

情報セキュリティ白書
10大脅威

2020年(個人)

- 1位 スマホ決済の不正利用
～スマホ決済サービス利用時は二要素認証等のセキュリティ機能を有効に～
- 2位 フィッシングによる個人情報の詐取
～フィッシングの件数は増加傾向、世界的なイベントに便乗したフィッシング詐欺にも注意～
- 3位 クレジットカード情報の不正利用
～ショッピングサイトでのクレジットカード情報の詐取被害が拡大～
- 4位 インターネットバンキングの不正利用
～フィッシングによる不正送金の被害が急増～
- 5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
～金銭を要求する脅迫・詐欺メールは無視を～
- 6位 不正アプリによるスマートフォン利用者への被害
～インストールしているのは本当に正規のアプリ？～
- 7位 ネット上の誹謗・中傷・デマ
～安易な拡散により、他者も自身も不幸に～
- 8位 インターネット上のサービスへの不正ログイン
～パスワードリスト攻撃による不正ログインが横行～
- 9位 偽警告によるインターネット詐欺
～落ち着いて！あの手この手の騙しの警告画面～
- 10位 インターネット上のサービスからの個人情報の窃取
～会員サイトやショッピングサイトから情報流出するおそれ～

犯罪グループ・犯罪者
→ 個人(スマホ決済サービス利用者)、組織(サービス事業者・サービス利用店舗・クレジットカード会社)

<攻撃手口>アカウントの乗っ取り、スマホ決済サービスの不備の悪用

<対策/対応>被害の予防、被害の早期検知、被害を受けた後の対応

犯罪グループ・犯罪者
→ 個人(インターネット利用者)、組織(インターネット利用者)

<攻撃手口>有名企業を騙るメールを不特定多数に送信、ワンタイムパスワード等も入力させて詐取

<対策/対応>被害の予防(被害に備えた対策含む)、被害の早期検知、被害を受けた後の対応

犯罪グループ・犯罪者
→ 個人(クレジットカード利用者)、組織(サービス事業者、クレジットカード会社)

<攻撃手口>フィッシング詐欺、正規の決済画面を改ざんし入力情報を詐取、不正に取得したアカウントでなりすまし、ウイルス感染

<対策/対応>被害の予防、被害の早期検知、被害を受けた後の対応

犯罪グループ・犯罪者
→ 個人(インターネットバンキング利用者)、組織(インターネットバンキング利用者)、組織(金融機関)

<攻撃手口>フィッシング詐欺、ウイルス感染

<対策/対応>被害の予防(被害に備えた対策含む)、被害の早期検知、被害を受けた後の対応

犯罪グループ
→ 個人(インターネット利用者)

<攻撃手口>セクストーション(性的脅迫)、不正アクセスしているように見せかける、電話窓口への誘導

<対策/対応>被害の予防(被害に備えた対策含む)、被害を受けた後の対応

犯罪グループ・犯罪者
→ 個人(スマートフォン利用者)

<攻撃手口>公式マーケットに不正アプリを紛れ込ませる、メールやSMS等を利用して不正アプリのダウンロードサイトへ誘導する

<対策/対応>被害の予防、被害を受けた後の対応

情報モラル、情報リテラシーが低い人・悪意を持っている人
→ 個人、組織(教育機関、公共機関、企業)

<要因>情報モラルや自己抑制力の欠如、個人が匿名で発信できる場の増加、情報の真偽を確認せずに拡散

<対策/対応>情報モラルや情報リテラシーの向上、法令遵守の意識の向上、誹謗・中傷や公序良俗に反する投稿をしない、冷静な対応と支援者への相談

犯罪グループ、犯罪者(愉快犯、スターカー等)
→ 個人(サービス利用者)、組織(サービス運営者)

<攻撃手口>パスワードリスト攻撃、パスワード推測攻撃、ウイルス感染

<対策/対応>被害の予防(被害に備えた対策含む)、被害の早期検知、被害を受けた後の対応

犯罪グループ
→ 個人(インターネット利用者等)

<攻撃手口>巧妙に細工が施された偽の警告画面、偽セキュリティソフトの購入を誘導、サポート契約詐欺、スマホアプリのインストールへ誘導

<対策/対応>被害の予防(被害に備えた対策含む)、被害を受けた後の対応

犯罪グループ
→ 個人(サービス利用者)、組織(サービス利用者)

<攻撃手口>サービスの脆弱性や設定不備を悪用、他のサービス等から窃取した認証情報を悪用

<対策/対応>情報モラルやリテラシーの向上、被害の早期検知、被害を受けた後の対応

- 2019年(個人)
- 2018年(個人)
- 2017年
- 2016年
- 2015年
- 2014年度
- 2013年度
- 2012年度