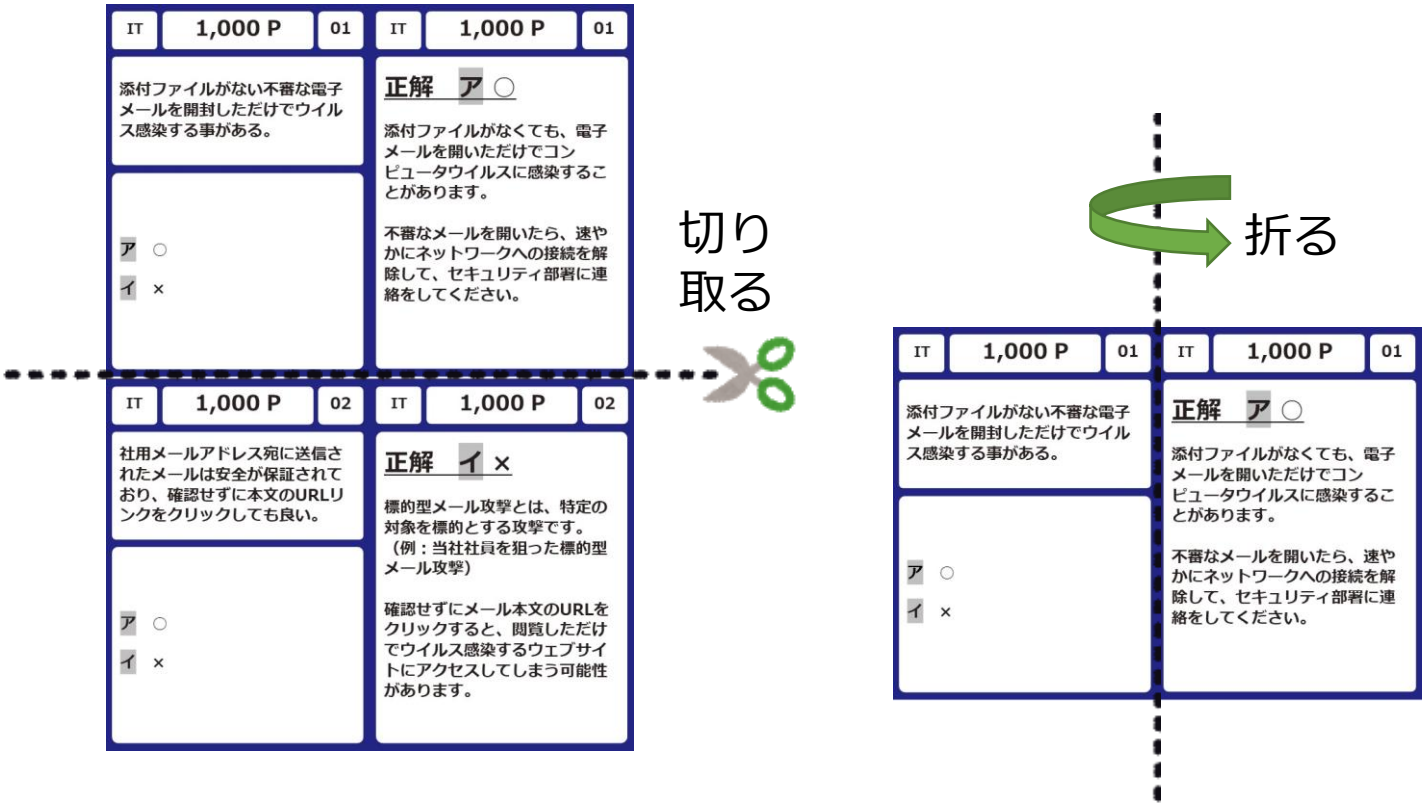
# クイズカード

クイズに正解すると獲得できるカードです。
全部で26枚あります。

情報システム（青色）・制御システム（緑色）・事例（赤色）
に関するクイズが記載されています。

## 上下で切り取り、左右で折って ご使用ください。



IT | 1,000 P | 01

添付ファイルがない不審な電子メールを開封しただけでウイルス感染する事がある。

ア　○

イ　×

IT | 1,000 P | 01

## 正解　ア ○

添付ファイルがなくても、電子メールを開いただけでコンピュータウイルスに感染することがあります。

不審なメールを開いたら、速やかにネットワークへの接続を解除して、セキュリティ部署に連絡をしてください。

IT | 1,000 P | 02

社用メールアドレス宛に送信されたメールは安全が保証されており、確認せずに本文のURLリンクをクリックしても良い。

ア　○

イ　×

IT | 1,000 P | 02

## 正解　イ ×

標的型メール攻撃と呼ばれる、特定の対象を標的とするサイバー攻撃があります。（例：当社社員を狙った標的型メール攻撃）

メール本文のURLをクリックすると、閲覧しただけでウイルス感染するウェブサイトにアクセスしてしまう可能性があります。

IT | 2,000 P | 03

IoT機器利用時に注意すべき事項として適切なものはどれか。（1つ選択）

ア　問い合わせ窓口・サポートがないIoT機器であっても使用して良い

イ　ID、パスワードは初期設定のまま使用する

ウ　使用しなくなった機器の電源は、必ずしも切る必要はない

エ　IoT機器を一時的に貸し出す際は、データの消去等を行う

IT | 2,000 P | 03

## 正解　エ

IoT機器に限られた話ではありませんが、情報機器を手放す際は必ずデータ、キャッシュの削除を行いましょう。
機密情報、個人情報が漏えいする恐れがあります。

参考：「IoTセキュリティガイドライン Ver1.0」（平成28年7月5日 総務省、経済産業省、IoT 推進コンソーシアム）

IT | 2,000 P | 04

ファイアウォールの説明として適切なものはどれか。（1つ選択）

ア　火で覆われた壁。外敵の侵入を防ぐため、中世ヨーロッパの要塞などに用いられた

イ　ネットワークに流れてきたデータを読み、行先を割り振る機器

ウ　インターネットからの不正な通信を防ぐシステムまたは仕組み

IT | 2,000 P | 04

## 正解　ウ

社内システムを不正な通信から守るために、ファイアウォールで通信の制限を行います。
ただし、設定ミスやファイアウォールの脆弱性を突いた攻撃を受ける場合があるので、注意してください。

イは「スイッチ」という機能の説明です。

OT　2,000 P　05

制御システムをウイルス感染から防ぐための方法として適切なものはどれか。（1つ選択）

ア　来客の入構をチェックなしで許可する

イ　古いバージョンのOSを使用する

ウ　管理されていないUSBメモリを許可なく利用する

エ　使用していないUSBポートを物理的に塞ぐ

OT　2,000 P　05

## 正解　エ

多くの制御システムはインターネットと繋がっていませんが、USB ポートに挿した機材（USBメモリ、充電のため接続した携帯等）や、SDカードからの感染や侵入に注意を払う必要があります。

事例　2,000 P　06

自動車メーカーで工場内のシステムがウイルスに感染し、自動車の生産が50分停止しました。損害額はいくらと言われているでしょう？

ア　170万円

イ　1,700万円

ウ　1.7億円

エ　17億円

事例　2,000 P　06

## 正解　エ

外部から持ち込まれたノートPCを工場のネットワークへ接続したところ、工場内のシステムでウイルスが感染・拡大しました。

50,000人の従業員が作業を中断し、生産が50分停止しました。

部品サプライヤへの感染も疑われる事態となり、損害額は17億円にのぼると言われています。

事例 | 2,000 P | 07

海外の電力会社がランサムウェア（身代金請求型ウイルス）による攻撃を受けた。攻撃内容として適切なものはどれか。（1つ選択）

ア　内部通信の不正受信

イ　ファイアウォールの設定値改ざん

ウ　データベース、利用端末内ファイルの暗号化

エ　機密データの流出

事例 | 2,000 P | 07

## 正解　ウ

ランサムウェアに感染すると、利用端末内に保存しているデータを暗号化され、制御システムのパソコン端末／サーバが使用できない状態になります。

事例 | 2,000 P | 08

真冬に海外の電力会社がサイバー攻撃を受け、電力供給に障害が発生した。どの位の顧客に影響があったか。（１つ選択）

ア　約1万顧客

イ　約8万顧客

ウ　約12万顧客

エ　約23万顧客

事例 | 2,000 P | 08

## 正解　エ

2015年12月23日、東欧の某国西部で大規模な停電が発生し約22万5千顧客に影響が出ました。原因はリモートアクセスの権限を盗まれて外部から変電所のコントロールセンターを勝手に制御されたことでした。

OT | 3,000 P | 09

インターネットに接続できるカメラやルーター等の電子機器に不正アクセスされないために有効な手段はどれか。（1つ選択）

ア　使用していない電子機器を起動したままにする

イ　初期IDやパスワードが設定されている場合、変更する

ウ　古いバージョンのファームウェアを使用し続ける

エ　パスワードが設定されていない電子機器を使用する

OT | 3,000 P | 09

## 正解　イ

インターネットに接続できる電子機器には、初期IDやパスワードが設定されているものがあります。初期設定のままであったり、ファームウェアの更新を実施しないと、不正アクセスの被害を受ける可能性があります。

IT | 2,000 P | 10

ランサムウェア（身代金請求型ウイルス）の特徴として適切なものはどれか。（1つ選択）

ア　Windows XPなどサポートが終了しているOSは感染しない

イ　感染した端末の操作ができなくなるタイプのランサムウェアはない

ウ　自分で感染先を見つけて拡散するタイプのランサムウェアはない

エ　感染するとデータを暗号化し、身代金（ランサム）を請求される

IT | 2,000 P | 10

## 正解　エ

ランサムウェアは、感染したパソコン内にあるデータを暗号化するもので、その後に攻撃者が暗号化の解除を条件に身代金（ランサム）を要求してくるものです。ランサムウェアの中にはア～ウに記載のタイプのものもあります。

IT | 2,000 P | 11

添付ファイルがあるメールを受信した。対応として適切なものはどれか。（1つ選択）

ア　怪しいメールアドレスからのメールのため、添付ファイルは開かなかった

イ　メールの文脈が明らかに不自然であったが、確認のため添付ファイルを開封した

ウ　心当たりのない送信元であったため、メールに返信した

IT | 2,000 P | 11

## 正解　ア

心当たりのない送信元からのメールの添付ファイルは開封するべきではありません。（メールを開くだけでウイルス感染するものもあります。）
知り合いや実在の組織になりすましてメールが送信される場合もあるため、不用意に心当たりの無いメール、添付ファイルは開封せずに、セキュリティ部署・担当者へ連絡してください。

IT | 2,000 P | 12

個人利用しているショッピングサイトやSNS、メールのパスワード設定で適切なものはどれか。（1つ選択）

ア　簡単なパスワード（「0000」や「Password」など）にする

イ　全て同じパスワードを設定する

ウ　英語、数字、記号（大文字小文字、&や_など）を組み合わせ、文字数はできるだけ長くする

エ　設定者の誕生日など覚えやすいパスワードにする

IT | 2,000 P | 12

## 正解　ウ

パスワードを推測されやすいものや、同じものを使い回すことで、SNSでの「なりすまし」によるトラブルや、ネットショッピングでの金銭的な被害が発生しています。今一度、自分のパスワードが安全かチェックしてみてください。

事例 | 1,000 P | 13

安全計装システム（SIS）がサイバー攻撃を受け、誤作動し、操業停止した事例がある。

※安全計装システム＝緊急停止装置

ア　○

イ　×

事例 | 1,000 P | 13

**正解　ア ○**

2017年12月に安全計装システム（SIS）を標的としたサイバー攻撃が行われました。SIS コントローラがウイルスに感染したことで、SIS のフェールセーフ機能が作動し、操業が一時停止する事態となりました。

IT | 2,000 P | 14

標的型攻撃の攻撃手口としてもっとも適切なものはどれか。（1つ選択）

IPA「情報セキュリティ10大脅威 2021」解説書

ア　メール（添付ファイル、リンク）

イ　FAX

ウ　自然災害

エ　宅配便

IT | 2,000 P | 14

**正解　ア**

標的型攻撃は特定の組織における機密情報の窃取を目的としています。

自然災害は直接的な攻撃手口ではありませんが、自然災害発生時は様々な混乱が生じるため、攻撃の機会となり得ます。普段からのセキュリティ対策が必要となります。

事例 | 2,000 P | 15

海外のウラン濃縮工場で施設が破壊されるサイバー攻撃が発生した。感染原因として適切なものはどれか。（1つ選択）

ア　工場内のPCで電卓の機能を使った

イ　工場内のPCで持ち主不明のUSBメモリの中身を閲覧した

ウ　工場内のPCを再起動した

事例 | 2,000 P | 15

## 正解　イ

2010年にウラン濃縮工場で持ち主不明のUSBを使用したことで、ウイルスがPCを経由し工場内に侵入、ウランの遠心分離機が破壊されるサイバー攻撃が起こりました。この工場のネットワークはインターネットから隔離されていましたが、USBを経由しウイルスが侵入・拡大し、施設が破壊されるという事態にまで発展したと推察されています。

IT | 2,000 P | 16

コンピュータウイルスの説明として適切なものはどれか。（1つ選択）

ア　ウイルスに感染してもすぐに発症しないものがある

イ　ウイルスに感染するとファイルを破壊するものがある

ウ　ウイルスに感染すると他のコンピュータに感染を広げるものがある

エ　ア、イ、ウ全て当てはまる

IT | 2,000 P | 16

## 正解　エ

ウイルスが自身を複製し、他のコンピュータへ拡散する場合があります。

全てのコンピュータが感染しても復旧出来るように、 外部記憶媒体へバックアップを取って、安全に保管しておきましょう。

OT | 1,000 P | 17

国内の制御システムを狙ったサイバー攻撃が発生している。

引用：情報セキュリティ白書2020(p.158)より

ア　○

イ　×

OT | 1,000 P | 17

## 正解　ア ○

制御システムを狙ったサイバー攻撃は約80件/年（2017年実績）発生しており、国内企業や社会全体に大きなダメージを与えています。

セキュリティ対策が不十分な制御システムは、サイバー攻撃により被害を受ける可能性があります。

事例 | 2,000 P | 18

保守用のパソコン上でマウスカーソルが勝手に動きだした。その時の対応として正しいものはどれか。（1つ選択）

ア　リモート保守等でマウスカーソルが勝手に動くことがあるため、何もしない

イ　不審に思い、セキュリティ部署に相談する

事例 | 2,000 P | 18

## 正解　イ

海外の浄水場で設定値が改ざんされるサイバー攻撃が発生しました。「ファイアウォールが有効な状態で設定されていなかった」ことや、「不正アクセスされたPCが古いOS（Windows7）を使用していた」ことなど、セキュリティ衛生の欠如やシステムの脆弱性が重なった結果、このサイバー攻撃が発生したとされています。

https://piyolog.hatenadiary.jp/entry/2021/02/10/181319

事例 | 3,000 P | 19

国内のIT企業でランサムウェアによるサイバー攻撃が、意外な機器を発端として発生した。侵入口となった機器は以下のうちどれか。（1つ選択）

ア　HMI（現場の状態確認、操作を行うためのモニタ機器等）

イ　電子顕微鏡

ウ　USBマウス

エ　Wi-Fiルータ

事例 | 3,000 P | 19

## 正解　イ

社内のオフィス系ネットワークを狙ったランサムウェアの感染拡大により、工場の生産ラインが停止する事態に陥りました。

最初に感染した端末は電子顕微鏡でしたが、現在でもどの経路で感染したか判明していません。

事例 | 3,000 P | 20

海外のエネルギー関連企業のパイプラインが爆発するサイバー攻撃が発生した。侵入口となった機器は以下のうちどれか。（1つ選択）

ア　電子顕微鏡

イ　HMI（現場の状態確認、操作を行うためのモニタ機器等）

ウ　監視カメラ

エ　USBメモリ

事例 | 3,000 P | 20

## 正解　ウ

セキュリティを守るための機器である「監視カメラ」の脆弱性を利用してシステムに侵入し、制御システムの警報装置の動作を停止させたうえで、パイプライン管内の圧力を異常に高めて爆発を引き起こしたとされています。プラントシステム以外のセキュリティもしっかりと確認することが大事です。

https://www.ipa.go.jp/files/000057714.pdf

事例 | 3,000 P | 21

国内のテレビ局のWebサイトに対するサイバー攻撃が発生した。本事象の説明として適切なものはどれか。（全て選択）

ア　個人情報の漏えいはなかった

イ　個人情報約35万件が漏えいした

ウ　未知の脆弱性を利用したサイバー攻撃だった

エ　被害内容の公表はなかった

事例 | 3,000 P | 21

## 正解　イ、ウ

本サイバー攻撃の発覚後、専門家による調査委員会を設置するなど、早急な対処が行われ、本事象の詳細な経緯と原因、再発防止策について、約3ヶ月後に公表されました。

IT | 2,000 P | 22

ウイルスメールを開封してしまった。最初の行動として正しいものはどれか。（1つ選択）

ア　メール削除
→セキュリティ部署へ連絡

イ　セキュリティ部署へ連絡
→メール削除

ウ　メール削除
→ネットワーク切断

エ　ネットワーク切断
→セキュリティ部署へ連絡

IT | 2,000 P | 22

## 正解　エ

ウイルスメールを開封してしまった際は、ウイルスの感染拡大を防止するため、ネットワーク切断（LANケーブル抜線、Wi-Fiオフ）を行い、直ちにセキュリティ部署へ連絡してください。

OT | 3,000 P | 23

「産業用制御システムのセキュリティ-10大脅威と対策2019-」で紹介されているランキング1位の脅威はなにか。(1つ選択)

https://www.ipa.go.jp/security/controlsystem/bsi2019.html

ア　リムーバルメディアや外部機器（USBデバイス、SDカード）経由のマルウェア感染

イ　スマートデバイス（スマートホンやタブレット型端末）への攻撃

ウ　リモートアクセスからの侵入

エ　インターネットに接続された制御機器

OT | 3,000 P | 23

## 正解　ア

IPA（情報処理推進機構）では、セキュリティに関する様々な情報を発信しています。

イは10位、ウは8位、エは7位です。その他の脅威として、ヒューマンエラーと妨害行為（3位）などが挙げられます。

IT | 2,000 P | 24

街でUSBをノベルティとして配布していたので受け取った。
行動として適切なものはどれか。（1つ選択）

ア　何が入っているかPCに挿して中身を確認する

イ　使わない

ウ　後で使えそうなので会社に置いておく

IT | 2,000 P | 24

## 正解　イ

街やイベントで知らない人から受け取ったUSB・SDカード等の外部機器は、PCに挿さないようにしましょう。

コンピュータウイルスが仕込まれている可能性があります。

OT | 2,000 P | 25

制御システムの保守員が保守作業を行う場合の工場側の対応として適切なものはどれか。（1つ選択）

ア　信頼できる保守員のため、時間の効率化のためにも、ひとりでやってもらう

イ　保守員の作業時は必ず立ち合いを行い、作業内容を確認する

OT | 2,000 P | 25

## 正解　イ

制御システムの保守作業等を行う際は、作業ミスや、身の安全の確保、また内部犯行の機会低減のため、立ち合いの元行われるのが理想とされています。

OT | 2,000 P | 26

制御システムに「試験中」と貼り紙が貼られた、覚えのない機器が接続されていた。適切な行動はどれか。（1つ選択）

ア　試験中と貼り紙があったため、そのままにする

イ　制御システム担当者に連絡する

ウ　覚えのない機器のため、すぐに取り外す

OT | 2,000 P | 26

## 正解　イ

覚えのない貼り紙や端末は攻撃者／内部犯が接続したものである可能性があります。

発見次第、制御システム担当者に報告・確認を行いましょう。