



サイバーニュース

R 5 年 第 3 号
奈良県警察本部
サイバー犯罪対策課

情報セキュリティ10大脅威 2023発表！

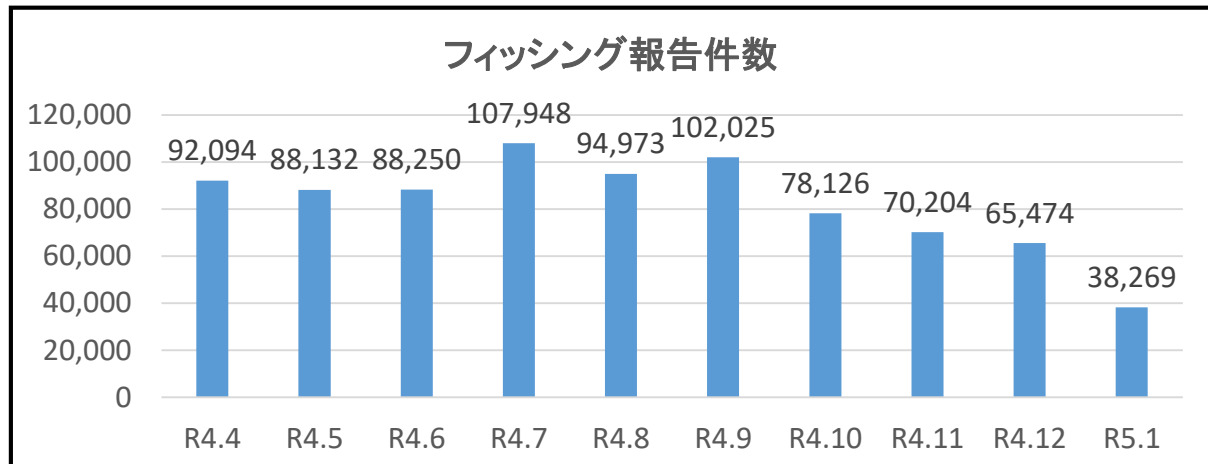
昨年順位	個人	順位	組織	昨年順位
1位	フィッシングによる個人情報等の詐取	1位	ランサムウェアによる被害	1位
2位	ネット上の誹謗・中傷・デマ	2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3位	標的型攻撃による機密情報の窃取	2位
4位	クレジットカード情報の不正利用	4位	内部不正による情報漏えい	5位
5位	スマホ決済の不正利用	5位	テレワーク等のニューノーマルな働き方を狙った攻撃	4位

【参考】独立行政法人 情報処理推進機構「情報セキュリティ10大脅威2023」 <https://www.ipa.go.jp/security/vuln/10threats2023.html>



「個人」「組織」の第1位はどちらも去年と変わらない結果となりました。ちなみに、個人第1位の「フィッシング…」は2年連続、組織第1位の「ランサムウェア…」は3年連続で脅威の1位となっています！

続いて昨年度中、フィッシング対策協議会宛によせられたフィッシングの報告件数を見てみましょう



【参考】フィッシング対策協議会「2023/01 フィッシング報告状況」 <https://www.antiphishing.jp/report/monthly/202301.html>

昨年は、7月～9月に「クレジットカードの利用確認を装うフィッシング」の報告件数が急増しました！

最近では、誘導先のURLをQRコードにしてメールに埋め込んだフィッシングメールの報告件数が増えています。みなさんご注意ください！



例えば・・・

奈良県警察HP
<https://www.police.pref.nara.jp>

QRコード
を作成



QRコード
を添付

フィッシングメール



Check



- SMSやメールに記載されたURLにはアクセスしない！
- 個人情報及びクレジットカード情報（口座情報）は容易に入力しない！