「不正アクセス行為対策の実態調査」

報告書

平成14年3月

警察庁生活安全局
生活安全企画課

●目　次

◆はじめに

◆調査概要　1

◆調査結果

1．回答者プロフィール　3

2．情報設備等の環境　7

3．インターネットへの接続状況　17

4．外部からの情報システムへのアクセス環境　21

5．情報システムへの被害　26

6．情報システムにおける被害対策　28

7．不正アクセス等の被害状況　30

8．セキュリティ対策状況　39

9．情報セキュリティ教育の取り組み　50

10．アクセスログの取得状況　54

11．不正アクセス等の検知対策について　57

12．具体的な攻撃に対する情報セキュリティ対策　59

13．セキュリティサービス業者の利用状況　65

14．情報システム関連重要施設への入退室管理　68

15．情報セキュリティ対策のための情報入手先　70

16．情報セキュリティ対策を実施する上での問題点　73

添付1）　セキュリティ関連用語集
添付2）　調査票

●はじめに

平成13年に入り、5年以内に世界最先端のIT国家をめざすe-Japan戦略の具体的な推進が始まった。その基本となる施策の一つとして、世界最高水準の高度情報通信ネットワークの形成がある。誰もが、いつでも、どこでも簡単に情報を利用できる「ユビキタス」時代のネットワークインフラとして、高速・大容量通信を可能とするブロードバンドネットワークが期待されている。

特に、低価格の固定料金化でインターネットの常時接続利用を可能とする非対称デジタル加入者伝送方式(ADSL等)は、多くの利用者に高い支持を得て急速に普及を広げている。また、手軽に利用できる携帯電話のiモードを含むモバイル機器によるインターネット利用者も急増した。総務省の統計によると、我が国のインターネット人口も平成12年末で4,700万人(世界で5億人)を超え、いよいよ高度情報化社会がダイナミックに動き出したと言える。

一方、Code RedやNimda等の新しい強力なコンピュータウイルスが猛威を振るい、IIS(Internet Information Server)の脆弱性によるWebサイトのホームページ改ざん被害等、多くの事件が発生している。平成13年中のハイテク犯罪の検挙件数は810件で、その中での不正アクセス禁止法違反の検挙件数が35件、警察に寄せられたハイテク犯罪に関する相談受理件数は17,277件にのぼっている。これら背景の下、情報セキュリティ問題に適切な対応を行い、より安全で信頼できる高度情報化社会を実現することがますます重要な課題となってきている。

このような状況のもと、警察庁では昨年度に引き続き「アクセス制御機能の技術開発の状況に関する調査」、「不正アクセス対策の実態調査」の2つのテーマとしたアンケート調査を実施し、それらの進展の状況を検証する事となった。
特に、本年度調査では、調査対象範囲及びサンプル数を拡大し、出来るだけ多くの情報を収集することで、より客観的、より総合的な視点からの状況分析を可能にするとともに、簡単な技術的解説等を加えることにより、判り易い報告書としてまとめることに努めた。少しでも多くの方々に情報セキュリティへの対応の啓発材料になることを期待したい。

平成14年3月
警察庁生活安全局
生活安全企画課

◆調査概要

●調査概要

(1) 調査目的

警察庁では昨年2月に施行された「不正アクセス禁止法」をはじめとして、インターネット上での犯罪防止に力を入れている。
そこで、今現在ネット上での不正アクセスに関する状況を把握し、警察庁のホームページなどを通して情報セキュリティに関する啓発及び知識の普及を行うことを目的とした。

(2) 調査対象

	発送(件)	有効回収(件)	回収率(%)
全体	1529	631	41.3%
大学	109	55	50.5%
役所 (県庁、政令指定都市、市役所、特殊法人)	160	55	34.4%
企業	1260	514	40.8%
(特定事業者)	504	212	42.1%
不明(業種無回答の為)	-	7	-

※特定事業者とは、企業の中の業種、「エネルギー、交通、金融、情報通信、医療」を抜き出したもの。

(3) 調査方法

郵送調査

(4) 調査期間

２００２年　3月

(5) 調査項目

①回答者プロフィール
②情報設備等の環境
③インターネットへの接続状況
④外部からの情報システムへのアクセス環境
⑤情報システムへの被害
⑥情報システムにおける被害対策
⑦不正アクセス等の被害状況
⑧セキュリティ対策状況
⑨情報セキュリティ教育の取り組み
⑩アクセスログの取得状況
⑪不正アクセス等の検知対策について
⑫具体的な攻撃に対する情報セキュリティ対策
⑬セキュリティサービス業者の利用状況
⑭情報システム関連重要施設への入退室管理
⑮情報セキュリティ対策のための情報入手先
⑯情報セキュリティ対策を実施する上での問題点

●調査結果の掲載について

本報告書における調査結果を下記に従って掲載している。

調査項目タイトル：
・調査票の「問n」に対応

調査項目内でのサブタイトル：
・問nの内での(i)に対応
・(MA)と付記されているものは複数選択式の調査項目

コメント欄：

グラフ表示：
下記の3タイプのグラフでデータを表示している。
例は【縦棒＆折れ線】

①【縦棒＆折れ線】
棒：大学/役所/企業別
折れ線：全体での表示

②【100%積み上げ横棒】
全体/大学/役所/企業別

③【ドーナツグラフ】
使用している所で注釈

データ項目欄：

全体データ：

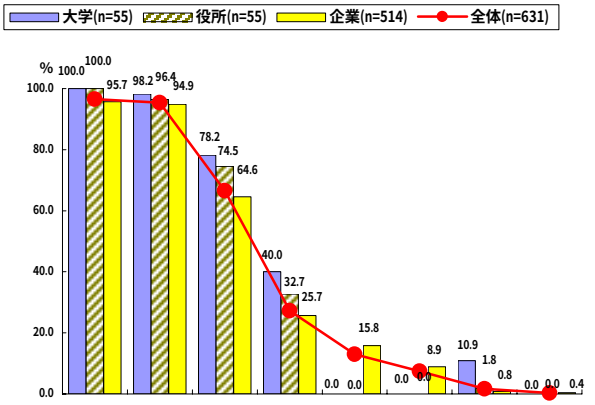
業種分類別データ：

3．インターネットへの接続状況（2／4）

(2)インターネットの接続目的(MA) (n =631)

●利用目的として「各種情報収集」「電子メール」との回答が95%以上となっている。

●「顧客や外部に向けての情報提供」での利用の割合は66.6%であったが、昨年度調査の55.6%を大幅に上回った。また役所での「社内（構内）拠点間を結ぶ業務用」の割合も32.7%と、昨年度調査の7.2%を大幅に上回った。



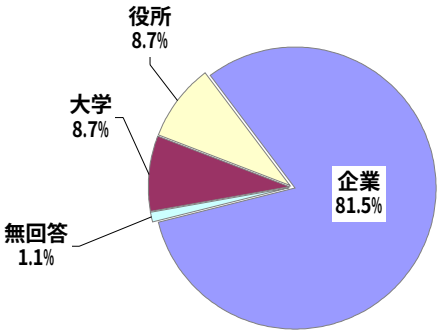
		n	各種の情報収集	電子メール	顧客や外部に向けての情報提供	社内（校内）拠点間を結ぶ業務用	インターネット販売	オンライントレーディング、バンキング、	その他	無回答
全体		631	96.5	95.4	66.6	27.3	13.0	7.4	1.7	0.3
大 学		55	100.0	98.2	78.2	40.0	-	-	10.9	-
役 所		55	100.0	96.4	74.5	32.7	-	-	1.8	-
企業業種別	運輸	10	100.0	100.0	70.0	50.0	30.0	10.0	-	-
	製造	167	98.8	96.4	65.9	25.1	15.0	5.4	1.2	-
	サービス	97	96.9	95.9	63.9	33.0	27.8	6.2	-	-
	不動産	25	100.0	96.0	80.0	36.0	12.0	-	4.0	-
	エネルギー	33	90.9	97.0	54.5	24.2	6.1	6.1	-	-
	交通	23	82.6	91.3	69.6	8.7	39.1	8.7	-	-
	金融	74	93.2	90.5	71.6	18.9	8.1	33.8	-	1.4
	情報通信	43	93.0	95.3	60.5	25.6	14.0	2.3	-	-
	医療	39	94.9	92.3	46.2	20.5	-	-	2.6	2.6

◆調査結果

１．回答者プロフィール（１／４）

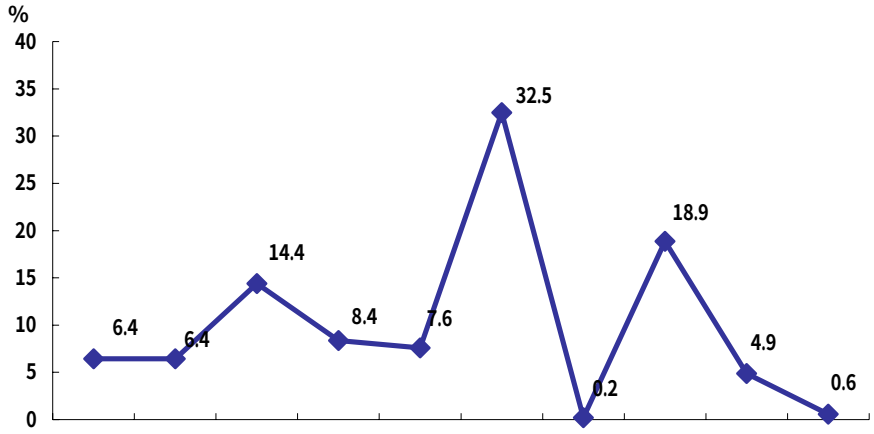
(1) 業種について

(ア) 大学/役所/企業 (n=631)



	n	大学	役所	企業	無回答
全体	631	8.7	8.7	81.5	1.1

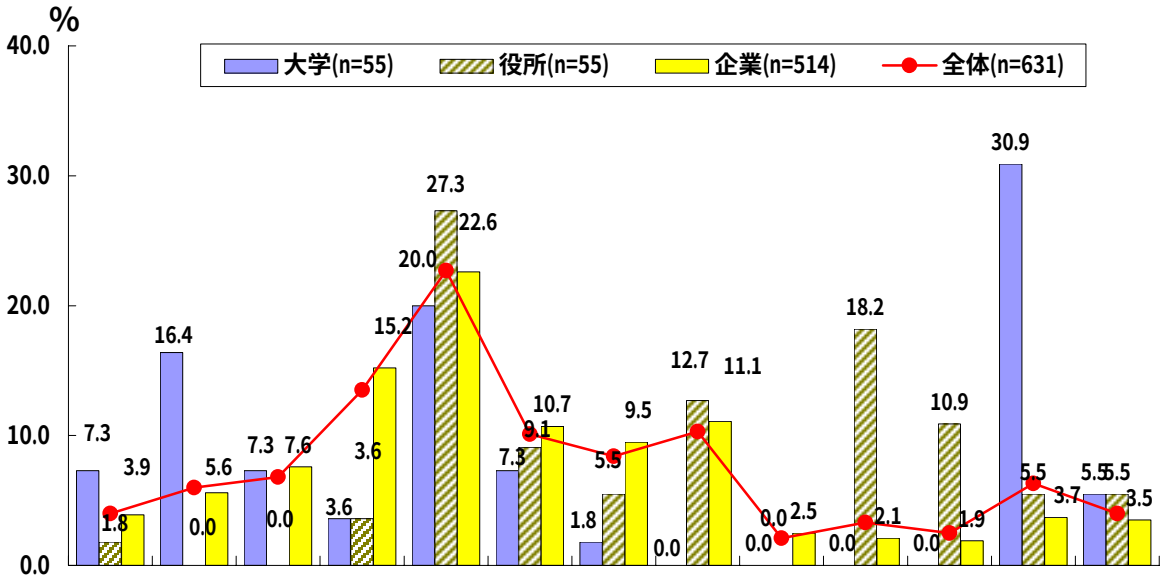
(イ) 業種 (n=514)



	n	エネルギー	運輸業	金融	情報通信	医療	製造業	農林・水産・鉱業	サービス	不動産・建築	無回答
全体	514	6.4	6.4	14.4	8.4	7.6	32.5	0.2	18.9	4.9	0.6

1．回答者プロフィール（2／4）

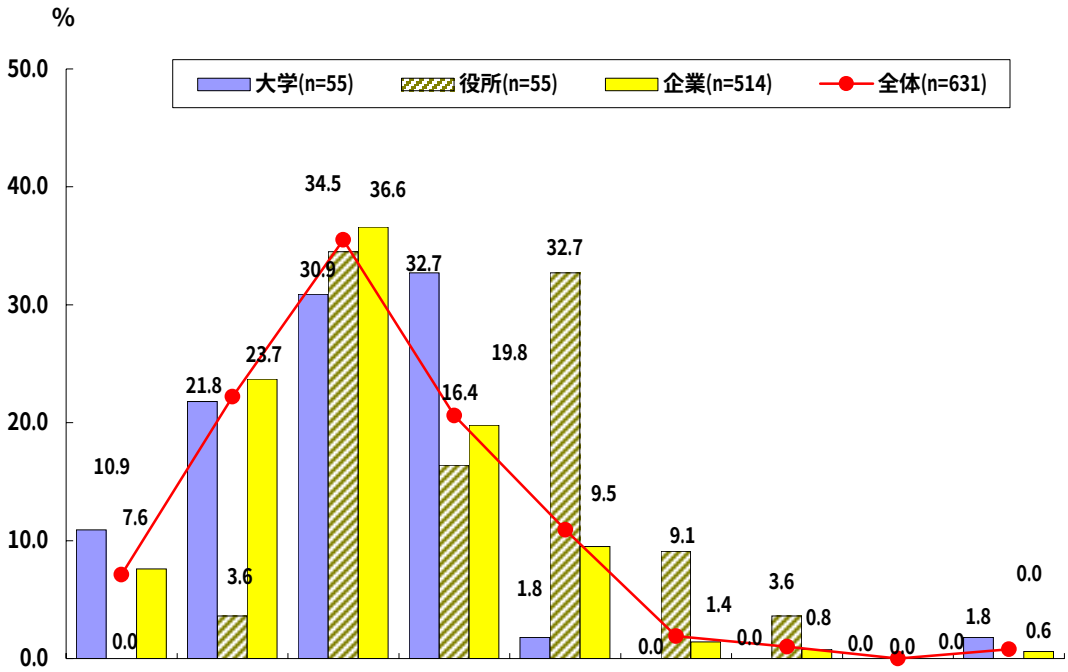
(2) 年間売上、予算規模について



		n	～10億円未満	10億～30億円未満	30億～50億円未満	50億～100億円未満	100億～300億円未満	300億～500億円未満	500億～1000億円未満	1000億～3000億円未満	3000億～5000億円未満	5000億～1兆円未満	1兆円以上～	金額で示せる適切な指標がない	無回答
全体		631	4.0	6.0	6.8	13.5	22.7	10.1	8.4	10.3	2.1	3.3	2.5	6.3	4.0
大 学		55	7.3	16.4	7.3	3.6	20.0	7.3	1.8	-	-	-	-	30.9	5.5
役 所		55	1.8	-	-	3.6	27.3	9.1	5.5	12.7	-	18.2	10.9	5.5	5.5
企業業種別	運輸	10	20.0	-	-	30.0	10.0	-	10.0	10.0	10.0	10.0	-	-	-
	製造	167	0.6	4.2	7.2	12.6	24.0	15.0	9.6	15.6	2.4	3.6	2.4	-	3.0
	サービス	97	2.1	-	8.2	9.3	29.9	14.4	18.6	10.3	2.1	3.1	1.0	-	1.0
	不動産	25	-	4.0	4.0	-	12.0	24.0	12.0	28.0	12.0	-	4.0	-	-
	エネルギー	33	6.1	12.1	9.1	24.2	18.2	3.0	-	6.1	6.1	3.0	6.1	-	6.1
	交通	23	21.7	8.7	13.0	21.7	8.7	4.3	4.3	13.0	-	-	-	-	4.3
	金融	74	5.4	8.1	9.5	9.5	12.2	8.1	8.1	6.8	1.4	-	2.7	24.3	4.1
	情報通信	43	4.7	18.6	7.0	34.9	16.3	2.3	9.3	4.7	-	-	-	-	2.3
	医療	39	2.6	2.6	2.6	25.6	48.7	2.6	-	-	-	-	-	2.6	12.8

1．回答者プロフィール（3／4）

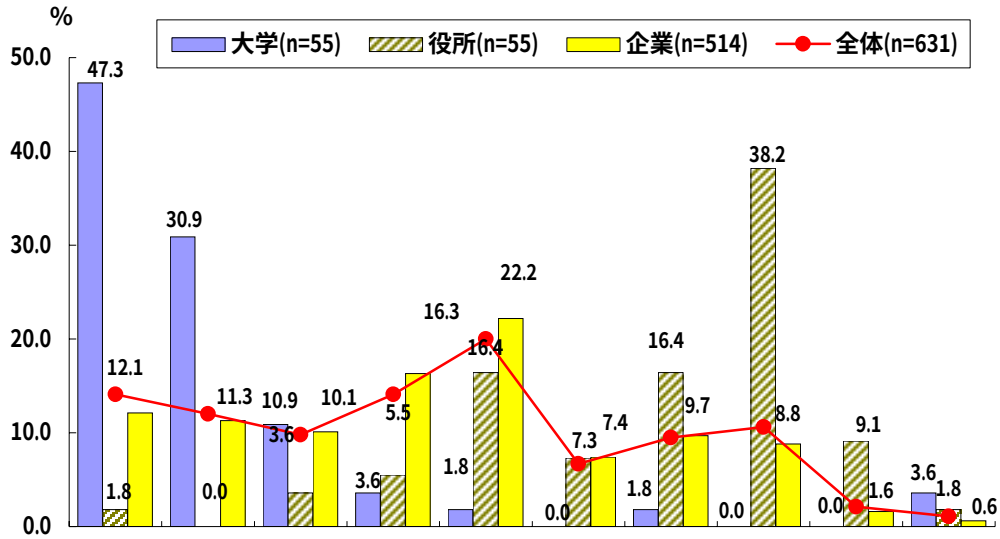
(3) 従業員数 (n=631)



		n	～100人未満	100～300人未満	300～1000人未満	1000～3000人未満	3000～1万人未満	1万～3万人未満	3万～10万人未満	10万人以上	無回答
全体		631	7.1	22.2	35.5	20.6	10.9	1.9	1.0	-	0.8
大 学		55	10.9	21.8	30.9	32.7	1.8	-	-	-	1.8
役 所		55	-	3.6	34.5	16.4	32.7	9.1	3.6	-	-
企業業種別	運輸	10	20.0	10.0	40.0	10.0	10.0	10.0	-	-	-
	製造	167	3.0	19.2	37.7	26.3	9.6	1.8	1.8	-	0.6
	サービス	97	6.2	23.7	42.3	17.5	8.2	2.1	-	-	-
	不動産	25	-	12.0	28.0	36.0	24.0	-	-	-	-
	エネルギー	33	21.2	48.5	12.1	6.1	9.1	-	3.0	-	-
	交通	23	26.1	13.0	39.1	-	21.7	-	-	-	-
	金融	74	8.1	21.6	32.4	24.3	12.2	1.4	-	-	-
	情報通信	43	16.3	55.8	18.6	7.0	2.3	-	-	-	-
	医療	39	-	2.6	71.8	20.5	-	-	-	-	5.1

１．回答者プロフィール（４／４）

(4) 事業所数(n=631)

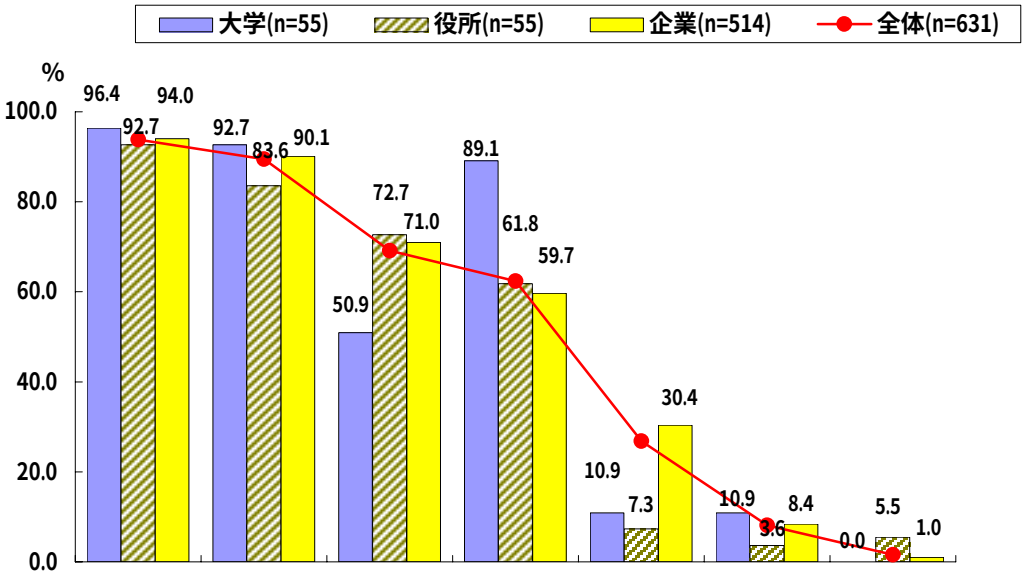


	n	1ヶ所	2～3ヶ所	4～5ヶ所	6～9ヶ所	10～29ヶ所	30～49ヶ所	50～99ヶ所	100～300ヶ所	301ヶ所以上	無回答
全体	631	14.1	12.0	9.8	14.1	20.0	6.7	9.5	10.6	2.1	1.1
大 学	55	47.3	30.9	10.9	3.6	1.8	-	1.8	-	-	3.6
役 所	55	1.8	-	3.6	5.5	16.4	7.3	16.4	38.2	9.1	1.8
企業業種別 運輸	10	20.0	-	20.0	-	20.0	-	20.0	10.0	10.0	-
企業業種別 製造	167	3.6	15.0	11.4	25.7	26.9	5.4	9.0	1.8	0.6	0.6
企業業種別 サービス	97	2.1	8.2	7.2	10.3	27.8	13.4	12.4	15.5	3.1	-
企業業種別 不動産	25	-	8.0	8.0	8.0	36.0	12.0	4.0	20.0	4.0	-
企業業種別 エネルギー	33	33.3	27.3	9.1	12.1	3.0	6.1	6.1	3.0	-	-
企業業種別 交通	23	4.3	21.7	17.4	21.7	13.0	4.3	4.3	13.0	-	-
企業業種別 金融	74	1.4	2.7	4.1	8.1	27.0	12.2	18.9	23.0	2.7	-
企業業種別 情報通信	43	11.6	14.0	23.3	32.6	11.6	2.3	4.7	-	-	-
企業業種別 医療	39	84.6	2.6	5.1	-	2.6	-	-	-	-	5.1

２．情報設備等の環境（１／１０）

(1) コンピュータの種類別保有率 (MA) (n=631)

●保有コンピュータの種類は、全体で「クライアント」「ＮＴサーバ」「汎用機／オフコン」の順で保有率が高い。大学では「ＵＮＩＸサーバ」の保有率が高く、企業では「モバイル端末」の保有率が高い。

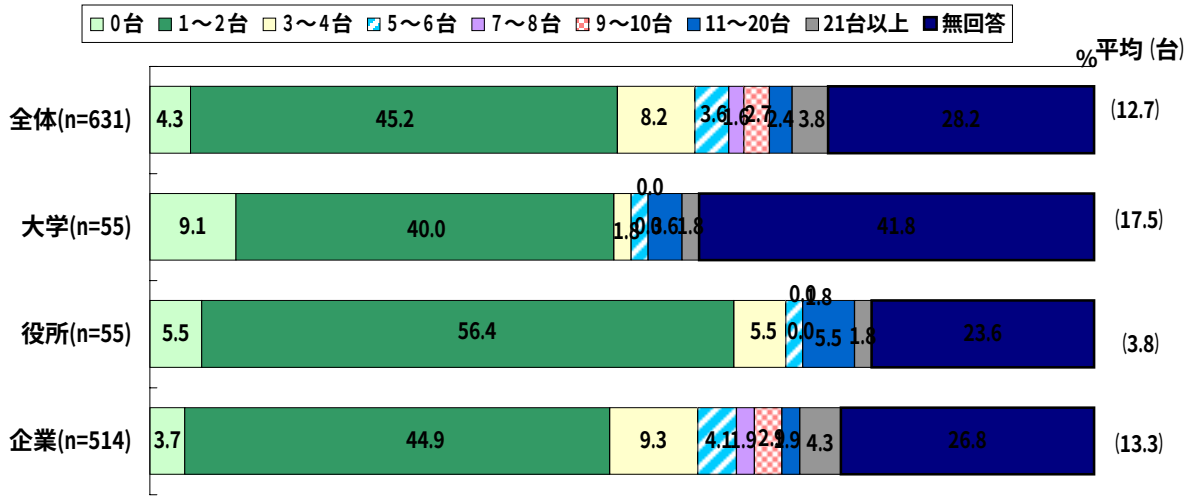


		n	クライアント（パソコン）	Windows NT/2000 サーバ	汎用機／オフコン	UNIX サーバ	モバイル端末	その他	無回答
全体		631	93.8	89.5	69.1	62.4	26.8	8.1	1.6
大 学		55	96.4	92.7	50.9	89.1	10.9	10.9	-
役 所		55	92.7	83.6	72.7	61.8	7.3	3.6	5.5
企業業種別	運輸	10	70.0	60.0	50.0	40.0	30.0	-	10.0
	製造	167	95.2	95.8	85.6	61.7	40.1	7.8	0.6
	サービス	97	96.9	92.8	73.2	61.9	34.0	7.2	-
	不動産	25	92.0	88.0	56.0	52.0	24.0	12.0	-
	エネルギー	33	90.9	84.8	51.5	48.5	30.3	21.2	3.0
	交通	23	78.3	65.2	56.5	30.4	4.3	8.7	4.3
	金融	74	97.3	91.9	68.9	58.1	14.9	9.5	-
	情報通信	43	95.3	93.0	58.1	76.7	44.2	4.7	-
	医療	39	92.3	79.5	66.7	71.8	15.4	5.1	2.6

２．情報設備等の環境（２／１０）

（ア）汎用機/オフコンの保有台数（ｎ=631）

●汎用機の保有台数は大学が平均17.5台と高い値となっているが、１校で500台との回答があり、これを除くと、平均3.0台となる。

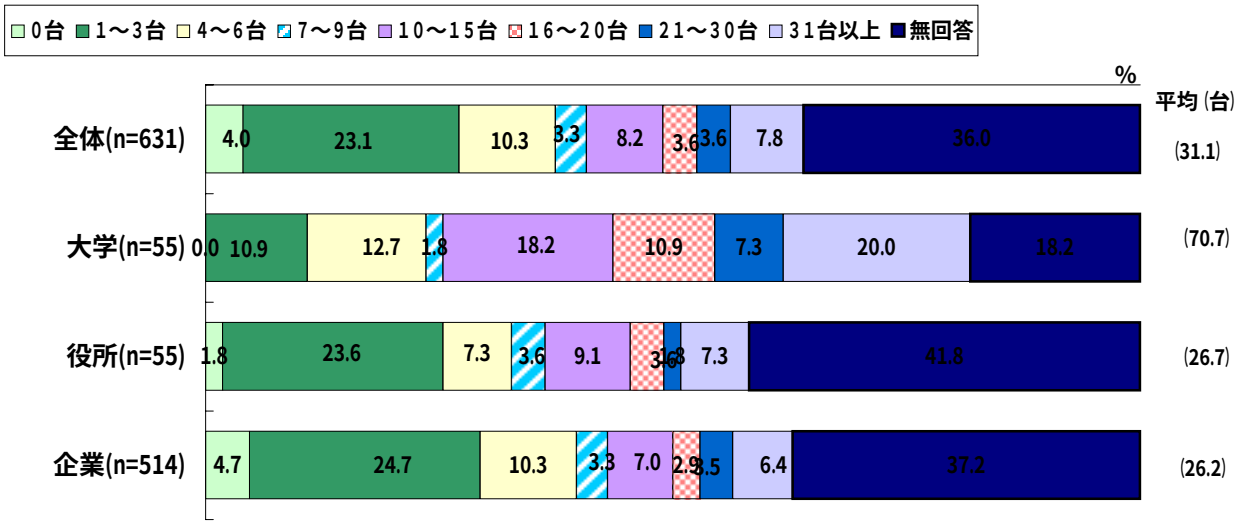


		n	0台	1～2台	3～4台	5～6台	7～8台	9～10台	11～20台	21台以上	無回答	平均
全体		631	4.3	45.2	8.2	3.6	1.6	2.7	2.4	3.8	28.2	12.7
大学		55	9.1	40	1.8	1.8	-	-	3.6	1.8	41.8	17.5
役所		55	5.5	56.4	5.5	1.8	-	-	5.5	1.8	23.6	3.8
企業種別	運輸	10	20.0	30.0	-	-	-	-	10.0	10.0	30.0	11.4
	製造	167	2.4	56.9	10.2	5.4	3.6	3.6	0.6	3.0	14.4	6.8
	サービス	97	6.2	48.5	8.2	3.1	1.0	4.1	3.1	4.1	21.6	5.5
	不動産	25	-	32	-	4.0	-	8.0	4.0	8.0	44.0	164.2
	エネルギー	33	9.1	30.3	6.1	-	-	-	9.1	3.0	42.4	6.2
	交通	23	-	34.8	4.3	4.3	-	4.3	4.3	4.3	43.5	7.5
	金融	74	-	29.7	23.0	5.4	2.7	1.4	-	4.1	33.8	15.2
	情報通信	43	4.7	39.5	7.0	7.0	-	2.3	-	2.3	37.2	3.3
	医療	39	5.1	53.8	-	-	2.6	-	-	10.3	28.2	7.0

２．情報設備等の環境（３／１０）

（イ）UNIXサーバの保有台数（ｎ=631）

●ＵＮＩＸサーバの保有台数は「１～３台」が23.1%を占める。
全体平均は31.1台である。

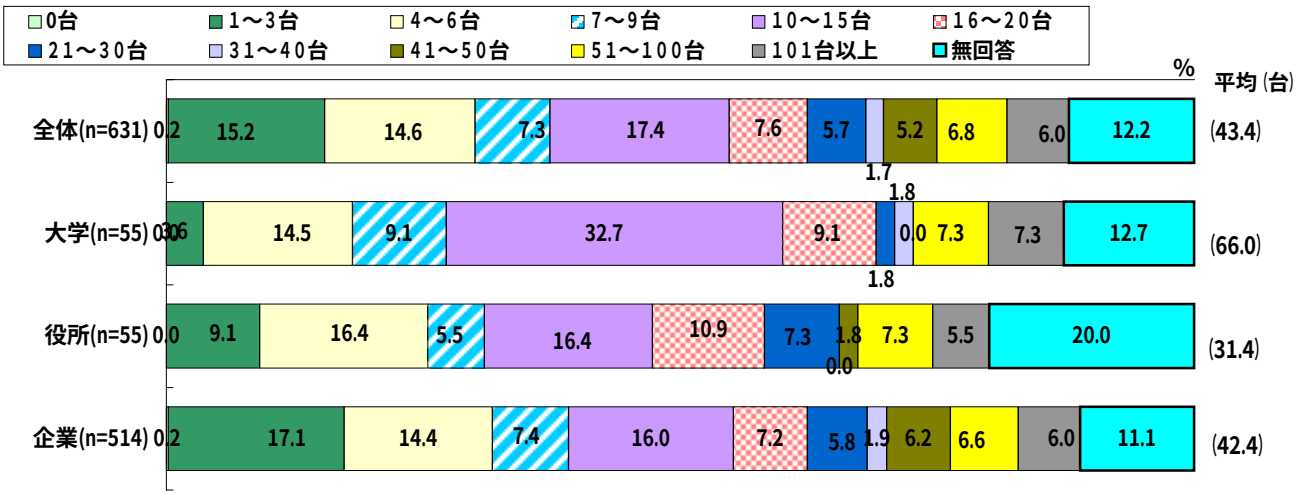


		n	0台	1～3台	4～6台	7～9台	10～15台	16～20台	21～30台	31台以上	無回答	平均
全体		631	4.0	23.1	10.3	3.3	8.2	3.6	3.6	7.8	36.0	31.1
大学		55	-	10.9	12.7	1.8	18.2	10.9	7.3	20.0	18.2	70.7
役所		55	1.8	23.6	7.3	3.6	9.1	3.6	1.8	7.3	41.8	26.7
企業業種別	運輸	10	10	20.0	10.0	-	10.0	-	-	-	50.0	3.8
	製造	167	5.4	22.8	7.8	4.2	9.6	1.8	4.8	9.0	34.7	49.1
	サービス	97	7.2	32	10.3	2.1	3.1	2.1	3.1	9.3	30.9	20.3
	不動産	25	4	16	8.0	4.0	-	20.0	-	4.0	44.0	11.5
	エネルギー	33	6.1	27.3	6.1	-	-	3.0	-	9.1	48.5	22.4
	交通	23	-	8.7	4.3	4.3	13.0	-	-	-	69.6	6.3
	金融	74	2.7	23.0	10.8	2.7	10.8	2.7	4.1	1.4	41.9	13.3
	情報通信	43	2.3	23.3	25.6	7.0	2.3	2.3	4.7	9.3	23.3	12.1
	医療	39	2.6	35.9	12.8	2.6	10.3	2.6	5.1	-	28.2	6.3

2．情報設備等の環境（4／10）

(ウ) NTサーバの保有台数 (n=631)

●NTサーバの保有台数は「10～15台」が最も高く17.4%。次いで「1～3台」「4～6台」の順になっている。全体の平均値は43.4台である。

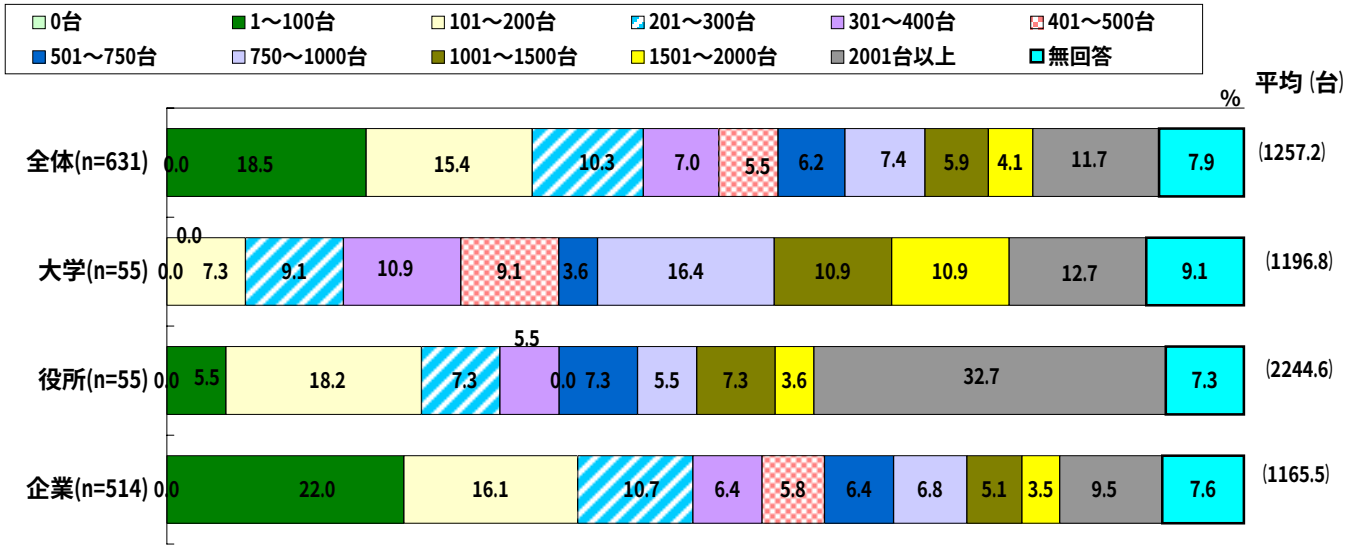


		n	0台	1～3台	4～6台	7～9台	11～50台	21～60台	31～100台	41～150台	51～200台	101～500台	101台以上	無回答	平均
全体		631	0.2	15.2	14.6	7.3	17.4	7.6	5.7	1.7	5.2	6.8	6.0	12.2	43.4
大学		55	-	3.6	14.5	9.1	32.7	9.1	1.8	1.8	-	7.3	7.3	12.7	66.0
役所		55	-	9.1	16.4	5.5	16.4	10.9	7.3	-	1.8	7.3	5.5	20.0	31.4
企業業種別	運輸	10	-	20.0	10.0	-	-	-	-	10.0	10.0	-	10.0	40.0	57.8
	製造	167	0.6	14.4	11.4	7.8	19.2	7.8	6.0	2.4	8.4	9.6	7.2	5.4	64.5
	サービス	97	-	17.5	16.5	6.2	14.4	9.3	6.2	2.1	4.1	10.3	6.2	7.2	41.3
	不動産	25	-	8.0	8.0	8.0	24.0	16.0	12.0	-	4.0	4.0	4.0	12.0	25.5
	エネルギー	33	-	27.3	15.2	9.1	9.1	3.0	3.0	-	3.0	3.0	9.1	18.2	35.0
	交通	23	-	26.1	13.0	8.7	-	-	4.3	-	8.7	4.3	-	34.8	16.7
	金融	74	-	20.3	12.2	6.8	16.2	4.1	5.4	2.7	6.8	6.8	8.1	10.8	33.5
	情報通信	43	-	16.3	25.6	11.6	18.6	2.3	4.7	2.3	7.0	-	4.7	7.0	18.3
	医療	39	-	15.4	17.9	5.1	12.8	15.4	7.7	-	2.6	-	-	23.1	12.7

２．情報設備等の環境（５／１０）

(エ) クライアントＰＣ保有台数 (n=631)

●クライアント保有台数は「１～100台」が最も高く18.5%。次いで「101～200台」「201～300台」の順になっている。全体の平均は1257.2台である。

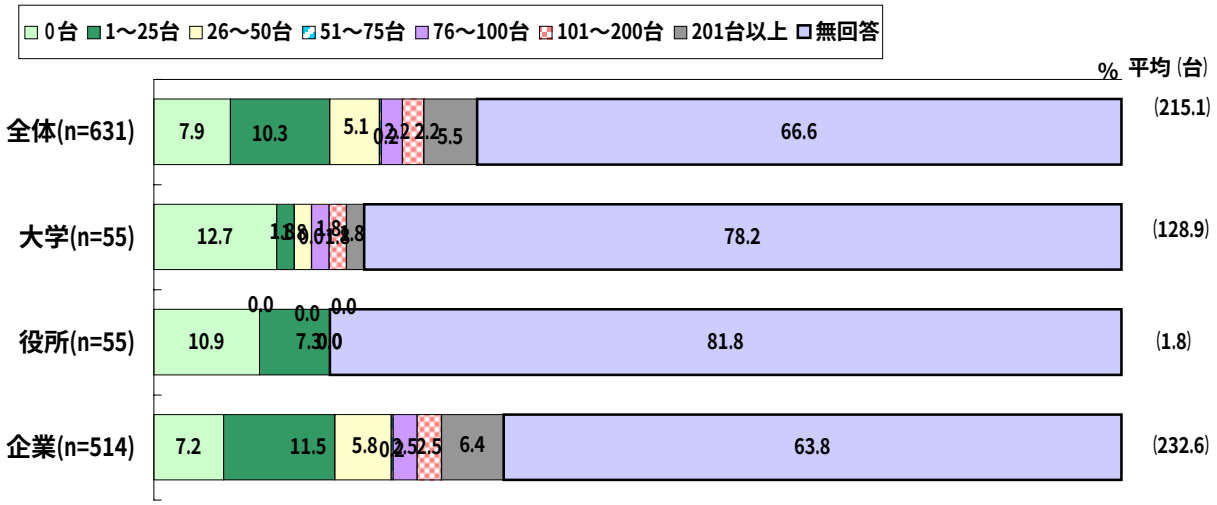


		n	0台	1～100台	101～200台	201～300台	301～400台	401～500台	501～750台	751～1000台	1001～1500台	1501～2000台	2001台以上	無回答	平均
全体		631	-	18.5	15.4	10.3	7.0	5.5	6.2	7.4	5.9	4.1	11.7	7.9	1257.2
大 学		55	-	-	7.3	9.1	10.9	9.1	3.6	16.4	10.9	10.9	12.7	9.1	1196.8
役 所		55	-	5.5	18.2	7.3	5.5	-	7.3	5.5	7.3	3.6	32.7	7.3	2244.6
企業業種別	運輸	10	-	30.0	-	10.0	-	-	10.0	10.0	-	-	10.0	30.0	1142.9
	製造	167	-	11.4	16.8	12.6	6.0	7.2	6.6	7.2	6.0	5.4	13.8	7.2	2046.4
	サービス	97	-	23.7	15.5	12.4	8.2	7.2	7.2	10.3	3.1	3.1	6.2	3.1	782.4
	不動産	25	-	8.0	4.0	4.0	4.0	8.0	12.0	4.0	16.0	8.0	24.0	8.0	1633.5
	エネルギー	33	-	51.5	12.1	3.0	-	3.0	3.0	-	3.0	3.0	9.1	12.1	805.2
	交通	23	-	56.5	4.3	-	-	-	-	8.7	4.3	-	4.3	21.7	360.2
	金融	74	-	21.6	20.3	8.1	6.8	5.4	6.8	5.4	8.1	2.7	9.5	5.4	814.2
	情報通信	43	-	27.9	32.6	14.0	2.3	-	7.0	4.7	2.3	2.3	2.3	4.7	382.1
	医療	39	-	17.9	7.7	17.9	20.5	10.3	5.1	7.7	-	-	2.6	10.3	412.3

２．情報設備等の環境（６／１０）

(オ) モバイル端末の保有台数 (n=631)

●モバイル端末の保有台数は「１～25台」が最も高く10.3%。次いで「0台」「201台以上」の順になっている。全体の平均は215.1台である。

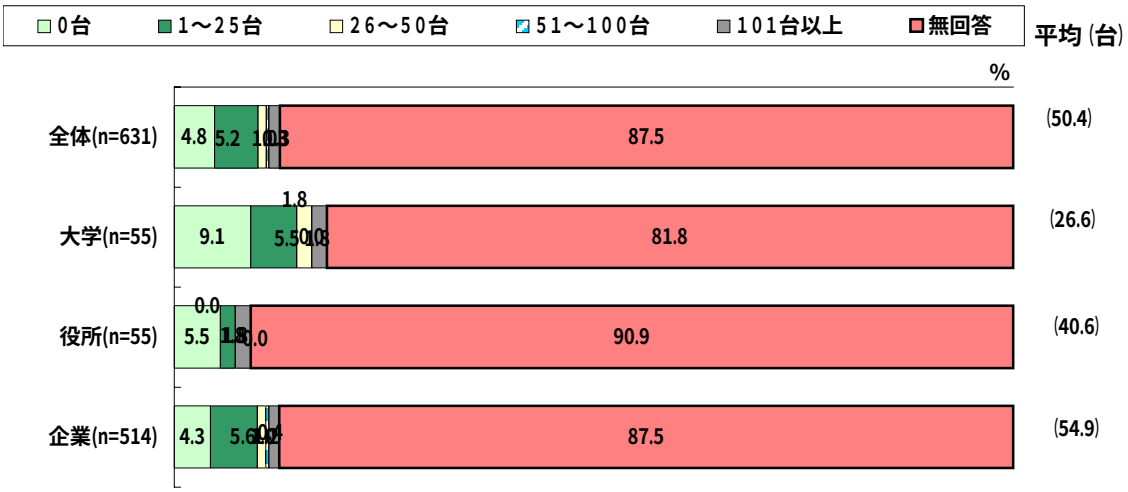


		n	0台	1～25台	26～50台	51～75台	76～100台	101～200台	201台以上	無回答	平均
全体		631	7.9	10.3	5.1	0.2	2.2	2.2	5.5	66.6	215.1
大学		55	12.7	1.8	1.8	-	1.8	1.8	1.8	78.2	128.9
役所		55	10.9	7.3	-	-	-	-	-	81.8	1.8
企業業種別	運輸	10	20	-	10.0	-	-	10.0	10.0	50.0	3038.0
	製造	167	4.8	13.8	6.6	0.6	3.6	4.2	9.0	57.5	140.1
	サービス	97	10.3	10.3	9.3	-	2.1	4.1	7.2	56.7	231.1
	不動産	25	4	12	4.0	-	-	-	8.0	72.0	155.7
	エネルギー	33	9.1	12.1	9.1	-	3.0	-	3.0	63.6	41.3
	交通	23	4.3	4.3	-	-	-	-	-	91.3	2.5
	金融	74	12.2	6.8	1.4	-	-	-	5.4	74.3	141.9
	情報通信	43	2.3	23.3	9.3	-	4.7	-	7.0	53.5	188.8
	医療	39	5.1	7.7	-	-	5.1	2.6	-	79.5	44.4

２．情報設備等の環境（７／１０）

(カ) その他 (n=631)

●その他の台数を見ると「１～25台」が最も多く5.2%。次いで「０台」「101台以上」の順になっている。全体の平均は81.2台である。
●その他の回答内容を見てみると、「Ｌｉｎｕｘサーバ」「ＯＳ２サーバ」「外部委託」などである。

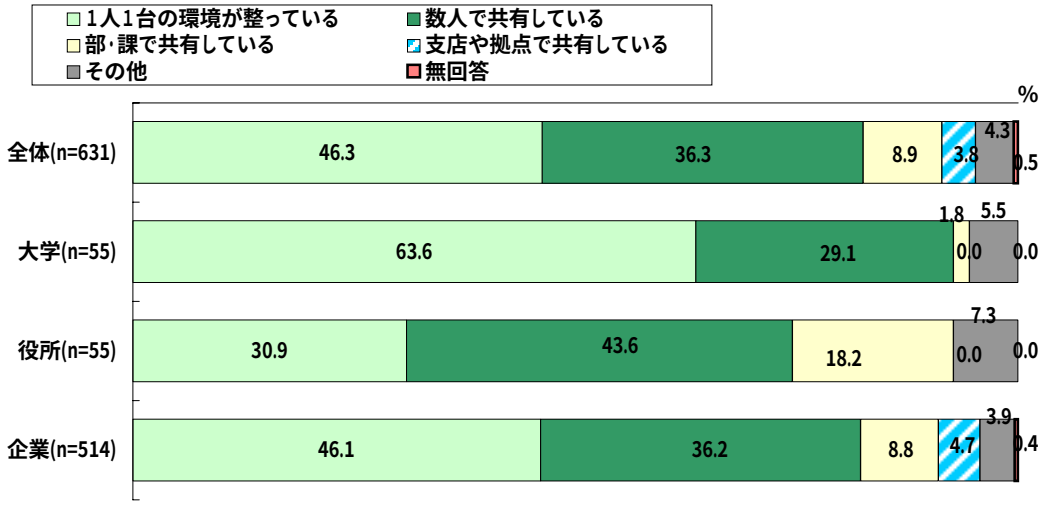


		n	0台	1～25台	26～50台	51～100台	101台以上	無回答	平均
全体		631	4.8	5.2	1.0	0.3	1.3	87.5	50.4
大学		55	9.1	5.5	1.8	-	1.8	81.8	26.6
役所		55	5.5	1.8	-	-	1.8	90.9	40.6
企業業種別	運輸	10	-	-	-	-	-	100.0	-
	製造	167	3	4.8	1.2	-	1.2	89.8	46.2
	サービス	97	6.2	4.1	-	2.1	1.0	86.6	36.8
	不動産	25	4	12	-	-	-	84.0	3.8
	エネルギー	33	9.1	18.2	3.0	-	-	69.7	12.8
	交通	23	4.3	8.7	-	-	-	87.0	7.0
	金融	74	5.4	4.1	1.4	-	4.1	85.1	186.2
	情報通信	43	2.3	4.7	-	-	-	93.0	1.3
	医療	39	2.6	2.6	2.6	-	-	92.3	10.3

２．情報設備等の環境（８／１０）

(2) 端末装置の利用状況 (n=631)

●「１人１台の環境が整っている」の割合が46.3%と最も高くなっている。
その中でも、大学、３０００人以上の企業では「１人１台の環境が整っている」の割合が60%を超えており、端末環境の設備が進んでいると思われる。



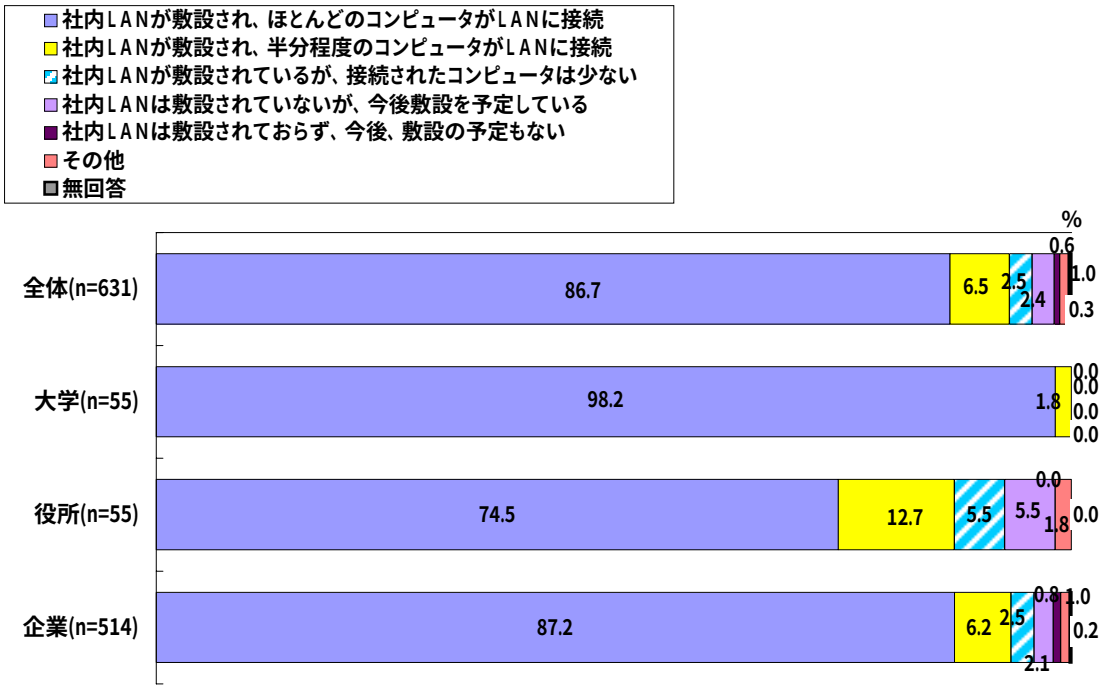
		n	1人1台の環境が整っている	数人で共有している	部・課で共有している	支店や拠点で共有している	その他	無回答
全体		631	46.3	36.3	8.9	3.8	4.3	0.5
大学		55	63.6	29.1	1.8	-	5.5	-
役所		55	30.9	43.6	18.2	-	7.3	-
企業業種別	運輸	10	20.0	50.0	10.0	20.0	-	-
	製造	167	58.7	32.3	3.6	0.6	4.2	0.6
	サービス	97	60.8	28.9	4.1	5.2	1.0	-
	不動産	25	64	32.0	-	-	4.0	-
	エネルギー	33	42.4	36.4	12.1	3.0	6.1	-
	交通	23	8.7	56.5	17.4	13.0	4.3	-
	金融	74	24.3	48.6	8.1	14.9	4.1	-
	情報通信	43	51.2	27.9	14.0	-	7.0	-
	医療	39	7.7	46.2	35.9	2.6	5.1	2.6

２．情報設備等の環境（９／１０）

(3) ネットワークの接続状況 (n=631)

●95%以上でＬＡＮが導入されている。特に、全体の86.7%が「ほとんどのコンピュータがＬＡＮに接続されている」と回答しており、ネットワークでの利用の進展が伺える。

●大学では特に「ほとんどのコンピュータがＬＡＮに接続されている」割合が全体と比べ高く、98.2%に達している。

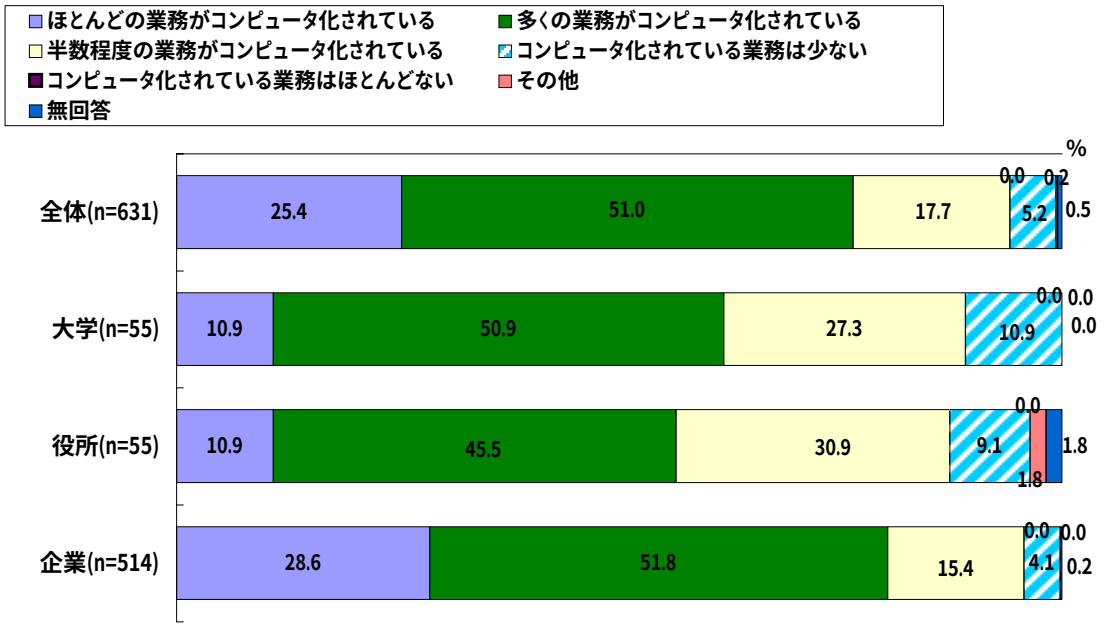


		n	社内ＬＡＮが敷設され、ほとんどのコンピュータがＬＡＮに接続されている	社内ＬＡＮが敷設され、半分程度のコンピュータがＬＡＮに接続されている	社内ＬＡＮが敷設されているが、接続されたコンピュータは少ない	社内ＬＡＮは敷設されていないが、今後敷設を予定している	社内ＬＡＮは敷設されておらず、今後、敷設の予定もない	その他	無回答
全体		631	86.7	6.5	2.5	2.4	0.6	1.0	0.3
大 学		55	98.2	1.8	-	-	-	-	-
役 所		55	74.5	12.7	5.5	5.5	-	1.8	-
企業業種別	運輸	10	100.0	-	-	-	-	-	-
	製造	167	96.4	3.0	-	0.6	-	-	-
	サービス	97	84.5	11.3	2.1	1.0	-	-	1.0
	不動産	25	88.0	12.0	-	-	-	-	-
	エネルギー	33	78.8	9.1	3.0	6.1	-	3.0	-
	交通	23	56.5	8.7	8.7	8.7	13.0	4.3	-
	金融	74	89.2	2.7	4.1	-	1.4	2.7	-
	情報通信	43	86.0	7.0	2.3	4.7	-	-	-
	医療	39	71.8	7.7	10.3	7.7	-	2.6	-

２．情報設備等の環境（１０／１０）

(4) 業務のコンピュータ化の程度 (n=631)

●90%以上で「半数以上の業務がコンピュータ化されている」と回答している。

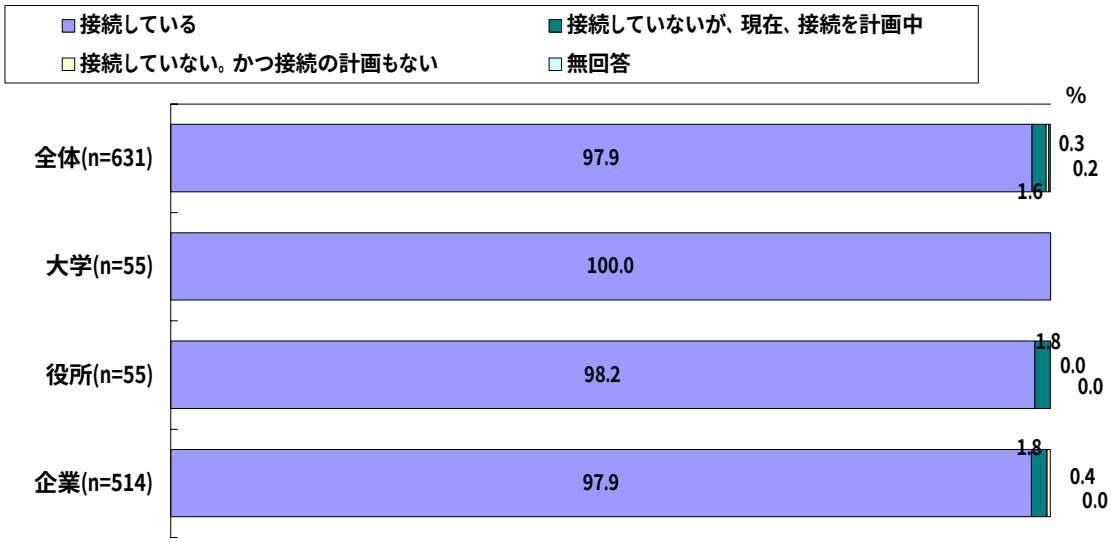


		n	ほとんどの業務がコンピュータ化されている	多くの業務がコンピュータ化されている	半数程度の業務がコンピュータ化されている	コンピュータ化されている業務は少ない	コンピュータ化されている業務はほとんどない	その他	無回答
全体		631	25.4	51.0	17.7	5.2	-	0.2	0.5
大 学		55	10.9	50.9	27.3	10.9	-	-	-
役 所		55	10.9	45.5	30.9	9.1	-	1.8	1.8
企業業種別	運輸	10	30.0	50.0	20.0	-	-	-	-
	製造	167	31.1	54.5	12.6	1.2	-	-	0.6
	サービス	97	34.0	49.5	12.4	4.1	-	-	-
	不動産	25	28.0	52.0	20.0	-	-	-	-
	エネルギー	33	36.4	54.5	3.0	6.1	-	-	-
	交通	23	13.0	34.8	26.1	26.1	-	-	-
	金融	74	29.7	52.7	16.2	1.4	-	-	-
	情報通信	43	23.3	51.2	23.3	2.3	-	-	-
	医療	39	10.3	51.3	25.6	12.8	-	-	-

３．インターネットへの接続状況（１／４）

(1) インターネットへの接続状況 (n=631)

●全体の97.9%が「接続している」と回答している。
●ほとんどインターネットへ接続している状況であり、特に大学では100%となっている。



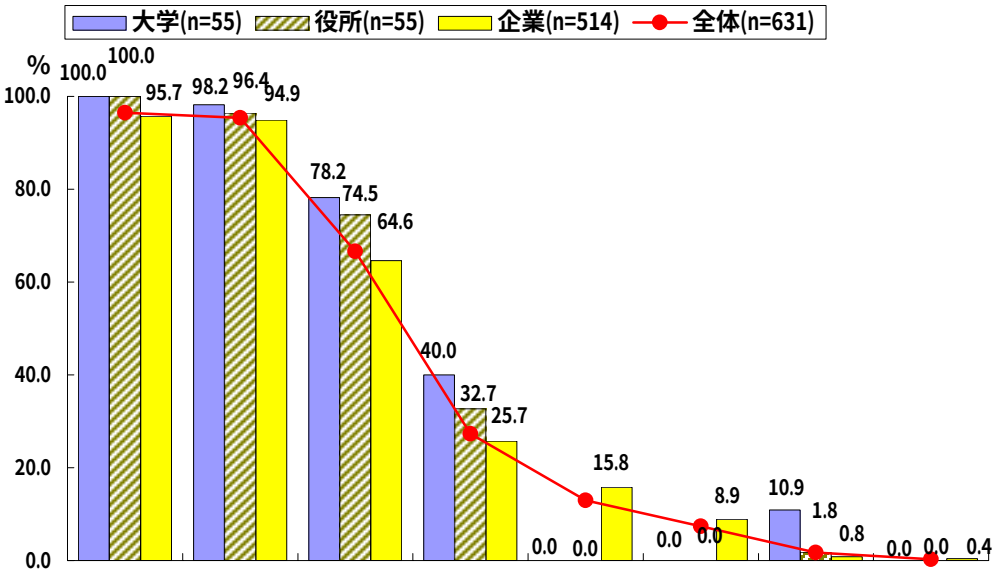
		n	接続している	接続していないが、現在、接続を計画中	接続していない。かつ接続の計画もない	無回答
全体		631	97.9	1.6	0.3	0.2
大 学		55	100	-	-	-
役 所		55	98.2	1.8	-	-
企業業種別	運輸	10	100.0	-	-	-
	製造	167	99.4	0.6	-	-
	サービス	97	99.0	1.0	-	-
	不動産	25	100.0	-	-	-
	エネルギー	33	93.9	6.1	-	-
	交通	23	95.7	4.3	-	-
	金融	74	97.3	1.4	1.4	-
	情報通信	43	100.0	-	-	-
	医療	39	89.7	7.7	2.6	-

３．インターネットへの接続状況（２／４）

(2)インターネットの接続目的（MA）（n=631）

●利用目的として「各種情報収集」「電子メール」との回答が95%以上となっている。

●「顧客や外部に向けての情報提供」での利用の割合は66.6%であったが、昨年度調査の55.6%を大幅に上回った。また役所での「社内（構内）拠点間を結ぶ業務用」の割合も32.7%と、昨年度調査の17.2%を大幅に上回りネットワーク化が進んでいることが伺える。



		n	各種の情報収集	電子メール	顧客や外部に向けての情報提供	社内（校内）拠点間を結ぶ業務用	インターネット販売	オンラインバンキング、トレーディング	その他	無回答
全体		631	96.5	95.4	66.6	27.3	13.0	7.4	1.7	0.3
大 学		55	100.0	98.2	78.2	40.0	-	-	10.9	-
役 所		55	100.0	96.4	74.5	32.7	-	-	1.8	-
企業業種別	運輸	10	100.0	100.0	70.0	50.0	30.0	10.0	-	-
	製造	167	98.8	96.4	65.9	25.1	15.0	5.4	1.2	-
	サービス	97	96.9	95.9	63.9	33.0	27.8	6.2	-	-
	不動産	25	100.0	96.0	80.0	36.0	12.0	-	4.0	-
	エネルギー	33	90.9	97.0	54.5	24.2	6.1	6.1	-	-
	交通	23	82.6	91.3	69.6	8.7	39.1	8.7	-	-
	金融	74	93.2	90.5	71.6	18.9	8.1	33.8	-	1.4
	情報通信	43	93.0	95.3	60.5	25.6	14.0	2.3	-	-
	医療	39	94.9	92.3	46.2	20.5	-	-	2.6	2.6

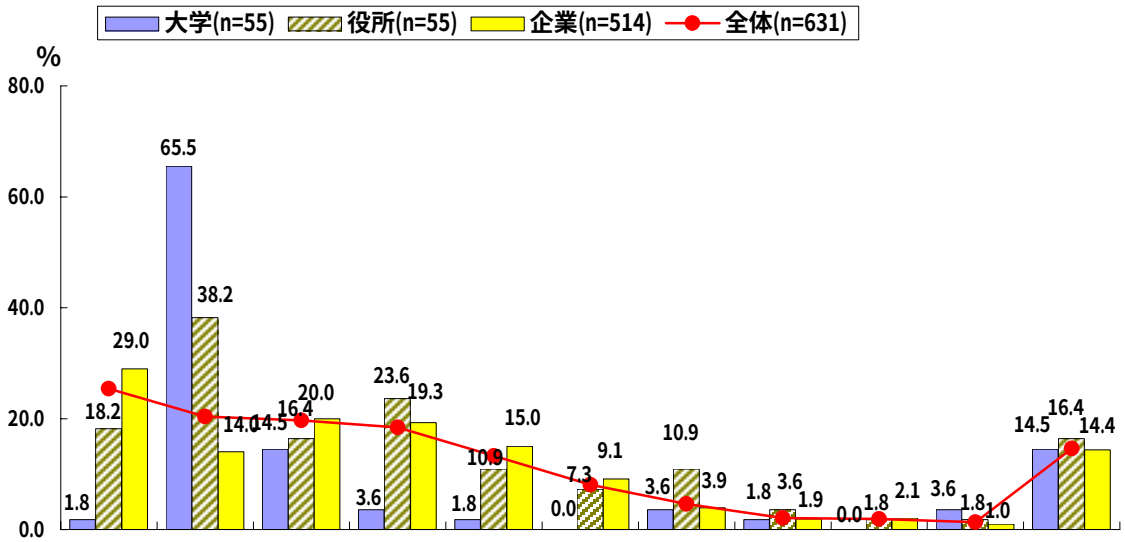
３．インターネットへの接続状況（３／４）

(3)インターネットの接続方法(MA)(n=631)

●「専用回線（256pps以下）」の割合が最も高く25.4%。次いで「超高速専用回線（1.5Mbps以上）」「高速専用回線（1.5Mbbps）」となっている。

●「ＩＳＤＮ回線」が18.4%と昨年度調査の39.7%を下回っており、逆に「ＡＤＳＬ／ＳＤＳＬ回線」が13.3%と昨年度調査の0.5%を大きく上回った。

●大学では、「超高速専用回線（1.5Mbps以上）」の割合が65.5%と全体に比べて高くなっている。

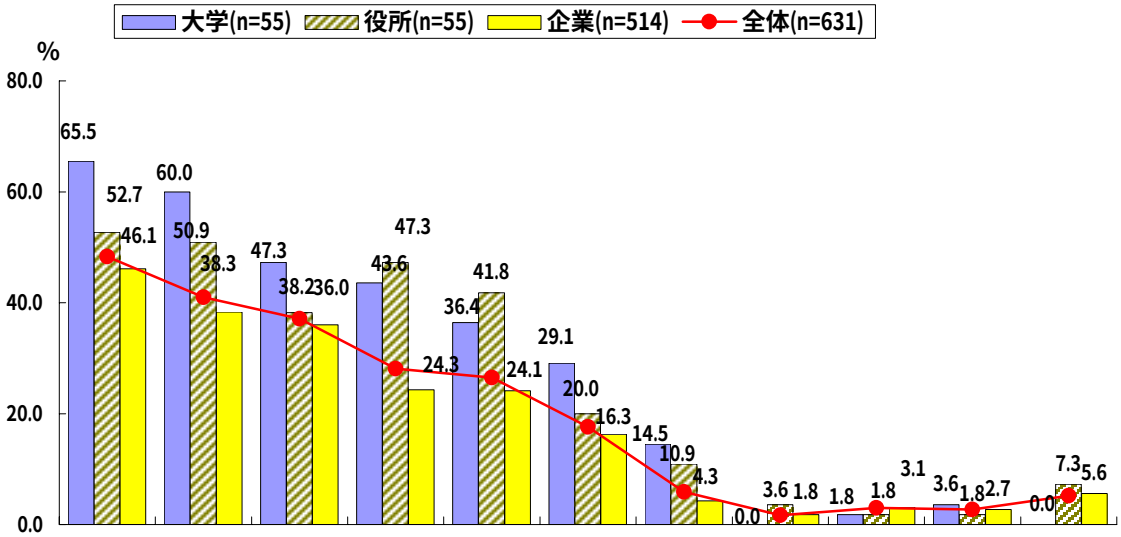


		n	専用回線（256bps以下）	超高速専用回線（1.5Mbps以上）	高速専用回線（1.5Mbps未満）	ISDN回線	ADSL／SDSL回線	アナログ電話回線	CATV回線	無線回線	携帯電話回線	その他	無回答
全体		631	25.4	20.4	19.7	18.4	13.3	8.1	4.6	2.1	1.9	1.3	14.6
大学		55	1.8	65.5	14.5	3.6	1.8	-	3.6	1.8	-	3.6	14.5
役所		55	18.2	38.2	16.4	23.6	10.9	7.3	10.9	3.6	1.8	1.8	16.4
企業業種別	運輸	10	20.0	-	60.0	20.0	-	30.0	-	-	-	-	10.0
	製造	167	30.5	18.0	26.3	15.0	13.8	7.2	2.4	3.0	1.8	1.2	7.2
	サービス	97	29.9	12.4	23.7	19.6	20.6	9.3	1.0	2.1	4.1	2.1	18.6
	不動産	25	20.0	24.0	24.0	20.0	12.0	12.0	4.0	-	4.0	-	16.0
	エネルギー	33	21.2	21.2	6.1	24.2	6.1	9.1	6.1	3.0	-	3.0	15.2
	交通	23	17.4	13.0	4.3	17.4	26.1	13.0	13.0	-	-	-	17.4
	金融	74	24.3	9.5	16.2	29.7	13.5	13.5	4.1	1.4	1.4	-	21.6
	情報通信	43	39.5	9.3	16.3	14.0	18.6	4.7	4.7	-	2.3	-	14.0
	医療	39	38.5	7.7	5.1	20.5	12.8	5.1	10.3	2.6	2.6	-	15.4

３．インターネットへの接続状況（４／４）

(4)インターネットの接続点へのアクセス制御対策（MA）（n=631）

●全体で見ると、「ファイアウォールの導入」が48.3%と最も高く、次いで「ＰＲＯＸＹサーバーの設置」「ルータによるプロトコル制御」となっている。

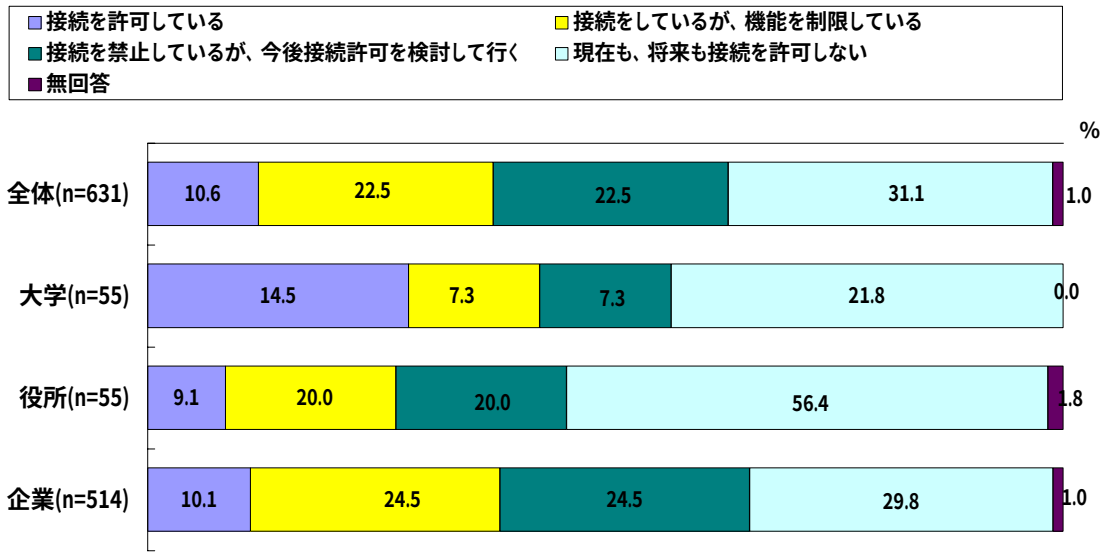


		n	ファイアウォールの導入	PROXYサーバの設置	ルータによるプロトコル制御	アクセスログ収集の強化・充実	DMZの構築	ID／認証パスワード	自動侵入監視システム（IDS）の導入	電子証明書（PKI）	その他	特に何も行っていない	無回答
全体		631	48.3	41.0	37.1	28.1	26.5	17.6	5.9	1.7	3.0	2.7	5.2
大 学		55	65.5	60.0	47.3	43.6	36.4	29.1	14.5	-	1.8	3.6	-
役 所		55	52.7	50.9	38.2	47.3	41.8	20.0	10.9	3.6	1.8	1.8	7.3
企業種別	運輸	10	60.0	40.0	40.0	10.0	10.0	30.0	-	-	-	-	10.0
	製造	167	50.9	45.5	36.5	26.3	28.7	15.6	2.4	3.0	2.4	1.2	3.0
	サービス	97	44.3	35.1	33.0	26.8	27.8	15.5	5.2	1.0	3.1	3.1	4.1
	不動産	25	48.0	40.0	32.0	32.0	24.0	20.0	4.0	4.0	-	-	4.0
	エネルギー	33	45.5	42.4	24.2	18.2	27.3	18.2	9.1	-	6.1	6.1	15.2
	交通	23	34.8	30.4	47.8	17.4	21.7	8.7	4.3	-	-	17.4	8.7
	金融	74	44.6	36.5	47.3	24.3	12.2	25.7	8.1	2.7	6.8	1.4	6.8
	情報通信	43	37.2	30.2	27.9	32.6	27.9	11.6	2.3	-	-	-	4.7
	医療	39	46.2	28.2	33.3	7.7	15.4	5.1	2.6	-	5.1	5.1	10.3

４．外部からの情報システムへのアクセス環境（１／５）

(1)外部からの接続の許可 (n=631)

●「接続をしているが、機能を制限している」が34.9%と最も高い。逆に「現在も将来も接続を許可しない」も31.1%と高くなっている。

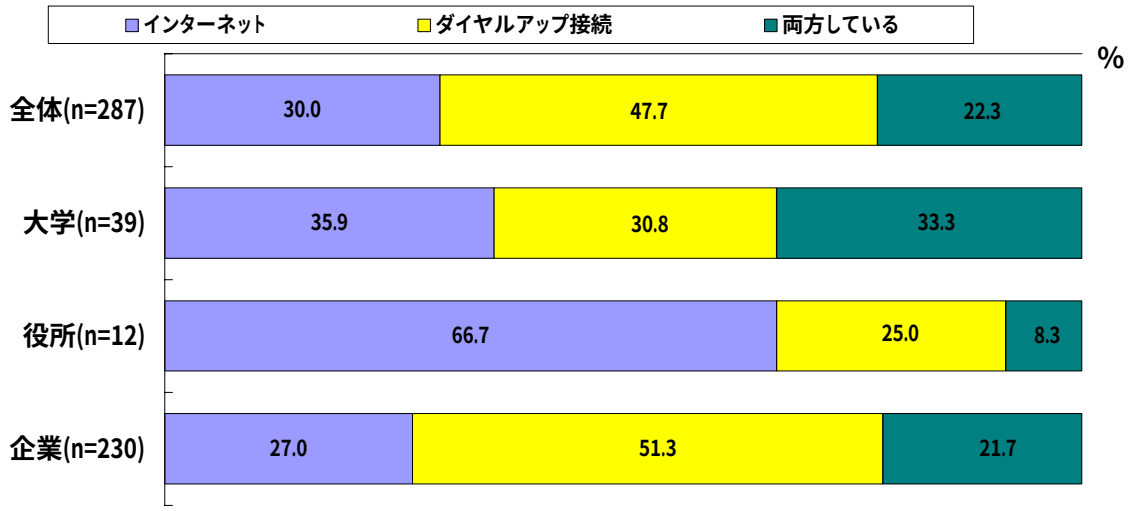


		n	接続を許可している	接続をしているが、機能を制限している	接続を禁止しているが、今後接続許可を検討していく	現在も、将来も接続を許可しない	無回答
全体		631	10.6	34.9	22.5	31.1	1.0
大 学		55	14.5	56.4	7.3	21.8	-
役 所		55	9.1	12.7	20.0	56.4	1.8
企業業種別	運輸	10	20.0	30.0	30.0	20.0	-
	製造	167	12.6	49.1	22.8	15.0	0.6
	サービス	97	10.3	36.1	29.9	22.7	1.0
	不動産	25	20.0	36.0	32.0	12.0	-
	エネルギー	33	9.1	27.3	12.1	45.5	6.1
	交通	23	4.3	21.7	34.8	39.1	-
	金融	74	1.4	18.9	18.9	60.8	-
	情報通信	43	14	34.9	23.3	25.6	2.3
	医療	39	7.7	12.8	28.2	51.3	-

４．外部からの情報システムへのアクセス環境（２／５）

(2) 接続方法 (n=287)

●接続方法では、インターネット経由が（「インターネット」「両方している」の合計）で50%を超えており、昨年度調査の25.9%を大幅に上回った。



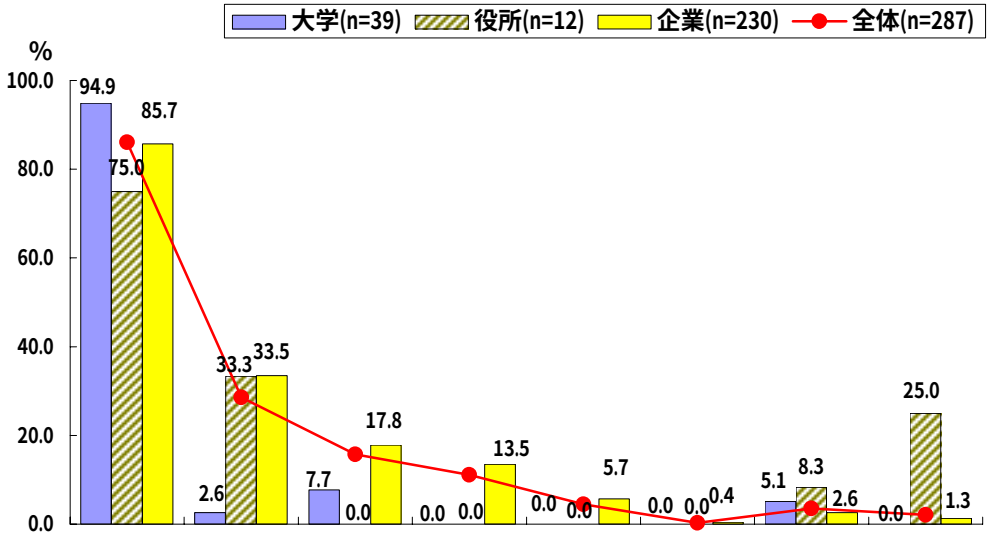
		n	インターネット	ダイヤルアップ接続	両方している
全体		287	30.0	47.7	22.3
大 学		39	35.9	30.8	33.3
役 所		12	66.7	25.0	8.3
企業種別	運輸	5	60.0	20.0	20.0
	製造	103	20.4	51.5	28.2
	サービス	45	22.2	53.3	24.4
	不動産	14	21.4	50.0	28.6
	エネルギー	12	50.0	33.3	16.7
	交通	6	33.3	50.0	16.7
	金融	15	40.0	60.0	-
	情報通信	21	33.3	61.9	4.8
	医療	8	50.0	37.5	12.5

４．外部からの情報システムへのアクセス環境（３／５）

(3)認証方法（MA）（n=287）

●認証方法として「ＩＤ／パスワード認証」の割合が86.1%と最も高くなっている。

●役所、企業では、30%以上の比率で「電話番号規制」を採用しているが、大学では2.6%と極端に低い割合になっている。



		n	パスワード認証（ＩＤ／）	電話番号規制	ワンタイムパスワード	コールバック	電子証明書（ＰＫＩ）	バイオメトリクス（指紋等での認証）	その他	無回答
全体		287	86.1	28.6	15.7	11.1	4.5	0.3	3.5	2.1
大 学		39	94.9	2.6	7.7	-	-	-	5.1	-
役 所		12	75.0	33.3	-	-	-	-	8.3	25.0
企業業種別	運輸	5	100.0	40.0	-	-	40.0	-	20.0	-
	製造	103	83.5	30.1	22.3	15.5	8.7	-	2.9	-
	サービス	45	88.9	33.3	13.3	15.6	2.2	-	-	2.2
	不動産	14	92.9	42.9	21.4	7.1	-	-	-	-
	エネルギー	12	75.0	25.0	16.7	-	-	-	-	8.3
	交通	6	66.7	33.3	-	16.7	-	-	33.3	-
	金融	15	93.3	46.7	6.7	26.7	6.7	6.7	-	-
	情報通信	21	90.5	28.6	28.6	9.5	-	-	-	-
	医療	8	75.0	50.0	-	-	-	-	-	12.5

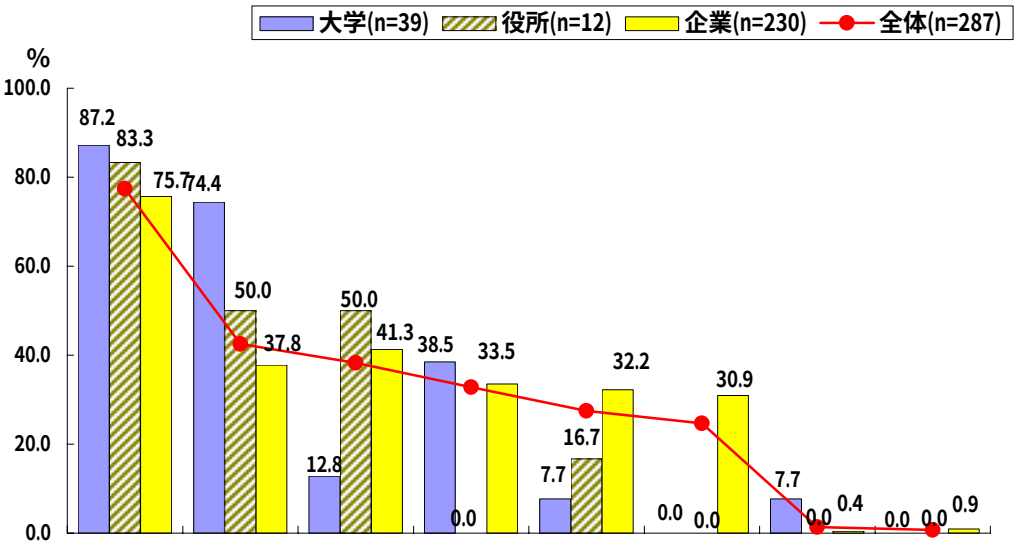
４．外部からの情報システムへのアクセス環境（４／５）

(4)利用目的（MA）（n=287）

●利用目的は「メールサーバーへのアクセス」が77.4%と最も高い。

●大学では、「Ｗｅｂサーバへのアクセス」の割合が全体と比べて74.4%と高い割合になっている。

●役所では、「スケジュール等のグループウエアの利用」の割合が50.0%と全体と比べて高い。



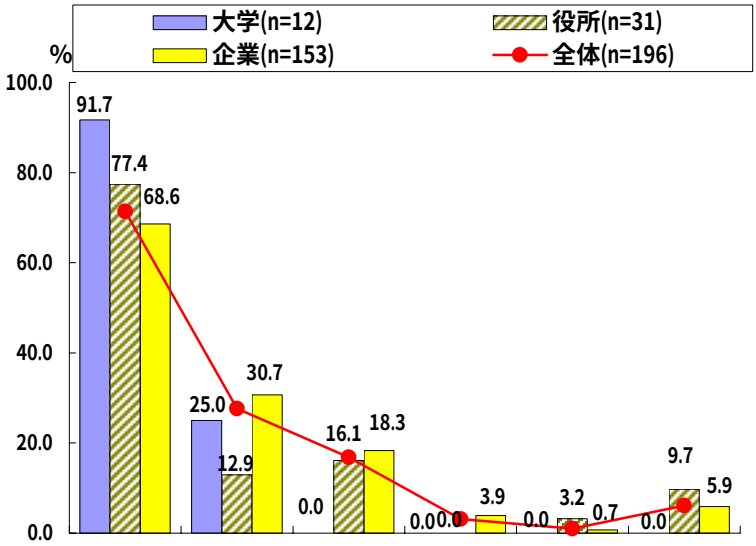
		n	メールサーバーへのアクセス	Webサーバへのアクセス	スケジュール等のグループウエアの利用	情報システムメンテナンス	業務支援システムへのアクセス	営業支援システムへのアクセス	その他	無回答
全体		287	77.4	42.5	38.3	32.8	27.5	24.7	1.4	0.7
大学		39	87.2	74.4	12.8	38.5	7.7	-	7.7	-
役所		12	83.3	50.0	50.0	-	16.7	-	-	-
企業業種別	運輸	5	60.0	80.0	-	-	60.0	-	-	-
	製造	103	84.5	37.9	49.5	35.0	30.1	35.0	1.0	1.0
	サービス	45	80.0	42.2	48.9	44.4	33.3	46.7	-	-
	不動産	14	92.9	42.9	57.1	21.4	35.7	35.7	-	-
特定事業	エネルギー	12	66.7	16.7	41.7	25.0	33.3	16.7	-	-
	交通	6	50.0	16.7	-	16.7	50.0	-	-	-
	金融	15	20.0	33.3	13.3	53.3	6.7	20.0	-	-
	情報通信	21	76.2	38.1	33.3	14.3	33.3	19.0	-	-
	医療	8	50.0	37.5	-	37.5	50.0	-	-	12.5

４．外部からの情報システムへのアクセス環境（５／５）

(5)接続を認めない理由（MA）（n=196）

●「社内システム、情報守るため」が71.4%を占めている。

●大学では、「セキュリティポリシー」が0%となっており、役所、企業との違いが表れている。

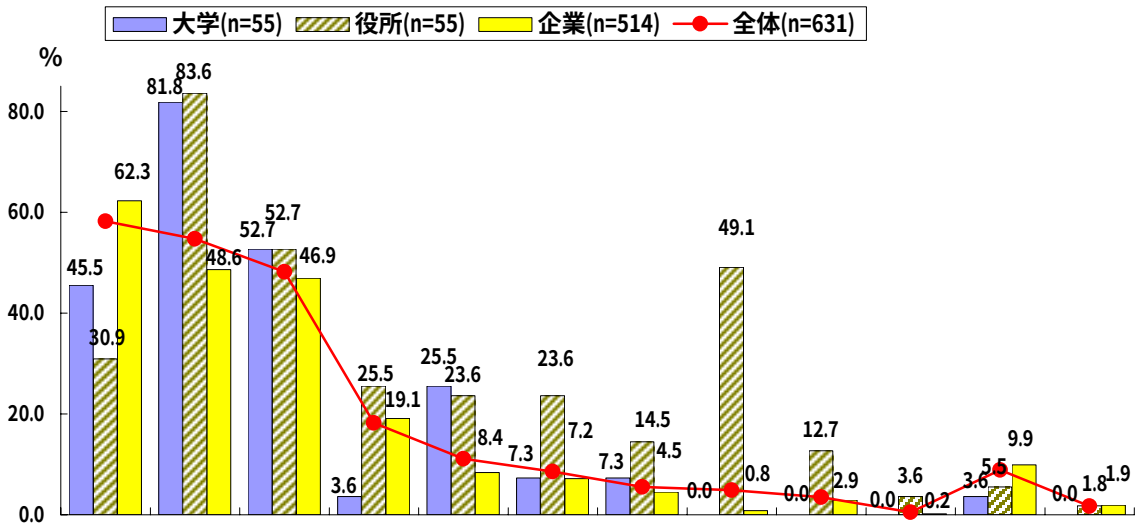


		n	社内システム、情報を守るため	必要がないため	セキュリティポリシー	経費がかかるため	その他	無回答
全体		196	71.4	27.6	16.8	3.1	1.0	6.1
大 学		12	91.7	25.0	-	-	-	-
役 所		31	77.4	12.9	16.1	-	3.2	9.7
企業業種別	運輸	2	50.0	50.0	-	-	-	-
	製造	25	60.0	24.0	20.0	16.0	-	12.0
	サービス	22	81.8	27.3	4.5	4.5	-	4.5
	不動産	3	66.7	33.3	33.3	-	-	-
特定事業	エネルギー	15	73.3	40.0	26.7	-	-	-
	交通	9	33.3	66.7	11.1	11.1	-	11.1
	金融	45	77.8	24.4	31.1	-	-	2.2
	情報通信	11	63.6	27.3	-	-	-	9.1
	医療	20	60.0	35.0	10.0	-	5.0	10.0

５．情報システムの被害（１／２）

(1)社会的に深刻な被害を及ぼす情報システム（MA）（n=631）

●「社会的に被害はないが、自社にとって被害に至るシステムがある」「個人のプライバシーが侵害される情報を扱うシステムがある」の割合が50%を超えている。
特に、大学、役所、特定事業者では、「個人のプライバシーが侵害される情報を扱うシステムがある」の割合が、全体と比べると高くなっている。

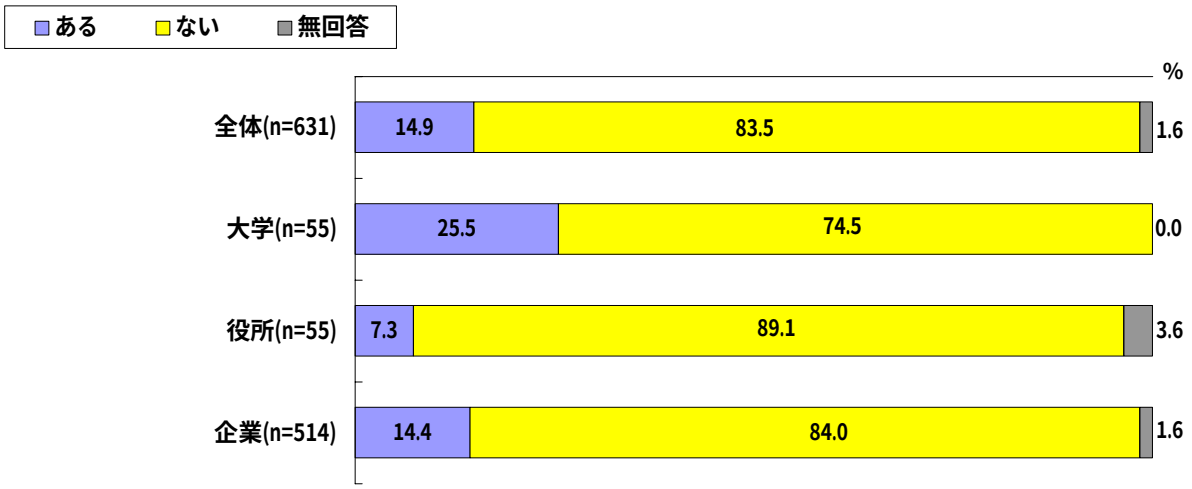


		n	社会的に深刻な被害はないが、自社にとって深刻な被害に至るシステムがある	個人のプライバシーが侵害される情報を扱うシステムがある	情報の改ざんによる信用低下につながるシステムがある	顧客の財産が脅かされるシステムがある	他人になりすますことのできる情報を扱うシステムがある	社会的活動・経済的活動を脅かすシステムがある	人命にかかわるシステムがある	国防や治安維持、行政機能が脅かされるシステムがある	ライフラインやプラントが停止／暴走してしまうシステムがある	その他	深刻な被害となるシステムはない	無回答
全体		631	58.2	54.7	48.2	18.2	11.1	8.6	5.5	4.9	3.5	0.5	8.9	1.7
大 学		55	45.5	81.8	52.7	3.6	25.5	7.3	7.3	-	-	-	3.6	-
役 所		55	30.9	83.6	52.7	25.5	23.6	23.6	14.5	49.1	12.7	3.6	5.5	1.8
企業業種別	運輸	10	70.0	50.0	60.0	40.0	-	-	-	10.0	-	-	-	-
	製造	167	75.4	31.7	38.9	10.2	7.2	3.6	0.6	-	3.0	-	11.4	2.4
	サービス	97	64.9	34.0	44.3	13.4	9.3	2.1	-	-	1.0	-	12.4	3.1
	不動産	25	76.0	40.0	28.0	12.0	-	-	-	-	-	-	8.0	-
	エネルギー	33	33.3	63.6	45.5	24.2	6.1	9.1	-	6.1	18.2	3.0	15.2	-
	交通	23	69.6	39.1	47.8	-	4.3	8.7	-	-	4.3	-	17.4	-
	金融	74	51.4	85.1	71.6	59.5	17.6	20.3	-	-	-	-	2.7	1.4
	情報通信	43	55.8	48.8	58.1	11.6	2.3	11.6	-	-	-	-	14.0	2.3
	医療	39	38.5	87.2	38.5	7.7	12.8	10.3	56.4	2.6	5.1	-	2.6	2.6

５．情報システムの被害（２／２）

(2) 深刻な被害の有無 (n=631)

●全体の14.9%が「深刻な被害があった」と答えている。



		n	ある	ない	無回答
全体		631	14.9	83.5	1.6
大 学		55	25.5	74.5	-
役 所		55	7.3	89.1	3.6
企業業種別	運輸	10	10.0	90.0	-
	製造	167	15	82.0	3.0
	サービス	97	19.6	79.4	1.0
	不動産	25	8	92.0	-
	エネルギー	33	12.1	87.9	-
	交通	23	4.3	95.7	-
	金融	74	10.8	87.8	1.4
	情報通信	43	14	83.7	2.3
	医療	39	20.5	79.5	-

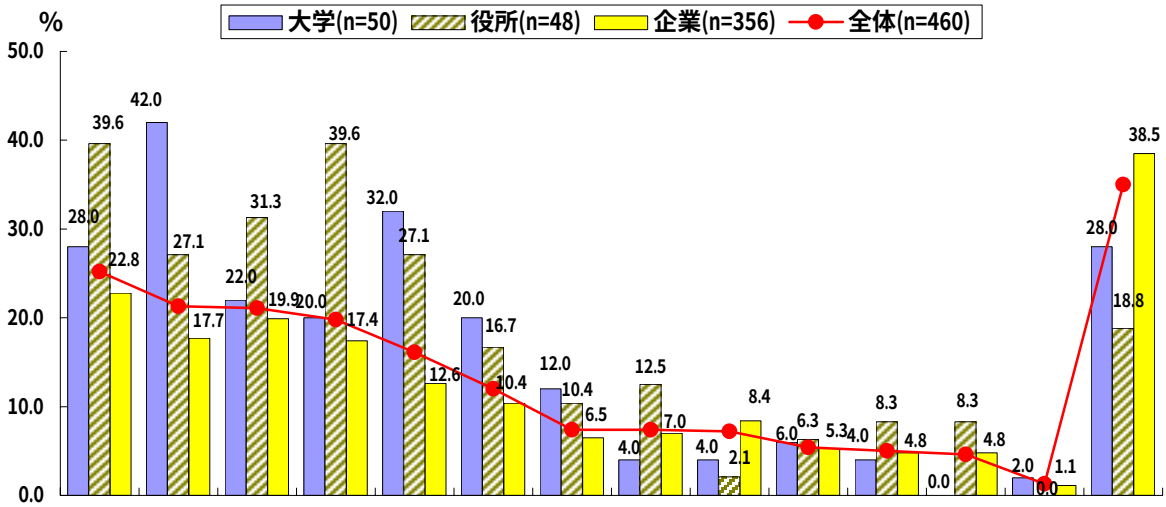
６．情報システムにおける被害対策（１／２）

(1)システム侵入阻止の為のセキュリティ対策（MA）（n=460）

●全体で見ると上位３項目の割合が20%を超えている。

●役所では「他のネットワークとは分離した専用のネットワークを構築している」、「ＩＤとパスワードでユーザ認識」「システムへのアクセスログを取得している」の割合が全体と比べて高くなっている。

●大学では、「ソフトのセキュリティホールに対するパッチやバージョンアップ」の割合が全体と比べて高く、逆に企業では割合が全体に比べて低くなっている。

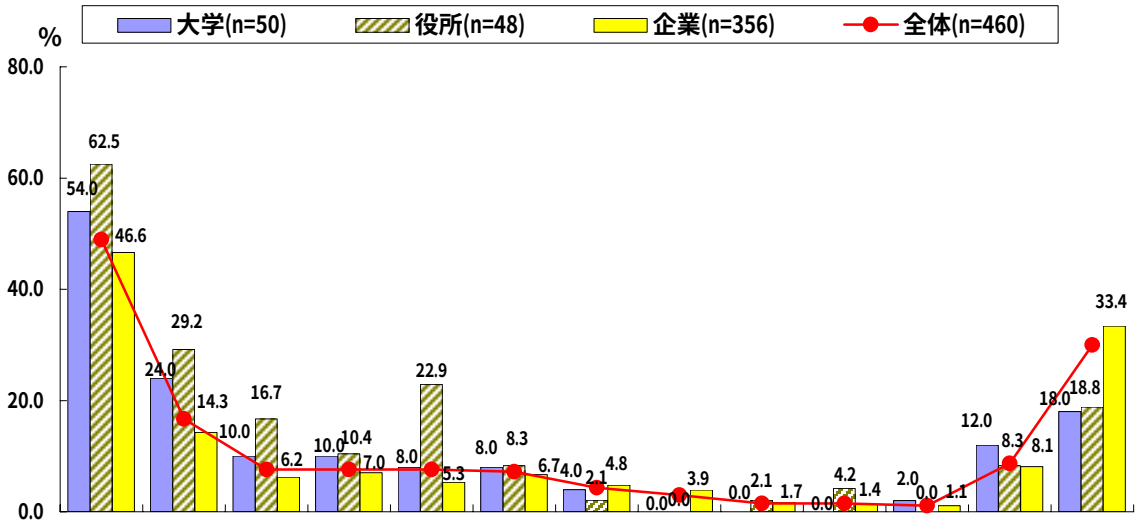


		n	他のネットワークとは分離した専用のネットワークを構築している	ソフトのセキュリティホールに対するパッチやバージョンアップ	ＩＤとパスワードでユーザ認識	システムへのアクセスログを取得している	基幹システム専用のファイアウォールを導入している	ネットワークのアクセスコントロールを行っている	ネットワークには接続していない	不正アクセスを自動的に検出する仕組みを導入している	指定回数以上のログインに失敗すると、失効機能を組み込んでいる	擬似アタックを定期的に行い、対策をチェックしている	通信を暗号化する仕組みを導入している	ＩＤと強化パスワードでユーザ認証をしている	上記のような対策は行っていない	無回答
全体		460	25.2	21.3	21.1	19.8	16.1	12.0	7.4	7.4	7.2	5.4	5.0	4.6	1.3	35.0
大学		50	28.0	42.0	22.0	20.0	32.0	20.0	12.0	4.0	4.0	6.0	4.0	-	2.0	28.0
役所		48	39.6	27.1	31.3	39.6	27.1	16.7	10.4	12.5	2.1	6.3	8.3	8.3	-	18.8
企業業種別	運輸	7	14.3	-	14.3	14.3	14.3	-	-	14.3	-	-	-	-	-	57.1
	製造	94	13.8	19.1	19.1	11.7	7.4	11.7	2.1	5.3	7.4	4.3	4.3	5.3	3.2	51.1
	サービス	57	5.3	21.1	17.5	10.5	10.5	8.8	3.5	8.8	8.8	15.8	3.5	1.8	-	42.1
	不動産	13	7.7	30.8	15.4	15.4	-	-	-	-	7.7	-	-	15.4	-	53.8
	エネルギー	28	39.3	3.6	21.4	10.7	10.7	14.3	14.3	7.1	-	3.6	-	-	-	42.9
	交通	16	25.0	31.3	12.5	12.5	6.3	18.8	6.3	12.5	12.5	-	6.3	6.3	-	37.5
	金融	70	42.9	21.4	30.0	35.7	18.6	20.0	10.0	11.4	15.7	4.3	10.0	10.0	-	22.9
	情報通信	33	18.2	9.1	15.2	21.2	18.2	-	6.1	3.0	6.1	6.1	-	3.0	-	30.3
	医療	36	33.3	13.9	16.7	13.9	22.2	-	13.9	2.8	5.6	-	8.3	-	2.8	22.2

６．情報システムにおける被害対策（２／２）

(2)システムに侵入された場合を想定したセキュリティ対策（MA）（n=460）

●「データのバックアップ対策を行っている」の割合が最も高い。



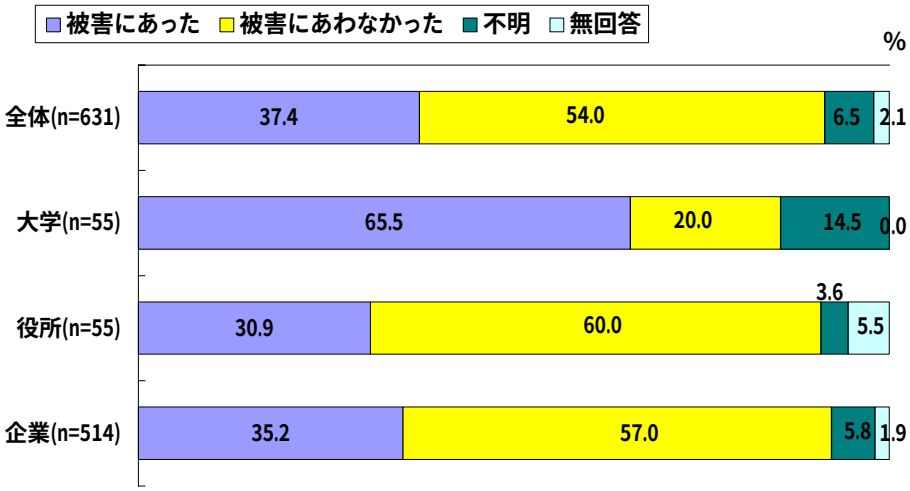
		n	データのバックアップ対策を行っている	システムへのアクセスログを取得している	システムの冗長（二重化等）を行っている	ネットワークの冗長化を行っている	コンソール以外からの設定変更を出来ない設定にしている	不正行為を自動検知するシステムを導入している	重要データを暗号化して送受信	重要データを暗号化して保存	プログラムの改ざんを自動検知するシステムを導入している	緊急時には自動停止する仕組みを導入	データ突合せ確認等の監査プログラムを導入	上記のような対策は行っていない	無回答
全体		460	48.9	16.7	7.6	7.6	7.6	7.2	4.3	3.0	1.5	1.5	1.1	8.7	30.0
大学		50	54.0	24.0	10.0	10.0	8.0	8.0	4.0	-	-	-	2.0	12.0	18.0
役所		48	62.5	29.2	16.7	10.4	22.9	8.3	2.1	-	2.1	4.2	-	8.3	18.8
企業業種別	運輸	7	14.3	14.3	-	-	14.3	14.3	-	-	-	-	-	-	42.9
	製造	94	43.6	11.7	2.1	5.3	2.1	3.2	4.3	3.2	-	1.1	2.1	9.6	38.3
	サービス	57	36.8	8.8	7.0	7.0	3.5	7.0	1.8	1.8	-	-	-	12.3	35.1
	不動産	13	69.2	15.4	-	15.4	7.7	-	-	7.7	-	-	-	-	30.8
	エネルギー	28	39.3	14.3	7.1	3.6	7.1	10.7	-	-	3.6	-	-	10.7	39.3
	交通	16	56.3	18.8	6.3	12.5	-	6.3	-	-	6.3	-	-	6.3	37.5
	金融	70	58.6	27.1	15.7	11.4	10.0	10.0	14.3	12.9	2.9	5.7	2.9	2.9	24.3
	情報通信	33	54.5	9.1	3.0	3.0	6.1	9.1	-	-	3.0	-	-	9.1	24.2
	医療	36	41.7	8.3	2.8	5.6	5.6	5.6	5.6	-	2.8	-	-	11.1	33.3

7．不正アクセス等の被害状況（1／9）

(1) 被害の有無 (n=631)

●「被害にあった」割合が37.4%と昨年度調査の19.8%を大幅に上回った。

●大学では、「被害にあった」割合が65.5%と全体に比べて高くなっている。



		n	被害にあった	被害にあわなかった	不明	無回答
全体		631	37.4	54	6.5	2.1
大 学		55	65.5	20	14.5	-
役 所		55	30.9	60.0	3.6	5.5
企業業種別	運輸	10	30.0	60.0	10.0	-
	製造	167	37.1	50.9	8.4	3.6
	サービス	97	38.1	50.5	9.3	2.1
	不動産	25	40	56.0	4.0	-
	エネルギー	33	30.3	60.6	9.1	-
	交通	23	30.4	65.2	4.3	-
	金融	74	27.0	73.0	-	-
	情報通信	43	41.9	53.5	-	4.7
	医療	39	33.3	64.1	2.6	-

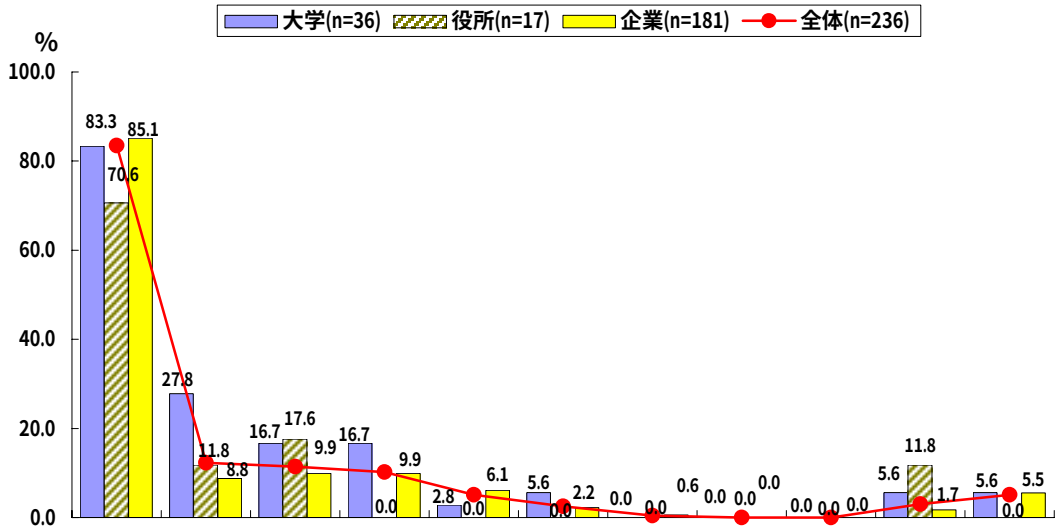
7．不正アクセス等の被害状況（2／9）

(2)発生した被害内容(MA)(n=236)

●「ウイルス感染」の割合が83.5%と最も高く、昨年度調査の55.0%と比べても大幅に増加している。本年におけるウイルス被害の大きさが伺える。

●「ホームページの改ざん」も12.3%と昨年度調査の2.5%を大幅に上回った。

●逆に「踏み台」が11.4%、「メールの不正中継」が10.2%と昨年度調査の27.5%、45.0%から大幅に比率が下がった。



		n	ウイルス感染	ホームページの改ざん	踏み台	メールの不正中継	サービス停止	なりすまし	システム破壊	情報漏洩	盗聴	その他	無回答
全体		236	83.5	12.3	11.4	10.2	5.1	2.5	0.4	-	-	3.0	5.1
大 学		36	83.3	27.8	16.7	16.7	2.8	5.6	-	-	-	5.6	5.6
役 所		17	70.6	11.8	17.6	-	-	-	-	-	-	11.8	-
企業種別	運輸	3	66.7	-	33.3	-	-	-	-	-	-	-	33.3
	製造	62	85.5	16.1	9.7	8.1	4.8	1.6	-	-	-	1.6	4.8
	サービス	37	86.5	10.8	13.5	13.5	10.8	2.7	2.7	-	-	-	5.4
	不動産	10	90.0	-	20.0	10.0	-	-	-	-	-	-	-
特定事業	エネルギー	10	90.0	-	-	-	-	-	-	-	-	-	10.0
	交通	7	85.7	-	-	14.3	-	-	-	-	-	-	-
	金融	20	85.0	5.0	-	15.0	15.0	-	-	-	-	5.0	-
	情報通信	18	77.8	-	16.7	16.7	5.6	11.1	-	-	-	5.6	11.1
	医療	13	84.6	-	7.7	-	-	-	-	-	-	-	7.7

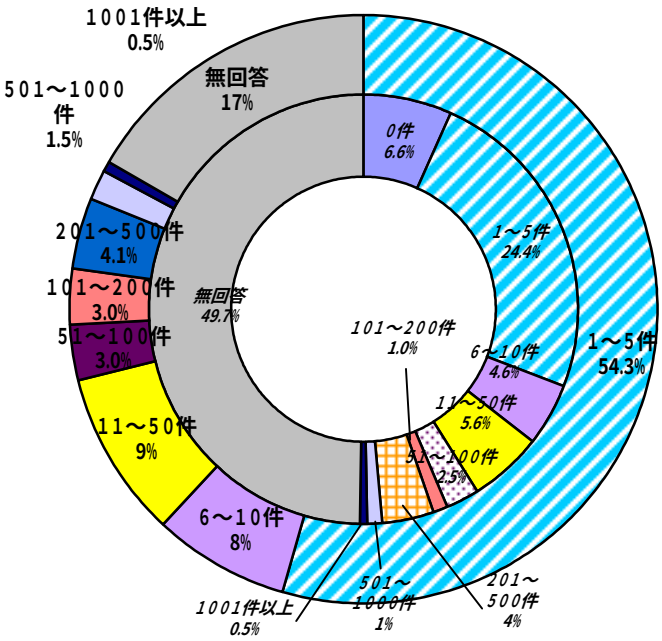
7．不正アクセス等の被害状況（3／9）

(2)発生した被害内容 (MA) (n=236)

●被害にあった内容を見ると、「ウイルス感染」が回答数、被害件数とも最も多い。被害件数の54.3%が1～5件であるが、100件を超える被害があったとの回答も多くあった。

●対策をしていたが被害を受けたとの回答は、「被害有り」回答の内の30～40%であり、残りの60～70%は対策をしていないでの被害と推定できる。また、対策を「している」場合の被害件数は、「していない」場合に比べて明らかに少なくなっている。

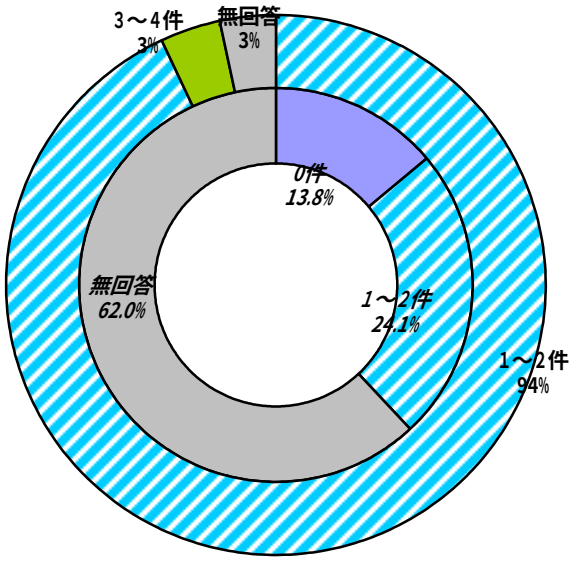
1. ウイルス感染 (n=197)



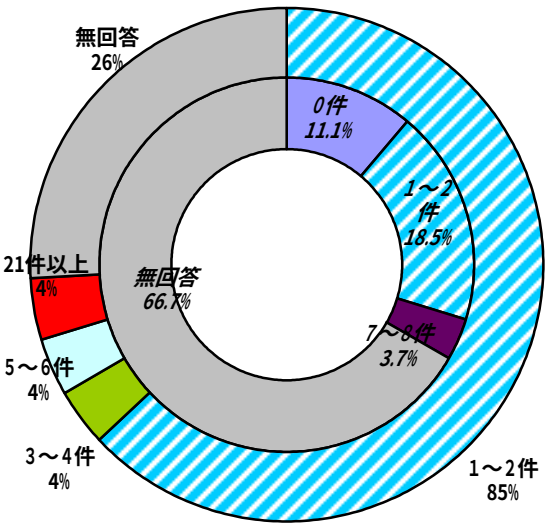
【ドーナグラフの見方】

①グラフは「被害あり」回答数の多い順に掲載している。
②被害内容の右の括弧内のｎ値は「被害あり」の回答数。
③外側ドーナツ
「被害あり」回答における、被害件数区分による比率。
④内側ドーナツ
被害件数の内で何らかの対策をしていた物もの、件数区分比率。
⑤外側／内側ドーナツでは、同じ件数区分は同じ色で示している。
⑤ラベルの文字
標準：外側ドーナツ
斜体：内側ドーナツ
⑥盗聴、情報漏洩は「被害あり」回答が０件であった。掲載なし。

2. ホームページの改ざん (n=29)



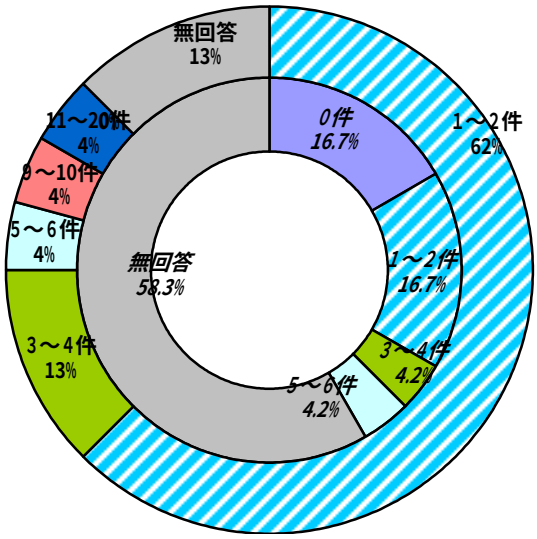
3．踏み台 (n=27)



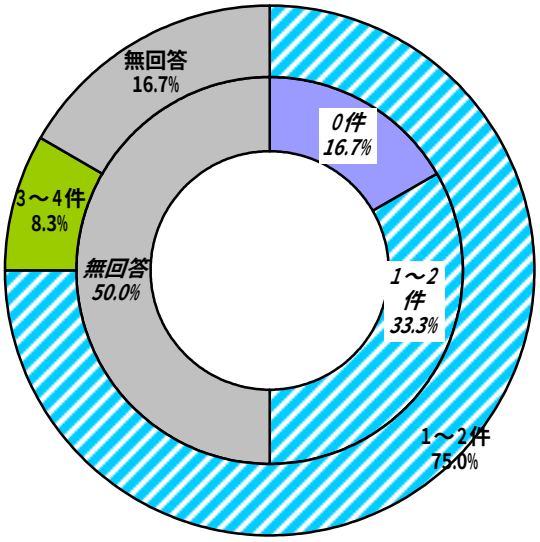
次頁につづく→

→前頁からのつづき

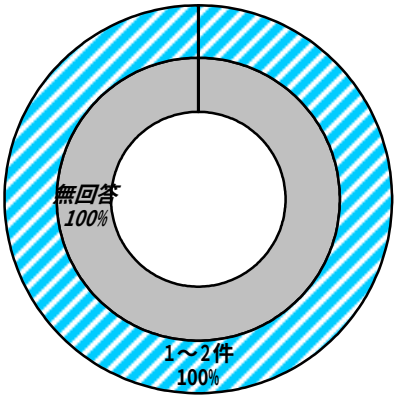
4. メールの不正中継 (n=24)



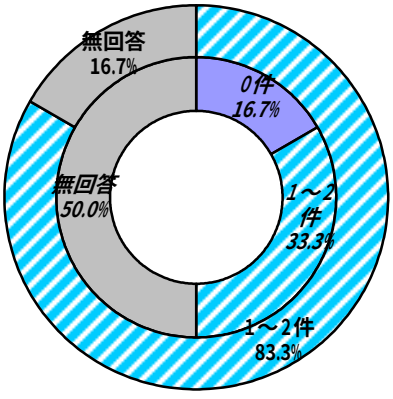
5. サービス停止 (n=12)



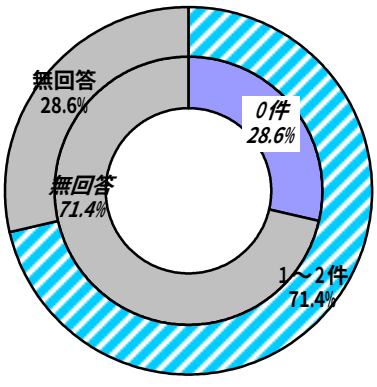
7. システム崩壊 (n=1)



6. なりすまし (n=6)



8. その他 (n=7)



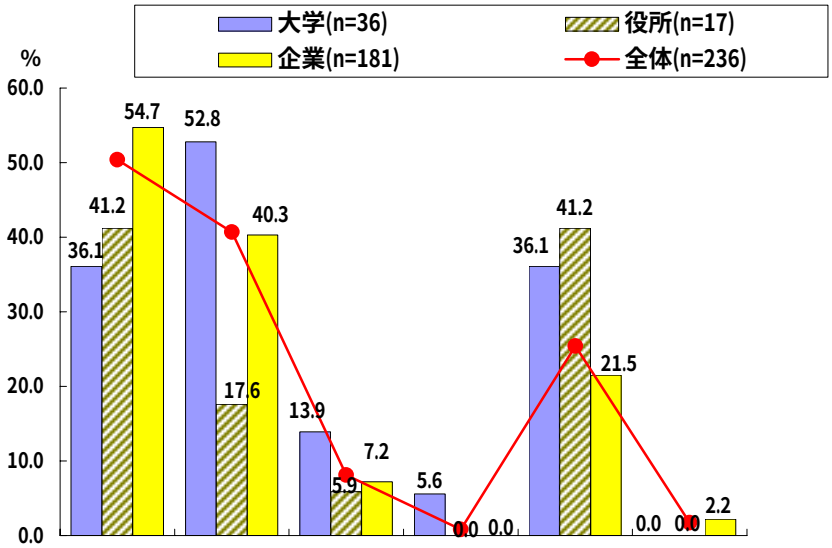
7．不正アクセス等の被害状況（5／9）

(3)不正アクセス等のアクセスもと(MA)

●「社（学）外（国内）から」の割合が50.4%と最も高い。

●企業では、役所では、「社（学）外（国内）から」の割合が全体と比べて比較的高く、逆に大学では、「社（学）外（国外）から」の割合が高くなっている。

●また、「不明」の割合も25.4%となっている。



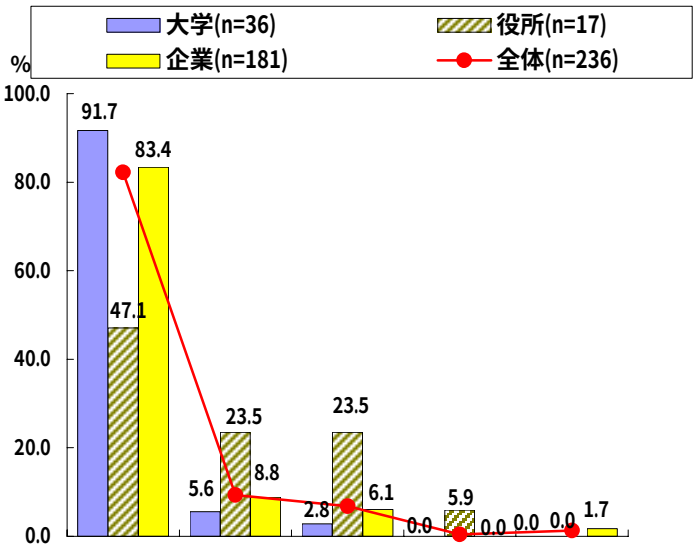
		n	社（学）外から（国内）	社（学）外から（国外）	社（学）内から	その他	不明	無回答
全体		236	50.4	40.7	8.1	0.8	25.4	1.7
大 学		36	36.1	52.8	13.9	5.6	36.1	-
役 所		17	41.2	17.6	5.9	-	41.2	-
企業業種別	運輸	3	33.3	-	-	-	66.7	-
	製造	62	51.6	54.8	11.3	-	17.7	1.6
	サービス	37	51.4	37.8	5.4	-	24.3	-
	不動産	10	60.0	30.0	10.0	-	20.0	-
特定事業	エネルギー	10	50.0	30.0	20.0	-	40.0	10.0
	交通	7	57.1	57.1	14.3	-	14.3	-
	金融	20	70.0	30.0	-	-	10.0	-
	情報通信	18	61.1	33.3	-	-	22.2	5.6
	医療	13	46.2	23.1	-	-	30.8	7.7

7．不正アクセス等の被害状況（6／9）

(4)被害時の対応（MA）（n=236）

●「自社（自校）で対応」の割合が82.2%を占めている。

●役所では、「自社（自校）で対応」の割合が47.1%と全体に比べ低くなっており、逆に「専門業者への相談」「専門業者へのアウトソーシング」の割合が全体に比べて高くなっている。



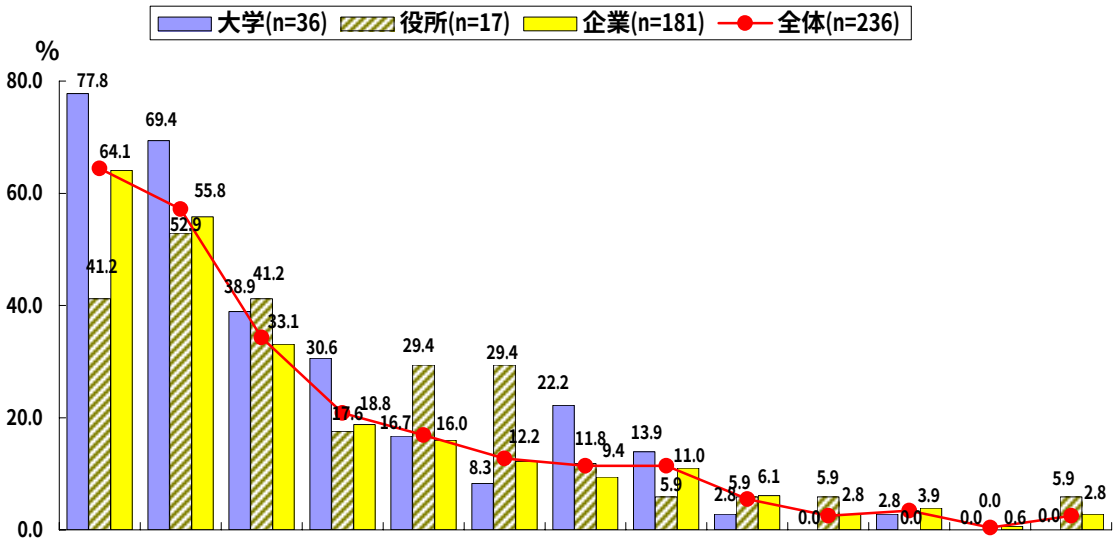
		n	自社（自校）で対応	専門業者への相談	専門業者へのアウトソーシング	対応はとっていない	無回答
全体		236	82.2	9.3	6.8	0.4	1.3
	大　学	36	91.7	5.6	2.8	-	-
	役　所	17	47.1	23.5	23.5	5.9	-
企業種別	運輸	3	66.7	33.3	-	-	-
	製造	62	91.9	4.8	3.2	-	-
	サービス	37	83.8	8.1	8.1	-	-
	不動産	10	80.0	-	20.0	-	-
特定事業	エネルギー	10	60.0	10.0	20.0	-	10.0
	交通	7	100.0	-	-	-	-
	金融	20	95.0	5.0	-	-	-
	情報通信	18	72.2	16.7	5.6	-	5.6
	医療	13	61.5	23.1	7.7	-	7.7

7．不正アクセス等の被害状況（7／9）

(5)被害後に実施したセキュリティ対策(MA)(n=236)

●「ウイルス対策製品の導入／強化」の割合が64.4%と最も高く、昨年度調査の22.5%を大幅に上回った。今年度のウイルス被害の多さが表れているものと思われる。

●また、「最新パッチの適応」が57.2%、「ソフトウェアのバージョンアップ」が　34.3%、「不必要なサービスの停止」が20.8%、「ファイアウォールの設置／強化」が16.9%と、昨年度調査の37.5%、30.0%、26.3%、10.0%を上回り、何らかの対策を講じる所が増えている。



		n	ウイルス対策製品の導入／強化	最新パッチの適応	ソフトウェアのバージョンアップ	不必要なサービスの停止	ファイアウォールの設置／強化	システム上にセキュリティホールがないか検査、診断	セキュリティポリシーの策定、見直し	不正アクセスが行われていないかネットワークの監視	ネットワークの再構築	認証機能の導入／強化	その他	不明	無回答
全体		236	64.4	57.2	34.3	20.8	16.9	12.7	11.4	11.4	5.5	2.5	3.4	0.4	2.5
大学		36	77.8	69.4	38.9	30.6	16.7	8.3	22.2	13.9	2.8	-	2.8	-	-
役所		17	41.2	52.9	41.2	17.6	29.4	29.4	11.8	5.9	5.9	5.9	-	-	5.9
企業業種別	運輸	3	-	66.7	-	33.3	33.3	66.7	33.3	33.3	-	-	-	-	-
	製造	62	66.1	54.8	33.9	19.4	14.5	12.9	11.3	8.1	6.5	3.2	4.8	-	1.6
	サービス	37	59.5	67.6	32.4	27.0	16.2	13.5	16.2	13.5	5.4	5.4	5.4	-	-
	不動産	10	60.0	60.0	30.0	30.0	20.0	10.0	-	20.0	-	-	-	-	-
特定事業	エネルギー	10	80.0	60.0	20.0	-	20.0	-	-	-	-	-	-	-	10.0
	交通	7	71.4	42.9	28.6	14.3	28.6	-	14.3	-	14.3	-	14.3	-	-
	金融	20	65.0	45.0	35.0	5.0	25.0	20.0	-	15.0	5.0	-	-	-	-
	情報通信	18	61.1	55.6	38.9	27.8	5.6	5.6	11.1	16.7	11.1	5.6	5.6	5.6	11.1
	医療	13	69.2	38.5	38.5	7.7	7.7	-	-	-	7.7	-	-	-	7.7

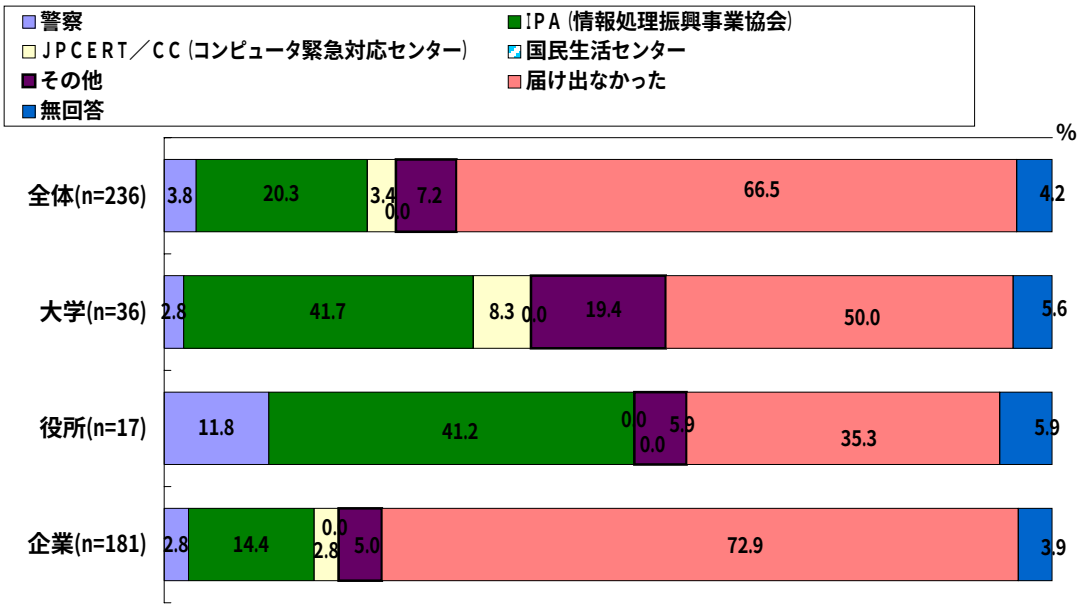
7．不正アクセス等の被害状況（8／9）

(6)被害の届け出状況 (n=236)

●66.5%が「届けなかった」と回答している。

●届け出をしたという回答の中では、「ＩＰＡ（情報処理振興事業協会）」の割合が20.3%と最も高くなっている。

●特定事業者の情報通信では、「警察」の割合が22.2%、「ＩＰＡ（情報処理振興事業協会）」の割合が0%、と他と違う傾向が見られる。

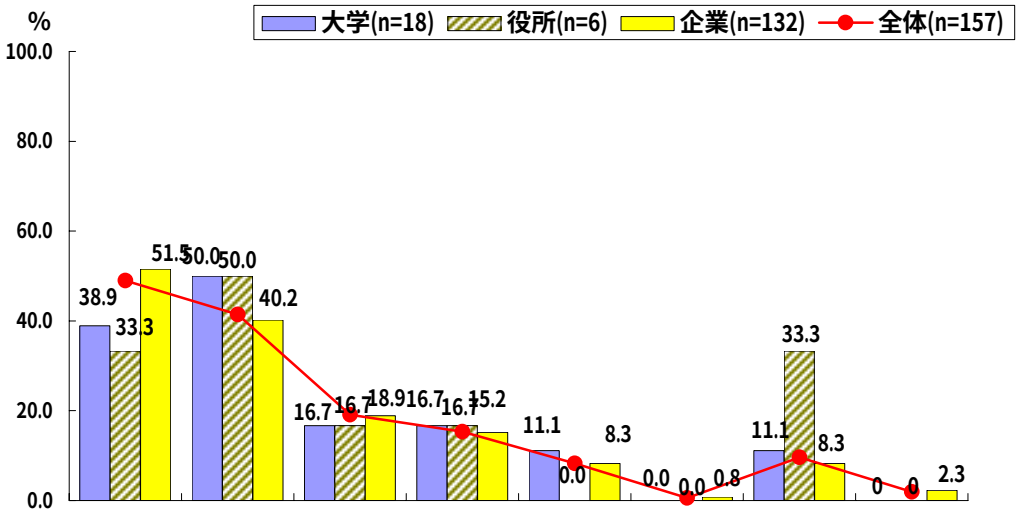


		n	警察	IPA（情報処理振興事業協会）	JPCERT／CC（コンピュータ緊急対応センター）	国民生活センター	その他	届け出なかった	無回答
全体		236	3.8	20.3	3.4	-	7.2	66.5	4.2
大 学		36	2.8	41.7	8.3	-	19.4	50.0	5.6
役 所		17	11.8	41.2	-	-	5.9	35.3	5.9
企業種別	運輸	3	-	33.3	-	-	-	66.7	-
	製造	62	-	9.7	3.2	-	3.2	83.9	1.6
	サービス	37	-	13.5	5.4	-	8.1	70.3	2.7
	不動産	10	-	40.0	-	-	-	60.0	-
特定事業	エネルギー	10	-	10.0	-	-	-	70.0	20.0
	交通	7	-	42.9	-	-	-	57.1	-
	金融	20	5.0	30.0	5.0	-	-	70.0	-
	情報通信	18	22.2	-	-	-	16.7	50.0	11.1
	医療	13	-	-	-	-	7.7	84.6	7.7

7．不正アクセス等の被害状況（9／9）

(7)届けなかった理由（MA）（n=157）

●届けなかった理由として「大した被害ではなかったので」「社内（学内）で対応できたので」の割合が40%以上になっている。

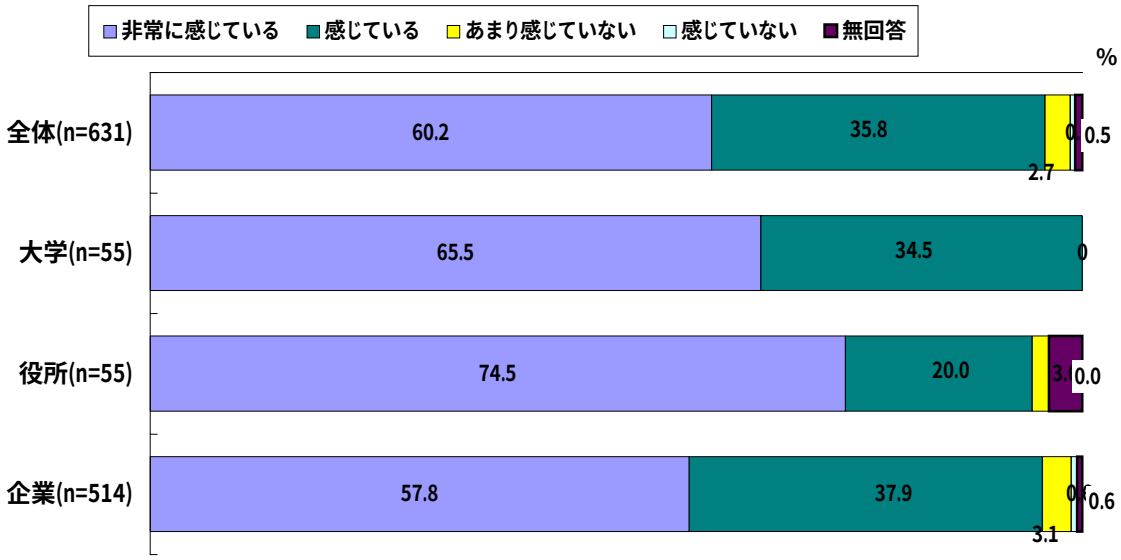


		n	大した被害ではなかったので	社内（学内）で対応できたので	問題解決にならないので	届け出義務がないので	面倒なので	企業（学校）の評判が悪くなるので	その他	無回答
全体		157	49.0	41.4	19.1	15.3	8.3	0.6	9.6	1.9
	大 学	18	38.9	50.0	16.7	16.7	11.1	-	11.1	-
	役 所	6	33.3	50.0	16.7	16.7	-	-	33.3	-
企業業種別	運輸	2	50.0	-	50.0	-	-	-	-	-
	製造	52	55.8	42.3	23.1	15.4	13.5	-	9.6	1.9
	サービス	26	42.3	42.3	26.9	7.7	-	3.8	3.8	3.8
	不動産	6	66.7	16.7	-	33.3	16.7	-	-	-
特定事業	エネルギー	7	42.9	42.9	42.9	28.6	14.3	-	-	14.3
	交通	4	50.0	25.0	25.0	50.0	25.0	-	-	-
	金融	14	57.1	57.1	-	-	-	-	14.3	-
	情報通信	9	22.2	44.4	-	11.1	11.1	-	22.2	-
	医療	11	63.6	27.3	9.1	27.3	-	-	9.1	-

８．セキュリティ対策状況（１／11）

(1)情報セキュリティの必要性 (n=631)

●情報セキュリティの必要性では「情報セキュリティの必要性を感じている」との回答が90%以上になっている。

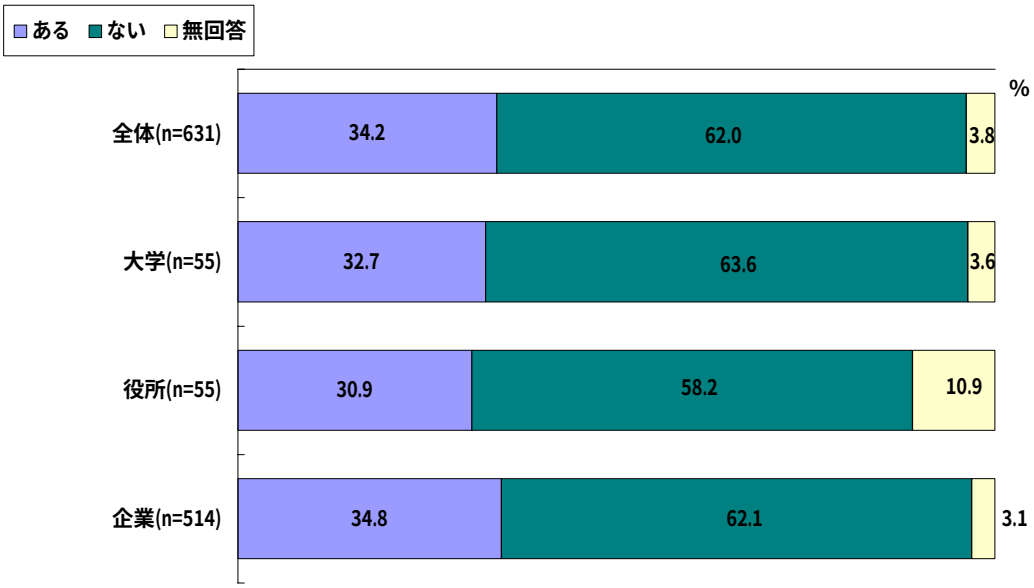


		n	非常に感じている	感じている	あまり感じていない	感じていない	無回答
全体		631	60.2	35.8	2.7	0.5	0.8
大 学		55	65.5	34.5	-	-	-
役 所		55	74.5	20.0	1.8	-	3.6
企業業種別	運輸	10	70.0	20.0	10.0	-	-
	製造	167	52.7	42.5	3.6	-	1.2
	サービス	97	44.3	51.5	3.1	-	1.0
	不動産	25	56	44.0	-	-	-
	エネルギー	33	48.5	51.5	-	-	-
	交通	23	43.5	47.8	8.7	-	-
	金融	74	79.7	18.9	1.4	-	-
	情報通信	43	72.1	25.6	2.3	-	-
	医療	39	66.7	20.5	5.1	7.7	-

８．セキュリティ対策状況（２／11）

(2) 情報セキュリティの為の運用・組織のための組織の有無 (n=631)

●管理組織の有無では60%以上が「組織がない」と回答している。

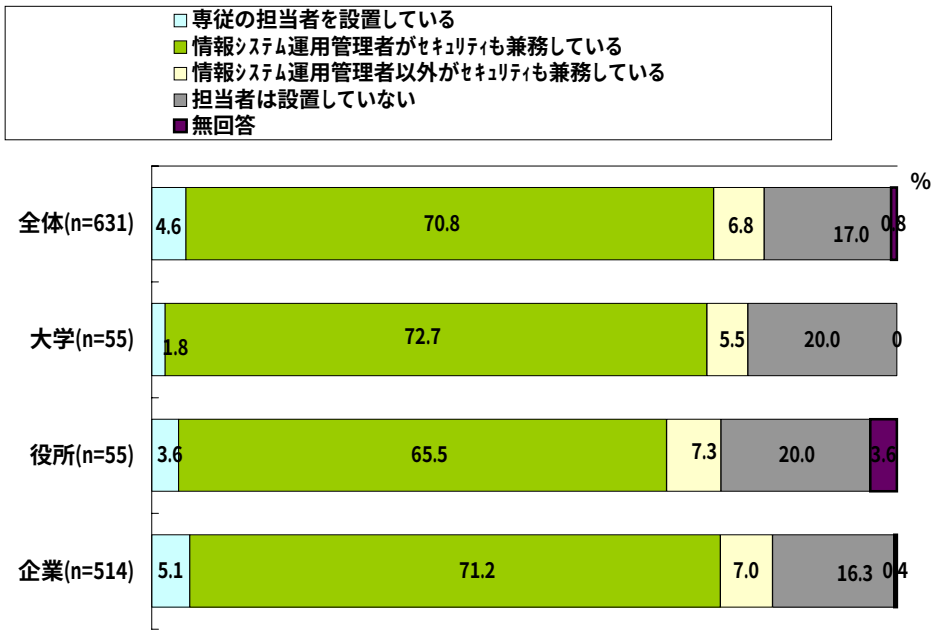


		n	ある	ない	無回答
全体		631	34.2	62	3.8
大 学		55	32.7	63.6	3.6
役 所		55	30.9	58.2	10.9
企業業種別	運輸	10	50.0	50.0	-
	製造	167	27.5	67.1	5.4
	サービス	97	33	66.0	1.0
	不動産	25	40	60.0	-
	エネルギー	33	36.4	57.6	6.1
	交通	23	21.7	78.3	-
	金融	74	51.4	44.6	4.1
	情報通信	43	44.2	55.8	-
	医療	39	30.8	66.7	2.6

8．セキュリティ対策状況（3／11）

(3)管理者、担当者の設置状況 (n=631)

●管理者または担当者では「情報システム運用管理者がセキュリティも兼務している」の割合が70.8%を占めている。

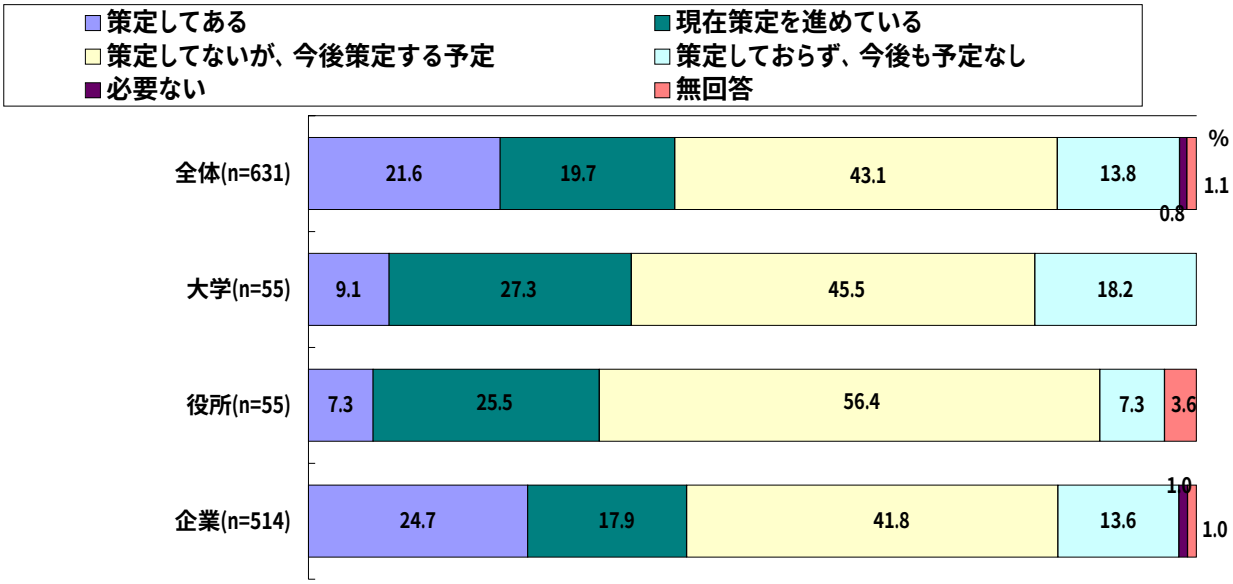


		n	専従の担当者を設置している	情報システム運用管理者がセキュリティも兼務している	情報システム運用管理者以外がセキュリティも兼務している	担当者は設置していない	無回答
全体		631	4.6	70.8	6.8	17	0.8
大 学		55	1.8	72.7	5.5	20	-
役 所		55	3.6	65.5	7.3	20.0	3.6
企業種別	運輸	10	-	90.0	-	10.0	-
	製造	167	4.2	75.4	5.4	13.8	1.2
	サービス	97	4.1	76.3	3.1	16.5	-
	不動産	25	-	88.0	4.0	8.0	-
	エネルギー	33	9.1	60.6	12.1	18.2	-
	交通	23	-	65.2	4.3	30.4	-
	金融	74	8.1	60.8	21.6	9.5	-
	情報通信	43	7	76.7	2.3	14.0	-
	医療	39	7.7	48.7	2.6	41.0	-

8．セキュリティ対策状況（4／11）

(4) 情報セキュリティの為のセキュリティポリシーの策定状況 (n=631)

●セキュリティポリシーの策定状況は「策定済み」、「策定中」が41.3%であるが、「策定してないが、今後策定する予定」を含めると84.4%に達している。昨年度調査では54.4%でありセキュリティポリシー策定の必要性に対する認識が向上していることが伺える。

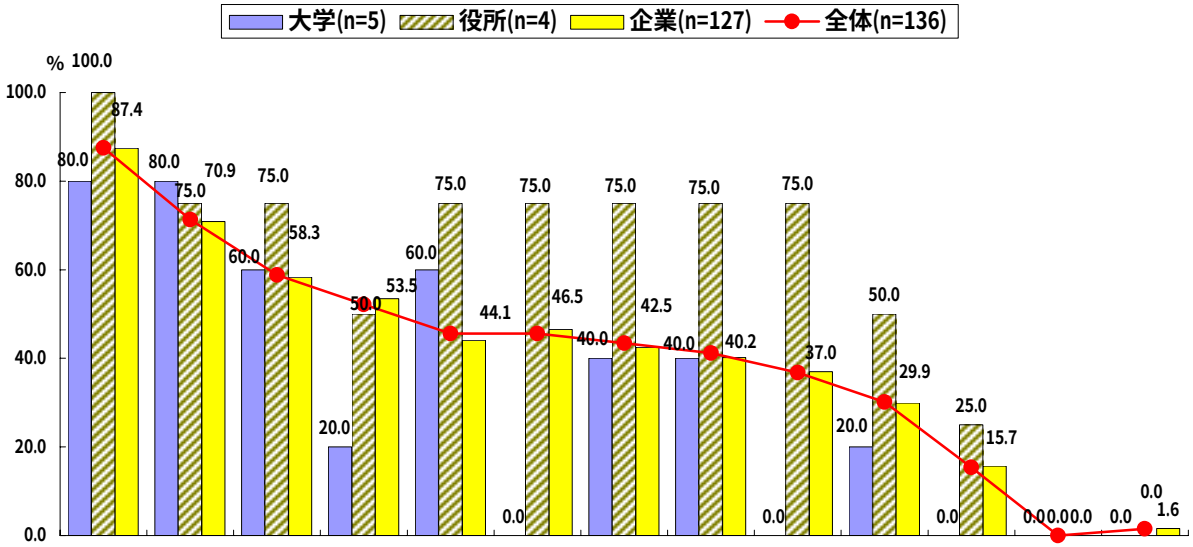


		n	策定してある	現在策定を進めている	策定してないが、今後策定する予定	策定しておらず、今後も予定なし	必要ない	無回答
全体		631	21.6	19.7	43.1	13.8	0.8	1.1
大 学		55	9.1	27.3	45.5	18.2	-	-
役 所		55	7.3	25.5	56.4	7.3	-	3.6
企業種別	運輸	10	40.0	10.0	20.0	20.0	10.0	-
	製造	167	19.2	24.6	38.9	14.4	-	3.0
	サービス	97	20.6	17.5	47.4	14.4	-	-
	不動産	25	12	36.0	48.0	4.0	-	-
	エネルギー	33	30.3	6.1	48.5	15.2	-	-
	交通	23	8.7	17.4	39.1	30.4	4.3	-
	金融	74	55.4	10.8	27.0	6.8	-	-
	情報通信	43	14	14.0	58.1	9.3	4.7	-
	医療	39	23.1	7.7	46.2	20.5	2.6	-

８．セキュリティ対策状況（５／11）

(5)セキュリティポリシーでの規定事項(MA)(n=136)

●全体で見ると、「情報セキュリティの基本方針」が最も高く87.5%、次いで「情報システムの運用管理規定」「情報セキュリティ管理組織」の順となっている。

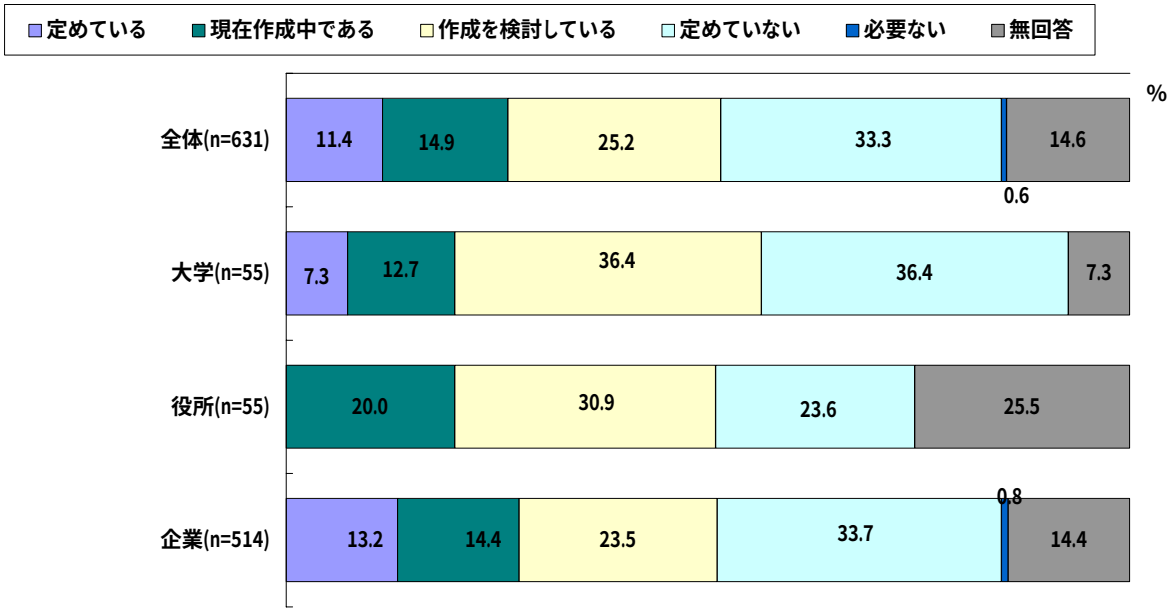


	n	情報セキュリティの基本方針	情報システムの運用管理規定	情報セキュリティ管理組織	情報資産（データ）の分類・管理規準	情報セキュリティ教育	情報システムの設置環境	重要情報へのアクセスの管理規定	非常事態発生時における応対	システム開発及びメンテナンス	セキュリティ監査の基準	法的要求への対応	その他	無回答
全体	136	87.5	71.3	58.8	52.2	45.6	45.6	43.4	41.2	36.8	30.1	15.4	-	1.5
大学	5	80.0	80.0	60.0	20.0	60.0	-	40.0	40.0	-	20.0	-	-	-
役所	4	100.0	75.0	75.0	50.0	75.0	75.0	75.0	75.0	75.0	50.0	25.0	-	-
企業業種別 運輸	4	100.0	75.0	25.0	25.0	-	50.0	25.0	25.0	25.0	-	-	-	-
企業業種別 製造	32	87.5	59.4	46.9	40.6	46.9	43.8	31.3	25.0	21.9	31.3	9.4	-	6.3
企業業種別 サービス	20	80.0	80.0	45.0	45.0	25.0	40.0	45.0	25.0	35.0	20.0	15.0	-	-
企業業種別 不動産	3	100.0	100.0	33.3	33.3	33.3	66.7	33.3	66.7	66.7	33.3	-	-	-
企業業種別 エネルギー	10	70.0	70.0	60.0	50.0	20.0	40.0	40.0	20.0	30.0	10.0	20.0	-	-
企業業種別 交通	2	100.0	50.0	50.0	-	50.0	50.0	50.0	50.0	50.0	-	50.0	-	-
企業業種別 金融	41	95.1	75.6	90.2	87.8	61.0	58.5	56.1	61.0	53.7	48.8	22.0	-	-
企業業種別 情報通信	6	66.7	66.7	16.7	16.7	50.0	16.7	33.3	50.0	16.7	33.3	-	-	-
企業業種別 医療	9	88.9	66.7	33.3	22.2	44.4	33.3	33.3	44.4	33.3	-	22.2	-	-

８．セキュリティ対策状況（６／11）

(6)セキュリティガイドラインの制定 (n=631)

●ガイドラインの制定では「作成を検討している」を含めると51.5%になっている。

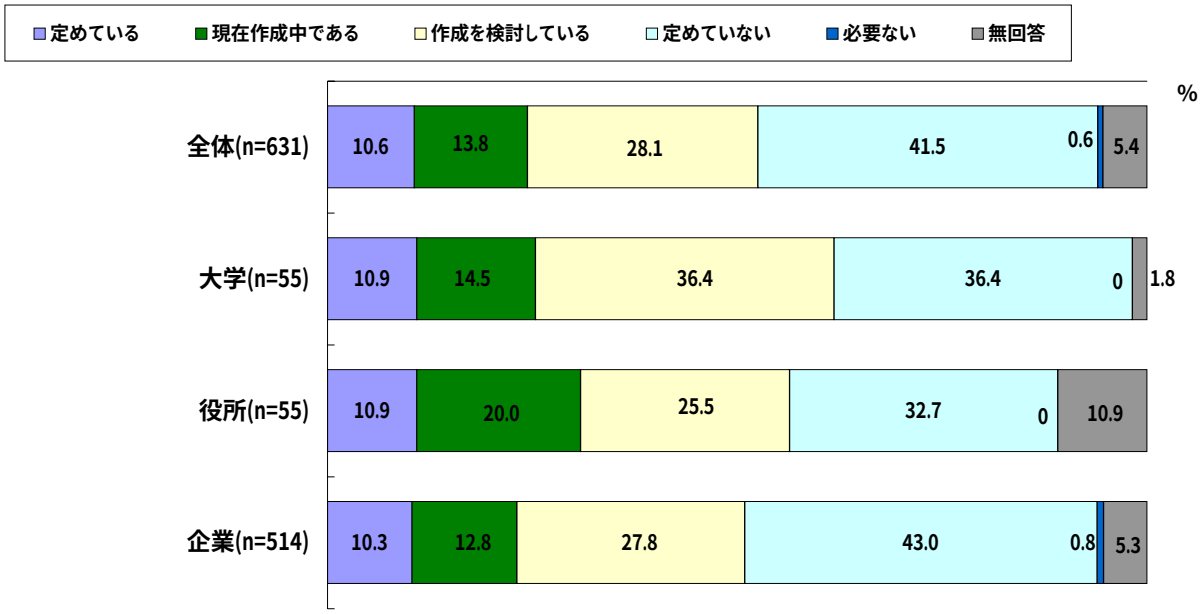


		n	定めている	現在作成中である	作成を検討している	定めていない	必要ない	無回答
全体		631	11.4	14.9	25.2	33.3	0.6	14.6
大 学		55	7.3	12.7	36.4	36.4	-	7.3
役 所		55	-	20.0	30.9	23.6	-	25.5
企業業種別	運輸	10	20.0	10.0	10.0	40.0	-	20.0
	製造	167	7.8	19.2	23.4	33.5	-	16.2
	サービス	97	6.2	15.5	24.7	39.2	1.0	13.4
	不動産	25	8	20.0	28.0	20.0	-	24.0
	エネルギー	33	15.2	9.1	15.2	51.5	3.0	6.1
	交通	23	-	4.3	21.7	39.1	4.3	30.4
	金融	74	47.3	14.9	21.6	12.2	-	4.1
	情報通信	43	7	9.3	20.9	44.2	-	18.6
	医療	39	5.1	2.6	35.9	41.0	2.6	12.8

８．セキュリティ対策状況（７／11）

(7)非常事態発生時の応対計画 (n=631)

●非常事態発生時の応対計画の制定では「定めていない」が41.5%を占めている。



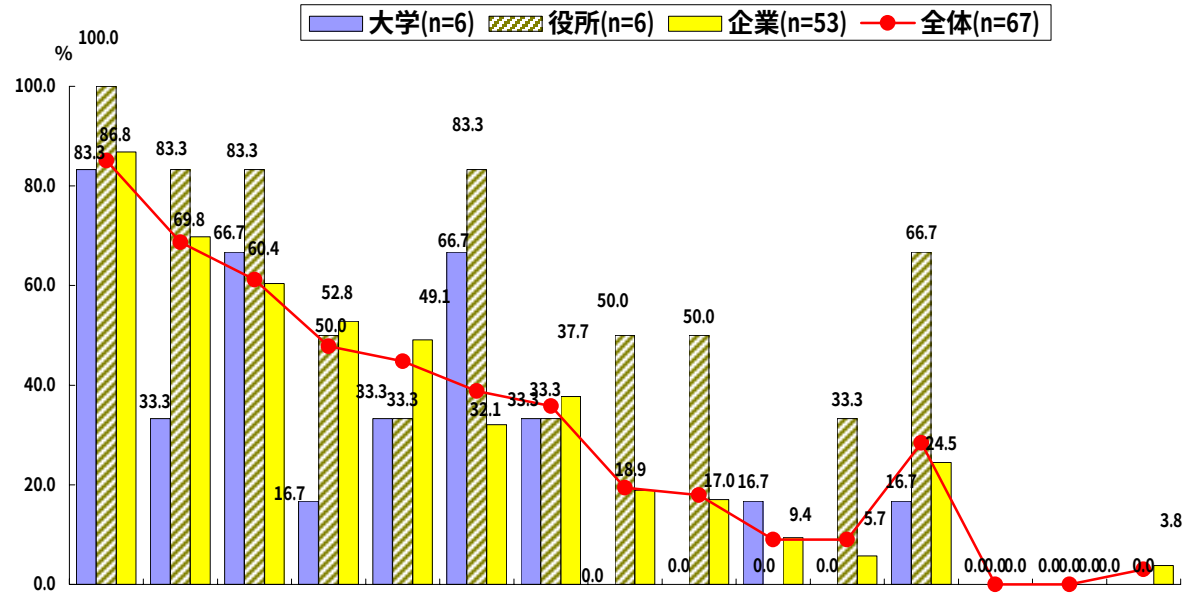
		n	定めている	現在作成中である	作成を検討している	定めていない	必要ない	無回答
全体		631	10.6	13.8	28.1	41.5	0.6	5.4
大 学		55	10.9	14.5	36.4	36.4	-	1.8
役 所		55	10.9	20.0	25.5	32.7	-	10.9
企業業種別	運輸	10	30.0	10.0	30.0	20.0	-	10.0
	製造	167	7.2	15.0	26.3	43.1	-	8.4
	サービス	97	5.2	11.3	26.8	50.5	1.0	5.2
	不動産	25	-	28.0	36.0	24.0	-	12.0
	エネルギー	33	9.1	12.1	15.2	60.6	3.0	-
	交通	23	-	13.0	30.4	47.8	4.3	4.3
	金融	74	31.1	12.2	33.8	21.6	-	1.4
	情報通信	43	7	11.6	30.2	46.5	-	4.7
	医療	39	10.3	-	28.2	59.0	2.6	-

８．セキュリティ対策状況（８／11）

(8)非常事態における応対計画の内容（MA）（n=67）

●全体で見ると、「社内報告経路・指揮系統」が最も高く85.1%。次いで「回復・復旧手順」「原因の究明」の順となっている。

●役所では非常事態における対応計画が細かに規定される傾向にある。

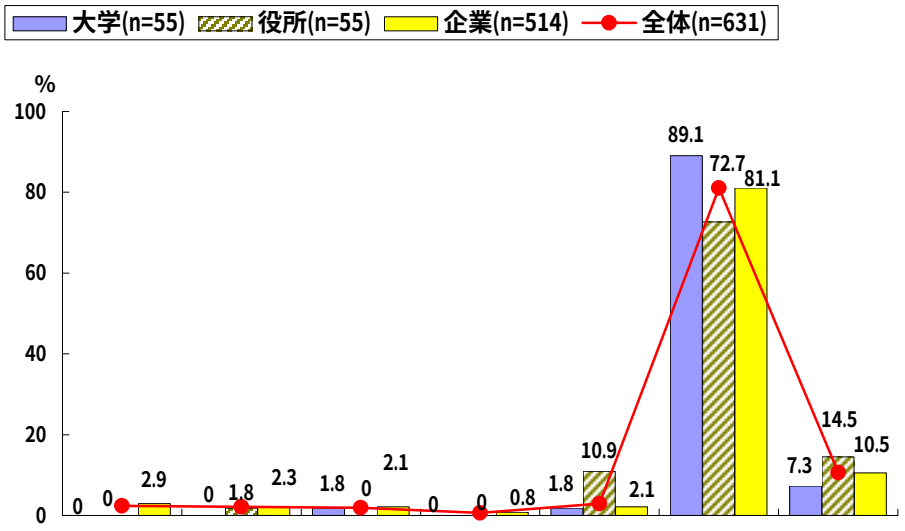


		n	社内報告経路・指揮系統	回復・復旧手順	原因の究明	システムの縮退、代替運用手順	サービス利用者への広報活動	証拠（状況・ログ等）の保全	サービス停止の判断基準	マスコミへの広報活動	警察への連絡	犯人の追及	JPCERT／CCへの連絡	その他関連機関への連絡	上記のような事項は記載されていない	その他	無回答
全体		67	85.1	68.7	61.2	47.8	44.8	38.8	35.8	19.4	17.9	9.0	9.0	28.4	-	-	3.0
大学		6	83.3	33.3	66.7	16.7	33.3	66.7	33.3	-	-	16.7	-	16.7	-	-	-
役所		6	100.0	83.3	83.3	50.0	33.3	83.3	33.3	50.0	50.0	-	33.3	66.7	-	-	-
企業業種別	運輸	3	66.7	100.0	66.7	66.7	-	33.3	33.3	-	33.3	33.3	33.3	-	-	-	-
	製造	12	100.0	58.3	75.0	25.0	75.0	41.7	41.7	8.3	8.3	8.3	8.3	8.3	-	-	-
	サービス	5	80.0	60.0	60.0	80.0	40.0	20.0	60.0	-	-	20.0	-	-	-	-	20.0
	不動産	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	エネルギー	3	100.0	66.7	66.7	66.7	33.3	66.7	33.3	-	33.3	-	-	33.3	-	-	-
	交通	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	金融	23	87.0	78.3	52.2	52.2	47.8	26.1	30.4	39.1	26.1	4.3	4.3	47.8	-	-	4.3
	情報通信	3	100.0	66.7	100.0	33.3	66.7	33.3	33.3	-	-	33.3	-	-	-	-	-
	医療	4	50.0	50.0	25.0	100.0	25.0	25.0	50.0	-	-	-	-	-	-	-	-

８．セキュリティ対策状況（9／11）

(9)第三者機関による評価・認証の取得状況（MA）（n=631）

●「取得の予定なし」の割合が81.1%と非常に高い。

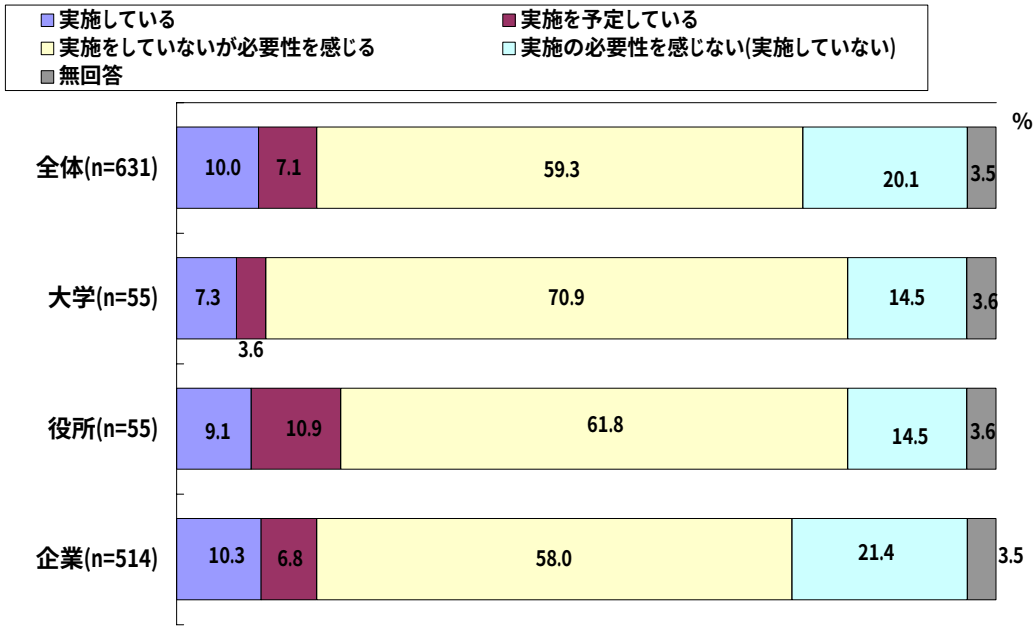


		n	プライバシーマーク	ISMS	BS7799	ISO15408	その他	取得の予定なし	無回答
全体		631	2.4	2.1	1.9	0.6	2.9	81.1	10.6
大 学		55	-	-	1.8	-	1.8	89.1	7.3
役 所		55	-	1.8	-	-	10.9	72.7	14.5
企業業種別	運輸	10	10.0	-	10.0	-	-	50.0	30.0
	製造	167	2.4	1.8	4.2	1.2	3.6	77.2	13.8
	サービス	97	1.0	5.2	1.0	2.1	4.1	79.4	7.2
	不動産	25	4.0	4.0	4.0	-	-	76.0	12.0
	エネルギー	33	-	3.0	-	-	-	93.9	3.0
	交通	23	4.3	-	4.3	-	-	87.0	8.7
	金融	74	4.1	-	-	-	-	86.5	9.5
	情報通信	43	7.0	4.7	-	-	2.3	83.7	7.0
	医療	39	2.6	-	-	-	-	87.2	10.3

８．セキュリティ対策状況（10／11）

(10)セキュリティ監査に対する取り組み (n=631)

●セキュリティ監査に対する取り組みでは、「実施している」「実施予定」を合わせても17.1%に留まっているが、「実施の必要性を感じている」の割合が59.3%と高い。

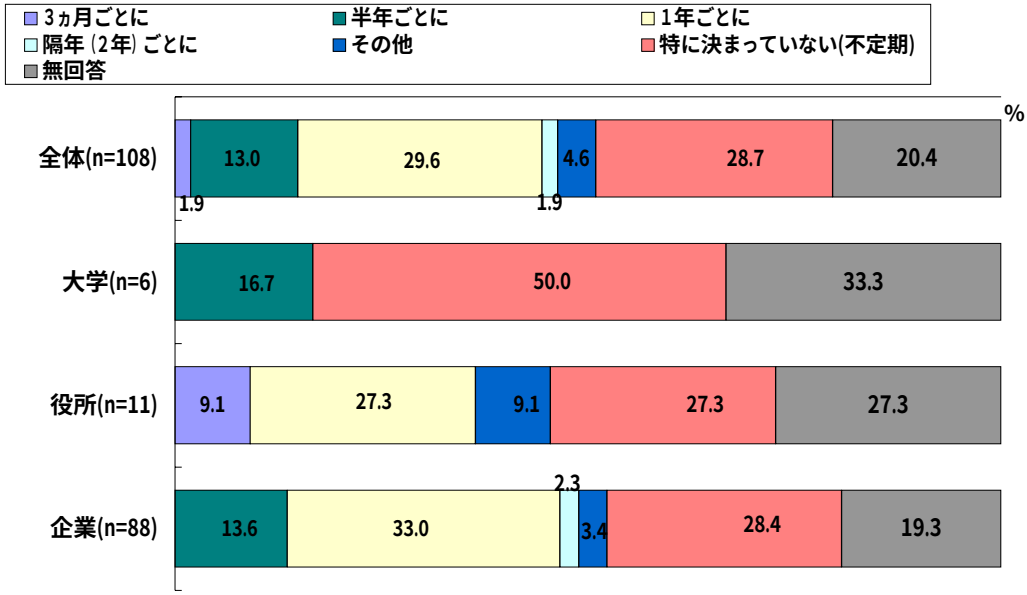


		n	実施している	実施を予定している	実施をしていないが必要性を感じる	実施の必要性を感じない（実施していない）	無回答
全体		631	10.0	7.1	59.3	20.1	3.5
大 学		55	7.3	3.6	70.9	14.5	3.6
役 所		55	9.1	10.9	61.8	14.5	3.6
企業業種別	運輸	10	30.0	10.0	20.0	40.0	-
	製造	167	7.2	9.0	55.7	23.4	4.8
	サービス	97	9.3	3.1	68.0	17.5	2.1
	不動産	25	-	12.0	72.0	4.0	12.0
	エネルギー	33	9.1	6.1	51.5	30.3	3.0
	交通	23	-	4.3	47.8	47.8	-
	金融	74	29.7	6.8	51.4	9.5	2.7
	情報通信	43	7	4.7	65.1	23.3	-
	医療	39	2.6	5.1	59.0	28.2	5.1

８．セキュリティ対策状況（11／11）

(11) セキュリティ監査の実施頻度 (n=108)

●実施頻度は「１年ごとに」が最も高く29.6%。次いで「特に決まっていない」となっている。

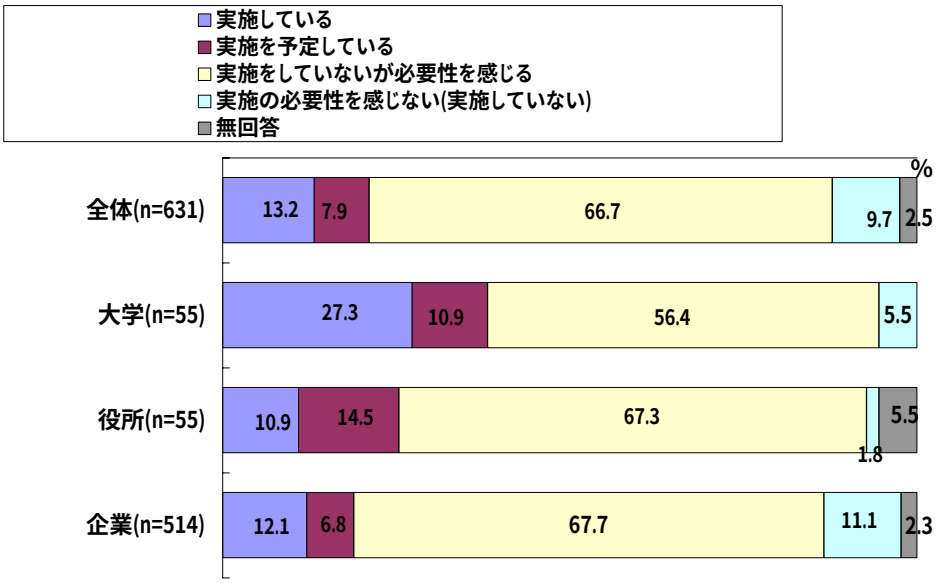


		n	3ヵ月ごとに	半年ごとに	1年ごとに	隔年（2年）ごとに	その他	特に決まっていない（不定期）	無回答
全体		108	1.9	13.0	29.6	1.9	4.6	28.7	20.4
	大 学	6	-	16.7	-	-	-	50	33.3
	役 所	11	9.1	-	27.3	-	9.1	27.3	27.3
企業業種別	運輸	4	-	25.0	25.0	-	-	50.0	-
	製造	27	-	11.1	22.2	3.7	3.7	29.6	29.6
	サービス	12	-	33.3	41.7	-	-	16.7	8.3
	不動産	3	-	-	-	-	-	-	100.0
	エネルギー	5	-	-	40.0	-	-	60.0	-
	交通	1	-	-	-	-	-	-	100.0
	金融	27	-	7.4	51.9	3.7	3.7	22.2	11.1
	情報通信	5	-	40.0	20.0	-	-	20.0	20.0
	医療	3	-	-	-	-	33.3	66.7	-

９．情報セキュリティ教育の取り組み（１／４）

(1)教育の実施状況 (n=631)

●教育の実施状況は、「実施している」、「実施を予定している」を合わせ21.1%であるが、「実施をしていないが必要性を感じる」の割合が全体の66.7%と非常に高い。

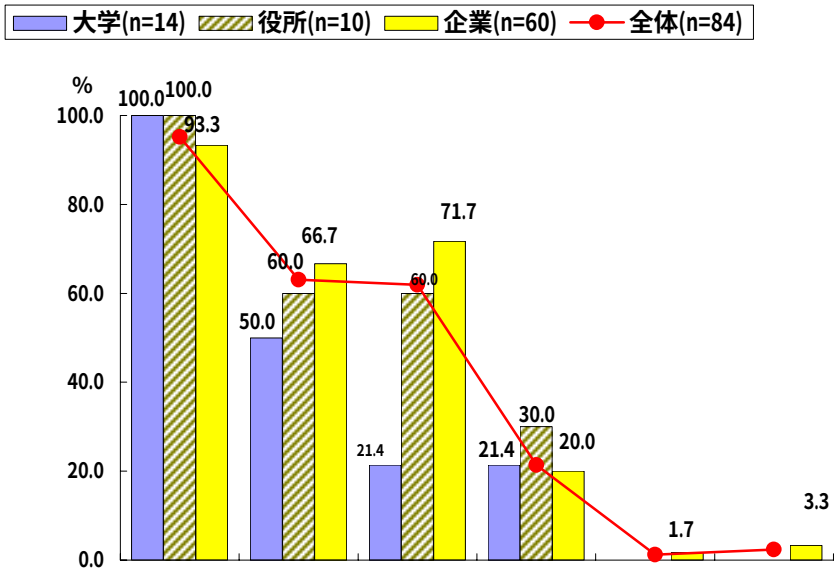


		n	実施している	実施を予定している	実施をしていないが必要性を感じる	実施の必要性を感じない（実施していない）	無回答
全体		631	13.2	7.9	66.7	9.7	2.5
大 学		55	27.3	10.9	56.4	5.5	-
役 所		55	10.9	14.5	67.3	1.8	5.5
企業業種別	運輸	10	10.0	10.0	70.0	10.0	-
	製造	167	13.8	9.6	60.5	13.2	3.0
	サービス	97	8.2	5.2	71.1	14.4	1.0
	不動産	25	4	4.0	92.0	-	-
	エネルギー	33	6.1	6.1	78.8	9.1	-
	交通	23	-	8.7	60.9	30.4	-
	金融	74	23.0	8.1	59.5	5.4	4.1
	情報通信	43	14	2.3	76.7	4.7	2.3
	医療	39	10.3	2.6	71.8	10.3	5.1

９．情報セキュリティ教育の取り組み（２／４）

(2)情報セキュリティの教育目的 (MA) (n=84)

●「セキュリティに対する意識の向上」の割合が90%を超え、「社内不正行為の防止」、「ポリシーの普及」が続いている。

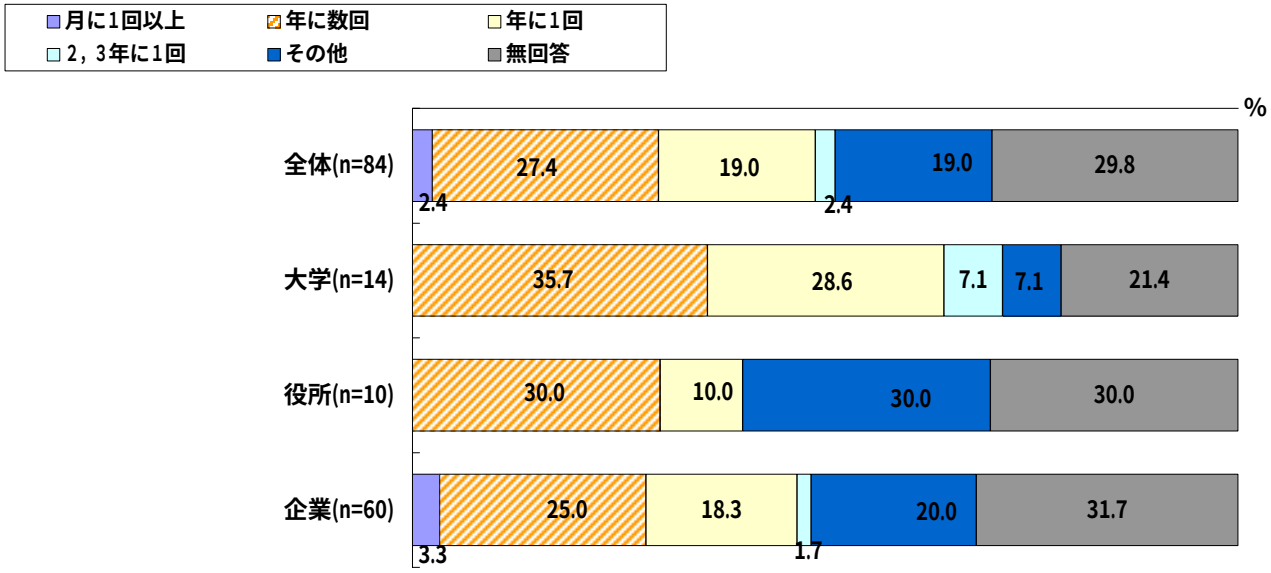


		n	セキュリティに対する意識の向上	社内不正行為の防止	ポリシーの普及	自己啓発	その他	無回答
全体		84	95.2	63.1	61.9	21.4	1.2	2.4
大 学		14	100.0	50.0	21.4	21.4	-	-
役 所		10	100.0	60.0	60.0	30.0	-	-
企業業種別	運輸	1	-	100.0	100.0	100.0	-	-
	製造	20	100.0	65.0	65.0	10.0	-	-
	サービス	8	75.0	75.0	62.5	12.5	12.5	12.5
	不動産	1	100.0	-	100.0	100.0	-	-
	エネルギー	4	100.0	50.0	50.0	-	-	-
	交通	1	100.0	100.0	100.0	-	-	-
	金融	18	94.4	72.2	77.8	22.2	-	5.6
	情報通信	4	100.0	75.0	100.0	50.0	-	-
	医療	3	100.0	33.3	66.7	33.3	-	-

９．情報セキュリティ教育の取り組み（３／４）

(3)教育の頻度 (n=84)

●全体で見ると「年に数回」の割合が27.4%と最も高く、次いで「年に１回」となっている。



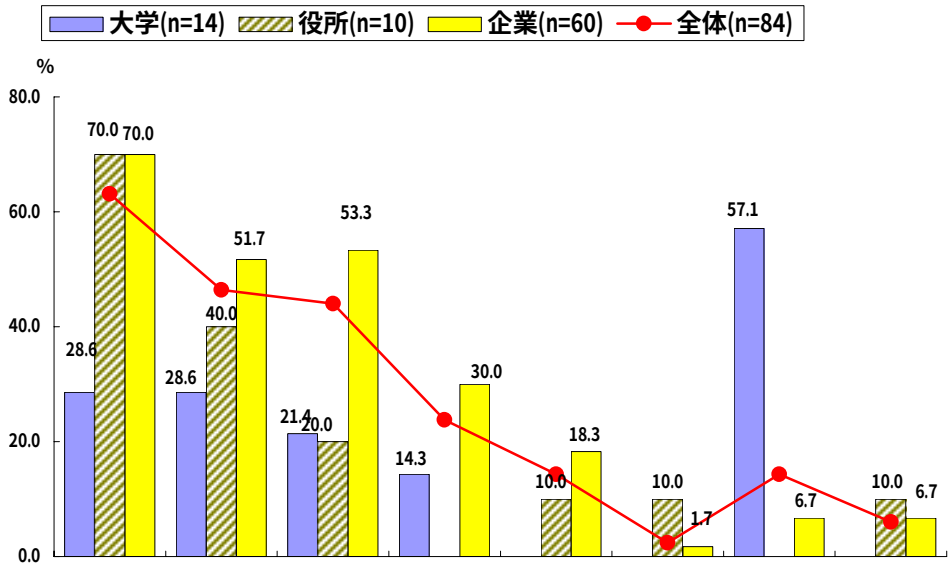
		n	月に1回以上	年に数回	年に1回	2，3年に1回	その他	無回答
全体		84	2.4	27.4	19.0	2.4	19.0	29.8
大 学		14	-	35.7	28.6	7.1	7.1	21.4
役 所		10	-	30.0	10.0	-	30.0	30.0
企業種別	運輸	1	-	-	-	-	-	100.0
	製造	20	-	10.0	20.0	5.0	20.0	45.0
	サービス	8	-	12.5	12.5	-	37.5	37.5
	不動産	1	-	-	-	-	-	100.0
	エネルギー	4	-	50.0	25.0	-	25.0	-
	交通	1	-	-	-	-	-	100.0
	金融	18	5.6	44.4	11.1	-	16.7	22.2
	情報通信	4	25.0	25.0	50.0	-	-	-
	医療	3	-	33.3	33.3	-	33.3	-

９．情報セキュリティ教育の取り組み（４／４）

(4)情報セキュリティ教育の対象者（MA）（n=84）

●全体で見ると「正社員・職員」が最も高く63.1%。次いで「管理者」「新規採用者」の順になっている。

●大学でのその他は「学生」が対象となっている。



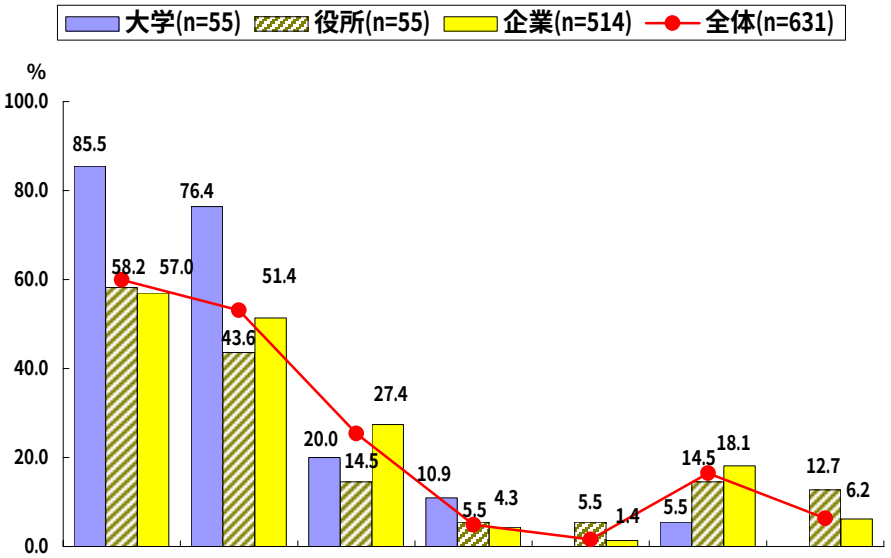
		n	正社員・職員	管理者	新規採用者	派遣社員	関連会社の社員・職員	取引先社員・職員	その他	無回答
全体		84	63.1	46.4	44.0	23.8	14.3	2.4	14.3	6.0
大学		14	28.6	28.6	21.4	14.3	-	-	57.1	-
役所		10	70.0	40.0	20.0	-	10.0	10.0	-	10.0
企業業種別	運輸	1	100.0	100.0	-	-	-	-	-	-
	製造	20	65.0	50.0	55.0	40.0	25.0	-	10.0	5.0
	サービス	8	75.0	50.0	62.5	50.0	25.0	12.5	-	12.5
	不動産	1	100.0	-	-	-	-	-	-	-
	エネルギー	4	50.0	50.0	75.0	-	-	-	-	-
	交通	1	100.0	100.0	100.0	100.0	100.0	-	-	-
	金融	18	72.2	50.0	44.4	22.2	16.7	-	5.6	11.1
	情報通信	4	75.0	75.0	50.0	-	-	-	-	-
	医療	3	66.7	33.3	66.7	33.3	-	-	33.3	-

１０．アクセスログの取得状況（１／３）

(1)取得しているログの種類(MA)(n=631)

●全体で見ると「サーバー上のアクセスログ」が最も高く59.9%。次いで「ファイアウォール上のログ」「トランザクションログ」の順になっている。

●全くアクセスログを取得していない所が16.5%ある。

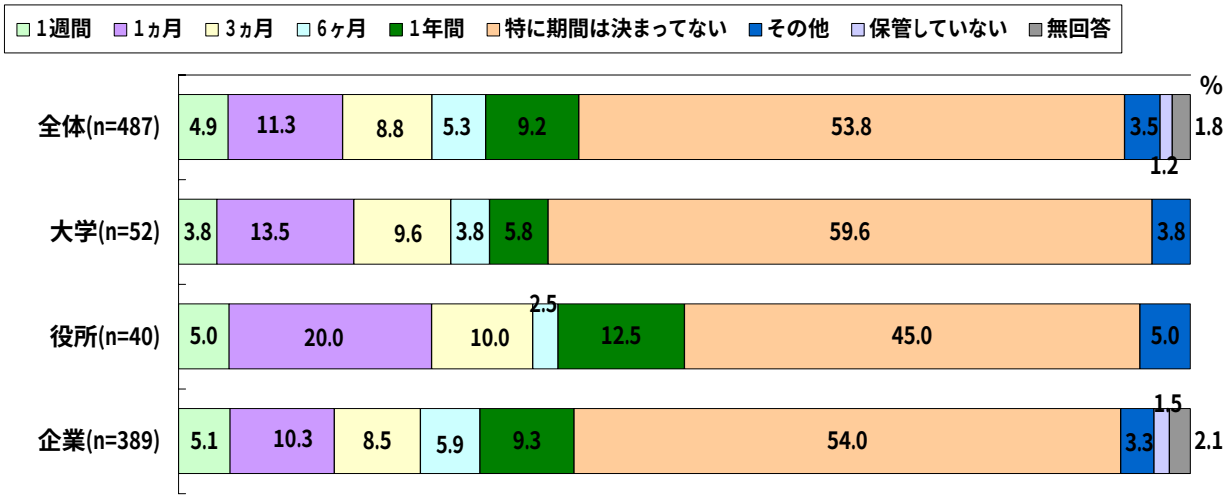


		n	サーバ上のアクセスログ	ファイアウォール上のログ	トランザクションログ	IDSのログ	その他	取得していない	無回答
全体		631	59.9	53.1	25.4	4.9	1.6	16.5	6.3
大学		55	85.5	76.4	20.0	10.9	1.6	5.5	-
役所		55	58.2	43.6	14.5	5.5	-	14.5	12.7
企業業種別	運輸	10	70.0	60.0	20.0	-	-	10.0	-
	製造	167	60.5	53.9	29.9	3.6	1.8	17.4	4.8
	サービス	97	60.8	61.9	28.9	6.2	-	15.5	4.1
	不動産	25	64.0	68.0	16.0	-	-	8.0	-
	エネルギー	33	39.4	39.4	9.1	9.1	-	36.4	9.1
	交通	23	34.8	30.4	17.4	4.3	8.7	39.1	8.7
	金融	74	63.5	39.2	43.2	4.1	2.7	12.2	6.8
	情報通信	43	62.8	58.1	18.6	7.0	-	9.3	7.0
	医療	39	30.8	35.9	23.1	-	-	30.8	17.9

１０．アクセスログの取得状況（２／３）

(2)ログの保管機関 (n=487)

●ログの保管期間は「特に期間が決まっていない」の割合が全体で53.8.%を占めている。

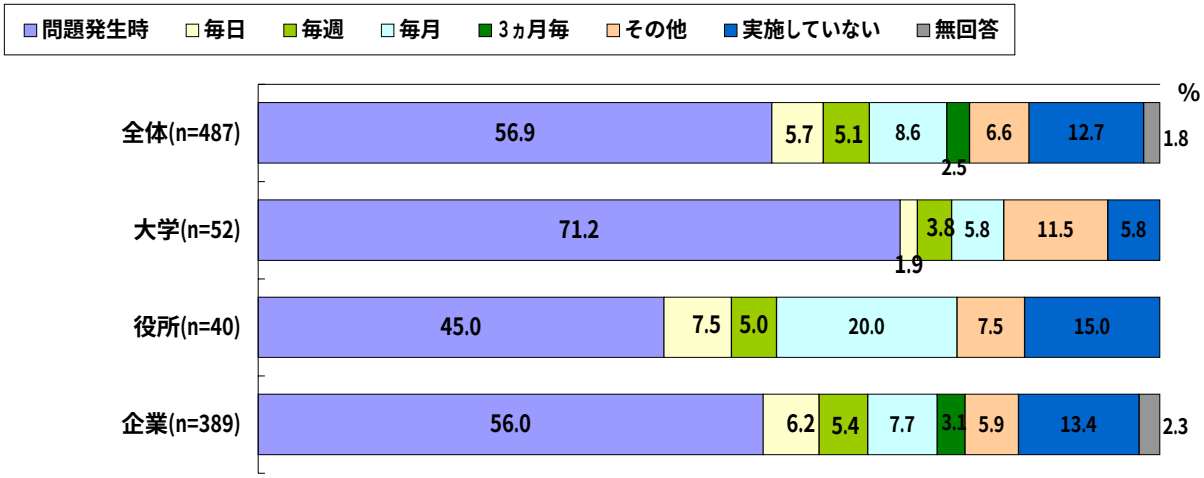


		n	1週間	1ヵ月	3ヵ月	6ヶ月	1年間	特に期間は決まってない	その他	保管していない	無回答
全体		487	4.9	11.3	8.8	5.3	9.2	53.8	3.5	1.2	1.8
大学		52	3.8	13.5	9.6	3.8	5.8	59.6	3.8	-	-
役所		40	5.0	20.0	10.0	2.5	12.5	45.0	5.0	-	-
企業業種別	運輸	9	-	22.2	-	11.1	11.1	55.6	-	-	-
	製造	130	4.6	13.1	6.2	8.5	11.5	48.5	2.3	2.3	3.1
	サービス	78	7.7	10.3	9.0	7.7	3.8	56.4	1.3	2.6	1.3
	不動産	23	4.3	13.0	8.7	-	13.0	52.2	8.7	-	-
	エネルギー	18	5.6	-	5.6	5.6	11.1	72.2	-	-	-
	交通	12	-	8.3	8.3	8.3	-	58.3	8.3	8.3	-
	金融	60	3.3	8.3	13.3	-	11.7	53.3	8.3	-	1.7
	情報通信	36	5.6	8.3	8.3	8.3	13.9	47.2	2.8	-	5.6
	医療	20	10	5.0	15.0	-	-	70.0	-	-	-

１０．アクセスログの取得状況（３／３）

(3) 情報セキュリティ対策としてのログの解析頻度 (n=487)

●解析頻度は「問題発生時」の割合が全体の56.9%を占めている。

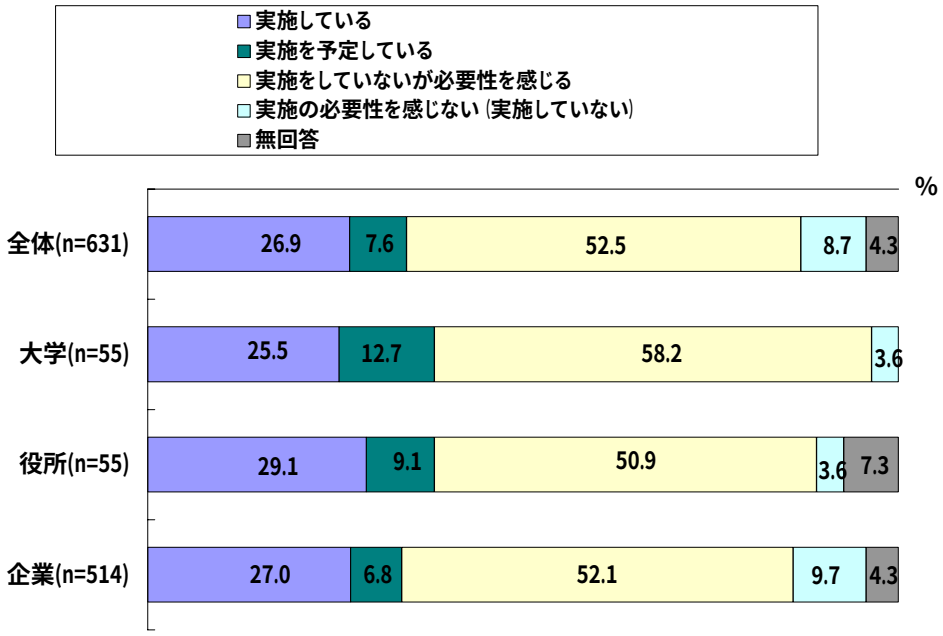


		n	問題発生時	毎日	毎週	毎月	3ヵ月毎	その他	実施していない	無回答
全体		487	56.9	5.7	5.1	8.6	2.5	6.6	12.7	1.8
大 学		52	71.2	1.9	3.8	5.8	-	11.5	5.8	-
役 所		40	45.0	7.5	5.0	20.0	-	7.5	15.0	-
企業業種別	運輸	9	66.7	-	-	-	-	-	33.3	-
	製造	130	55.4	6.9	6.2	4.6	2.3	8.5	13.8	2.3
	サービス	78	57.7	3.8	3.8	9.0	3.8	3.8	16.7	1.3
	不動産	23	52.2	4.3	8.7	4.3	13.0	8.7	8.7	-
	エネルギー	18	55.6	5.6	11.1	11.1	5.6	-	11.1	-
	交通	12	50	-	8.3	8.3	-	8.3	25.0	-
	金融	60	56.7	10.0	-	6.7	1.7	10.0	11.7	3.3
	情報通信	36	52.8	8.3	5.6	16.7	2.8	-	5.6	8.3
	医療	20	65	5.0	10.0	10.0	-	-	10.0	-

１１．不正アクセス等の検知対策について（１／２）

(1)不正アクセス等の検知対策の有無 (n=631)

●「実施をしていないが必要性を感じる」の割合が最も高く52.5%。次いで「実施している」となっている。



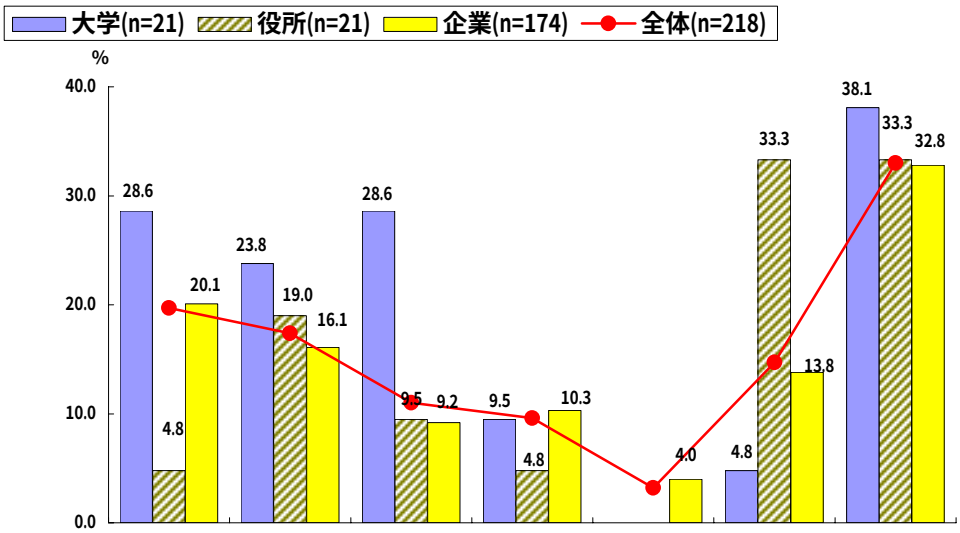
		n	実施している	実施を予定している	実施をしていないが必要性を感じる	実施の必要性を感じない（実施していない）	無回答
全体		631	26.9	7.6	52.5	8.7	4.3
大 学		55	25.5	12.7	58.2	3.6	-
役 所		55	29.1	9.1	50.9	3.6	7.3
企業業種別	運輸	10	30.0	-	50.0	10.0	10.0
	製造	167	24.0	8.4	53.9	9.6	4.2
	サービス	97	29.9	8.2	47.4	9.3	5.2
	不動産	25	28.0	4.0	68.0	-	-
	エネルギー	33	21.2	3.0	63.6	12.1	-
	交通	23	17.4	4.3	56.5	21.7	-
	金融	74	36.5	5.4	44.6	8.1	5.4
	情報通信	43	32.6	9.3	53.5	-	4.7
	医療	39	17.9	2.6	48.7	23.1	7.7

１１．不正アクセス等の検知対策について（２／２）

(2)提供されている機能に対する不足、不満点（MA）（n=218）

●「価格が高い」が最も高く19.7%。次いで「日本語化されていない」、「特に不足点や不満点はない」となっている。

●大学では「誤検出が多すぎる」、役所では「特に不足点、不満点はない」の割合が全体と比べて高くなっている。



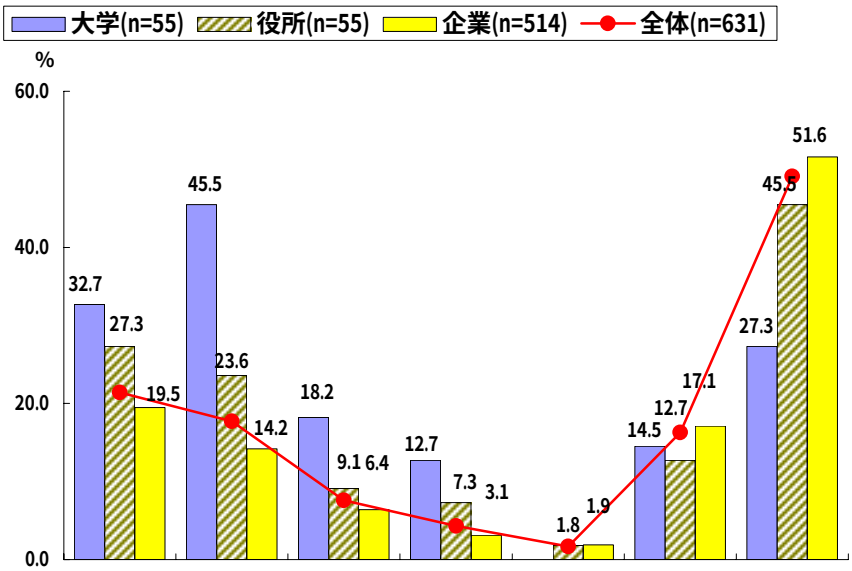
		n	価格が高い	日本語化されていない	誤検出が多すぎる	使いこなせない	その他	特に不足点や不満点はない	無回答
全体		218	19.7	17.4	11.0	9.6	3.2	14.7	33.0
	大　学	21	28.6	23.8	28.6	9.5	-	4.8	38.1
	役　所	21	4.8	19.0	9.5	4.8	-	33.3	33.3
企業業種別	運輸	3	-	33.3	-	-	-	33.3	33.3
	製造	54	22.2	18.5	9.3	14.8	3.7	5.6	33.3
	サービス	37	18.9	16.2	5.4	10.8	8.1	5.4	43.2
	不動産	8	37.5	-	-	-	-	25.0	37.5
	エネルギー	8	12.5	-	12.5	25.0	-	25.0	25.0
	交通	5	-	-	-	40.0	-	20.0	40.0
	金融	31	22.6	22.6	16.1	-	6.5	22.6	16.1
	情報通信	18	27.8	-	5.6	5.6	-	11.1	55.6
	医療	8	-	37.5	25.0	12.5	-	37.5	-

１２．具体的な攻撃に対する情報セキュリティ対策（１／６）

(1)DOS攻撃に対する対策（MA）（n=631）

●全体で見ると、「ファイアウォールのＤｏＳ対策機能」の割合が21.4%と最も高く、次いで「サーバプログラムへの最新パッチの適応」の順になっている。

●大学の「サーバプログラムへの最新パッチの適応」の割合が全体に比べて高くなっている。



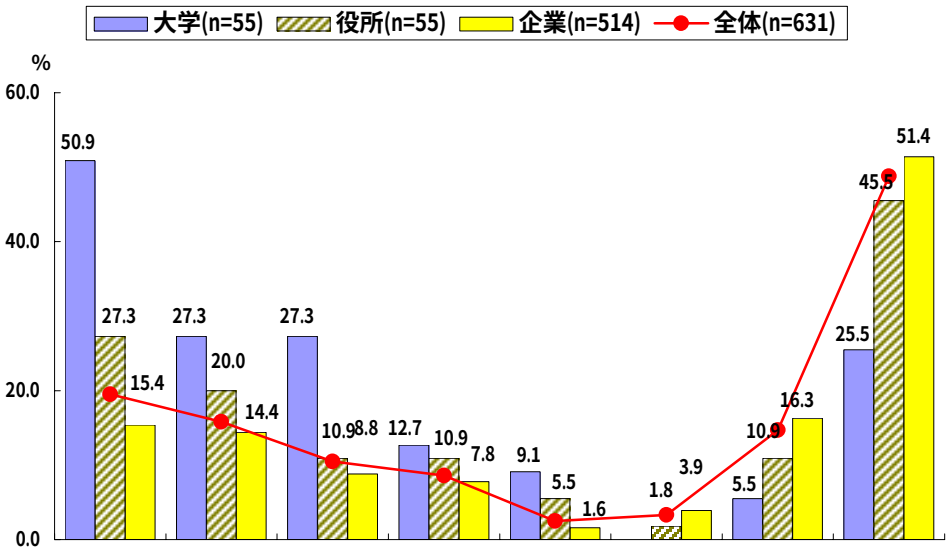
		n	ファイアウォールのＤｏＳ対策機能	サーバプログラムへの最新パッチの適応	ルータのＤｏＳ対策機能	IDSによるＤｏＳ対策機能	その他	実施していない	無回答
全体		631	21.4	17.7	7.6	4.3	1.7	16.3	49.1
大 学		55	32.7	45.5	18.2	12.7	-	14.5	27.3
役 所		55	27.3	23.6	9.1	7.3	1.8	12.7	45.5
企業業種別	運輸	10	20.0	10.0	-	-	-	10.0	60.0
	製造	167	22.2	18.0	6.0	1.2	1.8	15.0	49.7
	サービス	97	16.5	9.3	4.1	4.1	2.1	12.4	58.8
	不動産	25	24.0	20.0	12.0	-	4.0	12.0	48.0
	エネルギー	33	21.2	15.2	9.1	12.1	3.0	30.3	39.4
	交通	23	21.7	13.0	8.7	4.3	-	34.8	39.1
	金融	74	20.3	17.6	10.8	5.4	4.1	16.2	47.3
	情報通信	43	16.3	14.0	4.7	2.3	-	7.0	65.1
	医療	39	12.8	2.6	2.6	-	-	33.3	51.3

１２．具体的な攻撃に対する情報セキュリティ対策（２／６）

(2)スパムメールの不正中継対策（MA）（n=631）

●全体で見ると、「メールサーバの設定の修正」の割合が最も高く19.5%。次いで「ファイアウォールによる遮断」、「実施していない」の順になっている。

●大学では、「メールサーバの修正」「メールソフトのバージョンアップ」などソフトのメンテナンスが他に比べて高い比率で実施されている。



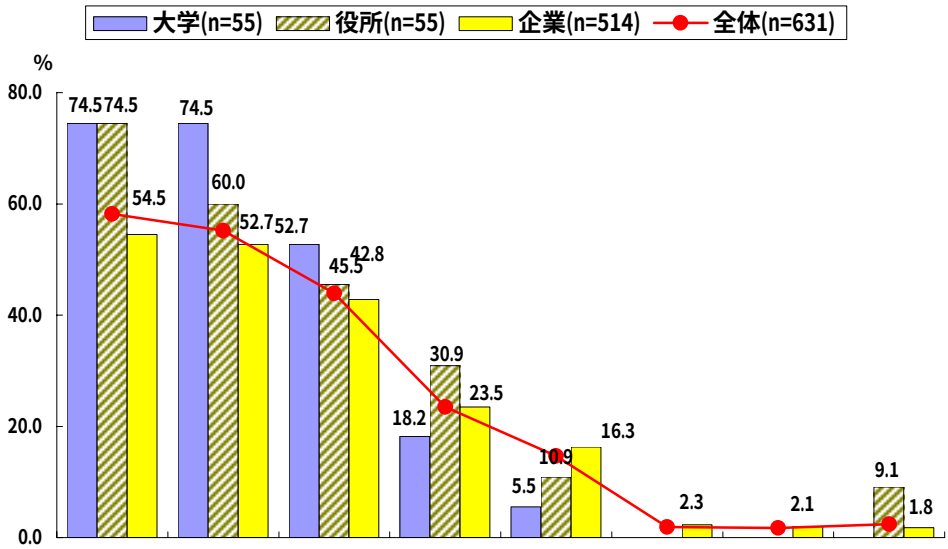
		n	メールサーバの設定の修正	ファイアウォールによる遮断	メールソフトのバージョンアップ	メールサーバへの対策ソフトの導入	ＩＤＳによる検知	その他	実施していない	無回答
全体		631	19.5	15.8	10.5	8.6	2.5	3.3	14.7	48.8
大 学		55	50.9	27.3	27.3	12.7	9.1	-	5.5	25.5
役 所		55	27.3	20.0	10.9	10.9	5.5	1.8	10.9	45.5
企業業種別	運輸	10	10.0	20.0	-	-	-	-	10.0	60.0
	製造	167	13.8	16.2	9.6	8.4	1.2	4.8	16.8	50.3
	サービス	97	14.4	13.4	7.2	7.2	-	1.0	12.4	60.8
	不動産	25	8.0	36.0	4.0	8.0	-	8.0	8.0	48.0
	エネルギー	33	27.3	12.1	18.2	9.1	9.1	3.0	24.2	36.4
	交通	23	8.7	17.4	-	8.7	-	4.3	26.1	43.5
	金融	74	17.6	12.2	13.5	8.1	4.1	8.1	17.6	44.6
	情報通信	43	20.9	2.3	7.0	7.0	-	-	11.6	62.8
	医療	39	12.8	12.8	5.1	7.7	-	2.6	23.1	48.7

１２．具体的な攻撃に対する情報セキュリティ対策（３／６）

(3)コンピューターウイルス対策（MA）（n=631）

●「パターンファイルの更新」の割合が58.2%と最も高く、次いで「ワクチンソフト（クライアント）の使用」「ワクチンソフト（サーバ）の使用」となっている。

●大学、役所では「パターンファイルの更新」の割合が全体と比べて高くなっている。



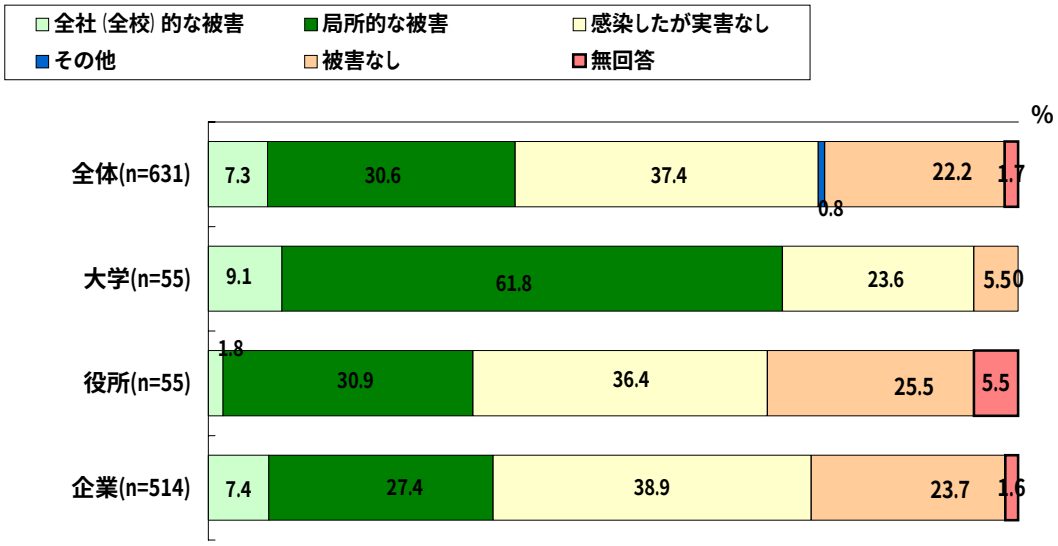
		n	パターンファイルの更新	ワクチンソフト（クライアント）の使用	ワクチンソフト（サーバ）の使用	許可されないソフトウェアのインストール制限	ファイル等のダウンロードの制限	その他	実施していない	無回答
全体		631	58.2	55.2	43.9	23.5	14.7	1.9	1.7	2.4
大 学		55	74.5	74.5	52.7	18.2	5.5	-	-	-
役 所		55	74.5	60.0	45.5	30.9	10.9	-	-	9.1
企業業種別	運輸	10	40.0	60.0	40.0	30.0	10.0	10.0	-	-
	製造	167	61.7	54.5	46.1	16.2	15.0	0.6	1.2	1.2
	サービス	97	54.6	50.5	45.4	19.6	11.3	1.0	1.0	1.0
	不動産	25	56.0	40.0	40.0	36.0	12.0	-	-	-
	エネルギー	33	48.5	66.7	51.5	33.3	12.1	6.1	3.0	-
	交通	23	43.5	52.2	26.1	21.7	4.3	4.3	13.0	4.3
	金融	74	51.4	54.1	47.3	44.6	33.8	5.4	1.4	1.4
	情報通信	43	55.8	41.9	39.5	16.3	23.3	2.3	2.3	4.7
	医療	39	41.0	56.4	25.6	17.9	7.7	2.6	5.1	5.1

１２．具体的な攻撃に対する情報セキュリティ対策（４／６）

(4)1年間にコンピュータウイルスを受けた被害の規模 (n=631)

●「感染したが実害なし」の割合が37.4%と最も高く、次いで「局所的な被害」「被害なし」の順になっている。

●大学では、コンピュータウイルスの被害の割合が、役所、企業に比べて非常に高くなっている。



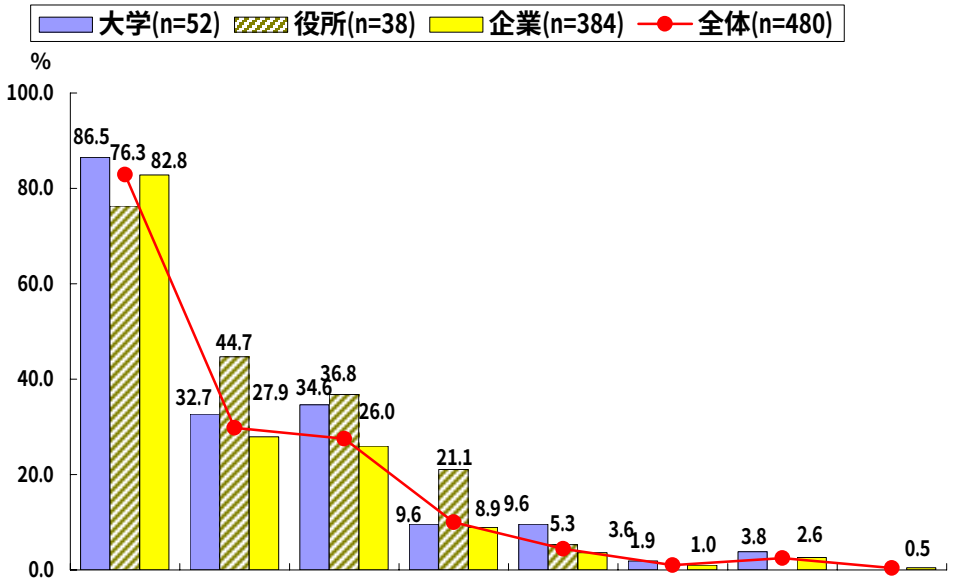
		n	全社（全校）的な被害	局所的な被害	感染したが実害なし	その他	被害なし	無回答
全体		631	7.3	30.6	37.4	0.8	22.2	1.7
大 学		55	9.1	61.8	23.6	-	5.5	-
役 所		55	1.8	30.9	36.4	-	25.5	5.5
企業種別	運輸	10	10.0	20.0	50.0	-	20.0	-
	製造	167	11.4	31.7	35.9	1.8	16.8	2.4
	サービス	97	11.3	35.1	39.2	-	14.4	-
	不動産	25	12	36.0	44.0	-	8.0	-
	エネルギー	33	3	24.2	30.3	3.0	36.4	3.0
	交通	23	-	17.4	34.8	-	47.8	-
	金融	74	1.4	14.9	41.9	1.4	39.2	1.4
	情報通信	43	4.7	27.9	39.5	-	23.3	4.7
	医療	39	-	17.9	48.7	-	33.3	-

１２．具体的な攻撃に対する情報セキュリティ対策（５／６）

(5)コンピュータウイルスの主な感染ルート(MA)(n=480)

●主な感染ルートとして「電子メール」の割合が82.9%を占めている。

●本年に話題となったＷＥＢアクセスからの感染が27.5%になっていることが注目される。

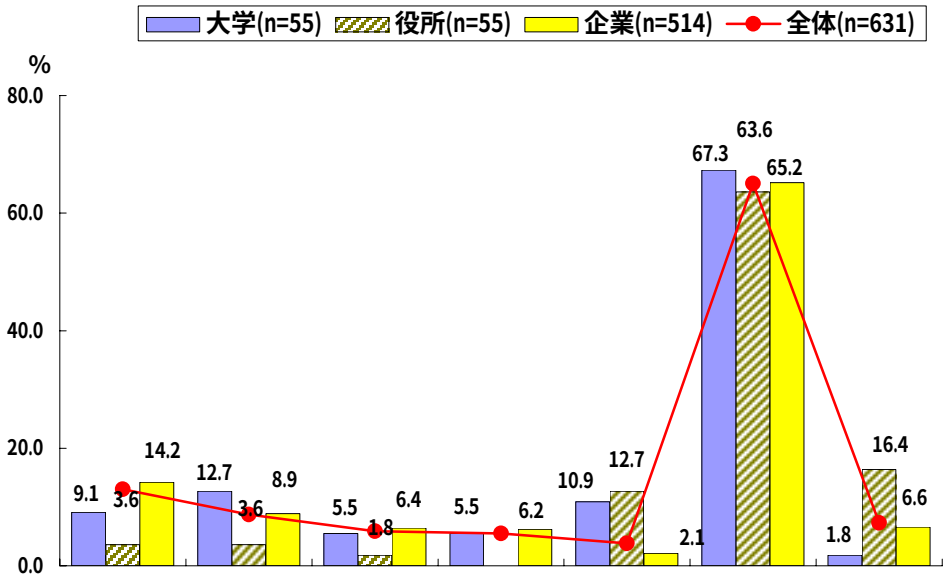


		n	電子メール	社外からの記憶媒体	WEBアクセス	社内からの記憶媒体	ダウンロードしたソフトウェア	その他	不明	無回答
全体		480	82.9	29.8	27.5	10.0	4.4	1.0	2.5	0.4
大学		52	86.5	32.7	34.6	9.6	9.6	1.9	3.8	-
役所		38	76.3	44.7	36.8	21.1	5.3	-	-	-
企業業種別	運輸	8	87.5	12.5	-	12.5	-	-	12.5	-
	製造	135	88.9	24.4	27.4	5.9	1.5	2.2	0.7	0.7
	サービス	83	81.9	21.7	25.3	9.6	1.2	1.2	3.6	-
	不動産	23	82.6	56.5	26.1	13.0	8.7	-	-	-
	エネルギー	20	75.0	35.0	40.0	10.0	20.0	-	10.0	-
	交通	12	75.0	25.0	25.0	25.0	-	-	-	-
	金融	44	70.5	34.1	20.5	9.1	4.5	-	-	2.3
	情報通信	31	93.5	19.4	32.3	3.2	3.2	-	3.2	-
	医療	26	69.2	38.5	23.1	15.4	7.7	-	7.7	-

１２．具体的な攻撃に対する情報セキュリティ対策（６／６）

(6)通信機密に関する暗号化(MA)(n=631)

●暗号化の状況では「利用していない」の割合が全体の60%を超えている。
本格的な普及はこれからと思われる。



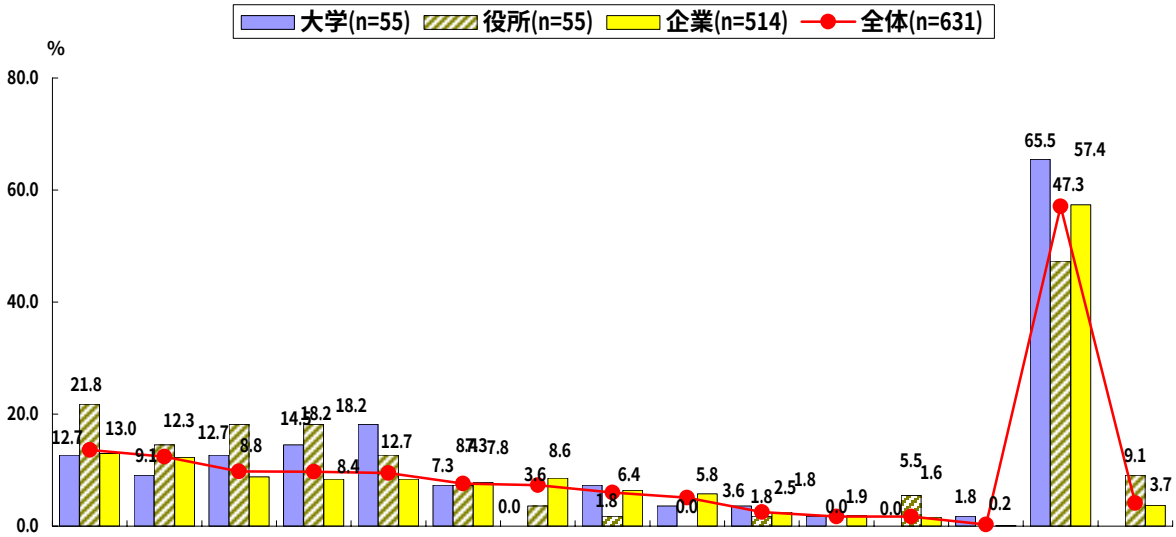
		n	認証情報（電子証明書）	暗号メール	記憶媒体上の情報（ファイルの暗号化）	クレジットカード番号等の重要なトラザクションの転送	その他	利用していない	無回答
全体		631	13.0	8.7	5.9	5.5	3.8	65.0	7.3
大 学		55	9.1	12.7	5.5	5.5	10.9	67.3	1.8
役 所		55	3.6	3.6	1.8	-	12.7	63.6	16.4
企業業種別	運輸	10	50.0	10.0	10.0	10.0	-	30.0	10.0
	製造	167	15.6	13.2	5.4	1.2	3.0	65.3	6.6
	サービス	97	12.4	9.3	5.2	10.3	-	64.9	6.2
	不動産	25	24.0	8.0	8.0	4.0	4.0	56.0	-
	エネルギー	33	9.1	6.1	6.1	-	3.0	75.8	9.1
	交通	23	17.4	-	-	8.7	-	69.6	8.7
	金融	74	14.9	6.8	13.5	18.9	4.1	52.7	6.8
	情報通信	43	14.0	7.0	7.0	4.7	-	74.4	4.7
	医療	39	-	5.1	2.6	-	2.6	79.5	10.3

１３．セキュリティサービス業者の利用状況（１／３）

(1)サービス内容(MA)(n=631)

●全体で見ると、57.1%が「利用していない」と回答しているが昨年度調査での83.5%と比べるとサービス業者の利用が進んだと思われる。

●利用されているサービスでは、「ウイルス監視」が13.6%と最も多くなっている。昨年度調査では「セキュリティ診断」が最も多く、次いで「運用支援」「ログ解析」の順で「ウイルス監視」は７番目の項目であった。本年におけるウイルス被害の増大の影響と思われる。

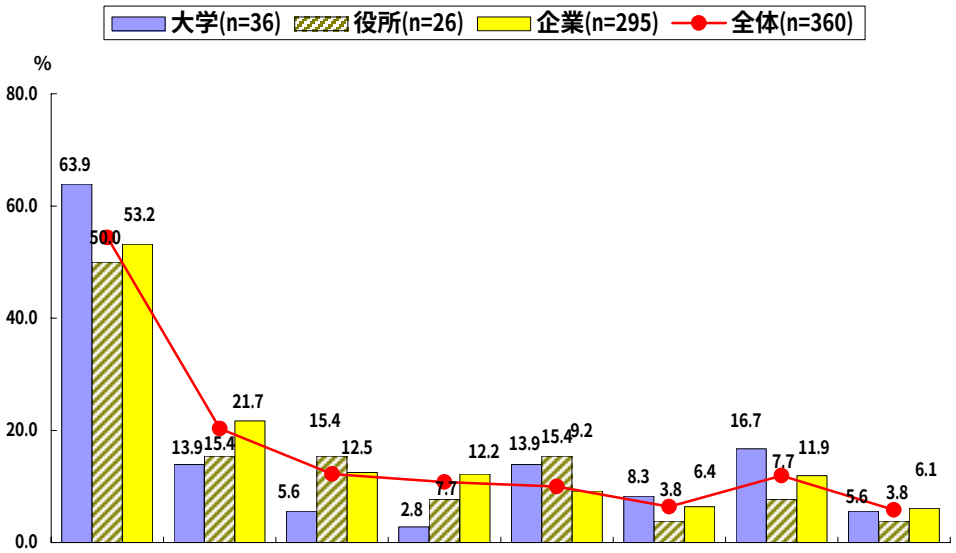


		n	ウイルス監視	セキュリティ診断	ソフトウェアメンテナンス	セキュリティ監視	ログ解析	セキュアシステム構築	ハウジングサービス	認証サービス	ポリシー策定	セキュリティ監査	リスク分析	社員教育	その他	利用していない	無回答
全体		631	13.6	12.4	9.8	9.7	9.5	7.6	7.3	6.0	5.1	2.5	1.7	1.7	0.3	57.1	4.1
大学		55	12.7	9.1	12.7	14.5	18.2	7.3	-	7.3	3.6	3.6	1.8	-	1.8	65.5	-
役所		55	21.8	14.5	18.2	18.2	12.7	7.3	3.6	1.8	-	1.8	-	5.5	-	47.3	9.1
企業種別	運輸	10	10.0	20.0	-	-	10.0	-	20.0	-	-	-	10.0	-	-	70.0	-
	製造	167	12.0	17.4	6.0	4.8	7.2	9.0	10.8	7.8	6.0	2.4	2.4	1.8	-	55.1	2.4
	サービス	97	13.4	8.2	8.2	7.2	10.3	8.2	11.3	8.2	6.2	1.0	3.1	2.1	-	56.7	4.1
	不動産	25	16.0	4.0	8.0	16.0	16.0	12.0	8.0	4.0	8.0	4.0	-	-	-	56.0	-
	エネルギー	33	9.1	15.2	9.1	9.1	3.0	-	3.0	-	12.1	3.0	3.0	-	-	60.6	6.1
	交通	23	4.3	-	4.3	8.7	-	4.3	4.3	-	4.3	-	-	-	-	78.3	4.3
	金融	74	17.6	9.5	16.2	10.8	10.8	9.5	8.1	13.5	4.1	5.4	-	-	1.4	51.4	5.4
	情報通信	43	20.9	20.9	14.0	23.3	11.6	11.6	7.0	2.3	9.3	2.3	2.3	4.7	-	46.5	2.3
	医療	39	7.7	5.1	7.7	2.6	5.1	2.6	-	-	-	-	-	2.6	-	74.4	7.7

１３．セキュリティサービス業者の利用状況（２／３）

(2)利用しない理由（MA）（n=360）

●「コストを負担できない」の割合が54.4%と最も高くなっており、「社内（学内）にノウハウの蓄積を行いたい」の割合20.3%を大幅に上回っている。セキュリティサービス業者を利用する際にコストに関する負担が大きい壁になっていることが表れていると思われる。



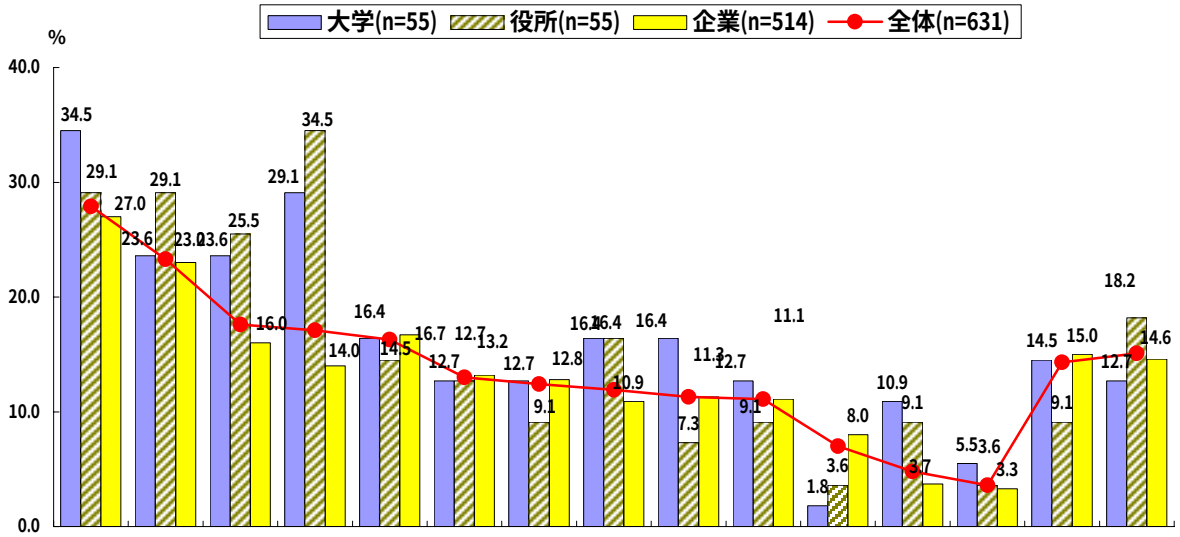
		n	コストを負担できない	社内、（学内）にノウハウの蓄積を行いたい	要求に合致するサービスが提供されていない	社内、（学内）担当者だけで必要な人員が確保されている	機密情報の漏洩につながることが懸念される	社内、（学内）に高い専門性や技術力があり、必要性がない	その他	無回答
全体		360	54.4	20.3	12.2	10.8	10.0	6.4	11.9	5.8
大学		36	63.9	13.9	5.6	2.8	13.9	8.3	16.7	5.6
役所		26	50.0	15.4	15.4	7.7	15.4	3.8	7.7	3.8
企業業種別	運輸	7	28.6	14.3	-	57.1	-	-	-	-
	製造	92	58.7	23.9	3.3	14.1	3.3	4.3	13.0	5.4
	サービス	55	50.9	23.6	10.9	18.2	9.1	9.1	9.1	5.5
	不動産	14	64.3	14.3	21.4	7.1	7.1	14.3	14.3	-
	エネルギー	20	40.0	20.0	25.0	-	20.0	5.0	20.0	5.0
	交通	18	55.6	16.7	16.7	5.6	5.6	-	16.7	5.6
	金融	38	44.7	23.7	21.1	13.2	21.1	10.5	10.5	5.3
	情報通信	20	65.0	35.0	25.0	-	10.0	10.0	-	10.0
	医療	29	51.7	6.9	10.3	6.9	10.3	3.4	17.2	13.8

１３．セキュリティサービス業者の利用状況（３／３）

(3)今後利用したいサービス内容（MA）（n=631）

●「セキュリティ診断」が27.9%と最も高く、次いで「セキュリティ監視」の順となっている。

●大学、役所では「ポリシー策定」の割合が全体に比べて高くなっている。



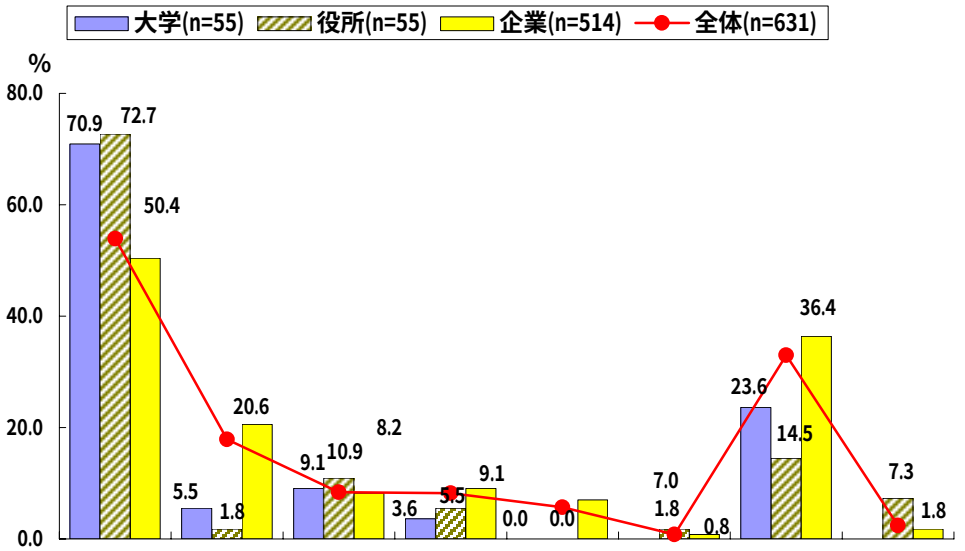
		n	セキュリティ診断	セキュリティ監視	セキュリティ監査	ポリシー策定	ウィルス監視	社員教育	認証サービス	ログ解析	セキュアシステム構築	リスク分析	ハウジングサービス	ソフトウェアメンテナンス	その他	利用したいと思わない	無回答
全体		631	27.9	23.3	17.6	17.1	16.3	13.0	12.4	11.9	11.3	11.1	7.0	4.8	3.6	14.3	15.1
大 学		55	34.5	23.6	23.6	29.1	16.4	12.7	12.7	16.4	16.4	12.7	1.8	10.9	5.5	14.5	12.7
役 所		55	29.1	29.1	25.5	34.5	14.5	12.7	9.1	16.4	7.3	9.1	3.6	9.1	3.6	9.1	18.2
企業業種別	運輸	10	20.0	10.0	20.0	10.0	10.0	20.0	10.0	10.0	10.0	20.0	10.0	-	10.0	40.0	-
	製造	167	28.1	19.2	14.4	17.4	9.0	13.2	14.4	13.2	9.6	12.0	6.6	2.4	3.0	13.8	15.6
	サービス	97	22.7	18.6	15.5	14.4	14.4	15.5	16.5	9.3	8.2	11.3	12.4	5.2	1.0	16.5	14.4
	不動産	25	52.0	36.0	28.0	24.0	16.0	16.0	20.0	20.0	12.0	28.0	16.0	8.0	-	12.0	-
	エネルギー	33	18.2	30.3	18.2	6.1	33.3	18.2	6.1	3.0	12.1	3.0	9.1	-	-	12.1	15.2
	交通	23	17.4	13.0	8.7	4.3	34.8	17.4	8.7	8.7	13.0	4.3	4.3	4.3	-	21.7	26.1
	金融	74	29.7	29.7	18.9	10.8	18.9	5.4	9.5	6.8	14.9	13.5	5.4	-	5.4	13.5	12.2
	情報通信	43	25.6	23.3	16.3	11.6	18.6	11.6	14.0	14.0	14.0	4.7	9.3	4.7	4.7	11.6	20.9
	医療	39	30.8	30.8	10.3	15.4	25.6	12.8	7.7	10.3	15.4	7.7	-	12.8	10.3	15.4	15.4

１４．情報システム関連重要施設への入退室管理（１／２）

(1)対象となる場所、区画（MA）（n=631）

●全体で見ると「部屋（マシン室）」の割合が53.9%と最も高い。次いで「実施していない」「建物内全体」となっている。

●企業、特定事業者では、「建物内全体」の割合が全体に比べてやや高くなっており、逆に大学、役所では全体に比べ低くなっている。



		n	部屋（マシン室）	建物内全体	部屋（資料室）	フロア全体	敷地内全体	その他	実施していない	無回答
全体		631	53.9	17.9	8.4	8.2	5.7	0.8	33.0	2.4
大 学		55	70.9	5.5	9.1	3.6	-	-	23.6	-
役 所		55	72.7	1.8	10.9	5.5	-	1.8	14.5	7.3
企業種別	運輸	10	40.0	10.0	-	10.0	-	-	60.0	-
	製造	167	53.9	14.4	6.0	5.4	12.6	-	38.9	1.2
	サービス	97	47.4	17.5	3.1	11.3	1.0	1.0	41.2	1.0
	不動産	25	64.0	20.0	4.0	12.0	-	-	20.0	-
	エネルギー	33	45.5	12.1	6.1	9.1	6.1	3.0	39.4	3.0
	交通	23	30.4	17.4	4.3	-	-	-	60.9	4.3
	金融	74	58.1	45.9	18.9	18.9	14.9	2.7	16.2	-
	情報通信	43	53.5	32.6	11.6	11.6	2.3	-	23.3	2.3
	医療	39	33.3	7.7	12.8	-	-	-	53.8	7.7

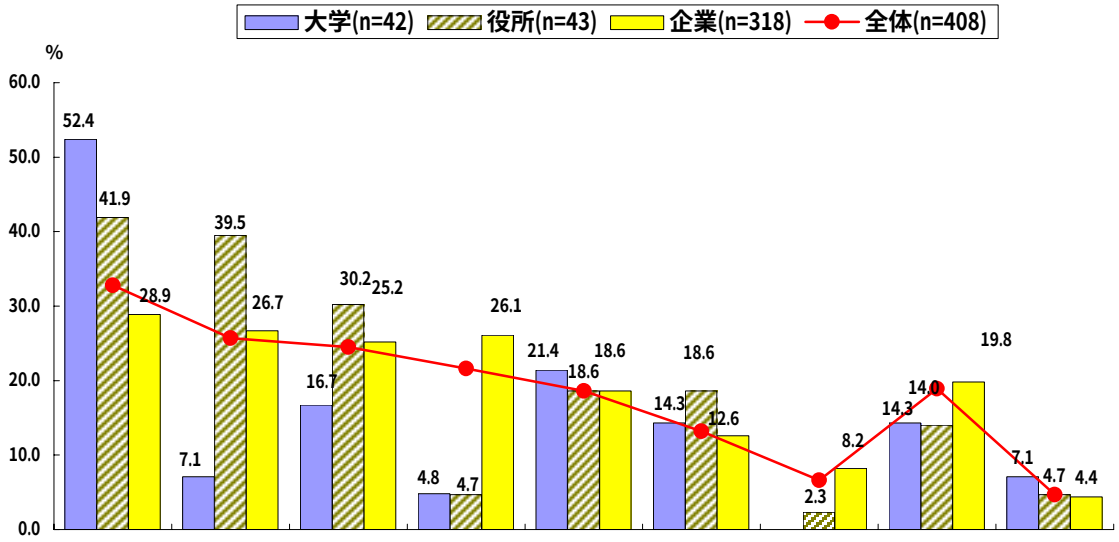
１４．情報システム関連重要施設への入退室管理（２／２）

(2)入退室の管理方法(MA)(n=408)

●全体で見ると、「磁気カード」が最も高く32.8%である。

●役所では、「記帳」の割合が全体に比べて高くなっている。

●企業、特定事業者では、「警備員」の割合が全体と比べて高くなっており、逆に大学、役所では全体に比べ低くなっている。

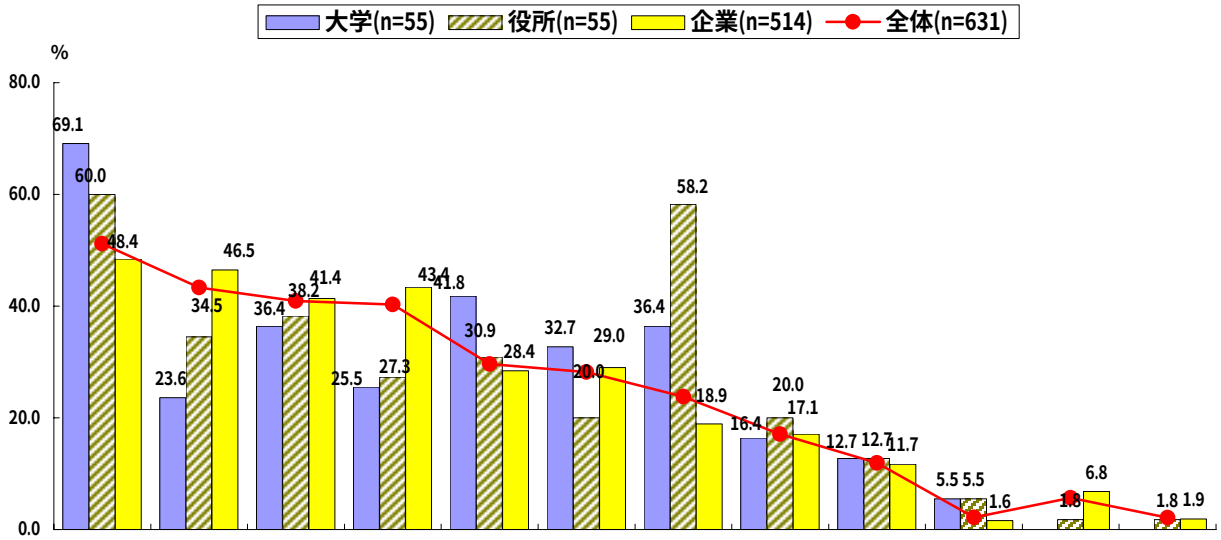


		n	磁気カード	記帳	暗証番号	警備員	ビデオカメラ	ICカード	バイオメトリクス（指紋等での認証）	その他	無回答
全体		408	32.8	25.7	24.5	21.6	18.6	13.2	6.6	18.9	4.7
大 学		42	52.4	7.1	16.7	4.8	21.4	14.3	-	14.3	7.1
役 所		43	41.9	39.5	30.2	4.7	18.6	18.6	2.3	14.0	4.7
企業業種別	運輸	4	50.0	50.0	25.0	-	-	25.0	-	-	-
	製造	100	28.0	27.0	16.0	26.0	12.0	14.0	7.0	20.0	7.0
	サービス	56	17.9	25.0	28.6	12.5	7.1	8.9	12.5	17.9	5.4
	不動産	20	25.0	30.0	25.0	15.0	10.0	15.0	5.0	20.0	-
	エネルギー	19	26.3	15.8	10.5	15.8	15.8	15.8	5.3	36.8	15.8
	交通	8	37.5	25.0	12.5	37.5	37.5	-	12.5	25.0	-
	金融	62	43.5	32.3	45.2	41.9	45.2	19.4	11.3	11.3	1.6
	情報通信	32	28.1	21.9	25.0	37.5	15.6	3.1	6.3	25.0	-
	医療	15	13.3	26.7	20.0	20.0	6.7	6.7	-	33.3	-

１５．情報セキュリティ対策のための情報入手先（１／３）

(1)情報入手先（MA）（n=631）

●「セキュリティ関連のホームページから」の割合が51.2%と最も高く、よく利用されていることを表していると思われる。



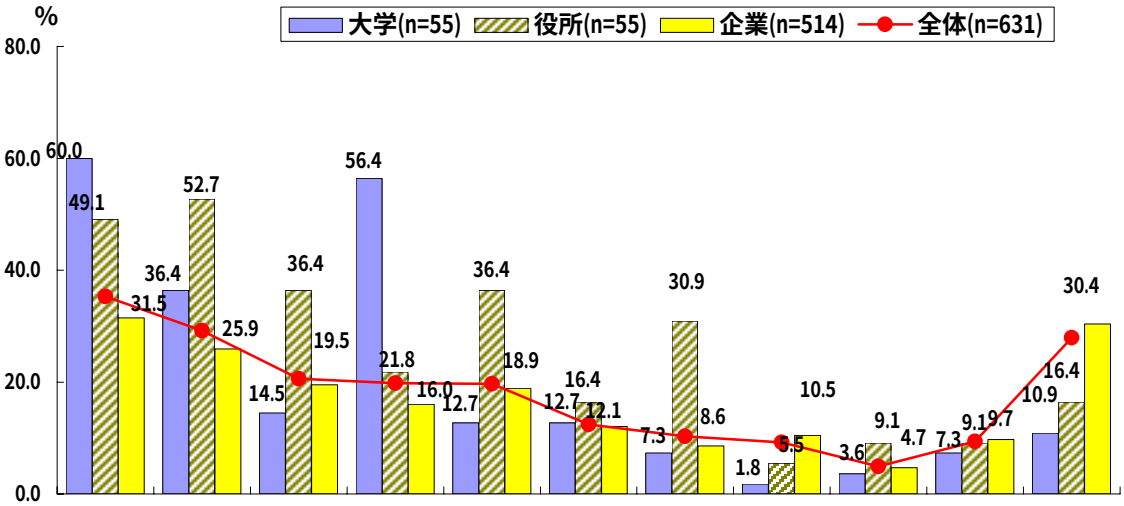
	n	セキュリティ関連のホームページから	ベンダーの営業マンから	専門雑誌や新聞から	外部のセミナーへの参加	ベンダーのホームページから	ベンダーの電子メールから	関係省庁・団体等のガイドライン	他企業の担当者との情報交換	セキュリティ専門会社から	その他	入手していない	無回答
全体	631	51.2	43.3	40.9	40.3	29.6	28.2	23.8	17.1	11.9	2.2	5.7	2.1
大 学	55	69.1	23.6	36.4	25.5	41.8	32.7	36.4	16.4	12.7	5.5	-	-
役 所	55	60.0	34.5	38.2	27.3	30.9	20.0	58.2	20.0	12.7	5.5	1.8	1.8
運輸	10	50.0	50.0	30.0	30.0	20.0	10.0	-	-	20.0	-	-	-
製造	167	47.3	46.1	44.3	46.1	36.5	38.9	11.4	13.2	9.6	3.0	5.4	1.8
サービス	97	51.5	49.5	47.4	44.3	21.6	33.0	12.4	17.5	13.4	1.0	4.1	1.0
不動産	25	52.0	68.0	52.0	52.0	24.0	36.0	16.0	36.0	12.0	-	-	-
エネルギー	33	48.5	21.2	36.4	39.4	36.4	18.2	15.2	21.2	9.1	3.0	15.2	3.0
交通	23	56.5	34.8	30.4	43.5	8.7	13.0	26.1	17.4	8.7	-	17.4	-
金融	74	40.5	55.4	37.8	50.0	27.0	17.6	39.2	24.3	12.2	1.4	4.1	2.7
情報通信	43	46.5	51.2	37.2	51.2	34.9	30.2	30.2	11.6	18.6	-	9.3	2.3
医療	39	51.3	33.3	30.8	10.3	17.9	15.4	23.1	12.8	7.7	-	15.4	5.1

１５．情報セキュリティ対策のための情報入手先（２／３）

(2)情報セキュリティ対策を実施するうえで参考にするもの（MA）（n=631）

●「ＩＰＡのホームページ」の割合が35.3%と最も高く、次いで「情報セキュリティポリシーに関するガイドライン」となっている。

●大学では、「ＪＰＣＥＲＴ／ＣＣのホームページ」の割合が全体に比べて高くなっている。



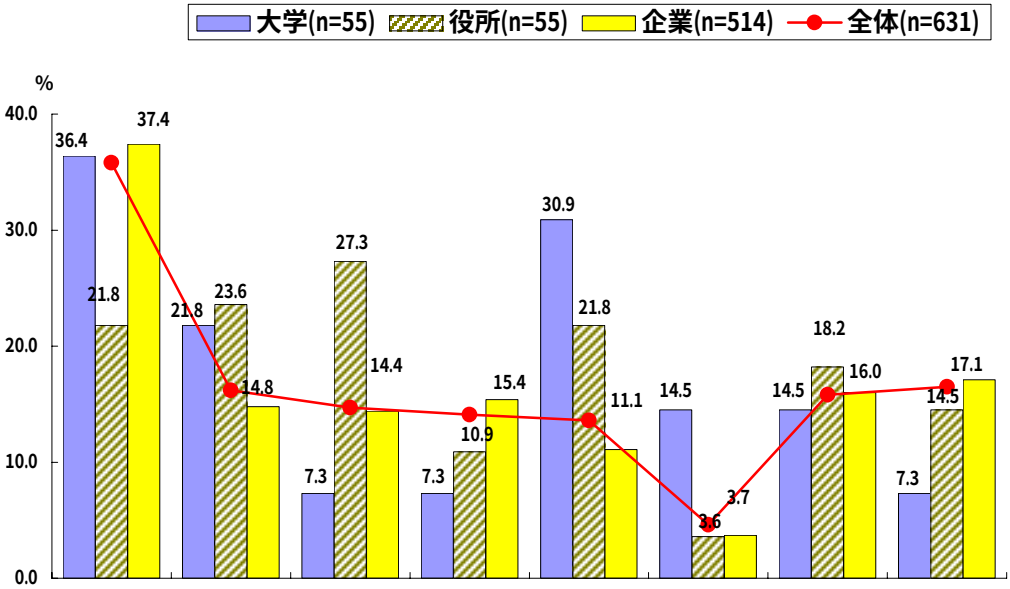
		n	IPAのホームページ	情報セキュリティポリシーに関するガイドライン	コンピュータ不正アクセス対策基準	JPCERT／CCのホームページ	情報システム安全対策基準	情報システム安全対策指針（国家公安委員会）	情報通信ネットワーク安全・信頼性基準の概要	金融機関等コンピュータシステムの安全対策基準	警察庁のホームページ	その他	無回答
全体		631	35.3	29.2	20.6	19.8	19.7	12.4	10.3	9.2	4.9	9.4	27.9
大学		55	60.0	36.4	14.5	56.4	12.7	12.7	7.3	1.8	3.6	7.3	10.9
役所		55	49.1	52.7	36.4	21.8	36.4	16.4	30.9	5.5	9.1	9.1	16.4
企業業種別	運輸	10	-	20.0	30.0	-	40.0	10.0	10.0	-	-	-	50.0
	製造	167	36.5	32.9	22.2	16.2	19.2	12.0	4.8	3.0	3.6	7.8	28.7
	サービス	97	29.9	27.8	17.5	18.6	17.5	15.5	8.2	3.1	10.3	14.4	33.0
	不動産	25	48.0	36.0	48.0	28.0	36.0	32.0	24.0	-	8.0	4.0	24.0
	エネルギー	33	24.2	21.2	18.2	24.2	18.2	15.2	6.1	3.0	3.0	12.1	39.4
	交通	23	30.4	17.4	17.4	13.0	13.0	4.3	4.3	-	4.3	26.1	43.5
	金融	74	31.1	24.3	9.5	5.4	18.9	9.5	5.4	60.8	4.1	6.8	13.5
	情報通信	43	30.2	14.0	20.9	25.6	14.0	4.7	25.6	-	2.3	9.3	30.2
	医療	39	20.5	10.3	10.3	10.3	12.8	7.7	7.7	-	-	7.7	46.2

１５．情報セキュリティ対策のための情報入手先（３／３）

(3)提供されている情報の不足、不満点（MA）（n=631）

●「具体的に何をやれば良いのかわからない」の割合が最も高く35.8%となっている。

●役所では、「情報の絶対数が少ない」が、大学では「日本語に訳されていないので利用しにくい」が全体に比べて高くなっている。



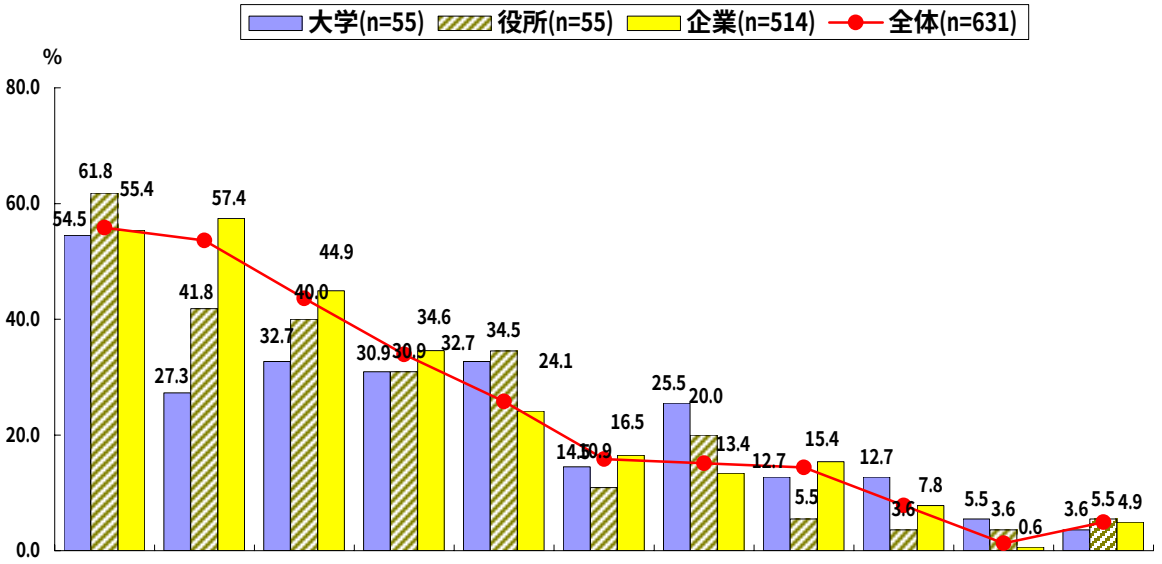
		n	具体的に何をやれば良いのかわからない	情報の公開が遅い	情報の絶対数が少ない	必要ではない情報が多い	日本語に訳されていないので利用しにくい	その他	特に不足点や不満点はない	無回答
全体		631	35.8	16.2	14.7	14.1	13.6	4.6	15.8	16.5
大 学		55	36.4	21.8	7.3	7.3	30.9	14.5	14.5	7.3
役 所		55	21.8	23.6	27.3	10.9	21.8	3.6	18.2	14.5
企業業種別	運輸	10	40.0	10.0	10.0	-	10.0	-	10.0	30.0
	製造	167	41.9	10.8	19.8	13.8	14.4	4.8	12.0	16.8
	サービス	97	34.0	19.6	11.3	17.5	7.2	2.1	22.7	16.5
	不動産	25	40.0	16.0	20.0	20.0	20.0	4.0	12.0	16.0
	エネルギー	33	45.5	21.2	3.0	21.2	12.1	3.0	9.1	18.2
	交通	23	30.4	13.0	8.7	21.7	4.3	4.3	21.7	21.7
	金融	74	36.5	8.1	17.6	16.2	8.1	4.1	18.9	16.2
	情報通信	43	30.2	18.6	7.0	20.9	11.6	4.7	14.0	14.0
	医療	39	33.3	23.1	10.3	2.6	10.3	2.6	20.5	17.9

１６．情報セキュリティ対策を実施する上での問題点（１／１）

(1)情報セキュリティ対策を実施するうえでの問題点（MA）（n=631）

●「コストがかかりすぎる」の割合が55.8%と最も多くなっている。

●企業では、「費用対効果が見えない」の割合も57.4%と大学、役所に比べて高くなっている。



		n	コストがかかりすぎる	費用対効果が見えない	どこまで行えば良いのか基準が示されていない	構築するノウハウが不足している対策を	教育訓練が行き届かない	トップの理解が得られない	従業員への負担がかかりすぎる	情報を資産として考える習慣がない	最適なツール・サービスがない	その他	無回答
全体		631	55.8	53.6	43.6	33.9	25.8	15.8	15.1	14.4	7.8	1.3	4.9
大学		55	54.5	27.3	32.7	30.9	32.7	14.5	25.5	12.7	12.7	5.5	3.6
役所		55	61.8	41.8	40.0	30.9	34.5	10.9	20.0	5.5	3.6	3.6	5.5
企業種別	運輸	10	60.0	50.0	50.0	10.0	30.0	10.0	-	10.0	-	-	-
	製造	167	55.7	59.9	49.1	37.7	23.4	21.6	7.8	16.2	7.8	1.2	4.2
	サービス	97	60.8	58.8	37.1	29.9	27.8	15.5	15.5	14.4	9.3	-	5.2
	不動産	25	64.0	68.0	48.0	32.0	40.0	28.0	4.0	36.0	8.0	-	-
	エネルギー	33	30.3	54.5	48.5	51.5	21.2	6.1	15.2	12.1	9.1	-	6.1
	交通	23	60.9	65.2	39.1	34.8	30.4	30.4	13.0	26.1	8.7	4.3	4.3
	金融	74	52.7	51.4	50.0	36.5	20.3	5.4	18.9	8.1	4.1	-	5.4
	情報通信	43	62.8	62.8	39.5	25.6	9.3	18.6	27.9	16.3	16.3	-	2.3
	医療	39	51.3	43.6	43.6	35.9	28.2	7.7	12.8	12.8	2.6	-	12.8

●添付資料

添付1） セキュリティ関連用語集

BS7799/ISO17799	：	英国規格協会が、情報セキュリティマネジメントシステムにおけるベストプラクティス（最善の慣行）を取りまとめたもので、企業等の組織体が、その情報及び情報システムを保護し、且つ積極的に活用・実施する為の組織的取組みについて標準化されている。また、BS7799 の Part1 が 2000 年 11 月に ISO/IEC17799 として国際標準化された。
CA	：	Certification Authority：認証局 PKI において、公開鍵の登録を受け、その公開鍵の管理、持ち主であるかの証明書を発行するための中立的な第三者機関。
CERT／CC	：	Computer Emergency Response Team〈コンピュータ緊急対応チーム〉 コンピュータへの不正な侵入が行われた組織に対して、被害の実態調査や侵入手口の分析、再発防止のための対策の検討と助言を行う公的組織。CERT Advisory というセキュリティホール情報を発出している。 正しくは CERT coordination Center(CERT(R)/CC)。 (CERT は米国特許庁に商標登録されている) http://www.cert.org 参照。
CGI プログラム	：	Common Gateway Interface WWW サーバ上で、WWW クライアント側からの要求でプログラムを実行し、その結果をクライアント側へ返す仕組み。
DMZ	：	Demilitarized Zone ：非武装緩衝地帯 ファイアウォールの考え方において、インターネットとイントラネットの中間部に設置するサブネットの通称で、インターネットからのアクセスを許可する Web サーバや DNS サーバなどのサーバを配置する。外部からイントラネットへのアクセスには、さらにファイアウォールを設けて容易には侵入できない様にしている。
ＤｏＳ攻撃	：	Denial of Service attack： サービス妨害攻撃 ネットワークやサーバに、過剰な負荷をかけて本来のサービス提供を不可能（又はそれに近い状態）にする攻撃手段。サービス不能攻撃

GPKI	：	Government PKI：政府認証基盤 行政機関に対する申請･届出等や行政機関からの結果の通知等は、署名又は記名押印した書面に行われるのが通常である。インターネットを利用してこのやり取りを行う場合には、申請･届出等や結果の通知等が本当にその名義人(申請者や行政機関の処分権者)によって作成されたものか、申請書や通知文書の内容が改ざんされていないかを確認できなければならない。これを確認できるようにするための行政機関側の仕組みが政府認証基盤である。
ICカード	：	IC Card プラスチックカードの中に IC チップを組み込んだもので、インテリジェントカード、スマートカードとも言われている。従来の磁気カードに比べセキュリティ性が高く、格納できる情報量も多い。再利用も可能。
IDS	：	Intrusion Detection System： 侵入検知システム システムに対する侵入／侵害を検出･通知するシステム。 システムを監視し、セキュリティポリシーを侵害するような行為を検出した場合に、その行為を可能な限り早く管理者に伝えるとともに、調査分析の作業を支援するために必要な情報を保存･提供することが目的である。 ネットワークベース IDS と、ホストベース IDS に分類されることがある。その分類法は、搭載場所がゲートウェイであるかホストであるかによる場合と、検査対象がネットワークパケット情報かホスト内で生成する情報かによる場合がある。
IPSec	：	Security Architecture for Internet Protocol アイピーセック IP のパケットを暗号化して送受信することにより、インターネットで暗号通信を行うための規格。現在インターネットで使われている IPv4 ではオプションとして使用することができるが、次世代の IPv6 では標準で実装される。
ISMS	：	Information Security Management System：情報セキュリティマネジメントシステム 情報セキュリティ管理に関する国際標準化動向を勘案し、日本国はもとより国際的にも信頼を得られる情報セキュリティ管理に対する第三者適合性評価制度を確立し、情報セキュリティレベル全体の向上を図ることを目的に設立された制度。
ISO15408	：	IT 関連製品のセキュリティ機能及び品質を第三者が評価するための国際的な評価基準である。1999 年 12 月に ISO/IEC 15408 として国際標準化、日本においては、2000 年 7 月に JIS X5070 として国内標準化されている。

JPCERT／CC	：	米国の CERT／CC と同様な趣旨で通産省の主導で設立された。事務局は〈財〉日本情報処理開発協会（JIPDEC）内に置かれている。http://www.jpcert.or.jp 参照
PKI	：	Public Key Infrastructure：公開鍵インフラストラクチャ インターネットのようなネットワーク上で公開鍵暗号技術を応用して構築されるセキュア通信を実現するための環境をいう。ネットワーク越しの通信において、本人認証、メッセージやデータのインテグリティ、非否認性を確保する。
PROXY サーバ	：	Proxy Server： proxy(プロキシ)は代理という意味。 インターネットとのゲートウェイに、セキュリティ確保や Web アクセスの高速化のために設置される。外部の第三者が利用可能な状態になっていると身元隠し・匿名化に利用されるリスクがある。
S/MIME	：	Secure Multipurpose Internet Mail Extensions 電子メールの暗号化方式の標準。公開鍵暗号方式を用いてメッセージを暗号化して送受信する。
SSH	：	Secure Shell セキュアシェル 主に UNIX で利用される、ネットワークを介して別のコンピュータにログインしたり、遠隔地のマシンでコマンドを実行したり、他のマシンへファイルを移動したりするためプログラム。ネットワーク上を流れるデータは暗号化される。
SSL	：	Secure Socket Layer インターネット上で情報を暗号化して送受信するプロトコルで、WWW や FTP などのデータ送受信の際に、用いられる。公開鍵暗号や秘密鍵暗号、デジタル証明書、ハッシュ関数などのセキュリティ技術を組み合わせる事で、データの盗聴や改ざん、なりすましを防ぐことができる。
VPN	：	Virtual Private Network：バーチャルプライベートネットワーク インターネットのような公衆ネットワークをまたぐ複数のプライベートネットワークを、仮想的に統一されたプライベートなネットワークとして構築する技術。プライベートネットワーク間は IPsec プロトコルのような暗号・認証機能をもつプロトコルで接続される。
ウイルス	：	Virus PC 環境におけるコンピュータウイルスにおいては、ファイルやシステムに寄生・感染（自己複製）する機能をもつプログラムをいう。この場合、システム中に単体として存在し、ネットワークを伝わって移動する「Worm（ワーム）」は、ウイルスとは区別される。また、潜伏機能・発病機能しか持たない「Trojan（トロイの木馬）」も、ウイルスと区別される。

シングルサインオン	：	Single Sign-On ユーザが 1 回のログインで、複数のサーバにアクセスできるようにする機能。ディレクトリサービスと同期して、複数サーバの認証とユーザのアクセス制御を一元管理し、ユーザの利便性と管理機能を向上させる。SSO と呼ばれることもある。
セキュリティホール	：	Security Hole ネットワークやシステム上のセキュリティに関する欠陥のこと。修復をしないとクラッカーからの攻撃に対しシステム全体が破綻する恐れがある。
セキュリティポリシー	：	セキュリティポリシーとは、企業として経営者のセキュリティに対する考え方、及びセキュリティ対策を実施するための基本ポリシーや規程、及び必要なセキュリティレベルを達成するために遵守すべき行為や判断等の基準を明文化したもので、「基本ポリシー」「スタンダード」「プロシジャ」から構成される。
トークンデバイス	：	Token Device IC カードや USB 接続のデバイス等で、デジタル証明書をトークンとして記録したもの。コンピュータのメモリー上には置かないため、盗難、故障などでの漏洩の危険を回避できる。
トロイの木馬	：	Trojan Horse 良性なプログラムのふりをして、実はセキュリティ上の問題を引き起こすプログラムのこと。たとえば有名なフリーソフトウェアと同じ名前で、実はファイルを破壊するプログラム等。
なりすまし	：	「なりすまし」とは、一言で表すと、他人の ID やパスワードを盗み出し、ネットワーク上であたかもその人のようなふりをして不正行為を行うこと。
バイオメトリクス認証	：	Biometrics Authentication 人間の身体的特徴や行動的特徴を抽出して数値化することをバイオメトリクスといい、そのような人間の身体的特徴や行動的特徴を利用して本人確認をすることをバイオメトリクス認証という。 身体的特徴としては、指紋、掌形、顔、虹彩、網膜血管、静脈パターン、DNA や、行動的特長として音紋、サイン、キーストローク等を利用した個人識別が実用化されている。
ハッカー	：	Hacker 本来は、高度なコンピュータの知識を持つものの尊称であったが、最近では、仕事のほか、趣味としてコンピュータに興味を持ち、技術の取得に没入する人の総称として使われている。 また悪意を持ってシステムへの侵入を試みたり、パスワードを探り当てたり、機密情報を探しだそうとする人。(呼び名を分けてクラッカー (cracker) ということも多い)

ファイアウォール　：　Firewall
特定のネットワークセグメントを他のネットワークとの接続部分において防護する考え方であり、外部のインターネットから内部のイントラネットを防護するのが典型的である。 インターネットファイアウォールの場合、通常インターネットサーバーも運用されるので、単純な外部と内部をコントロールする関係にはならない。外部インターネットと内部イントラネットの間に DMZ と呼ばれる境界ネットワークを構築することがある。ファイアウォールの考え方には、このような DMZ の構築も含まれる。ファイアウォールを実現するための技術としては、しばしばパケットフィルタの利用とプロキシの利用が挙げられる。これらは組み合わされて実装されることがある。また、ネットワークベース IDS によるミスユース検出、IP マスカレード等の技術も利用されることがある。

ワーム　：　Worm
コンピュータネットワーク上で、自己のコピーをネットワーク上の他のコンピュータに送り込むことで繁殖するプログラムのこと。コンピュータウイルスと異なり、ファイルに感染したりはしない

ワンタイムパスワード　：　One Time Password：
認証のたびに以前とは異なるパスワードを使用することで、他者が認証されるリスクを軽減化するパスワード機構。

共通鍵暗号方式　：　Conventional Encryption System
データの機密を守る暗号方式の 1 つで、秘密鍵暗号方式 (Secret Key Cryptosystem) ともいう。暗号鍵と復号鍵に同じ鍵を使う方式。

公開鍵暗号方式　：　Public Key Cryptosystem
データの機密を守る暗号方式の1つ。暗号鍵と復号鍵に異なるかぎを使う方式。データを暗号化する際に使う暗号鍵を公開とし、データを復元する復号鍵は非公開とすることでデータの機密を守る方式。

電子透かし　：　Digital Watermarking
電子データ内部に、著作権者などの情報を埋め込む技術。電子データの著作権保護を実現する上での一手法で、著作権者などの情報を、ユーザの操作によって簡単に取り除くことができない形に変換した上で、電子データに埋め込む技術。

電子認証　：　Digital Authentication
広義には、電子的手段を用いて個人認証等を行う技術のことであるが、一般的には、公開鍵暗号技術に基づく個人認証等を行う技術のこと言う。

添付2) 調査票

問１．　貴社（貴校）についてお尋ねします。

(1) 貴社（貴校）の業種は、以下のどれですか。あてはまる番号１つに○をつけて下さい。

業種分類	業　　種
エネルギー	1-1 電力　1-2 ガス　1-3 水道　1-4 石油製造(精製) 1-5 その他(　　)
運輸業	2-1 鉄道・地下鉄　2-2 航空　2-3 陸運　2-4 海運 2-5 倉庫 2-6 その他(　　)
金融	3-1 銀行　3-2 証券　3-3 保険　3-4 クレジット　3-5 消費者金融 3-6 信用金庫/組合　3-7 その他(　　)
情報通信	4-1 新聞　4-2 放送　4-3 通信　4-4 ＩＳＰ 4-5 その他(　　)
医療	5-1 病院　5-2 その他(　　)
製造業	6-1 食品　6-2 繊維　6-3 紙・パルプ　6-4 化学　6-5 薬品 6-6 ゴム・窯業　6-7 非鉄金属　6-8 機械　6-9 電気機器　6-10 造船 6-11 輸送機器　6-12 精密機器　6-13 その他(　　)
農林・水産・鉱業	7-1 農林・水産　7-2 鉱業 7-3 その他(　　)
サービス	8-1 流通・卸売　8-2 小売・飲食　8-3 その他(　　)
不動産・建築	9-1 不動産　9-2 建設 9-3 その他(　　)
教育	10-1 大学　10-2 短大　10-3 専門学校 10-4 その他(　　)
行政サービス	11-1 都道府県　11-2 政令指定都市　11-3 市町村

(2) 貴社（貴校）の年間売上、予算規模等は、およそどの程度ですか。あてはまる番号１つに○をつけて下さい。

１．　～10億円未満	７．500億円～1000億円未満
２．10億円～30億円未満	８．1000億円～3000億円未満
３．30億円～50億円未満	９．3000億円～5000億円未満
４．50億円～100億円未満	10．5000億円～1兆円未満
５．100億円～300億円未満	11．1兆円以上～
６．300億円～500億円未満	12．金額で示せる適切な指標がない

(3) 貴社（貴校）の社員数は、およそ何人くらいですか。あてはまる番号１つに○をつけて下さい。

１．　～100人未満	５．3000～１万人未満
２．100～300人未満	６．１万～３万人未満
３．300～1000未満	７．３万～10万人未満
４．1000～3000人未満	８．10万人以上

(4) 貴社（貴校）の事業所は、およそ何ヶ所ありますか。あてはまる番号１つに○をつけて下さい。

１．１ヶ所	６．30～49 ヶ所
２．２～３ヶ所	７．50～99 ヶ所
３．４～５ヶ所	８．100～300 ヶ所
４．６～９ヶ所	９．301 ヶ所以上
５．10～29 ヶ所	

問２．　貴社（貴校）での情報システム等の環境についておたずねします。

⑴　現在、保有しているコンピュータの種類と台数をお聞かせください。保有している種類すべての番号に○印をつけて、保有しているおおよその台数をご記入してください。

コンピュータの種類	保有台数
１．汎用機／オフコン	台
２．UNIX サーバ	台
３．Windows NT/2000 サーバ	台
４．クライアント（パソコン）	台
５．モバイル端末（データ通信用の携帯電話含む）	台
６．その他（　　）	台

⑵　端末装置（パソコン等）の利用環境は次のどれにあてはまりますか。

１．１人１台の環境が整っている	４．支店や拠点で共有している
２．数人で共有している	５．その他（　　）
３．部・課で共有している	６．端末は利用していない

⑶　ネットワーク接続状況はどの程度ですか。最も近いものに○をつけてください。

１．社内ＬＡＮが敷設されていて、ほとんどのコンピュータがＬＡＮに接続されている	４．社内ＬＡＮは敷設されていないが、今後、敷設を予定している
２．社内ＬＡＮが敷設されていて、半分程度のコンピュータがＬＡＮに接続されている	５．社内ＬＡＮは敷設されておらず、今後、敷設の予定もない
３．社内ＬＡＮが敷設されているが、接続されているコンピュータは少ない	６．その他

⑷　業務は、どの程度コンピュータ化が進んでいますか。最も近いものに○をしてください。

１．ほとんどの業務がコンピュータ化されている	４．コンピュータ化されている業務はまだ少なく、依然として手作業による業務が大半である
２．多くの業務がコンピュータ化されている	５．コンピュータ化されている業務はほとんどなく、手作業による業務がほとんどである
３．半数程度の業務がコンピュータ化されているが、手作業による作業も半数程度ある	６．その他

問３．　貴社（貴校）でのインターネットへの接続状況についておたずねします。

(1) インターネットに接続していますか。

１．接続している	２．接続していないが、現在、接続を計画中	３．接続していないかつ接続の計画もない

(2) インターネットへの接続目的はどこにありますか。あてはまる番号すべてに○をつけてください

１．電子メール	５．オンラインバンキング、トレーディング
２．各種の情報収集	６．社内（校内）拠点間を結ぶ業務用
３．顧客や外部に向けての情報提供	７．その他（　　）
４．インターネット販売	

(3) どのような回線を利用していますか。あてはまる番号に○をつけてください。

１．アナログ電話回線	６．専用回線（256bps 以下）
２．ＩＳＤＮ回線	７．高速専用回線（1.5Mbps 未満）
３．ＡＤＳＬ／ＳＤＳＬ回線	８．超高速専用回線（1.5Mbps 以上）
４．携帯電話回線	９．ＣＡＴＶ回線
５．無線回線	10．その他（　　）

(4) インターネットへの接続点においてどのようなアクセス制御等の対策を行なっていますか。あてはまる番号すべてに○をつけてください。

１．ファイアウォールの導入	６．自動侵入監視システム(IDS)の導入
２．ルータによるプロトコル制御	７．ＤＭＺの構築
３．PROXY サーバの設置	８．アクセスログ収集の強化・充実
４．ID/パスワード認証	９．その他（　　）
５．電子証明書（PKI）	10．特に何も行なっていない

問４．　外部から貴社（貴校）の情報システム（営業支援システム、業務システムなど）へのアクセス環境についておたずねします。

(1) 外部から社内（学内）の情報に接続することを認めていますか。

１．接続を許可しており、社内（学内）にいる場合と同様の機能が提供されている	３．現在、接続を一切禁止しているが、今後接続許可の検討してゆく予定。
２．接続を許可しているが、社内（学内）にいる場合より制限された機能が提供されている	４．現在も、将来も接続を許可しない →**(5)をお答えください**

(2) 接続を認めている場合、接続方法は何ですか。

1.インターネット	２．ダイヤルアップ接続	３．両方使用している

(3) 外部からの接続時に利用している認証方法は何ですか。あてはまる番号すべてに○印をつけてください。

1．ＩＤ/パスワード認証	5．電話番号規制
2．ワンタイムパスワード	6．コールバック
3．電子証明書（PKI）	7．その他(　　)
4．バイオメトリクス（指紋等での認証）	

(4) 利用の目的は何ですか。あてはまる番号すべてに○印をつけてください。

1．メールサーバへのアクセス	5．Web サーバへのアクセス
2．スケジュール等のグループウエアの利用	6．情報システムメンテナンス
3．営業支援システムへのアクセス	7．その他（　　）
4．業務支援システムへのアクセス	

(5) 接続を認めないとお答えの方は、その理由は何ですか。あてはまる番号すべてに○印をつけてください。

1．必要がないため	4．セキュリティポリシー
2．経費がかかるため	5．その他（　　）
3．社内システム、情報を守るため	

問５．　貴社（貴校）の情報システムについておたずねします。

(1) 不正アクセス等により、以下のように社会的に深刻な被害を及ぼす情報システムがありますか。あてはまる番号すべてに○印をつけてください。

1．人命にかかわるシステムがある	7．他人になりすますことのできる情報を扱うシステムがある
2．国防や治安維持、行政機能が脅かされるシステムがある	8．情報の改ざんによる信用低下につながるシステムがある
3．顧客の財産が脅かされるシステムがある	9．社会的に深刻な被害には至らないが、自社にとって深刻な被害に至るシステムがある
4．ライフラインやプラントが停止／暴走してしまうシステムがある	10．その他（　　）
5．社会的活動・経済的活動を脅かすシステムがある	11．深刻な被害となるシステムはない
6．個人のプライバシーが侵害される情報を扱うシステムがある	

(2) 貴社（貴校）では、これまでに、不正アクセス等に限らず、過失や事故を含め、情報システムが原因となり深刻な被害が発生した事がありますか

1．ある	2．ない

（3）被害が発生したことがある場合は、その発生原因、状況を具体的にご記入ください

問６．　問５で、社会的に深刻な被害を及ぼす情報システムがあるとご回答の方に、それらの情報システムでのセキュリティ対策についておたずねします。

（1）システムへの侵入阻止を目的に、どのようなセキュリティ対策を導入していますか。あてはまる番号すべてに○をつけて下さい。

１．ネットワークには接続していない	８．ＩＤと強化パスワード（ワンタイムパスワード、ＩＣカード、電子証明書等）でユーザ認証をしている
２．他のネットワークとは分離した専用のネットワークを構築している	９．ソフトウェアのセキュリティホールに対し、パッチやバージョンアップを行なっている
３．基幹システム専用のファイアウォールを導入している	10．不正アクセスを自動的に検出する仕組みを導入している。
４．ネットワークのアクセスコントロールを行なっている	11．システムへのアクセスログを取得している
５．ＩＤとパスワードでユーザ認識	12．擬似アタックを定期的に行い、対策をチェックしている
６．指定回数以上のログインに失敗すると、ログイン権限の失効機能を組み込んでいる。	13．上記のような対策は行なっていない
７．通信を暗号化する仕組みを導入している	

（2）システムに侵入されてしまった場合のセキュリティ対策として、どのようなセキュリティ対策を導入していますか。あてはまる番号すべてに○をつけて下さい。

１．システムの冗長化（二重化等）を行っている。	７．不正行為を自動検知するシステムを導入している
２．ネットワークの冗長化を行なっている	８．プログラムの改ざんを自動検知するシステムを導入している
３．データのバックアップ対策を行なっている	９．コンソール以外からの設定変更を出来ない設定にしている
４．重要データを暗号化して保存	10．データ突合せ確認等の監査プログラムを導入
５．重要データを暗号化して送受信	11．緊急時には自動停止する仕組みを導入
６．システムへのアクセスログを取得している	12．上記のような対策は行なっていない

問７．　貴社（貴校）で、この１年間に発生した、不正アクセス等の被害状況についておたずねします。

(1) 被害にあいましたか。

１．被害にあった　　２．被害にあわなかった　３．不明

(2) 発生した被害について、あてはまる番号すべてに○印をつけてください。また、被害にあった件数とそのうちで何らかの対策をしていた件数についてご記入ください。

不正アクセス等の内容	被害にあった 件数(件)	対策してあった 件数(件)
1. ホームページの改ざん		
2. メールの不正中継		
3. 踏み台		
4. サービス停止		
5. システム破壊		
6. 盗聴		
7. なりすまし		
8. ウイルス感染		
9. 情報漏洩		
10. その他（　　）		

(3) 被害にあった不正アクセス等はどこからのものでしたか。あてはまる番号すべてに○印をつけて下さい。

１．社(学)外(国内)から	４．その他（　　）
２．社(学)外(国外)から	５．不明
３．社(学)内から	

(4) 被害にあった時の対応はどのように行ないましたか

１．自社（自校）で対応	３．専門業者への相談
２．専門業者へのアウトソーシング	４．対応はとっていない

(5) 被害を受けてから、実際にお取りになった対応策は何ですか。あてはまる番号すべてに○印をつけてください。

１．ファイアウォールの設置／強化	７．不必要なサービスの停止
２．最新パッチの適応	８．セキュリティポリシーの策定・見直し
３．ウイルス対策製品の導入／強化	９．不正アクセスが行われていないかネットワークの監視
４．ソフトウェアのバージョンアップ	10. システム上にセキュリティホールがないか検査、診断
５．認証機能の導入／強化	11. その他（　　）
６．ネットワークの再構築	12. 不明

(6) どこに届け出ましたか。あてはまる番号すべてに○印をつけてください。

1．警察	4．国民生活センター
2．ＩＰＡ（情報処理振興事業協会）	5．その他（　　）
3．ＪＰＣＥＲＴ／ＣＣ（コンピュータ緊急対応センター）	6．届け出なかった

(7) 届け出なかったとお答えの方は、その理由は何ですか。あてはまる番号すべてに○印をつけてください。

1．企業（学校）の評判が悪くなるので	5．問題解決にならないので
2．社内（学内）で対応できたので	6．面倒なので
3．届け出義務がないので	7．その他（　　）
4．大した被害ではなかったので	

問８．　貴社（貴校）での情報セキュリティ対策についておたずねします。

(1) どの程度の必要性を感じていますか。

1．非常に感じている	3．あまり感じていない
2．感じている	4．感じていない

(2) 情報セキュリティの運用・管理のための企業（学校）が認めた組織がありますか。

1．　ある	2．　ない

(3) 情報セキュリティ管理者または担当者を置いていますか。

1．専従の担当者を設置している	3．情報システム運用管理者以外がセキュリティについても兼務している
2．情報システム運用管理者がセキュリティについても兼務している	4．担当者は設置していない

(4) 情報セキュリティ対策のあり方に関するセキュリティポリシー（基本方針・規定）を策定していますか。

1．策定してある	4．策定しておらず、今後も策定の予定なし
2．現在策定を進めている	5．必要ない
3．策定してないが、今後策定をする予定	

(5) セキュリティポリシー（基本方針・規定）ではどのようなことを規定していますか。あてはまる番号すべてに○をつけて下さい。

1．情報セキュリティの基本方針	7．重要情報へのアクセスの管理規定
2．情報セキュリティ管理組織	8．システム開発及びメンテナンス
3．情報資産（データ）の分類・管理規準	9．セキュリティ監査の基準
4．情報セキュリティ教育	10．非常事態発生時における応対
5．情報システムの設置環境	11．法的要求への対応
6．情報システムの運用管理規定	12．その他（　　）

(6) セキュリティポリシーに基づき、具体的な操作や業務処理手順などを規定したセキュリティガイドラインを定めていますか。

1．定めている	4．定めていない
2．現在作成中である	5．必要ない
3．作成を検討している	

(7) 不正アクセス等により被害が発生した時のための非常事態発生時における応対計画を定めていますか。

1．定めている	4．定めていない
2．現在作成中である	5．必要ない
3．作成を検討している	

(8) 不正アクセス等により被害が発生した時のための非常事態発生時における応対計画を定めている場合、どのようなことが盛り込まれていますか。あてはまる番号すべてに○をつけて下さい。

1．社内報告経路・指揮系統	8．原因の究明
2．システムの縮退、代替運用手順	9．犯人の追及
3．回復・復旧手順	10. 警察への連絡
4．サービス停止の判断基準	11. ＪＰＣＥＲＴ/ＣＣへの連絡
5．証拠（状況・ログ等）の保全	12. その他関連機関への連絡
6．サービス利用者の広報活動	13. 上記のような事項は記載されていない
7．マスコミへの広報活動	14. その他（　　）

(9) 貴社（貴校）情報システムのセキュリティ対策に関し、第三者機関による評価・認証を取得、又は取得を予定しておりますか。あてはまる番号すべてに○をつけて下さい

1．ＩＳＯ１５４０８	4．プライバシーマーク
2．ＢＳ７７９９	5．その他（　　）
3．ＩＳＭＳ	6．取得の予定なし

(10) セキュリティ監査に対する取り組みについてお聞かせください。

1．実施している	3．実施をしていないが必要性を感じる
2．実施を予定している	4．実施の必要性を感じない(実施していない)

(11) セキュリティ監査はどの程度の頻度で実施していますか。

1．３ヵ月ごとに	4．隔年（２年）ごとに
2．半年ごとに	5．その他（　　）
3．１年ごとに	6．特に決まっていない（不定期）

問９．　貴社（貴校）での情報セキュリティ教育に関する取り組みについてお聞かせください。

(1) 情報セキュリティ教育の実施状況をお答えください

１．実施している	３．実施をしていないが必要性を感じる
２．実施を予定している	４．実施の必要性を感じない（実施していない）→問 10 へ

(2) 情報セキュリティ教育の内容について、具体的にお答えください。

(3) 情報セキュリティ教育の目的は何ですか。あてはまる番号すべてに○印をつけてください。

１．ポリシーの普及	４．自己啓発
２．社内不正行為の防止	５．その他(　　)
３．セキュリティに対する意識の向上	

(4) 情報セキュリティ教育はどのくらいの頻度で実施していますか。

１．月に１回以上	４．２,３年に１回
２．年に数回	５．その他(　　)
３．年に１回	

(5) 情報セキュリティ教育の対象はどなたですか。 あてはまる番号すべてに○印をつけてください。

１．新規採用者	５．関連会社の社員・職員
２．管理者	６．取引先社員・職員
３．正社員・職員	７．その他(　　)
４．派遣社員	

問１０．　貴社（貴校）でのアクセスログの取得状況についておたずねします。

(1) どのようなログを取得していますか。あてはまる番号すべてに○印をつけてください。

１．トランザクションログ	４．ＩＤＳのログ
２．サーバ上のアクセスログ	５．その他(　　)
３．ファイアウォール上のログ	６．取得していない

(2) ログの保管期間はどの程度ですか。

１．１週間	５．１年間
２．１ヵ月	６．特に期間は決まっていない
３．３ヵ月	７．その他（　　）
４．６ヵ月	８．保管していない

(3) 情報セキュリティ対策としてログの解析の頻度はどのくらいですか。

1．問題発生時	5．３ヵ月毎
2．毎日	6．その他(　　)
3．毎週	7．実施していない
4．毎月	

問１１．　貴社（貴校）での不正アクセス等を検知する対策についておたずねします。

(1) 不正アクセス等を検知する対策を実施していますか。

1．実施している	3．実施をしていないが必要性を感じる
2．実施を予定している	4．実施の必要性を感じない（実施していない)

(2) 提供されている機能で不足している点や不満に思っている点は何ですか。あてはまる番号すべてに○印をつけてください。

1．誤検出が多すぎる	4．使いこなせない
2．日本語化されていない	5．その他(　　)
3．価格が高い	6．特に不足点や不満点はない

問１２．　貴社（貴校）での具体的な攻撃に対する情報セキュリティ対策についておたずねします。

(1) ＤｏＳ攻撃に対する対策についておたずねします。どのような対策を実施していますか。あてはまる番号すべてに○印をつけてください。

1．ファイアウォールのＤｏＳ対策機能	4．サーバプログラムへの最新パッチの適応
2．ルータのＤｏＳ対策機能	5．その他(　　)
3．ＩＤＳによるＤｏＳ対策機能	6．実施していない

(2) スパムメールの不正中継対策についておたずねします。どのような対策を実施していますか。あてはまる番号すべてに○印をつけてください。

1．メールサーバの設定の修正	5．メールサーバへの対策ソフトの導入
2．メールソフトのバージョンアップ	6．その他(　　)
3．ＩＤＳによる検知	7．実施していない
4．ファイアウォールによる遮断	

(3) コンピュータウイルス対策に対する取り組みについておたずねします。どのような対策を実施していますか。あてはまる番号すべてに○印をつけてください。

1．ワクチンソフト（クライアント）の使用	5．ファイル等のダウンロードの制限
2．ワクチンソフト（サーバ）の使用	6．その他(　　)
3．パターンファイルの更新	7．実施していない
4．許可されないソフトウェアのインストール制限	

(4)　この１年間にコンピュータウイルス感染を受けた被害の規模はどの程度でしたか。

１．全社〔全校〕的な被害	４．その他（　　）
２．局所的な被害	５．被害なし
３．感染したが実害なし	

(5) コンピュータウイルスの主な感染ルートは何ですか。あてはまる番号すべてに○印をつけて下さい。

１．電子メール	５．ＷＥＢアクセス
２．社外からの記憶媒体	６・その他（　　）
３．社内からの記憶媒体	７．不明
４．ダウンロードしたソフトウェア	

(6) 通信の機密保持に関する暗号化についておたずねします。どのような用途で暗号化を実施していますか。あてはまる番号すべてに○印をつけて下さい。

１．暗号メール	４．クレジットカード番号等の重要なトラザクションの転送
２．記録媒体上の情報（ファイルの暗号化）	５．その他（　　）
３．認証情報（電子証明書）	６．利用していない

問１３．　貴社（貴校）でのセキュリティサービス業者の利用状況についておたずねします。

(1) どのようなサービスを利用しましたか。あてはまる番号すべてに○印をつけてください。

１．セキュリティ診断	８．ハウジングサービス
２．リスク分析	９．社員教育
３．ポリシー策定	10．セキュリティ監視
４．セキュリティ監査	11．ウイルス監視
５．ログ解析	12．セキュアシステム構築
６．認証サービス	13．その他(　　)
７．ソフトウェアメンテナンス	14．利用していない

(2) 利用していないとご回答の方は、その理由をお答えください。あてはまる番号すべてに○印をつけてください。

１．社内、（校内）に高い専門性やノウハウ、技術力があり、必要性がない
２．社内、（校内）担当者だけで必要な人員が確保されているため、必要性がない
３．社内、（校内）にノウハウの蓄積を行いたい
４．コストを負担できない
５．要求に合致するサービスが提供されていない
６．機密情報の漏洩につながることが懸念される
７．その他（具体的に　　）

(3) 今後新たにどのようなサービスを利用したいと考えていますか。あてはまる番号すべてに○印をつけてください。

1．セキュリティ診断	8．ハウジングサービス
2．リスク分析	9．社員教育
3．ポリシー策定	10．セキュリティ監視
4．セキュリティ監査	11．ウイルス監視
5．ログ解析	12．セキュアシステム構築
6．認証サービス	13．その他(　　)
7．ソフトウェアメンテナンス	14．利用したいと思わない

問１４．　貴社（貴校）での情報システム関連重要施設への入退室管理についておたずねします。

(1) どのような場所､区画を対象に実施していますか。あてはまる番号すべてに○印をつけてください。

1．敷地内全体	5．部屋(マシン室)
2．建物内全体	6．その他(　　)
3．フロア全体	7．実施していない
4．部屋(資料室)	

(2) 入退室の管理方法は何ですか。あてはまる番号すべてに○印をつけてください。

1．記帳	5．ビデオカメラ
2．暗証番号	6．警備員
3．磁気カード	7．バイオメトリクス(指紋等での認証)
4．ＩＣカード	8．その他(　　)

問１５．　貴社（貴校）での情報セキュリティ対策のための情報の入手についておたずねします。

(1) どのようにして入手していますか。あてはまる番号すべてに○印をつけてください。

1．ベンダーの営業マンから	7．セキュリティ関連のホームページから
2．ベンダーのホームページから	8．他企業の担当者との情報交換
3．ベンダーの電子メールから	9．関係省庁・団体等のガイドライン
4．専門雑誌や新聞から	10．その他(　　)
5．外部のセミナーへの参加	11．入手していない
6．セキュリティ専門会社から	

(2) 情報セキュリティ対策を実施するうえで参考にしているものは何ですか。あてはまる番号すべてに○印をつけてください。

1．情報システム安全対策指針（国家公安委員会）	6．金融機関等コンピュータシステムの安全対策基準（ＦＩＳＣ：金融情報システムセンター）
2．情報セキュリティポリシーに関するガイドライン（情報セキュリティ対策推進室）	7．警察庁のホームページ
3．情報システム安全対策基準（経済産業省）	8．ＩＰＡ（情報処理振興事業協会）のホームページ
4．　コンピュータ不正アクセス対策基準（経済産業省）	9．ＪＰＣＥＲＴ／ＣＣ（コンピュータ緊急対応センター）のホームページ
5．　情報通信ネットワーク安全・信頼性基準の概要（総務省）	10．その他（　　）

(3) 現在、情報セキュリティ対策のために提供されている情報で不足している点や不満な点は何ですか。あてはまる番号すべてに○印をつけてください。

1．情報の公開が遅い	5．日本語に訳されていないので利用しにくい
2．必要ではない情報が多い	6．その他
3．情報の絶対数が少ない	（　　）
4．具体的に何をやれば良いのかわからない	7．特に不足点や不満点はない

問１６．　貴社（貴校）での情報セキュリティ対策を実施するうえでの問題点は何ですか。あてはまる番号すべてに○印をつけてください。

1．コストがかかりすぎる	6．どこまで行えば良いのか基準が示されていない
2．費用対効果が見えない	7．トップの理解が得られない
3．教育訓練が行き届かない	8．情報を資産として考える習慣がない
4．従業員への負担がかかりすぎる	9．最適なツール・サービスがない
5．対策を構築するノウハウが不足している	10．その他　（　　）

問１７．　セキュリティ対策を講ずるにあたって困難に感じていること、不正アクセスを受けた場合、不安に感じること等、ご意見をお聞かせください。

問１８．　行政に望むセキュリティ対策について、ご意見をお聞かせください。

※ご協力いただいた方に、謝礼をお送りさせていただきますので、ご担当者名をご記入ください。

貴社(貴校)名			
所在地・電話番号	〒　　－　　ＴＥＬ(　　)　　－		
お名前 (ご記入者の)		役職名	
所属部門名		担当職種	

＊長時間ご協力ありがとうございました。返送用の封筒に入れてご返送ください。