

業務に必要な情報セキュリティ知識

東京税理士会麹町支部情報システム委員会・業務対策部主催 合同研修会
2022年10月18日

東京税理士会情報システム部
菅沼俊広

1.税理士を取り巻く環境の変化

2.情報セキュリティ基礎知識

3.情報セキュリティ知識(中級編)

1.税理士を取り巻く環境の変化

概 要

経済・社会の更なるICT化が進展する中、ウィズコロナ・アフターコロナの社会・経済状況を見据え、ICTを前提とした税理士制度への変革が求められている。また、税理士には税理士業務のみならず、公益性の高い業務を担うことも求められている。

これら税理士を取り巻く状況の変化に的確に対応すべく、多様な人材の確保を図るとともに、税理士の資質の一層の向上など国民・納税者の税理士に対する信頼と納税者利便の向上を図る観点から、次のとおり税理士法の改正を要望する。

ICT化とウィズコロナ時代への対応

- 税理士の業務のICT化推進の明確化
- 税務代理における利便の向上
- 税理士会等の通知等の電子化
- 電子記録媒体の見直し
- 事務所規定の見直し

多様な人材の確保

- 受験資格要件の見直し

税理士に対する信頼の向上を図るための環境整備

- 税理士法人の業務範囲拡充
- 社員税理士の法定脱退事由の整備
- 税理士法違反行為の時効制度の創設

その他

- 法33条の2に規定する書面の名称変更及び資産税用の様式制定

① 税理士の業務のICT化推進の明確化

【改正要望内容】

経済のデジタル化、グローバル化の進展等の環境変化に伴う税理士制度の継続的発展を期するため、電子申告・納税、電子帳簿、マイナポータルの利用など税理士の業務のICT化の推進を通じて、納税義務者の利便性向上に努めることを明確化すべきである。

【要望の背景】

経済・社会の更なるICT化が進展する中、ウィズコロナ・アフターコロナの新しい社会も見据え、納税環境の電子化を推進していくことが喫緊の課題。こうした中、税理士は、税務に関する専門家としての使命を果たすため、ICTを積極的に利用し、納税者の利便の向上と社会全体の効率化・高度化に寄与していく必要。

【税理士法等改正の効果等（イメージ）】

税理士の業務のICT化の推進を通じた納税義務者の利便性向上

- ・納税者(依頼者)対応のデジタル化の推進
⇒ 資料授受の非書面化、税務相談等の非対面化による業務の迅速化・効率化
- ・行政対応のデジタル化の推進
⇒ 行政手続、調査対応等のペーパーレス化による迅速化・効率化
- ・業務環境のデジタル化の推進
⇒ ウェブ・クラウド・イントラネット等を活用したテレワークなどの働き方の多様化への対応



② 税務代理における利便の向上

【改正要望内容】

現状、税務代理は「税務官公署に対してする主張若しくは陳述につき、代理し、又は代行すること」とされているところ、その範囲に「税務官公署から納税者に対する通知等の受領を代理すること」が含まれることを明確化すべきである。

また、納税証明書の受領などで任意の委任状の提出が求められるが、税務代理権限証書で対応できるようにすべきである。

【要望の背景】

税務代理の円滑化に資する観点から、税務代理(法第2条第1項第1号)について、税務官公署から納税者に対する処分通知等の受領の代理を含めた整理をする必要。

また、納税者と税務代理人の関係に関する明示手続について、所要の整備を行う必要。

【税理士法等改正の効果等（イメージ）】

税理士が行う主な代理行為	税務代理への該当性	代理関係を示すために必要な書類	
<ul style="list-style-type: none"> 申告書の作成・提出 申告に関する税務官公署の質問への回答 調査での指摘に対する主張・陳述 調査の事前通知の受領 ※ 1 調査の結果通知・説明の受領 ※ 1 処分の通知の受領 	税務代理に該当する	法定の税務代理権限証書	※ 1 国税通則法等において、税務代理人のみが代理受領できることが明示されている（ただし税務代理の該当性については言及なし）。 ※ 2 納税証明書の交付請求自体は、国税通則法に基づく請求行為であるため、税務代理に該当する。
<ul style="list-style-type: none"> マイナポータルに格納されている納税義務者等の情報の取得 税務官公署に提出されている申告書等の閲覧 請求した納税証明書の受領 ※ 2 	税務代理に該当しない (一般的な代理)	任意の委任状	

① 税務代理に該当する旨を通告で明確化

② 税務代理権限証書に記載できるように、様式の見直し

③ 税理士会等の通知等の電子化

【改正要望内容】

税理士会総会等招集通知などについては、書面により行うこととされているところ、電子的に行うことができるよう改正すべきである。

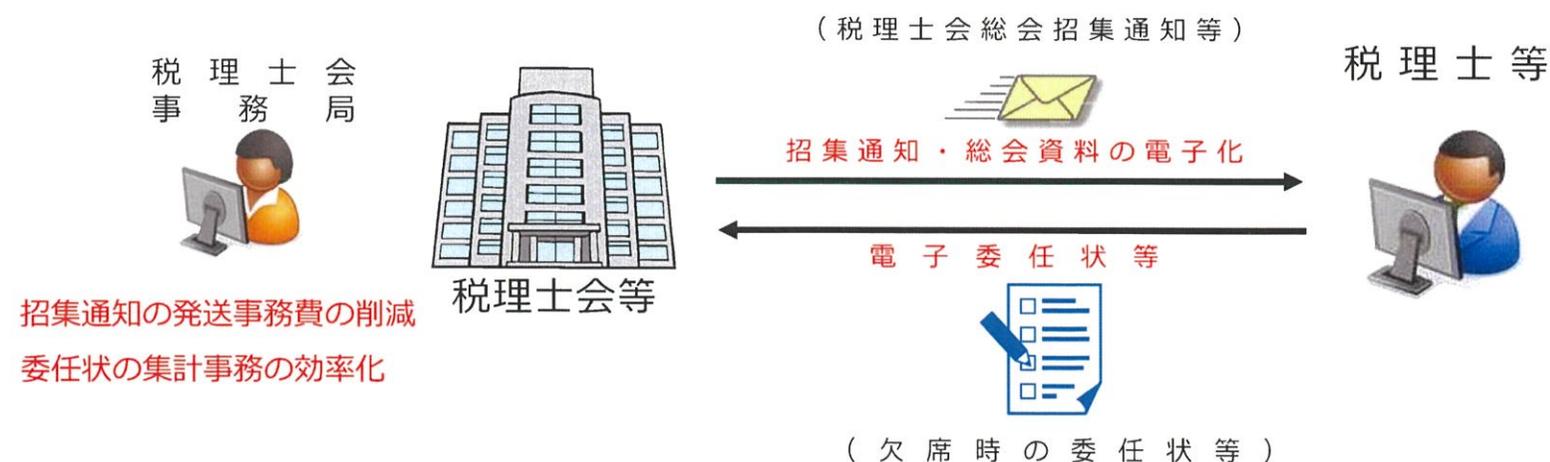
【要望の背景】

ウィズコロナ・アフターコロナの社会・経済状況を見据え、書面が前提とされている、税理士会総会等招集通知などの行政機関以外に対する通知等について、電子的な方法により「通知」を可能とする必要。

【対象文書等】

- ・ 税理士会総会における招集通知（令第7条第2項）
- ・ 総会欠席時の委任状（令第7条第4項）など

【税理士法等改正の効果等（イメージ）】



④ 電子記録媒体の見直し

【改正要望内容】

税理士法における電子記録媒体が「磁気ディスク」とされているところ、光ディスクその他の媒体が含まれるよう「電磁的記録」に改正すべきである。

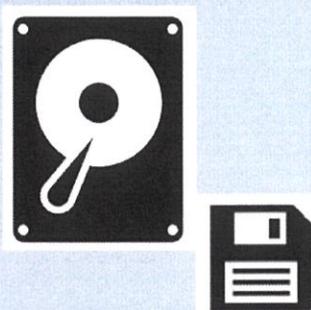
【要望の背景】

税理士名簿(法第19条)及び税理士が作成する帳簿(法第41条)において、電子記録媒体が「磁気ディスク」と規定されているところ、光ディスク等のその他の電子記録媒体をもって作成できるようにする必要。

【税理士法等改正の効果等（イメージ）】

【現状（限定）】

HDD・FDD
(磁気ディスク)



これに加えて

【電子記録媒体の例】

SSD
(フラッシュメモリ)



USBメモリ
(フラッシュメモリ)



DVD・CD
(光ディスク)



⑤ 事務所規定の見直し

【改正要望内容】

税理士業務のICT化や多様化する働き方に対応するため、物理的な設備の状況等のみを判定基準とする税理士事務所の定義を見直すべきである。

【要望の背景】

令和2年5月に作成した「税理士の業務とテレワーク(在宅勤務)～新型コロナウイルス感染防止対応版～」は在宅勤務に焦点を当てたものであり、在宅勤務以外の方策(例えば、サテライトオフィスの利用)について、検討を進め、税理士法基本通達を見直す必要。

【税理士法等改正の効果等（イメージ）】

【改正の方向性】

- ・ 事務所とは対外表示など委嘱者との契約上の所在地を表すものであり、かつ、税理士会や行政からの指導連絡監督が遅滞なく行われる環境下にあることが重要
- ・ 応接セットや事務用備品、会計・税務書類作成ソフト等を使用するためのPC等の設備は税理士業務を執行するために必要な備品ではあるが、デジタル化社会においては、事務所に固定的に設置されていなくても税理士業務を執行することは可能
- ・ 法第40条第3項（二ヶ所事務所禁止規定）の趣旨は、「①法律関係を明確にする上で便宜であること、②個人の監督能力を超えて業務の範囲を拡大することを規制すること」とされているが、使用人等に対する税理士の監督が機能・確保される限りにおいては、本規定以外の規定によって使用人による非違行為を抑止することが可能

○ 税理士法基本通達<抄> (事務所)

40-1 法第40条に規定する「事務所」とは、継続的に税理士業務を執行する場所をいい、継続的に税理士業務を執行する場所であるかどうかは、外部に対する表示の有無、設備の状況、使用人の有無等の客観的事実によって判定するものとする。

人との接触を8割減らす、10のポイント

緊急事態宣言の中、誰もが感染するリスク、誰でも感染させるリスクがあります。
新型コロナウイルス感染症から、あなたと身近な人の命を守れるよう、日常生活を見直してみましよう。

1 ビデオ通話で オンライン帰省 	2 スーパーは1人 または 少人数で すいている時間に 	3 ジョギングは 少人数で 公園は すいた時間、 場所を選ぶ 
4 待てる買い物は 通販 で 	5 飲み会は オンライン で 	6 診療は 遠隔診療 定期受診は間隔を調整 
7 筋トレやヨガは 自宅で動画を活用 	8 飲食は 持ち帰り、 宅配も 	9 仕事は 在宅勤務 通勤は医療・インフラ・ 物流など社会機能維持 のために 
10 会話は マスク をつけて 	3つの密を 避けましよう 1. 換気の悪い 密閉空間 2. 多数が集まる 密集場所 3. 間近で会話や発声をする 密接場面	
		手洗い・ 咳エチケット・ 換気や、健康管理 も、同様に重要です。

厚生労働省 新しい生活様式の実践例

(1) 一人ひとりの基本的感染対策

感染防止の3つの基本：①身体的距離の確保、②マスクの着用、③手洗い

- 人との間隔は、できるだけ2m（最低1m）空ける。
 - 会話をする際は、可能な限り真正面を避ける。
 - 外出時や屋内でも会話をするとき、人との間隔が十分とれない場合は、症状がなくてもマスクを着用する。ただし、夏場は、熱中症に十分注意する。
 - 家に帰ったらまず手や顔を洗う。
人混みの多い場所に行った後は、できるだけすぐに着替える、シャワーを浴びる。
 - 手洗いは30秒程度かけて水と石けんで丁寧に洗う（手指消毒薬の使用も可）。
- ※ 高齢者や持病のあるような重症化リスクの高い人と会う際には、体調管理をより厳重にする。

移動に関する感染対策

- 感染が流行している地域からの移動、感染が流行している地域への移動は控える。
- 発症したときのため、誰とどこで会ったかをメモにする。接触確認アプリの活用も。
- 地域の感染状況に注意する。

(2) 日常生活を営む上での基本的生活様式

- まめに手洗い・手指消毒 □咳エチケットの徹底
- こまめに換気（エアコン併用で室温を28℃以下に） □身体的距離の確保
- 「3密」の回避（密集、密接、密閉）
- 一人ひとりの健康状態に応じた運動や食事、禁煙等、適切な生活習慣の理解・実行
- 毎朝の体温測定、健康チェック。発熱又は風邪の症状がある場合はムリせず自宅で療養



密集回避



密接回避



密閉回避



換気



咳エチケット



手洗い

厚生労働省 新しい生活様式の実践例

(3) 日常生活の各場面別の生活様式

買い物

- 通販も利用
- 1人または少人数ですいた時間に
- 電子決済の利用
- 計画をたてて素早く済ます
- サンプルなど展示品への接触は控えめに
- レジに並ぶときは、前後にスペース

娯楽、スポーツ等

- 公園はすいた時間、場所を選ぶ
- 筋トレやヨガは、十分に人との間隔を
もしくは自宅で動画を活用
- ジョギングは少人数で
- すれ違うときは距離をとるマナー
- 予約制を利用してゆったりと
- 狭い部屋での長居は無用
- 歌や応援は、十分な距離かオンライン

公共交通機関の利用

- 会話は控えめに
- 混んでいる時間帯は避けて
- 徒歩や自転車利用も併用する

食事

- 持ち帰りや出前、デリバリーも
- 屋外空間で気持ちよく
- 大皿は避けて、料理は個々に
- 対面ではなく横並びで座ろう
- 料理に集中、おしゃべりは控えめに
- お酌、グラスやお猪口の回し飲みは避けて

イベント等への参加

- 接触確認アプリの活用を
- 発熱や風邪の症状がある場合は参加しない

(4) 働き方の新しいスタイル

- テレワークやローテーション勤務
- 時差通勤でゆったりと
- オフィスはひろびろと
- 会議はオンライン
- 対面での打合せは換気とマスク

※ 業種ごとの感染拡大予防ガイドラインは、関係団体が別途作成

「ニューノーマル時代」のイメージ

新しい住まいのあり方

- ・ 郊外への移住、複数拠点化
- ・ リフレッシュのための自然環境
- ・ パーソナルスペース/ワークスペースの確保 等



新しいオフィスのあり方

- ・ 開放的・分散的なレイアウト
- ・ 拠点の分散化、シェア化
- ・ 転勤、単身赴任の減少 等



オンライン化の定着

- ・ あらゆる接点がオンラインに (医療、教育、公的手続き等)



バーチャル空間/体験の普及

- ・ VR/ARによる新たなバーチャル体験の広まり
- ・ バーチャルならではの付加価値



リアルな体験価値の再認識

- ・ 野球や歌劇、旅行等、リアルな体験でしか味わうことができない喜びや感動の渴望



オペレーションの省人化

- ・ 自動化や遠隔化による、人どうしが接しない無人オペレーション



パーソナルモビリティの普及

- ・ 3密を避けた移動手段の広まり
- ・ 混雑を避けた快適な移動空間



シェアリングの環境変化

- ・ 移動や居住空間など経済的な合理性よりも所有による安全を優先



全員参加のデジタル活用

- ・ 多言語対応範囲の拡大、新しいインタフェースの提供、デジタルライフを支援するサービス



パーソナライズされたサービス

- ・ 必要な人に対して必要なレベルのサービスを必要なだけ、必要なタイミングで提供



電子政府

- ・ 全ての行政手続きをオンラインで
- ・ ワンストップ、ワンスオンリー
- ・ IT基本法等諸制度の適時改訂



データ利活用

- ・ 医療、教育、税等の分析結果を用いた適切な対応および評価
- ・ 産官学の連携促進



個人認証

- ・ サイバー空間における個人認証の新しい仕組み
- ・ マイナンバー等の活用促進



災害対策

- ・ 災害シミュレーションの実施
- ・ 災害発生時のスピード感のある行政支援の実現



趣旨

デジタル社会の形成が、我が国の国際競争力の強化及び国民の利便性の向上に資するとともに、急速な少子高齢化の進展への対応その他の我が国が直面する課題を解決する上で極めて重要であることに鑑み、デジタル社会の形成に関する施策を迅速かつ重点的に推進し、もって我が国経済の持続的かつ健全な発展と国民の幸福な生活の実現に寄与するため、デジタル社会の形成に関し、基本理念及び施策の策定に係る基本方針、国、地方公共団体及び事業者の責務、デジタル庁の設置並びに重点計画の作成について定める。

概要

1. デジタル社会

「デジタル社会」を、インターネットその他の高度情報通信ネットワークを通じて自由かつ安全に多様な情報又は知識を世界的規模で入手し、共有し、又は発信するとともに、先端的な技術をはじめとする情報通信技術を用いて電磁的記録として記録された多様かつ大量の情報を適正かつ効果的に活用することにより、あらゆる分野における創造的かつ活力ある発展が可能となる社会と定義する。

2. 基本理念

デジタル社会の形成に関し、ゆとりと豊かさを実感できる国民生活の実現、国民が安全で安心して暮らせる社会の実現、利用の機会等の格差の是正、個人及び法人の権利利益の保護等の基本理念を規定する。

3. 国、地方公共団体及び事業者の責務

デジタル社会の形成に関し、国、地方公共団体及び事業者の責務等を規定する。

4. 施策の策定に係る基本方針

デジタル社会の形成に関する施策の策定に当たっては、多様な主体による情報の円滑な流通の確保（データの標準化等）、アクセシビリティの確保、人材の育成、生産性や国民生活の利便性の向上、国民による国及び地方公共団体が保有する情報の活用、公的基礎情報データベース（ベース・レジストリ）の整備、サイバーセキュリティの確保、個人情報保護等のために必要な措置が講じられるべき旨を規定する。

5. デジタル庁の設置等

別に法律で定めるところにより内閣にデジタル庁を設置し、政府がデジタル社会の形成に関する重点計画を作成する。

6. 高度情報通信ネットワーク社会形成基本法の廃止等

高度情報通信ネットワーク社会形成基本法（IT基本法）を廃止するほか、関係法律の規定の整備を行う。

7. 施行期日

令和3年9月1日

「デジタルライフを支援するサービス」のイメージ

- デジタルシフトは経済の効率性を高める一方で、新しい格差を生み出す可能性が高い
- 全員参加のデジタルシフトが重要であり、対応が困難な個人を支援する仕組みが必要

デジタルライフ支援サービス(仮称)



新たなオンラインサービスを
上手く活用できない・・・

- 社会サービスは「デジタル化」、
「オンライン化」が一気に加速
 - － オンライン行政手続き
 - － オンライン診療
 - － オンライン教育 など
- デジタルサービスに馴染みの
ない方でもこれらのサービスを
利用可能となるように支援

コールセンター

自宅訪問

Webサイト

相談窓口
(駆け込み寺)



多様なチャネルで個人を支援
(新たな事業創出の可能性)



初期設定の代行、サービス利用に関する研修機会の提供等、サービス利用開始時点における課題解消支援を重点的に実施
物理的・精神的なサービス利用の障壁をなくし、生活の一部としてサービスを利活用出来る風土を醸成

※緊急事態宣言発出に伴う事務局の執務体制について

 会員専用ページ[ホーム](#) [税理士とは](#) [税についての相談](#) [税理士を目指す](#)[日本税理士会連合会とは](#) [税理士会の事業](#) [お知らせ](#)[ホーム](#) > [お知らせ](#) > [コロナ対策](#) > 「税理士の業務とテレワーク(在宅勤務)～新型コロナウイルス感染防止対応版～」の掲載について (会員専用ページ)

「税理士の業務とテレワーク(在宅勤務)～新型コロナウイルス感染防止対応版～」の掲載について (会員専用ページ)

2020年4月15日 [お知らせ](#)

本会では、従前より税理士の業務とテレワークについて検討しているところ、新型コロナウイルスの感染防止の観点から、緊急的に、開業税理士、社員税理士、使用人等及び所属税理士の在宅勤務に特化した標題FAQを作成しました。

関連情報

[税理士の業務とテレワーク\(在宅勤務\)～新型コロナウイルス感染防止対応版～](#)
[PDF/184KB] 

お知らせ

- ▶ [2020年](#)
- ▶ [2019年](#)
- ▶ [2018年](#)
- ▶ [2017年](#)
- ▶ [2016年](#)
- ▶ [2016年1月以前の納税者向けのお知らせ](#)
- ▶ [2016年1月以前の税理士向けのお知らせ](#)

税理士を探す

<https://www.nichizeiren.or.jp/whats-new/200415b/>

税理士の業務とテレワーク(在宅勤務)～新型コロナウイルス感染防止対応版～ 日本税理士会連合会 業務対策部 令和2年4月

新型コロナウイルスの感染拡大は社会のいたるところで深刻な影響をもたらし、外出自粛が要請される中、税理士事務所における業務のあり方についても通常の従事形態ではない方法を探らざるを得ない状況となっています。

業務対策部では、現行税理士法下の税理士の業務とテレワークについて検討を進めているところですが、今般の新型コロナウイルス感染拡大への対応の観点から、緊急に、テレワーク類型のうち在宅勤務に関するFAQを取りまとめましたので、参考としてください。

ただし、いずれの場合であっても、**税理士法第38条(秘密を守る義務)及び同法第54条(税理士の使用人等の秘密を守る義務)**にご注意願います。

開業税理士

Q1 開業税理士が、登録している事務所所在地とは別の自宅で税理士業務を行う場合、税理士法上の問題点・留意事項はありますか？

社員税理士

Q2 税理士法人の社員税理士が、自宅で税理士業務を行う場合、税理士法上の問題点・留意事項はありますか？

使用人等

Q3 税理士又は税理士法人の使用人等(所属税理士を除く。)が、その自宅で税理士業務の補助業務を行う場合、税理士法上の問題点や留意事項はありますか？

所属税理士が行う直接受任業務

Q4 所属税理士が、自宅で直接受任業務を行う場合に、税理士法上の問題点・留意事項はありますか？

所属税理士が行う補助者としての業務

Q5 所属税理士が、自宅で補助者として税理士業務の補助業務や補助者としての税理士業務を行う場合に、税理士法上の問題点や留意事項はありますか？

<https://www.nichizeiren.or.jp/wp-content/uploads/member/doc/telework.pdf>

税理士の業務とテレワーク(在宅勤務)～新型コロナウイルス感染防止対応版～ 日本税理士会連合会 業務対策部 令和2年4月

* 税理士又は税理士法人の使用人等に対する監督が明確である状態とは？

使用人等が税理士の監督下にあるか否かの判断については、当該監督義務が置かれた趣旨が、税理士事務所の使用人等の非違行為の防止の観点からのものであることを考慮すれば、自宅での業務に非税理士行為を防止するための一定の制限を加えることで、使用人等に対する税理士の監督が存する状態と捉えることは可能であると考えます。

具体的には、平時においては、次のようなシステムが組み立てられていることで、使用人等に対する監督義務が果たされていると捉えることは可能であると考えます。

イ 自宅で業務を開始する際の確認

- ・システムログイン、ログアウトの際の確認を税理士又は税理士法人が行うような機能を加えることなど。
- ・使用人等の自宅での業務記録(ログ)を保存し、税理士又は税理士法人が確認できるような機能を加えることなど。

ロ 自宅で行うことができる業務を制限

- ・特に税務書類作成業務の補助業務について、税理士又は税理士法人の確認を経てからでないと申告事務に入れないような機能を加えることなど。
- ・自宅における使用人等の非税理士行為を防ぐため、税務書類等の印刷、電子送信を自宅においてできない機能を加えることなど。

ハ 新規顧客登録事務の制限

- ・新規顧客の登録事務を制限すると、当該事務は税理士事務所では行えなくなり、非税理士行為等の防止に相当程度期待できる。

<参考: 税理士法第41条の2、同法第48条の16、同法第52条>

<https://www.nichizeiren.or.jp/wp-content/uploads/member/doc/telework.pdf>

従来型



進化型

業務実施場所は問わない



税理士の管理



税理士



ノートパソコン



スマートフォン



サーバ(クラウド)



税理士



ノートパソコン



スマートフォン

税理士法40条（事務所の設置） 通達 40-1（事務所）

ノートパソコンとスマートフォンがあればどこにいても業務はできる

(事務所の設置)

第40条

税理士(税理士法人の社員(財務省令で定める者を含む。第4項において同じ。))を除く。次項及び第3項において同じ。)及び税理士法人は、税理士業務を行うための事務所を設けなければならない。

2 税理士が設けなければならない事務所は、税理士事務所と称する。

3 税理士は、税理士事務所を二以上設けてはならない。

(事務所)

40-1

法第40条第1項に規定する「**税理士業務を行うための事務所**」とは、**税理士業務の本拠**をいい、**税理士業務の本拠**であるかどうかは、**委嘱者等に示す連絡先など外部に対する表示に係る客観的事実**によって判定するものとする。**この場合において、「外部に対する表示」には、看板等物理的な表示やウェブサイトへの連絡先の掲載のほか、契約書等への連絡先の記載などが含まれることに留意する。**

(二ヶ所事務所の禁止)

40-2

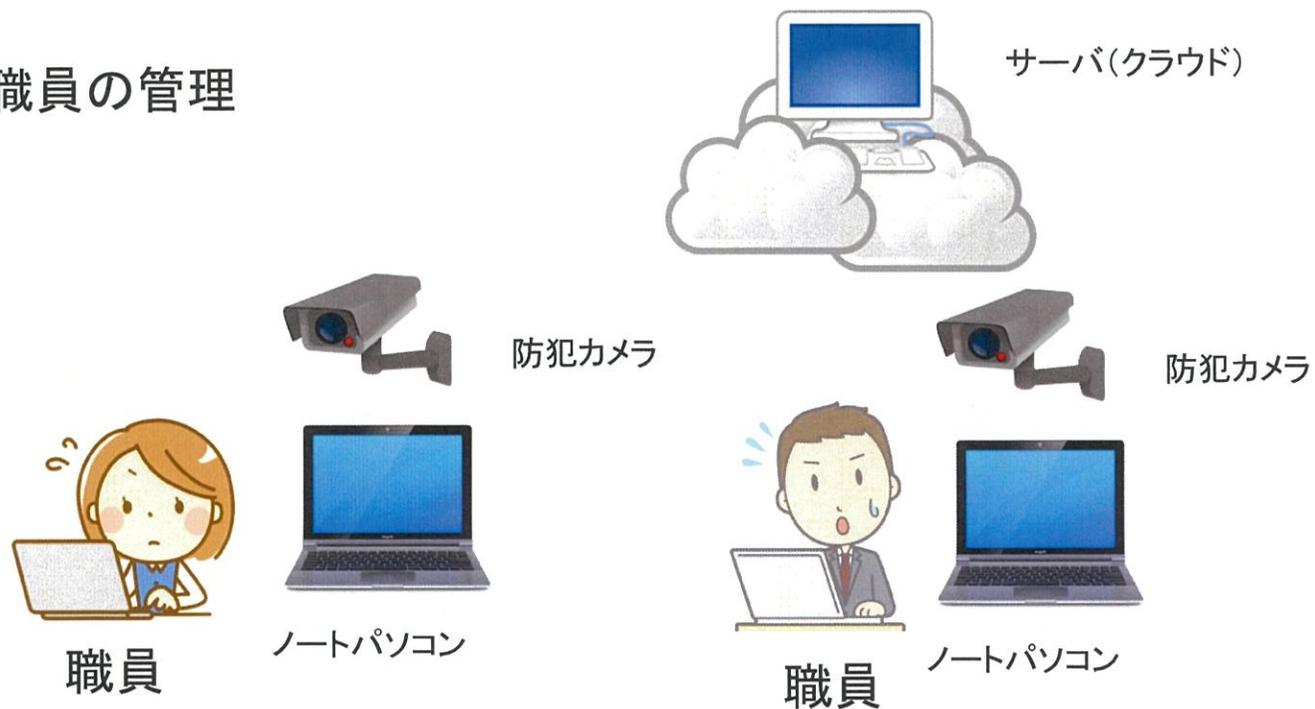
法第40条第3項の「**税理士事務所を二以上設けて**」いる場合とは、**例えば、自宅以外の場所に税理士事務所を設け、40-1の「外部に対する表示」をしている状態で、自宅においても40-1の「外部に対する表示」をして税理士業務を行っている場合などをいう。**したがって、**自宅等の税理士事務所以外の場所で税理士業務を行っていても、その場所に40-1の「外部に対する表示」に係る客観的事実がなく、法第40条第1項に規定する「税理士業務を行うための事務所」と判定される状態でない場合には、税理士事務所を二以上設けている場合には該当しない。**

改正後の税理士法令通達集(法律・政令・省令・通達)〈未施行条文含む〉

※令和4年4月1日現在

税理士法改正に係る参考資料について 2022年4月14日 日本税理士会連合会 より

職員の管理



税理士



税理士法41条の2（使用人等に対する監督義務）

貸与するノートパソコンは、税理士が設定し、

- ・ログ情報管理(キーログ)
- ・業務処理データは日次でサーバ(クラウド)に保管
- ・私物端末使用禁止
- ・監視カメラによる監視

(使用人等に対する監督義務)

第41条の2

税理士は、税理士業務を行うため使用人その他の従業者を使用するときは、税理士業務の適正な遂行に欠けるところのないよう当該使用人その他の従業者を監督しなければならない

(使用人等に対する監督義務)

41の2-1

税理士の使用人その他の従業者(以下「使用人等」という。)に対する監督義務は、税理士及びその使用人等が事務を行う場所によって異なることはない。

したがって、使用人等に対する監督方法として、対面による監督を行うことができない場合でも、情報通信技術を利用する方法などにより、適切に監督が行われている場合には、監督義務が果たされていると判断することに留意する。

なお、情報通信技術を利用した使用人等の適切な監督方法としては、例えば、次に掲げるような、事前及び事後の確認を行う方法がある。

- (1) 使用人等と委嘱者等との情報通信技術を利用した打合せに、使用者である税理士が情報通信技術を利用して参加する方法
- (2) 使用人等が税理士業務の補助を行った履歴について情報通信技術を利用して確認する方法

改正後の税理士法令通達集(法律・政令・省令・通達)〈未施行条文含む〉

※令和4年4月1日現在

税理士法改正に係る参考資料について 2022年4月14日 日本税理士会連合会 より



情報通

2020. September 9月号

発行：東京税理士会 情報システム部
 題字：神津 信一（四谷）
 （税理士会員章の日輪と八重桜をイメージしています。）

ツールを利用した事務所職員の管理監督について

情報システム部委員 杉山 靖彦

1. テレワークの準備は進んでいますか？

会員の先牛方の事務所においてテレワークの準備は進んでおりますでしょうか？新型コロナウイルスに対し、4、5月の自粛は私たちにとって感染予防のためのものでしたが、感染第2波による陽性者数拡大下においては、私たちの税理士事務所においても、職員が出勤停止になったり、場合によっては事務所閉鎖が求められるもおかしくない状況となってきています。

職員のご家族の学校や職場で陽性者が出るだけで、その職員は明日から急に出勤を控えなければいけなくなるかもしれません。万が一、その職員にも陽性反応が出たとしたら、事務所は一定期間閉鎖となってしまいます。

今やテレワークの準備は、予防のためのものから、陽性者が出てしまったとしても税理士事務所業務を続けるためのものへとその意味が変わってきているのです。

2. ふたつの管理監督

「簡単にテレワークというが、私たち税理士にとって大きな問題として職員の管理監督義務があるではないか。テレワークにおいて、どのようにして職員の管理監督を行うのか？」という声を耳にします。そこで今回は、テレワーク下における職員の管理監督について、技術的な考え方を解説していきたいと思えます。

職員の管理監督には、大きく分けて、労務管理としての管理監督の側面と、税務会計業務の内容の管理監督の側面があります。

3. 労務管理としての管理監督

労務管理としての管理監督は、税理士事務所に限った話ではなく、労働者として何時から何時まで、職員が業務に精勤しているかどうかという管理となります。テレワークの大きな問題として、この管理ができないという点を挙げる企業が数多くあり、実際にサボっている労働者も一定数いることは間違いなさそうです。

しかしながら、単にサボっていないか、過重労働になっていないかというだけでなく、勤務中に事故などから職員を守るという責任も税理士は負っていることを忘れてはいけません。

その観点から私は、税理士は職員と必要に応じて常にコミュニケーションを取ることができる状態にあるべきです。真面目に業務に取り組んでいるか？体調の急変などもなく、順調に業務に取り組んでいるか？ということが確認できる体制です。

私は、勤務中に常にカメラを通じて、顔を見てコミュニケーションを取ることができる状態を維持することが、その体制であると考えています。カメラによる監視ではありません。事務所に出勤したら、必要に応じて顔を見て話しができる状態にあるのと同じ状態を維持するという事です。

4. 税務会計業務の内容の管理監督

そして税理士にとって最も重要なのが、税務会計業務の内容の管理監督です。要は、その職員がいつどのような作業をしているかということ。税理士が確認でき、必要に応じて税理士に相談報告をして、職員が業務を遂行できる環境をテレワークにおいて実現することです。

上述のとおり、常に顔を見てコミュニケーションが取れる体制を作ることそのひとつですが、職員がやっている業務を常に見ることができ、自動的に記録を取る環境こそが税務会計業務の内容の管理監督の肝だと考えています。それを実現するのが、事務所のパソコンをリモート操作するアプリケーションであり、操作ログを記録するアプリケーションです。セキュリティの観点からも、基本的には事務所からデータを持ち出させません。証憑やデータは事務所内のサーバーやパソコン内にあり、その閲覧や処理はすべて事務所内のパソコンで行われます。職員が事務所勤務していれば当たり前のことですが、テレワークにおいても同じ環境を構築するのです。職員はリモートでその事務所のパソコンを操作することによって業務を行います。しかも、その操作については記録を自動的に取っていくのです。

このような環境を構築すれば、職員に対する牽制も効きますし、万が一の場合でもその証憑が残ります。

しかし、ここまで行くと単なる監視にとどまってしまう。出来上がった資料や税務書類については、紙に印刷したものを税理士が確認するなどコミュニケーションがとれていたかと思いますが、テレワーク下ではそのようにアナログな紙でのやり取りはできません。

そこで出てくるのがワークフローです。一般企業では多くの企業において、稟議書の回覧がデジタル化されてワークフローに置き換わってきています。

会計事務所では職員と税理士の二人でのやり取りかもしれませんが、テレワーク下における資料や書類の確認依頼と承認のやり取りを実現するのが、このワークフローなのです。

本会業務の対応について(重要) 令和4年4月4日
税理士登録関係等のお手続きにつきましては郵便での提出のみ対応させていただいており、通常より手続き完了までにお時間をいただいております。ご不便をおかけいたしますが、ご理解、ご協力の程お願いいたします。
詳しくはこちら

新型コロナウイルス感染症の影響による所得税等の確定申告の申告期限等の延長の申請について 令和4年2月3日更新(国税庁)
詳しくはこちら

【第五世代ICカードを取得した税理士の方へ】e-Tax・eTAXで使用するICカードの更新・登録作業が必要です!
詳しくはこちら

申告所得税等の申告・納付期限を延長した場合の振替日について 令和4年3月16日更新(国税庁)
詳しくはこちら

東京税理士会について

お知らせ

一般の方へ

税理士の方へ

東京税理士会 税理士の方へ 税理士のためのICT講座 「情報通(紙面版)」バックナンバー

税理士の方へ

お知らせ

会報「東京税理士界」より

会報相談室・相談事例紹介

国際部レポート

税理士のためのICT講座

業務資料

手続・届出・証明について

お知らせ

よくある質問

変更

税理士法人

税理士証書の定期交換

証書・バッジ

証明書

入会・退会

その他手続き

「情報通(紙面版)」バックナンバー [2003年~] (更新日:2022年5月1日)

「情報通」バックナンバーはPDF書類です

2022年 5月号	<ul style="list-style-type: none"> e-Taxによる情報誌明書の交付手続き
2022年 4月号	<ul style="list-style-type: none"> 情報誌編集@千秋ヶ谷とは
2022年 3月号	<ul style="list-style-type: none"> 電子帳簿保存法(電子取引の保存)の改正その後
2022年 2月号	<ul style="list-style-type: none"> 確定申告書等作成コーナーについて
2022年 1月号	<ul style="list-style-type: none"> 「支部事務局と会員間の連絡方法に関するアンケート」の結果について
2021年 12月号	<ul style="list-style-type: none"> 第五世代税理士用電子証明書取得について
2021年 11月号	<ul style="list-style-type: none"> 年末調整手続きの電子化はどうなった?
2021年 10月号	<ul style="list-style-type: none"> デジタル化相談室について
2021年 9月号	<ul style="list-style-type: none"> 電子申告に関する税理士交代時の注意点と手続き
2021年 8月号	<ul style="list-style-type: none"> クレジットカード納付とスマートフォン納付へ税理士が知っておいた方がよいことへ
2021年 7月号	<ul style="list-style-type: none"> デジタル化委員会創設記念～デジタル庁設置の経緯と税理士業務のデジタル化へ
2021年 6月号	<ul style="list-style-type: none"> 電子帳簿保存法、令和3年度改正について～続編～
2021年 5月号	<ul style="list-style-type: none"> 電子帳簿保存法、令和3年度改正について

テレワークを活用する企業、労働者の皆さまへ



テレワークの

適切な導入及び 実施の推進のための ガイドライン



事業主、企業の労務担当者の方へ

テレワークガイドラインを改定しました 新たな日常、新しい生活様式に対応した良質なテレワークを推進しましょう

テレワークとは、インターネットなどのICTを活用し自宅などで仕事をする、働く時間や場所を柔軟に活用できる働き方です。

1 はじめに

厚生労働省は、令和3年3月にテレワークガイドラインを改定しました。

このガイドラインは、使用者が適切に労務管理を行い、労働者が安心して働くことができる良質なテレワークを推進するため、テレワークの導入と実施に当たり、労務管理を中心に、労使双方にとって留意すべき点、望ましい取り組み等を明らかにしたものです。

このガイドラインを参考に、労使が十分に話し合いを行い、良質なテレワークを導入し、定着させていくことが期待されます。

2 テレワークのメリット

- 業務効率化による生産性の向上にも役立つ
 - 育児や介護等を理由とした労働者の離職の防止、遠隔地の優秀な人材の確保
 - オフィスコストの削減
- などのメリットがあります。

3 業務を行う場所に応じたテレワークの特徴

在宅勤務 通勤を要しないことから、事業場での勤務の場合に通勤に要する時間を柔軟に活用できます。
また、例えば育児休業明けに短時間勤務等と組み合わせて勤務したり、保育所の近くで勤務したりすることが可能となることから、仕事と家庭生活との両立に資する働き方です。

自宅の近くや通勤途中の場所等に設けられたサテライトオフィス（シェアオフィス、コワーキングスペースを含む）での勤務は、通勤時間を短縮しつつ、在宅勤務やモバイル勤務以上に作業環境の整った場所で就労可能な働き方です。

2. サテライトオフィス勤務

労働者が自由に働く場所を選択できる、外勤における移動時間を利用できるなど、働く場所を柔軟にすることで業務の効率化を図ることが可能な働き方です。

3. モバイル勤務

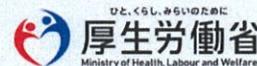
テレワークで困ったらどこに相談すればいいんだろう

⇒P6へ



労働者が自宅等でテレワークを行うときは、何に気をつけてもらえばいいんだろう

⇒P7へ



ガイドラインの概要は次のページをご確認ください

費用負担 ▶ P3

労働時間管理 ▶ P4

安全衛生 ▶ P5

中小企業事業主の皆様がご利用可能な助成金については最終ページをご確認ください

人材確保等支援助成金（テレワークコース）のご案内

良質なテレワークを制度として導入し、実施することにより、労働者の人材確保や雇用管理改善等の観点から効果をあげる中小企業事業主（※）を支援します！

※ テレワーク勤務を、新規に導入する事業主の方及び試行的に導入している又は試行的に導入していた事業主の方が対象です。

支給要件及び支給額は次のとおりです。詳細は支給要領等をご確認ください。

	支給要件	支給額
① 機器等導入助成	<ul style="list-style-type: none"> 新たに、テレワークに関する制度を規定した就業規則または労働協約を整備すること。 テレワーク実施計画認定日以降、機器等導入助成の支給申請日までに、助成対象となる取組を1つ以上行うこと。 評価期間（機器等導入助成）における、テレワークに取り組む者として事業主が指定した対象労働者のテレワーク実績が、次のいずれかを満たすこと。 <ul style="list-style-type: none"> ✓ 評価期間（機器等導入助成）に1回以上対象労働者全員がテレワークを実施する 又は ✓ 評価期間（機器等導入助成）に対象労働者がテレワークを実施した回数の週平均を1回以上とする テレワークの実施促進について企業トップ等からのメッセージ発信を行うなど、労働者がテレワークを実施しやすい職場風土作りの取組を行う事業主であること。 	<p>支給対象経費の 30%</p> <p>※以下のいずれか低い方の金額が上限額 ・100万円 又は ・20万円×対象労働者数</p>
	<ul style="list-style-type: none"> 評価期間後1年間の離職率が、計画提出前1年間の離職率以下であること。 評価期間後1年間の離職率が30%以下であること。 評価期間（目標達成助成）に、1回以上テレワークを実施した労働者数が、評価期間（機器等導入助成）初日から1年を経過した日における事業所の労働者数に、計画認定時点における事業所の労働者全体に占める対象労働者の割合を掛け合わせた人数以上であること。 <p>※()内は生産性要件を満たした場合に適用</p>	<p>支給額</p> <p>支給対象経費の 20% (35%)</p> <p>※以下のいずれか低い方の金額が上限額 ・100万円 又は ・20万円×対象労働者数</p>

助成対象となる取組

- 就業規則・労働協約・労使協定の作成・変更
- 外部専門家によるコンサルティング
- テレワーク用通信機器等（※）の導入・運用
 - ※ 以下のテレワーク用サービス利用料も助成対象となります。
 - リモートアクセス及びリモートデスクトップサービス
 - 仮想デスクトップサービス
 - クラウドPBXサービス
 - web会議等に用いるコミュニケーションサービス
 - ウイルス対策及びエンドポイントセキュリティサービス
- 労務管理担当者に対する研修
- 労働者に対する研修

ご利用の流れ等については裏面をご確認ください。

- 使用者が適切に労務管理を行いながら、労働者が安心して働くことのできる形で良質なテレワークを推進し、定着させていくことができるよう、厚生労働省では「テレワークの適切な導入及び実施の推進のためのガイドライン」を策定しています。
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/koyou_roudou/roudoukijun/shiqoto/guideline.html
- テレワークの導入に当たっては、セキュリティへの配慮も必要です。テレワークセキュリティガイドライン（総務省）などもご参照ください。
https://www.soumu.go.jp/main_sosiki/joho_tsusin/telework/index.htm

ご利用の流れ



助成金の詳細・問合せ先

助成金の支給要件や申請方法等の詳細については、厚生労働省HPをご確認いただくか、最寄りの都道府県労働局雇用環境・均等部（室）へお問い合わせください。

人材確保等支援助成金 検索



厚生労働省HPは
こちらのQRコードからも
アクセス可能です。

テレワークを有効に活用しましょう

～新型コロナウイルス感染症対策のためのテレワーク実施～

テレワークの活用

「テレワーク」とは、インターネットなどのICTを活用し自宅などで仕事をする、時間や場所を有効に活用できる柔軟な働き方です。
新型コロナウイルス感染症の感染拡大防止の観点からも、有効な働き方です。

テレワークの効果

企業のメリット

- 非常時に感染リスクを抑えつつ、事業の継続が可能
- 労働者の通勤負担の軽減が図れる
- 優秀な人材の確保や、雇用継続につながった
- 資料の電子化や業務改善の機会となった

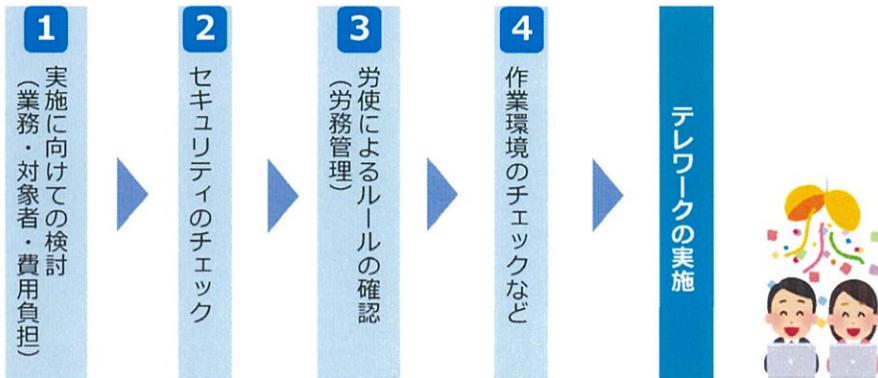


労働者のメリット

- 通勤の負担がなくなった
- 外出しなくて済むようになった
- 家族と過ごす時間や趣味の時間が増えた
- 集中力が増して、仕事の効率が良くなった



テレワーク実施までの流れ



1 実施に向けての検討(業務の切り出し・対象者の選定・費用負担)

業務の切り出し

- 対象作業の選定は、「業務単位」で整理することがポイント。
- テレワークでは難しいと思われる業務についても、緊急事態宣言を受けて、一旦やってみたら意外にできることが多かったというケースも多い。
- 仕事のやり方を工夫することで一気に進む場合も。



仕事のやり方を変える5つの取り組み例

1. 仕事の見える化
2. 仕事のプロセスの見直し
3. 電子化・ペーパーレス化
4. コミュニケーションのIT化
(メール、チャット、WEB会議等)
5. 申請業務のクラウド化
タイムカード、出張申請、経費精算、スケジュールボードetc.

出典：「テレワークではじめる働き方改革 テレワークの導入・運用ガイドブック」

対象者の選定

- 業務命令として在宅勤務を命じる場合には、業務内容だけでなく、**本人の希望も勘案**しつつ、決定しましょう。
- 正規雇用労働者、非正規雇用労働者といった雇用形態の違いのみを理由として対象者から除外することがないようにしましょう。
 (※) 正規雇用労働者と非正規雇用労働者との不合理な待遇差については、パートタイム・有期雇用労働法、労働者派遣法により禁止されており、雇用形態のみを理由にテレワークの対象者から除外することは、これらの法律に違反する可能性があります。

費用負担

- 労働者に過度の負担が生じることは望ましくありません。費用負担についてはトラブルになりやすいので、労使でよく話し合うことが必要です。

機器購入費

パソコン本体や周辺機器、携帯電話、スマートフォンなどについては、会社から貸与しているケースが多い

通信費

通信回線の使用料等は個人使用と業務使用との切り分けが困難であるため、一定額を会社負担としている例も見られる

消耗品購入費

・ 文具消耗品は会社が購入したものを使用
 ・ 切手や宅配メール便等は事前に配布
 ・ 会社宛の宅配便は着払いとするなど

光熱費

頻度により様々。光熱費は、業務使用分との切り分けが困難なため、テレワーク勤務手当てに含めて支払う企業の例もみられる

出典：「テレワーク導入のための労務管理等Q&A集」

2 セキュリティのチェック

- 会社のパソコン(PC)を社外に持ち出す場合には、**PCの盗難や紛失による情報漏洩**のリスクがあることから、**セキュリティ対策のなされたPCやシンクライアントパソコンを貸与する**などの工夫が必要です。
- また、自宅のPCを使って業務を行う場合には、ウイルス対策ソフトや最新アップデートの適用などの**セキュリティ対策が適切に行われているかを確認**する必要があります。
- その他、総務省においてテレワークセキュリティに関するガイドラインやチェックリストが公開されていますので、ご活用ください。

3 ルールの確認 (労務管理)

労働時間

在宅勤務などのテレワーク時にも、労働基準法などの労働法令を遵守することが必要です。テレワーク時の労務管理について確認し、ルールを定めましょう。
詳しくは「テレワーク実施のための参考資料(p.4)」をご参照ください。

労働時間

- 労働時間を適正に把握・管理し、長時間労働を防ぐためにも、労働者の労働日ごとの始業・終業時刻を確認し、記録しましょう。
- 通常の労働時間制、フレックスタイム制のほかに、労働者が事業場外で業務に従事した場合で労働時間を算定することが困難なときには事業場外みなし労働時間制なども活用できます。
- 中抜け時間の取扱いや、時間外・休日・所定外深夜の労働を行う場合のルールを労使でよく話し合い就業規則等で定めておくことが重要です。

【労働時間管理方法の一例】

■ 電子メール

- ・使い慣れている
- ・業務の報告を同時に行いやすい
- ・担当部署も一括で記録を共有できる

■ 電話

- ・使い慣れている
- ・時間がかからない
- ・コミュニケーションの時間が取れる

■ 勤怠管理ツール

- ・電子メール通知なくてよい
- ・大人数を管理しやすい
- ・担当部署も記録を共有できる

■ 勤怠管理システム

- (仮想オフィス、グループウェア等)
- ・個別に報告する手間がかからない

安全衛生

- テレワーク中に孤独や不安を感じることがあります。オンライン会議などを活用して、上司・部下や同僚とコミュニケーションをとるようにしましょう。
- なお、業務中の傷病は労災の対象になります。
- 長時間労働とならないようにしましょう。

業績評価、人事管理、ハラスメントへの対応

- テレワークを行う労働者について特別の取扱いを行う場合は、よく確認しましょう。
- 新規で採用する場合には、就業場所などについて労働条件の明示が必要です。
- 事業主はテレワークの際にも、関係法令・関係指針に基づき、ハラスメントの防止対策を適切に講じる必要があります。

4 作業環境のチェック

以下をふまえ、労働者が作業しやすい環境で作業するよう、労働者にアドバイスしましょう。



新しいテレワークガイドラインには、安全衛生確保のためのチェックリストがありますので、ご活用ください。

チェックリストはこちら→



テレワーク実施のための参考資料・相談先

導入マニュアル



テレワークではじめる働き方改革

はじめてテレワークを導入する際のハウツーが書かれた手引き書です。

<https://telework.mhlw.go.jp/wp/wp-content/uploads/2019/12/H28hatarakikatakaikaku.pdf>



ガイドライン



テレワークの適切な導入及び実施の推進のためのガイドライン

テレワークにおける適切な労務管理の実施につき、その留意すべき点を明らかにしたガイドライン。
<https://www.mhlw.go.jp/content/000766329.pdf>



セキュリティ



テレワークセキュリティガイドライン

テレワークのセキュリティに特化した専門マニュアル。ひと通り押さえておく安心です。

https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/



好事例



テレワーク推進企業等厚生労働大臣表彰～輝くテレワーク賞～事例集

テレワークを導入した企業の事例集。中小企業や、テレワークが難しいと考えられている企業の事例も掲載。

<https://telework.mhlw.go.jp/wp/wp-content/uploads/2020/12/e89b1130e110af17e2f87c566c261ee.pdf>



テレワーク総合ポータルサイト▶▶ <https://telework.mhlw.go.jp/>

実施にあたり困った際のご相談先

テレワーク相談センター (テレワーク協会)
電話 : 0120-861009
平日9:00~17:00(祝日、年末年始を除く)
メール : sodan@japan-telework.or.jp

厚生労働省委託事業
テレワーク相談センター
テレワーク(在宅勤務やモバイルワーク)の導入・推進の企業の相談窓口

孤独や不安を感じた際のご相談先

働く人の「こころの耳」相談窓口

電話相談

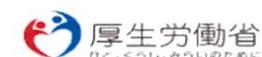
0120-565-455
月・火 17時~22時
土・日 10時~16時
(祝日、年末年始は除く)

メール相談

24時間受付 / 1週間以内にお返事します



テレワーク総合ポータルサイト



テレワークについて

効果・効用

導入方法

導入事例

セミナー・イベント

助成金・コンサル情報

Q&A

関連情報

このポータルサイトでは、テレワークに関する様々な情報をご覧いただけます。
テレワーク導入をご検討されている企業様、テレワークに関心のある方はぜひご利用ください。

テレワークに関するご相談は

メリット・効果は？

テレワーク導入のプロセスは？

人事評価など労働管理上の留意点は？

労働時間管理や安全衛生の確保は？

無料でお答えします

テレワーク相談センター

お電話はこちら
0120-861009

テレワークとは



テレワークについて知りたい

関連情報



テレワークに関する資料を入手したい【NEW】

セミナー・イベント



セミナーやイベントに参加したい【NEW】

効果・効用



テレワークを導入したい・効果を高めたい【NEW】

導入事例



企業の取り組み事例を知りたい【NEW】

関連情報



利用できるサテライトオフィスを知りたい

Q&A



テレワークに関するQ&A

関連情報



テレワークに関するリンク/関連情報

関連情報



自営型テレワークについて

テレワークに関する役立つ情報サイト

テレワークセキュリティ ガイドライン

第5版

(令和3年5月)



 総務省

目次

本ガイドラインの構成.....	2
目次.....	3
第1章 はじめに.....	5
1. 本ガイドラインの背景.....	5
2. テレワークの形態.....	7
3. 本ガイドラインの目的.....	8
4. 本ガイドラインの想定読者像.....	9
第2章 テレワークにおいて検討すべきこと.....	10
1. 「ルール」「人」「技術」のバランスがとれた対策.....	10
2. 組織の立場に応じた重要な役割.....	12
(1) 経営者の役割.....	13
(2) システム・セキュリティ管理者の役割.....	15
(3) テレワーク勤務者の役割.....	16
【コラム】情報漏えい.....	17
3. クラウドサービスの活用の考え方.....	18
(1) クラウドサービスとは.....	18
(2) テレワークにおけるクラウドサービスの有効性.....	20
(3) テレワークへのクラウドサービス活用の考慮事項.....	21
4. ゼロトラストセキュリティの考え方.....	22
(1) ゼロトラストセキュリティとは.....	22
(2) ゼロトラストセキュリティの有効性（注目される背景）.....	23
第3章 テレワーク方式の解説.....	24
1. テレワーク方式の選定.....	26
(1) フローチャート.....	26
(2) テレワーク方式の特性比較.....	27
2. テレワーク方式の詳細解説と考慮事項.....	28
(1) VPN方式.....	29
(2) リモートデスクトップ方式.....	32
(3) 仮想デスクトップ（VDI）方式.....	36
(4) セキュアコンテナ方式.....	39
(5) セキュアブラウザ方式.....	42
(6) クラウドサービス方式.....	45
(7) スタンドアロン方式.....	48
3. テレワーク方式の併用.....	52
(1) ローカルブレイクアウトとの併用.....	52
(2) テレワーク端末としてPCとスマートフォン等の併用.....	54
第4章 テレワークセキュリティ対策一覧.....	55
1. 経営者が実施すべき対策.....	56

行政手続・民間取引IT化に向けたアクションプラン

- デジタル・ガバメント推進方針に基づき、行政サービス全体の効率化と利便性向上を加速するため、基本的方向や具体的取組などを集中的に記載した「デジタルファースト・アクションプラン（通称）」を策定。
- 今後、概ね1年以内を目途に各種計画の策定を含め、取組を集中的に推進。（「デジタルガバメント推進方針」に基づく「実行計画」に統合）

これまでの取組

- 行政手続のIT化の推進（2001年～）
⇒「紙から電子への単なる置き換え」、「費用対効果視点の欠如」
- アクションプランの策定と全数調査の実施（2013年～）

最近の状況の変化

- 官民データ活用推進基本法の制定（2016年～）
行政手続のオンライン利用の原則化、民間取引のオンライン利用の促進
- マイナンバー制度等IT基盤の本格稼働（2017年～）

基本的考え方

- 「行政手続IT化にあたっての3原則」
⇒マイナンバー制度の徹底活用

①デジタルファースト
個々の手続が一貫してデジタルで完結
※原則オンライン利用の推進
※サービスデザイン思考に基づく取組の推進

②コネクテッド・ワンストップ
民間サービスも含め、どこでも／一か所でサービス実現

③ワンスオンリー
一度提出した情報は、再提出不要

※本3原則は、規制改革推進会議の「行政手続簡素化の3原則」（①デジタルファースト、②書式・様式の統一、③ワンスオンリー）と同じ方向。
※「行政手続簡素化3原則」は、短期集中の取組として、IT以外の取組も含めて原則化。本3原則は、デジタル社会を念頭に中長期的な視点で原則化。

アクションプランの個別項目 ※概ね1年以内目途に、取組を集中的に推進。

横断的な取組に係る項目（7項目）

<横断的な計画・プログラム策定>

- ・「行政手続オンライン化推進計画(仮称)」の策定
- ・地方自治体手続のオンライン利用促進に向けた方策
- ・「民間取引オンライン化促進プログラム(仮称)」の策定 など

<横断的な制度・システム導入>

- ・各種手続における住民票や戸籍の添付の省略化
- ・法人インフォメーション等を活用したバックオフィス連携の推進 など

個別分野に係る項目（7項目）

<行政手続のIT化>

- ・住民税の税額決定通知の電子正本化
- ・社会保険・労働保険関連の電子的申請の推進 など

<民間取引を含む社会全体のIT化>

- ・株主総会プロセスの電子化
- ・不動産取引における重要事項説明のオンライン化 など

デジタル・ガバメント推進方針の概要

<https://cio.go.jp/policy-egov> 平成29年5月30日より

目次

はじめに	2
1 税務行政のデジタル・トランスフォーメーション（総論）	
・ 税務行政のデジタル・トランスフォーメーション	5
・ 基本的な指針	6
2 あらゆる税務手続が税務署に行かずにできる社会（将来構想）	
・ あらゆる税務手続が税務署に行かずにできる社会を目指して	8
・ 構想1：税務署に行かずにできる「確定申告（納付・還付）」（申告の簡便化）	9
・ 構想2：税務署に行かずにできる「申請・届出」（申請等の簡便化）	10
・ 構想3：税務署に行かずにできる「特例適用状況の確認等」（自己情報のオンライン確認）	11
・ 構想4：税務署に行かずにできる「相談」①（チャットボットの充実等）	12
・ 構想5：税務署に行かずにできる「相談」②（プッシュ型の情報配信）	13
・ あらゆる税務手続が税務署に行かずにできる社会を目指して【工程表】	14
・ （参考）e-Tax利用率の推移	16
・ （参考）納付手段の多様化とキャッシュレス納付の推進	17
3 「課税・徴収の効率化・高度化」に関する取組状況	
・ 申告内容の自動チェック	19
・ AI・データ分析の活用	20
・ 照会等のオンライン化	21
・ Web会議システム等の活用（リモート調査）	22
・ （参考）国際的な課税・徴収逃れへの対応	23
・ （参考）共通報告基準（CRS）による情報交換の対象国及び情報授受件数	24
4 「税務行政の将来像2.0」を実現するためのインフラ整備	
・ システム高度化と人材育成	26
・ 内部事務の集約処理（センター化）	27
・ 関係機関（地方税当局・関係民間団体等）との連携・協調	28

税務行政のデジタル・トランスフォーメーション

デジタルを活用した、国税に関する手続きや業務の在り方の抜本的な見直し

(基本的な指針)

利用者目線の徹底

万全なセキュリティの確保

業務改革 (BPR)の徹底

税務行政の将来像2.0*

ICT社会への
的確な対応

税務手続きの
抜本的な
デジタル化



あらゆる税務手続
が税務署に行かず
にできる社会

 納税者の利便性の向上
(スムーズ・スピーディ) 

申告・申請等の簡便化

自己情報のオンライン確認

チャットボットの充実等

プッシュ型の情報配信

課税・徴収の効率化・高度化
(インテリジェント)

申告内容の自動チェック

AI・データ分析の活用

照会等のオンライン化

Web会議システム等の活用

重点課題への
的確な取組

租税回避への対応

富裕層に対する
適正課税の確保

消費税不正還付
等への対応

大口・悪質事案
への対応

(インフラ整備)

システム高度化と人材育成

内部事務の集約処理

関係機関との連携・協調

税務行政DXの構想実現に向けた「工程表」(概念図)

税務行政のデジタル・トランスフォーメーション(税務行政DX)

= デジタルを活用した、国税に関する手続や業務の在り方の抜本的な見直し

納税者の利便性の向上

(利便性向上によるオンライン手続の促進)

① 確定申告

② 申請等

- ▶ 一般的な申請・届出
- ▶ 納税証明書
- ▶ 申告書等の閲覧申請

③ 納付

④ 相談

課税・徴収の効率化・高度化

⑤ 内部事務(入力・審査等)

- ▶ センター化
- ▶ データ中心の事務処理

⑥ 調査・徴収事務

インフラ整備

⑦ 次世代システムの構築等

電子帳簿等保存制度の概要

- 電子帳簿等保存制度は、**納税者の文書保存に係る負担軽減を図る観点**から、帳簿や国税関係書類の電磁的記録等による保存を可能とする制度。
- ただし、**改ざんなど課税上問題となる行為を防止する観点**から、保存方法等について、**真実性・可視性の確保に係る一定の要件を設けている**。

① 電子帳簿等保存

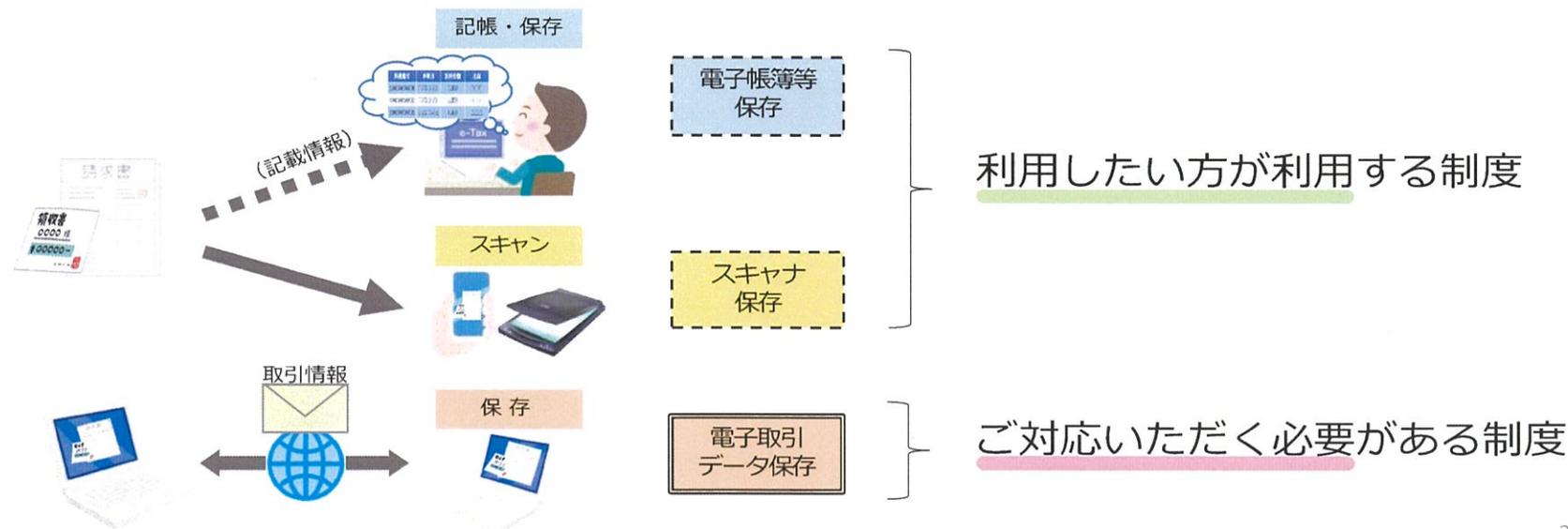
帳簿（仕訳帳等）や国税関係書類（決算関係書類等）のうち**自己が最初の記録段階から一貫して電子計算機を使用して作成しているもの**については、一定の要件の下、**データのままで保存等ができる**〔平成10年度税制改正で創設〕

② スキャナ保存

決算関係書類を除く国税関係書類（例：取引先から受領した領収書・請求書等）については、その書類を保存する代わりとして、一定の要件の下で**スマホやスキャナで読み取ったデータを保存することができる**〔平成17年度税制改正で創設〕

③ 電子取引データ保存

所得税・法人税に関する帳簿書類の保存義務者は、**取引情報のやりとりをデータで行った場合には**、一定の要件の下、**やりとりしたデータを保存することが必要**〔平成10年度税制改正で創設〕



(R3.12 国税庁・国税局・税務署)

電子取引とは

取引情報(取引に関して受領し、又は交付する注文書、契約書、送り状、領収書、見積書その他これらに準ずる書類に通常記載される事項をいう。)の授受を電磁的方式により行う取引をいう。

メールに添付



クラウドサービス



スマホアプリ決済



EDI取引



インターネット
FAX



電子帳簿保存法 第7条

電子取引の取引情報に係る電磁的記録の保存

(令和3年度税制改正対応版)

電子取引 取引情報保存 ガイドライン

第3.01版

2022年3月20日



公益社団法人 日本文書情報マネジメント協会
法務委員会

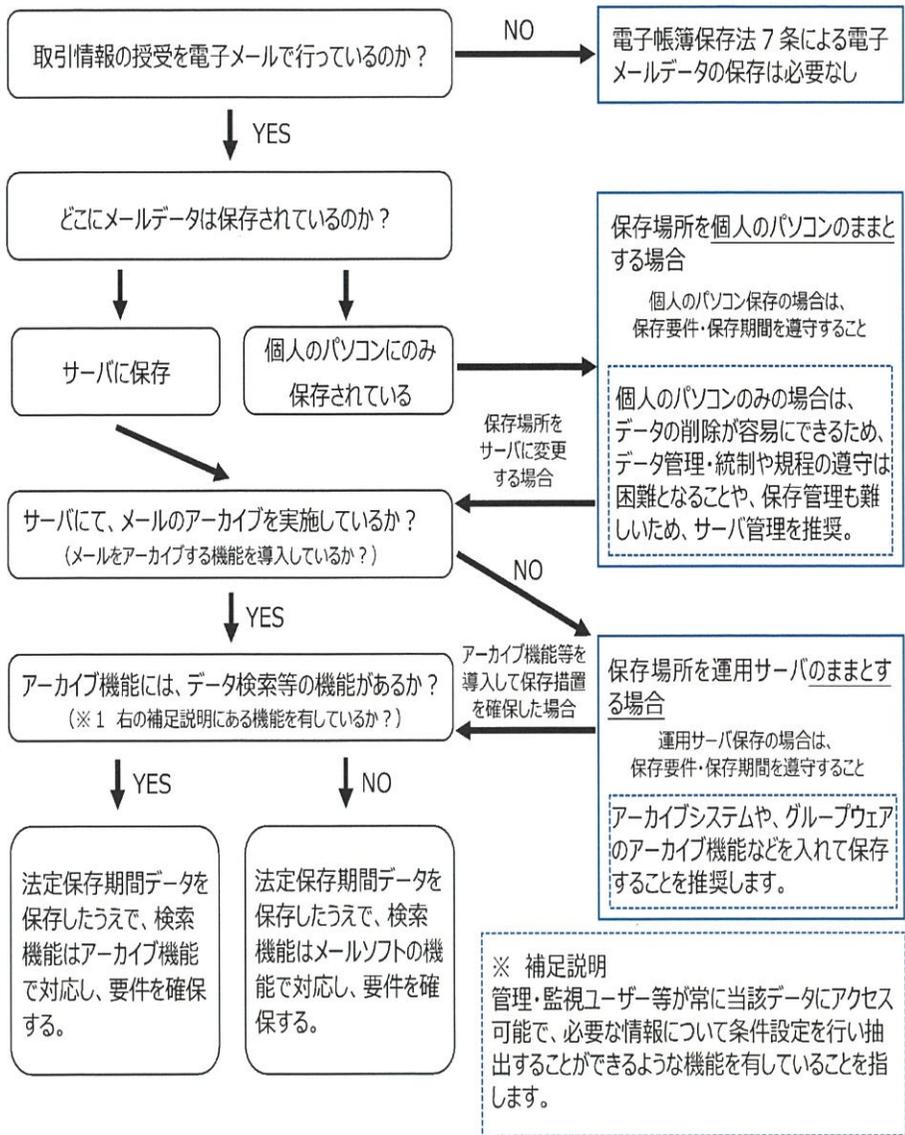
【電子取引 分類別一覧】

分類	概要	対象業務例	取引	システム・サービス例
EDI取引	異なる組織間で、取引のためのメッセージを、通信回線を介して標準的な規約を用いて、コンピュータ間で交換する取引（※1）	・調達や購買に関する 見積～発注～納品～検収～ 請求～支払の一連業務	B to B	・EDIシステム ・WEB-EDIシステム ・サプライチェーンマネジメントシステム
		・金融機関との取引業務 (入金・振込・取引情報)	B to B	・ネットバンキングシステム ・全銀EDIシステム ・APIを利用したシステム連携 ・Fintechサービス
電子メールによる 取引情報の授受	電子メールを利用した各種取引	・調達や購買に関する 見積～発注～納品～検収～ 請求～支払の一連業務 ・契約やその他取引	B to B B to C	・メールソフト ・ファイル転送サービス
インターネット等 による取引	インターネット等を利用した 各種取引	・経費の立替精算業務 (精算書の電子化)	社内	・経費精算システム
		・契約業務	B to B	・電子契約
		・請求書配信業務	B to B	・請求書WEB配信システム
	インターネット上のサイトを利用 した各種取引	・レシートの電子化 (電子レシート※2)	B to B B to C	・電子レシートアプリ
		・物品等の購入 (経費・仕入)	B to B B to C	・ECサイト (WEBサイト・スマホアプリ)
		・鉄道/航空・宿泊代の支払 (出張・移動の交通費等) ・ECサイトを利用した販売 (ネット販売)		
その他	・FAX(※3) (電話回線・インターネット) ・タブレットによる電子申込	B to B B to C	・FAXサーバ ・FAXソフト ・電子申込システム	

※1 通商産業省(現 経済産業省)の「電子計算機相互運用環境整備委員会(1989年度)」における定義。

※2 2018年2月に、経済産業省主導のもと電子レシートの実証実験が行われています。

※3 紙に出力せず、電子画像で保存する場合を指します。



- 個人で利用しているメールを使用した場合

個人で利用しているメールを、会社での取引に利用している場合、アーカイブソフトで連携して漏れなく保存でききょうにすることや、事務処理規程にて、「個人で利用しているメールの場合は、訂正削除することなく、データを保存すること」と定め、保存されたデータを管理・監視ユーザーが見ることができるようすることで要件を確保することができます。
- 無料のメールサービスを使用する場合

無料で利用できるメールについては、保存期間が担保されていない、提供事業者の都合により削除される場合がありますので、利用するサービスの規約を確認してください。
- 保存の媒体

保存については、サーバや DVD 等の外部記録媒体を利用することができ、過年度データについても、速やかに閲覧用サーバ等に戻すことができるのであれば問題ありません。
- メールデータの圧縮保存

メールデータを圧縮して保存することについても、解凍後、速やかに閲覧用サーバ等に戻すことができれば問題ありません。
- 重複メールの排除機能

宛先の CC を利用した受信メールの場合には、メールデータにも重複メールが発生し、総データ量が大きくなります。アーカイブシステム・機能には重複メールを排除する機能をもつソフトもあり、データ量の圧縮や検索・抽出作業の迅速化も図れます。
- 訂正・削除履歴

保存すべき取引情報授受メールの訂正や削除は原則禁止とすることを推奨します。
- 検索機能

送受信年月日や送受信メールアドレスにて検索できる必要があります。日付は範囲指定での検索や、2 以上の任意の記録項目の組み合わせで検索ができることも必要です。また、件名や本文内の言葉をあいまい検索できることが求められます。
- 添付ファイルの保存

電子メールに添付されている添付ファイルも含めて保存する必要があります。なお、添付ファイルにパスワードが掛かっている場合は、そのパスワードが書かれている電子メールも併せて保存することが重要です。

※ 補足説明
管理・監視ユーザー等が常に当該データにアクセス可能で、必要な情報について条件設定を行い抽出することができるような機能を有していることを指します。

電子取引調査確認書

以下該当する取引がある場合には、チェックを付し、内容を記載してください

	取引内容	チェック欄	取引相手先	取引頻度
1	電子メールのみで納品書・請求書・領収書等を授受する			
2	メッセージアプリ等の利用により請求書等を授受する			
3	インターネット利用サービスのサイトから直接請求書等をダウンロードして入手する			
4	スマホアプリを利用して請求書等を授受する			
5	クレジットカード利用明細はカード会社のウェブサイトでのみ確認している			
6	インターネットバンキングを利用して明細を確認している			
7	FAX受信する請求書等は印刷を行わずデータのみ確認している			
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

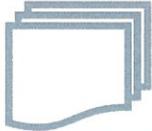
会社名：

調査者：

調査日：

電子取引の保存要件

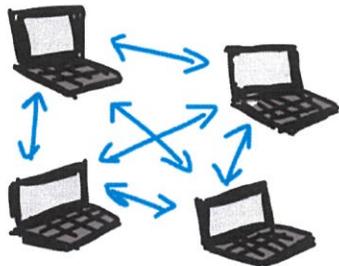
見読性の確保 可視性の確保 検索性の確保
AND

タイムスタンプ  OR 事務処理規程  OR 訂正削除履歴

メールに添付 クラウドサービス スマホアプリ決済



EDI取引



インターネット
FAX



クラウドサービス



特集 インボイス制度

令和5年10月1日から、消費税の仕入税額控除の方式としてインボイス制度が始まります。適格請求書(インボイス)を発行できるのは、「適格請求書発行事業者」に限られ、この「適格請求書発行事業者」になるためには、登録申請書を提出し、登録を受ける必要があります。

インボイス制度 国税庁

公表サイト

新着情報

登録申請書等に係る通知までの期間の目安については、[こちら](#)でご案内しております。

9月30日

- 制度の周知用パンフレット内に「[適格請求書等保存方式\(インボイス制度\)の手引き](#)」を掲載しました。

9月20日

- 「登録通知書」の様式変更について[こちら](#)をご確認ください。

7月29日

- 制度周知用リーフレット内の「[消費税の仕入税額控除の方式としてインボイス制度が始まります](#)」を更新しました。

インボイス制度の説明会
説明会のご案内は
こちらから



YouTube
国税庁動画
チャンネル



インボイス制度に関するお問合せ先



税務相談チャットボット

「チャットボット」ただいま公開中！
インボイス制度の疑問にふたばお答えします！

> チャットを開始する



制度の概要

お問合せが多い
質問等随時更新



Q&A



取扱通達



申請手続

軽減・インボイスコールセンター
インボイス制度に関する一般的なご質問やご相談を受け付けています。

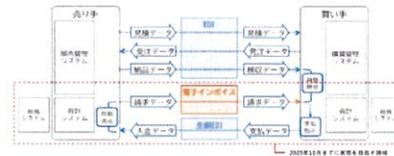
フリーダイヤル
0120-205-553(無料)
9:00~17:00(土日祝除く)

電子インボイスとは

バックオフィス業務全体のデジタル化を実現する

事業者のバックオフィス業務は、デジタル化が十分なだけでなく、紙・FAXのやり取りを中心とした多くのアナログなプロセスが存在しており、デジタルとアナログの世界を行き来する中途半端な状態となっており、そのことが効率化・生産性の向上の妨げとなっているとされています。

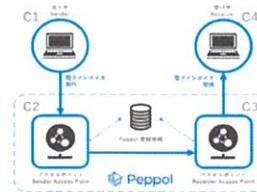
そのような状態を解消するためには、紙を前提とした業務プロセスを「電子化」(Digitization)するだけでは十分ではなく、その業務プロセス自体をデジタルを前提に見直す「デジタル化」(Digitalization)が不可欠となります。EIPAは、標準化された電子インボイスの利活用・普及を通じ、事業者のバックオフィス業務全体の「Digitalization」を推進していきたいと考えます。



標準化された電子インボイスの利活用等は、請求から支払、さらにはその後のプロセスである入金消込といった会計・税務の業務についても、エンド・トゥ・エンドでデジタルデータでつながり、事業者のバックオフィス業務全体が効率化するだけでなく、その結果としての新しい価値やベネフィットも期待できます。さらに、請求に係るプロセスのデジタル化により、その前のプロセスである契約・受発注といったプロセスのデジタル化も促され、「取引全体のデジタル化」が進むことも期待されます。

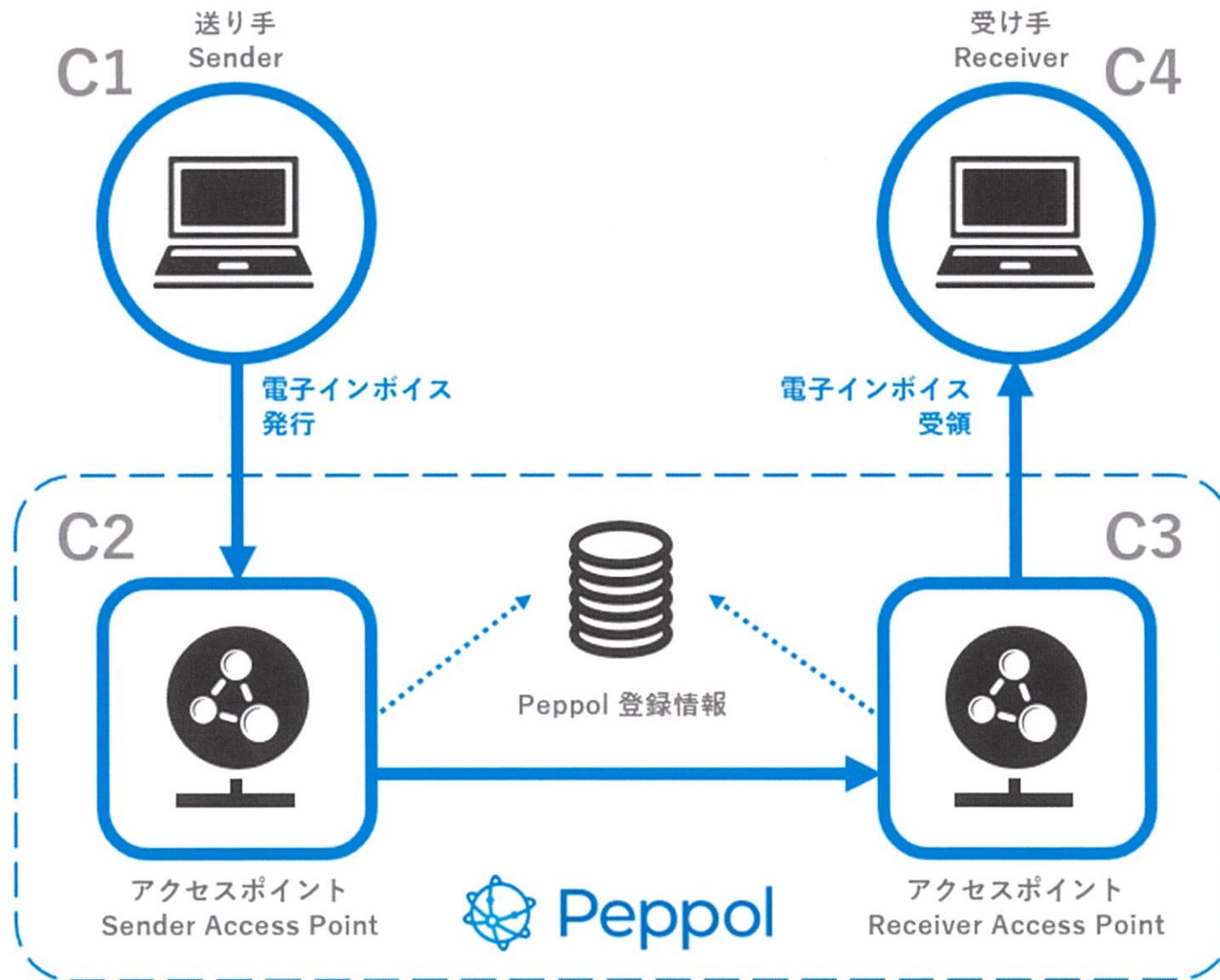
Peppol (ペポル) について

Peppol (Pan European Public Procurement Online)とは、請求書(インボイス)などの電子文書をネットワーク上でやり取りするための「文書仕様」「運用ルール」「ネットワーク」のグローバルな標準仕様であり、Open Peppol(ベルギーの国際的非常利組織)がその管理等を行っています。現在、欧州各国のみならず、オーストラリア、ニュージーランドやシンガポールなどの欧州域外の国も含め30か国以上で利用が進んでいます。

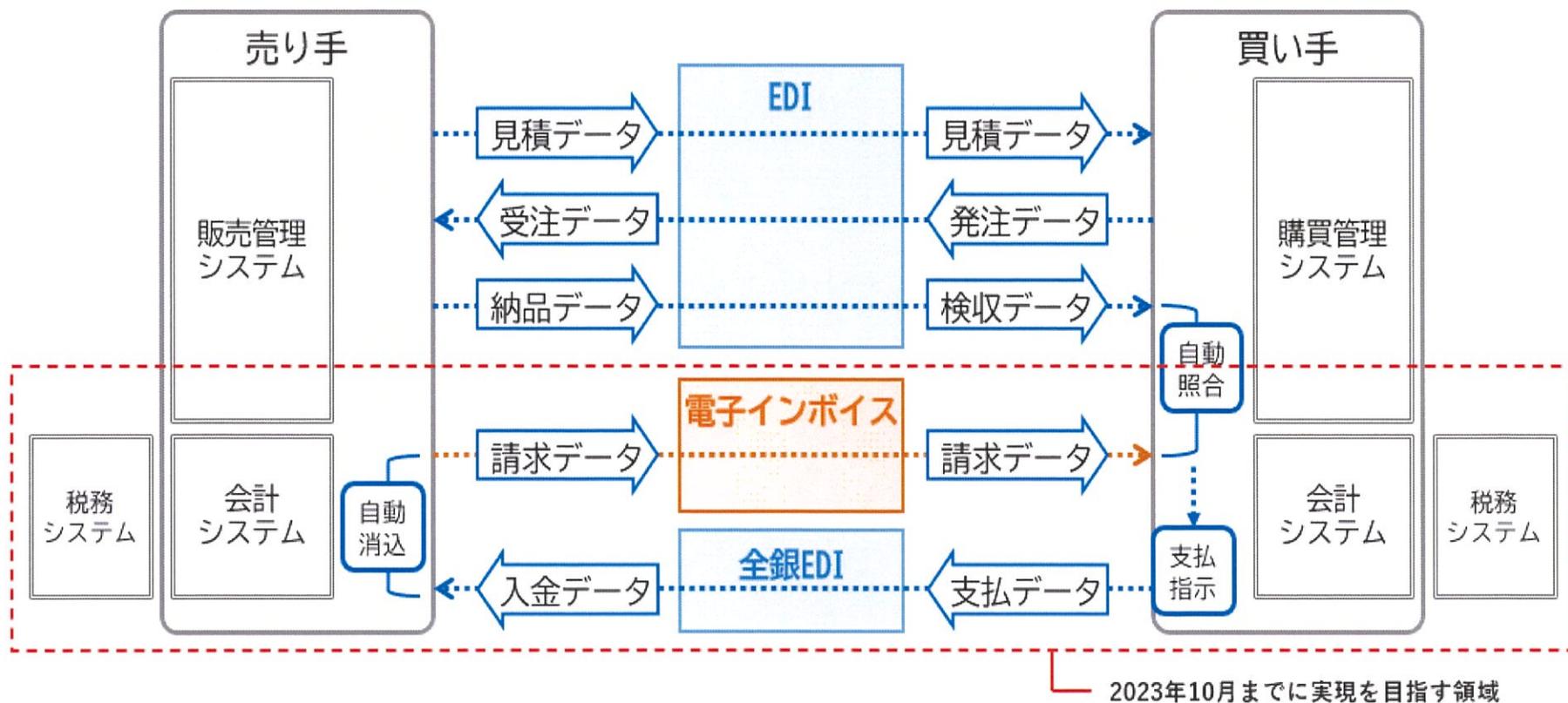


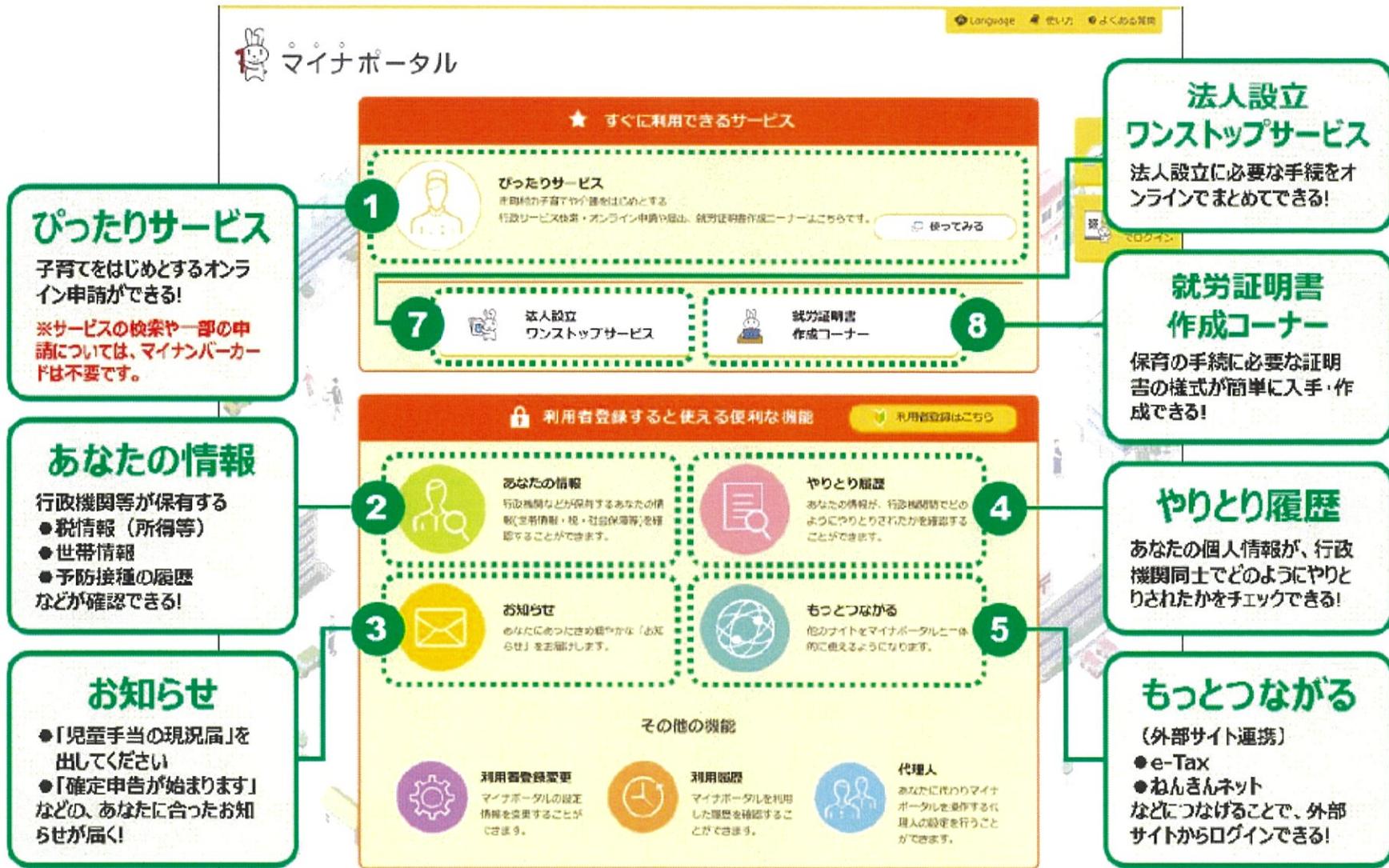
Peppolは、「4コーナーモデル」と呼ばれるアーキテクチャを採用しています。ユーザー(売り手(C1))は、自らのアクセスポイント(C2)を通じ、Peppolネットワークに接続し、買い手のアクセスポイント(C3)にインボイスデータを送信し、それが買い手(C4)に届くという仕組みです。Peppolユーザーは、アクセスポイントを経て、ネットワークに接続することで、Peppolネットワークに参加する全てのユーザーと電子インボイスをやり取りすることができます。この仕組みは、例えば、メール(アプリケーション)からインターネットプロバイダーを介して相手に届くという電子メールの仕組みに似ています。

なお、わが国の電子インボイスの標準仕様である「Peppol BIS Billing JP」は、売り手のアクセスポイント(C2)と買い手のアクセスポイント(C3)との間でやり取りされる電子インボイスの標準仕様です。その「Ver.0.9」(Peppol BIS Billing JP 0.9)(2021年12月15日版)については、Open Peppolのウェブサイトにて公開されており、2022年秋にPeppol対応サービスの提供が可能となるよう、今後、必要な更新等が行われていくこととなります。



<https://www.eipa.jp/>





マイナポータルとは より

1. サービス検索・オンライン申請機能(ぴったりサービス)

お住まいの市区町村の、子育てや介護をはじめとするサービスの検索やオンライン申請ができます。

2. 自己情報表示(あなたの情報)

行政機関等が保有するあなたの情報を検索して確認することができます。

3. お知らせ

行政機関等から配信されるお知らせを受信することができます。

4. 情報提供等記録表示(やりとり履歴)

あなたの個人情報、行政機関同士でどのようにやりとりされたかの履歴を確認することができます。

5. もっとつながる(外部サイト連携)

外部サイトを登録することで、マイナポータルから外部サイトへのログインが可能になります。

マイナポータルとe-Taxをつなげる

マイナポータルからつながる外部サイト

平成30年11月5日からマイナポータルとねんきんネットの連携が始まりました！(日本年金機構)

6. 民間送達サービスとの連携

民間企業からのお知らせなどを、民間送達サービスを活用して受け取ることができます。民間送達サービスである「e-私書箱」や「MyPost」とマイナポータルを連携させることで、年末調整や確定申告の手続きが簡便化されます。

マイナポータルを活用した年末調整及び所得税確定申告の簡便化(国税庁)

7. 法人設立ワンストップサービス

法人設立に必要な諸手続きをオンラインでまとめて行うことができます。

8. 就労証明書作成コーナー

認可保育所等の利用申込の際に必要な「就労証明書」の様式を簡単に入手・作成することができます。

9. 公金決済サービス

マイナポータルの「お知らせ」から、ネットバンキング(ペイジー)やクレジットカードでの公金決済が可能となります。

10. よくある質問／問い合わせ登録

操作方法に関するFAQを確認したり、問い合わせができます。

11. 代理人

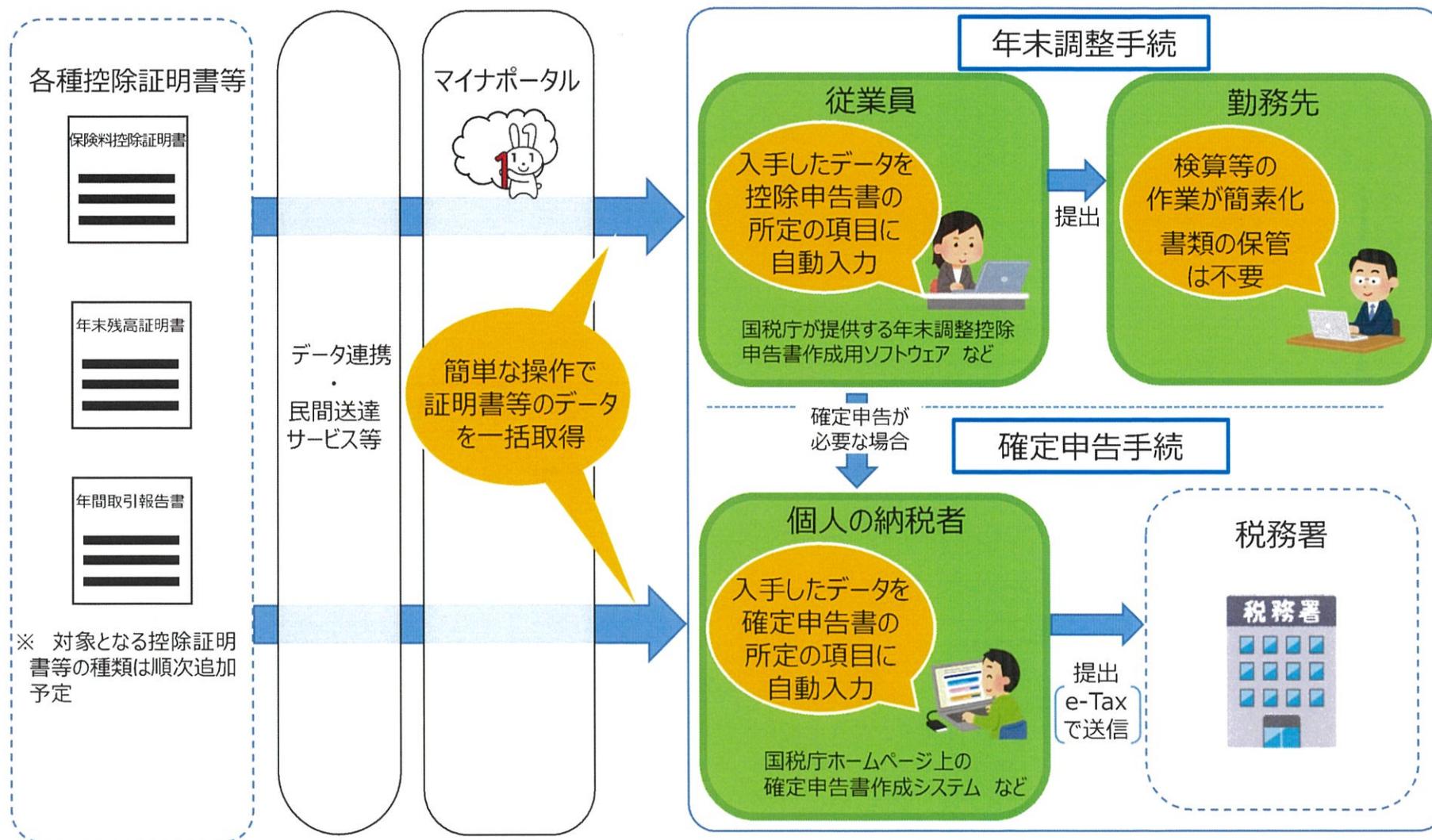
本人に代わって代理人がマイナポータルを利用できます。

12. マイナンバーカードのパスワード変更

マイナンバーカードのパスワードのうち、利用者証明用電子証明書、署名用電子証明書、券面事項入力補助用の3種類について変更することができます。

マイナポータルを活用した年末調整及び所得税確定申告の簡便化のイメージ

(年末調整は令和2年10月から、所得税確定申告は令和3年1月から、順次開始予定)



申告書の自動入力が始まります！

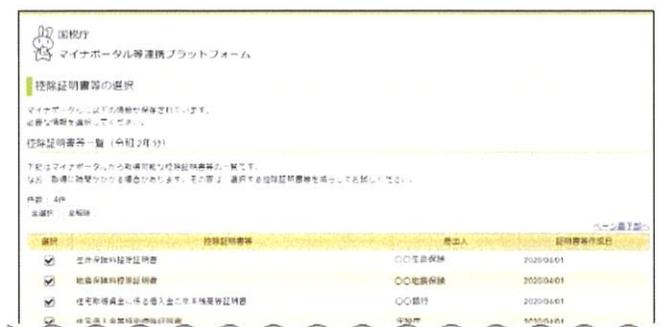
確定申告 × マイナポータル

マイナポータルと確定申告書等作成コーナーを利用すれば、生命保険料控除証明書などの情報をまとめて入手、各控除に自動入力されます。それが「**マイナポータル連携**」です。



証明書の発行主体

まとめて取得



自動入力

マイナンバーカードとマイナンバーカード読取対応のスマートフォン（又はICカードリーダー）をご用意ください。



証明書の内容の入力が不要！
保険料の区分も自動判定！
控除額も自動計算！

(注) ご利用には、保険会社等の控除証明書等の発行主体、マイナポータル連携に対応している必要があります。



※ 画面は開発中のものです。マイナポータルはこちら



国税庁特設ページ



マイナポータル連携のご利用に当たっては、マイナポータルの初期設定が必要となります。詳しくは国税庁ホームページのマイナポータル連携特設ページをご確認ください。

国税庁 法人番号7000012050002

申告書の自動入力が増えます！

確定申告 × マイナポータル

マイナポータル連携で自動入力される情報は今後順次拡大！！

注) ご利用には、保険会社等の控除証明書等の発行主体がマイナポータル連携に対応している必要があります。
令和2年10月時点の情報を基に作成しています。

令和2年分から自動入力

令和3年分から自動入力予定

令和4年分以降順次拡大予定

住宅ローン関係

医療費関係

社会保険

株式等の取引関係

ふるさと納税

源泉徴収票

生命保険控除証明

地震保険控除証明

その他

例えば...

詳しくはこちら



国税庁マイナポータル連携特設ページ

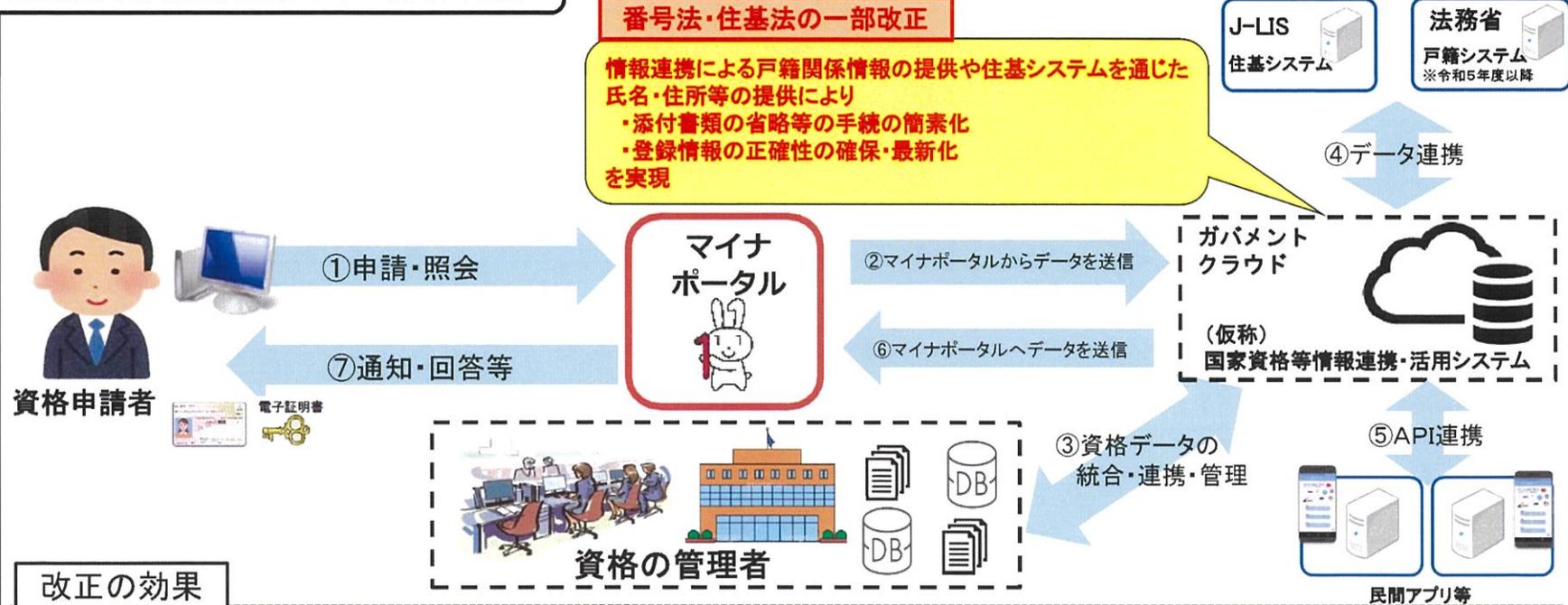


国家資格関係事務における個人番号の利用及び情報連携の拡大

改正の背景

各省庁が所管する各種免許・国家資格等の管理は、必ずしもデジタル化が進んでおらず、資格者の各種届出等が徹底されていない場合もある。また、対面や郵送での手続が必要となることや、紙ベースの処理が行われていること等、資格者の資格証明、行政機関等の資格確認の負担も少なくない。

国家資格等情報連携・活用システム(仮称)の構築



改正の効果

- 各種届出時に求められていた、戸籍抄(謄)本や住民票の写しの添付を省略
- マイナポータルを活用した、資格保有者から第三者への資格保有の証明及び就業支援情報の提供等
- 遺族からの死亡届を不要とし、資格管理者が職権で登録の抹消を行うことにより、登録原簿の正確性を確保

施行期日: 公布の日から4年以内で政令で定める日

国家資格関係事務におけるマイナンバーの利用及び情報連携の拡大(その2)

税・社会保障・災害等に係る以下の32資格は、個人番号利用事務に指定することにより、住基システム・戸籍システムとの連携を行う。これらの資格は先行して国家資格等情報連携・活用システム(仮称)によるデジタル化の検討を行い、令和6年度のサービス開始を目指す。

①	医師	⑫	言語聴覚士	⑳	介護福祉士
②	歯科医師	⑬	臨床検査技師	㉑	社会福祉士
③	薬剤師	⑭	臨床工学技士	㉒	精神保健福祉士
④	看護師	⑮	診療放射線技師	㉓	公認心理師
⑤	准看護師	⑯	歯科衛生士	㉔	管理栄養士
⑥	保健師	⑰	歯科技工士	㉕	栄養士
⑦	助産師	⑱	あん摩マッサージ指圧師	㉖	保育士
⑧	理学療法士	㉒	はり師	㉗	介護支援専門員
⑨	作業療法士	㉓	きゆう師	㉘	社会保険労務士
⑩	視能訓練士	㉔	柔道整復師	㉙	税理士
⑪	義肢装具士	㉕	救急救命士		

2. 1 マイナポータルをハブとしたデジタル・セーフティネット構築（民間情報と電子申請等の連携、税（所得情報）と社会保障の連携等）の検討

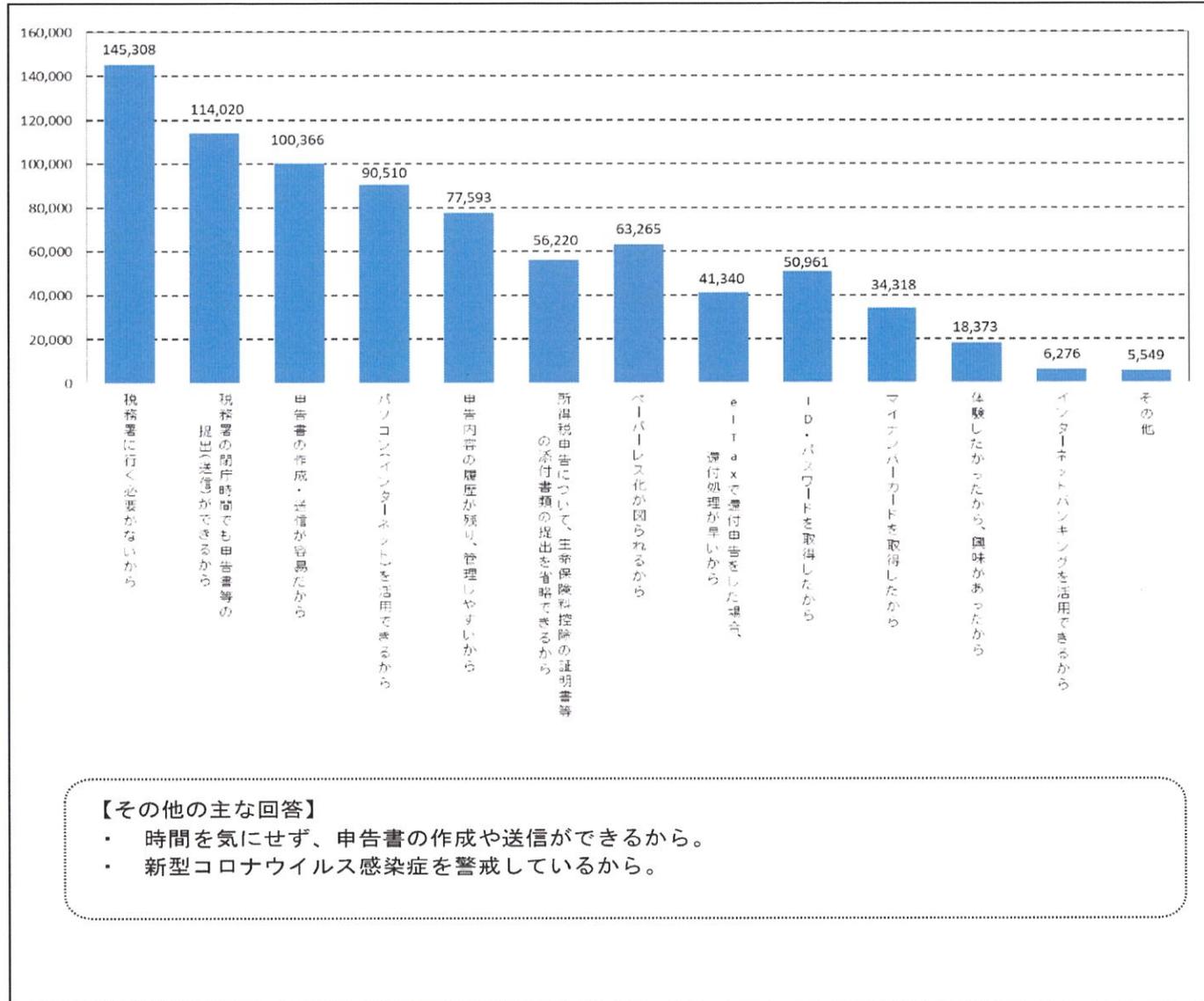
	2020年度 (令和2年度) 1~3月	2021年度 (令和3年度)	2022年度 (令和4年度)	2023年度 (令和5年度)	2024年度 (令和6年度)	2025年度 (令和7年度)
年末調整・確定申告における自動入力の実現	年末調整・確定申告の簡便化に係る取組み順次実施 (添付書類のデータ一括取得、自動入力)					
ふるさと納税に係る寄附金控除手続きにおける自動入力の実現	指定寄附仲介事業者と連携	確定申告における自動入力の実現				
DeCo手続きのオンライン化・デジタル化	DeCo手続きのオンライン化・デジタル化					
	国民年金基金連合会におけるオンライン化の検討・実現					
マイナポータルから取得できるデータの拡大	各種証明書等のマイナポータルにおける取得データの増加 ▲医療費通知証明データ (2022年1月(2021年9月診療分)) ▲公的年金等源泉徴収票、社会保険料(国民年金保険料)控除証明データ(2022年10月以降)					
民間事業者のデジタル化対応の加速化	集中的に支援実施					
クラウドを活用した新しいデータ授受策活用の検討	システム整備、民間事業者のシステム対応		金融機関等が税務署に提出する法定調書から順次利用開始			

2. 5 固定資産課税台帳とその他の土地に関する各種台帳等の情報連携等の検討

	2020年度 (令和2年度) 1~3月	2021年度 (令和3年度)	2022年度 (令和4年度)	2023年度 (令和5年度)	2024年度 (令和6年度)	2025年度 (令和7年度)
土地に関する各種台帳等の情報連携の高度化	方向性の検討	検討結果を踏まえ必要な措置を講じる				
固定資産課税台帳とマイナンバーとの紐づけの推進		現状調査・分析	必要な措置の検討を行う			
相続登記等の申請の義務化	法案の提出	施行に向けた措置等を講じる				

5. 利用しようと思った理由<複数回答>

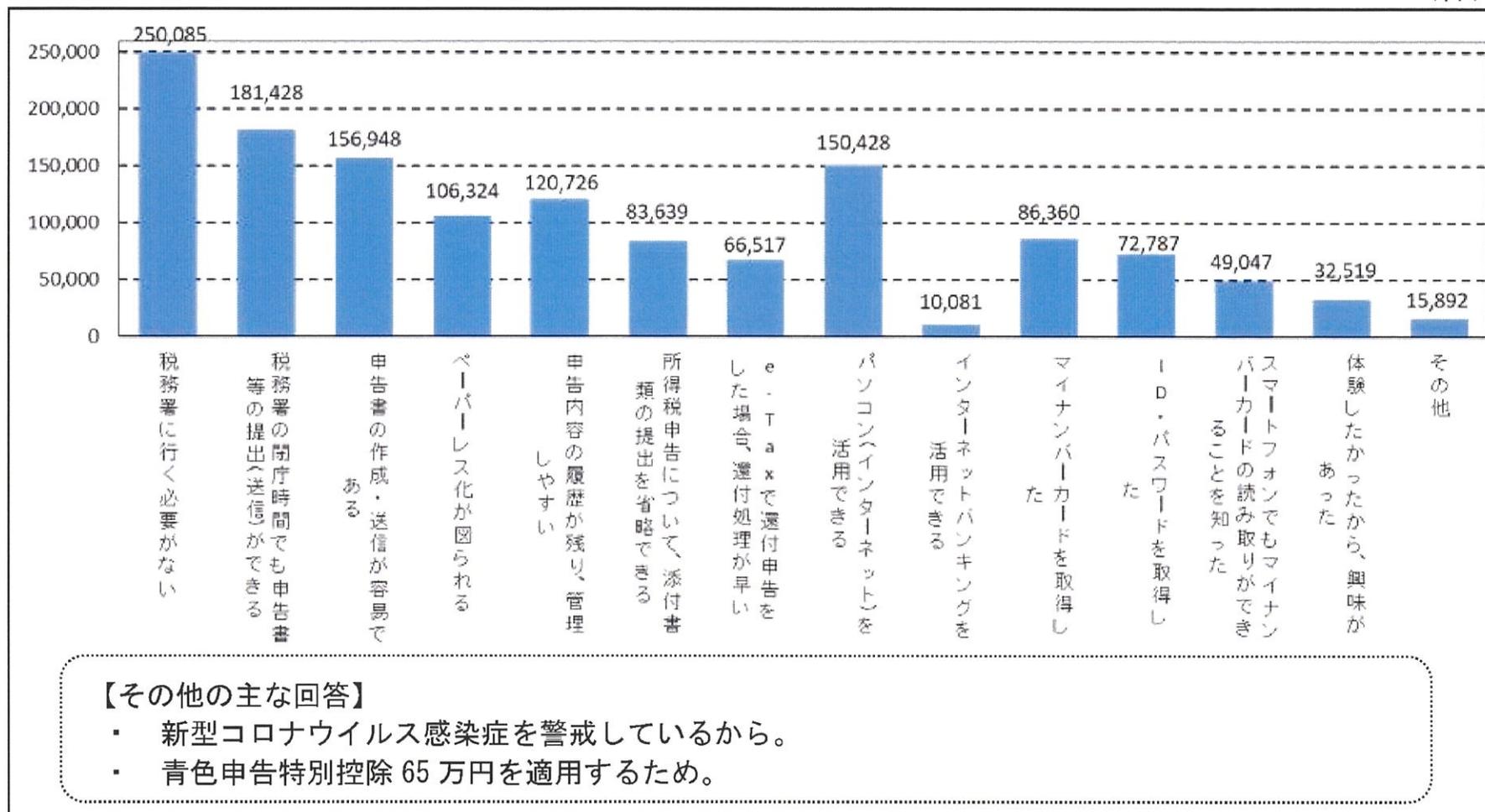
(件)



国税電子申告・納税システム(e-Tax)の利用に関するアンケートの実施結果について 令和2年8月 国税庁より

5. 利用しようと思った理由<複数回答>

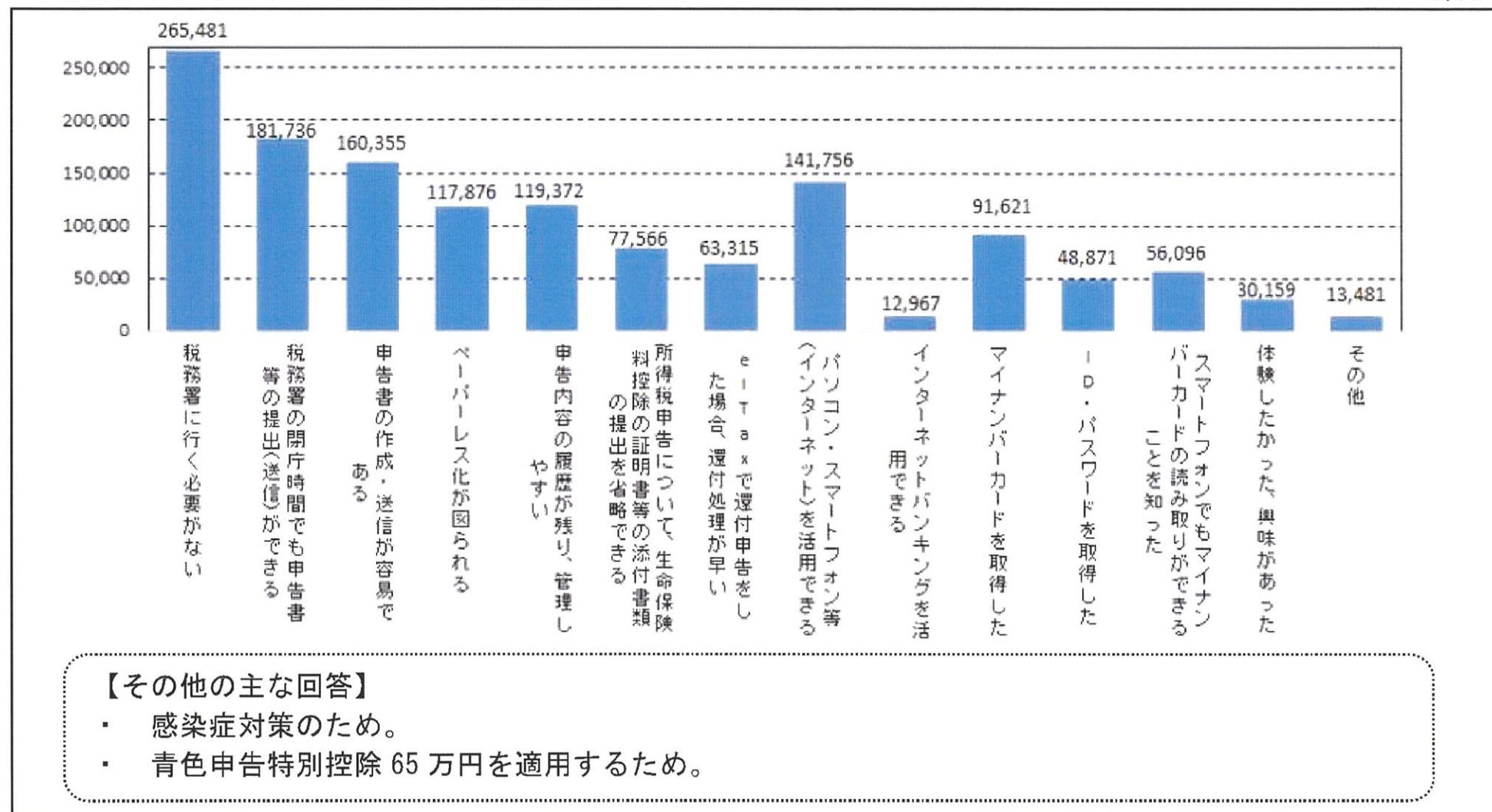
(件)



国税電子申告・納税システム(e-Tax)の利用に関するアンケートの実施結果について 令和3年8月 国税庁より

5. 利用しようと思った理由〈複数回答〉

(件)



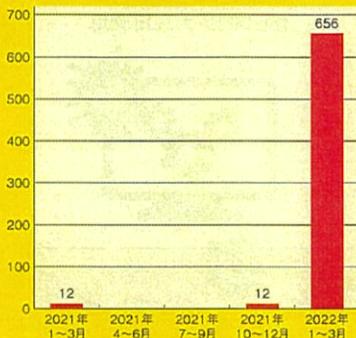
国税電子申告・納税システム(e-Tax)の利用に関するアンケートの実施結果について 令和4年8月 国税庁より

2.情報セキュリティ基礎知識

国税庁をかたるショートメッセージやメールがきていませんか？

このような「サイバー犯罪」に有効な情報セキュリティについて基礎知識を身につけましょう！

Emotetウイルス相談件数の推移



IPA情報セキュリティ安心相談窓口の相談状況
[2022年第1四半期(1月~3月)]より
(https://www.ipa.go.jp/security/txt/2022/q1_outline.html)

Emotetの感染例とその被害

「Emotet」は、情報の窃取に加え、他のウイルスを利用した二次感染にも悪用されており、悪意のある者によって、不正なメール(攻撃メール)に添付されるなどにより、感染の拡大が試みられます。

悪意を持った第三者が、顧問先や知人のメールアドレスを騙ったメールを送付し、そのメールに添付されたファイルを開くとメールアドレスが乗っ取られる被害や、ランサムウェア(※)の被害が確認されています。また、悪意を持った第三者が、乗っ取られたメールアドレスを悪用し、さらに上記の行動を繰り返すことにより、感染拡大が広がる等の被害が観測されています。

このような被害にあわないようにするために、情報セキュリティについての情報収集や基礎知識をつけることが必須です。

デジタル化委員会では、情報セキュリティについての基礎知識をつけるため、IPAや警視庁サイバーセキュリティ本部と協力して、税理士向けの情報セキュリティ研修を開催することとなりました。

税理士業務に必要な情報セキュリティ対策

開催日時 10月27日(木) 午後3時~5時
場所 ZOOMによるライブ配信(先着順250名)
講師 警視庁サイバーセキュリティ対策本部、IPAセキュリティセンター
申込方法 こちら(<https://forms.gle/gGPMoNRcdzfbjqEH9>)よりお申込みください。10月25日頃に送付された電子メールアドレスに対して、ZOOMの案内を送付いたします。

受講料
無料

研修受講時間
となります



参考

ランサムウェア: 感染したパソコン等のロックやファイルを暗号化する等により持ち主が使用できない状態にし、「元に戻して欲しいば…」とランサム(身代金)の支払いを要求するウイルスです。

ランサムウェア特設サイト <https://www.jpCERT.or.jp/magazine/security/nomore-ransom.html>

東京税理士会 デジタル化委員会

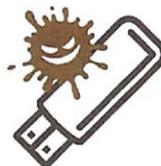
どんな形でやってくる!?

ランサムウェア対策

※ランサムウェアは、利用者のファイルやフォルダを勝手に暗号化し、データへのアクセスを妨げた上で、暗号化の解除を条件に金銭(身代金)を要求してくる脅迫を伴った攻撃です。

USBメモリ

事務所で使用許可を得ていないUSBメモリ等の接続



脆弱なシステム

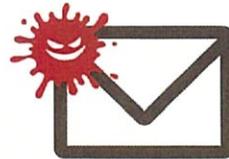
公開されている脆弱性の修正プログラムの未適用



犯罪手口を把握していないと
危険です!!

メール

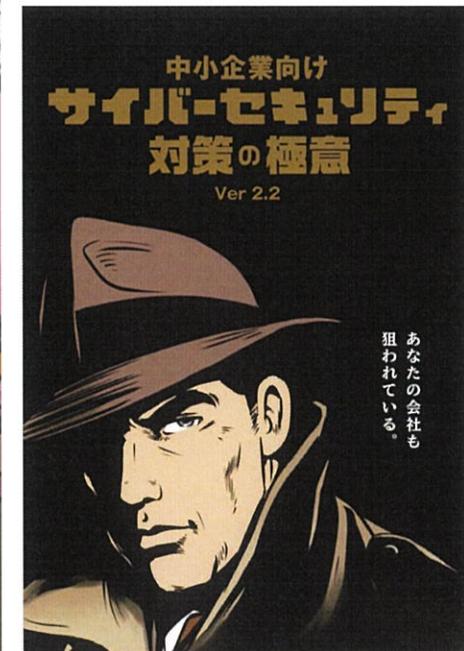
普段と文面等の印象が違う顧問先等からのメールの添付ファイルの開封



サイト改ざん

ブックマークしたURL以外への接続や、SMS・メール本文に付いているURLの軽率なクリック





ホーム

税の情報・手続・用紙▼

刊行物等▼

法令等▼

お知らせ▼

国税庁等について▼

🚨 緊急のお知らせ

・ [不審なショートメッセージやメールにご注意ください（令和4年9月29日更新）](#)

[新型コロナウイルス感染症に関する対応等について（詳しくはこちら）](#)

新着情報

トピックス	税の情報・手続・用紙	刊行物等	法令等	お知らせ	国税庁等について
令和4年10月6日	税務相談チャットボット（年末調整）が始まりました				
令和4年10月4日	令和4年台風第14号及び15号により被害を受けられた皆様へ（災害関連情報）				
令和4年9月29日	【酒類事業者向け】「フロンティア補助金」の第4期募集を開始します				
令和4年9月22日	「年末調整がよくわかるページ」を開設しました				
令和4年9月22日	令和4年分年末調整のための各種様式を掲載しました				
<p>表示件数を増やす</p> <p style="text-align: right;">▶ トピックス一覧へ</p>					

注目ワード

- 消費税のインボイス制度
- e-Tax
- 年末調整がよくわかるページ
- 不審な電話やメール等にご注意を
- 電子帳簿保存法
- 納税が困難な方へ
- 国税に関するご相談について
- 自宅からの手続方法
- お酒に関する情報
- 質疑応答事例
- 国税専門官採用試験に理工・デジタル系区分が創設

税務署を検索

郵便番号から税務署を検索
(半角数字)

分野別メニュー

令和4年7月21日

(令和4年8月18日更新)

(令和4年8月26日更新)

(令和4年9月29日更新)

国 税 庁

不審なショートメッセージやメールにご注意ください

現在、国税庁をかたるショートメッセージ及びメールから国税庁ホームページになりました偽のホームページへ誘導する事例が見つかっています。

国税庁（国税局、税務署を含む）では、ショートメッセージによる案内を送信しておりません。

また、国税の納付を求める旨や、差押えの執行を予告する旨のショートメッセージやメールも送信しておりません。

不審なショートメッセージやメール、国税庁ホームページになりましたサイト（送信元やリンク先アドレスの表記を装っている場合もあります。）にアクセスすると、被害を受けるおそれがありますので、アクセスしないようご注意ください。

また、支払い等に応じることがないようにご注意ください。

国税庁ホームページアドレスは、<https://www.nta.go.jp> です。

国税庁ホームページを利用するには、ブラウザのアドレス欄を必ずご確認ください。

なお、国税庁からのメールによる案内は、以下の場合に限られます。以下以外のメールは、国税庁から送信したものではありませんので、メールを開封せずに削除するなど、取り扱いには十分にご注意ください。

【国税庁からのメール案内】

- ・ 国税庁ホームページ新着情報の配信サービスの登録をされている場合
- ・ 国税庁メールマガジン配信サービスの登録をされている場合
- ・ e-Tax の利用にあたり、メールアドレスを登録されている場合

国税庁を装った不審なメールの実際の文面及び注意点などの詳細について、[e-Tax ホームページ](#)に掲載しておりますので、ご確認ください。

●不審な電話や振り込め詐欺にご注意を

「フィッシング対策協議会」のホームページに、国税庁をかたるフィッシング詐欺の事例や報告方法が掲載されております。

●[フィッシング対策協議会のウェブサイトはこちら（外部サイトへ）](#)

・不審なショートメッセージやメールにご注意ください(令和4年9月29日更新)

お知らせ

掲載日：令和4年8月15日

更新日：令和4年8月26日

更新日：令和4年9月29日

不審なショートメッセージやメールにご注意ください

現在、「未払い税金のお知らせ」などの件名で、支払の催促や差押の予告に関する内容やe-Taxから送信される「税務署からのお知らせ」に類似したメール（※）など、国税庁からの連絡を装った不審なメールが送信されていることを把握しております。

国税庁(国税局、税務署を含む)では、ショートメッセージによる案内を送信しておりません。

また、国税庁からのメール案内は以下の場合に限っており、以下のケース以外のメールが届いた場合、国税庁から送信したものではありません。メールを開封せずに削除するなど、取り扱いには十分にご注意ください。

【国税庁からのメール案内】

- | | |
|-----------------------------------|---------------------------------|
| ① 国税庁ホームページ新着情報の配信サービスの登録をされている場合 | ⇒ イメージは、「 こちら 」 |
| ② 国税庁メールマガジン配信サービスの登録をされている場合 | ⇒ イメージは、「 こちら 」 |
| ③ e-Taxの利用にあたり、メールアドレスを登録されている場合 | ⇒ イメージは、「 こちら 」 |

（※）「税務署からのお知らせ」は、e-Taxにメールアドレスを登録された方に対して、メッセージボックスに情報が格納された場合などに送信しておりますが、国税庁を装った不審なメールは、e-Taxの利用の有無に関係なく送信されていることが確認されております。

（参考）国税庁HP「[不審なショートメッセージやメールにご注意ください](#) PDF」

税務署からの【未払い税金のお知らせ】



e-Taxをご利用いただきありがとうございます。

あなたの所得（または延滞金（法律により計算した客助）について、これまで自主的に納付されるよう催促してきましたが、まだ納付されておられません。

もし最終期限までに納付がないときは、税法のきめるところにより、不動産、自動車などの登記登録財産や給料、売掛金などの債権などの差押処分に着手致します。

納税確認番号:****1729

滞納金合計:50000円

納付期限: 2022/08/31

最終期限: 2022/08/31（支払期日の延長不可）

お支払いへ⇒<https://nta.go.jp/information/tax>

※ 本メールは、「国税電子申告・納税システム（e-Tax）」にメールアドレスを登録いただいた方へ配信しております。

なお、本メールアドレスは送信専用のため、返信を受け付けておりません。ご了承ください。

発行元：国税庁

Copyright (C) NATIONAL TAX AGENCY ALL Rights Reserved.

国税庁では、このような支払の催促や差押の予告に関する内容のメールは、お送りしておりません。

税務署からのお知らせ【申告に関するお知らせ】 ✕ ☰ ㊄

e-Taxをご利用いただきありがとうございます。
国税に関する申告の参考となる情報について、メッセージボックスに格納しましたので、内容をご確認ください。

e-Taxの利用可能時間内に、以下の手順で確認することができます。

- パソコンから確認する場合
 - ※ 個人納税者の方が確認するためにはマイナンバーカード等が必要です。
 - 受付システムをご利用の場合
 - 1 「受付システム ログイン」画面からログインします。
 - 2 「メッセージボックス一覧」から該当のお知らせを選択すると、内容が表示されます。
⇒ 受付システムへ ⇒ <https://rhnvai.com/QxgZls8352>
 - e-Taxソフト（WEB版）をご利用の場合
 - 1 「e-Taxソフト（WEB版）メインメニュー」画面からログインします。
 - 2 「送信結果・お知らせ」を選択してください。
 - 3 「メッセージボックス一覧」から該当のお知らせを選択すると、内容が表示されます。
⇒ e-Taxソフト（WEB版）へ ⇒ <https://rhnvai.com/QxgZls8352>
- スマートフォン等から確認する場合
 - ※ 個人納税者の方が確認するためにはマイナンバーカード等が必要です。
 - 1 「e-Taxソフト（SP版） ログイン」画面からログインします。
 - 2 「送信結果・お知らせ」を選択してください。
 - 3 「メッセージボックス一覧」から該当のお知らせを選択すると、内容が表示されます。
⇒ e-Taxソフト（SP版）へ ⇒ <https://rhnvai.com/QxgZls8352>
- 注意事項
 - ・メッセージボックスのお知らせの内容の詳細を確認するためには、マイナンバーカード等の電子証明書による認証が必要です。詳細は、「メッセージボックスのセキュリティ強化について」からご確認ください。
⇒ <https://rhnvai.com/QxgZls8352>
 - ・e-Taxの利用可能時間は、e-Taxホームページでご確認してください。
⇒ <https://rhnvai.com/QxgZls8352>

※ 本メールは、「国税電子申告・納税システム（e-Tax）」にメールアドレスを登録いただいた方へ配信しております。
なお、本メールアドレスは送信専用のため、返信を受け付けておりません。ご了承ください。

発行元：国税庁
Copyright (C) NATIONAL TAX AGENCY ALL Rights Reserved.

e-Taxから送付する「税務署からのお知らせ」と同様の文面ですが、リンクが相違しています。
心当たりのない方は、メールに表示されたリンクをクリックしないでください。
また、心当たりのある方におかれましても、e-Taxホームページから各システムにログインするなど、慎重にご対応いただきますようお願いいたします。

国税庁からのお知らせ (メールアドレスが記載 様)  

メールアドレスが記載 様

国税庁をご利用いただきありがとうございます。
ダイレクト納付がエラーとなり、納付が完了しませんでした。
エラーとなった理由について、メッセージボックスに格納しましたので、内容をご確認ください。

- ・ 滞納金合計: 10119円
- ・ 最終期限: 2022-09-24

[⇒続けるにはこちらをクリック](#)

※ 本メールは、「国税庁」にメールアドレスを登録いただいた方へ配信しております。
なお、本メールアドレスは送信専用のため、返信を受け付けておりません。ご了承ください。

発行元：国税庁 Copyright (C) NATIONAL TAX AGENCY ALL Rights Reserved.

国税庁では、メール文面に滞納金などの金額を記載したメールは、お送りしておりません。
また、e-Taxから送信するメールの宛名は、利用者ご自身で登録いただいたものとなります。
登録された宛名の確認方法については、「[こちら](#)」をご確認ください。

国税電子申告・納税システム (e-Tax) [メニューに戻る](#) ログイン中

受付システム

メールアドレスの登録等・お知らせメールの宛名登録

■ メールアドレスの登録・変更・削除

! メールアドレスはお間違いのないよう入力してください。

メールアドレスを登録することで、「税務署からのお知らせ」メールを受信することができます。メインメールアドレス以外にも受信を希望される方は、サブメールアドレスを登録ください。

- ・登録する場合は、メールアドレスを入力してください。
- ・変更する場合は、新たに登録するメールアドレスを入力してください。
- ・削除する場合は、メールアドレス入力欄を空欄にしてください。

入力が完了しましたら、「登録・変更」ボタンを押してください。

メインメールアドレス [クリア](#)

確認のため、もう一度入力してください。 [クリア](#)

サブメールアドレス1 [クリア](#)

確認のため、もう一度入力してください。 [クリア](#)

サブメールアドレス2 [クリア](#)

確認のため、もう一度入力してください。 [クリア](#)

■ お知らせメールの宛名登録

「お知らせメールへ表示する宛名」には、e-Taxから送信されるお知らせメールの件名及び本文に表示したい宛名を任意に設定していただくことが可能です。

宛名の登録を行う場合は、入力されたメインメールアドレスに確認のための案内メールを送信します。

案内メールに記載されたURLよりアクセスし、利用者別番号と暗証番号にて認証を行うことで、宛名の登録が完了します。

※宛名の登録が完了するまでは、お知らせメールに宛名は表示されませんので、ご注意ください。

登録する

宛名 (全角30文字以内)

[メニューに戻る](#) [登録・変更](#)

拡大表示

メールアドレスの登録・変更・削除

e-Taxへメールアドレスを登録いただいた方には、メッセージボックスに情報が格納された際などに「[税務署からのお知らせ](#)」メールを送信しています。詳細は、「[メールアドレス等の登録について](#)」をご確認ください。

初めてメールアドレスを登録する場合は、「メインメールアドレス」にメールアドレスを入力します。

複数のメールアドレスを登録する場合は、2件目以降を「サブメールアドレス」にメールアドレスを入力します。

メールアドレスを削除する場合は、メールアドレス入力欄に何も設定せずに「登録・変更」をクリックしてください。

お知らせメールの宛名登録

宛名をe-Taxに登録すると、e-Taxからメインメールアドレス宛に送信する「[税務署からのお知らせ](#)」メールの件名や本文に登録した宛名が表示されます。

「メインメールアドレス」を入力後、「登録する」のチェックボックスにチェックを入れ、宛名の登録を行います。

登録後、宛名に誤りがないことを確認するために有効期限が設定された「[税務署からのお知らせ【宛名の登録確認】](#)」のメールが税務署からメインメールアドレスに送信されますので、メールに記載されているURLからメールの到達確認を行ってください。有効期限内にメールの到達確認を行わなかった場合、宛名は登録されません。



[市 サイトマップ](#)[よくあるご質問](#)[お問い合わせ](#)

文字サイズ

標準

大

[ログイン](#)[個人の方](#)[法人の方](#)[電子納税](#)[お知らせ](#)[利用可能時間](#)[各ソフト・コーナー](#)[ホーム](#) > [お知らせ一覧](#) > [国税庁からの連絡を装った不審なメールについて](#)[本文へ](#)

お知らせ

掲載日：平成31年1月22日

国税庁からの連絡を装った不審なメールについて

「所得税に関する重要なお知らせ」などの件名で、国税庁からの連絡を装った不審なメールが送信されていることを把握しました。

国税庁では、e-Taxの利用にあたり、メールアドレスを登録している方に対して、メッセージボックスに情報が格納された際などに、登録しているメールアドレス宛てに「e-Tax（国税電子申告・納税システム）<info@e-tax.nta.go.jp>」の送信元表記で、定型文の「税務署からのお知らせ」メールを送信しています。

定型文に当てはまらない「税務署からのお知らせ」メールについては、酷似又は偽装したメールであり、e-Taxから送信したものではありません。このようなメールを受信された場合は、メールを開封せずに削除するなど、取り扱いには十分にご注意ください。

e-Taxから送付する「税務署からのお知らせ」メールの件名等については、「[『税務署からのお知らせ』メールが届いた方へ](#)」をご確認ください。

http://www.e-tax.nta.go.jp/topics/topics_hushin_mail_2019.htm

「税務署からのお知らせ」等のメールが届いた方へ

- (1) 「税務署からのお知らせ」等のメールとは
- (2) 「税務署からのお知らせ」等のメールの種類

(1) 「税務署からのお知らせ」等のメールとは

【令和4年8月26日追記】

以下の赤字部分を追記しました。

e-Taxでは、メールアドレスを登録している方へ、メッセージボックスに情報が格納された場合や、暗証番号の再設定のための秘密の質問と答えなどの登録を受け付けた段階で、登録しているメールアドレスあてに「[税務署からのお知らせ](#)」又は「[国税庁からのお知らせ](#)」メールを送信しています。

事前にメールに表示する宛名をe-Taxに登録することで、「税務署からのお知らせ」等メールの件名や本文に登録した宛名が表示されます。また、「税務署からのお知らせ」等メールは、以下の送信元から送信されます。

送信元表記：e-Tax（国税電子申告・納税システム）<info@e-tax.nta.go.jp>

（注1）e-Taxが送信するお知らせメールは、定型文で「[税務署からのお知らせ](#)」等のメールの種類に掲載している件名や本文のみとなります。送信元表記や件名、本文を「[税務署からのお知らせ](#)」等メールに偽装又は内容が類似したメールは、e-Taxから送信したものではありませんので、取り扱いには十分にご注意ください。

（注2）「[税務署からのお知らせ](#)」等メールには、**添付ファイルを添付することはありません** ので、添付ファイルが添付されている場合は、取り扱いには十分にご注意ください。

（注3）現在、e-Taxから送信される「[税務署からのお知らせ](#)」に類似したメールが送信されていることが確認されております。「[税務署からのお知らせ](#)」は、メッセージボックスに情報が格納された場合などに送信していますが、心当たりのない方は、それらのメールに表示されたリンク先をクリックしないでください。また、心当たりのある方におかれましても、URLを確認してからクリックするなど、慎重に対応いただきますようお願いいたします。

(2) 「税務署からのお知らせ」等のメールの種類

申告に関するお知らせ

- ▼ (件名) 税務署からのお知らせ (****様) 【申告に関するお知らせ】

代理送信が可能となったことのお知らせ(税理士の方のみに送信されます。)

- ▼ (件名) 税務署からのお知らせ (****様) 【代理送信が可能となったことのお知らせ】

e-Taxを利用して納税証明書の請求を行われた方へのお知らせ

- ▼ (件名) 税務署からのお知らせ (****様) 【納税証明書に関するお知らせ】

納付完了に関するお知らせ

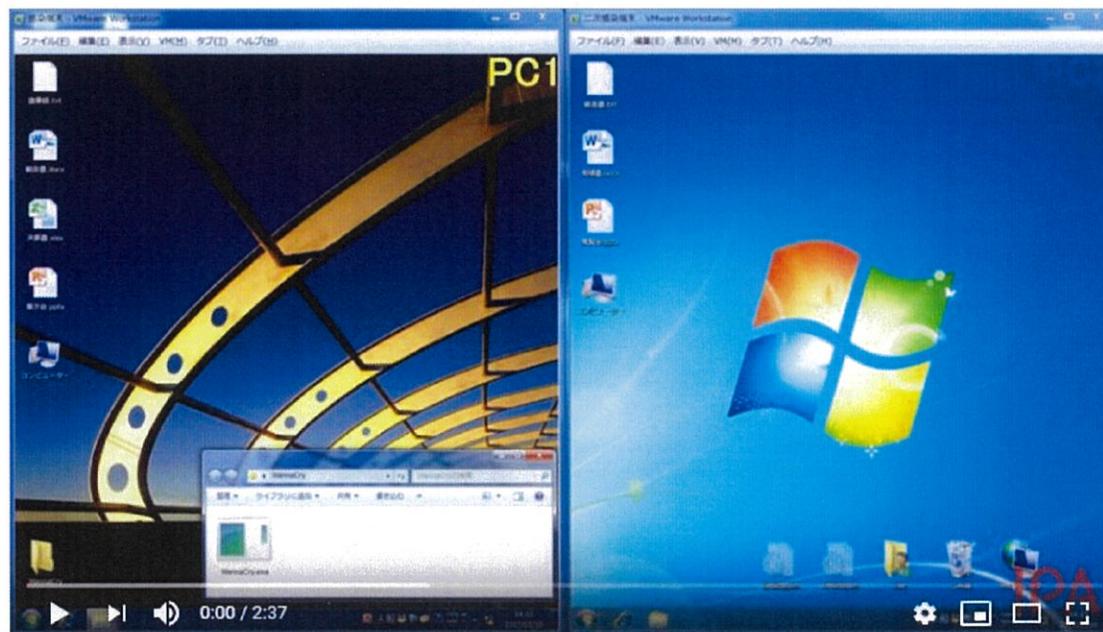
- ▼ (件名) 税務署からのお知らせ (****様) 【納付完了に関するお知らせ(納付手続重複)】

ダイレクト納付の利用者の方へのお知らせ

- ▼ (件名) 税務署からのお知らせ (****様) 【ダイレクト納付口座の登録完了に関するお知らせ】

- ▼ (件名) 税務署からのお知らせ (****様) 【ダイレクト納付口座の変更にに関するお知らせ】

- ▼ (件名) 税務署からのお知らせ (****様) 【ダイレクト納付口座の取り止めに関するお知らせ】



ランサムウェア「WannaCry (WannaCryptor)」感染実演デモ

27,481 回視聴

👍 高評価 🗨️ 低評価 ➦ 共有 📌 保存 ⋮

IPA ipajp
2017/05/31 に公開

登録済み 7264 🔔

ランサムウェア「WannaCry (WannaCryptor)」実演デモです。
同じネットワークにつながった2台のパソコンでランサムウェア「WannaCry (WannaCryptor)」
の感染が拡大する様子をデモンストレーションします。(映像時間：約3分)
[もっと見る](#)

<https://www.youtube.com/watch?v=duN9dYG4q3s>

情報セキュリティ

映像で知る情報セキュリティ ～映像コンテンツ一覧～

最終更新日：2022年9月2日
 独立行政法人情報処理推進機構
 セキュリティセンター

情報セキュリティに関する脅威や対策などを学んで頂くための映像コンテンツを、YouTube内の「[IPA Channel](#)」で公開しています。

【新作のお知らせ】

2022年3月31日 「[CVSSを活用し情報漏えいを防ごう](#)」【実証編】を公開。

2022年3月11日 「[What's BEC? ～ビジネスメール詐欺 手口と対策～](#)」を公開。

[映像で知る情報セキュリティ](#) | [情報セキュリティ技術解説映像](#) | [講演映像](#) | [ショート映像](#) | [その他](#)

映像で知る情報セキュリティ

情報セキュリティ上の様々な脅威と対策をドラマなどを通じて学べる映像シリーズです。社内研修などでご活用下さい。

IPA Channel動画の二次利用について

YouTubeの「[IPA Channel](#)」に公開している本シリーズの動画は、そのままブラウザ上で再生して社内研修用コンテンツなどにお使いいただけます。ご利用にあたっての事前申請は不要です。

YouTube動画のダウンロード、コンテンツの二次利用等につきましては、[YouTubeの利用規約](#)を遵守していただきますようお願いいたします。

主な情報セキュリティ対策動画は[動画ファイル](#)での提供も行っております。



動画ファイルのお申込み

	内容	再生時間	公開日
新作映像			
1	<p>What's BEC? ～ビジネスメール詐欺 手口と対策～</p> <p>ビジネスメール詐欺は、取引先などを装ったメールで担当者をだまし、攻撃者が用意した口座へ送金させる詐欺の手口です。海外拠点への啓発活動にも活用いただけるよう日本語字幕・英語字幕版の2種をご用意しています。</p> <p>日本語字幕版、英語字幕版</p> <p>またビジネスメール詐欺対策の特設ページを公開しています。事例の詳細な説明資料などもありますので併せてご活用下さい。</p> <p>(特設ページ)</p>	約12分	New 2022/ 03/11

情報セキュリティ

- > 脆弱性対策情報
- > 届出・相談・情報提供
- > 特集コンテンツ
- > **情報セキュリティ啓発**
 - > ここからセキュリティ！
 - > 情報セキュリティ白書
 - > 対策のしおり
 - > 映像で知る情報セキュリティ
 - > I Love スマホ生活
 - > 情報セキュリティ対策支援サイト
 - > 情報漏えい発生時の対応ポイント集
 - > 5分でできる！情報セキュリティポイント学習
 - > 標語・ポスター・4コマ漫画コンクール
 - > 情報セキュリティ読本
 - > インターネット安全教室
 - > 中小企業向け講習能力養成セミナー
 - > 中小企業の情報セキュリティ対策ガイドライン
 - > パスワード - もっと強くキミを守りたい -
 - > チョコッとプラスパスワード
 - > サイバーセキュリティのひみつ
- > 情報セキュリティ対策
- > 暗号技術
- > セキュリティエコノミクス
- > 情報セキュリティ認証関連
- > ISMAP

- 日本のIT国家戦略を技術面、人材面から支えるために設立された、経済産業省所管の独立行政法人
- 誰もが安心してITのメリットを実感できる“**頼れるIT社会**”の実現を目指しています

① 情報セキュリティ

- ウイルス、不正アクセス等の届出機関。及び、調査研究、情報セキュリティの普及啓発活動
- いち早く対策方法を広く国民に向けて発信

② 情報処理システムの信頼性向上

- 重要インフラを支える情報処理システムの信頼性向上に向けた取り組み

③ IT人材育成

- 国家試験「情報処理技術者試験」の実施機関
- IT人材の育成や発掘などの促進



1. SECURITY ACTION 制度とは
2. SECURITY ACTION 自己宣言と活用



SECURITY ACTION 制度とは

- 中小企業の“自発的な情報セキュリティ対策を促す”ための核となる取組みとして、2017年4月に創設された制度
- 日本税理士会連合会を含む、中小企業と関わりの深い商工団体、士業団体、IT関連団体、独立行政法人の強固な連携により、
中小企業の自発的な情報セキュリティ対策への取組みを促す活動を推進

(一社)中小企業診断協会
全国社会保険労務士会連合会
全国商工会連合会
全国中小企業団体中央会
(特非)ITコーディネータ協会

(特非)日本ネットワークセキュリティ協会
(独)情報処理推進機構
(独)中小企業基盤整備機構
日本商工会議所
日本税理士会連合会

<https://www.ipa.go.jp/security/security-action/>

- 中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度
 - 「中小企業の情報セキュリティ対策ガイドライン」の実践をベースに
2段階の取り組み目標を用意



セキュリティ対策自己宣言

1段階目(一つ星)

「情報セキュリティ5か条」に取り組むことを宣言



セキュリティ対策自己宣言

2段階目(二つ星)

「5分でできる！情報セキュリティ自社診断」で自社の状況を把握したうえで、情報セキュリティポリシー(基本方針)を定め、外部に公開したことを宣言

SECURITY ACTION 制度概要

普及賛同企業等

- SECURITY ACTION制度の趣旨に賛同し、当制度の普及促進に協力する企業及び団体
- 自己宣言事業者向けに様々な取組み支援策を提供



セキュリティ対策自己宣言
普及賛同団体



セキュリティ対策自己宣言
普及賛同企業

【普及賛同企業等が提供する支援策の例】

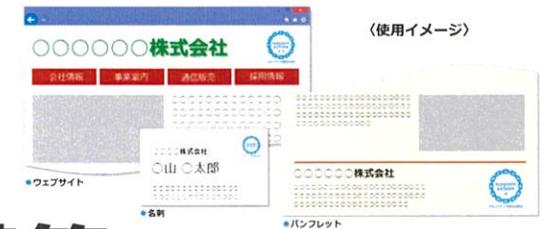
セキュリティに関する情報提供

セキュリティ体制の構築を支援

セキュリティ関連サービス提供時に優遇

・ 情報セキュリティ対策への取組みの見える化

👉 ログマークをウェブサイトに掲出したり、名刺やパンフレットに印刷することで自らの取組み姿勢をアピール



・ 顧客や取引先との信頼関係の構築

👉 既存顧客との関係性強化や、新規顧客の信頼獲得のきっかけに



・ 公的補助・民間の支援を受けやすく

👉 SECURITY ACTIONを要件とする補助金の申請、普及賛同企業から提供される様々な支援策が利用可能



CASE1

まずは「一つ星」からスタート

- ◆業種：製造業
- ◆地域：東京都大田区

取引先からセキュリティ対策状況の確認があり対策の必要性を感じていたところ、SECURITY ACTIONを知りました。まずは一つ星を宣言するために「情報セキュリティ5か条」に取組みました。低コストで行なえるのがありがたかったですし、どれも時間や手間がかかるものではありませんでした。名刺にロゴを刷り込んだので、お客様にもしっかりとアピールしたいと思います。

CASE2

“選ばれる会社”を目指して

- ◆業種：情報通信業
- ◆地域：北海道札幌市

二つ星を宣言するために自社診断を実施した結果は90点とまずまずの結果ですが、課題も見えてきました。技術的な対策を強化するとともに、人的・組織的には総務部長をセキュリティ担当者に任命し、全従業員への教育を行ないました。Webサイトにロゴマークを掲載したところお問い合わせが増え、また従業員も緊張感を維持しながら業務に臨めるなど、効果を実感しています。

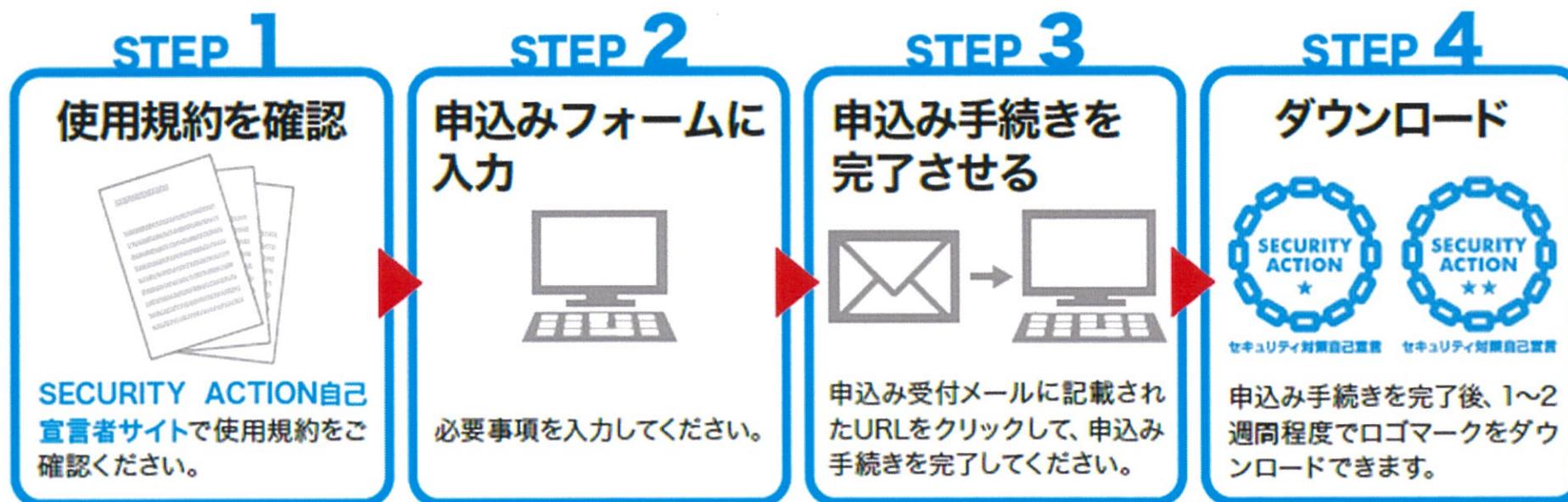
CASE3

次なるステップへの布石

- ◆業種：情報通信業
- ◆地域：大阪府大阪市

「自社のレベルを把握すること」「見えてきた弱点を強化すること」「取組みを社内外に発信すること」を狙いにSECURITY ACTIONの二つ星を宣言しました。宣言後は全ての従業員を集めて自社診断の結果を共有し、全社で対策を推進しました。SECURITY ACTIONをきっかけに社内のセキュリティ意識が高まったこともあり、次はISMS認証の取得に取組みたいと考えています。

(参考)SECURITY ACTION 申込手順

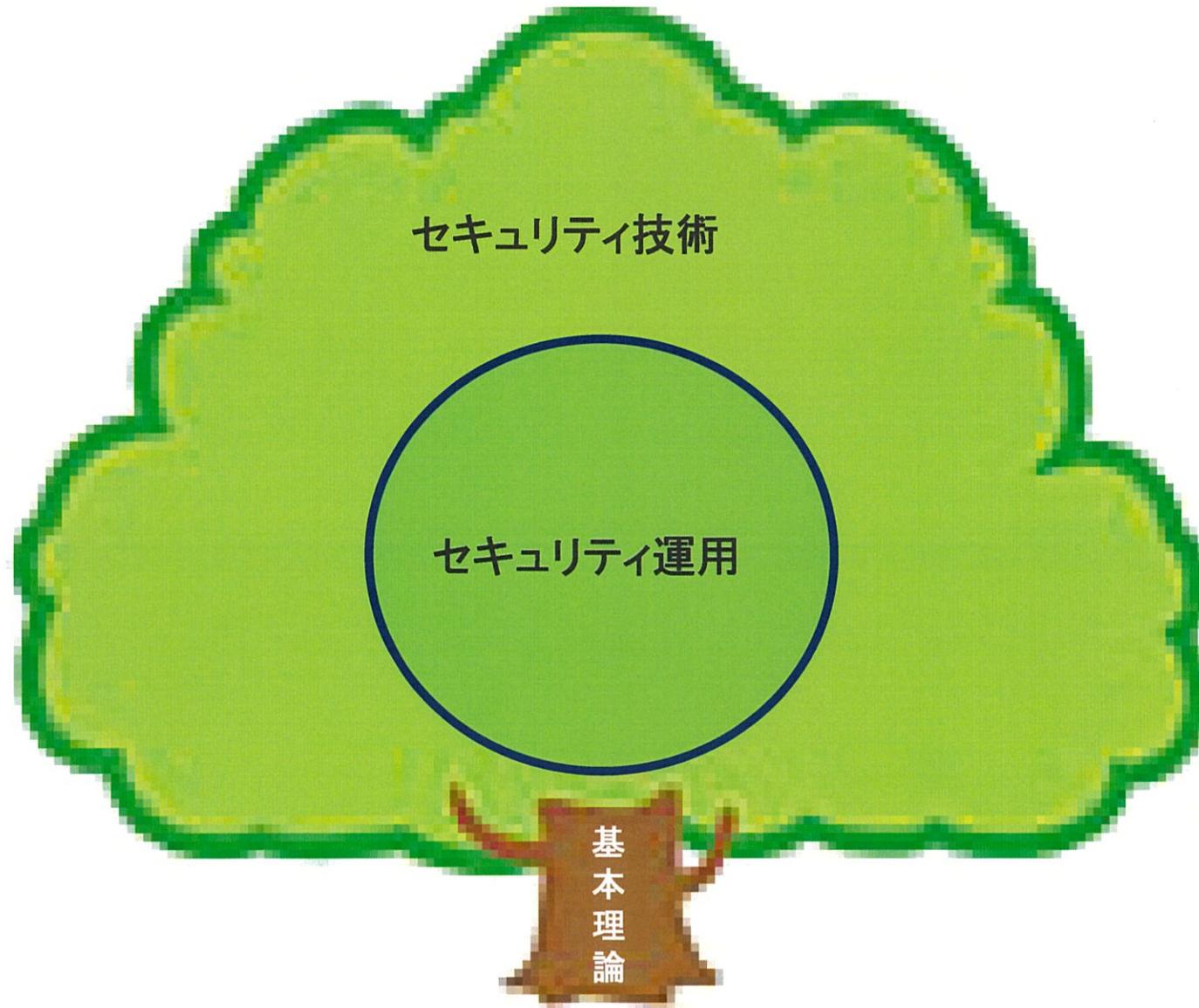


SECURITY ACTION自己宣言者サイト

<https://security-shien.ipa.go.jp/security/entry/>



セキュリティの構造



情報セキュリティとは？

下記の3つの要件を満たすもの＝情報セキュリティ

- **機密性**: アクセスを認可された者だけが、情報にアクセスできることを確実にすること。
- **完全性**: 情報および処理方法が正確であること及び完全であることを保護すること。
- **可用性**: 認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること。

情報セキュリティの問題 →

インターネット上のホームページの改ざん、ハードウェア／ソフトウェアのトラブルや関係者による情報の漏洩、コンピューターウィルスなど

→ 個別的に問題へ対処(対策)

→ 情報セキュリティマネジメントシステムとして包括的に対処(対策)

JIS Q 2700:2014 より

セキュリティとは何か？ →安全に生活するための各種の努力全般

具体的には？ → リスクを減らすこと＝セキュリティを高めること
→ リスクを減らすことが早道

リスクは何からできているか？ →資産、脅威、脆弱性

リスクを減らすにはどうするか
→資産、脅威、脆弱性のうち、どれかをなくす

三匹の子豚に見るセキュリティ



資産

脆弱性
=わらの家



脅威



資産

脆弱性
=木の家

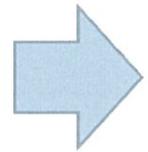


資産

脆弱性
=レンガの家+柵

ペリメーターモデル
=境界線によって安全側と危険側をわける方法

脆弱性を体系的に減らすために



ペリメーターモデル = 境界線によって安全側と危険側をわける方法
安全側において、危険側に出入りするものを厳しくチェックする考え方



ペリメーターライン = 境界線



怪しいものは入れない

価値のあるものは出さない



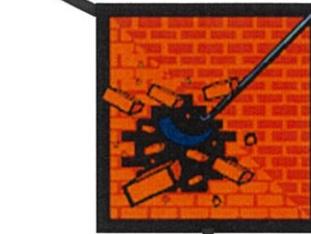
ペリメーターライン で行うこと

インターネット

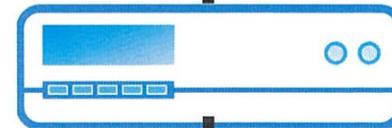


ファイヤーウォール

ペリメーターライン = 境界線

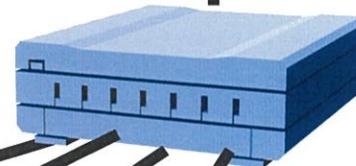


ルーター

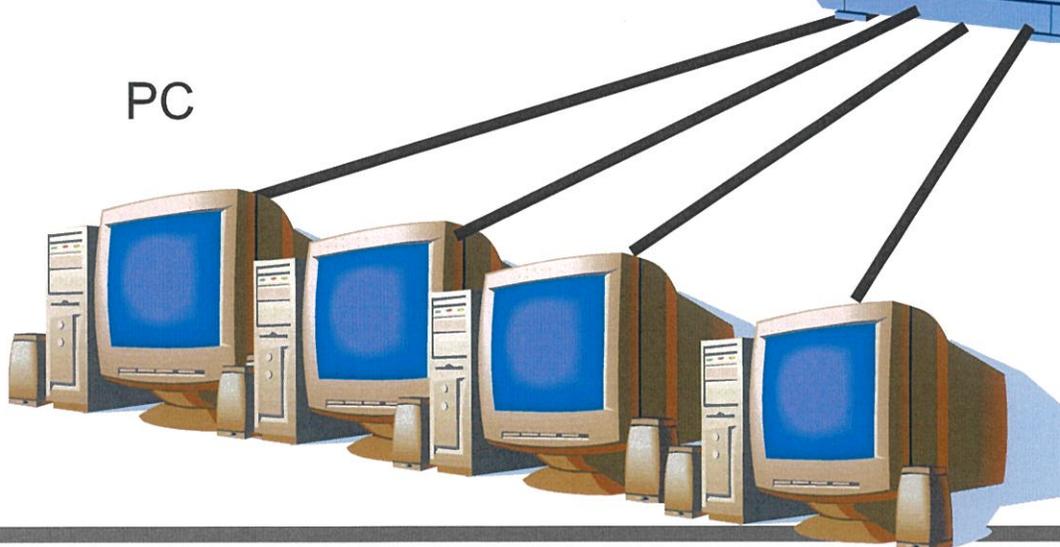


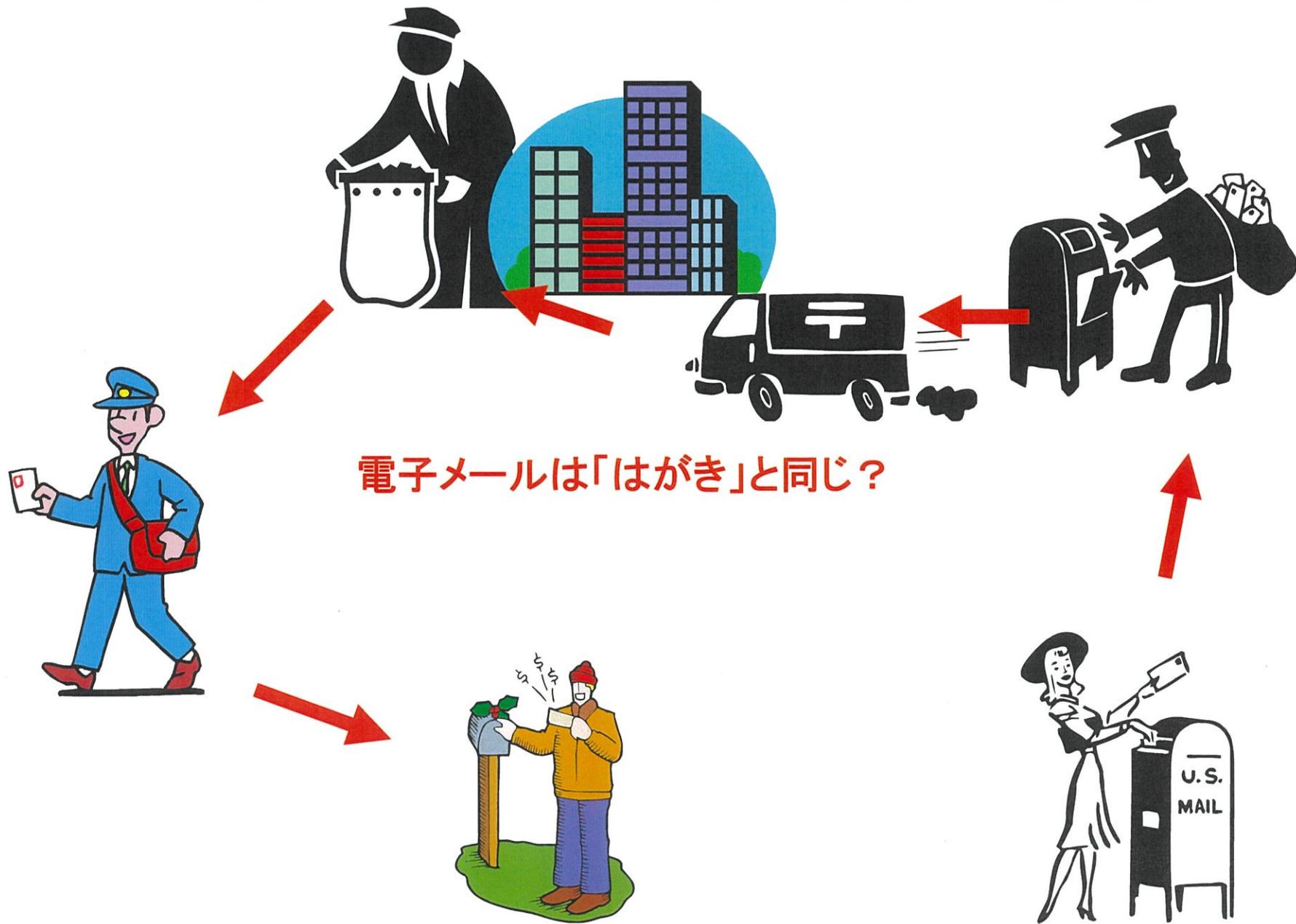
インターネットの接続にフ
ァイヤーウォールを設
定する

スイッチ



PC





1. SECURITY ACTIONとは
2. SECURITY ACTION自己宣言と活用



- **どこからどう始めたら良いか**

- 組織の実態に合わせて段階的に
- まずは、基本的なセキュリティ対策から

- **どこまで実施すれば良いか**

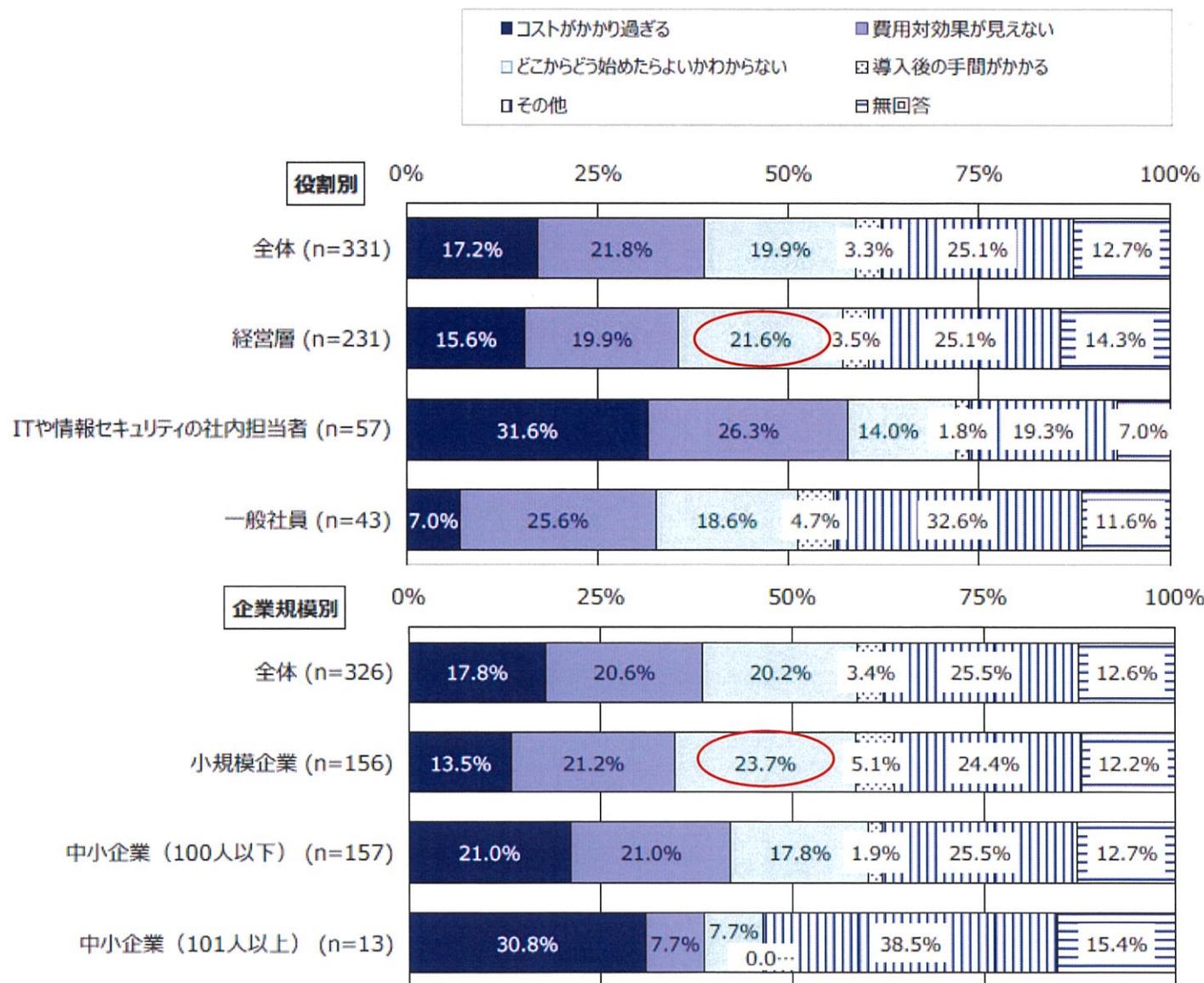
- リスクを受容できるレベルまで
- 組織における改善点を把握し、対策の周知・実践

- **誰が実施するのか**

- 経営者
- 経営者の指示のもとで重要な情報を管理する方

SECURITY ACTION の取組みから始める

(参考)IT分野の投資に情報セキュリティ対策が含まれない理由



(出典)IPA「2016年度 中小企業における情報セキュリティ対策に関する実態調査」

中小企業の情報セキュリティ対策ガイドライン第3版

IPA

<https://www.ipa.go.jp/security/keihatsu/sme/guideline/>

- 中小企業の経営者や実務担当者が、情報セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順等を示したガイドライン
- 「クラウドサービス安全利用の手引き」を追加
- 本編2部と付録より構成
 - 経営者が認識すべき「3原則」、経営者がやらなければならない「重要7項目の取組」を記載
 - 情報セキュリティ対策の具体的な進め方を分かりやすく説明
 - すぐに使える「情報セキュリティ基本方針」や「情報セキュリティ関連規程」等のひな形を付録



IPPA 中小企業の情報セキュリティ対策ガイドライン

ipa.go.jp/security/keihatsu/sme/guideline/

文字サイズ 標準 拡大 検索

IPPA Better Life with IT 情報処理推進機構

IPPAについて お知らせ サイトマップ お問い合わせ ENGLISH

HOME 情報セキュリティ 産業サイバーセキュリティセンター 社会基盤センター 未踏/セキュリティキャンプ IT人材の育成 情報処理技術者試験 情報処理安全確保支援士試験

HOME > 情報セキュリティ > 情報セキュリティ啓発 > 中小企業の情報セキュリティ対策ガイドライン 本文を印刷する

情報セキュリティ

中小企業の情報セキュリティ対策ガイドライン

最終更新日：2021年3月10日
独立行政法人情報処理推進機構
セキュリティセンター

IPPA（独立行政法人情報処理推進機構）は、中小企業の情報セキュリティ対策に関する検討を行い、より具体的な対策を示す「中小企業の情報セキュリティ対策ガイドライン」を公開しました。

概要

「中小企業の情報セキュリティ対策ガイドライン」（以下「本ガイドライン」）は、情報セキュリティ対策に取り組む際の、(1)経営者が認識し実施すべき指針、(2)社内において対策を実施する際の手順や手法をまとめたものです。経営者編と実践編から構成されており、個人事業主、小規模事業者をも含む中小企業（以下「中小企業等」）の利用を想定しています。

第3版は第2版（2016年11月公開）から2年4か月ぶりの大規模改訂で、「サイバーセキュリティ経営ガイドライン」の改訂や、中小企業等を対象としたクラウドサービスの充実化などの環境変化を受けたものです。改訂のポイントは、専門用語の使用を可能な限り避け、ITに詳しくない中小企業等の経営者にとって理解しやすい表現としたことです。

例えば実践編において、対策に取り組めていない中小企業等が組織的な対策の実施体制を段階的に進めていけるよう構成の見直しを行ったことです。また、クラウドサービスを安全に利用するための留意事項やチェック項目を記し、付録として新たに「中小企業のためのクラウドサービス安全利用の手引き」を追加しました。

中小企業等ではITの利活用が進む一方で、サイバー攻撃手法の巧妙化、悪質化などにより事業に悪影響を及ぼすリスクはますます高まってきています。また、サプライチェーンを構成する中小企業においては発注元企業への標的型攻撃の足掛かりとされる懸念も指摘されており、早急な対策実施が必須であると言えます。

本ガイドラインおよび「SECURITY ACTION」制度の活用によって、ITを利活用している中小企業が情報セキュリティ対策に取り組み、経済社会全体のサイバーリスク低減につながることを期待しています。

ガイドライン等のダウンロード

本編：中小企業の情報セキュリティ対策ガイドライン第3版（全60ページ、32.56MB）

情報セキュリティ

- 脆弱性対策情報
- 届出・相談・情報提供
- 特集コンテンツ
- 情報セキュリティ啓発
 - ここからセキュリティ！
 - セキュリティ白書2020
 - 対策のしおり
 - 映像で知る情報セキュリティ
 - I Love スマホ生活
 - 情報セキュリティ対策支援サイト
 - 情報漏えい発生時の対応ポイント集
 - 5分でできる！情報セキュリティポイント学習
 - 標語・ポスター・4コマ漫画コンクール
 - 漏れたら大変！個人情報
 - 情報セキュリティ読本

ここにを入力して検索

16°C 12:41 2021/10/18

ガイドラインの構成



ガイドラインP.3

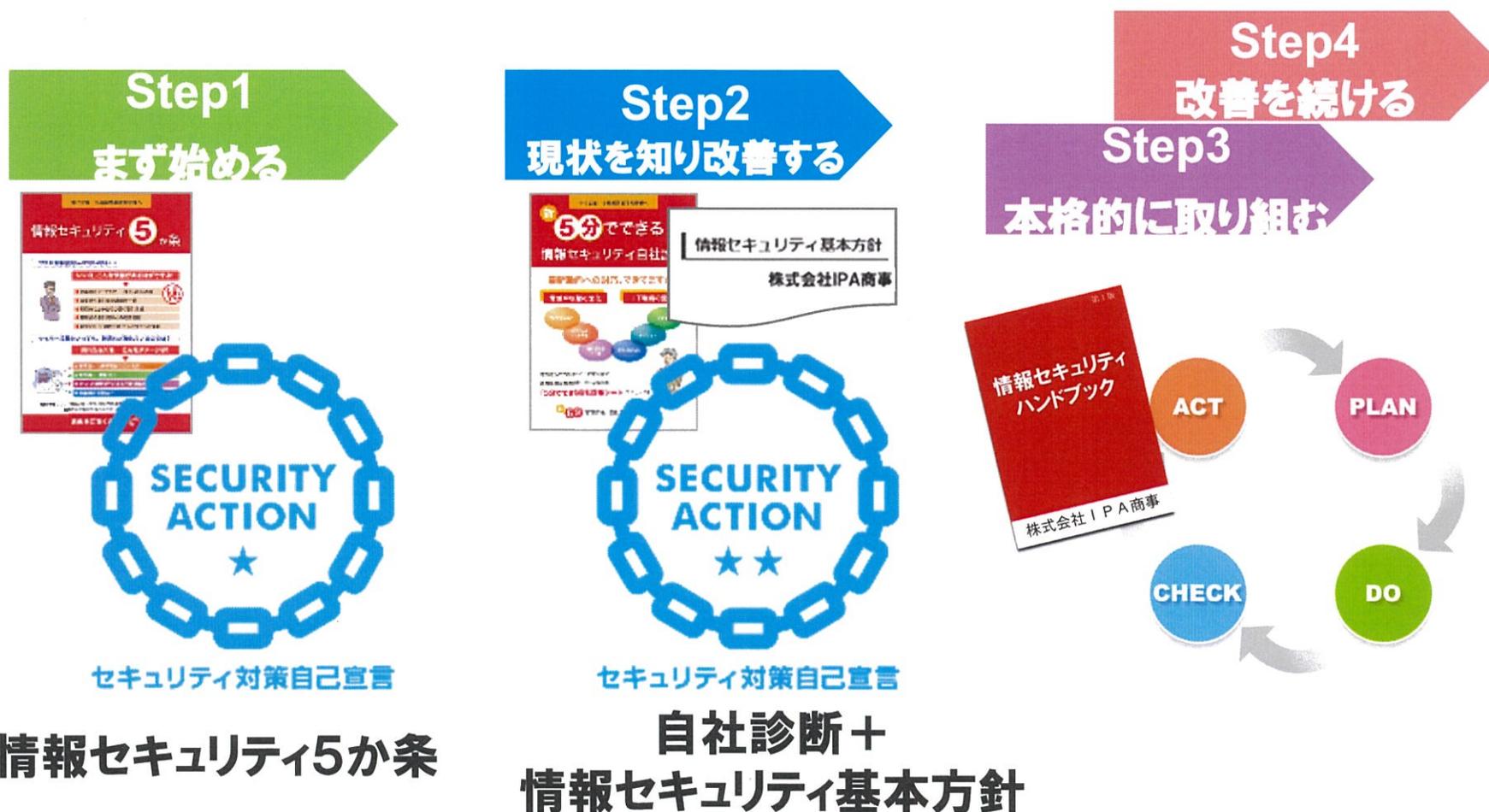
- 中小企業の情報セキュリティ対策の考え方や実践方法について、本編2部と付録より構成

	構成	概要
本編	第1部 経営者編	経営者が知っておくべき事項、および自らの責任で考えなければならない事項について説明しています。
	第2部 実践編	情報セキュリティ対策を実践する方向けに、対策の進め方についてステップアップ方式で具体的に説明しています。
付録	付録1 情報セキュリティ5か条	組織の規模を問わず必ず実行していただきたい重要な対策を5か条にまとめ説明しています。
	付録2 情報セキュリティ基本方針(サンプル)	組織としての情報セキュリティに対する基本方針書のサンプルです。
	付録3 5分でできる！ 情報セキュリティ自社診断	あまり費用をかけることなく実行することで効果がある25項目のチェックシートです。
	付録4 情報セキュリティハンドブック(ひな形)	従業員に対して対策内容を周知するために作成するハンドブックのひな形です。
	付録5 情報セキュリティ関連規程(サンプル)	情報セキュリティに関する社内規則を文書化したもののサンプルです。
	付録6 中小企業のための クラウドサービス安全利用の手引き	クラウドサービスを安全に利用するための手引きです。15項目のチェックシートが付いています。
	付録7 リスク分析シート	情報資産、脅威の状況、対策状況をもとに損害を受ける可能性(リスク)の見当をつけることができます。

情報セキュリティ対策ガイドラインと

SECURITY ACTION の位置づけ

- 「中小企業の情報セキュリティ対策ガイドライン」に従って取組みます





セキュリティ対策自己宣言

一つ星

情報セキュリティ5か条 に取り組む

- 一つ星を使用するには、「情報セキュリティ5か条」に取り組むことを宣言

- 1 OSやソフトウェアは常に最新の状態にしよう！
- 2 ウイルス対策ソフトを導入しよう！
- 3 パスワードを強化しよう！
- 4 共有設定を見直そう！
- 5 脅威や攻撃の手口を知ろう！

中小企業・小規模事業者の皆様へ

情報セキュリティ 5か条

ウチには秘密なんかいないなあ・・・

いいえ、こんな情報があるはずですよ!

- 従業員のマイナンバー、住所、給与明細
- お客様や取引先の連絡先一覧
- 取引先ごとの仕切り額や取引実績
- 新製品の設計図などの開発情報
- 取引先から“取扱注意”として預かった情報

サイバー攻撃といっても、被害など知れているのでは？

漏れたら大変! こんなダメージが!

- 被害者への損害賠償などの支払い
- 取引停止、顧客流出
- ネットの遮断などによる生産効率のダウン
- 従業員の士気低下

情報セキュリティ対策と言っても、何をすれば良いのか分からない組織では、裏面の5か条を守るところから始めてみましょう。

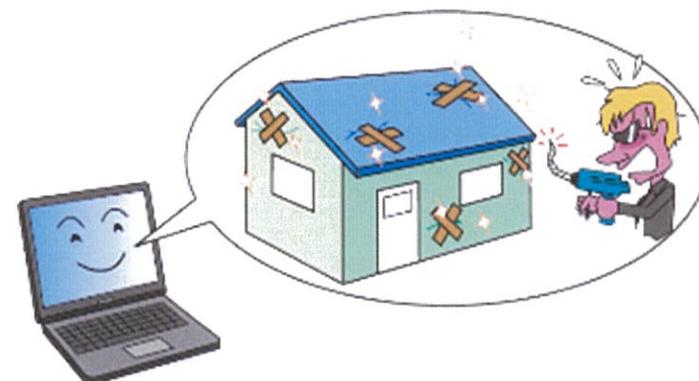
裏面をご覧ください

1 OSやソフトウェアは常に最新の状態に

- OS やソフトウェアのセキュリティ上の問題点を放置していると、それを悪用したウイルスに感染してしまう危険性があります。お使いの OS やソフトウェアに修正プログラムを適用する、もしくは最新版を利用しましょう。

<対策例>

- Windows Update(Windows OSの場合)/ソフトウェア・アップデート(Mac OSの場合)
- OSバージョンアップ(Android の場合)
- Adobe Flash Player/Adobe Reader/Java実行環境(JRE)など
利用中のソフトウェアを最新版にする

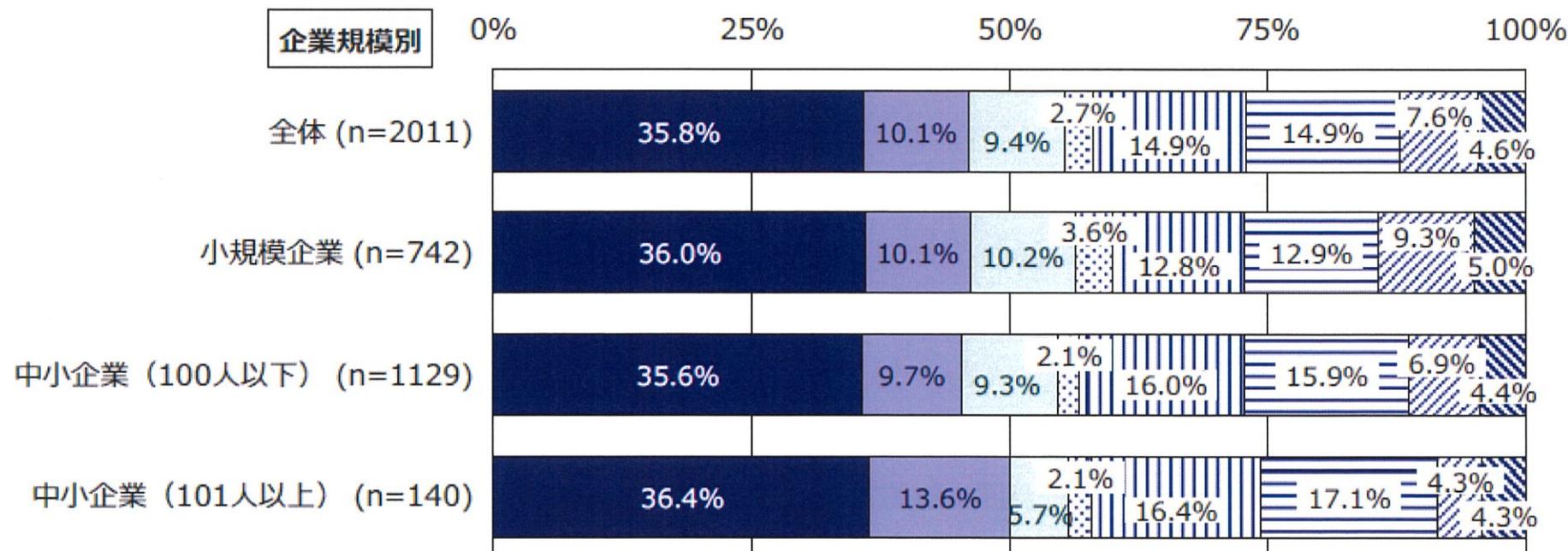


脆弱性を悪用された被害事例

事例	業種	所在地	従業員規模
<p>オフライン運用していたWindows XPパソコンを、不注意により ネットワーク接続したところ、ウェブサイトの閲覧を通じて ランサムウェアに感染し、ファイルが暗号化された。 バックアップファイルからデータを復元できたため被害は最小限で済んだ。</p>	製造業	新潟県	21～50名
<p>ウイルス対策ソフトの導入やOS・アプリケーションの定期的なアップデートが十分でない等、自社のメールサーバのセキュリティ管理が十分でなかったことが原因で、電子メールの不正送信の踏み台に されたことがあり、自社の実害は生じていないものの、知らない間に攻撃の一端を担うこととなった。</p>	情報 通信業	奈良県	5名以下
<p>CMS (Contents Management System) の脆弱性を攻撃され、ウェブサイトの一部が改ざんされることで、意図しない有害サイトへ誘導される事案が発生した。 機密情報などを扱うサーバではなかったため、実害はなかったが、自社内で実際に発生したため、セキュリティ被害は身近なものであると感じた。</p>	運輸業	宮崎県	101～300名

(参考)セキュリティパッチの適用状況

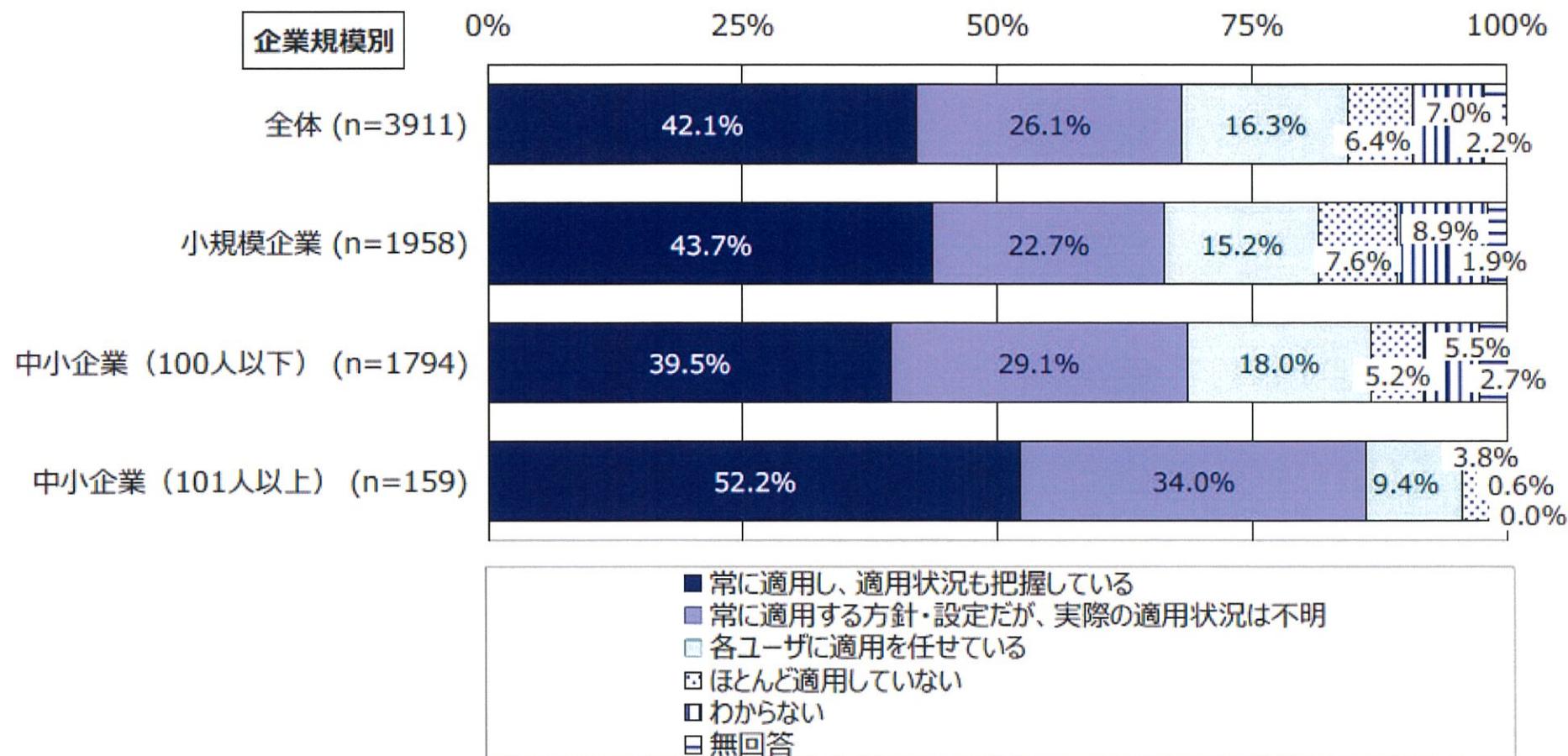
※外部に公開しているネットワークサーバ



- ほぼ全サーバに適用している
- アプリケーションに影響がないことを確認できたもののみを適用している
- 情報セキュリティ対策上重要なもののみを適用している
- ほとんど適用していない
- 外部事業者に運用を委託しているので、自ら適用する必要がない
- 該当するようなサーバを利用していない
- わからない
- 無回答

(出典)IPA「2016年度 中小企業における情報セキュリティ対策に関する実態調査」

(参考)PC へのセキュリティパッチの適用状況



(出典)IPA「2016年度 中小企業における情報セキュリティ対策に関する実態調査」

脆弱性を悪用した攻撃 ~ランサムウェア:WannaCry~

■ 攻撃者



何らかの手段により、
WannaCryを感染させる。

■ 被害を受けた組織

パソコン1



一次感染したパソコン



パソコン2

二次感染したパソコン

WindowsOSのファイル共有機能に存在する脆弱性を悪用して、組織内で感染を拡大

2 ウイルス対策ソフトを導入

- ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えています。ウイルス対策ソフトを導入し、ウイルス定義ファイル(パターンファイル)は常に最新の状態になるようにしましょう。

<対策例>

- ウイルス定義ファイルが自動更新されるように設定する
- 統合型のセキュリティ対策ソフト(ファイアウォールや脆弱性対策など統合的なセキュリティ機能を搭載したソフト)を導入する



ウイルス対策ソフト運用に伴う被害事例

事例	業種	所在地	従業員規模
<p>役員のパソコンがウイルスに感染し、保存されていた過去の電子メールが、これまでの送受信先などに大量に送信され、自社および取引先の重要な情報が漏えいしてしまった。取引先からはクレームが上がり、謝罪をしたものの信頼を失墜することとなった。</p> <p><u>ウイルス対策ソフトのアップデートが実施されていなかった</u></p>	製造業	栃木県	51～100名
<p><u>ウイルス対策ソフトの契約更新を失念</u>し、数日間サポートが切れた。そのわずかの間に、インターネットに繋がっていたパソコンが「トロイの木馬」に感染した。急ぎアプリケーションを停止し、自社でリカバリーしたが、復旧までに約2か月を要し、その間、仕事にも支障をきたした。</p>	卸売業	福岡県	21～50名
<p>ウイルス感染により、機密情報の漏えいや基幹システムの停止の被害を受けたが、ウイルスの感染経緯や原因を解明することはできなかった。</p> <p>その後、被害範囲の限定や、対策の検討、再発防止など、被害後の対応に多大の工数を要した。</p> <p>外部と接続している状況にも関わらず、<u>ウイルス対策ソフトを導入していなかった</u>。</p>	サービス業	東京都	21～50名

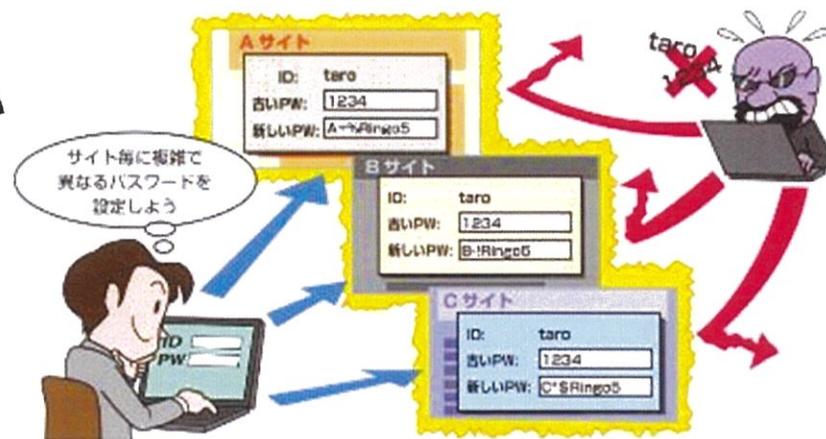
(出典)IPA「2016年度中小企業における情報セキュリティ対策の実態調査 - 事例集 -」をもとに作成

3 パスワードを強化

- パスワードが推測や解析されたり、ウェブサービスから窃取したID・パスワードが流用されることで、不正にログインされる被害が増えています。パスワードは「長く」「複雑に」「使い回さない」ようにして強化しましょう。

<対策例>

- パスワードは英数字記号含めて長い文字数にする
- 名前、電話番号、誕生日、簡単な英単語などはパスワードに使わない
- 同じID・パスワードをいろいろなウェブサービスで使い回さない



脆弱なパスワードの事例

事例	業種	所在地	従業員規模
<p>ある担当者が業績を上げたい一心で別担当者のシステム上の保守情報にアクセスした。 幸い目的が個人情報ではなく、業務処理件数、保守ノウハウ等の取得にあったため大事には至らなかった。 パスワードが推測可能なほど弱かったのが原因である。ユーザIDとパスワードの強化を徹底するなど、自社システムの情報セキュリティ対策についても改善に取り組むこととなった。</p>	サービス業	福岡県	6～20名
<p>個人情報保護法の制定と自社で扱う情報の増加をきっかけとして、経営トップの判断で情報セキュリティ対策を行うこととなり、 コンサルティング会社に調査を依頼したところ、パソコンを共有のパスワードで運用している例など100以上の指摘を受けた。</p>	金融業	熊本県	51～100名

パスワードの最大解読時間

• ZIPの場合

	4桁	6桁	8桁	10桁
英小文字 (26字)	1秒以下	1秒以下	46秒	9時間
英大小文字+数字 (62字)	1秒以下	13秒	13.5時間	6年
英大小文字+数字+記号 (93字)	1秒以下	2分24秒	14日	341年

• DOCXの場合

	4桁	6桁	8桁	10桁
英小文字 (26字)	20秒	44分	13.5時間	195年
英大小文字+数字 (62字)	10分42秒	29日	301年	1,158千年
英大小文字+数字+記号 (93字)	55分	326日	7,800年	66,726千年

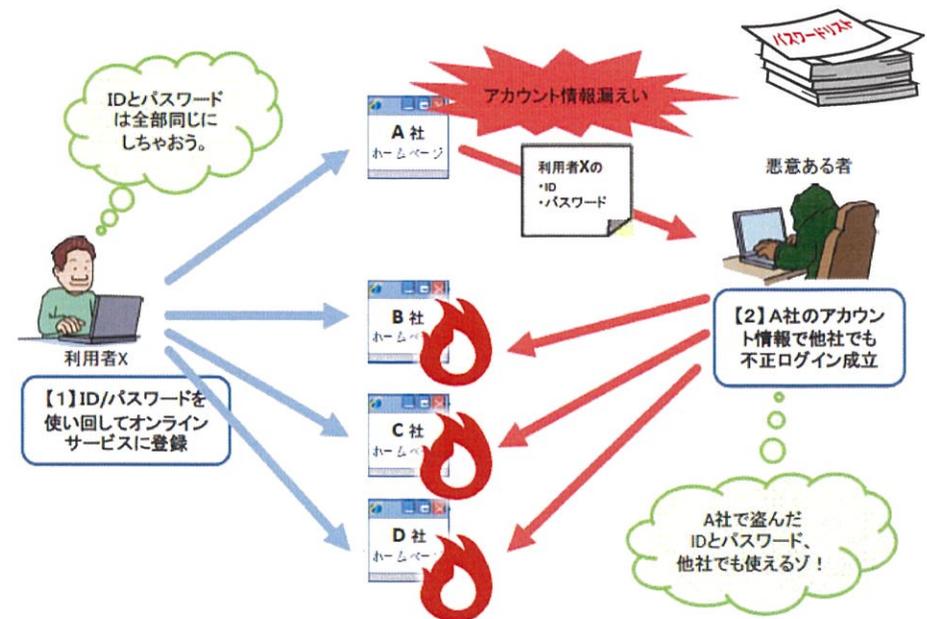
(出典)株式会社ディアイティ「パスワードの最大解読時間測定【暗号強度別】」2012年12月

最悪なパスワード

(参考) 最悪なパスワードランキング

順位	パスワード	
1	123456	—
2	password	—
3	12345678	1Up
4	qwerty	2Up
5	12345	2Down
6	123456789	New
7	letmein	New
8	1234567	—
9	football	4Down
10	iloveyou	New

出典: SplashData社「WORST PASSWORDS OF 2017」



パスワードリスト攻撃にご注意を!

パスワードの定期変更について

実は危ない、パスワードの定期変更

スタートアップ

2016/8/11 6:30

保存 共有 印刷

VB

アカウントを安全に保つため、学校や職場から2～3カ月ごとにパスワードを変更するよう求められているのではないかと。これは広く実施されているセキュリティの推奨事項だ。

ただし、これは完全に間違っている。

米連邦取引委員会（FTC）でチーフテクノロジーリストを務めるローリー・クレイナー氏は先週、米ラスベガスで開催されたセキュリティ会議でこの“通説”を打破した。

■かえって安全性が低下することも

つまり、定期的にパスワードの変更を要求

当たり前のように使われている「パスワードの定期的な変更」はかえってセキュリティを弱めることがある

日経平均(円)	22,580.83	-116.07	-0.51%
NYダウ(ドル)	25,974.99	+22.51	+0.08%
日経アジア300	1,291.85	-25.02	-1.89%
ドル(円)	111.49-50	+0.04円安	+0.03%
ユーロ(円)	129.70-74	+0.92円安	+0.71%
長期金利(%)	0.110	-0.005	
NY原油(ドル)	68.63	-0.09	-0.13%

日経平均について (銘柄一覧) Quick

日経ウーマノミクスプロジェクト

会員が20万人を突破しました

女性に役立つイベントを随時開催中

▶ 無料会員登録はこちら

認証の仕組みと必要性

インターネットでは、通信している相手が本人かどうかを確認する手段として認証と呼ばれる方法がとられます。

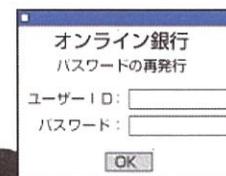
インターネットの認証は、利用者を識別する情報と、それを確認する情報を組み合わせることで行われます。利用者を識別する情報には、IDが一般的に使用されます。IDとは、情報機器やサービスの提供者が、一人ひとりの利用者を区別して割り振る符号です。IDと組み合わせて確認する情報として、パスワードが使用されます。パスワードとは、そのIDを割り振られた本人だけが知る情報で、それを入力することでIDを持つ本人であることを確認するための符号です。パスワード以外では、カードや生体(指紋や網膜などの、バイオメトリクス情報)などが使われることもあります。

IDとパスワードは、パソコンなどの情報機器や、インターネット上のサービスを利用する際に、許可された者であることを識別し、本人を確認するための重要な情報です。

利用者の範囲が制限されている情報機器やインターネットサービスに、IDとパスワードを入力して、その機器やサービスを利用できる状態にすることをログインといいます。この確認のやりとりのことを認証と呼んでいます。利用を終了して、機器やサービスから離れる行為のことはログアウトといいます。

このような認証の仕組みによって、ネットワークや情報機器を利用する際に、利用する権限のない第三者の利用を防止します。しかし、IDやパスワードなど認証で使っている情報(アカウント情報)が不適切な管理や、攻撃などで盗まれてしまうと、なりすましなどの不正行為が行われてしまう危険性もあります。

このような手口による被害にあわないよう、認証の仕組みと重要性を理解し、IDやパスワードなどのアカウント情報は厳重に管理するようにしましょう



オンライン銀行
パスワードの再発行

ユーザーID:

パスワード:

OK



総務省 国民のための情報セキュリティサイト より

http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/privacy/01-1.html

設定と管理のあり方

他人に自分のユーザアカウントを不正に利用されないようにするには、適切なパスワードの設定と管理が大切です。適切なパスワードの設定・管理には、以下の3つの要素があります。

1.安全なパスワードの設定 2.パスワードの保管方法 3.パスワードを複数のサービスで使い回さない(定期的な変更は不要)

1.安全なパスワードの設定

安全なパスワードとは、他人に推測されにくく、ツールなどで割り出しにくいものを言います。

- (1) 名前などの個人情報からは推測できないこと
- (2) 英単語などをそのまま使用していないこと
- (3) アルファベットと数字が混在していること
- (4) 適切な長さの文字列であること
- (5) 類推しやすい並び方やその安易な組合せにしないこと

逆に、危険なパスワードとしては、以下のようなものがあります。このような危険なパスワードが使われていないかどうか、チェックをするようにしましょう。

(1) 自分や家族の名前、ペットの名前

yamada、tanaka、taro、hanako(名前) 19960628、h020315(生年月日) tokyo、kasumigaseki(住所)
3470、1297(車のナンバー) ruby、koro(ペットの名前)

(2) 辞書に載っているような一般的な英単語

password、baseball、soccer、monkey、dragon

(3) 同じ文字の繰り返しやわかりやすい並びの文字列

aaaa、0000(同じ文字の組み合わせ) abcd、123456、200、abc123(安易な数字や英文字の並び)
asdf、qwerty(キーボードの配列) (4) 短すぎる文字列 gf、ps

この他、電話番号や郵便番号、生年月日、社員コードなど、他人から類推しやすい情報やユーザIDと同じものなどは避けましょう。

設定と管理のあり方

2. パスワードの保管方法

せっかく安全なパスワードを設定しても、パスワードが他人に漏れてしまえば意味がありません。以下が、パスワードの保管に関して特に留意が必要なものです。

パスワードは、同僚などに教えないで、秘密にすること

パスワードを電子メールでやりとりしないこと

パスワードのメモをディスプレイなど他人の目に触れる場所に貼ったりしないこと

やむを得ずパスワードをメモなどで記載した場合は、鍵のかかる机や金庫など安全な方法で保管すること

3. パスワードを複数のサービスで使い回さない(定期的な変更は不要)

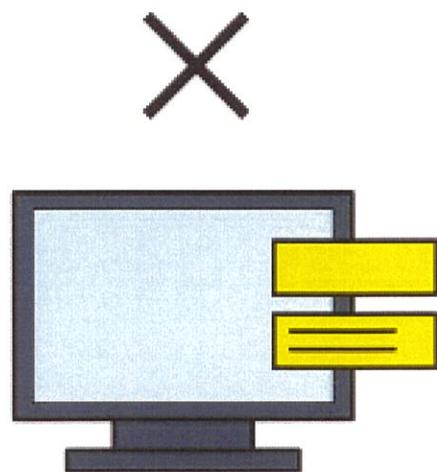
またパスワードはできる限り、複数のサービスで使い回さないようにしましょう。あるサービスから流出したアカウント情報を使って、他のサービスへの不正ログインを試す攻撃の手口が知られています。もし重要情報を利用しているサービスで、他のサービスからの使い回しのパスワードを利用していた場合、他のサービスから何らかの原因でパスワードが漏洩してしまえば、第三者に重要情報にアクセスされてしまう可能性があります。

なお、利用するサービスによっては、パスワードを定期的に変更することを求められることもありますが、実際にパスワードを破られアカウントが乗っ取られたり、サービス側から流出した事実がなければ、パスワードを変更する必要はありません。むしろ定期的な変更をすることで、パスワードの作り方がパターン化し簡単なものになることや、使い回しをするようになることの方が問題となります。定期的に変更するよりも、機器やサービスの間で使い回しのない、固有のパスワードを設定することが求められます。

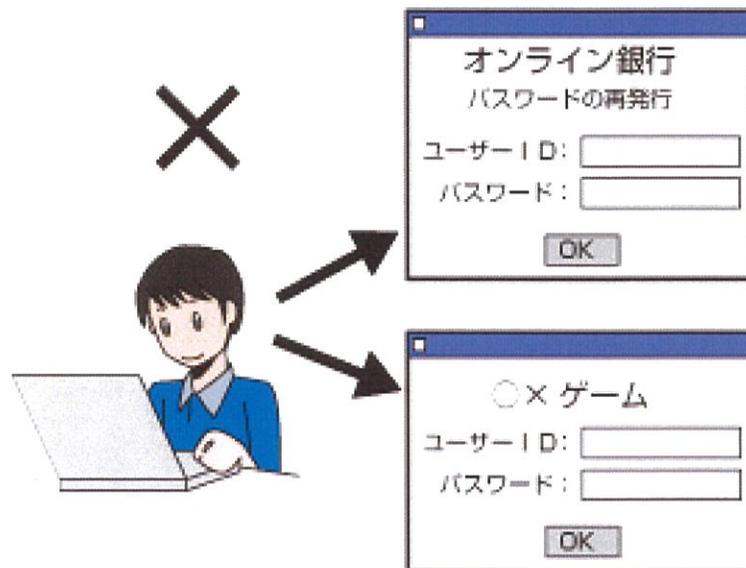
これまでは、パスワードの定期的な変更が推奨されてきましたが、2017年に、米国国立標準技術研究所(NIST)からガイドラインとして、サービスを提供する側がパスワードの定期的な変更を要求すべきではない旨が示されたところ(※1)。また、日本においても、内閣サイバーセキュリティセンター(NISC)から、パスワードを定期変更する必要はなく、流出時に速やかに変更する旨が示されています(※2)。

(※1) NIST SP800-63B(電子的認証に関するガイドライン)

(※2) <https://www.nisc.go.jp/security-site/handbook/index.html>



ディスプレイにパスワードを
貼り付けている



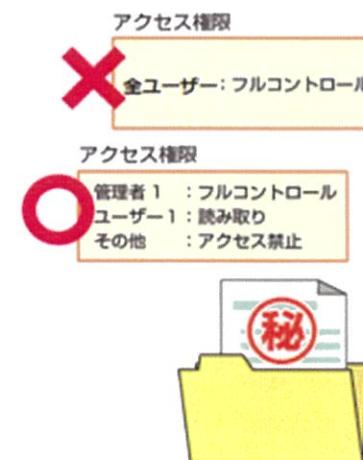
複数のサービスで同一の
パスワードを使い回している

4 共有設定を見直す

- データ保管などのクラウドサービスやネットワーク接続の複合機の設定を間違っただけ無関係な人に情報を覗き見られるトラブルが増えています。
クラウドサービスや機器は必要な人にのみ共有されるよう設定しましょう。

<対策例>

- クラウドサービスの共有範囲を限定する
- ネットワーク接続の複合機やカメラ、ハードディスク(NAS)などの共有範囲を限定する
- 従業員の異動や退職時に設定の変更(削除)漏れがないように注意する



不適切な共有設定による被害事例

事例	業種	所在地	従業員規模
<p><u>関係者しか立ち入ることのできない設備の写真</u>が、業務と直接関係がない非公式な文書に掲載されて委託元に送付される事案が発生した。</p> <p>調査の結果、退職した従業員によるものと判明し、委託元からは信用回復のため再発防止策を求められることとなった。</p>	サービス業	栃木県	6～20名
<p>多様な端末からの公式サイトへのアクセスを可能にし、当社が手掛けるサービスも幅広い端末で利用できるようするために、アクセス制御を緩めた。</p> <p>同時にSQL インジェクション、DoS・DDoS 攻撃など不正アクセスが目立つようになってきた。これらの攻撃により、ネットワークやCPU やメモリなどの資源が占有され、サービスに支障をきたした。</p>	情報通信業	東京都	5名以下
<p><u>共有フォルダにアクセス権が設定されておらず</u>、「ランサムウェア」に感染し、共有フォルダ内のいくつかのPDF ファイルが暗号化されてしまった。結局、そのファイルを削除し、紙ベースで管理していた情報をスキャナーで読み込んで復元した。</p> <p>販売店との契約書や従業員情報等があったが情報量としてはあまり多くないので、何とか復元でき、事なきを得た。</p>	卸売業	滋賀県	6～20名

5 脅威や攻撃の手口を知る

- 取引先や関係者と偽ってウイルス付のメールを送ってきたり、正規のウェブサイトにした偽サイトを立ち上げてID・パスワードを盗もうとする巧妙な手口が増えています。脅威や攻撃の手口を知って対策をとりましょう。

<対策例>

- IPAなどのセキュリティ専門機関のウェブサイトやメールマガジンで最新の脅威や攻撃の手口を知る
- 利用中のインターネットバンキングやクラウドサービスなどが提供する注意喚起を確認する



IPA 情報セキュリティ10大脅威 2021 : X +

ipa.go.jp/security/vuln/10threats2021.html

IPA Better Life with IT 情報処理推進機構

文字サイズ 標準 拡大 検索

IPAについて お知らせ一覧 サイトマップ お問い合わせ ENGLISH

HOME 情報セキュリティ 産業サイバーセキュリティセンター 社会基盤センター 未踏/セキュリティキャンプ IT人材の育成 情報処理技術者試験 情報処理安全確保支援士試験

HOME > 情報セキュリティ > 情報セキュリティ対策 > 脆弱性対策 > 情報セキュリティ10大脅威 2021 本文を印刷する

情報セキュリティ

情報セキュリティ10大脅威 2021

最終更新日：2021年8月23日

「情報セキュリティ10大脅威 2021」を公開

※2021年8月23日：「情報セキュリティ10大脅威 2021」簡易説明資料[個人編]（一般利用者向け）を公開しました。

「情報セキュリティ10大脅威 2021」は、2020年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約160名のメンバーからなる「10大脅威選考会」が脅威候補に対して審議・投票を行い、決定したものです。

■「情報セキュリティ10大脅威 2021」 **NEW**：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
1位	スマホ決済の不正利用	1位	ランサムウェアによる被害	5位
2位	フィッシングによる個人情報等の詐取	2位	標的型攻撃による機密情報の窃取	1位
7位	ネット上の誹謗・中傷・テマ	3位	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW

00008883510大脅威.pdf

すべて表示

ここに入力して検索

12:53 2021/10/18

情報セキュリティ

10大脅威 2022

～誰かが対策をしてくれている。そんなウマイ話は、ありません！！～



表 1.1 情報セキュリティ 10大脅威 2022 「個人」および「組織」向けの脅威の順位

「個人」向け脅威	順位	「組織」向け脅威
フィッシングによる個人情報等の詐取	1	ランサムウェアによる被害
ネット上の誹謗・中傷・デマ	2	標的型攻撃による機密情報の窃取
メールや SMS 等を使った脅迫・詐欺の手口による金銭要求	3	サプライチェーンの弱点を悪用した攻撃
クレジットカード情報の不正利用	4	テレワーク等のニューノーマルな働き方を狙った攻撃
スマホ決済の不正利用	5	内部不正による情報漏えい
偽警告によるインターネット詐欺	6	脆弱性対策情報の公開に伴う悪用増加
不正アプリによるスマートフォン利用者への被害	7	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)
インターネット上のサービスからの個人情報の窃取	8	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	9	予期せぬ IT 基盤の障害に伴う業務停止
インターネット上のサービスへの不正ログイン	10	不注意による情報漏えい等の被害

情報セキュリティ5か条は 10大脅威にも有効な対策！！

- 「10大脅威」の順位は毎年変動するが、基本的な対策の重要性は長年変わらない

情報セキュリティ**5**か条

情報セキュリティ10大脅威2018

順位	組織の脅威	ソフトウェアの更新	ウイルス対策ソフト	パスワードの強化	設定の見直し	手口を知る
1位	標的型攻撃による被害	○	○		○	○
2位	ランサムウェアによる被害	○	○		○	○
3位	ビジネスメール詐欺による被害	○	○	○		○
4位	脆弱性対策情報の公開に伴う悪用増加	○	○			○
5位	脅威に対応するためのセキュリティ人材の不足	—	—	—	—	—
6位	ウェブサービスからの個人情報の窃取	○	○	○	○	○
7位	IoT機器の脆弱性の顕在化	○				○
8位	内部不正による情報漏えい				○	○
9位	サービス妨害攻撃によるサービスの停止				○	○
10位	犯罪のビジネス化 (アンダーグラウンドサービス)	○	○	○	○	○

1 OSやソフトウェアは常に最新の状態にしよう！

2 ウイルス対策ソフトを導入しよう！

3 パスワードを強化しよう！

4 共有設定を見直そう！

5 脅威や攻撃の手口を知ろう！

凡例：○ 対策効果あり、または、部分的に効果あり



セキュリティ対策自己宣言

二つ星

**自社診断を実施し
情報セキュリティ基本方針を公開する**

5分でできる！情報セキュリティ自社診断

- 二つ星を使用するには、まず「**新** 5分でできる！情報セキュリティ自社診断」で自社のセキュリティ状況を把握します
 - **セキュリティ対策に関する25項目**に答えて、自社の問題点を把握します
 - **パンフレットやしおり**を参考にして、不足している対策の導入を検討します
 - 対策を社内で周知するために、「**情報セキュリティハンドブック ひな型**」を活用できます

中小企業・小規模事業者の皆へ

新 5分でできる！
情報セキュリティ自社診断

最新動向への対応、できていますか？

脅威や攻撃の変化 IT環境の変化

クラウド
タブレット
スマートフォン
メール
パスワードリスト攻撃
フィッシング攻撃

かかないことになる前のセキュリティ状況を「5分でできる自社診断シート」でチェック！

5分でできる！自社診断パンフレット

IPA 独立行政法人情報処理推進機構
セキュリティセンター
<http://www.ipa.go.jp/security/>

2017年6月30日 第1版

新

5分 できる！情報セキュリティ自社診断

自社診断シート 25項目

- あまり費用をかけることなく、実行することで効果がある絞り込んだ25項目の情報セキュリティ対策

✓ 基本的対策 5項目

脆弱性対策、ウイルス対策、
パスワード強化など
※情報セキュリティ5か条と同じ

✓ 従業員としての対策 13項目

事務所の安全管理、持ち出し、
廃棄、電子メール、Web利用など

✓ 組織としての対策 7項目

従業員、取引先、ルールなど

新 5分 できる自社診断シート 情報セキュリティ対策の自社診断シート IPA

※診断結果は、診断項目の○を印し、○を印した項目は、○を印してください。
 ※このシートは、診断結果を印刷するためのシートです。印刷結果を印刷してください。
 ※このシートは、診断結果を印刷するためのシートです。印刷結果を印刷してください。
 ※このシートは、診断結果を印刷するためのシートです。印刷結果を印刷してください。

項目番号	項目内容	実施状況	評価	対応	対応期限	対応担当者
1	脆弱性診断を実施しているか。	○	○	○	○	○
2	脆弱性診断の結果を適切に分析しているか。	○	○	○	○	○
3	脆弱性診断の結果を適切に報告しているか。	○	○	○	○	○
4	脆弱性診断の結果を適切に修正しているか。	○	○	○	○	○
5	脆弱性診断の結果を適切に報告しているか。	○	○	○	○	○
6	脆弱性診断の結果を適切に修正しているか。	○	○	○	○	○
7	脆弱性診断の結果を適切に報告しているか。	○	○	○	○	○
8	脆弱性診断の結果を適切に修正しているか。	○	○	○	○	○
9	脆弱性診断の結果を適切に報告しているか。	○	○	○	○	○
10	脆弱性診断の結果を適切に修正しているか。	○	○	○	○	○
11	脆弱性診断の結果を適切に報告しているか。	○	○	○	○	○
12	脆弱性診断の結果を適切に修正しているか。	○	○	○	○	○
13	脆弱性診断の結果を適切に報告しているか。	○	○	○	○	○
14	脆弱性診断の結果を適切に修正しているか。	○	○	○	○	○
15	脆弱性診断の結果を適切に報告しているか。	○	○	○	○	○
16	脆弱性診断の結果を適切に修正しているか。	○	○	○	○	○
17	脆弱性診断の結果を適切に報告しているか。	○	○	○	○	○
18	脆弱性診断の結果を適切に修正しているか。	○	○	○	○	○
19	脆弱性診断の結果を適切に報告しているか。	○	○	○	○	○
20	脆弱性診断の結果を適切に修正しているか。	○	○	○	○	○
21	脆弱性診断の結果を適切に報告しているか。	○	○	○	○	○
22	脆弱性診断の結果を適切に修正しているか。	○	○	○	○	○
23	脆弱性診断の結果を適切に報告しているか。	○	○	○	○	○
24	脆弱性診断の結果を適切に修正しているか。	○	○	○	○	○
25	脆弱性診断の結果を適切に報告しているか。	○	○	○	○	○

※この診断シートは、IPAが作成したものであり、IPAの承認を受けています。
 ※この診断シートは、IPAが作成したものであり、IPAの承認を受けています。

新

5分でできる！情報セキュリティ自社診断

やってみましょう！

新5分でできる！ 情報セキュリティ自社診断 (25のチェック)

- 診断内容を読み、チェック欄に○を付ける
- チェックが終了したら最下段に合計を記入

※以下を利用していない場合は、「実施している」に○を付ける

No. 4 ネットワーク接続の複合機やハードディスク

No. 5 ウェブサービス

No. 9 無線LAN

No.23 クラウドサービス



新

5分 できる！情報セキュリティ自社診断

(参考) SECURITY ACTION実態調査結果

- 自社診断を行ったときに、「25の診断項目」のなかで対策が難しいと感じられた項目



(出典) 東洋経済ONLINE「SECURITY ACTION実態調査結果」
<http://toyokeizai.net/articles/-/209001>

新 **5分** ができる！情報セキュリティ自社診断

対策の決定

- 実施できていなかったり、実施状況にバラツキがある項目は、パンフレット等を参考に、対策を決定します

中小企業・小規模事業者の皆様へ

新 **5分** ができる！
情報セキュリティ自社診断

最新動向への対応、できていますか？

脅威や攻撃の変化 IT環境の変化

クラウド
タブレット
スマートフォン
パソコン/ノートPC
モバイルデバイス

取り逃しのつかないことになる前に
あなたの会社のセキュリティ状況を
「5分で行える自社診断シート」でチェック！

新 **5分** ができる！自社診断パンフレット

「パンフレット」
診断項目解説
対策例紹介

「情報セキュリティ対策のしおり」
詳しく説明

IPA 社団法人 情報処理推進機構
セキュリティセンター

IPA 社団法人 情報処理推進機構
セキュリティセンター

IPA 社団法人 情報処理推進機構
セキュリティセンター

新

5分 できる！情報セキュリティ自社診断

情報セキュリティハンドブックの作成

- 情報セキュリティハンドブック(ひな形)を編集して、対策をルール化します

「情報セキュリティハンドブックひな形」

修正する箇所は赤字
 選択する箇所は青字

情報セキュリティ ハンドブック (ひな形)

ハンドブックの使い方

本ハンドブック(ひな形)は、従業員に配布し、自社の情報セキュリティルールを数値化してわかりやすくまとめたものです。5分でできる！情報セキュリティ自社診断に準拠しています。赤字で記載した箇所は任意で変更しますが、自社のルールにあわせて赤字を中心に修正し、また必要に応じて項目を追加してご利用ください。

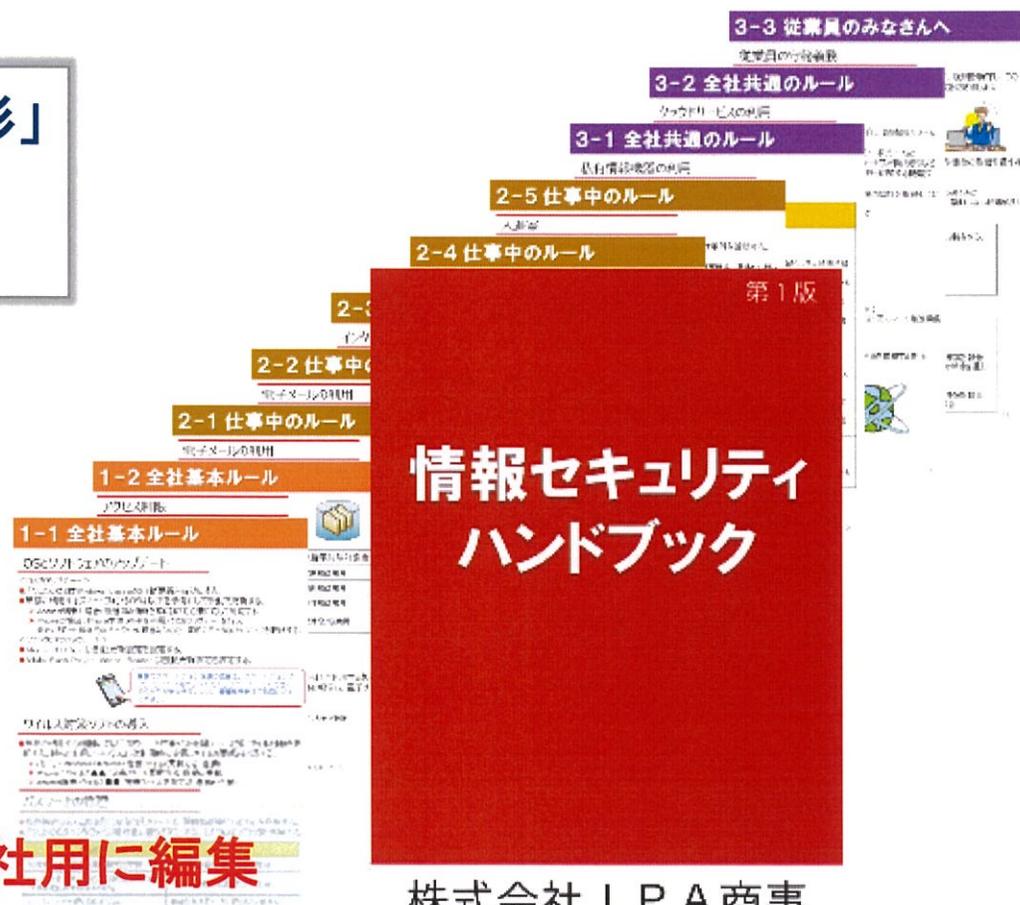
株式会社〇〇〇〇

自社用に編集

情報セキュリティ ハンドブック

第1版

株式会社IPA商事



基本方針の策定・公開

- 「情報セキュリティポリシーサンプル」を参考にするなどして、セキュリティポリシー（基本方針）を策定・公開します

中小企業の情報セキュリティ対策ガイドライン 付録3 <ツールB>

情報セキュリティポリシーサンプル

本ツールは、中小企業向けの情報セキュリティポリシーのサンプルです、をもとに自社に必要なサンプルを選択し、自社で実施する対策に編集が情報セキュリティポリシーを作成することができます。

※赤字箇所は、自社の事情に応じた内容（役職名、担当者名など）に書き換えてください。

※青字箇所は、自社の事情に応じた文言を記載してください。

1	組織的対策（基本方針）	改訂日	20yy.mm.dd
適用範囲 当全体			
1.情報セキュリティ基本方針			
情報セキュリティ基本方針を以下のとおり定める。情報セキュリティ基本方針を当社のホームページで公表する。/情報セキュリティ基本方針を本社各部署に提示し従業員及び関係者に周知する。/情報セキュリティ基本方針を顧客の要請に応じ適宜に公表する。			
<p style="text-align: center;"><情報セキュリティ基本方針サンプル></p> <p>当社は、●●事業を中核としてお客様のニーズに対応してきました。今後も、お客様にご満足いただける製品・サービスを提供するために、高度情報化社会における情報漏えい事故・災害・犯罪などの脅威から守り、お客様ならびに社会の信頼に応えるべく、情報セキュリティ基本方針を定め、当社の情報セキュリティに対する取り組みの指針といたします。</p> <p>1.社内体制および情報セキュリティポリシーの整備 当社は、セキュリティの維持及び改善のために必要な管理体制を確立し、必要な情報セキュリティ対策を社内での正式な規則として定めます。</p> <p>2.リーダーシップにおける責任および継続的改善 当社の経営者は、本方針の遵守により、当社及びお客様の情報セキュリティが適切に管理されるよう主導します。</p> <p>3.法令、契約上の要求事項の遵守 当社の従業員は、事業活動で利用する情報資産に関連する法令、規制、規格及びお客様との契約上のセキュリティ要求事項を遵守します。</p> <p>4.従業員の取組み 当社の従業員は、情報セキュリティの維持及び改善のために必要とされ知識、技術を習得し、情報セキュリティへの取り組みを積極的なものとします。</p> <p>5.違反及び事故への対応 当社は、情報セキュリティに関わる法令、規制、規格及びお客様との契約に関わる違反及び情報セキュリティ事故への対応のための体制を整備し、違反及び事故の影響を低減します。</p> <p style="text-align: right;">○年○月○日 株式会社○○○ 代表取締役社長 ○○○</p>			

目次

1	組織的対策（基本方針）
2	組織的対策
3	人的対策
4	情報資産管理
5	マイナンバー対応
6	アクセス制御及び認証
7	物理的対策
8	IT機器利用
9	IT基礎運用管理
10	システム開発及び保守
11	委託管理
12	情報セキュリティインシデント対応ならびに事業継続管理
13	社内体制
14	委託契約書機密保持条項サンプル

自社用に編集



株式会社IPA商事

製品のサービス Products & Services | モバイル Mobile | 会社情報 Company Information

情報セキュリティ基本方針

個人情報保護の推進について

情報セキュリティ基本方針

当社は、人員構成事業中核としてお客様のニーズに対応してきました。今後も、お客様にご満足いただけるサービスを提供するために、高度情報化社会における情報漏えい事故・災害・犯罪などの脅威から守り、お客様ならびに社会の信頼に応えるべく、情報セキュリティ基本方針を定め、当社の情報セキュリティに対する取り組みの指針といたします。

- 社内体制および情報セキュリティポリシーの整備
当社は、セキュリティの維持及び改善のために必要な管理体制を確立し、必要な情報セキュリティ対策を社内での正式な規則として定めます。
- リーダーシップにおける責任および継続的改善
当社の経営者は、本方針の遵守により、当社及びお客様の情報セキュリティが適切に管理されるよう主導します。
- 法令、契約上の要求事項の遵守
当社の従業員は、事業活動で利用する情報資産に関連する法令、規制、規格及びお客様との契約上のセキュリティ要求事項を遵守します。
- 従業員の取組み
当社の従業員は、情報セキュリティの維持及び改善のために必要とされ知識、技術を習得し、情報セキュリティへの取り組みを積極的なものとします。
- 違反及び事故への対応
当社は、情報セキュリティに関わる法令、規制、規格及びお客様との契約に関わる違反及び情報セキュリティ事故への対応のための体制を整備し、違反及び事故の影響を低減します。

2018年4月1日
株式会社IPA商事
代表取締役社長 田中 一郎

ツールB 情報セキュリティポリシーサンプル

ホームページで公開

情報セキュリティポリシー(基本方針)サンプル

情報セキュリティ基本方針

株式会社〇〇〇〇（以下、当社）は、お客様からお預かりした/当社の/情報資産を事故・災害・犯罪などの脅威から守り、お客様ならびに社会の信頼に応えるべく、以下の方針に基づき全社で情報セキュリティに取り組みます。

1. 経営者の責任

当社は、経営者主導で組織的かつ継続的に情報セキュリティの改善・向上に努めます。

2. 社内体制の整備

当社は、情報セキュリティの維持及び改善のために組織を設置し、情報セキュリティ対策を社内の正式な規則として定めます。

3. 従業員の取組み

当社の従業員は、情報セキュリティのために必要とされる知識、技術を習得し、情報セキュリティへの取り組みを確かなものにします。

4. 法令及び契約上の要求事項の遵守

当社は、情報セキュリティに関わる法令、規制、規範、契約上の義務を遵守するとともに、お客様の期待に応えます。

5. 違反及び事故への対応

当社は、情報セキュリティに関わる法令違反、契約違反及び事故が発生した場合には適切に対処し、再発防止に努めます。

制定日：20〇〇年〇月〇日

株式会社〇〇〇〇

代表取締役社長 〇〇〇〇

社内展開例

- ハンドブックの印刷配付や、社内ポータルに掲示する
- 説明会などを実施して、実践を促す



IP A 対策のしおり : IPA 独立行政法 政 府 情報セキュリティ推進機構 技術本部 セキュリティセンター

最終更新日: 2017年6月30日
独立行政法人情報処理推進機構 技術本部 セキュリティセンター

2017年6月30日

「企業(組織)における最低限の情報セキュリティ対策のしおり」を改訂しました。

本しおりは、情報セキュリティ対策について何をすれば良いかわからないという企業や組織に向けて、まず最低限実施すべき基本的な情報セキュリティ対策25項目について解説したものです。

今回の改訂では、2016年11月に改訂された「[新5分でできる情報セキュリティ自社診断シート](#)」に合わせた内容にしました。また最近の中小企業を取りまくIT環境の変化や、新しい形態のコンピュータウイルスやサイバー攻撃の出現を踏まえて、それらの解説や対策も盛り込みました。

本しおりのPDF版は[こちら](#)からダウンロードできます。

「IPA対策のしおりシリーズ」は、一般のご家庭や企業・組織の方々を対象に、情報セキュリティ上の様々な脅威への対策をテーマ別に分かりやすく説明した小冊子シリーズです。これらの脅威への対策を実践するために、ぜひご活用ください。なお、営利を目的としない用途に限り、原本のまま印刷し、配布することに関して、制限はございません。

IPA対策のしおりシリーズ

1		ウィルス対策のしおり (第10版) (815KB) ～コンピュータウイルスからあなたのパソコンを守るには!!～ (注1)	[英語版] ↓ (1.6MB)
2		スパイウェア対策のしおり (第10版) (822KB) ～気付かぬうちにスパイウェアに侵入されていませんか?～ (注1)	[英語版] ↓ (4.4MB)
		ボット対策のしおり (第10版) (1.0MB) あなたのパソコンはボットに感染していませんか?～(注1)	[英語版] ↓ (2.1MB)

<https://www.ipa.go.jp/security/keihatsu/redirect-munekyun-pw.html>

17:02 2019/03/21

<https://www.ipa.go.jp/security/antivirus/shiori.html>

3.情報セキュリティ知識(中級編)

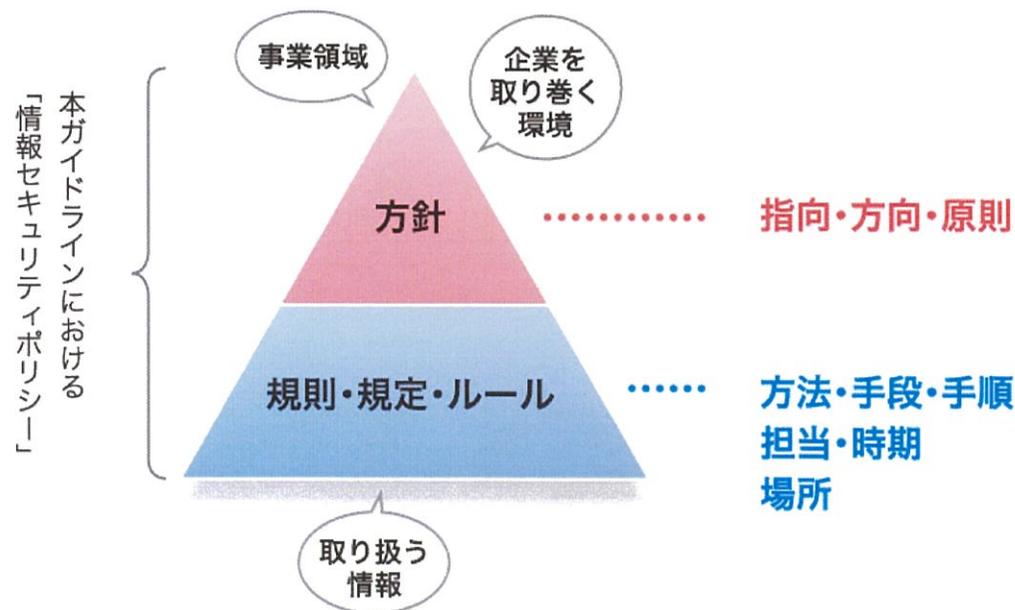
さらなる取組み

情報セキュリティポリシーの策定

基本的な考え方(1/2)

- 自社に適合したポリシーを策定

- 企業が直面するリスクは、事業領域や取り扱う情報、企業を取り巻く環境によっても異なるため、ポリシーのサンプルを入手して社名を変えるだけではうまく機能しない
- 本ガイドラインでは、対策基準と実施手順を1階層に簡素化したポリシーの策定について説明



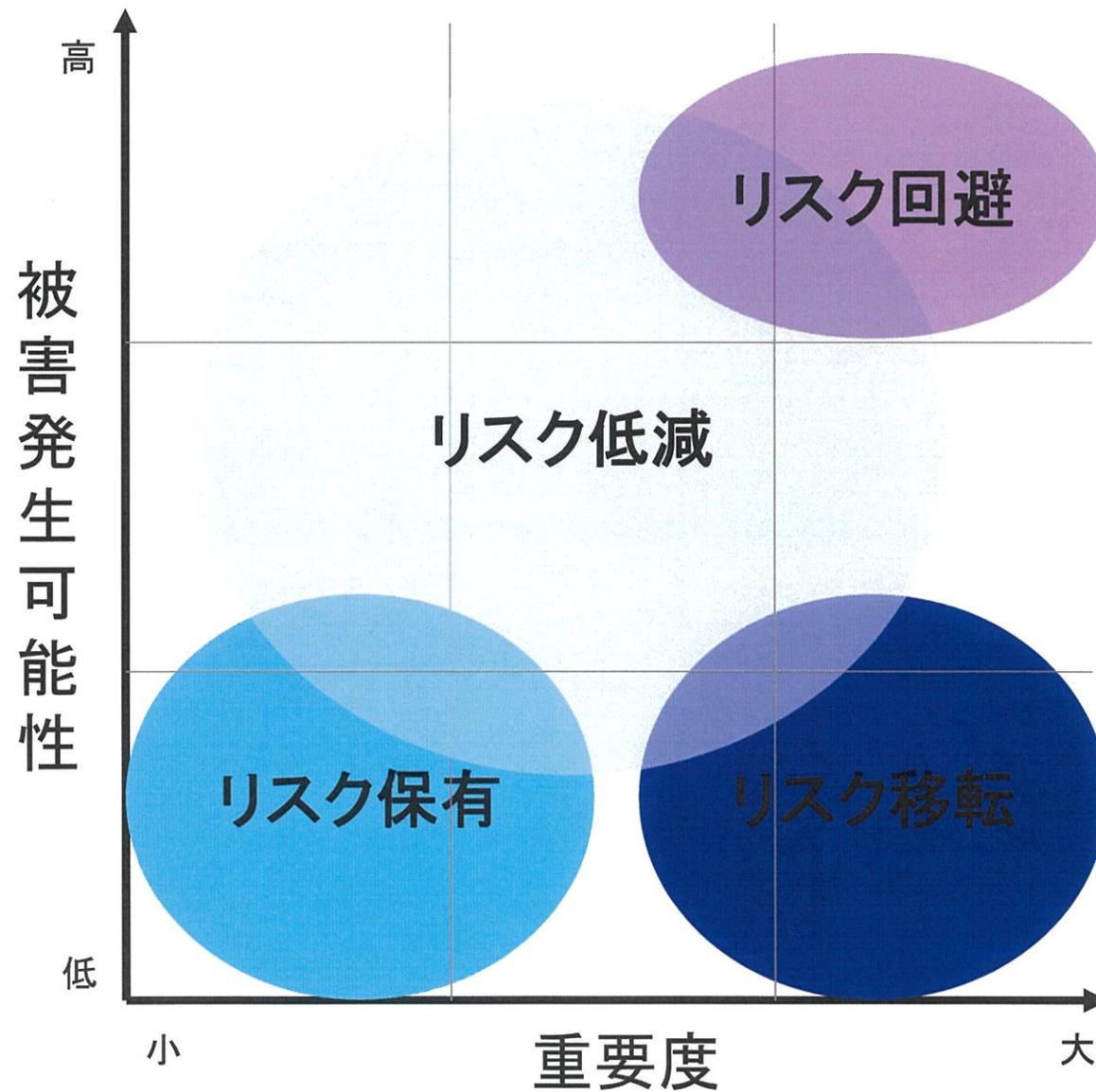
情報セキュリティポリシーの策定

基本的な考え方(2/2)

- リスクの大きなものから重点的に対策を実施
 - 限られた予算を有効に使うには、あらかじめリスク分析を行い、いつ事故が起きてもおかしくない、あるいは事故が起きると大きな被害になるなど、リスクが大きなものから重点的に対策を定める

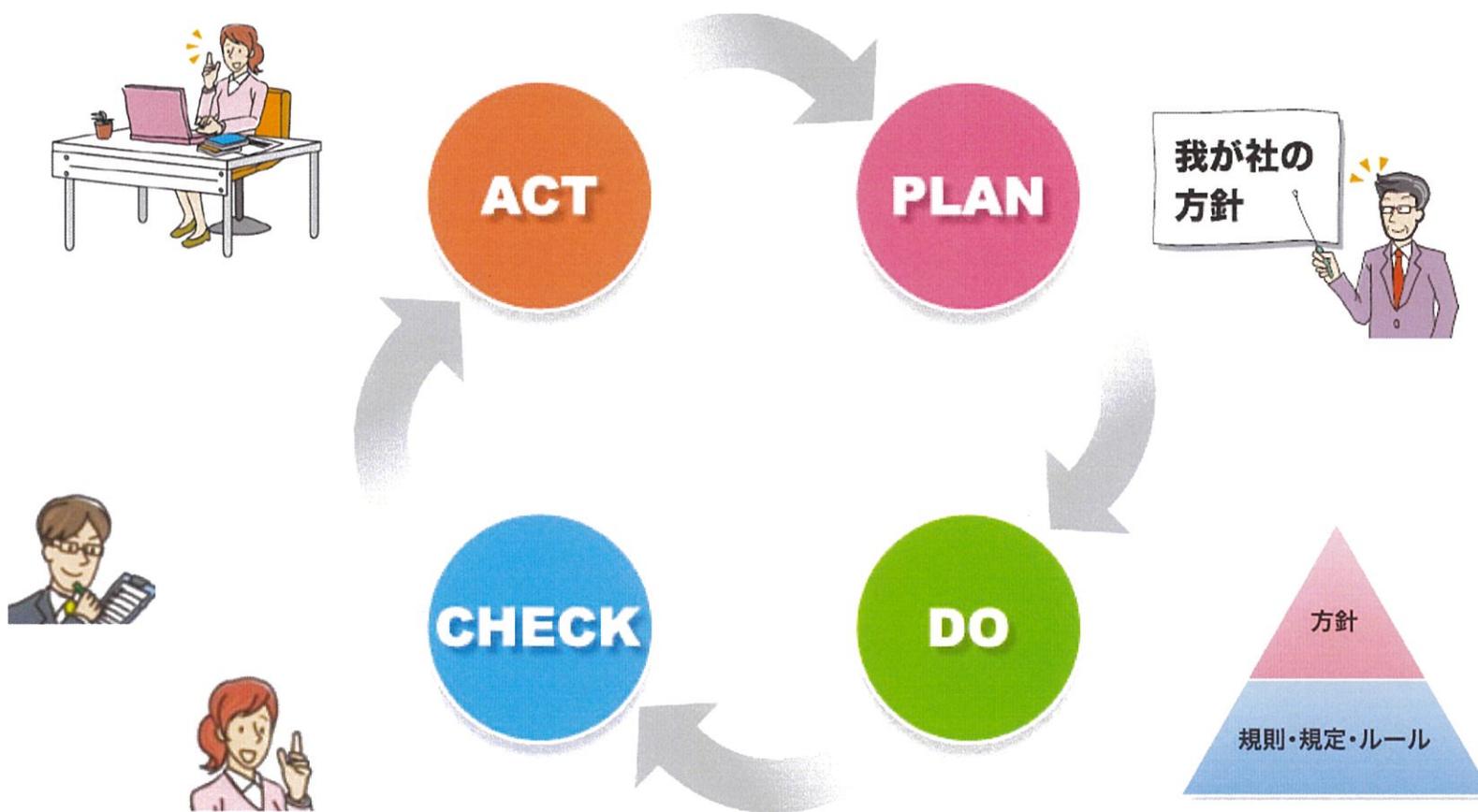


(参考)リスクへの対応



情報セキュリティ対策のさらなる改善に向けて

- Plan(計画)、Do(実行)、Check(チェック)、Act(改善)の4段階の活動により継続的に改善しましょう



自己宣言(一つ星)の案内

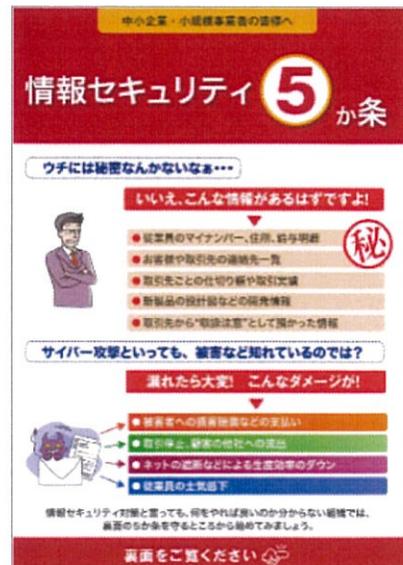


• SECURITY ACTION制度紹介

- 取組み目標
- ロゴマークの申込手順
- 自己宣言のメリット



• 基本的対策を確認



①OSやソフトウェアは常に最新の状態にしよう!

②ウイルス対策ソフトを導入しよう!

③パスワードを強化しよう!

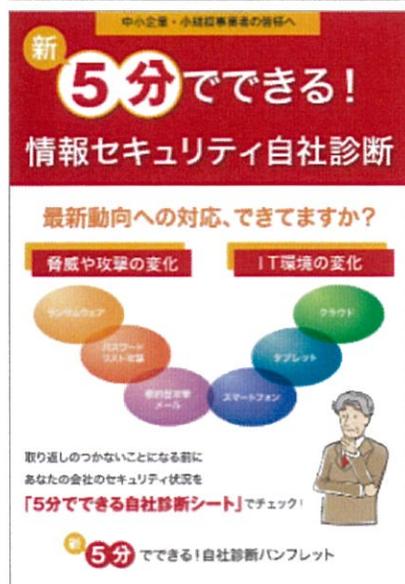
④共有設定を見直そう!

⑤脅威や攻撃の手口を知ろう!



● SECURITY ACTION制度紹介

- 取り組み目標
- ログマークの申込手順
- 自己宣言のメリット



● セキュリティ状況を把握

- 基本的対策 5項目
- 従業員としての対策 13項目
- 組織としての対策 7項目



● 基本方針の策定支援



セキュリティ対策自己宣言



IT導入補助金2022

令和元年度補正 サービス等生産性向上IT導入支援事業
令和3年度補正 サービス等生産性向上IT導入支援事業

補助金シミュレーター 資料ダウンロード お問い合わせ・相談窓口 よくあるご質問 Facebook 中小機構

セキュリティ対策推進枠
について

デジタル化基盤導入枠
(施設付導入型)について

gBizID

過去5か年のサービス等
生産性向上IT導入支援事業について

IT事業者
ポータル

申請
マイページ

IT導入補助金 について	事業概要	スケジュール	申請・手続き フロー	中小企業・ 小規模事業者の みなさま	ITベンダー・ サービス事業者の みなさま	関連資料・動画等	目的から探す
-----------------	------	--------	---------------	--------------------------	-----------------------------	----------	--------



中小企業・小規模事業者等のみなさまへ

セキュリティ対策推進枠の 申請受付を開始しました

詳細はこちら

詳細はこちら

IT導入支

IT導入支援事業
斡旋するという、
コールセンター
公募のスケジュー



IT導入支援事業者を結った
悪質な事業者にご注意ください



【交付申請_セキュリティアクションアカウントID入力画面のシステムメンテナンスのお知らせ】 8:00更新

これから申請をされる皆様へ：補助金の不正受給に関する注意喚起

※重要※ IT導入支援事業者を結った悪質な事業者にご注意ください

G BizIDの事前取得について

中小企業・小規模事業者のみなさま向け

新着情報

2022.10.6 【5次締切分 通常枠 (A・B類型)】 【1次締切分セキュリティ対策推進枠】 【10次締切分 デジタル化基盤導入枠 (デジタル化基盤導入型)】 交付決定事業者一覧を公開しました。一覧は、「交付決定事業者一覧」ページをご確認ください

2022.10.3 通常枠 (A・B類型) 6次締切分、セキュリティ対策推進枠2次締切分、デジタル化基盤導

更新情報

2022.10.7 「IT導入補助金2022 公募要領 通常枠 (A・B類型) 版」「IT導入補助金2022 公募要領 セキュリティ対策推進枠版」「IT導入補助金2022 公募要領 デジタル化基盤導入枠 (デジタル化基盤導入型) 版」を更新しました。

2022.10.6 「IT導入支援事業者一覧」を更新しました。

事業の目的

中小企業・小規模事業者等のみなさまがサイバーインシデントが原因で事業継続が困難となる事態を回避するとともに、サイバー攻撃被害が供給制約や価格高騰を潜在的に引き起こすリスクや生産性向上を阻害するリスクを低減していただく事を目的としています。

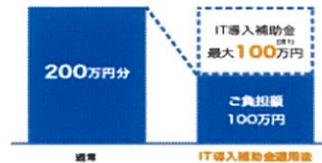
概要

POINT
1

サービス利用料の1/2以内、
最大100万円を補助

POINT
2

サービス利用料
最大2年分補助



最大**2年分**の補助！
¥ ¥

POINT
3

補助対象を「サイバーセキュリティ
お助け隊サービス」に特化

POINT
4

独立行政法人情報処理推進機構が
登録・公表するサービス



補助対象について

セキュリティ対策推進枠

セキュリティ対策推進枠	
補助額	5万～100万円
補助率	1/2以内
機能要件	独立行政法人情報処理推進機構が公表する「サイバーセキュリティお助け隊サービスリスト」に掲載されているいずれかのサービス
補助対象	サービス利用料（最大2年分）



IT導入補助金2022 交付規程 セキュリティ対策推進枠版
更新日：2022年7月25日



IT導入補助金2022 公募要領 セキュリティ対策推進枠版
更新日：2022年10月7日



セキュリティ対策推進枠

交付申請期間		2022年8月9日（火）受付開始～終了時期は後日案内予定	
1次締切分	締切日	9月5日（月）17：00	
2次締切分	締切日	10月3日（月）17：00	
3次締切分	締切日	10月31日（月）17：00（予定）	
4次締切分	締切日	11月28日（月）17：00（予定）	

セキュリティ対策のための制度・ツール

「サイバーセキュリティお助け隊サービス」制度



「サイバーセキュリティお助け隊サービス」制度とは、中小企業に対するサイバー攻撃への対処に不可欠なワンパッケージのサービスを要件としてまとめ、これを満たすことが所定の審査機関により確認された民間サービスを、IPAが登録・公表する制度です。

「見守り」「駆付け」「保険」など中小企業のセキュリティ対策に不可欠なサービスをワンパッケージで安価に提供

見守り

(異常の監視)
24時間 365日監視
挙動や問題のある攻撃を検知し
あなたのPCとネットワークを守ります。

駆付け

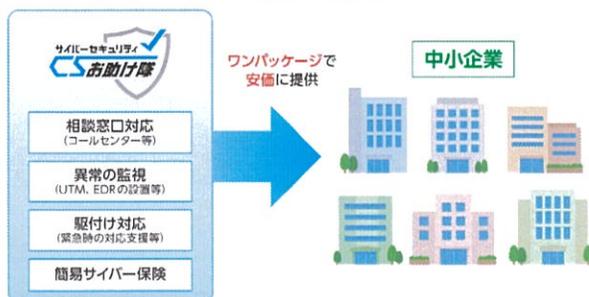
問題が発生したときに、
地域のIT事業者等が
駆付け対応します。
(リモート支援の場合あり)

保険

簡易サイバー保険で、
駆付け支援等インシデント対応時に
突発的に発生する各種コストが
補償されます。

サイバーセキュリティお助け隊サービスの活用をご検討ください！

サイバーセキュリティ
お助け隊サービスのイメージ



サイバーセキュリティお助け隊サービス
<https://www.ipa.go.jp/security/otasuketai-pr/>

サイバーセキュリティ対策 かた

日常の業務に潜むリスク
をかたで紹介
対策のヒントにも役立ち
ます



サイバーセキュリティ お助け隊サービス THE MOVIE

サイバーセキュリティお助け隊サービス
についてラップ調のMOVIEでご紹介



経済産業省施策紹介

ものづくり補助金のデジタル枠の創設

DX(デジタルトランスフォーメーション)に資する革新的な製品・サービスの開発や、デジタル技術を活用した生産プロセス・サービス提供方法の改善等を行う事業者を対象に、補助率を2/3に引き上げた新たな申請類型が創設されました。

ものづくり補助金総合サイト

<https://portal.monodukuri-hojo.jp/>



IT導入補助金 2022

中小企業・小規模事業者のみならずITツール導入に活用いただける補助金です。

会計ソフト、受発注システム、決済ソフト等の導入について補助率を最大3/4に引き上げ、クラウド利用料を2年分まとめて補助するとともに、PC・タブレット、レジ等の購入費を補助対象に追加しました。(補助金申請にあたって、SECURITY ACTIONの取得が要件となっています。)

IT導入補助金について

<https://www.it-hojo.jp/>



事業継続力強化計画認定制度

中小企業が策定した防災・減災の事前対策に関する計画を、経済産業大臣が「事業継続力強化計画」として認定する制度です。

認定を受けた中小企業は、**税制措置や金融支援、補助金の加算などの支援策**が受けられます。

自然災害リスク(地震、洪水等)のほか、**サイバー攻撃、感染症**その他自然災害以外のリスクも支援対象です。

事業継続力強化計画

<https://www.chusho.meti.go.jp/keiei/antei/bousai/keizokuryoku.htm#gaiyou>



情報セキュリティ対策支援サイト

<https://security-shien.ipa.go.jp/>

The screenshot shows the homepage of the Information Security Countermeasure Support Site. At the top, there is a navigation bar with the site's name and logo on the left, and utility links for '文字サイズ' (Text Size), '標準' (Default), '大きく' (Large), 'ログイン' (Login), '利用者登録' (User Registration), and 'お問い合わせ' (Contact Us) on the right. Below the navigation bar is a horizontal menu with tabs for 'このサイトについて' (About this site), 'サービス一覧' (Service List), and 'セキュリティプレゼンター支援' (Security Presenter Support). Under 'このサイトについて', there are sub-tabs for '経営者の方' (For Business Owners), '対策実践者の方' (For Countermeasure Practitioners), '従業員の方' (For Employees), '啓発者/教職員の方' (For Promoters/Teachers), and '一般/学生の方' (For General/Students).

The main content area is titled 'このサイトについて' (About this site) and contains three search buttons: 'セキュリティの専門家を探す' (Find security experts), 'SECURITY ACTION 自己宣言事業者を探す' (Find SECURITY ACTION self-declaration businesses), and 'セキュリティ対策に関する資料・ツールを探す' (Find materials and tools related to security countermeasures).

Below this is a section titled 'このサイトでできること' (What you can do on this site). It explains that the site supports various roles (business owners, practitioners, employees, promoters/teachers, general/public) in advancing their security countermeasures. It encourages users to select a role from the tabs and start their countermeasures.

The page is divided into five main activity sections:

- 知りたい (I want to know):** Features '情報セキュリティ診断' (Information Security Audit). It includes a sub-section with a ruler icon and text: '《入門編》5分でできる！情報セキュリティ自社診断', '《基本編》情報セキュリティ対策ベンチマーク', '《応用編》情報セキュリティ対策ベンチマークPLUS', and 'サイバーセキュリティ経営可視化ツール'. The description states that users can grasp their company's security status by answering questions, and after the audit, they can confirm recommended materials and countermeasures. It also mentions that users can save their audit results and compare them with other companies.
- 学びたい (I want to learn):** Features '5分でできる！ポイント学習' (5-minute learning!). It includes a sub-section with a pencil icon and text: '自社診断の質問を1テーマ5分で学べる'. The description explains that users can learn about information security through e-learning, with a focus on practical examples and correct response methods. It also notes that users can pause and resume their learning and check their progress.
- 始めたい (I want to start):** Features 'SECURITY ACTION自己宣言者サイト' (SECURITY ACTION self-declaration site). It includes a sub-section with a megaphone icon and text: '情報セキュリティ対策の取り組みを外部にアピールしよう'. The description states that the site supports businesses in taking security countermeasures and making self-declarations. It also provides a search function for SECURITY ACTION self-declaration businesses.
- 続けたい (I want to continue):** This section is currently empty.

At the bottom of the page, there are three search buttons: '情報セキュリティに関する資料の検索' (Search for materials related to information security), 'セキュリティ専門家の検索' (Search for security experts), and 'セキュリティ専門家のセミナー開催情報' (Information on seminars for security experts).

5分でできる！自社診断 オンライン版

- 中小企業でも実施が望まれる基本的な情報セキュリティ対策の実施状況を診断できる無料のツール
- 25の質問に答えるだけで診断でき、過去の診断結果や同業他社との比較もできます

自社診断

5分でできる自社診断シート

Part 1 基本的対策

1-1 Windows update (マイクロソフトが提供するソフトウェアのバグ修正や脆弱性の修正プログラム) を実行していますか？

実施している 一部実施している 実施していません わからない

1-2 ネットワークにインターネットを介してアクセス可能なサーバー (ウェブサーバーやデータベースサーバー、メールサーバー、ファイルサーバー) がありますか？ (※インターネットに接続可能なサーバーは、必ずしもインターネットに接続しているとは限りません)

実施している 一部実施している 実施していません わからない

1-3 ネットワークは自分の名前、住所番号、誕生日が簡単にわかるような公開情報サービスに登録していませんか？ (※自分の名前、住所番号、誕生日がわかるような公開情報サービスとは、例えば、マイページ、マイページ、マイページなどです)

実施している 一部実施している 実施していません わからない

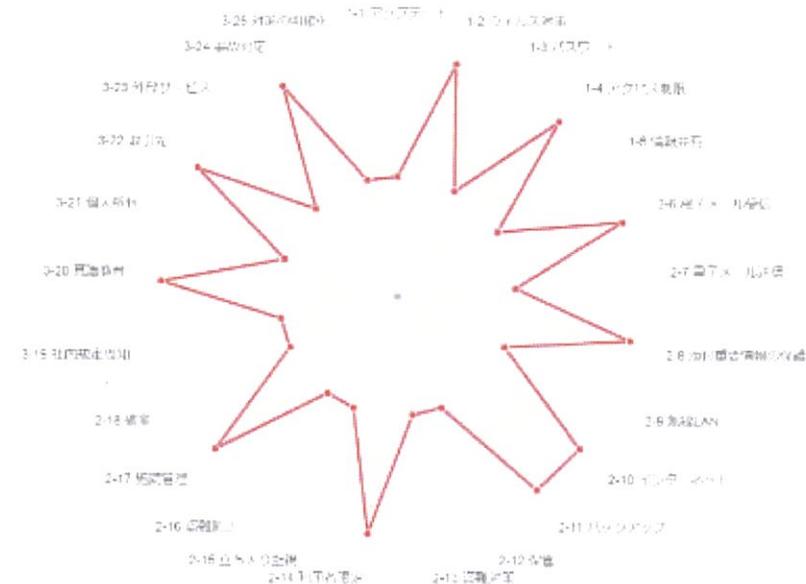
1-4 ネットワーク上の機器の稼働がインターネット上の機器に接続されているかどうか、その稼働状況を確認していますか？

実施している 一部実施している 実施していません わからない

1-5 利用するウェブサイトに、インターネット上のサーバー (ウェブサーバー) を利用して、ウェブページ、コンテンツなどをインターネット経由で提供しているかどうか (※ウェブサーバーが提供しているウェブページやコンテンツは、必ずしもインターネット上で公開されているとは限りません)

実施している 一部実施している 実施していません わからない

今回



Information-technology Promotion Agency [JP] | https://security-shien.ipa.go.jp/selfcheck/sheet1/question/

情報セキュリティ対策
支援サイト

TOP > 自社診断

自社診断

5分でできる自社診断シート

① 診断の前にお読みください。

- 診断内容に記載されている対策例以外の何らかの方法で対策を実施している場合は、「実施している」または「一部実施している」を選択してください。
- 診断内容を読み、回答欄から該当するもの1つを選択してください。
- 「実施している」はすべての社員が実施している場合に選んでください。
- 経営者または管理者の方がご回答ください。

Part 1 基本的対策

1-1 Windows Update (マイクロソフト社が提供しているウィンドウズパソコンの不具合を修正するプログラム) を行うなどのように、常にOSやソフトウェアを安全な状態にしていますか？

実施している 一部実施している 実施していない わからない

1-2 パソコンにはウイルス対策ソフトを入れてウイルス定義ファイル (コンピュータウイルスを検出するためのデータベースファイル「パターンファイル」とも呼ばれる) を自動更新するなどのように、パソコンをウイルスから守るための対策を行っていますか？

実施している 一部実施している 実施していない わからない

1-3 パスワードは自分の名前、電話番号、誕生日など推測されやすいものを選んで複数のウェブサイトで使いまわしをしないなどのように、強固なパスワードを設定していますか？

実施している 一部実施している 実施していない わからない

1-4 ネットワーク接続の複合機やハードディスクの共有設定を必要な人だけに限定するなどのように、重要情報に対する適切なアクセス制限

18:08
2018/09/13

診断結果

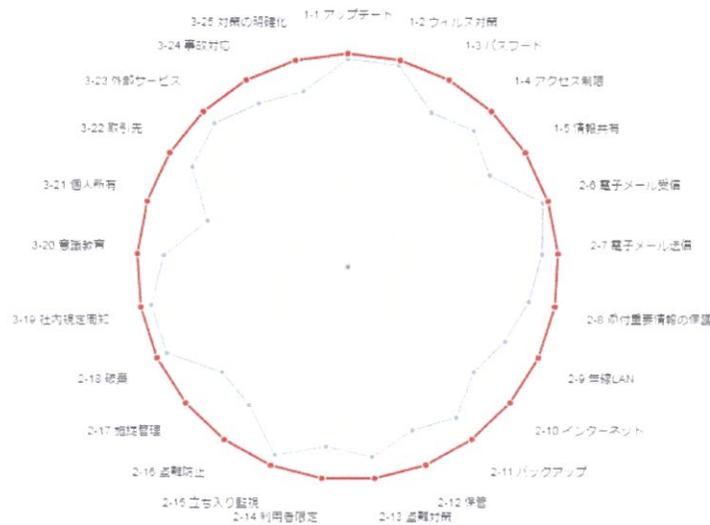
i 診断が完了しました。診断結果をご確認ください。

過去との比較 **同業種平均と比較** 全企業平均と比較

レーダーチャート説明
 企業プロフィールの「業種」ごとに出した平均値との比較です。

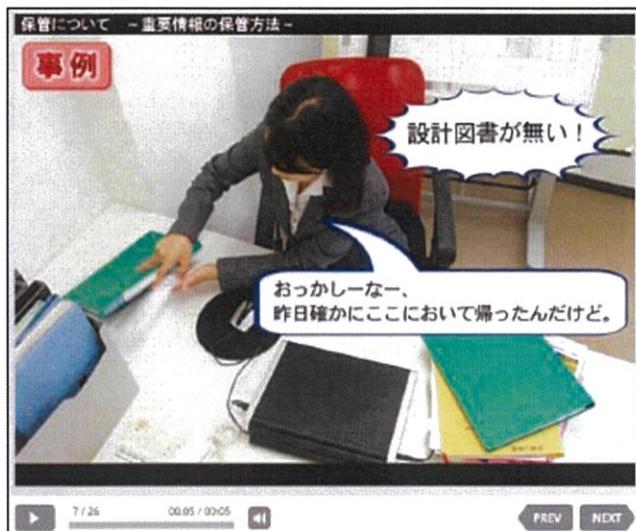
金融業, 保険業

■ 今回 ■ 業種平均



5分でできる！ポイント学習

- 職場での日常のひとコマを取り入れた親しみやすいシナリオ仕立てで、セキュリティに関する様々な事例を疑似体験しながら正しい対処法を1テーマ5分で学ぶことができます
- 学習テーマは自社診断の25の質問と連動しています



A01保管について ～重要情報の保管方法～

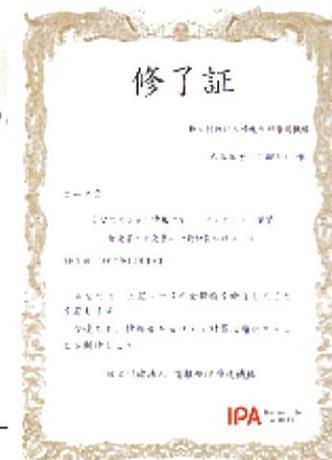
確認テスト 100点

Q1 正解

重要書類の保管方法として不適切なのはどれでしょう。

正答 回答 選択肢

- 机の上に書類を放置しない
- 机の隅にきれいに重ねておく
- 書類の性質や内容を明確にする
- 鍵付き書庫を利用する



修了証も発行できます

セキュリティプレゼンター 検索サービス

- セキュリティプレゼンターは、IPAの情報セキュリティ啓発コンテンツを使用して、中小企業等に向けて情報セキュリティの普及活動をしている方々です
- 活動地域や保有資格などを条件にセキュリティプレゼンターを検索することができます

セキュリティプレゼンター詳細

ログイン

ログインID

パスワード

ログイン

パスワードを忘れた方はこちら

アカウントを申請したい方

セキュリティプレゼンター登録申請

セキュリティプレゼンターのご紹介

メニュー

訂書情報

姓	相戸	名	真子
姓(フリガナ)	アイビー	名(フリガナ)	ニイ
プレゼンター名			
活動地域	東京都 埼玉県 神奈川県 千葉県		
生年月			
メールアドレス	ipa@pa.go.jp		
郵便番号	113-0561		
郵便名	東京都		
〒区町村/〒地	東京都本郷3-20-8		
ビル名など	文京グリーンコートセンターオフィス		

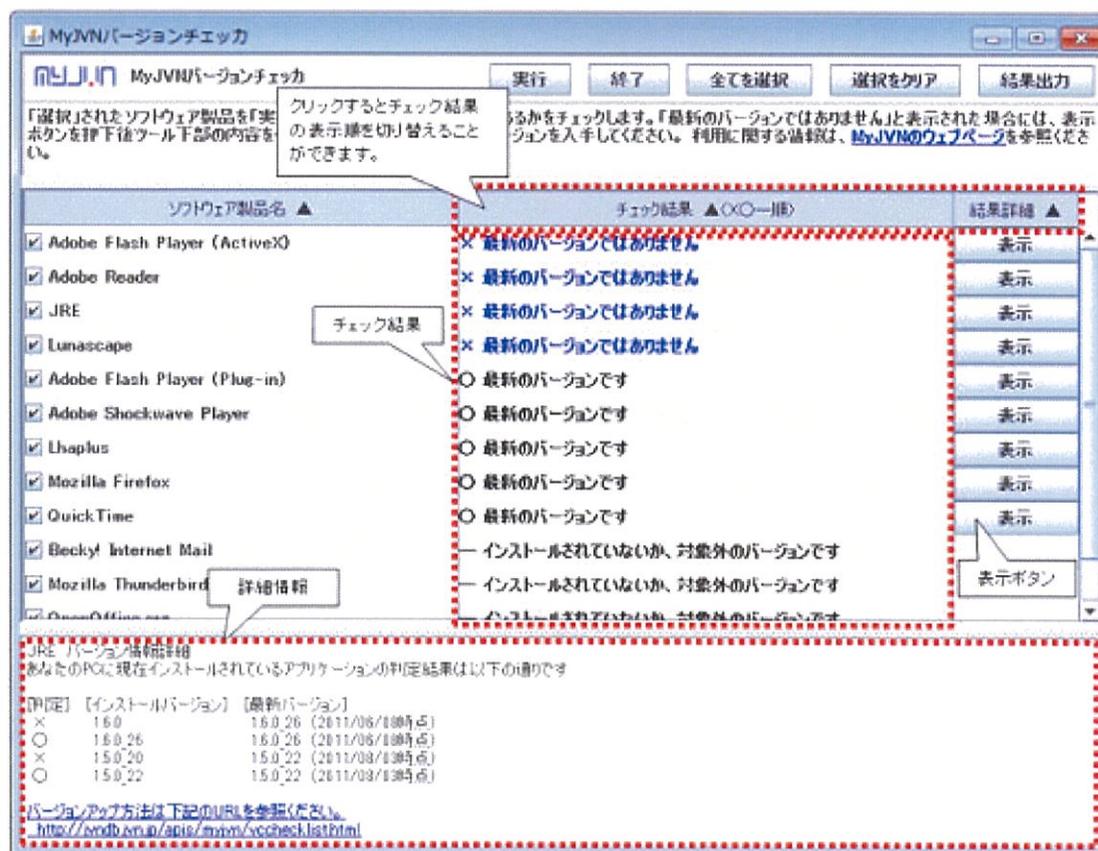
所属情報-1	
所属組織名	株式会社安全支援
所属組織名(カナ)	カブシキガイシャアンゼンシユン
部署	情報セキュリティ支援部
役職	情報セキュリティコンサルタント
所属先電話番号	03-5978-7508
所属先住所	東京都文京区本郷3-20-8
所属先メールアドレス	ipa@pa.go.jp

主要取得資格	情報セキュリティスペシャリスト試験 ITコーディネータ
その他取得資格	情報処理安全確保支援士、システム監査技術者、公認情報システム監査人 (CISA)、ISMS審査員、QMS審査員、ITコーディネータ、知的財産管理技能士
自己PR	情報セキュリティ関連に関する支援、監査等を中心として活動しています。
受講終了確認	5分で出来る！情報セキュリティ員社診断 5分で出来る！情報セキュリティポイント学習

MyJVNバージョンチェッカ

<https://jvndb.jvn.jp/apis/myjvn/>

- Windows PCによくインストールされているソフトウェア製品のバージョンが最新であるかを簡単な操作で確認する無償ツール



IPAメールニュース & SNS公式アカウント

- IPAから情報セキュリティ対策やソフトウェアの脆弱性など各種最新情報を発信



IPAメールニュース IPA Better Life with IT
SNS公式アカウントのご案内

🔒 情報セキュリティ 🔄 ソフトウェアの高度進化 👤 IT人材育成

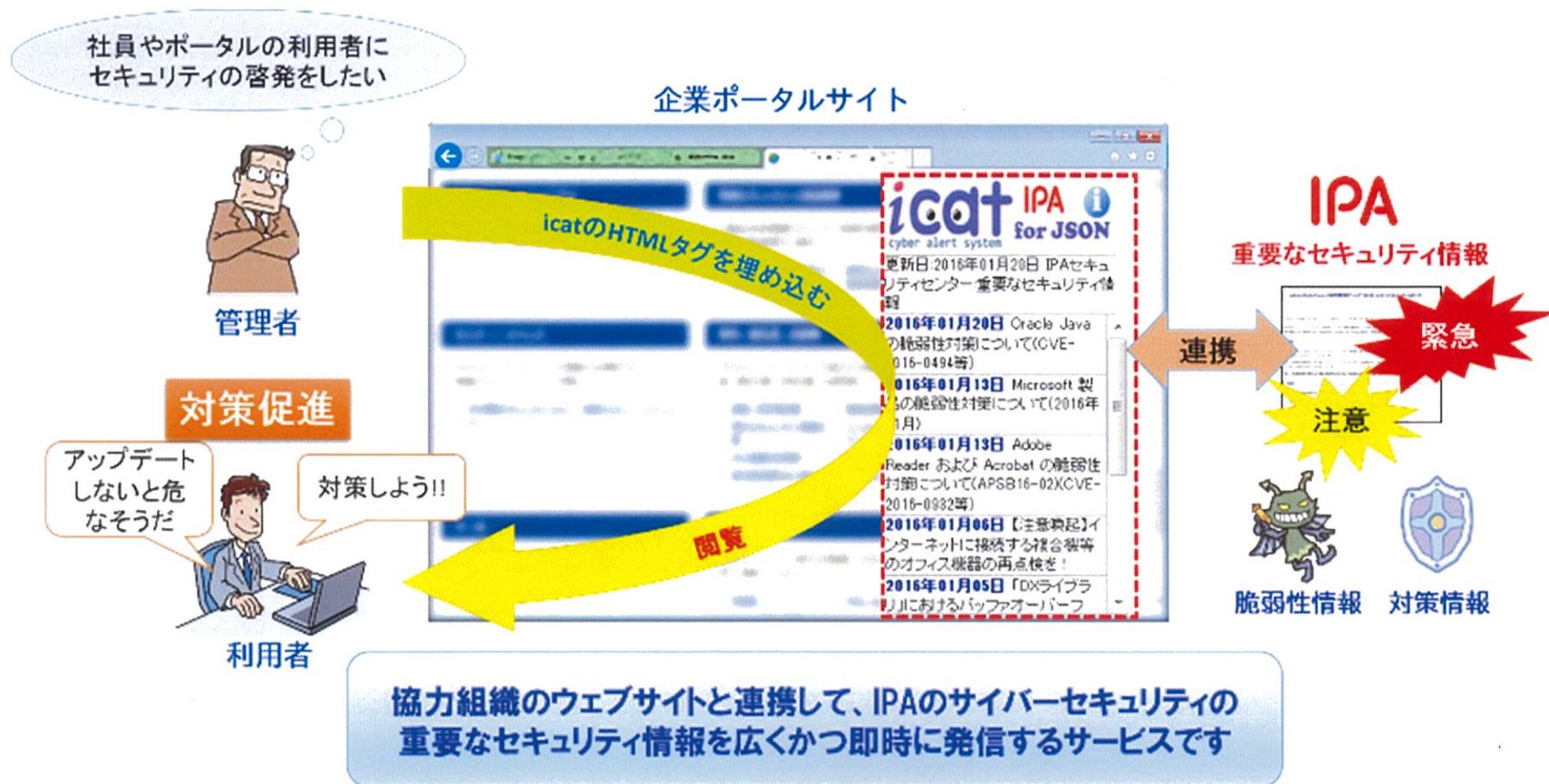
- メールニュース**
IPAの公開・入札情報、セキュリティ関連情報、イベント・セミナーの開催情報や情報処理技術者試験に関する情報をメール配信しています。
メールニュースご登録
<http://www.ipa.go.jp/infobase/Email/index.html> IPA メールニュース
- Twitter**
IPAの各種情報を発信する公式アカウントです。このほか、各専門分野の最新情報を発信するアカウントも取り上げます！ 詳細は画像をご覧ください。
IPA
@IPAjp
<https://twitter.com/IPAjp> IPA Twitter
- Facebook**
IPAのイベント情報や情報セキュリティ関連などの最新情報を発信するIPA公式アカウントです。
IPA
独立行政法人情報処理推進機構
<http://www.facebook.com/ipa.jp/> IPA Facebook
- YouTube**
情報セキュリティソフトウェア開発関連など、研修や個人学習に最適な映像コンテンツを見ることが出来ます！
IPA Channel
<http://www.youtube.com/ipa.jp> IPA Channel
- IPA NEWS**
IPAが毎月発行している広報紙。IPAの活動内容をわかりやすくご紹介しています。紙版やご自宅にも郵送でお届けします！
IPA NEWS
http://www.ipa.go.jp/kan/jac/jac_news/index.html IPA NEWS

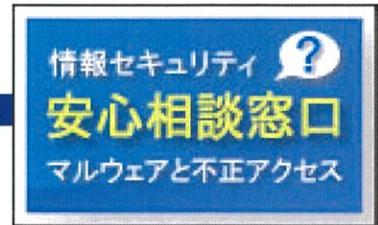
独立行政法人情報処理推進機構 (IPA) <http://www.ipa.go.jp/>

サイバーセキュリティ注意喚起サービス icat for JSON

<https://www.ipa.go.jp/security/vuln/icat.html>

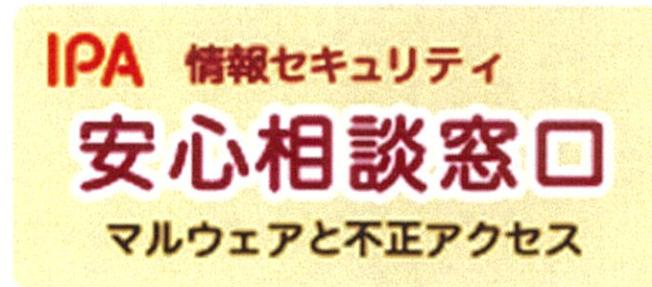
- 「重要なセキュリティ情報」をリアルタイムに配信するサイバーセキュリティ注意喚起サービス





<https://www.ipa.go.jp/security/anshin/>

ウイルスおよび不正アクセスに関する技術的な相談を受け付ける窓口



電話	03-5978-7509 (オペレータ対応は、平日10:00~12:00 および 13:30~17:00)
E-mail	anshin@ipa.go.jp ※このメールアドレスに特定電子メールを送信しないでください。
FAX	03-5978-7518
郵送	〒113-6591 東京都文京区本駒込2-28-8 文京グリーンコート センターオフィス16階 IPAセキュリティセンター 安心相談窓口
URL	https://www.ipa.go.jp/security/anshin/

情報セキュリティ

情報セキュリティ安心相談窓口



「情報セキュリティ安心相談窓口」は、IPAが国民に向けて開設している、一般的な情報セキュリティ（主にウイルスや不正アクセス）に関する技術的な相談に対してアドバイスを提供する窓口です。

▼ 安心相談窓口で承れない相談の例はこちら ▼

	2015年	2016年	2017年	2018年	2019年	2020年	2021年
実際に相談員が対応した件数	6,904	8,961	7,600	8,000	8,031	9,698	6,403

「情報セキュリティ安心相談窓口」の公式SNSアカウントを開設中です。ぜひフォローをお願いします！（情報発信専用のアカウント）



はじめよう、情報セキュリティ対策

【ほぼ15秒アニメ】
子ブタと学ぼう！情報セキュリティ対策のキホン

安心相談窓口ナビゲーション

1. よくあるご相談



安心相談窓口によく寄せられるご相談内容をピックアップして、その中で多くいただいた質問にQ&A形式で回答しています。
まずはこちらで、ご自分が遭遇した被害・手口が掲載されているかご確認ください。

2. 役立つコンテンツ



「1. よくあるご相談」の中にご自分が遭遇している被害についての情報が無ければ、安心相談窓口が公開している「安心相談窓口たより」をご確認ください。
また、被害に遭った際だけでなく普段のパソコン操作にも役立つ資料を紹介しています。

- 2-1. 情報セキュリティ対策
- 2-2. 安心相談窓口たより
- 2-3. ランサムウェア対策特集ページ
- 2-4. 不正ログイン対策特集ページ
- 2-5. 手口検証動画シリーズ
- 2-6. 役立つパソコンの基本操作

情報セキュリティ

脆弱性対策情報

届出・相談・情報提供

ウイルス・不正アクセスの届出

4-3. 安心相談窓口で承れない相談の例

直接当機構へ来訪してのご相談（面談）や下記のようなご相談は承っておりませんので、ご了承ください。

法的解釈に関する相談

電磁波や電波に関する不安・苦情

インターネットサービスの品質や役務不履行に関する相談

契約・支払い方法に関する相談

個別の依頼に基づく端末やログの調査、その他調査行為全般の依頼

特定の製品やサービスの紹介またはそれらに対する良否の質問

他組織への連絡や通報などの仲介

犯罪者の検挙、事件捜査の要望

パソコンやスマホの基本操作や手順等の案内

IPAでは承れないご相談でも他の機関が開設している窓口で対応できる場合もあります。下のリンクバナーより各相談窓口の連絡先を参照することができます。

» 他の機関が開設している窓口はこちら

ご相談いただいた情報については、国内の被害防止策の啓発を目的とし、相談者が特定されない形で、事例情報として公表させていただきます場合があります。

情報セキュリティ

他の機関が開設している相談窓口等

安心相談窓口では対応できない内容でも、他の機関が開設している窓口において対応できることもあります。相談したい内容によって、下記の窓口への問い合わせも検討願います。

サービス提供または購入などの契約に関するトラブルで困っている場合

[消費者ホットライン（消費者庁）](#) [E](https://www.caa.go.jp/policies/policy/local_cooperation/local_consumer_administration/hotline/)
https://www.caa.go.jp/policies/policy/local_cooperation/local_consumer_administration/hotline/

[国民生活センター](#) [E](http://www.kokusen.go.jp/)
<http://www.kokusen.go.jp/>

犯罪行為に関する被害届や捜査について相談をしたい場合

[郵道府県警察本部のサイバー犯罪相談窓口等一覧](#) [E](https://www.npa.go.jp/cyber/soudan.htm)
<https://www.npa.go.jp/cyber/soudan.htm>

法的トラブルの相談をしたい場合

[日本司法支援センター法テラス](#) [E](https://www.houterasu.or.jp/)
<https://www.houterasu.or.jp/>

インターネット上での違法・有害情報に関し相談したい場合

[違法・有害情報相談センター](#) [E](http://www.ihaho.jp/)
<http://www.ihaho.jp/>

[一般社団法人 コンピュータソフトウェア著作権協会不正コピー情報受付](#) [E](https://www2.accs.jp.or.jp/piracy/)
<https://www2.accs.jp.or.jp/piracy/>

インターネット上の違法情報を通報したい場合

[インターネット・ホットラインセンター](#) [E](http://www.internethotline.jp/)
<http://www.internethotline.jp/>

迷惑メールの受信に関して困っている場合

[一般財団法人 日本データ通信協会迷惑メール相談センター](#) [E](https://www.dekya.or.jp/soudan/index.html)
<https://www.dekya.or.jp/soudan/index.html>

フィッシングサイトの発見または被害に関して困っている場合

[フィッシング対策協議会](#) [E](https://www.antiphishing.jp/registration.html)
<https://www.antiphishing.jp/registration.html>

[警察庁 フィッシング110番](#) [E](https://www.npa.go.jp/cyber/policy/phishing/phishing110.htm)
<https://www.npa.go.jp/cyber/policy/phishing/phishing110.htm>

インターネットに繋がらないなどのトラブルで困っている場合

利用プロバイダまたはパソコンのメーカー・購入店の各サポート窓口

情報セキュリティ

▶ 脆弱性対策情報
▼ 届出・相談・情報提供
▶ ウイルスの届出
▶ 不正アクセスの届出
▶ 脆弱性関連情報の届出
▼ 情報セキュリティ安心相談窓口
▶ 標的型サイバー攻撃の特別相談窓口
▶ 情報提供受付
▶ 特集コンテンツ
▶ 情報セキュリティ啓発
▶ 情報セキュリティ対策
▶ 暗号技術
▶ セキュリティエコノミクス
▶ 情報セキュリティ認証関連
▶ ISMAP
▶ セミナー・イベント
▶ 資料・報告書・出版物
▶ ツール
▶ サポート情報
▶ セキュリティセンターについて
▶ その他

IT利用者に求められるIT知識を習得できる国家試験

ITパスポート試験

試験の特徴

- ・ITパスポートは、ITを利活用するすべての社会人・学生が備えておくべきITに関する基礎的な知識が証明できる国家試験です。

メリット

試験勉強を通じ、幅広い分野の基礎知識が取得可能！

- ・情報セキュリティや情報モラルに関する知識が身に付きます
- ・企業コンプライアンス・法令遵守に貢献する正しい知識が身に付きます
- ・経営戦略、財務など、経営全般に関する基礎知識が身に付きます
- ・業務に必要なITの基礎知識が身に付きます

試験時間・出題形式

時間区分	試験時間	出題形式	出題数 解答数	基準点
午前	120分	四肢択一	100問	60点 (100点満点)

試験実施概要



- ・試験実施日
CBT方式で随時実施中
CBTとは、コンピュータを利用して実施する試験方式のことです。
- ・インターネットにて受付

情報セキュリティマネジメント試験

試験の特徴

- ・IT利用者の情報セキュリティ対策に特化した国家試験です。
社会人として必要な情報セキュリティの知識を体系的に習得できます。
- ・身近な事例をベースにした実践的な出題。

受験を特にお勧めする方

- ・業務で個人情報を取り扱う方
- ・業務部門・管理部門で情報管理を担当する方

試験時間・出題形式

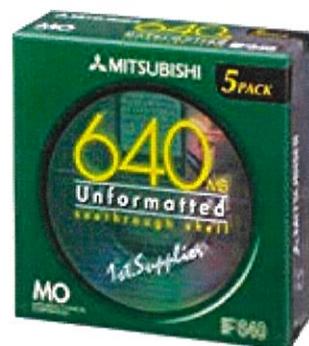
時間区分	試験時間	出題形式	出題数 解答数	基準点
午前	90分	多肢選択式 (四肢択一)	50問 50問	60点 (100点満点)
午後	90分	多肢選択式	3問 3問	60点 (100点満点)

試験実施概要

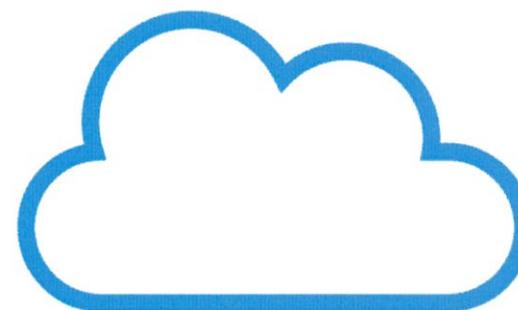


- ・試験実施日
年2回実施（春期・秋期）
春期：4月第三日曜日
秋期：10月第三日曜日
- ・インターネット・郵便にて受付

メディアの寿命



クラウド



メディアの寿命

メディアの名称	容量	信頼性	寿命	欠点	備考
フロッピーディスク(FD)	1.44MB前後	低い	10年	磁気、埃、汚れに弱い	容量が少なすぎてバックアップに向いていない
大容量磁気ディスク(ZIP/Jaz)	100MB～数GB	-	-	磁気、埃、汚れに弱い	書き込み速度は速いが廃れたメディアである
磁気テープ	数10GB～数TB	高い	10年	定期メンテナンスが必須	主に業務用の記憶メディアである
光ディスク(CD/DVD/BD)	640MB～128GB	高い	10-30年	書き込み速度が遅い	海外製品は寿命が0年のものがあるので注意
フラッシュメモリ(USBメモリ/SDカード/Flash SSD)	数10MB～数GB	低い	5年	書き換え回数に限度がある	一時的に保存するもので長期保存には適さない
光磁気ディスク(MO)	100MB～2.3GB	高い	50年	専用ドライブが入手困難	信頼性は高いが廃れたメディアである
ハードディスクドライブ(HDD)	数10GB～数TB	高い	3-5年	磁気や振動、衝撃に弱い	耐用年数が低い
ソリッドステートドライブ(SSD)	数10GB～数TB	低い	5年	書き換え回数に制限、価格が高い	データが消失する可能性があり長期保存には適さない

ご清聴ありがとうございました

