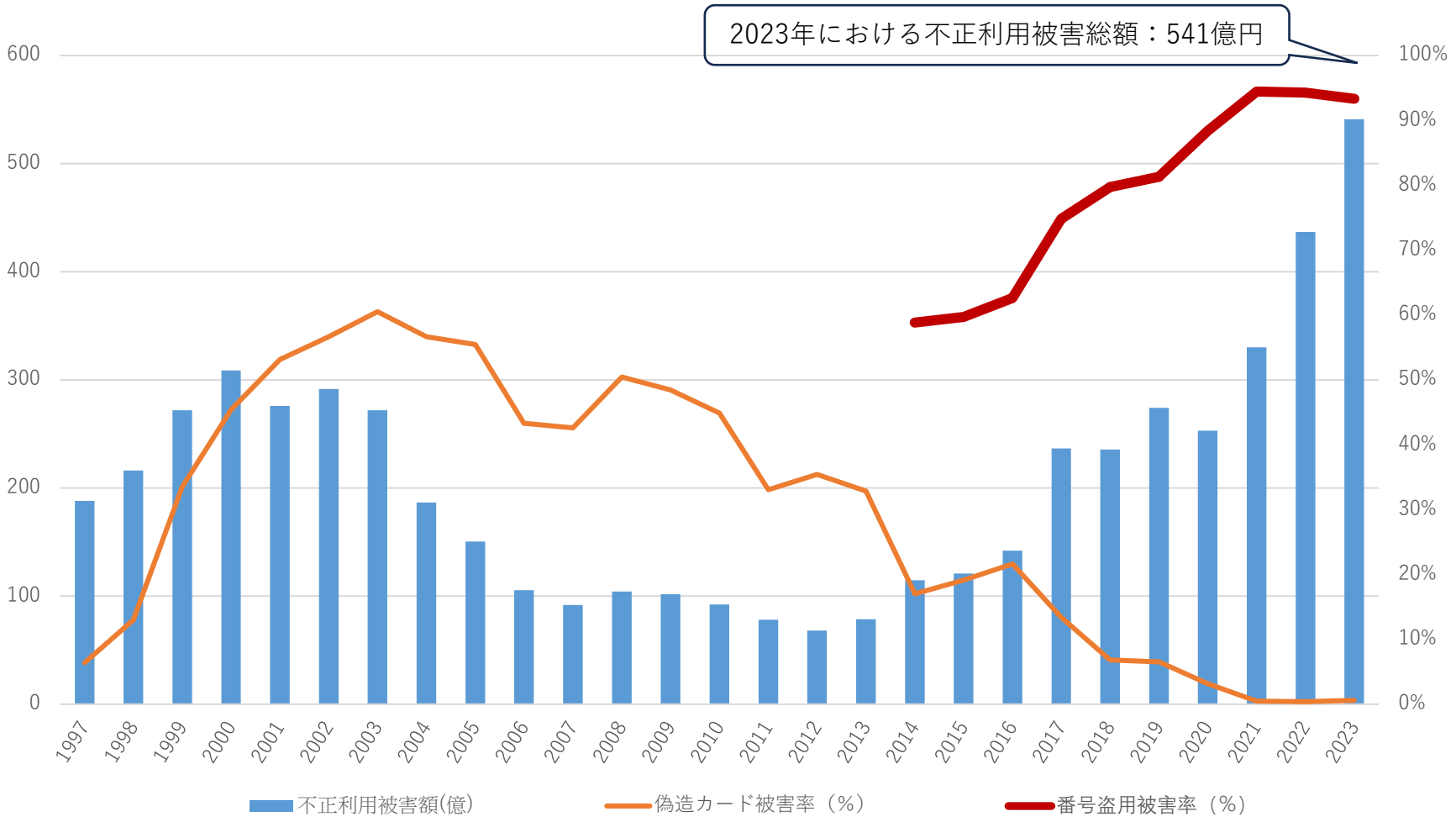
（資料2-2）

クレジットカード不正利用被害の状況について

【2024年7月】

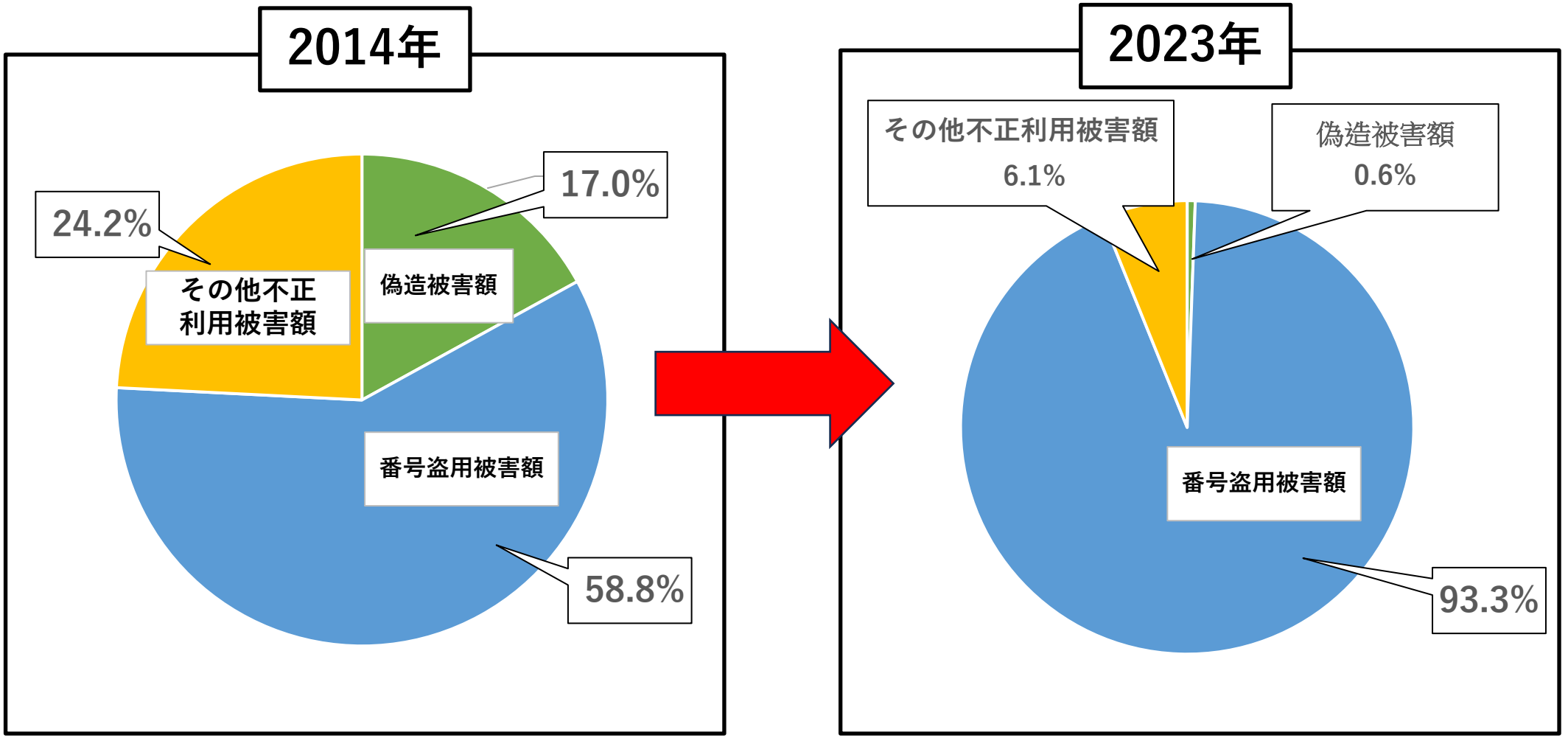
一般社団法人
日本クレジット協会

1.国内発行クレジットカードにおける年間不正利用被害額推移



出典：日本クレジット協会（2024年３月）

2.クレジットカード不正利用被害の状況



※出典:(一社)日本クレジット協会　日本のクレジット統計

3.クレジットカード不正利用被害（番号盗用）について

□番号盗用の手口としては、EC加盟店やPSP等に対するサイバー攻撃のほか、カード利用者からクレジットカード番号等（カード情報）を窃取する目的で、実在のサービスや企業をかたり、偽のメールや ＳＭＳ（携帯電話のショートメッセージ）で偽サイトに誘導し、カード情報を入力させるなどにより窃取する、いわゆる「フィッシング」などがある。

□この「フィッシング」の手口などにより、窃取したカード情報を使って、カード利用者本人に“なりすまし”て不正な利用が行われている。

□このような番号盗用による不正利用を防止するためには、カード利用者がカード情報を取られないように不審なメール等への日頃からの注意が求められる。

□一方、クレジット業界は、“なりすまし”を防ぐための有効な対策として、カード利用者本人であるかの確認強化に取り組むとともに、カード利用者にフィッシングに関する注意喚起を実施している。

4.フィッシングへの注意喚起のための周知・啓発活動

□消費者に向けたフィッシングへの注意喚起を目的とした周知・啓発活動として、（一社）日本クレジット協会（JCA）ではフィッシングに関する周知・啓発動画等を作成し、JCAのHP上に掲載している。本動画については、JCA会員のカード会社がフィッシング詐欺に関する注意喚起を行う際にもご活用いただいている。

〔日本クレジット協会HP 守ろうクレカ 防ごう不正利用〕
https://www.j-credit.or.jp/customer/security-movie/#block01

5.カード利用者の本人確認(本人認証サービス)登録推進

□クレジットカード関係事業者では、“なりすまし”防止対策として「本人認証サービス（EMV3-Dセキュア）※を推進している。

※本人認証サービス（EMV3-Dセキュア）
オンラインショッピング時に、カード決済が本人によるものなのかをデバイス情報や行動情報、属性情報といった様々な観点から総合的に判定し、判定結果に応じて追加の本人認証や取引の拒否を行う本人認証の仕組みである。

□追加認証のためには、カード所有者に追加の情報提供を求めるためのメールアドレスや、電話番号などをカード会社に登録してもらい、登録された連絡先に「ワンタイムパスワード」などの本人しか知りえない情報を送信し、当該情報をカード会社に送信することで認証できる。

6.本人認証サービスの登録推進に係る広報・啓発活動
(1) クレジットカード業界の取組み

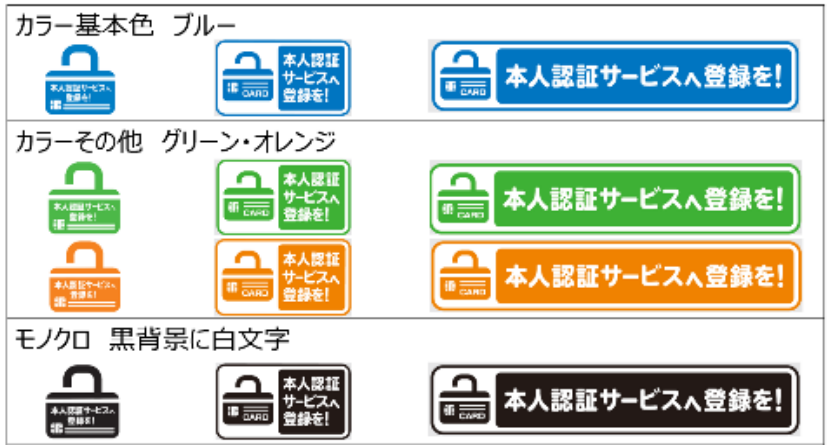
カード利用者に「本人認証サービス」の必要性と登録推進への強いメッセージを伝えられるように、「統一メッセージ」、「統一ロゴ」を作成、カード会社各社の取組みに加え、クレジットカード業界全体として、横断的な広報・啓発活動を展開している。

□統一メッセージ

「より安全安心なオンラインショッピングのために、本人認証サービスへ登録を！」

□統一ロゴ

セキュリティをイメージしやすい「鍵」をモチーフとし、統一メッセージのうちキーとなる文（本人認証サービスへの登録）を記載



(2) クレジット業界団体（JCA）の取組み

JCAのHP上に本人認証サービス登録推進のための特設ページを作成、周知啓発動画「ワンタにおまかせ！」を掲載。また、このコンテンツをもとに、新聞・駅サイネージ・youtube・LINE等で周知啓発を行った。

〔日本クレジット協会HP 特設ページ〕
https://www.j-credit.or.jp/customer/honnin-ninsho-wanta/

〔ワンタにおまかせ！の一場面〕