

# 応用情報技術者試験

---

## テクノロジ系Ⅵ

---

3-5-4

# 情報セキュリティ対策

優先度： 低

# 目次

- 情報セキュリティ対策の種類
- 個人情報保護対策
- 典型的なサイバー攻撃
- セキュリティ対策

## 要約

情報セキュリティというと、技術面での対策を思い浮かべがちであるが、それだけでは十分でない。人的セキュリティ、物理的セキュリティの対策を行い、総合的に情報資産を守っていく必要がある。また、実際のセキュリティ攻撃を知ることで、守る方法が見えてくる

# 情報セキュリティ対策 の種類



# 技術的セキュリティ対策



- 暗号化, 認証, アクセス制御など
  - \* **入口対策** : 攻撃を防いで内部に侵入させない
  - \* **出口対策** : 侵入された後にその被害を外部に広げない
    - ▶ **多層防御** : 1つの対策だけではなく複数の対策を組み合わせる

# 人的セキュリティ対策



- 教育, 訓練や契約などにより, 人に対して行うセキュリティ対策
  - \* 組織における不正行為は, **内部関係者**によって行われることが多い
- IPAでは, 「**組織における内部不正防止ガイドライン**」を公表し, 内部不正を防止するための証拠確保などの具体的な方法を示している

# 物理的セキュリティ対策



- 建物や設備などを対象
  - \* 入退出管理やバックアップセンタ設置
- **クリアスクリーン**：離席時にはPCの画面を見えないようにする
- **クリアデスク**：帰宅時に机の上のものをPCなども含めて全てロッカーにしまって施錠する

# 個人情報保護対策



# 個人情報保護対策

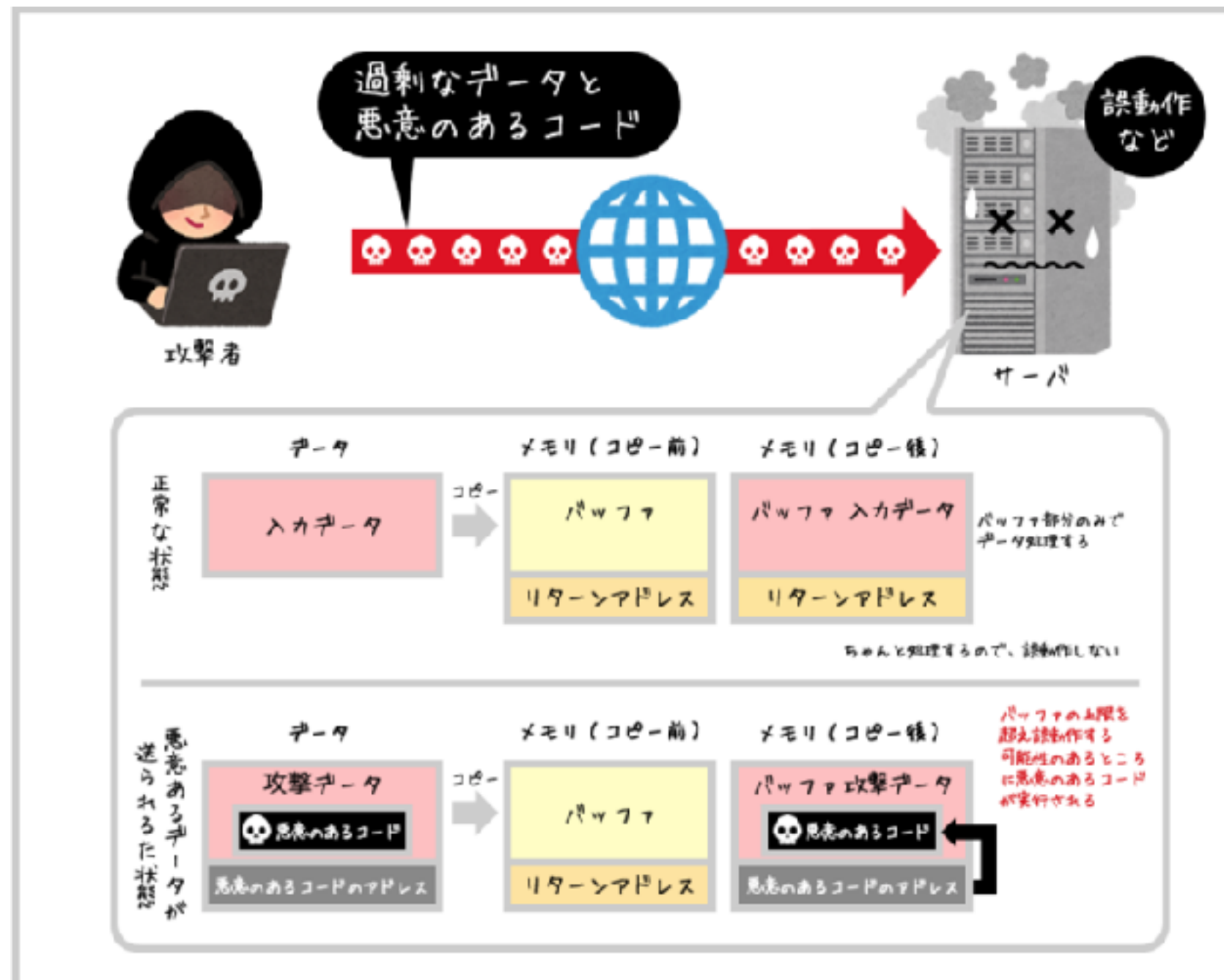
- 個人情報：それ単体もしくは組み合わせることによって個人を特定できる情報
  - \* 氏名，住所，メールアドレスなど
- 個人情報の保護に関する法律(**個人情報保護法**)では，主に以下のことが定められている
  - \* 個人情報の**利用目的の特定**と公表
  - \* 個人情報の適正な**管理**
  - \* 本人の権利(開示・訂正・苦情など)への対応

# 典型的なサイバー攻撃



# バッファオーバーフロー攻撃

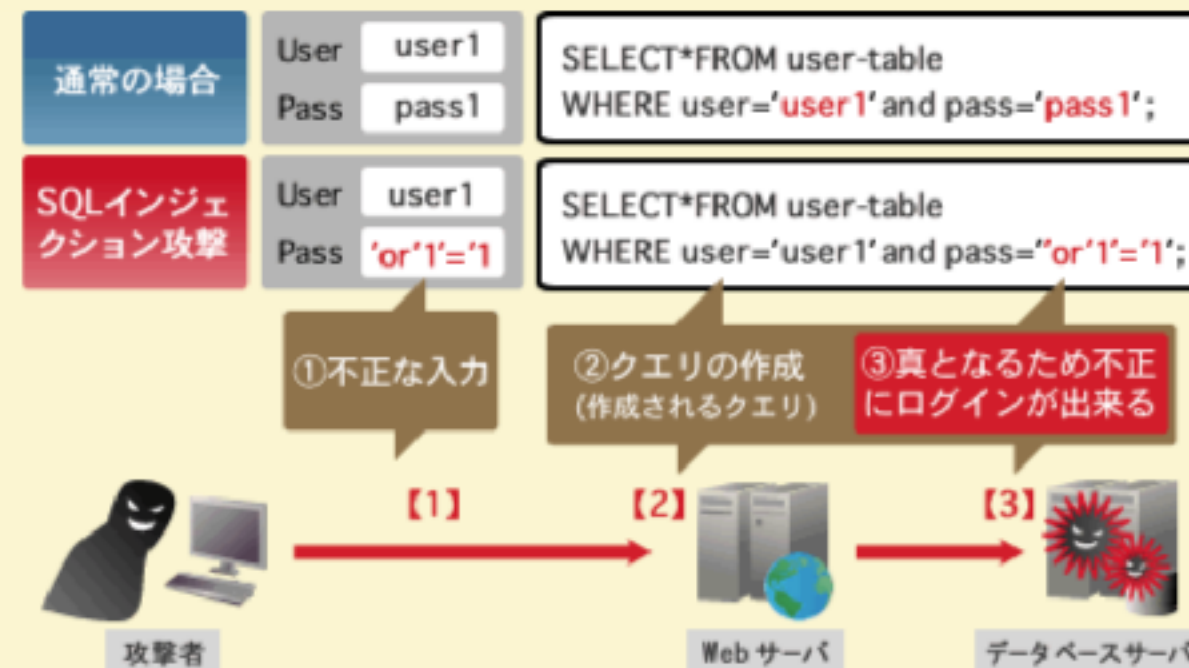
- バッファの長さを超えるデータを送り込むことによって、バッファの後ろにある領域を破壊して動作不能にし、プログラムを破壊



# SQLインジェクション

- 不正なSQLを投入することで、通常はアクセスできないデータにアクセスしたり更新したりする攻撃
  - \* 対策としては制御文字を置き換えるエスケープ処理や、プレースホルダを利用するバインド機能など

## ◆ SQL インジェクションの例

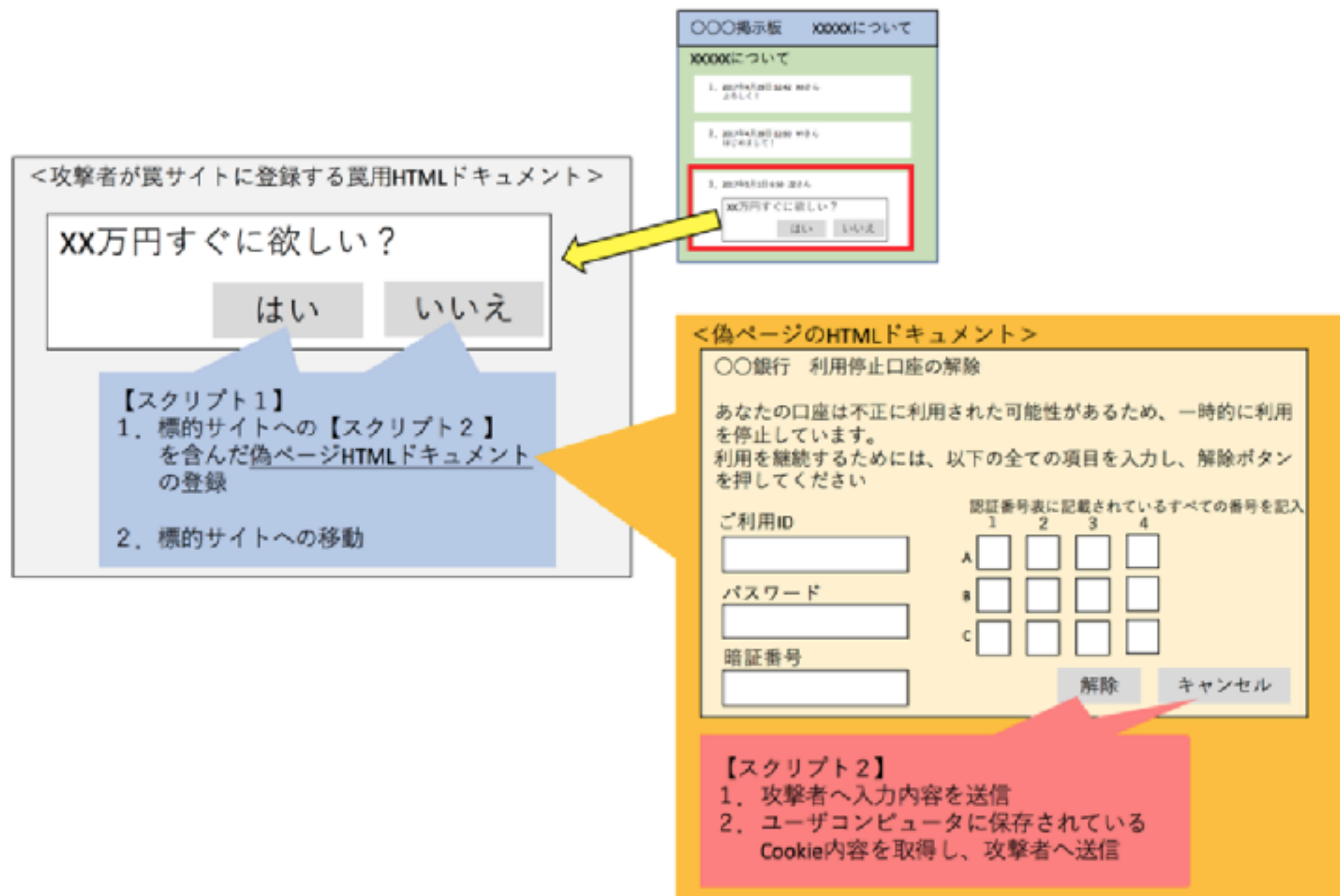


上の図は、不正な文字列により認証を回避するSQLインジェクションの攻撃の例です。データベースのSQLクエリのパラメータとなる入力に、攻撃者は不正な文字列を入力して【1】、不正なSQLクエリを実行させます【2】【3】。

不正アクセスによるWebサイトからの情報漏えい事件の原因は、その多くがSQLインジェクションによるものとなります。

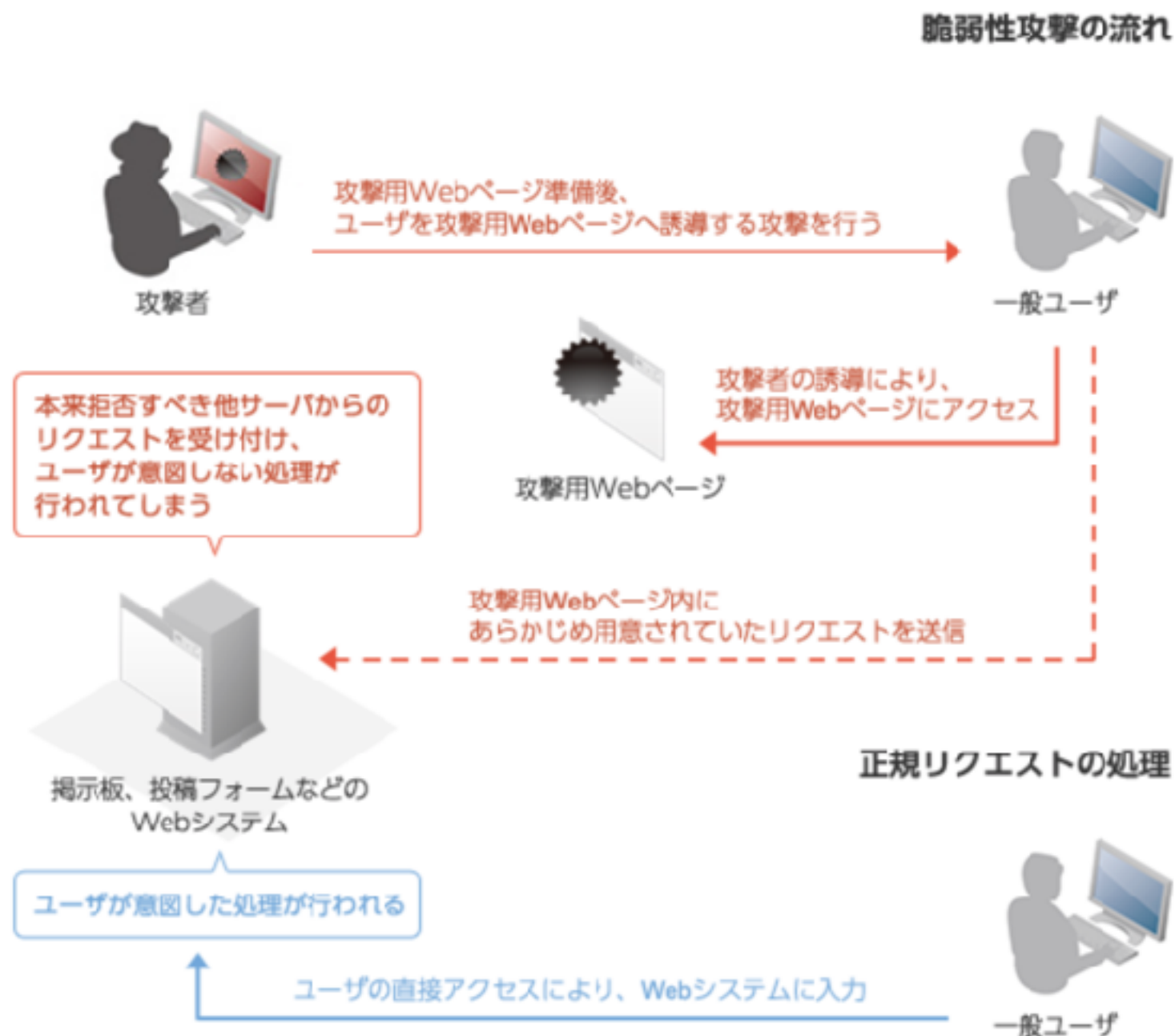
# クロスサイトスクリプティング攻撃

- 悪意のあるスクリプトを、標的サイトに埋め込む攻撃



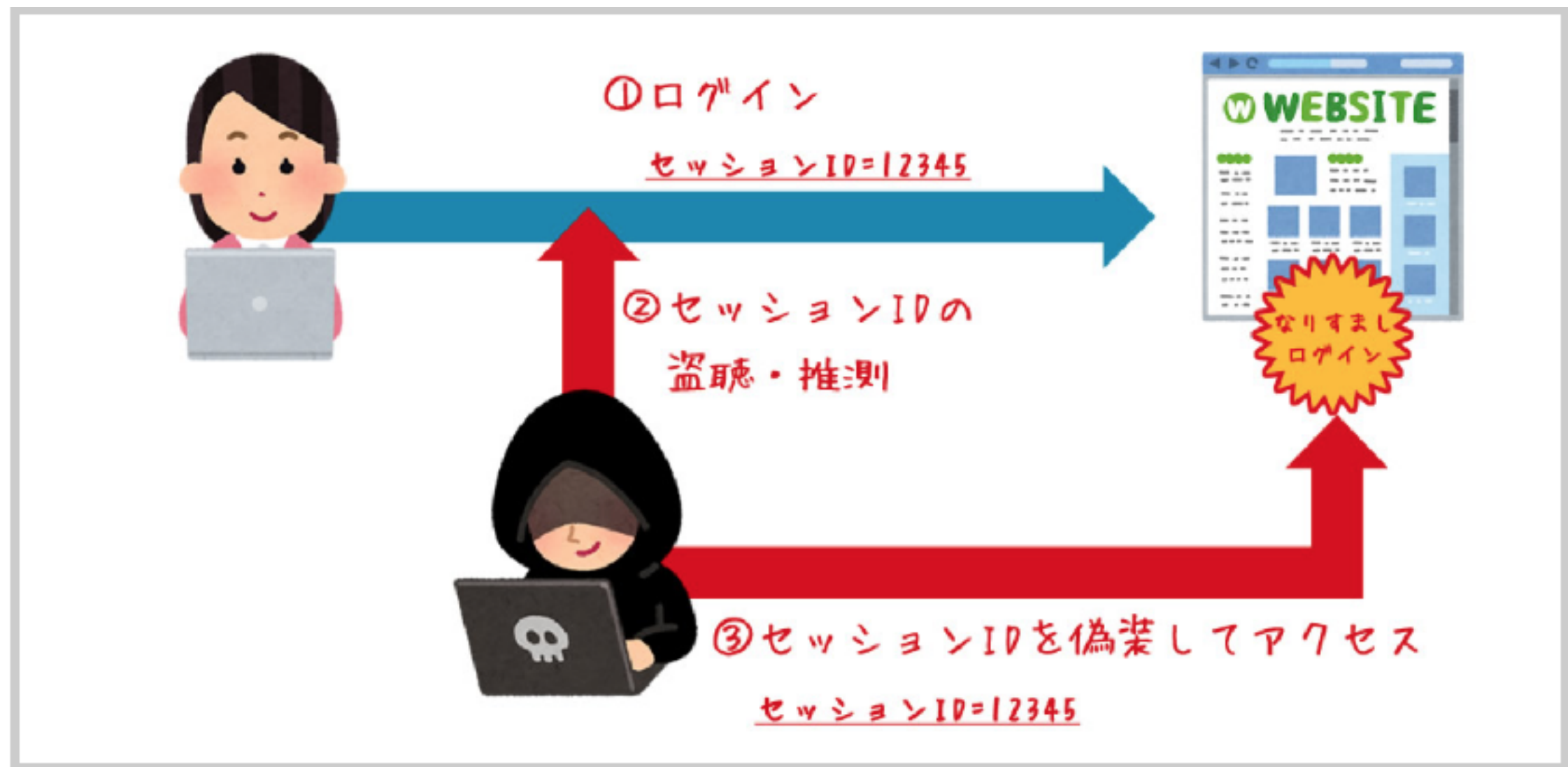
# クロスサイトリクエストフォージェリ攻撃(CSRF)

- Webサイトにログイン中のユーザのスク립トを操ること  
とで、Webサイトに被害を与える攻撃



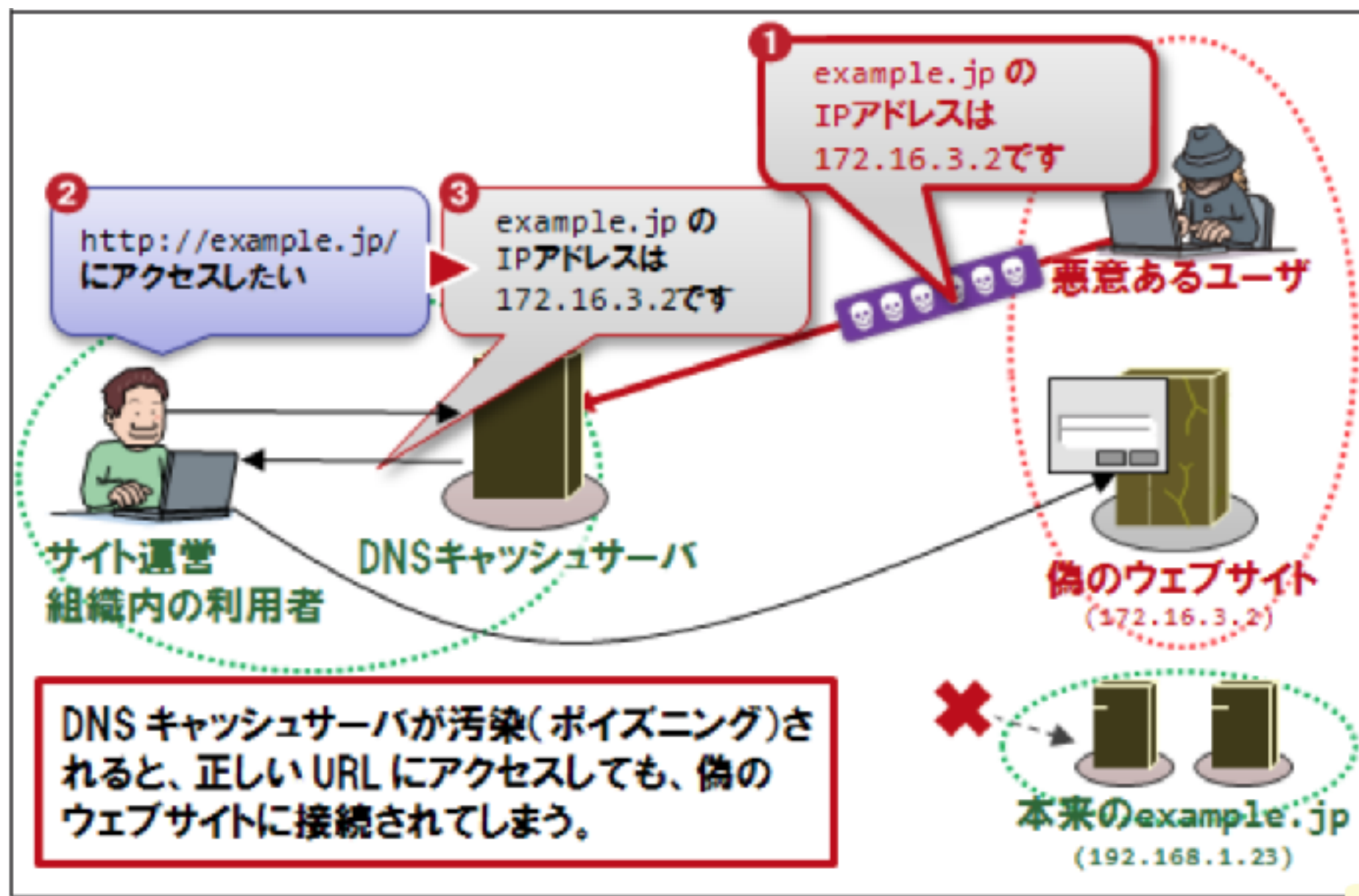
# セッションハイジャック

- セッションIDやクッキーを盗むことで、別のユーザになりすましてアクセスするという不正アクセスの手口



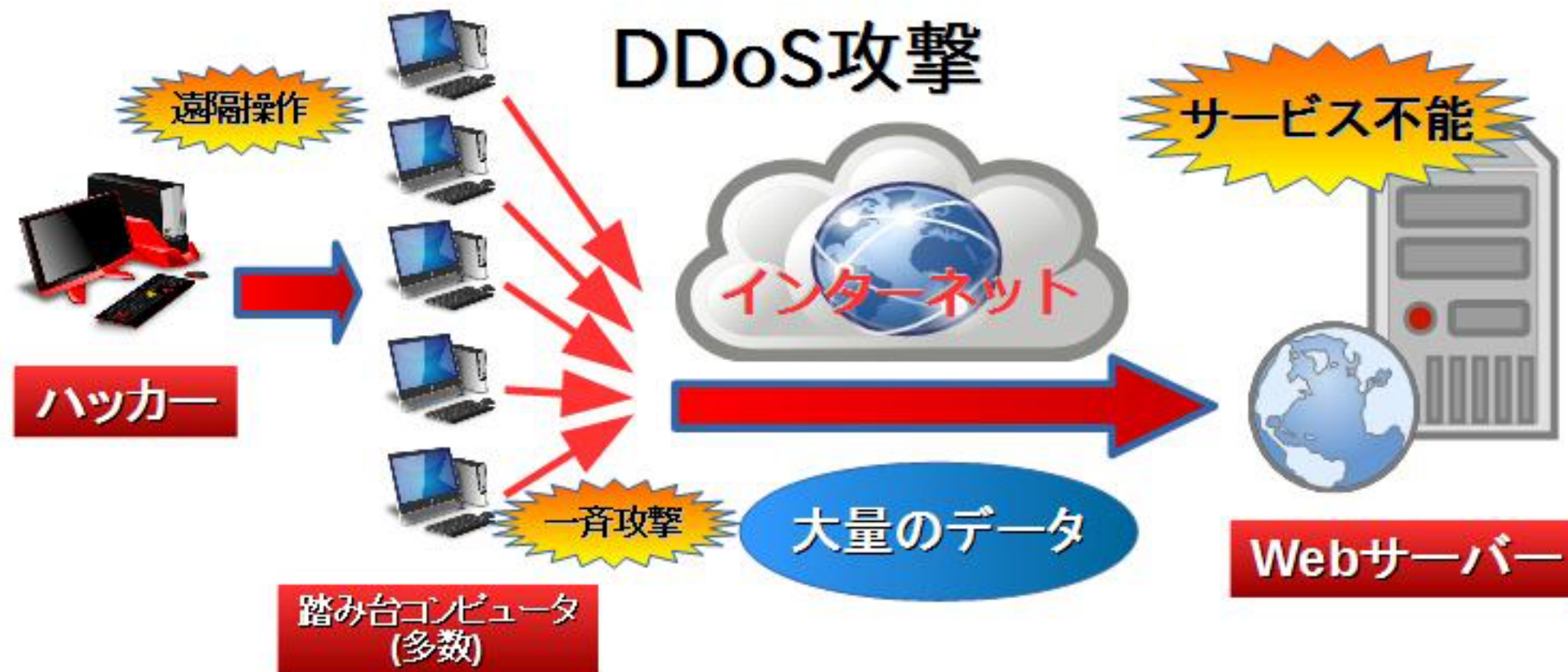
# DNSキャッシュポイズニング攻撃

- DNSのキャッシュに不正な情報を注入することで、不正なサイトへのアクセスを誘導する攻撃



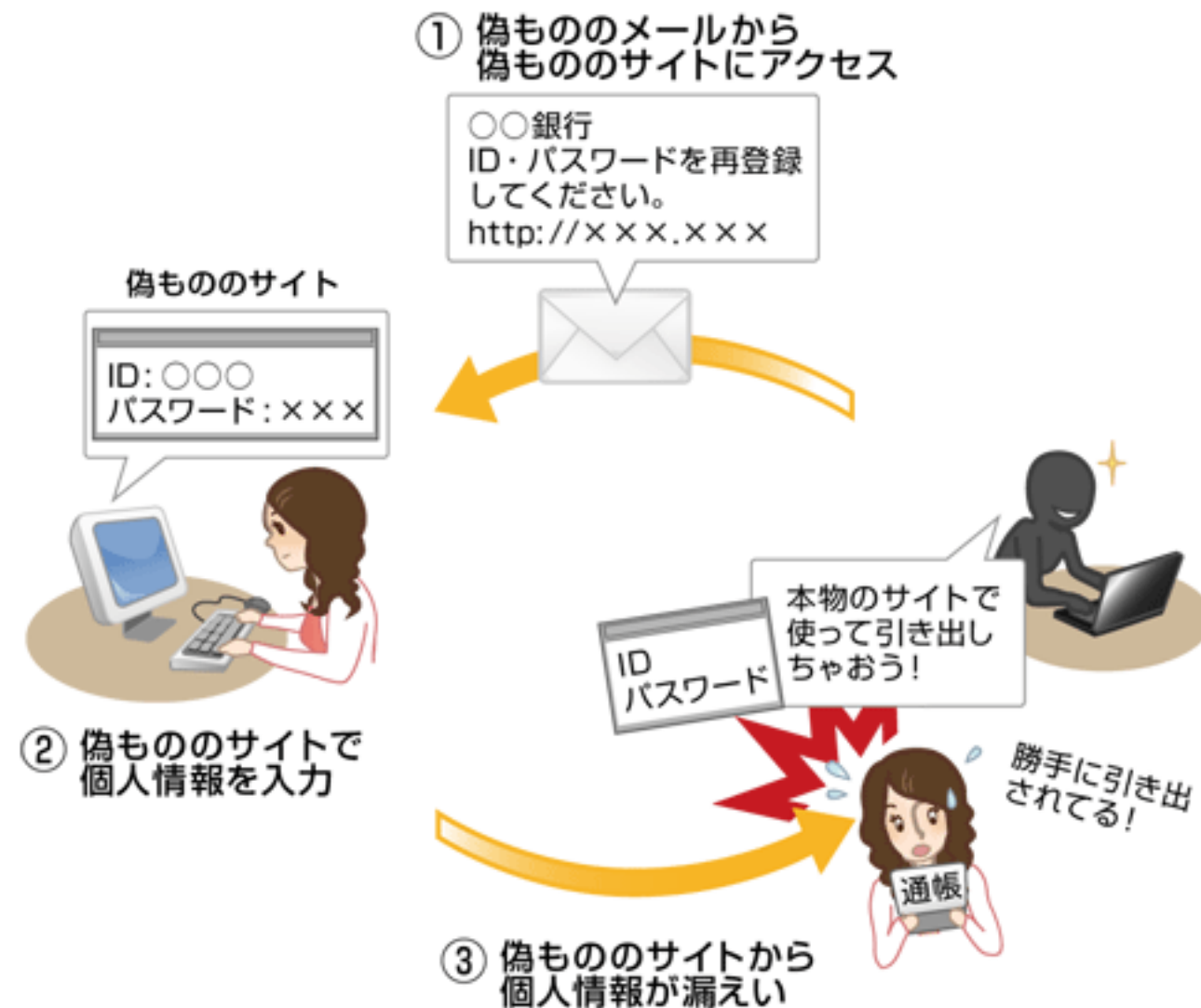
# DoS(Denial of Service)攻撃

- サーバなどのネットワーク機器に大量のパケットを送るなどしてサービスの提供を不能にする攻撃
  - \* DDoS(Distributed Dos)：踏み台と呼ばれる複数のコンピュータから一斉に攻撃を行う



# フィッシング

- 信頼できる機関を装い、偽のWebサイトに誘導する攻撃



# パスワードクラック

- パスワードを不正に取得する攻撃

- \* ブрутフォースアタック：適当な文字列を組み合わせで力任せに攻撃を繰り返す
- \* スニффイング：パスワードを盗聴する



# ランサムウェア

- コンピュータをロックしたり重要なファイルを暗号化したりしてシステムへのアクセスを制限し、その制限を解除するための身代金を要求するマルウェア



こんな時あなたは どう  
しますか？

# ケース 1

# こんなメールが送られてきました

Owner様

あなたのApple IDが他人に利用されていることが確認されたため、ロックします。

あなたのアカウントを守るために、セキュリティの設定を再設定していただく必要がございます。

以下のURLより設定をお願いいたします。

<http://www.apple.com/jp/>

このメールはご本人様であることを確認するために送信されています。

万が一このメールに心当たりがない場合は、[iforgot.apple.com](http://iforgot.apple.com) にアクセスしてパスワードを変更することをおすすめします。

[Apple ID: セキュリティと Apple ID](#) を参考にしてください。

今後ともよろしくをお願いいたします。

Apple



[Apple ID の概要](#) ・ [販売条件](#) ・ [プライバシーポリシー](#)

Copyright © 2018 iTunatuna K.K.

[All rights reserved](#)

# そのメール、本物ですか？

Owner様

名前は正しい??

あなたのApple IDが他人に利用されていることが確認されたため、ロックします。

アドレスは本物??

あなたのアカウントを守るために、セキュリティの設定を再設定していただく必要がございます。

以下のURLより設定をお願いいたします。

<http://www.apple.com/jp/>

Appleなのにhttps://やないやん

このメールはご本人様であることを確認するために送信されています。

万が一このメールに心当たりがない場合は、[iforgot.apple.com](https://iforgot.apple.com) にアクセスしてパスワードを変更することをおすすめします。

ID: セキュリティと Apple ID を参考にしてください。

今後ともよろしくお願いいたします。

Apple

心当たりがなかったら押しちゃだめ



[Apple ID の概要](#) ・ [販売条件](#) ・ [プライバシーポリシー](#)

Copyright © 2018 iTunatuna K.K.

[All rights reserved](#)

tunatunaやん!!

# ケース 2

# パズドラをインストールしよう



パズル&ドラゴンズ

★★★★☆ 1.82万

入手



パズドラレーダー

★★★★☆ 3,070

入手



パズドラチャレンジ

★★★★☆ 479

入手



パズル&ドラゴンズ

★★★★★ 6

入手

あれ、ここにもパズドラあるやん！  
評価高いしこっちにしようかな！

# だめです



# セキュリティ対策

# セキュリティ対策

- アカウント管理

- \* ユーザとアカウントを1対1で対応させ、ユーザに必要な際上限のアクセス権を与える

- ログ管理

- \* ログを収集し、その完全性を管理する。 **デジタルフォレンジック** **ス**を意識し、証拠となるようにログを残すことが大切

- 入退出管理

- \* ICカードなどを用いて、入退出を管理・記録する

# セキュリティ対策

- アクセス制御

- \* ファイアウォールなどを用いてアクセスを制御する

- マルウェア対策

- \* ウイルス対策ソフトを全PCに導入し、ウイルス定義ファイルを最新版にアップデートするなど、マルウェアに感染しない対策を行う。また、**検疫ネットワーク**を用いて、ウイルス対策を行っていないPCはネットワークに接続させないという手法も有効

- 不正アクセス対策

- \* IDS/IPSなどの侵入検知/防止の対策を行い、不正アクセスに対処する

ハニーポット



# セキュリティ対策

- 情報漏洩対策

- \* データを暗号化したり，物理的に持ち出さないようにしたりして，情報が漏洩しないようにする

- 無線LANセキュリティ

- \* WEPやWPAで暗号化，IEEE802.1Xで認証などを行うことで，無線LANのセキュリティを確保する

- 携帯端末のセキュリティ

- \* スマートフォンやタブレットPCなどの携帯端末は，PCと同様の機能を持っている

- ペネトレーションテスト

- \* サーバやファイアウォールなどのシステムに対して擬似体験を行うテスト