多要素認証(MFA)を破る攻撃と対策

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

米マイクロソフト社が大規模なフィッシング攻撃が展開されていると注意喚起
(2022/7/12)

- 原文）From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud

  https://www.microsoft.com/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

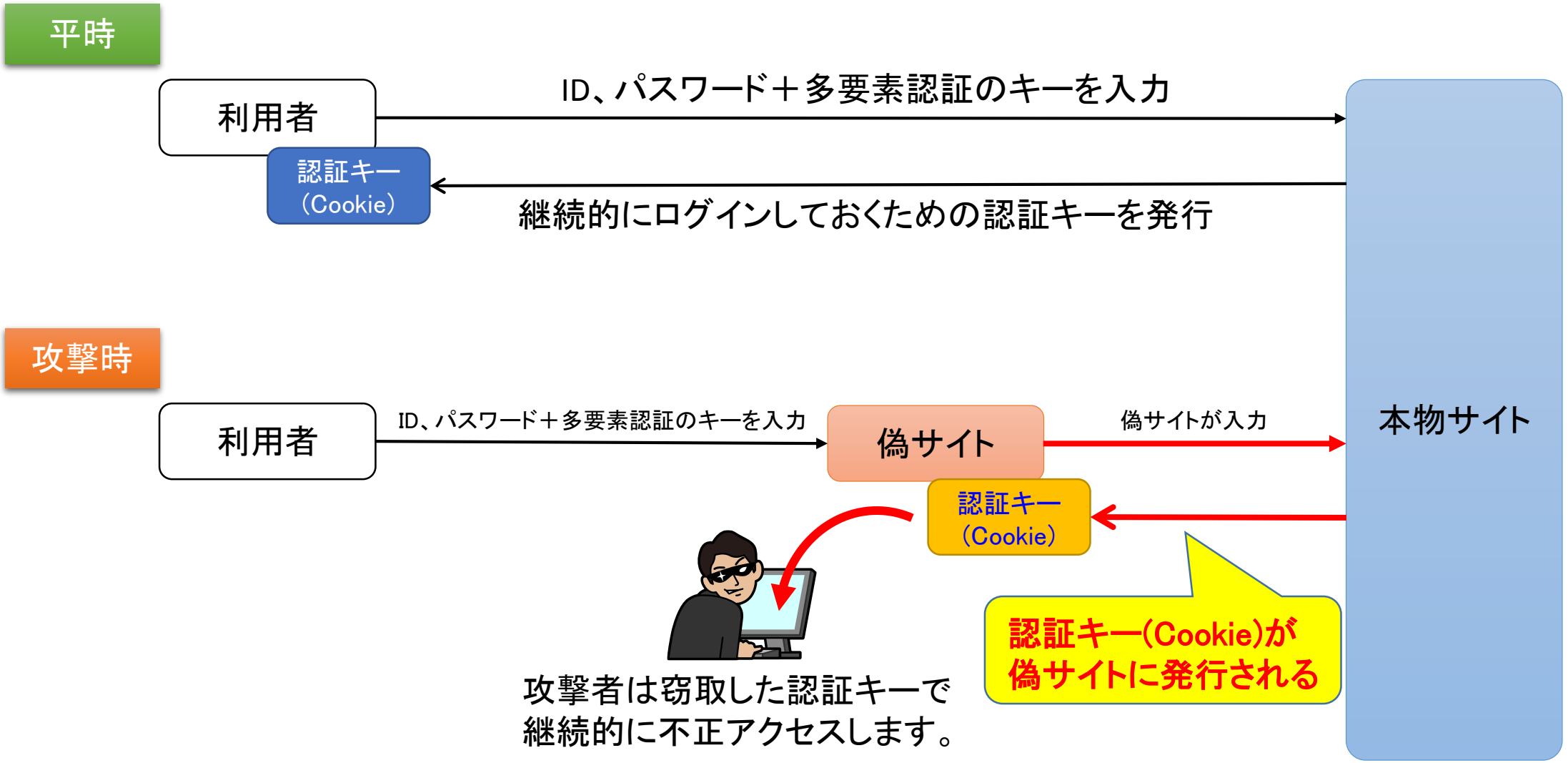
- 日本国内でも新聞、ウェブメディアで多数報道

- 攻撃は、Webサイトと利用者端末の間に攻撃者が割り込み、偽サイト(フィッシングサイト)を設置して利用者を騙してIDやパスワードを窃取する従来からある手法であるが、今回の攻撃では『本物サイトに継続的にログインできる認証キー(Cookie)が窃取されてしまう』点に注意が必要。

- 二要素認証はIDとパスワードが漏れても、ログインには別の(一時的な)キーを必要とする仕組みだが、今回の手口の場合、一度でも偽サイトで自分のID/PWおよび二要素認証のキーを入力してしまうと、攻撃者がそれらの認証情報無しに窃取したCookieを使って継続的に不正ログインが可能。
  - **まさに「多要素認証」を破る攻撃**

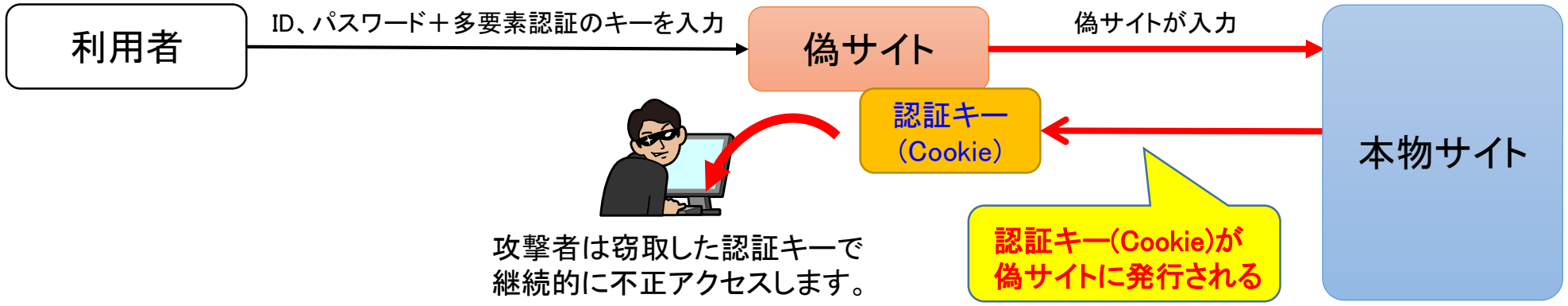
多要素認証(MFA)を破る攻撃と対策

- 攻撃イメージは以下の通りです。



多要素認証(MFA)を破る攻撃と対策

- 対策は利用者側が偽サイトにアクセスしないようにするものと、認証方式を高度化して攻撃者からのアクセスを防ぐものが考えられます。



■偽サイトにアクセスさせない対策
（偽サイトに気づく or アクセスをブロック）
① SSO製品を利用する
② フィッシング対策製品を利用する

■偽サイトからアクセスを受けない対策
（認証方式の高度化）
① 証明書ベースの認証(MS推奨策)
② FIDO認証(MS推奨策)
③ リスクベース認証
④ アクセス元Global IPアドレス認証

セコムトラストシステムズ株式会社

www.secomtrust.net

お問い合わせは

ソリューション営業本部
03-5931-5210

受付時間：9～12時、13～18時
土・日・祝日・年末年始（12/30～1/3）は除きます。