

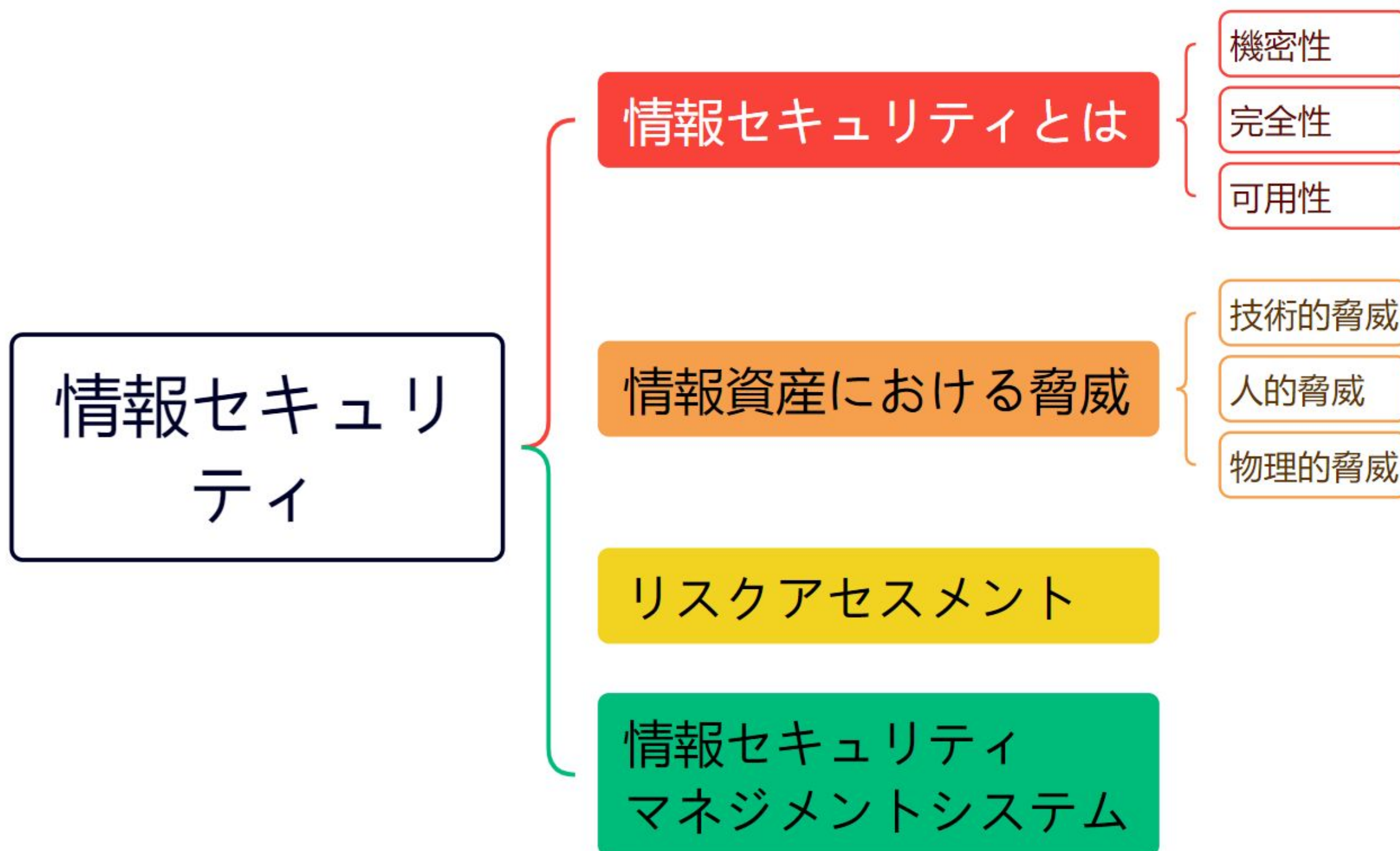


IT日本語2

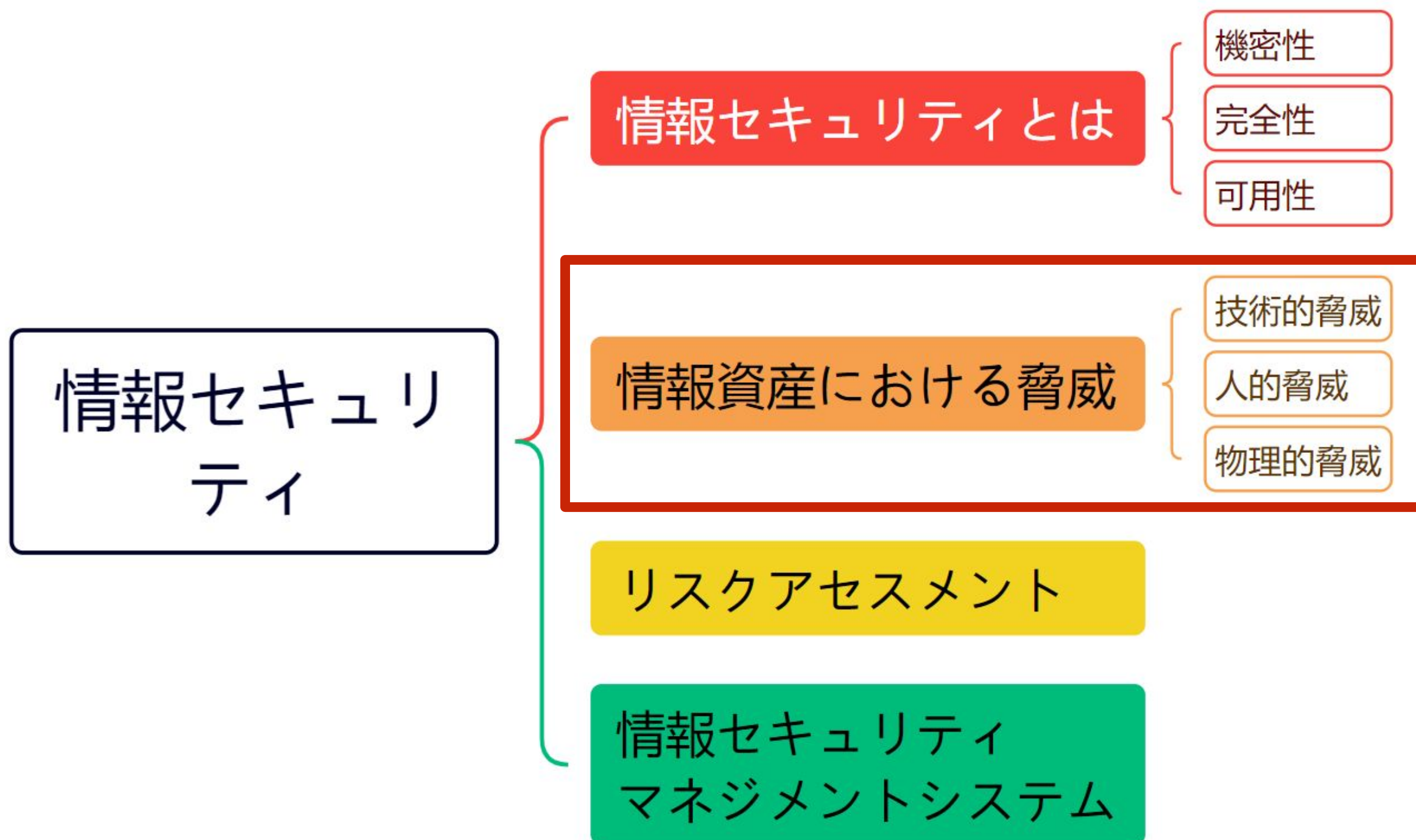
9.1 情報セキュリティ(2) 事前学習


情報セキュリティ

情報セキュリティの全体内容



情報セキュリティの全体内容





情報資産における脅威 技術的脅威

情報資産における脅威

情報セキュリティ対策を行うには、まず情報資産が、どのような脅威にさらされているのかをきちんと把握する必要があります。

情報資産をとりまく脅威には、技術的脅威、人的脅威、物理的脅威の3種類があります。

- Để thực hiện các biện pháp bảo mật thông tin, trước tiên cần phải nắm bắt chính xác tài sản thông tin đứng trước các mối đe dọa nào. Trong các mối đe dọa xoay quanh tài sản thông tin, có 3 loại là: mối đe dọa kỹ thuật, mối đe dọa con người và mối đe dọa vật lý.

技術的脅威

コンピュータ技術を使った脅威を技術的脅威といいます。
技術的脅威は、不正アクセスやコンピュータウイルスをはじめ、
さまざまな攻撃の手口があります。

- Các mối đe dọa sử dụng kỹ thuật máy tính gọi là mối đe dọa kỹ thuật. Mỗi đe dọa kỹ thuật bao gồm nhiều thủ thuật tấn công khác nhau, tiêu biểu là truy cập trái phép, vi rút máy tính.

技術的脅威

- パスワードリスト攻撃
- フィッシング
- DNS キャッシュポイズニング
- SEOポイズニング
- SQL インジェクション
- DoS 攻撃
- ディレクトリトラバーサル攻撃
- Web ビーコン
- スパイウェア
- ブルートフォース攻撃

-
- Tấn công danh sách mật khẩu
 - Phishing (Tấn công giả mạo)
 - DNS Cache Poisoning
 - SEO Poisoning
 - SQL Injection
 - Tấn công DoS
 - Tấn công Directory Traversal
 - Web beacon
 - Spyware
 - Tấn công Brute-force

パスワードリスト攻撃

あるインターネットサービスの利用者が、別のサービスでも同じIDやパスワードを使い回す可能性が高いことに着目し、攻撃者が別の脆弱なサービスから入手したIDとパスワードのリストを用いて、本人になりすまして不正アクセスを試みる攻撃をパスワードリスト攻撃といいます。

→ **Tấn công danh sách mật khẩu** là cuộc tấn công nhắm vào việc người sử dụng dịch vụ Internet nào đó có khả năng cao sẽ sử dụng lại cùng một ID và mật khẩu cho các dịch vụ khác, kẻ tấn công sẽ sử dụng danh sách ID và mật khẩu thu được từ một dịch vụ để bị tấn công bất kỳ, mao danh người dùng, cố gắng truy cập bất hợp pháp.

フィッシング

銀行などを装った偽のWebサイトを作り、URLを載せた電子メールを送り、ユーザにアクセスさせて暗証番号やパスワードをだまし取ることをフィッシングといいます。

→ **Phishing** là việc tao một trang web giả, ngụy trang dưới dạng một ngân hàng, thực hiện gửi email chứa URL và cho phép người dùng truy cập, đánh lừa để lấy đi mã PIN hoặc mật khẩu.



DNSキャッシュポイズニング

PCが参照するDNSサーバに誤ったドメイン管理情報を覚え込ませて、偽のサーバに誘導する攻撃を**DNSキャッシュポイズニング**と
いいます。

→ **DNS Cache Poisoning** (Nhiễm độc bộ nhớ đệm DNS) là cuộc tấn công khiến máy chủ DNS mà PC tham chiếu sẽ ghi nhớ thông tin quản lý tên miền không chính xác, sau đó chuyển hướng đến một máy chủ giả mạo.

SEOポイズニング

検索サイトの検索結果の上位に、マルウェアなどを含んだ悪意のあるサイトが紛れ込むように細工する攻撃を**SEOポイズニング**といいます。事件やイベントなど、頻繁に検索されるキーワードの検索結果で上位に来るようWebサイトを細工し、アクセス数を増やすことで、被害を大きくします。

→ **SEO Poisoning** là cuộc tấn công mà (hacker) sẽ dùng thủ thuật nhỏ để một trang web ác ý chứa phần mềm độc hại sẽ bị lẫn vào trong các kết quả tìm kiếm hiển thị đầu tiên của một trang tìm kiếm. Bằng cách dùng thủ thuật lươn lẹo để trang web (độc hại) có xếp hạng cao trong kết quả tìm kiếm với các từ khóa được tìm kiếm thường xuyên như sự cố, sự kiện, làm tăng số lượng truy cập thì sẽ làm thiệt hại tăng lên.

SQLインジェクション

Web アプリケーションの入力フォームには、ログイン情報や注文情報といったWebサイトで指定される情報を利用者が入力します。
攻撃者は、本来入力されるはずのないデータベースの操作言語であるSQL文を入力欄に打ち込み送信することで、データベースを不正に操作してデータを改ざんしたり不正に情報を引き出そうとします。
この攻撃を**SQLインジェクション**といいます。

→ Trong các biểu mẫu nhập của ứng dụng web, người dùng nhập thông tin do trang web chỉ định như thông tin đăng nhập và thông tin đặt hàng. Kẻ tấn công cố gắng thao tác trái phép cơ sở dữ liệu, làm sai lệch dữ liệu hoặc trích xuất thông tin bất hợp pháp bằng cách nhập các câu lệnh SQL là ngôn ngữ vận hành của cơ sở dữ liệu, các câu lệnh này vốn dĩ không được phép nhập, vào các trường nhập liệu rồi gửi đi. Cuộc tấn công này được gọi là **SQL Injection**.

SQLインジェクション

この攻撃を防ぐためには、入力されたデータをチェックし、SQL文が入力されても実行されないように、文字を変換することで、無効化します。

- Để ngăn chặn cuộc tấn công này, chúng ta cần kiểm tra dữ liệu được nhập vào và vô hiệu hóa bằng cách chuyển đổi các ký tự để câu lệnh SQL sẽ không được thực thi ngay cả khi nó được nhập vào.

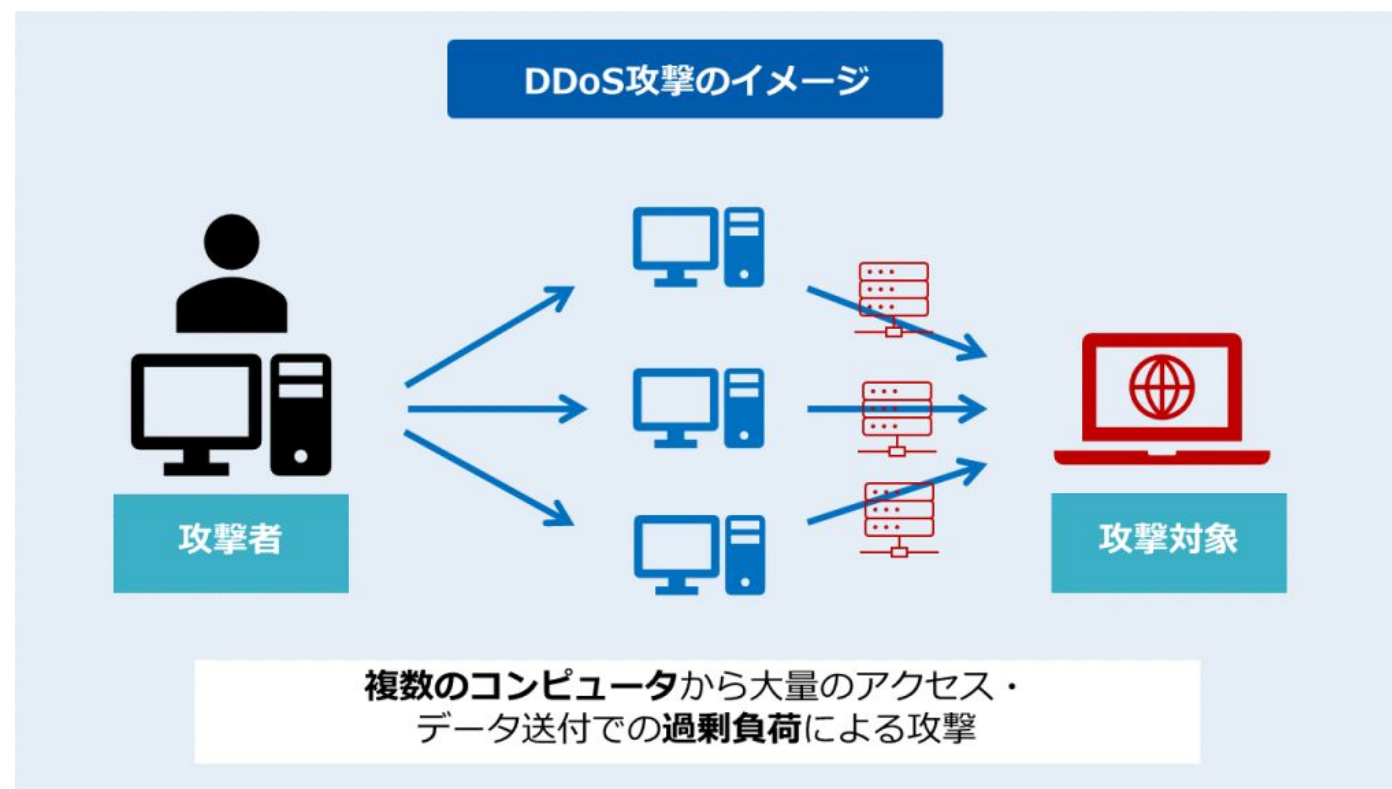
〈SQLインジェクション〉



DoS 攻撃

サーバに大量のデータを送信し、サーバの機能を停止させる攻撃を**DoS攻撃**といいます。

→ **Tấn công DoS** (tấn công từ chối dịch vụ) là cuộc tấn công gửi một lượng lớn dữ liệu đến máy chủ và khiến các chức năng của máy chủ ngừng hoạt động.



ディレクトリトラバーサル攻撃

Webサーバは多くの人にアクセスされるため、サーバ管理者は設定により公開範囲を限定しています。しかし、Webサーバの設定が甘いと、管理者が公開するつもりではないファイルの場所であっても、ユーザがアクセスできてしまいます。この脆弱性を狙って、重要なファイルを不正に見る攻撃を**ディレクトリトラバーサル攻撃**といいます。

- Vì máy chủ web được nhiều người truy cập nên quản trị viên máy chủ sẽ cài đặt để giới hạn phạm vi công khai. Tuy nhiên, nếu việc cài đặt máy chủ web lỏng lẻo thì người dùng có thể truy cập vào các vị trí tệp mà quản trị viên không có ý định công khai. Một cuộc tấn công nhắm vào lỗ hổng này để xem trái phép các tệp quan trọng được gọi là **tấn công Directory Traversal**.

Web ビーコン

WebページやHTML形式の電子メールに非常に小さい画像を埋め込み、ユーザのIPアドレスやアクセス日時、サイトへの訪問頻度といったアクセス動向を収集する仕組みのことを、**Webビーコン**といいます。

- **Web beacon** (Tập tin chỉ báo) là cơ chế nhúng một hình ảnh rất nhỏ vào trang web hay mail điện tử định dạng HTML để thu thập các xu hướng truy cập như là địa chỉ IP của người dùng, ngày giờ truy cập hay tần suất truy cập vào trang web.

スパイウェア

PC内にある利用者の個人情報や、どんなWebサイトを見ているかといった行動を監視し、利用者が知らないところで収集した情報を外部サーバに自動送信するプログラムをスパイウェアと
いいます。

例えば、キーボード入力を監視して記録するキーロガーをPCに仕掛けて、入力パスワードを収集するなどの手口があります。

- **Spyware** (Phần mềm gián điệp) là chương trình giám sát thông tin cá nhân của người dùng trên PC và hành vi của họ, chẳng hạn như đang xem trang web nào, sau đó tự động gửi thông tin thu thập được đến máy chủ bên ngoài mà người dùng không hề hay biết. Ví dụ, có 1 thủ thuật là cài đặt keylogger vào PC để theo dõi và ghi lại dữ liệu nhập từ bàn phím cũng như thu thập mật khẩu nhập vào.

ブルートフォース攻撃

パスワード解析や暗号解読の手法で、考えられるすべての文字の組合せパターンを順に試す攻撃をブルートフォース攻撃といいます。

- Tấn công Brute-force là một phương pháp phân tích mật khẩu hoặc giải mã, là hình thức tấn công mà (hacker) sẽ thử tuần tự tất cả các kiểu tổ hợp ký tự có thể nghĩ ra.

人的脅威

人的脅威

「人」が原因である脅威を**人的脅威**といいます。コンピュータの置き忘れや操作ミスなど、情報のもち主のうっかりミスによるものや、内部関係者が意図的に情報を漏えいしたりすることがこれに当たります。

- ソーシャルエンジニアリング
- なりすまし
- サラミ法

→ Các mối đe dọa do "con người" gây ra được gọi là **mối đe dọa con người**. Điều này bao gồm những lỗi vô ý của chủ sở hữu thông tin, chẳng hạn như để quên máy tính, lỗi thao tác, hay việc người trong cuộc làm rò rỉ thông tin một cách có chủ ý.

- Tấn công phi kỹ thuật
- Giả mạo dữ liệu
- Phương pháp salami

ソーシャルエンジニアリング

システム管理者などを装って、利用者に問い合わせでパスワードを聞き出したり、緊急事態を装って組織内部の機密情報を聞き出したりするなど、人間の心理の隙について情報を盗む行為をソーシャルエンジニアリングといいます。

→ **Tấn công phi kỹ thuật** là hành vi đánh cắp thông tin bằng cách lợi dụng lỗ hổng trong tâm lý con người, chẳng hạn như giả mạo là quản trị viên hệ thống, truy vấn người dùng để hỏi mật khẩu, hoặc là giả vờ là trường hợp khẩn cấp để hỏi thông tin bí mật của nội bộ tổ chức.

なりすまし

盗んだIDやパスワードなどを使い、ネットワーク上でその人の
ふりをすることをなりすましといいます。

なりすましによって、情報を盗んだり、他人に迷惑な行動をしたりします。

- Mạo danh là việc sử dụng ID hoặc mật khẩu đã ăn cắp, rồi giả vờ là người đó ở trên mạng.
Bằng việc mạo danh, họ sẽ lấy cắp thông tin hoặc có hành vi gây phiền toái cho người khác.

サラミ法

不正行為が表面化しない程度に、多数の資産から少しずつ詐取する方法を**サラミ法**といいます。サラミソーセージを少しずつスライスして盗むと、盗みが発覚しづらいことに由来しています。

→ **Phương pháp Salami** là phương pháp lừa đảo từng chút một số lượng lớn tài sản ở mức độ mà các hành vi bất hợp pháp/gian lận không lộ diện. Cái tên này xuất phát từ việc nếu bạn ăn trộm xúc xích salami bằng cách cắt nó thành từng miếng nhỏ thì rất khó bị phát hiện hành vi trộm cắp.

物理的脅威

物理的脅威



大雨や地震、落雷などの災害、またはコンピュータの故障など、コンピュータが物理的に損害を受けて情報を失う脅威を**物理的脅威**といいます。空き巣によるコンピュータの盗難や破壊などもこれに当たります。

- Các mối đe dọa như thảm họa mưa lớn, động đất, sấm sét; hay những hư hại của máy tính khiến máy tính bị hư hỏng vật lý, làm mất thông tin thì được gọi là **các mối đe dọa vật lý**. Mối đe dọa vật lý cũng bao gồm việc trộm cắp và phá hủy máy tính gây ra bởi các vụ trộm.

授業予告

授業予告

**本授業では、
事前学習の確認と実践ワークを実施します**

本授業では、事前学習の内容について確認はしますが
詳しい説明はしません

実践ワーク中心の授業になるので、しっかりと
読んで理解しておいてください

The background of the slide features a scenic view of Mount Fuji under a clear blue sky with some light clouds. In the foreground, there are cherry blossom trees in full bloom, their pink flowers creating a dense canopy. To the right, a traditional Japanese temple with a red wooden structure and a dark tiled roof is partially visible. The text is overlaid on a semi-transparent white rectangular area in the center.

**事前学習は終わります
授業当日で会いましょう！**

Hẹn gặp các em vào buổi học trên lớp.