経済産業省

実務経験者に対する講習制度（案）

–情報処理安全確保支援士の新たな講習制度の創設について–

令和７年12月25日

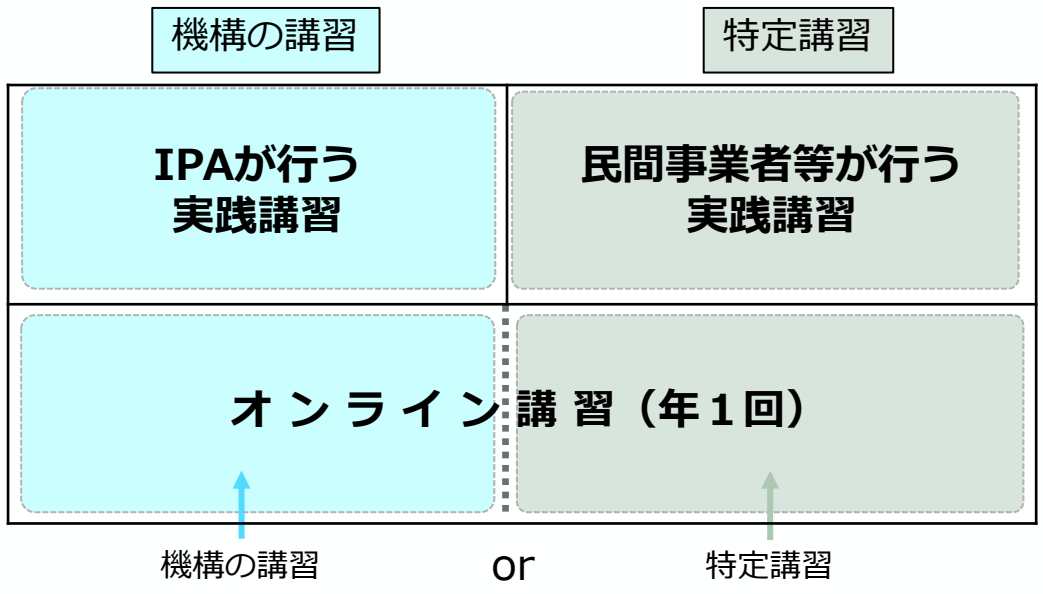
商務情報政策局サイバーセキュリティ課

実務経験者に対する講習制度創設の背景

- サイバーセキュリティ分野で必要とされる知識が技術の進歩により変化している中、**情報処理安全確保支援士には、サイバーセキュリティの専門家としてその知識や技能を最新の状態としておくために、講習受講が課せられている。**
- 一方、情報処理安全確保支援士の中には、**実践講習で得られる知識・技能と同等以上の知識・技能を、企業のサイバーセキュリティ対策の支援等の実務を通じて得られるケース**がある。
- また、更新制度が実施されている中で、**実務から遠のいている情報処理安全確保支援士を実務に向かわせるインセンティブを設定**することが、情報処理安全確保支援士の一層の活用促進、ひいては事業者のサイバーセキュリティ対策向上に資する。

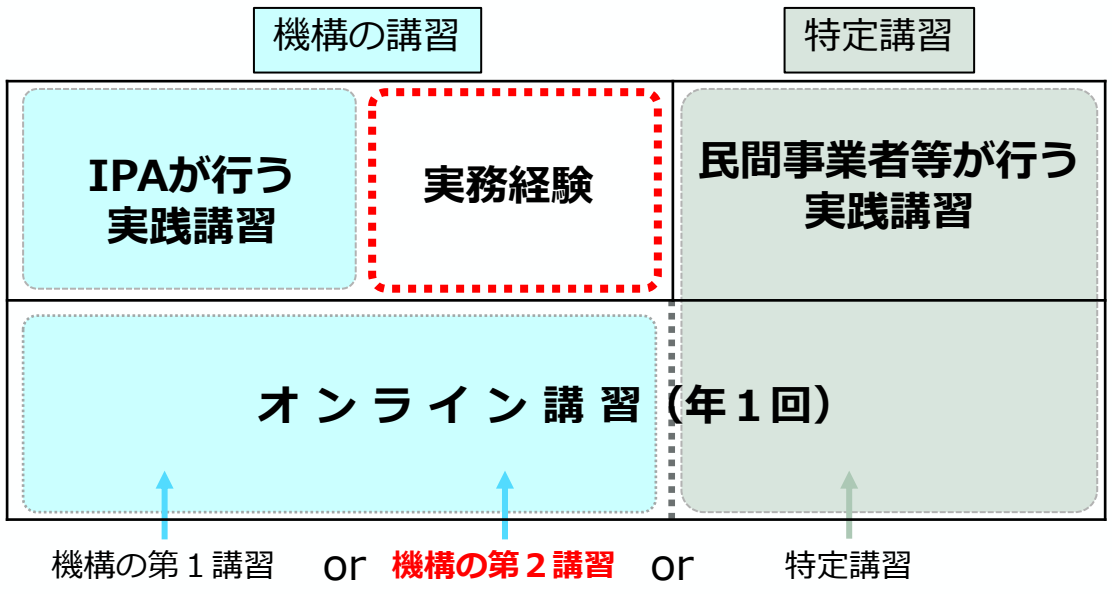
このような講習制度や情報処理安全確保支援士の実務の実態を踏まえ、**実務経験から、講習から習得できる知識・技能と同等以上の知識・技能を得ている情報処理安全確保支援士に対して、受講すべき講習をオンライン講習のみとする、新たな講習制度を創設。**

【現行】



【いずれかを選択して受講】

【見直し後】



【いずれかを選択して受講】

実務経験者に対する講習制度の概要

実務経験者に対する講習制度とは、**下表の実務経験を積んでいる情報処理安全確保支援士に向けた新たな講習制度**であり、具体的には、当該情報処理安全確保支援士が受講する講習をオンライン講習のみとするもの。

実践講習として求める要素

・ＩＴスキル標準レベル４相当（一つまたは複数の専門を獲得したプロフェッショナルとして、専門スキルを駆使し、業務上の課題の発見と解決をリードするレベル、プロフェッショナルとして求められる、経験の知識化とその応用（後進育成）に貢献するレベル）

・情報処理安全確保支援士試験の出題分野の内容を含む

～ 特定講習（※）募集等要領（抜粋）～　　（※民間事業者等が行う実践講習部分を指す）
・・・特定講習は「ＩＴスキル標準レベル４相当」とし・・・登録セキスペの知識・技能の継続的な維持・向上を図り、実践的な活用力を修得 できるものであることが必要なため、特定講習が対象とする科目は、「情報処理安全確保支援士試験」の出題分野の内容を含むこと・・・

実務経験者に対する受講制度の対象となる実務の方向性

○ＩＴスキル標準レベル４に相当する、情報処理安全確保支援士試験の出題科目に該当するもの
○上記以外で、実務経験者に対する講習制度の対象とすることが望ましいもの
から、ＩＰＡ有識者検討会での議論を踏まえて以下のとおり決定

○ＩＴスキル標準レベル４相当の情報処理安全確保支援士試験の出題科目に該当するもの

対象業務	情報処理安全確保支援士試験出題科目の該当項目
セキュリティ監査／システム監査 セキュリティ統括	1．情報セキュリティマネジメントの推進又は支援に関すること
デジタルシステムストラテジー デジタルシステムアーキテクチャ デジタルプロダクト開発 デジタルプロダクト運用	2．情報システムの企画・設計・開発・運用でのセキュリティ確保の推進又は支援に関すること 3．情報及び情報システムの利用におけるセキュリティ対策の適用の推進又は支援に関すること
脆弱性診断・ペネトレーションテスト セキュリティ監視・運用 セキュリティ調査分析・研究開発	2．情報システムの企画・設計・開発・運用でのセキュリティ確保の推進又は支援に関すること 3．情報及び情報システムの利用におけるセキュリティ対策の適用の推進又は支援に関すること 4．情報セキュリティインシデント管理の推進又は 支援に関すること
※いずれも、一定期間（６か月/１年）の従事期間を満たした場合に限る。	

○左表以外で実務経験者に対する講習制度の対象とするもの

対象業務	採用理由
セキュリティ経営 デジタル経営	特定講習 募集等要項(*) 別表１において講習の対象外とされる「経営層」について、ITSS＋（セキュリティ領域）分野に従い、左表の従事期間を満たすことで実践講習と同等の役割があると判断
情報セキュリティ規程の整備 情報資産の洗い出しとリスク分析 クラウドサービスの安全利用 セキュリティインシデント対応 従業員向け情報セキュリティ教育	「中小企業向けサイバーセキュリティ対策支援者リスト」に掲載される者が、左記指導テーマに基づく支援業務として、３回以上の中小企業への支援実績がある場合に限り、実践講習と同等と判断
ＩＰＡまたは民間事業者等が行う実践講習の講師	講師として２回以上登壇した場合に限り、実践講習と同等と判断

*出典： 経済産業省「情報処理安全確保支援士特定講習」募集等要領 別表１ https://www.meti.go.jp/policy/it_policy/jinzai/bosyuu250922.pdf

実務経験者と認定されるための要件（案）

① 下表の「具体的業務」について、「認定基準」以上の実務経験を積み「評価者からの証明」を受けること。

② 登録・更新を受けた日から２年を経過していること。

③ 上記を満たした上でIPAに申請し認定を受けること（申請の受付は令和８年４月１日から開始予定）。

対象実務	具体的業務	認定基準 （従事回数/従事期間）	認定基準の評価者 （証明する者）
ITSS＋（セキュリティ領域）に定めるサイバーセキュリティに関係する実務	・セキュリティ経営 ・セキュリティ監査 ・システム監査 ・セキュリティ統括 ・脆弱性診断・ペネトレーションテスト ・セキュリティ監視・運用 ・セキュリティ調査分析・研究開発	従事期間**６か月**以上	法人所属として受けた業務 ：企業内の上長 個人として受けた業務 ：顧客
	・デジタル経営 ・デジタルシステムストラテジー ・デジタルシステムアーキテクチャ ・デジタルプロダクト開発 ・デジタルプロダクト運用	従事期間**１年**以上	法人所属として受けた業務 ：企業内の上長 個人として受けた業務 ：顧客
「中小企業向けサイバーセキュリティ対策支援者リスト」（※１）に掲載される指導テーマに基づく支援業務	以下テーマに基づく中小企業に対するマネジメント指導 （今後、セキュリティアセスメントに関するテーマ（※２）を追加予定） ・「情報セキュリティ規程の整備」 ・「情報資産の洗い出しとリスク分析」 ・「クラウドサービスの安全利用」 ・「セキュリティインシデント対応」 ・「従業員向け情報セキュリティ教育」	支援業務件数 **３件**以上	顧客
実践講習の講師として登壇する実務	・IPAまたは民間事業者等が行う実践講習の講師	登壇回数**２回**以上	事業者（講師の上長）

（※１）中小企業がサイバーセキュリティ対策の相談先を見つける際に活用できるよう、中小企業支援が可能な情報処理安全確保支援士を可視化したリスト。リストには、各情報処理安全確保支援士の得意分野や専門領域に加え、中小企業支援にあたってIPAが設定した５つのセキュリティマネジメント指導テーマを掲載。

（※２）「サプライチェーン強化に向けたセキュリティ対策評価制度」における三つ星の要求事項・評価基準について、中小企業の適合可否の評価と助言を行うことを念頭にしたもの

（参考）対象となるITSS＋（セキュリティ領域）分野とタスク等の対応

	分野名	セキュリティ関連タスクの例	担当部署／機能の例
経営層	セキュリティ経営（CISO）	セキュリティ意識啓発、対策方針の指示、 セキュリティポリシー・予算・対策実施事項の承認 等	経営者、経営層（CISOを含む）
	デジタル経営（CIO/CDO）		
戦略マネジメント層	セキュリティ監査	セキュリティ監査、報告・助言 等	監査部門 セキュリティベンダー・監査法人（セキュリティ監査サービス）
	システム監査	システム監査、報告・助言 等	監査部門 ITベンダー・監査法人（システム監査サービス）
	セキュリティ統括	セキュリティ教育・普及啓発、セキュリティ関連の講義・講演、 セキュリティリスクアセスメント、 セキュリティポリシー・ガイドラインの策定・管理・周知、 警察・官公庁等対応、社内相談対応、インシデントハンドリング 等	セキュリティ専門部門、CSIRT セキュリティ委員会 IT・デジタル部門のセキュリティ対策機能
	デジタルシステムストラテジー	デジタル事業戦略立案、システム企画、要件定義・仕様書作成、 プロジェクトマネジメント 等	経営企画部門、IT企画部門、IT・デジタル部門の企画機能 IT/セキュリティコンサルタント
実務者・技術者層	脆弱性診断・ペネトレーションテスト	脆弱性診断、ペネトレーションテスト 等	IT・デジタル部門の運用機能、IT子会社 セキュリティベンダー（脆弱性診断サービス）
	セキュリティ監視・運用	セキュリティ製品・サービスの導入・運用、 セキュリティ監視・検知・対応、インシデントレスポンス、 連絡受付 等	IT・デジタル部門の運用機能、IT子会社 セキュリティベンダー（セキュリティ監視・運用サービス）
	セキュリティ調査分析・研究開発	サイバー攻撃捜査、原因究明・フォレンジック、マルウェア解析、 脅威・脆弱性情報の収集・分析・活用、 セキュリティ理論・技術の研究開発、セキュリティ市場動向調査 等	CSIRT/IT・デジタル部門のリサーチ機能、IT子会社 セキュリティベンダー（デジタルフォレンジックサービス）
	デジタルシステムアーキテクチャ	セキュアシステム要件定義、セキュアシステムアーキテクチャ設計、セキュアソフトウェア方式設計、テスト計画 等	IT・デジタル部門の設計機能、IT子会社 IT/OTベンダー
	デジタルプロダクト開発	基本設計、詳細設計、セキュアプログラミング、テスト・品質保証、パッチ開発 等	IT・デジタル部門の開発・保守機能、IT子会社 IT/OTベンダー
	デジタルプロダクト運用	構成管理、運用設定、利用者管理、サポート・ヘルプデスク、 脆弱性対策・対応、インシデントレスポンス 等	IT・デジタル部門の運用機能、IT子会社 IT/OT/セキュリティベンダー

従事期間６か月以上を認定基準とするもの

従事期間１年以上を認定基準とするもの

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 Ver2.0 付録F　サイバーセキュリティ体制構築・人材確保の手引き
図表12　17分野のサイバーセキュリティ関連タスクと担当部署の割り当て例　https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf