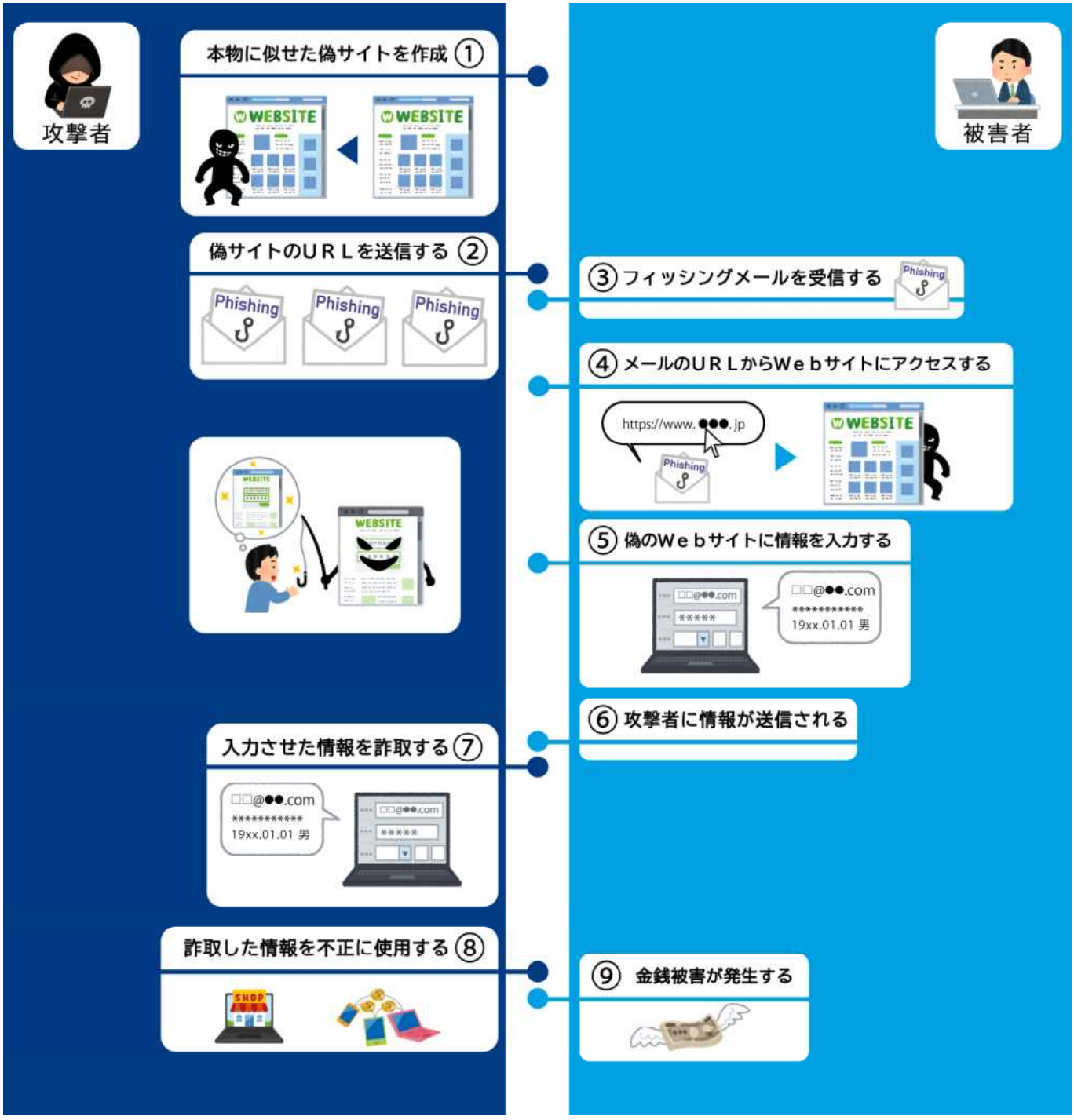
フィッシング対策について

フィッシングとは…

携帯電話会社、宅配業者、金融機関、官公庁等を装い、偽の電子メールやＳＭＳ（ショート・メッセージ・サービス）を送付し、偽サイト（フィッシングサイト）に誘導した上で、ＩＤやパスワード、クレジットカード番号等の情報を騙し取ったり、マルウェアに感染させたりする手口です。



出典：フィッシング対策協議会（https://www.antiphishing.jp/consumer/abt_phishing.html）

被害防止対策

○　電子メールやＳＭＳに記載されているリンクはクリックしない。
○　パソコンやスマートフォンのソフトウェアをアップデートする。
○　携帯電話会社などが提供するセキュリティサービスを導入する。
○　ＩＤパスワードの使いまわしはしない。
○　ワンタイムパスワードなどを利用する。

もしもフィッシングの被害に遭ってしまったら…

○　サービス提供会社に相談する。（被害の拡大防止、補償など）
○　パスワードを入力してしまった場合は変更する。
○　最寄りの警察署に通報・相談する。

警察署の一覧（https://www.police.pref.okinawa.jp/category/bunya/shokai/keisatsusho）

情報提供のお願い

フィッシングメールを受信した場合やフィッシングサイトを発見した場合は、
インターネット・ホットラインセンター（https://internethotline.jp）
へ通報をお願いします。

※　参考リンク

○　**フィッシング対策協議会**（https://www.antiphishing.jp/）
フィッシング対策協議会では、フィッシングに対する情報収集・提供、注意喚起などの活動を中心とした対策を推進しています。

○　**独立行政法人情報処理推進機構（ＩＰＡ）**（https://www.ipa.go.jp/）
ＩＰＡでは、情報セキュリティの最新情報や具体的な対策情報・対策手段など、幅広いセキュリティ関連情報を提供しています。