『重要インフラにおけるサイバーテロ対策状況に関する調査結果』

警　察　庁

調査概要

調査対象　東証一部上場企業から無作為抽出した1，151社
特定業種の売上高上位から抽出した1，019社
合計2，000社
（うち170社は東証一部上場企業かつ特定業種企業）

調査期間　平成12年3月6日～3月17日

調査方法　郵送による調査

回答数		
	東証一部上場企業からの無作為抽出対象	476社（41．4%）
	特定業種の売上高上位から抽出した対象	459社（45．0%）
	合計	844社（42．2%）

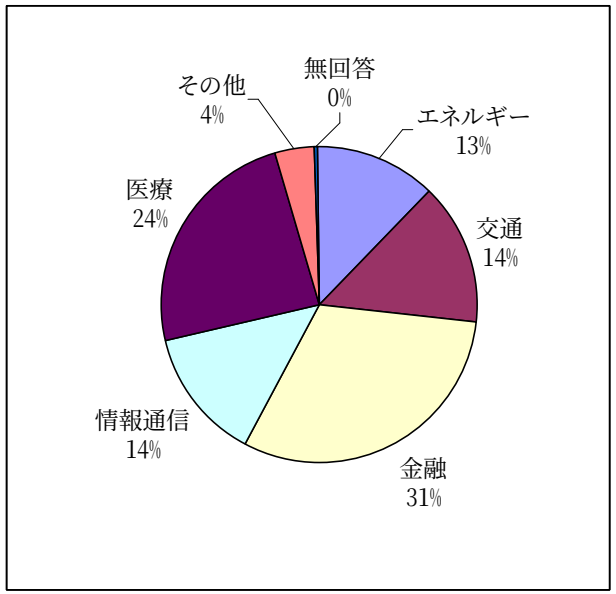
※特定業種とは、**重要な社会インフラ** を担う、エネルギー、交通、金融、情報通信、医療機関。

問1-1 貴社の業種は、以下のどれですか。（○はひとつ） **特定重要業種**

調査対象グループ：特定重要業種

n=459　n-x=458

業種カテゴリ	業種	回答数	割合	割合 除く無回答
エネルギー	電力	23	5.0%	5.0%
	ガス	13	2.8%	2.8%
	原子力関連	1	0.2%	0.2%
	石油卸	6	1.3%	1.3%
	石油製造	6	1.3%	1.3%
	水道局	9	2.0%	2.0%
	エネルギー計	**58**	**12.6%**	**12.7%**
交通	鉄道・地下鉄	54	11.8%	11.8%
	航空	12	2.6%	2.6%
	交通計計	**66**	**14.4%**	**14.4%**
金融	銀行	84	18.3%	18.3%
	証券	10	2.2%	2.2%
	信販	11	2.4%	2.4%
	その他金融機関	35	7.6%	7.6%
	金融計	**140**	**30.5%**	**30.6%**
情報通信	新聞	15	3.3%	3.3%
	通信	30	6.5%	6.6%
	放送	16	3.5%	3.5%
	ｲﾝﾀｰﾈｯﾄｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ	2	0.4%	0.4%
	情報通信計	**63**	**13.7%**	**13.8%**
医療	病院・医院	112	24.4%	24.5%
	医療計	**112**	**24.4%**	**24.5%**
その他	その他サービス	5	1.1%	1.1%
	農林水産	1	0.2%	0.2%
	不動産	1	0.2%	0.2%
	建設	1	0.2%	0.2%
	非鉄/金属製品	1	0.2%	0.2%
	その他製造	1	0.2%	0.2%
	その他	9	2.0%	2.0%
	その他計	**19**	**4.1%**	**4.1%**
無回答	無回答	1	0.2%	-
総計		**459**	**100.0%**	**100.0%**



総計459社のうち91社は東証一部上場企業でもある。

問1-1 貴社の業種は、以下のどれですか。（○はひとつ） **東証一部上場企業**

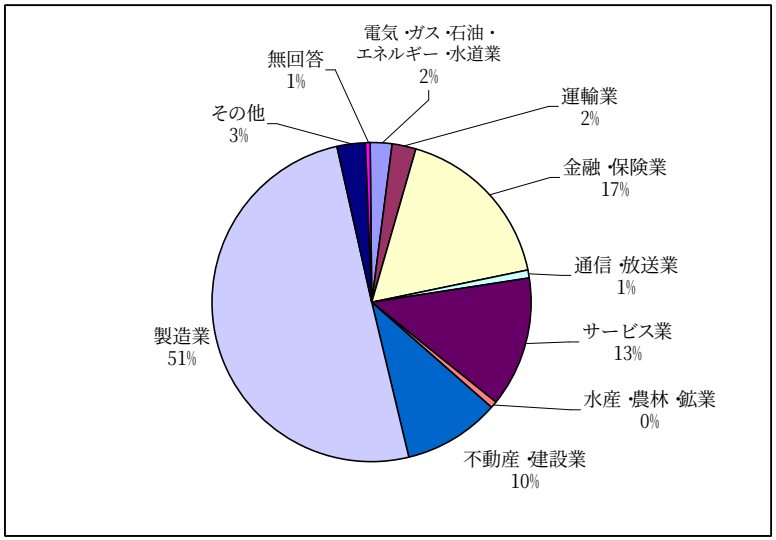
調査対象グループ:東証一部上場企業

業種カテゴリ	業種	回答数	割合	割合 除く無回答
電気・ガス・石油・エネルギー・水道業	電力	6	1.3%	1.3%
	ガス	1	0.2%	0.2%
	石油卸	1	0.2%	0.2%
	石油製造	3	0.6%	0.6%
	水道局	0	0.0%	0.0%
	電気・ガス・石油・エネルギー・水道業計	**11**	**2.3%**	**2.3%**
運輸業	鉄道・地下鉄	10	2.1%	2.1%
	航空	1	0.2%	0.2%
	運輸業計	**11**	**2.3%**	**2.3%**
金融・保険業	銀行	62	13.0%	13.1%
	証券	5	1.1%	1.1%
	保険	6	1.3%	1.3%
	信販	4	0.8%	0.8%
	その他金融機関	6	1.3%	1.3%
	金融・保険業計	**83**	**17.4%**	**17.5%**
通信・放送業	通信	2	0.4%	0.4%
	放送	1	0.2%	0.2%
	ｲﾝﾀｰﾈｯﾄｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ	0	0.0%	0.0%
	通信・放送業計	**3**	**0.6%**	**0.6%**
サービス業	**病院・医院**	0	0.0%	0.0%
	流通・卸売	25	5.3%	5.3%
	小売・飲食	21	4.4%	4.4%
	その他サービス	17	3.6%	3.6%
	サービス業計	**63**	**13.2%**	**13.3%**
製造業	食品	26	5.5%	5.5%
	繊維	13	2.7%	2.7%
	紙・パルプ	6	1.3%	1.3%
	化学	29	6.1%	6.1%
	医療品	7	1.5%	1.5%
	ゴム・窯業	9	1.9%	1.9%
	鉄鋼	12	2.5%	2.5%
	非鉄/金属製品	13	2.7%	2.7%
	機械	22	4.6%	4.7%
	電気機器	34	7.1%	7.2%
	造船	1	0.2%	0.2%
	輸送用機器	32	6.7%	6.8%
	精密機器	12	2.5%	2.5%
	その他製造	25	5.3%	5.3%
	製造業計	**241**	**50.6%**	**51.0%**

n=476　n-x=473

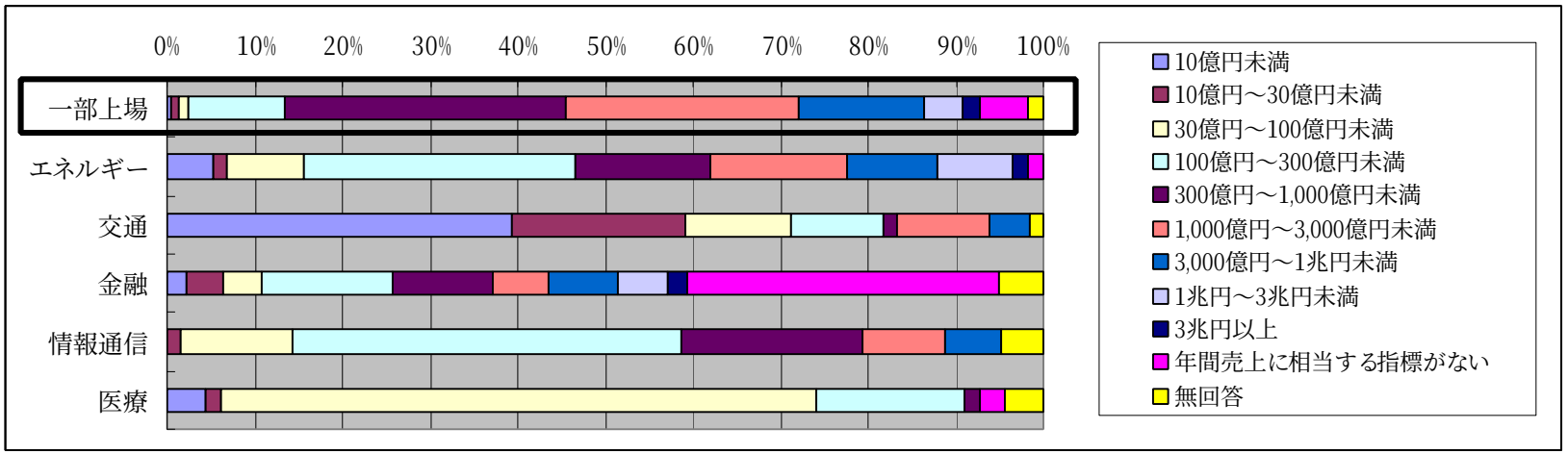
業種カテゴリ	業種	回答数	割合	割合 除く無回答
水産・農林・鉱業	農林水産	1	0.2%	0.2%
	鉱業	1	0.2%	0.2%
	水産・農林・鉱業計	**2**	**0.4%**	**0.4%**
不動産・建設業	不動産	7	1.5%	1.5%
	建設	39	8.2%	8.2%
	不動産・建設業計	**46**	**9.7%**	**9.7%**
その他	その他	13	2.7%	2.7%
	その他計	**13**	**2.7%**	**2.7%**
無回答	無回答	3	0.6%	-
総計		**476**	**100.0%**	**100.0%**

総計476のうち91社は特定業種企業でもある。



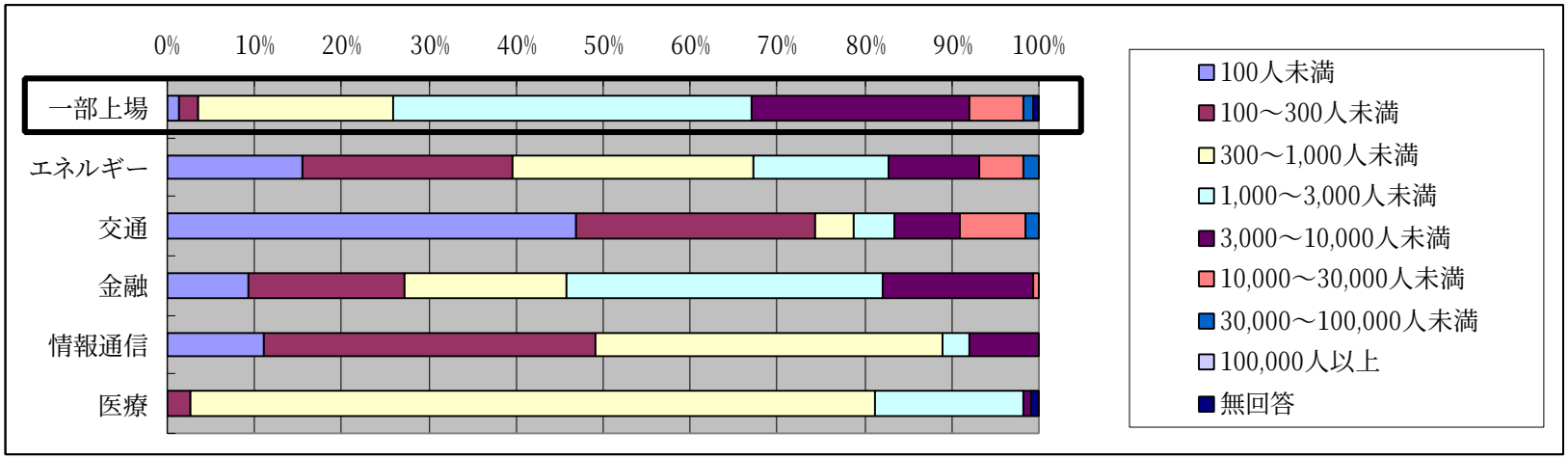
問1-2 貴社の年間売上は、およそどの程度ですか。（○は一つ）

	一部上場 n=476	エネルギー n=58	交通 n=66	金融 n=140	情報通信 n=63	医療 n=112
10億円未満	0.4%	5.2%	39.4%	2.1%	0.0%	4.5%
10億円～30億円未満	0.8%	1.7%	19.7%	4.3%	1.6%	1.8%
30億円～100億円未満	1.1%	8.6%	12.1%	4.3%	12.7%	67.9%
100億円～300億円未満	11.1%	31.0%	10.6%	15.0%	44.4%	17.0%
300億円～1,000億円未満	32.1%	15.5%	1.5%	11.4%	20.6%	1.8%
1,000億円～3,000億円未満	26.5%	15.5%	10.6%	6.4%	9.5%	0.0%
3,000億円～1兆円未満	14.3%	10.3%	4.5%	7.9%	6.3%	0.0%
1兆円～3兆円未満	4.4%	8.6%	0.0%	5.7%	0.0%	0.0%
3兆円以上	1.9%	1.7%	0.0%	2.1%	0.0%	0.0%
年間売上に相当する指標がない	5.7%	1.7%	0.0%	35.7%	0.0%	2.7%
無回答	1.7%	0.0%	1.5%	5.0%	4.8%	4.5%



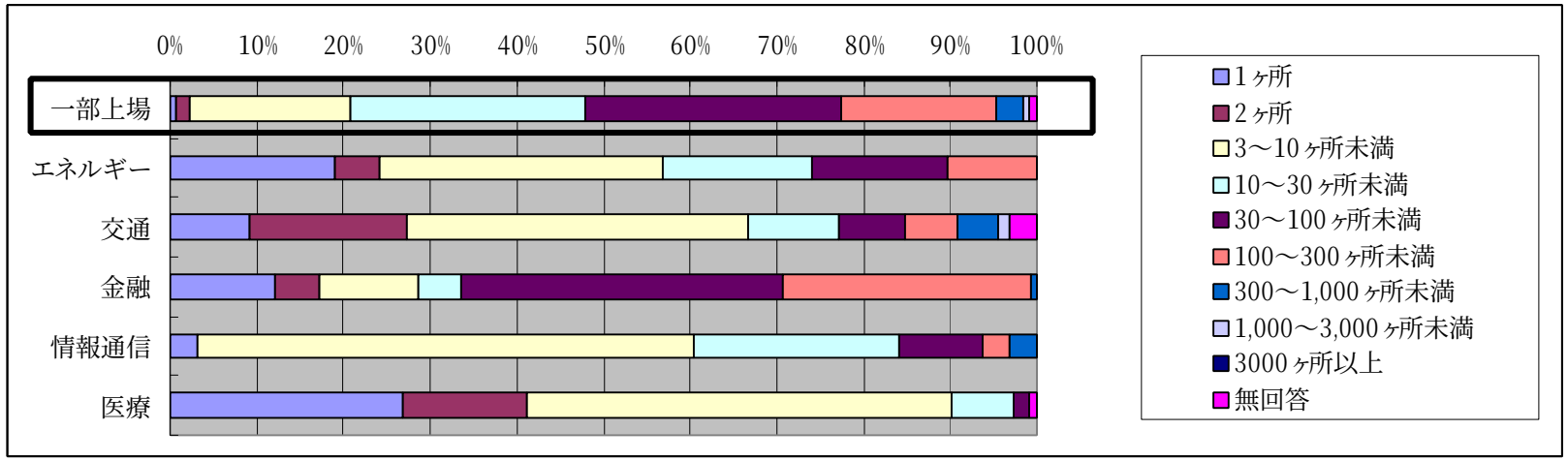
問1-3 貴社の社員数は、およそ何人くらいですか。（○は一つ）

	一部上場 n=476	エネルギー n=58	交通 n=66	金融 n=140	情報通信 n=63	医療 n=112
100人未満	1.3%	15.5%	47.0%	9.3%	11.1%	0.0%
100～300人未満	2.3%	24.1%	27.3%	17.9%	38.1%	2.7%
300～1,000人未満	22.3%	27.6%	4.5%	18.6%	39.7%	78.6%
1,000～3,000人未満	41.2%	15.5%	4.5%	36.4%	3.2%	17.0%
3,000～10,000人未満	25.0%	10.3%	7.6%	17.1%	7.9%	0.9%
10,000～30,000人未満	6.3%	5.2%	7.6%	0.7%	0.0%	0.0%
30,000～100,000人未満	1.1%	1.7%	1.5%	0.0%	0.0%	0.0%
100,000人以上	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
無回答	0.6%	0.0%	0.0%	0.0%	0.0%	0.9%



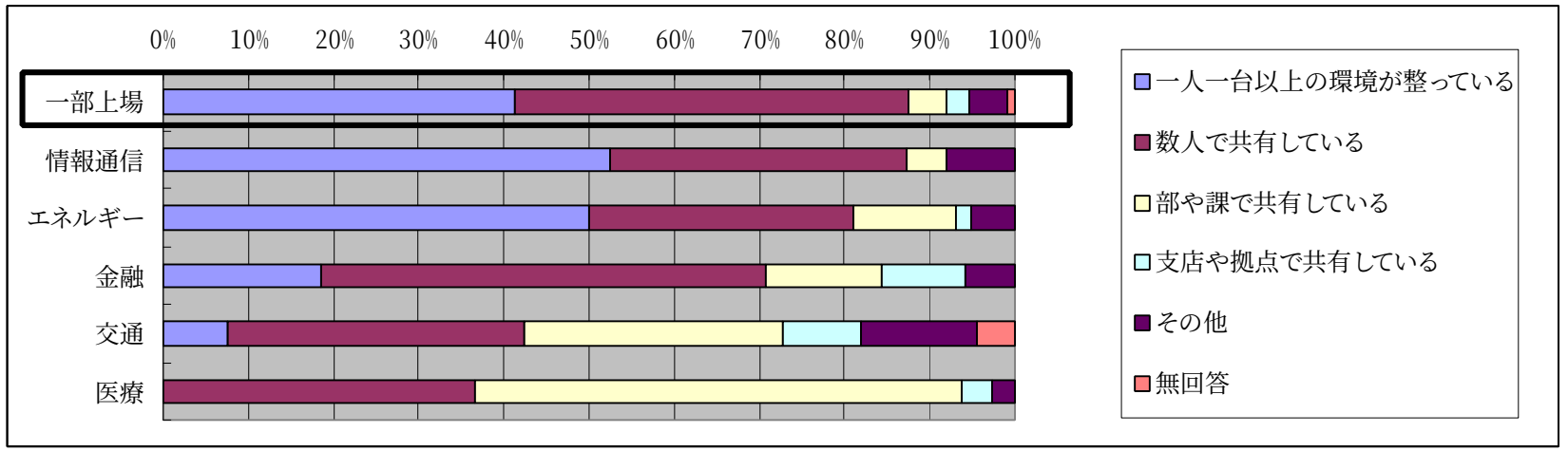
問1-4 貴社の事業所（社員が常駐している拠点）は、およそ何ヶ所くらいありますか。
（○は一つ）

	一部上場 n=476	エネルギー n=58	交通 n=66	金融 n=140	情報通信 n=63	医療 n=112
1ヶ所	0.6%	19.0%	9.1%	12.1%	3.2%	26.8%
2ヶ所	1.7%	5.2%	18.2%	5.0%	0.0%	14.3%
3～10ヶ所未満	18.5%	32.8%	39.4%	11.4%	57.1%	49.1%
10～30ヶ所未満	27.1%	17.2%	10.6%	5.0%	23.8%	7.1%
30～100ヶ所未満	29.4%	15.5%	7.6%	37.1%	9.5%	1.8%
100～300ヶ所未満	18.1%	10.3%	6.1%	28.6%	3.2%	0.0%
300～1,000ヶ所未満	3.2%	0.0%	4.5%	0.7%	3.2%	0.0%
1,000～3,000ヶ所未満	0.6%	0.0%	1.5%	0.0%	0.0%	0.0%
3000ヶ所以上	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
無回答	0.8%	0.0%	3.0%	0.0%	0.0%	0.9%



問2 貴社のコンピュータ（汎用コンピュータの端末やPCなど）の利用環境はどの程度ですか。貴社の状況に最も近いものに○をつけてください。（○は一つ）

	一部上場 n=476	情報通信 n=63	エネルギー n=58	金融 n=140	交通 n=66	医療 n=112
一人一台以上の環境が整っている	41.4%	52.4%	50.0%	18.6%	7.6%	0.0%
数人で共有している	46.2%	34.9%	31.0%	52.1%	34.8%	36.6%
部や課で共有している	4.4%	4.8%	12.1%	13.6%	30.3%	57.1%
支店や拠点で共有している	2.5%	0.0%	1.7%	10.0%	9.1%	3.6%
その他	4.6%	7.9%	5.2%	5.7%	13.6%	2.7%
無回答	0.8%	0.0%	0.0%	0.0%	4.5%	0.0%

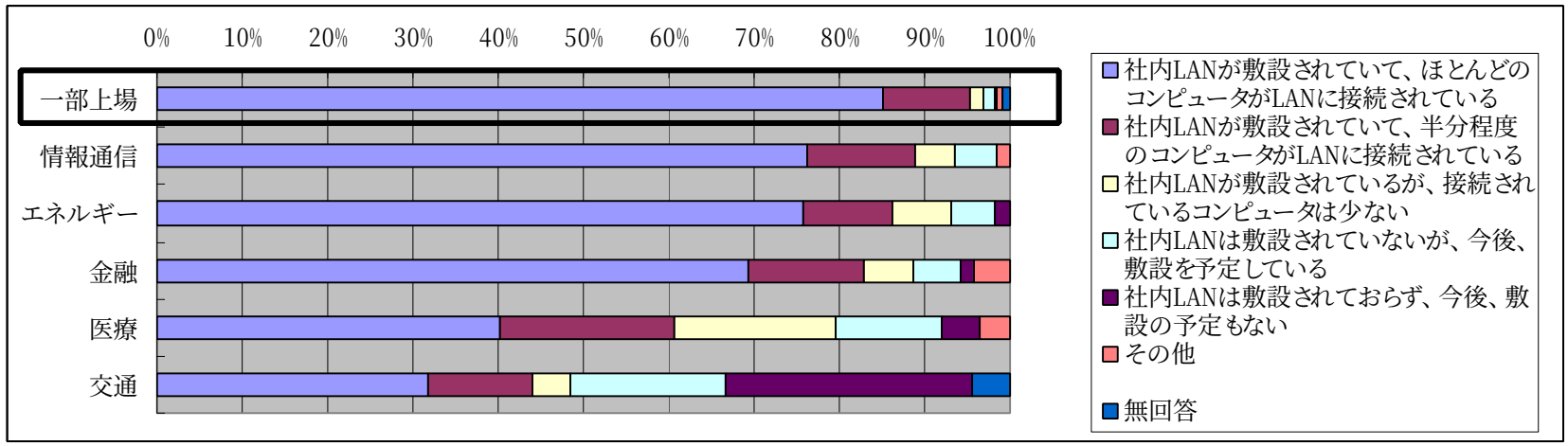


Point

- 一部上場企業では、4割以上が1人1台の端末・PC環境となっている。また、情報通信、エネルギーの業種では、一般の企業よりも情報化（PC化）が推進されている。医療機関においては、数人以上での共有が基本的な利用形態である。

問3 貴社のネットワーク接続状況はどの程度ですか。貴社の状況に最も近いものに○をつけてください。（○は一つ）

	一部上場 n=476	情報通信 n=63	エネルギー n=58	金融 n=140	医療 n=112	交通 n=66
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	85.1%	76.2%	75.9%	69.3%	40.2%	31.8%
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	10.3%	12.7%	10.3%	13.6%	20.5%	12.1%
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	1.5%	4.8%	6.9%	5.7%	18.8%	4.5%
社内LANは敷設されていないが、今後、敷設を予定している	1.5%	4.8%	5.2%	5.7%	12.5%	18.2%
社内LANは敷設されておらず、今後、敷設の予定もない	0.2%	0.0%	1.7%	1.4%	4.5%	28.8%
その他	0.6%	1.6%	0.0%	4.3%	3.6%	0.0%
無回答	0.8%	0.0%	0.0%	0.0%	0.0%	4.5%

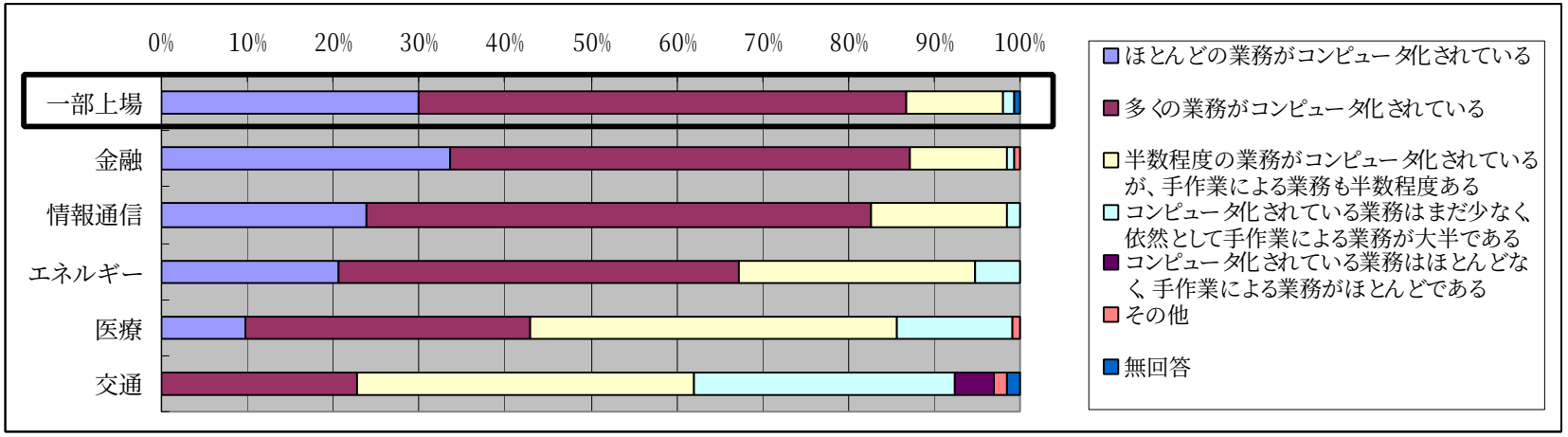


Point

- 情報通信やエネルギーといった重要インフラを担う企業よりも、一般の企業の方がよりネットワーク化されている。
- 今後の予定も含めると、交通機関以外では9割以上が社内LAN環境が整備される状況となる。

問4 貴社の業務は、どの程度コンピュータ化が進んでいますか。貴社の状況に最も近いものに○をつけてください。（○は一つ）

	一部上場 n=476	金融 n=140	情報通信 n=63	エネルギー n=58	医療 n=112	交通 n=66
ほとんどの業務がコンピュータ化されている	30.0%	33.6%	23.8%	20.7%	9.8%	0.0%
多くの業務がコンピュータ化されている	56.7%	53.6%	58.7%	46.6%	33.0%	22.7%
半数程度の業務がコンピュータ化されているが、手作業による業務も半数程度	11.3%	11.4%	15.9%	27.6%	42.9%	39.4%
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	1.3%	0.7%	1.6%	5.2%	13.4%	30.3%
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	0.0%	0.0%	0.0%	0.0%	0.0%	4.5%
その他	0.0%	0.7%	0.0%	0.0%	0.9%	1.5%
無回答	0.6%	0.0%	0.0%	0.0%	0.0%	1.5%

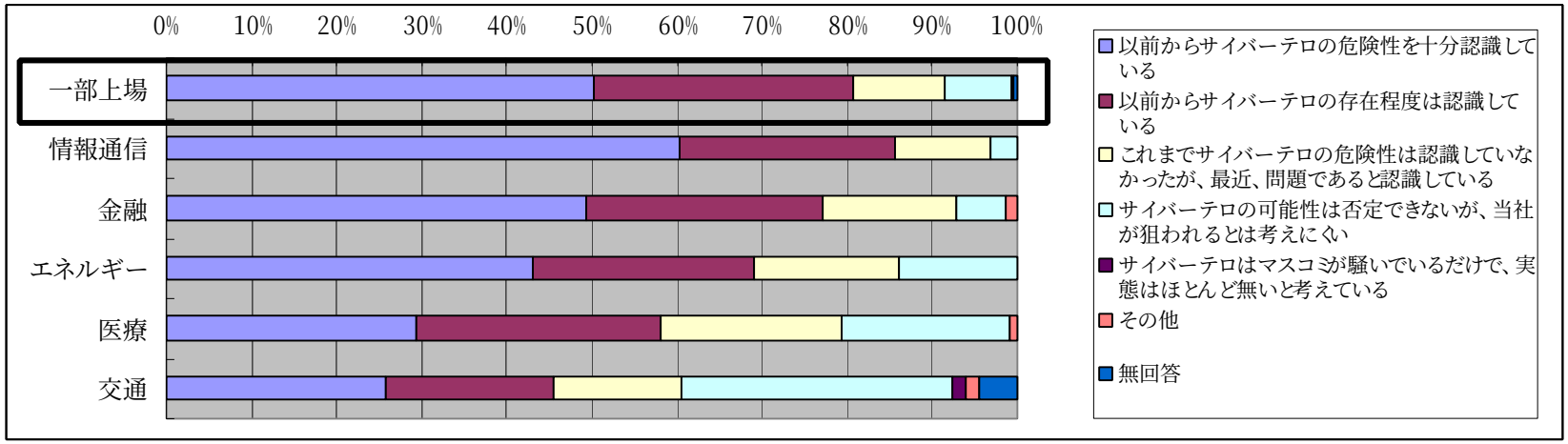


Point

- 一部上場企業、特定業種企業のいずれも業務のコンピュータ化が促進されている。交通については、コンピュータを使用しない業務も依然多く残っている状況である。

問5 貴社では、このようなサイバーテロの危険性に対して、どのような認識をしていますか。貴社の状況に最も近いものに○をつけてください。（○は一つ）

	一部上場 n=476	情報通信 n=63	金融 n=140	エネルギー n=58	医療 n=112	交通 n=66
以前からサイバーテロの危険性を十分認識している	50.21%	60.32%	49.29%	43.10%	29.46%	25.76%
以前からサイバーテロの存在程度は認識している	30.46%	25.40%	27.86%	25.86%	28.57%	19.70%
これまでサイバーテロの危険性は認識していなかったが、最近、問題であると認識している	10.71%	11.11%	15.71%	17.24%	21.43%	15.15%
サイバーテロの可能性は否定できないが、当社が狙われるとは考えにくい	7.98%	3.17%	5.71%	13.79%	19.64%	31.82%
サイバーテロはマスコミが騒いでいるだけで、実態はほとんど無いと考えている	0.00%	0.00%	0.00%	0.00%	0.00%	1.52%
その他	0.21%	0.00%	1.43%	0.00%	0.89%	1.52%
無回答	0.42%	0.00%	0.00%	0.00%	0.00%	4.55%

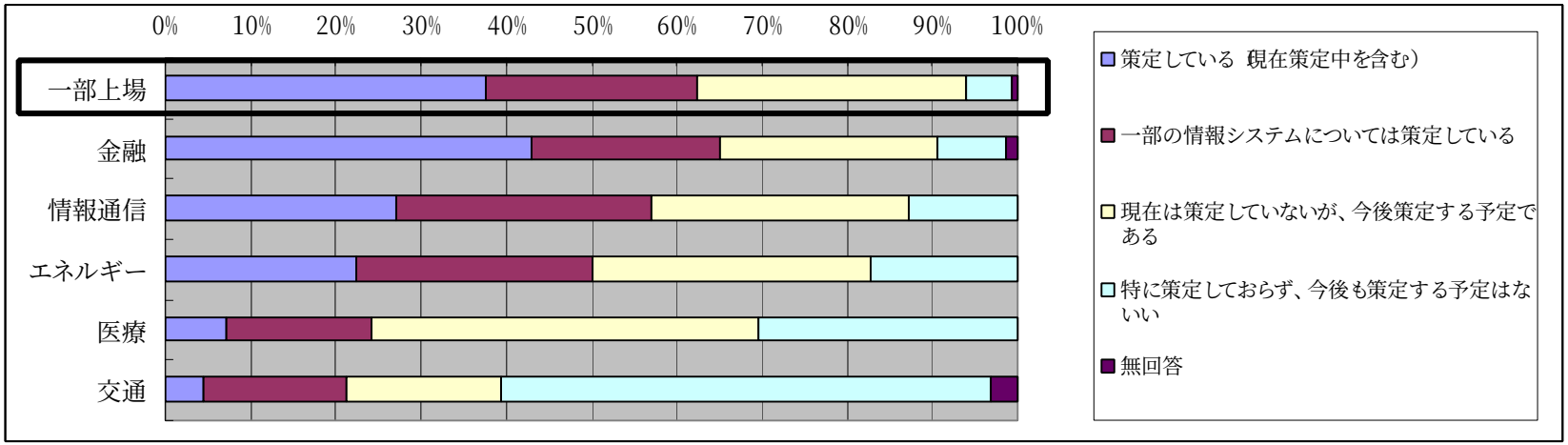


Point

- 情報通信は一部上場企業の平均よりもサイバーテロの危険性に対する意識が高く、金融・エネルギーは一部上場企業並である。逆に、交通、医療分野では危険性に対する意識が低い。

問6-1 貴社では、情報システムに関するセキュリティポリシーを策定していますか。
以下のうちからあてはまるものに○をつけて下さい。（○は一つ）

	一部上場 n=476	金融 n=140	情報通信 n=63	エネルギー n=58	医療 n=112	交通 n=66
策定している（現在策定中を含む）	37.6%	42.9%	27.0%	22.4%	7.1%	4.5%
一部の情報システムについては策定している	24.8%	22.1%	30.2%	27.6%	17.0%	16.7%
現在は策定していないが、今後策定する予定である	31.5%	25.7%	30.2%	32.8%	45.5%	18.2%
特に策定しておらず、今後も策定する予定はない	5.5%	7.9%	12.7%	17.2%	30.4%	57.6%
無回答	0.6%	1.4%	0.0%	0.0%	0.0%	3.0%

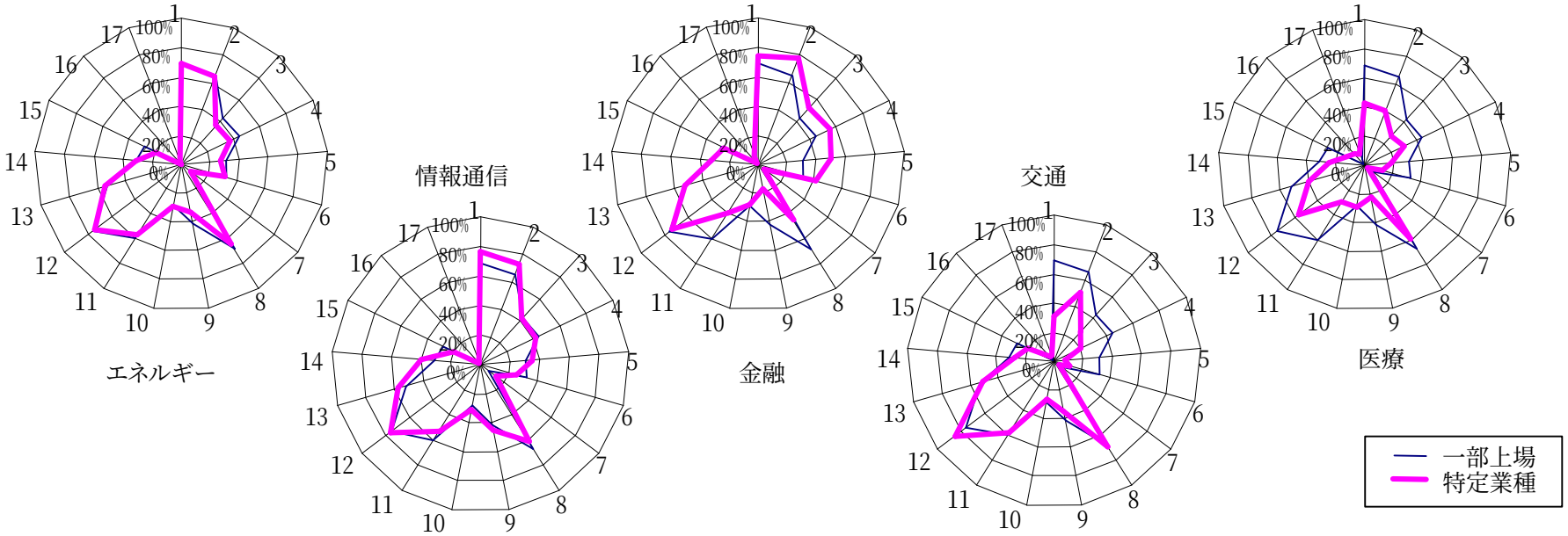


Point

- 金融では多くの企業がセキュリティポリシーを策定しており、情報通信・エネルギーでも多くの企業が一部の情報システムについては策定している。
- 全体に予定まで含めると大半の企業でセキュリティポリシーを策定する予定を持っているが、特に交通でセキュリティポリシー策定が遅れている。

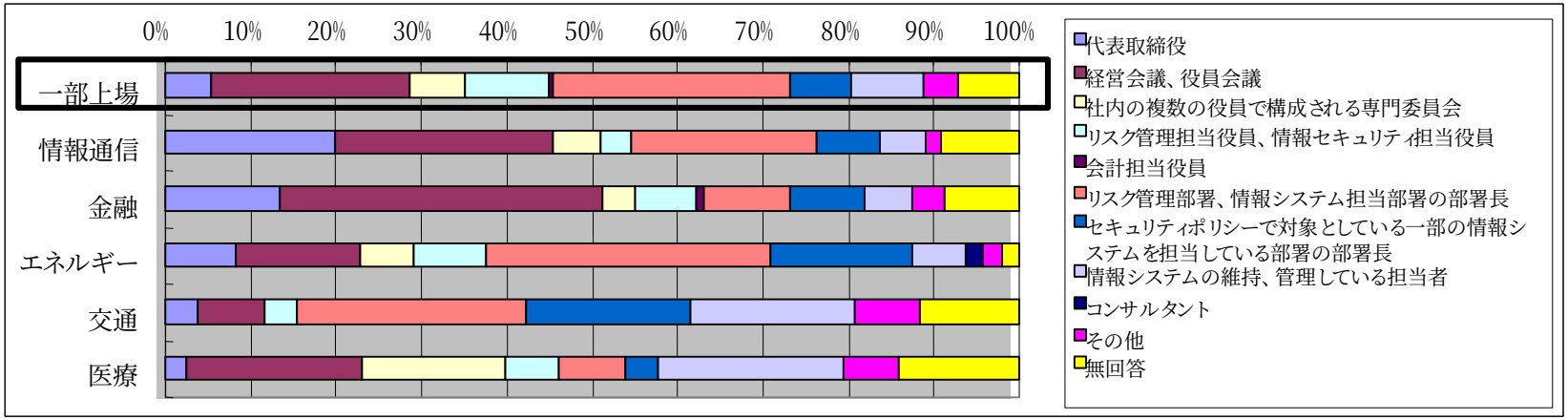
問6-2 貴社のセキュリティポリシーにはどのようなことが記載されていますか。以下のうちからあてはまるものすべてに○をつけてください。（○はいくつでも）

	一部上場 n=447	エネルギー n=48	交通 n=26	金融 n=127	情報通信 n=55	医療 n=78
1 セキュリティ対策の基本的な考え方（目的や戦略）	69.1%	68.8%	30.8%	74.0%	76.4%	42.3%
2 情報セキュリティに関する責任者や担当部署	64.9%	64.6%	50.0%	77.2%	72.7%	39.7%
3 情報セキュリティに関する社員の職責	43.0%	35.4%	26.9%	52.0%	41.8%	26.9%
4 重要度による情報（データ）の分類	43.6%	37.5%	19.2%	55.1%	41.8%	29.5%
5 重要度による情報システムの分類	30.6%	27.1%	7.7%	50.4%	34.5%	17.9%
6 情報システムの設計、開発におけるセキュリティの社内標準	32.4%	31.3%	11.5%	40.9%	25.5%	12.8%
7 セキュリティ基準（ISO 15408など）に準拠した機器の調達	6.9%	8.3%	3.8%	4.7%	12.7%	2.6%
8 インターネット接続におけるセキュリティ対策	68.2%	64.6%	69.2%	44.9%	61.8%	59.0%
9 ダイアルアップ接続におけるセキュリティ対策	41.6%	33.3%	34.6%	17.3%	45.5%	21.8%
10 専用線接続におけるセキュリティ対策	28.9%	29.2%	26.9%	28.3%	30.9%	29.5%
11 社員の電子メールやWWW閲覧における留意事項	59.7%	56.3%	57.7%	38.6%	52.7%	29.5%
12 社内システムの利用者パスワードの取扱い	75.8%	75.0%	84.6%	73.2%	76.4%	56.4%
13 社内システムの管理者パスワードの取扱い	52.3%	54.2%	50.0%	52.0%	58.2%	39.7%
14 社員への情報セキュリティに関する教育	30.9%	31.3%	26.9%	32.3%	40.0%	24.4%
15 セキュリティポリシーに違反した時の罰則	27.7%	18.8%	19.2%	26.0%	20.0%	14.1%
16 上記のような事項は記載されていない	0.7%	0.0%	3.8%	1.6%	1.8%	10.3%
17 無回答	4.3%	2.1%	3.8%	6.3%	1.8%	9.0%



問6-3 貴社のセキュリティポリシーはどのような方々によって承認されていますか。
貴社の状況に最も近いものに○をつけてください。（○は一つ）

	一部上場 n=447	エネルギー n=48	交通 n=26	金融 n=127	情報通信 n=55	医療 n=78
代表取締役	5.4%	8.3%	3.8%	13.4%	20.0%	2.6%
経営会議、役員会議	23.3%	14.6%	7.7%	37.8%	25.5%	20.5%
社内の複数の役員で構成される専門委員会	6.5%	6.3%	0.0%	3.9%	5.5%	16.7%
リスク管理担当役員、情報セキュリティ担当役員	9.8%	8.3%	3.8%	7.1%	3.6%	6.4%
会計担当役員	0.4%	0.0%	0.0%	0.8%	0.0%	0.0%
リスク管理部署、情報システム担当部署の部署長	27.7%	33.3%	26.9%	10.2%	21.8%	7.7%
セキュリティポリシーで対象としている一部の情報システムを担当している部署の部署長	7.2%	16.7%	19.2%	8.7%	7.3%	3.8%
情報システムの維持、管理している担当者	8.5%	6.3%	19.2%	5.5%	5.5%	21.8%
コンサルタント	0.0%	2.1%	0.0%	0.0%	0.0%	0.0%
その他	4.0%	2.1%	7.7%	3.9%	1.8%	6.4%
無回答	7.2%	2.1%	11.5%	8.7%	9.1%	14.1%

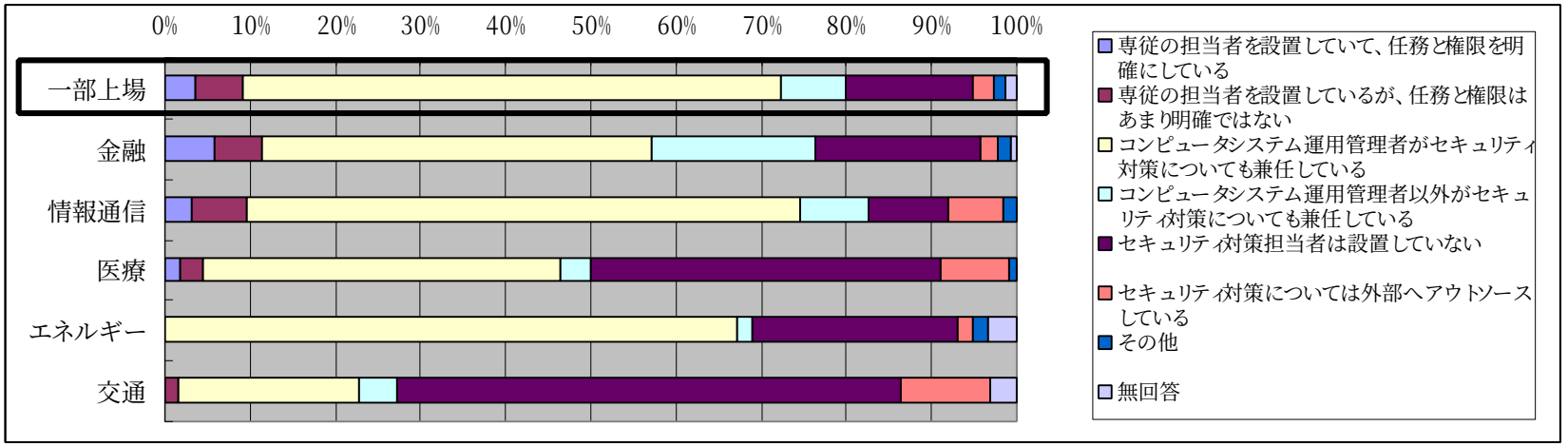


Point

- 情報通信および金融で一部上場企業の平均よりもセキュリティポリシーが代表取締役や経営会議・役員会議などのハイレベルな会議で決定されている一方で、エネルギーでは担当部署長に任され、さらに交通・医療では情報システムの維持・管理をしている担当者に任されているなど、業種によって大きな差がある。

問7-1 貴社では、コンピュータシステムのセキュリティ対策の担当者はいらっしゃますか。（○は一つ）

	一部上場 n=476	エネルギー n=58	交通 n=66	金融 n=140	情報通信 n=63	医療 n=112
専従の担当者を設置していて、任務と権限を明確にしている	3.6%	0.0%	0.0%	5.7%	3.2%	1.8%
専従の担当者を設置しているが、任務と権限はあまり明確ではない	5.7%	0.0%	1.5%	5.7%	6.3%	2.7%
コンピュータシステム運用管理者がセキュリティ対策についても兼任している	63.0%	67.2%	21.2%	45.7%	65.1%	42.0%
コンピュータシステム運用管理者以外がセキュリティ対策についても兼任している	7.6%	1.7%	4.5%	19.3%	7.9%	3.6%
セキュリティ対策担当者は設置していない	15.1%	24.1%	59.1%	19.3%	9.5%	41.1%
セキュリティ対策については外部へアウトソースしている	2.3%	1.7%	10.6%	2.1%	6.3%	8.0%
その他	1.5%	1.7%	0.0%	1.4%	1.6%	0.9%
無回答	1.3%	3.4%	3.0%	0.7%	0.0%	0.0%

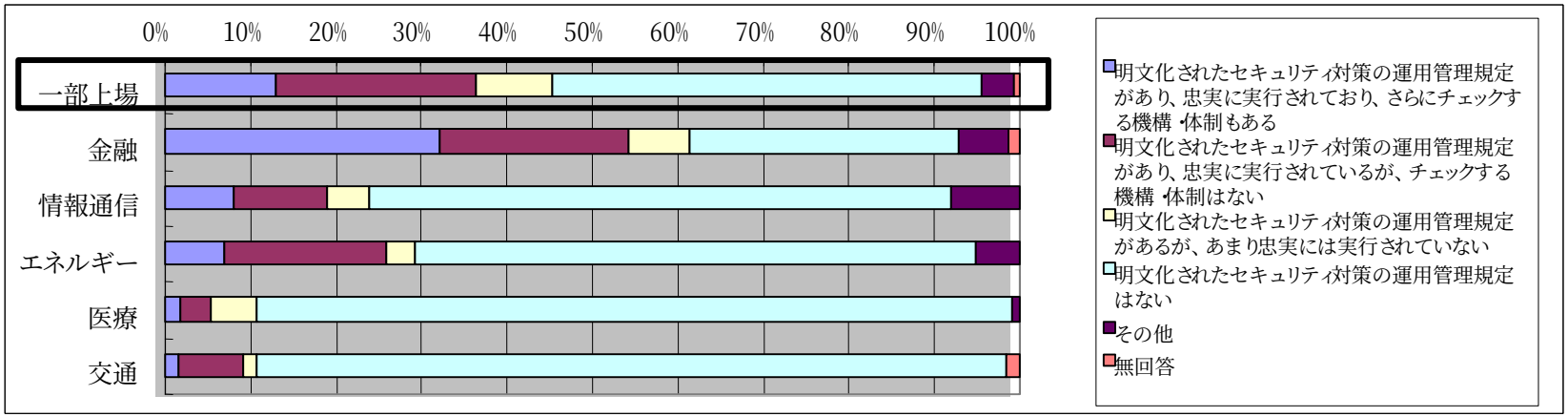


Point

- 交通・医療を除く、どの業種においてもコンピュータシステム運用管理者がセキュリティ対策についても兼任してるのが現状である。金融・情報通信では約10%の企業で専従の担当者をおいている。
- 他方、交通・医療ではセキュリティ対策担当者を設置していない企業が多く、特に交通では60%近くの企業でセキュリティ担当を設置していない。

問7-2 貴社では、コンピュータシステムのセキュリティ対策の運用管理規程やマニュアルはありますか。（○は一つ）

	一部上場 n=476	エネルギー n=58	交通 n=66	金融 n=140	情報通信 n=63	医療 n=112
明文化されたセキュリティ対策の運用管理規定があり、忠実に実行されており、さらにチェックする機構・体制もある	13.03%	6.90%	1.52%	32.14%	7.94%	1.79%
明文化されたセキュリティ対策の運用管理規定があり、忠実に実行されているが、チェックする機構・体制はない	23.32%	18.97%	7.58%	22.14%	11.11%	3.57%
明文化されたセキュリティ対策の運用管理規定があるが、あまり忠実には実行されていない	9.03%	3.45%	1.52%	7.14%	4.76%	5.36%
明文化されたセキュリティ対策の運用管理規定はない	50.21%	65.52%	87.88%	31.43%	68.25%	88.39%
その他	3.78%	5.17%	0.00%	5.71%	7.94%	0.89%
無回答	0.63%	0.00%	1.52%	1.43%	0.00%	0.00%

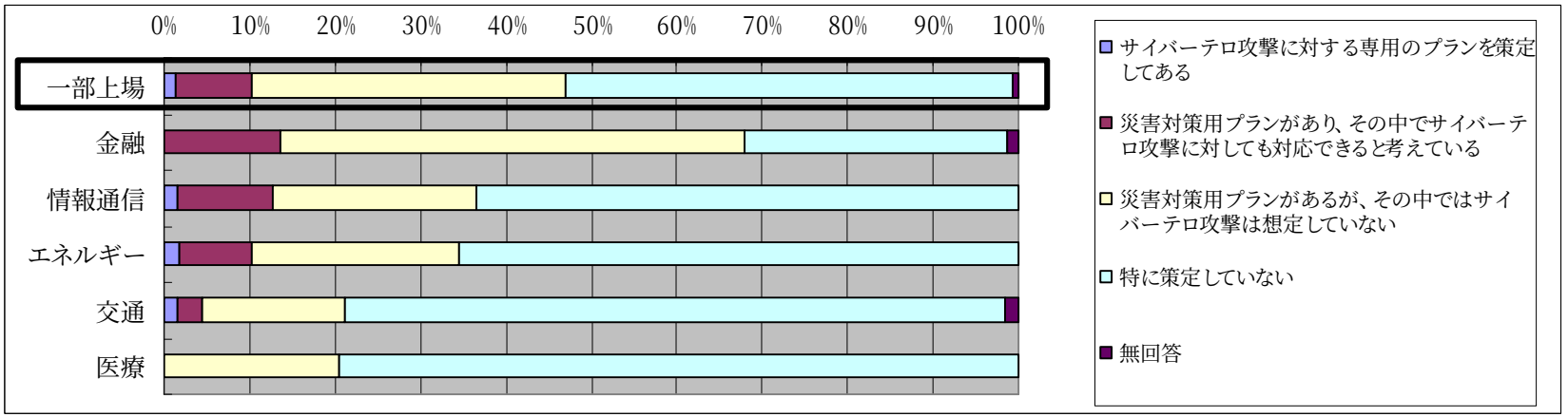


Point

- 金融だけが半数を超える企業で明文化されたセキュリティ対策の運用管理規定があり、一部上場企業でも半数近くの企業で明文化された規定がある。しかし、重要インフラを構成する金融以外の4業種では大半が明文化されたセキュリティ管理規定を持っていない。

問8-1 貴社では、サイバーテロ攻撃による被害が発生した時のための不測事態対応計画（コンティンジェンシープラン）を策定していますか。（○は一つ）

	一部上場 n=476	エネルギー n=58	交通 n=66	金融 n=140	情報通信 n=63	医療 n=112
サイバーテロ攻撃に対する専用のプランを策定してある	1.26%	1.72%	1.52%	0.00%	1.59%	0.00%
災害対策用プランがあり、その中でサイバーテロ攻撃に対しても対応できると考えている	9.03%	8.62%	3.03%	13.57%	11.11%	0.00%
災害対策用プランがあるが、その中ではサイバーテロ攻撃は想定していない	36.76%	24.14%	16.67%	54.29%	23.81%	20.54%
特に策定していない	52.31%	65.52%	77.27%	30.71%	63.49%	79.46%
無回答	0.63%	0.00%	1.52%	1.43%	0.00%	0.00%

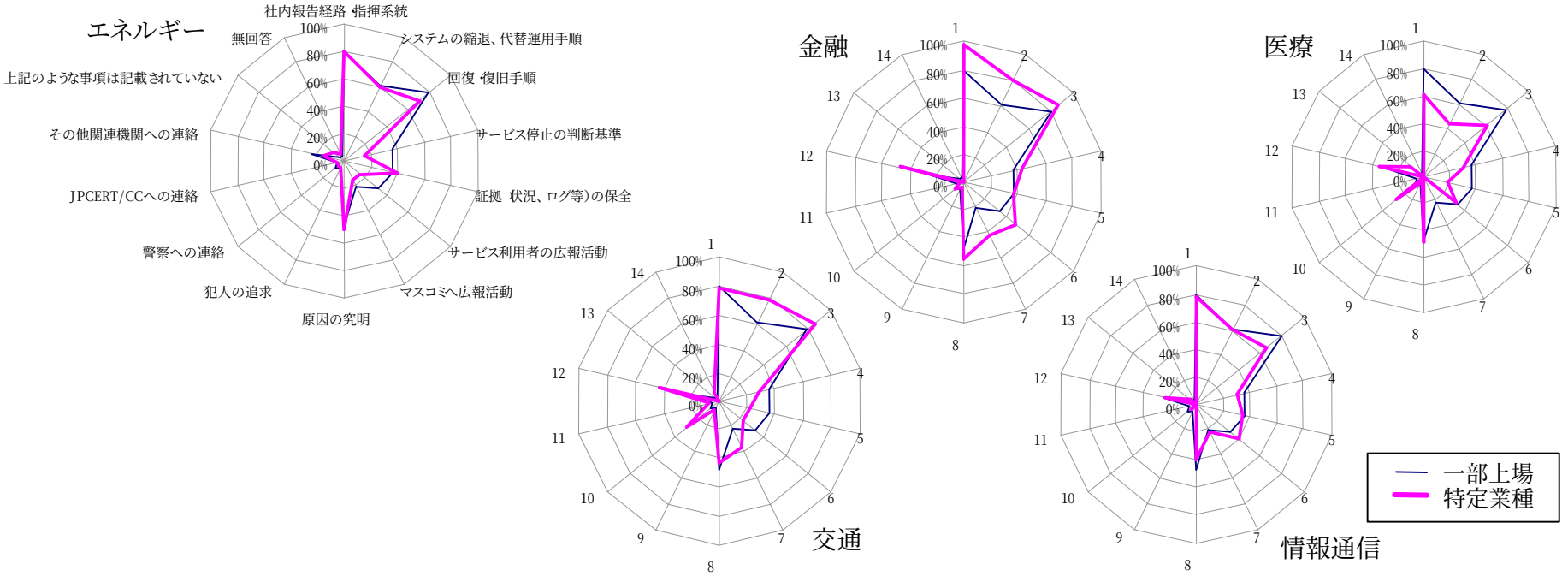


Point

- コンティンジェンシープランを策定している企業であっても、サイバーテロ攻撃は想定されていないと回答する企業が多い。
- コンティンジェンシープランを持たない企業に策定を促すことに加えて、コンティンジェンシープランを既に持っている企業に対しても、サイバーテロのリスクを明示し、コンティンジェンシープランの中に組み込むよう働きかけることが重要だと思われる。

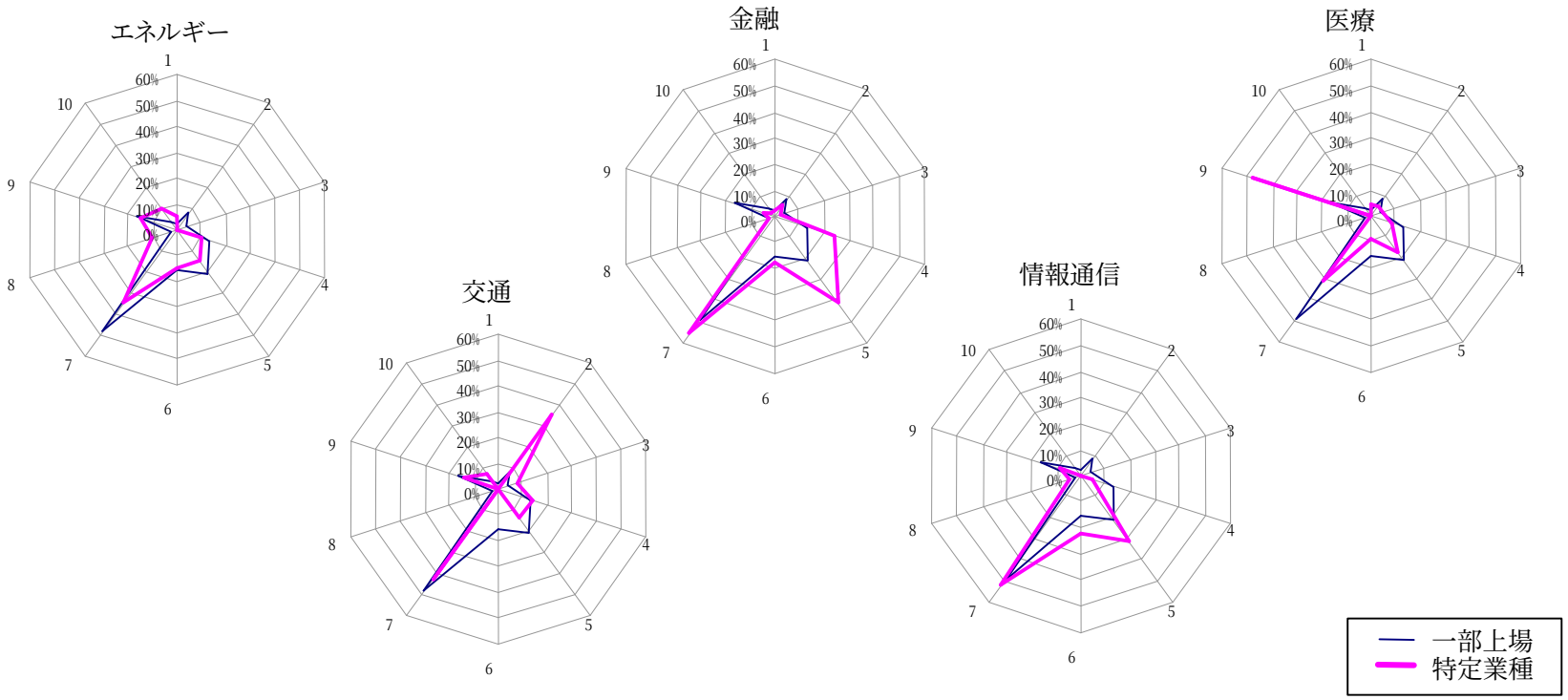
問8-2 貴社のコンティンジェンシープランで盛り込まれている事柄をお答えください。
以下のうちからあてはまるものすべてに○をつけてください。（○はいくつでも）

		一部上場 n=224	エネルギー n=20	交通 n=14	金融 n=95	情報通信 n=23	医療 n=23
1	社内報告経路・指揮系統	79.5%	80.0%	78.6%	97.9%	78.3%	60.9%
2	システムの縮退、代替運用手順	60.7%	60.0%	78.6%	81.1%	60.9%	43.5%
3	回復・復旧手順	79.0%	70.0%	85.7%	86.3%	65.2%	60.9%
4	サービス停止の判断基準	36.2%	15.0%	28.6%	43.2%	30.4%	30.4%
5	証拠（状況、ログ等）の保全	36.2%	40.0%	21.4%	36.8%	34.8%	17.4%
6	サービス利用者の広報活動	32.6%	15.0%	21.4%	47.4%	39.1%	30.4%
7	マスコミへ広報活動	21.0%	15.0%	35.7%	43.2%	21.7%	0.0%
8	原因の究明	47.3%	50.0%	42.9%	54.7%	39.1%	47.8%
9	犯人の追求	4.9%	5.0%	7.1%	4.2%	0.0%	4.3%
10	警察への連絡	8.5%	5.0%	28.6%	8.4%	4.3%	26.1%
11	JPCERT/CCへの連絡	4.9%	5.0%	7.1%	2.1%	0.0%	0.0%
12	その他関連機関への連絡	24.1%	15.0%	42.9%	46.3%	21.7%	34.8%
13	上記のような事項は記載されていない	3.1%	10.0%	0.0%	0.0%	4.3%	13.0%
14	無回答	3.1%	5.0%	7.1%	1.1%	0.0%	0.0%



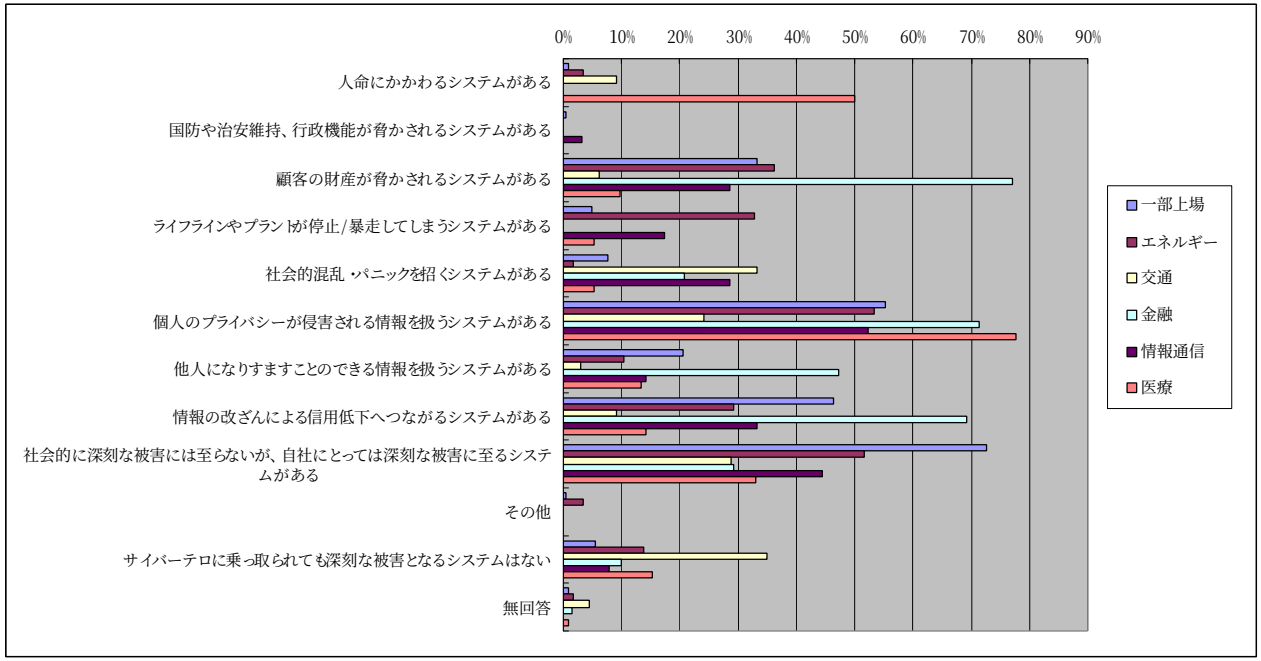
問8-3 貴社ではコンティンジェンシープランの普及、維持のためにどのおうなことを行っていますか。以下のうちからあてはまるものすべてに○をつけてください。（○はいくつでも）

	一部上場 n=224	エネルギー n=20	交通 n=14	金融 n=95	情報通信 n=23	医療 n=23
1 定期的に全社員を対象に社内研修で教育を行っている	2.2%	5.0%	0.0%	2.1%	0.0%	4.3%
2 一部の社員に定期的に社内研修で教育を行っている	8.0%	0.0%	35.7%	5.3%	0.0%	4.3%
3 昇格時などのタイミングで教育を行っている	3.6%	0.0%	7.1%	2.1%	0.0%	4.3%
4 定期的に訓練を行っている	13.4%	10.0%	14.3%	24.2%	4.3%	8.7%
5 定期的ではないが、訓練を行っている	21.0%	15.0%	14.3%	41.1%	30.4%	17.4%
6 現状と乖離しないよう、定期的にプランの見直しをおこなっている	15.6%	15.0%	0.0%	17.9%	21.7%	8.7%
7 定期的ではないが、プランの見直しをおこなっている	49.1%	35.0%	42.9%	55.8%	52.2%	30.4%
8 その他	2.2%	10.0%	0.0%	2.1%	4.3%	0.0%
9 そのようなことは特に行っていない	16.1%	15.0%	14.3%	4.2%	8.7%	47.8%
10 無回答	3.6%	10.0%	7.1%	2.1%	0.0%	0.0%



問9-1 貴社では、サイバーテロに侵入され、乗っ取られた場合、以下のように社会的に深刻な被害に至る情報システムがありますか。（○はいくつでも）

	一部上場 n=476	エネルギー n=58	交通 n=66	金融 n=140	情報通信 n=63	医療 n=112
人命にかかわるシステムがある	0.8%	3.4%	9.1%	0.0%	0.0%	50.0%
国防や治安維持、行政機能が脅かされるシステムがある	0.4%	0.0%	0.0%	0.0%	3.2%	0.0%
顧客の財産が脅かされるシステムがある	33.2%	36.2%	6.1%	77.1%	28.6%	9.8%
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	4.8%	32.8%	0.0%	0.0%	17.5%	5.4%
社会的混乱・パニックを招くシステムがある	7.6%	1.7%	33.3%	20.7%	28.6%	5.4%
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	55.3%	53.4%	24.2%	71.4%	52.4%	77.7%
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	20.6%	10.3%	3.0%	47.1%	14.3%	13.4%
情報の改ざんによる信用低下へつながるシステムがある	46.4%	29.3%	9.1%	69.3%	33.3%	14.3%
社会的に深刻な被害には至らないが、自社にとっては深刻な被害に至るシステムがある	72.7%	51.7%	28.8%	29.3%	44.4%	33.0%
その他	0.4%	3.4%	0.0%	0.0%	0.0%	0.0%
サイバーテロに乗っ取られても深刻な被害となるシステムはない	5.5%	13.8%	34.8%	10.0%	7.9%	15.2%
無回答	0.8%	1.7%	4.5%	1.4%	0.0%	0.9%



問9-1 貴社では、サイバーテロに侵入され、乗っ取られた場合、以下のように社会的に深刻な被害に至る情報システムがありますか。（○はいくつでも） 続き）

Point

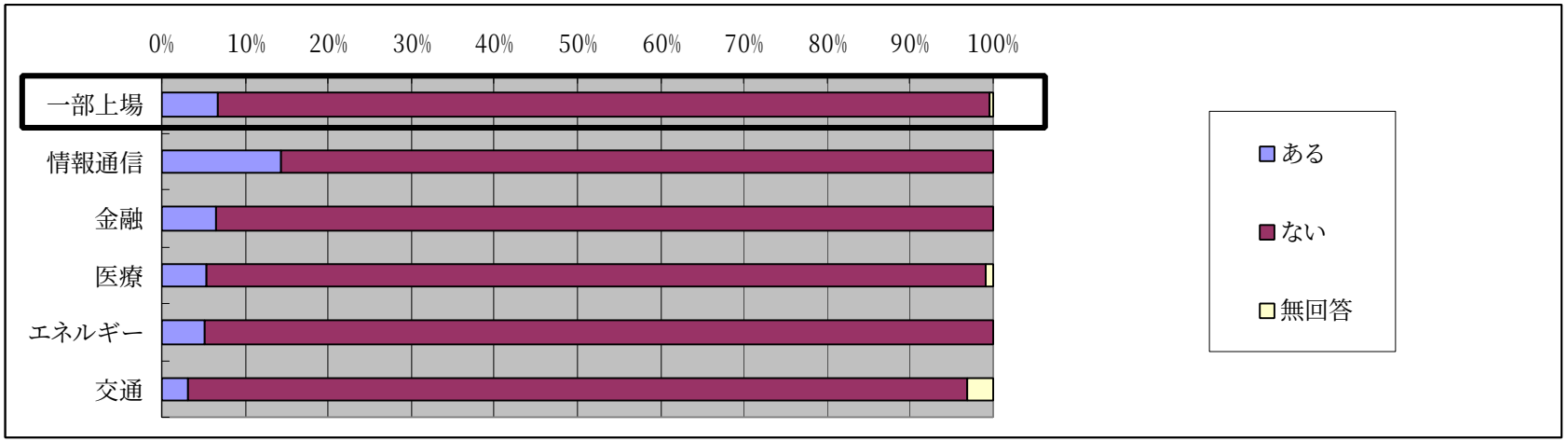
- 半数の医療機関で「サイバーテロに乗っ取られた場合人命にかかわるシステムがある」と回答している。また、金融機関の多く（8割弱）が、顧客の財産が脅かされると回答している。また3割のエネルギー関連企業が「ライフラインやプラントが停止/暴走する可能性がある」としている。

- 「個人にプライバシーが侵害されるシステムがある」では、交通を除く業種で半数を超える企業がそういったシステムがあると回答している。特に金融、医療の業種では7割以上となっている。

- 「国防や治安維持、行政機能が脅かされるシステムがある」と回答したのは3社で、一部上場の輸送用機器業、一部上場の通信業、一部上場ではな通信業である。

問10-1 貴社では、これまでに、サイバーテロに限らず過失や事故も含め、情報システムが原因となって深刻な被害が発生したことがありますか。（○は一つ）

	一部上場 n=476	情報通信 n=63	金融 n=140	医療 n=112	エネルギー n=58	交通 n=66
ある	6.7%	14.3%	6.4%	5.4%	5.2%	3.0%
ない	92.9%	85.7%	93.6%	93.8%	94.8%	93.9%
無回答	0.4%	0.0%	0.0%	0.9%	0.0%	3.0%



Point

- どの業種でも5%前後の企業がなんらかの深刻な被害を受けている。
- 被害内容を次の設問で自由記入回答していただいているが、故障、天災、ウィルス、SPAMなどが多いようである。
- 情報通信業では、他の業種に比して被害を経験した割合が高い。

問10-2 被害の発生原因、状況など具体的にご記入ください。

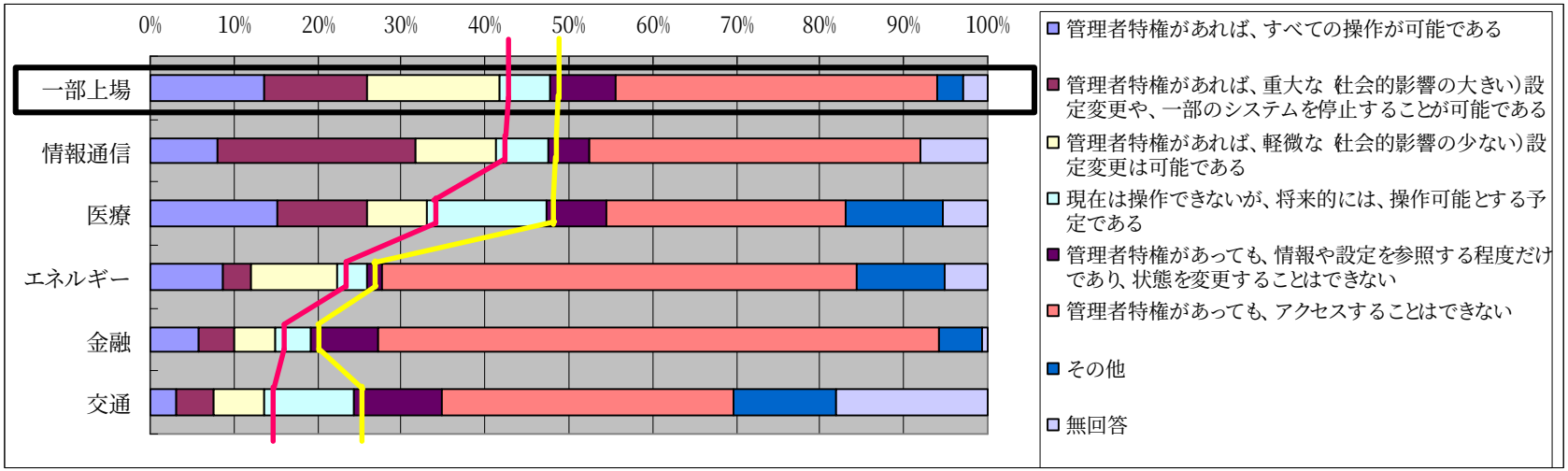
項番	対象グループ	業種	問10-2 被害の発生原因、状況
1	[特定]	病院 ･医院	オペレーションミスによる情報の消失
2	[特定]	病院 ･医院	インターネットwebサーバを利用したスパムメール
3	[特定]	病院 ･医院	窓口会計システムホストのハードディスクがクラッシュ ･窓口会計の全端末がストップ ･バックアップから復旧まで半日所要 ･2週間前のバックアップしかなかったので2週間分の会計再入力が発生
4	[特定]	病院 ･医院	停電によるシステム停止
5	[特定]	病院 ･医院	情報システムが過去において停止したことがあります。過失およびディスククラッシュ等が原因です。これによりオーダリングシステムが停止し、患者に大変な迷惑をかけましたがほとんど全てのデータを復旧いたしました。
6	[特定]	病院 ･医院	システムダウンにより、医療費請求不可となったため、収入未済額が発生。病院への信用が失われた
7	[特定]	電力	データの消去
8	[特定]	通信	サーバー故障 原因は部品の劣化によるもの）によりデータ消去
9	[特定]	ｲﾝﾀｰﾈｯﾄｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ	ルータの故障
10	[特定]	新聞	回線関係機器の故障でニュースサービスが一時停止になった
11	[特定]	新聞	プログラムバグやハード障害などにより、新聞製作工程が大幅に遅れた
12	[特定]	新聞	深刻ではないが、SPAMメールの踏み台にされ、あたかも本社から発信したかのようなメールを多数のユーザに送られた。
13	[特定]	航空	PCの内臓HARDDISK破損
14	[特定]	銀行	通信機器、ディスク、プログラム、回線等の異常
15	[特定]	その他金融機関	口座振替におけるデータの二重送信
16	[特定]	その他金融機関	プログラム障害によるバンキングオンラインサービスの一時停止
17	[特定]	その他金融機関	･プログラムバグによる取引停止 ･取引量増大による取引停止
18	[特定]	その他	インターネット用サーバがスパムメールの不正中継に利用された。その結果、全く関係のない人達から苦情が多数寄せられて困った。
19	[特定]	その他	研究所のサーバーがハッキングを受け、データを一部紛失した。
20	[特定かつ上場]	石油製造	社内にウイルスが発生。スパンメール
21	[特定かつ上場]	石油卸	現在、弊社のファイアーウォールが外部から転送メールのアタックを受けている。たぶんセキュリティーホールのサーチと思われる。深刻な被害ではないが、ファイアーウォールのLOGがパンクするため、インターネットが利用できないことがある。

問10-2 被害の発生原因、状況など具体的にご記入ください。(続き)

項番	対象グループ	業種	問10-2 被害の発生原因、状況
22	[特定かつ上場]	信販	クレジットカード情報の盗用による不正利用
23	[特定かつ上場]	銀行	ハード障害により顧客取引が不可となった
24	[特定かつ上場]	銀行	オンライン停止による窓口、自動機（CD・ATM）の取扱中止
25	[特定かつ上場]	銀行	NTTの回線障害により、ATMおよび営業店の端末が使用不能となった
26	[上場]	流通・卸売	スパンメール
27	[上場]	輸送用機器	SPAMメールによるインターネット接続の停止
28	[上場]	輸送用機器	社外メールにEXCELのマクロウィルスが添付、社内PC数十台に感染
29	[上場]	電気機器	スパムメール（なりすましメール被害）
30	[上場]	繊維	専用線故障による業務中断
31	[上場]	精密機器	・スパムメールにより、不特定多数にいかがわしい内容のメールが発信された。送られた側より通知を受け判明した
32	[上場]	精密機器	外部と接続するメールシステムがスパムメールのアタックを受け、パフォーマンス低下し、システムダウンに至った
33	[上場]	食品	受注・出荷システムのトラブルにより得意先への配荷が遅延した
34	[上場]	食品	コンピュータトラブルにより受注システムが不能となり、結果として製品出荷が遅れて量販店からペナルティを取られた。
35	[上場]	食品	ホストシステムのダウン
36	[上場]	小売・飲食	雪による停電のためにホストコンピュータが数日稼働不能となった。そのため発注業務がFAXでの対応となり販売業務に支障をきたした
37	[上場]	小売・飲食	物流システムにおいて、コンピュータがハード的な原因によりダウンし、店舗への配送に遅延・誤りが生じた
38	[上場]	紙・パルプ	アプリケーション負荷大により出荷停止となり売上計上できない。サーバーダウンによりネットワークの停止が発生
39	[上場]	建設	サーバソフトの不具合のために、ファイルサーバ上のデータ更新ができなくなる
40	[上場]	機械	過失によるDiskの初期化
41	[上場]	化学	アプリケーションプログラムのバグによるデータの不整合
42	[上場]	化学	水害で通信機能が麻痺した
43	[上場]	その他製造	弊社のインターネットサーバを経由してスパムメールが配布された
44	[上場]	その他サービス	サイバーテロではないがウイルスが外部に漏れた
45	[上場]	その他サービス	フレームリレー網の障害等
46	[上場]	その他サービス	他人のユーザーID、パスワードを利用し物品の手配を行いその物品を持ちさる
47	[上場]	その他	システム停止による出庫業務不能

問11 貴社の重要基幹システムは、管理者特権を所有している場合、社外ネットワークからどの程度操作可能ですか。（○は一つ）

	一部上場 n=476	情報通信 n=63	医療 n=112	エネルギー n=58	金融 n=140	交通 n=66
管理者特権があれば、すべての操作が可能である	13.7%	7.9%	15.2%	8.6%	5.7%	3.0%
管理者特権があれば、重大な（社会的影響の大きい）設定変更や、一部のシステムを停止することが可能である	12.2%	23.8%	10.7%	3.4%	4.3%	4.5%
管理者特権があれば、軽微な（社会的影響の少ない）設定変更は可能である	16.0%	9.5%	7.1%	10.3%	5.0%	6.1%
現在は操作できないが、将来的には、操作可能とする予定である	5.9%	6.3%	14.3%	3.4%	4.3%	10.6%
管理者特権があっても、情報や設定を参照する程度だけであり、状態を変更することはできない	8.0%	4.8%	7.1%	1.7%	7.9%	10.6%
管理者特権があっても、アクセスすることはできない	38.2%	39.7%	28.6%	56.9%	67.1%	34.8%
その他	3.2%	0.0%	11.6%	10.3%	5.0%	12.1%
無回答	2.9%	7.9%	5.4%	5.2%	0.7%	18.2%

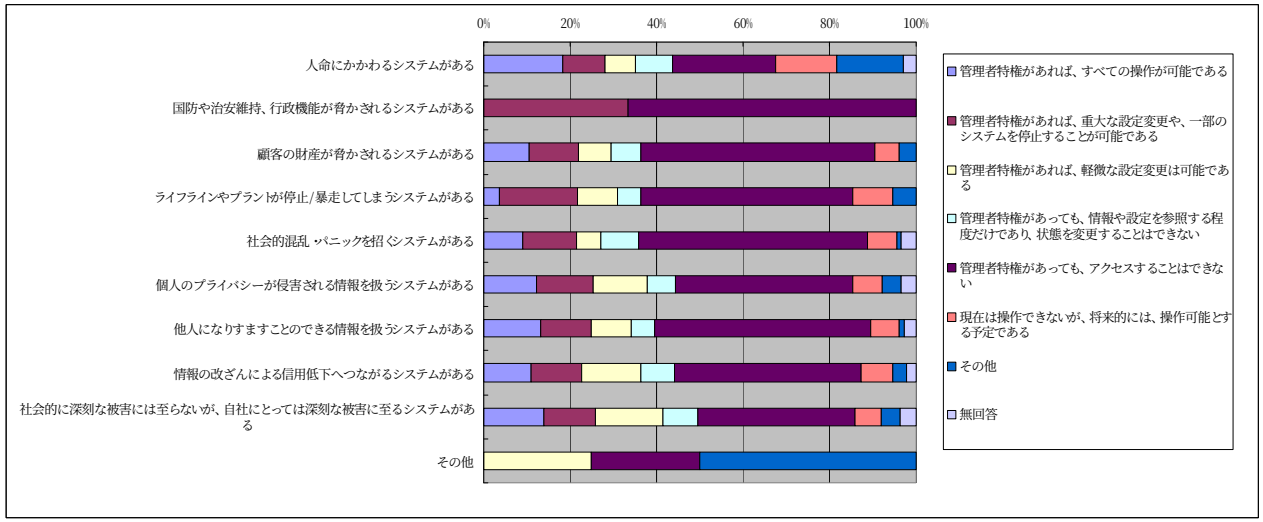


Point

- 社外から操作可能としている範囲（軽微であっても）を図中に赤線で示す。情報通信を除く特定業種は一部上場平均よりも厳格な管理を行っていることが伺える。
- 他方、医療機関においては「すべての操作が可能」と回答した割合が一部上場平均を超えている。またいずれの業種でも今後は社外から操作可能とする予定の企業があり、特に医療機関では他の業種以上にこの傾向がある。（図中の黄色線）

問11 vs問9-1 重要基幹システムと外部からの操作

	人命にかかわるシステムがある n=71	国防や治安維持、行政機能が脅かされるシステムがある n=3	顧客の財産が脅かされるシステムがある n=250	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 n=55	社会的混乱・パニックを招くシステムがある n=89	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 n=467	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 n=152	情報の改ざんによる信用低下へつながるシステムがある n=317	社会的に深刻な被害には至らないが、自社にとっては深刻な被害に至るシステムがある n=478	その他 n=4
管理者特権があれば、すべての操作が可能である	18.3%	0.0%	10.4%	3.6%	9.0%	12.2%	13.2%	11.0%	14.0%	0.0%
管理者特権があれば、重大な設定変更や、一部のシステムを停止することが可能である	9.9%	33.3%	11.6%	18.2%	12.4%	13.3%	11.8%	11.7%	11.7%	0.0%
管理者特権があれば、軽微な設定変更は可能である	7.0%	0.0%	7.6%	9.1%	5.6%	12.2%	9.2%	13.6%	15.7%	25.0%
管理者特権があっても、情報や設定を参照する程度だけであり、状態を変更することはできない	8.5%	0.0%	6.8%	5.5%	9.0%	6.6%	5.3%	7.9%	8.2%	0.0%
管理者特権があっても、アクセスすることはできない	23.9%	66.7%	54.0%	49.1%	52.8%	41.1%	50.0%	43.2%	36.2%	25.0%
現在は操作できないが、将来的には、操作可能とする予定である	14.1%	0.0%	5.6%	9.1%	6.7%	6.9%	6.6%	7.3%	6.3%	0.0%
その他	15.5%	0.0%	4.0%	5.5%	1.1%	4.3%	1.3%	3.2%	4.4%	50.0%
無回答	2.8%	0.0%	0.0%	0.0%	3.4%	3.4%	2.6%	2.2%	3.6%	0.0%

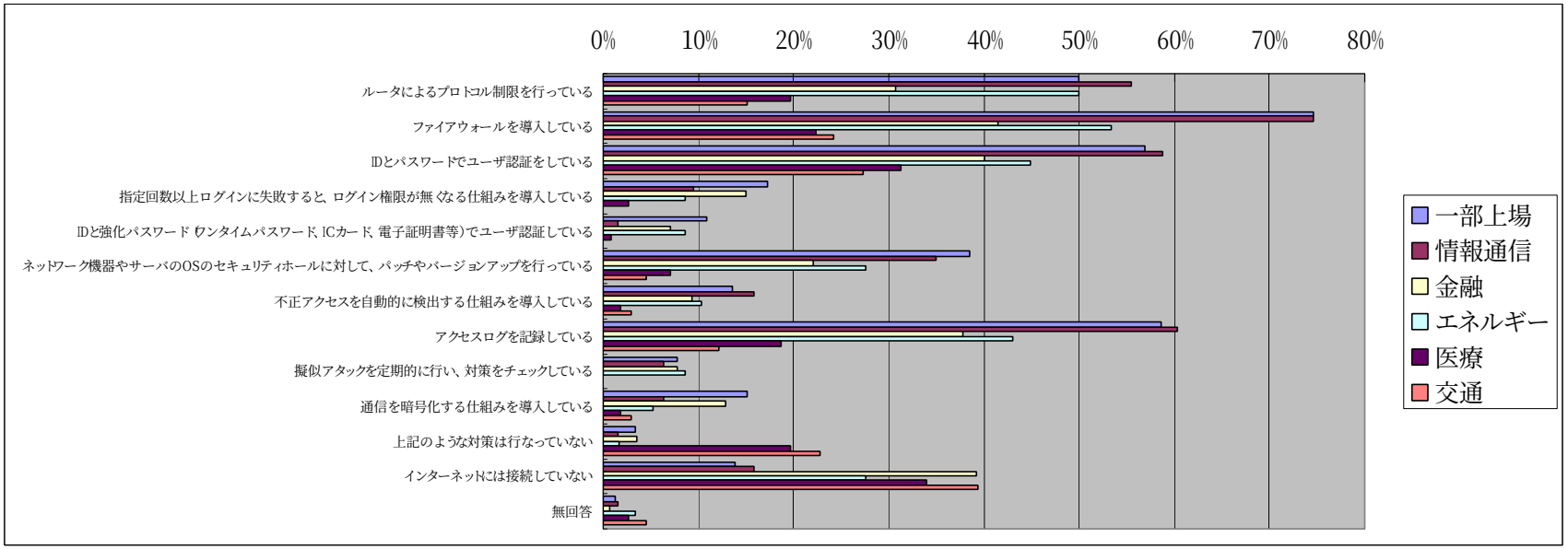


Point

- 外部からの重要基幹システムの操作可能程度を保有する重要基幹システムの種類別にまとめたものである 重要基幹システムは複数回答であるため、必ずしも当該のシステムについて回答しているわけではないことに注意）。
- 国防・治安を脅かすシステムを保有する企業においては、外部からの管理者操作を制限している。一方、人命にかかわるシステムを保有する企業であっても2割に近い企業が外部から全ての操作を可能としている。

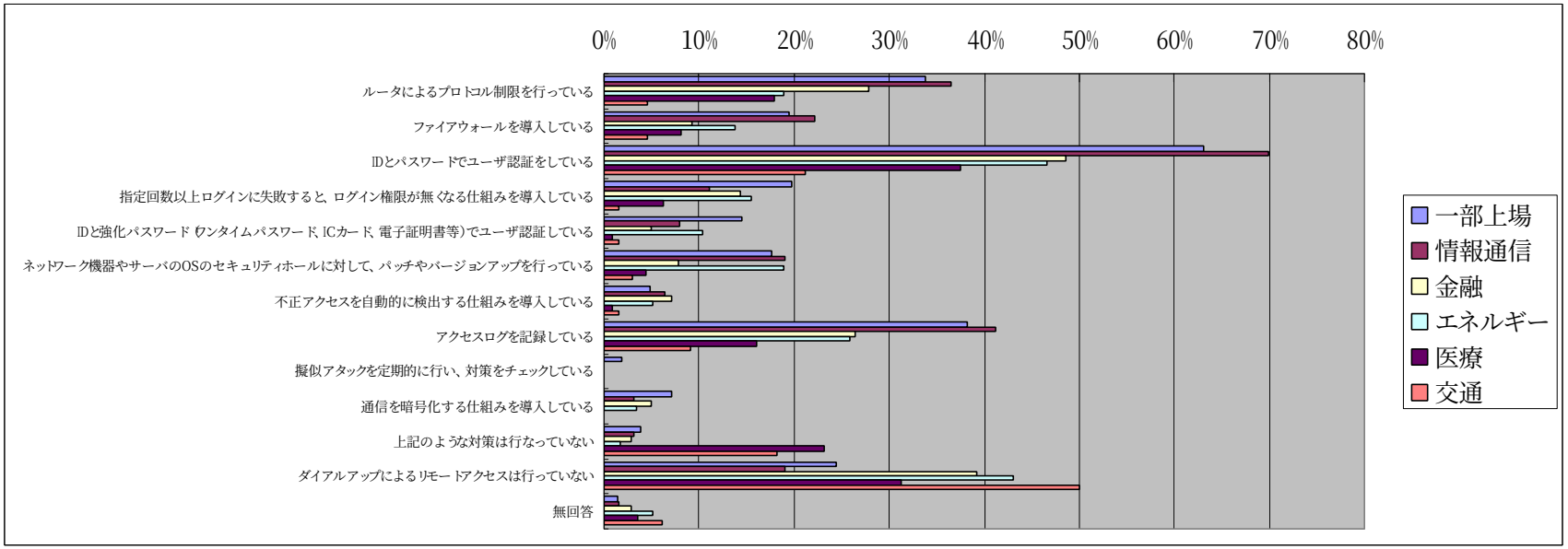
問12-1 インターネットの接続点および、インターネットから社内ネットワークへの侵入に対して、どのようなセキュリティ対策を導入していますか。（○はいくつでも）

	一部上場 n=476	情報通信 n=63	金融 n=140	エネルギー n=58	医療 n=112	交通 n=66
ルータによるプロトコル制限を行っている	50.0%	55.6%	30.7%	50.0%	19.6%	15.2%
ファイアウォールを導入している	74.6%	74.6%	41.4%	53.4%	22.3%	24.2%
IDとパスワードでユーザ認証をしている	56.9%	58.7%	40.0%	44.8%	31.3%	27.3%
指定回数以上ログインに失敗すると、ログイン権限が無くなる仕組みを導入している	17.2%	9.5%	15.0%	8.6%	2.7%	0.0%
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）でユーザ認証している	10.9%	1.6%	7.1%	8.6%	0.9%	0.0%
ネットワーク機器やサーバのOSのセキュリティホールに対して、パッチやバージョンアップを行っている	38.4%	34.9%	22.1%	27.6%	7.1%	4.5%
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	13.7%	15.9%	9.3%	10.3%	1.8%	3.0%
アクセスログを記録している	58.6%	60.3%	37.9%	43.1%	18.8%	12.1%
擬似アタックを定期的に行い、対策をチェックしている	7.8%	6.3%	7.9%	8.6%	0.0%	0.0%
通信を暗号化する仕組みを導入している	15.1%	6.3%	12.9%	5.2%	1.8%	3.0%
上記のような対策は行なっていない	3.4%	1.6%	3.6%	1.7%	19.6%	22.7%
インターネットには接続していない	13.9%	15.9%	39.3%	27.6%	33.9%	39.4%
無回答	1.3%	1.6%	0.7%	3.4%	2.7%	4.5%



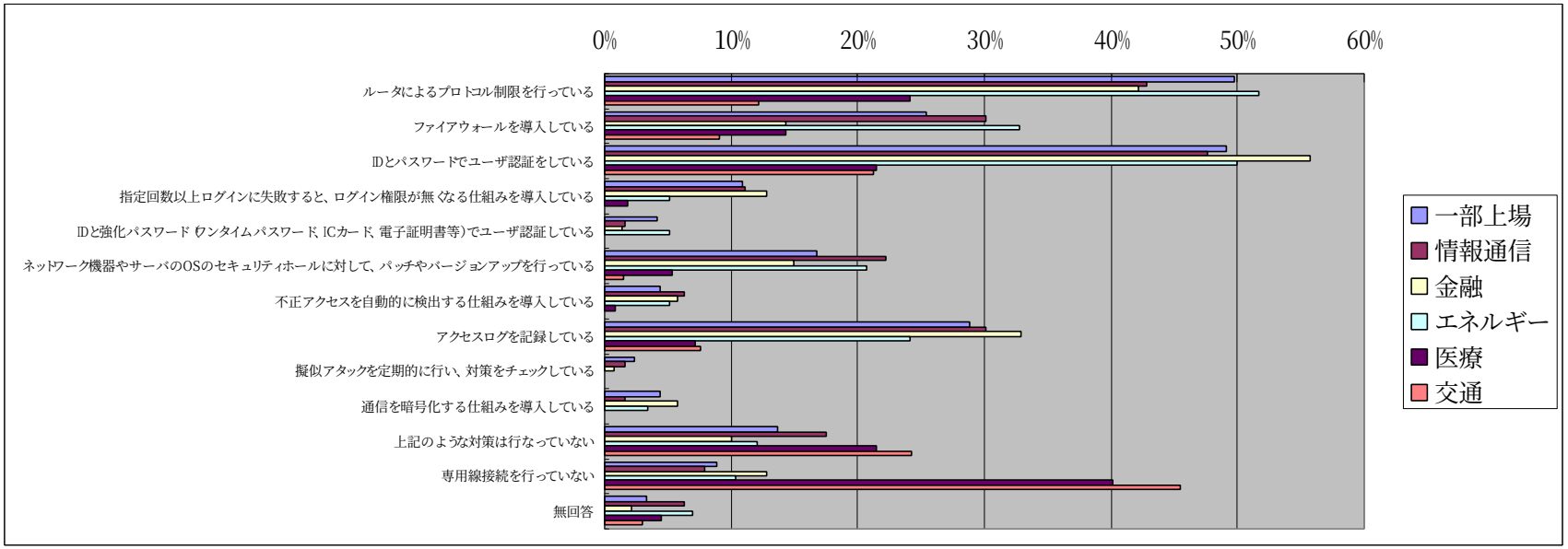
問12-2 ダイアルアップによるリモートアクセスの接続点および、社内ネットワークへの侵入に対して、どのようなセキュリティ対策を導入していますか。（○はいくつでも）

	一部上場 n=476	情報通信 n=63	金融 n=140	エネルギー n=58	医療 n=112	交通 n=66
ルータによるプロトコル制限を行っている	33.8%	36.5%	27.9%	19.0%	17.9%	4.5%
ファイアウォールを導入している	19.5%	22.2%	9.3%	13.8%	8.0%	4.5%
IDとパスワードでユーザ認証をしている	63.0%	69.8%	48.6%	46.6%	37.5%	21.2%
指定回数以上ログインに失敗すると、ログイン権限が無くなる仕組みを導入している	19.7%	11.1%	14.3%	15.5%	6.3%	1.5%
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）でユーザ認証している	14.5%	7.9%	5.0%	10.3%	0.9%	1.5%
ネットワーク機器やサーバのOSのセキュリティホールに対して、パッチやバージョンアップを行っている	17.6%	19.0%	7.9%	19.0%	4.5%	3.0%
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	4.8%	6.3%	7.1%	5.2%	0.9%	1.5%
アクセスログを記録している	38.2%	41.3%	26.4%	25.9%	16.1%	9.1%
擬似アタックを定期的に行い、対策をチェックしている	1.9%	0.0%	0.0%	0.0%	0.0%	0.0%
通信を暗号化する仕組みを導入している	7.1%	3.2%	5.0%	3.4%	0.0%	0.0%
上記のような対策は行なっていない	3.8%	3.2%	2.9%	1.7%	23.2%	18.2%
ダイアルアップによるリモートアクセスは行っていない	24.4%	19.0%	39.3%	43.1%	31.3%	50.0%
無回答	1.5%	1.6%	2.9%	5.2%	3.6%	6.1%



問12-3 専用線の接続点および、社内ネットワークへの侵入に対して、どのようなセキュリティ対策を導入していますか。（○はいくつでも）

	一部上場 n=476	情報通信 n=63	金融 n=140	エネルギー n=58	医療 n=112	交通 n=66
ルータによるプロトコル制限を行っている	49.8%	42.9%	42.1%	51.7%	24.1%	12.1%
ファイアウォールを導入している	25.4%	30.2%	14.3%	32.8%	14.3%	9.1%
IDとパスワードでユーザ認証をしている	49.2%	47.6%	55.7%	50.0%	21.4%	21.2%
指定回数以上ログインに失敗すると、ログイン権限が無くなる仕組みを導入している	10.9%	11.1%	12.9%	5.2%	1.8%	0.0%
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）でユーザ認証している	4.2%	1.6%	1.4%	5.2%	0.0%	0.0%
ネットワーク機器やサーバのOSのセキュリティホールに対して、パッチやバージョンアップを行っている	16.8%	22.2%	15.0%	20.7%	5.4%	1.5%
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	4.4%	6.3%	5.7%	5.2%	0.9%	0.0%
アクセスログを記録している	28.8%	30.2%	32.9%	24.1%	7.1%	7.6%
擬似アタックを定期的に行い、対策をチェックしている	2.3%	1.6%	0.7%	0.0%	0.0%	0.0%
通信を暗号化する仕組みを導入している	4.4%	1.6%	5.7%	3.4%	0.0%	0.0%
上記のような対策は行なっていない	13.7%	17.5%	10.0%	12.1%	21.4%	24.2%
専用線接続を行っていない	8.8%	7.9%	12.9%	10.3%	40.2%	45.5%
無回答	3.4%	6.3%	2.1%	6.9%	4.5%	3.0%



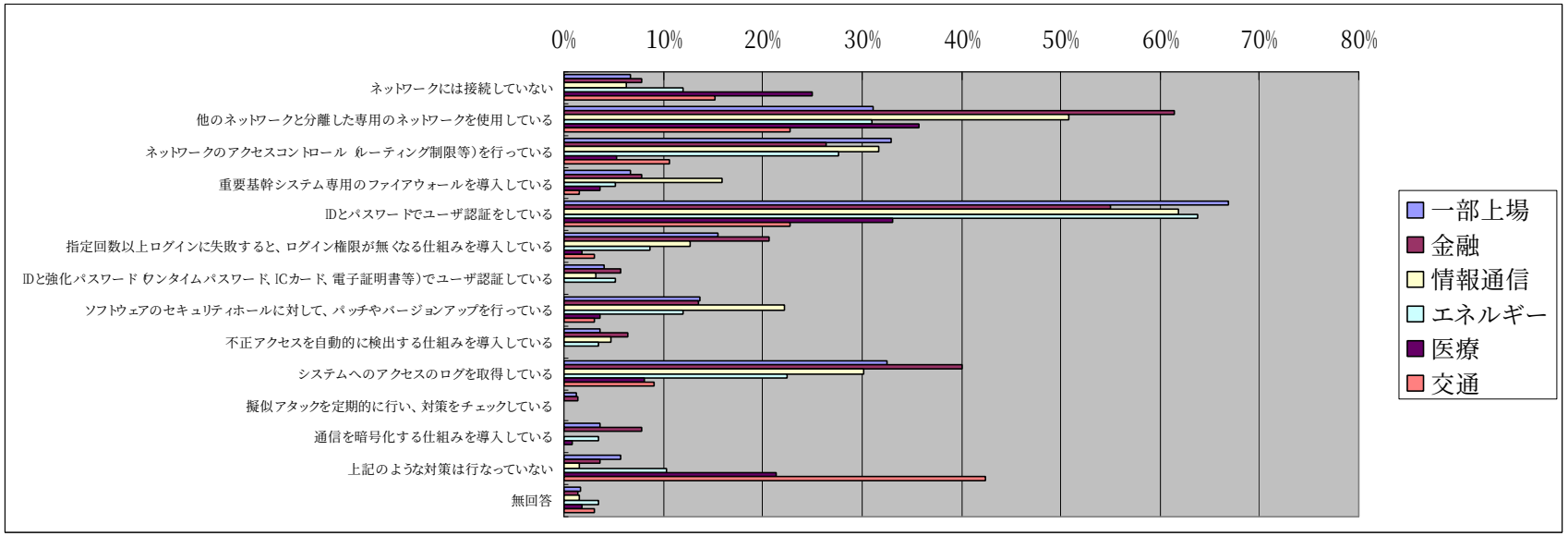
問12　会社の外部とのネットワーク接続におけるセキュリティ対策について

Point

- インターネット接続では「ファイアウォール」、ダイアルアップ接続では「IDとパスワードによるユーザ認証」、専用線接続では「プロトコル制限およびIDとパスワードによるユーザ認証」の対策を講じていることが多い。
- 問12-1～問12-3を通じて、金融/情報通信関連の企業でさえ、特定一部上場企業並みか、それ以下の実施率である場合も多かった。しかし、これらの特定業種は、一部上場企業に比べて、そもそも外部接続していない割合が高いことを考慮に入れるべきであろう。なお、医療/交通では専用線接続の割合が少なく、一部上場/金融/情報通信では専用線接続の割合が高い傾向があった。
- インターネット接続およびダイアルアップ接続では、医療および交通関連の企業が対策を施していない割合が高い。一方、専用線接続では、金融/情報通信関連の企業でさえ、対策を施していない割合が高くなっている。

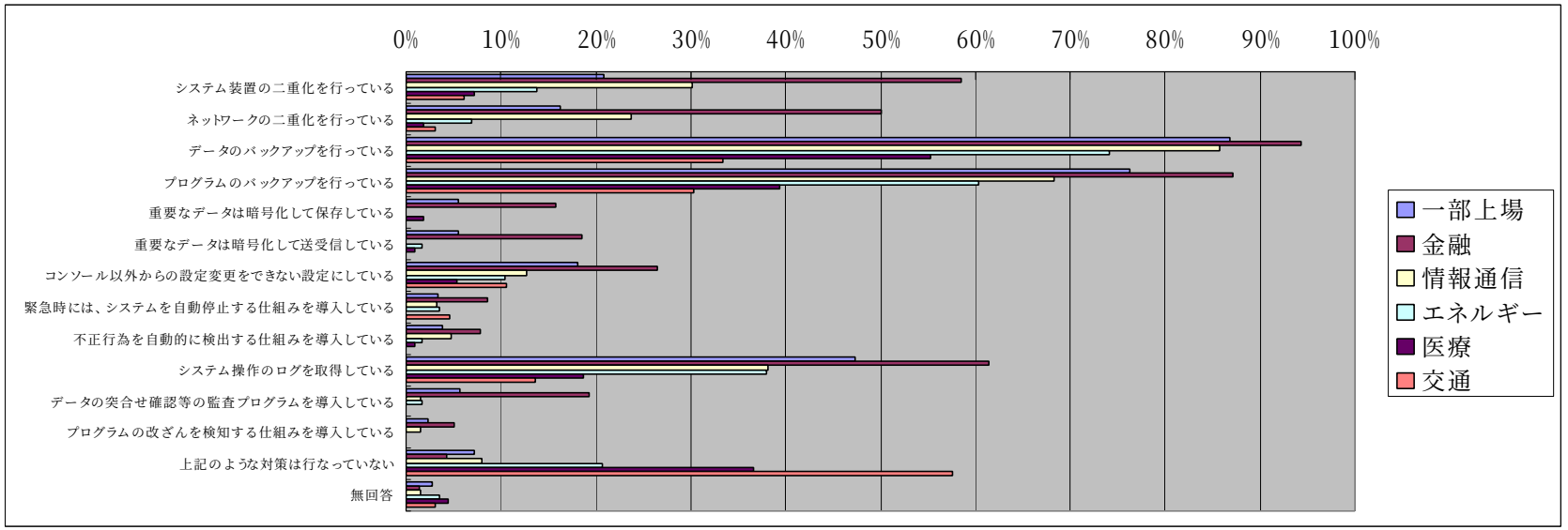
問13 貴社では、重要基幹システムへの侵入に対して、どのようなセキュリティ対策を導入していますか。（○はいくつでも）

	一部上場 n=476	金融 n=140	情報通信 n=63	エネルギー n=58	医療 n=112	交通 n=66
ネットワークには接続していない	6.7%	7.9%	6.3%	12.1%	25.0%	15.2%
他のネットワークと分離した専用のネットワークを使用している	31.1%	61.4%	50.8%	31.0%	35.7%	22.7%
ネットワークのアクセスコントロール（ルーティング制限等）を行っている	33.0%	26.4%	31.7%	27.6%	5.4%	10.6%
重要基幹システム専用のファイアウォールを導入している	6.7%	7.9%	15.9%	5.2%	3.6%	1.5%
IDとパスワードでユーザ認証をしている	66.8%	55.0%	61.9%	63.8%	33.0%	22.7%
指定回数以上ログインに失敗すると、ログイン権限が無くなる仕組みを導入している	15.5%	20.7%	12.7%	8.6%	1.8%	3.0%
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）でユーザ認証している	4.0%	5.7%	3.2%	5.2%	0.0%	0.0%
ソフトウェアのセキュリティホールに対して、パッチやバージョンアップを行っている	13.7%	13.6%	22.2%	12.1%	3.6%	3.0%
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	3.6%	6.4%	4.8%	3.4%	0.0%	0.0%
システムへのアクセスのログを取得している	32.6%	40.0%	30.2%	22.4%	8.0%	9.1%
擬似アタックを定期的に行い、対策をチェックしている	1.3%	1.4%	0.0%	0.0%	0.0%	0.0%
通信を暗号化する仕組みを導入している	3.6%	7.9%	0.0%	3.4%	0.9%	0.0%
上記のような対策は行なっていない	5.7%	3.6%	1.6%	10.3%	21.4%	42.4%
無回答	1.7%	1.4%	1.6%	3.4%	1.8%	3.0%



問14 貴社では、重要基幹システムでの侵入後の不正行為に対して、どのようなセキュリティ対策を導入していますか。（○はいくつでも）

	一部上場 n=476	金融 n=140	情報通信 n=63	エネルギー n=58	医療 n=112	交通 n=66
システム装置の二重化を行っている	20.8%	58.6%	30.2%	13.8%	7.1%	6.1%
ネットワークの二重化を行っている	16.2%	50.0%	23.8%	6.9%	1.8%	3.0%
データのバックアップを行っている	86.8%	94.3%	85.7%	74.1%	55.4%	33.3%
プログラムのバックアップを行っている	76.3%	87.1%	68.3%	60.3%	39.3%	30.3%
重要なデータは暗号化して保存している	5.5%	15.7%	0.0%	0.0%	1.8%	0.0%
重要なデータは暗号化して送受信している	5.5%	18.6%	0.0%	1.7%	0.9%	0.0%
コンソール以外からの設定変更をできない設定にしている	18.1%	26.4%	12.7%	10.3%	5.4%	10.6%
緊急時には、システムを自動停止する仕組みを導入している	3.4%	8.6%	3.2%	3.4%	0.0%	4.5%
不正行為を自動的に検出する仕組みを導入している	3.8%	7.9%	4.8%	1.7%	0.9%	0.0%
システム操作のログを取得している	47.3%	61.4%	38.1%	37.9%	18.8%	13.6%
データの突合せ確認等の監査プログラムを導入している	5.7%	19.3%	1.6%	1.7%	0.0%	0.0%
プログラムの改ざんを検知する仕組みを導入している	2.3%	5.0%	1.6%	0.0%	0.0%	0.0%
上記のような対策は行なっていない	7.1%	4.3%	7.9%	20.7%	36.6%	57.6%
無回答	2.7%	1.4%	1.6%	3.4%	4.5%	3.0%



問13及び問14　重要基幹システムにおけるセキュリティ対策

Point

- 一部上場企業に比べ、金融/情報通信関連の企業は、「他のネットワークと分離した専用のネットワークを使用している」割合が高い傾向がある。（問13)
- 問14に示す「重要基幹システムでの侵入後の不正行為」対策に関しては、すべての選択肢において金融機関が最多であった。「システム装置の二重化」、「ネットワークの二重化」、「暗号化して保存」、「暗号化して送受信」、「緊急時自動停止」など多くの項目で一部上場企業の倍以上の実施率を示した。
- 医療/交通分野では、重要基幹システムにおけるセキュリティ対策を施していない割合が高い。

問13 vs問9-1 重要基幹システムとセキュリティ対策（不正侵入防止）

	人命にかかわるシステムがある n=71	国防や治安維持、行政機能が脅かされるシステムがある n=3	顧客の財産が脅かされるシステムがある n=250	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 n=55	社会的混乱・パニックを招くシステムがある n=89	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 n=467	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 n=152	情報の改ざんによる信用低下へつながるシステムがある n=317	社会的に深刻な被害には至らないが、自社にとっては深刻な被害に至るシステムがある n=478	その他 n=4
ネットワークには接続していない	22.5%	0.0%	5.6%	10.9%	9.0%	9.4%	6.6%	5.7%	8.4%	0.0%
他のネットワークと分離した専用のネットワークを使用している	38.0%	66.7%	47.2%	40.0%	52.8%	38.1%	46.1%	42.9%	28.9%	25.0%
ネットワークのアクセスコントロール（ルーティング制限等）を行っている	4.2%	33.3%	30.8%	34.5%	32.6%	28.7%	31.6%	32.2%	32.8%	0.0%
重要基幹システム専用のファイアウォールを導入している	2.8%	33.3%	6.8%	10.9%	6.7%	6.2%	5.9%	7.6%	7.5%	0.0%
ネットワークアクセスコントロール計	54.9%	100.0%	74.0%	76.4%	76.4%	66.0%	71.1%	67.8%	60.7%	25.0%
IDとパスワードでユーザ認証をしている	33.8%	100.0%	65.6%	60.0%	55.1%	66.2%	69.7%	66.2%	65.9%	100.0%
指定回数以上ログインに失敗すると、ログイン権限が無くなる仕組みを導入している	2.8%	33.3%	19.2%	12.7%	14.6%	14.1%	20.4%	18.9%	12.6%	25.0%
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）でユーザ認証している	0.0%	33.3%	5.2%	7.3%	3.4%	3.9%	5.3%	4.7%	4.0%	0.0%
アカウント・パスワード管理計	33.8%	100.0%	67.6%	63.6%	55.1%	67.7%	70.4%	67.5%	67.4%	100.0%
ソフトウェアのセキュリティホールに対して、パッチやバージョンアップを行っている	2.8%	33.3%	17.6%	18.2%	20.2%	15.2%	20.4%	16.7%	13.8%	0.0%
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	0.0%	0.0%	5.6%	3.6%	6.7%	3.6%	5.3%	5.0%	3.3%	25.0%
システムへのアクセスのログを取得している	7.0%	33.3%	39.2%	34.5%	36.0%	32.8%	42.1%	39.7%	29.1%	50.0%
擬似アタックを定期的に行い、対策をチェックしている	0.0%	0.0%	2.0%	1.8%	2.2%	1.5%	3.3%	2.2%	1.3%	0.0%
通信を暗号化する仕組みを導入している	0.0%	33.3%	4.8%	3.6%	3.4%	2.6%	5.9%	3.5%	2.3%	25.0%
上記のような対策は行なっていない	26.8%	0.0%	4.8%	9.1%	9.0%	6.2%	3.3%	6.6%	6.5%	0.0%
無回答	0.0%	0.0%	0.8%	0.0%	0.0%	0.9%	0.7%	0.9%	2.5%	0.0%

Point

- 上図は重要基幹システムの種類毎に、対策の状況を見たものである。
- 「人命にかかわるシステム」を保有する企業においては、ネットワークの物理・論理アクセスコントロールを行っているものが半数強(54.9%)、ID・パスワードによる対策を行っている企業が1/3社程度に留まっている。
- また、「顧客の財産が脅かされるシステム」「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」「社会的混乱・パニックを招くシステム」を保有する企業では、重要基幹システムに対して4社に3社の割合(74.0%, 76.4%, 76.4%)でネットワークアクセスコントロールを行っており、またID・パスワードでの対策も3社に2社の割合で対策を施している。
- システムへのアクセスログを取得しているのは、全体的に3割から4割程度であり、有事の際の対応に懸念が残る。また「人命にかかわるシステム」を保有する企業では、アクセスログの取得は7%に留まっている。

問14 vs問9-1 重要基幹システムとセキュリティ対策（侵入後の対策）

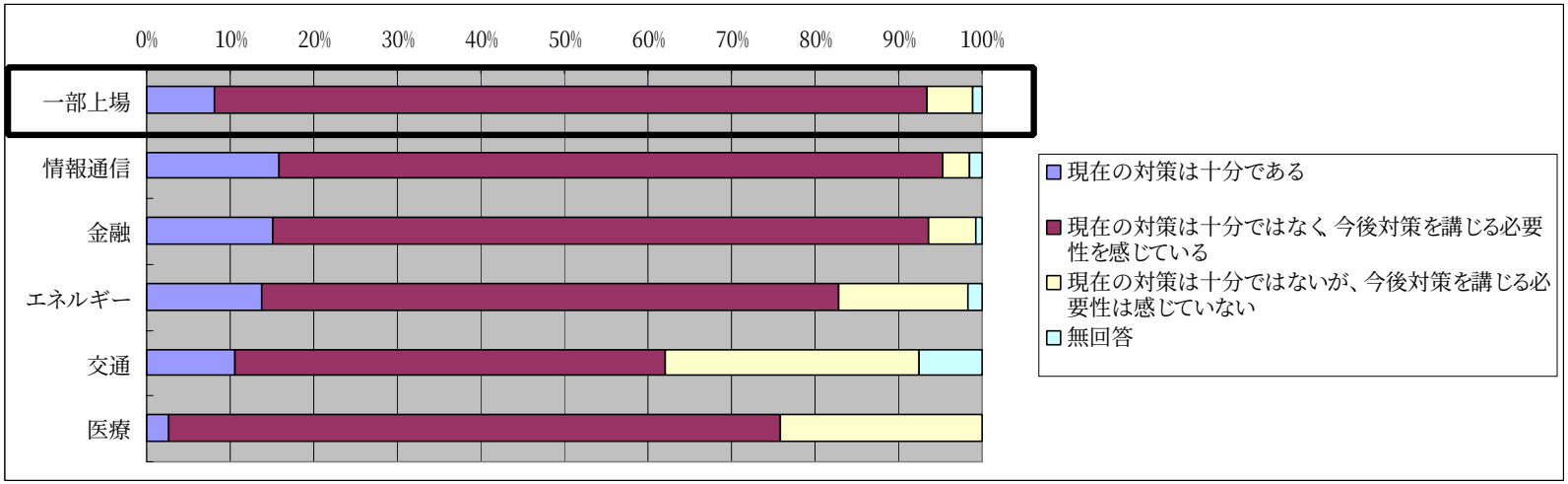
	人命にかかわるシステムがある n=71	国防や治安維持、行政機能が脅かされるシステムがある n=3	顧客の財産が脅かされるシステムがある n=250	ライフラインやプラントが停止/暴走してしまうシステムがある n=55	社会的混乱・パニックを招くシステムがある n=89	個人のプライバシーが侵害される情報を扱うシステムがある n=467	他人になりすますことのできる情報を扱うシステムがある n=152	情報の改ざんによる信用低下へつながるシステムがある n=317	社会的に深刻な被害には至らないが、自社にとっては深刻な被害に至るシステムがある n=478	その他 n=4
システム装置の二重化を行っている	8.5%	33.3%	40.8%	20.0%	43.8%	25.5%	44.7%	30.9%	15.1%	50.0%
ネットワークの二重化を行っている	2.8%	66.7%	32.4%	18.2%	33.7%	18.8%	36.8%	23.7%	10.9%	0.0%
データのバックアップを行っている	49.3%	100.0%	90.8%	80.0%	75.3%	85.7%	91.4%	87.4%	83.3%	100.0%
プログラムのバックアップを行っている	38.0%	100.0%	84.0%	67.3%	69.7%	76.0%	84.9%	77.9%	71.8%	100.0%
重要なデータは暗号化して保存している	1.4%	0.0%	9.2%	5.5%	4.5%	6.0%	12.5%	7.9%	2.7%	0.0%
重要なデータは暗号化して送受信している	0.0%	0.0%	10.0%	1.8%	10.1%	6.2%	12.5%	8.5%	2.7%	25.0%
コンソール以外からの設定変更をできない設定にしている	7.0%	33.3%	18.8%	16.4%	20.2%	14.3%	21.1%	17.0%	15.3%	0.0%
緊急時には、システムを自動停止する仕組みを導入している	1.4%	0.0%	6.0%	5.5%	9.0%	4.1%	9.2%	5.7%	2.1%	0.0%
不正行為を自動的に検出する仕組みを導入している	1.4%	0.0%	6.4%	7.3%	6.7%	4.1%	7.2%	5.4%	2.9%	25.0%
システム操作のログを取得している	25.4%	66.7%	59.2%	43.6%	46.1%	49.0%	60.5%	57.7%	41.8%	0.0%
データの突合せ確認等の監査プログラムを導入している	0.0%	0.0%	10.8%	1.8%	7.9%	6.0%	13.8%	8.2%	2.1%	0.0%
プログラムの改ざんを検知する仕組みを導入している	0.0%	0.0%	4.8%	3.6%	3.4%	2.6%	5.3%	4.1%	1.7%	0.0%
上記のような対策は行なっていない	45.1%	0.0%	6.0%	12.7%	18.0%	10.1%	5.9%	7.9%	9.0%	0.0%
無回答	0.0%	0.0%	1.6%	0.0%	0.0%	1.1%	1.3%	1.3%	3.3%	0.0%

Point

- 「顧客の財産が脅かされるシステム」を保有する企業では、一部上場平均よりも対策を行っている割合が高い。
- 「人命に関わるシステム」「国防や治安維持、行政機能を脅かされるシステム」以外の重要インフラを担う企業では、総じて一部上場平均並みの対策状況となっている。
- 対策として多いのは、データやプログラムのバックアップ、ログの取得等で、いずれも旧来からの対策であり、不正侵入やサイバーテロに対する対策として有効な暗号化、改ざん検知、不正行為検出などの対策の普及率は、重要基幹インフラを担う企業においてもまだ高くはない。

問15 貴社の現在のセキュリティ対策は、サイバーテロに対して有効だと考えていますか。担当者自身のご意見で結構ですのでお答えください。（○は一つ）

	一部上場 n=476	情報通信 n=63	金融 n=140	エネルギー n=58	交通 n=66	医療 n=112
現在の対策は十分である	8.2%	15.9%	15.0%	13.8%	10.6%	2.7%
現在の対策は十分ではなく、今後対策を講じる必要性を感じている	85.3%	79.4%	78.6%	69.0%	51.5%	73.2%
現在の対策は十分ではないが、今後対策を講じる必要性は感じていない	5.5%	3.2%	5.7%	15.5%	30.3%	24.1%
無回答	1.1%	1.6%	0.7%	1.7%	7.6%	0.0%

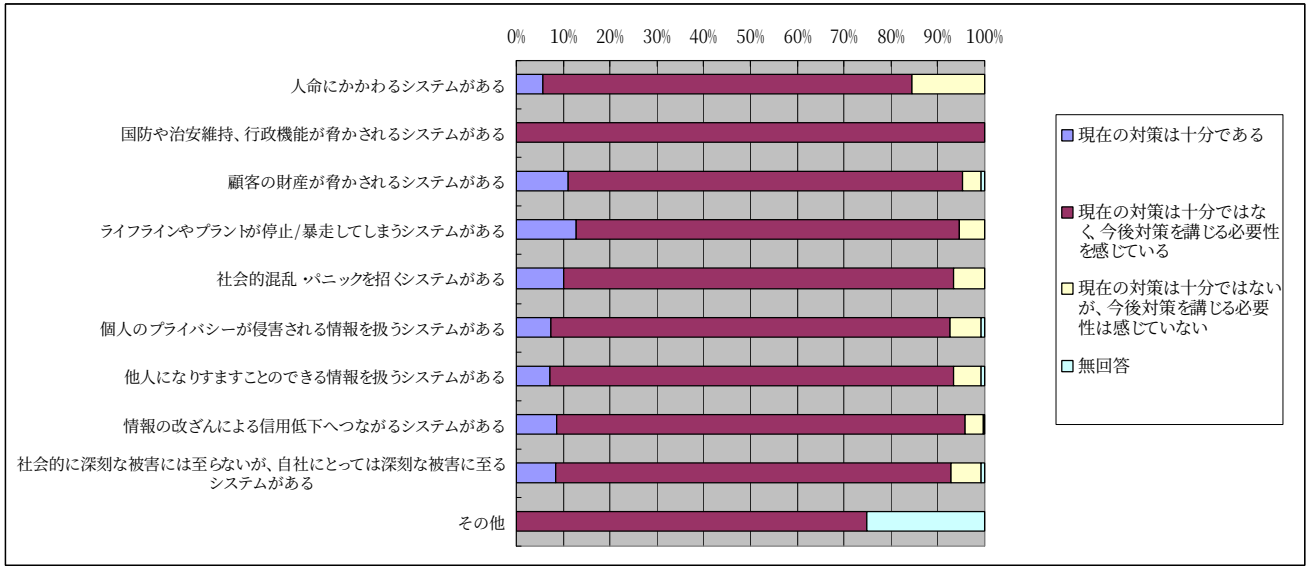


Point

- どの業種でも多くの企業が、「今後対策を講じる必要性」を感じている。
- 対策実施度の高い金融/情報通信関連の企業に比べ、対策実施度の低い交通/医療関連の企業の方が「今後対策を講じる必要性を感じていない」割合が高い。

問15 vs問9-1 重要基幹システムとセキュリティ対策の十分性

	人命にかかわるシステムがある n=71	国防や治安維持、行政機能が脅かされるシステムがある n=3	顧客の財産が脅かされるシステムがある n=250	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 n=55	社会的混乱・パニックを招くシステムがある n=89	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 n=467	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 n=152	情報の改ざんによる信用低下へつながるシステムがある n=317	社会的に深刻な被害には至らないが、自社にとっては深刻な被害に至るシステムがある n=478	その他 n=10
現在の対策は十分である	5.6%	0.0%	11.2%	12.7%	10.1%	7.5%	7.2%	8.5%	8.4%	0.0%
現在の対策は十分ではなく、今後対策を講じる必要性を感じている	78.9%	100.0%	84.8%	81.8%	83.1%	85.0%	86.2%	87.4%	84.5%	75.0%
現在の対策は十分ではないが、今後対策を講じる必要性は感じていない	15.5%	0.0%	4.0%	5.5%	6.7%	6.6%	5.9%	3.8%	6.3%	0.0%
無回答	0.0%	0.0%	0.8%	0.0%	0.0%	0.9%	0.7%	0.3%	0.8%	25.0%



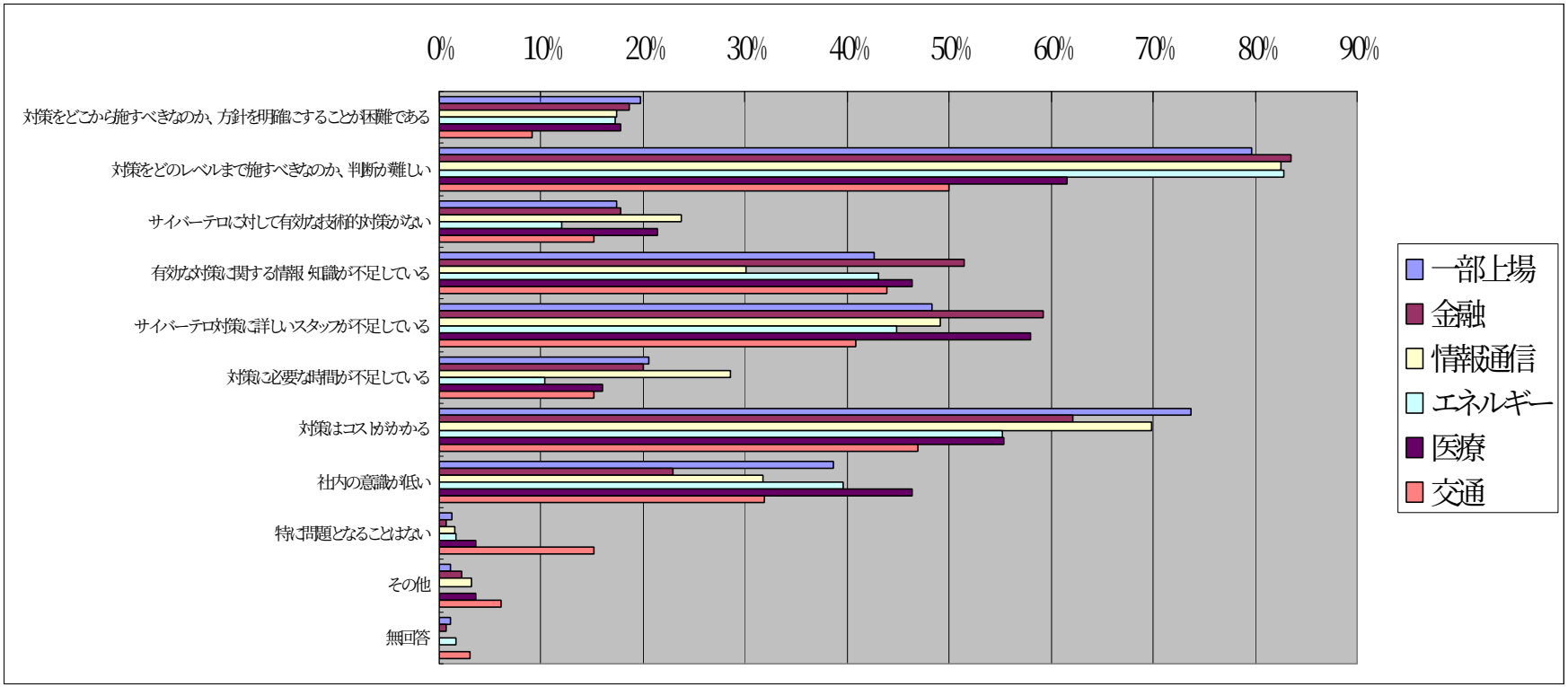
Point

- 重要基幹システムを保有する企業では、いずれの種類のシステムでも8割以上の企業で「今後対策を講じる必要性がある」と回答している。これは、一部上場平均の意識(85.3%)と同程度の危機意識である。
- 一方、「人命にかかわるシステム」を保有する企業では、「対策は十分ではないものの、今後の対策の必要性はない」としている企業が、他の種類の重要基幹システムを保有する企業よりも3倍程度多い結果となっている。

問16 サイバーテロに対するセキュリティ対策を実施する上でどのようなことが問題になるとお考えですか。担当者自身のご意見で結構ですのでお答えください。（○はいくつでも）

	一部上場 n=476	金融 n=140	情報通信 n=63	エネルギー n=58	医療 n=112	交通 n=66
対策をどこから施すべきなのか、方針を明確にすることが困難である	19.7%	18.6%	17.5%	17.2%	17.9%	9.1%
対策をどのレベルまで施すべきなのか、判断が難しい	79.6%	83.6%	82.5%	82.8%	61.6%	50.0%
サイバーテロに対して有効な技術的対策がない	17.4%	17.9%	23.8%	12.1%	21.4%	15.2%
有効な対策に関する情報・知識が不足している	42.6%	51.4%	30.2%	43.1%	46.4%	43.9%
サイバーテロ対策に詳しいスタッフが不足している	48.3%	59.3%	49.2%	44.8%	58.0%	40.9%
対策に必要な時間が不足している	20.6%	20.0%	28.6%	10.3%	16.1%	15.2%
対策はコストがかかる	73.7%	62.1%	69.8%	55.2%	55.4%	47.0%
社内の意識が低い	38.7%	22.9%	31.7%	39.7%	46.4%	31.8%
特に問題となることはない	1.3%	0.7%	1.6%	1.7%	3.6%	15.2%
その他	1.1%	2.1%	3.2%	0.0%	3.6%	6.1%
無回答	1.1%	0.7%	0.0%	1.7%	0.0%	3.0%

No.	対象グループ	業種	問16　サイバーテロ対策を実施する上での問題（その他）
1	[特定]	信販	社内ネットワークからの協力者をつてにしてのテロに対する対策は抜本的な対策が難しい
2	[特定]	病院・医院	OFFラインで処理している
3	[特定]	病院・医院	企業の代表者（経営者）の関心が低く、対策を講じる費用、時間、体制が得られていない状況です。本来、社内ネットワークからインターネットや外部ネットワークと接続する場合、サーバー（ファイアウオール）を経由し、行うべきでありますが、各々のパソコンについているモデムを使用して接続しているケースが大半です。
4	[上場]	鉱業	メインフレーム系のセキュリティ対策の技術情報が不足
5	[上場]	機械	頻度が高い現像ではないため、切実性があまりない面がありセキュリティーホールができやすい
6	[特定]	その他金融機関	プロバイダー内のホームページに関するセキュリティ
7	[特定]	病院・医院	現状では必要性がない
8	[特定]	鉄道・地下鉄	今後の情報システムの強化により対策が必要となってくる
9	[特定]	病院・医院	現在の技術的状況から見ると、自前での防御だけでは非現実的で、低コストの強力なツールないしアウトソーシング化を期待し
10	[上場]	不動産	日本では海外よりも不正侵入の認識があまく、役職員のシステムへの関心も低い。不正侵入への危険だけ見ている
11	[上場]	その他サービス	基幹システムとネットワーク系を切り離している
12	[特定]	通信	誤った情報の流布等に対処する方法がない
13	[特定かつ上場]	銀行	①システムのアクセスログをすべて取得していくためには膨大なシステム投資が必要 ②「不正行為を自動的に検出する仕組み」は、複数サイト等を対応すると非常に高額となる



Point

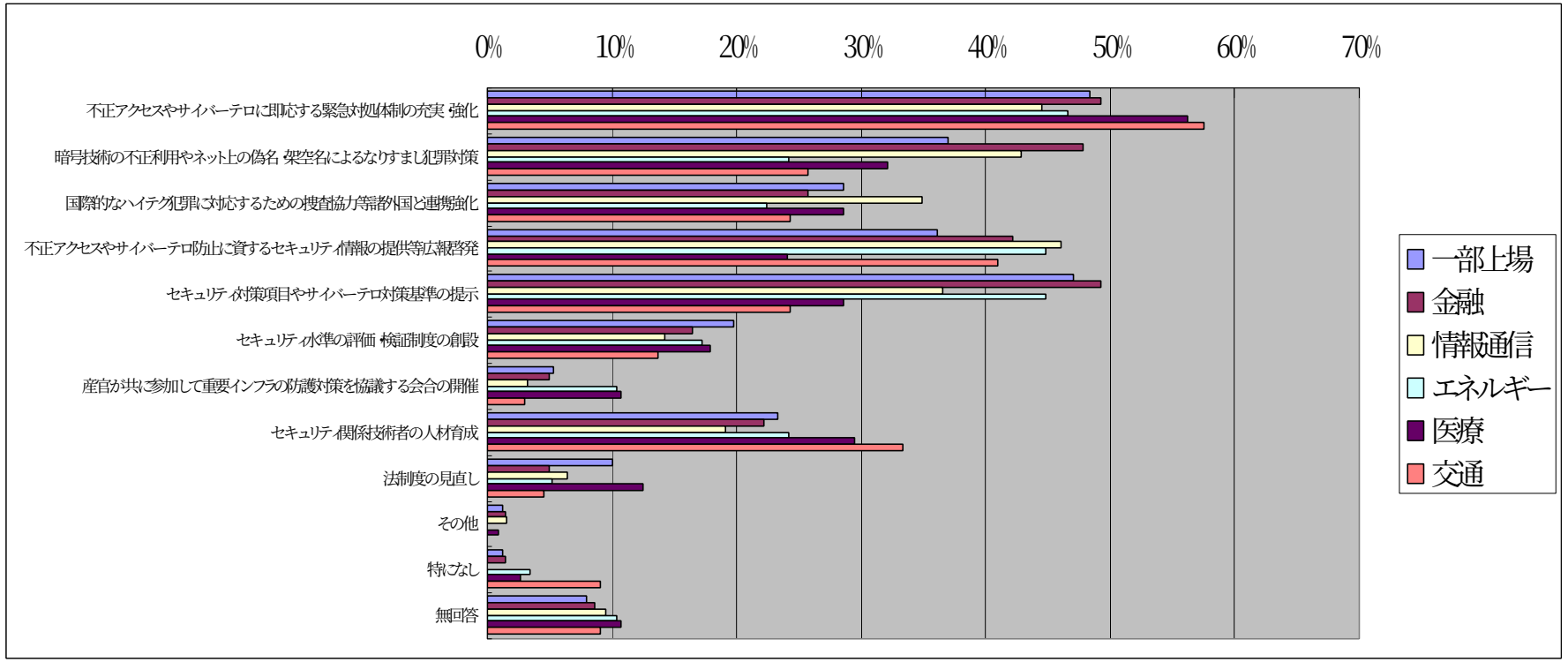
- 業種間のばらつきは少ない
- 「対策をどこから施すかが明確」であっても、「対策をどのレベルまで施すか」の判断が難しいようである。

問17　行政で検討している以下の施策のうち、最も期待するものを3つ選択してください。（○は3つ）

	一部上場 n=476	金融 n=140	情報通信 n=63	エネルギー n=58	医療 n=112	交通 n=66
不正アクセスやサイバーテロに即応する緊急対処体制の充実・強化	48.3%	49.3%	44.4%	46.6%	56.3%	57.6%
暗号技術の不正利用やネット上の偽名・架空名によるなりすまし犯罪対策	37.0%	47.9%	42.9%	24.1%	32.1%	25.8%
国際的なハイテク犯罪に対応するための捜査協力等諸外国と連携強化	28.6%	25.7%	34.9%	22.4%	28.6%	24.2%
不正アクセスやサイバーテロ防止に資するセキュリティ情報の提供等広報啓発	36.1%	42.1%	46.0%	44.8%	24.1%	40.9%
セキュリティ対策項目やサイバーテロ対策基準の提示	47.1%	49.3%	36.5%	44.8%	28.6%	24.2%
セキュリティ水準の評価・検証制度の創設	19.7%	16.4%	14.3%	17.2%	17.9%	13.6%
産官が共に参加して重要インフラの防護対策を協議する会合の開催	5.3%	5.0%	3.2%	10.3%	10.7%	3.0%
セキュリティ関係技術者の人材育成	23.3%	22.1%	19.0%	24.1%	29.5%	33.3%
法制度の見直し	10.1%	5.0%	6.3%	5.2%	12.5%	4.5%
その他	1.3%	1.4%	1.6%	0.0%	0.9%	0.0%
特になし	1.3%	1.4%	0.0%	3.4%	2.7%	9.1%
無回答	8.0%	8.6%	9.5%	10.3%	10.7%	9.1%

No.	対象グループ	業種	問17.10　行政で検討している施策に期待 その他具体的に）
1	[上場]	その他サービス	公的な認証機関（ex.ベリサイン）のようなものが必要。早急に
2	[上場]	鉱業	セキュリティ関係ベンチャー育成のため、開発などを伴うプロジェクトの立ち上げ
3	[上場]	建設	不正アクセスが犯罪であることの周知と罰則の強化
4	[特定]	新聞	サイバーポリス等、専門警察官の養成、組織作り
5	[特定かつ上場]	銀行	不正アクセスを自動的に検出する仕組みの安価な供給、税制優遇
6	[特定かつ上場]	銀行	不正アクセス禁止法等の実際の運用、取り締まり

No.	対象グループ	業種	問17.9　行政で検討している施策に期待（法制度見直しを具体的に）
1	[特定]	病院・医院	罪は罪。罰則の軽いものはダメ！罰則は軽い犯罪でも重くするべき！
2	[上場]	その他（）	罰則の強化
3	[特定]	信販	不正に入手した情報を保有・保持していることに対する罰則
4	[上場]	食品	税の減免
5	[上場]	化学	罰則の強化
6	[上場]	食品	PR、広報活動の活発化
7	[上場]	機械	防止（発生前）、発生時の対処方策、即発事案への総合的な罰則法体系を整えること
8	[上場]	不動産	サイバーテロに関する法律の整備
9	[特定]	ガス	対策実施の優遇措置
10	[上場]	非鉄/金属製品	罰則の明確化と強化
11	[特定]	病院・医院	罰則の強化
12	[上場]	その他サービス	アタックをかけた者に対する罰則
13	[上場]	機械	罰則規定
14	[特定]	通信	サイバー犯罪に関する事項および取り締まりの強化等
15	[上場]	ゴム・窯業	処罰条項の整備・強化
16	[特定]	建設	ネット犯罪に対する罰則の強化、プロバイダー等の捜査協力の制度化
17	[上場]	流通・卸売	罰の強化
18	[上場]	流通・卸売	国際的な基準が必要
19	[特定]	病院・医院	罰則規定の強化
20	[特定かつ上場]	銀行	サイバーテロに対する罰則強化
21	[上場]	建設	罰則の強化、適用範囲の拡大
22	[上場]	食品	処罰等の強化
23	[特定]	病院・医院	罰則の強化
24	[上場]	小売・飲食	もっと重い刑罰を課してほしい
25	[上場]	機械	罰則強化
26	[上場]	建設	罰則対象の拡大と強化
27	[特定]	その他金融機関	クレジットカード不正使用に関する取り締まり強化のための法整備
28	[上場]	繊維	企業（セキュリティ義務）に対する罰則がない
29	[特定]	病院・医院	不正アクセス行為禁止法
30	[特定]	その他サービス	刑法などの法規の改正や新法の作成において罰則の盛り込み
31	[上場]	電気機器	罰則の設定、犯罪との境を明確に
32	[特定]	その他サービス	偽造カード利用やスキミング、不正アクセスに対し法制度が追いついていない
33	[特定]	その他金融機関	不正アクセス行為禁止法
34	[上場]	流通・卸売	罰則を強化し、ネット犯罪に適応できる法制度にする
35	[上場]	その他製造	罰則規定の明確化
36	[上場]	小売・飲食	罰則強化を



Point

- 情報通信関連企業を除いて、「緊急対処体制の充実・強化」を望む声が多かった。
- 業種間のばらつきは少ない。
- 「法制度の見直し」を求める割合は10%弱であったが、その具体的内容は、「罰則の強化」が多かった。

問18 サイバーテロに対する警察の取り組みに関して、ご意見・期待すること等があればご記入ください。（以下に集計した回答を原文のまま掲載します。）

No.	対象グループ	業種	問18　サイバーテロに対する警察の取り組み（自由記入）
1	[上場]	建設	重罪を課す。
2	[特定]	病院・医院	セキュリティの指導、育成（個別企業へ）。
3	[特定]	病院・医院	新しい犯罪形態であり、影響の深刻度を考慮すると早い段階での対応が必要かと思います。素人的には、刑罰の程度を通常よりあげるなどの環境を作り、少なくともハッカー的な行為は最小限に抑えるべきだと思います。
4	[特定]	ｲﾝﾀｰﾈｯﾄｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ	テロに関するセキュリティの在り方、情報の開示。
5	[上場]	その他（）	他の一般犯罪と同程度の対応（取締及び罰則）を実施する。
6	[上場]	食品	担当部署が上申しても経営者は景気低迷時につき許可しない。法律で義務づけないと難しいのではないか？
7	[特定]	病院・医院	期待することはないが、この情報が漏れないのでしょうか？
8	[特定かつ上場]	鉄道・地下鉄	日本の警察は、人の生死が問題になると真剣に動くが、それ以外のことには事なかれ主義でなるべく首を突っ込まない所だと解釈しております。権利権益についても同じことが言えると思いますので、なお一層の努力をお願いします。
9	[上場]	建設	「不正アクセス行為禁止法」による取締には期待していますが、技術変革のスピードの早い世界です。産官が共同で対策を協議する機関の設置等を期待します。
10	[上場]	化学	1. 不正アクセス発生時の窓口を明確にすべき。現在JPCERTに連絡しているが、別に存在するのかどうかよくわからない。 2. 迅速な対応。JPCERTでは受付から回答まで2～3日を要する。 3. 対応策の具体化。JPCERTの回答では抽象的すぎて対応のわからないことがある（実害が発生する可能性が高くなる）。責任範囲の明確化、企業が必要とする技術レベルの制度化が必要と考えます。
11	[上場]	紙・パルプ	迅速なる対策をお願い致します。社名や、自社のネットワークの弱点を記したこのアンケートの封筒の表に「サイバーテロ…」と記されている。この郵便物が盗まれた時のことを考えると不安である。
12	[上場]	精密機器	問題が発生したから実施するのではなく、全体の流れを見て早めの対応を期待します。刑罰の強化も一つの方法かもしれません。
13	[上場]	建設	1. 罰則を重くすることと被害者への償い範囲の明文化 2. 上場企業に大使監査と助言の実施
14	[上場]	その他サービス	1. 関連機関（JPCERT/cc、IPAセキュリティセンター、海外の機関など）との迅速な情報交換 2. 不正アクセス、サイバーテロ情報の開示、広告（マスコミ、URLなどを利用）
15	[特定]	新聞	World Wideな取り組みでなければ無意味。日本国内だけの取り組みではほとんど無意味。
16	[特定かつ上場]	石油卸	サイバーテロは犯罪であるという確固たる姿勢の下に、国家的レベルで対策を講じてほしい。
17	[特定]	病院・医院	コンピュータシステムのほとんどが、警察が介入してからでは遅く、結果は災厄の状態になると考えられます。まず自己防衛、次に法的規制、そして教育が必要だと思われます。 これから10年のうちに「電子商取引」がますます盛んになり、ネットバンキング、キャッシュカードのICカード他など。仮想空間と実在の区別がなくなりつつある現在、各個人のレベルにまでネット犯罪の「魔の手」が伸びつつあります。 これはわが国だけの問題としてではなく、他国の連携により情報収集するとともに、次世代を担う子供達にも「悪いこと」であるという「教育」も行うべきだと考えます。
18	[特定]	放送	サイバーテロに対し警察がどの程度スキルがあるのかが不明であり、相当のレベルに達していないとテロ防止につながらないのでは……。外国のような、クラッカーの採用など「毒には毒を」の考え方が有効と考える。
19	[上場]	非鉄/金属製品	専門チームを編成し、意欲的に取り組んでほしい。
20	[特定]	病院・医院	本件は、とにかく焦眉の急務です。一刻も早く、サイバーテロに対応する体制を確立して頂きたいと願っています。

No.	対象グループ	業種	問18　サイバーテロに対する警察の取り組み（自由記入）
21	[特定かつ上場]	銀行	産官での情報の共有化が重要である。ホームページ等で具体的事例、対応すべき方策等を案内し、また情報収集も一層綿密に実施していただきたい。一企業で対応を検討することは相当の体力が必要であり、多くの情報提供を期待する。
22	[上場]	食品	サイバーテロの検挙率を上げることにより、再発、模倣版の発生を防ぐことを期待します。
23	[特定]	電力	・サイバーテロリスト、内容、対策の公表 ・サイバーテロリストに対する厳しい罰則 ・通信プロバイダーのサイバーテロ防止に対する情報提供の義務づけと違反プロバイダーに対する免許取消し（法改正）
24	[上場]	小売・飲食	行政が被害を受けてからこのように騒がれておりますが、一般社会ではかなり以前から大小とわず被害は発生していたと思います。防止策も大切ですが、被害を受けた時にすぐに復帰できる環境作りが我々にとって一番と思います。
25	[特定かつ上場]	銀行	積極的な情報提供を期待します。
26	[上場]	鉱業	予算の配分を見直して、サイバーテロ関係の比率を上げてほしい。
27	[特定]	通信	サイバーテロ対策を広く啓発すること、それによる情報流出とのバランス、対策を十分検討してほしい。
28	[上場]	機械	活動の水準として米国FBIやこの分野の先進諸国の同等機関の行っている内容と、同等のレベルを維持し、日本独自の手法と順次対かされていくことを希望いたします。
29	[特定]	病院・医院	今後、インターネットが急速に発展するものと予想されるので、民も官もそれに対応できる人材の育成が重要と思われます。
30	[上場]	建設	被害の度合いにより罪を重くする。
31	[上場]	化学	技術的に限界がある以上、自己防衛だけでは被害防止にはなり得ない。そのため、法律による取締が重要と思うので、今後はいかに不正行為をパトロールし、立証していくことができるかがカギとなる。技術、体制強化に期待する。
32	[上場]	不動産	官庁へのシステム進入が相次ぎ、信頼が失われている。外部発注ではなく、内部で運営管理できる仕組みを作ってほしい。
33	[上場]	非鉄/金属製品	国境なき電子商取引が現実になろうとしている中で、安全にインターネットに産業の一部を任せられるとよいと考える。
34	[特定]	ガス	不正アクセスデータの逆探知調査技術の向上
35	[特定]	石油製造	警察の取り組みよりも、まず法整備の法が先決ではないでしょうか。
36	[特定]	銀行	専門集団で威厳のある組織で取り組んでいただきたい。
37	[上場]	その他製造	我が国のお粗末な対応状況から判断して、各企業は自助努力にて守るしかないと思っています。もし国が支援してくれるなら、こういった対策ではなく有効なアプリケーション購入の補助を金銭面でお願いします。
38	[上場]	流通・卸売	日本だけ対象にしていては意味が無いと思っています。
39	[特定]	航空	今後、サイバーテロは増加していく傾向にあると思われます。ハイテク化していく中で、取締を行うことは容易ではないと思われます。関係機関並びに民間企業（プロバイダー、メーカー等）と共同で対策を講ずることが必要と思われます。 特にインターネット経由での不正アクセスに対し、プロバイダー等からの情報提供を法制化するのもやむおえない処置と考えます。一方で個人のプライバシーを守るという大前提に基づき取り組んでほしい。
40	[特定]	病院・医院	組織の管理者に対する啓発を行ってほしい。年齢が高く、インフラのセキュリティに対して認識が低い。

No.	対象グループ	業種	問18　サイバーテロに対する警察の取り組み（自由記入）
41	[上場]	紙・パルプ	情報流出・改ざんに対して罪を重くすべき。
42	[上場]	精密機器	現在の法律の中での警察活動に多くの限界があるらしいことは承知しておりますが、「犯罪を犯す気になれない」割に合わない」仕組みが作られることで、ある程度の牽制が働くことをまずは望みます。
43	[特定]	放送	ほとんど期待していません。スキル不足が重大なミスにつながり被害を拡大しかねない。
44	[特定]	病院・医院	当病院では、患者、技師を対象としたHPを外注のサーバーにて運用しています。また院内の情報システムとは別系統になっているため、インターネットを通じて入ることはあり得ません。 ただ、今後インターネットからの受信予約も考えており、院内の情報システムとリンクする可能性があります。国としての基準を作ってもらい、国公立の病院当に病院の基本的なセキュリティポリシーを作ってもらいたい。 民間病院はそういった見本がでkないとなかなか難しいと思う。
45	[上場]	電気機器	問17では行政の視点で回答したが、警察の取り組みとしてはグローバルベースでのハイテク犯罪への対応のためには諸外国、民間IT（ハイテク）企業と連携を強くする必要がある。
46	[特定]	放送	セキュリティ危機管理の重要性の広報と啓発
47	[特定]	新聞	サイバーテロまでいかなくても企業や個人に対する誹謗、中傷はある。多くが直接相手側と接触するのを避け、我慢をしている。これらが訴えより、適切な処置ができるようになればもっとスムーズな意思の疎通ができるようになるのではないか。 このために警察の中に相談の窓口を設けるなどの対策が必要と思う。
48	[上場]	その他製造	取り組みに対する情報公開を適切に行ってほしい。
49	[特定]	病院・医院	警察にはサイバーテロを防止するだけのコンピュータや、ネットワークに詳しい人がいないのではやるだけ無駄だと思う。警察には何もできない。
50	[特定かつ上場]	航空	これからサイバーポリスの役割はますます重要になると思っています。民間企業の支援や協力や体制を含め、積極的に関って頂きたいところですが、警察そのものが官僚的であったり、信頼度が高まらないと相互協力も生まれませんので、ぜひ内部の改善も御願いします。
51	[特定]	建設	今後の情報化、特に電子取引はネットワークセキュリティの強化充実によるところが大きいと思います。ネットワークセキュリティは原則としては利用者の自己責任であると思うが、警察による犯罪対策の強化は大きな抑止力となると思います。
52	[特定かつ上場]	石油製造	社内的にセキュリティポリシーを策定し運用展開したいが、なかなか必要性の認識が少ないので思うように進まない。 理由は罰則がないためもあると思うので、法制度より必須的な環境になってくれれば、各社の取り組みも進んでいくと思われる。
53	[特定]	鉄道・地下鉄	侵入方法の事例と対策に関する啓発を期待。
54	[特定]	その他金融機関	取り組みのスピードが遅すぎるように感じます。もっとスピーディーに取り組めるよう警察自体のシステムを見直す必要があるのではないでしょうか。
55	[特定]	病院・医院	迅速な情報提供
56	[特定]	病院・医院	Net上で週刊サイバーテロ新聞とかいうMailマガジンを発行し、今現実に起こっている犯罪の手口などを紹介してほしいです。
57	[特定]	病院・医院	地域ごとにサイバーテロに関する施設・部門を作成設置してほしい。技術者を公的機関で育成教育するシステムを作成してほしい。
58	[上場]	ゴム・窯業	セキュリティは費用の割には効果が今ひとつ見えにくい分野ですので、何かきっかけがないと、大々的に導入するのは難しいです。最近のサイバーテロの手口と、その具体的な対策を公開していって頂きたいです。
59	[特定]	石油卸	正直に言って、現在の警察にはサイバーテロへの対策に深く参画することは賛成できない。対策に名を借りた情報の閲覧等の権限を与えると、別のことに利用するため防止策がはっきりせず、国家による情報官制につながる不安がある。
60	[特定]	航空	テロ対策はもちろん必要であるが、それ以前に利用するシステム、プログラム等の正しい運用（ロピーライetc）を徹底する必要がある。

No.	対象グループ	業種	問18　サイバーテロに対する警察の取り組み（自由記入）
61	[上場]	建設	・迅速な対応 ・人員の強化 ・警察内部の意識の向上（末端まで）
62	[上場]	ゴム・窯業	1. サイバーテロを100%阻止するのは困難で、コストも必要であるが、最低限この程度は必要であるとの基準が判ると良い。 2. インターネットが繋がっているどこからでもテロ行為は可能であり、発生した時の犯人の特定、検挙を全世界的に協力して行える大成がないと、いつまでたってもサイバーテロの危険性は少なくならないと思う。 3. コンピュータ技術の進歩と共に、サイバーテロの技術も進歩しており、一企業、個人がその対策を行っているとキリがない。セキュリティー対策の指針があると便利と思われる。
63	[特定]	病院・医院	犯罪者の特定、技術の向上
64	[上場]	小売・飲食	ネット上での本人確認、本人特定の仕組みを国レベルで確立し、その運用の法制度による保護。
65	[特定]	銀行	サイバーテロの手口や対策等の情報開示
66	[特定]	通信	サイバーポリスの創設は良いことと思います。
67	[上場]	小売・飲食	サイバーテロを行う人間は、軽い気持ちで行うかも知れないが、場合によっては大きな被害を受ける事もあるので、法制度を根本から見直し、思い付きでこの様な事が行えないような社会にしてほしい。
68	[上場]	輸送用機器	サイバーテロに関する具体的な事例、及び予想される事態を示し、啓発活動をしてほしい。
69	[特定]	病院・医院	問題が起きてから対応するのではなく、ある程度の予防対策をして欲しい。
70	[特定]	通信	サイバーテロは2つに分けて考慮する必要があると考える。ひとつは外部からの不正アクセスに対する問題。もうひとつは内部からの不正アクセスに対する問題である。どちらにしても問題発生後は警察が介入する必要があるかもしれないが、発生自体を予防する必要がある。これは警察というよりも、行政の関係省庁から企業に対して、十分なセキュリティを備えるための経済的な支援が必要ではないかと考える。また、特に内部からの不正アクセスについては、先日オウム関連企業がシステム開発に関わっていたという報道があったように、システム開発企業とは機密保持契約で縛るしかないのが現状であるが、更に踏み込んだセキュリティ対策の必要性を感じる。これに対する指針なり、検証方法について行政当局に何らかの対応を期待する。
71	[特定]	銀行	ネット上の口座作成屋（身分証明などの偽造）、口座情報売買（ネット上）の取り締まり。他人のデータ改ざん等の取り締まり。
72	[上場]	その他（）	ネットワーク（特にインターネット）での犯罪が頻繁におきている気がします。日本としてその対応が悪い。すべてに対応するのは難しいかもしれないが、何かしらの対応が出来るようにしたい（特に相手を特定できるようにしたい）。
73	[特定]	病院・医院	予防の観点から量刑を重くすべき。又、損害賠償発生事例等を広報し、犯罪の抑制を強化。
74	[特定かつ上場]	鉄道・地下鉄	当社では、当面サイバーテロ、不正アクセス等の侵入があったとして、大きな被害にいたるとは現在考えてはおりませんが、昨今の急速なインターネットの普及、発展等を考えると安心もしていられません。今後、警察の方に期待、希望することは、優秀な人材、組織力を活用し、常に最先端の技術をもって緊急体制を整えて頂きたい。又、民間企業担当者を対象とした講習会等、人材育成にも積極的に取り組んで頂きたい。
75	[特定]	病院・医院	セキュリティ対策の技術面に関することについて、懸賞をかけて地球規模で募集してみる。おもしろい成り行きになるかも知れない。真面目に技術、アイディアを提供する種族・挑戦派タイプ等、何か潜在的テロ行為が見つかるかもしれない（組織的なサイバーテロの発見は困難かも知れないが、天才人個人レベルは見えるかも）。
76	[上場]	その他製造	すべての面で迅速にかつ具体的に推進願いたい。また、法制度とからめ現在は、実質ボランティア的に技術者の良心に頼って行われている社内のセキュリティ対策を、そのようなスペシャリストの設置を法的に義務づけるレベルにまで高めてもらいたい。
77	[上場]	不動産	ハイテク犯罪はこれから多くの問題を起こし、被害を発生させると予想される。その対策、発生的に対応を十分にとって頂きたい。犯罪を犯す者以上の技術者を育成していく必要があると思います。
78	[特定]	通信	積極的な情報開示を希望する。
79	[上場]	繊維	国際間連携による早急な対処を期待。
80	[上場]	保険	企業外で発生が予測される不正、不法行為について、ネットワーク社会の情報インフラとして制度上の法整備と伴に、実際の犯行事例、対策情報のスピーディーな公開を期待します。

No.	対象グループ	業種	問18　サイバーテロに対する警察の取り組み（自由記入）
81	[上場]	電気機器	インターネットを活用し、電子メールまたは掲示板により、ユーザーのサイバーテロ被害届出やサイバーテロを含む不正侵入情報等の通知・開示について、警察またはこれに準じた機関による双方向の通知・開示体制の整備を希望する。
82	[特定]	鉄道・地下鉄	危機管理に対し、後手の感がいなめない。先手必勝を期待します。
83	[特定]	鉄道・地下鉄	新聞等で見聞きする限り、対応が後手になっているように思えます。会社、省庁等の対応も非常にのんびりしているように思われる。対策を早急にたてるべきではないでしょうか。
84	[特定]	病院・医院	新たな組織が結成されたと聞き及んでいますが、今後の世情を考えると、更に強化されていくことを期待しています。
85	[特定]	石油卸	国際犯罪が多く考えられるため、関係諸外国との連携を強化し、犯罪の摘発に努力して欲しい。
86	[特定]	鉄道・地下鉄	本調査を実施する意図については理解しており、今後とも協力していきたい。
87	[特定]	放送	サイバーテロという抽象的な言葉ではなく、具体的にどのような危険、障害が発生し日常を侵犯するかをもっと分かりやすくPRしてほしい。
88	[特定]	ガス	サイバーテロに対する警察の一掃の取り組みをお願いすると共に、いい指針ができれば是非御衆知下さるようお願いします。
89	[特定かつ上場]	通信	他の刑事犯罪と同様に、ハッカーに対する取り締まり強化。
90	[上場]	電気機器	サイバーテロと共に匿名性による犯罪への対策も強化を望む。
91	[上場]	輸送用機器	コンピュータウィルス製作や不正アクセスによる破壊行動に対し、国際協力のもとで厳しい対応をお願いしたい。少なくとも日本の中での発生は国際的な信用低下を招くばかりでなく、日本での経済発展に支障となるので、警察の積極的な対応を期待したい。
92	[特定]	航空	最近の警察内で起こる事件が多発すぎて、サイバーテロという難問題以前に基本を正せよと思います。
93	[特定]	鉄道・地下鉄	現在当社では社内LANや外部とのネットワークが確立されていないため、サイバーテロに関しての被害は極めて低いと考えています。しかし今後の導入の際に、サイバーテロに対する犯罪対策、対策基準の提示等を施行管理する機関が必要であり、テロ犯を必ず追求できる警察庁のシステムの創設が必要であると思います。
94	[上場]	輸送用機器	諸外国等の先進国の行政の取り組み情報開示、先取による未然防止への積極的行動に期待する。
95	[特定]	その他サービス	・海外からのテロも考えられ、外国との連携協力が必須。犯罪者を漏れなく早期に摘発し、犯罪を防止してほしい。 ・民間知識、技術の活用が必要だと思われます。
96	[上場]	電気機器	電子商取引の発展を阻害しない。特に個人情報保護との間で摩擦の少ない捜査手段の確立に期待いたします。
97	[特定かつ上場]	銀行	サイバーテロ対策推進計画の中で、平成13年度以降の項目が多いようですが、前倒しで実施できる様、予算を確保されたらどうでしょうか。
98	[特定]	病院・医院	知能犯罪に対して、高度の知識や知恵を有する人材を育成する必要がある。
99	[上場]	建設	コンピュータウィルスへの対応もあわせて行って頂きたく思っています。
100	[上場]	流通・卸売	捜査技術を高める。軽微な交通違反の取り締まりなどやめて、悪質な犯罪の取り締まりに人とコストを集中すべし。
101	[特定]	水道局	技術的にどのような侵入が可能なのか、過去の事例の調査と公開をしてください。
102	[上場]	無回答	サイバーテロに対する専門部署の新設、拡充。情報システム技術者の早急な育成等をお願いしたい。
103	[特定]	放送	当社のセキュリティの管理からするといくつかの問のみ答えられません。アンケートであろうとセキュリティの内容を外にだすことはセキュリティを甘くすることになるから。
104	[特定]	水道局	過去の犯罪履歴や、セキュリティ対策の手法から分かる資料があれば提供いただきたい。
105	[特定]	病院・医院	官庁HPへのハッカーの侵入時、一部のプロバイダがログイン記録の公開を拒否しました。犯罪である以上、警察への協力は必要と考えますが、警察倫理が問われている今プライバシー保護の点からも、その取扱には細心の注意が必要と考えます。
106	[上場]	その他金融機関	広く民間の力を借り、取り組んでいただきたいと思います。
107	[特定かつ上場]	電力	サイバーテロに対する司法的取り組みの重要性が今後ますます大きくなると予想される。