とも減り続けており、対策の効果が如実に表れている。

一方で、クレジットカード番号盗用による被害は増え続けている。2021年第2四半期以降は被害額の95%を占めるに至っており、クレジットカード不正利用の主戦場は完全にオンラインに移ったといえる。2020年、2021年は新型コロナウィルス感染拡大に伴い、物販、デジタルコンテンツ等分野でEC市場が拡大していることもこの傾向を後押ししていると考えられる。

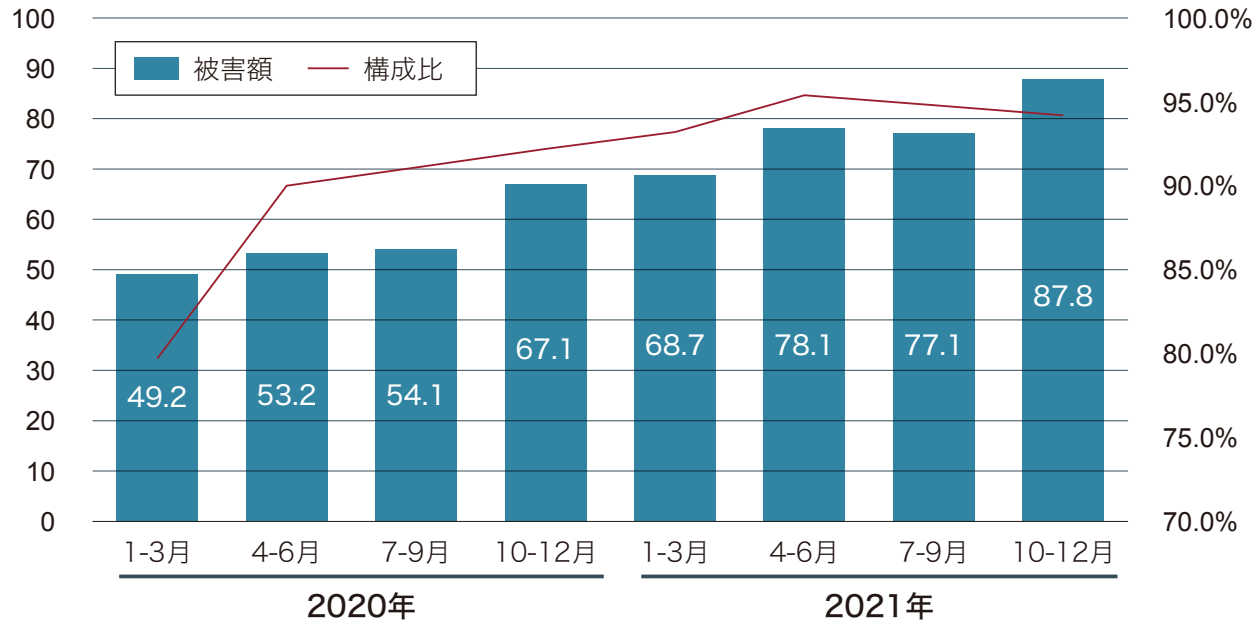
▼図1-13. クレジットカード不正利用被害の推移
出所：『クレジットカード不正利用被害の発生状況』（一般社団法人日本クレジット協会 2022年3月）



▼図1-14. クレジットカード偽造被害の推移
出所：『クレジットカード不正利用被害の発生状況』（一般社団法人日本クレジット協会 2022年3月）



▼図1-15. クレジットカード番号盗用の推移
出所：『クレジットカード不正利用被害の発生状況』（一般社団法人日本クレジット協会 2022年3月）



1-2-2. 具体的な番号盗用の手口

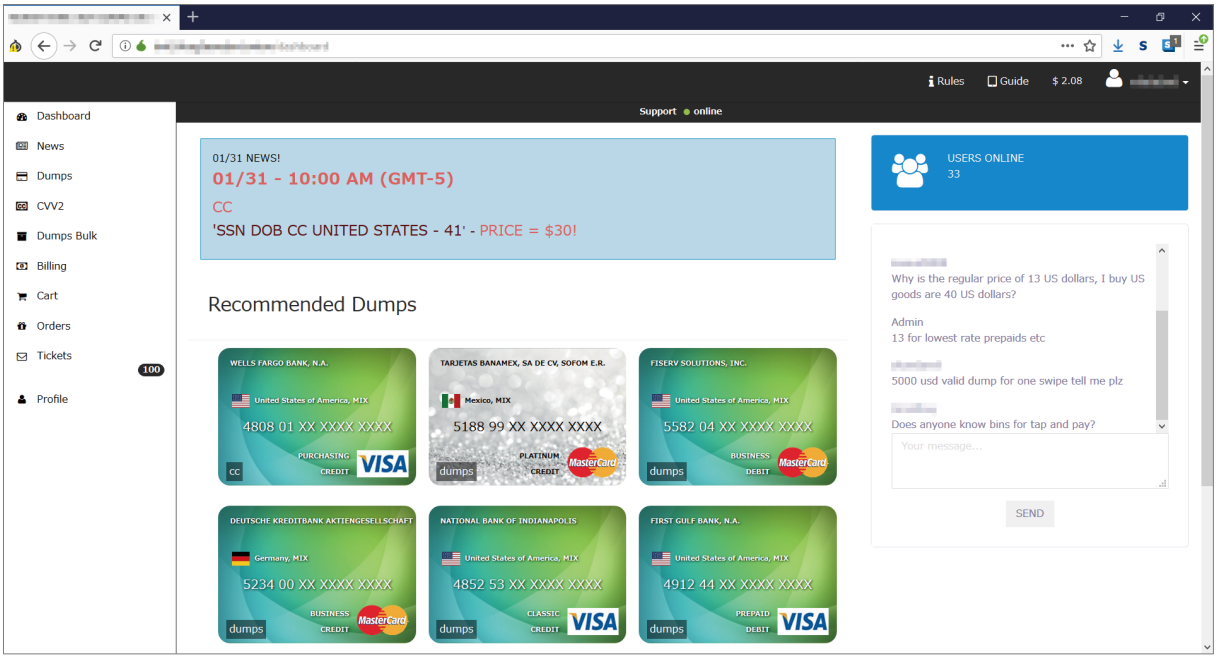
ECサイトで他人のクレジットカード番号を利用して不正な決済を行う手口を挙げる。

1）流出したクレジットカード情報の利用

最もシンプルなのは、ECサイト等からクレジットカード情報を窃取した犯人が、盗んだ番号を不正に利用するケースだ。オンラインスキミングにより流出したカード番号は、カード番号、有効期限、セキュリティコードがセットになっているので、そのまま決済に使用できる。

また、盗んだ番号を自分で使わず、まとめて販売するケースもある。カード番号の売買はダークウェブ（アクセスするために特定のソフトウェアや設定が必要で、通常のインターネットからはアクセスできないウェブサイト）で行われると言われている。不正利用犯は購入したカード番号を利用して不正利用を行う、一種のエコシステムが成立している。

▼図1-16. カード情報が売買されるダークウェブのサイトの一例



2）クレジットマスターによるカード番号生成

クレジットマスターとは、クレジットカード番号の規則性を利用して、有効なクレジットカード番号を割り出す手口である。カード情報を入力するシステム向けのテストデータ生成を目的に、大量のカード番号を生成するウェブサービスやプログラムが多数公開されており、これらが悪用されることがある。有効期限やセキュリティコードについてはランダムに入力するか、後述のリバースブルートフォースアタックを併用することで特定することが可能である。

3）リバースブルートフォースアタック

クレジットマスターで生成する、あるいはダークウェブで購入するなどして入手した、大量のカード番号を利用するために必要な、正しいセキュリティコードを入力する方法として用いられる。カード情報入力画面で、3桁もしくは4桁の数字であるセキュリティコードを固定し、カード番号を入れ替えて決済を試行する。

セキュリティコードは3桁もしくは4桁の数字なので、1,000回～10,000回の試行により正しい番号を突き止めることができる。そのため、『実行計画』およびその後継となる『クレジットカード・セキュリティガイドライン』では、クレジットカード発行会社に対し、連続して大量のオーソリゼーションが発生した場合はそれを検知して取引を不成立とする対策が必要であるとしており、ほとんどの場合一定回数以上のセキュリティコードの間違いは不正利用とみなしてロックされる。だが、リバースブルートフォースアタックの場合、カード番号の方は入力の都度変更されるため全て異なるカード番号に対する試行とみなされ、この方法では防げないことが多い。

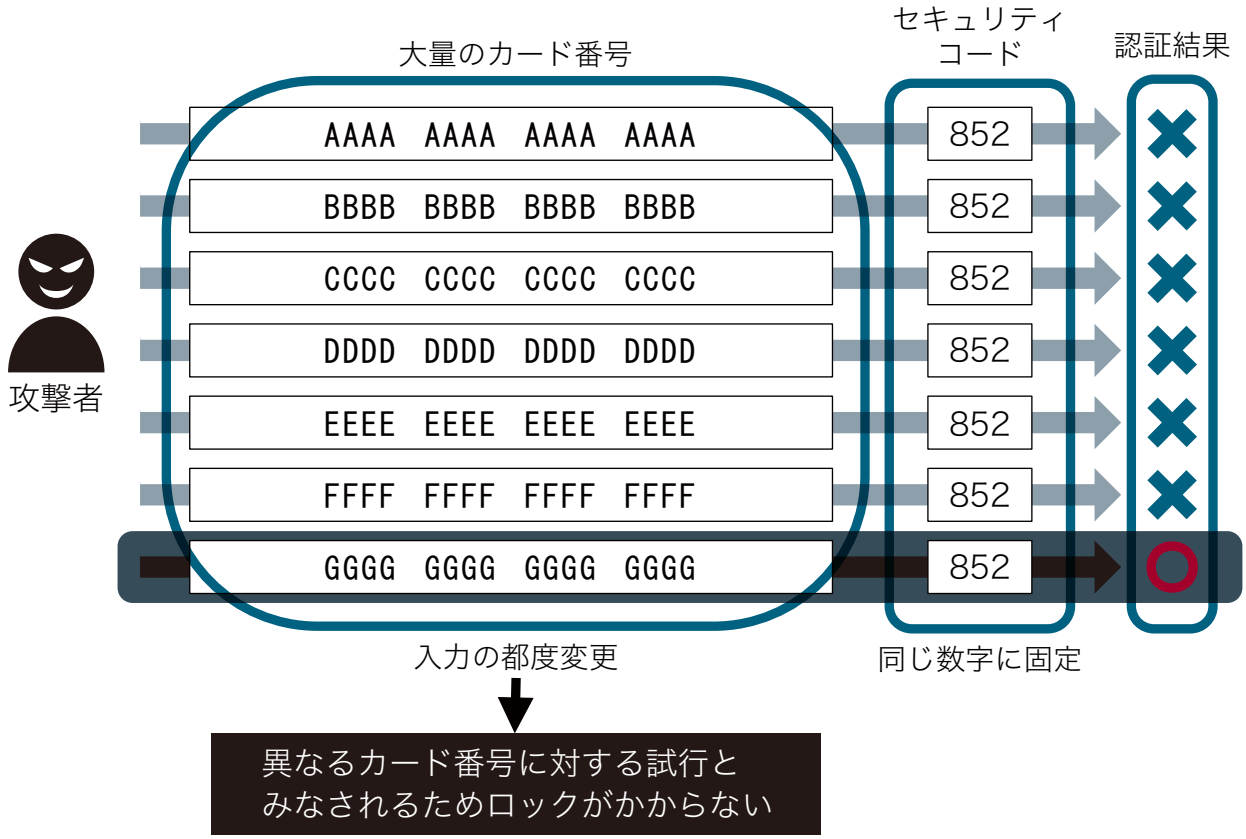
4）フィッシング

カード会社やECサイトを騙り、「利用が制限されています」等の内容と確認用のURLを記載したメールやSMSを送付してフィッシング（偽）サイトに誘導する手口である。送付されるURLにアクセスすると、本物のサイトにそっくりの画面が表示され、個人情報やカード情報を入力するよう促される。犯人は入力された情報を窃取し、不正利用する（図1-18）。

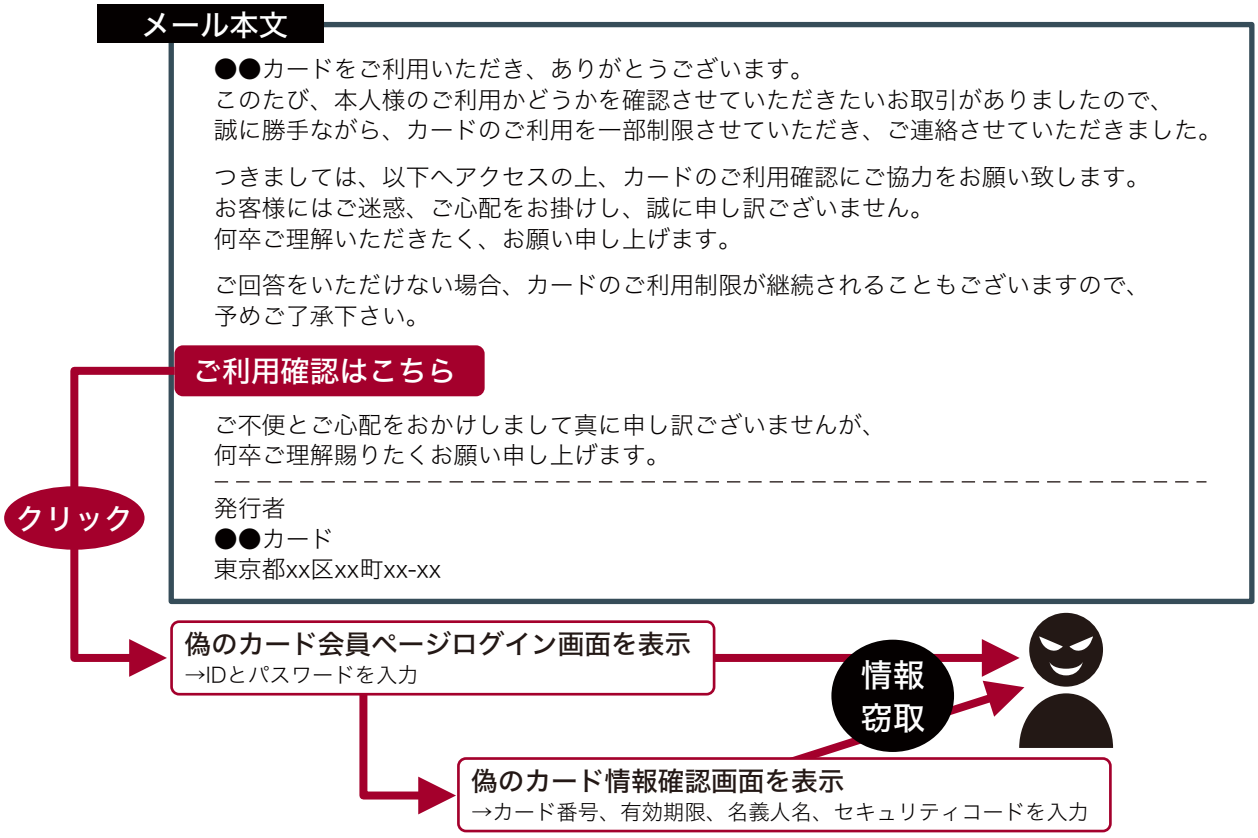
フィッシング対策協議会は、報告を受けたフィッシング事例について、メッセージのタイトル、文面、実際に表示されるフィッシングサイトの画面のスクリーンショットを緊急情報として公表し、注意喚起している。2021年はクレジットカード番号とセキュリティコードを窃取するフィッシングが延べ57件報告された。中にはクレジットカード番号とセキュリティコードを入力させた後、偽の3Dセキュアの認証画面を表示し、3Dセキュアのパスワードまで、まとめて窃取するものもある。

フィッシングメールのタイトルや内容にはその時の社会の状況が反映される。2021年に東京オリンピック・パラリンピックに関連したフィッシングが発生した。警視庁サイバーセキュリティ対策本部は、オリンピックの映像配信を装い、アカウント作成とクレジットカード情報の入力を促すサイトが複数確認されているとして注意を呼び掛けた。また、新型コロナウィルス関連では、公的機関を騙った給付金の案内やワクチン接種の案内などの件名のフィッシングメールが報告されている。

▼図1-17. リバースブルートフォースアタック



▼図1-18. フィッシングメールの例



■1-3. その他のキャッシュレス不正被害

1-3-1.認証情報窃取によるキャッシュレス手段不正利用

自社サービスのIDにクレジットカード以外の支払手段を紐づけ決済機能を提供するサービスで、フィッシングで認証情報を窃取し決済手段を不正利用する事件が公表されている。

1）通信キャリアT社のキャリア決済不正利用

2021年10月2日、通信キャリアT社より、同社を名乗るSMSによるフィッシングの発生が公表された。スマートフォンで料金支払いの確認などを求めるメッセージに記載されたリンク先にアクセスすると、同社公式アプリを装った不正なアプリがインストールされ、ネットワーク暗証番号（T社が提供するサービスを利用する際に入力を求められる4桁の暗証番号）の入力を求められる。入力すると、T社公式オンラインストアでキャリア決済によりApp Store & iTunesギフトカード、Google Playギフトカードが不正に購入される。

T社公式オンラインストアのIDに使用しているアカウントは、T社のISPサービスで接続しているユーザーについては、IDとパスワードではなくSIMカードとネットワーク暗証番号の組み合わせでログインや決済が可能となっている。この仕様が悪用され、インストールされた不正アプリによりオンラインストアへのログインと決済が行われたと推測される。

事件の発生から公表されるまでの2日間で、被害者は1,200名以上、被害金額は1億円を超えた。T社は被害金額を全額補償する方針を発表している。

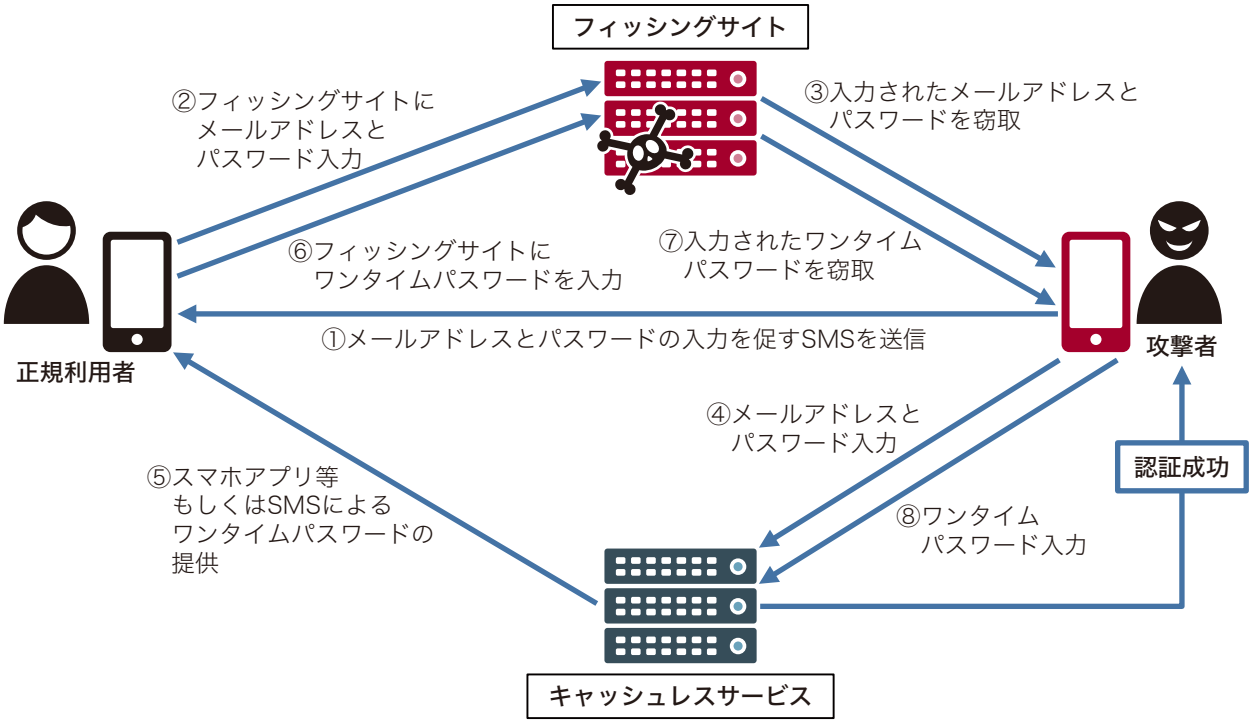
2）フリマアプリUの不正ログインによるコード決済サービスの不正利用

フリマアプリサイトUを運営するU社は、同社を装うメールやSMSが急増しており、同社アプリを装って認証情報を窃取され、アプリと連携したコード決済サービスを加盟店で不正利用される取引を確認したことを公表している。U社のコード決済アプリはチャージに銀行口座紐づけや現金以外にもフリマアプリUの売上とポイントが利用できる（クレジットカードは利用不可）他、利用額をまとめて翌月末に精算できるサービスを提供している。また、2021年8月には、フリマアプリU利用実績により20万円を上限とした少額融資を受けられるサービスの提供を開始した。これらの手段を組み合わせることで、銀行口座情報が紐づけられていないアカウントでもクレジットカードと同等の限度額での利用が可能となる場合がある。

フリマアプリUはログイン時に登録した電話番号宛にSMSによる認証コードを送信する二段階認証を実装している。一方で、誘導先の偽サイトもメールアドレスとパスワードを入力させた後、認証コードを入力させる画面が表示されるようになっている。MIB攻撃（マン・イン・ブラウザ、ブラウザに表示された偽サイトから入力された情報を攻撃者が受信し、即座に正規のサイトに入力することで不正ログインを成功させる）により二段階認証が突破され、不正利用されたと推測される（図1-19）。

U社コード決済サービスの不正利用は2021年末ごろから増加しており、2022年第一四半期の決算発表では、決済サービスの不正利用の補填に６億円を充てたことが公表された。

▼図1-19. マン・イン・ブラウザ攻撃の概要



1-3-2. ランサムウェアによるカード情報流出

感染したコンピューターのストレージにあるデータを暗号化して身代金を要求する、ランサムウェアによる攻撃は増加の一途をたどっている。イスラエルのセキュリティ分析会社Cognyte Softwareの調査によれば、2021年上半期は全世界で1,097件の組織がランサムウェア攻撃を受けた。2020年の攻撃は年間で1,121件だったので、昨年1年分のランサムウェア攻撃が半年で起きていたことになる。国内でも警察庁が2021年上半期だけで61件、下半期で85件のランサムウェア被害報告があったと発表しており、2020年下半期の21件に比べると激増している。IPAは2021年、2022年と2年連続で「ランサムウェアによる被害」を情報セキュリティ10大脅威（組織部門）の第1位に選定した。

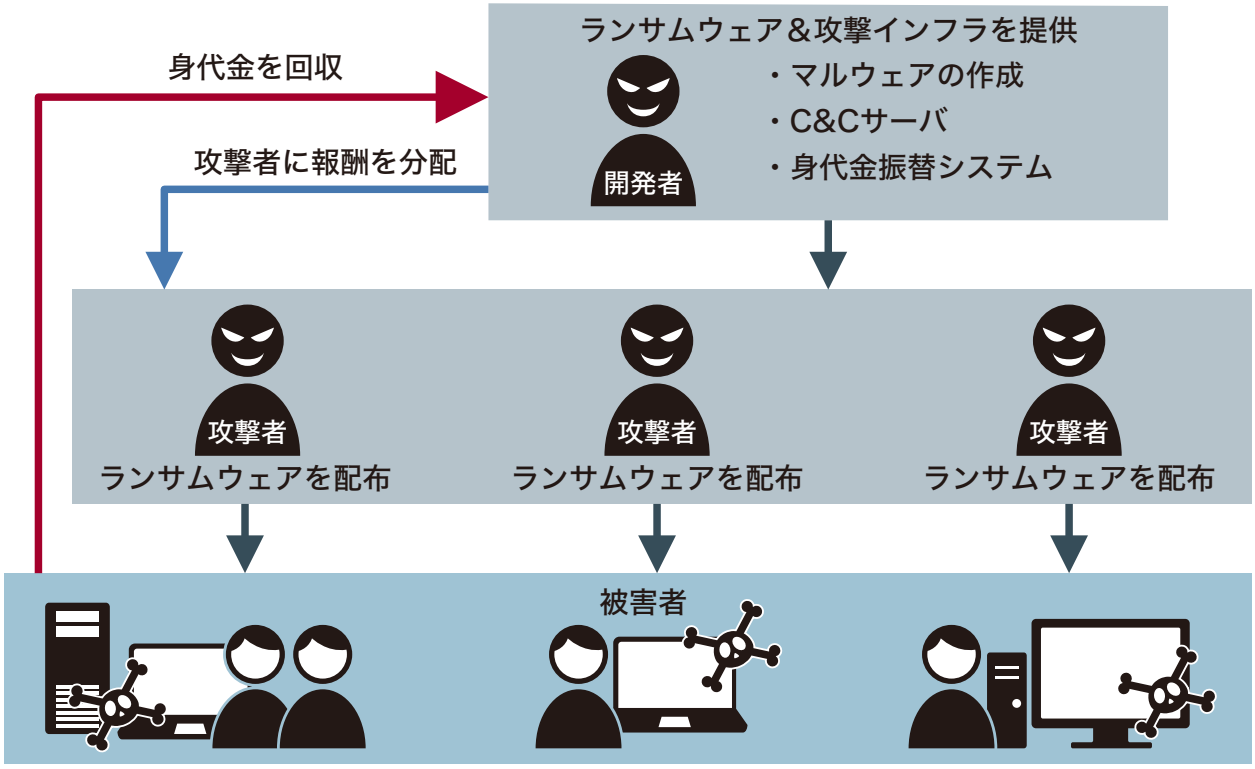
最近はデータを暗号化するだけでなく、データを窃取した上で企業に対し「支払わなければデータをする」として身代金を要求する二重恐喝（ダブルエクストーション）を行う事例が増えている。感染手法も、以前は無差別に送り付けたスパムメールでマルウェアを感染させるばらまき型が主流だったが、特定の企業を標的にしたフィッシングやVPNを標的としてネットワークに侵入をはかるような標的型攻撃が増えている。RaaS（Ransomware as a Service）モデルと呼ばれる、ウィルスや暗号化したデータを公開するサーバーなどを提供するプレイヤーと、提供されるウィルスを利用して実際の攻撃を行う協力者が分業して攻撃を行い、収益を分配するエコシステムも出来上がっているという。多くのセキュリティ専門家がランサムウェアを2022年の最大のセキュリティ脅威と位置付けている。

ランサムウェアによりカード情報が流出した例も報じられている。2020年2月、大手のランサムウェア攻撃者集団であるMazeは、コスタリカ銀行（Banco de Costa Rica）から400万件のユニークなカード情報を入手していると主張し、証拠としてセキュリティコード付きのクレジットカード番号240件を流出させた。

国内では、2021年6月にスポーツクラブV社が会員管理システムのサーバーがランサムウェア感染してデータを暗号化されたことを公表した。暗号化されたデータには150,084人分の個人情報が含まれ、うち34,920件にはクレジットカード情報が含まれていた。ただし、クレジットカード情報は2014年2月11日以降当該サーバーに保存していなかったため、暗号化されたカード情報は全て有効期限が切れていた。また、暗号化されたデータの流出は2022年5月現在で確認されておらず、身代金の要求もないとのことである。

2022年7月末現在、国内ではランサムウェアによるカード情報の流出は公表されていない。国内では加盟店のほとんどが自社のシステムにカード情報を保存しない「非保持化」を選択しており、カード情報を自社サーバーに保存しているのはカード発行会社や決済代行事業者など限定されている。これは逆にカード情報を狙う攻撃者の視点から見れば、狙うべき対象が明確で限られていることにもなる。攻撃者がカード情報の入手に成功した場合は、二重恐喝で身代金を得るよりもダークウェブでそのまま販売する方が早く確実に金銭的な利益が得られると推測される。

▼図1-20. RaaSの仕組みの例

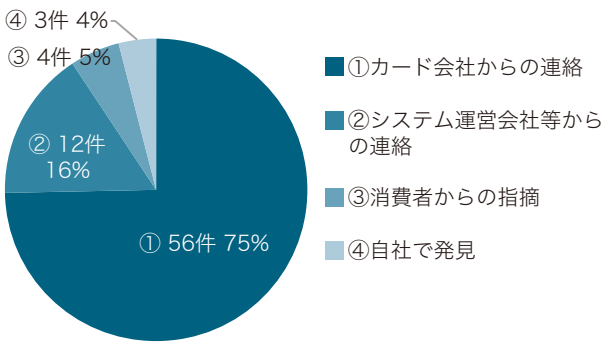


■1–4. カード情報が流出した際の対応

1-4-1. カード情報流出発覚のきっかけ

カード情報流出事件はEC加盟店に集中して発生している。そのほとんどは加盟店と契約を結んでいるカード会社（加盟店契約カード会社）からの通知によって発覚している。ｆｊコンサルティングでは、2021年に発生した75件のカード情報流出事件の発覚のきっかけを公表内容から推定したところ、全体の75%にあたる56件がカード会社から情報流出の可能性を指摘されたという結果となった。対して、自社でシステムの異常や不正アクセスの可能性に気づいたのはわずか3件（4%）にとどまっている。

▼図1–21. カード情報流出発覚の経緯



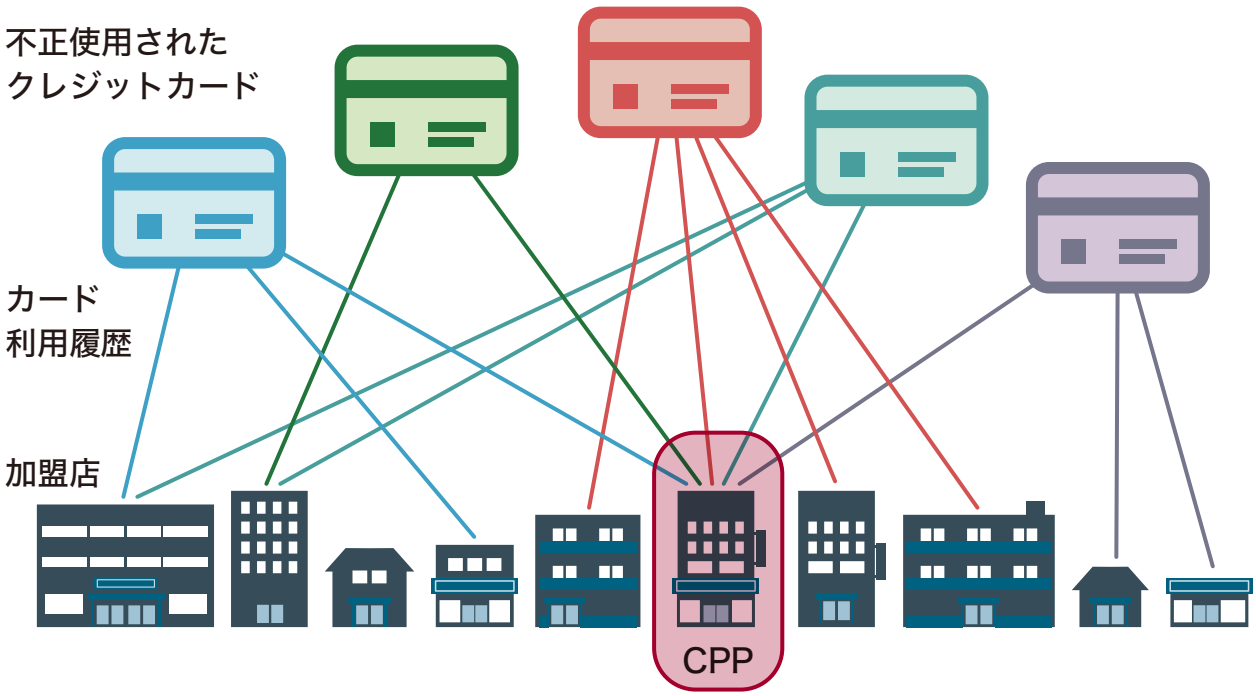
1-4-2. カード会社はどうやってカード情報が流出した加盟店を割り出すのか

加盟店から流出したカード情報は、別の加盟店でカード会員になりすまして不正利用されることが多い。その結果、正規のカード会員が、利用明細に身に覚えのない履歴が記載されていることに気づき、カードを発行しているカード会社に問い合わせし、不正利用が確認されれば届け出する。

届けを受けたカード発行会社は国際ブランドと連携し、そのカードがいつどこで利用されたかを調査する。不正利用された複数のカードを調査することによって、過去に共通に利用された加盟店（Common Purchase Point：以下CPP）が特定できる。CPPの情報に基づき、カード発行会社や国際ブランドから当該加盟店と直接契約を結んでいる加盟店契約カード会社に通知される。

連絡を受けた加盟店契約カード会社は、CPPとなった加盟店に対してカード情報流出の可能性を通知し、第三者機関による調査（フォレンジック調査）を依頼する。調査費用は通常当該加盟店が負担する。フォレンジック調査は、国際ブランドのルールによって、PCI SSCが認定しているフォレンジック機関（PFI：PCI Forensic Investigator）が原則実施する必要がある。

▼図1-22. Common Purchase Pointの特定



1-4-3. 加盟店に求められる初動対応

カード情報流出発覚のきっかけは、流出したカード情報が不正利用されたことである。したがって、カード情報の流出自体は、発覚よりもかなり以前から発生したことになる。加盟店契約カード会社から調査依頼があった時点では流出から数ヶ月以上経過していることも珍しくない。一度流出した穴が自然に塞がることはない。調査依頼時にもカード情報は流出し続けていると考え、まずは流出を止める必要がある。

初動対応の第1段階は、停止可能なネットワークを切断することである。仮想化環境の場合はネットワークのインターフェースを停止する必要がある。ネットワークの停止が難しい場合は、インターネットへの不審なアウトバウンド通信がないかを調査及び監視する。

同時に、フォレンジック調査機関に提出するために、ログを保全する。アクセスログ、システムログ、データベースログ、アンチウイルス製品の検知ログ、ファイアウオールやルーターの通信ログ、侵入検知のログなど、あらゆるログを速やかに保全する必要がある。保存期間はPCI DSSの要件では1年間となっているので、1年以上を目安とする。なおカード情報が流出した加盟店は、PCI DSSに準拠していないことも多いので実際には1年分に満たないケースもあるがその場合は最大限の期間を保全することになる。

なお、これらの対応を実施している間は、サーバーやネットワーク機器の停止・再起動やデータの削除は絶対に行ってはいけない。停止や再起動によって、不正アクセスの痕跡を消してしまうようなプログラムが仕掛けられていることがある。

同時に、フォレンジック調査に備えて、自社のシステムの現状を把握する必要がある。図1-23のような事項を社内で速やかに確認する。

調査が終了して再発防止策を講じるまでは原則としてカード決済は一時停止となる。EC加盟店にとって主要な決済手段を失うことになりビジネス上のダメージは避けられない。

▼図1-23. カード情報流出時の確認事項

1. カード情報流出の認識	・顧客からのカード情報流出に関する問い合わや指摘の有無 ・調査実施の有無　など
2. システムの異常	・ウェブサイトへの接続不調 ・見慣れないエラーメッセージ ・不審なログ など
3. カード情報の保存・管理状況	・システム構成図 ・カード会員データフロー（カード情報が通過、処理、保存される場所） ・カード情報保存の有無（旧システムも含む） ・カード情報の項目

1-4-4. フォレンジック調査では何が調べられるのか

「フォレンジック」とは、直訳すると「法廷の」「科学捜査の」という意味である。カード情報流出事件における「フォレンジック調査」とは、ログなどの電磁的記録の調査・分析を行い、不正アクセスが実際に発生していたのか、発生していた場合の原因は何か、カード情報はどの程度流出したのか、といった被害状況を明らかにするための調査を指す。

先にも述べた通り、カード情報流出事件が発生したときのフォレンジック調査は、PCI認定フォレンジック機関（PFI）が実施する。

調査結果はPFIから依頼主である加盟店に提出され、加盟店から加盟店契約カード会社に報告する。最終的には国際ブランドにも報告される。調査費用は事件の規模によるが、おおむね数百万円から1,000万円程度となる。海外で発生した大規模な流出事件では、数億円の調査費用を要したケースもある。調査費用だけでも加盟店側の負担は大きい。

調査の報告書には、侵害の原因、流出したカード情報の項目、流出が発生していた期間やカード情報の件数などが記載される。侵害の痕跡はウェブサーバーやアプリケーションサーバーなどのログから分析することが多い。これらの調査結果とログによって、流出期間と件数を特定する。

フォレンジック調査の重要な目的の一つが、流出したカード番号の特定である。カード発行会社を介して当該カードの利用者に対して注意喚起を行うと同時に、カード発行会社や国際ブランドの不正利用の監視対象にすることで二次被害を防ぐことができる。

PFIの最新のリストはPCI SSCのウェブサイトで公開されている。「Servicing Country」で「Japan」を選択すると、日本国内でサービスを提供しているPFIが一覧で表示される。

1-4-5. なぜ流出の公表には時間がかかるのか

加盟店がカード情報流出を外部に公表するのは、ほとんどの場合フォレンジック調査が完了してPFIから最終報告書が提出された後となる。PFIの報告書提出までは、調査着手からおよそ１ヶ月程度が目処となる。その後、加盟店契約カード会社と行政機関への報告、カード情報が流出したカード会員へのお詫びの連絡、問い合わせに対応するための体制準備を行う。カード発行会社にも問い合わせがあることが想定されるため、流出規模によってはカード発行会社にも臨時コールセンター設置などの体制整備が必要となる。その後、自社ウェブサイトやプレスリリースでの公表となるため、実際には調査完了から公表までに時間を要することがある。

1-4-6. カード決済再開の条件

カード決済を再開するためには、当然、再発防止策を講じる必要がある。再開の可否は加盟店契約カード会社が判断する。原因特定と再発防止策の構築完了を加盟店契約カード会社が確認して、はじめて取引再開が認められる。

PCI DSSに準拠していない加盟店の場合は、一般に加盟店契約カード会社がPCI DSS準拠や非保持化の対策を確認した上でカード取引の再開が認められるとされる。加盟店契約カード会社からの通知からカード取引再開までに、通常であれば最短でも3カ月、長ければ1年以上かかることも珍しくない。その期間を考慮し、ECサイトをECモールなどに移して自社サイトでのクレジットカード決済を取りやめたり、サービスの再開自体を諦めるケースもある。

▼図1-24 カード情報流出事件公表時のプレスリリース内容

1. 事案概要	・流出していた時期 ・流出したカード情報の件数 ・流出の可能性がある情報（項目） ・原因
2. 発覚と対応の経緯	・カード情報流出を知った日時と経緯 ・サイト閉鎖、カード決済停止などの対応をした日時 ・第三者機関による調査完了の日時　など
3. 自社の対応	・お客様への対応（カード情報流出の可能性があるお客様への通知、コールセンター開設など） ・行政機関への対応（個人情報保護委員会への報告など） ・警察への対応（被害届の提出など）
4. お客様へのお願い	・カード明細確認のお願い、再発行時の手数料の案内など
5. 公表が遅れた経緯	・対応準備が整ってからの告知となったことのお詫び
6. 再発防止策	・（原因に応じた対応）

2. 制度の動向

■2-1. 『クレジットカード・セキュリティガイドライン』改訂

日本におけるクレジットカードの規制法は割賦販売法である。割賦販売法ではクレジットカード情報を取り扱う事業者に対してセキュリティ対策義務を課している。その具体的な内容は、クレジット取引セキュリティ協議会（以下協議会）が発行する『クレジットカード・セキュリティガイドライン』で規定されている。

最新版の『クレジットカード・セキュリティガイドライン【3.0版】』（以下『セキュリティガイドライン3.0』）は2022年3月に公表された。以下、クレジットカード情報保護と不正利用対策に分け、主要な改訂のポイントを紹介する。

2-1-1.クレジットカード情報保護

クレジットカード情報保護については、割賦販売法第35条の16第1項1号～7号で義務付けの対象となる事業者が規定されている。『セキュリティガイドライン3.0』では、事業者の号数ごとに業務内容と対象となる業務の例示が整理された。2号事業者（加盟店）に関しては、カード情報を扱う業務を全て外部に委託し、自社ではカード情報を保存・処理・通過しない「非保持化」が認められるが、その他の事業者についてはPCI DSS準拠を義務付けている。

特に7号事業者については、カード情報の伝送、処理、保存を行っている事業者だけでなく、決済代行会社または加盟店契約カード会社に接続できる決済モジュールを提供している事業者も含まれることが明記された。

1-1-5で取り上げたサプライチェーン攻撃を受けたECシステム提供会社Q社は、7号事業者に相当すると考えられが、同社はカード情報の取り扱いを決済代行事業者に委託し、自社で保存・処理・通過していなかったため、自社にPCI DSS準拠義務があることを認識していなかったと思われる。同様の認識である加盟店向け決済システム提供事業者は多数あると推測される。

▼図2-1: 改正割賦販売法（2021年4月施行）第35条の16第1項で
クレジットカード情報保護を義務付けられた事業者と求められる対策

	『セキュリティガイドライン』内での名称	業種の例示	認められるカード情報保護対策	
			非保持化	PCI DSS
1号事業者	カード発行会社（イシュアー）	・カード発行会社（イシュアー）	ー	●
2号事業者	加盟店	・加盟店（対面/非対面）	●	●
3号事業者	カード会社（アクワイアラー）	・加盟店契約会社（アクワイアラ）	ー	●
4号事業者	決済代行業者等	・決済代行業者（対面/非対面取引双方） ・ECモール事業者（デジタルプラットフォーマーなど） ・ショッピングセンター、モール等（対面取引） ・CCT端末先（端末取引） 等	対面取引のみ取扱う事業者の一部（※1）	●
5号事業者	QRコード決済事業者等	・QRコード決済事業者 ・スマートフォン決済事業者 ・ID決済事業者 等 ※名称にかかわらずカード情報と紐づけた他の決済用番号で決済を行う事業者	ー	●
6号事業者	5号事業者の委託会社	・第5号事業者からカード情報の管理を受託している事業者	ー	●
7号事業者	加盟店向け決済システム提供事業者	・EC システム提供会社(ASP/SaaS として EC 事業者にサービス提供する事業者、EC 事業者に購入プラットフォームを提供する事業者) 等 ※カード会員データの伝送処理保存を行っている事業者、決済代行会社又はアクワイアラーに接続できる決済モジュールを提供している事業者も含まれる。	ー	●

※1 合わせて協議会が定める「セキュリティ対策チェック項目」に基づく対策が必要

2-1-2. 不正利用対策

『セキュリティガイドライン3.0』では対面取引と非対面取引に分けて不正利用対策について記載している。

1）対面取引におけるサイン取得の任意化とPINバイパス廃止

偽造カード対策として進められた対面のクレジットカード取引のIC化が完了したことにより、対面取引における本人確認はサインの照合からPINによる認証へと変わりつつある。これに伴い、国際ブランドもルールを変更して、取引時のサインの取得を加盟店の任意とする動きがある。

『セキュリティガイドライン3.0』では、2025年3月をめどに対面加盟店での取引で本人確認を行う場合はPINを必須とし、サイン取得は加盟店の任意とすることが記載された。これに伴い、消費者のPIN忘れの救済措置としてPIN入力の代わりにサインによる本人確認を認める「PINバイパス」は2025年3月で原則廃止となる。

2）非対面取引におけるEMV 3-Dセキュア導入推進

非対面加盟店の不正利用被害は増え続けており、その大部分がEC加盟店におけるものである。『セキュリティガイドライン3.0』では、EC加盟店に対して、オーソリゼーションと加盟店契約上の善良なる管理者の注意義務を求めるとともに、リスクに応じた複数の方法による対策を求めている。具体的には、図2–2に示す高リスク商材取扱加盟店および不正顕在化加盟店に対しては、不正利用対策として「本人認証」「券面認証」「属性・行動分析」「配送先情報」の4つのうち1つないしは2つの導入を求めている。（図2–3）

4つの方策のうち、「本人認証」については、従来用いられていた3-Dセキュアのサービスが2022年10

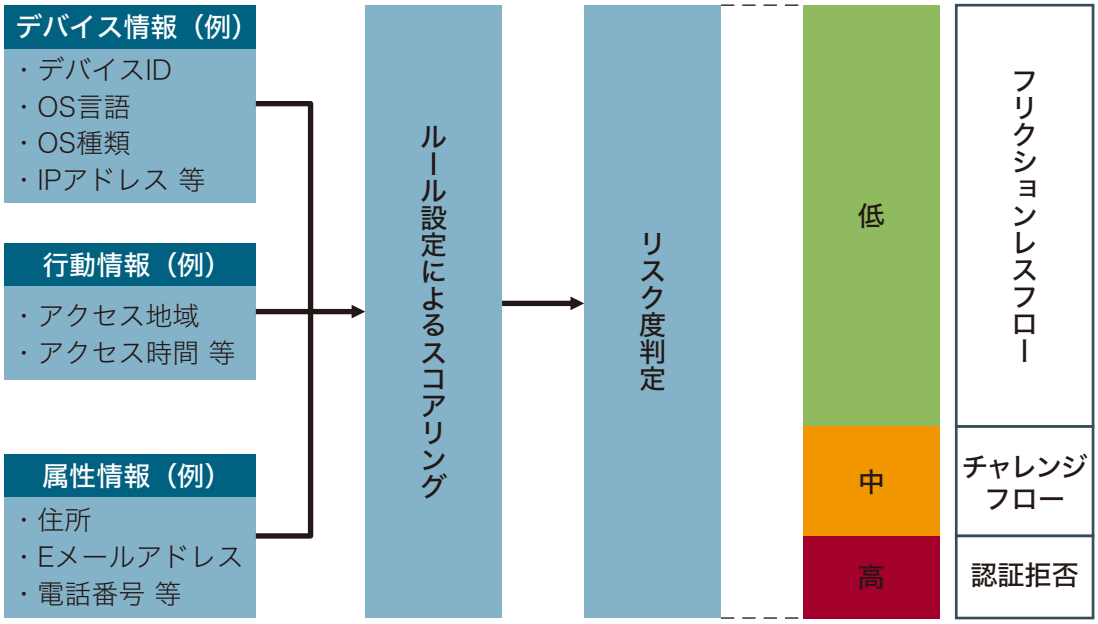
▼図2-2 EC加盟店の区分と求められる不正利用対策

対象			求められる不正利用対策
全てのEC加盟店			・オーソリゼーションの導入 ・善管注意義務
追加の対策が求められるEC加盟店	1）高リスク加盟店	不正利用被害の発生状況からリスクの高い商材として選定した以下を主たる商材として扱うEC加盟店 ①デジタルコンテンツ（オンラインゲームを含む） ②家電 ③電子マネー ④チケット ⑤宿泊予約サービス	・全てのEC加盟店に求められる対策に加え、4つの方策のうちから1つ
	2）不正顕在化加盟店	加盟店契約カード会社が各社が把握する不正利用金 額が「3 ヵ月連続 50 万円超」に該当する EC 加盟店	・全てのEC加盟店に求められる対策に加え、4つの方策のうちから2つ

▼図2–3 EC加盟店の不正利用対策の具体的な方策

不正利用防止の方策	説明
1. 本人認証	利用者本人が取引を行っていることを確認 ①3-D セキュア ②認証アシスト ※3-D セキュア 1.0 は 2022 年 10 月に取扱終了するため EMV 3-D セキュアへの移行が必要
2. 券面認証（セキュリティコード）	クレジットカードの券面に記載された 3〜4 桁の数字を入力させることにより正規の券面を持っていることを確認
3. 属性・行動分析（不正検知システム）	カード決済時に使用したデバイス情報などについて過去の取引実績と照合したり、過去の不正利用時との共通点などを総合的に分析して不正取引の可能性を特定
4. 配送先情報	過去の不正利用発生時の配送先情報と商品の配送先を照合し、合致する場合は出荷を差し止めることで不正利用を防止

▼図2–4　リスクベース認証のイメージ
出所：『EMV 3-Dセキュア導入ガイドライン』（クレジット取引セキュリティ対策協議会 2022年3月）



月に終了する。『セキュリティガイドライン3.0』では、3-Dセキュアの後継規格であるEMV 3-Dセキュアへの早期移行が必要となることが記載された。

EMV 3-Dセキュアは、以下の特徴をもつ。

①リスクベース認証により、消費者はIDやパスワードの入力の手間なく認証が完了する

②スマートフォンアプリ内での利用が可能

③モバイルウォレットやコード決済アプリへの支払い手段登録など、決済を伴わない場面の本人認証で利用可能

①のリスクベース認証は、ECサイトでの決済時に、取引がカード会員本人によるものかどうかの確からしさによって認証の強さを変える認証方法である。利用者の属性情報、行動情報、デバイス情報などを活用して、取引がカード会員本人によるものかをスコアで評価し、リスク度を判定する。リスクが低いと判定された取引は、利用者のEMV 3-Dセキュアのパスワード入力が不要な「フリクションレスフロー」が実現される。逆に、リスクが一定以上と判定された取引は、自動で取引を拒否したり、リスク度が中間の取引については、EMV 3-Dセキュアのパスワードなど追加の認証情報を要求する「チャレンジフロー」に切り替えることで安全性を高める。（図2-4）

国際ブランドが提供する3-Dセキュア1.0のサービスは2022年10月に終了が予定されている。そのため、高リスク加盟店あるいは不正顕在化加盟店のうち、現在3-Dセキュア1.0を導入して不正利用対策をおこなっている加盟店は、期日までにEMV 3-Dセキュアへの切り替えもしくは他の方策の実施がされない場合は必要な不正利用対策が不十分な状態となる。また、3-DセキュアとEMV 3-Dセキュアは互換性がないので、現在独自にリスクベース認証持つ3-Dセキュア1.0を導入してフリクションレスフローを実現している加盟店やPSPも期日までにEMV 3-Dセキュアへの切り替えが必要となる。

▼図2-5 EMV 3-Dセキュアの不正リスク負担
出所：『EMV 3-Dセキュア導入ガイドライン』（クレジット取引セキュリティ対策協議会 2022年3月）

	ステータス	リスク負担
1	EMV 3-Dセキュア認証成功	加盟店は免責対象（※）
2	会員のカード発行会社または会員がEMV 3-D セキュア未参加	
3	EMV 3-Dセキュア認証取引外	加盟店は免責対象外

※カード登録時にEMV 3-Dセキュア認証していても、以降の取引時にもEMV 3-Dセキュア認証しない限りは免責対象外となる。

2-1.3. EMV 3-Dセキュア導入ガイド

3-Dセキュア終了の影響が大きく、EMV 3-Dセキュアへの移行を早急に推進する必要があることから、協議会では非対面加盟店不正利用対策ワーキンググループの下にEMV 3-Dセキュア推進プロジェクトを新たに立ち上げ、『EMV 3-Dセキュア導入ガイド』（以下『導入ガイド』）を新たに公表した。

『導入ガイド』では、具体的な3-Dセキュアの処理フローや導入手続きが記載されている。また、不正利用被害発生時の損失負担についても、「EMV 3-D セキュアを実装した取引のうち、 認証成功/カード会社もしくは会員未参加の取引において不正利用が発生した場合、原則リスク負担はカード会社（イシュア）となる。」と明記された（図2-5）

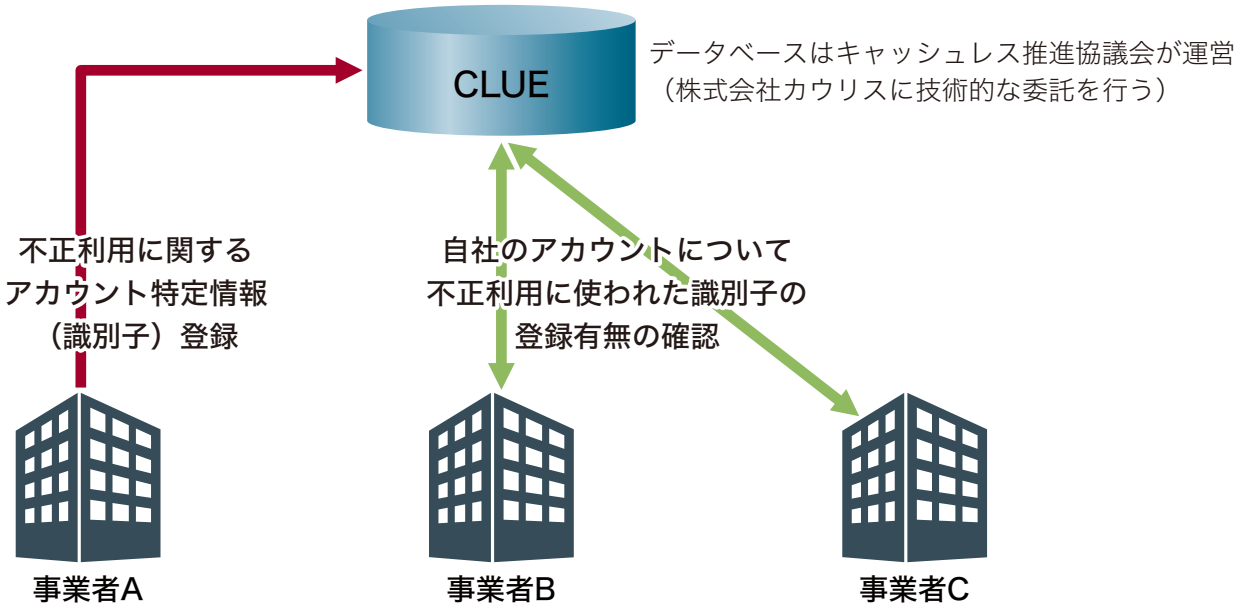
■2-2. キャッシュレス推進協議会（不正利用情報の共有）

1-3で取り上げた事例のように、クレジットカードを利用しないキャッシュレスサービスでも、フィッシングなどによる不正利用事件が発生している。中には組織的な犯罪も見られ、フィッシングサイト等で入手した消費者の個人情報等を用いて複数の決済サービスへ攻撃を行う手口も見受けられる。

2021年12月、キャッシュレス推進協議会は、キャッシュレス不正利用の被害拡大防止を目的に、キャッシュレス決済事業者間で不正利用されたアカウントに関連する情報を共有する「不正利用確認データベース（Cross-referencing List of User's Encrypted data：以下「CLUE」）」の構築を発表した。発表時にはコード決済を対象として仕様や運用ルールの検討を重ねているとしており、NTTドコモ、KDDI、コモニー、ファミマデジタルワン、LINE　Pay、楽天ペイメントが初期メンバーとしての参画を検討中であるとしている。

CLUEの運用開始は2022年度中を予定している。キャッシュレス推進協議会は、2022年度のプロジェクト活動の中で、CLUEの利用範囲拡大に向け運用規定の策定とコード決済以外の参加希望事業者による検討を行うとしている。

▼図2-6 不正利用確認データベース（CLUE）の概要出所：『キャッシュレス推進協議会 組織・活動概要』（キャッシュレス推進協議会 2022年4月公表）



■2-3. PCI DSSのメジャーバージョンアップ

クレジットカードを含むペイメントカードセキュリティの国際基準であるPCI　DSSの新しいバージョンであるPCI DSS v4.0が2022年3月に公開された。日本語版も2022年5月に公開されている。前回のメジャーバージョンアップから約8年ぶりの大きな改訂となる。この間に登場した新技術や新しい攻撃手法への対応を目的として、4つの目標を掲げた改訂が行われた。

＜PCI DSS v4.0の目標＞
①ペイメント業界のセキュリティニーズを満たしていること

②セキュリティを向上するために柔軟性と新しい手法への対応を追加すること

③継続的なプロセスによりセキュリティを促進すること

④各要件の検証方法と手順をさらに改良すること

PCI DSS v3.2.1までは、国際カードブランド5社（American Express、Discover、JCB、Mastercard、Visa）が関与していたが、2020年にUnionPay（銀聯）がPCI SSCのStrategic Memberとして加入したことを受け、v4.0では6社が関与している。

内容については、PCI DSS v3.2.1の枠組みとなっていた6つの目標・12のセキュリティ要件の構成については変わらないが、新技術への対応を意図して表記が変更されている。（図2-7）
セキュリティ強化のために以下のような要件が追加・更新されている。

①準拠する事業体が PCI DSS の対象範囲を検証するための要件

②リスク管理プロセスをより明確にし、事業体に指針を提供するためのリスクアセスメント要件の更新

③サービスプロバイダ向けの追加要件

④クラウドサービスの要件への取り込み
- 外部クラウドサービスをPCI DSS対象範囲として扱えるような要件表記の変更
- クラウドサービスプロバイダの役割と対応の明確化

対象範囲の検証については、従来からPCI DSSにおける最も重要な要素の一つである。カード情報のデータフローやシステムの追加、変更により、対象範囲は変化することが想定されるため、12ヶ月に1回（サービスプロバイダは６ヶ月に1回）または大きな変更があった場合に検証する新要件が追加された。

▼図2–７　PCI データセキュリティ基準の概要
出所『PCI DSS要件とセキュリティ基準 v4.0』（PCI Security Stanndards Council 2022年3月）

安全なネットワークとシステムの構築と維持	
要件1	ネットワークのセキュリティコントロールを導入し、維持します。
要件2	すべてのシステムコンポーネントに安全な設定を適用します。
アカウントデータの保護	
要件3	保存されたアカウントデータを保護します。
要件4	オープンな公共ネットワークでカード会員データを伝送する場合、強力な暗号化技術でカード会員データを保護します。
脆弱性管理プログラムの維持	
要件5	すべてのシステムとネットワークを悪意のあるソフトウェアから保護します。
要件6	安全性の高いシステムおよびソフトウェアを開発し、保守します。
強力なアクセス制御手法の導入	
要件7	システムコンポーネントおよびカード会員データへのアクセスを、業務上必要な適用範囲に制限します。
要件8	ユーザを識別し、システムコンポーネントへのアクセスを認証します。
要件9	カード会員データへの物理的なアクセスを制限します。
ネットワークの定期的な監視およびテスト	
要件10	システムコンポーネントおよびカード会員データへのすべてのアクセスを記録し、監視します。
要件11	システムおよびネットワークのセキュリティを定期的にテストします。
情報セキュリティポリシーの維持	
要件12	事業体のポリシーとプログラムにより、情報セキュリティを維持します。

▼図2-8 v3.2.1→ v4.0　変更点の種類と数
出所：『PCI DSS 変更点のまとめ バージョン 3.2.1 から4.0』（PCI Security Standards Council 2022年3月）を元に作成

区分	定義	変更箇所数
新規追加／変更	新たな脅威や技術、決済業界の変化に対応し、基準を最新のものにするための変更。例としては、要件やテスト手順の新規追加や変更、要件の削除などがあります。	73
明確化またはガイダンス	特定のトピックに関する理解を深めるため、またはさらなる情報やガイダンスを提供するために、言葉遣い、説明、定義、追加のガイダンス、および／または指示を更新します。	68
内容の再構成	要件の内容を揃えるための結合、分離、番号の付け直しなど、内容の再編成	43

大きな変更点としては、「カスタマイズバリデーション」の導入が挙げられる。従来のPCI DSSは、決められたセキュリティ要件を厳密に満たすように対策を求める技術基準であった。適合性の評価は、要件書に定義されたテスト手順に従って行う。

PCI DSS v4.0では、従来の手法に加え、よりセキュリティ目標にフォーカスした新たな要件の評価の方法として認められたのが「カスタマイズバリデーション」である。カスタマイズバリデーションは、PCI DSS要件の意図とセキュリティ目標に着目し、意図に沿ってセキュリティ目標が満たせていることが示せれば良いとするものである。各アプローチの概要を図2-9に示す。PCI DSSは今後も頻繁にバージョンアップしていくことは想定されないため、新技術や新しい攻撃手法に基準そのものを即座に対応させることは困難である。こうした目まぐるしい変化の中でも、カスタマイズバリデーションにより、PCI DSS要件に柔軟性を持たせ、準拠する事業体のセキュリティ向上を図っていくという考え方が導入された。

▼図2-9：定義済みアプローチとカスタマイズアプローチの概要

アプローチの種別	説明
定義されたアプローチ	基準の中で定義された要件とテスト手順を使用 ・事業体は指定された要件を満たすようにセキュリティコントロールを実施 ・評価者は定義されたテスト手順に従って要件が満たされていることを検証
代替コントロール	**定義された手法の一環として、**正当かつ文書化された技術上またはビジネス上の制約により、PCI DSS 要件を明示的に満たすことができない事業体が利用可能 ・その要件に関連するリスクを十分に軽減する別のコントロール ・年次ベースで代替コントロールは事業体によって文書化され、評価者によってレビューおよび検証され、準拠に関する報告書の提出時に添付される必要がある。
カスタマイズアプローチ	各 PCI DSS 要件の目的に焦点を当て、PCI DSS 要件に規定されているカスタマイズアプローチの目的を、定義された要件に厳密に従わない方法で満たす。 ・事業体は、定義された要件に厳密に従わない方法で、要件に記載されたカスタマイズアプローチの目的を満たすためのコントロールを実装することができる。 ・評価者は、実装された統制が表明された目的を満たしていることを検証するために、特定の実装に適したテスト手順を導き出す必要がある。 ・カスタマイズアプローチを使用して実装および検証されたコントロールは、定義されたアプローチの要件によって提供されるセキュリティを満たすか、またはそれを上回ることが期待される。

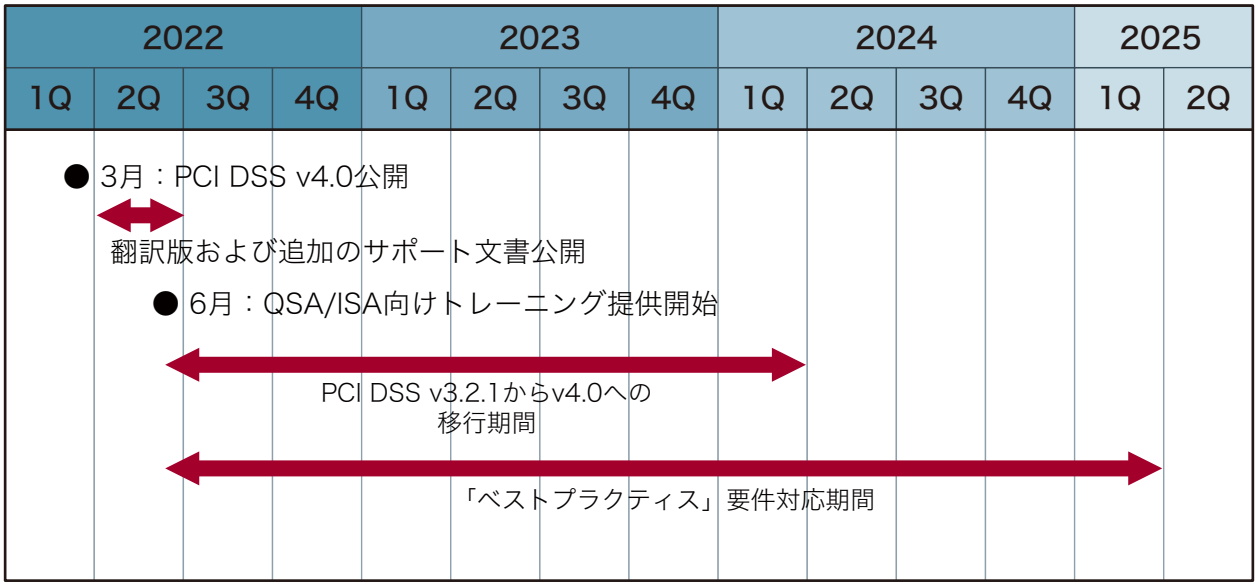
カスタマイズアプローチを使用する場合、PCI DSSに準拠する事業者は、使用するカスタマイズコントロールと、それがどのように要件の目的を満たすかを文書化する必要がある。カスタマイズコントロールに対する評価は、PCI SSCから認定されたQSA（認定評価人）もしくはISA（内部評価人）が、評価手順を作成する必要がある。一方で従来からPCI DSS準拠をしている事業体は、代替コントロールを使用していることが多い。代替コントロールは、図2-9に記載の通り、正当な技術的な制約またはビジネス上の制約がない限り適用できない。カスタマイズアプローチは、これらの制約なく準拠する事業体の意思によって適用が可能である点に違いがある。ただし、カスタマイズアプローチが適用できない要件が明示的に区分されているため注意が必要である。

最後に、PCI DSS v4.0の移行スケジュールについて説明する。2022年3月にPCI DSS v4.0公開後、各国語への翻訳や自己問診票などのサポート文書が2022年第二四半期に順次公開された。2022年6月から、既存のQSA、ISAへのトレーニングが開始され、PCI DSS v4.0での審査および準拠が可能となる。

PCI DSS v3.2.1の終了は2024年3月31日と発表された。それまでの間は、v3.2.1とv.4.0のどちらでも準拠が可能となる。

2024年4月以降は、PCI DSS v4.0での準拠が必要となる。ただし、新しい要件のうち、技術的に難易度が高かったり、対応に時間がかかる要件と区分されているものについては、2025年3月31日まではベストプラクティスとして扱われ、満たさなくても不適合とはみなされない。2025年4月1日以降はそれらが必須となる。

▼図2-10：PCI DSS v4.0移行期間



＜参考文献＞

1. 『2021年のキャッシュレス決済比率を算出しました』(経済産業省商務・サービスグループ　キャッシュレス推進室 2022年6月1日)
https://www.meti.go.jp/press/2022/06/20220601002/20220601002.html

2. 『決済動向(2022年4月)』(日本銀行決済機構局 2022年5月31日)
https://www.boj.or.jp/statistics/set/kess/release/2022/kess2204.pdf

3. 『コード決済利用動向調査　2022年6月5日公開』(一般社団法人キャッシュレス推進協議会 2022年6月5日)
https://paymentsjapan.or.jp/code-payments/code-pymt_20220605/

4. 『沖縄県初、観光系路線バス5社でVisaのタッチ決済を導入による実証実験を開始』(ビザ・ワールドワイド・ジャパン 2022年1月31日)
https://www.visa.co.jp/about-visa/newsroom/press-releases/nr-jp-220131.html

5. 『EC-CUBE公式を装うフィッシングメールにご注意ください』(株式会社イーシーキューブ 2021年11月18日)
https://www.ec-cube.net/news/detail.php?news_id=398

6. 『ECサイトのクロスサイトスクリプティング脆弱性を悪用した攻撃』(JPCERT/CC Eyes 2021年7月6日)
https://blogs.jpcert.or.jp/ja/2021/07/water_pamola.html

7. 『株式会社イーシーキューブが提供するサイト構築パッケージ「EC-CUBE」の脆弱性等について(注意喚起)』
(経済産業省商務・サービスグループ 商取引監督課 2019年12月20日)
https://warp.da.ndl.go.jp/info:ndljp/pid/12232105/www.meti.go.jp/press/2019/12/20191220013/20191220013.html

8. 『クレジットカード情報漏洩事件のまとめ(2021年上半期)』(フォックスエスタ)
https://foxestar.hatenablog.com/entry/2021/02/09/110000

9. 『クレジットカード情報漏洩事件のまとめ(2021年下半期)』(フォックスエスタ)
https://foxestar.hatenablog.com/entry/2021/07/14/170000

10. 『【重要】クレジットカード流出被害が増加しています。EC-CUBEご利用店舗のセキュリティチェックをお願いいたします。(2019/12/23)』
(株式会社イーシーキューブ 2019年12月23日)
https://www.ec-cube.net/news/detail.php?news_id=348

11. EC-CUBE4.0におけるクロスサイトスクリプティングの脆弱性(JVN#95292458)
(株式会社イーシーキューブ 2021年6月22日)
https://www.ec-cube.net/info/weakness/weakness.php?id=78

12. EC-CUBE3.0におけるクロスサイトスクリプティングの脆弱性(JVN#95292458)
(株式会社イーシーキューブ 2021年6月22日)
https://www.ec-cube.net/info/weakness/weakness.php?id=79

13. 『クレジットカード不正利用被害の発生状況』(一般社団法人日本クレジット協会 2022年3月31日)
https://www.j-credit.or.jp/information/statistics/download/toukei_03_g_220331.pdf

14. 『フィッシングに関するニュース　緊急情報一覧』(一般社団法人フィッシング対策協議会)
https://www.antiphishing.jp/news/alert/

15. 『RANSOMWARE ATTACK STATISTICS 2021 – GROWTH & ANALYSIS』(Cognyte Software 2021年8月8日)
https://www.cognyte.com/blog/ransomware_2021/

16. 『令和３年におけるサイバー空間をめぐる脅威の情勢等について』(警察庁広報資料 2022年4月7日)
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf

17. 『情報セキュリティ10大脅威2022を公開』(情報処理推進機構(IPA) 2022年5月31日)
https://www.ipa.go.jp/security/vuln/10threats2022.html

18. 『ランサムウエアの脅威動向および被害実態調査報告書 1.0版』(JPCERT/CC 2018年7月30日)
https://www.jpcert.or.jp/research/Ransom-survey.html

19. 『Maze Ransomware claims to have stolen credit card details of 11 million customers』(ManageEngine Log360)
https://www.manageengine.com/log-management/ransomware-attacks/banco-bcr-maze-ransom-attack-steals-card-data.html

20. 『PCI FORENSIC INVESTIGATORS』(PCI Security Standards Council)
https://www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators

21. 『クレジットカード・セキュリティガイドライン【3.0版】』(クレジット取引セキュリティ対策協議会、2022年3月)
https://www.j-credit.or.jp/download/news20220309b1.pdf

22. 『EMV 3-Dセキュア導入ガイド』(クレジット取引セキュリティ対策協議会、2022年3月)
https://www.j-credit.or.jp/download/news20220309b4.pdf

23. 『キャッシュレス推進協議会 組織・活動概要』(一般社団法人キャッシュレス推進協議会 2022年4月)
https://paymentsjapan.or.jp/wp-content/uploads/2022/04/PJ_FY2022_202204.pdf

24. 『Payment Card Industry データセキュリティ基準 要件とテスト手順v4.0』(PCI DSS v4.0)
https://www.pcisecuritystandards.org/document_library

25. 『Payment Card Industry データセキュリティ基準 変更点のまとめ v3.2.1→ v4.0』
https://www.pcisecuritystandards.org/document_library

26. 『PCI DSS v4.0へのカウントダウン』(PCI Security Standards Council 2021年2月25日)
https://www.jcdsc.org/news/pdf/2022/20220303_ssc-news.pdf

<執筆者プロフィール>
瀬田 陽介(せた・ようすけ)
ｆｊコンサルティング株式会社代表取締役CEO
PCI DSSの認定評価機関(QSA)代表、日本初のPCI SSC認定フォレンジック機関(PFI)ボードメンバーを経て2013年ｆｊコンサルティング株式会社を設立。キャッシュレスやセキュリティのコンサルタントとして、講演・執筆活動を行う。直近の著書は『改正割賦販売法でカード決済はこう変わる』(日経BP社)

<編集協力>
板垣朝子(ｆｊコンサルティング株式会社)

キャッシュレスセキュリティレポート2022
2022年7月31日発行
発行者
ｆｊコンサルティング株式会社
https://www.fjconsulting.jp