2019/04/19 版

2019

苫小牧地区における
情報セキュリティ意識に関する調査

苫小牧工業高等専門学校 創造工学科 情報科学・工学系

情報処理安全確保支援士　土居 茂雄

苫小牧高専協力会・苫小牧商工会議所・苫小牧高専 連携事業
「苫小牧地区における情報セキュリティ意識に関する調査」

目次

図表目次

表目次

図目次

1. 要旨

中小企業における情報セキュリティに関する意識は，その投資が直接企業への利益に結び付かないと考えられ，その意識も乏しい．中小企業における情報セキュリティ意識の全国規模調査が IPA により実施されており [1]，地域に根付いた調査は大阪商工会議所が実施したものがある [2]が，北海道内を対象とした情報セキュリティ意識に関するアンケートが実施された例はない．このため苫小牧高専が主体となって，高専が立地する苫小牧地区に所在する中小企業や支店の現状の情報セキュリティに対する対応状況やセキュリティ意識を把握し，今後苫小牧や北海道での情報セキュリティ意識をどのように向上させられるかを考察する．

本報告書においては，2 章に結果の概要，3 章に提言，4 章にアンケートで得られた結果，5 章に今回の調査で用いたアンケートをそれぞれ示す．本調査は，苫小牧高専情報工学科 5 年生の卒業研究の一環として実施され，IPA によるアンケート [1]をベースとし実情に合わせて改変や追加を行っている．また本調査は国立高等専門学校機構情報セキュリティ人材育成事業の支援を受け実施されたものである．

2. アンケート

2.1. アンケートの概要

本研究では，苫小牧商工会議所の協力を得てアンケート調査を実施した．概要は以下のとおりである．

- アンケート送付企業数: 苫小牧商工会議所に加盟している企業から 452 社，苫小牧高専協力会加盟企業から 148 社，計 600 社を抽出．
- アンケート返答数: 208 社，34.7%の返答率
- 回答者: 情報セキュリティの担当者
- アンケート期間: 2018 年 8 月 1 日～10 月 31 日
- 回答の匿名性: 無記名で回答
- 回答方式: 郵送，アンケート返送時は料金受取人払郵便を利用

2.2. 企業の従業員数分布

回答があった企業の従業員数の分布に表 2　回答企業の従業員数分布図 1 に示す．図 1 よりわかるように，40 名以下の企業が 50%以上を占めている．

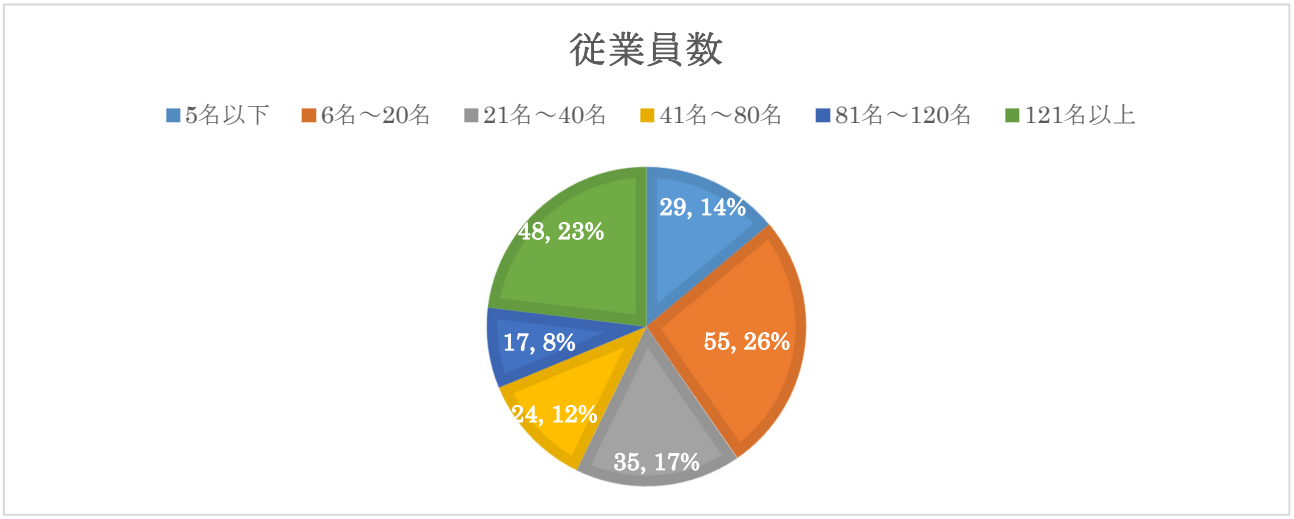


図 1　回答企業の従業員数分布

以下の結果では，中小企業庁における「中小企業」の定義では，「中小企業」と「大企業」の境界が業種によって異なる [3]が，今回の調査では比較のために「大企業」を従業員数 121 名以上の会社，「中小企業」を従業員数 120 名以下の会社をそれぞれ表すものとし，以下の比較はこの「大企業」と「中小企業」に基づき行っていく．

2.3. OS の利用状況

OS の利用状況について図 2 に示す. 中小企業では OS がまだ Windows XP が現役で利用されている．利用しているアプリケーションやハードウェアが Windows XP までにしか対応しておらずやむを得ず利用するケースがあるだろうと想定される．しかし，サポートがすでに打ち切られていることから，今後は利用しないような対応が必要である．また，2020 年 1 月に Windows7 のサポートが切れる [4]ため，Windows10 等への更新をいかに円滑に進めるかは課題となり，早急な啓蒙活動が必要となるだろう．

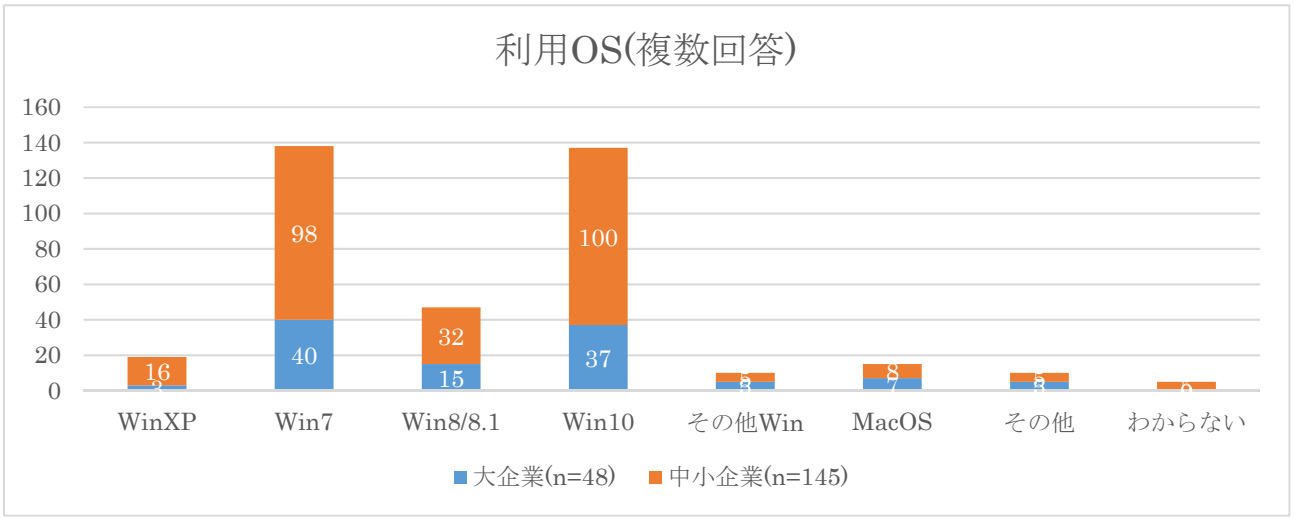


図 2 利用している OS の分布

2.4. セキュリティインシデントとその状況

図 3 にウイルス感染・発見の状況を示す．中小企業においてもウイルスが発見されたことのある会社が 89 社あり半数以上を占める．大企業からみれば比率は少ないものの，警戒する必要がある．P2P 接続による感染例はない．また，「わからない」という回答が中小企業で 16 社あり，ウイルスについて管理できていない状況がうかがえる．また，アンケート結果からは感染経路は「電子メール」あるいは「インターネット経由」が大部分を占めていた．

また，サイバー攻撃を受けた企業について抽出を行い，その手口を分析した．その結果を図 4 に示す．具体的な手口としては，中小企業では「標的型攻撃」が 12 件と多く，「ランサムウェア」や「ID/パスワード漏洩」が 3 件でつづく．一方で大企業では最も多いのは「DoS 攻撃」が 7 件で多く，「ランサムウェア」と「脆弱性による不正アクセス」が 3 件と続く．また，「手口がわからない」と回答している中小企業も 12 件と多く，情報セキュリティ担当者の教育も必要な可能性がある．

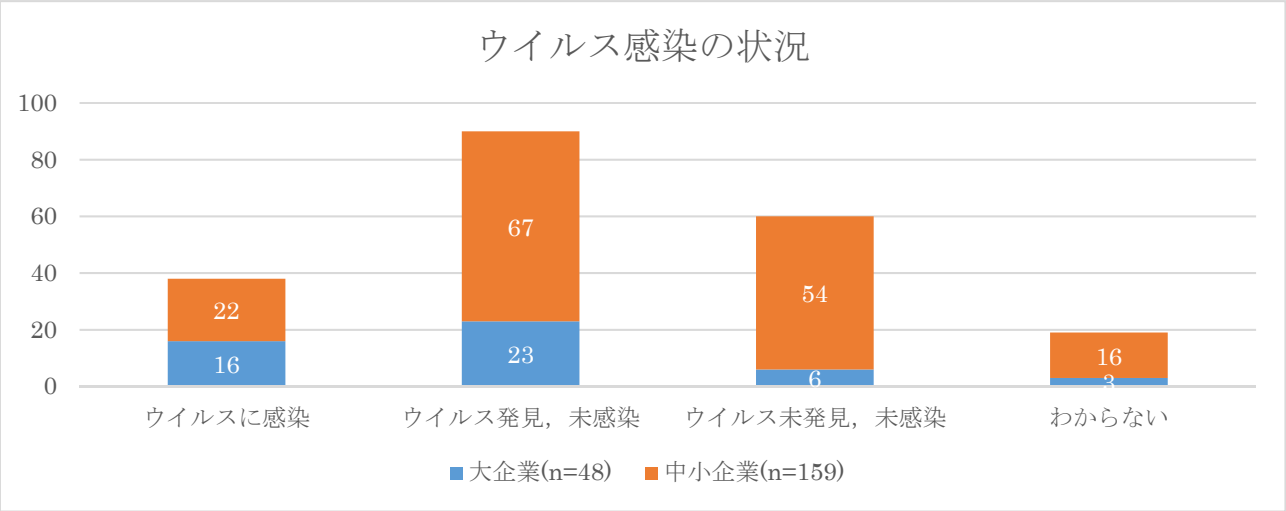


図 3　ウイルス感染の状況

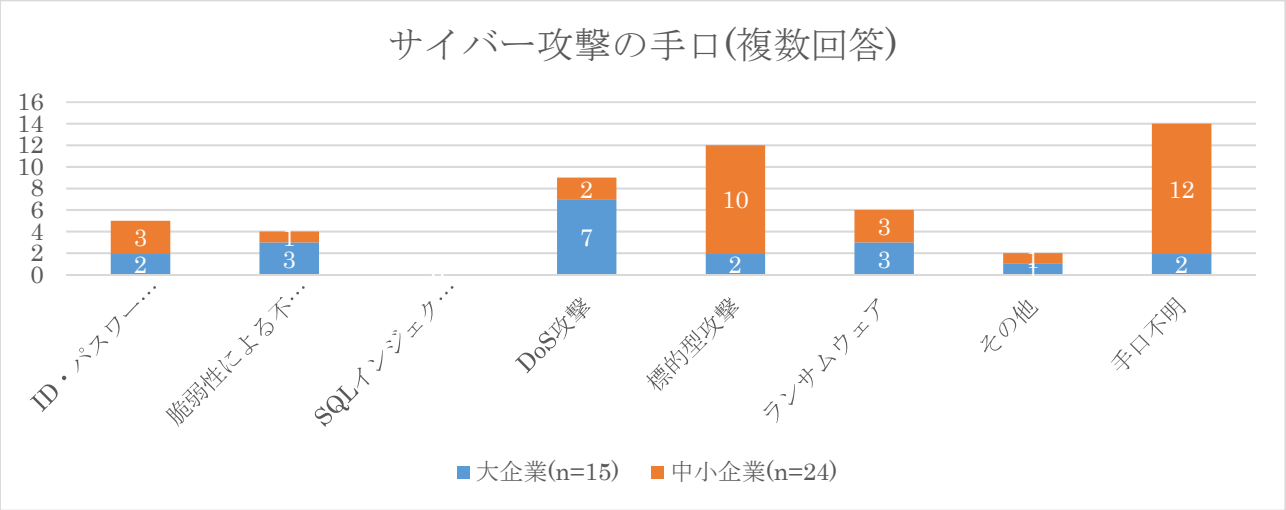


図 4　サイバー攻撃の手口(複数回答)

2.5.　セキュリティに対する対策意識

中小企業においては「情報セキュリティ対策は十分か」の問いに対しての回答分布を図 5 に示す．図 5 から，中小企業においては「あまりそう思わない」「思わない」「わからない」を合わせると半数を超えるものの，具体的にどこから手をつければよいかがわからない現状がうかがえる．また，今後具体的にどのような対策が必要かについての回答結果を図 6 に示す．図 6 では企業規模を問わずに，「従業員への教育」「企業内体制整備」「技術向上」が対策項目としてあがった．

3.　今後の提言

情報セキュリティにおける対策は十分ではない・わからないという認識が半数程度あることがわかった．具体的には「従業員教育」「企業内の体制整備」「情報セキュリティ技術の習得」が順にあがった．

苫小牧高専協力会・苫小牧商工会議所・苫小牧高専 連携事業
「苫小牧地区における情報セキュリティ意識に関する調査」

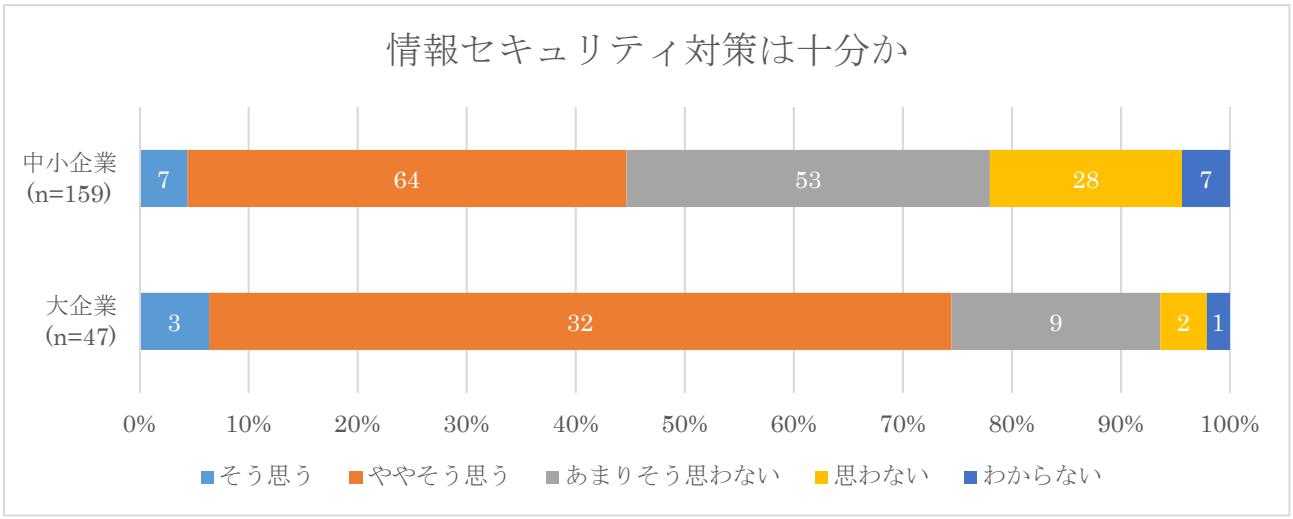


図 5　自社の情報セキュリティ対策に関する認識

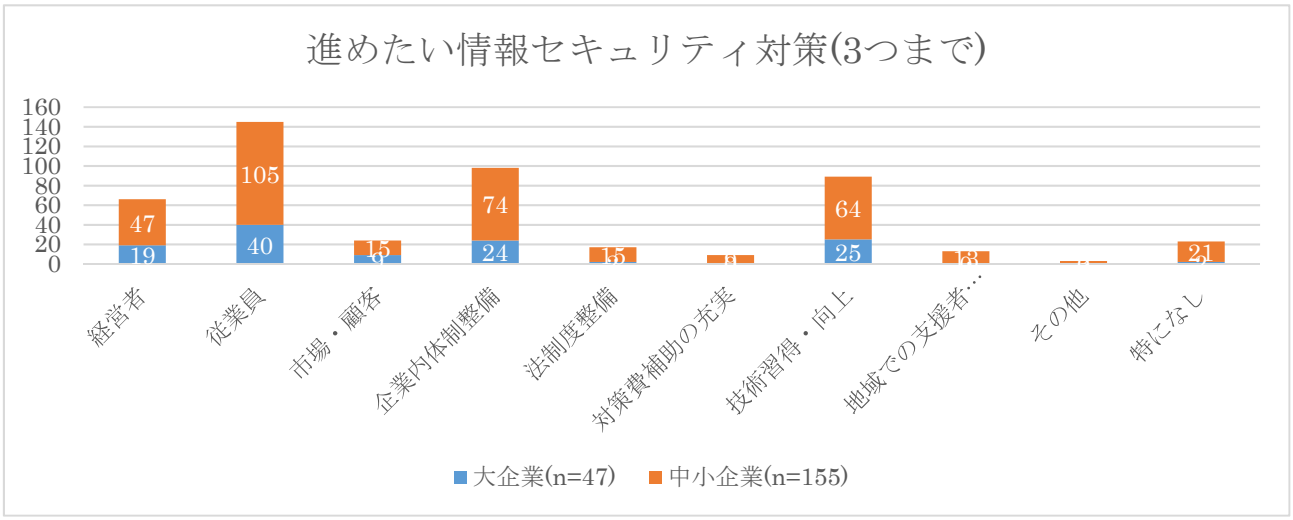


図 6　今後実施したい具体的な対策

本概要には挙げていないものの，中小企業において情報セキュリティについてどこに相談するかについて，「IT 関連業者」「社内担当者」が上がっており，情報収集元についても，これに「インターネット」が加わったものであり，情報セキュリティに関する相談先が限られていることも分かった．また，少数ではあるものの，地域での支援者養成やサポートセンターの充実に関する意見が上がった．

中小企業の対策では現在 IPA が出している情報セキュリティガイドライン [5]があり，まずそれに沿って対策をすることが望まれる．一方で中小企業においては従業員が少なく各社ごとに対策をとることが難しいと想定されるため，情報セキュリティの対策を地域で行えるような枠組みを提供することが今後必要になってくると考える．例えば大阪商工会議所では「中小企業向けサイバー攻撃対策支援事業」を実施しており，平成 29 年度は 500 円と廉価な費用でサイバーパトロールや人材育成の支援に参加できる．このように，地域で情報セキュリティレベル維持の取り組みが必要となる．そこに情報処理安全確保支援士の有資格者を配置することにより，地域の情報セキュリティレベルの底上げが期待できるであろう．

【以降は調査データとなります】

4. 資料

4.1. 今回アンケートに回答した企業に関する諸元

アンケートに回答した企業の諸元について以下に示す．なお，以下のアンケート結果においては 2.2 項で示した「中小企業」(従業員数 120 名以下)，「大企業」(従業員数 121 人以上)の定義を用いている．

4.1.1. 回答企業の業種

回答企業の業種分布を以下に示す．建設業が最も多く約 30%を占め，続いて製造業が約 15%を占める．

表 1 回答企業の業種(n=208)

業種	回答社数
農業	1
林業	0
漁業	0
鉱石業・採石業・砂利採取業	1
建設業	60
製造業	30
電気・ガス・熱供給・水道業	8
情報通信業	11
運輸業	11
卸売業	12
小売業	15

業種	回答社数
金融・保険業	7
不動産業	5
学術研究・専門・技術サービス業	12
宿泊業・飲食サービス業	2
生活関連サービス業，娯楽業	0
教育学習支援業	0
医療福祉	3
複合サービス業	2
その他サービス業	25
未回答	3

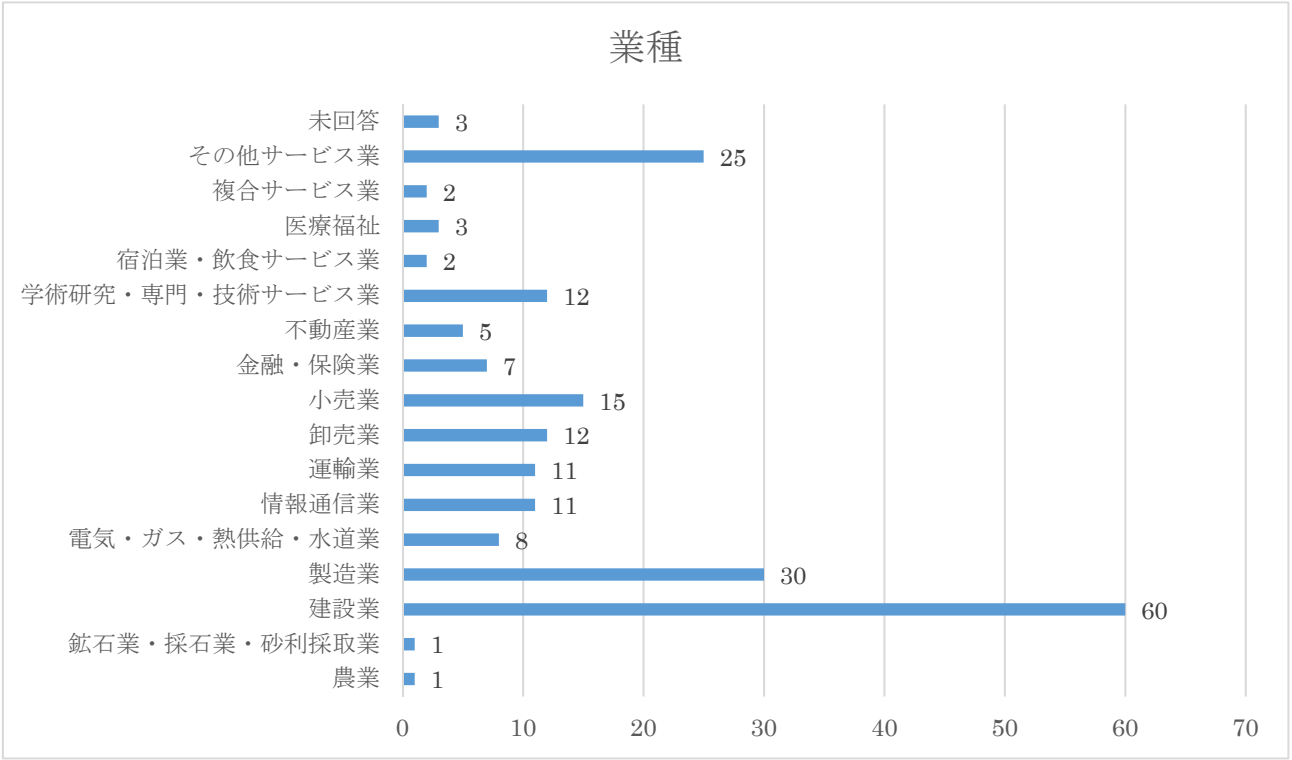


図 7 回答企業の業種分布

4.1.2. 回答企業の従業員数分布

回答企業の従業員数分布を以下に示す．40 名以下の企業が半分以上を占めている．

表 2　回答企業の従業員数分布(n=208)

	5 名以下	6 名～20 名	21 名～40 名	41 名～80 名	81 名～120 名	121 名以上
従業員数	29	55	35	24	17	48

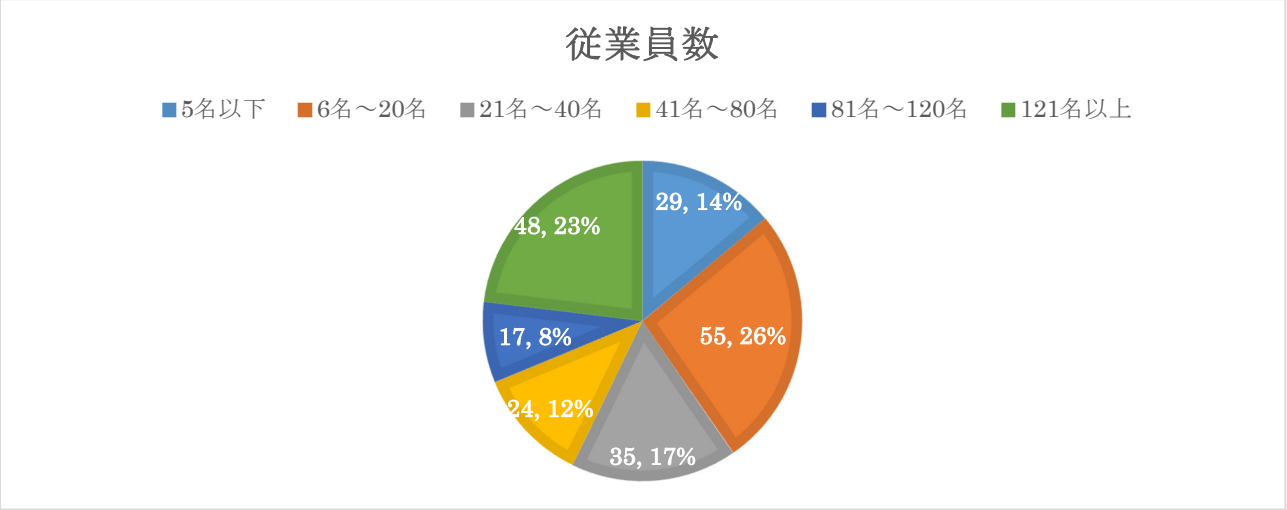


図 8　回答企業の従業員数分布

4.1.3.　資本金に関する分布

資本金に関する分布を以下に示す．なお，4 社については未回答であった．

表 3　回答企業の資本金分布

	500 万円以下	500 万円超 2000 万円以下	2000 万円超 4000 万円位以下	4000 万円超 1 億円以下	1 億円超
資本金	31	63	37	43	30

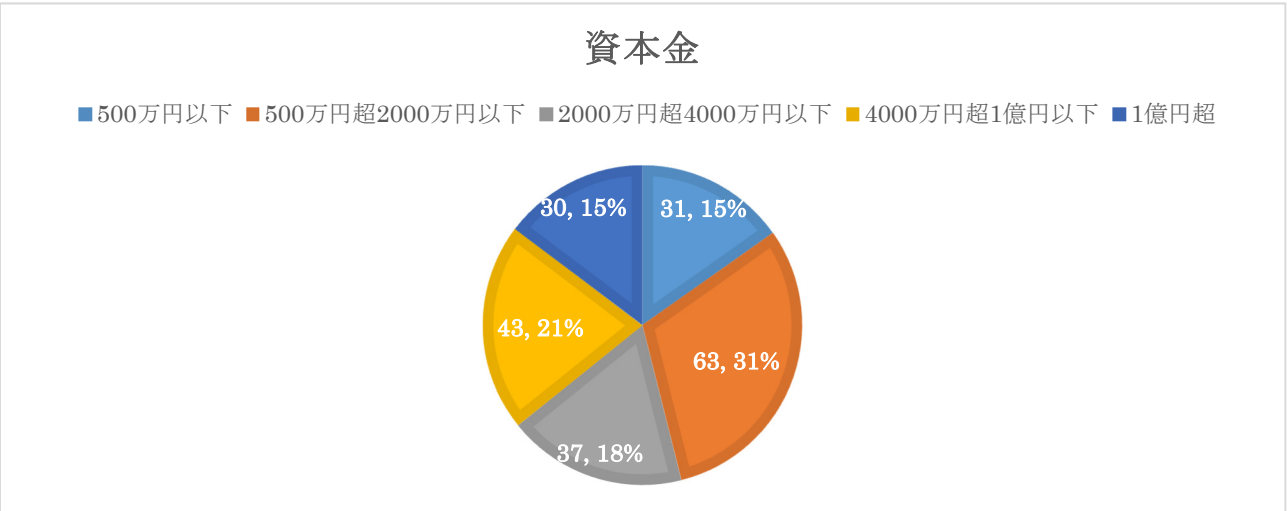


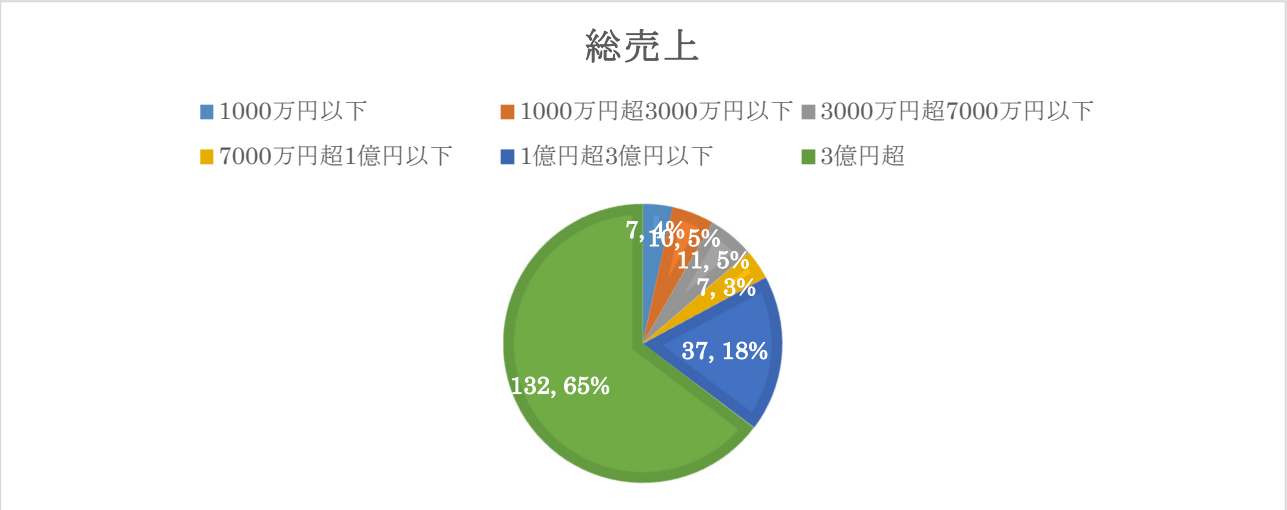
図 9　回答企業の資本金の分布

4.1.4.　総売上に関する分布

総売上に関する分布を以下に示す．なお，4 社については未回答であった．

表 4　回答企業の総売上に関する分布

	1000 万円以下	1000 万円超 3000 万円以下	3000 万円超 7000 万円以下	7000 万円超 1 億円以下	1 億円超 3 億円以下	3 億円超
総売上	7	10	11	7	37	132



4.1.5.　IT 活用に関する意識

IT 活用に関する意識に関する調査結果を以下に示す．3 社については未回答であった．中小企業であれば，「あまりそう思わない」「そう思わない」と回答している割合が高くなっている．

表 5　IT 活用に関する意識の分布

分類＼回答	そう思う	ややそう思う	あまりそう思わない	そう思わない	わからない
中小企業(n=158)	6	56	72	22	2
大企業(n=47)	18	18	7	2	2
全体	24	74	79	24	4

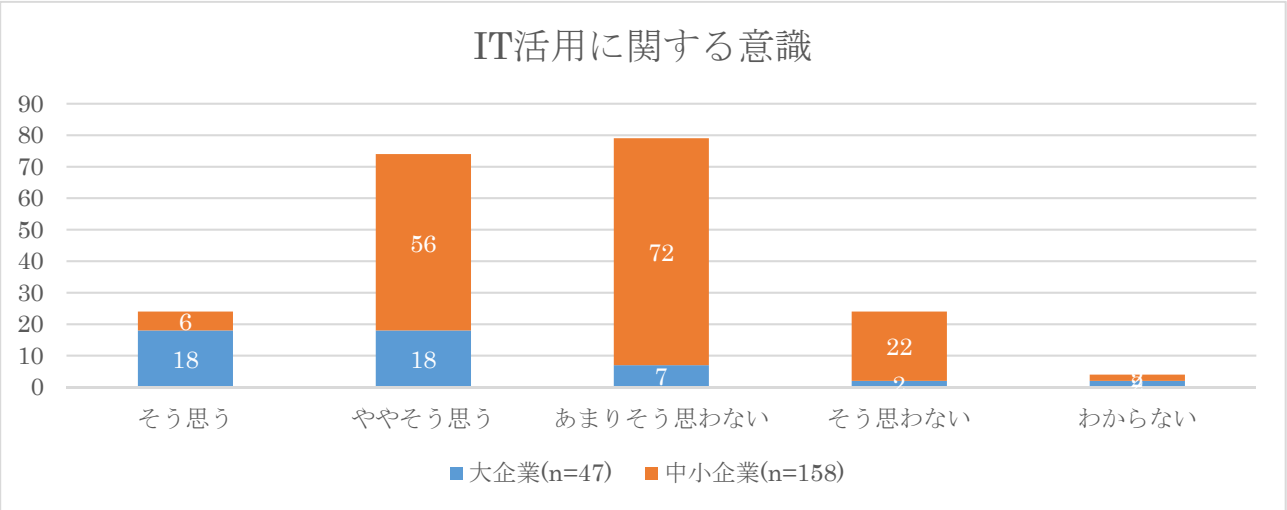


図 10　IT 活用に関する意識の分布

4.1.6. PC の業務利用と利用台数

PC の業務利用状況について以下に示す．中小企業であっても約 90%の企業で PC を利用していることがわかり，何らかの形で業務において PC 利用はほぼ浸透しているといえる．

表 6 PC の業務利用に関する分布

分類＼回答	利用している	利用していない
中小企業(n=160)	145	15
大企業(n=48)	48	0
全体(n=208)	193	15

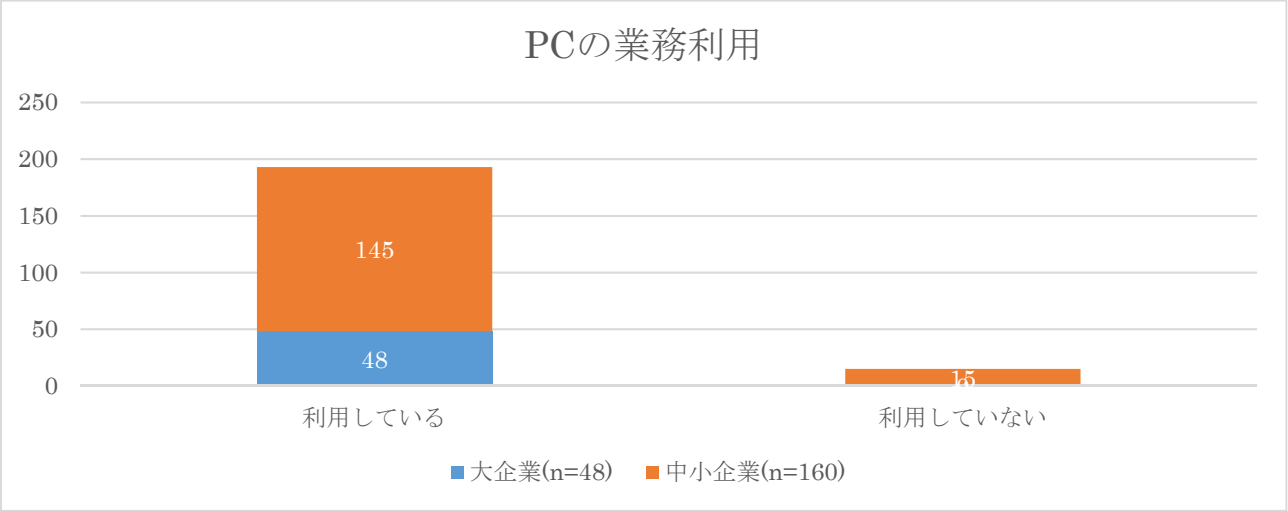


図 11 PC の業務利用に関する分布

また，PC を業務で利用している場合の PC 利用台数の分布について以下に示す．大企業 1 社が未回答であった．台数はおおむね従業員数に比例して台数が増えている様子が見て取れる．

表 7 業務利用している PC 台数の分布

分類＼台数	1～5	5～10	11～20	21～40	41～60	61～80
中小企業(n=145)	46	34	27	13	14	4
大企業(n=47)	1	1	0	1	6	1
全体	47	35	27	14	20	5
分類＼台数	81～100	101～200	201～300	301～400	401～1000	1001 以上
中小企業(n=145)	4	2	1	0	0	0
大企業(n=47)	1	8	11	4	7	6
全体	5	10	12	4	7	6

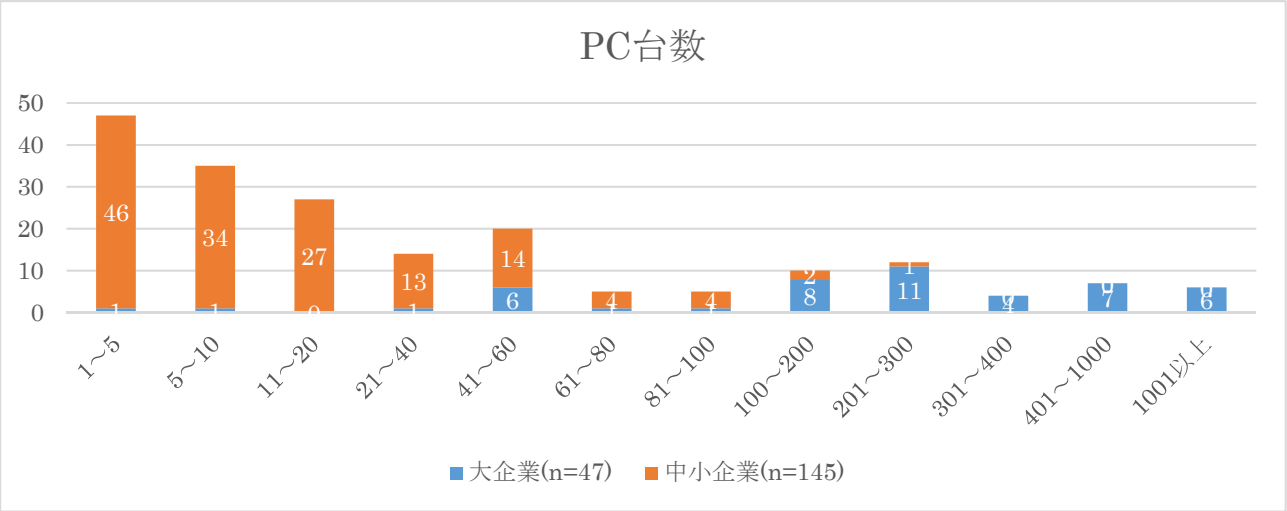


図 12　業務利用している PC 台数の分布

4.1.6.1. 利用 OS

PC を業務で利用している会社が利用している OS(複数回答)の回答について以下に示す．利用 OS のその他の記述としては，「サーバ OS」「Linux」「chromeOS」の回答が上がった．この結果から，業務利用している PC で稼働している OS の大多数は Windows 機であることがわかる．また，サポート切れとなっている WindowsXP の利用が 19 社ある．また Windows7 の利用も多い．WindowsXP はやむを得ず利用しているケースも多いかとも思われ，また Windows7 においても 2020 年 1 月にサポートが切れることが明示されている [4]ことからも，情報セキュリティの観点からは今後速やかな置き換えが望まれる．

表 8　PC での利用 OS に関する分布(複数回答)

分類＼OS	WinXP	Win7	Win8/8.1	Win10	その他 Win	MacOS	その他	わからない
中小企業(n=145)	16	98	32	100	5	8	5	5
大企業(n=48)	3	40	15	37	5	7	5	0
全体	19	138	47	137	10	15	10	5

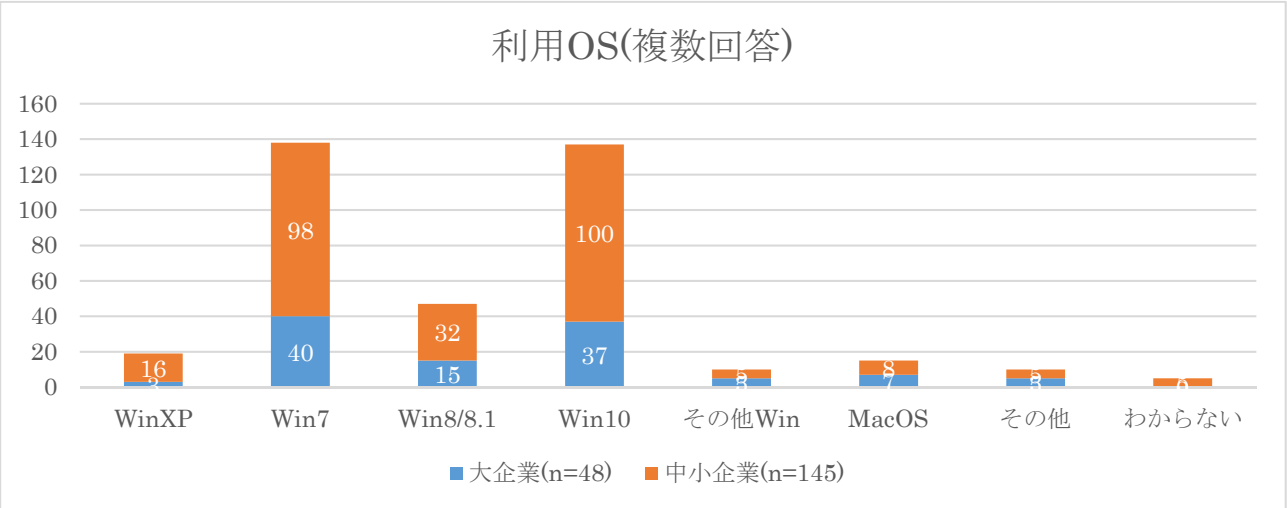


図 13　PC での利用 OS の分布

4.1.6.2. Windows Update の適用状況

PC を業務で利用している会社に対し，その会社の PC における Windows Update の適用状況について調査した結果を以下に示す．大企業で 1 社，中小企業で 1 社が未回答であった．中小企業においては，Windows Update の適用が PC を利用する個人任せになっている傾向が伺える．

表 9 Windows Update の適用状況に関する分布

分類＼回答	常に適用する方針 適用状況も把握	常に適用する方針 適用状況は不明	各ユーザに任せる	ほとんど適用していない	わからない
中小企業 (n=144)	43	47	42	8	4
大企業 (n=47)	27	16	3	1	0
全体	70	63	45	9	4

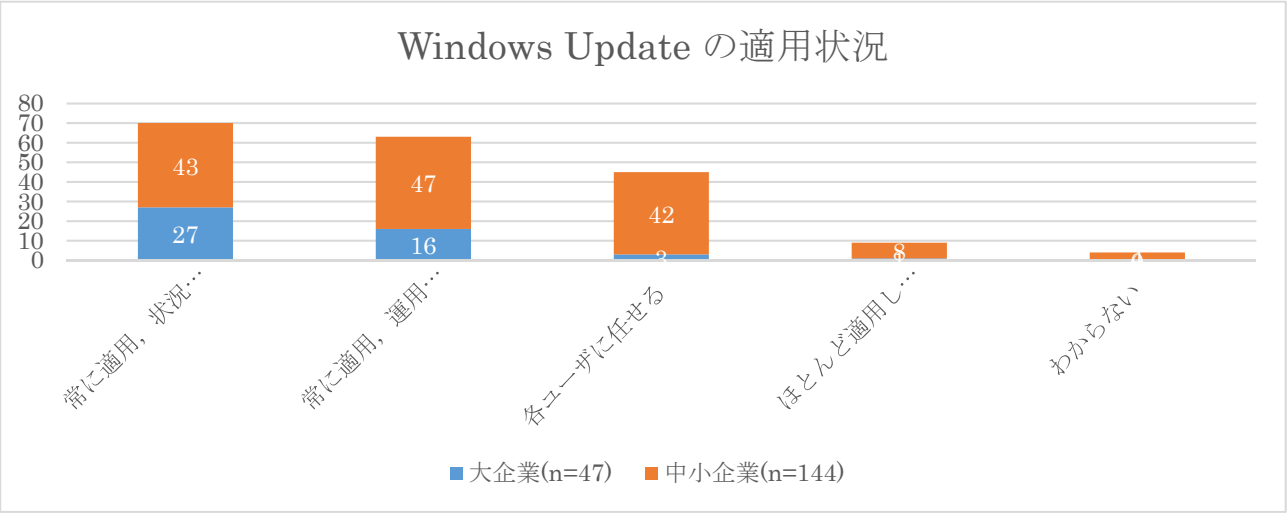


図 14 Windows Update の適用状況に関する分布

4.1.7. タブレット・スマートフォンの業務利用

タブレット・スマートフォンの業務利用について以下に示す．なお，2 社が未回答であった．PC の利用状況と比較するとまだ業務利用への普及はこれからである現状が伺える．

表 10 タブレット・スマートフォンの業務利用に関する分布

分類＼回答	利用している	利用していない
中小企業(n=159)	97	62
大企業(n=47)	41	6
全体	193	15

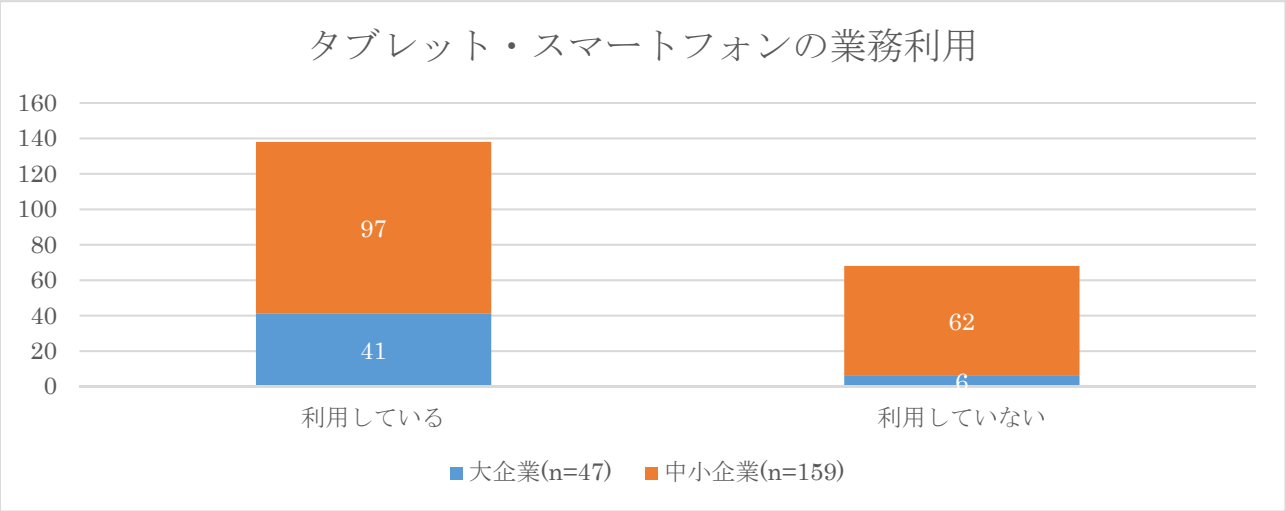


図 15　タブレット・スマートフォンの業務利用に関する分布

4.1.7.1. タブレット・スマートフォンにおいて取られている対策

タブレット・スマートフォンを業務利用している企業を対象に，どのようなセキュリティ対策が取られているかを回答していただいた．その他としては，「利用機種の統一」「指紋認証」といった項目が挙がった．パスワード設定やセキュリティソフトの導入が主だった対策で，特に実施されていないケースも見られる．

表 11　タブレット・スマートフォンにおいて取られている対策の分布(複数回答)

分類＼対策	パスワード設定	リモートデータ消去	セキュリティソフトの導入	端末管理	ルール策定	その他	特に実施せず
中小企業(n=97)	54	5	37	5	14	1	21
大企業(n=41)	36	22	22	21	23	2	3
全体	90	27	59	26	37	3	24

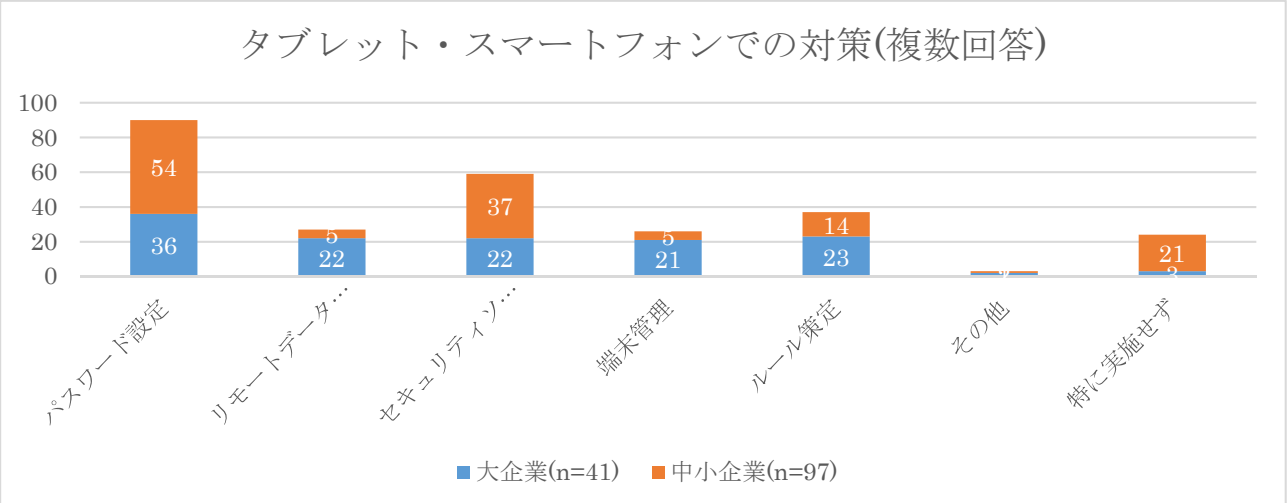


図 16　タブレット・スマートフォンにおいて取られている対策の分布(複数回答)

4.1.7.2. BYOD(私的端末の個人利用)について

個人所有の端末を業務にも利用することを BYOD(Bring Your Own Device)と呼ぶ．タブレット・スマートフォンを業務利用している企業に対して, BYOD の実情について調査した結果を以下に示す. なお, 2 社が未回答であった．中小企業では認めている企業が多くなっている傾向がある.

表 12　BYOD の許可状況の分布

分類＼回答	認めている	検討中	未検討	認める予定なし
中小企業(n=96)	36	9	17	34
大企業(n=40)	9	4	5	22
全体	45	13	22	56

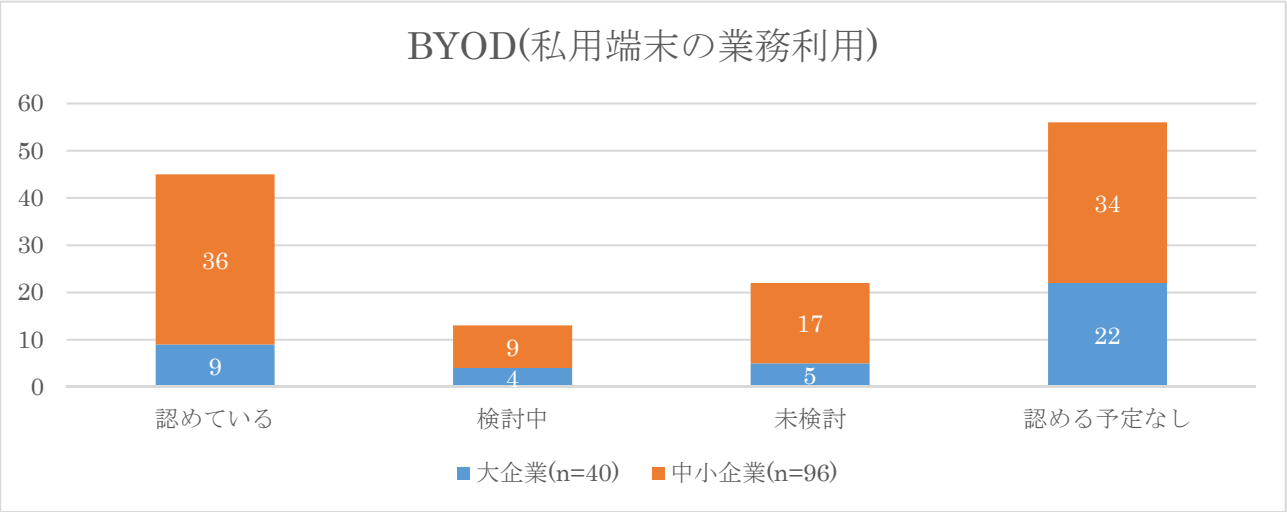


図 17　BYOD の許可状況の分布

4.1.8. サーバの利用について

サーバの利用状況について以下に示す．5 社が未回答であった．中小企業においてはサーバを利用していない割合が高いことがうかがえる．中小企業の実情としては，サーバ PC を導入するのではなく，NAS 等のネットワークストレージをサーバとして代用しているケースも多いことが想像される.

表 13　サーバの利用状況に関する分布

分類＼回答	利用している	利用していない
中小企業(n=156)	111	45
大企業(n=47)	46	1
全体	157	46

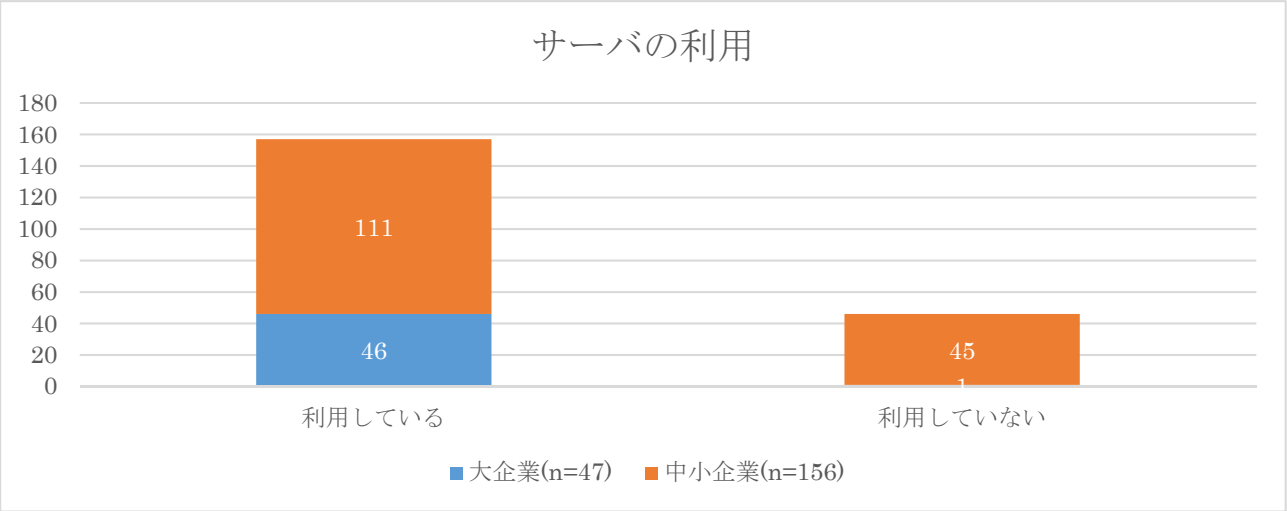


図 18　サーバの利用状況に関する分布

4.1.8.1. 外部サーバへの更新プログラム適用状況について

サーバを導入している企業について，外部サーバ(インターネットからアクセス可能であるセグメントに置かれているサーバ)について，更新プログラムの適用状況を調査した．結果を以下に示す．なお，2 社は未回答であった．更新プログラムがほとんど適用されていない会社も見られる．情報セキュリティの観点からは，合理的な理由がない限りは更新プログラムを適用すべきであり，改善する必要があると考える．

表 14　外部サーバへの更新プログラム適用状況に関する分布

分類＼対策	全部に適用	影響のないもののみ適用	重要なもののみ適用	ほとんど適用せず	外部運用者に委託	該当サーバを利用せず	わからない
中小企業(n=110)	39	10	14	4	21	17	5
大企業(n=45)	15	8	5	0	10	4	3
全体	54	18	19	4	31	21	8

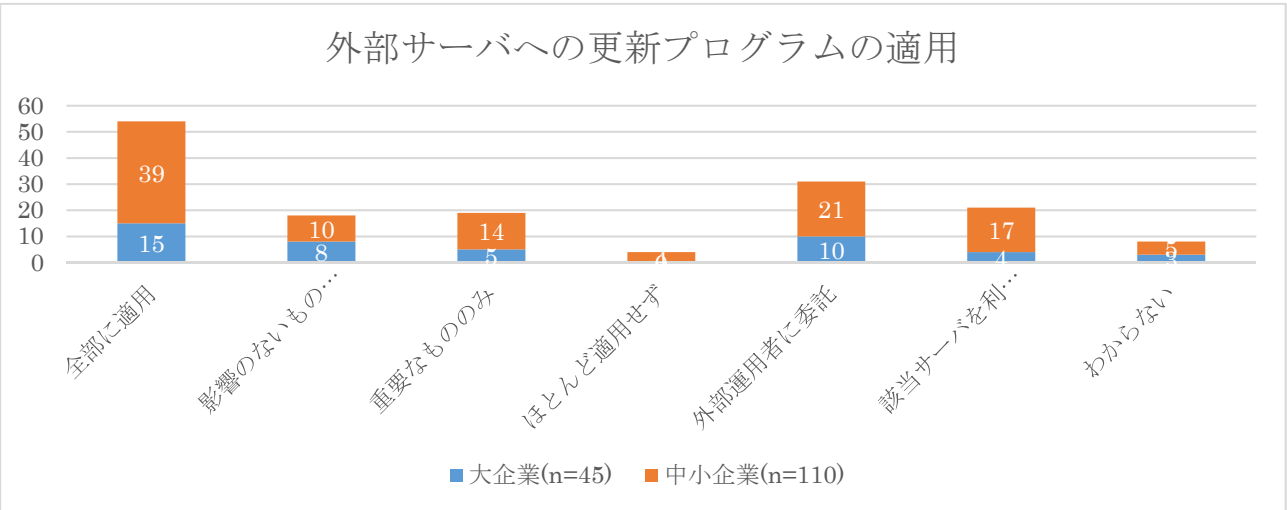


図 19　外部サーバへの更新プログラム適用状況に関する分布

4.1.8.2. 内部サーバへの更新プログラム適用状況について

外部サーバと同様に内部サーバ(インターネットからアクセス可能ではないセグメントに置かれているサーバ)についても更新プログラムの適用状況を調査した．結果を以下に示す．なお，2 社は未回答であった．全部に適用している会社が増えているものの，ほとんど適用せずという回答も増えている．インターネットから直接はアクセスできないサーバとはいえ，更新プログラムが適用されていない状況は問題があると考えられる．

表 15　内部サーバへの更新プログラム適用状況に関する分布

分類＼対策	全部に適用	影響のないもののみ適用	重要なもののみ適用	ほとんど適用せず	外部運用者に委託	該当サーバを利用せず	わからない
中小企業(n=109)	48	10	10	10	16	8	7
大企業(n=46)	15	12	8	4	3	1	3
全体	63	22	18	14	19	9	10

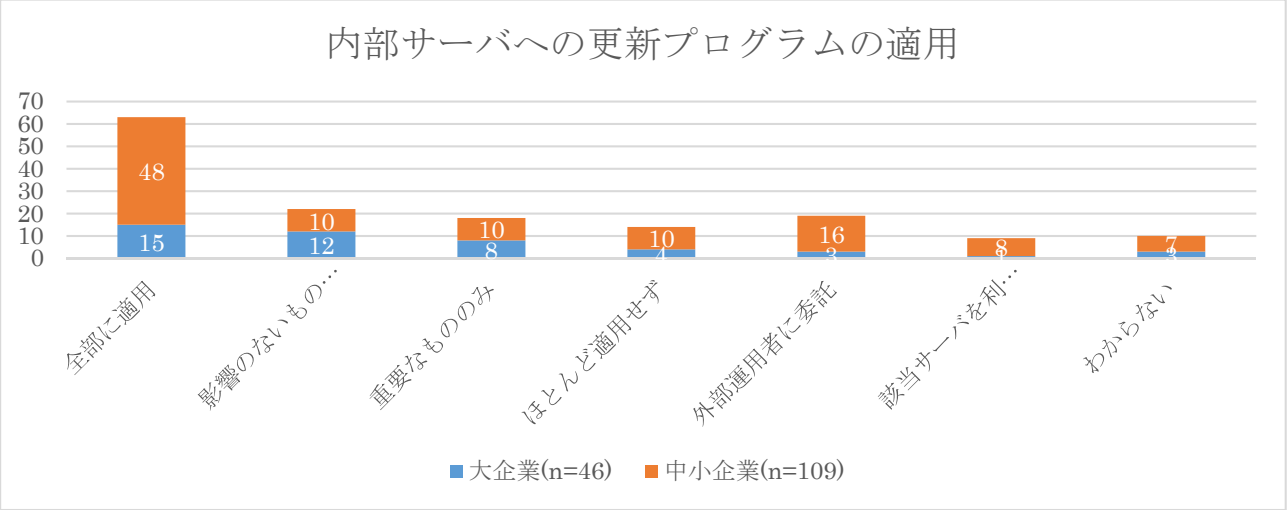


図 20　内部サーバへの更新プログラム適用状況に関する分布

4.1.8.3. サーバの分離

内部サーバと外部サーバの分離状況についての質問に関する回答を以下に示す．中小企業ではプロキシサーバが分離されていない現状，また分離がされていない現状が伺える．

表 16　サーバの分離状況に関する分布(複数回答)

分類＼項目	Web サーバを分離	メールサーバを分離	DNS サーバを分離	プロキシサーバを分離	特に分離せず	外部委託のため不明	該当サーバを利用せず	わからない
中小企業(n=109)	28	32	8	1	36	16	8	12
大企業(n=46)	26	26	24	17	2	3	4	3
全体	54	58	32	18	38	19	12	15

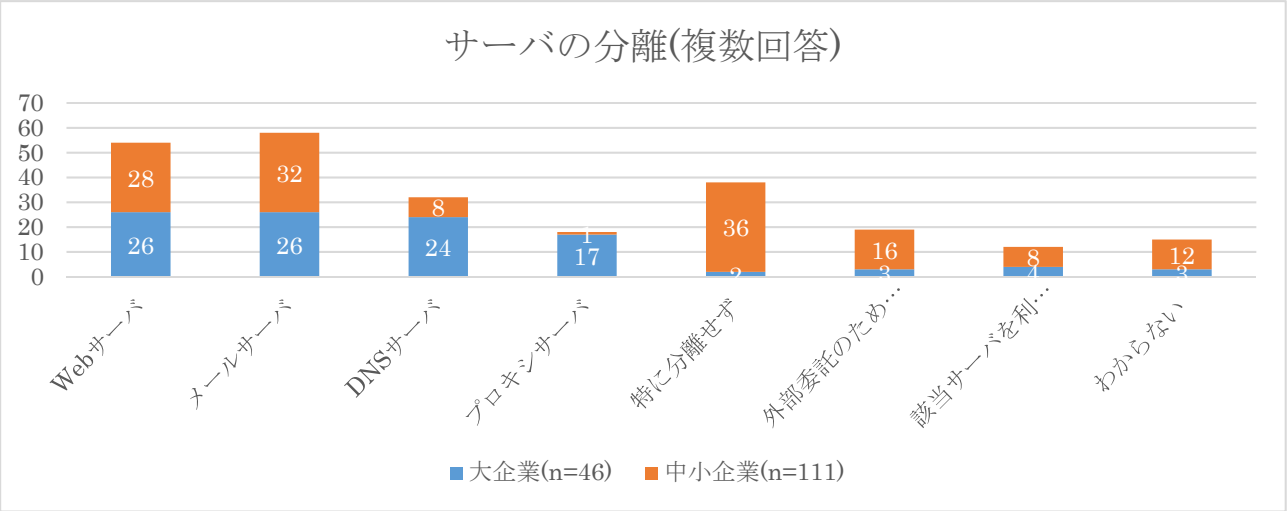


図 21　サーバの分離状況に関する分布(複数回答)

4.1.8.4. サーバに更新プログラムを適用しない理由

外部サーバ，内部サーバに対して更新プログラムを「ほとんど適用していない」企業に対してその理由を伺った結果を以下に示す．他の回答としては「最新サーバには適用しているが古いサーバには適用していない」「外部業者に任せている」が挙がった．現状正しく機能しているものに更新プログラムを適用することにより正しく機能しなくなることを懸念する意見が多い．

表 17　サーバに更新プログラムを適用しない理由に関する分布

分類＼対策	プログラム適用によるリスク回避	プログラム適用以外の手段が有効	プログラム未適用でも問題ないと判断	プログラム適用や評価にコストがかかる	その他
中小企業(n=10)	4	0	2	2	2
大企業(n=4)	3	0	0	1	0
全体	7	0	2	3	2

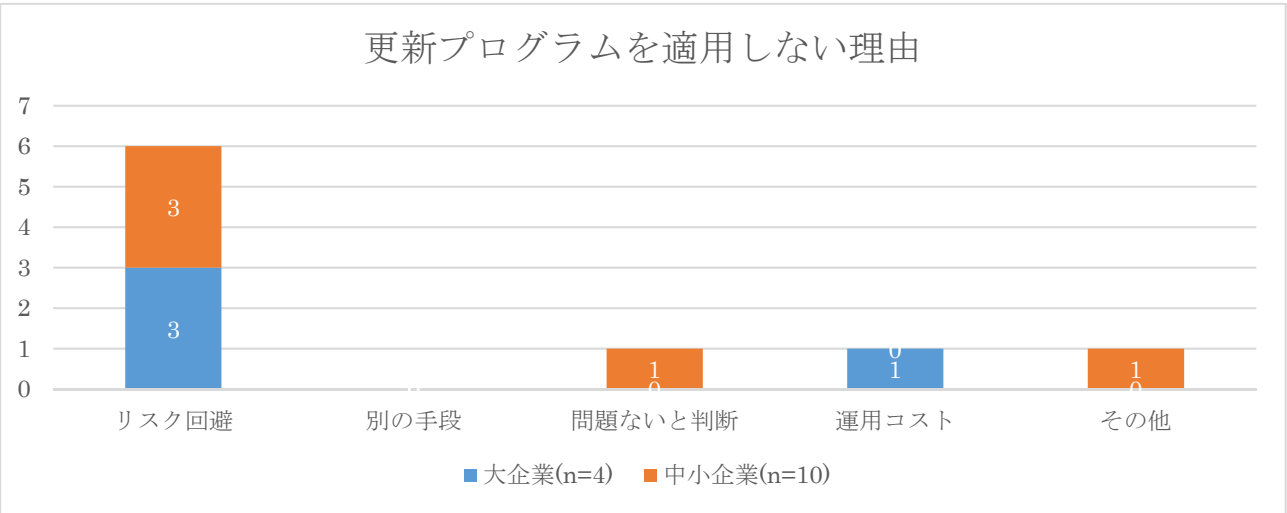


図 22　サーバに更新プログラムを適用しない理由に関する分布

4.1.9. IT 投資・情報セキュリティ投資について

過去 3 年間に IT 投資を実施したか否かの結果を以下に示す．なお，2 社が未回答であった．中小企業においては IT 投資があまり盛んでない傾向が伺える．

表 18 過去 3 年間に IT 投資を行ったかに関する分布

分類＼回答	行った	行っていない	わからない
中小企業(n=158)	95	58	5
大企業(n=40)	39	5	4
全体	134	63	9

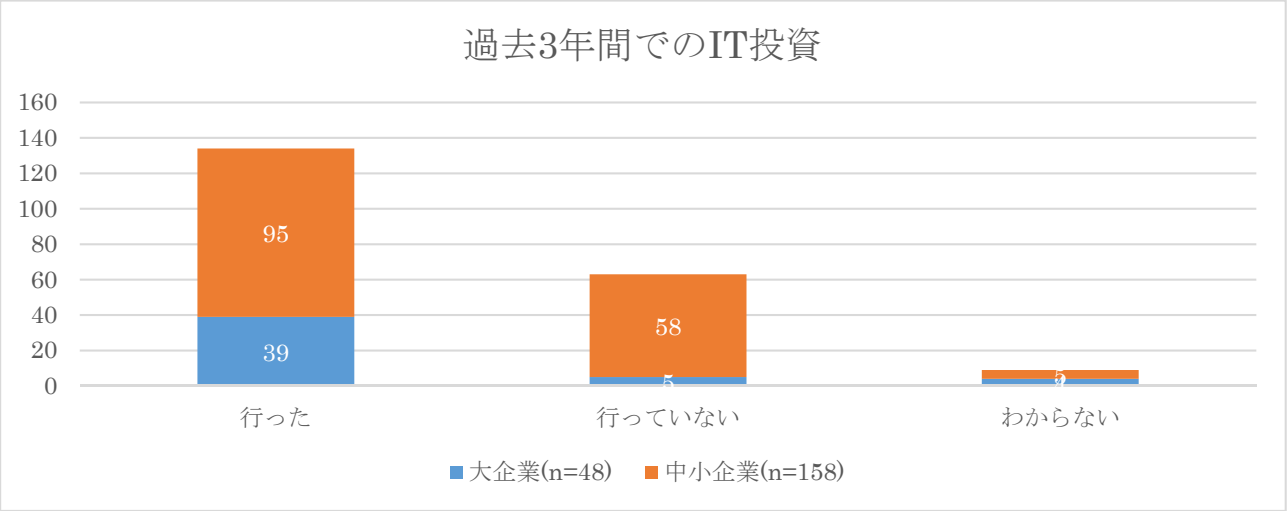


図 23 過去 3 年間に IT 投資を行ったかに関する分布

4.1.9.1. 過去 3 年の IT 投資の平均額

過去 3 年に IT 投資を行った企業に対して，その平均の投資額に関する結果は以下のとおりである．なお，2 社が未回答であった．従業員数の企業規模に比例した投資結果となっている．

表 19 過去 3 年の IT 投資の平均額の分布

分類＼費用	10 万円以下	10 万円超 50 万円以下	50 万円超 100 万円以下	100 万円超 200 万円以下	200 万円超 500 万円以下	500 万円超 1000 万円以下	1000 万円超 4000 万円以下	4000 万円超	わからない
中小企業(n=93)	8	25	20	12	15	5	4	2	2
大企業(n=39)	1	1	1	2	5	3	10	9	7
全体	9	26	21	14	20	8	14	11	9

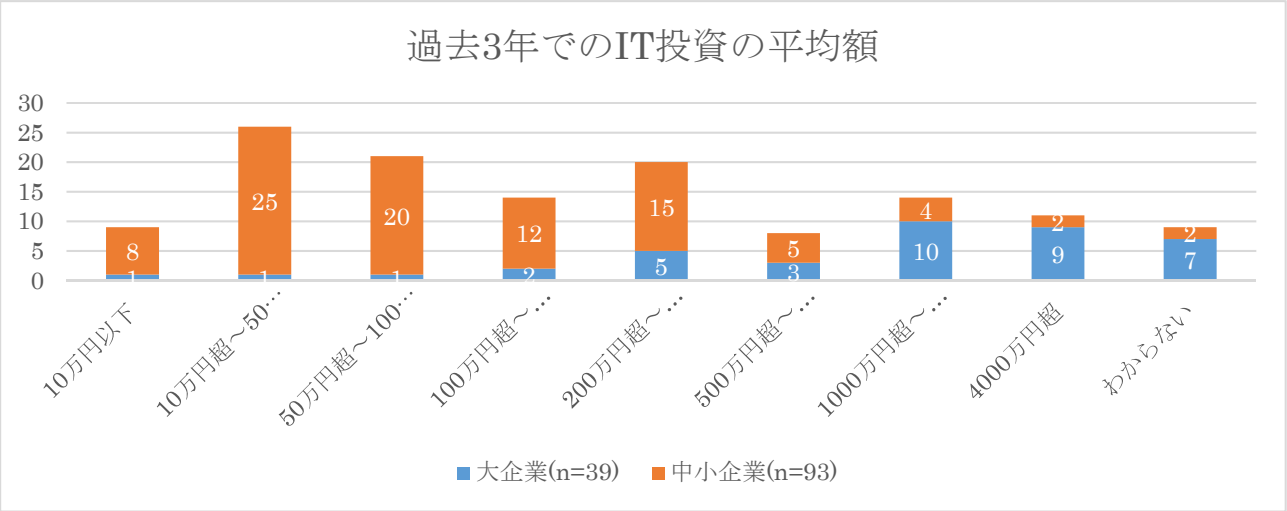


図 24　過去 3 年での IT 投資平均額の分布

4.1.9.2. IT 投資に情報セキュリティ投資が含まれるか

過去 3 年に IT 投資を実施した企業に対して，その投資の中に情報セキュリティに関する投資が含まれるかの調べた．結果を以下に示す．なお，1 社が未回答であった．中小企業では大企業に比べて情報セキュリティ投資が含まれないケースが多い割合を占める．

表 20　IT 投資に情報セキュリティの投資が含まれるかの分布

分類＼回答	含まれる	含まれない	わからない
中小企業(n=94)	71	20	3
大企業(n=39)	35	3	1
全体	106	23	4

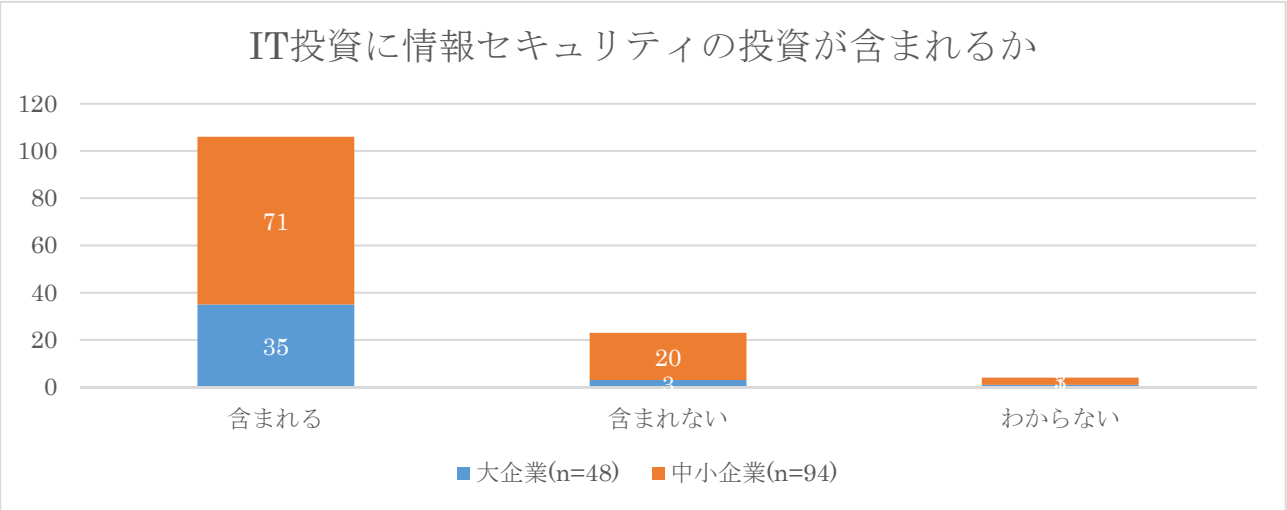


図 25　IT 投資に情報セキュリティに関する投資が含まれるかの分布

4.1.9.3. 過去 3 年の情報セキュリティへの投資の平均額

過去 3 年に IT 投資を行った企業に対して，その中で情報セキュリティに関する投資額がいくらかを調査した．結果は以下のとおりである．なお，1 社が未回答であった．従業員数の企業規模に比例した投資結果となっている．中小企業の 70%程度では IT 投資のうち 50 万円までが情報セキュリティに対して投資されていることがわかり，エンドポイントでのウイルス対策ソフトウェア費用などに使われている現状が伺える．

表 21　情報セキュリティ投資額の分布

分類＼費用	10 万円以下	10 万円超 50 万円以下	50 万円超 100 万円以下	100 万円超 200 万円以下	200 万円超 500 万円以下	500 万円超 1000 万円以下	1000 万円超 4000 万円以下	4000 万円超	わからない
中小企業(n=70)	22	26	11	4	1	0	0	1	5
大企業(n=35)	0	5	1	6	6	3	6	1	7
全体	22	31	12	10	7	3	6	2	12

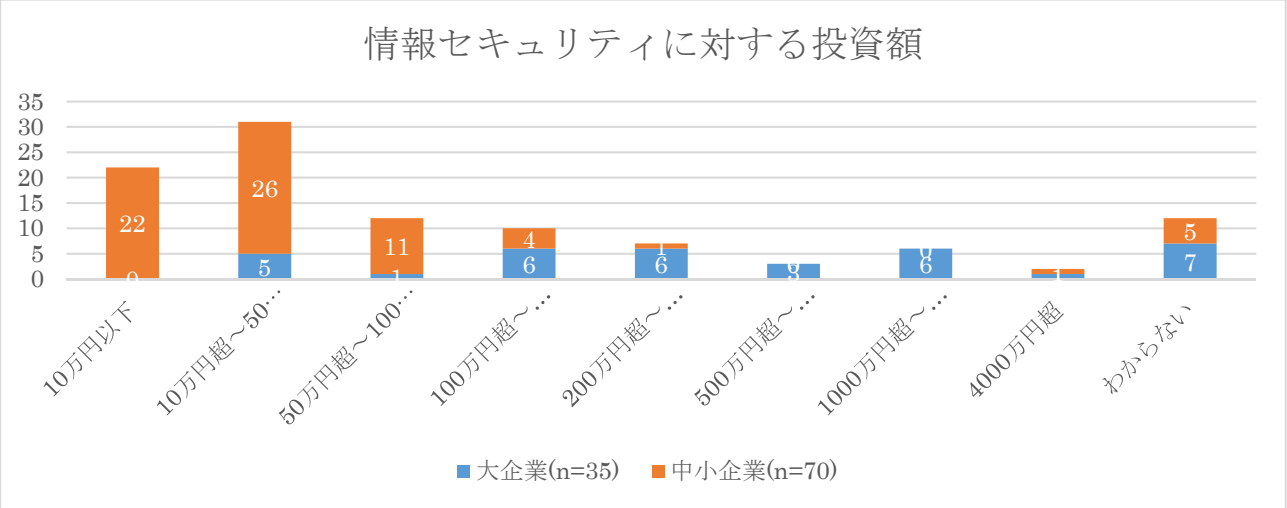


図 26　情報セキュリティ投資額の分布

4.1.9.4. 情報セキュリティ投資を行わない理由

過去 3 年に IT 投資を行ったものの，情報セキュリティ投資を行わなかった企業に対して，その理由を調査した．結果は以下のとおりである．その他の理由としては，「投資済み」「弊社担当が自己管理」「1 年以内に実施予定」「投資するものがない」「本社予算」が挙げられた．中小企業においては，費用対効果が見えない他に，コストや運用が不明といった理由により，情報セキュリティ投資に及び腰になっている現状がわかる．

表 22　情報セキュリティ投資を行わない理由に関する分布(複数回答)

分類＼対策	コストがかかりすぎる	費用対効果が見えない	どこからどう始めたらよいかわからない	導入後の手間がかかる	その他
中小企業(n=20)	5	7	5	3	5
大企業(n=3)	0	0	0	0	3
全体	5	7	5	3	8

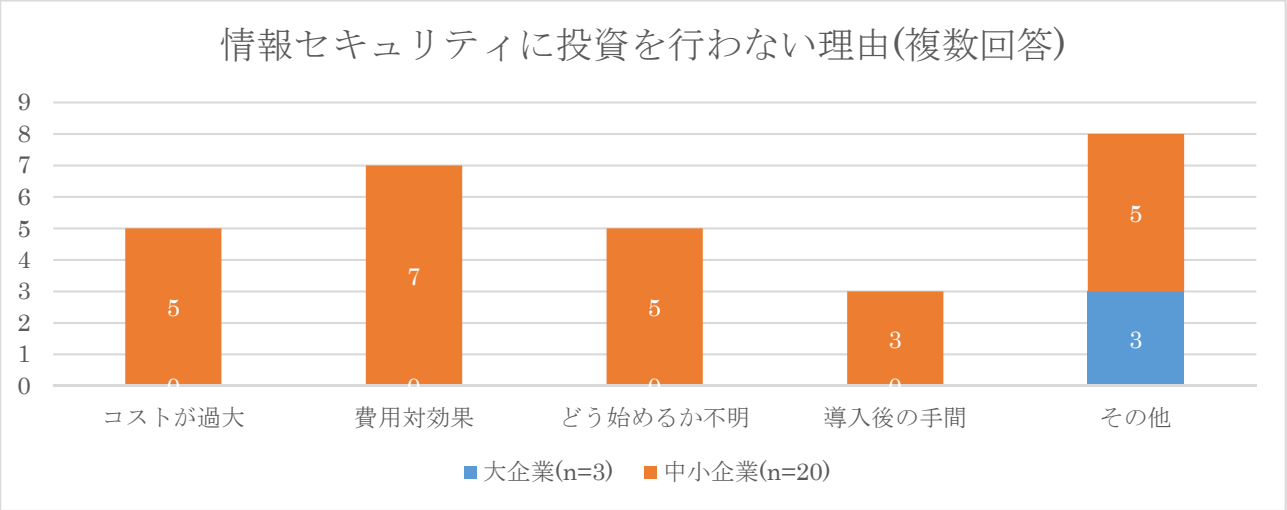


図 27　情報セキュリティ投資を行わない理由に関する分布(複数回答)

4.1.10. 利用しているシステム・サービス

経営資源の確保や業務効率化のために利用している情報システムとしてどのようなものがあるかを調査した．調査結果を以下に示す．その他で挙げられた回答としては「原価管理システム」「CAD システム」「土木管理システム」「グループウェア」「電子入札・電子契約」「Office365」「必要なものは自社で開発」といった項目が挙げられた．主にはホームページ開設等の広報業務に関する部分や，会計や給与を計算する，いわば間接部門で使われていることがわかる．一方で，中小企業においてこれらの業務では活用していないという回答も挙げられていた．

表 23　経営資源確保・業務効率化のために利用されているシステム・サービス(複数回答)

分類＼システム・サービス	フリーメール(Gmailなど)	顧客管理システム(CRM)	Webサイト，ホームページ開設	インターネットを活用した流通・決済	会計システム・アプリケーション	人事システム・アプリケーション
中小企業(n=160)	34	36	81	28	98	6
大企業(n=48)	6	16	45	18	43	30
全体	40	52	136	46	141	36
分類＼システム・サービス	給与システム・アプリケーション	出退勤管理システム・アプリケーション	稟議システム	文書管理システム	生産管理システム	コミュニケーションツール
中小企業(n=160)	80	18	9	17	14	21
大企業(n=48)	42	30	13	22	13	20
全体	122	48	22	39	27	41
分類＼システム・サービス	クラウドストレージ・無料	クラウドストレージ・有料	クラウドファンディング	クラウドソーシング	その他	活用していない
中小企業(n=160)	9	15	0	0	5	16
大企業(n=48)	6	15	0	0	4	0
全体	15	30	0	0	9	16

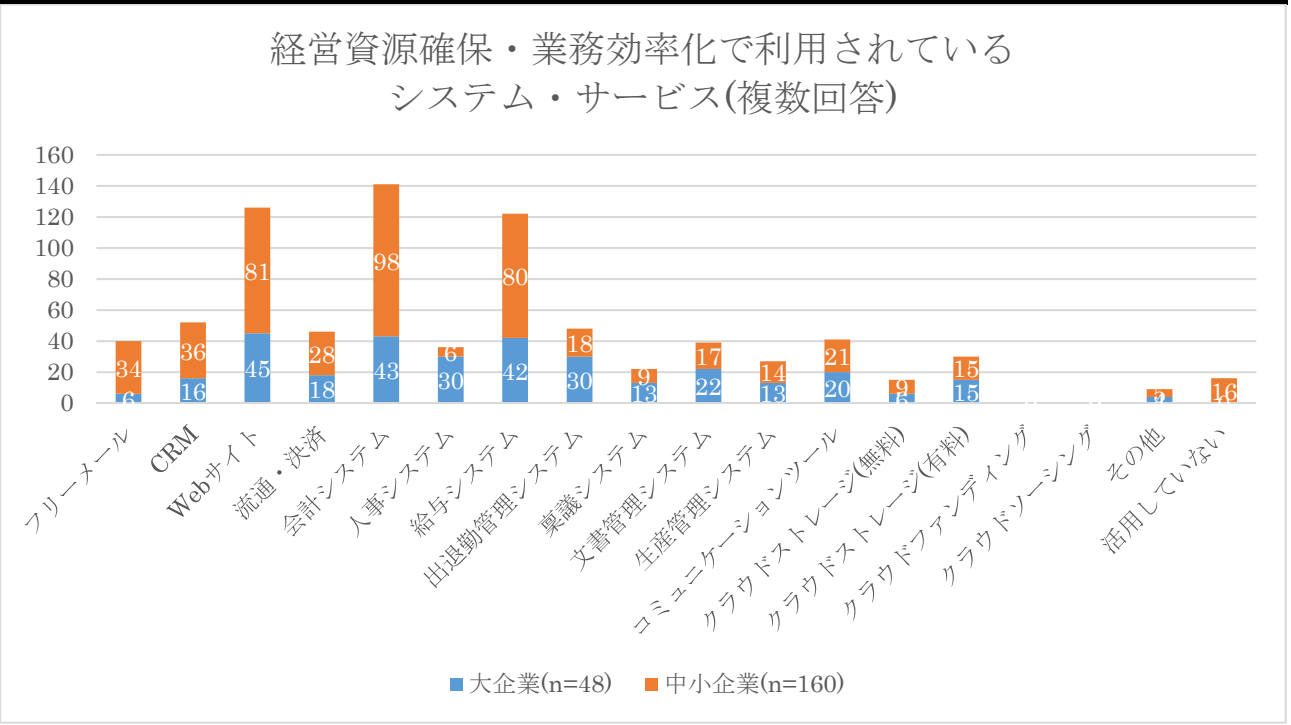


図 28　経営資源確保・業務効率化のために利用されているシステム・サービス(複数回答)

4.1.10.1. Web サイトにおける情報セキュリティ対策

利用しているシステム・サービスにおいて，「Web サイトやホームページの開設」を選択した企業について，実際にどのような情報セキュリティがとられているかを調査した．結果を以下に示す．中小企業においては対策があまりとられていない現状が伺える．

表 24　Web サイトにおける情報セキュリティ対策(複数回答)

分類＼対策	ログやファイル情報に基づく改ざん検知	定期的な Web コンテンツ診断	Web サイト管理者権限アカウントのルール策定
中小企業(n=81)	11	19	34
大企業(n=45)	20	16	36
全体	31	35	70

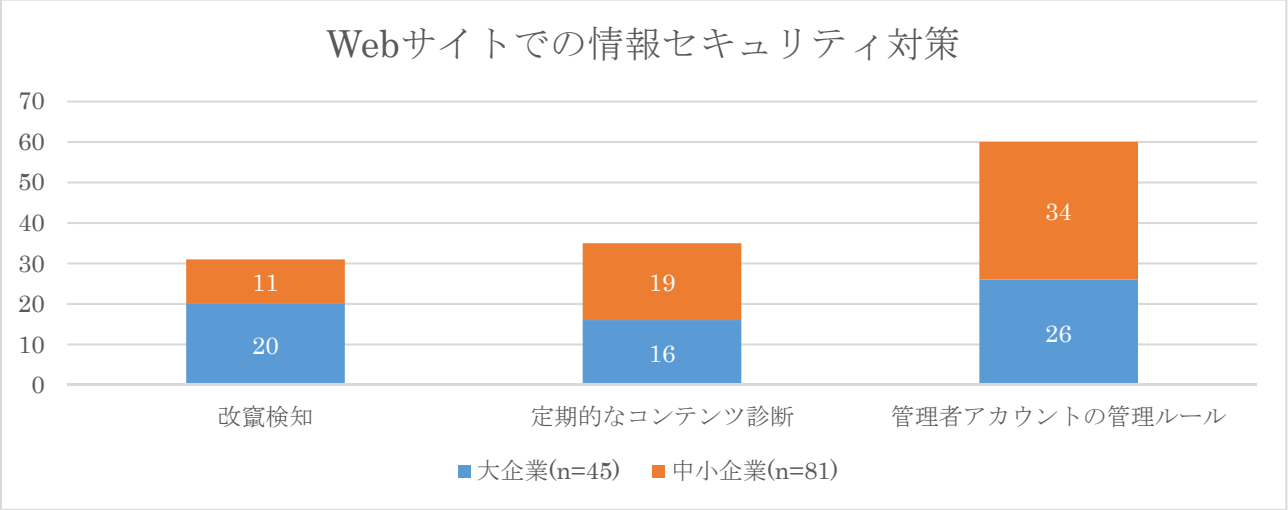


図 29　Web サイトにおける情報セキュリティ対策

4.1.11. サイバー保険への加入検討状況

企業に対してサイバー保険に加入しているか，また検討しているかの調査を行った．結果を以下に示す．なお，3 社が未回答であった．サイバー保険の内容を知らない企業も多く，サイバー保険に関する内容を周知する必要性がある現状が伺える．

表 25　サイバー保険に関する加入検討状況

分類＼状況	加入している	検討している，未加入	内容は知っている，未加入	内容を知らない，未加入	加入しているか不明
中小企業(n=157)	9	29	25	76	18
大企業(n=48)	3	7	12	10	16
全体	12	36	37	86	34

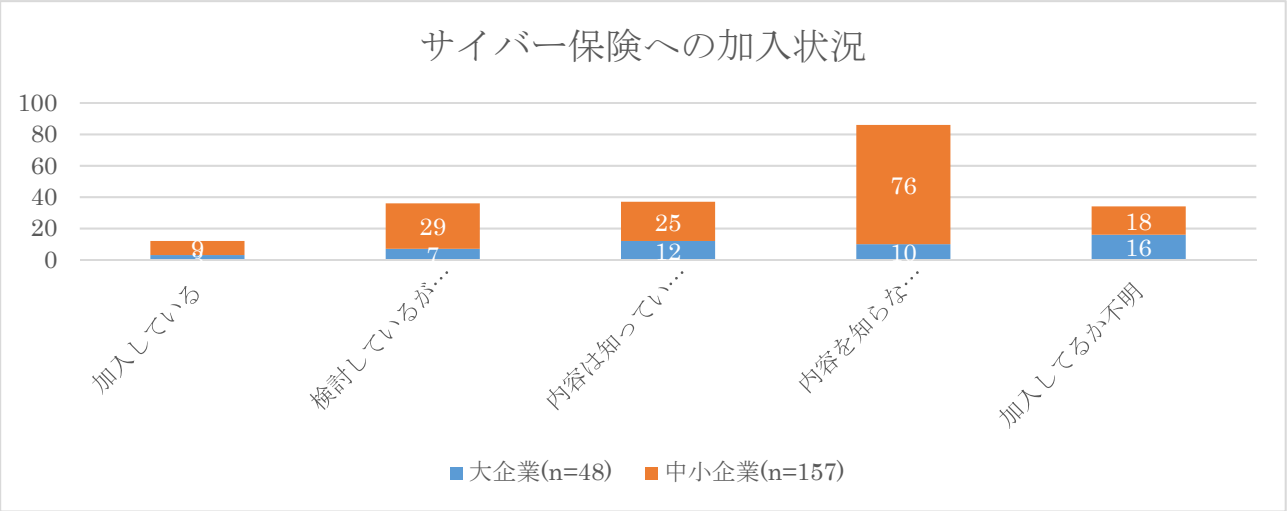


図 30　サイバー保険に関する加入検討状況

4.1.12. 情報漏洩賠償責任保険への加入検討状況

企業に対して情報漏洩賠償責任保険に加入しているか，また検討しているかの調査を行った．結果を以下に示す．なお，4 社が未回答であった．サイバー保険よりも情報漏洩賠償責任保険の内容が具体的でもあるため加入している企業が多くなっているものの，情報漏洩賠償責任保険の内容を知らない企業も多く，情報漏洩賠償責任保険に関する内容を周知する必要性がある現状が伺える．

表 26　情報漏洩賠償責任保険に関する加入検討状況

分類＼状況	加入している	検討している，未加入	内容は知っている，未加入	内容を知らない，未加入	加入しているか不明
中小企業(n=156)	17	26	20	74	19
大企業(n=48)	6	6	11	9	16
全体	23	32	31	83	35

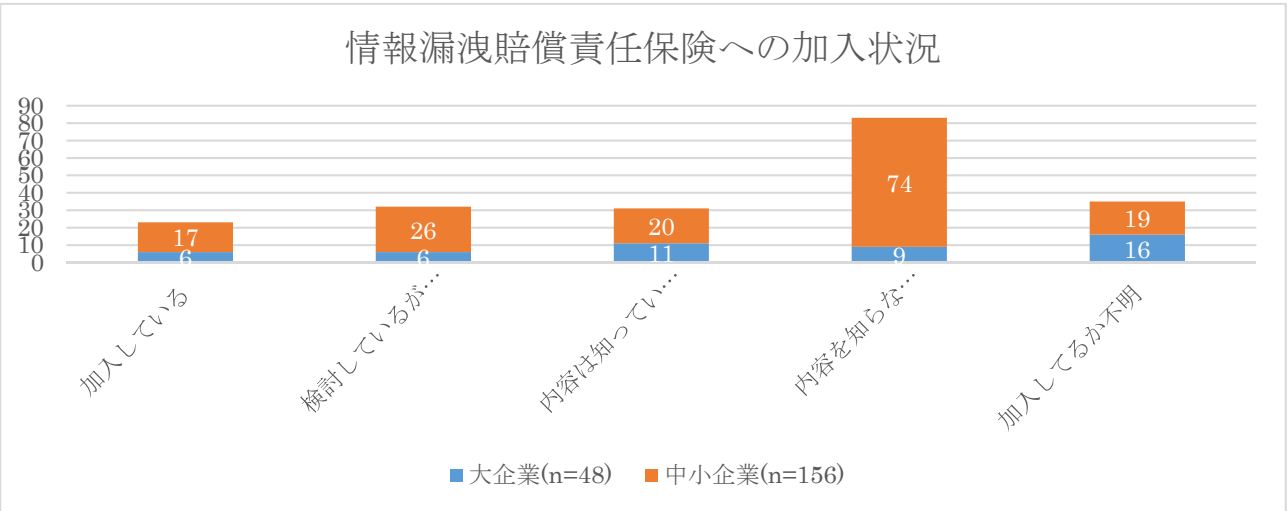


図 31　情報漏洩賠償責任保険に関する加入検討状況

4.1.13. コンピュータウイルスの感染・発見状況

コンピュータウイルスに感染したことがあるかについての調査を行った．調査結果を以下に示す．なお，1 社が未回答であった．ウイルスに感染した企業が 18.8%あり，また 62%の企業がウイルスに感染・ウイルスの発見といったインシデントに遭遇している．

表 27　コンピュータウイルスの感染・発見の状況の分布

分類＼状況	ウイルスに感染した	ウイルスを発見したが，感染には至らなかった	ウイルスを発見せず，感染に至らなかった	わからない
中小企業(n=159)	22	67	54	16
大企業(n=48)	16	23	6	3
全体	39	90	60	19

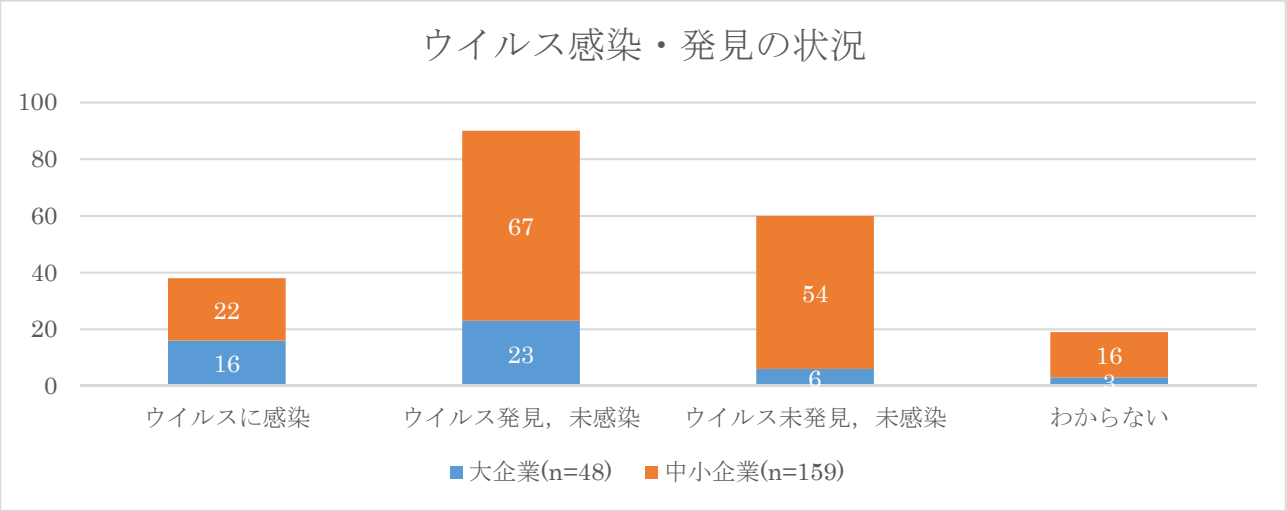


図 32　コンピュータウイルスの感染・発見の状況の分布

4.1.13.1. ウイルスの感染経路

ウイルスに感染した，あるいはウイルスを発見した企業に対して，ウイルスの侵入経路がどのようなものと想定されるかについて調査を行った．調査は複数回答である．結果を以下に示す．主だったところは，電子メールやインターネット接続が多く，持ち込み PC や P2P 共有によるものはほぼ皆無であった．

表 28　ウイルス侵入経路の分布(複数回答)

分類＼経路	電子メール	インターネット接続	ダウンロードしたファイル	ファイル共有ソフト	外部記憶媒体	持ち込み PC	その他	わからない
中小企業(n=89)	58	40	18	0	17	0	0	1
大企業(n=39)	30	21	8	0	13	1	0	1
全体	88	61	26	0	30	1	0	2

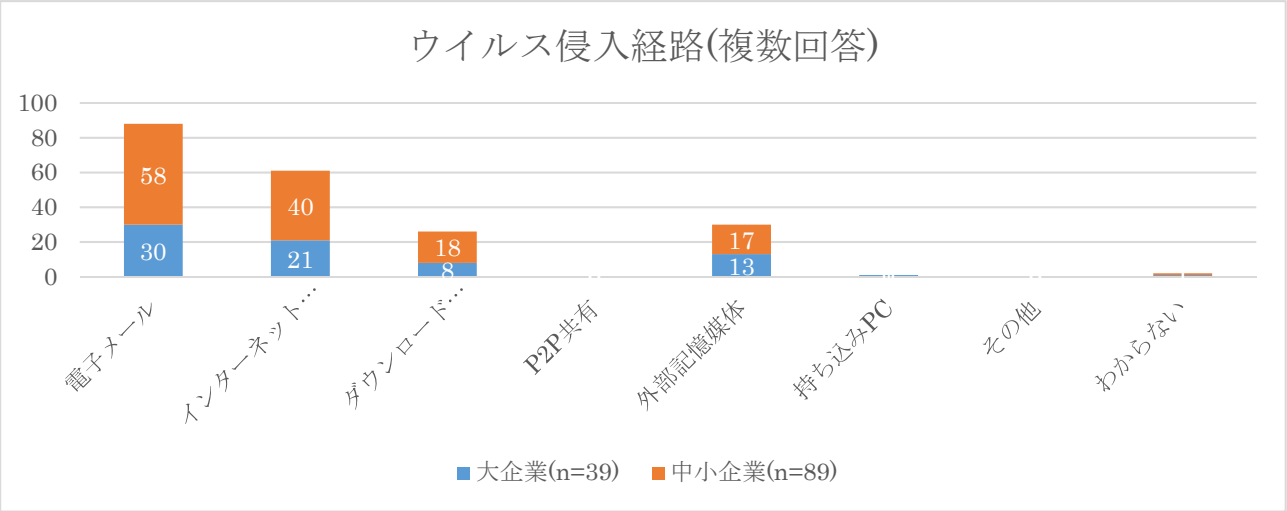


図 33　ウイルス侵入経路の分布(複数回答)

4.1.13.2. ウイルス感染時の被害

ウイルスに感染した企業を対象に，ウイルス感染時の被害を複数回答していただいた．結果を以下に示す．パソコン単体の停止とそれに伴う業務停滞，またデータ破壊といったところが主な項目で，ウイルスに感染した企業の外部へと感染を拡大した例はないことがわかる．

表 29　ウイルス感染時の被害(複数回答)

分類＼被害	データの破壊	情報の漏洩	ウイルスメール等の発信	ネットワークの遅延	システム停止・性能低下	パソコン単体の停止
中小企業(n=22)	4	2	4	3	4	7
大企業(n=16)	7	0	0	2	4	5
全体	11	2	4	5	8	12

分類＼被害	関連部門の業務停滞	個人の業務停滞	取引先への感染拡大	その他	特になし
中小企業(n=22)	2	7	0	0	4
大企業(n=16)	4	6	0	0	0
全体	6	13	0	0	4

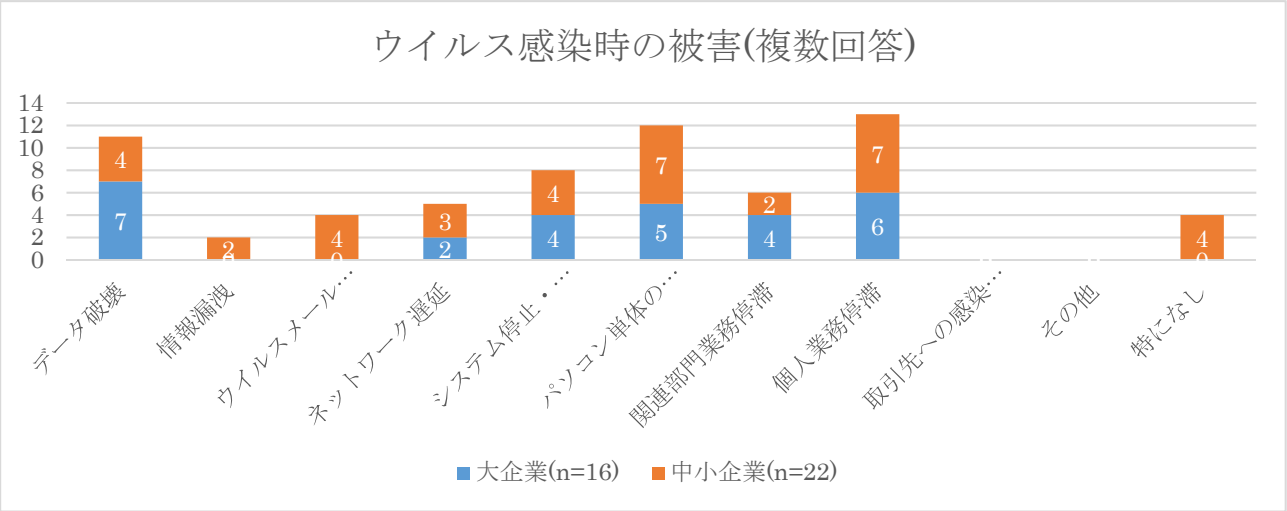


図 34　ウイルス感染時の被害(複数回答)

4.1.14. 内部不正による情報セキュリティ上のトラブル

内部不正者や外部委託者による情報セキュリティ上のトラブルがあったかについて調査した．結果を以下に示す．なお，4 社が未回答であった．不正による被害はなかったという回答が 82.6%を占めたものの，大企業では内部者の不正による被害があった割合が中小企業と比較して高く，従業員に目が届きづらいことが内部不正を起こしやすくしていることがわかる．

表 30　内部不正による情報セキュリティ上のトラブルの分布

分類＼状況	内部者の不正による被害があった	委託者の不正による被害があった	不正による被害はなかった	わからない
中小企業(n=157)	4	1	136	16
大企業(n=47)	3	0	36	8
全体	7	1	172	24

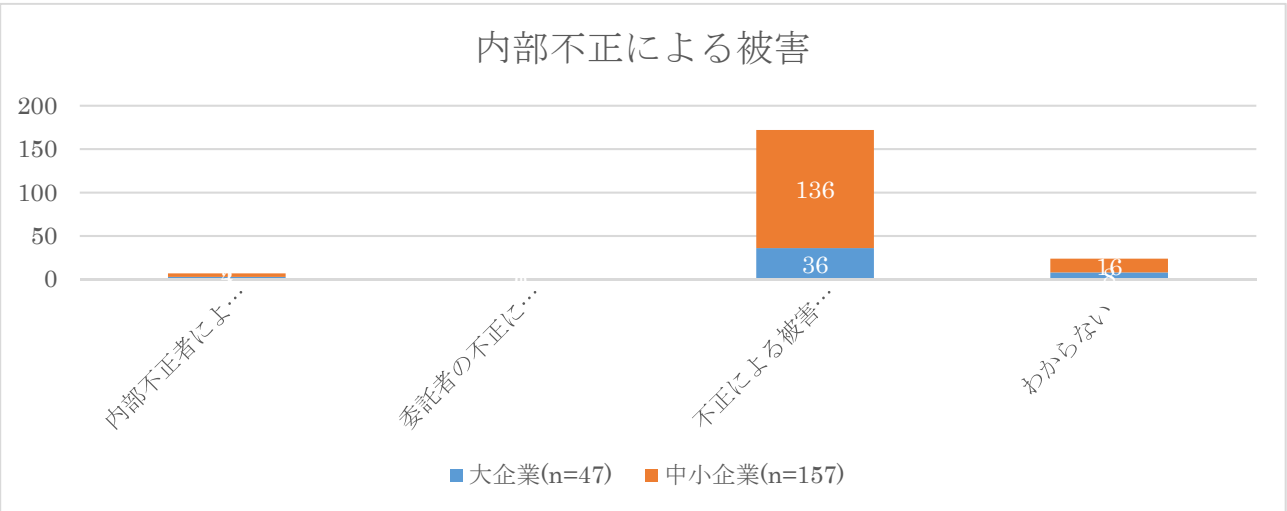


図 35　内部不正による情報セキュリティ上のトラブルの分布

4.1.15. サイバー攻撃を受けたか

サイバー攻撃を受けたかについての調査を行った．結果を以下に示す．なお，4 社が未回答であった．サイバー攻撃による被害を受けたケースは約 4%と少ないものの，わからないケースが 20%程度を占めており，サイバー攻撃に対して知覚できるような技術的な能力を有することも重要となると考える．

表 31　サイバー攻撃およびその被害状況に関する分布

分類＼状況	サイバー攻撃を受けた，被害あり	サイバー攻撃を受けた，被害なし	サイバー攻撃を全く受けなかった	わからない
中小企業(n=156)	4	20	101	31
大企業(n=48)	5	10	23	10
全体	9	30	124	41

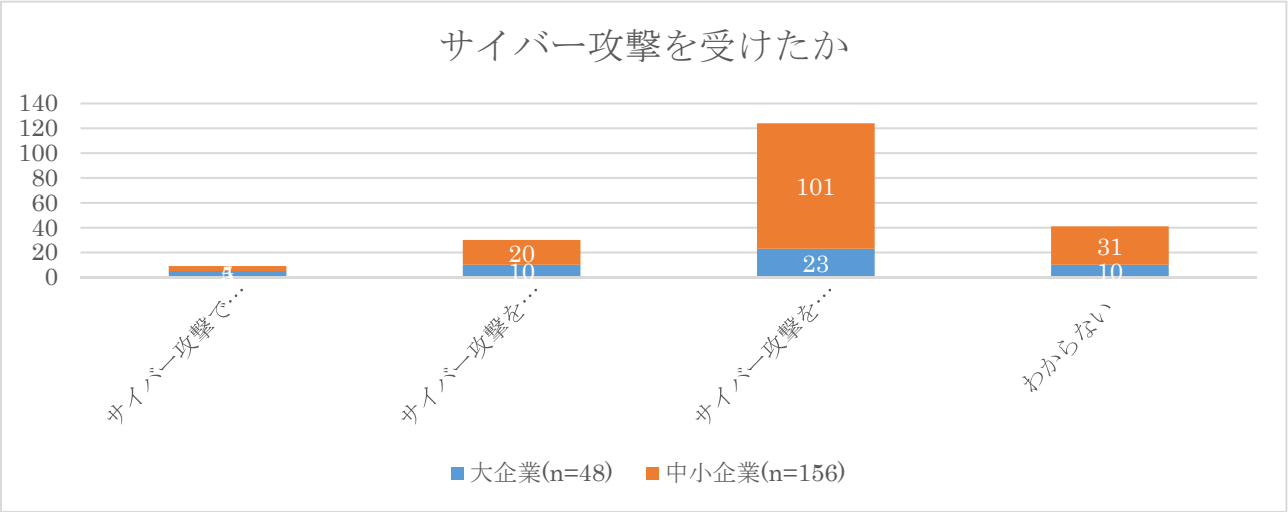


図 36　サイバー攻撃及びその被害状況に関する分布

4.1.15.1. サイバー攻撃の手口

被害の有無にかかわらず，サイバー攻撃を受けた企業に対してその攻撃がどのような手法であったかの調査を行った．結果を以下に示す．その他としては，「メール添付」が 2 件挙げられた．標的型攻撃や DoS(Denial of Service)攻撃，ID パスワード漏洩による不正アクセスが主だったものとなるが，一方で手口不明であるという数も多くを占めており，サイバー攻撃に対する理解が進んでない状況が伺える．

表 32　サイバー攻撃の手口に関する分布(複数回答)

分類＼手口	ID パスワード漏洩による不正アクセス	脆弱性を突かれたことによる不正アクセス	SQL インジェクション
中小企業(n=24)	3	1	0
大企業(n=15)	2	3	0
全体	5	4	0

分類＼手口	DoS 攻撃	標的型攻撃	ランサムウェア	その他	手口はわからない
中小企業(n=24)	2	10	3	1	12
大企業(n=15)	7	2	3	1	2
全体	9	12	6	2	14

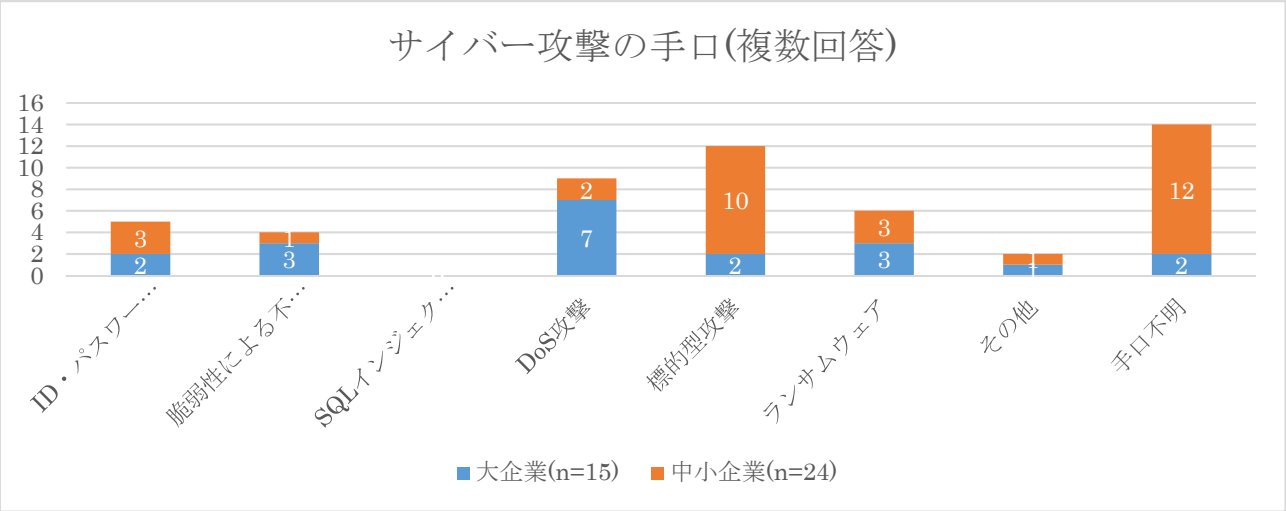


図 37　サイバー攻撃の手口に関する分布(複数回答)

4.1.15.2. サイバー攻撃による被害の状況

サイバー攻撃を受け，被害にあった企業に対して具体的な被害状況を調査した．結果を以下に示す．その他では「PC の停止」「PC の初期化」「メールサーバの停止」といった項目が挙げられた．

表 33　サイバー攻撃による被害の状況に関する分布(複数回答)

分類＼被害	Web サイトの改竄	Web サイトの停止・機能低下	業務サーバの内容改竄	業務サーバの停止・機能低下	運用するネットサービスでのなりすまし	取引先企業や個人への被害拡大	情報が盗まれた	その他
中小企業(n=4)	0	0	0	0	2	0	0	2
大企業(n=5)	2	0	0	2	0	0	0	1
全体	2	0	0	2	2	0	0	3

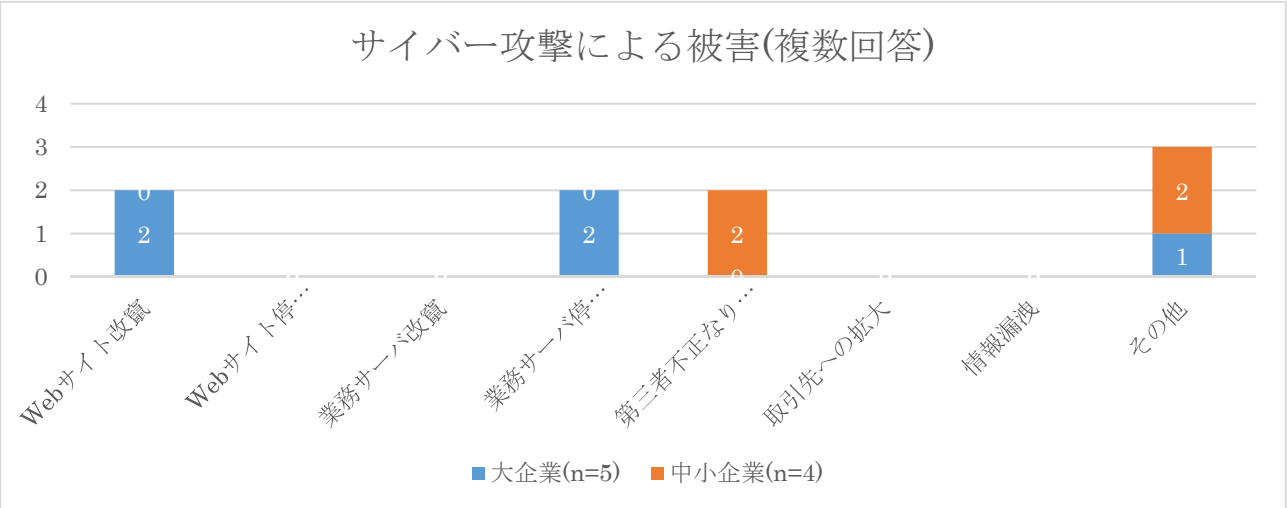


図 38　サイバー攻撃による被害の状況に関する分布(複数回答)

4.1.15.3. サイバー攻撃からの復旧に要した時間

サイバー攻撃を受け被害にあった企業に対して，サイバー攻撃からの復旧に要した時間を調査した．結果を以下に示す．すべてで 1 週間以内には復旧していることがわかる．またサンプル数が少ないものの，中小企業においては大企業に比べて復旧に時間を要する傾向がある．

表 34　サイバー攻撃からの復旧に要した時間に関する分布

分類＼被害	1 日以下	2～3 日以内	1 週間以内	1～2 週間以内	1 か月以内	1 か月以上
中小企業(n=4)	1	1	2	0	0	0
大企業(n=5)	4	0	1	0	0	0
全体	5	1	3	0	0	0

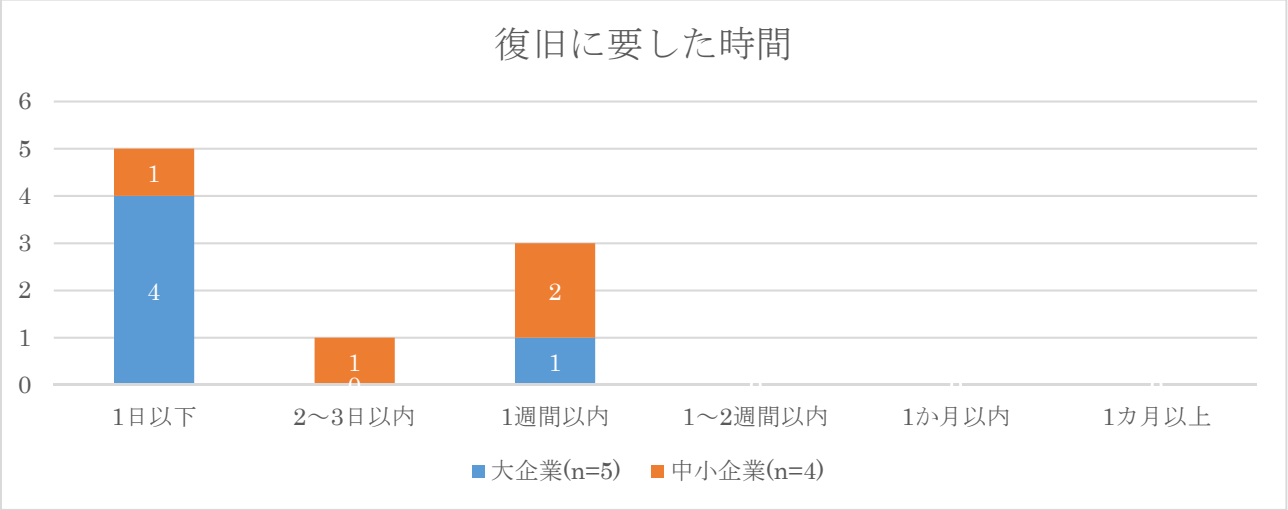


図 39　サイバー攻撃からの復旧に要した時間に関する分布

4.1.15.4. サイバー攻撃の被害の金銭換算

サイバー攻撃を受け被害を受けた企業に対して，その被害を金銭換算するといくらになるかの調査を行った．結果を以下に示す．中小企業において 500 万円超 1000 万円以下という額は企業体力を大きく奪うものになる可能性がある．また，大企業においてすべてが「わからない」という回答となった．

表 35　サイバー攻撃の被害の金銭換算に関する分布

分類＼費用	10 万円以下	10 万円超 50 万円以下	50 万円超 100 万円以下	100 万円超 200 万円以下	200 万円超 500 万円以下	500 万円超 1000 万円以下	1000 万円超 4000 万円以下	4000 万円超	わからない
中小企業(n=4)	2	0	1	0	0	1	0	0	0
大企業(n=5)	0	0	0	0	0	0	0	0	5
全体	2	0	1	0	0	1	0	0	5

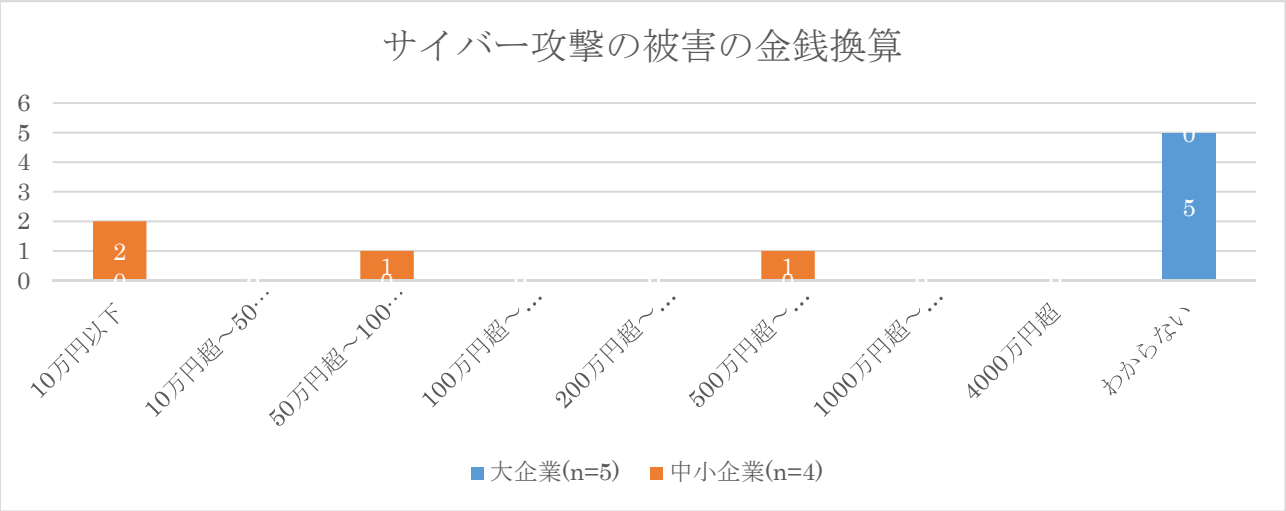


図 40　サイバー攻撃の被害の金銭換算に関する分布

4.1.16. 情報セキュリティに関する意識状況について

社員の不正により営業上の秘密や個人情報等の情報漏洩が起こるかに関する調査を行った．結果を以下に示す．なお，1 社が未回答であった．中小企業では，「あまりそう思わない」「思わない」といった割合が高くなっている傾向がある．

表 36　社員の不正による情報漏洩の可能性があるかの意識に関する分布

分類＼意識	そう思う	ややそう思う	あまりそう思わない	思わない	わからない
中小企業(n=159)	22	33	51	41	12
大企業(n=48)	17	14	10	4	3
全体	39	47	61	45	15

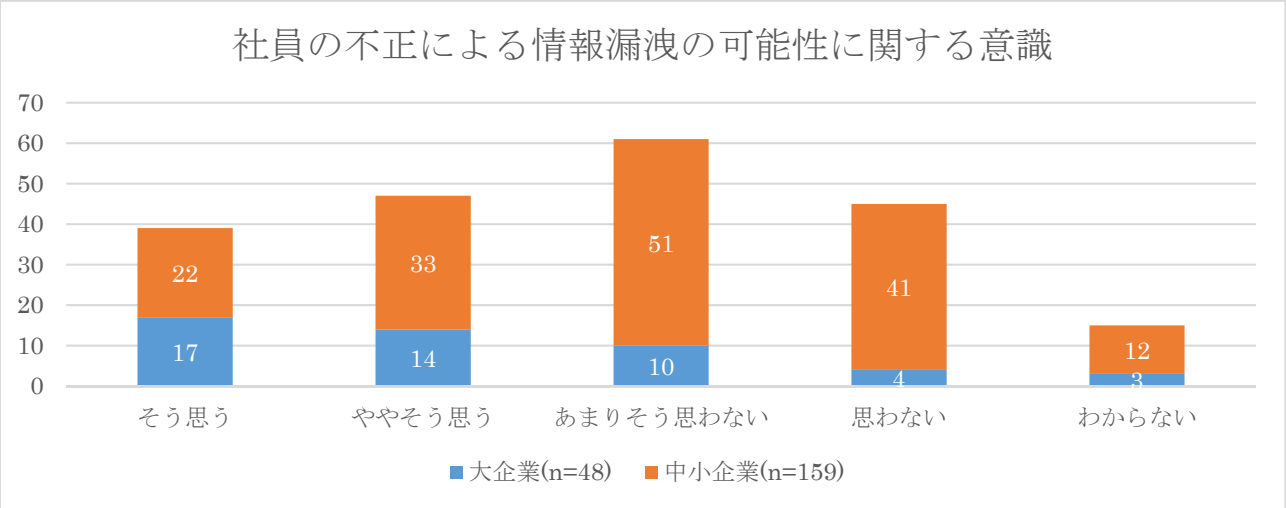


図 41　社員の不正による情報漏洩の可能性があるかの意識に関する分布

外部からのサイバー攻撃により，営業上の秘密や個人情報等の情報漏洩が起こるかに関する調査を行った．結果を以下に示す．なお，2 社が未回答であった．全体的な傾向では社員不正による情報漏洩の可能性の意識と大きく変わるところはないが，「思わない」というやや可能性があるという認識が大きくなっている．

表 37　外部からのサイバー攻撃による情報漏洩の可能性があるかの意識に関する分布

分類＼意識	そう思う	ややそう思う	あまりそう思わない	思わない	わからない
中小企業(n=158)	23	35	56	24	20
大企業(n=48)	6	16	18	2	6
全体	29	51	74	26	26

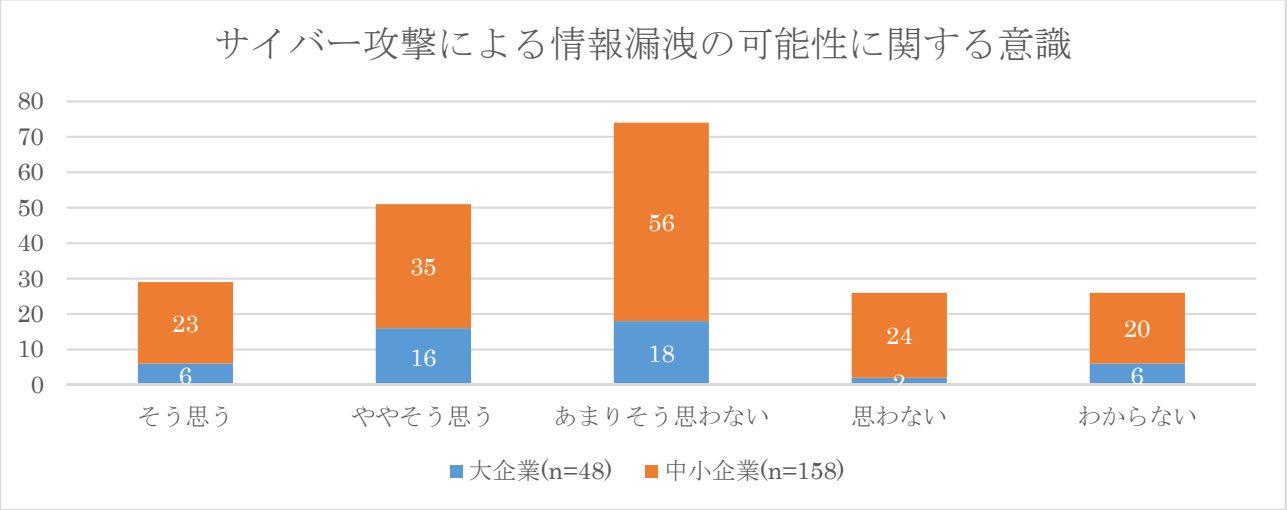


図 42　外部からのサイバー攻撃による情報漏洩の可能性があるかの意識に関する分布

また，情報セキュリティに関する理解度が高いかの認識に関する調査を行った．結果を以下に示す．情報セキュリティに対する理解度では，「あまりそう思わない」という回答が多くなっている．

表 38　情報セキュリティに関する理解度が高いかに関する分布

分類＼意識	そう思う	ややそう思う	あまりそう思わない	思わない	わからない
中小企業(n=158)	9	48	74	21	6
大企業(n=48)	15	17	13	3	0
全体	24	65	87	24	6

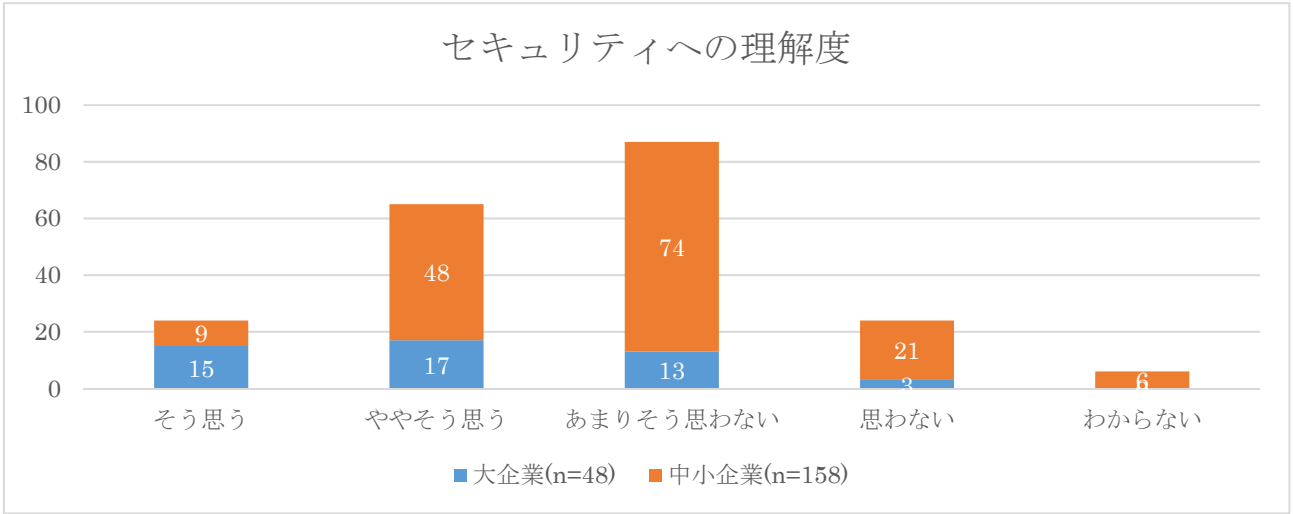


図 43　情報セキュリティに関する理解度が高いかに関する分布

4.1.17. 情報セキュリティの実施体制

情報セキュリティのレベルを日々維持していくためには，組織作りが大事な要素の 1 つとなる．実際に会社に情報セキュリティ担当の文書があるかについて調査を行った．結果を以下に示す．なお，5 社が未回答であった．従業員数が少ないせいか，中小企業では組織的な体制がとられていない割合が 50%程度をとっており，インシデントが発生した場合の対応が個人任せになっている可能性がある．

表 39　情報セキュリティの実施体制に関する分布

分類＼状況	専門部署(担当者)がある	兼務だが担当者が任命されている	組織的に行っていない	わからない
中小企業(n=155)	13	54	80	8
大企業(n=48)	31	13	4	0
全体	44	67	84	8

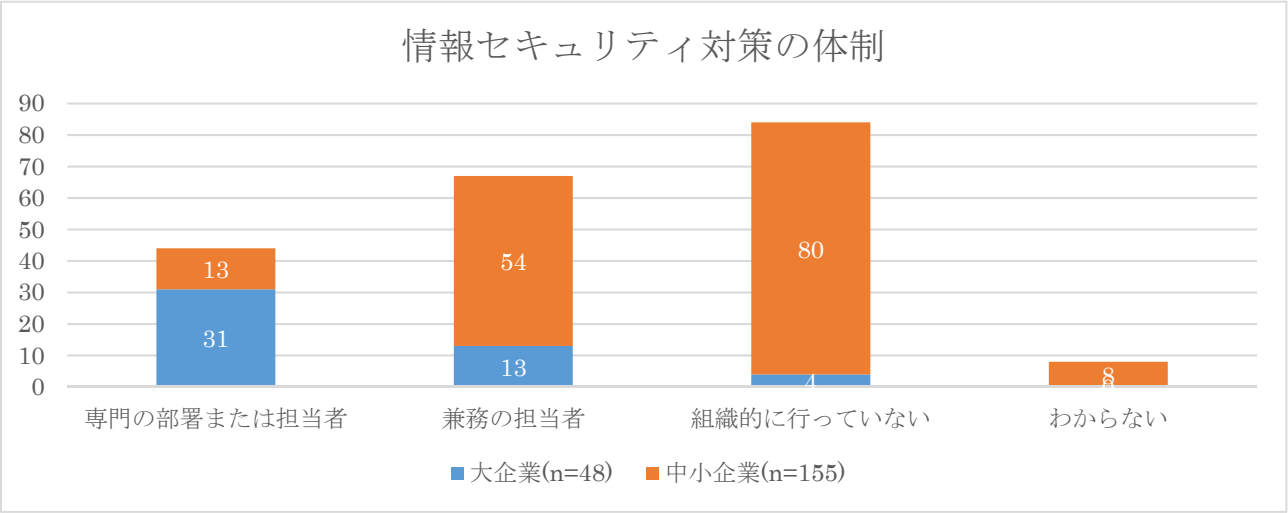


図 44　情報セキュリティの実施体制に関する分布

4.1.18. 情報セキュリティに関する相談先・情報収集先

情報セキュリティに際し，困ったことがあった場合に関する相談先について調査を行った．結果を以下に示す．なお，その他では「取引先」「親会社」「グループ会社」「知人」といった回答が挙げられた．IT 関連業者が最も多い結果となっており，社内担当者がそれに続いている．また，中小企業では，困ったことがあっても相談先がない企業が約 19%あり，万が一インシデント等が発生し，自社内で解決できない場合に懸念される状況である．

表 40　情報セキュリティに関する困ったことの相談先の分布(複数回答)

分類＼相談先	社内担当者	IT 関連業者	中小企業診断士	IT コーディネータ	商工団体	公的機関	その他	特にない
中小企業(n=160)	48	108	0	7	3	5	11	19
大企業(n=48)	27	27	0	1	0	3	3	0
全体	75	135	0	8	3	8	14	19

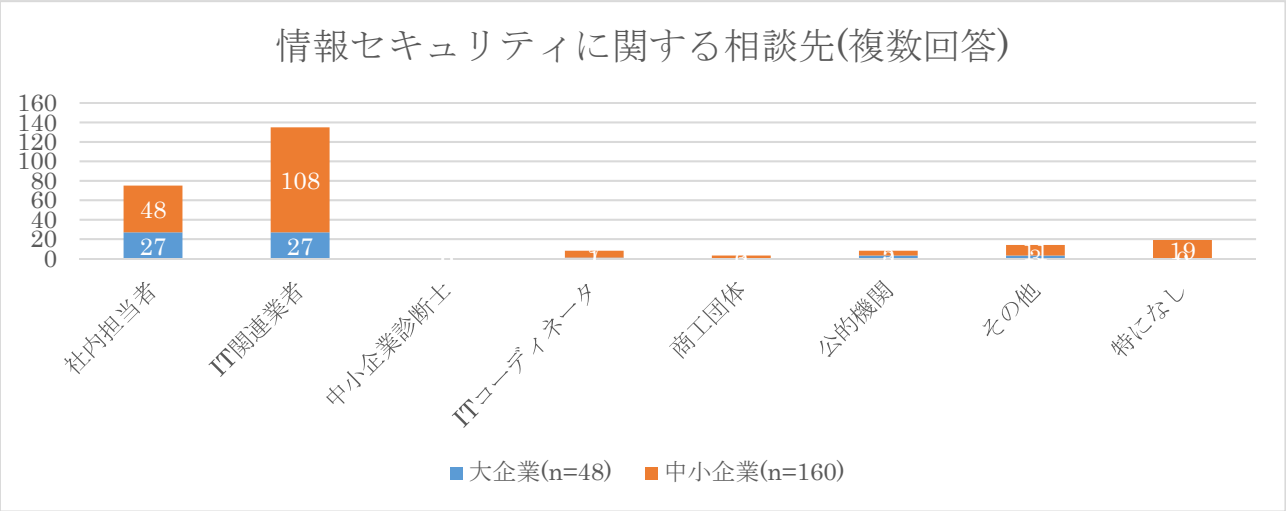


図 45　情報セキュリティに関する困ったことの相談先の分布(複数回答)

続いて，情報セキュリティに関する情報をどこから収集するかの調査を行った．結果を以下に示す．主には，情報セキュリティに関する相談先の分布の傾向と同様であるが，これに加えてインターネットやマスメディアといった，比較的容易に情報をとりやすい手段がとられることが多いことが伺える．

表 41　情報セキュリティに関する情報収集先の分布(複数回答)

分類＼収集先	社内担当者	IT 関連業者	中小企業診断士	IT コーディネータ	商工団体	公的機関	雑誌・新聞
中小企業(n=160)	44	107	1	9	4	13	18
大企業(n=48)	28	30	0	1	1	7	7
全体	72	137	1	10	5	20	25

分類＼収集先	テレビ	インターネット	無料のセミナー・実務研修	有料のセミナー・実務研修	その他	特になし
中小企業(n=160)	15	53	19	9	7	20
大企業(n=48)	3	25	12	9	5	0
全体	18	78	31	18	12	20

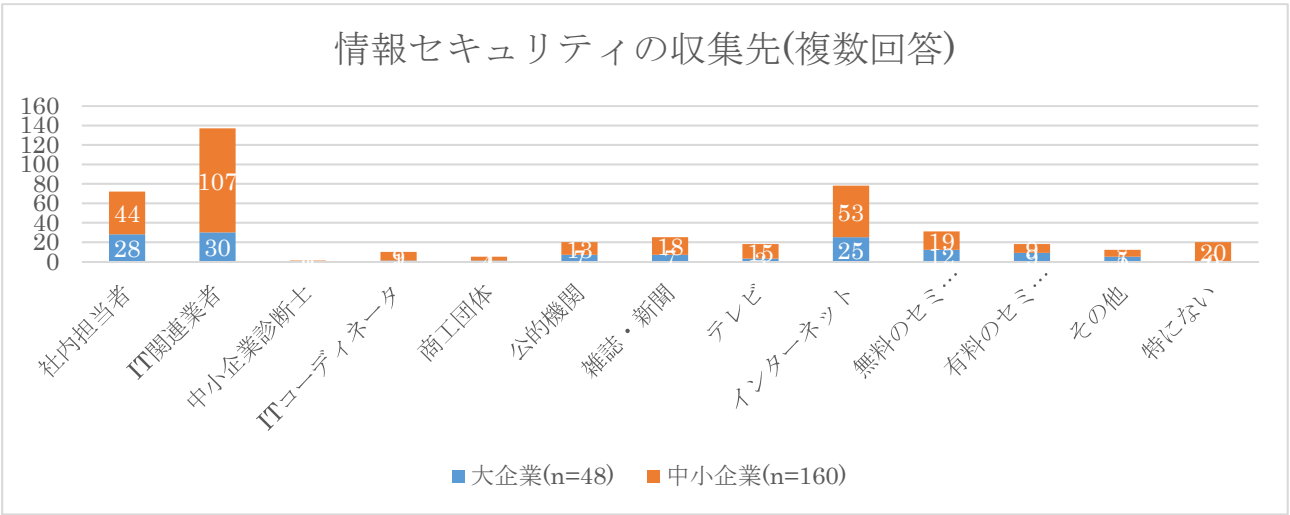


図 46　情報セキュリティに関する情報収集先の分布(複数回答)

4.1.19. 情報セキュリティに関する教育

企業内における情報セキュリティ教育の実施状況とその手段について調査した．結果を以下に示す．実施している場合には関連情報の周知，社内研修が多く，中小企業においては特に実施されていない企業が 65%超を占めている．

表 42　情報セキュリティ教育の実施状況の分布(複数回答)

分類＼実施方法	関連情報の周知	e-ラーニング	外部講習会・セミナー聴講	外部講師の招へい	社内研修・勉強会	特に実施なし
中小企業(n=160)	33	3	10	3	20	109
大企業(n=48)	40	19	5	4	24	4
全体	73	22	15	7	44	113

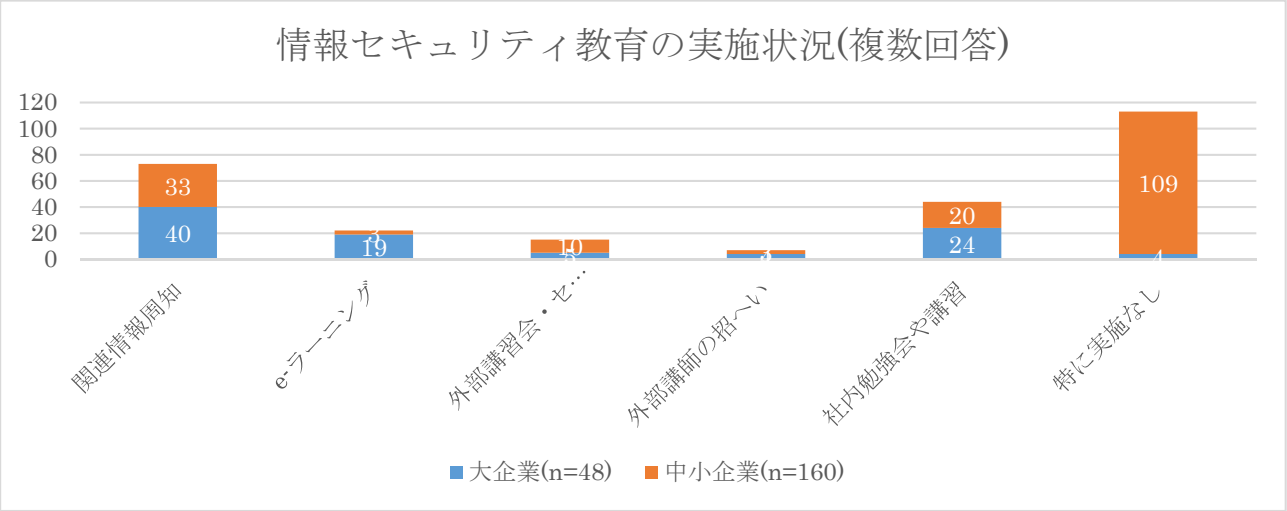


図 47　情報セキュリティ教育の実施状況の分布(複数回答)

4.1.19.1. 情報セキュリティに関する社内研修・勉強会の定期的な実施

情報セキュリティに関する社内研修や勉強会を実施している企業を対象に，それらを定期的に実施しているかの調査を行った．結果を以下に示す．なお，1 社が未回答であった．期間として挙げられたのは，「新入社員研修や雇用時(3 社)」「年 1 度(7 社)」「半年ごと」「3 カ月ごと」「1 か月ごと」といった頻度が挙げられた．また，定期的に行う研修と不定期に行う研修を組み合わせて実施している会社も 1 社あった．

表 43　情報セキュリティに関する社内研修・勉強会の定期的な実施の分布

分類＼定期性	定期的に実施	不定期に実施	わからない
中小企業(n=20)	4	16	0
大企業(n=24)	9	14	0
全体	13	30	0

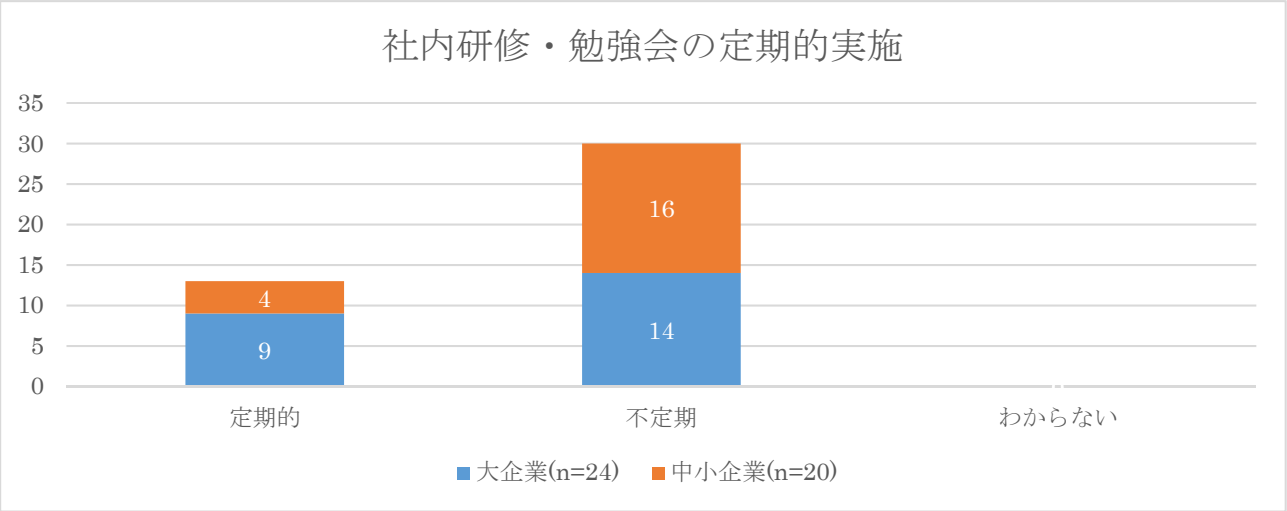


図 48　情報セキュリティに関する社内研修・勉強会の定期的な実施の分布

4.1.20. 情報セキュリティに関するルールや規定の文章化

情報セキュリティに関するルールや規定が文章化されているかについて調査を行った．結果を以下に示す．なお，5 社が未回答であった．大企業ではほぼ文章化されているのに対し，中小企業では文章化されていない企業が 65%超を占めていた．従業員の顔が見えやすいことが，かえってルールや規定を文章化しづらいように出ている傾向が伺える．

表 44　情報セキュリティに関するルールや規定の文章化

分類＼定期性	文章化されている	文章化されていない	わからない
中小企業(n=155)	36	109	10
大企業(n=48)	42	5	1
全体	78	114	11

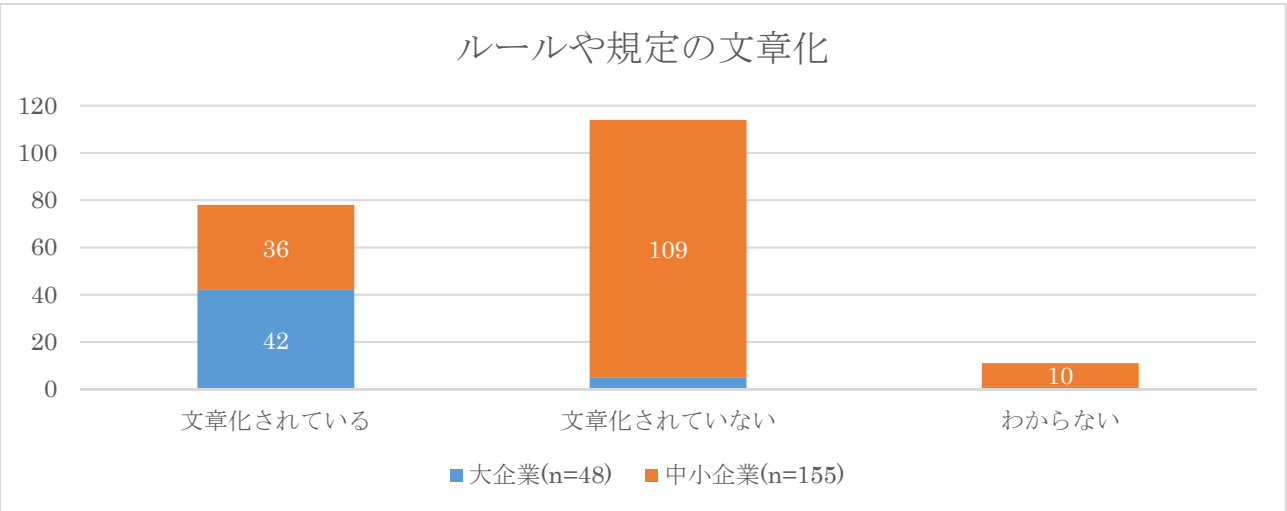


図 49　情報セキュリティに関するルールや規定の文章化

4.1.20.1. 文章化されているルール・規定

情報セキュリティに関するルールや規定が文章化されている企業に対して，具体的にどのような項目が文章化されているかを調査した．結果を以下に示す．その他では，「ISO27001(ISMS)にかかる項目」や，「グループ会社での対応」という回答が挙がった．中小企業では基本的なルールが策定されているのみにとどまっている．

表 45　文章化されているルール・規定に関する分布(複数回答)

分類＼規定項目	基本的ルール	責任者の任命	従業員または部署の権限や役割	情報資産の識別・重要度の分類
中小企業(n=36)	34	16	10	7
大企業(n=42)	41	26	25	24
全体	75	42	35	31
分類＼規定項目	機器等の利用制限・破損紛失の項目	著作権侵害	その他	特にない
中小企業(n=36)	17	2	0	1
大企業(n=42)	31	14	3	0
全体	48	16	3	1

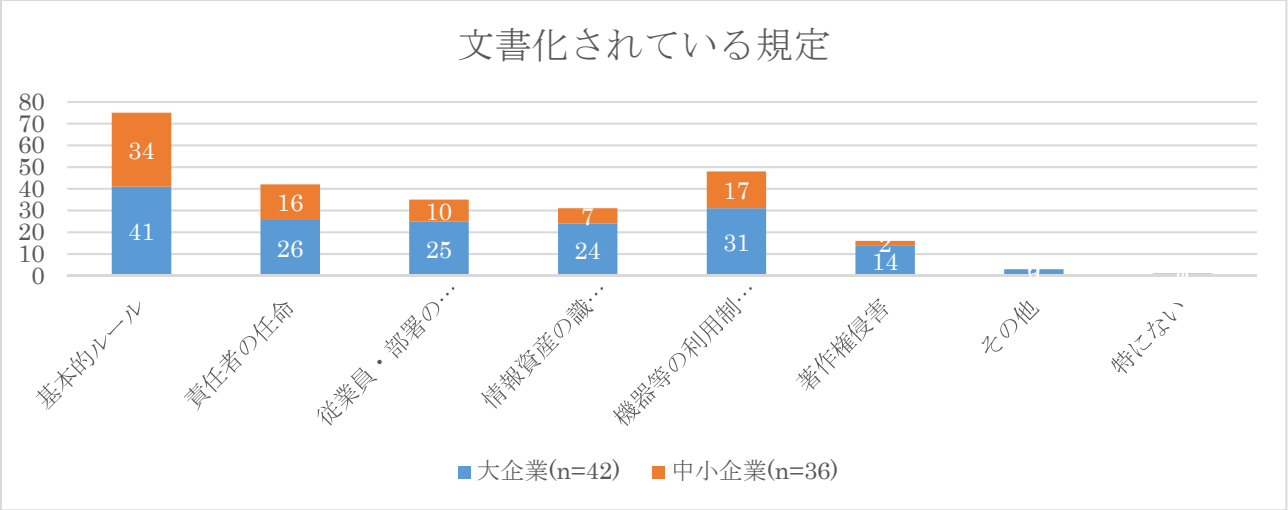


図 50　文章化されているルール・規定に関する分布(複数回答)

4.1.21. 情報セキュリティに関するルールからの逸脱措置の規定

情報セキュリティに関するルールや規定からの逸脱した場合について，その措置が就業規則等で規定されているかについて調査を行った．結果を以下に示す．なお，4 社が未回答であった．

表 46　情報セキュリティに関するルールからの逸脱措置の規定状況に関する分布

分類＼規定項目	規定されている	規定されていない	わからない	就業規則がない
中小企業(n=156)	42	93	14	7
大企業(n=48)	34	11	3	0
全体	76	104	17	

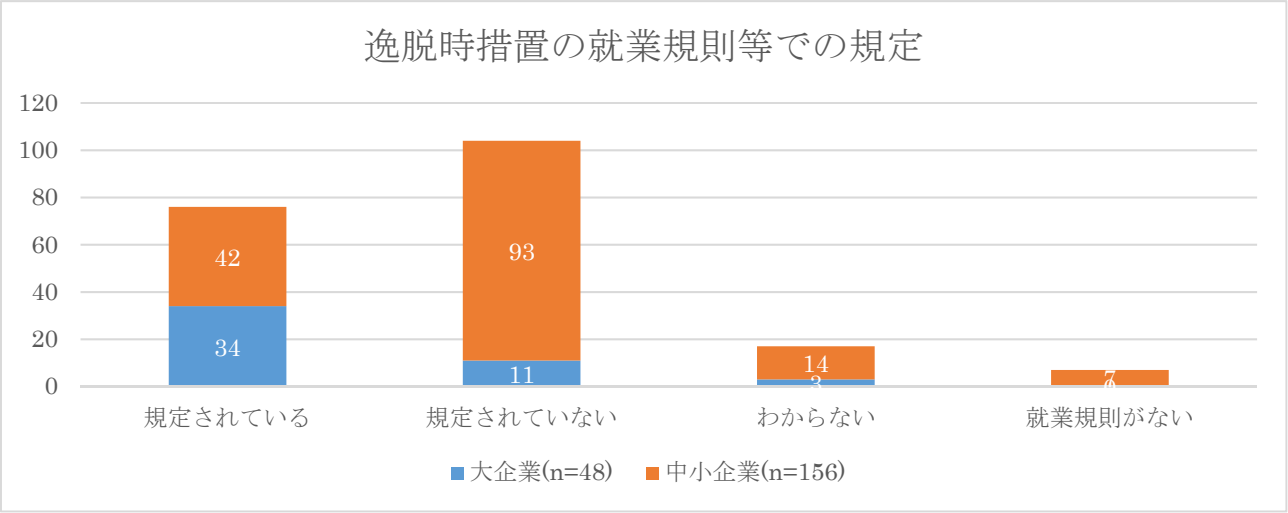


図 51　情報セキュリティに関するルールからの逸脱措置の規定状況に関する分布

4.1.22. 情報漏洩等の情報セキュリティ事故または兆候発生時の対策方法の規定

情報漏洩等の情報セキュリティ事故または兆候発生時に対策方法が規定されているかについて調査を行った．結果を以下に示す．なお，4 社が未回答であった．大企業であれば規定されている割合が 70%を超えるのに対し，中小企業においては約 16%であった．いざ情報セキュリティ上の事故があった場合に，上述した組織的な対応ができているところが少ないことから，組織として適切な対応が取れない可能性があることが示唆される．

表 47　情報セキュリティ事故または兆候発生時の対策方法の規定状況に関する分布

分類＼定期性	規定されている	規定されていない	わからない
中小企業(n=156)	26	119	11
大企業(n=48)	34	12	2
全体	60	131	13

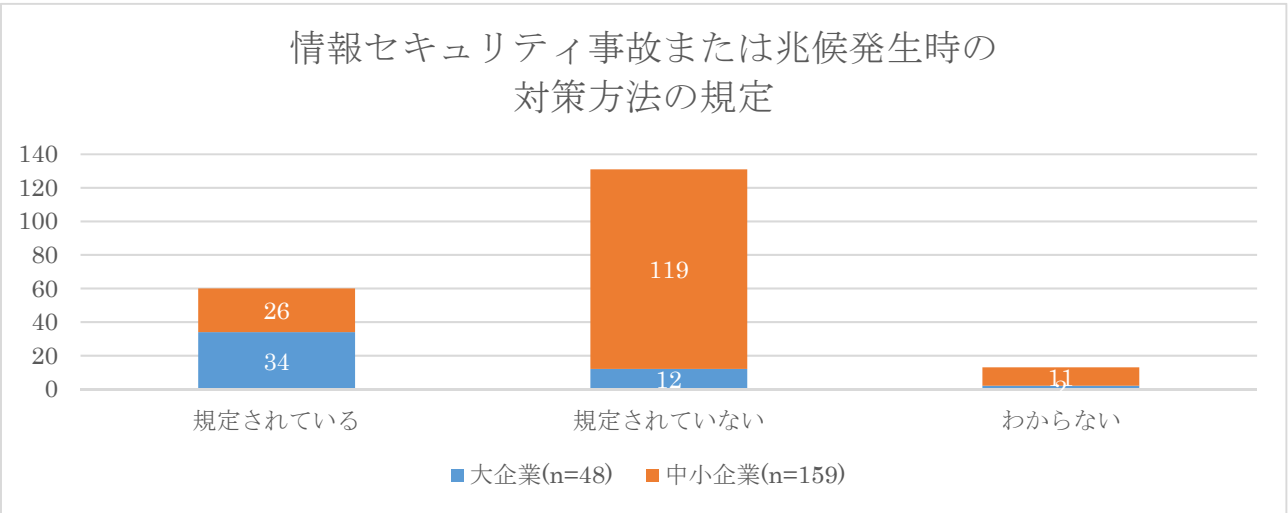


図 52　情報セキュリティ事故または兆候発生時の対策方法の規定状況に関する分布

4.1.22.1. 対策方法の具体的な内容

情報セキュリティ事故や兆候の発生時に「対策が規定されている」企業に対して，具体的にどのような項目が規定されているかを調査した．結果を以下に示す．その他では「親会社への報告」「グループへの報告」が挙げられた．

表 48　情報セキュリティ事故や兆候発生時の具体的な対策方法の分布(複数回答)

分類＼経路	経営者への報告	責任者への報告	原因究明	本人・関係者への連絡	官公庁への報告	再発防止策の規定	世間への発表	その他
中小企業(n=26)	23	23	13	13	3	11	1	2
大企業(n=34)	27	34	24	23	15	25	12	1
全体	50	57	37	36	18	36	13	3

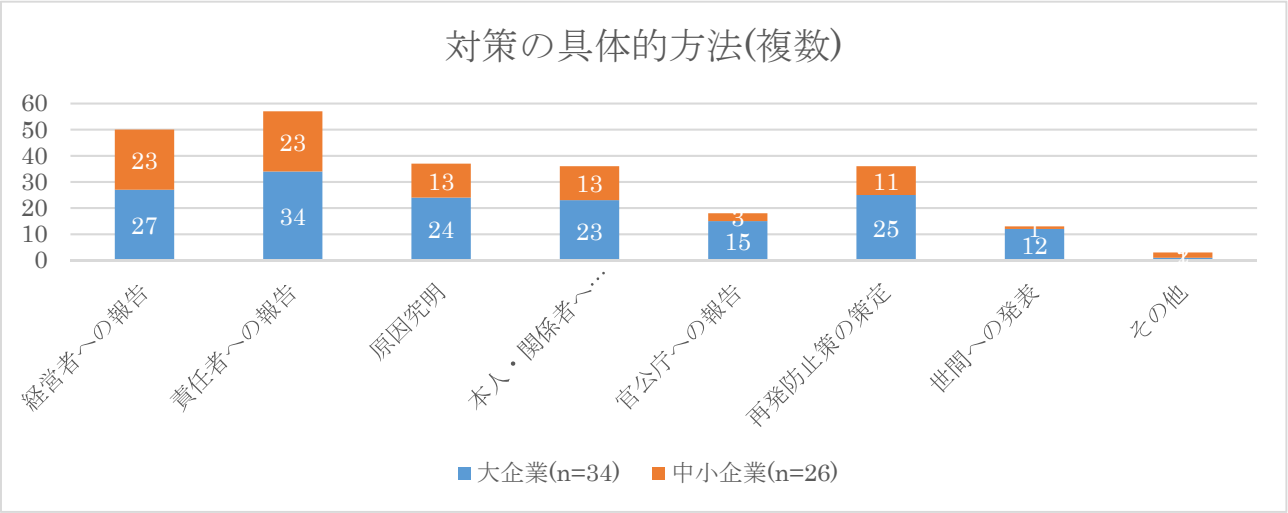


図 53　情報セキュリティ事故や兆候発生時の具体的な対策方法の分布(複数回答)

4.1.23. 情報セキュリティの組織面・運用面での対策

情報セキュリティに関する組織面・運用面での対策を調査した．結果を以下に示す．その他での項目としては，「セキュリティソフトの運用委託」「退勤時の PC の施錠保管」が挙げられた．中小企業および大企業においては，「データのバックアップ」「一般アカウントのルール策定」「書類の施錠管理」が主だった項目として挙げられているが，それ以外の項目で大企業と中小企業において差が出ている部分となっていることがわかる．

表 49　情報セキュリティの組織面・運用面での対策の分布(複数回答)

分類＼対策	事業継続計画の策定	情報セキュリティのリスク分析	一般アカウントのルール策定	フロアや施設の入退室管理	書類の施錠管理	ワイヤーによる機器固定	監視サービスの活用
中小企業(n=160)	11	9	59	18	50	8	19
大企業(n=48)	29	22	42	26	26	16	21
全体	40	31	101	44	76	24	40

分類＼対策	情報セキュリティ監査の実施	重要なシステム・データのバックアップ	情報セキュリティ対策の定期的な見直し	委託先の情報セキュリティの確認	その他	特に実施していない
中小企業(n=160)	8	80	9	8	2	27
大企業(n=48)	20	43	24	13	0	0
全体	28	123	33	21	2	27

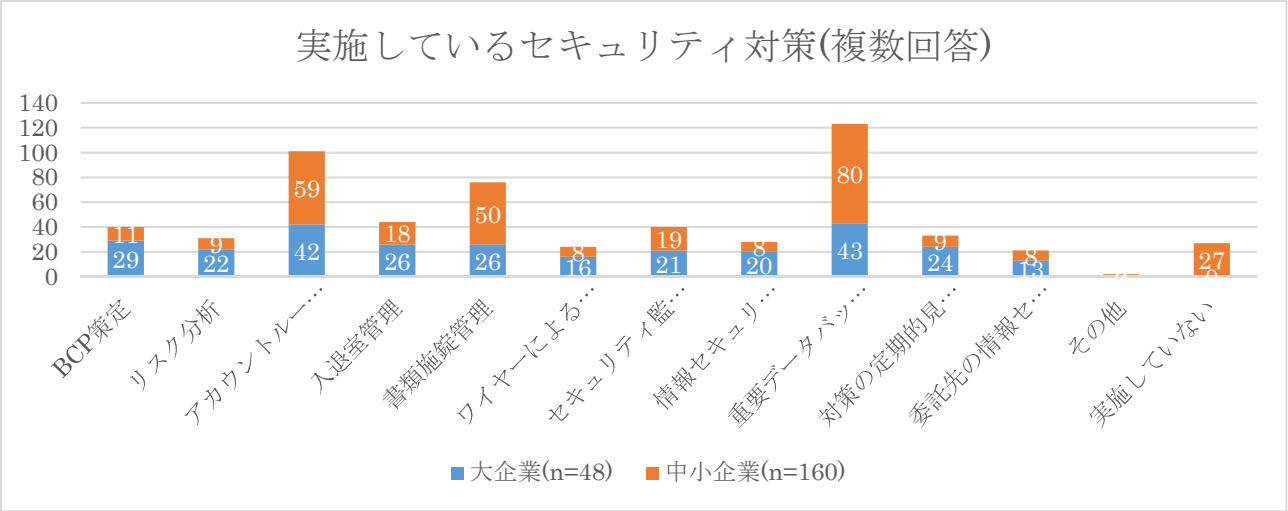


図 54　情報セキュリティの組織面・運用面での対策の分布(複数回答)

4.1.24. 紙媒体の処分方法

紙媒体の処分方法について調査を行った. 結果を以下に示す. なお, 1 社が未回答であった. その他は,「シュレッダーと資源ごみ・裏紙(5 社)」「シュレッダー，そのまま，資源ごみ・裏紙(1 社)」「シュレッダーと焼却処分(1 社)」「シュレッダーと専門業者に依頼(2 社)」「5 年間保存または返す(1 社)」「業者委託(2 社)」「焼却処分(3 社)」「溶解処分(1 社)」「内容に応じてシュレッダー，そのまま，裏紙(1 社)」という回答であった．シュレッダーで処分している企業がほとんどであるが，中小企業では一部裏紙やそのまま処分など，印刷された内容によっては情報漏洩のリスクが生じる状態となっている.

表 50　紙媒体の処分方法の分布

分類＼規定項目	シュレッダー	そのまま処分	資源ごみ・裏紙	その他
中小企業(n=159)	133	5	11	10
大企業(n=48)	41	0	0	7
全体	174	5	11	17

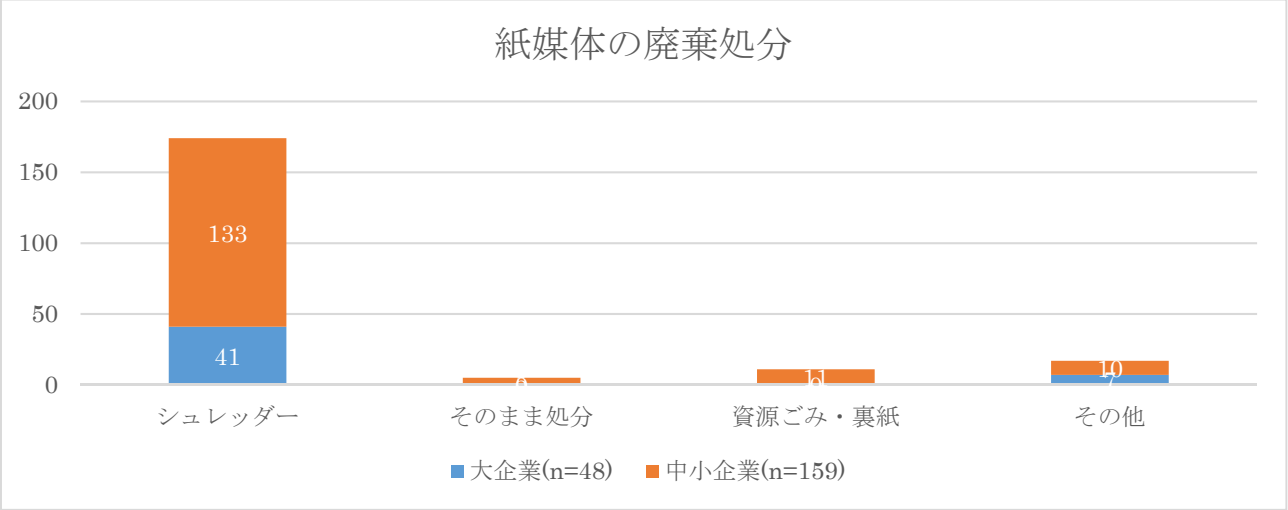


図 55　紙媒体の処分方法の分布

4.1.25. ハードディスク等の廃棄処分

ハードディスク等の記憶媒体の処分方法に関する調査を行った．結果を以下に示す．なお，6 社が未回答であった．その他の項目としては，「業者・外部業者に委託(11 社)」「リース元に返却(2 社)」「データ消去ソフトウェア(5 社)」「磁気消去と 2 点穿孔」「5 年間保存もしくは返す(1 社)」「なし(1 社)」」があった，

表 51　ハードディスク等の廃棄処分方法の分布

分類＼定期性	破砕・溶解	そのまま処分	その他
中小企業(n=154)	110	29	15
大企業(n=48)	40	3	5
全体	150	32	20

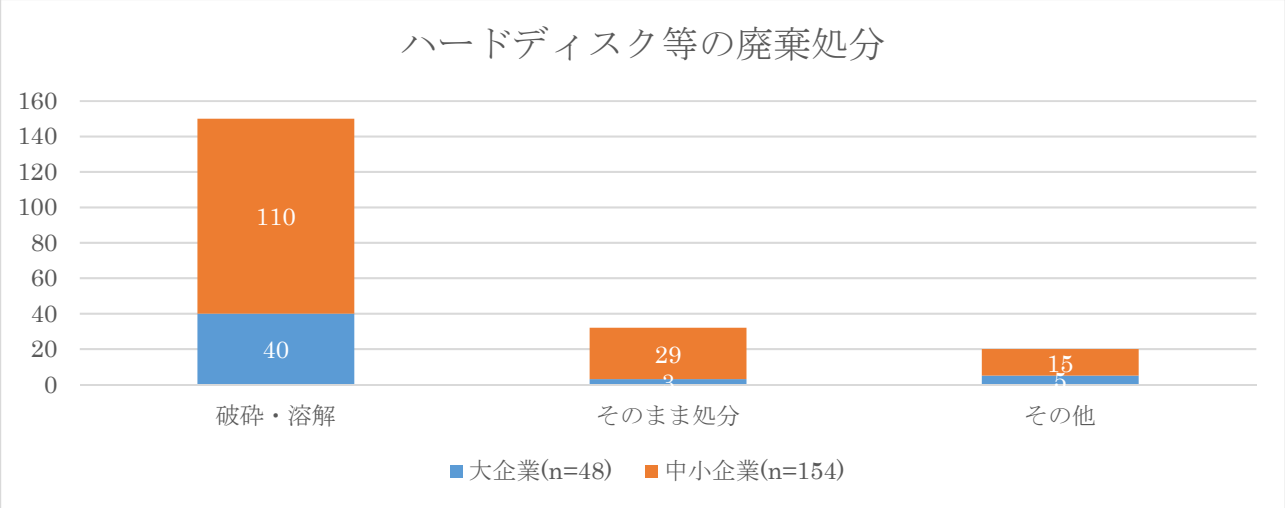


図 56　ハードディスク等の廃棄処分方法の分布

4.1.26. 導入しているセキュリティ製品・サービス

導入している情報セキュリティ製品あるいはサービスに関して調査を行った．結果を以下に示す．ウイルス対策ソフトは約 93%の企業に導入されており浸透しているといえるが，他の製品については，中小企業は大企業に比較して導入が進んでいない．一方で中小企業であれば管理するアカウントや PC 台数は大企業のそれと比較して少なくなると考えられ，こういった製品に対するニーズがそもそもないということが推測される．

表 52　導入しているセキュリティ製品・サービスの分布(複数回答)

分類＼対策	ウイルス対策ソフト・サービス	ウェブ閲覧フィルタリングソフト	ファイアーウォール	VPN	暗号化製品	IT 資産管理	個人認証
中小企業(n=160)	146	21	72	26	11	12	22
大企業(n=48)	47	25	39	34	25	27	21
全体	193	46	111	60	36	39	43

分類＼対策	アイデンティティ管理	セキュリティ情報管理システム	クライアント PC 管理システム	メールフィルタリングソフト	その他	特に導入してない
中小企業(n=160)	3	8	3	17	1	9
大企業(n=48)	14	21	21	17	1	0
全体	17	29	24	34	2	9

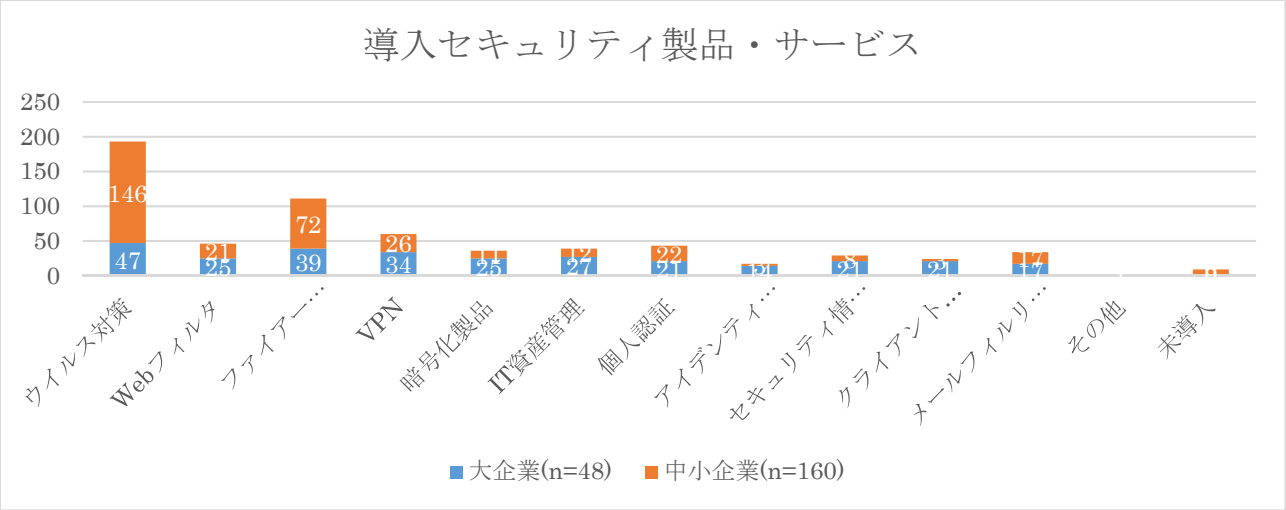


図 57　導入しているセキュリティ製品・サービスの分布(複数回答)

4.1.27. 情報セキュリティの外部委託状況

情報セキュリティの外部委託状況について調査した. 結果を以下に示す. なお, 4 社が未回答であった. 中小企業においては約 50%の企業が外部委託していない現状である.

表 53　情報セキュリティの外部委託状況に関する分布

分類＼委託状況	ほぼすべて委託している	一部委託している	委託していない	わからない
中小企業(n=156)	31	36	79	10
大企業(n=48)	2	25	15	6
全体	33	61	94	16

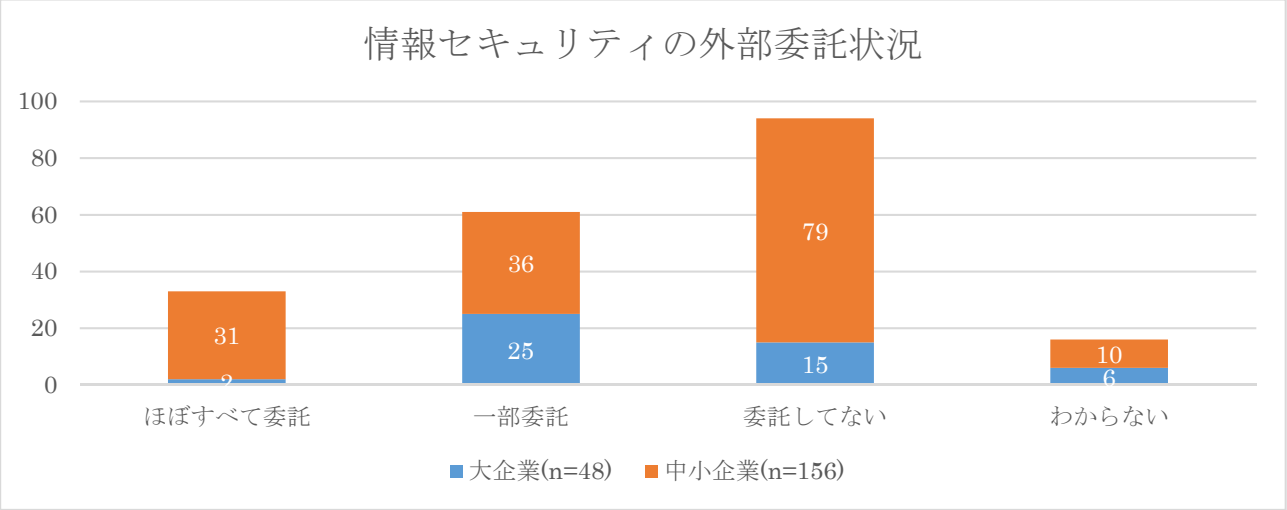


図 58　情報セキュリティの外部委託状況に関する分布

4.1.28. 情報セキュリティ対策の公開状況

各社がとっている情報セキュリティ対策を公開しているかについて調査を行った．結果を以下に示す．なお，3 社が未回答であった．大企業の 50%以上，中小企業の 80%が公開していない．これについては，公開することによるメリットがないことが理由として考えられる．

表 54　情報セキュリティ対策の公開状況に関する分布

分類＼公開状況	HP で公開している	個別に公開する	公開していない	わからない
中小企業(n=157)	3	13	128	13
大企業(n=48)	9	6	26	7
全体	12	19	154	20

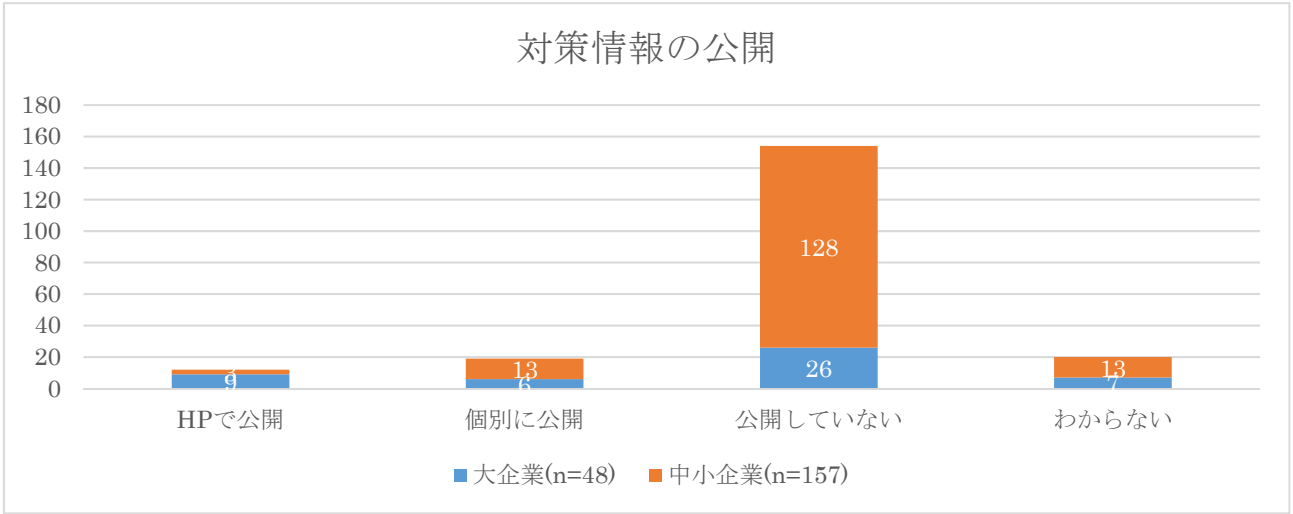


図 59　情報セキュリティ対策の公開状況に関する分布

4.1.29. 情報セキュリティ対策の必要性を感じたきっかけ

企業が情報セキュリティ対策を感じたきっかけについて調査した．結果を以下に示す．その他では「親会社の指示・意向(4 社)」「当然実施すべきもの(2 社)」「コンプライアンス(1 社)」「株主からの要望(1 社)」といった項目が挙げられた．選択肢の中で回答が多いのが「他社のセキュリティ事故」「IT 関連業者・専門家の勧奨」「マイナンバー制度」「法令制定」など，企業外からの働きかけがきっかけとなって対策されることが多いことがわかる．また，中小企業においては対策の必要性を感じない企業も約 16%存在していることがわかる．

表 55　情報セキュリティ対策の必要性を感じたきっかけに関する分布(複数回答)

分類＼対策	法令の制定	業界基準の制定・業界団体の呼びかけ	取引先からの要請	自社社員からの要請	自社のセキュリティ事故	他社のセキュリティ事故(ニュース含む)	取引先へのアピール
中小企業(n=160)	34	11	21	9	8	47	5
大企業(n=48)	18	15	17	5	5	16	7
全体	52	26	38	14	13	63	12
分類＼対策	同業他社の対策状況	マイナンバー制度の開始	セキュリティベンダーからの勧奨	IT 関連業者・専門家の勧奨	重要情報の保持	その他	対策の必要性を感じたことがない
中小企業(n=160)	8	42	8	45	19	3	25
大企業(n=48)	13	17	6	14	17	5	0
全体	21	59	14	59	36	8	25

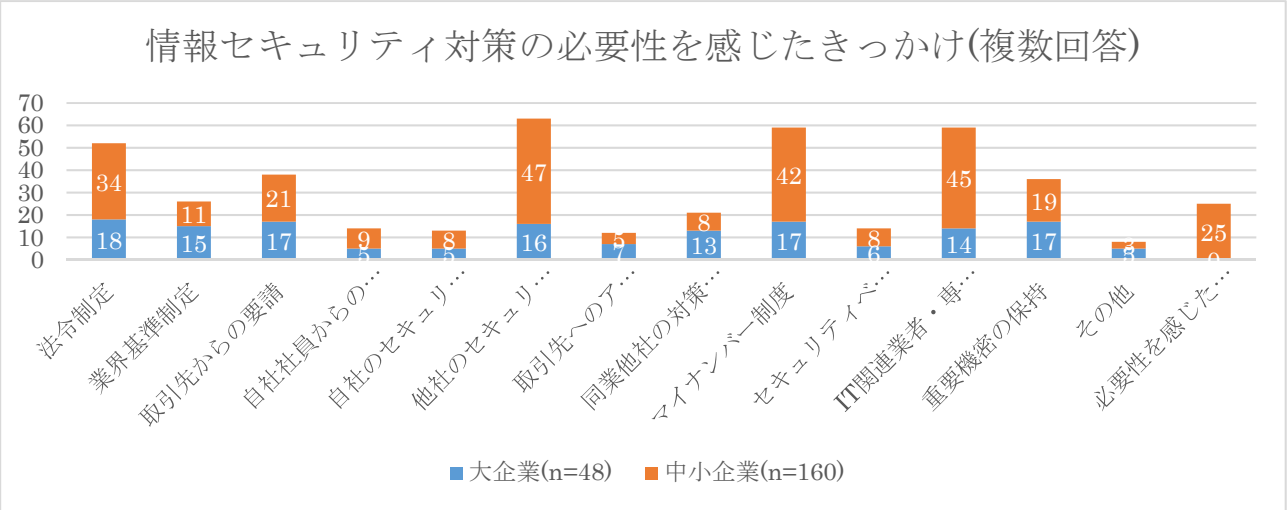


図 60　情報セキュリティ対策の必要性を感じたきっかけに関する分布(複数回答)

4.1.30. 情報セキュリティの脅威度に関する意識

企業の情報セキュリティの認識について調査した．結果を以下に示す．脅威度の認識では，中小企業では「あまり脅威と感じない」と感じる割合が多くなっている．

表 56　中小企業における情報セキュリティの脅威度意識の分布(n=160)

分類＼対策	ウイルス	不正アクセス	DoS攻撃	標的型攻撃	情報漏洩	内部不正	システム機能不全	外部委託先サービス不全
非常に脅威である	80	67	68	79	79	61	97	69
どちらかといえば脅威である	64	78	70	63	60	60	49	56
あまり脅威と感じない	14	14	21	17	19	38	12	31
未回答	2	1	1	1	2	1	2	4

表 57　大企業における情報セキュリティの脅威度意識の分布(n=48)

分類＼対策	ウイルス	不正アクセス	DoS攻撃	標的型攻撃	情報漏洩	内部不正	システム機能不全	外部委託先サービス不全
非常に脅威である	29	30	22	30	31	29	34	27
どちらかといえば脅威である	15	13	18	15	15	17	12	14
あまり脅威と感じない	3	3	7	2	1	1	1	5
未回答	1	2	1	1	1	1	1	2

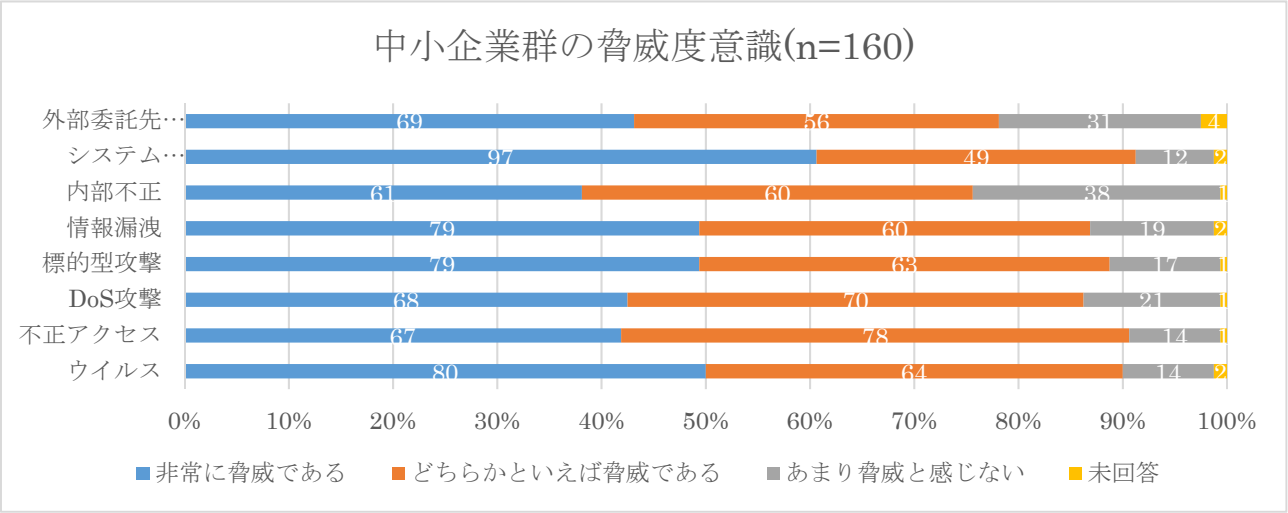


図 61　中小企業における情報セキュリティの脅威度意識の分布(n=160)

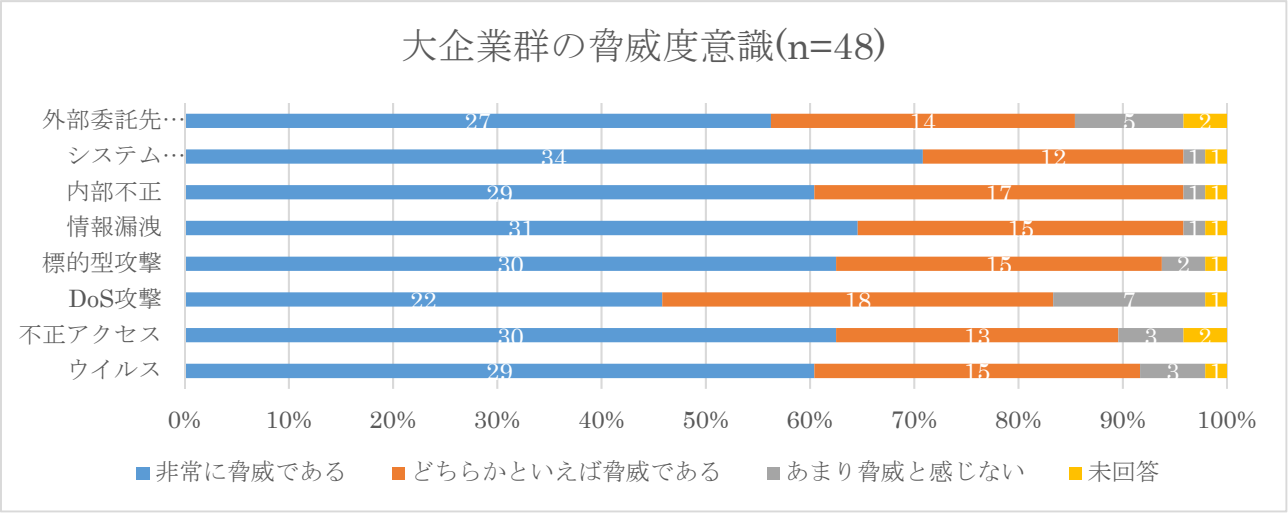


図 62　大企業における情報セキュリティの脅威度意識の分布(n=48)

4.1.31. 情報セキュリティの個別の脅威に対する対策に関する意識

企業の個別の脅威に対する情報セキュリティの対策の認識について調査した．結果を以下に示す．脅威度の対策の認識では，中小企業では「十分と感じない」「十分と感じる」と感じる割合が多くなっており，「どちらかといえば十分である」という割合が少なくなっている．

表 58　中小企業における情報セキュリティの対策意識の分布(n=160)

分類＼対策	ウイルス	不正アクセス	DoS攻撃	標的型攻撃	情報漏洩	内部不正	システム機能不全	外部委託先サービス不全
十分と感じる	18	19	16	14	18	14	13	21
どちらかといえば十分と感じる	88	79	75	82	67	69	77	79
十分と感じない	51	58	65	59	70	73	65	53
未回答	3	4	4	5	5	4	5	7

表 59　大企業における情報セキュリティの対策意識の分布(n=48)

分類＼対策	ウイルス	不正アクセス	DoS攻撃	標的型攻撃	情報漏洩	内部不正	システム機能不全	外部委託先サービス不全
十分と感じる	10	6	6	1	1	1	4	7
どちらかといえば十分と感じる	31	34	36	33	36	34	36	33
十分と感じない	7	8	6	13	11	13	8	8
未回答	0	0	0	1	0	0	0	0

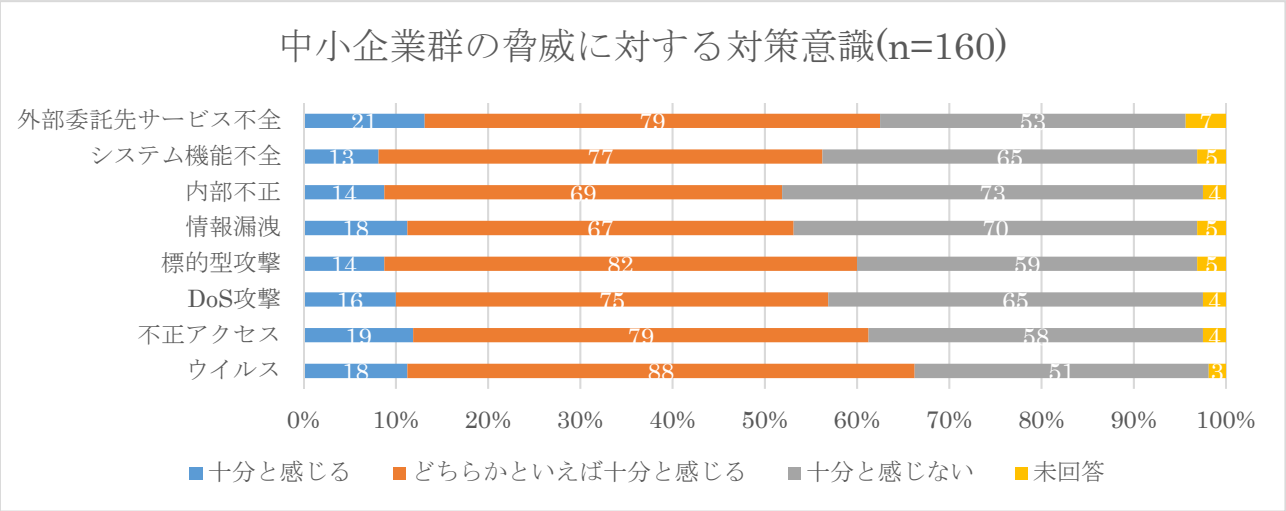


図 63　中小企業における情報セキュリティの脅威度意識の分布(n=160)

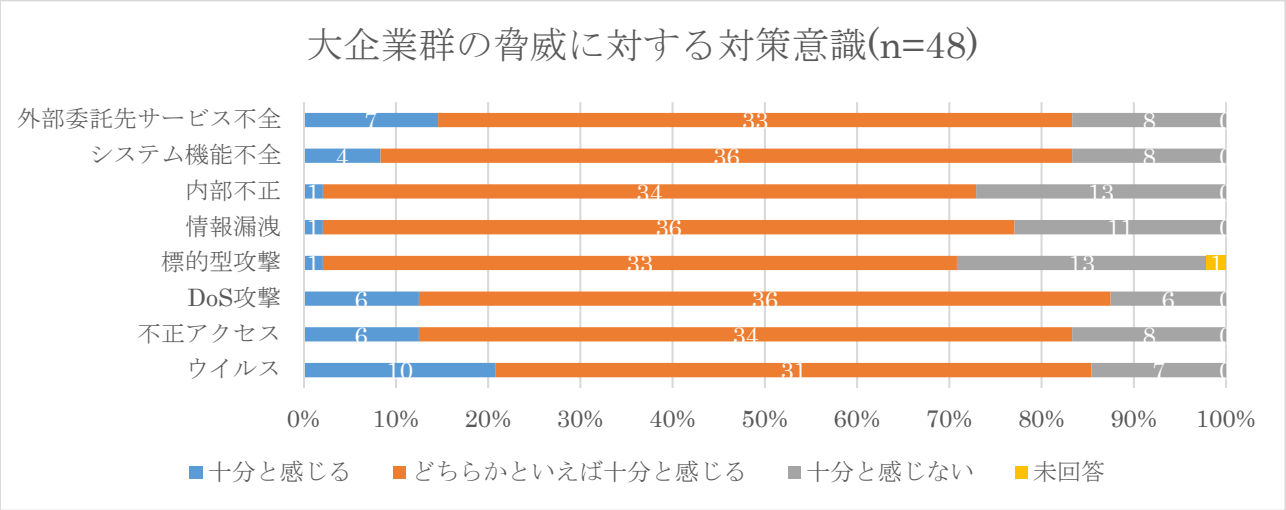


図 64　大企業における情報セキュリティの対策意識の分布(n=48)

4.1.32. 情報セキュリティの対策意識

企業の情報セキュリティの対策が十分か否かの認識について調査した．結果を以下に示す．なお，2 社が未回答であった．脅威度の対策の認識では，中小企業では「そう思う」「まあそう思う」を加えて 50%を切っている状態であり，対策は十分にとられてない認識の企業が大企業群と比較して多いことがわかる．

表 60　情報セキュリティ対策の認識に関する分布

分類＼認識	そう思う	ややそう思う	あまりそう思わない	思わない	わからない
中小企業(n=159)	7	64	53	28	7
大企業(n=47)	3	32	9	2	1
全体	10	96	62	30	8

苫小牧高専協力会・苫小牧商工会議所・苫小牧高専 連携事業
「苫小牧地区における情報セキュリティ意識に関する調査」

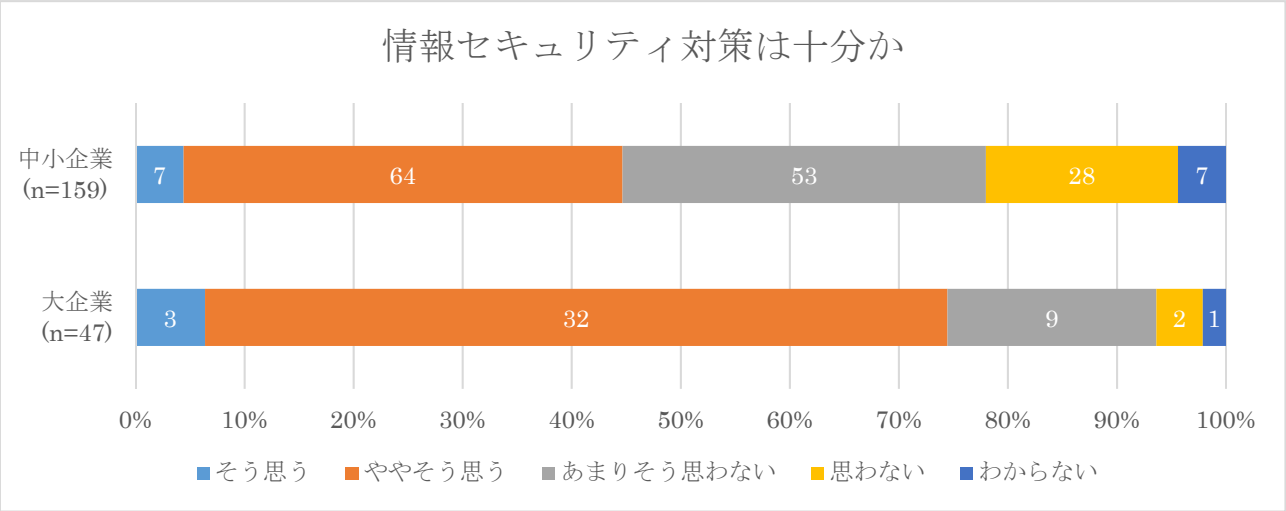


図 65　情報セキュリティ対策の認識に関する分布

4.1.33. 情報セキュリティで具体的に進めたい対策

実際に情報セキュリティの対策をするうえでどのような項目から対策をしたいか，企業に 3 つまで回答していただいた．結果を以下に示す．なお，6 社が未回答であった．また，その他として「バックアップデータの管理方法(1 社)」「PC の他に紙媒体の併用(1 社)」「情報セキュリティ担当者の後継者の育成(1 社)」といった回答があった．上位 4 つでは上から順に「従業員へのセキュリティ意識向上，教育」「企業内の体制整備」「情報セキュリティ対策技術の習得・向上，ツール利用」「経営者へのセキュリティ意識向上，教育」となった．これらの対策は設備投資がほとんど必要ないと考えられ，また日々変化する情報セキュリティとその対策において，教育が重要であることは認識していただいているようである．

表 61　具体的に進めたい情報セキュリティ対策の分布(3 つまで)

分類＼具体的対策	経営者へのセキュリティ意識向上、教育	従業員へのセキュリティ意識向上、教育	市場や顧客からの信頼・評価	企業内の体制整備	情報セキュリティ関連法制度の整備
中小企業(n=155)	47	105	15	74	15
大企業(n=47)	19	40	9	24	2
全体	66	145	24	98	17
分類＼具体的対策	対策支援費等の補助制度の充実	情報セキュリティ対策技術の習得・向上、ツール利用	地域での支援者育成や確保、サポートセンターの充実	その他	特にはない
中小企業(n=155)	9	64	13	3	21
大企業(n=47)	0	25	0	0	2
全体	9	89	13	3	23

苫小牧高専協力会・苫小牧商工会議所・苫小牧高専 連携事業
「苫小牧地区における情報セキュリティ意識に関する調査」

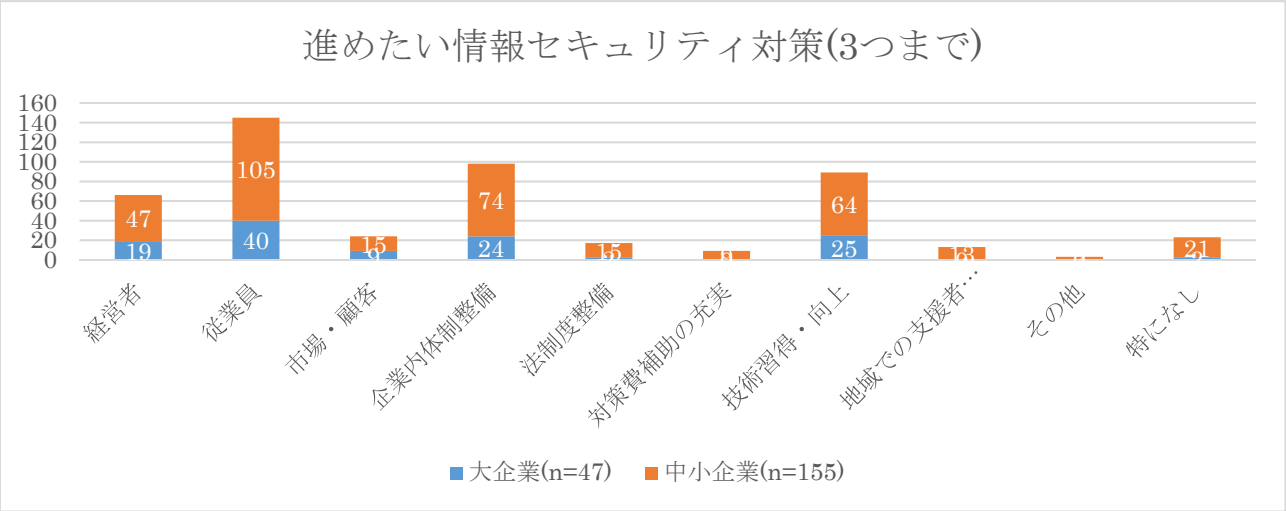


図 66　具体的に進めたい情報セキュリティ対策の分布(3 つまで)

4.2.　今回利用したアンケートについて

本調査に用いたアンケートの質問項目を以下に示す．本調査の元となっているのは IPA「2016 年度 中小企業における情報セキュリティ対策の実態調査票」 [1]である． [1]から変更した質問と選択肢は**太字**で，追加した質問と選択肢は**太字と下線**で示す．

Ⅰ.貴社の企業規模についてお尋ねします
問 1　貴社の主な業務をお答えください。(○は 1 つ)
1. 農業　2. 林業　3. 漁業
4. 鉱業、採石業、砂利採取業　5. 建設業 6. 製造業
7. 電気・ガス・熱供給・水道業 8. 情報通信業　9. 運輸業,郵便業
10. 卸売業 11. 小売業 12. 金融業、保険業
13. 不動産業、物品賃貸業　14. 学術研究、専門・技術サービス業 15. 宿泊業、飲食サービス業
16. 生活関連サービス業、娯楽業 17. 教育、学習支援業 18. 医療、福祉
19. 複合サービス事業 20. その他のサービス業

問 2　貴社の総従業員数をお答えください。(経営者、パート等を含む)(○は 1 つ)
1. 5 名以下　2. 6～20 名　**3. 21～40 名**
4. 41～80 名　**5. 81～120 名**　**6. 121 名以上**

問 3　貴社の資本金について、直近会計年度の金額をお答えください。(○は 1 つ)
1. 500 万円以下　**2. 500 万円超～2000 万円以下**　**3. 2000 万円超～4000 万円以下**
4. 4000 万円超～1 億円以下　**5. 1 億円超**

問 4　貴社の総売上高について、金額をお答えください。(○は 1 つ)
1. 1000 万円以下　**2. 1000 万円超～3000 万円以下**　**3. 3000 万円超～7000 万円以下**
4. 7000 万円超～1 億円以下　**5. 1 億円超～3 億円以下**　**6. 3 億円超**

Ⅱ.貴社の IT(インフォメーション・テクノロジー)導入状況についてお尋ねします
Q1.貴社では IT を十分に活用していると思いますか。一番近いものをお答え下さい。(○は 1 つ)
1. そう思う　2. ややそう思う　3. あまりそう思わない
4. 思わない　5. わからない

Q2.貴社において、業務で PC を利用していますか。利用している場合は、台数をご記入ください。
1. 利用している 約【　　】台　2. 利用していない

Q2-1.Q2 で「1 利用している」と回答した方にお尋ねします。
貴社の下記項目における状況について最も近いものをそれぞれお答えください。

a) 利用している OS(いくつでも)

1. Windows XP　2. Windows 7　3. Windows 8/8.1
4. Windows 10　5. その他 Windows　6. Mac OS
7. その他(具体的に:【 】)
8. わからない

b) Windows アップデート等の PC への更新プログラムの適用(○は 1 つ)

1. 常に適用し、適用状況も把握している
2. 常に適用する方針・設定だが、実際の適用状況は不明
3. 各ユーザに適用を任せている
4. ほとんど適用していない
5. わからない

Q3.貴社において、業務でタブレット端末及びスマートフォンを利用していますか。利用している場合は台数をご記入ください。

1. 利用している 約【　　】台
2. 利用していない

Q3-1.Q3 で「1 利用している」と回答した方にお尋ねします。(以下 Q3-2 も同様)
業務で利用されているスマートフォンやタブレット端末について、実施されている対策をお答えください。(いくつでも)

1. 端末のパスワード設定
2. 紛失・盗難時のデータ消去
3. セキュリティソフトの導入
4. MDM(モバイルデバイス管理ツール)による端末管理
5. 利用ルールの策定
6. その他(具体的に:【　　】)
7. 特に実施していない

Q3-2.業務で利用されているスマートフォンやタブレット端末について、社員の私有端末の業務利用(BYOD: Bring Your Own Device)を認めていますか。(○は 1 つ)

1. 認めている
2. 現在、認めるかどうか検討中
3. 未検討
4. 認める予定はない

Q4.貴社において、業務でサーバを利用していますか。利用している場合は台数をご記入ください。

1. 利用している 約【　　】台
2. 利用していない

Q4-1.Q4 で「1 利用している」と回答した方にお尋ねします。
貴社ではサーバに更新プログラムを適用していますか。最も近いものをお答えください。

a) 外部に公開しているネットワークサーバ(メールサーバ、Web サーバなど)　(○は 1 つ)

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

b) 内部で利用しているネットワークサーバ(ファイルサーバ、プリントサーバなど)　(○は 1 つ)

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

c) 貴社では、サーバの利用について、外部と内部のネットワークを分離していますか。(いくつでも)

1. Web サーバは、それぞれ分離している
2. メールサーバは、それぞれ分離している
3. DNS サーバは、それぞれ分離している
4. Proxy サーバは、それぞれ分離している
5. 外部用と内部用といった分離は特にしていない
6. 外部事業者に運用を委託しているため、分からない

7. 該当するようなサーバを利用していない　　8. わからない

Q4-2.Q4-1-a,b で「4 ほとんど適用していない」と回答した方にお尋ねします。
貴社ではサーバに更新プログラムを適用しない理由として当てはまるものをお答えください。(いくつでも)

1. プログラムの適用が悪影響を及ぼすリスクを避けるため
2. プログラム適用以外の手段が有効であるため
3. プログラムを適用しなくても問題ないと判断したため
4. プログラムの評価や適用に多大なコストがかかるため
5. その他(具体的に:【　　】)

Q5.貴社では IT 分野の投資を過去 3 年の間に行いましたか。(○は 1 つ)

1. 行った　2. 行っていない　　3. わからない

Q5-1.Q5 で「1 行った」と回答した方にお尋ねします。(以下 Q5-2 も同様)(○は 1 つ)
IT 投資額の 3 年間の平均は概算でどのくらいですか。

1. 10 万円以下	**2. 10 万円超～50 万円**	**3. 50 万円超～100 万円**
4. 100 万円超～200 万円	**5. 200 万円超～500 万円**	**6. 500 万円超～1000 万円**
7. 1000 万円超～4000 万円	**8. 4000 万円超**	9. わからない

Q5-2.その IT 投資の中に情報セキュリティ対策は含まれていましたか。(○は 1 つ)

1. 含まれている　2. 含まれていない　　3. わからない

Q5-3.Q5-2 で「1 含まれている」と回答した方にお尋ねします。
情報セキュリティ対策に関する投資額は、概算でどのくらいですか。(○は 1 つ)

1. 10 万円以下	**2. 10 万円超～50 万円**	**3. 50 万円超～100 万円**
4. 100 万円超～200 万円	**5. 200 万円超～500 万円**	**6. 500 万円超～1000 万円**
7. 1000 万円超～4000 万円	**8. 4000 万円超**	9. わからない

Q5-4.Q5-2 で「2 含まれていない」と回答した方にお尋ねします。
含まれていない理由は何ですか。(いくつでも)

1. コストがかかり過ぎる　2. 費用対効果が見えない　3. どこからどう始めたらよいかわからない
4. 導入後の手間がかかる　5. その他(具体的に:【　　】)

Q6.貴社では経営資源の確保や業務の効率化に IT を活用されていますか。
利用・導入されているサービスやシステムを次の項目から選択して下さい。(いくつでも)

1. フリーメール(Gmail など)　2. 顧客管理システム(CRM)
3. Web サイト、ホームページの開設　4. インターネットを活用した流通・決済
5. 会計システム・アプリケーション　6. 人事システム・アプリケーション
7. 給与システム・アプリケーション　8. 出退勤管理システム・アプリケーション
9. 稟議システム　10. 文書管理システム
11. 生産管理システム　12. コミュニケーションツール
13. クラウドストレージ・無料　14. クラウドストレージ・有料
15. クラウドファンディング　16. クラウドソーシング
17. その他　(具体的に:【　　】)
18. 活用していない

Q6-1.Q6 で「3 Web サイト、ホームページの開設」と回答した方にお尋ねします。
Web サイトにおける情報セキュリティ対策で実施している対策をお答えください。(いくつでも)

1. ログやファイル情報に基づく改ざん検知　2. 定期的な Web コンテンツ診断
3. Web サイト管理者権限アカウントの管理ルール策定

Q7.貴社はサイバー保険や情報漏えい賠償責任保険に加入されていますか。
a) サイバー保険 (○は 1 つ)

1. 加入している　2. 検討しているが加入していない
3. 内容を知っているが加入する予定がない　4. 内容を知らないし加入していない
5. 加入しているかどうかわからない

b) 情報漏えい賠償責任保険（○は１つ）

1. 加入している　　2. 検討しているが加入していない
3. 内容を知っているが加入する予定がない　　4. 内容を知らないし加入していない
5. 加入しているかどうかわからない

Ⅲ.貴社の情報セキュリティ被害についてお尋ねします

Q8.貴社ではこれまでにコンピュータウイルスに感染したことがありましたか。一度でもあればお答えください。(○は１つ)

1. ウイルスに感染した　　2. ウイルスを発見したが、感染には至らなかった
3. ウイルスを全く発見しなかった・感染していない　　4. わからない

Q8-1.Q8 で「1 ウイルスに感染した」もしくは「2 ウイルスを発見したが、感染には至らなかった」と回答した方にお尋ねします。
感染あるいは発見したウイルスの侵入経路はどのように想定されますか。(いくつでも)

1. 電子メール　　2. インターネット接続
3. ダウンロードしたファイル　　4. P2P(Peer to Peer)等ファイル共有ソフト
5. USB メモリ等の外部記憶媒体　6. 持ち込みパソコン
7. その他(具体的に:【　　】)
8. わからない

Q8-2.Q8 で「1 ウイルスに感染した」と回答した方にお尋ねします。
ウイルスに感染した影響で生じた被害として当てはまるものをお答えください。(いくつでも)

1. データの破壊　　2. 情報の漏えい
3. ウイルスメール等の発信　　4. ネットワークの遅延
5. システム停止・性能低下　　6. パソコン単体の停止
7. 関連部門の業務停滞　　8. 個人の業務停滞
9. 取引先への感染拡大　　10. その他(具体的に:【　　】)
11. 特になし

Q9.貴社では**これまでに**内部者の不正による情報セキュリティ上のトラブルはありましたか。一度でもあればお答えください。(○は１つ)

1. 内部者の不正による被害があった　　2. 委託者の不正による被害があった
3. 不正による被害はなかった　　4. わからない

Q10.貴社ではこれまでに自社のサーバやパソコンがサイバー攻撃にあったことがありますか。一度でもあればお答えください。(○は１つ)

※主なサイバー攻撃・・・DoS 攻撃(大量もしくは不正なデータでシステムを機能不全に追い込む攻撃)
不正アクセス(他者の ID の利用や脆弱性を利用したアクセス)
標的型攻撃(受信者に関連のある話題のメールにウイルスなどを添付する攻撃)

1. サイバー攻撃で被害にあった　　2. サイバー攻撃を受けたが、被害には至らなかった
3. サイバー攻撃を全く受けなかった　　4. わからない

Q10-1.Q10 で「1 サイバー攻撃で被害にあった」もしくは「2 サイバー攻撃を受けたが、被害には至らなかった」と回答した方にお尋ねします。
貴社が受けたサイバー攻撃の手口に当てはまるものをお答えください。(いくつでも)

1. ID・パスワードを騙し取られてなりすまされたことによる不正アクセス
2. 脆弱性(更新プログラム等の未適用)を突かれたことによる不正アクセス
3. SQL インジェクション(Web サイトの入力欄に特別な記号文字を埋め込み、データベースを不正に操作する)
4. DoS 攻撃　　5. 標的型攻撃
6. ランサムウェア(PC をロックしたり、ファイルを暗号化し、解除に身代金を要求するウイルス)
7. その他(具体的に:【　　】)
8. 手口はわからない

苫小牧高専協力会・苫小牧商工会議所・苫小牧高専 連携事業
「苫小牧地区における情報セキュリティ意識に関する調査」

Q10-2.Q10 で「1 サイバー攻撃で被害にあった」と回答した方にお尋ねします。
a)貴社が受けたサイバー攻撃の被害として当てはまるものをお答えください。(いくつでも)

1. 貴社の Web サイトが改ざんされた
2. 貴社の Web サイトのサービス停止、または機能が低下させられた
3. 業務サーバの内容が改ざんされた
4. 業務サーバのサービス停止、または機能が低下させられた
5. 貴社が提供するネットサービスにおいて、第三者のなりすましによる不正使用があった
6. 取引先の企業や個人に被害が拡大した
7. 情報が盗まれた
8. その他(具体的に:【 】)

b)復旧にどれくらいの期間を要しましたか。(○は 1 つ)

1. 1 日以下　2. 2～3 日以内
3. 1 週間以内　4. 1～2 週間以内
5. 1 ヶ月以内　6. 1 ヶ月以上

c)被害を金額に換算すると、どれくらいになりますか。(発生、復旧・弁済まで)(○は 1 つ)

1. 10 万円以下　2. 10 万円超～50 万円　3. 50 万円超～100 万円
4. 100 万円超～200 万円　5. 200 万円超～500 万円　6. 500 万円超～1000 万円
7. 1000 万円超～4000 万円　8. 4000 万円超　9. わからない

Ⅳ.貴社の情報セキュリティに関する意識状況についてお尋ねします
Q11.貴社の下記項目における状況について、それぞれお答えください。

a) 社員の不正により営業上の秘密や個人情報等の情報漏えいが発生する可能性はあると思いますか。(○は 1 つ)

1. そう思う　2. ややそう思う　3. あまりそう思わない
4. 思わない　5. わからない

b) 外部からサイバー攻撃を受け、情報漏えいが発生する可能性はあると思いますか。(○は 1 つ)

1. そう思う　2. ややそう思う　3. あまりそう思わない
4. 思わない　5. わからない

c) 貴社の情報セキュリティへの理解度は高いと思いますか。(○は 1 つ)

1. そう思う　2. ややそう思う　3. あまりそう思わない
4. 思わない　5. わからない

Q12.貴社の情報セキュリティ対策はどのような体制で行われていますか。(○は 1 つ)

1. 専門部署(担当者)がある　2. 兼務だが担当者が任命されている
3. 組織的には行っていない(各自の対応)　4. わからない

Q13.情報セキュリティに関して困ったことがあった際にどこに相談しますか。(いくつでも)

1. 社内の担当者　2. IT 関連業者
3. 中小企業診断士　4. IT コーディネータ
5. 商工団体　**6. 公的機関**
7. その他(具体的に:【 】)
8. 特にない

Q14.貴社の情報セキュリティに関する情報収集先を教えてください。(いくつでも)

1. 社内の担当者　2. IT 関連業者
3. 中小企業診断士　4. IT コーディネータ
5. 商工団体　**6. 公的機関**
7. 雑誌・新聞　8. テレビ
9. インターネット　10. 無料のセミナー・実務研修
11. 有料のセミナー・実務研修　12. その他(具体的に:【 】)
13. 特にない

Q15.貴社では従業員に対する情報セキュリティ教育はどのようにされていますか。(いくつでも)

1. 関連情報の周知(社内メール・掲示板など)　2. e ラーニング(ネットを用いた学習)
3. 外部講習会やセミナーの聴講　**4. 外部講師の招聘**
5. 社内の研修や勉強会　6. 特に実施していない

Q15-1.Q15 で「5 社内の研修や勉強会」と回答した方にお尋ねします。
社内の研修や勉強会はどの程度の期間ごとに行っていますか。(○は１つ)

1. 定期的(具体的に:【　　】)　2. 不定期に行っている　3. わからない

Q16.社内の情報セキュリティに関するルールや規定は文章化されていますか。(○は１つ)

1. 文章化されている　2. 文章化されていない　3. わからない

Q16-1.Q16 で「1 文章化されている」と回答した方にお尋ねします。
文章化されている規定は何ですか。該当するものを下記よりお選びください。(いくつでも)

1. 基本的なルール　2. 責任者の任命
3. 各従業員または部署の権限や役割　4. 情報資産の識別、重要度の分類
5. 機器等の利用制限、破損、紛失に関する項目
6. 著作権侵害について
7. その他(具体的に:【　　】)
8. 特にない

Q17.社内の情報セキュリティに関するルールから逸脱した場合の措置について、就業規則等で規定されていますか。(○は１つ)

1. 規定されている　2. 規定されていない　3. 規定されているかわからない
4. そもそも就業規則はない

Q18.貴社において、情報漏えい等の事故またはその兆候を発見した場合、対策方法は規定されていますか。(○は１つ)

1. 規定されている　2. 規定されていない　3. 規定されているかわからない

Q18-1.Q18 で「1 規定されている」と回答した方にお尋ねします。
情報漏えい等の事故またはその兆候を発見した場合の対応方法として規定されているものは何ですか。
該当するものを下記より全てお選びください。(いくつでも)

1. 経営者への報告　2. 責任者への報告
3. 原因究明　4. 本人、関係者への連絡
5. 官公庁への報告　6. 再発防止策の策定
7. 世間への発表　8. その他(具体的に:【　　】)

Q19.貴社での情報セキュリティ対策として実施している組織面・運用面の対策をお答えください。(いくつでも)

1. 事業継続計画(BCP)の策定　2. 情報セキュリティに関するリスク分析
3. 一般ユーザアカウントのルール策定(パスワード設定、インストール制限、アクセス制御等)
4. フロアや施設の入退室管理　5. 書類の施錠管理
6. セキュリティワイヤーによる機器の固定　7. セキュリティ監視サービスの活用
8. 情報セキュリティ監査の実施　9. 重要なシステム・データのバックアップ
10. 情報セキュリティ対策の定期的な見直し　11. 委託先の情報セキュリティの確認
12. その他(具体的に:【　　】)
13. 特に実施していない

Q20.社内の情報の廃棄処分についてそれぞれお答えください。

a) 紙媒体の廃棄処分 (○は１つ)

1. シュレッダーにかけて廃棄　2. そのまま処分　3. 資源ゴミまたは裏紙として利用
4. その他(具体的に:【　　】)

b) ハードディスク等の廃棄処分 (○は１つ)

1. 破砕・溶解する　2. そのまま処分
3. その他(具体的に:【　　】)

苫小牧高専協力会・苫小牧商工会議所・苫小牧高専 連携事業
「苫小牧地区における情報セキュリティ意識に関する調査」

Q21.貴社では情報セキュリティ関連製品やサービスを導入していますか。導入しているものをお答えください。(いくつでも)

1. ウイルス対策ソフト・サービスの導入　2. ウェブ閲覧のフィルタリングソフトウェア
3. ファイアウォール　4. VPN(安全なデータ通信の仕組み)
5. 暗号化製品(ディスク、ファイル、メール等)　6. ソフトウェアライセンス管理/IT 資産管理製品
7. ワンタイムパスワード、IC カード、USB キー、生体認証等による個人認証
8. アイデンティティ管理/ログオン管理/アクセス許可製品(SSO を含む)
9. セキュリティ情報管理システム製品(ログの統合・管理などセキュリティ情報の総合的な管理システム)
10. クライアント PC の設定・動作の管理システム製品
11. メールフィルタリングソフトウェア
12. その他(具体的に:【　】)
13. 特に導入していない

Q22.情報セキュリティの外部委託の状況についてお答えください。(○は 1 つ)

1. ほぼ全て委託している　2. 一部委託している
3. 委託していない　4. わからない

Q23.情報セキュリティ対策の実施内容は外部に公開していますか。(○は 1 つ)

1. ホームページで公開している　2. 取引先の要望があれば個別に公開している
3. 公開していない　4. わからない

Q24.情報セキュリティ対策の必要性を感じたきっかけは何ですか。下記より全てお選びください。(いくつでも)

1. 法令の制定　2. 業界基準の制定、業界団体の呼びかけ
3. 取引先からの要請　4. 自社社員からの要請
5. 自社のセキュリティ事故　6. 他社のセキュリティ事故(ニュース含む)
7. 取引先等へのアピール　8. 同業他社の対策状況
9. マイナンバー制度の開始　10. セキュリティベンダーからの勧奨
11. IT 関連業者・専門家の勧奨　12. 重要情報の保持
13. その他(具体的に:【　】)
14. 対策の必要性を感じたことがない

Q25.以下の情報セキュリティに関する事象の脅威度はどの程度ですか。

a) コンピュータウイルス(悪意のあるプログラム) (○は 1 つ)
1. 非常に脅威である　2. どちらかといえば脅威である　3. あまり脅威ではない

b) 不正アクセス(他者の ID の利用や脆弱性を利用したアクセス) (○は 1 つ)
1. 非常に脅威である　2. どちらかといえば脅威である　3. あまり脅威ではない

c) DoS 攻撃(大量のデータや不正なデータでシステムを機能不全に追い込む攻撃) (○は 1 つ)
1. 非常に脅威である　2. どちらかといえば脅威である　3. あまり脅威ではない

d) 標的型攻撃(受信者に関連のある話題のメールにウイルスなどを添付する攻撃) (○は 1 つ)
1. 非常に脅威である　2. どちらかといえば脅威である　3. あまり脅威ではない

e) 情報漏えい(内部の情報が外に漏れてしまうこと) (○は 1 つ)
1. 非常に脅威である　2. どちらかといえば脅威である　3. あまり脅威ではない

f) 内部不正(組織内部者によって不正に情報が持ち出されること) (○は 1 つ)
1. 非常に脅威である　2. どちらかといえば脅威である　3. あまり脅威ではない

g) システム機能不全(社内のシステムが正常に動作しなくなること) (○は 1 つ)
1. 非常に脅威である　2. どちらかといえば脅威である　3. あまり脅威ではない

h) 外部委託先のサービス停止(外部のサーバなどが停止し、業務に支障をきたすこと) (○は 1 つ)
1. 非常に脅威である　2. どちらかといえば脅威である　3. あまり脅威ではない

Q26.前問の脅威に対して対策は十分だと感じますか。

a) コンピュータウイルス（○は１つ）
1. 十分と感じる　2. どちらかといえば十分と感じる　3. 十分と感じない

b) 不正アクセス（○は１つ）
1. 十分と感じる　2. どちらかといえば十分と感じる　3. 十分と感じない

c) DoS 攻撃（○は１つ）
1. 十分と感じる　2. どちらかといえば十分と感じる　3. 十分と感じない

d) 標的型攻撃（○は１つ）
1. 十分と感じる　2. どちらかといえば十分と感じる　3. 十分と感じない

e) 情報漏えい（○は１つ）
1. 十分と感じる　2. どちらかといえば十分と感じる　3. 十分と感じない

f) 内部不正（○は１つ）
1. 十分と感じる　2. どちらかといえば十分と感じる　3. 十分と感じない

g) システム機能不全（○は１つ）
1. 十分と感じる　2. どちらかといえば十分と感じる　3. 十分と感じない

h) 外部委託先のサービス停止（○は１つ）
1. 十分と感じる　2. どちらかといえば十分と感じる　3. 十分と感じない

Q27.貴社の情報セキュリティ対策は十分だと思いますか。(○は１つ)
1. そう思う　2. ややそう思う　3. あまりそう思わない
4. 思わない　5. わからない

Q28.貴社は今後どのような対策を進めていこうと思いますか。優先度の高いもの 3 つお選びください。(3 つまで)

1. 経営者へのセキュリティ意識向上、教育　**2. 従業員へのセキュリティ意識向上、教育**
3. 市場や顧客からの信頼・評価　4. 企業内の体制整備
5. 情報セキュリティ関連法制度の整備　6. 対策支援費等の補助制度の充実
7. 情報セキュリティ対策技術の習得・向上、ツール利用
8. 地域での支援者育成や確保、サポートセンターの充実
9. その他(具体的に:【　】)
10. 特にはない

苫小牧高専協力会・苫小牧商工会議所・苫小牧高専 連携事業
「苫小牧地区における情報セキュリティ意識に関する調査」

謝辞

まず，ご多忙の業務の中，また 2018 年 9 月 6 日に発生した胆振東部地震からの復旧の最中に貴重なお時間を割いていただいて学生の卒業研究に協力していただいた企業のご担当者の皆様に感謝申し上げます．また，苫小牧商工会議所ならびに苫小牧高専協力会には会員企業へのアンケートの依頼をご快諾いただきまして厚く御礼申し上げます．

本調査にあたっては，[1]に示す IPA のアンケートを元に，調査項目を地域の実情に合わせて調整したものとなっております．この場を借りて感謝の意を表します．

また，高専セキュリティ人材育成事業(K-SEC)からはアンケートにかかる費用の支出をしていただきました．この場を借りて感謝の意を表します．

最後に，本アンケートの実施にあたり，卒業研究の一環として調査項目の設定やアンケート結果の集計に多大なる労力を割いていただいた苫小牧高専 情報工学科(当時)の学生，アンケートに際してアドバイスやお手伝いをいただきました北海道警察サイバーセキュリティ対策本部の皆様に感謝の意を表します．

参考文献

[1] 独立行政法人情報処理推進機構(IPA), 2016 年度 中小企業における情報セキュリティ対策に関する実態調査, 2017. https://www.ipa.go.jp/security/fy28/reports/sme/index.html

[2] 大阪商工会議所, “中小企業におけるサイバー攻撃対策に関するアンケート調査結果（大阪府内）,” 2017. http://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/Iken_Youbou/k290630cyb_ank.pdf

[3] 中小企業庁, “中小企業・小規模企業者の定義,” http://www.chusho.meti.go.jp/soshiki/teigi.html

[4] Microsoft, “OS にはサポート期限があります!,” https://www.microsoft.com/ja-jp/atlife/article-windows10-portal-eos.aspx

[5] 独立行政法人情報処理推進機構(IPA), 中小企業の情報セキュリティ対策ガイドライン 第3版, 2019. https://www.ipa.go.jp/files/000055520.pdf