情報セキュリティ

第5回： 小テストとネットワーク上の各種攻撃の紹介

授業計画

① ガイダンス
② インターネット上の脅威について
③ 攻撃について
④ コンピュータウイルス（マルウェア）について
⑤小テスト，ネットワーク上の各種攻撃の紹介
⑥ 攻撃の技術
⑦ 情報・ネットワーク技術の基礎
⑧ ネットワークセキュリティに関する技術と方法
⑨ 暗号の基礎
⑩ 小テスト，セキュリティ技術と方法に対する確認
⑪ 対処法１（システムリスク）
⑫ 対処法２（ソーシャルリスク：SNS）
⑬ 対処法３（ソーシャルリスク：インターネット・スマホゲーム）
⑭ 対処法に関する小テスト
⑮ 全体のまとめ

本日の講義内容

1．［小テスト］
2．ネットワーク上の各種攻撃の紹介

小テスト実施要領

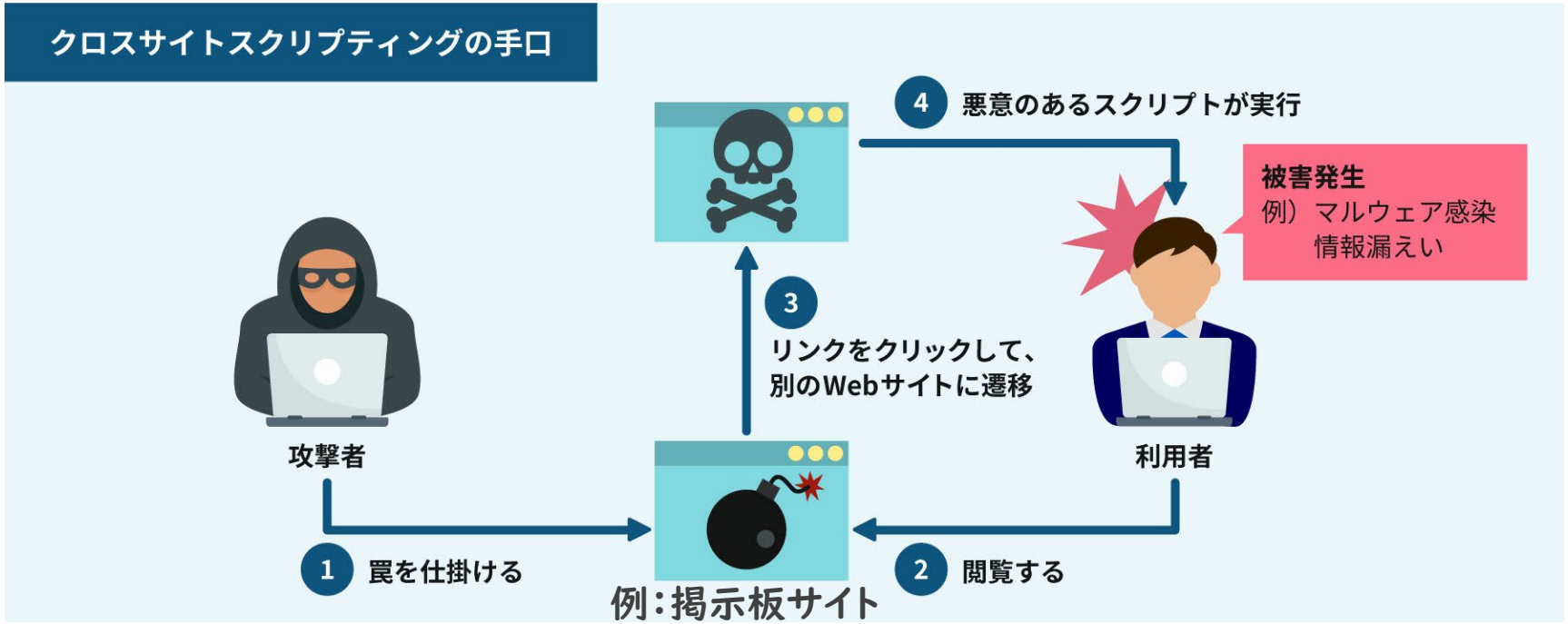
- 学籍番号および氏名を忘れずに記入してください．
- 回答の際は、テキストや講義資料などを参照してかまいません．
- 必ずご自分で解答してください（他の受講者との相談は不可とします）．
- 問題および解答用紙は、試験終了後すべて回収します（採点後に返却予定です）．なお，メモを取ったり、写真を撮ったりすることは認められません．

2. ネットワーク上の各種攻撃の紹介

2. 1 Webブラウザを狙った攻撃 （代表例）

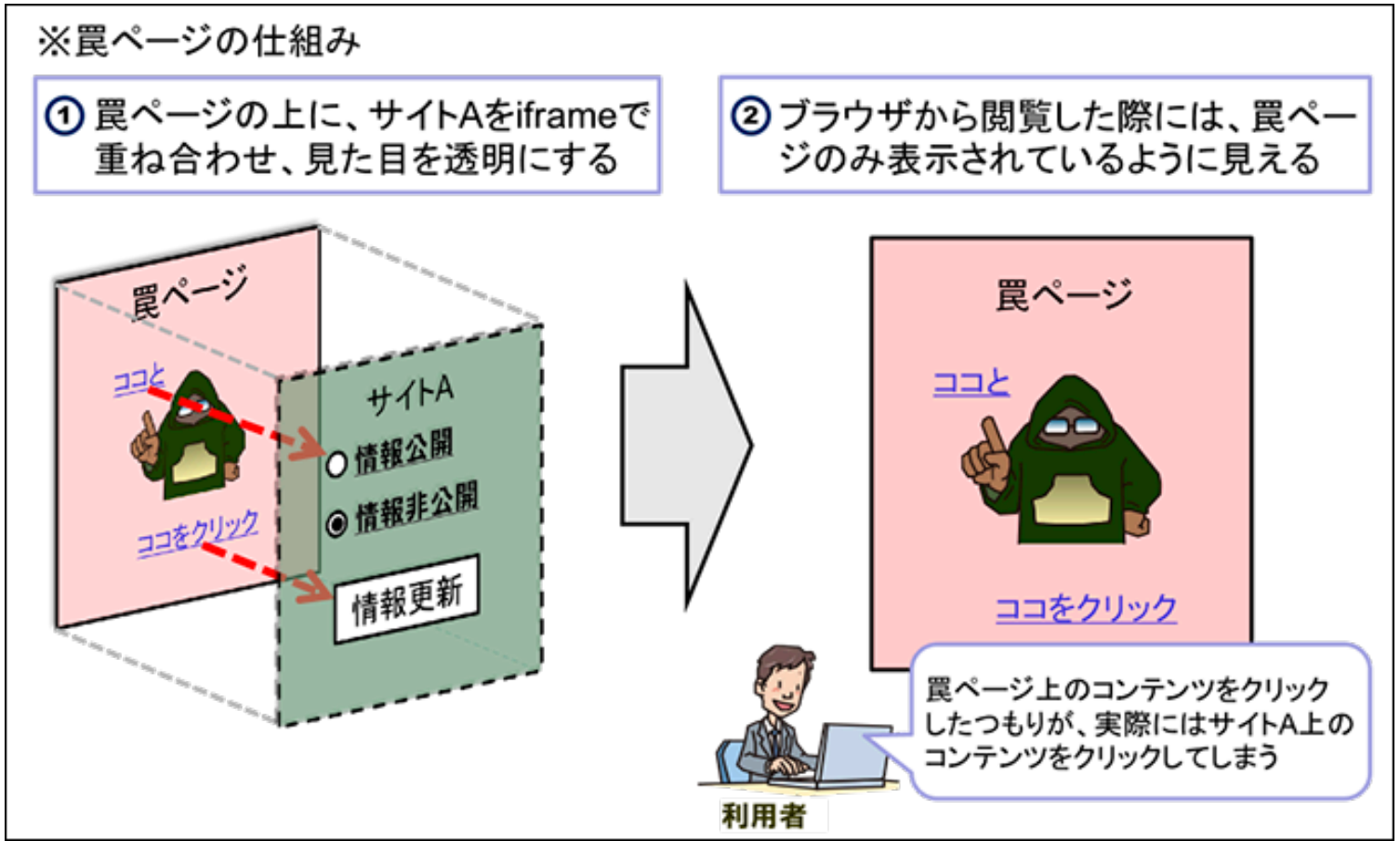
（1）XSS（クロス・サイト・スクリプティング）

- 攻撃者は入力フォームにスクリプト付のリンクを入力し罠を仕掛ける.
- 利用者が該当Webページにアクセスする.
- リンクをクリックしてスクリプトが実行され，別のWebサイトに遷移（クロスする）して悪意のある内容（スクリプト）が実行される.



(2) クリックジャッキング

- 利用者が罠ページに誘導され，クリックする．
- 利用者が罠ページのコンテンツをクリックしたつもりが，実際にはサイトAのコンテンツをクリックしてしまう．
- 利用者の意図しない処理を実行してしまう．

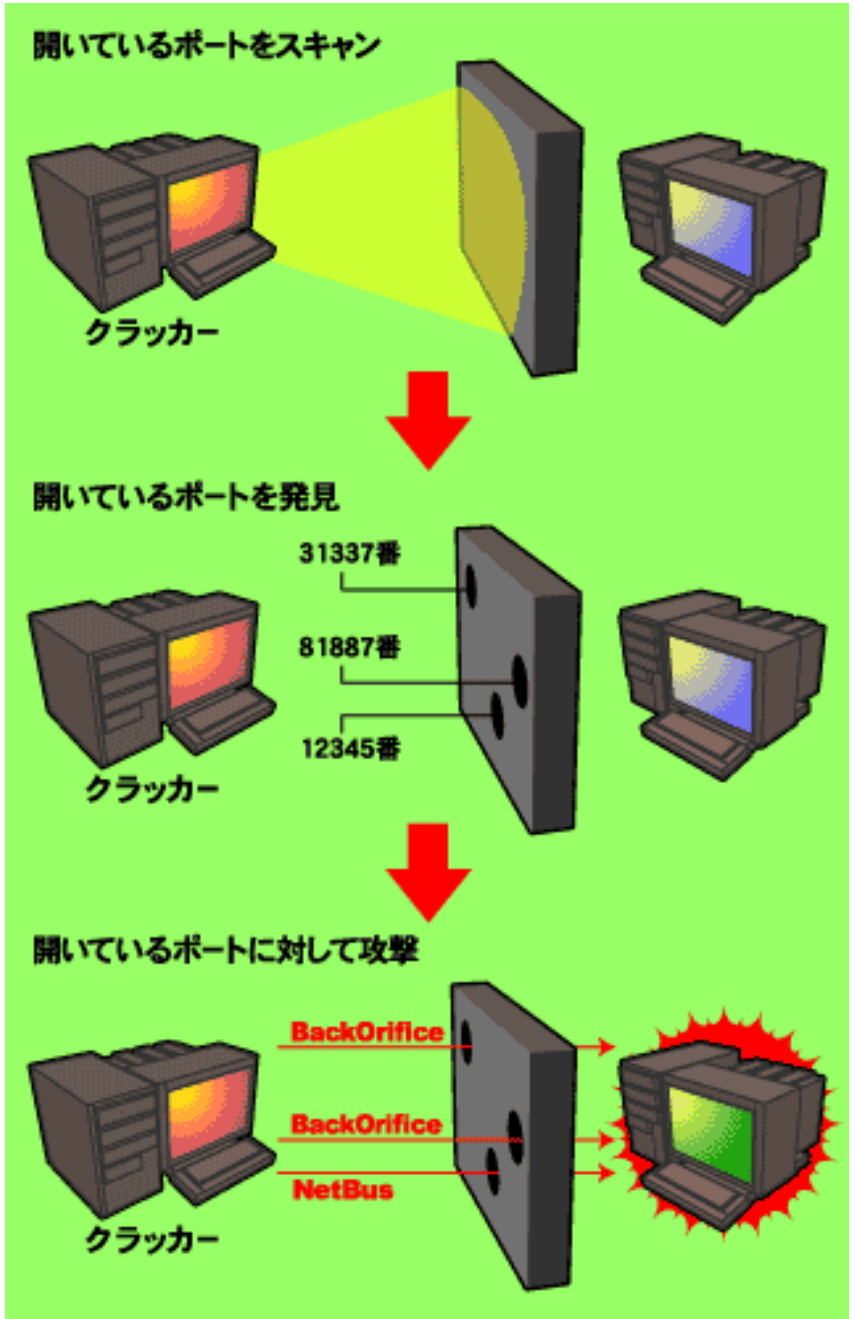


2.2 サーバを狙った攻撃 （代表例）

（1）ポートスキャン

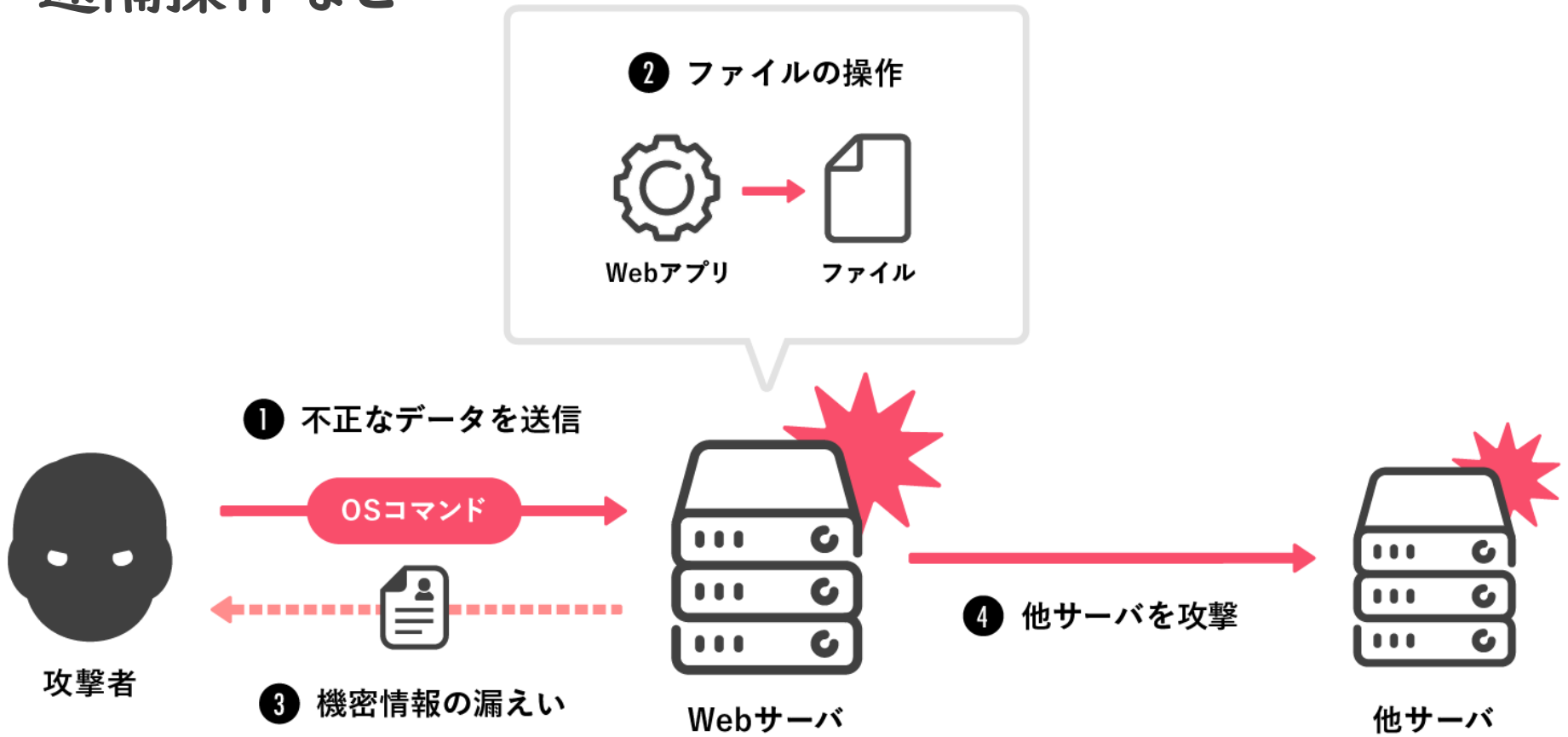
- 稼働しているサービスは？
- OSの種類は？
- ソフトウェアのバージョンは？
- 脆弱性はあるか？

⇒ どんな攻撃をすればよいかが具体的に定まってきます．
そして，攻撃を開始．．．



（2）OSコマンド・インジェクション

- データ改ざん
- 情報漏えい
- 踏み台として他サイトを攻撃
- 遠隔操作など



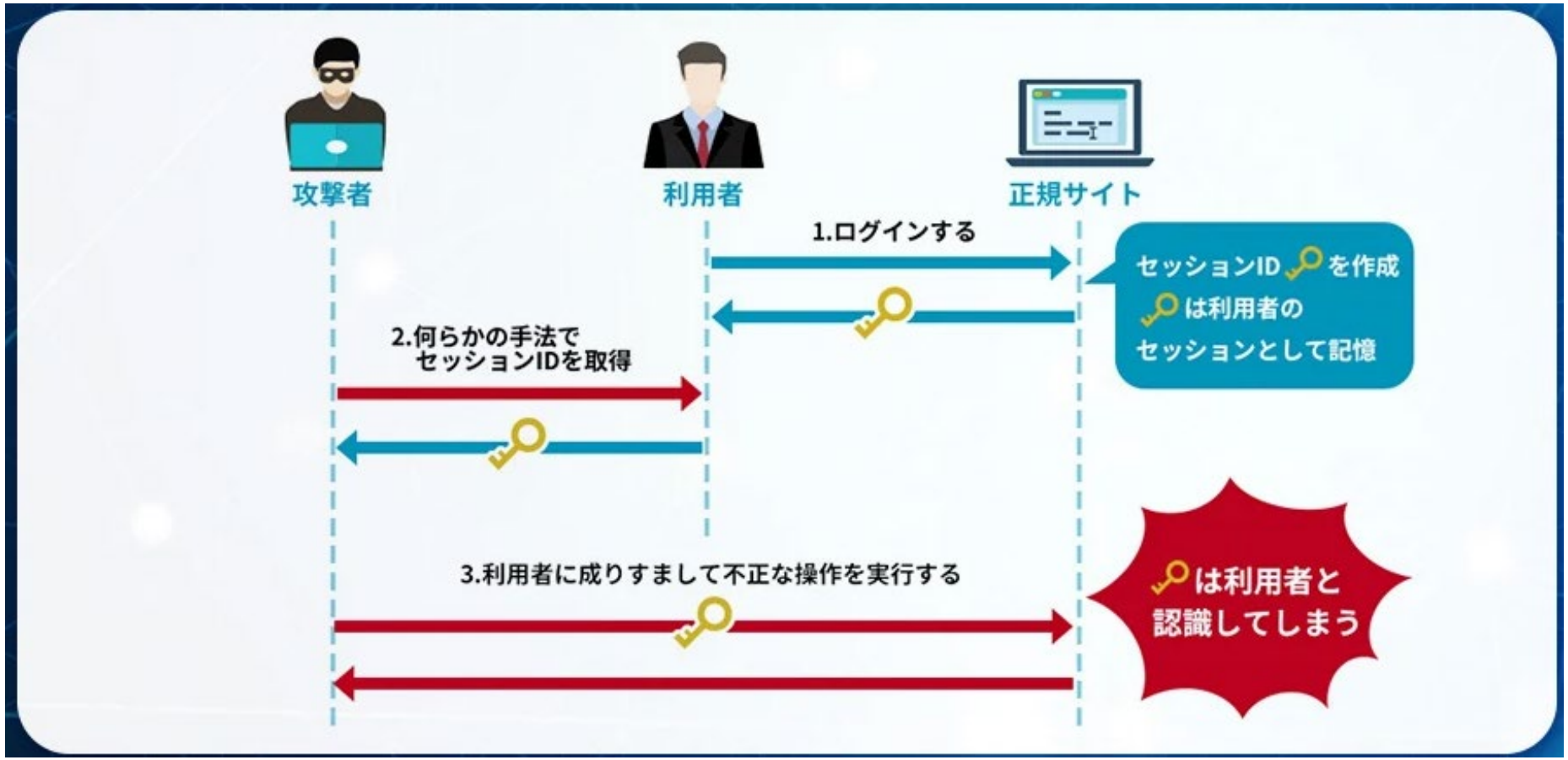
（3）SQLインジェクション

- 入力フォームに不正な命令を含んだSQL文を注入
- Webアプリケーションを通じてデータベースを不正に操作

2.3 乗っ取り／なりすまし （代表例）

（1）セッション・ハイジャック

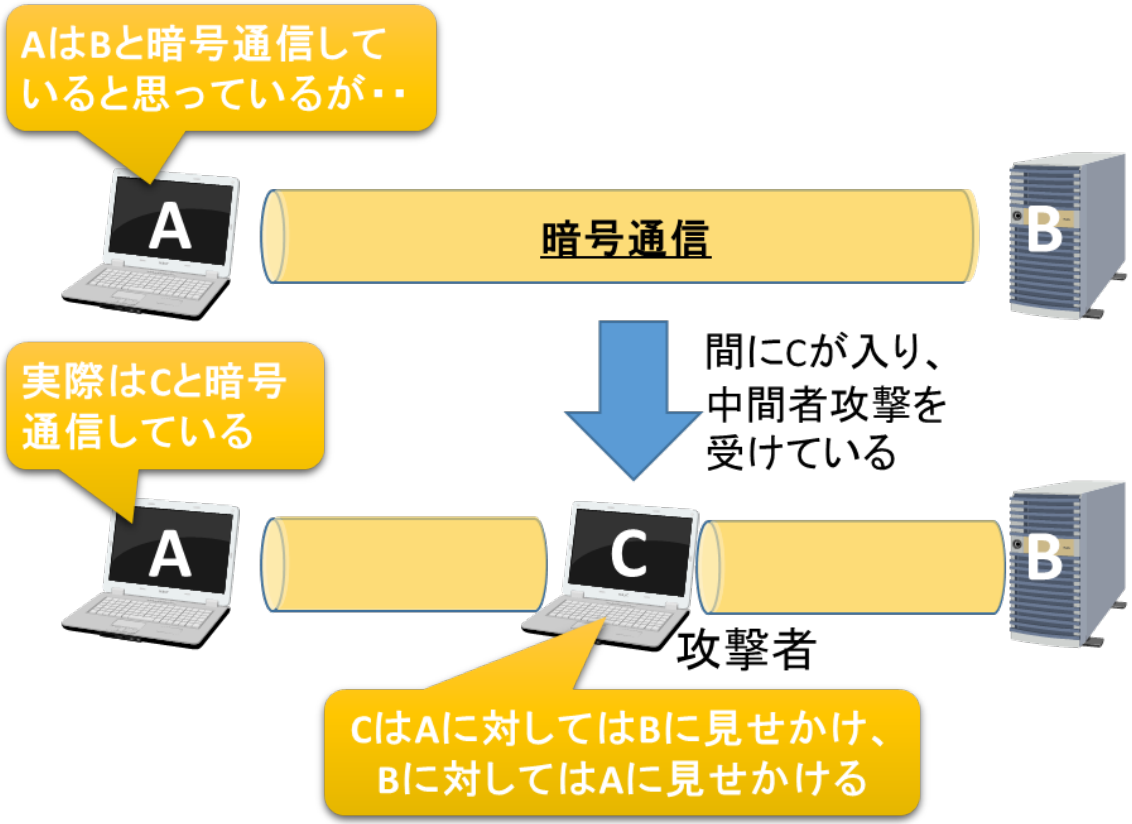
- 盗聴によるセッションIDの不正取得
- セッションIDの推測または固定化



（2）中間者（Man-in-the-Middle）攻撃

- 通信同士の間に攻撃者が割って入り，通信を中継することで盗聴やデータの改ざんを行う．
- 通信を暗号化しても意味がなく，情報を奪われてしまうことになる．

中間者攻撃の例



2.4 負荷をかける攻撃 （代表例）

～ DoS（Denial of Service）攻撃

- Ping Flood攻撃
- UDP Flood攻撃
- SYN/FIN Flood攻撃
- Connection Flood攻撃
- HTTP Get Flood攻撃