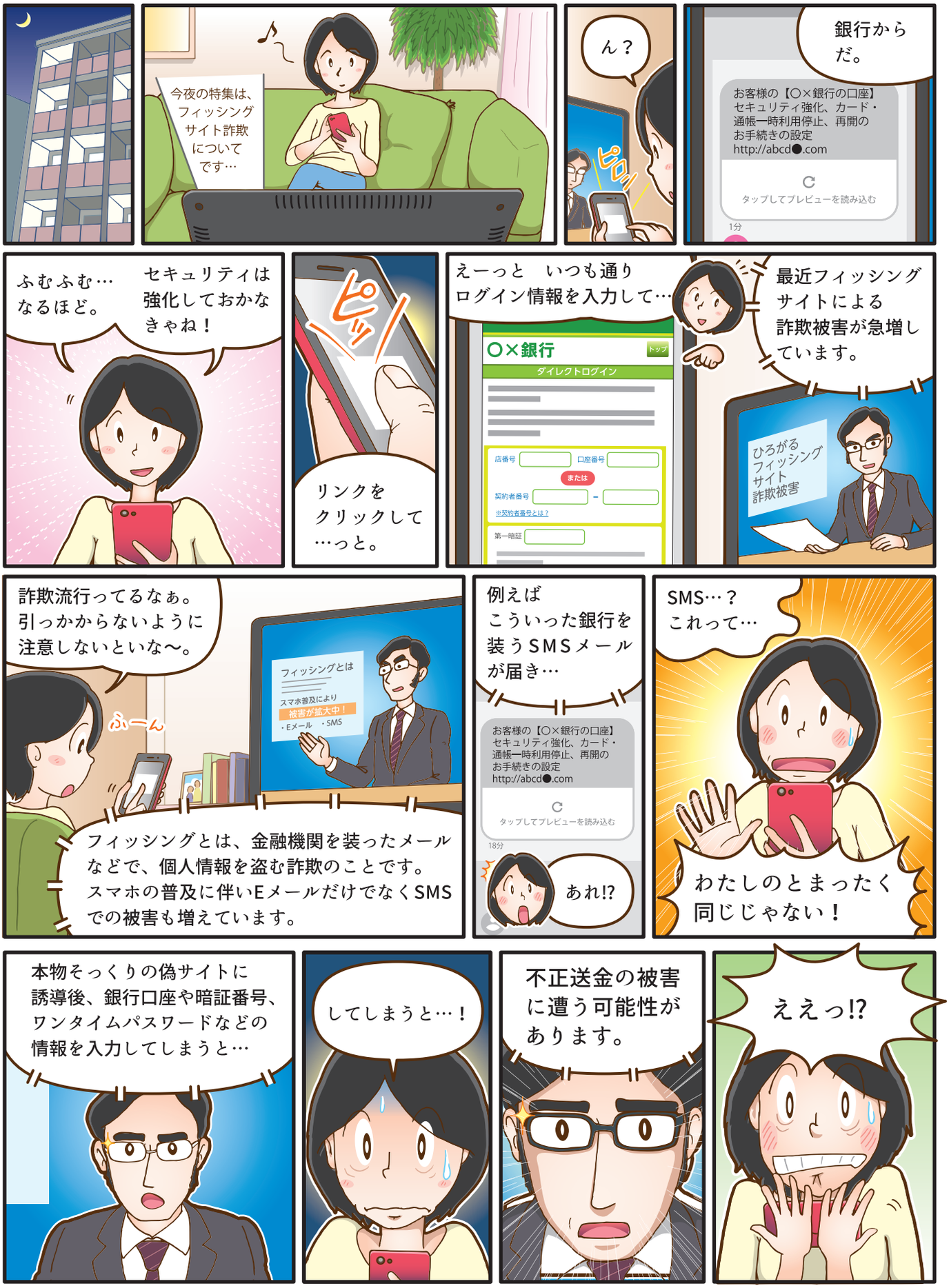
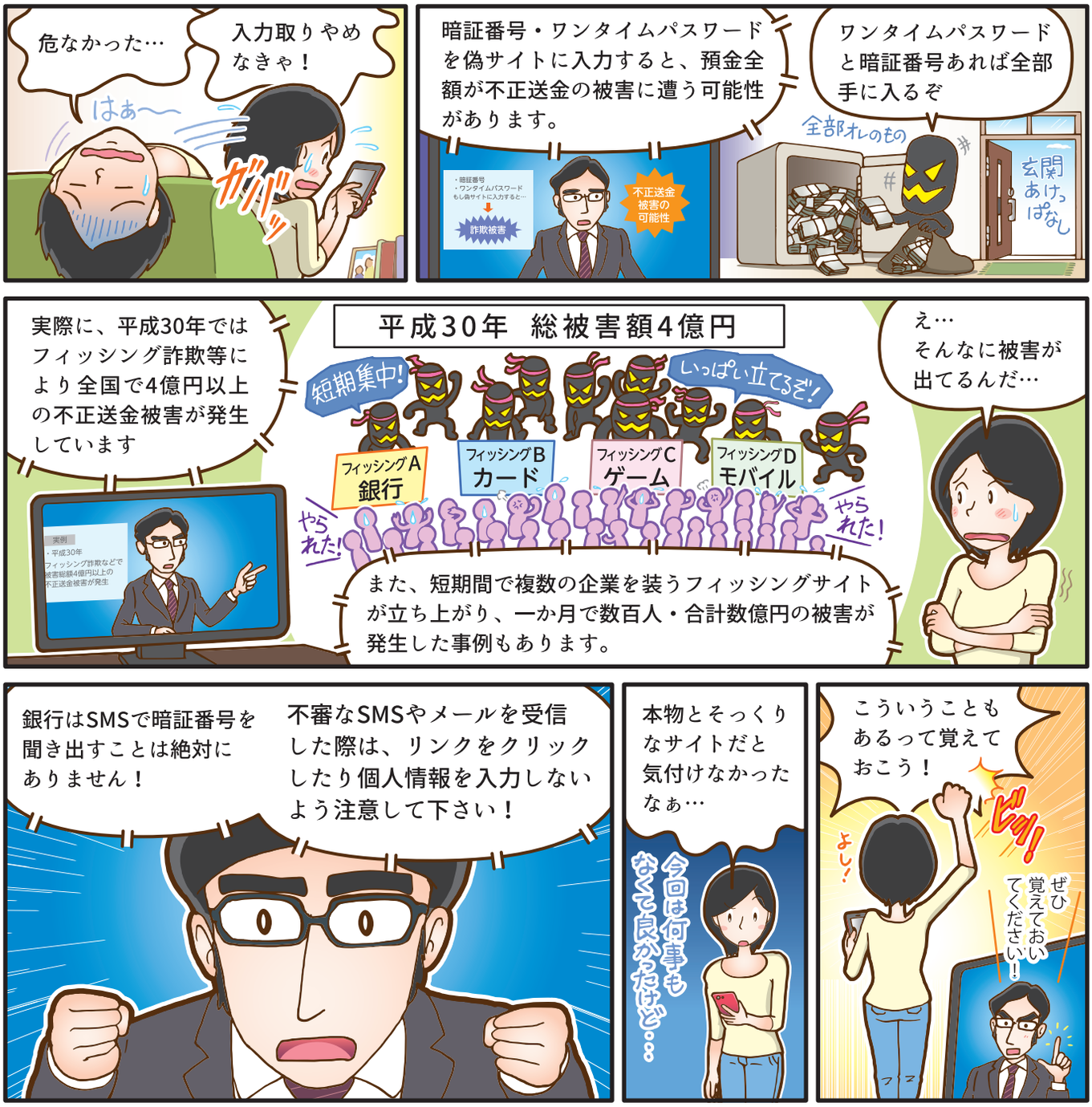
マンガでわかる

サイバーセキュリティ

フィッシングサイトには注意しよう





他の事例

- 銀行やクレジットカード会社、ショッピングサイト等を装う、様々なフィッシングサイトが立ち上がった事例がある
- フィッシングサイトを閲覧したユーザの端末に情報を盗取する機能を持ったウイルスをダウンロードさせる事例もある
- 個人だけでなく、法人もフィッシングの被害にあった事例がある (※1)
- フィッシング SMS には、次のような例もある：【●●銀行】お客様がご利用の口座が不正利用されている可能性があります。口座一時利用停止、再開手続き：https://●●.com

ここがポイント

- SMS やメールを受信した際は、リンクがフィッシングサイトの URL に偽装されている場合あるので、安易にクリックしないことが重要 (※2)
- 受信したSMSやメールが怪しいと感じた場合、同様のフィッシングメールがないか確認することが有効 (※3)
  また、公式サイトをブックマークに登録することも有効
- フィッシングサイトを検知・ブロックできる場合もあるので、ウイルス対策ソフトをインストールすることが有効
- 万が一不正送金等の被害に遭ってしまった場合は、速やかに電話受付窓口等に連絡することが重要

(※1) 警察庁広報資料によると、平成 30 年では個人で合計約 3 億 6400 万円、法人で合計約 4,000 万円の被害が発生しています。
(※2) 銀行等の一部の企業は、電子メールに電子署名を付与してメールを送っています。メールに正規の電子署名が付いてれば、正規のメールであることが確認できます。
(※3) フィッシング対策協議会の Web サイトでは、実際に確認されているフィッシングメールの一部が公開されています。