



# IT日本語2

## 9.2 コンピュータウイルス(2)



# カタカナ語

# カタカナ語の発声練習

No	英語	カタカタ
1	OS	オーエス
2	Patch	パッチ
3	Install	インストール
4	Signature code	シグネチャコード
5	Pattern matching	パターンマッチング
6	Assemble	アセンブル
7	Binary code	バイナリコード
8	Source code	ソースコード
9	Client	クライアント
10	Buffer overflow	バッファオーバーフロー



# ウイルスの予防



# Phòng ngừa virus

## → ● Phòng ngừa virus

Nguồn lây nhiễm vi rút chủ yếu là thư điện tử và các trang web. **Để** tránh lây nhiễm qua thư điện tử, **điều quan trọng** là không mở tùy tiện các tệp đính kèm được gửi từ người lạ. **Để** ngăn chặn lây nhiễm từ việc duyệt các trang web, có **các biện pháp đối phó** như cài đặt không hiển thị các trang web đáng ngờ trong trình duyệt.

**Ngoài ra**, áp dụng thích hợp các bản vá lỗi cho hệ điều hành và ứng dụng **để** ngăn chặn sự lây nhiễm bằng cách khai thác các lỗ hổng bảo mật trong PC.

# 回答1

クライアント PC で行うマルウェア対策のうち、適切なものはどれか。

1. PCにおけるウイルスの定期的な手動検査では、ウイルス対策ソフトの定義ファイルを最新化した日時以降に作成したファイルだけを対象にしてスキャンする。
2. ウイルスが PC の脆弱性を突いて感染しないように、OS及びアプリケーションの修正パッチを適切に適用する。
3. 電子メールに添付されたウイルスに感染しないように、使用しないTCPポート宛ての通信を禁止する。
4. ワームが侵入しないように、クライアント PC に動的グローバルIPアドレスを付与する。

# 回答1

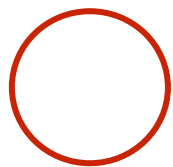
## Chọn phương án đúng trong số các đối sách phòng chống Malware thực hiện trên PC phía client?

1. Khi kiểm tra định kỳ virus trên PC bằng cách thủ công, chỉ quét các file được tạo sau ngày và giờ cập nhật file định nghĩa của phần mềm chống virus
2. Áp dụng các bản vá cho OS và ứng dụng một cách thích hợp để ngăn chặn virus khai thác các lỗ hổng trong PC
3. Cấm giao tiếp với các cổng TCP không sử dụng để tránh lây nhiễm vi-rút đính kèm trong e-mail.
4. Cấp phát địa chỉ IP Global động cho PC client để ngăn chặn sâu xâm nhập

# 回答2

ウェブサイトの閲覧による感染を防ぐ方法はどれか。

1. OSやアプリケーションの修正パッチを適切に適用すること
2. コンピュータをすぐにネットワークから切り離すこと
3. 知らない人から送られてきた添付ファイルをむやみに開かないこと
4. ブラウザに怪しいWebサイトは表示しない設定をしておくこと





# ウイルスの検知



# Phát hiện virus

## → ● Phát hiện virus

Đảm bảo **cài đặt sẵn** phần mềm chống virus trên máy tính. Phần mềm chống virus có chứa thông tin (mã chữ ký) về các virus đã biết **dưới dạng** tệp định nghĩa virus, sẽ thực hiện so sánh với thông tin này rồi phát hiện và loại bỏ virus. Đây **được gọi là phương pháp đối sánh mẫu (Pattern matching)**. **Vì** các loại virus chủng mới được tạo ra hàng ngày, **nên** các tệp định nghĩa virus cần được cập nhật định kỳ **để** có thể đối phó với những loại virus mới nhất.



# ウイルス定義ファイル

## ウイルス定義ファイル

既知ウイルス情報(シグネチャコード)を持っている  
ウイルスに特有のパターンが大量に登録されている

### → File định nghĩa virus

Chứa thông tin về virus đã biết (mã chữ ký)

Chứa một số lượng lớn các mẫu tiêu biểu của virus

# パターンマッチング方式

## パターンマッチング方式

既知ウイルス情報(シグネチャコード)を使用して、  
対象ファイルと比較しウイルスを検出

### → Phương pháp đối sánh mẫu

Việc sử dụng thông tin virus đã biết (mã chữ ký), so sánh với file đối tượng để phát hiện ra virus



# 回答4

ウイルス対策ソフトのパターンマッチング方式を説明したものはどれか。

1. 感染前のファイルと感染後のファイルを比較し、ファイルに変更が加わったかどうかを調べてウイルスを検出する。
2. 既知ウイルスのシグネチャと比較して、ウイルスを検出する。
3. システム内でのウイルスに起因する異常現象を監視することによって、ウイルスを検出する。
4. ファイルのチェックサムと照合して、ウイルスを検出する。

## 回答4

**Chọn phương án giải thích về phương thức so sánh mẫu của phần mềm diệt virus?**

1. Phát hiện virus bằng cách so sánh các file trước khi lây nhiễm và sau khi lây nhiễm để xem liệu có bất kỳ thay đổi nào được thực hiện đối với các tệp hay không.
2. Phát hiện virus bằng cách so sánh với chữ ký của các virus đã biết.
3. Virus được phát hiện bằng cách theo dõi các hiện tượng bất thường do virus gây ra trong hệ thống.
4. Phát hiện virus bằng cách so sánh với checksum của file.



# 感染後の対応



# 感染後の対応

## Đổi ứng sau lây nhiễm

### ●感染後の対応

ウイルスに感染してしまったら、コンピュータを**すぐに**ネットワークから切り離すことが**重要**です。これは、ネットワークを**通じて**さらに感染を広げてしまう**など**、被害の拡大を防ぐ**ため**です。

### → ● Đổi ứng sau lây nhiễm

Nếu lỡ bị nhiễm virus, **việc quan trọng** là phải ngắt máy tính **khỏi** kết nối mạng **ngay lập tức**. Điều này là **để** ngăn chặn sự lan rộng của thiệt hại, **chẳng hạn như** lan rộng sự lây nhiễm xa hơn **thông qua** mạng.



# これを知っとこ！



## 逆アセンブル

新種ウイルスの動作を解明するのに有効な手法として、逆アセンブルがあります。バイナリコードからソースコードに変換することで、新種ウイルスの動作を解明します。

### → Disassemble (Phương pháp dịch ngược hợp ngữ)

Disassemble là một phương pháp hiệu quả để làm rõ hoạt động của các chủng loại virus mới. Bằng cách chuyển đổi từ mã nhị phân sang mã nguồn, sẽ làm sáng tỏ hoạt động của các loại virus mới.



# 実践



# 【Q&A】



①ウイルスは主にどこから来ているんですか。

①主に電子メールと Web サイトです。





# 【Q&A】



②電子メールによる感染を防ぐためには、  
どうすればいいですか。

②知らない人から送られてきた添付ファイル を  
むやみに開かないことが重要です。



# 【Q&A】



③Web サイトの閲覧による感染を防ぐためには  
どうすればいいですか。

③ブラウザに怪しい Web サイトは表示しない 設  
定をしておくなどの対策方法があります。



# 【Q&A】




④ウイルス対策ソフトをパソコンにインストールしておきましたか。※何のソフトですか。

④例：インストールしておきました。  
カスペルスキー(Kaspersky)など





# 【Q&A】



⑤ウイルス定義ファイルは定期的に更新する必要がありますか。

⑤必要です。ウイルスは毎日新しい種類のものが作られているから。



# 【Q&A】



⑥ウイルスに感染してしまったら、まず何をすればいいですか。どうしてですか。

⑥コンピュータをすぐにネットワークから切り離してください。  
ネットワークを通じてさらに感染を広げてしま  
うなどの被害の拡大を防ぐためです。

