情報処理安全確保支援士（登録セキスペ）制度の紹介

2024年5月

独立行政法人情報処理推進機構（IPA）
デジタル人材センター
国家資格・試験部　登録・講習グループ

目次

１．情報処理安全確保支援士（登録セキスペ）とは

２．業務範囲、期待される役割

３．制度活用のメリット

４．登録状況について

１．情報処理安全確保支援士（登録セキスペ）とは

1．情報処理安全確保支援士（登録セキスペ）とは
情報処理安全確保支援士とは

サイバーセキュリティ分野初の登録制の国家資格として2016年10月に創設

法律上の資格名称	情報処理安全確保支援士
通称名	登録セキスペ （登録情報セキュリティスペシャリスト）
英語名	RISS：アール アイ エス エス （Registered Information Security Specialist）
根拠となる法律	情報処理の促進に関する法律（昭和四十五年法律第九十号） ・平成28(2016)年　4月22日 改正情促法公布 ・平成28(2016)年10月21日 改正情促法・政省令施行 ・令和　2(2020)年　5月15日　　情促法の一部改正法施行

【ロゴマーク】

説明

フレーム：盾（シールド）を意味し、様々な脅威から情報組織や社会を守る存在であること、深みのある青は誠実と冷静さを意味する。

地　　球：国際社会とデジタル社会を現す。

羽　　：ＩＴによる人々の生活の拡がりと飛翔を意味する。

４つの星：技術水準　レベル４という重要性の高い資格として目指す存在となることをイメージ。

1．情報処理安全確保支援士（登録セキスペ）とは
制度創設の背景

日本年金機構をはじめ、大規模な情報漏えい被害が頻発するなど
日本の組織・企業等に対するサイバー攻撃の件数は年々増加

2020年東京オリンピック・パラリンピック競技大会を狙った
サイバー攻撃のリスク

サイバーセキュリティ対策を担う高度かつ実践的な能力を有する
セキュリティ人材の育成・確保は急務

IPAや民間団体等によりセキュリティの能力を測る試験が複数実施されているものの、人材の所在が「見える化」されておらず、日進月歩のセキュリティ知識を適時・適切に評価できるものにはなっていない。

試験制度見直しの検討過程において、
サイバーセキュリティ分野における国家資格創設が提言されたことを受け
（注釈1）**「情報処理の促進に関する法律」を改正**

（注釈1）**セキュリティ人材の確保に関する研究会 中間報告 2015年8月**
https://www.meti.go.jp/shingikai/sankoshin/shomu_ryutsu/joho_keizai/pdf/006_s01_00.pdf
セキュリティ人材の確保に関する研究会：2015年8月に設置された研究会（全5回開催）経済産業省とIPAが事務局

1．情報処理安全確保支援士（登録セキスペ）とは
参考）情報処理の促進に関する法律

情報処理の促進に関する法律

情報処理の促進に関する法律
施行令（政令）・施行規則（経済産業省令）

・平成28(2016)年 4月22日 改正情促法公布
・平成28(2016)年10月21日 改正情促法・政省令施行
・令和 2(2020)年 5 月15日 情促法の一部改正法施行

【情報処理の促進に関する法律】

（情報処理安全確保支援士の業務）
第6条　情報処理安全確保支援士は、情報処理安全確保支援士の名称を用いて、事業者その他の電子計算機を　利用する者によるサイバーセキュリティの確保のための取組に関し、サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うとともに、必要に応じその取組の実施の状況についての調査、分析及び評価を行い、その結果に基づき指導及び助言を行うことその他事業者その他の電子計算機を利用する者のサイバーセキュリティの確保を支援することを業とする。

（登録）
第15条　情報処理安全確保支援士となる資格を有する者が情報処理安全確保支援士となるには、情報処理安全確保支援士登録簿に、氏名、生年月日その他経済産業省令で定める事項の登録を受けなければならない。
2　前項の登録は、三年ごとにその更新を受けなければ、その期間の経過によって、その効力を失う。

（登録事務の代行）
第22条　経済産業大臣は、機構[注釈]に、登録の実施に関する事務（第19条の規定による登録の取消し及び命令に関する事務を除く。次条第1項及び第2項並びに第51条第2項において「登録事務」という。）を行わせることができる。
注釈:独立行政法人情報処理推進機構

（受講義務）
第26条　情報処理安全確保支援士は、経済産業省令で定めるところにより、機構の行うサイバーセキュリティに関する講習又はこれと同等以上の効果を有すると認められる講習として経済　産業省令で定めるもの（同条において「特定講習」という。）を受けなければならない。

1．情報処理安全確保支援士（登録セキスペ）とは 制度の全体像

1．登録資格を取得する

① 試験合格者（情報処理安全確保支援士試験）

・情報セキュリティスペシャリスト試験をベースに新設
・全部又は一部免除制度
- 情報処理技術者試験との連携による一部免除
- 国内外の類似資格合格者や大学等でセキュリティを専門とする教育課程の修了者を一部免除
⇒告示（CoE注釈：全部免除、大学・大学院・専門学校(4年制)：午前Ⅱ免除）2017/9/29施行

② 資格試験合格と同等以上の能力を有する方

・国が指定するポストであって、当該ポストでの従事年数が一定期間を超える場合を想定。
⇒第一弾告示（警察・自衛隊）
2017/4/7施行
⇒第二弾告示（内閣官房、試験委員）
2017/9/29施行

情報処理安全確保支援士となる資格を有する者

2．登録する

登録申請

登録簿への登録

情報処理安全確保支援士

注釈：登録簿への登録、登録証の交付は、次のとおり年２回とする
4月1日 【申請締切日：2月15日（当日消印有効）】
10月1日 【申請締切日：8月15日（当日消印有効）】

義務違反の場合
登録取消し
又は
一定期間の名称使用停止

取消し後、2年間は再登録不可

3．活動・維持する

人材の見える化

登録情報の公開
必須項目（登録番号等）を除き、公開する項目は選択可能

資格名称の独占使用
登録セキスペ以外が名称を使用した場合は、30万円以下の罰金刑

人材活用の安心感

登録セキスペとしての義務遵守

（１）信用失墜行為の禁止

（２）秘密保持
・義務に違反した場合は、1年以下の懲役又は50万円以下の罰金刑が課される。

（3）講習受講
・オンライン講習を年1回、実践講習または特定講習を3年に1回受講。

（4）登録資格の更新
・3年に1度の更新が必要

人材の質の担保

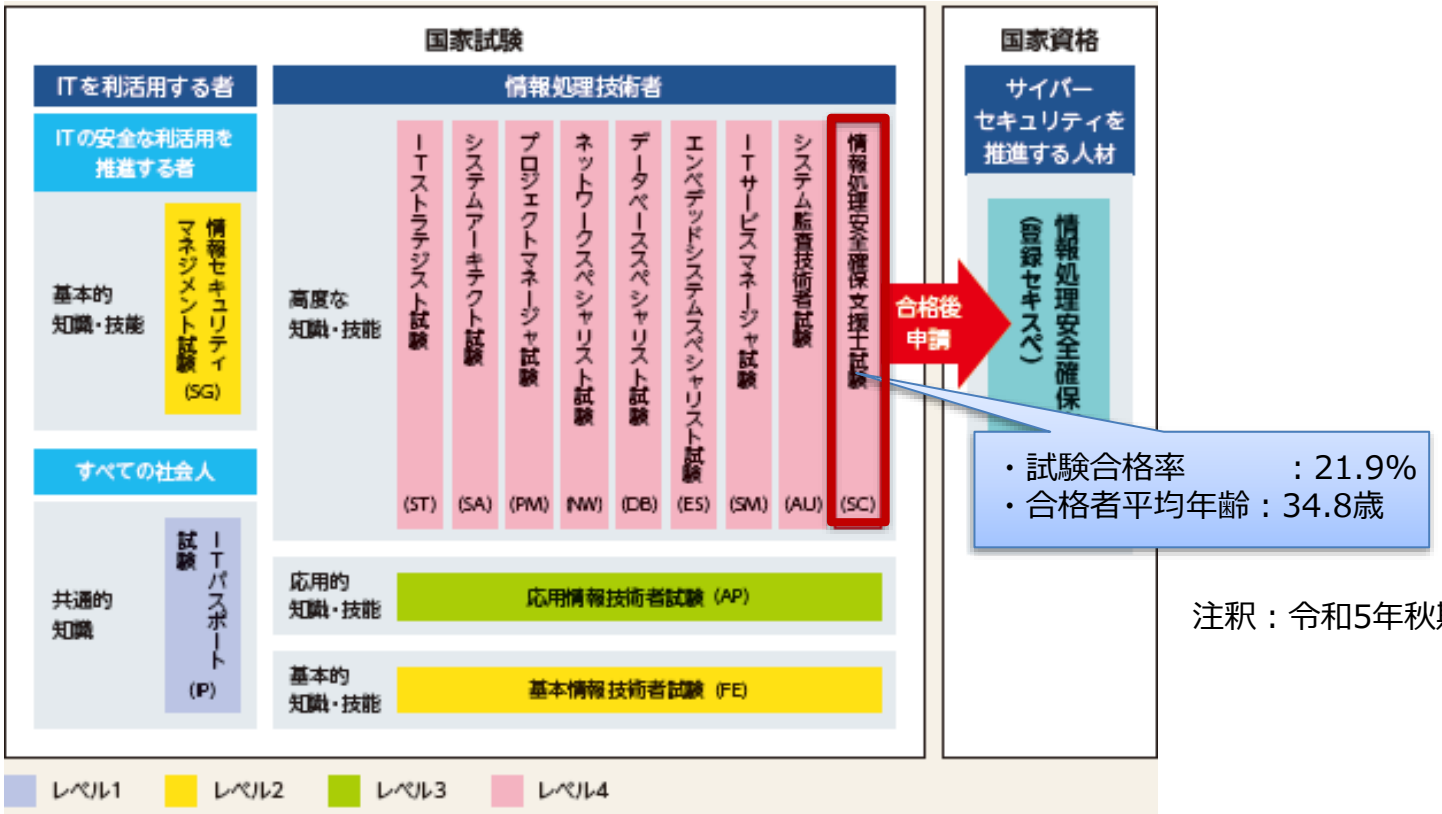
注釈：CoE：ここでは、IPA 産業サイバーセキュリティセンター中核人材育成プログラム修了者のこと
詳細）https://www.ipa.go.jp/jinzai/ics/core_human_resource/about.html

1．情報処理安全確保支援士（登録セキスペ）とは
情報処理安全確保支援士試験(SC)とは

1．登録資格を取得する

- IPAが実施する国家試験の中でも難易度の高いレベル4に分類され、高度なセキュリティの知識・技術が問われる試験
- 試験は年に2回実施（春期（4月予定）、秋期（10月予定））

・情報処理安全確保支援士試験（SC）の位置づけ



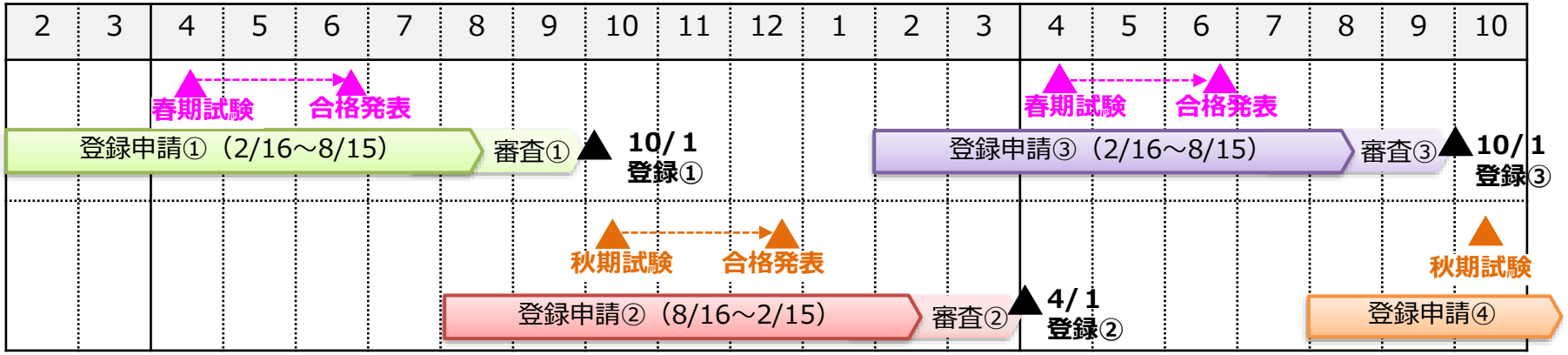
注釈：令和5年秋期実績

- **試験についての詳細**　→　情報処理技術者試験・情報処理安全確保支援士試験<https://www.ipa.go.jp/shiken/>
- （参考URL）IPANEWS vol.57 P3 <https://www.ipa.go.jp/about/ipanews/ps6vr70000001lxr-att/ipanews-057.pdf>

1．情報処理安全確保支援士（登録セキスペ）とは 資格取得までのスケジュールと必要な費用

1．登録資格を取得する | **2．登録する** | **3．活動・資格を維持する**

情報処理安全確保支援士試験日程と資格の登録申請スケジュール



情報処理安全確保支援士試験合格後、登録までの有効期限はありません。

資格取得～講習受講に必要な費用

初期費用

1.受験

受験手数料 7,500円

合格

登録費用

2.申請・登録

登録免許税： 9,000円
登録手数料：10,700円

登録

講習受講費用

3.講習受講

1年に1回	オンライン講習：20,000円
3年に1回	実践講習・特定講習：受講料は講習により異なります。(例)実践講習A：80,000円

注釈：実践講習・特定講習の中から1講習を選択して受講

1．情報処理安全確保支援士（登録セキスペ）とは 欠格事由、信用失墜行為の禁止・秘密保持

IPA

1．登録資格を取得する | 2．登録する | 3．活動・資格を維持する

欠格事由 (情報処理の促進に関する法律)

次の各号のいずれかに該当する者は、情報処理安全確保支援士となることができない。（第8条）

一 心身の故障により情報処理安全確保支援士の業務を適正に行うことができない者として経済産業省令で定める者

二 禁錮以上の刑に処せられ、その執行を終わり、又は執行を受けることがなくなつた日から起算して二年を経過しない者

三 この法律の規定その他情報処理に関する法律の規定であつて政令で定めるもの(注釈)により、罰金の刑に処せられ、その執行を終わり、又は執行を受けることがなくなつた日から起算して二年を経過しない者

四 第19条第1項第2号又は第2項の規定により登録を取り消され、その取消しの日から起算して二年を経過しない者

注釈：刑法（第168条の2及び第168条の3） 不正アクセス行為の禁止等に関する法律（第11条～13条）

信用失墜行為の禁止・秘密保持 (情報処理の促進に関する法律)

（信用失墜行為の禁止）

第24条　情報処理安全確保支援士は、情報処理安全確保支援士の信用を傷つけるような行為をしてはならない。

（秘密保持義務）

第25条　情報処理安全確保支援士は、正当な理由がなく、その業務に関して知り得た秘密を漏らし、又は盗用してはならない。 情報処理安全確保支援士でなくなつた後においても、同様とする。

（罰則）

第59条　第25条の規定に違反した者は、**一年以下の懲役**又は**五十万円以下の罰金**に処する。

2　前項の罪は、告訴がなければ公訴を提起することができない。

1．情報処理安全確保支援士（登録セキスペ）とは
登録資格の更新

3．活動・資格を維持する

登録資格は、３年ごとに更新が必要です

■更新制の目的

登録資格の更新制は、サイバーセキュリティに関する最新の知識・技能の維持のみならず、欠格事由に該当していないかなど、情報処理安全確保支援士としての資格を有しているかを改めて確認することで、情報処理安全確保支援士制度の信頼性を向上することを目的としています。

■更新手続き

- 登録資格の**有効期限は、登録日から起算して３年**となります。
- 登録更新申請は、**更新期限の60日前まで**に行う必要があります。
- 登録更新申請を行うためには、**毎年の受講が義務付けられている講習をすべて修了する必要があります。**
- 登録更新申請において、**更新手数料はかかりません。**

更新手続きの詳細は、IPAホームページ（https://www.ipa.go.jp/jinzai/riss/forriss/koushin.html）をご覧ください。

1．情報処理安全確保支援士（登録セキスペ）とは 登録証（カード）、ロゴマーク、徽章（バッジ）

2．登録する　3．活動・資格を維持する

登録証

登録セキスペには、登録証（カード型）が交付されます。
登録や更新回数に応じた3種類のカラーパターン（ 「グリーン」「ブルー」「ゴールド」）があります。

＜登録証のカラーパターン＞

ロゴマーク

登録セキスペは名刺などの任意の文書に
ロゴマークを使用することが可能です。

＜ロゴマークの利用例＞

徽章（バッジ）

登録セキスペは有資格者であることのアピールとして仕事の
機会等において着用することができます。

登録セキスペロゴマーク
をもとにしたデザイン

- 登録セキスペを対象として、希望者に徽章（バッジ）の貸与を行っています。
- 貸与手数料は2,970円（税込）です。

１．情報処理安全確保支援士（登録セキスペ）とは
登録情報の公開（1）

２．登録する　３．活動、資格を維持する

○ **情報処理安全確保支援士の見える化を行い、企業等がその人材を安心して活用できるようにするため、登録情報などをＩＰＡのウェブサイトで公開**

（１）公開情報

① 登録番号
② 登録年月日
③ 支援士試験の合格年月
④ 講習の修了年月日
⑤ 更新年月日
⑥ 更新期限
⑦ 登録更新回数

（２）任意公開情報

注釈：本人からの届出に基づき公開

① 氏名
② 生年月
③ 試験合格証書番号
④ 自宅住所（都道府県のみ）
⑤ 勤務先名称
⑥ 勤務先住所（都道府県のみ）

1．情報処理安全確保支援士（登録セキスペ）とは
登録情報の公開（２）

2．登録する　**3．活動、資格を維持する**

情報処理安全確保支援士検索サービスについて　https://riss.ipa.go.jp/

→業務の拡大や自己PR等への活用が可能

国が認めた情報セキュリティの専門家の所在が可視化され、その活躍の場が広がり、わが国の情報セキュリティ対策の強化につながることを期待しています。勤務先所在地や連絡先情報（電話番号、メールアドレス）の公開有無による検索が可能です。各都道府県において情報セキュリティのサービス提供事業者を探す場合などに、本検索サービスを活用できます。

□情報処理安全確保支援士検索サービスの機能

登録セキスペ向け機能

- **プロフィールのビジュアル化**
  →顔写真の掲載も可能。
- **リアルタイムにプロフィール編集**
  →マイページが一人ひとりに用意され、編集が可能。

一般利用者向け機能

- **Web上からの登録セキスペ検索**
  →様々な条件を指定した検索が可能。
- **登録セキスペの詳細プロフィール閲覧**

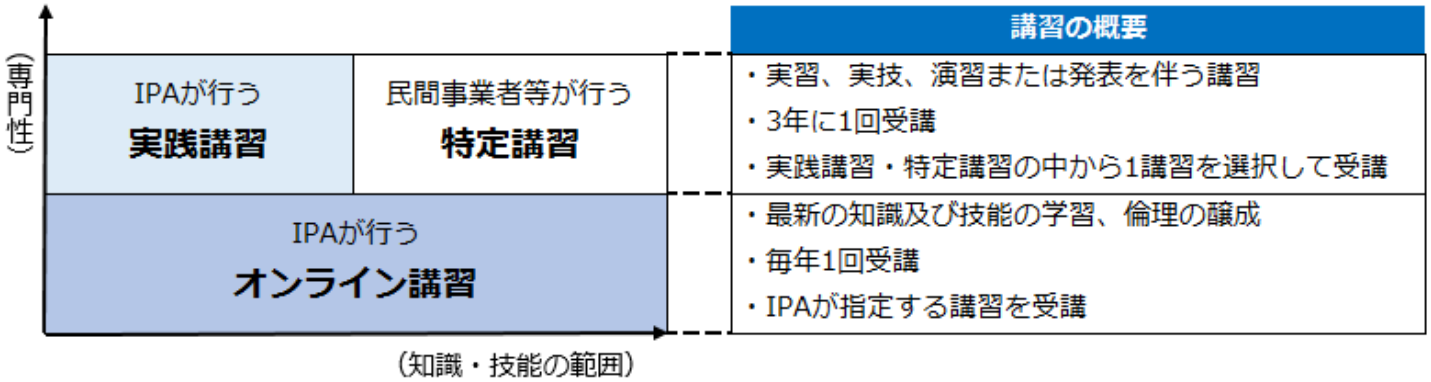
1．情報処理安全確保支援士（登録セキスペ）とは 講習制度の全体像と受講サイクル

3．活動・資格を維持する

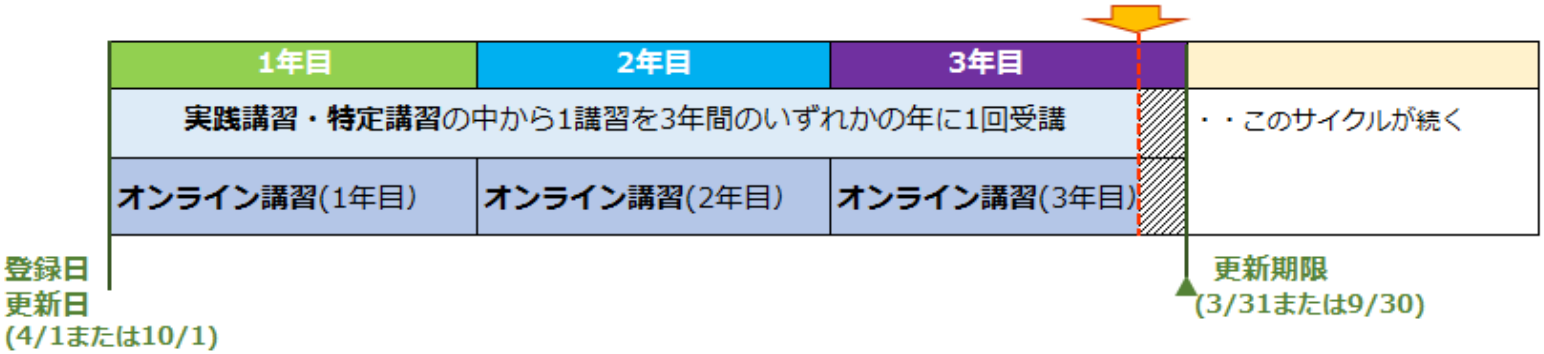
急速に変化するIT環境やサイバー脅威に対応できる活きた知識を身につけるため、定期的な講習受講が義務付けられています。

登録セキスペ 講習受講
https://www.ipa.go.jp/jinzai/riss/forriss/koushu.html

[講習制度の全体像]



[講習受講と更新のサイクル]



1．情報処理安全確保支援士（登録セキスペ）とは
オンライン講習と実践講習・特定講習

3．活動・資格を維持する

○ 1年に1回の**オンライン講習**と3年に1回の**実践講習・特定講習**を継続的に受講することで登録セキスペの業務に必要となる**知識・技能の維持・向上**及び**倫理観の醸成**が可能となります。

（1）科目及び範囲

① **知識：**攻撃手法及びその技術的対策、関連制度等の概要及び動向

② **技能：**脆弱性・脅威の分析、情報セキュリティ機能に関する企画・要件定義・開発・運用・保守、情報セキュリティ管理支援、インシデント対応

③ **倫理：**登録セキスペとして遵守すべき倫理

（2）実施形式

◆**オンライン講習**　：e-ラーニング形式

◆**実践講習・特定講習**　：リモート／集合形式　注釈：講習によって実施形式が異なります。

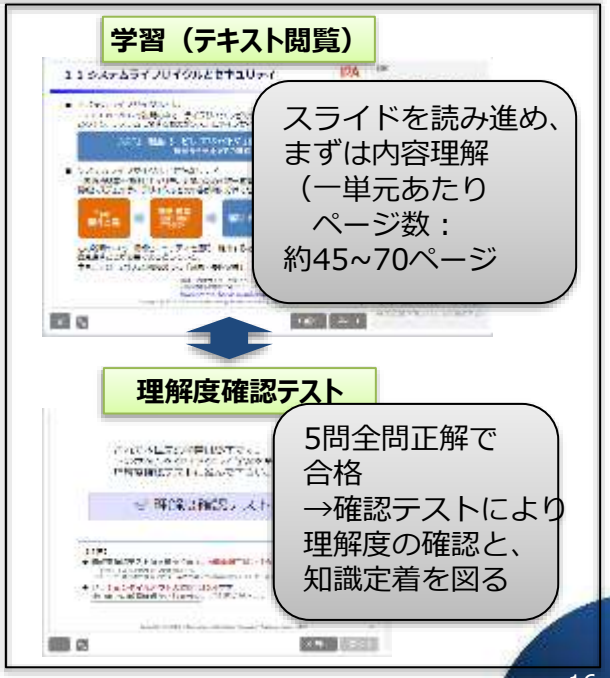
1．情報処理安全確保支援士（登録セキスペ）とは
オンライン講習の概要

3．活動・資格を維持する

オンライン講習の受講を通し、登録セキスペの業務に必要な最新知識の修得および技術のスキルアップを行うことができます。

講習のねらい：
- 設計・開発・運用の各段階において、セキュリティを組み込むために行うべき内容がわかる
- セキュリティの提案・指導・助言する際にその根拠となるガイドライン、事例を示すことができる
- IT環境、技術、法令の変化に対応してどのようなセキュリティ対策をすればよいか学ぶことができる

オンライン講習（e-ラーニング形式）
- 受講頻度：1年に1回（受講開始後90日以内）
- 標準学習時間：約6時間



➢**コース概要（2023年度の例）**　注釈：教材は毎年見直しを実施

知識	•情報処理安全確保支援士に期待される役割と知識
技能	•サイバーセキュリティ体制構築・人材育成 •セキュリティアーキテクチャ •事例から学ぶサイバー攻撃と対策 •データバックアップとセキュリティ
倫理	•倫理とコンプライアンス

1．情報処理安全確保支援士（登録セキスペ）とは
実践講習・特定講習の種類

3．活動・資格を維持する

3年に1回、情報セキュリティ対策を担う実践的な能力の修得・向上を目的として、
実践講習と特定講習の中から１講習を選択して受講します。

IPAが行う実践講習

①実践講習A　注釈：登録セキスペ登録後1～3年目の講習受講時にお勧め

インシデント対応などのグループ演習を通じ、登録セキスペとして求められる情報セキュリティ実践のための具体的な技術や手法を習得します。

②実践講習B　注釈：登録セキスペ登録後4年目以降の方にお勧め

新規事業を立ち上げる際のセキュリティ上の助言をグループで検討するという演習を通じ、業務で利用するための実践的な能力を習得します。

③業界別サイバーレジリエンス強化演習（CyberREX）

企業等の部門責任者層が、業界別の仮想企業におけるシナリオによる演習を通じ、サイバーリスクへの対応力・回復力の強化について学びます。

④制御システム向けサイバーセキュリティ演習（CyberSTIX）

企業等の制御システムに関わる実務者が、模擬システムにおけるサイバー攻撃や防御の演習を通じ、制御システムのセキュリティについてより深く実践的に学びます。

⑤民間事業者等が行う特定講習

IPAが行う実践講習と同等以上の効果を有すると認められる講習として経済産業大臣が定める、民間事業者等が行う講習です。

13実施機関、40講習（令和5年度）

- **情報処理安全確保支援士特定講習(経済産業省)**　https://www.meti.go.jp/policy/it_policy/jinzai/tokutei.html

いずれか１つを選択して受講（３年に１回）

1．情報処理安全確保支援士（登録セキスペ）とは ①実践講習A、②実践講習Bの概要

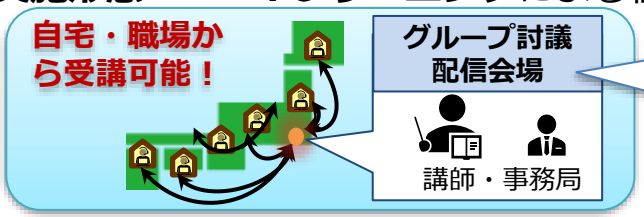
3．活動・資格を維持する

実践講習A、実践講習Bでは、培ったセキュリティ知識・技術をもとにグループ討議や意見交換を通じ、登録セキスペとして必要とされる実践的な能力を身に付けることができます。

講習のねらい：

- インシデント発生時の対応や予防策、新規事業企画の際のセキュリティリスク洗い出しや対策に関する検討、助言など、実践的な対応方法を学ぶことができる
- 「教科書的な判断」だけでは対応できない、実際に起こり得る課題に対しての対処方法を学べる
- 様々な地域や所属組織、異なる立場の登録セキスペの意見交換により新たな気づきを得ることができる

実施形態　：e-ラーニングによる個人学習、および、web会議システムを利用したグループ討議



配信会場の様子

コーススケジュール

①実践講習A 注釈：登録セキスペ登録後1～3年目の講習受講時にお勧め

1．個人学習（e-ラーニング形式）《標準学習時間：2時間》
(1)インシデント対応手法
(2)情報セキュリティにおける倫理

2．グループ討議 《10:00～17:00》
【ケーススタディ(1)】インシデント対応
【ケーススタディ(2)】予防策の検討
【ケーススタディ(3)】倫理的な判断・行動に関するケース

②実践講習B　注釈：登録セキスペ登録後4年目以降の方にお勧め

1．個人学習（e-ラーニング形式）《標準学習時間：3時間》
(1)個人情報の保護
(2)DX with Cybersecurity
(3)インシデントに備える

2．グループ討議 《10:00～18:00》
(1)【ケーススタディ 課題1】デジタル変革企画への対応
(2)【ケーススタディ 課題2】インシデントに備える
(3)振り返り

1．情報処理安全確保支援士（登録セキスペ）とは
①実践講習A、②実践講習Bの講師紹介

3．活動、資格を維持する

実践講習A、実践講習Bは、
有識者による委員会にて認定
された講師が担当
セキュリティ分野の第一線で
活躍し、ファシリテーターと
しても高い実績を持つ専門家

IPAホームページで認定講師
の写真、プロフィールを紹介

https://www.ipa.go.jp/jinzai/riss/forriss/koushu/jissen-koushi.html

1．情報処理安全確保支援士（登録セキスペ）とは
①実践講習Aのアンケート結果

3．活動・資格を維持する

実践講習A満足度アンケート（5段階・平均） 注釈：2022年度受講者より集計
講習全体：4.33　グループ演習 ：4.22
講師：4.65　個人学習の役立度：4.11

実践講習A 受講者アンケートコメント

実務上、役に立つことがあった

- 業務では調査・分析を主に行っており、**経営者からの観点の理解が不十分であったが、講習を通じて理解を深めることができた**ため、今後の業務に役立つと感じた。
- **技術的な立場で助言するだけでなく、各役割の立場に寄り添った助言・報告とすべき**という点を今後の行動指針としていきたい。

インシデントハンドリングを学べて/試せてよかった

- 講師の方や同じグループの方から**インシデント対応の際の話が聞けて発生時のイメージがつかめた。**
- 自分が普段携わっていないインシデント対応やCSIRT構築・運用や経営目線など**さまざまな視点の考え方を学ぶことができた。**

倫理面への意識ができた

- 情報処理安全確保支援士倫理綱領を基に、**実際に起こりうる事象について柔軟かつ適切に対処できる**よう、日ごろから意識と訓練をしていきたいと感じた。

講師の指導がよかった

- 講師の進行、解説、雰囲気、内容いずれも良く、**初めてのリモート受講でしたが安心して受講することができた。**
- テキストだけでは得られない、大変**多くの有意義な気付きを得られた。**

様々な視点が持てた、受講者間の交流が有意義だった

- さまざまな立場の方がいて、**セキュリティ技術者だけのミーティングより面白いと思った。従来の仕事、経験で気づかなかったことなどもあり参考になった。**
- 他業種の方はセキュリティについての目線に違いがあることに気づき、**考え方の幅が広がった。**

地域にとらわれず、全国の方と意見交換ができた

- 地域で集まるのではなく、**全国の方と意見交換できるのはリモート講習ならではの貴重な場**だと感じた。

1．情報処理安全確保支援士（登録セキスペ）とは ③CyberREX、④CyberSTIXの概要

3．活動、資格を維持する

③業界別サイバーレジリエンス強化演習（CyberREX）（2日間）

責任者向けプログラム

■**目的**　：業界特性に応じたシナリオを通じてサイバーセキュリティに関する対応力・回復力の強化
■**対象業界**：募集対象となる業界は毎回異なります。
過去の募集業界例：
電力、ビル、情報通信、物流、鉄道、航空、船舶、ガス、金属、石油、化学、自動車(製造)、ファクトリーオートメーション等
■**対象者**　：上記企業において、
・CISOに相当する役割を担っている方
・IT部門、生産部門などの責任者・マネージャークラスの方
■**内容**　：・業界別に仮想企業を想定した、シナリオによる実践的演習の形式を中心としたトレーニング
・海外子会社、系列企業、サプライチェーン等のビジネスパートナーが直面するサイバーセキュリティ規制やガイドライン等の解説に関する集中講義

④制御システム向けサイバーセキュリティ演習（CyberSTIX）(1.5日間)

実務者向けプログラム

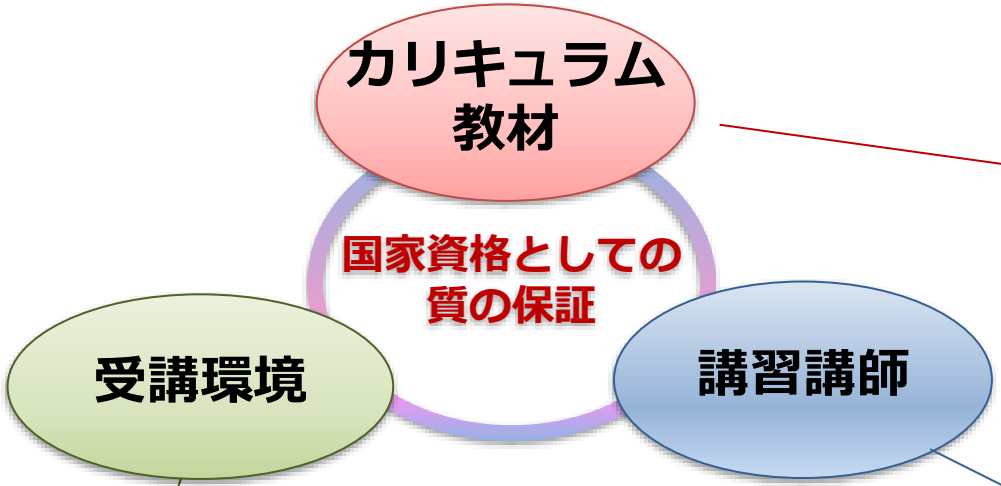
■**目的**　：産業制御システムにおけるサイバーセキュリティ対策を実践するための、基礎的な知識や技術を、講義と演習を通じて習得
■**対象者**：制御システムのサイバーセキュリティを担当している方、または今後担当される予定の方
■**内容**　：・講義を通して、産業制御システム(ICS)の基礎知識およびICSのサイバーリスクを学び、ICSのサイバーリスクに対し、取るべき対策を理解
・ハンズオンを通して、ICSに関連するサイバーインシデントを体験
・ディスカッションを通じて、どのような対策を組織でとるべきか、気づきを高める

1．情報処理安全確保支援士（登録セキスペ）とは
(参考)IPAが行う講習の基本方針

IPA

3．活動・資格を維持する

○高品質で効果的かつ受講しやすい講習を提供



■**効果を意識したカリキュラム設計**
→インストラクショナルデザイン(注釈)等に基づく設計
→オンライン講習による知識の習得と、
それを活用して実践力を養うことを目的とした実践講習の組合せによる学習効果
→実践にマッチしたケーススタディ中心による実践講習

■**教材開発・維持管理**
・知識・技術・倫理分野を含んだ実践に即した内容
・毎年見直しを実施

■**理解度の確認**
・確認テスト実施や、演習ファシリテーターによる理解度チェック

注釈：ADDIE（分析→設計→開発→実施→評価）と呼ばれるインストラクショナルデザインのプロセスに基づき、効果的・効率的に教育を行う科学的な手法。

■**登録セキスペ個人へのきめ細かい案内**
・メールによる受講フォロー

■**居住地によらない受講機会の提供**
・オンラインでの提供(オンライン講習)
・Web会議システムを活用した講習の開催 (実践講習A、実践講習B)
・首都圏以外での講習の開催(業界別サイバーレジリエンス強化演習（CyberREX）、制御システム向けサイバーセキュリティ演習（CyberSTIX））

■**障害者受講時の配慮**
・「障害を理由とする差別の解消の推進に関する法律」に基づく合理的配慮の提供

■**法定講習の登壇要件を満たしている講師**
（講師認定基準に基づく審査を実施）
・セキュリティ分野の第一人者
・ファシリテーションの実績豊富

1．情報処理安全確保支援士（登録セキスペ）とは
（参考）身体障害者等の講習受講時の合理的配慮について

IPA

3．活動、資格を維持する

注釈:講習受講時の特別措置を必要とする場合は、登録申請書類にてIPAにお知らせください。

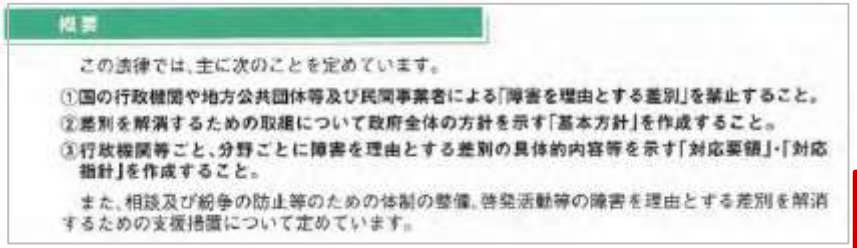
●IPAにおける障害者対応の基本方針

障害者差別解消法(注釈)の主旨に則り合理的配慮を行うことを基本方針として対応する。

(注釈) 障害を理由とする差別の解消の推進に関する法律

国連の「障害者の権利に関する条約」の締結に向けた国内法制度の　整備の一環として、全ての国民が、障害の有無によって分け隔てられる　ことなく、相互に人格と個性を尊重し合いながら共生する社会の実現に向け、障害を理由とする差別の解消を推進することを目的として、平成25年6月、「障害を理由とする差別の解消の推進に関する法律」（いわゆる「障害者差別解消法」）が制定され、平成28年4月1日から施行されました。

(出典)内閣府HP
https://www8.cao.go.jp/shougai/suishin/sabekai.html


概要

この法律では、主に次のことを定めています。

①国の行政機関や地方公共団体等及び民間事業者による「障害を理由とする差別」を禁止すること。
②差別を解消するための取組について政府全体の方針を示す「基本方針」を作成すること。
③行政機関等ごと、分野ごとに障害を理由とする差別の具体的内容等を示す「対応要領」・「対応指針」を作成すること。

また、相談及び紛争の防止等のための体制の整備、啓発活動等の障害を理由とする差別を解消するための支援措置について定めています。

(出典)
内閣府リーフレット「障害者差別解消法が制定されました」より
https://www8.cao.go.jp/shougai/suishin/pdf/leaf_seitei.pdf

1．情報処理安全確保支援士（登録セキスペ）とは
⑤民間事業者等が行う特定講習(1/3)

IPA

3．活動・資格を維持する

2024年4月9日時点

特定講習は、IPAが行う実践講習と同等以上の効果を有すると認められる講習として、経済産業大臣が定める講習であり、個々の登録セキスペが目指すキャリアパスに応じて、受講したい分野を選択可能

令和6年度特定講習一覧 (1/3)　14実施機関、48講習

No	実施機関名	講習名	受講対象者
1	大日本印刷株式会社	サイバー・インシデントレスポンス・マネジメントコース基礎演習	セキュリティ担当者、またはIT分野で3年以上の実務経験のある方
2		サイバー・インシデントレスポンス・マネジメントコース基礎演習１日版	セキュリティ担当者。またはIT分野で3年以上の実務経験者。
3		サイバー・インシデントレスポンス・マネジメントコース基礎演習２日版	セキュリティ担当者。またはIT分野で3年以上の実務経験者。
4	株式会社ワイ・イー・シー	Ｗｉｎｄｏｗｓ　Ｆｏｒｅｎｓｉｃｓ	インシデントレスポンスの実務経験とコマンドラインを利用した操作ができることが望ましい CSIRT要員（技術系）、SOC要員（運用、監視）
5		Ｍａｃ　Ｆｏｒｅｎｓｉｃｓ	デジタルフォレンジックの実務経験（OS問わず）、WindowsやLinux等でのコマンドラインによる操作が出来ることが望ましい CSIRT要員（技術系）
6		Ｆｉｌｅ　Ｓｙｓｔｅｍ　Ｆｏｒｅｎｓｉｃｓ	デジタルフォレンジックの実務経験（OS問わず）があることが望ましい
7		マルウェア解析基礎	インシデントレスポンスの実務経験、コマンドラインを利用した操作、仮想化技術（VMware、VirtualBox等）の操作ができることが望ましい CSIRT要員（技術系）、SOC要員（運用、監視）
8	トレンドマイクロ株式会社	標的型攻撃対応・防御トレーニング５日版	・SOC/CSIRTへの技術者としての従事 ・組織のLANシステムの運用者 ・セキュリティ関連職への技術者としての従事
9		標的型攻撃対応・防御トレーニング３日版	・SOC/CSIRTへの技術者としての従事 ・組織のLANシステムの運用者 ・セキュリティ関連職への技術者としての従事
10		インシデント調査トレーニング　クライアント端末版	・SOC/CSIRTへの技術者としての従事 ・組織のLANシステムの運用者 ・クライアント端末セキュリティの運用者
11		ランサムウェア　対応・防御トレーニング	IT/セキュリティ技術者としての従事 組織のIT環境の運用者
12	ＮＥＣビジネスインテリジェンス株式会社	ＣＳＩＲＴ強化トレーニング　マルウェア感染対応編	・組織における情報システム、ネットワーク運用管理経験があることが望ましい ・Windowsアプリケーション開発経験があることが望ましい
13		ＣＳＩＲＴ強化トレーニング　テクニカル編（ＣＴＦ形式）	・Windows、Linuxのシステム管理経験があることが望ましい ・Windows操作、Linuxのコマンドライン操作ができることが望ましい ・Windowsアプリケーションの開発経験があることが望ましい
14		サイバー防御トレーニング―Ｂｌｕｅ　Ｔｅａｍ　Ｔｒａｉｎｉｎｇ―	・Windows、Linuxのシステム管理経験があることが望ましい ・Windows操作、Linuxのコマンドライン操作ができることが望ましい
15		インシデントレスポンス基礎　－マルウェア解析編－	・Windows、Linuxのシステム管理経験があることが望ましい。 ・Windows操作、Linuxのコマンドライン操作ができることが望ましい。
16		【フリーシナリオ形式】実践！サイバーセキュリティ演習	・Windows、Linuxのシステム管理経験があることが望ましい。 ・Windows操作、Linuxのコマンドライン操作ができることが望ましい。 ・セキュリティに関する実務経験があることが望ましい。

1．情報処理安全確保支援士（登録セキスペ）とは
⑤民間事業者等が行う特定講習(2/3)

3．活動・資格を維持する

令和6年度特定講習一覧(2/3)

No	実施機関名	講習名	受講対象者
17	ＮＥＣビジネスインテリジェンス株式会社	【ステップバイステップ形式】実践！サイバーセキュリティ演習	・Windows、Linuxのシステム管理経験があることが望ましい。 ・Windows操作、Linuxのコマンドライン操作ができることが望ましい。
18		サイバー攻撃トレーニング　－Ｒｅｄ　Ｔｅａｍ　Ｔｒａｉｎｉｎｇ－	・組織における情報システム、ネットワーク運用管理経験があることが望ましい ・Linuxサーバ構築または運用経験があることが望ましい ・Windowsサーバ構築または運用経験があることが望ましい
19		インシデントレスポンス基礎　－フォレンジック解析編－	・Windows、Linuxのシステム管理経験があることが望ましい。 ・Windows操作、Linuxのコマンドライン操作ができることが望ましい。
20		インシデントレスポンス基礎　－ログ解析編－	・Windows、Linuxのシステム管理経験があることが望ましい。 ・Windows操作、Linuxのコマンドライン操作ができることが望ましい。
21	株式会社ラック	Ｗｅｂアプリケーション脆弱性診断ハンズオンコース	IT技術全般（インフラ系・開発系）、情報システム・セキュリティ推進部門担当者、SOC（セキュリティ運用）要員、 CSIRT要員（技術系）、システム系監査担当
22		プラットフォーム脆弱性診断ハンズオンコース	IT技術全般（インフラ系・開発系）、情報システム・セキュリティ推進部門担当者、SOC（セキュリティ運用）要員、 CSIRT要員（技術系）、システム系監査担当
23		マルウェア解析ハンズオン入門コース	IT技術全般業務（インフラ系・開発系） SOC（セキュリティ運用）要員業務 CSIRT要員（技術系）業務 情報セキュリティ関連調査研究業務
24		マルウェア解析ハンズオン専門コース	IT技術者（インフラ系・開発系）、SOC（セキュリティ運用）要員、CSIRT要員（技術系）、インシデント調査技術、 マルウェア解析業務等々、セキュリティ調査関連の専門業務経験全般
25		セキュリティオペレーション実践コース 初級編	IT技術全般（インフラ系・開発系）、情報システム・セキュリティ推進業務、SOC（セキュリティ運用）要員業務、その 他インシデント対応に関連した業務
26		セキュリティオペレーション実践コース 中級編	IT技術全般（インフラ系・開発系）、情報システム・セキュリティ推進業務、SOC（セキュリティ運用）要員業務、その他インシデント対応に関連した業務
27		デジタル・フォレンジックコース	IT技術全般（インフラ系・開発系）、情報システム・セキュリティ推進業務、SOC（セキュリティ運用）要員業務、その他インシデント対応に関連した業務
28		情報セキュリティ事故対応１日コース　机上演習編	管理職、IT技術者（インフラ系・開発系）、情報システム・セキュリティ推進部門担当者、SOC（セキュリティ運用）要員、CSIRT要員（管理系・技術系）、監査担当、経営者等、セキュリティインシデントに影響のある業務の経験
29		マルウェア解析ハンズオン専門演習コース	SOC（セキュリティ運用）要員 CSIRT要員（技術系）
30		情報セキュリティ事故対応2日コース　実機演習編	セキュリティインシデントに影響のある業務の経験
31	株式会社アイ・ラーニング	情報セキュリティマネジメント構築	特に不要です。
32		プロが教えるインシデント対応実践ワークショップ	情報セキュリティもしくはサイバーセキュリティの分野で3年以上の実務経験を有することが望ましい

1．情報処理安全確保支援士（登録セキスペ）とは
⑤民間事業者等が行う特定講習(3/3)

3．活動・資格を維持する

令和6年度特定講習一覧(3/3)

No	実施機関名	講習名	受講対象者
33	株式会社インターネットイニシアティブ	インシデントハンドリング実践コース	・情報システム部（ネットワーク運用、システム管理） ・CSIRT（PoC、インシデント対応）
34		攻撃技術理解・防御 APT対策基礎コース	・セキュリティ業務経験がある方
35		セキュリティ対策基礎 実践コース	・セキュリティ業務経験がある方
36	国立研究開発法人情報通信研究機構（NICT）	実践サイバー演習RPCI(リプシィ)～大規模演習環境を活用してリアリティを高めたインシデントハンドリング演習～	・CISO、CSIRT管理者、CSIRTメンバー、インシデントが発生した際の対応に携わる方 ・情報システム管理、運用に携わる方 ・情報システムの調達・企画・開発に携わる方
37	株式会社バルクホールディングス	Ｃｙｂｅｒ－Ｔｈｒｅａｔｓ ａｎｄ Ｄｅｆｅｎｓｅ Ｅｓｓｅｎｔｉａｌｓ	システム部門またはセキュリティ部門で１年以上従事経験がある
38		Ｆｏｒｅｎｓｉｃｓ Ｔｒａｉｎｉｎｇ	セキュリティ業務経験3年以上
39	NRIセキュアテクノロジーズ株式会社	セキュアＥｇｇｓ応用編（インシデント対応）	・情報セキュリティインシデントへの対応を考えている方 ・インシデント対応チーム(CSIRT)にたずさわる方 ・SANS SEC504(GCIH)にむけて準備したい方
40		セキュアＥｇｇｓ応用編（フォレンジック）	・これからフォレンジックを学び始める方 ・インシデント対応チーム(CSIRT)にたずさわる方 ・SANS SEC508(GCFA)にむけて準備したい方
41		セキュアＥｇｇｓ応用編（Ｗｅｂアプリケーションセキュリティ）	・これからWebアプリケーションのセキュリティテストを学びはじめる方 ・Webアプリケーションの開発、運用にたずさわる方 ・SANS DEV522(GWEB)にむけて準備したい方
42	グローバルセキュリティエキスパート株式会社	Ｍｉｃｒｏ Ｈａｒｄｅｎｉｎｇ：Ｅｎｔｅｒｐｒｉｓｅ Ｅｄｉｔｉｏｎ（マイクロハードニング：エンタープライズエディション）	サイバー攻撃に関する一般的な知識をお持ちの方。また、サーバやネットワーク等のシステム運用経験があると望ましい。
43	株式会社アクト	Ｃｙｂｅｒ－Ｔｈｒｅａｔｓ ａｎｄ Ｄｅｆｅｎｓｅ Ｅｓｓｅｎｔｉａｌｓ	・システム部門またはセキュリティ部門で１年以上従事経験がある ・インターネットブラウザを使用して日本語で各種情報を検索・閲覧できる ※プログラミングの知識や経験は問いません
44	株式会社日立アカデミー	ケーススタディから学ぶ情報セキュリティリスク対策	・情報資産の洗い出しとリスクアセスメント（リスク査定）の経験があること ・情報セキュリティマネジメントの構築または運用に関連した業務の経験があること
45	株式会社サイバーディフェンス研究所	OTシステムハッキング－独自プロトコル解析とサイバー攻撃の実践	Wiresharkの利用経験（キャプチャファイルを眺めた程度で問題ありません） 何らかのプログラム学習経験（数日の学習経験で問題ありません）
46		ハッキング－ハードウェア	Linux端末でのCUI操作 はんだ付け（趣味のレベルで問題ありません）
47		マルウェア解析Ⅰ	システム/ネットワークの運用経験 プログラミング経験
48		マルウェア解析Ⅱ	システム/ネットワークの運用経験 プログラミング経験

➢ **令和6年度特定講習一覧：**
https://www.meti.go.jp/policy/it_policy/jinzai/tokutei_file/koushu_r6/240401_ichiran.pdf

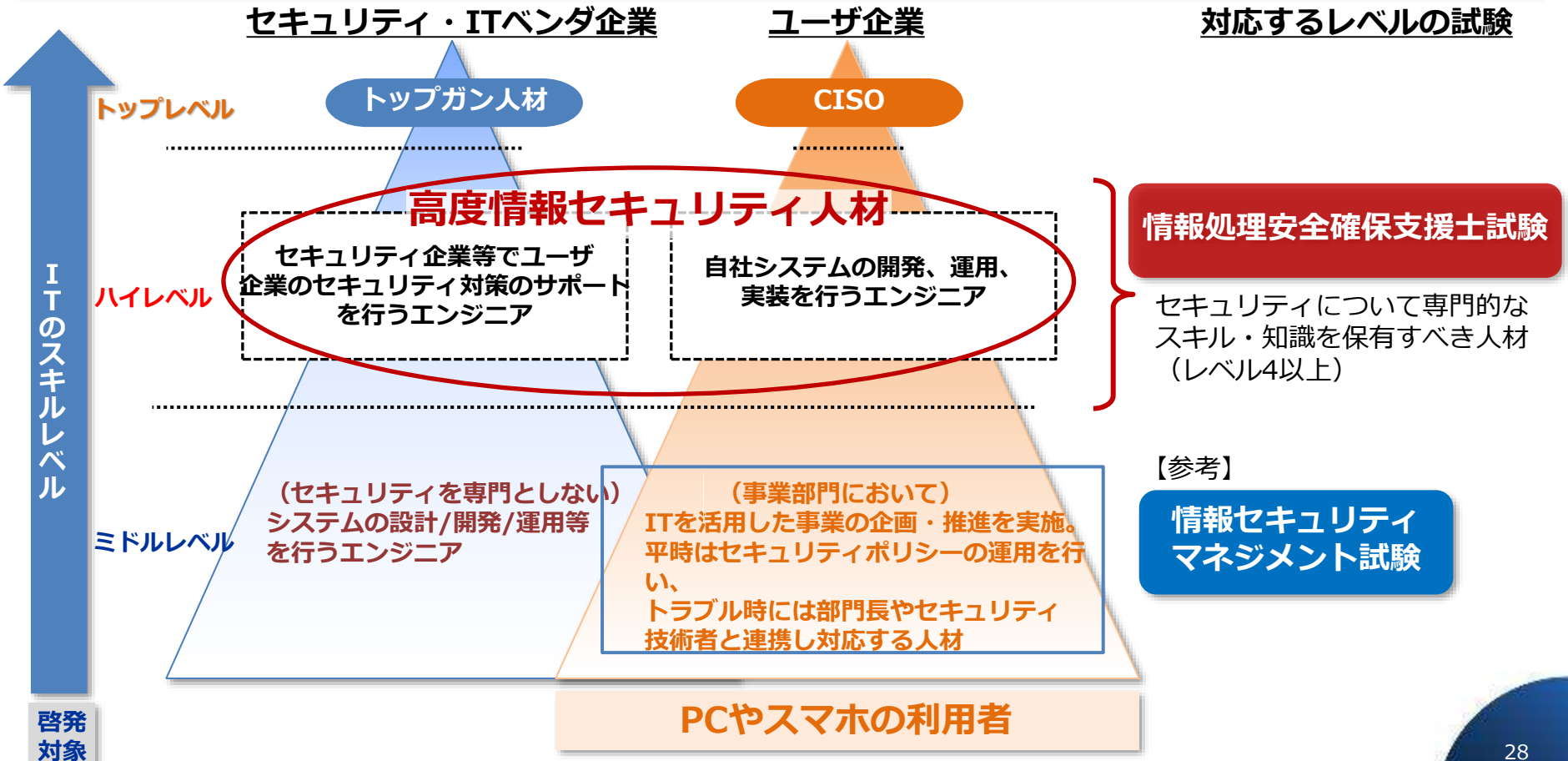
2．業務範囲、期待される役割

2．業務範囲、期待される役割
高度情報セキュリティ人材の位置づけ

【情報処理の促進に関する法律】（抜粋）

（情報処理安全確保支援士の業務）

第6条　情報処理安全確保支援士は、**サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うとともに、必要に応じその取組の実施の状況についての調査、分析及び評価を行い、その結果に基づき指導及び助言を行うこと**その他事業者その他の電子計算機を利用する者の**サイバーセキュリティの確保を支援すること**を業とする。



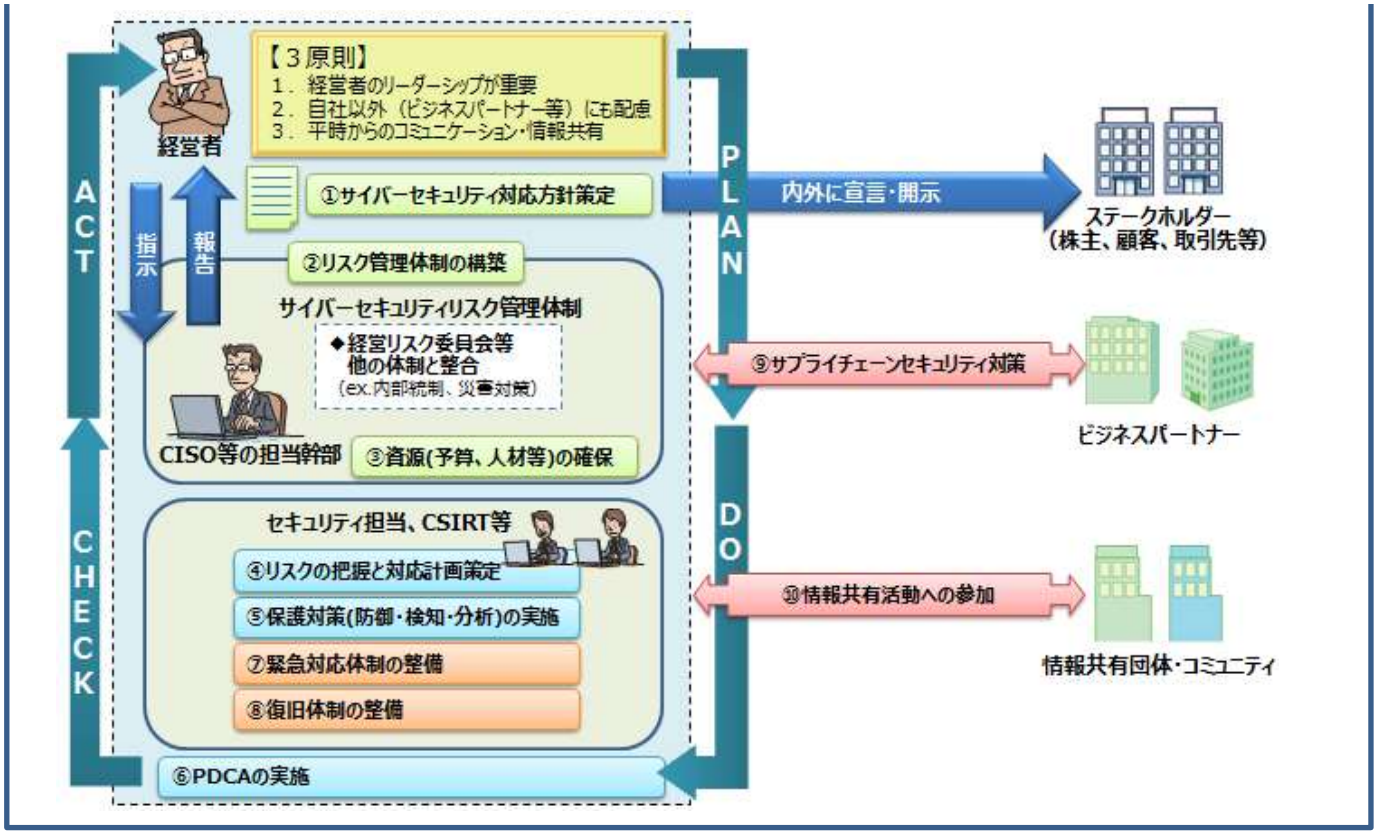
2．業務範囲、期待される役割
期待される役割

「サイバーセキュリティの確保は積極的な経営への「投資」であり、経営者の重要な責務の一つ」

しかし、経営層が必ずしも技術やセキュリティに詳しいわけではなく、セキュリティ対策の現場担当者は経営層とのコミュニケーションに慣れていない

経営と現場をつなぐ「経営層の右腕」としての活躍が期待されている

経営者が認識する必要のある「3原則」に基づき、経営者がCISO等に指示すべき「重要10項目」の概要



出典：経済産業省　サイバーセキュリティ経営ガイドライン（http://www.meti.go.jp/policy/netsecurity/mng_guide.html）

登録セキスペの業務例（経営層の右腕として）

・CISOが策定するサイバーセキュリティ対応方針を、実践で活用できる確実なものとするよう支援する。

・緊急対応時の経営判断に必要となる情報を経営者やCISOに提供。そのために、普段から事業担当部門のリスク把握と対応計画策定を行っておく。

2．業務範囲、期待される役割
想定される業務

想定される業務

1．経営課題への対応
セキュリティ対策策定・更改・実施指導
組織・技術上のリスク評価
上記のための監査・検査・調査・分析

2．システム等の設計・開発
設計段階までのセキュリティ対策、
セキュアコーディングの推進、
セキュリティテストの実施・評価　等

3．運用・保守
ポリシー実践、脆弱性への対応
品質管理、情報収集
教育・啓発活動　等

4．緊急対応
緊急時に備えた準備、
インシデント対応の全体統制、
インシデント処理・復旧

情報処理安全確保支援士を活用する企業のメリット
提供する機能やサービスの信頼性確保、企業の社会的信用度の向上
⇒ **ビジネスチャンスの拡大**

ITベンダ企業での期待・効果

○セキュアなものづくりにおける技術者としての活躍
○ユーザ企業へのコンサル、研修等への対応
○自社セキュリティ対策の企画・立案
○システムの運用・保守、監視、調査等の実施

ITユーザ企業・官公庁等での期待・効果

○システムの運用・保守、監視、インシデントの調査分析等への対応（自社人材として又は外部実施者との調整者として）
○自社セキュリティ対策の企画・立案
○社内情報セキュリティ教育の実施
○ＣＩＳＯ、ＣＩＯ（又は補佐）への登用

活躍

支援

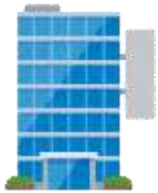
情報処理安全確保支援士のメリット
最新の知識・技能を有することの証明、個人の信頼度向上
⇒ **活躍の場の拡大**

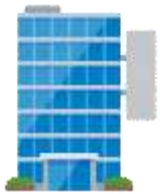
○国家資格の取得により、最新の情報セキュリティに関する知識・技能を有することの証し
○登録セキスペとして義務を果たしていることによる、資格保有者個人の信頼度の付加又は向上
○企業内におけるステータスの獲得
○IPAによる登録状況の見える化（登録セキスペであることの表示・公表）

3. 制度活用のメリット

3．制度活用のメリット
情報処理安全確保支援士のメリット、所属組織のメリット

情報処理安全確保支援士になることで得られるメリットは、
本人に留まらず、セキュアな社会実現への貢献にも繋がる。





	情報処理安全確保支援士	ITベンダー	ユーザ企業
スキルアップ	知識の最新化 専門家同士の繋がり 関連資格取得の優遇	顧客視点のセキュリティ要求事項の理解 セキュアなシステムの設計・開発・運用	経営者と一体となったセキュリティ対策の推進 セキュアに必要なシステム要求の提示
ビジネス	・就業機会の増加　・活躍の場の拡大　・入札要件の充足		
社会的評価	セキュアな社会実現への貢献		

3．制度活用のメリット
情報処理安全確保支援士のメリット

技術者

サイバー攻撃が増加する中で、サイバーセキュリティ対策を担う専門人材は不足しており、社会全体として、早急な人材の確保が求められている

脅威や攻撃手法は刻々と変わり、規模も拡大

サイバーセキュリティ人材母集団の拡大の必要性
関係者間のネットワークづくり、情報共有の必要性

①情報セキュリティに関する高度な知識・技能を保有する証

・「情報処理安全確保支援士試験」の合格者が登録対象者であり、かつ毎年の講習受講が義務付けられていることから、登録を維持していることが継続的に自己研鑽を実施していることの証になります。
・名称の独占使用ができます。(登録セキスペでない方が使用した場合、30万円以下の罰金になります。)

②継続的・効果的な自己研鑽が可能

・毎年講習の受講が義務付けられており、その中で、サイバーセキュリティの専門家が監修した、最新情報を反映した内容を学ぶことができます。
講習は、インストラクショナルデザインに基づく講習設計など効果的な学習を実現する手法を取り入れています。
・最新の知識・技能の維持のため、毎年1回のオンライン講習と、3年に1回の実践講習・特定講習の受講が義務付けられています。実践講習では、他業種の登録セキスペとのネットワークづくりや情報共有が可能です。

3．制度活用のメリット
所属組織のメリット

組織・企業

グローバルな競争環境の変化の中でサイバーセキュリティは
より積極的な経営への「投資」注釈

ビジネスチャンスの拡大　　サイバー攻撃などのリスクの増大

サイバーセキュリティの確保は、企業の経営層が
果たすべき責任の一つ

①提供する機能やサービスそのものへの信頼の向上

・緊急対応（インシデント）のみならず、ものづくり、運用など企業活動の多岐にわたって登録セキスペの関与が進むことにより、事業継続・機能保障など総合的な観点から、信頼性が向上します。

②社会的評価・信頼の向上

・自組織における登録セキスペの保有人数や、登録セキスペの監査や助言を受けていること等を積極的に情報開示していくことで、組織としてのサイバーセキュリティ確保への取り組み姿勢の表明が可能です。
・厳格な秘密保持義務等や信用失墜行為の禁止などの義務があり、採用面での安心感につながります。

③ビジネスチャンスの拡大

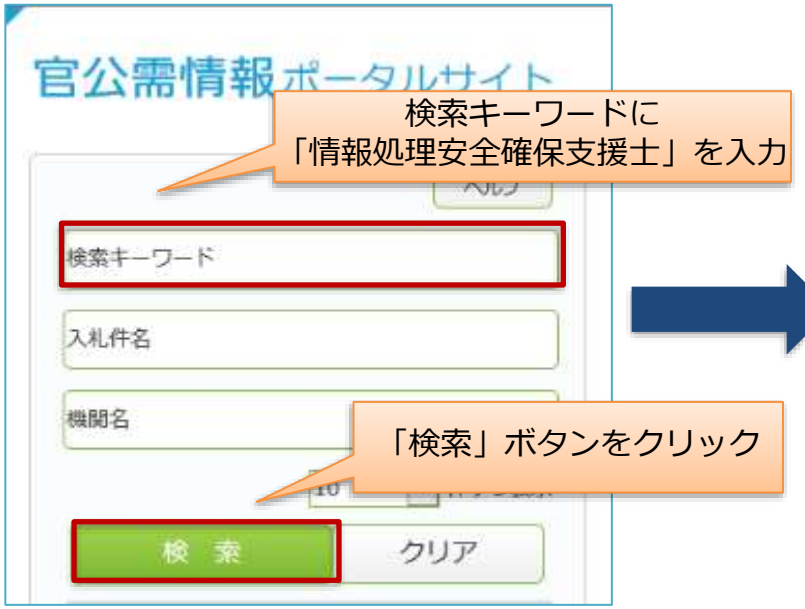
・ITによるビジネス革新（プロセスや取引範囲の変化）が進む中で、サプライチェーンにおける組織のセキュリティ管理責任は増大します。今後は調達における登録セキスペの参画の要件化なども想定されることから、登録セキスペの育成が企業競争力の向上につながります。

注釈：出典「企業経営のためのサイバーセキュリティの考え方の策定について」平成28年8月2日 NISC

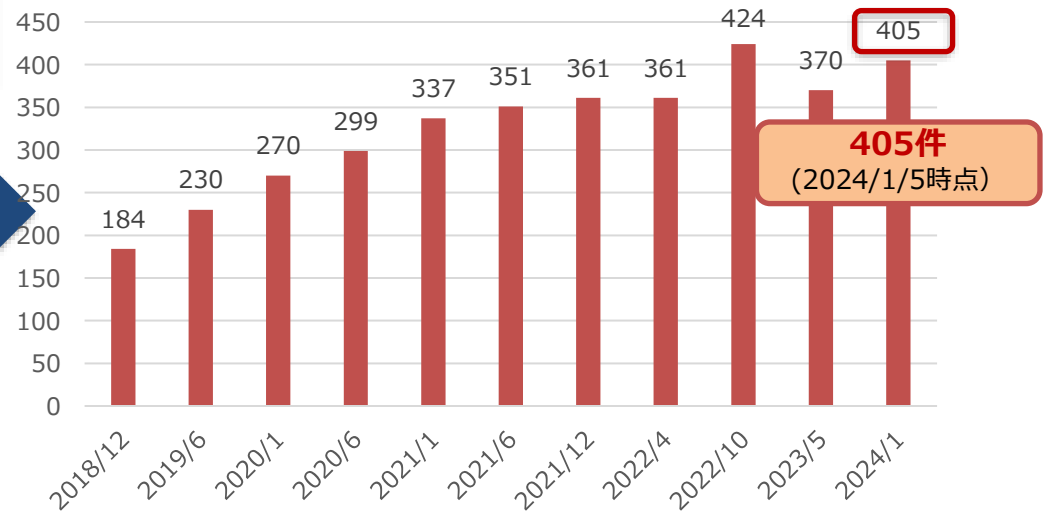
3．制度活用のメリット
登録セキスペの配備が入札要件となる案件の増加

- ✓ 政府CIOポータル内の標準ガイドライン群に掲載されている「デジタル・ガバメント推進標準ガイドライン実践ガイドブック」（注釈1）別紙6章「調達仕様書テンプレート例」（注釈2）において、「調達する作業内容」の「設計・開発」、「運用」、「保守」に**「情報処理安全確保支援士」が例示**されています。
- ✓ 情報処理安全確保支援士の配備が入札要件となる案件が、今後も一定数あることが予測されます。

中小企業庁運営の「官公需情報ポータルサイト」（https://www.kkj.go.jp/s/）



「情報処理安全確保支援士」が記載されている入札情報



（注釈1）「デジタル・ガバメント推進標準ガイドライン実践ガイドブック」とは
標準ガイドライン、標準ガイドライン付属文書及び標準ガイドライン解説書の下位文書として、これまで得られたノウハウや教訓等を盛り込んだ実践的な参考文書。

（注釈2） 別紙6章の記載箇所についての詳細は次のURLをご覧ください。
制度について＞制度活用のメリット＞所属組織のメリット（ITベンダー）https://www.ipa.go.jp/jinzai/riss/katsuyou/benefits.html

3．制度活用のメリット
関連資格取得の優遇（1）

「PCI DSS」の監査人に対する資格要件に登録セキスペが追加

- ✓2020年2月にクレジットカード業界のセキュリティ基準である「PCI DSS」の監査人に対する資格要件に
  登録セキスペが追加されました。
- ✓ 「PCI DSS」は、加盟店やサービスプロバイダにおいて、クレジットカード会員データを安全に取り扱う事を
  目的として策定された、クレジットカード業界のセキュリティ基準です。

QSA資格要件のList A資格項目に、新規の資格が追加されました。
経済産業省の国家資格である**情報処理安全確保支援士（RISS）**が、A資格から選択できるようになっています。

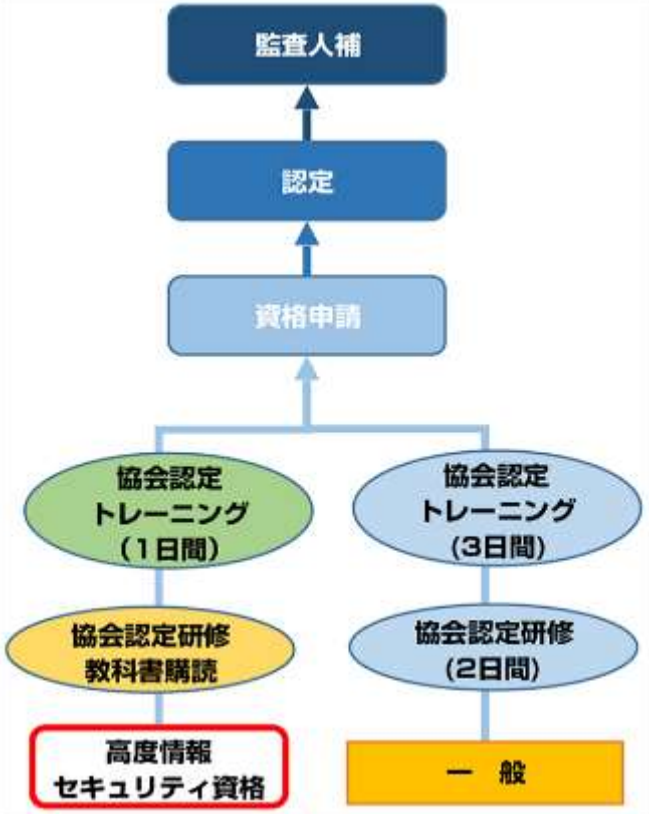
QSAが保持するList A資格がRISSのみの場合は、PCI DSS 評価のすべてを日本のみで実施しなければなりません。現在のところ、QSAはList Aから１つ以上の業界認定資格、およびList Bから1つ以上の資格を保持しなければなりません。

注釈：PCI SSCのサイト（日本語版）より抜粋
https://ja.pcisecuritystandards.org/minisite/env2/

3．制度活用のメリット
関連資格取得の優遇（2）

情報処理安全確保支援士は、情報セキュリティ監査人の業務に携わるための資格取得の優遇制度があります。

– １日のトレーニングで「情報セキュリティ監査人補」の資格取得ができます（通常5日間）
– 筆記試験が免除されます



情報セキュリティ監査人補について

- 情報セキュリティ監査制度（経済産業省）に則り情報セキュリティ監査を行う専門家です。
- 情報セキュリティ監査人補は内部監査を行うことができます。
- 情報セキュリティ監査人補が実務経験に基づき、試験に合格した場合には、公認情報セキュリティ監査人として、外部監査を行うことができます。

詳細は以下をご覧ください：
日本セキュリティ監査協会「高度情報セキュリティ資格特例制度」
http://www.jasa.jp/qualification/info_secure_supporter.html

3．制度活用のメリット

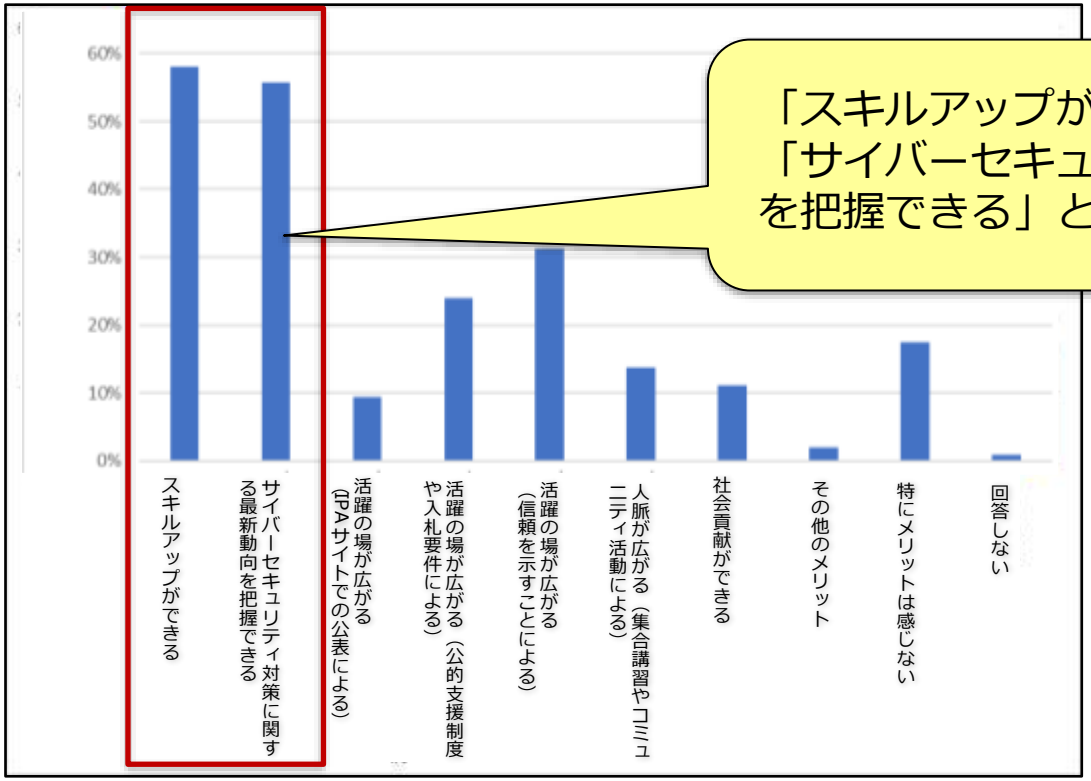
「情報処理安全確保支援士（登録セキスペ）の活動に関する実態調査」調査報告書より①

- IPAでは2018年12月～2019年1月にかけて登録セキスペを対象とした実態調査を行いました。

登録セキスペ制度のメリット

― 登録セキスペと高度IT人材の両方に対し、情報処理安全確保支援士制度への登録によって得られるメリットは何かを確認した（今後実施される可能性もある施策も含めている）。

（設問文：情報処理安全確保支援士への登録によって得られることのうち、あなたにとってメリットとなることをすべて選択してください。なお、選択肢には現在実施されていないが、今後情報処理安全確保支援士を対象に実施される可能性のある施策を含めて挙げています。）



「スキルアップができる」との回答が58%、「サイバーセキュリティ対策に関する最新動向を把握できる」との回答が55.7%であった

IPA「情報処理安全確保支援士（登録セキスペ）の活動に関する実態調査」報告書
P.64「図2-91 メリットとなること（登録セキスペ、高度IT人材）」をもとに作成
https://www.ipa.go.jp/jinzai/riss/reports/reports/gmcbt80000007m1z-att/000076775.pdf

すでに登録している人は、スキルアップや情報収集を最も大きなメリットと考えている。

3．制度活用のメリット

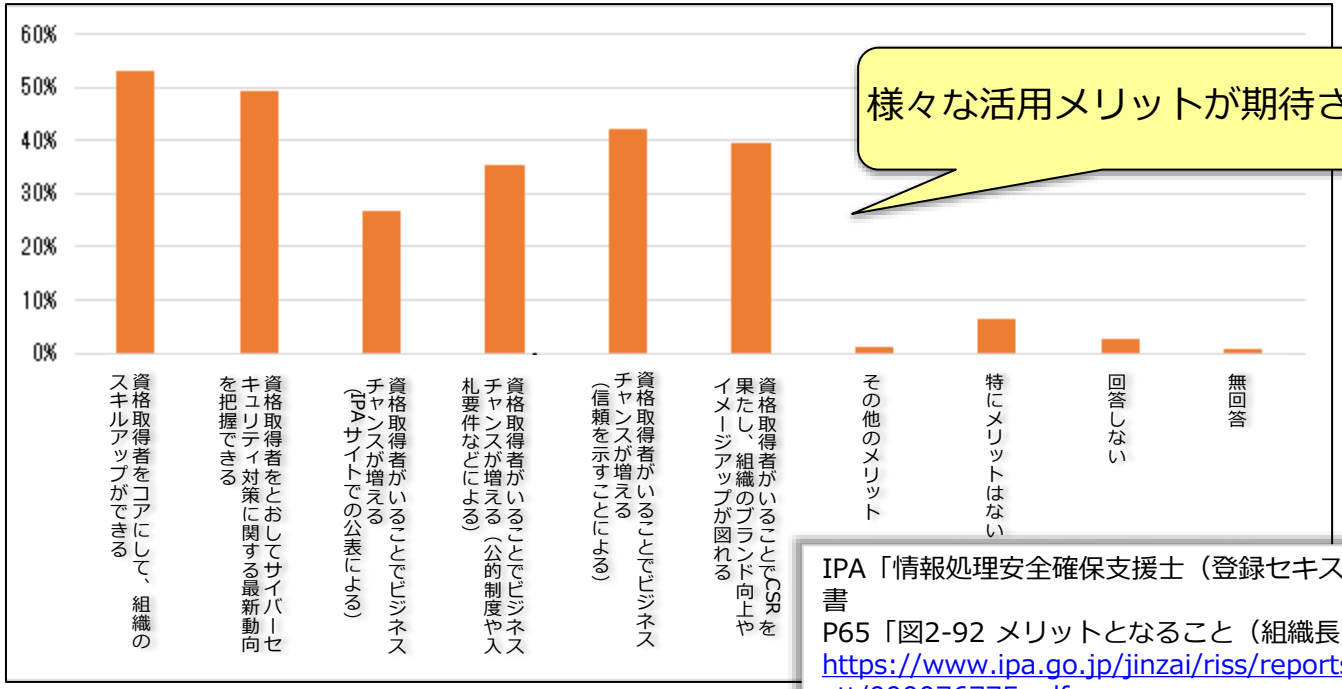
「情報処理安全確保支援士（登録セキスペ）の活動に関する実態調査」調査報告書より②

- IPAでは2018年12月～2019年1月にかけて登録セキスペを対象とした実態調査を行いました。

  組織における登録セキスペの活用メリット

  ― 組織における登録セキスペの活用がメリットとなるかどうかを、組織長に対して確認した。

（設問文：情報処理安全確保支援士への登録によって得られるメリットとして、以下のようなものが想定されています。これらの中であなたが魅力的と感じられるメリットをすべて選択してください。注釈：なお、選択肢には現在実施されていないが、今後情報処理安全確保支援士を対象に実施される可能性のある施策を含めて挙げています。）



様々な活用メリットが期待される

IPA「情報処理安全確保支援士（登録セキスペ）の活動に関する実態調査」報告書
P65「図2-92 メリットとなること（組織長：n=156）」より引用
https://www.ipa.go.jp/jinzai/riss/reports/reports/gmcbt80000007m1z-att/000076775.pdf

組織長からは、制度活用のメリットとして、組織のスキルアップ、サイバーセキュリティ対策に関する　最新動向の把握、ビジネスチャンスの増加、組織のイメージアップなどを期待する意見が多数あり。

3．制度活用のメリット
登録セキスペ、活用企業・組織のインタビュー

登録セキスペインタビュー

サイバーセキュリティ対策の現場で活躍する登録セキスペをご紹介

◇登録セキスペインタビュー
https://www.ipa.go.jp/jinzai/riss/interview/riss.html

<掲載中のインタビュー記事>

・株式会社クロスフェイド 大島 真言様（注釈）
・広島市役所 坂本 昌宏様（注釈）
・株式会社日立システムズ 宇野 文康様（注釈）
・TMI総合法律事務所 寺門 峻佑様（注釈）
・プラスエス代表　大久保 茂人様（注釈）
・株式会社NTTPCコミュニケーションズ 藤ノ原 真雄様
・株式会社群馬銀行 松村 真人様

注釈：一般社団法人 情報処理安全確保支援士会にも所属し、活躍されています
（参考）一般社団法人 情報処理安全確保支援士会
https://www.jp-rissa.or.jp/

様々な分野で多数の登録セキスペが活躍中！

活用企業・組織のインタビュー

登録セキスペ制度を活用している企業・組織をご紹介

中部電力株式会社、中部電力パワーグリッド株式会社
重要インフラ事業者として、サイバーセキュリティは事業を守るための基盤です

他にも活用企業のインタビューを掲載中！

◇活用企業・組織のインタビュー
https://www.ipa.go.jp/jinzai/riss/interview/soshiki/index.html

中部電力株式会社 マネジメントサービス本部 ITシステムセンター
IT基盤・セキュリティグループ副長 鈴木 康人 様（左）
中部電力パワーグリッド株式会社 システム部
統括グループ 副長 長谷川 弘幸 様（右）
（掲載情報はインタビュー当時のものです。）

3．制度活用のメリット
情報処理安全確保支援士ポータルサイトの提供

□情報処理安全確保支援士ポータルサイトの機能（登録セキスペ限定）
- ✓ 登録セキスペに必要な各種オンラインでの手続きや情報の提供、講習の受講などが可能
- ✓ 今後登録セキスペの業務や活動に役立つ情報発信を強化予定

情報処理安全確保支援士ポータルTOP画面

◆各種変更、申請機能
- ・検索サービス公開情報編集
- ・登録情報変更申請
- ・登録更新申請
- ・徽章（バッジ）貸与申請

など

◆各種情報、関連ページへ
- ・講習情報
- ・ロゴマーク利用/徽章貸与について
- ・関連団体情報

など

◆オンライン講習システム

申し込み、受講費支払い/受講/受講状況確認など

◆各種お知らせ（メール配信）
- ・講習受講フォロー
- ・更新のご案内

４．登録状況について

4．登録状況について
年代別、地域別

2024年4月1日時点

情報処理安全確保支援士の登録人数は2024年4月1日時点で　**22,692名**　です。

【年代別】

平均年齢	10代	20代	30代	40代	50代	60代	70代	80代
44.0歳	7名	1,632名	5,541名	9,177名	5,314名	996名	24名	1名
	0.0%	7.2%	24.4%	40.4%	23.4%	4.4%	0.1%	0.0%

【都道府県別】

都道府県	登録者数	割合	都道府県	登録者数	割合	都道府県	登録者数	割合	都道府県	登録者数	割合
北海道	276名	1.2%	千葉県	1,879名	8.3%	京都府	277名	1.2%	香川県	105名	0.5%
青森県	45名	0.2%	神奈川県	4,154名	18.3%	大阪府	1,338名	5.9%	愛媛県	65名	0.3%
岩手県	89名	0.4%	新潟県	113名	0.5%	滋賀県	93名	0.4%	高知県	26名	0.1%
宮城県	253名	1.1%	富山県	128名	0.6%	兵庫県	639名	2.8%	福岡県	498名	2.2%
秋田県	46名	0.2%	石川県	142名	0.6%	奈良県	141名	0.6%	佐賀県	37名	0.2%
山形県	43名	0.2%	福井県	53名	0.2%	和歌山県	43名	0.2%	長崎県	59名	0.3%
福島県	58名	0.3%	山梨県	45名	0.2%	鳥取県	35名	0.2%	大分県	49名	0.2%
東京都	7,280名	32.1%	長野県	163名	0.7%	島根県	48名	0.2%	熊本県	76名	0.3%
茨城県	354名	1.6%	岐阜県	150名	0.7%	岡山県	109名	0.5%	宮崎県	33名	0.1%
栃木県	85名	0.4%	静岡県	236名	1.0%	広島県	211名	0.9%	鹿児島県	30名	0.1%
群馬県	117名	0.5%	愛知県	899名	4.0%	山口県	52名	0.2%	沖縄県	95名	0.4%
埼玉県	1,897名	8.4%	三重県	86名	0.4%	徳島県	39名	0.2%	海外	3名	0.0%

注釈：2024年4月1日時点の「自宅住所」（都道府県）に基づき集計

4．登録状況について
勤務先業種別、登録のきっかけ

【勤務先業種別】

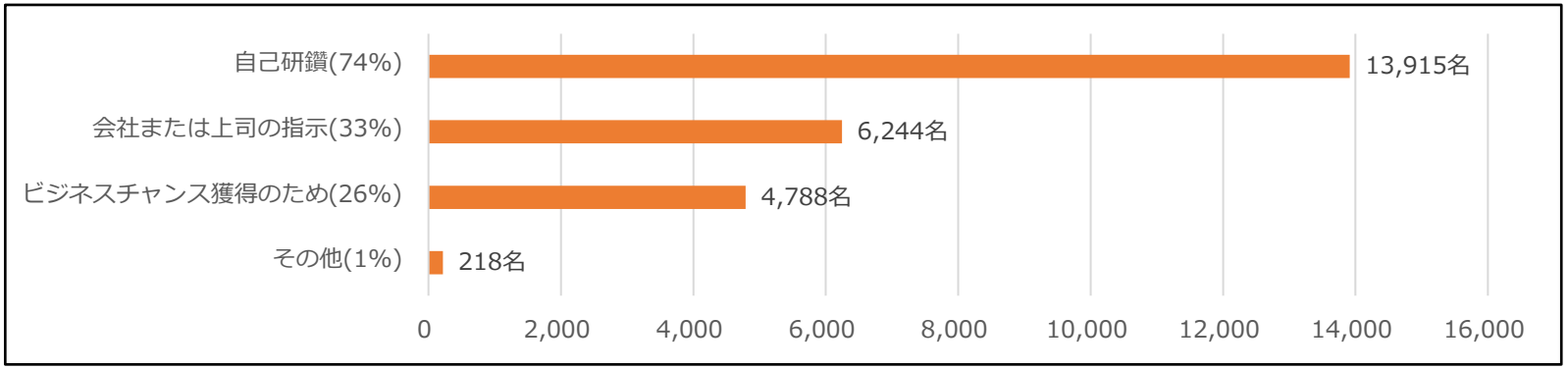
回答者数＝19,170　2024年4月1日時点

勤務先の業種	人数	割合
情報処理・提供サービス業	7,534名	39.3%
ソフトウェア業	4,337名	22.6%
製造業	1,589名	8.3%
運輸・通信業	1,329名	6.9%
サービス業	840名	4.4%
官公庁、公益団体	813名	4.2%
金融・保険業、不動産業	644名	3.4%
コンピュータ及び周辺機器製造又は販売業	612名	3.2%

勤務先の業種	人数	割合
建設業	315名	1.6%
教育（学校、研究機関）	261名	1.4%
卸売・小売業、飲食店	196名	1.0%
電気・ガス・熱供給・水道業	164名	0.9%
医療・福祉業	92名	0.5%
調査業、広告業	41名	0.2%
農業、林業、漁業、鉱業	6名	0.0%
その他（学生、未入力など）	397名	2.1%

【登録のきっかけ】

回答者数＝18,762、複数回答可



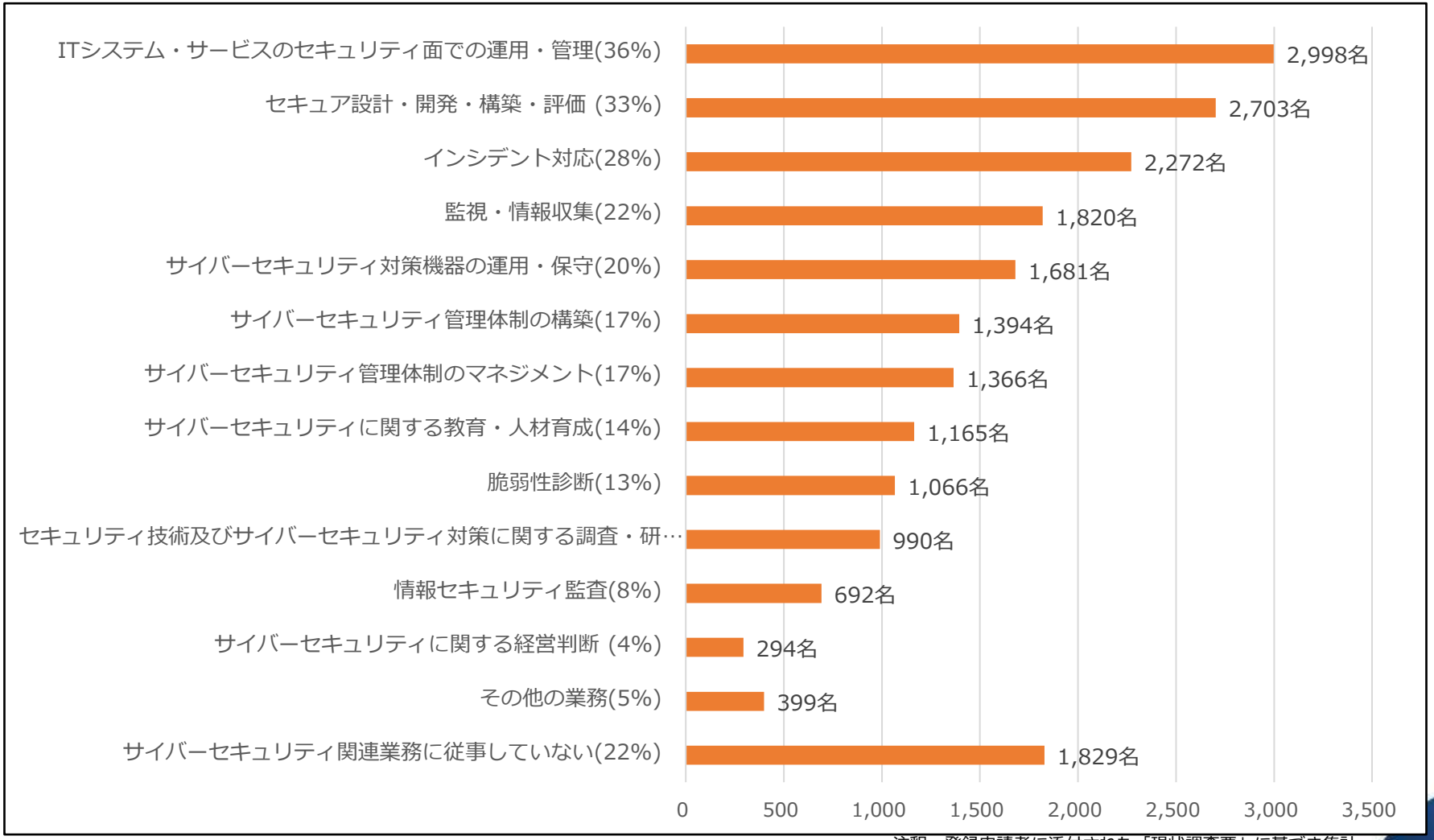
注釈：登録申請者に添付された「現状調査票」に基づき集計。
2017年6月以降の申請者のみ（回答は任意）

4．登録状況について
担当セキュリティ関連業務

【担当セキュリティ関連業務】

回答者数=8,234、複数回答可

2024年4月1日時点



注釈：登録申請者に添付された「現状調査票」に基づき集計。
2019年9月以降の申請者のみ（回答は任意）

関連URL

- **「情報処理の促進に関する法律の一部を改正する法律」（令和元年法律第67号）が施行されました**　プレスリリース日：令和2年5月15日
  https://www.meti.go.jp/press/2020/05/20200515001/20200515001.html
- **情報処理安全確保支援士（登録セキスペ）制度の見直しについて**
  https://www.ipa.go.jp/jinzai/riss/seido/kaisei.html
- **12月6日公布の法律改正に伴う情報処理安全確保支援士制度の見直しを公表**
  https://www.ipa.go.jp/archive/press/2019/press20191212_3.html　プレスリリース日：令和元年12月12日
- **情報処理の促進に関する法律の一部を改正する法律　令和元年12月6日**
  https://kanpou.npb.go.jp/old/20191206/20191206g00178/20191206g001780014f.html
- **試験ワーキンググループ中間取りまとめ　～情報処理安全確保支援士制度～平成28年4月**
  産業構造審議会商務流通情報分科会　情報経済小委員会　試験ワーキンググループ
  http://www.meti.go.jp/committee/sankoushin/shojo/johokeizai/shiken_wg/pdf/report_01_01_00.pdf
- **セキュリティ人材の確保に関する研究会 中間報告　平成27年8月**
  https://www.meti.go.jp/shingikai/sankoshin/shomu_ryutsu/joho_keizai/pdf/006_s01_00.pdf

まとめ

情報処理安全確保支援士

サイバーセキュリティ分野初の登録制の国家資格として2016年10月に誕生しました。

サイバーセキュリティに関する**専門的な知識・技能**を活用して企業や組織における**安全な情報システムの企画・設計・開発・運用**を支援し、また、**サイバーセキュリティ対策の調査・分析・評価**を行い、その結果に基づき**必要な指導・助言**を行うことを想定しています。

現在、2万人以上の情報処理安全確保支援士が様々な分野で活躍しています

個人としても、組織としても、情報処理安全確保支援士制度をご活用ください

情報処理安全確保支援士に関する詳細や手続きについて、
IPAのホームページでご案内しています。

https://www.ipa.go.jp/jinzai/riss/index.html

制度に関するお問い合わせ

IPA　デジタル人材センター　国家資格・試験部

登録・講習グループ

E-mail: riss-info@ipa.go.jp