中国経済産業局委託事業

令和2年度中小企業サイバーセキュリティ対策促進事業
（中国地域におけるセキュリティコミュニティ形成事業）

公開用資料

令和3年3月

公益財団法人中国地域創造研究センター

白　紙

目　次

白　紙

１．事業目的

IT や IoT の利活用は中小企業等の生産性向上に不可欠なものとなっている一方で、企業等が保有する顧客の個人情報や重要な技術情報等を狙うサイバー攻撃は増加傾向にあり、その手口は巧妙化している。また、新型コロナウイルス対応の一環でテレワーク等の業務のデジタル化が急速に進む中、セキュリティ投資に予算を割くことができず十分な対策がとれていない中小企業等にとって、サイバー攻撃の脅威はより一層増大している。

このようにセキュリティ対策の重要性が高まっている中、特に地方においては首都圏等と比較してサイバーセキュリティに関する情報格差や圧倒的な人材不足等が課題として指摘されているところであり、こうした課題に対応するため、地域の企業や業界団体、大学、支援機関、行政機関等との連携体制を構築すること、また、企業活動の現場においてセキュリティ対策の中核を担える人材を効果的かつ中長期的に育成できる体制の構築が必要となっている。

本事業は、セキュリティコミュニティ形成の促進及び企業のセキュリティ人材育成のための実証事業を行うことにより、中国地域におけるサイバーセキュリティに対する機運醸成とレベル向上を図ることを目的とする。

２．サイバーセキュリティ実態調査

２．１．アンケート・ヒアリング調査

中国地域の企業に対し、サイバーセキュリティに対する意識・課題、対応状況を中心にアンケート調査を行うとともに、アンケート回答企業に対し、ヒアリング調査を行った。

２．１．１．中小企業に対するアンケート調査

ａ．調査目的

地域におけるセキュリティ分野での連携および中核人材育成体制の構築のための基礎資料とするため、地域中小企業の情報セキュリティリスクの認識、社内体制、セキュリティ人材の育成・確保状況等について把握する。

ｂ．対象と方法

中国地域において過去に経済産業省の補助事業（過去３年間の中小企業庁「ものづくり補助金[1]」）を実施した企業　1,002 社を対象先に選定した。

調査は調査票を上述の企業に郵送で配布し、郵送またはインターネット回答により回収した。

ｃ．実施概要

・調査期間　　2020 年 10 月 9 日～10 月 29 日
・調査対象数　　1,002 件
・有効回答数　　363 件（有効回答率 36.2%）

[1] 「ものづくり・商業・サービス経営力向上支援補助金」、「ものづくり・商業・サービス生産性向上促進補助金」、「ものづくり・商業・サービス高度連携促進補助金」

ｄ．回答結果　概要

Ⅰ．回答企業の属性

・中国地域における過去３年間の中小企業庁「ものづくり補助金」採択企業に送付。回答率は 36.2%

・回答者の内訳は製造業：非製造業＝２：１。従業員 50 人未満の企業が約８割

Ⅱ．情報セキュリティリスクの認識

・情報セキュリティ対策の必要性の認知は約 84.7%。企業規模が大きいほど認知度は高まる

・懸念している情報セキュリティリスクは「情報漏えい」「サイバー攻撃」の順番。企業規模が大きくなれば、加えて「業務の停止」「企業イメージ・信用力低下」も懸念

・情報セキュリティ対策の実施企業は 84.8%であり、「必要性の認知」とほぼ同等。具体的には「アンチウイルスソフトの導入」「ファイアウォール[2]・UTM（Unified Threat Management）[3]等の機器の導入」等の技術的対応が目立ち、企業規模が小さいほど企業内での体制整備、人材育成は遅れがち

・情報セキュリティ対策における主たる課題は「人材・予算の不足」。企業規模が大きくなれば「他に優先順位が高い経営課題がある」「対策の効果測定が難しい」の割合が高まる

Ⅲ．情報セキュリティ体制

・情報セキュリティ担当者がいる企業は 43.2%。そのうち専任担当者の配置企業は全体の 6.1%。配置してない理由は「適任者がいない」「業務多忙のため対応できない」など

・情報セキュリティ年間経費は「10 万円未満」が 46.2%、「50 万円未満」が 80.1%。情報セキュリティにかける費用は企業規模の影響が大きい

・情報セキュリティに関する情報収集を行っている企業は 68.5%。収集手段は「Web サイト」「コンサルタント・社外専門家」が多い。企業規模が大きくなれば「セミナー・シンポジウム・勉強会」「メールマガジン」の割合が高まる

・情報セキュリティに関して知りたい情報は約８割の企業が「攻撃を受けた際の対処方法」「攻撃の種類・内容」を回答。企業規模が大きくなれば「社員の教育・研修・訓練方法」「セキュリティポリシーの策定方法」の割合が高まる

Ⅳ．情報セキュリティに関する被害

・情報セキュリティ関連の被害に遭ったことのある企業は 15.2%。被害の多くは近年流行している「標準型メール攻撃」「不正送金を促すビジネスメール詐欺やフィッシング

[2] 社内・外部ネットワークとの間に立って、不正なアクセスから社内ネットワークを守る機器
[3] ネットワークに関連するセキュリティ機能を統合して、１つのハードウェアに組み込んだ機器

サイト」などであり、制御システムやIoTデバイスへの攻撃は希少
・被害金額は「わからない」が約半数、「10万円未満」が43.1%
・被害時の相談先がない企業は18.7%。企業規模が小さくなるほど相談先がない企業の割合が高まる。企業規模の大きい企業は「取引先IT企業」を中心に対応。次いで「警察」「商工会議所等支援団体」の順

Ⅴ. 情報セキュリティ人材の育成・確保

・情報セキュリティに関する教育を実施している企業は17.4%。必要な能力・スキルの整理を行っている企業はそのうちの約2/3。実施状況は企業規模の影響が大きい
・人材育成・教育上の課題は「教育のための時間確保が難しい」「能力・スキル要件がわからない」などが上位
・小規模企業（従業員9人未満の企業）での情報セキュリティ教育の実施比率は9.0%であり、課題のないとする企業が40%以上となっている。教育実施比率の高い大規模企業では「魅力的な外部教育・研修サービスがない」等の課題の割合が高まる
・セミナー・講座に関して「習得できるスキル」「対象・レベル」などの情報が分かりやすく提供されれば（いわゆる「セキュリティ講座マップ」）、約半数が役立つと回答

Ⅵ. テレワークと情報セキュリティ

・現在、テレワーク実施企業は18.5%。そのうち新型コロナウイルス感染症流行以前からの実施企業は全体の5.3%。実施割合は企業規模により大きな影響を受ける
・テレワークに関しては会社端末を利用している企業が全体の33.3～54.5%で多数派。一方、個人端末を利用して実施している企業は7.6～22.7%。テレワークを実施に伴い情報セキュリティへの不安が増加した企業は34.8%
・テレワーク開始にあたり、「新たな設備、ソフトウェアの導入」「社員への教育」などを実施している企業もある

Ⅶ. 情報セキュリティレベルの向上のための施策・サポート

・情報セキュリティのレベル向上の施策・サポートとしては「経営者の情報セキュリティ意識向上」「従業員の情報セキュリティ意識向上」が最優先。次いで双方に対する「セキュリティ対策の教育」「対策費用等への補助制度の充実」の割合が高い。小規模企業では「地域での人材育成・確保、教育サポート体制の充実」にも期待
・情報セキュリティに関する自由記述では「セキュリティに関するセミナー・勉強会」「（IT補助金同様の）セキュリティ投資に対する支援」「セキュリティ相談・対応窓口の設置」「セキュリティソフトの無料配布」などを求める意見が複数みられる。また、小規模企業にとって情報セキュリティ人材の確保は困難との声もあり、担当者不在でも対応が可能な体制づくりも期待される

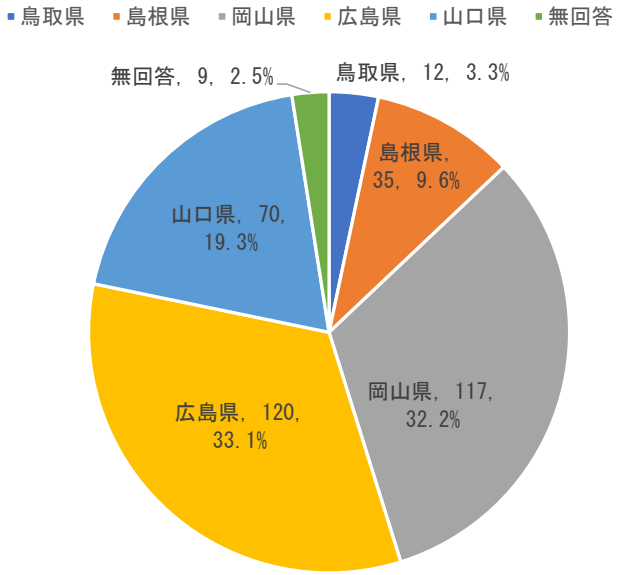
ｅ．回答結果

Ⅰ．回答企業の属性

問１．貴社の概要についてご記入ください
①所在地　（ｎ＝363）

所在地は「広島県」（33.1%）が最も多く、次いで「岡山県」（32.2%）、「山口県」（19.3%）となっている（図表２．１）。

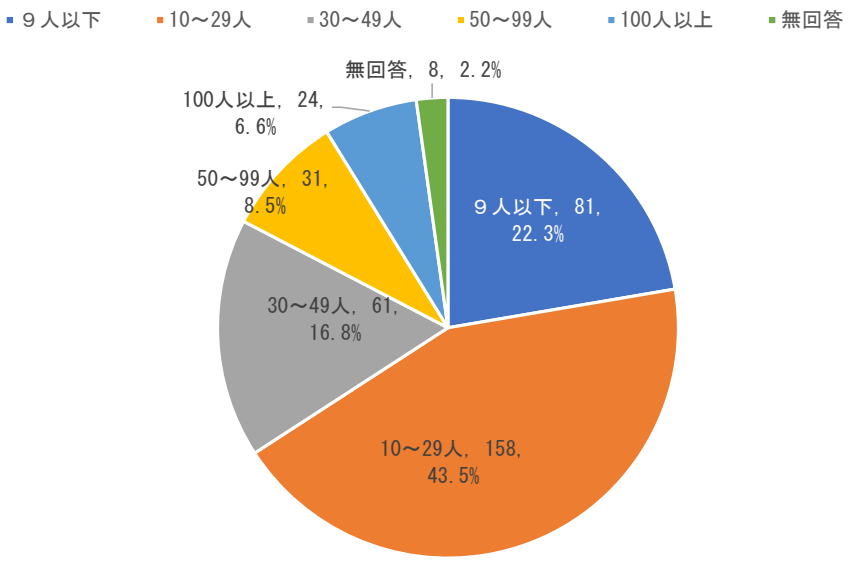
図表２．１　所在地



②従業員数　（ｎ＝363）

従業員数は「10～29人」（43.5%）が最も多く、次いで「９人以下」（22.3%）となっている。30人未満で約2/3を占めている（図表２．２）。

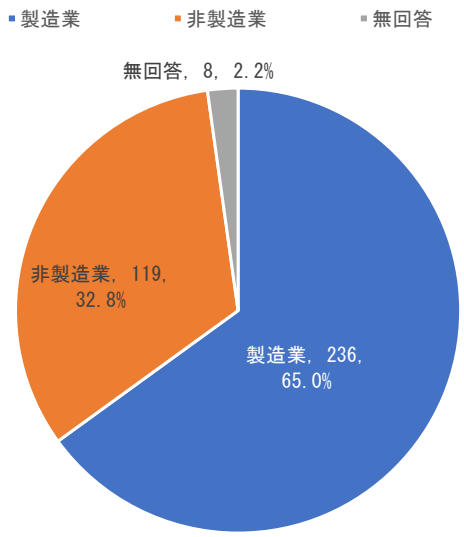
図表２．２　従業員数



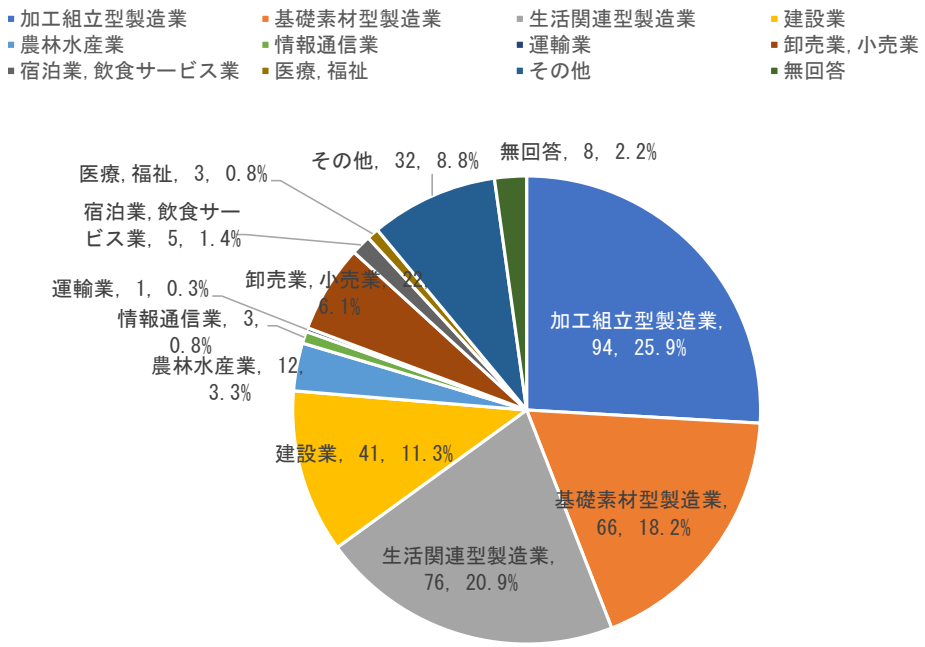
③業種　（ｎ＝363）

業種は「製造業」(65.0%) が約 2/3 である（図表２．３)。「製造業」の中では「加工組立型」(25.9%)、「生活関連型」（20.9%)、「基礎素材型」（18.2%）の順番となっている（図表２．４)。

図表２．３　業種【製造業・非製造業】



図表２．４　業種【詳細】

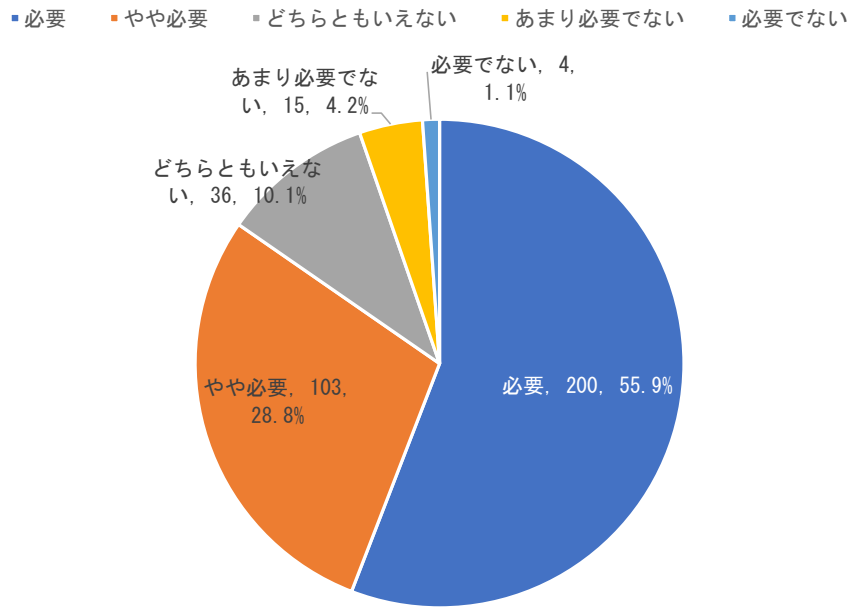


Ⅱ．情報セキュリティリスクの認識

問２．貴社において情報セキュリティ対策の必要性について、あてはまるものを１つだけ選んで○をおつけください　（ｎ＝358）

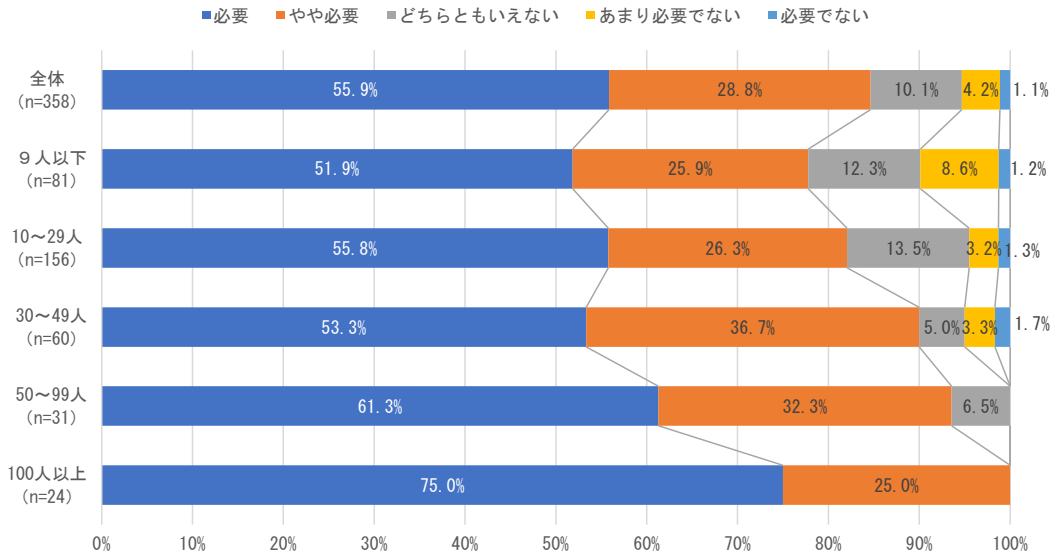
情報セキュリティ対策の必要性については「必要」（55.9%）、「やや必要」（28.8%）を合わせて 84.7%の企業が必要性を認識している。一方、「必要でない」（1.1%）、「あまり必要でない」（4.2%）を合わせると 5.3%となる（図表２．５）。

図表２．５　情報セキュリティ対策の必要性【全体】



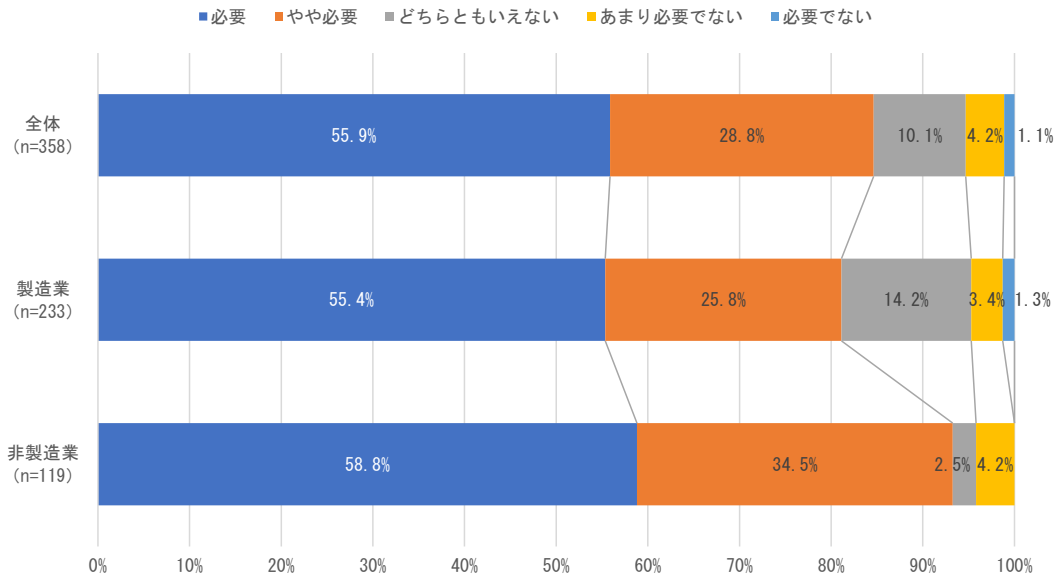
従業員数別にみると、規模が大きくなるほどその必要性（「必要」＋「やや必要」）の認識が高まる。従業員数「９人以下」で 77.8%であるが、「100 人以上」では 100.0%となっている（図表２．６）。

図表２．６　情報セキュリティ対策の必要性【従業員数別】



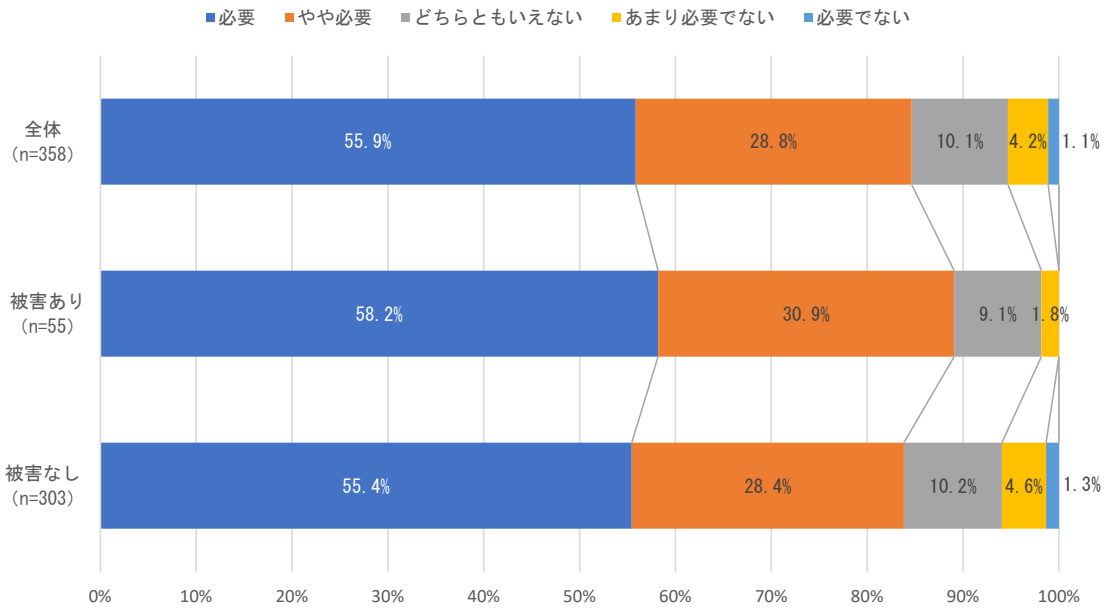
業種別に情報セキュリティ対策の必要性（「必要」＋「やや必要」）の認識では、「非製造業」（93.3%）が「製造業」（81.2%）を上回っている（図表２．７）。

図表２．７　情報セキュリティ対策の必要性【業種別】



被害状況別に情報セキュリティの必要性の認識をみると、「被害あり」（89.1%）が「被害なし」（83.8%）であり、大きな差異はみられなかった（図表２．８）。

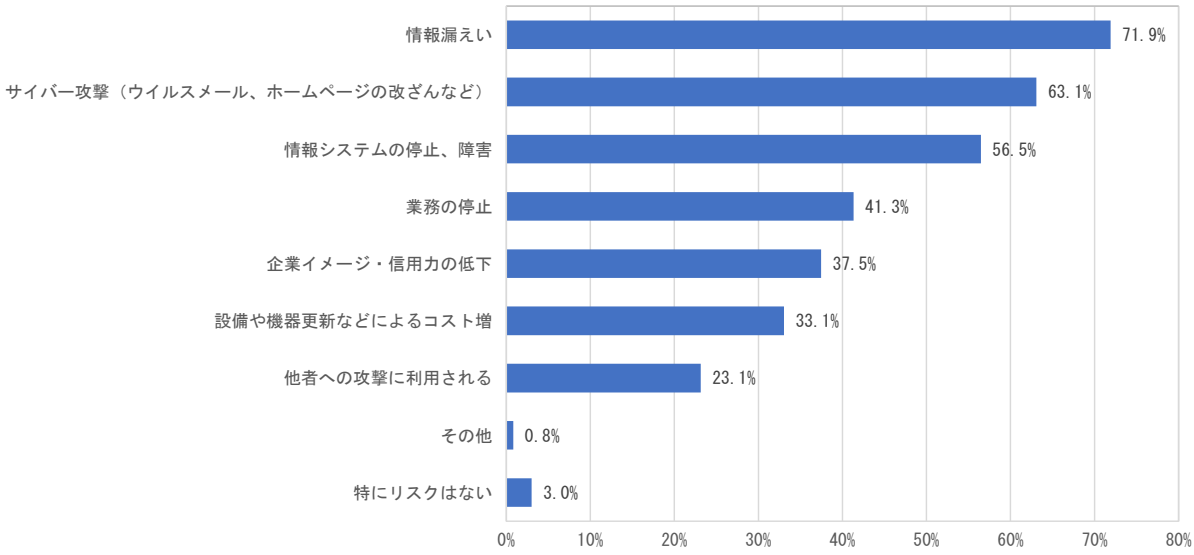
図表２．８　情報セキュリティ対策の必要性【被害状況別】



問３．貴社において情報セキュリティに関連して懸念しているリスクについて、あてはまるものをすべて選んで○をおつけください　（ｎ＝363）

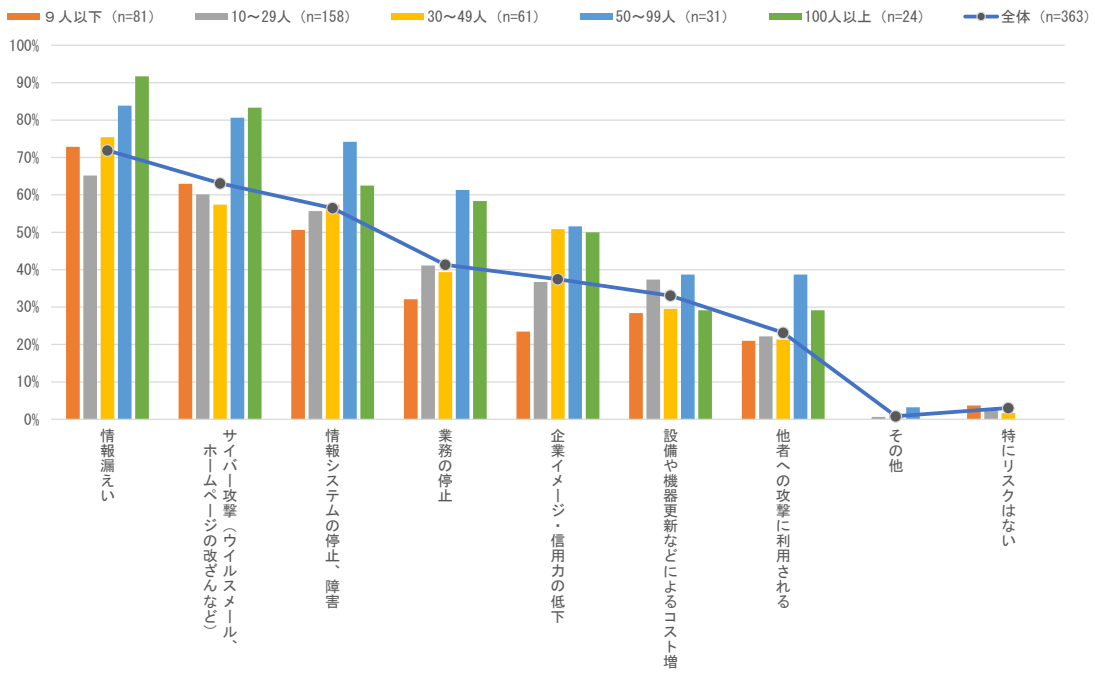
情報セキュリティに関して懸念されるリスク（複数回答）については「情報漏えい」（71.9%）、「サイバー攻撃（ウイルスメール、ホームページの改ざんなど）」（63.1%）、「情報システムの停止、障害」（56.5%）が上位を占めている（図表２．９）。

図表２．９　情報セキュリティに関するリスク【全体】（複数回答）



従業員数別にみると、各リスクにおいて概ね企業規模が大きくなるほど懸念する割合が高まる。特に「情報漏えい」「サイバー攻撃（ウイルスメール、ホームページの改ざんなど）」「業務の停止」の割合が高まる（図表２．10）。

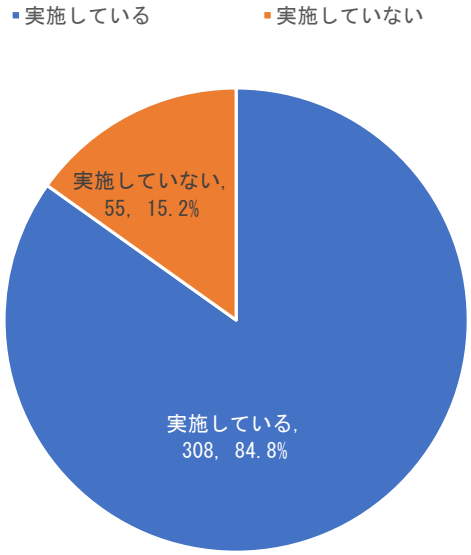
図表２．10　情報セキュリティに関するリスク【従業員数別】（複数回答）



問４．貴社において情報セキュリティ対策として実施している内容について、あてはまるものをすべて選んで○をおつけください　（ｎ＝363）

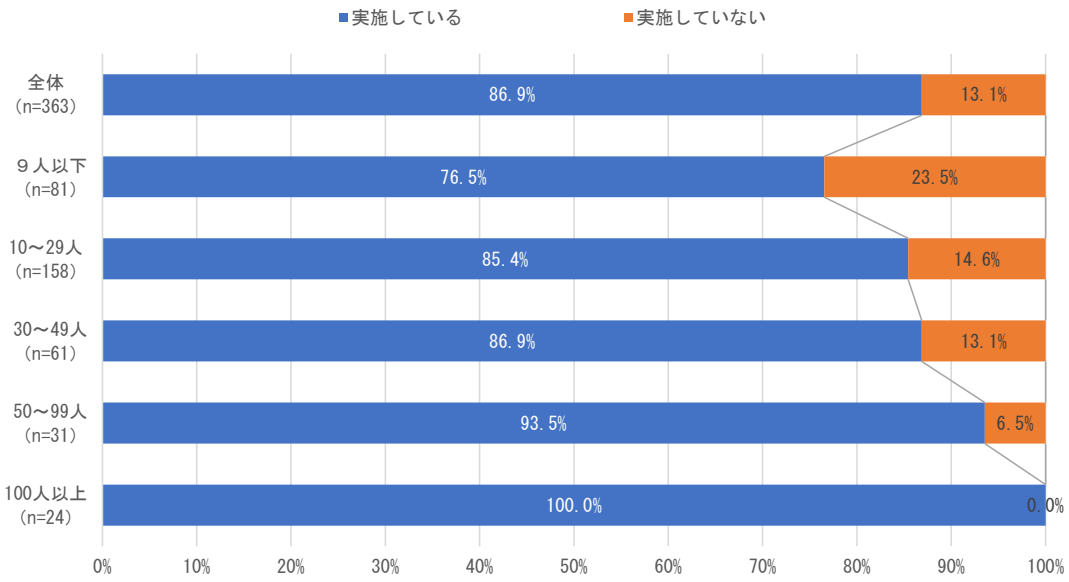
情報セキュリティ対策の実施状況は、「実施している」企業が全体の 84.8%となっている（図表２．11）。この実施率は問２の情報セキュリティの必要性の認知度（84.7%）とほぼ同じである。

図表２．11　情報セキュリティ対策の実施状況【全体】



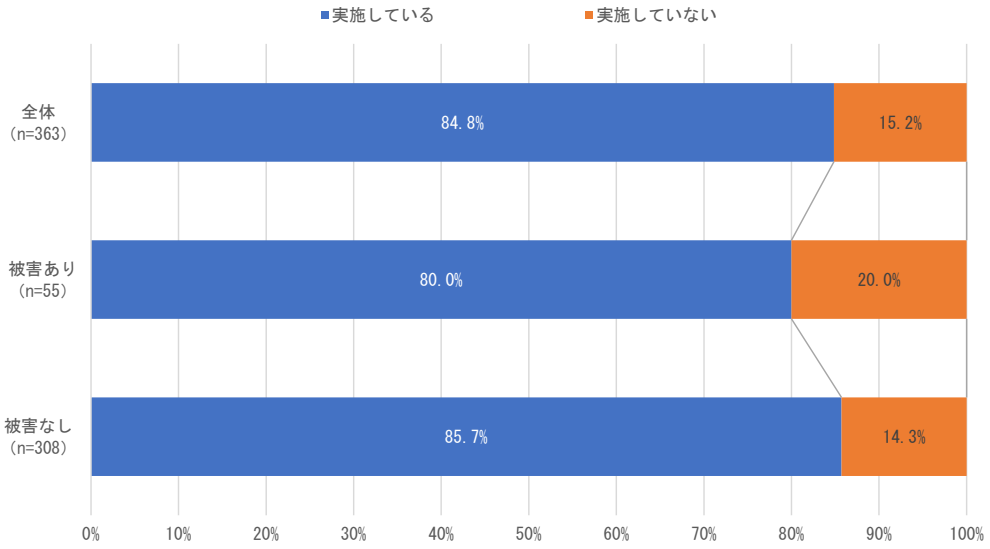
従業員数別にみると、企業規模が大きくなるほど対策の実施率が高まる。従業員数「９人以下」の企業の実施割合は 76.5%であるが、「100 人以上」では 100.0%となっている（図表２．12）。

図表２．12　情報セキュリティ対策の実施状況【従業員数別】



被害状況別にみると、過去に「被害あり」企業の実施率（80.0%）が「被害なし」企業の実施率（85.7%）を下回っている（図表２．13）。過去の被害経験が対策に十分に反映されていない状況がうかがえる。

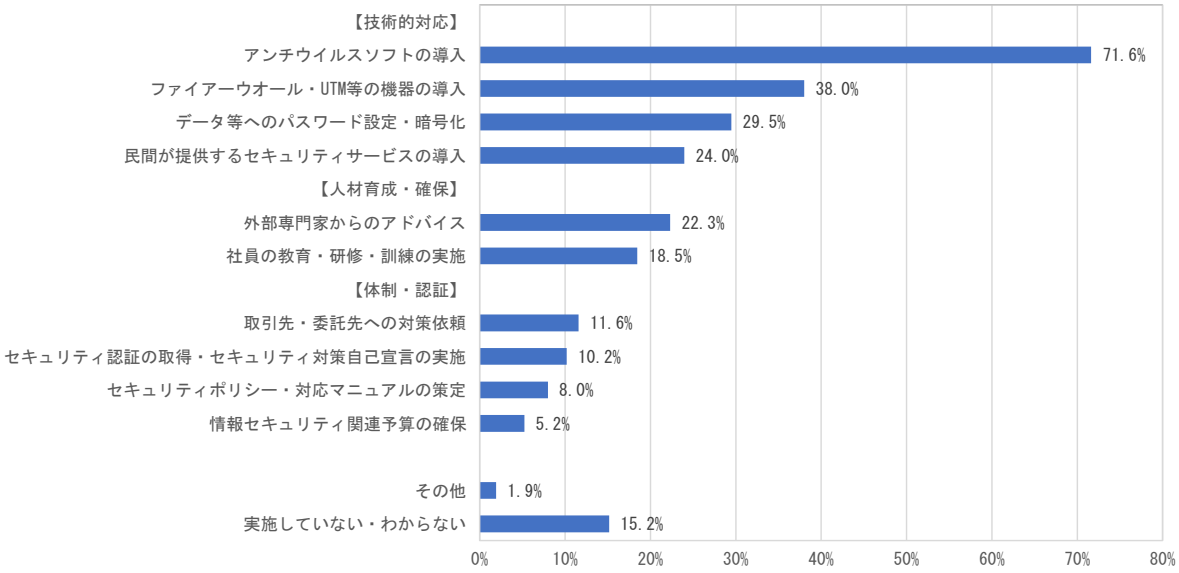
図表２．13　情報セキュリティ対策の実施状況【被害状況別】



具体的な情報セキュリティ対策（複数回答）としては、「技術的対応」である「アンチウイルスソフトの導入」（71.6%）、「ファイアウォール・UTM 等の機器の購入」（38.0%）、「データ等へのパスワード設定・暗号化」（29.5%）の割合が高い（図表２．14）。

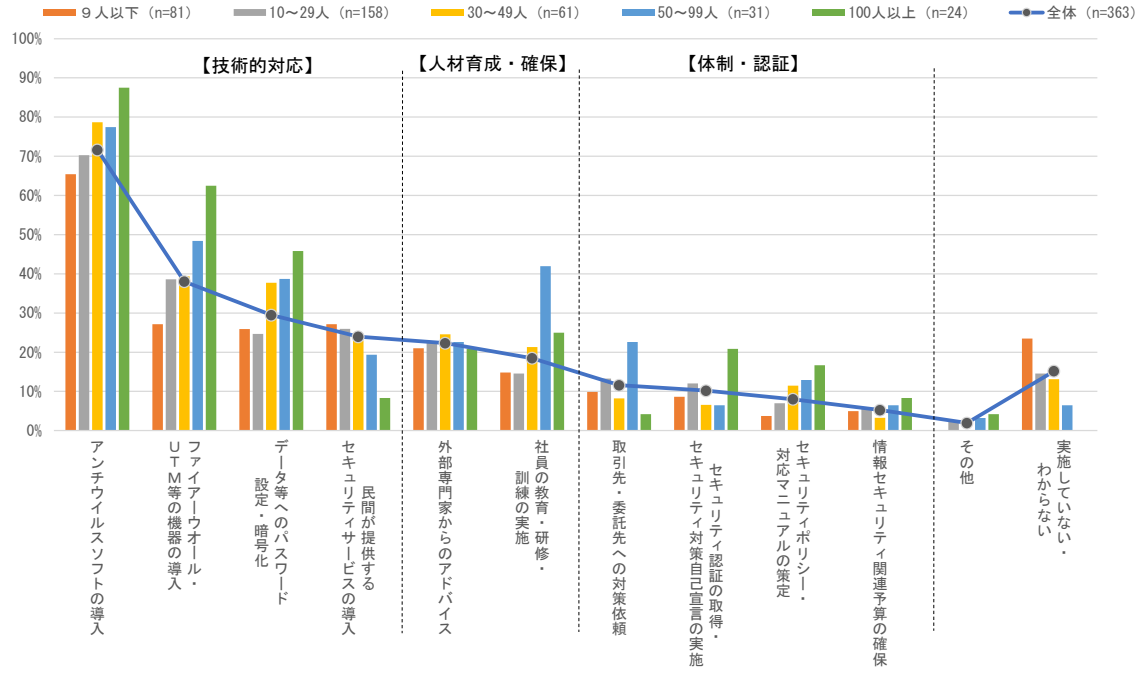
一方、「人材育成・確保」、「体制整備・認証取得」に関する取り組みを実施している企業は全体の１～２割程度となっている。

図表２．14　情報セキュリティ対策の実施内容【全体】（複数回答）



従業員数別にみると、「技術的対応」では「ファイアウォール・UTM 等の機器の購入」「データ等へのパスワード設定・暗号化」、「人材育成・確保」では「社員の教育・研修・訓練の実施」が規模の大きい企業において対応が進展している（図表２．15）。

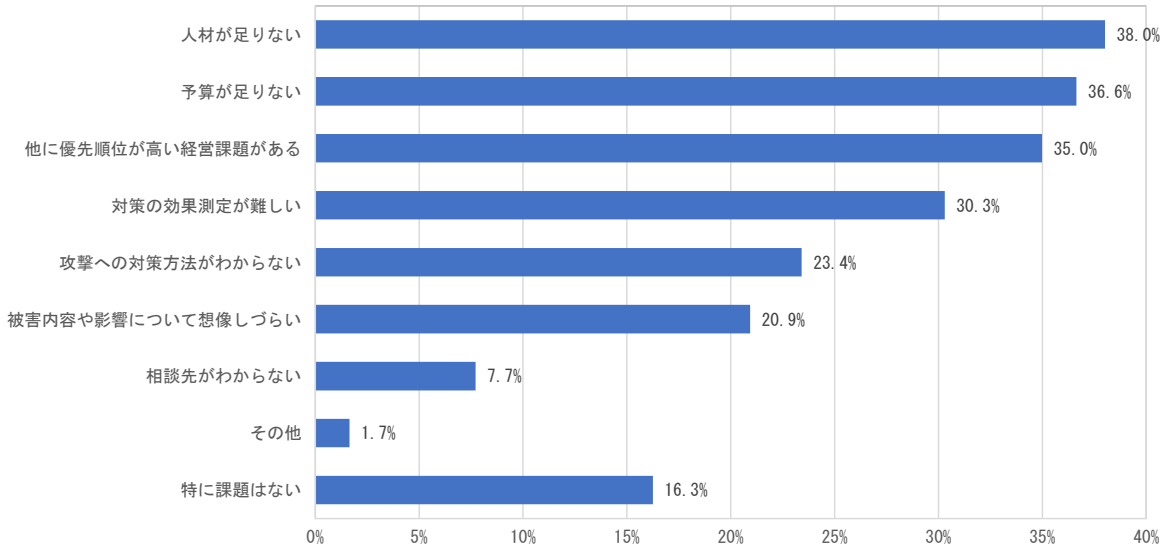
図表２．15　情報セキュリティ対策の実施内容【従業員数別】（複数回答）



問５．情報セキュリティ対策を進めるうえでの貴社の課題について、あてはまるものをすべて選んで○をおつけください　（ｎ＝363）

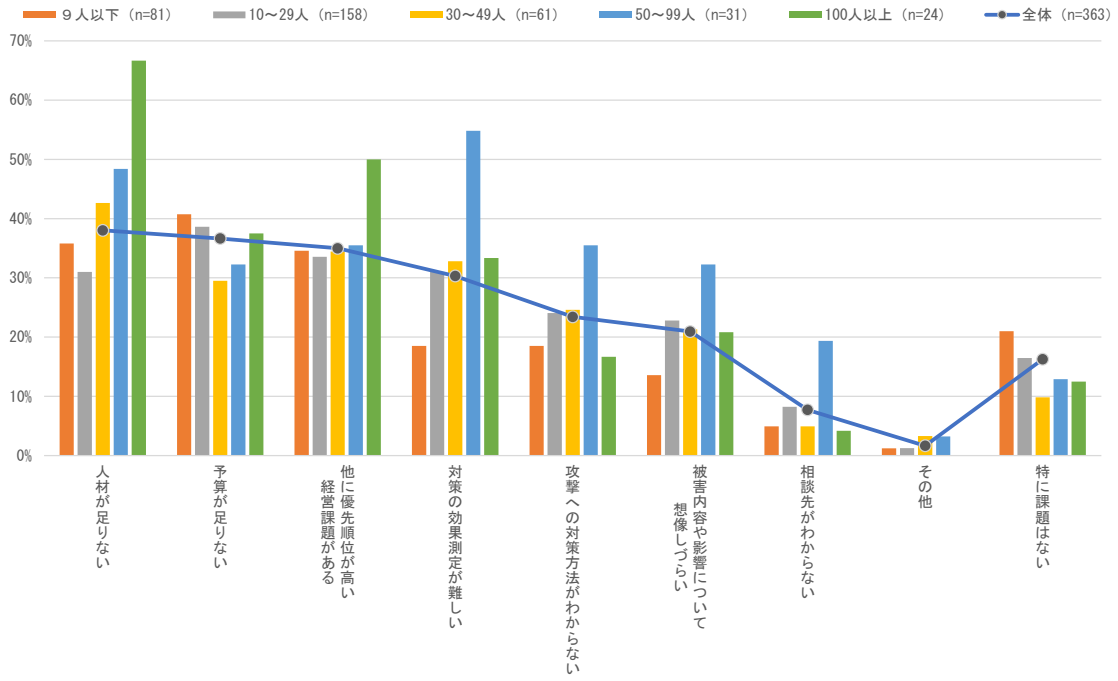
情報セキュリティ対策における課題（複数回答）としては「人材が足りない」（38.0%）、「予算が足りない」（36.6%）、「他に優先順位が高い経営課題がある」（35.0%）の割合が高い（図表２．16）。

図表２．16　情報セキュリティ対策における課題【全体】（複数回答）



従業員数別にみると、規模の大きい企業において「人材が足りない」「他に優先順位が高い経営課題がある」「対策測定が難しい」などの割合が高い（図表２．17）。これはセキュリティ対策に対する意欲の高さの裏返しともいえる。

図表２．17　情報セキュリティ対策における課題【従業員数別】（複数回答）

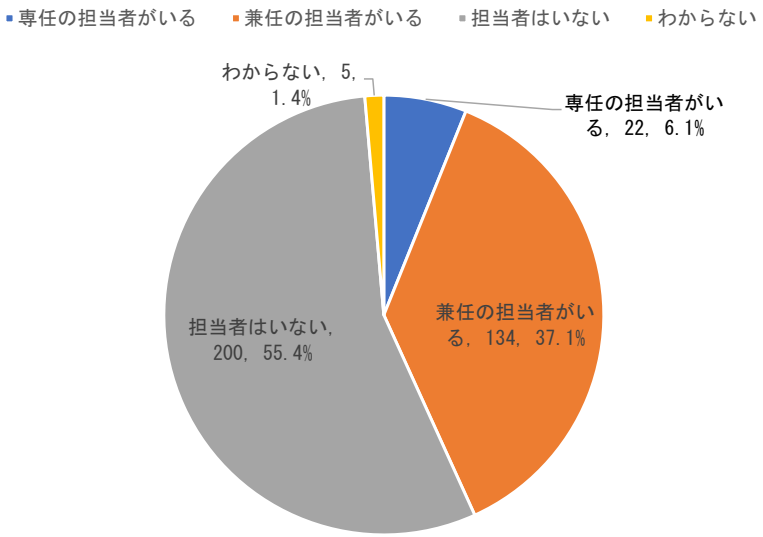


Ⅲ．情報セキュリティ体制

問６．貴社の情報セキュリティ担当者について、あてはまるものを１つ選んで○をおつけください（ｎ＝361）

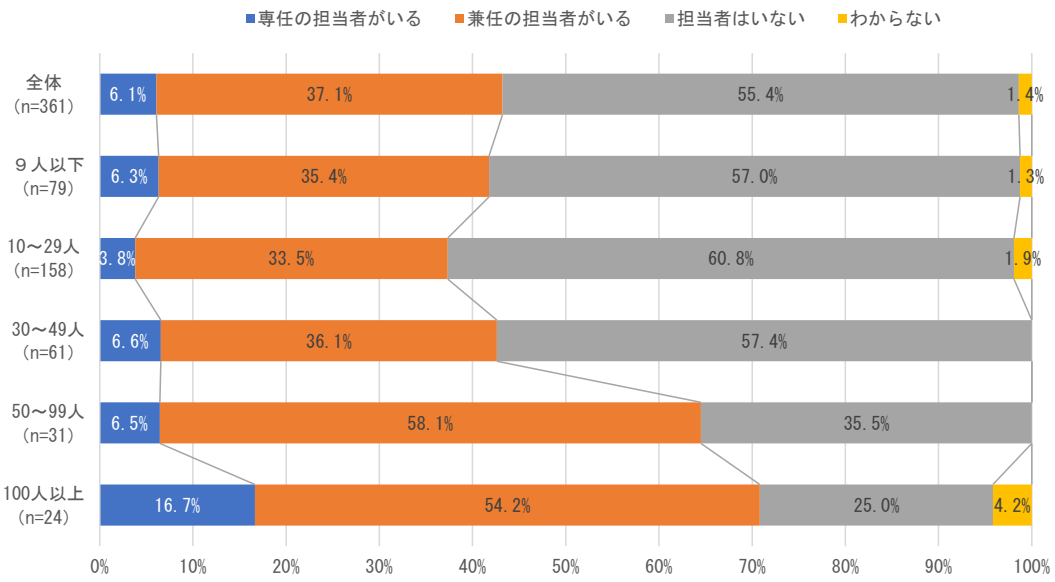
情報セキュリティ担当者の配置状況は「専任の担当者がいる」(6.1%)、「兼任の担当者がいる」(37.1%)であり、約４割の企業が担当者を配置している（図表２．18)。

図表２．18　情報セキュリティ担当者の配置状況【全体】



従業員数別にみると、概ね規模が大きくなるほど担当者の配置率（「専任の担当者がいる」＋「兼任の担当者がいる」）が高まる（図表２．19)。従業員数「９人以下」の企業での配置率は 41.7%であるが、「100 人以上」では 70.9%となっている。

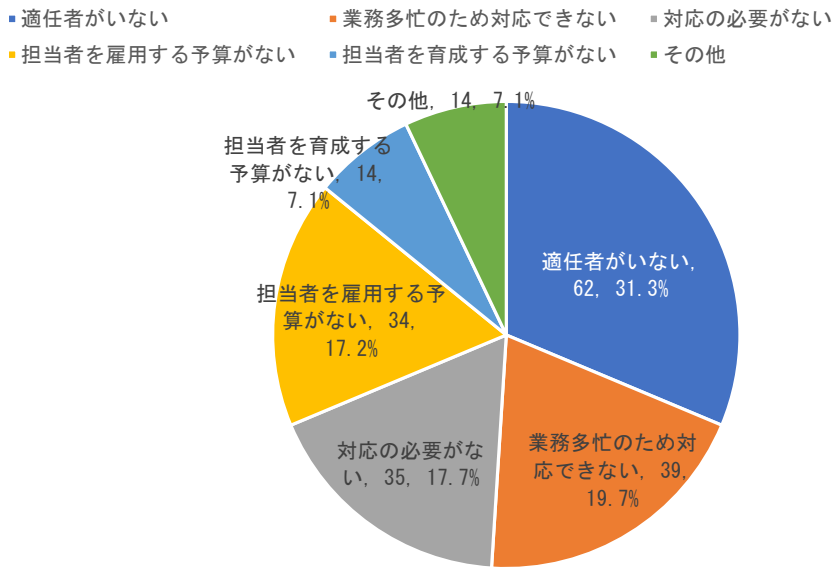
図表２．19　情報セキュリティ担当者の設置状況【従業員数別】



問７．前問で「3.担当者はいない」と答えた方にお伺いします。理由は、次のどれに近いですか。あてはまるものを１つ選んで○をおつけください　（ｎ＝198）

情報セキュリティ担当者を配置していない企業（全体の 55.4%）の非配置の理由は、「適任者がいない」(31.3%)が最も多く、次いで「業務多忙のため対応できない」(19.7%)、「対応の必要がない」(17.7%)となっている（図表２．20)。

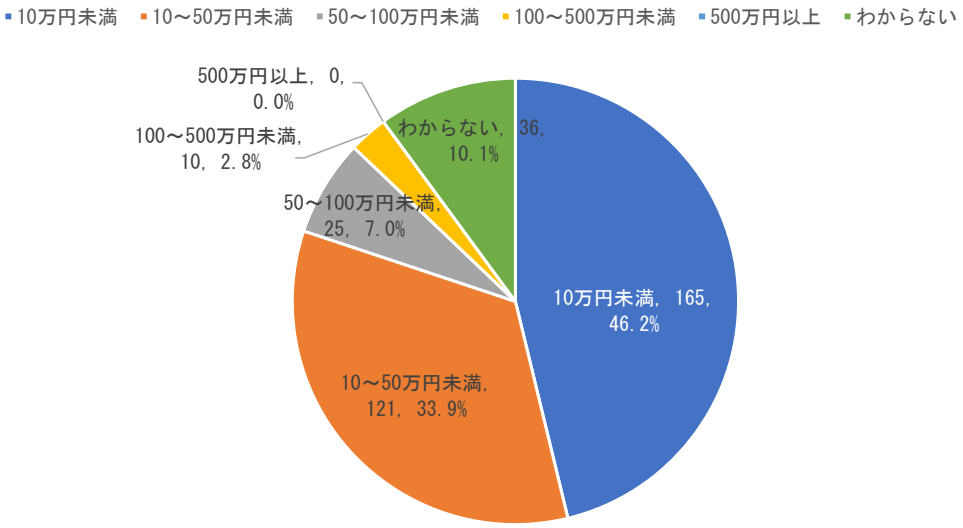
図表２．20　情報セキュリティ担当者を配置していない理由【全体】



問８．貴社の情報セキュリティ関連の年間経費について、あてはまるものを１つ選んで○をおつけください。　（ｎ＝357）

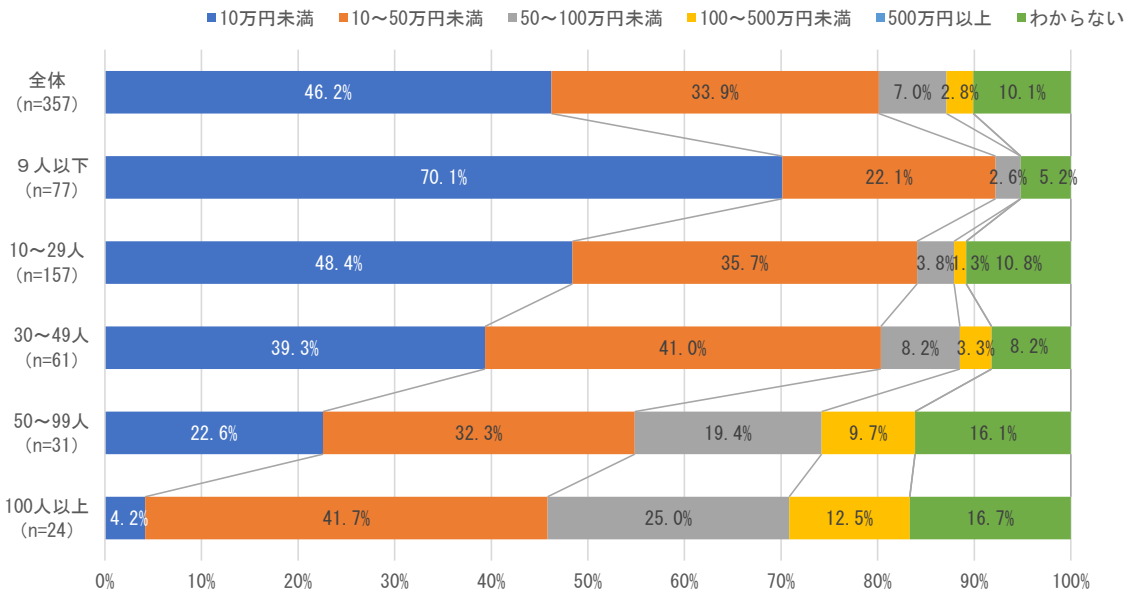
情報セキュリティ関連の年間経費は「10 万円未満」（46.2%）が最も多く、次いで「10～50 万円未満」（33.9%）、「50～100 万円未満」（7.0%）と、金額順となっている（図表２．21）。

図表２．21　情報セキュリティ関連の年間経費【全体】



従業員数別にみると、規模が大きくなるほど年間経費が増加している（図表２．22）。年間 50 万円以上の年間経費の割合は、従業員数「９人以下」の企業では 2.6%であるが、「100 人以上」では 37.5%となっている。

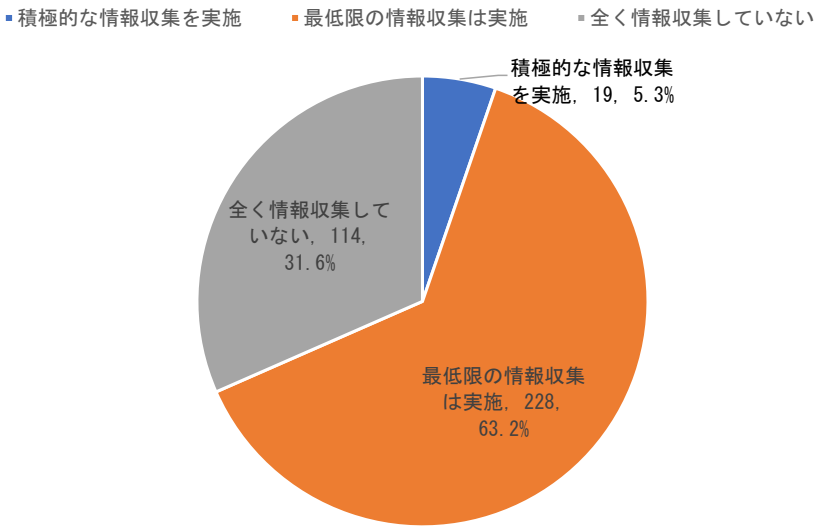
図表２．22　情報セキュリティ関連の年間経費【従業員数別】



問９．貴社の情報セキュリティに関する情報収集について、あてはまるものを１つ選んで○をおつけください　（ｎ＝361）

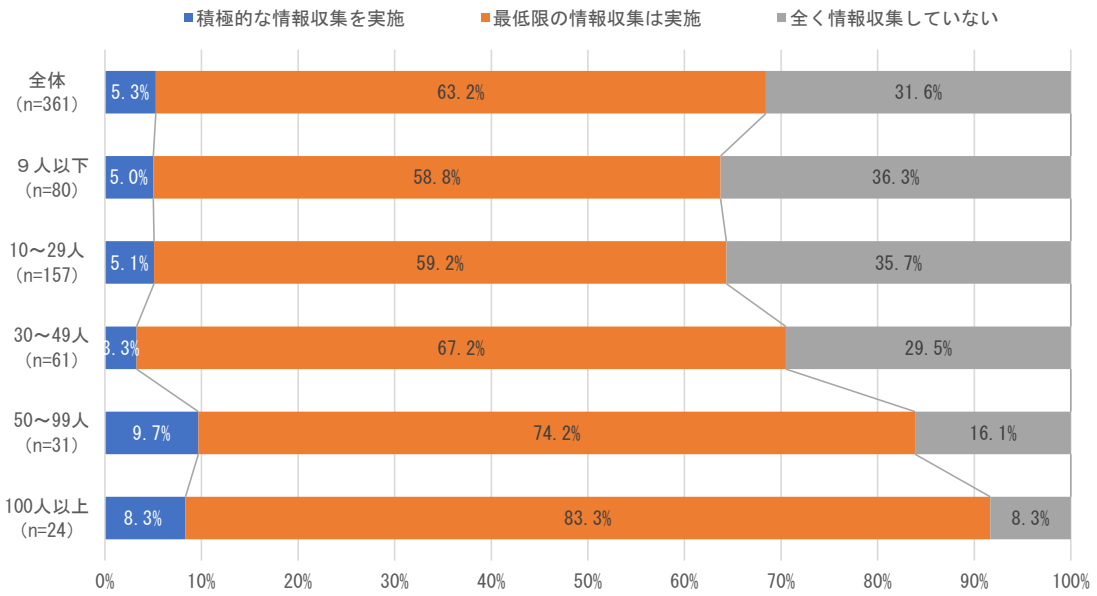
情報セキュリティに関する情報収集は、「積極的な情報収集を実施」が 5.3%、「最低限の情報収集は実施」が 63.2%であり、合せて何らかの情報収集を行っている企業が約７割となっている（図表２．23）。

図表２．23　情報セキュリティに関する情報収集【全体】



従業員数別にみると、規模が大きくなるほど情報収集の実施率（「積極的な情報収集を実施」＋「最低限の情報収集は実施」）が高まる（図表２．24）。従業員数「９人以下」の企業で 63.3%であるが、「100人以上」では 96.6%となっている。

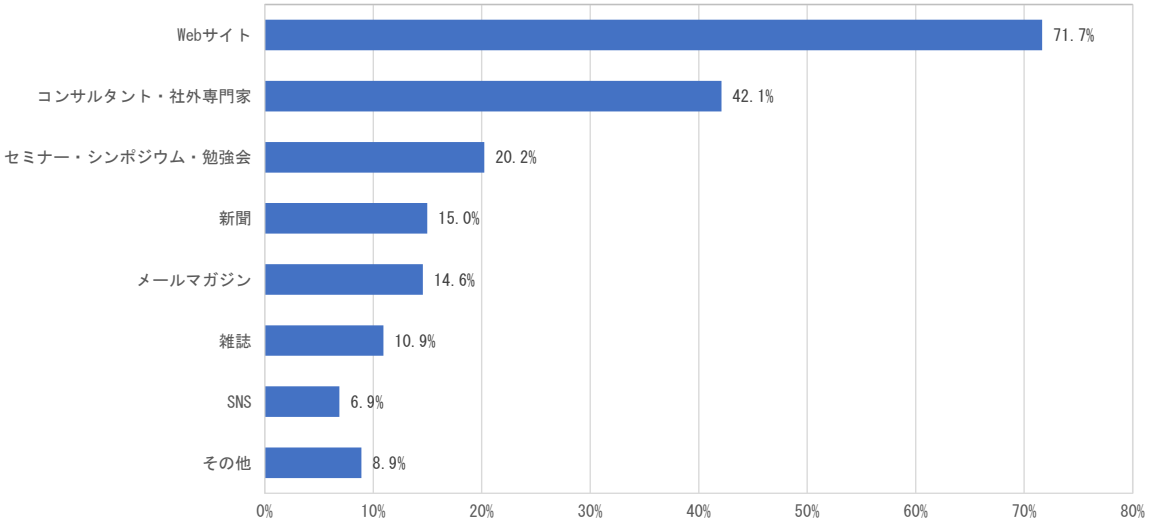
図表２．24　情報セキュリティに関する情報収集【従業員数別】



問 10. 情報セキュリティに関して情報収集している方にお伺いします。情報収集先についてあてはまるものをすべて選んで〇をおつけください （ｎ＝247）

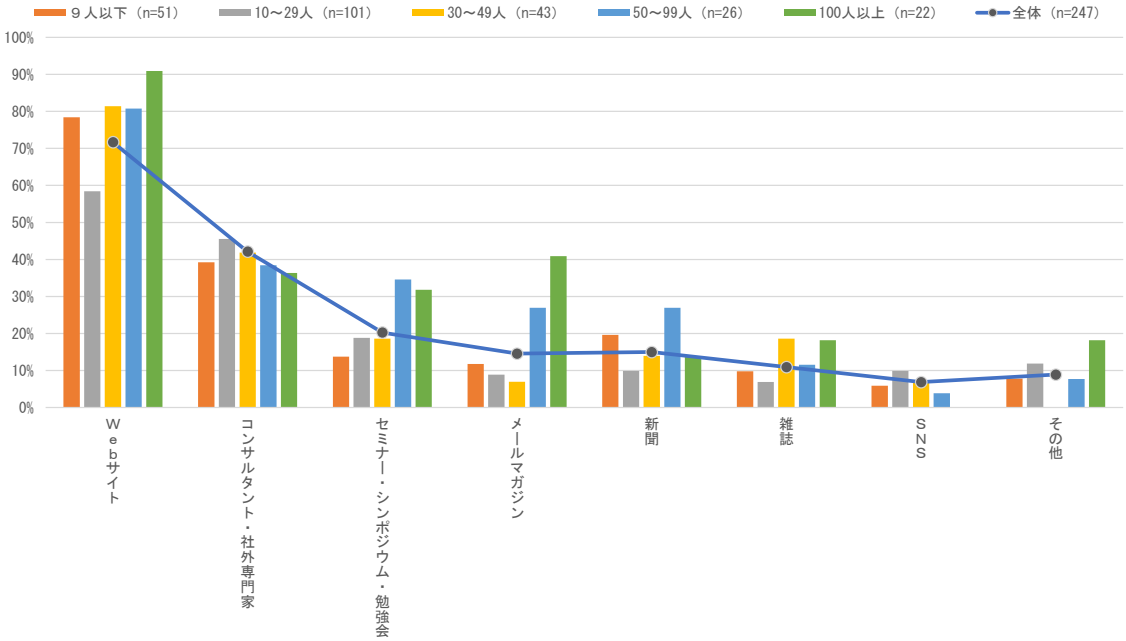
情報セキュリティに関する情報収集先（複数回答）は、「Web サイト」（71.3%）が最も多く、次いで「コンサルタント・社外専門家」（42.1%）となっている（図表２．25）。

図表２．25　情報セキュリティに関する情報収集先【全体】（複数回答）



従業員数別にみると、企業規模が大きくなるほど「セミナー・シンポジウム・勉強会」「メールマガジン」の比率が高まる（図表２．26）。

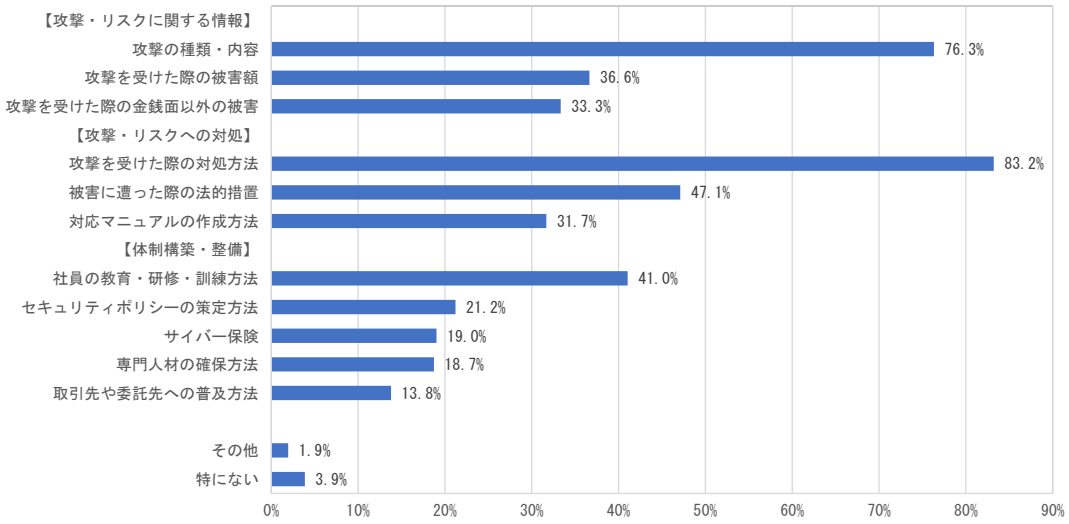
図表２．26　情報セキュリティに関する情報収集先【従業員数別】（複数回答）



問 11. 貴社が情報セキュリティに関して知りたい情報をすべて選んで〇をおつけください。
（ｎ＝363）

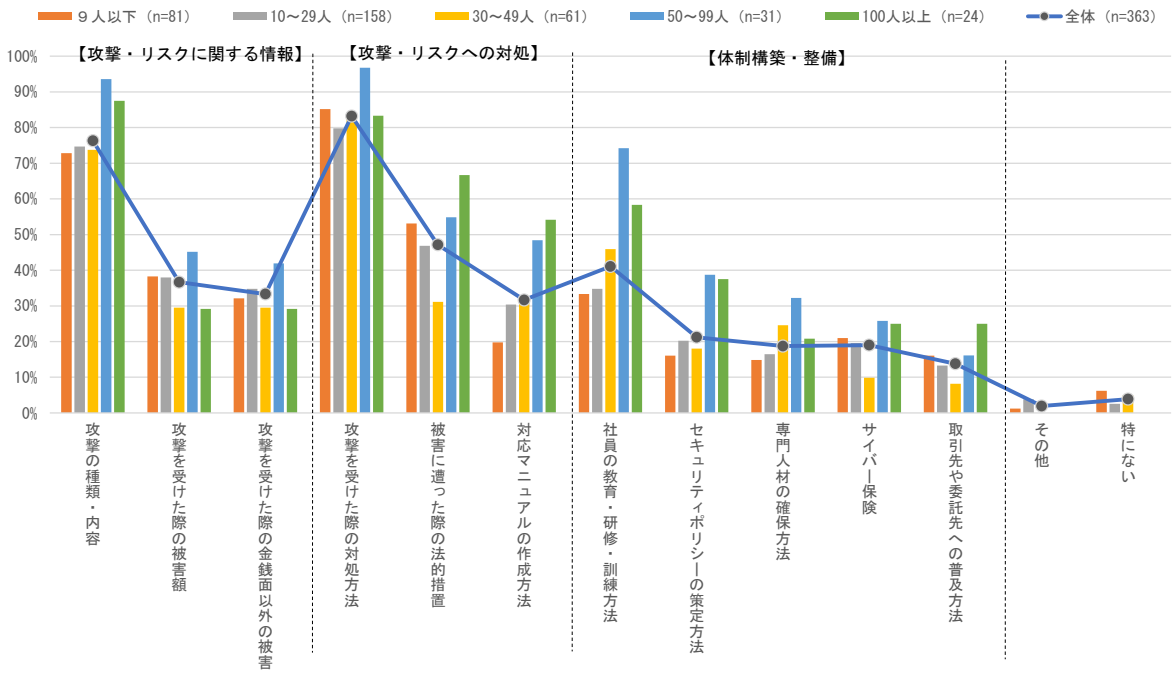
情報セキュリティに関して知りたい情報（複数回答）は、「攻撃・リスクへの対処」に関して「攻撃を受けた際の対処方法」（83.2%）が最も多く、次いで「攻撃・リスクに関する情報」に関して「攻撃の種類・内容」（76.3%）となっている。この２種類の情報へのニーズが圧倒的に高い（図表２．27）。

図表２．27　情報セキュリティに関して知りたい情報【全体】（複数回答）



従業員数別にみると、規模が大きい企業では「被害に遭った際の法的措置」「社員の教育・研修・訓練方法」「セキュリティポリシーの策定方法」の比率が大きく高まる（図表２．28）。

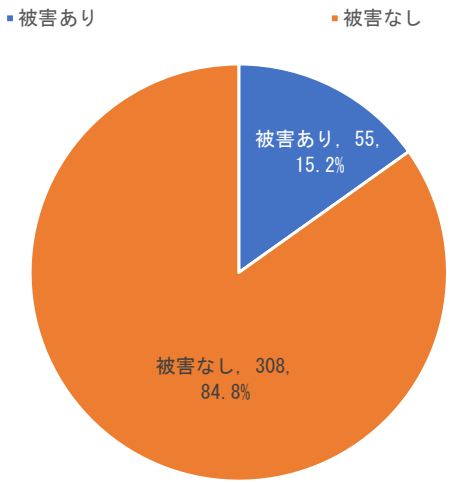
図表２．28　情報セキュリティに関して知りたい情報【従業員数別】（複数回答）



問 12. 貴社が情報セキュリティに関連して過去被害に遭ったことがある場合は、その被害内容についてすべて選んで○をおつけください （ｎ＝363）

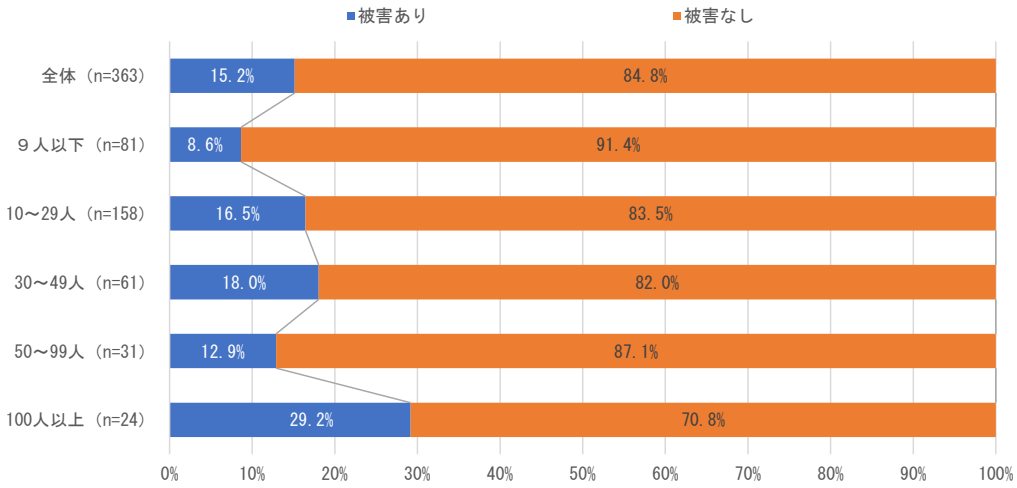
情報セキュリティ関連で被害を受けたことのある企業（「被害あり」）の割合は 15.2%である（図表２．29）。

図表２．29 情報セキュリティ関連の被害状況【全体】



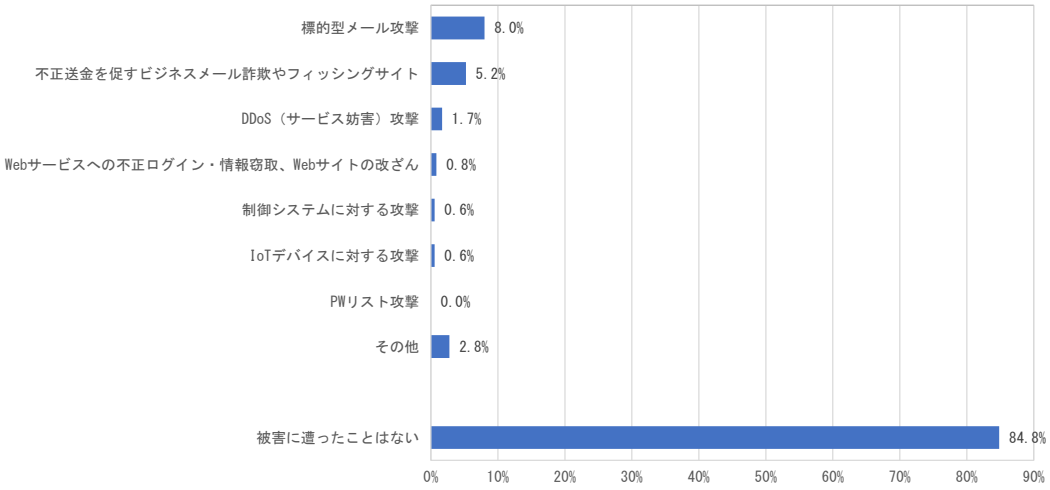
被害発生状況を従業員数別にみると、「100 人以上」（29.2%）が最も多く、次いで「30～49 人」（18.0%）、「10～29 人」（16.5%）となっている（図表２．30）。概ね規模が大きい企業ほど被害発生率が高い。

図表２．30 情報セキュリティ関連の被害状況【従業員数別】



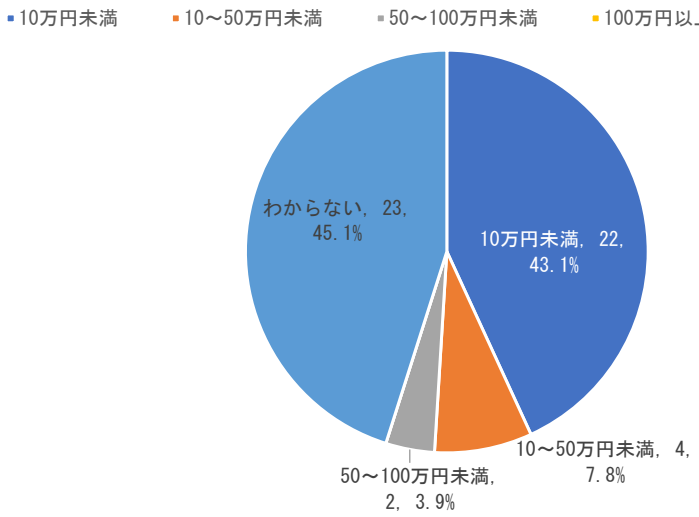
具体的な被害内容（複数回答）としては「標的型メール攻撃」（8.0%）、「不正送金を促すビジネスメール詐欺やフィッシングサイト」（5.2%）、「DDoS（サービス妨害）攻撃」（1.7%）などがあげられる（図表２．31）。

図表２．31　情報セキュリティ関連の被害内容【全体】（複数回答）



情報セキュリティ関連の被害金額は「10 万円未満」（43.1%）が最も多い。さらに「わからない」企業も 45.1%あり、被害に遭ったものの被害状況が正確に把握できていない企業も少なくない（図表２．32）。

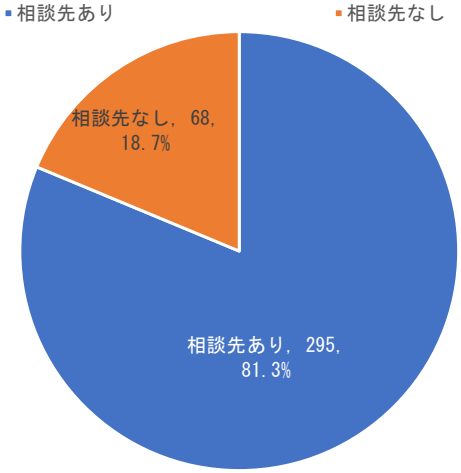
図表２．32　情報セキュリティ関連の被害金額



問 14. 貴社が情報セキュリティに関連して被害に遭った場合（今後の予定を含む）の相談先について、あてはまるものをすべて選んで○をおつけください（ｎ＝363）

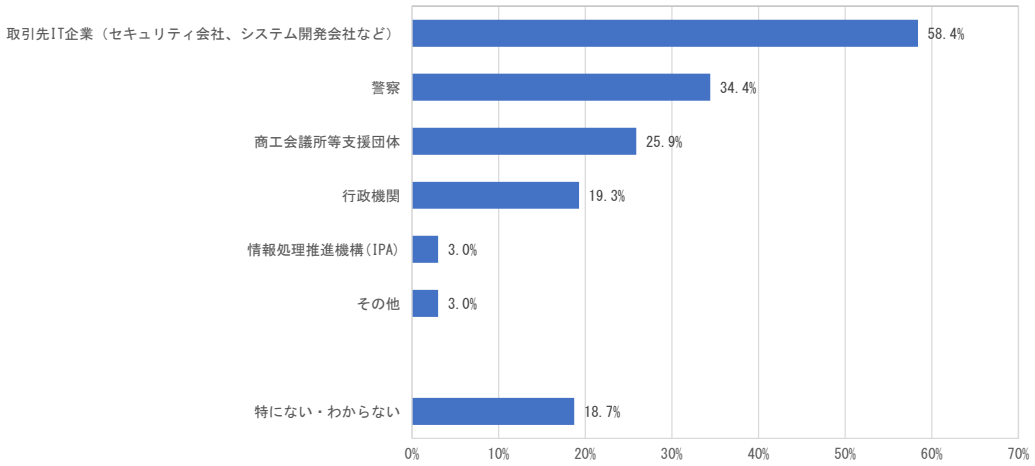
情報セキュリティ被害発生時の相談先の有無については、「相談先あり」が 81.3%である（図表２．33）。

図表２．33　情報セキュリティ被害時の相談先の有無【全体】



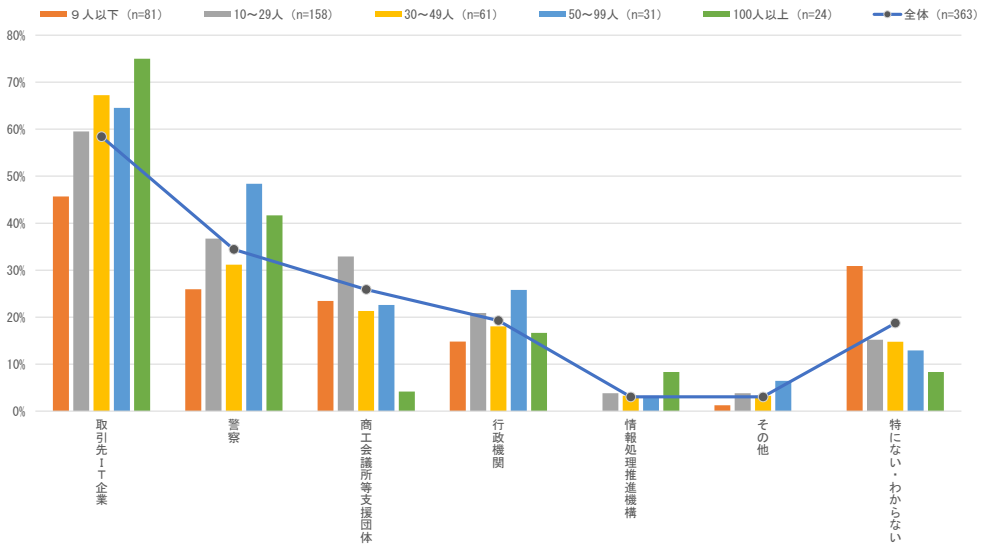
情報セキュリティ被害発生時の具体的な相談先（複数回答）は「取引先 IT 企業（セキュリティ企業、システム開発会社など）」（58.4%）が最も多く、次いで「警察」（34.4%）、「商工会議所等支援団体」（25.9%）となっている（図表２．34）。

図表２．34　情報セキュリティ被害時の相談先【全体：相談先別】（複数回答）



従業員数別にみると、規模の大きい企業ほど「取引先 IT 企業」を中心とした相談先が存在している一方で、規模の小さい企業には特定の相談先が存在しない傾向がみられる（図表２．35）。

図表２．35　情報セキュリティ被害時の相談先【従業員数別】（複数回答）

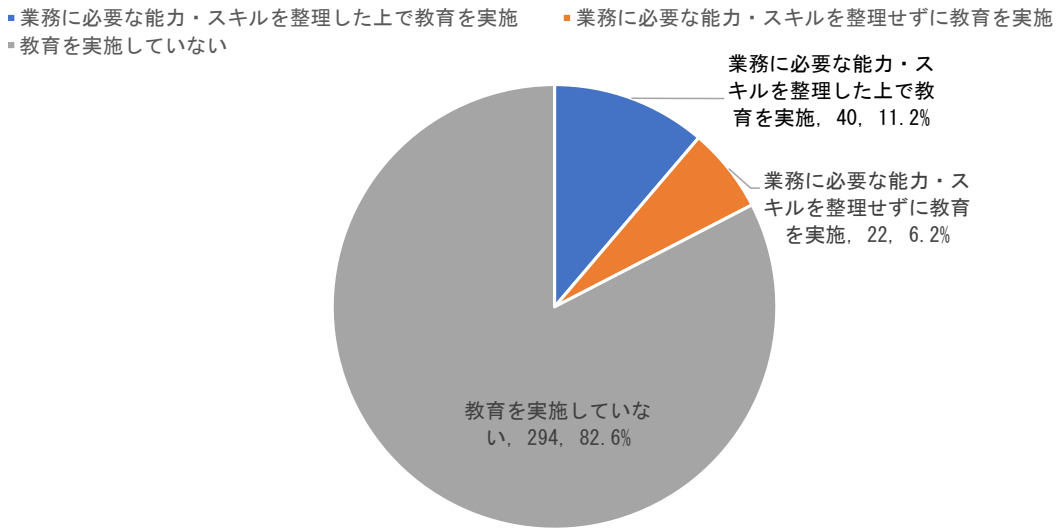


Ⅴ．情報セキュリティ人材の育成・確保

問 15．貴社の情報セキュリティ人材の育成・教育について、あてはまるものを１つ選んで○をおつけください　（ｎ＝356）

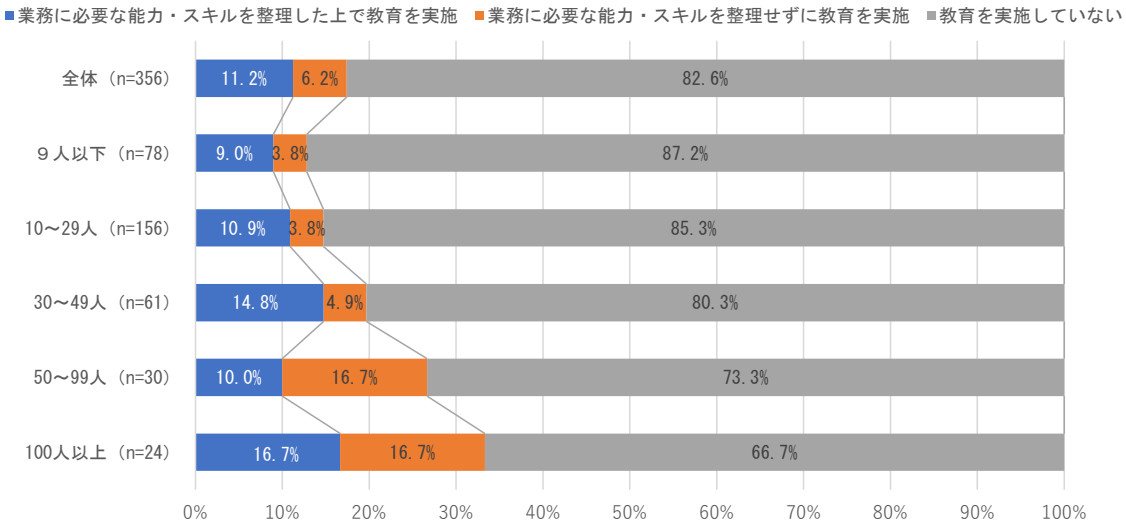
情報セキュリティ関連の人材育成・教育については、「業務に必要な能力・スキルを整理したうえで教育を実施」が 11.2%、「業務に必要な能力・スキルを整理せずに教育を実施」が 6.2%であり、体系化の状況にかかわらず、何らかの人材育成・教育を実施している企業は合わせて 17.4%となる（図表２．36）。

図表２．36　情報セキュリティ関連の人材育成・教育【全体】



従業員数別にみると、規模が大きくなるほど教育実施率（「業務に必要な能力・スキルを整理した上で教育を実施」＋「業務に必要な能力・スキルを整理せずに教育を実施」）が高まる（図表２．37）。従業員数「９人以下」の企業での実施率は 12.8%であるが、「100 人以上」では 33.4%となっている。また、「業務に必要な能力・スキルを整理」している割合も企業規模に応じて増加していく。

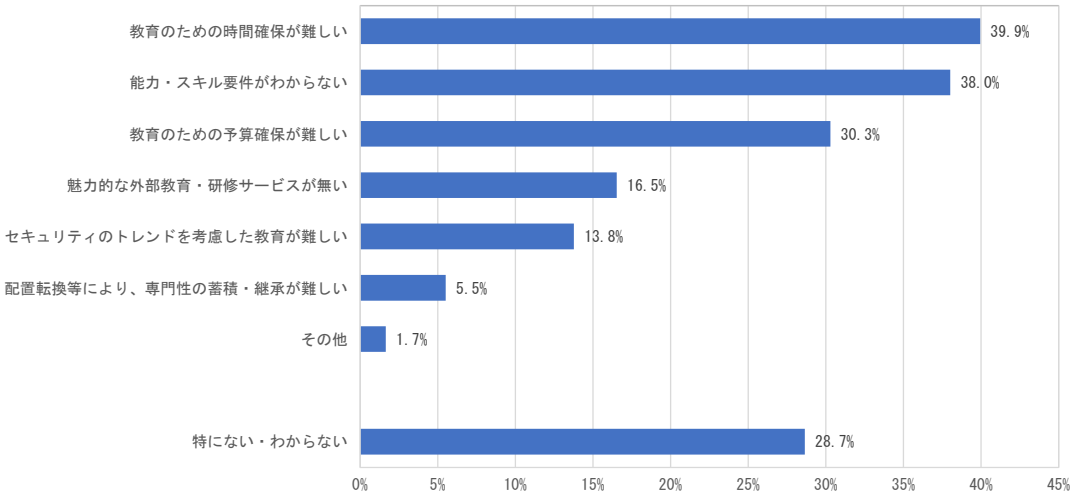
図表２．37　情報セキュリティ関連の人材の育成・教育【従業員数別】



問 16.　貴社における情報セキュリティ人材の育成・教育における課題について、あてはまるものをすべて選んで〇をおつけください　（ｎ＝363）

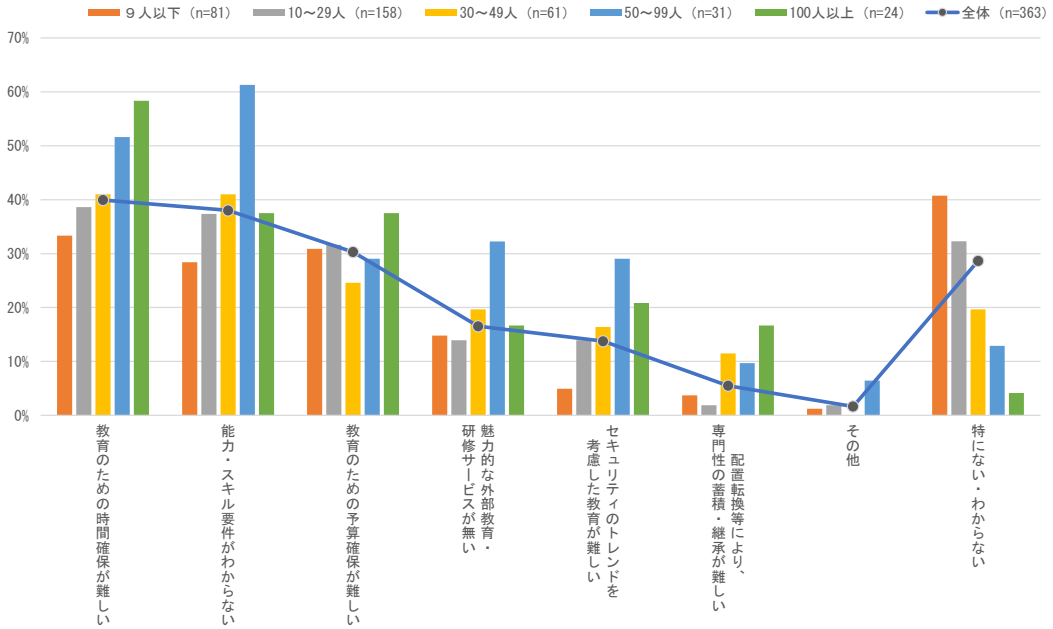
情報セキュリティ人材の育成・教育における課題（複数回答）は、「教育のための時間確保が難しい」（39.9%）が最も多く、次いで「能力・スキル要件がわからない」（38.0%）、「教育のための予算確保が難しい」（30.3%）となっている（図表２．38）。「お金」「時間」の確保のほか「教育内容」もネックとなっている状況がうかがえる。

図表２．38　情報セキュリティ関連の人材育成・教育の課題【全体】（複数回答）



従業員数別にみると、規模の大きい企業では「能力・スキル要件がわからない」に加え、「魅力的な外部教育・研修サービスがない」「セキュリティのトレンドを考慮した教育が難しい」などの教育内容に関わる項目が相対的に多くなる（図表２．39）。加えて、ジョブローテーションより「配置転換等により、専門性の蓄積・継承が難しい」の割合も高くなる。

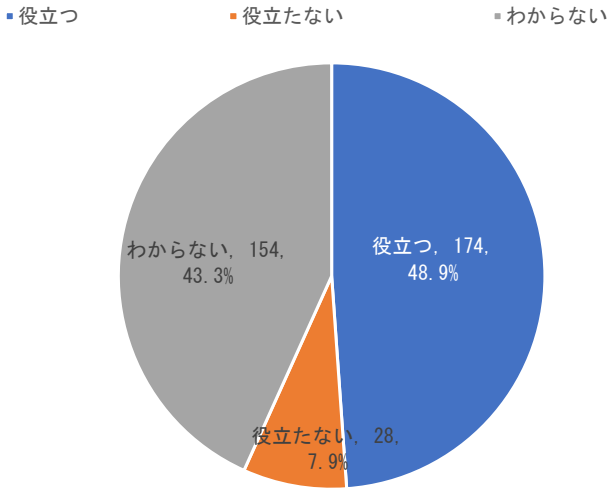
図表２．39　情報セキュリティ関連の人材育成・教育の課題【従業員数別】（複数回答）



問 17.　情報セキュリティのセミナー・講座に関して「習得できるスキル」「対象・レベル」等の情報が分かりやすく提供されれば、貴社における今後の人材育成・教育に役に立つと思いますか。あてはまるものを１つ選んで○をおつけください　（ｎ＝356）

情報セキュリティ関連のセミナー・講座に関して「習得できるスキル」「対象・レベル」等の情報が分かりやすく提供するもの（いわゆる「セキュリティ講座 カリキュラムマップ」）については、「役立つ」が 48.9%、「役立たない」が 7.9%となっており、概ね肯定的に捉えられている（図表２．40）。

図表２．40　セキュリティ講座マップの有用性

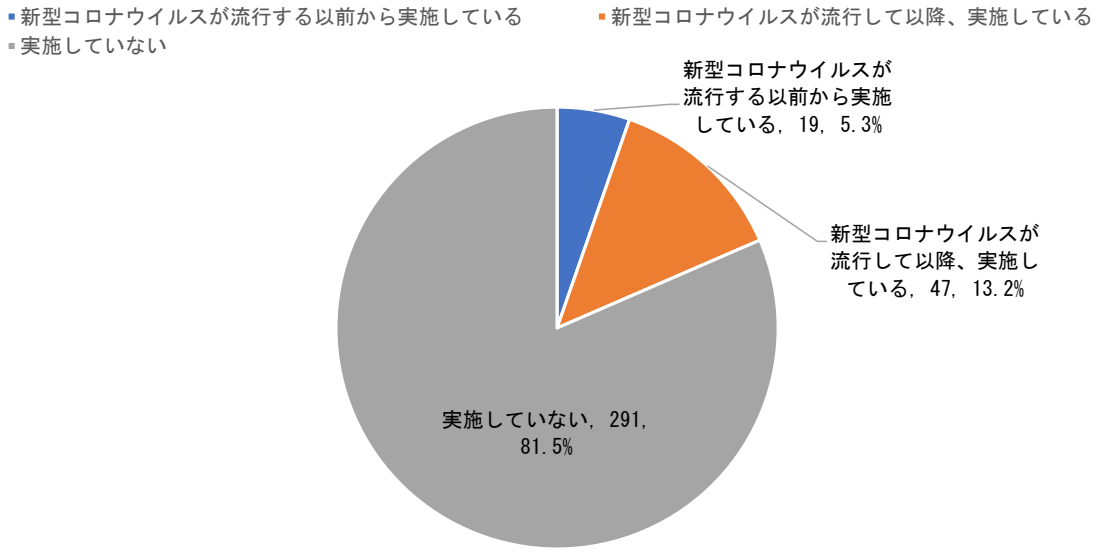


Ⅵ．テレワークと情報セキュリティ

問 18．現在、貴社はテレワーク（在宅勤務）を実施していますか。あてはまるものを１つ選んで○をおつけください　（ｎ＝357）

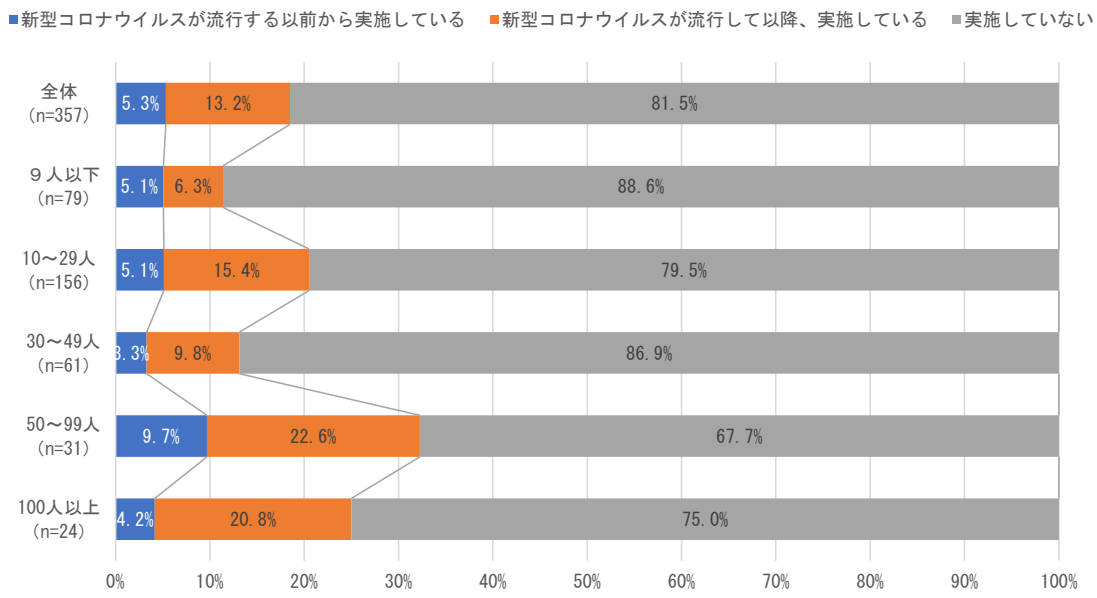
テレワーク（在宅勤務）の実施率は 18.5%であり、「新型コロナウイルスが流行する以前から実施」している企業が 5.3%、「新型コロナウイルスが流行して以降実施」している企業が 13.2%である（図表２．41）。新型コロナウイルス流行に伴い実施率は約４倍となっているが、「実施していない」企業も約８割に及んでおり、中小企業におけるテレワークの浸透は限定的である。

図表２．41　テレワークの実施状況【全体】



従業員数別にみると、新型コロナウイルス流行に伴いテレワーク実施している企業は「９人未満」の企業では約２倍（5.1%→11.4%）、「100 人以上」では約５倍（4.2%→25.0%）に増加している（図表２．42）。

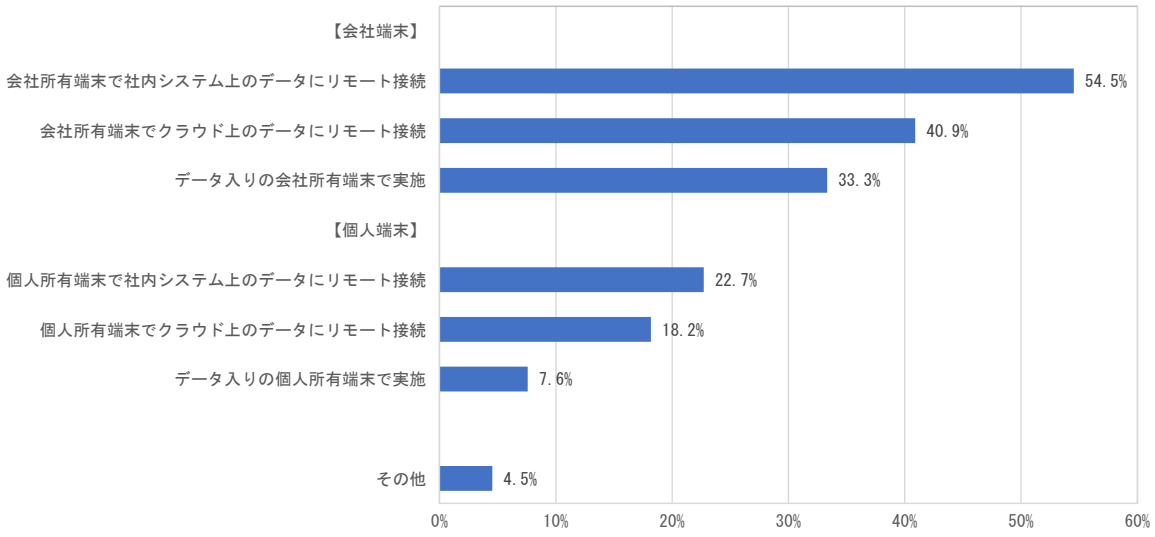
図表２．42　テレワークの実施状況【従業員数別】



問 19. テレワークを実施している方にお伺します。実施しているテレワークの種別について、あてはまるものをすべて選んで〇をおつけください　（ｎ＝66）

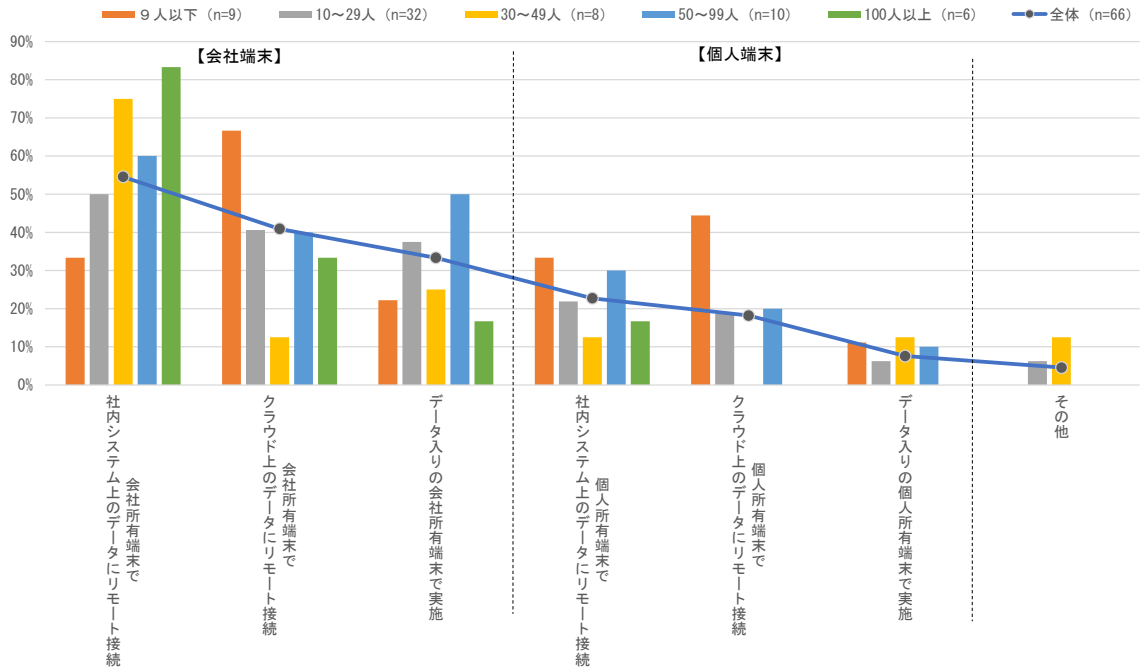
テレワークの実施種別では、「会社端末」を支給し「社内システム上のデータにリモート接続」(54.5%)、「クラウド上のデータにリモート接続」（40.9%）するケースが多い（図表２．43)。「個人端末」により接続する場合は「社内システム状のデータにリモート接続」（22.7%）するケースが最も多い。

図表２．43　テレワークの実施種別【全体】（複数回答）



従業員数別にみると、規模の小さい企業では「社内システム」にリモート接続するよりも「クラウド上のデータ」にリモート接続する割合が高く、規模の大きい企業では「会社端末」により「社内システム」にリモート接続する割合が相対的に高い（図表２．44)。

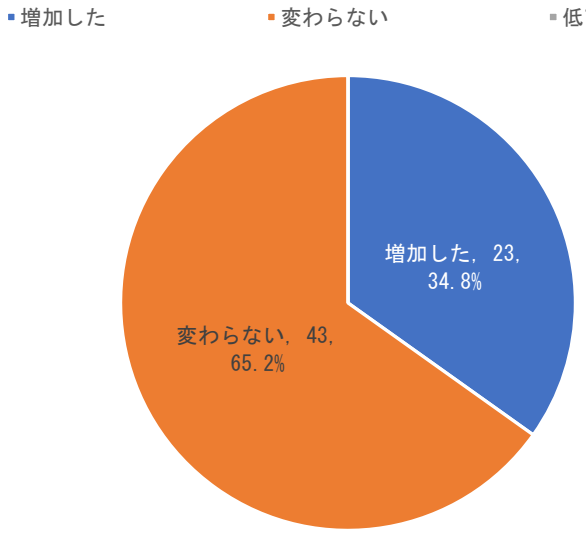
図表２．44　テレワークの実施種別【従業員数別】（複数回答）



問 20. テレワークを実施している方にお伺いします。テレワーク導入後、情報セキュリティへの不安はどのようになりましたか。あてはまものを１つ選んで○をおつけください　（ｎ＝66）

テレワークの実施に伴う情報セキュリティへの不安に関しては「増加した」が 34.8%、「変わらない」が 65.2%となっている（図表２．45）。

図表２．45　テレワークの実施に伴う情報セキュリティへの不安



問 21. テレワーク関連以外で新型コロナウイルス流行に伴い貴社で実施した「情報セキュリティ対応」や増大した「情報セキュリティへの不安」等がございましたら、ご記入ください

テレワーク関連以外で実施した「情報セキュリティ対応」や増大した「情報セキュリティへの不安」としては、新たに導入したテレビ会議システム(Zoom 等)、クラウドサービス等の利用時のデータ流出、個人端末、記憶媒体の紛失・ウイルス感染等の懸念があげられた（図表２．46)。これらへの対策は行われているものの、不安の完全なる払拭には至っていない状況がうかがえる。

図表２．46　新型コロナウイルス流行に伴い実施した「情報セキュリティ対応」および増大した「情報セキュリティへの不安」等

所在地	業　種	内　容
鳥取県	加工組立型製造業	メール添付されるウイルスの不安
島根県	生活関連型製造業	SNS（Social networking service）への情報投稿に誤情報を投稿する危険性
岡山県	基礎素材型製造業	テレワーク以外で新型コロナ関連の情報セキュリティ対応を行っていない
岡山県	基礎素材型製造業	社外ネットワークでのクラウド接続となりセキュリティレベルが適当なのか判断できないところが不安
岡山県	卸売業,小売業	システム管理者が感染することによる、システム障害発生時の対応計画が未策定（対応できる人材がいない）
岡山県	その他	Zoom 動画などの流出
広島県	加工組立型製造業	クラウド会計、クラウド販売管理へ移行
広島県	加工組立型製造業	持ち出し用のノートパソコン返却時の状態（履歴やログイン情報の初期化、ウイルス感染状態）
広島県	基礎素材型製造業	基礎知識（技術）がないため、対応が難しい
広島県	基礎素材型製造業	TV 会議（Zoom 等）をおこなうことが増えたため、専用ソフトやアプリを使用するにあたってセキュリティ面で不安あり
広島県	生活関連型製造業	社員の個人情報持ち出しによる流出
広島県	生活関連型製造業	EMOTET[4]対策が急務
山口県	加工組立型製造業	従業員に対する教育を実施
山口県	加工組立型製造業	社内データ化は数年前から進めているが、全体的に知識不足であるのと、外部に委託している状況である。現在まで被害は見受けられてない状況ですが、実際に被害を被った場合にしっかりと認識できるか不安はある
山口県	基礎素材型製造業	情報を記憶した媒体や試作品の持ち出し、紛失など人の手で引き起こされる脅威への対策として要所に防犯カメラを設置
山口県	建設業	テレワークで社内ネットワーク接続のために VPN（Virtual Private Network）[5]を導入。外部より、社内端末をリモート操作可能なソフトの導入。 経理担当事務員のテレワークにより、情報漏えいが心配
山口県	その他	育休医師向けに実施していた在宅診断を新型コロナウイルス流行に伴い、多くの医師で行えるようにするため、クラウドでのシステムをやめて在宅画像診断用のサーバを社内に構築。考えられる対策はしているものの不安はある

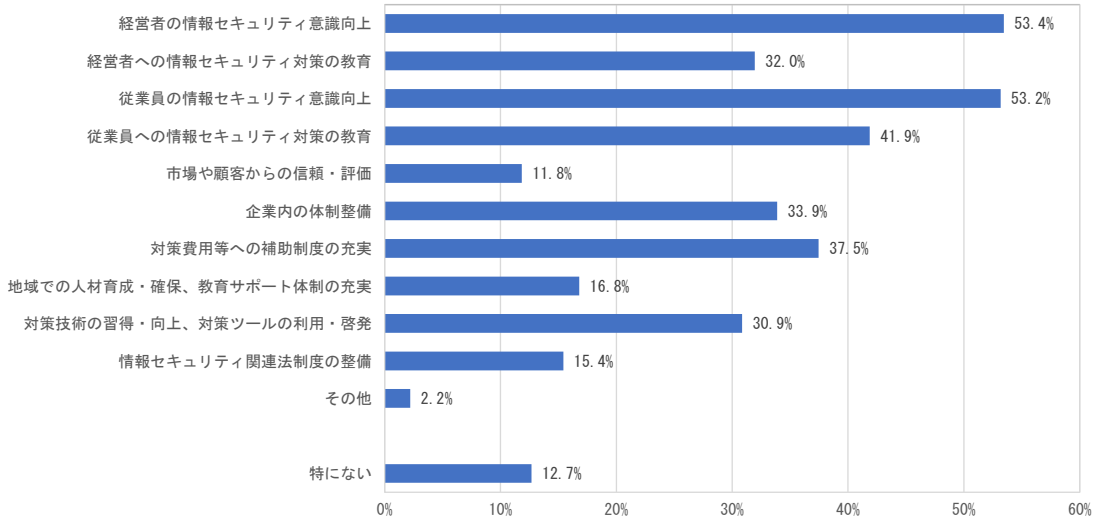
Ⅶ. 情報セキュリティレベルの向上のための施策・サポートについて

問 22. 貴社の情報セキュリティのレベルを向上させるために必要と思われることをすべて選んで○をおつけください　（ｎ＝363）

情報セキュリティのレベルを向上させるための必要なものとして、「経営者の情報セキュリティ意識向上」(53.4%)、「従業員の情報セキュリティ意識向上」(53.2%) の割合が高い（図表２．47)。会社全体での情報セキュリティに対する意識向上が最優先視されている。次いで経営者・従業員に対する「セキュリティ対策の教育」(各 32.0%、41.9%)、「対策費用等への補助制度の充実」(37.5%) となっている。

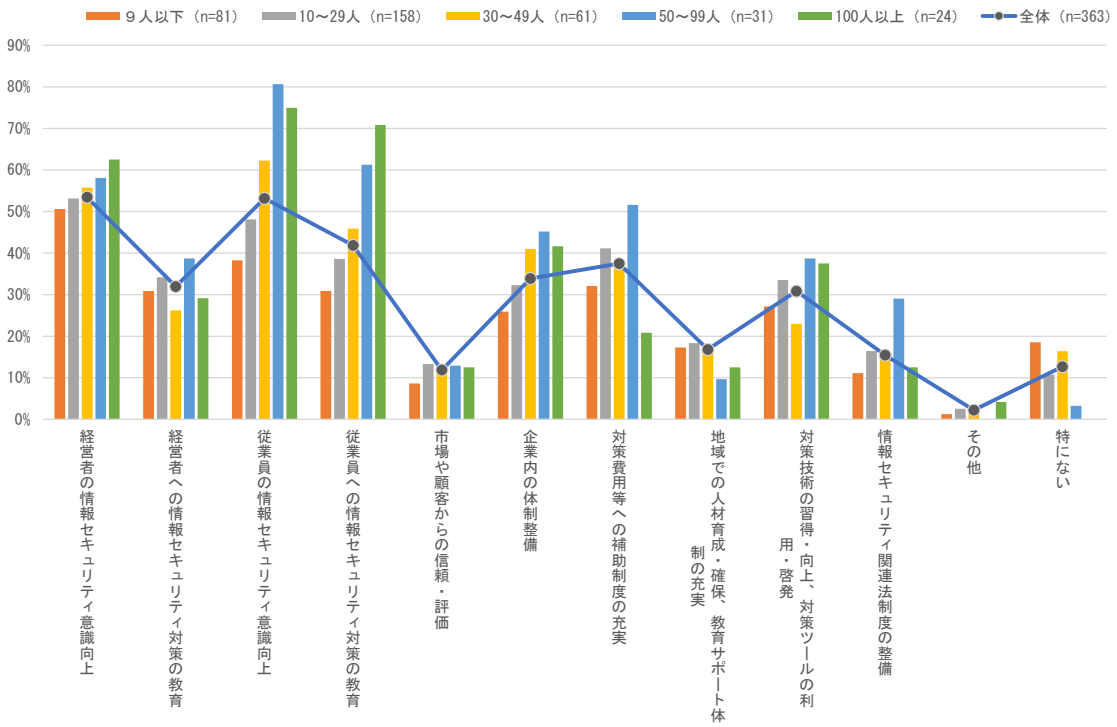
[4] 強力な感染力・拡散力を持ったマルウェア。特徴として、受信者が過去にメールのやり取りをしたことのある内容が利用される
[5] インターネット（本来は公衆網である）に跨って、プライベートネットワークを拡張する技術

図表２．47　情報セキュリティのレベルを向上させるために必要なもの【全体】（複数回答）



従業員数別にみると、規模の大きい企業では経営者・従業員双方における「情報セキュリティ意識向上」、従業員に対する「セキュリティ対策の教育」「情報セキュリティ関連法制度の整備」などの割合が相対的に高い（図表２．48）。一方、規模の小さな企業では資源制約等から「地域での人材育成・確保、教育サポート・体制の充実」の割合が相対的に高く、企業単体ではなく地域全般での取り組みの広がりが期待されている。

図表２．48　情報セキュリティのレベルを向上させるために必要なもの【従業員数別】（複数回答）



問 23. 貴社での情報セキュリティに関する特徴的な取り組み、支援のあり方等について意見・コメント等がございましたら、ご自由にご記入ください

情報セキュリティに関する自由記述では「セキュリティに関するセミナー・勉強会」「(IT 補助金同様の）セキュリティ投資に対する支援」「セキュリティ相談・対応窓口の設置」「セキュリティソフトの無料配布」などを求める意見が複数みられる（図表２．49)。

また、小規模企業にとって情報セキュリティ人材の確保は困難との声もあり、担当者不在でも対応が可能な体制づくりなども期待される。

図表２．49　情報セキュリティに関する特徴的な取り組み、支援のあり方

所在地	業　種	内　容
広島県	加工組立型製造業	公的機関による無料の仕組みづくり応援および構築
広島県	加工組立型製造業	セキリュティーソフトを入れたり、クラウドを利用したり、別置きの情報保存装置の導入が精々であり、専門スキルを持った人材を置けるのは、規模が大きくならないと費用が出ない
広島県	加工組立型製造業	常に新しいセキュリティ管理をしておく
広島県	基礎素材型製造業	すぐ変化するためついていけない。国などが小規模の企業に無償でもダウンロードできるよう整備を進めてもらいたい
広島県	基礎素材型製造業	セキュリティ関係が重要なことだと認識していますが、何をどうすれば良いのかわかりません。また、その問題に対する予算もない
広島県	建設業	結局のところ、弊社みたいな小規模事業者の場合、社員がセキュリティ対策などせず、代表がすべてやるしかない。今回の働き方改革により、社員は休んでも経営者は無休。ある意味「365 日 24 時間働きますか？」状態
山口県	加工組立型製造業	私共の会社は情報が少なく、保管やシュレッダーで外部に出ないようにしている
山口県	加工組立型製造業	IT 補助金や経営持続化補助金などを有効に活用していきたいとは考えているが、情報セキュリティ関連する対策や設備にどういったものが対象になるのか理解できていない。その辺りの相談窓口やコンサルなど有効的な支援があれば知りたい
山口県	生活関連型製造業	能力に合わせ段階を踏んで教育してもらえる勉強会が、近場にあると助かる
山口県	卸売業, 小売業	通信インフラはもとより、国県市行政の意識と設備投資が低い。便利になり誰でも活用・利用できる社会になれば情報セキュリティについての考えも変わり、対策も変わってくる
山口県	その他	客先（医療機関）と接続している回線は専用線の閉域関として安全を確保しているものの画像診断を実施する医師の方はテレワークを行うことからインターネットを利用せざるを得ない。IP-VPN（IP Virtual Private Network）[6]等の技術も活用するが、どこまで安全が担保されるかはわからないところがある

[6] 点間の接続に、プロバイダなどの通信事業者の閉域 IP（Internet Protocol）ネットワーク網を使った通信技術のこと。通信業者と契約した人のみが利用できる閉ざされたネットワークを指す。

２．１．２．中小企業ヒアリング調査

ａ．調査の目的

中小企業における情報セキュリティリスクに対する認識、社内体制・対応、課題および効果的な支援等について把握する。

ｂ．ヒアリング先

アンケート回答のあった受入可能企業より企業規模、業種、所在地の網羅性 、セキュリティ対応・人材育成の優良性、特徴的な取り組み等の観点から５社を選定した（図表２．50)。

図表２．50　中小企業ヒアリング訪問先

	訪問先	従業員数	業　　種	主な製品サービス
①	Ａ社	300 人以上	基礎素材型製造業	金属製品製造
②	Ｂ社	10～29 人	その他	サービス業
③	Ｃ社	30～49 人	基礎素材型製造業	木材加工品製造・販売
④	Ｄ社	10～29 人	生活関連型製造業	印刷物請負
⑤	Ｅ社	10～29 人	基礎素材型製造業	非鉄金属製品製造・販売

ｃ．ヒアリング項目

ヒアリング項目は図表２．51 のとおり。

図表２．51　中小企業ヒアリング訪問先

Ⅰ．情報セキュリティの認識
Ⅱ．情報セキュリティリスク関連の取り組み
Ⅲ．社内対応体制
Ⅳ．セキュリティ人材の確保・育成
Ⅴ．セキュリティ情報の入手
Ⅵ．テレワークの実施状況
Ⅶ．情報セキュリティに関連して実施してほしい施策・支援

d．ヒアリング結果　概要

Ⅰ．情報セキュリティの認識

多くの企業が情報が流出した場合、企業の信用・存立に関わる事象となるとのイメージはあるものの、情報資産に関わるリスクの全体像が把握できていない。また、リスクが顕在化していないこともあり「何から手を付けたら良いのか分からない状況」の企業も少なくない。

一方で「人」の介在する部分こそリスクが高いとの認識から、セキュリティソフトの導入等を含め一般職員に負担なく従事してもらうための環境作りが重要であると考えている企業が複数みられる。

Ⅱ．情報セキュリティリスク関連の取り組み

情報セキュリティリスク関連の取り組みとしてはセキュリティソフトの導入、UTM 設置・最新セキュリティ機器への更新が多い。さらに生体（顔）認証の利用、ハードディスク暗号化を導入している企業もある。

重要データをネットワーク上にて送受信している企業では他のネットワークから分離された IP-VPN の構築等により万全なセキュリティを実現している。

一方で業務特性からの制約によりセキュリティソフトウェア等の導入することのできない企業もあり、インシデントが発生しているが、それすら気付かず被害が拡大することが危惧されている。

また、体制整備の面でセキュリティポリシー策定を検討している企業も複数あるが、独自での策定は困難を伴うため専門家派遣等の公的なサポートが期待されている。

さらに、情報セキュリティ対策の実効性の確保、職員の意識醸成に向けて、特に経営層の理解・リーダーシップ発揮（トップダウン指示等）が重要であるとされた。

Ⅲ．社内対応体制

企業規模が小さい場合、総務担当者または職員の中で IT に詳しい職員が他業務を兼務しつつ情報セキュリティ担当者となることが多い。他事業所を含め全社の情報セキュリティ業務を担当するとともに、情報セキュリティに関する知識が不十分であることもあり負担感が大きい。

このような状況に対し IT サポートサービスを活用し、トラブル発生時に総務担当者を介さずに、サポート企業とトラブル発生箇所が直接やりとりすることにより、担当者の負担を軽減しつつセキュアな状態を確保する体制の構築がみられた。

ただし、IT 設備の保守に関してはオフサイトでのサポートサービスでの対応は困難であるため、地元 IT 企業を利用するという使い分けがみられる。設備関連は小規模企業の担当者が完全にアウトソースできない部分ともいえる。

企業規模が大きい場合は IT 専任担当者が存在し、担当者は情報セキュリティに関する一定の知識・スキルを有するものの、基本的には直営対応であるため、この場合

も負担感は少なくない。ただし、インシデント発生時には直営で速やかに対応できるというメリットがある。

経験則上、従業員数 50 人未満の企業では専任担当者はおらず、100 人程度で専任担当１人、300～500 人規模の企業では３～４人程度といったコメントもみられた。

Ⅳ．セキュリティ人材の確保・育成

職員のセキュリティ教育に関しては「研修側（＝セキュリティ管理者・担当者)」および「受講側」とも時間確保が困難な状況にあり、セキュリティ教育を実施する場合の際の最大のネックとなっている。特に「受講側」が業務多忙であり、セキュリティ教育を実施する雰囲気になりづらいとのコメントもみられた。

職員への教育等は諦め、セキュリティ管理者側における対応のみ行うケースも少なくないが、この場合、「人」（受講者）の介在する余地が少なからず残るため、セキュリティリスクは極小化されることなく、存続することとなる。

社外研修についても「近隣での基礎的なセミナー」を希望するケースと「(基礎的なセミナーでは不十分であり）高度なセミナー」を希望するケースに二分される。そのため受講者知識・スキルに応じた複数レベルでのセミナー開催が求められる。

また、セミナーの内容について「実用性に乏しく、ニーズに即していない」とのコメントもあり、実際の被害事例への対応等の事例紹介への期待もみられた。

Ⅴ．セキュリティ情報の入手

情報セキュリティに関して入手したい情報は、主に「最新脅威」および「当該脅威に対する対策」である。情報は地元システム会社、情報機器メーカー等の営業担当者から入手することが多く、「最新脅威に対応するため、複数の相談先を確保している」とのコメントもみられた。

Ⅵ．テレワーク等の実施状況

新型コロナウイルス感染症流行により多くの企業においてテレワーク導入および Zoom 等によるオンライン会議が進展した。テレワーク導入企業の中には新たにセキュリティ対策を実施する企業もみられる一方で、Zoom についてはセキュリティに関する問題が指摘される状況にあり、漠然とした不安を抱えながら利用している企業も少なくない。

Ⅶ．情報セキュリティに関連して求める施策・支援

支援施策としては「最新脅威に関する情報提供」「相談窓口の設置」への要望が複数みられた。中小企業の中には IT 企業と疎遠である場合も少なくなく、緊急時にワンストップ対応や専門家派遣してくれる窓口が求められている。

さらに、緊急時以外にも社内情報システムに対し、ホワイトハッカーから攻撃を仕

掛けてもらい、セキュリティホールを発見・通知するという取り組み（「ホワイトハッカーペネストレーションテストサービス」）への要望もみられた。

また、補助金について、IT 関連はソフトウェアのみが対象となっているケースが多いが、テレワークのために新たに IT 機器を導入することもあり、ハードウェアも対象とすべきという意見がみられた。現状、自前のサーバで運用する企業にとっては補助金を受ける機会が限定的であるためである。

２．２．地域のキーパーソン発掘、整理

地域において高度なセキュリティノウハウ・スキルを持つ人材の発掘に向け、地域 IT 企業に対し情報セキュリティに関する事業展開等についてアンケート調査を行うとともに、アンケート回答企業よりヒアリング調査を行い、「情報セキュリティサービス事業者一覧表」としてとりまとめた。

なお、当初予定していた大学等教育機関の訪問については、新型コロナウイルス感染症流行の影響により困難となった。

２．２．１．情報セキュリティサービス事業に関するアンケート調査

ａ．調査の目的

地域におけるセキュリティ分野での連携および中核人材育成体制の構築のための基礎資料とするため、地域 IT 企業における情報セキュリティサービス事業の提供状況、提供サービス従事者数、情報セキュリティ関連の所有資格（人材育成）等について把握する。

ｂ．対象と方法

中国地域において情報通信業を営む企業（各県「情報産業協会」所属企業）　320 社を対象先に選定した。

調査は調査票を上述の企業に郵送で配布し、郵送またはインターネット回答により回収した。

ｃ．実施概要

・調査期間　　2020 年 10 月 13 日～10 月 30 日
・調査対象数　　320 件
・有効回答数　　123 件（有効回答率 38.4%）

d．回答結果　概要

Ⅰ．回答企業・事業所の概要

・回答企業・事業所の規模は「９人以下」～「300 人以上」までほぼ均等にばらつく

Ⅱ．情報セキュリティサービスの提供状況

・情報セキュリティサービス提供企業・事業所は回答企業の 27.6%
・提供サービスは「セキュアなシステム設計構築・運用（ファイアウォール、VPN、電子認証システム、セキュアサーバ等)」「障害復旧（データリカバリ、データバックアップ)」「監視（不正アクセス検知、ログ監視、ログ解析等)」の割合が高い
・各サービス提供企業が得意分野・業種、特徴的なサービスを有する

Ⅲ．新型コロナウイルスの影響

・回答企業・事業所の約 30%が「新型コロナウイルスの流行以降、情報セキュリティサービスに関連して変化があり」と回答。リモートワークの実施に伴うクラウド前提の業務内容へのシフトへの対応が増加している

Ⅳ．提供サービス従事者数

・情報セキュリティサービス事業の従事人員は「３人以下」が 44.1%。一方で「10 人以上」の企業も 20.6%ある

Ⅴ．提供サービス対象

・提供サービス対象業種は「情報通信業」「卸売業・小売業」が多い。製造業は約 20～35%の提供企業が主たる顧客としている

Ⅵ．所有資格

・所有資格は「情報セキュリティマネジメント」「情報処理安全確保支援士」の比率が高い。また、それらの前身の資格である「情報セキュリティアドミニストレータ」「情報セキュリティスペシャリスト」も同様に所有比率が高い。さらに、セキュリティポリシー関連サービスを提供している企業は監査関連の資格〔ISMS（Information Security Management System）[7]等〕を保有しているケースが多い

[7] 組織における情報資産のセキュリティを管理するための枠組み

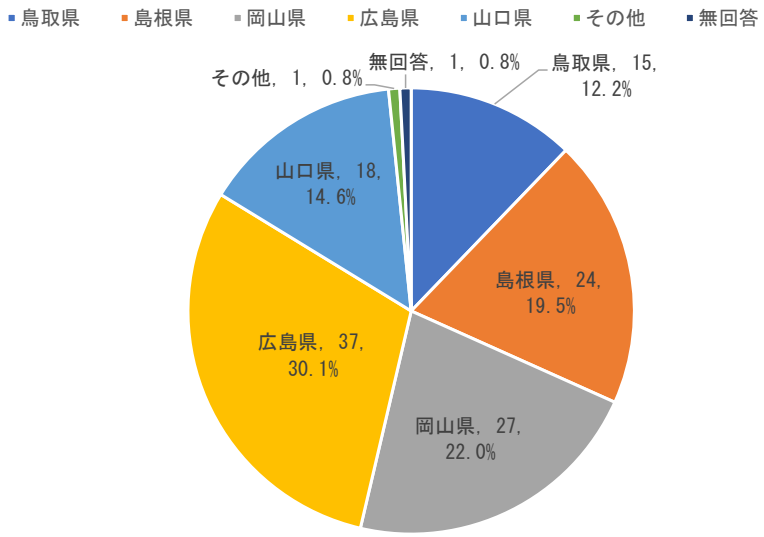
ｅ．回答結果

Ⅰ．回答企業・事業所の概要

問１．貴社・貴事業所の概要についてご記入ください
①所在地　（ｎ＝123）

回答企業・事業所の所在地は「広島県」（30.3%）が最も多く、次いで「岡山県」（22.0%）、「島根県」（19.5%）となっている（図表２．52）。

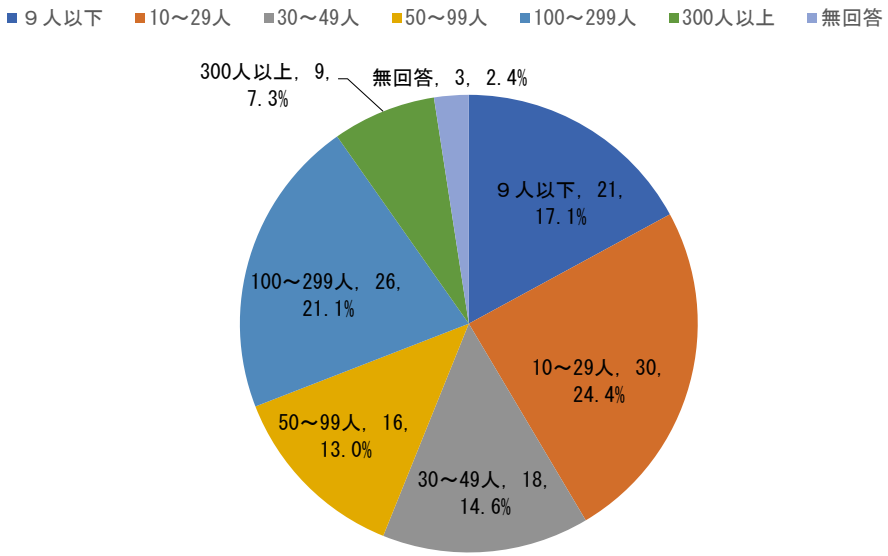
図表２．52　所在地（回答者）



②従業員数　（ｎ＝123）

回答企業・事業所の従業員数は「10～29人」（24.4%）が最も多く、次いで「100～299人」（21.1%）、「９人以下」（17.1%）となっている。30人未満が約４割を占めている（図表２．53）。

図表２．53　従業員数（回答者）

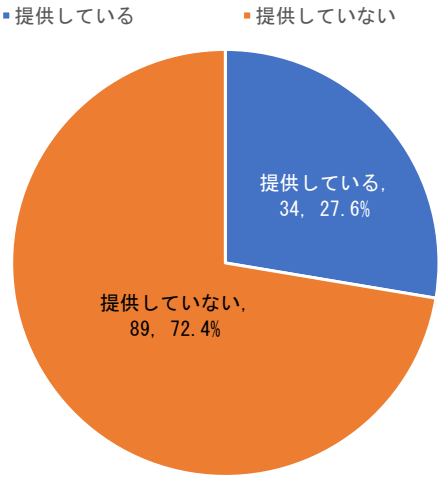


Ⅱ．情報セキュリティサービスの提供状況

問２．貴社・貴事業所では情報セキュリティサービスを提供していますか　（ｎ＝123）

情報セキュリティサービスを提供している企業・事業所は回答企業・事業所の 27.6%（34 企業・事業所）となっている（図表２．54）。

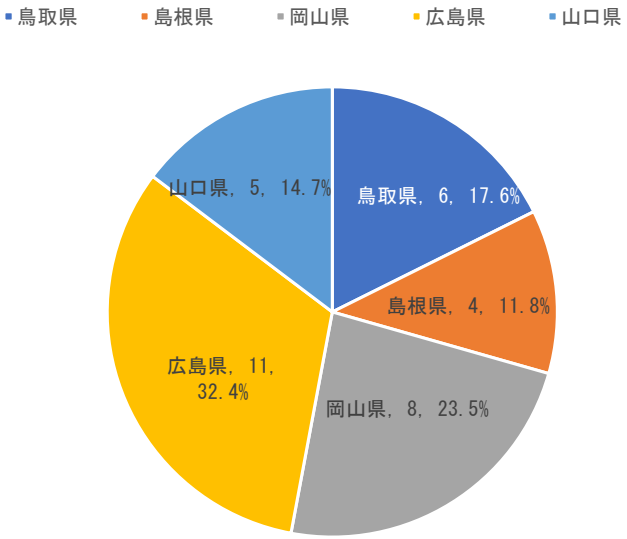
図表２．54　情報セキュリティサービスの提供状況



情報セキュリティサービス提供企業・事業所
①所在地　（ｎ＝34）

情報セキュリティサービス提供企業・事業所の所在地は「広島県」（32.4%）が最も多く、次いで「岡山県」（23.5%）、「鳥取県」（17.6%）となっている（図表２．55）。

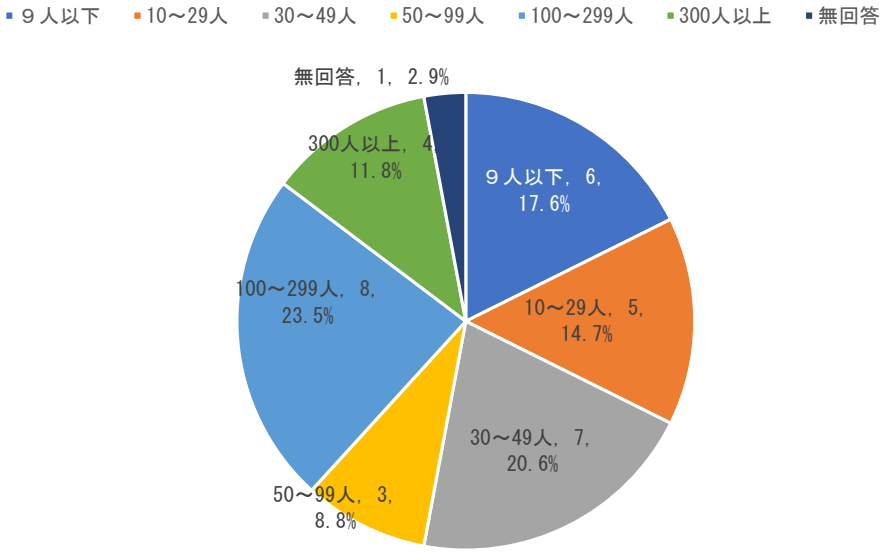
図表２．55　情報セキュリティサービス提供企業・事業所　所在地



情報セキュリティサービス提供企業・事業所
②従業員数　（ｎ＝34）

情報セキュリティサービス提供企業・事業所の従業員数は「100～299 人」(23.5) が最も多く、次いで「30～49 人以下」(20.6%) となっている。企業規模は比較的ばらつきがみられる（図表２．56)。

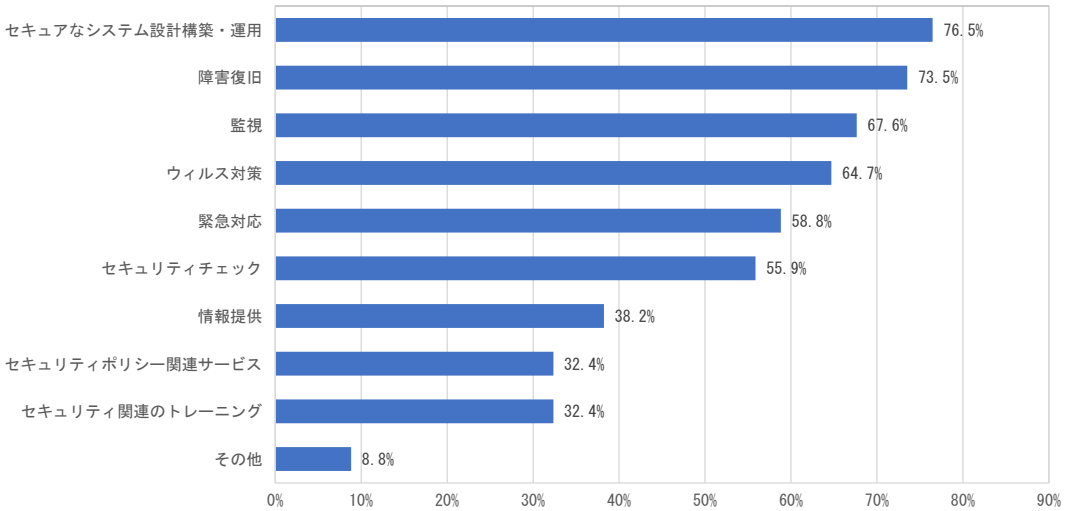
図表２．56　情報セキュリティサービス提供企業・事業所　従業員数



問３．問２で「1.はい」を選んだ方にお伺いします。貴社・貴事業所ではどのような情報セキュリティサービスを提供していますか　（ｎ＝34）

提供している情報セキュリティサービス（複数回答）は「セキュアなシステム設計構築・運用（ファイアウォール、VPN、電子認証システム、セキュアサーバ等)」(76.5%) が最も多く、次いで「障害復旧（データリカバリ、データバックアップ)」(73.5%)、「監視（不正アクセス検知、ログ監視、ログ解析等)」(67.6%) となっている（図表２．57)。

図表２．57　情報セキュリティ関連の提供サービス（複数回答）



・セキュアなシステム設計構築・運用＝ファイアウォール、VPN、電子認証システム、セキュアサーバ等
・障害復旧＝データリカバリ、データバックアップ　　・監視＝不正アクセス検知、ログ監視、ログ解析等
・緊急対応＝不正アクセスなどの被害を受けた際に、現場への急行、サービスを停止等
・セキュリティチェック＝監査、検査、診断　　・ウイルス対策＝ウイルス監視、ウイルス情報提供・アップデート
・情報提供＝不正アクセス関連情報など　　・.セキュリティ関連のトレーニング＝教育、研修

問４．問３に関連して貴社・貴事業所の提供している情報セキュリティサービスで特徴的なものがあればお答えください （ｎ＝34）

各提供企業・事業が得意分野（ハードウェア、ソフトウェア、サービス等)、得意対象業種〔民間企業(中小企業)、自治体等〕を有する（図表２．58)。

図表２．58　情報セキュリティサービスの特徴的

県	内　　容
鳥取県	監視については EDR（Endpoint Detection and Response）[8]というエンドポイント監視に注力
	サーバ機器、通信機器、ソリューション提供等、一括でのサービス提供を実施
	社内ネットワークのセキュリティ対策が得意。UTM や拠点間 VPN を絡めたなどのインフラ回線構築が強い
	中小事業者向けのセキュリティ対策サービス
	自治体向けにセキュアなシステムの提供、監視
島根県	情報資産の利用者としての個人レベルの対策から、管理としての対策、技術的な対策までを実習を交えて教育
	OSS（Open Source Software）[9]を利用してソリューションを構築しているため、OSS のセキュリティに関する情報を常に入手確認
	統合システム監視ソフトウェア Zabbix[10]を利用した死活監視・リソース監視
岡山県	設計・構築だけでなくネットワーク保守サービスの提供を行っています
	運用コンサルティング、インシデント発生時の調査対応サービス
	ISMS の審査実務を実施している審査員による研修やコンサルティングを実施
	LGWAN（Local Government Wide Area Network）[11]を利用したセキュリティサービスの提供
	サーバの構築、ネットワークの設計、施工、監視等
広島県	全方位的にセキュリティサービスを提供できるが、特にメールセキュリティサービス(SMX)は長期にわたり国内シェア１位となっている
	セキュリティ診断から監視、CSIRT（Computer Security Incident Response Team）[12]運用支援など、豊富な経験を持つセキュリティアナリストが顧客満足度の高いサービスを提供
	機密ファイル保護・管理システムの構築
	金融関係のセンター業務の運用
	シンクライアントソリューション
	監視サービス（リソース、メッセージ DB)ネットワークマネジメントサービス（ウイルス監視、不正侵入含）バックアップサービス、プリント事務代行サービス、定型オペレーションサービス等の IDC（Internet Data Center）サービス、ハウジング～クラウドサービスを提供。メール/ホームページについての多彩なセキュリティ機能を搭載したサービスシステムを提供
山口県	グループの各社に対してのみ実施している

Ⅲ．新型コロナウイルスの影響

問５．新型コロナウイルスの流行以降、貴社・貴事業所の提供している情報セキュリティサービスに関連して変化があればお答えください（例：問い合わせ件数・売上金額の増加、提供サービス内容の変化等） （ｎ＝34）

回答企業の約 30%が「新型コロナウイルスの流行以降、情報セキュリティサービスに関連して変化があり」と回答。リモートワークを含めクラウドを前提とした業務へのシフトに関する対応件数が増加している（図表２．59)。

図表２．59　新型コロナウイルスの影響

県	内　　容
鳥取県	EMOTET に関する問い合わせ増加、契約件数増加した
島根県	テレワーク推進に関わる案件・問い合わせが増加傾向にある
岡山県	VPN、リモートアクセス上のセキュリティ対策の相談数の増加
	テレワークに関する問い合わせが増加した
	テレワーク、Web ミーティングの相談、導入の案件が増加している。特に RDP（Remote Desktop Protocol）[13]接続の需要が増加している
	ISMS の審査において、オンライン審査の機会が増えた
	テレワーク商談（自宅からのセキュアな社内 NW への接続）が増加傾向。セキュリティ研修は集合型研修の中止が多く、オンライン型研修へ変化している

[8] ユーザーが利用するパソコンやサーバ（エンドポイント）における不審な挙動を検知し、迅速な対応を支援するソリューション
[9] 利用者の目的を問わずソースコードを使用、調査、再利用、修正、拡張、再配布が可能なソフトウェアの総称
[10] IT インフラストラクチャ・コンポーネントの可用性やパフォーマンスを監視するためのエンタープライズ向けソフトウェア
[11] 地方公共団体を相互に接続する行政専用のネットワーク
[12] セキュリティ事故対応チーム
[13] サーバコンピューターの画面をネットワークを通じて別のコンピューターに転送して表示・操作するリモートデスクトップ

図表２．59　新型コロナウイルスの影響（続き）

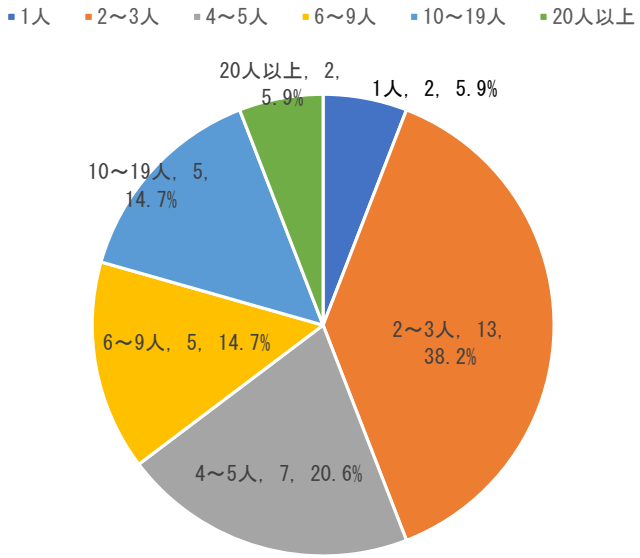
県	内　　容
広島県	テレワーク＋セキュリティでの引き合いがかなりの件数となった。導入後の運用なども採用のポイントとなっている
	リモートワークを中心にした、クラウド前提の業務内容へのシフトへの検討
	在宅勤務、テレワークを活用したサービスの利用相談が増加
	在宅勤務が可能なサービスを増強したため、それに関連する環境、機器、要員工数等について、売上が増加
	エモテットに関する問い合わせ増加、契約件数が増加
	テレワーク推進に関わる案件・問い合わせが増加傾向
	VPN、リモートアクセス上のセキュリティ対策の相談数の増加
山口県	テレワークに関する問い合わせが増加した

Ⅳ．提供サービス従事者数

問６．貴社・貴事業所で情報セキュリティサービス事業（問３で列挙したもの）に主に従事している従業員数についてお答えください（概算で結構です）　（ｎ＝34）

主に情報セキュリティサービス事業に従事している人員数は各企業・事業所において「２～３人以下」（38.2%）が最も多く、次いで「４～５人」（20.6%）となっている（図表２．60）。一方で「10 人以上」の大規模に事業展開を行う企業も 20.6%ある。

図表２．60　情報セキュリティサービス事業　従事者数

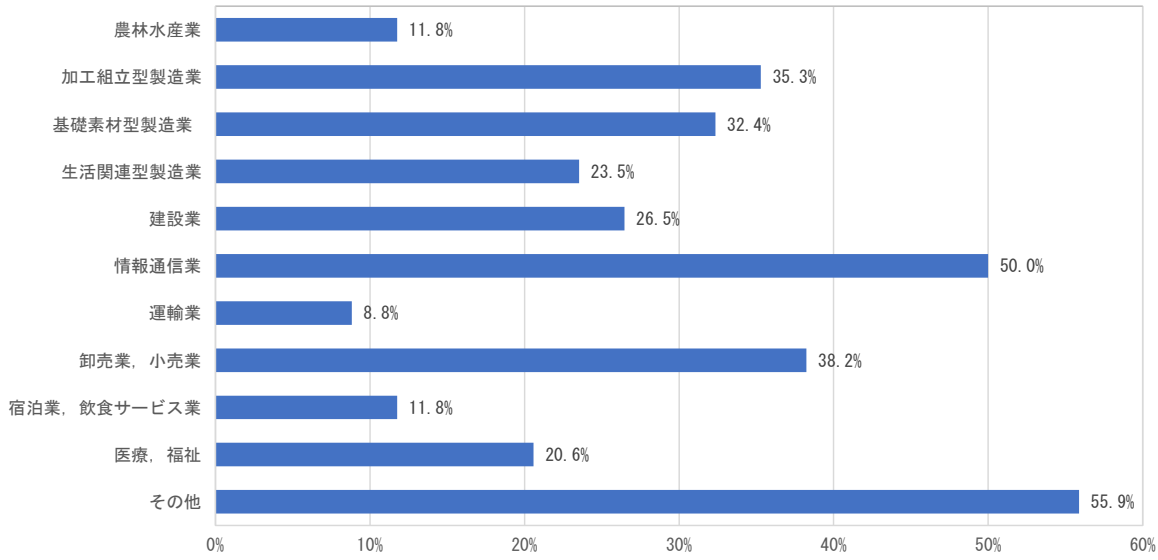


Ⅴ．提供サービス対象

問７．貴社・貴事業所の情報セキュリティサービス事業の主な顧客の業種をお答えください（複数回答）　（ｎ＝34）

情報セキュリティサービス事業における主な顧客の業種（複数回答）としては、「情報通信業」（50.0%）、「卸売業・小売業」（38.2%）と非製造業が上位となっている。一方、製造業では「加工組立型製造業」（35.3%）、「基礎素材型製造業」（32.4%）、「生活関連型製造業」（23.5%）の順となっている（図表２．61）。

図表２．61　主な顧客(業種)（複数回答）



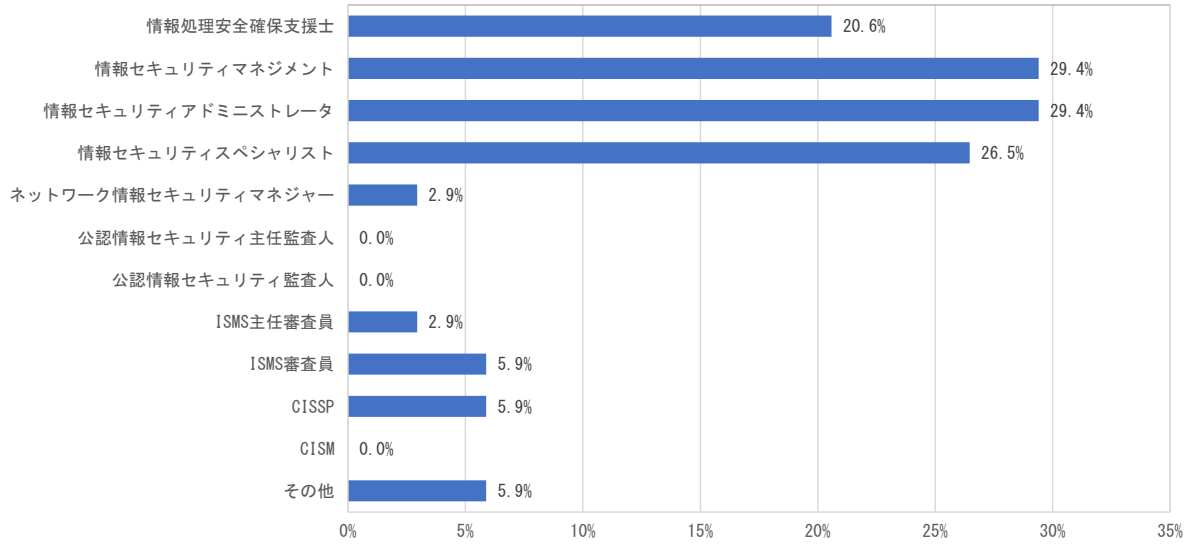
Ⅵ．所有資格

問８．貴社・貴事業所の情報セキュリティ関連従事者が取得している関連資格をお答えください（分かる範囲で結構です）　（ｎ＝34）

情報セキュリティ関連従事者が取得している関連資格（複数回答）としては現行の「情報セキュリティマネジメント」(29.4%)、「情報処理安全確保支援士」(20.6%）の割合が高い。また、それらの前身の資格である「情報セキュリティアドミニストレータ」(29.4%)、「情報セキュリティスペシャリスト」(26.5%）も同様に割合が高い（図表２．62)。

さらに、セキュリティポリシー関連サービスを提供している企業は監査関連の資格（ISMS 等）を保有しているケースが多い。

図表２．62　取得資格（複数回答）



２．２．２．情報セキュリティサービス事業者 ヒアリング調査

ａ．調査の目的

情報セキュリティサービス事業者のサービス内容および提供先の状況等について把握する。

ｂ．ヒアリング先

アンケート回答のあった受入可能企業より情報セキュリティサービスにおいて特徴的なサービス、多様なサービスを提供している３先を選定した（図表２．63)。

図表２．63　情報セキュリティサービス事業者　ヒアリング先

	訪問先	従業員数	セキュリティ関連要員	主なセキュリティ関連サービス
①	A社	９人以下	１人	ISMS 導入コンサルティング
②	B社	100～299 人	４～５人	運用コンサルティング、インシデント発生時の調査対応サービス
③	C社	300 人以上	６～９人	セキュリティ診断・監視、CSIRT 運用支援等

ｃ．ヒアリング項目

ヒアリング項目は図表２．64 のとおり。

図表２．64　情報セキュリティサービス事業者　ヒアリング項目

Ⅰ．情報セキュリティサービス事業の内容
Ⅱ．新型コロナウイルスの影響
Ⅲ．情報セキュリティ人材の確保・育成
Ⅳ．情報キュリティサービス提供先の課題
Ⅴ．情報セキュリティ関連の有効な支援・施策

d．ヒアリング結果　概要

Ⅰ．情報セキュリティサービス事業の内容

ヒアリング先は3先。①「ISMS 審査、IT コンサルティングサービス」を提供する「小規模事業者」、②「クラウド・インターネット接続サービスの一環としてのウイルス対策サービス」を提供する「中規模事業者」、③「情報インフラ管理・保守サービス、インフラ産業へのセキュリティ対応・トレーニング、SOC（Security Operation Center）[14]、NOC（Network Operation Center）[15]サービス」を提供する「大規模事業者」と企業規模・サービス内容も分かれる。

Ⅱ．新型コロナウイルス感染症の影響

新型コロナウイルス感染症流行によるテレワーク導入に伴い情報セキュリティ関連の問い合わせ件数が増加している。ワークスタイル変革に伴い新たな情報セキュリティリスクが発生するとともに、ISMS 審査業務においても、在宅ワーク等の審査対象が広がるなどの影響が出ている。

Ⅲ．情報セキュリティ人材の確保・育成

情報セキュリティ関連人材としては「セキュリティ専門人材」よりも「IT ゼネラリスト」として人材確保するとともに OJT にて育成されるケースが多い。セキュリティ業務もチーム制で行われることが多く、業務情報、セキュリティに関する情報も共有化が図られている。

情報セキュリティ担当者にはセキュリティに限定されない IT 全般の“幅広い深い知識”の蓄積が求められる。特定チャネルに依存した情報収集では十分といえず、有償セミナー・展示会への参加、IPA・ベンダーからの情報収集等と多様なチャネルを有するケースが多い。

Ⅳ．情報セキュリティサービス提供先の課題

サービス提供先のうち IT リテラシーが高くない企業では「セキュリティ対策」＝「コンピューターウイルス対策」となっている場合が多い。そのため情報セキュリティ対策の進展のためには、リスクは Web 上以外にもあることを認識してもらうことが重要であるとされた。

また、セキュリティ対策は直接利益を生み出すわけではないため、中小企業では取り組みに対して経営者の理解を得がたいケースも少なくない。セキュリティ対策は「費用」ではなく「投資」と考え、その「投資」を PR するという意識の変革が求められ

[14] 24 時間 365 日体制でネットワークやデバイスを監視し、サイバー攻撃の検出や分析、対応策のアドバイスを行う組織

[15] IT チームが通信ネットワークのパフォーマンスと健全性を常時監視する集中管理・運用する施設
NOC は、ネットワークのパフォーマンスと可用性の管理に特化しているのに対して、SOC ではセキュリティの専用ツールと専任スタッフが社内のセキュリティの状況を監視し、問題を検出、分析する

るとの提言があった。

セキュリティ対策は企業にとって、「役に立つのか」「どのくらいすればいいか」分かりづらいものであるが、ISMS を活用すれば「どのくらいのレベル」で「どれくらい対策を行うか」が判別でき、効果的なセキュリティ対策が可能となるとされた。

Ⅴ．情報セキュリティ関連の有効な支援・施策

情報セキュリティに対する意識向上のためには企業に対してその重要性を認識してもらうための広報活動が重要であり、特に IPA が制作している教材・動画はツールとして有効であるとされた。

また、サービス提供企業が最新の脅威情報を容易に収集できるような環境整備が求められている。現状では最新情報を収集する手段が限られているため、Web 検索等に頼らざるをえず、手間がかかっているとの指摘があった。

中小企業にとってはセキュリティに対して割ける時間は限定的であるため、専門家派遣事業は有効である。「どこに相談していいか分からない」という課題については身近な「商工会議所・商工会」等で人材バンクを構築し、相談の受け入れを行うことも一つの方法である。今の時代なら相談員が現地にいなくても Zoom 等で対応できるため体制構築は可能とされた。

３．サイバーセキュリティセミナー

３．１．サイバーセキュリティセミナー概要

国のサイバーセキュリティ月間（２月１日～３月 18 日）に合せ、中国地域２ヵ所（広島市、島根県松江市）においてサイバーセキュリティに関するセミナーを開催し、地域企業等のセキュリティに対する機運醸成を図った。

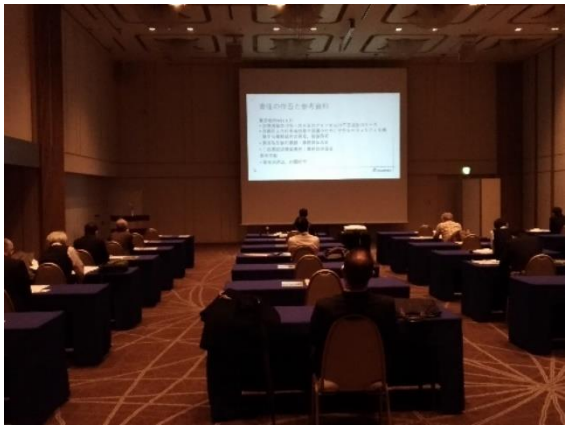
地域の中小企業・団体等の経営層、セキュリティ担当者等を対象に「2021 年 サイバーセキュリティセミナー in 広島／松江～ニューノーマル時代におけるサイバーセキュリティセミナー～」と題し、最近の脅威の傾向や事故後の対応、支援策などを紹介した。

なお開催方法にあたっては当初会場での講師による講演を予定していたが、新型コロナウイルス感染症の流行に伴い、オンライン（マイクロソフト　Teams）およびオンライン画面の会場上映に変更のうえ実施した。なお、実施内容・結果の概要は図表３．１のとおりである。

図表３．１　2021 年　サイバーセキュリティセミナー in 広島／松江の概要

区　分		広島会場	松江会場
日　時		2021 年３月４日（木）　13:30～16:30	2021 年３月５日（金）　13:30～16:30
聴講方法	ｵﾝﾗｲﾝ	マイクロソフト　Teams	
	会　場	ホテルグランヴィア広島 ４階　悠久の間（広島市南区松原町１－５）	松江エクセルホテル東急 ２階　オーク（島根県松江市朝日町 590）
募集人員		計 60 名（会場＋Web）／会場	
参加人数		計 57 名（会場　15 名、Teams　42 名）	計 25 名（会場　11 名、Teams　14 名）
内容	講演①	「情報セキュリティ 10 大脅威とその対策」 （独法）情報処理推進機構　セキュティセンター　セキュリティ対策推進部 脆弱性対策グループリーダー　渡辺　貴仁	
	講演②	「情報セキュリティ事故後の法的対応と経営リスク」光雲法律事務所 弁護士 吉井 和明	
	講演③	「情報セキュリティの考え方と取り組み」（株）広瀬印刷　代表取締役社長　瀬尾　淳	
	情報提供	「中小企業におけるセキュリティ対策支援の紹介」 （独法）情報処理推進機構 セキュティセンター 企画部 中小企業支援グループ 鈴木 浩之	
主　催		中国経済産業局、中国総合通信局、中国地域サイバーセキュリティ一連絡会	
後　援		サイバーセキュリティ戦略本部、中国経済連合会	

図表３．２　広島会場（３月４日）



松江会場（３月５日）

図表３．３　サイバーセキュリティセミナー in 広島／松江　募集チラシ

３．２．サイバーセキュリティセミナーの内容

①「情報セキュリティ 10 大脅威とその対策」

（独法）情報処理推進機構　セキュティセンター　セキュリティ対策推進部
脆弱性対策グループリーダー　渡辺　貴仁

IPA が選定する「情報セキュリティ 10 大脅威（「個人」向け・「組織」向け)」のうち「組織」向け脅威 上位６位について詳細に説明するとともに、まとめとして情報セキュリティ対策の基本について説明を行った。

②「情報セキュリティ事故後の法的対応と経営リスク」

光雲法律事務所　弁護士　吉井　和明

経営リスクを生じさせる情報セキュリティ事故および主に「裁判」および「個人情報」に関連する企業対応について説明を行った。加えて企業の関心の高い損害金額等についても言及した。

③「情報セキュリティの考え方と取り組み」

（株）広瀬印刷　代表取締役社長　瀬尾　淳

P マーク取得のための取り組みと社内への影響およびその経験を活かした新規事業への展開について説明を行った。併せて新型コロナウイルス感染症対策としてのテレワーク環境についても言及した。

④「中小企業におけるセキュリティ対策支援の紹介」

（独法）情報処理推進機構 セキュティセンター 企画部 中小企業支援グループ 鈴木 浩之

「SECURITY ACTION」「情報セキュリティ対策ガイドライン」「サイバーセキュリティお助け隊」を中心とした中小企業向け支援事業、IPA のツール・制度等について説明を行った。

４．社会人セキュリティ人材育成実証事業

４．１．サイバーセキュリティ講座 カリキュラムマップ

４．１．１．サイバーセキュリティ講座 カリキュラムマップ概要

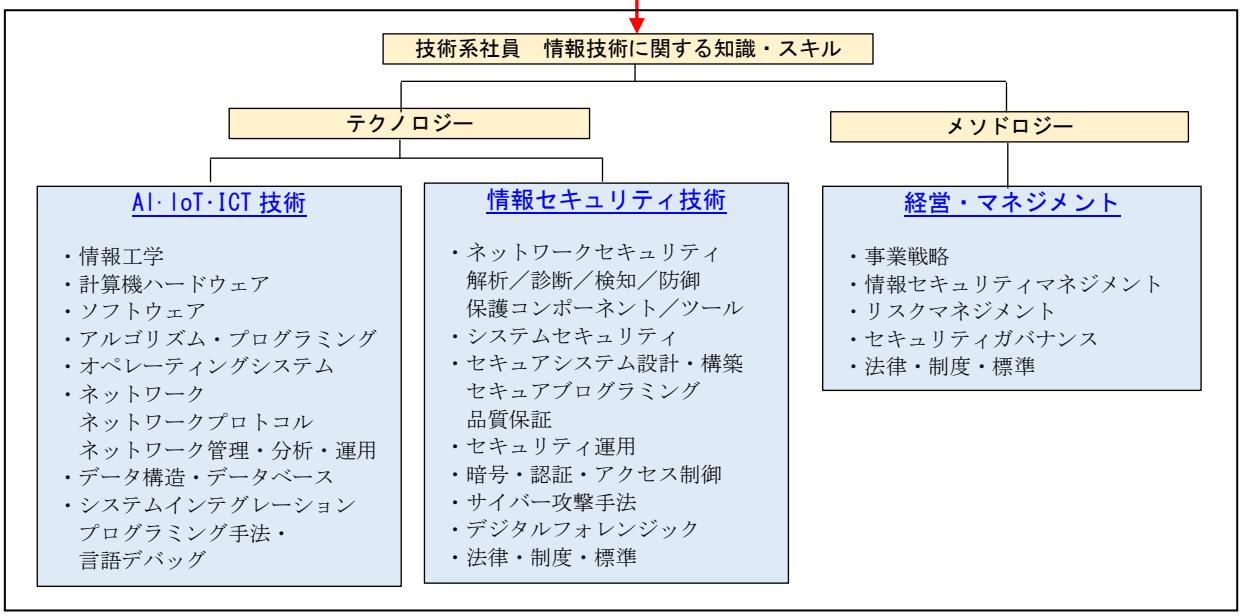
情報セキュリティに関する知識・スキルの習得を目指す中小企業等の実務者リーダーや技術者、経営層等が、各自のレベル・目的に応じた効率的な学習を可能とするため、情報セキュリティ人材の育成に先進的に取り組んでいる中国地域内外の大学等での社会人向けセキュリティ講座の調査を行い、当該セキュリティ講座をスキルレベルごとに整理したマップ（＝「カリキュラムマップ」）を作成した。

４．１．２．企業人材に求められる知識・スキル

サイバーセキュリティ講座 カリキュラムマップの作成にあたり対象である企業人材（主に技術系人材）に求められる関連知識・スキルを図表４．１のとおり整理する。

図表４．１　企業人材に求められる知識・スキル（IT・セキュリティ関連）

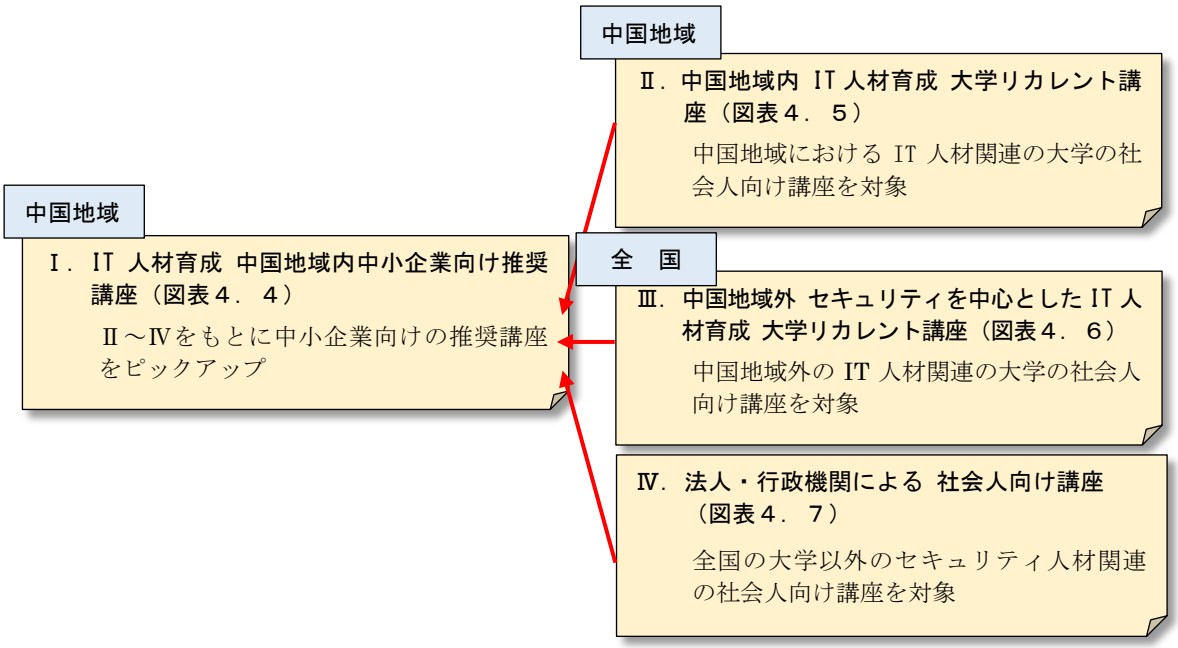
社内人材	部　　門	修得が求められる情報技術に関する知識・業務内容
一般社員	間接部門 （経理・調達・営業・人事）	・情報セキュリティリテラシー（情報漏えいを防ぐルールの遵守）
主たる対象 技術系	生産部門 （生産技術・設備管理・品質保証）	・情報セキュリティリテラシー（情報漏えいを防ぐルールの遵守） ・生産設備（工場）ネットリークの構築・運用・セキュリティ管理 生産工程における各種データ（生産効率・品質維持など）の収集・解析 ・法・制度・標準に関する知識と品質管理業務への適用
	開発部門 （研究開発・設計）	・情報セキュリティリテラシー（情報漏えいを防ぐルールの遵守） ・AI・IoT・ICT に関する知識とこれらを活用する技術 ・サイバーセキュリティに関する知識と、脆弱性を評価・改善する技術 ・法・制度・標準に関する知識と製品への適用
	情報システム部門 （社内インフラ構築・運用）	・情報セキュリティリテラシー（情報漏えいを防ぐルールの遵守） ・社内情報システムの構築・運用・管理・情報セキュリティ推進 ・インシデント対応 ・法・制度・標準に関する知識と情報セキュリティ業務への適用
経営・管理	経営・部門統括	・情報セキュリティガバナンス・マネジメント ・インシデント対応 ・法・制度・標準に関する知識



４．１．３．サイバーセキュリティ講座 カリキュラムマップ

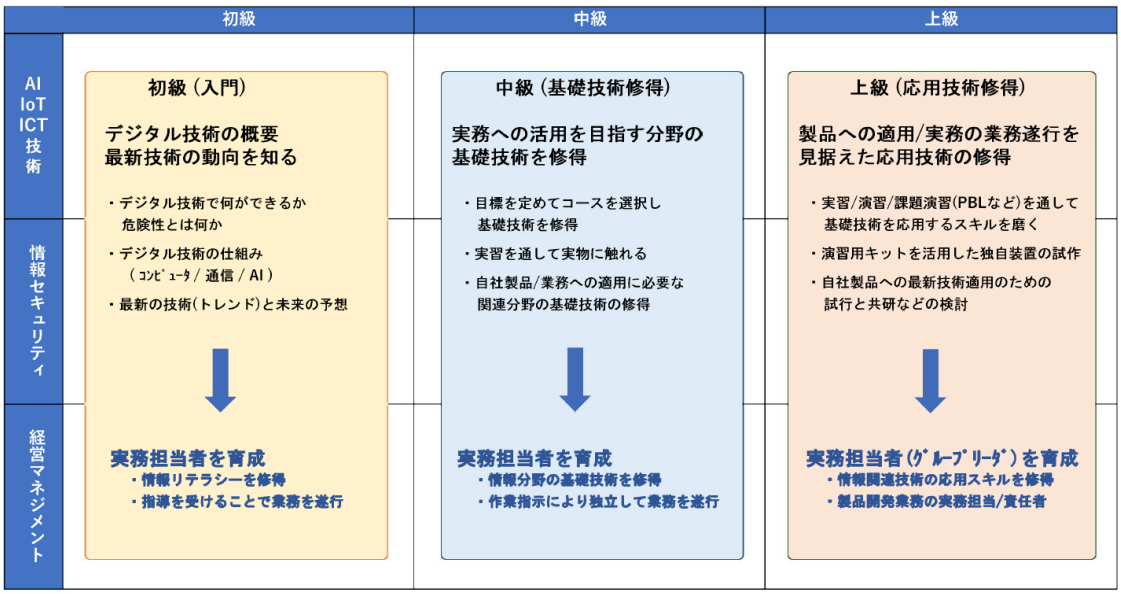
図表４．１の情報セキュリティに関連して企業人材に求められる知識・スキルをもとに中国地域内外のサイバーセキュリティ講座を取りまとめるとともに、地域の中小企業向けに推奨講座のピックアップを行った（図表４．２）。

図表４．２　サイバーセキュリティ講座 カリキュラムマップ　概要



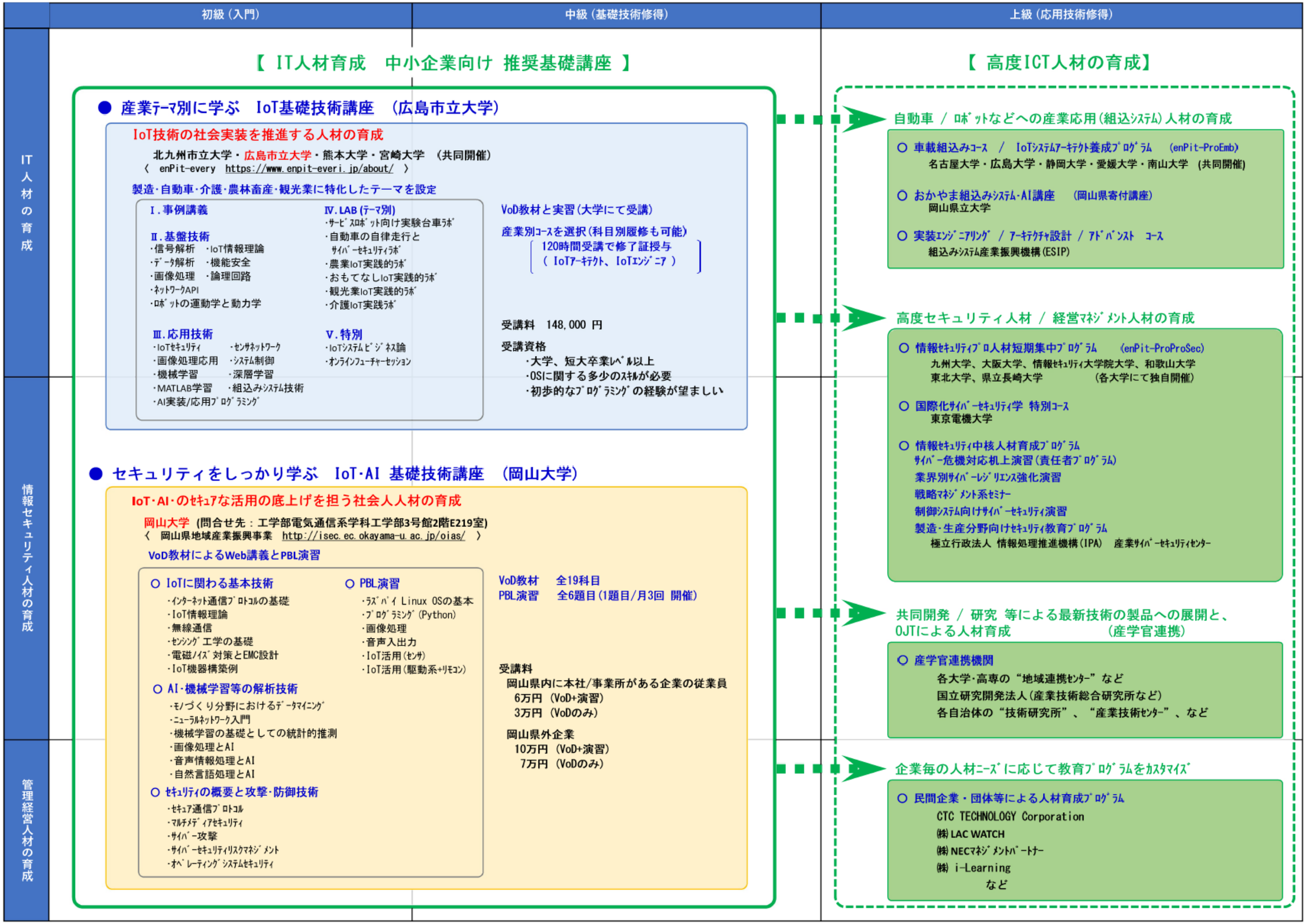
カリキュラムマップ縦軸に対象人材（IT 人材、情報セキュリティ人材、経営管理人材）、横軸に難易度（「初級（入門）」「中級（基礎技術習得）」「上級（応用技術習得）」）で各講座をプロットしたものである。カリキュラムマップの対象人材、難易度の考え方は図表４．３に示す。

図表４．３　カリキュラムマップの考え方



白　紙

図表４．４　IT 人材育成 中国地域内中小企業向け推奨講座



図表４．５　中国地域内 IT 人材育成 大学リカレント講座

	初級（入門）	中級（基礎技術修得）	上級（応用技術修得）
IT人材の育成	**組込みｼｽﾃﾑ技術者の育成（広島大学 / 岡山県立大学）** **組込みｼｽﾃﾑ技術者の育成** 〈enPit-ProEmb https://www.nces.i.nagoya-u.ac.jp/enpit-pro-emb/ ： 名古屋大学・広島大学・静岡大学・愛媛大学・南山大学〉 ○ 車載組込みｺｰｽ （名古屋大学・広島大学） ：受講料 40万円/人 受講期間 1年間(通学による受講 修了条件 履修時間が120時間以上 履修証明ﾌﾟﾛｸﾞﾗﾑ） 厚労省「教育訓練給付金制度」と連携 ・ﾘｱﾙﾀｲﾑ性保証技術 ・ﾘｱﾙﾀｲﾑOSの内部構造 ・組込みｼｽﾃﾑのｾｰﾌﾃｨ/ｾｷｭﾘﾃｨ入門 ・ﾏﾙﾁﾌﾟﾛｾｯｻ用RTOS内部構造/ｱﾌﾟﾘ開発 ・FPGAを用いた ﾊｰﾄﾞｳｪｱ/ｿﾌﾄｳｪｱ ｺﾃﾞｻﾞｲﾝ ・ｿﾌﾄｳｪｱ 品質/信頼性評価/構成管理 演習 ・C-ﾌﾟﾛｸﾞﾗﾐﾝｸﾞ入門 ・AUTOSAR CP概論/AP入門 ・ｶｰｴﾚｸﾄﾛﾆｸｽ ・分散ｼｽﾃﾑとｸﾗｳﾄﾞ技術 ・IoT環境における画像処理/理解技術 ○ IoTｼｽﾃﾑｱｰｷﾃｸﾄ養成ﾌﾟﾛｸﾞﾗﾑ （静岡大学・愛媛大学・南山大学） ：計16日間日帰り実習 受講料 36万円/人（会員は割引） 3年程度の実務（ﾌﾟﾛｸﾞﾗﾐﾝｸﾞ）経験者向け ・IoTﾊﾝｽﾞｵﾝ ・ｿﾌﾄｳｪｱ品質と検証技術 ・統計解析入門 ・IoT環境における画像処理/理解技術 ・IoT環境における知的情報処理技術 ・IoT実践演習 **組込みｼｽﾃﾑ技術者の育成** 〈岡山県地域産業振興事業 寄付講座 https://www.oka-pu.ac.jp/info/info_detail/index/event/107.html?type=event： 岡山県立大学地域共同研究機構 COC+推進室〉 ○ おかやま組込みｼｽﾃﾑ・AI講座 ：講義（18ｺﾏ 各60分）・演習（全6ｺﾏ 各80分）ともｵﾝﾗｲﾝ 受講料3万円/人（県内企業は2万円/人、演習ｷｯﾄ費用（～2万円）別途必要） ・組込みｼｽﾃﾑ基礎 （組込ｼｽﾃﾑとは / ﾊｰﾄﾞｳｪｱと開発環境 / 開発ﾌﾟﾛｾｽと要求分析 / 基本設計 / 詳細設計 / ﾃｽﾄ・検証 / 応用と要素技術） ・組込みﾌﾟﾛｸﾞﾗﾐﾝｸﾞ基礎 （C言語概論（1）（2） / 組込みﾏｲｺﾝ制御演習（1）（2）） ・組込みAI基礎 （組込AI概論（1）（2）（3））		
	IoTの入門～基礎技術を修得し、応用技術をﾃｰﾏ別に学ぶ（広島市立大学） **IoT技術の社会実装を推進する人材の育成** 〈enPit-every https://www.enpit-everi.jp/about/ ： 北九州市立大学・広島市立大学・熊本大学・宮崎大学〉 製造・自動車・介護・農林畜産・観光業に特化したテーマを選択 ： VoDと大学において演習を受講(120時間履修により修了証授与) 受講料148,000円/人 初歩的なﾌﾟﾛｸﾞﾗﾐﾝｸﾞの経験が望ましい **Ⅰ．事例講義** ・製造業IoT(工場のIoT導入) ・自動運転とﾓﾋﾞﾘﾃｨ ・ｽﾏｰﾄ農林畜産 ・ｽﾏｰﾄﾗｲﾌｹｱ ・おもてなしIoT **Ⅱ．基盤技術** ・信号解析 ・IoT情報理論 ・ﾃﾞｰﾀ解析 ・機能安全 ・画像処理 ・論理回路 ・ﾈｯﾄﾜｰｸAPI ・ﾛﾎﾞｯﾄの運動学と動力学 **Ⅲ．応用技術** ・IoTｾｷｭﾘﾃｨ ・ｾﾝｻﾈｯﾄﾜｰｸ ・画像処理応用 ・ｼｽﾃﾑ制御 ・機械学習 ・深層学習 ・MATLAB学習 ・組込みｼｽﾃﾑ技術 ・AI実装/応用ﾌﾟﾛｸﾞﾗﾐﾝｸﾞ **Ⅳ．LAB（ﾃｰﾏ別）** ・ｻｰﾋﾞｽﾛﾎﾞｯﾄ向け実験台車ﾗﾎﾞ ・自動車の自律走行とｻｲﾊﾞｰｾｷｭﾘﾃｨﾗﾎﾞ ・農業IoT実践的ﾗﾎﾞ ・おもてなしIoT実践的ﾗﾎﾞ ・観光業IoT実践的ﾗﾎﾞ ・介護IoT実践ﾗﾎﾞ **Ⅴ．特別** ・IoTｼｽﾃﾑﾋﾞｼﾞﾈｽ論 ・ｵﾝﾗｲﾝﾌｭｰﾁｬｰｾｯｼｮﾝ	
情報セキュリティ人材の育成	**IoT・AIのｾｷｭｱな活用を目指す人材を育成（岡山大学）** **IoT・AI・のｾｷｭｱな活用の底上げを担う社会人人材の育成** 〈岡山県地域産業振興事業 http://isec.ec.okayama-u.ac.jp/oias/ ： 岡山大学〉 VoD教材によるWeb講義とPBL演習 ： VoD 全19科目 演習 全6題目(1題目/月3回開催) 受講料 6万円(VoD+演習)/人 3万円(VoDのみ)/人 （県外企業については、各10万円/人 7万円/人） ○ IoTに関わる基本技術 ・ｲﾝﾀｰﾈｯﾄ通信ﾌﾟﾛﾄｺﾙの基礎 （ｲﾝﾀｰﾈｯﾄにおける情報伝送のしくみの概観 / ｲﾝﾀｰﾈｯﾄにおける通信ﾌﾟﾛﾄｺﾙ群 / ｱﾌﾟﾘｹｰｼｮﾝ層ﾌﾟﾛﾄｺﾙ（1）（2） / ﾈｯﾄﾜｰｸ層ﾌﾟﾛﾄｺﾙ（1）（2） / ﾃﾞｰﾀﾘﾝｸ層ﾌﾟﾛﾄｺﾙ（1）（2） / 物理層ﾌﾟﾛﾄｺﾙ ） ・IoT情報理論 （序論 / 情報理論で扱う問題 / 情報源 / 通信路 / 通信符号化 / 軟判定複号 / 信頼度情報の精度） ・無線通信 （無線通信の概要 / 電波の性質 / 無線通信を支える基盤技術 / 無線通信ｼｽﾃﾑの具体例） ・ｾﾝｼﾝｸﾞ工学の基礎 （電気電子計測の基礎 / ｾﾝｻ信号処理 / 各種ｾﾝｻ（1）（2）） ・電磁ﾉｲｽﾞ対策とEMC設計 （電磁ﾉｲｽﾞと発生のしくみ / 電磁ﾉｲｽﾞの評価法 / ﾉｲｽﾞ対策部品と使用法 / IoTﾊｰﾄﾞｳｪｱに対する脅威 / 電磁ﾉｲｽﾞの伝搬 / 電磁ﾉｲｽﾞの共振 / 電磁ﾉｲｽﾞの放射と遮蔽 / ｻｲﾄﾞﾁｬﾝﾈﾙ情報漏洩のﾒｶﾆｽﾞﾑ） ・IoT機器構築例 （IoTﾃﾞﾊﾞｲｽ準備（RaspberryPi3） / ｶﾒﾗの接続と動画配信 / CAN接続されたﾓｰﾀの駆動） ○ AI・機械学習等の解析技術 ・ﾓﾉづくり分野におけるﾃﾞｰﾀﾏｲﾆﾝｸﾞ （ﾃﾞｰﾀﾏｲﾆﾝｸﾞの基礎 / ﾃﾞｰﾀをｸﾞﾙｰﾌﾟ化する / ﾃﾞｰﾀから特徴を抽出する / ﾃﾞｰﾀから将来傾向を予測する / ﾃﾞｰﾀﾏｲﾆﾝｸﾞの実践（量的ﾃﾞｰﾀ）（時系列ﾃﾞｰﾀ）） ・ﾆｭｰﾗﾙﾈｯﾄﾜｰｸ入門 （ﾃﾞｰﾀへの直線・曲線のあてはめ / ﾆｭｰﾗﾙﾈｯﾄﾜｰｸとその学習法 / 深層ﾆｭｰﾗﾙﾈｯﾄﾜｰｸ） ・機械学習の基礎としての統計的推測 （確率論の基礎 / 確率論の基礎 ﾍﾞｲｽﾞの公式 / 最尤推定） ・画像処理とAI （AIによる画像認識 / AIによる画像の変化検出 / AIのﾗｲﾌﾞﾗﾘと利用法） ・音声情報処理とAI （音声生成過程とﾓﾃﾞﾘﾝｸﾞ１～３） / 音声の特徴１～３ / 音声合成 / 音声合成（深層学習）） ・自然言語処理とAI （自然言語処置の基礎と近年の話題 / 実習（機械学習（SVMによるﾃｷｽﾄ分類） / 実習（機械学習によるﾃｷｽﾄ分類）） ○ ｾｷｭﾘﾃｨの概要と攻撃・防御技術 ・ｾｷｭｱ通信ﾌﾟﾛﾄｺﾙ （通信に対する様々な脅威 / 暗号の概要 / 一方向ﾊｯｼｭ関数 / ﾒｯｾｰｼﾞ認証ｺｰﾄﾞ / ﾃﾞｼﾞﾀﾙ署名 / SSL/TLS） ・ﾏﾙﾁﾒﾃﾞｨｱｾｷｭﾘﾃｨ （電子透かし技術の概要 / ｽﾍﾟｸﾄﾙ拡散型電子透かし / 量子化型電子透かし / 改ざん検知 / ﾃﾞｼﾞﾀﾙﾌｫﾚﾝｼﾞｸｽ / ﾌｪｲｸｺﾝﾃﾝﾂの識別） ・ｻｲﾊﾞｰ攻撃 （ｻｲﾊﾞｰ攻撃の概要（1）（2） / ﾏﾙｳｪｱ感染と対策（1）（2） / ｻｰﾊﾞへの攻撃と対策（1）（2）） ・ｻｲﾊﾞｰｾｷｭﾘﾃｨﾘｽｸﾏﾈｼﾞﾒﾝﾄ （ﾘｽｸﾏﾈｼﾞﾒﾝﾄとは / ﾘｽｸﾏﾈｼﾞﾒﾝﾄﾌﾟﾛｾｽ（1）（2） / ﾘｽｸｱｾｽﾒﾝﾄとﾘｽｸ対応（1）（2）） ・ｵﾍﾟﾚｰﾃｨﾝｸﾞｼｽﾃﾑｾｷｭﾘﾃｨ （OSの機能概要 / ﾌﾟﾛｾｽ管理とﾌﾟﾛｸﾞﾗﾑ / ﾒﾓﾘ管理とﾒﾓﾘ保護 / ｱｸｾｽ制御 / 強制ｱｸｾｽ制御 / ﾒﾓﾘ破壊の脆弱性）		
管理経営人材の育成			

図表４．６　中国地域外 セキュリティを中心とした IT 人材育成 大学リカレント講座

	初級（入門）	中級（基礎技術修得）	上級（応用技術修得）

IT人材の育成

コースを選択して基礎技術を学び、演習を通して応用技術を修得（金沢工業大学）

入門から応用・実装までをｻﾎﾟｰﾄするIoT人材育成講座　〈KIT情報技術教育　https://www.kanazawa-it.ac.jp/kit-ite/　：　金沢工業大学〉

全13科目/3ｺｰｽ（学生とともに受講、夏季集中講義 8/1～9/22、春季集中講義 2/1～3/31）　受講料 144,000円/人（ｺｰｽ内指定科目6単位　履修証明ﾌﾟﾛｸﾞﾗﾑ　ﾃｷｽﾄ・教材費別途必要））

○ AIとﾋﾞｯｸﾞﾃﾞｰﾀ ｺｰｽ

(AIの基礎)	(ﾃﾞｰﾀｻｲｴﾝｽの基礎)	(AI応用　演習)
①AIの概念と基本的仕組み	①ﾌﾟﾛｸﾞﾗﾐﾝｸﾞ(Python)の基礎	①深層学習(画像識別手法)
②画像認識・自然言語処理・音声認識などの活用術	②統計的検定手法・回帰分析などの多変量解析	②形態素解析・構文解析
③機械学習に必要な基礎的なﾃﾞｰﾀ処理法	③ｸﾗｽﾀｰ分析・ﾃﾞｰﾀﾏｲﾆﾝｸﾞ	③scikit-learnを用いたﾋﾞｯｸﾞﾃﾞｰﾀの解析

○ IoTとﾛﾎﾞﾃｨｸｽ ｺｰｽ

(IoTの基礎)	(ﾛﾎﾞﾃｨｸｽの基礎)	(IoT応用　演習)
①IoTの概要と基本的な仕組み	①IoTｼｽﾃﾑ構築のためのC言語	①IoTｴｯｼﾞﾃﾞﾊﾞｲｽの知識と技術
②ｺﾝﾋﾟｭｰﾃｨﾝｸﾞ技術・通信方式	②ﾘｱﾙﾀｲﾑOSのﾌﾟﾛｸﾞﾗﾐﾝｸﾞ	②MATLAB/Simulinkによる制御系設計
③ｾｷｭﾘﾃｨの基礎	③PID制御などの制御理論	③Linuxﾄﾞﾗｲﾊﾞﾌﾟﾛｸﾞﾗﾐﾝｸﾞ

○ ICTと情報ｾｷｭﾘﾃｨ ｺｰｽ

(ICTの基礎)	(情報ﾈｯﾄﾜｰｸの基礎)	(ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ　演習)
①基本的なﾌﾟﾛｸﾞﾗﾐﾝｸﾞ手法	①TCP/IPの基礎	①ﾈｯﾄﾜｰｸへの攻撃手法と対策技術
	②ﾈｯﾄﾜｰｸの各階層の役割とﾌﾟﾛﾄｺﾙ	②暗号理論と実装
	③ﾈｯﾄﾜｰｸ状況の把握方法	

情報セキュリティ人材の育成

学部卒ﾚﾍﾞﾙ対象の情報ｾｷｭﾘﾃｨﾌﾟﾛ人材育成ﾌﾟﾛｸﾞﾗﾑ

enPit-ProProSec
情報ｾｷｭﾘﾃｨﾌﾟﾛ人材育成短期集中ﾌﾟﾛｸﾞﾗﾑ

ｾｷｭﾘﾃｨ技術・ﾀﾞｲﾊﾞｰｼﾃｨｰ力・ｺﾐｭﾆｹｰｼｮﾝ力を修得〈 https://cy2sec.comm.eng.osaka-u.ac.jp/miyaji-lab/pro-sec/index-jp.html 〉
大阪大学　VoD+PBL演習（全14単位、1講義2単位 15回×90分、8単位以上で履修証明書授与）　受講料 1単位14,400円 入学金28,200円　検定料9,800円

○ ｻｲﾊﾞｰｾｷｭﾘﾃｨ系
包括的ｻｲﾊﾞｰｾｷｭﾘﾃｨ演習(PBL)/ﾈｯﾄﾜｰｸﾄﾗﾌｨｯｸ処理の基盤技術と実装/高度ｾｷｭｱﾈｯﾄﾜｰｸ設計演習

○ 暗号系
公開暗号の設計と解読PBL/ﾃﾞｰﾀ活用のための準同型暗号PBL/情報ｾｷｭﾘﾃｨとｱﾙｺﾞﾘｽﾞﾑ/ｾｷｭﾘﾃｨ基盤技術(離散数学と計算の理論)

ｾｷｭﾘﾃｨを考慮した情報ｼｽﾃﾑの構築を可能とする人材を育成　〈 http://sun.ac.jp/siebold/sec/enPiT-prosec/ 〉
長崎県立大学　ﾒｲﾝｺｰｽ 120時間（15ｺﾏ×5科目）　修了認定証授与　受講料 118,400円

○ ｾｷｭﾘﾃｨ実践者・開発者向けﾒｲﾝｺｰｽ
SMBｾｷｭﾘﾃｨ対策の理論と実践 / ﾃﾞｰﾀｾｷｭﾘﾃｨ / 計算量安全暗号 / 情報理論的安全暗号 / ｾｷｭｱ開発技術（人工知能技術・数理科学とその応用） / ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ / 情報ｾｷｭﾘﾃｨとｴｺﾉﾐｸｽ）

○ ｾｷｭﾘﾃｨ実践者・開発者向けﾊｰﾌｺｰｽ
（ﾒｲﾝｺｰｽから2科目を選択）

設計・開発段階でのｾｷｭﾘﾃｨ対策が可能な人材育成　〈enPit-Pro ProSec https://cs.kyushu-u.ac.jp/enpit-pro/ 〉
九州大学　ﾒｲﾝｺｰｽ 67.5時間（必修）＋144時間（選択）　履修証明書交付（120時間以上履修）　受講料 205,800円（ﾒｲﾝｺｰｽ）

○ ﾒｲﾝｺｰｽ
情報ｼｽﾃﾑｾｷｭﾘﾃｨ演習(webｾｷｭﾘﾃｨ演習・ﾓﾊﾞｲﾙﾌﾟﾛｸﾞﾗﾐﾝｸﾞ・ｻｲﾊﾞｰﾚﾝｼﾞ演習)/ｾｷｭﾘﾃｨｴﾝｼﾞﾆｱﾘﾝｸﾞ演習/暗号と情報ｾｷｭﾘﾃｨ/情報ﾈｯﾄﾜｰｸ/情報ｼｽﾃﾑとｾｷｭﾘﾃｨ/ｲﾝｼﾃﾞﾝﾄ対応のための机上演習

○ ｸｲｯｸｺｰｽ
情報ｾｷｭﾘﾃｨ演習（webｾｷｭﾘﾃｨ演習・ﾓﾊﾞｲﾙﾌﾟﾛｸﾞﾗﾐﾝｸﾞ・ｻｲﾊﾞｰﾚﾝｼﾞ演習） / ｾｷｭﾘﾃｨｴﾝｼﾞﾆｱﾘﾝｸﾞ演習 〉

ﾋﾞｯｸﾞﾃﾞｰﾀ分析を技術・管理の両面で牽引できるﾘｰﾀﾞの育成〈 https://www.iisec.ac.jp/admissions/prosec/ 〉
情報ｾｷｭﾘﾃｨ大学院大学　受講料390,000円　審査料20,000円

○ 企業経営者向けﾋﾞｯｸﾞﾃﾞｰﾀ分析とﾘｽｸ経営　受講時間225時間(通学)　履修証明書交付(必修1演習、2実践講義、選択3科目)
ｲﾝｼﾃﾞﾝﾄ対応とCSIRT基礎演習/ｻｲﾊﾞｰｲﾝﾃﾘｼﾞｪﾝｽ実践講義/ﾃﾞｰﾀｻｲｴﾝｽとｱﾅﾘﾃｨｸｽ実務講義/ｾｷｭｱｼｽﾃﾑ構成論/ｾｷｭｱ法則と情報理論/ｻｲﾊﾞｰｾｷｭﾘﾃｨ技術論/組織行動と情報ｾｷｭﾘﾃｨ/国際標準とｶﾞｲﾄﾞﾗｲﾝ/ｾｷｭﾘﾃｨ経営とｶﾞﾊﾞﾅﾝｽ/情報ｾｷｭﾘﾃｨ心理学

○ ｾｷｭﾘﾃｨとﾃﾞｰﾀｻｲｴﾝｽ　受講時間 157.5時間（通学）　履修証明書交付（必修1演習、選択4科目）
ﾌﾞﾛｯｸﾁｪｰﾝ理論実践演習/ﾃﾞｰﾀｻｲｴﾝｽとｱﾅﾘﾃｨｸｽ実践講義/情報ｼｽﾃﾑ構成論/暗号ﾌﾟﾛﾄｺﾙ/実践的IoTｾｷｭﾘﾃｨ/ｾｷｭｱｼｽﾃﾑ構成論/ｻｲﾊﾞｰｾｷｭﾘﾃｨ技術論

ｾｷｭﾘﾃｨ対策・ｲﾝｼﾃﾞﾝﾄﾚｽﾎﾟﾝｽの運用・設計ができるﾘｰﾀﾞを育成
和歌山大学　〈 http://www.wakayama-u.ac.jp/dtier/ 〉

○ ﾒｲﾝｺｰｽ　受講時間 144時間　受講料 76,032円（必修）　14,400円/単位（選択科目）　入学料 10,000円
修得する知識・技術・能力：ｻｰﾊﾞ構築・運用術/ﾈｯﾄﾜｰｸ構築・運用術/ｲﾝｼﾃﾞﾝﾄ原因の切り分けと封じ込め/事後観察やﾛｸﾞ解析を含む業務ｶﾊﾞｰ方法
科目：情報理論/ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ/情報ﾈｯﾄﾜｰｸ演習/ｲﾝｼﾃﾞﾝﾄﾚｽﾎﾟﾝｽ実践演習

○ ｸｲｯｸｺｰｽ　受講時間 54時間　受講料 76,032円
修得する知識・技術・能力：ｻｰﾊﾞ構築・運用術/ﾈｯﾄﾜｰｸ構築・運用術/ｲﾝｼﾃﾞﾝﾄ原因の切り分けと封じ込め/事後観察やﾛｸﾞ解析を含む業務ｶﾊﾞｰ方法
科目：ｲﾝｼﾃﾞﾝﾄﾚｽﾎﾟﾝｽ実践演習

設計・開発段階のｾｷｭﾘﾃｨ対策、ﾃﾞｰﾀ解析、情報ｾｷｭﾘﾃｨﾏﾈｼﾞﾒﾝﾄのｽｷﾙを修得
東北大学　〈 http://www.esprit.is.tohoku.ac.jp/prosec.html 〉

○ ｾｷｭﾘﾃｨﾏｲﾝﾄﾞ　ﾒｲﾝｺｰｽ　受講時間126時間　受講料162,800円　（入学料28,200円、検定料98,00円）
ﾃﾞｰﾀ科学基礎/学際情報科学論/ﾋﾞｯｸﾞﾃﾞｰﾀｽｷﾙｱｯﾌﾟ演習/ﾃﾞｰﾀ科学ﾄﾚｰﾆﾝｸﾞ/応用ﾃﾞｰﾀ科学/ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ実践/情報ｾｷｭﾘﾃｨ法務経営論

○ ｾｷｭﾘﾃｨﾏｲﾝﾄﾞ　ｸｲｯｸｺｰｽ（ｾｷｭﾘﾃｨ）　受講時間 45時間　受講料 59,200円　（入学・検定料 同上）
ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ/情報ｾｷｭﾘﾃｨ法務経営論

○ ｾｷｭﾘﾃｨﾏｲﾝﾄﾞ　ｸｲｯｸｺｰｽ（科学）　受講時間 67.5時間　受講料 88,800円　（入学・検定料 同上）
ﾃﾞｰﾀ科学基礎/学際情報科学論/応用ﾃﾞｰﾀ科学/情報ｾｷｭﾘﾃｨ法務経営論

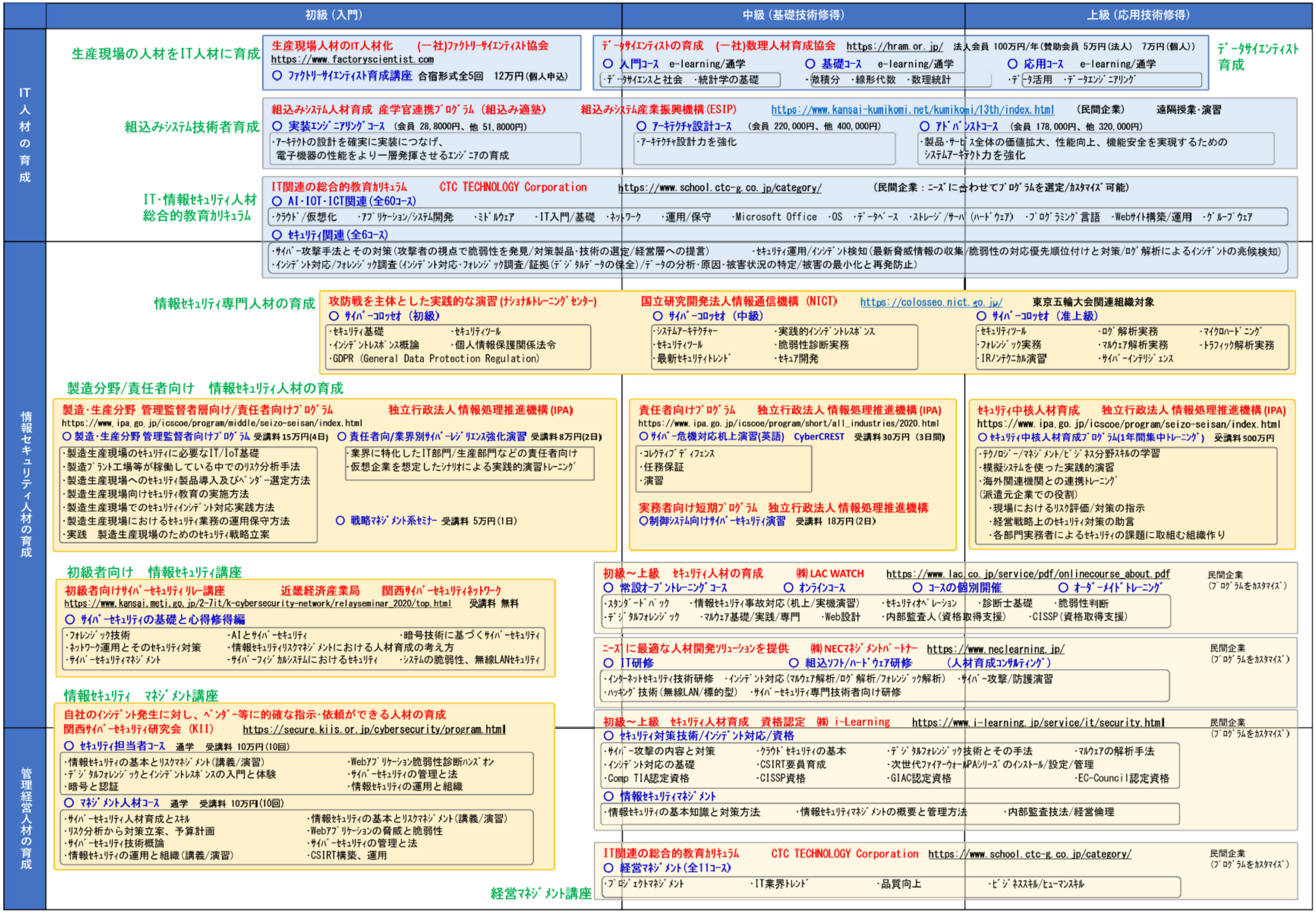
管理経営人材の育成

高度情報ｾｷｭﾘﾃｨ人材の育成（東京電機大学）

最高情報ｾｷｭﾘﾃｨ責任者/ｴﾝｼﾞﾆｱの育成　〈https://cysec.dendai.ac.jp/ 〉
東京電機大学　受講審査料 10,000円、登録料 10,000円、施設利用料 10,000円
受講時間 98時間　受講費 32,000円/科目、教材費 226,000円

○ 国際化ｻｲﾊﾞｰｾｷｭﾘﾃｨ学 特別ｺｰｽ（Cysec）
ｻｲﾊﾞｰｾｷｭﾘﾃｨ基盤ⅠⅡ / ｻｲﾊﾞｰﾃﾞｨﾌｪﾝｽと心理・倫理・法 / ﾃﾞｼﾞﾀﾙﾌｫﾚﾝｼﾞｯｸ / 情報ｾｷｭﾘﾃｨﾏﾈｼﾞﾒﾝﾄとｶﾞﾊﾞﾅﾝｽ / ｾｷｭｱｼｽﾃﾑ設計・開発

図表４．７　法人・行政機関による 社会人向け講座



４．２．セキュリティ人材研修

岡山大学、広島市立大学、大阪大学により社会人向けに作成されたセキュリティ関連の VoD（Video on Demand）コンテンツを利用したオンライン研修（各大学 50～60 名）を実施するとともに、オンライン研修受講者を対象に演習（＝「ミニキャンプ」）を１回開催した。

なお、研修終了後は受講者に対しアンケート等を実施し、カリキュラムにおける課題、企業ニーズ等の分析を行った。

４．２．１．社会人セキュリティ人材育成講座 概要

ａ．人材育成講座の概要

社会人セキュリティ人材育成講座の概要は図表４．８のとおりである。なお受講者は３大学 計で 170 名であるが、複数大学講座の受講者がいるため実受講者数は 107 名である。

図表４．８　セキュリティ人材研修の概要

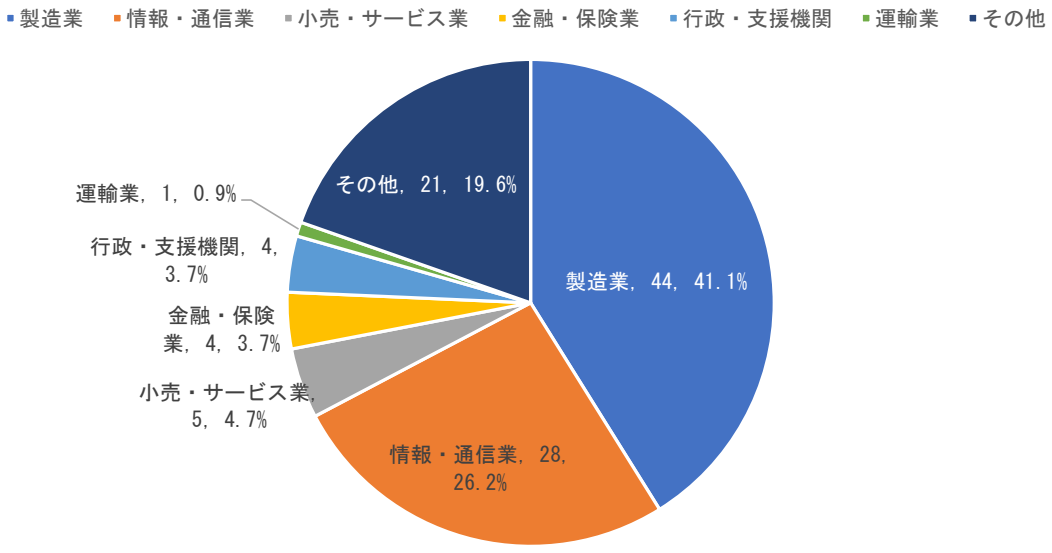
項目		岡山大学	広島市立大学	大阪大学
受講期間	VoD	2020 年 11 月 1 日～2021 年 1 月 31 日		2020 年 10 月 16 日 ～2021 年 1 月 22 日
	ﾐﾆｷｬﾝﾌﾟ	―		2020 年 12 月 12 日
受講科目		７科目	６科目	４科目（VoD） ３科目（ﾐﾆｷｬﾝﾌﾟ）
受講時間		約４時間	６時間	30 時間（VoD） ４時間（ﾐﾆｷｬﾝﾌﾟ）
受講 登録者数		各 60 名		50 名（VoD） 15 名（ﾐﾆｷｬﾝﾌﾟ）

ａ．受講者の属性

（ａ）業種別

受講者（107 名）の所属組織・企業の業種は「製造業」（41.1%）が最も多く、次いで「情報・通信業」（26.2%）、「小売・サービス業」（4.7%）となっている（図表４．９）。

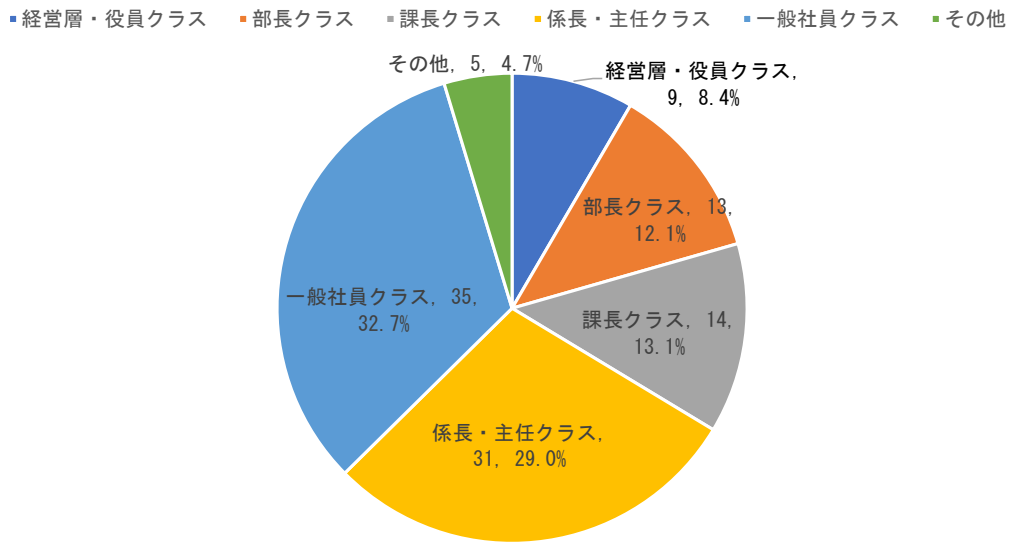
図表４．９　受講者の属性（業種別：ｎ＝107）



（ｂ）役職別

受講者の所属組織・企業における役職は「一般職員」（32.7%）が最も多く、次いで「係長・主任」（29.0%）、「課長」（13.1%）となっている（図表４．10）。

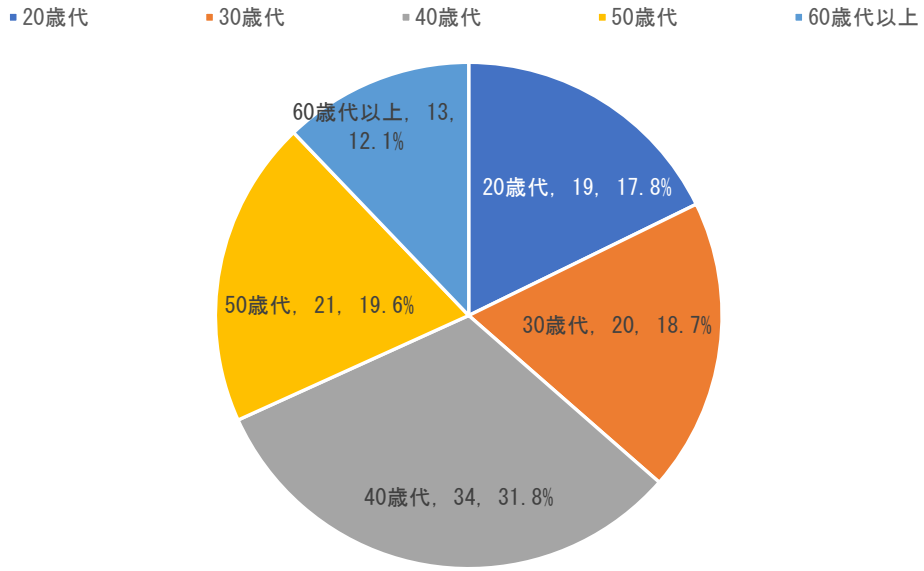
図表４．10　受講者の属性（役職別：ｎ＝107）



（ｂ）年齢別

受講者の年齢は「40 歳代」（31.8%）が最も多く、次いで「50 歳代」（19.6%）、「30 歳代」（18.7%）となっている（図表４．11）。

図表４．11　受講者の属性（年齢別：ｎ＝107）



図表４．12　社会人セキュリティ人材育成講座　募集チラシ

※応募者多数のため各大学の定員を増員（各 40 名→各 50～60 名）

４．２．２．社会人セキュリティ人材育成講座の内容

ａ．岡山大学

岡山大学のカリキュラムは「IoT・AI・セキュリティ入門講座」として、主に情報セキュリティの基礎技術とセキュリティガイドライン（開発指針）およびサイバー攻撃・IoT 向け暗号の概要について解説を行った（図表４．13)。

図表４．13　岡山大学カリキュラム

No.	科　　目	講　　師	概　　要	
①	IoT デバイス用暗号	野上 保之　教授	暗号の入口	(1)情報セキュリティとは
				(2)個別テーマのセキュリティ
				(3)データセキュリティ
②	セキュリティガイドライン	野上 保之　教授	つながる世界の開発指針	(1)開発指針の目的
				(2)開発指針の対象
				(3)リスク想定・開発指針
				(4)開発指針
③	マルチメディアセキュリティ	栗林 稔　准教授	電子透かし技術の概要	(1)電子透かしの分類
				(2)埋め込みと検出
④	オペレーティングシステムセキュリティ	山内 利宏　准教授	OS の機能概要	
⑤	セキュア通信プロトコル	福島 行信　准教授	通信に対する様々な脅威	
⑥	ハードウェアセキュリティ	五百旗頭健吾　助教	IoT ハードウェアに対する脅威	
⑦	サイバー攻撃	樽谷 優弥　助教		

ｂ．広島市立大学

広島市立大学のカリキュラムは「スマートファクトリー・セキュリティ入門講座」として、ロボットや自動車の最新技術を中心に、with コロナ等の至近動向を織り交ぜ、企業のセキュリティ確保について多様な観点から解説を行った（図表４．14)。

図表４．14　広島市立大学カリキュラム

No.	科　　目	講　　師	概　　要
①	組込みシステム概論	弘中 哲夫 教授	小型コンピューターとそれを組み込んだシステムを具体的な応用例を交えながら紹介。組込みシステムで何ができるか？どんな可能性を秘めているか？を中心に解説
②	無線ネットワーク概論	大田 知行 准教授	概要：無線ネットワークの仕組みを中心に解説。また、無線ネットワークを利用したサービスなどを紹介
③	IoT セキュリティ概論	井上 博之 准教授	IoT システムの危険性について解説。自動車を中心に、様々な IoT システムに潜む危険性を紹介
④	機械学習概論	神尾 武司 講師	人工知能と機械学習の概要を解説。特に近年注目されている技術を紹介
⑤	産業用ロボット概論	岩城 敏 教授	産業用ロボットの基礎についてアーム型ロボットを中心に解説。最新のトピックスを交えながらロボット技術の現状を紹介
⑥	データマイニング概論	田村 慶一 教授	データマイニングでできることについて応用例を交えながら解説。ビッグデータ活用法についても紹介

ｃ．大阪大学

（ａ）VoD 講座

大阪大学のカリキュラムは、「データサイエンス・セキュリティ入門講座」として、データサイエンスの基礎技術と、その活用を中心に、データサイエンスに関わる情報セキュリティの概要を含めて解説を行った（図表４．15)。

図表４．15　大阪大学カリキュラム

No.	科　　目	講　師	概　　要	
データサイエンスリテラシー				
①	データサイエンスと社会	朝倉 准教授	1. イントロダクション	4. データサイエンス入門 (2) エクセルによるデータ解析（回帰分析）
			2. 実社会でのデータサイエンスの実例	5. スクーリング
			3. データサイエンス入門 (1) エクセルによるデータ解析（データの整理）	
②	数理統計の基礎		6. 数理統計　(1)母集団と標本	9. 重回帰分析
			7. 数理統計　(2)推定と検定	10. スクーリング
			8. 単回帰分析	
③	データサイエンスの活用		11. R によるデータ解析の基礎	14. クラスタリング
			12. ロジスティック回帰	15. スクーリング
			13. ニューラルネットワークの基礎	
情報セキュリティ入門				
④	情報セキュリティの脅威・対策	松原 繁夫 教授	1. 暗号と認証の基礎	4. Web セキュリティ
			2. ネットワークセキュリティ：脅威	5. サイバー法と情報セキュリティ
			3. ネットワークセキュリティ：防御	

（ｂ）ミニキャンプ

ア．概要

社会人セキュリティ人材育成講座受講者を対象とした、データサイエンスおよび情報セキュリティに関するスクーリングや講演会を集合形式で行うミニキャンプを開催した（図表４．16)。

図表４．16　ミニキャンプの概要

区　　分		内　　容
日　　時		2021 年 12 月 12 日（土）　13:30～17:30
会　　場		ホテルグランヴィア広島　４階　悠久の間（広島市南区松原町１－５）
参加人数		15 名
内容	講　演	「“with コロナ”に事業継続と情報セキュリティを考える」 広島大学　情報メディア教育研究センター　教授　西村　浩二
	講義①	「データサイエンスリテラシー」 大阪大学　数理・データ科学教育研究センター　特任准教授　朝倉　暢彦
	講演③	「情報セキュリティ入門」 大阪大学　数理・データ科学教育研究センター　特任教授　松原　繁夫
	事務局連絡	「一般社団法人 数理人材育成協会について」 大阪大学　数理・データ科学教育研究センター　特任専門職員　竹山　博昭

イ．講演・講義内容

①「“with コロナ”に事業継続と情報セキュリティを考える」

広島大学　情報メディア教育研究センター　教授　西村　浩二

広島大学における「新型コロナウイルス感染症への対応」「セキュリティインシデント対応」「情報基盤サービスにおける情報セキュリティ管理」「おけるクラウドサービス利用の取り組み」等について説明を行った（図表４．17)。

②「データサイエンスリテラシー」

大阪大学　数理・データ科学教育研究センター　特任准教授　朝倉　暢彦

「ロジスティック回帰」「ニューラルネットワーク」「クラスタリング」「主成分分析」について講義を行った（図表４．18)。

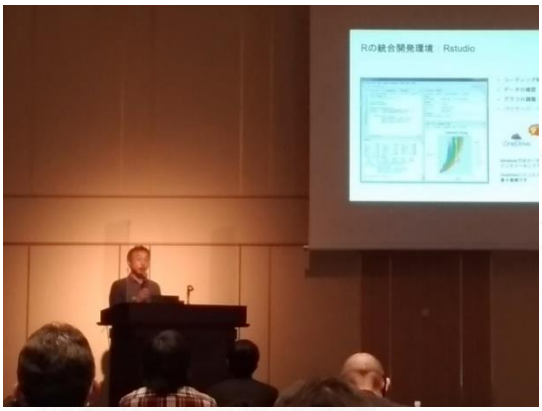
③「情報セキュリティ入門」

大阪大学　数理・データ科学教育研究センター　特任教授　松原　繁夫

「情報セキュリティ講義のねらい・概要」「情報セキュリティとは」「データサイエンスと情報セキュリティ」について説明を行った（図表４．19)。

図表４．17　広島大学　西村教授　講演

図表４．18　大阪大学　朝倉特任准教授　講義



図表４．19　大阪大学　松原特任教授　講義

４．２．３．社会人セキュリティ人材育成講座における課題整理

社会人セキュリティ人材育成講座については、概ね「IT・IoT 等のデジタル技術に関して基礎から網羅的に学習できる」「VoD の活用により業務（テレワーク等）の合間に少しずつ受講できる」「本来有料のものが無料で受講でき、費用負担の面で助かる」等の点において受講者より評価を受け、受講者の継続的な受講意欲も高いため、今後も継続して実施することが期待される。

その一方で以下のような課題も見受けられ、今後の実施にあたっては配慮・検討が求められる。

〇講義内容

講義内容が学生の向けの「教科書の授業」との印象を受ける受講者も一部におり、社会人向けに会社での業務に即した内容や具体的な事例を含めた内容を付加することが期待されている。

〇受講システムのインターフェース

受講にあたっての「e ラーニングシステム（Moodle）のインターフェースが分かりづらい」、大学における e ラーニング講座の一部を公開しているため「受講できる科目が分かりづらい」との意見が寄せられた。

システムの変更は困難であるため、受講方法に関する事務局からの追加説明、受講者へのフォローが期待される。

〇受講率の向上

VoD による講義であるため、「受講の進捗が受講生に委ねられている」「講師の「顔」が見えない」「受講料が無料でありひとまず申し込む」等の理由から全く講義を受講していない受講生も一定割合存在している。

さらに、上記の講義内容、インターフェースについても受講率に影響を及ぼすと考えられる。

このような状況に対し、受講率の向上に向け、事務局における管理・運営の面では「受講状況の把握による細やかな受講者への督促」「受講完了者へのインセンティブ（修了証の発行等）」「意欲のある受講生の試験等による選抜」、講義方式の面では「リアルタイムでのオンライン講義の併用」「PBL（Problem-Solving-Learning）演習の実施」等が期待される。

また、今回は一人の受講生が複数大学を受講することも可能としているが、受講者負担と受講率の関係からも検討が求められる。

○講座全体のカリキュラムの体系化

今回の講座は各大学とも「入門講座」として位置づけており、受講者の中には「難しい」と感じるものもいる一方で、実際の機器・システム開発等には「内容的に不十分」とのコメントもある。

さらに、「セキュリティを含めたデジタル技術全般を対象とした講座」は、概ね評価を受ける一方で、「セキュリティへ特化した講座」を求める意見も複数みられる。

このような状況は、今回の講座開設にあたっての事務局による各大学の講座の位置づけの明確化や体系化が十分なされておらず、受講生に十分浸透しなかったことが影響していると考えられる。今後の実施にあたっては、大学間のカリキュラム面での連携等を含めた検討が求められる。

４．３．ハッカソン

４．３．１．ハッカソン概要

ハッカソンイベントに関しては、当初、セキュリティ人材育成に資するイベントを岡山市内で開催する予定であったが、同地にて類似イベントである「Web×IoT メイカーズチャレンジ 2020-21 in 岡山」（主催：中国総合通信局等）が開催予定であったため、関係先と協議の結果、本事業においては当該イベントに関して「協力」という形で参画することとなり、イベントの関係先への周知および会場運営協力を行った。

なお、ハッカソンイベントは「ハンズオン講習会」と「ハッカソン」から構成されている。

４．３．２．ハンズオン講習会

ハンズオン講習会は座学講座「IoT/電波や無線通信の基礎知識」を受講のうえ、支給された Raspberry Pi４[16]によりサンプルプログラムを触りながら、実際に自分でセンサーやアクチュエータを制御する実習を行った。

さらにハッカソンに向け「With　コロナ時代を楽しむための IoT デバイス」をテーマに各チーム（６チーム×４人／チーム）の作品づくりのアイデアワークショップ（アイデアソン）を実施した（図表４．20）。

図表４．20　　ハンズオン講習会の概要

区　　分		内　　容
日　　時		2021 年 11 月 22 日（日）　10:00～17:00、2020 年 11 月 23 日（月）　10:00～17:00
会　　場		ももたろう・スタートアップカフェ（岡山市北区駅前町 1 丁目 8 番地 18 号 ICOT NICOT 内）
参加人数		24 名
内容	座学講座	「IoT/電波や無線通信の基礎知識」　岡山大学大学院自然科学研究科　野上教授
	ハンズオン講習	「CHIRIMEN for Raspberry Pi を使った IoT システム開発のハンズオン講習」　WebDINO Japan　渡邉氏
	アイデアワークショップ	「With　コロナ時代を楽しむための IoT デバイス」　WebDINO Japan　井作氏

４．３．３．ハッカソン

ハンズオン講習会（11 月 23 日）後、各チームにて必要な材料をチームで準備のうえ、作品制作の準備を進め、ハッカソン１週間前の 12 月 13 日にはオンラインで各チームから中間報告を行うとともに、岡山大学のメンターが制作のサポートを行った。

なお、ハッカソン制作物の条件としては、「無線の活用を前提として、ネットワークサービスの連携もしくはネットワークからのコントロールが可能」「Web 技術を活用したシステム」「講習で学んだ知識に基づいた創作物」「ハードウェア（モノ）を伴った作品」である。

12 月 20 日のハッカソン当日には６チームから制作物の発表があり、「最優秀賞（中国総合通信局長賞）」にＢチーム「手洗いチェッカー　TEGOSHI」が選出された。（図表４．21、図表４．22）。

[16] ARM プロセッサを搭載したシングルボードコンピュータ。イギリスのラズベリーパイ財団によって開発。日本語では略してラズパイとも呼ばれる

なお、最優秀チームは 2021 年３月に東京にて開催される「スマート IoT 推進フォーラム」にメンバー招待のうえ発表の機会が与えられた。

図表４．21　ハッカソンの概要

区　分		内　容
日　時		2020 年 12 月 20 日（日）　10:00～18:00
会　場		クリエイティブ コワーキングスペース TOGITOGI（岡山市北区磨屋町 3-10 TOGITOGI ２F）
参加人数		24 名（６チーム×４人／チーム）
内容	ハッカソン	Aチーム：ぬくくま Bチーム：手洗いチェッカー　TEGOSHI（「最優秀賞」） Cチーム：鬼が監視するコロナ退治 Dチーム：QR コードリーダー付買い物カート Eチーム：ホットパイプ（「特別賞」） Fチーム：IoT マスク

図表４．22　ハッカソン発表風景

令和２年度中小企業サイバーセキュリティ対策促進事業
（中国地域におけるセキュリティコミュニティ形成事業）
公開用資料

2021（令和 3）年 3 月 31 日　1 版 1 刷

編集　公益財団法人 中国地域創造研究センター
〒730-0041　広島市中区小町 4 番 33 号

白　紙