

JIPDEC



セキュリティ・キャンプ2023
会員企業紹介イベント

安心・安全なデジタル社会の実現に向けて

一般財団法人日本情報経済社会推進協会

常務理事 山内 徹

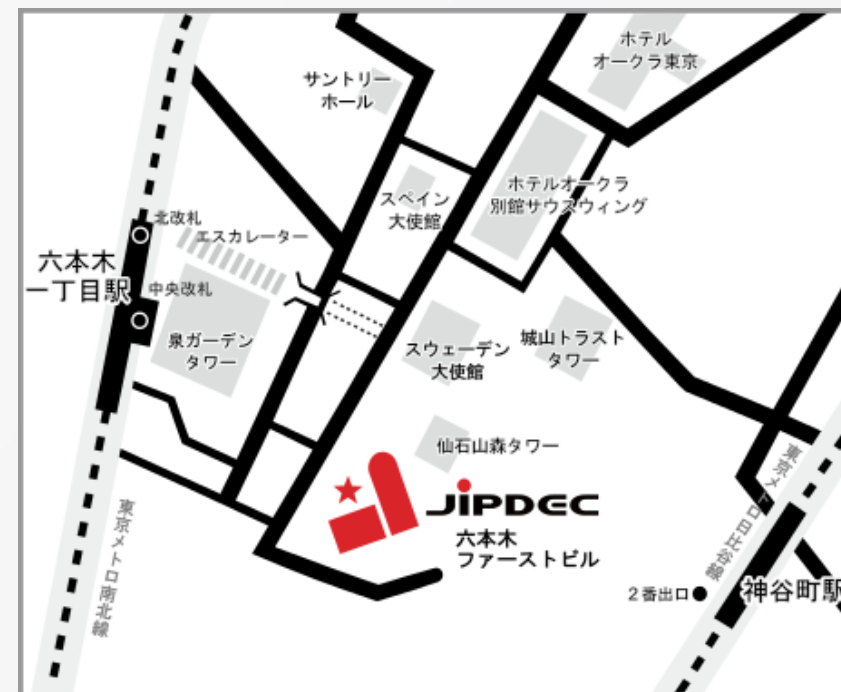
2023.08.08

JIPDECの概要

- 名称 一般財団法人日本情報経済社会推進協会（じぷでっく）
- 法人番号 1 0104 0500 9403
- 所在地 東京都港区六本木一丁目9番9号
- 設立 1967年12月20日
- 主な事業

- ✓ プライバシーマーク制度の運営
- ✓ デジタルトラストに関する評価
- ✓ セキュリティマネジメントに関する普及等
- ✓ 電子情報に係る調査研究等

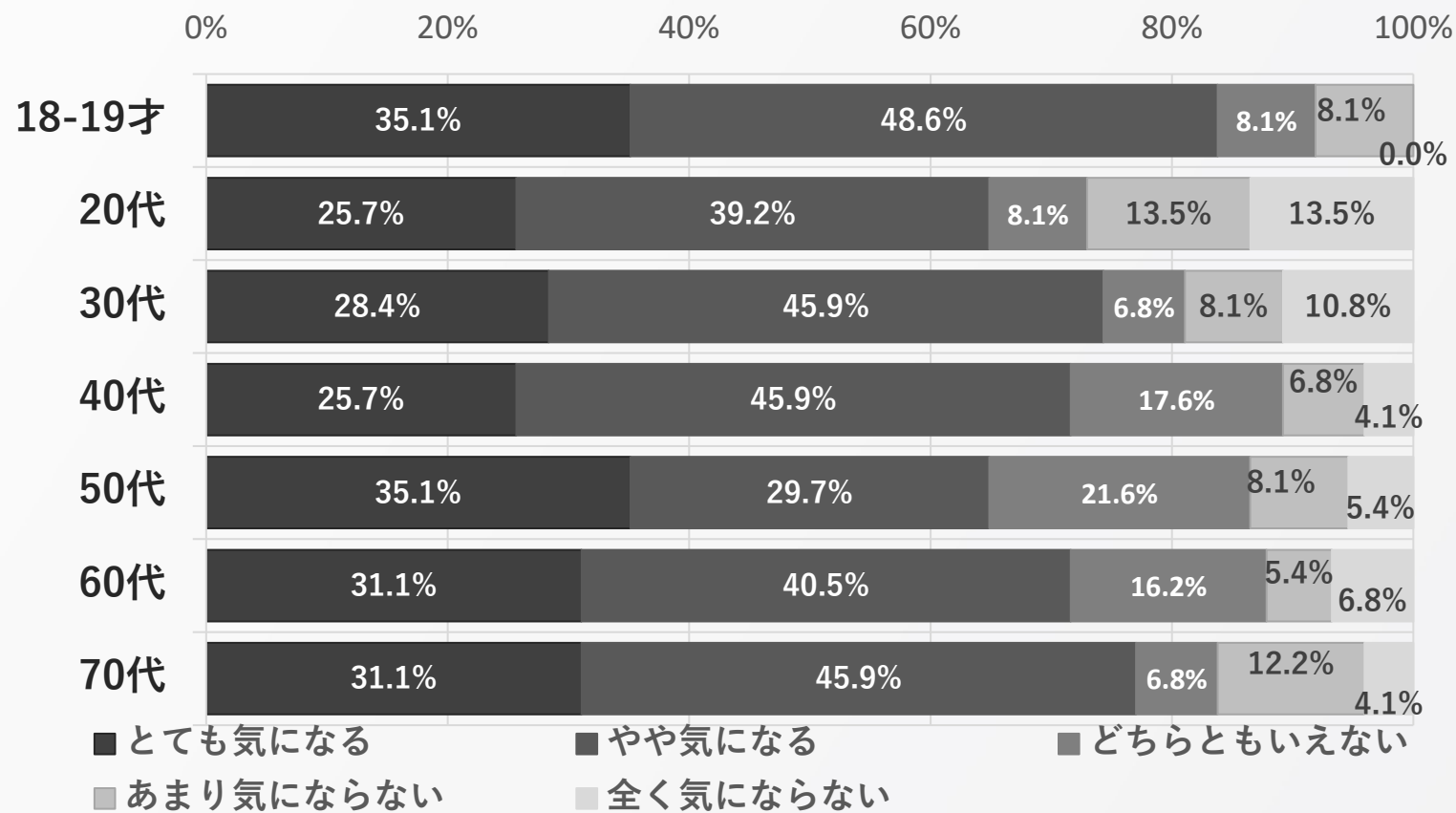
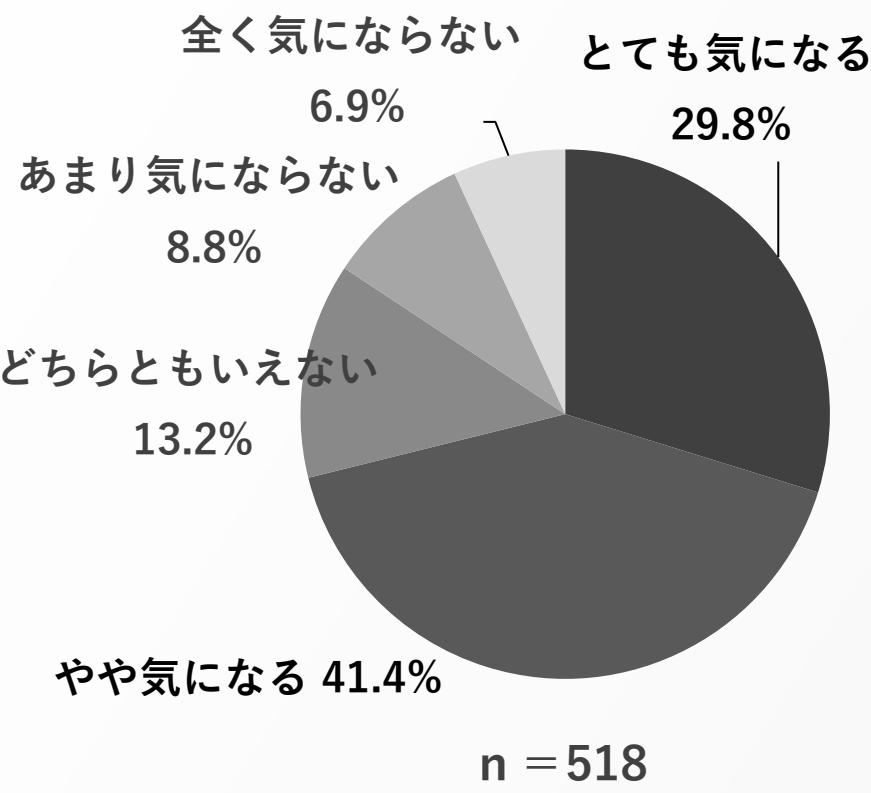
本日
紹介



01

プライバシーマーク制度の紹介

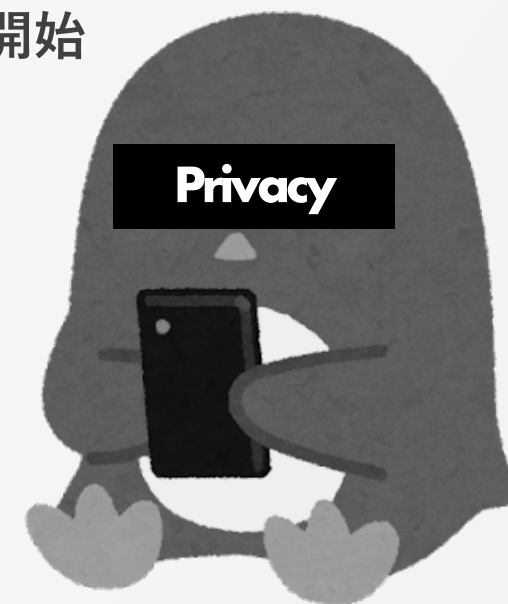
あなたの個人情報を企業等がどのように取り扱っているか、気になりますか



「デジタル社会における消費者意識調査2023」 (JIPDEC)

デジタル社会へと変化する中で

- デバイスの普及、IoT、センサー技術の高度化等により、個人に関する様々な情報がデータとして蓄積され、新たなサービスの源泉に
- 2018年、ケンブリッジ・アナリティカ社により8700万件のFacebook利用者データが不正に収集し、大統領選活動に利用されていたことが発覚
- 2019年、Appleがスマホのプライバシー保護を前面に打ち出したCMを開始
- 現在、プライバシー/個人情報保護への姿勢/取組みが、組織の**信頼性、ブランディング**にも直結



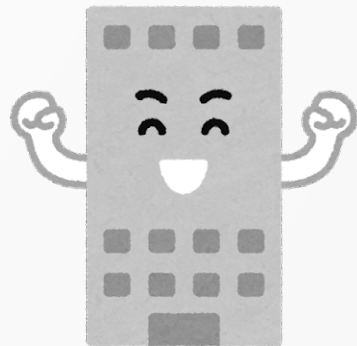
見たことありますか？このマーク



見えない努力を“見える化”するプライバシーマーク

プライバシーマークとは

個人情報について適切な保護措置を講ずる体制を整備している事業者等を評価して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用をJIPDECが認める制度



申請準備からマーク使用開始まで

PMS = 個人情報保護のマネジメントシステム



申請前に
マネジメントシステム原則に基づいた計画の作成(P)、実施(D)、点検・評価(C)、改善(A)というPDCAサイクルを、少なくとも1回以上実施

文書審査

1. 内部規程のプライバシーマークにおける個人情報保護マネジメントシステム構築・運用指針への適合状況
2. すべての従業員が内部規程を遵守するための、具体的な手順、手段等の策定状況

&

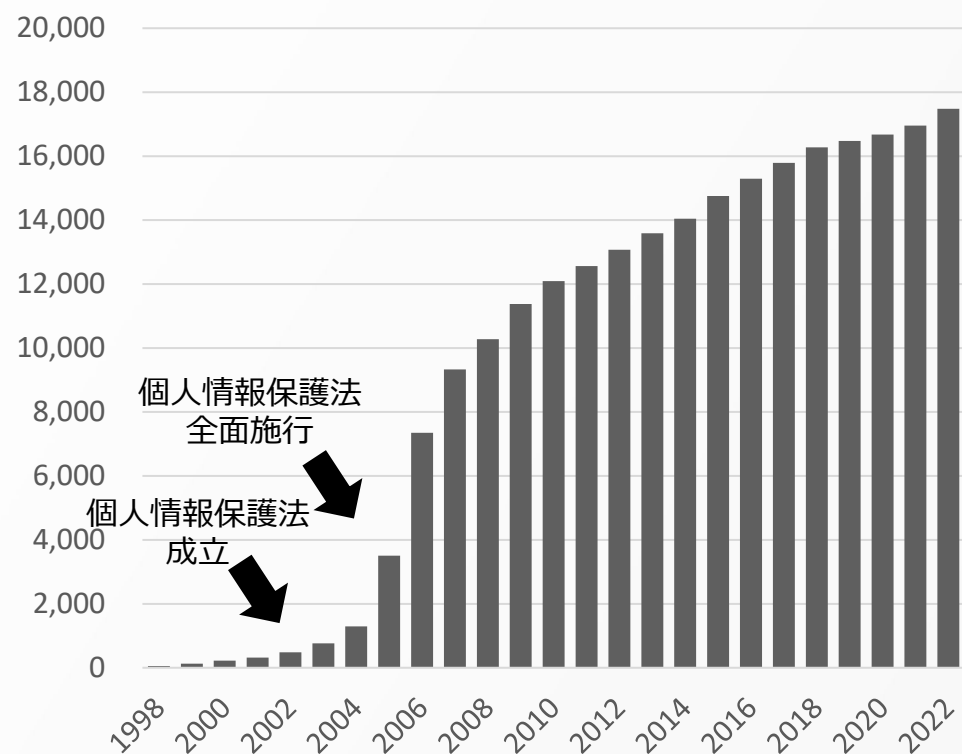
現地審査

1. トップインタビュー
2. PMS運用状況の確認
3. 現場での実施状況の確認

プライバシーマークは日本に根付いた制度

現在の付与事業者数 **約17,500社**
そのうち**40%強**が情報サービス・調査業ですが

企業に限らず、**病院や学術機関、政治・経済・文化団体**にも取得していただいています。



あなたの未来を守る、創る。



今年で**制度創設25周年**

02

デジタルトラストへの取組

デジタルトラストとは何か？

- コロナ禍は、テレワークやWeb会議とともに、書面、押印、対面等の原則の見直しとデジタル化を前倒し



デジタル庁は、データ戦略の一環としてトラストを重視
JIPDECは、トラストサービスの評価を通じて貢献

デジタルトラストの確立の必要性

- ✓ データの担い手の人や法人等が本物であること
- ✓ データが改ざんされていないこと

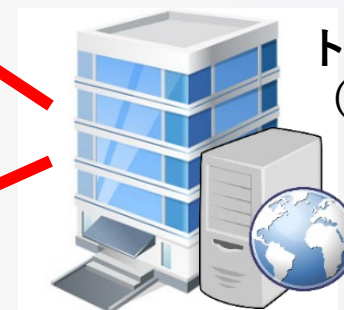
デジタルトラストの具体例(1)

● マイナンバーカード等を使ったデジタル身分証明

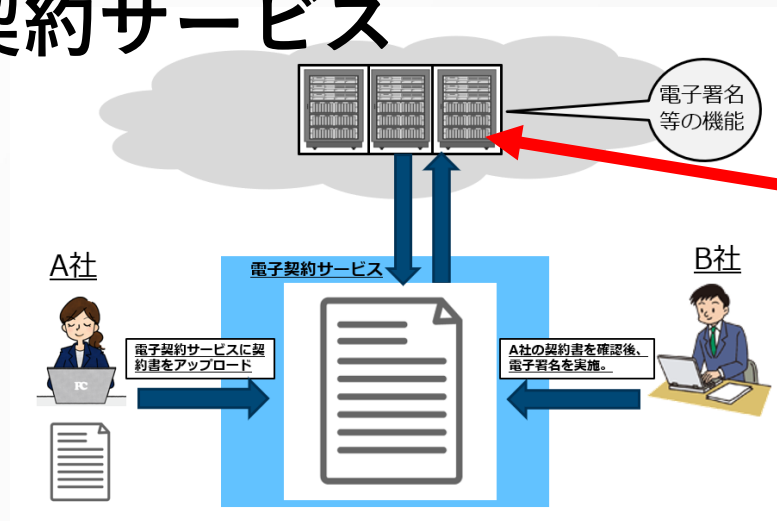
- 電子申請 (特別定額給付金等)
- 電子申告 (e-Tax等)
- マイナポータル、コンビニ交付サービス等へのログイン他



マイナンバーカードの公的個人認証サービスによる身元確認を用いた民間デジタルIDもありうる

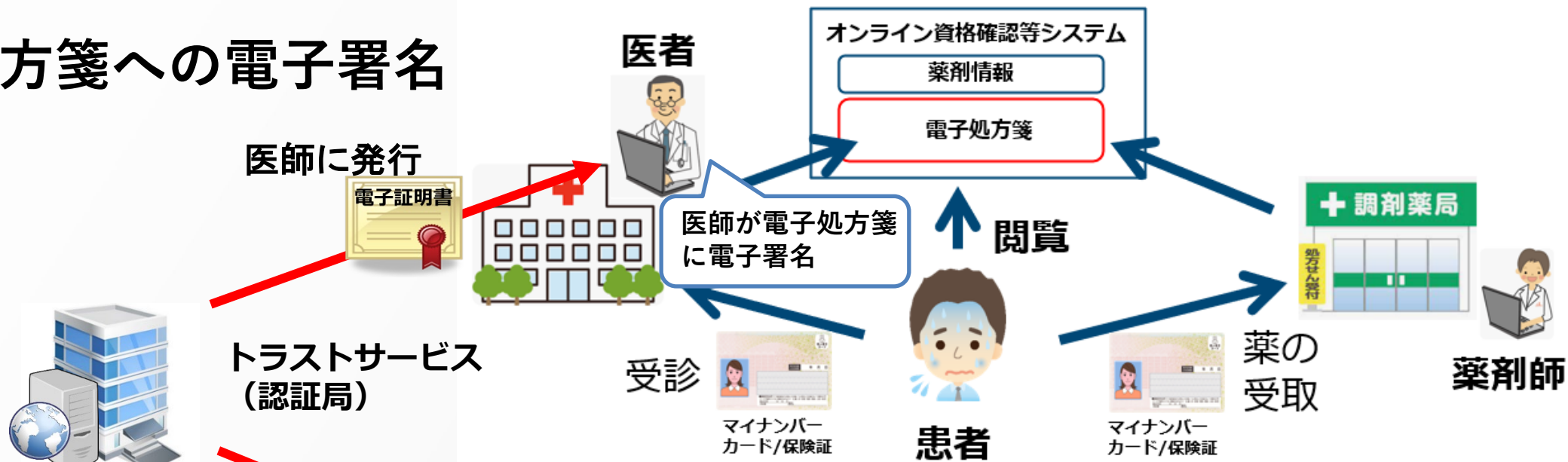


● 電子契約サービス

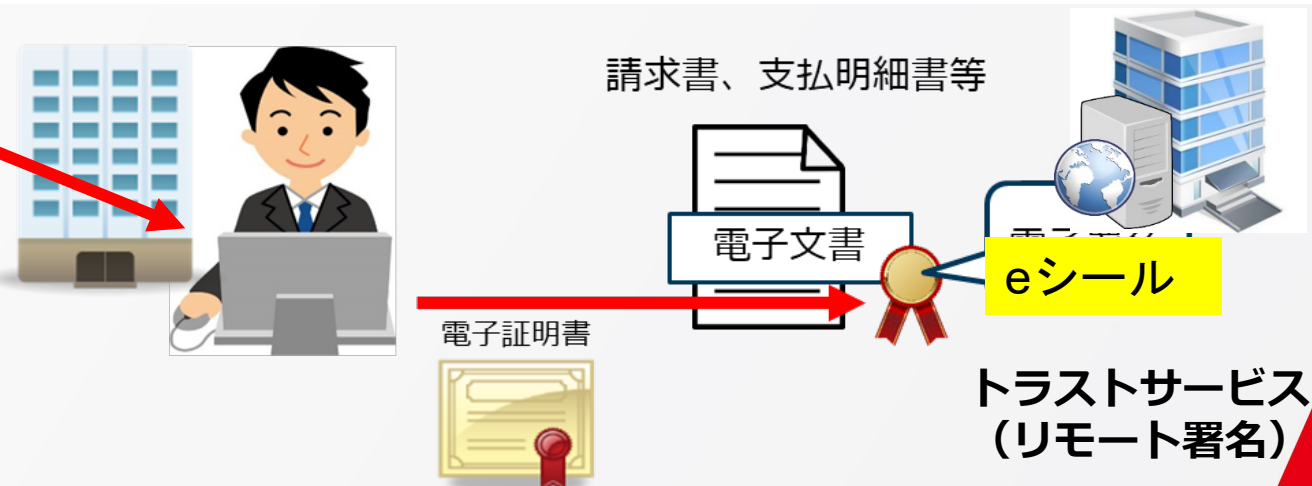


デジタルトラストの具体例(2)

● 電子処方箋への電子署名



● 電子インボイス制度の適格請求書等へのeシール



トラストサービスの役割

トラストサービスとは、
→ ネット利用者の本人確認やデータの改ざん防止等の仕組み

【特徴 1】

✓ 単独では使われることは（多分）ない。

【特徴 2】

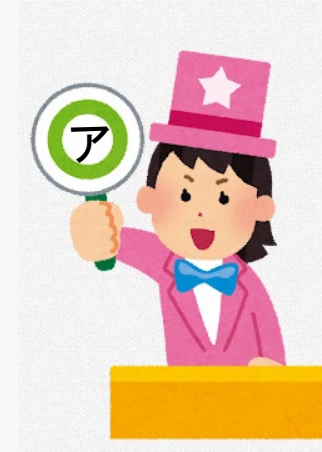
✓ その品質が一般にはわかりにくい。

デジタル社会の縁の下での力持ち！

君はITエキスパートになれるか？

クイズに挑戦！

03



(注) IPAの広報誌「IPA NEWS：国家試験に挑戦！」を参考にしました。

第1問：

暗号化に関する記述のうち、適切なものはどれか？

- ア 共通鍵暗号方式では暗号文と共通鍵を同時に送信する。
- イ 公開鍵暗号方式では暗号化のための鍵と平文に戻すための鍵が異なる。
- ウ 暗号文を平文に戻すことをリセットという。
- エ 電子署名には、共通鍵暗号方式が使われる。



正答：イ

公開鍵暗号方式は「公開鍵」と「秘密鍵」というペアとなる2つの鍵を使用します。「公開鍵」は誰でも利用できるように公開しておき、「秘密鍵」は秘匿します。

暗号化通信を行う際には、送信者が「受信者の公開鍵」で平文を暗号化し、受信者は「自身の秘密鍵」で暗号文を復号します。暗号化は誰でもできますが、復号できるのは「秘密鍵」を持っている受信者だけなので安全に通信ができます。

第2問：

公開鍵暗号方式では、暗号化のために鍵と復号のための鍵が必要となる。4人が相互に通信内容を暗号化して送りたい場合、全部で8個の鍵が必要である。

このうち非公開にする鍵は何個か？

- ア 1個
- イ 2個
- ウ 4個
- エ 6個



正答：ウ

公開鍵暗号方式では、1人の受信者に対して送信者が複数存在する場合でも、公開鍵1つ、秘密鍵1つあれば足ります。

設問では受信者が4人なので、8個の鍵のうち公開鍵は4つ、秘密鍵は4つになります。

第3問：

全ての通信区間で盗聴されるおそれがある通信環境において、受信者以外に内容を知られたくないファイルを電子メールに添付して送る方法として、最も適切なものはどれか？

- ア S/MIMEを利用して電子メールを暗号化する。
- イ SSL/TLSを利用してプロバイダのメールサーバとの通信を暗号化する。
- ウ WPA2を利用して通信を暗号化する。
- エ パスワードで保護されたファイルを電子メールに添付して送信した後、別の電子メールでパスワードを相手に知らせる。



正答：ア

S/MIMEは、電子メールを盗聴や改ざんなどから守るために、公開鍵暗号技術を利用した暗号化、改ざん防止、認証をメールソフト上でできるようにする仕組みです。

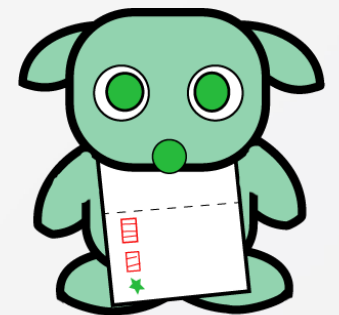
第4問：

eシールの説明はどれか？

- ア インターネット上のゲーム内に限定されたキャラクターのイメージデータの作成者を証明する仕組みの一つである。
- イ 個人の意思表示や、意思表示をしている個人の本人確認が必要な電子文書データについて、その電子文書データの作成者の証明と改ざん防止のために、個人が行う電子署名である。
- ウ 電子文書データの作成者の証明と改ざん防止のために、重要文書を扱う国や地方自治体などの公共機関だけに使用が許されている電子署名である。
- エ 法人等が作成した電子文書データについて、その作成者が間違いなくその法人等であり、かつ、その電子文書データが作成後に改ざんされていないことを証明するものである。

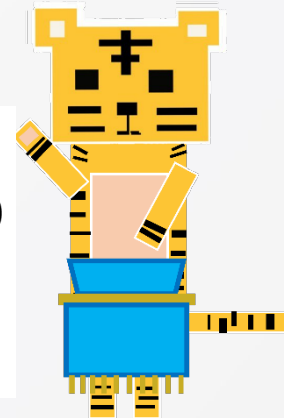
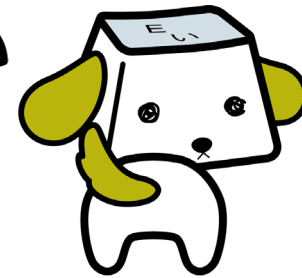
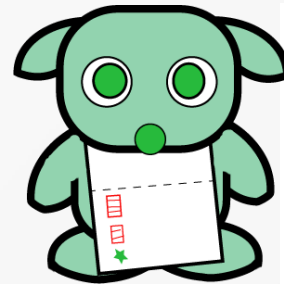
正答：エ

総務省が公表した「eシールに係る指針」（2021年6月）では、eシールとは、電子文書等の発行元の組織等を示す目的で行われる暗号化等の措置であり、当該措置が行われて以降に当該文書等が改ざんされていないことを確認する仕組みとされています。



どうだったかな？

全問正解したら自慢しよう！
いろいろな国家試験があるんだって
チャレンジするのもいいかもね



JIPDEC



あなたの未来を守る、創る。

25th
Anniversary