NISC
National center of Incident readiness and Strategy for Cybersecurity

資料4

企業のサイバーセキュリティに関するNISCの調査結果（速報）について

平成28年12月7日

サイバーセキュリティ戦略本部 普及啓発・人材育成専門調査会

内閣サイバーセキュリティセンター（NISC）

Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

今回の調査について

対象：日経225の企業

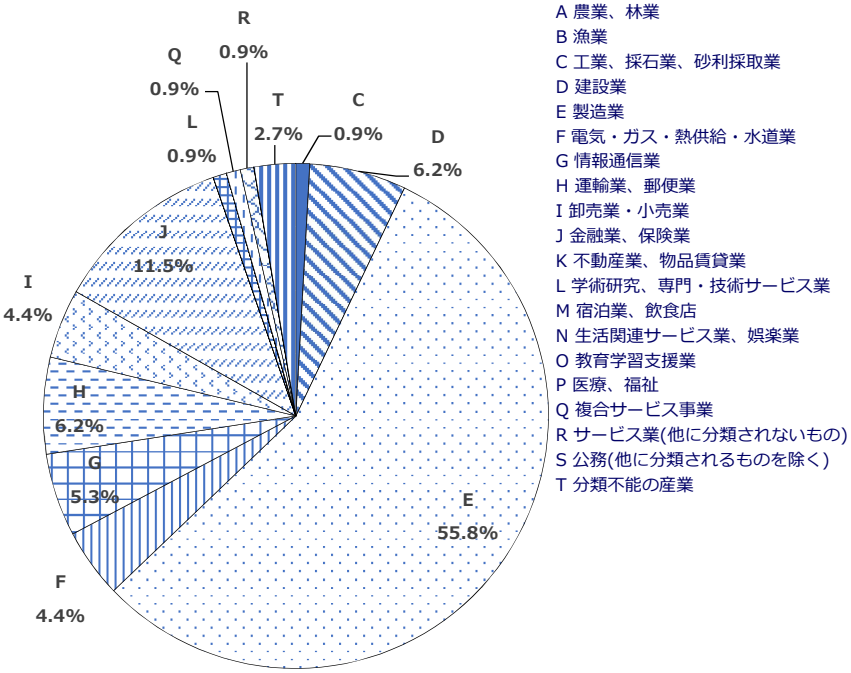
方式：サイバーセキュリティ経営及び人材に関する記名回答方式のアンケート調査票（郵送）による

実施期間：2016年9月30日～10月末日

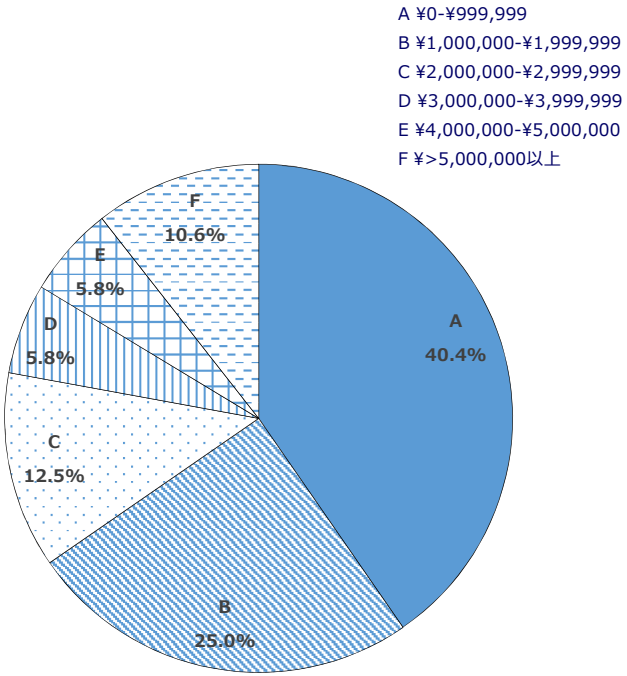
有効回答数：114（回答率 約51%）

回答企業の概要：

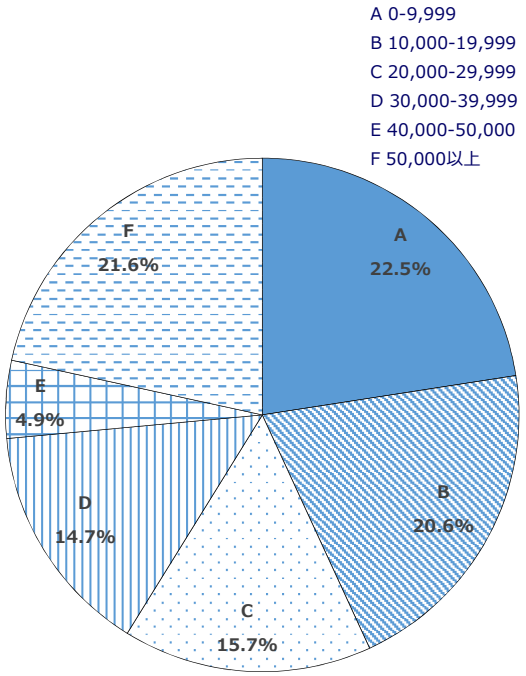
業種



売上高(百万円)



従業員数



Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

調査結果

1．経営層のリーダーシップについて

○経営層のサイバーセキュリティの重要性の認識は高いが、理解を深め、推進することが課題。[p.7/p.10]

○サイバーセキュリティをやむを得ない「費用」ではなく「投資」と捉え、ブランド価値として位置づけている企業は、経営層の関与や情報発信、キャリアパスの構築などに積極的。[p.9/p.11/p.12/p.13]

・事業戦略の中にITの利活用を位置づけ、事業で「攻める」ためにITを利活用としている企業が9割
・7割以上の企業がサイバーセキュリティを経営戦略として位置づけ、問題が生じる前から経営陣が関与して取り組んでいる。ただし、経営層のサイバーセキュリティに対する理解と対策の推進については、6割以上が課題と認識。
・サイバーセキュリティを「投資」と捉え、ブランド価値として位置づけている企業は、全体の2割程度であり、以下の傾向がある。
①経営陣の積極的なサイバーセキュリティへの関与、②積極的な情報発信の認識、③セキュリティ人材のキャリアパスの存在、④情報システム部門の年齢層が若い

2．サイバーセキュリティを推進する経営層・実務者層間の橋渡し人材（旗振り役）について

○橋渡し人材（旗振り役）の配置は進んでいるものの、多くの企業が不足を感じている状況。[p.15/p.17]

・6割の企業が橋渡し人材を配置している。また、7割の企業が橋渡し人材が不足していると回答。
・6割の企業が、橋渡し人材は内部の人材で確保・育成していると回答。

3．企業内の様々な部門のサイバーセキュリティ人材について（組織面）について

○事業でITを利活用して「攻める」ための組織として情報システム部門が期待をされているが、同部門は、事業に対する知識や経験が十分ではない傾向。[p.22/p.23]

○事業部門のサイバーセキュリティ人材が不足している企業は、より多くの人数確保が必要。[p.24]

○ITやサイバーセキュリティのスキルだけが重視されているわけではない。[p.25]

○製造部門やプラント運用部門におけるサイバーセキュリティ人材配置の必要性が高まっている。[p.27]

・事業部門にサイバーセキュリティ人材が配置されている、もしくは今後配置する予定と回答した企業は全体のわずか２５％。
・約8割の企業が、事業で攻めるためのサイバーセキュリティを情報システム部門が担っている。
・情報システム部門が事業で「攻める」際のサイバーセキュリティの課題として、７５％の企業が事業に対する知識や経験が十分ではないと回答。
・事業部門のサイバーセキュリティ人材が不足していると回答している企業は、情報システム部門よりも不足人数が多い傾向にある。
・中途採用時に重視するサイバーセキュリティ人材のスキルとして、基礎力や事業に対する知識といったIT・サイバーセキュリティ以外を選択する企業も一定程度（１５％以上）存在。
・製造部門やプラント運用部門のサイバーセキュリティ人材は、現在いないものの、今後配置する予定と回答した割合が他の人材に比べて高い。

4．その他（情報開示の状況等）

○有価証券報告書における情報開示については、年々増加傾向にあるものの、分野によって状況が大きく異なり、特に、金融、運輸・公共といった重要インフラ事業者の開示率は高い。[p.31/p.32]

Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

（参考資料）

Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

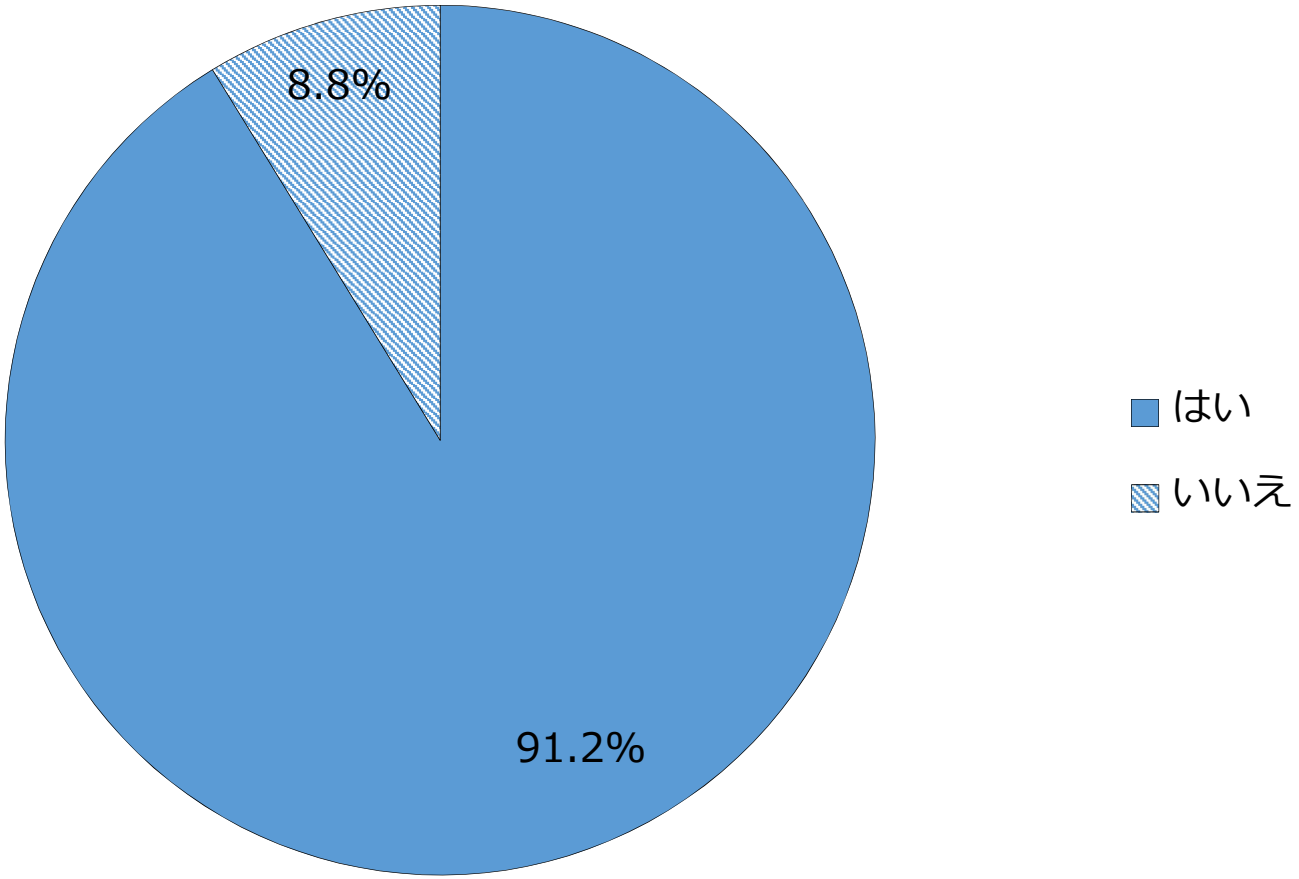
１．経営層のリーダーシップについて

Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

事業で「攻める」ためのにITを利活用している企業

事業戦略の中にITの利活用を位置づけ、事業で「攻める」ためにITを利活用としている企業が９割

n=114



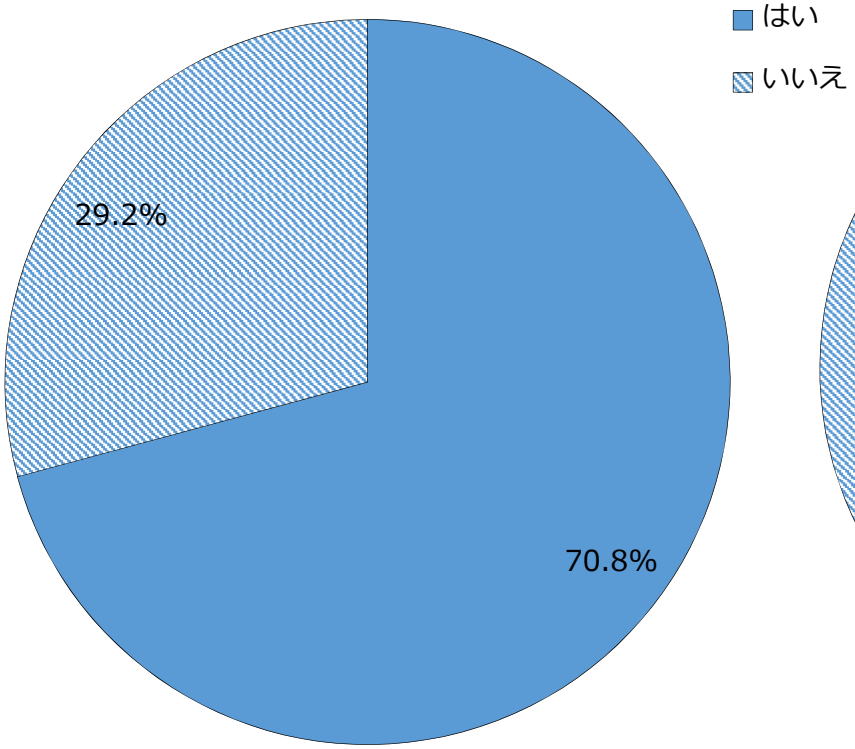
質問：事業戦略の中にITの利活用を位置づけ、事業で「攻める」ためにITを利活用しようとしているか？

Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

サイバーセキュリティへの経営層の関与

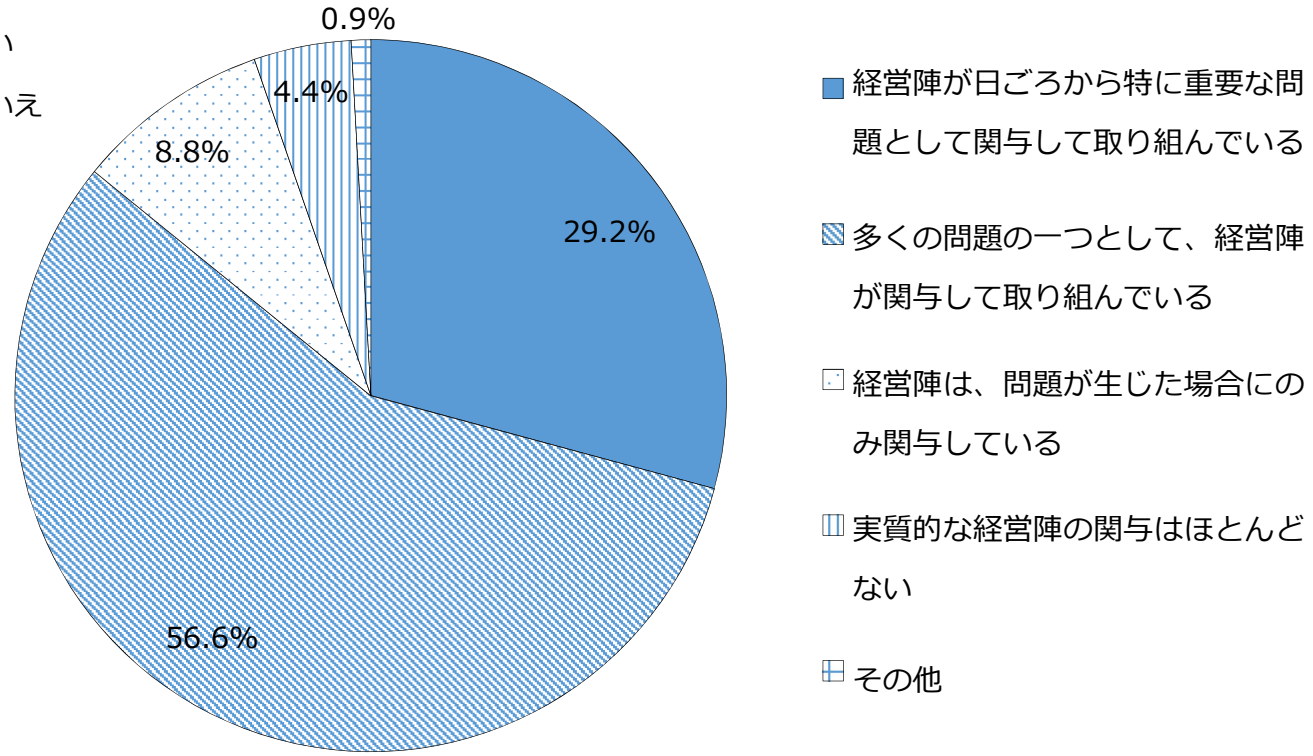
多くの企業（７割以上）が、サイバーセキュリティを経営戦略として位置づけ、問題が生じる前から経営陣が関与して取り組んでいる

n=114



質問：サイバーセキュリティが経営戦略として位置づけられているか

n=113



質問：サイバーセキュリティに対する経営陣の関与について

Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

企業がサイバーセキュリティに取り組む姿勢

多くの企業は、リスク管理や社会的責任の観点からセキュリティに取り組んでいる。一方、自社の未来への投資と考え、ブランド価値として取り組んでいる企業は3割以下にとどまっている。

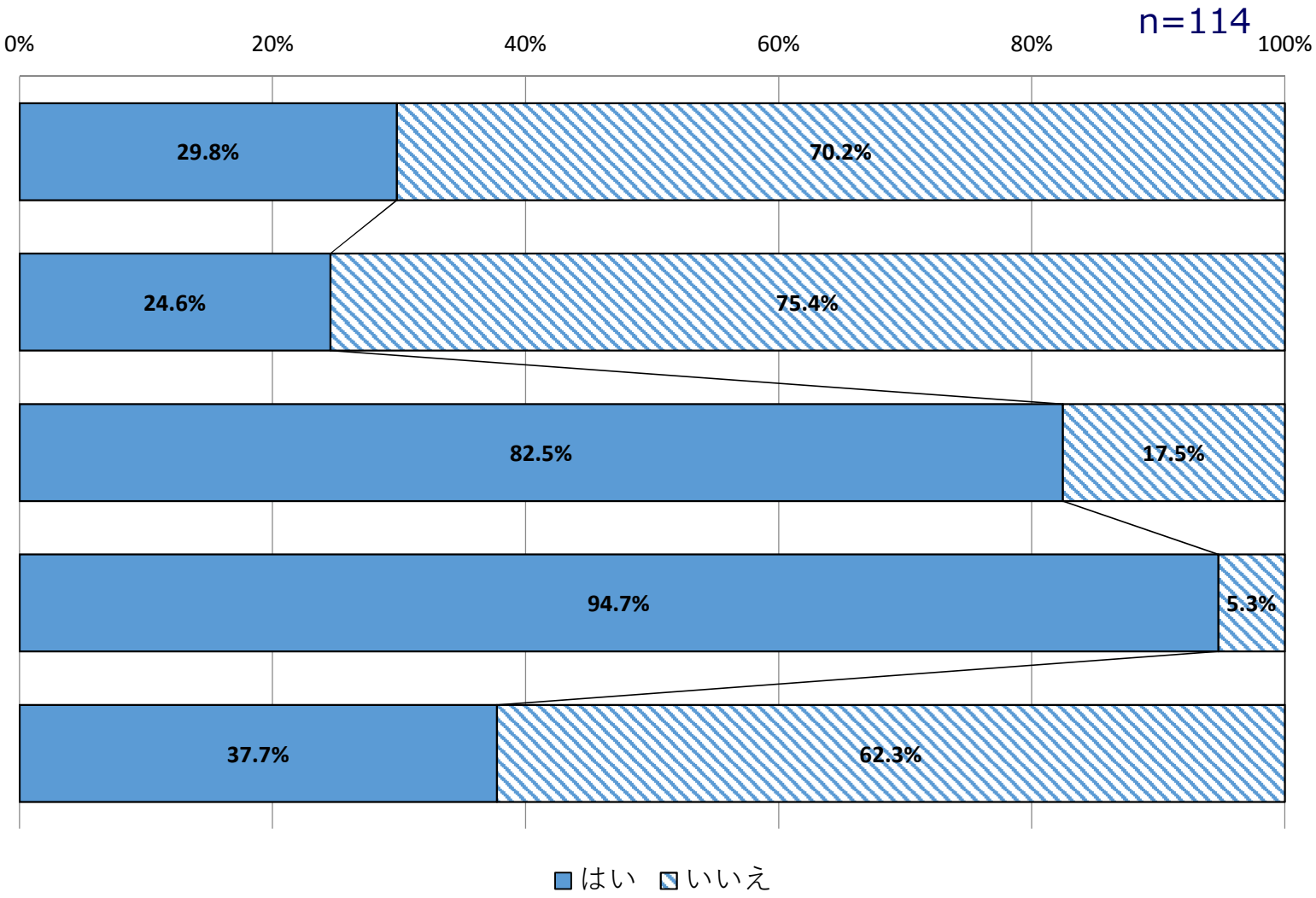
サイバーセキュリティをやむを得ない「費用」としてではなく、将来に向けた積極的な「投資」ととらえている。

サイバーセキュリティに対する積極的な取組やサイバーセキュリティ品質の高さを自社のブランド価値として位置づけている。

自社のリスク管理の一環としてサイバーセキュリティに取り組んでいる。

企業の社会的責任を果たす観点からサイバーセキュリティに取り組んでいる。

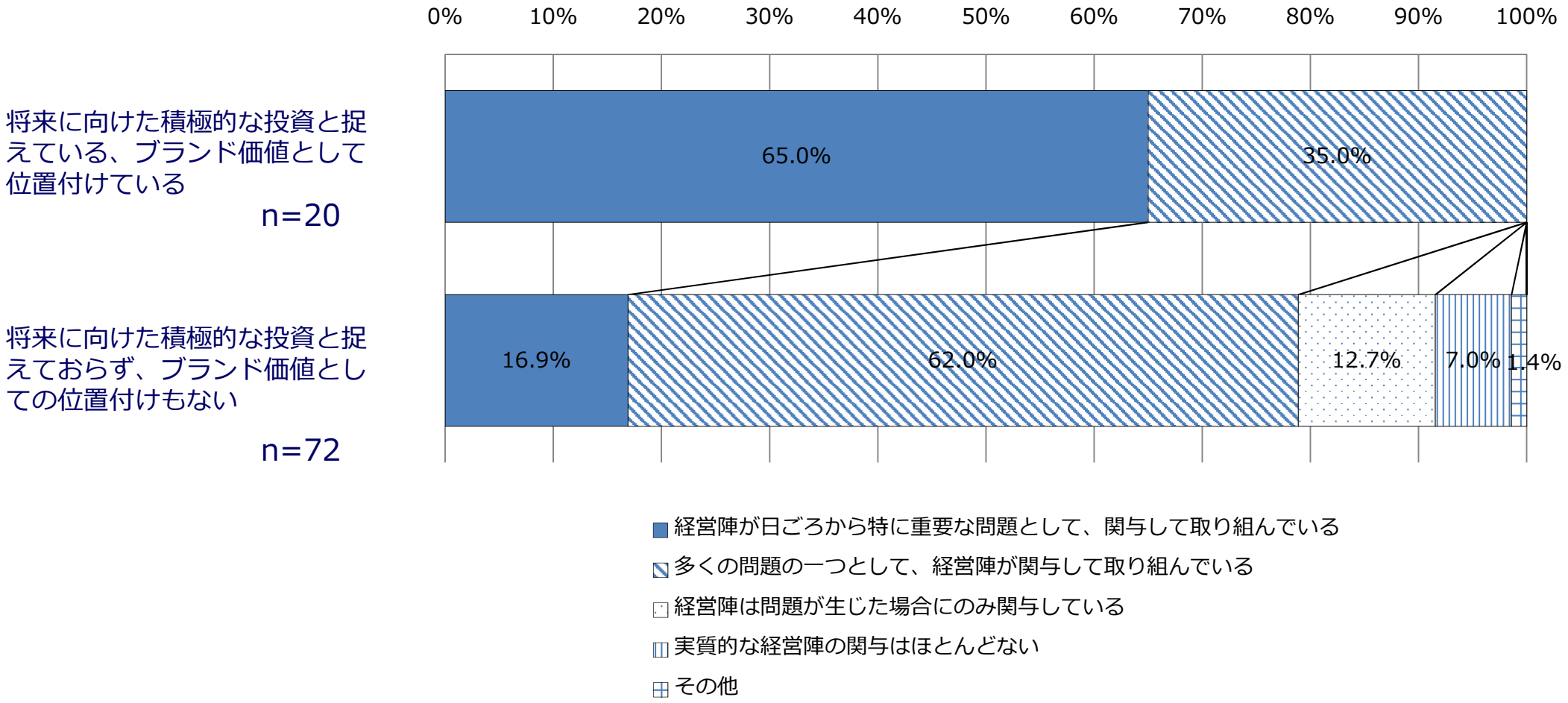
取引先との関係で、サイバーセキュリティ対策が求められている。



Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

サイバーセキュリティを投資と捉えブランド価値として位置づけている企業とそれ以外の企業との経営陣の関与の関係

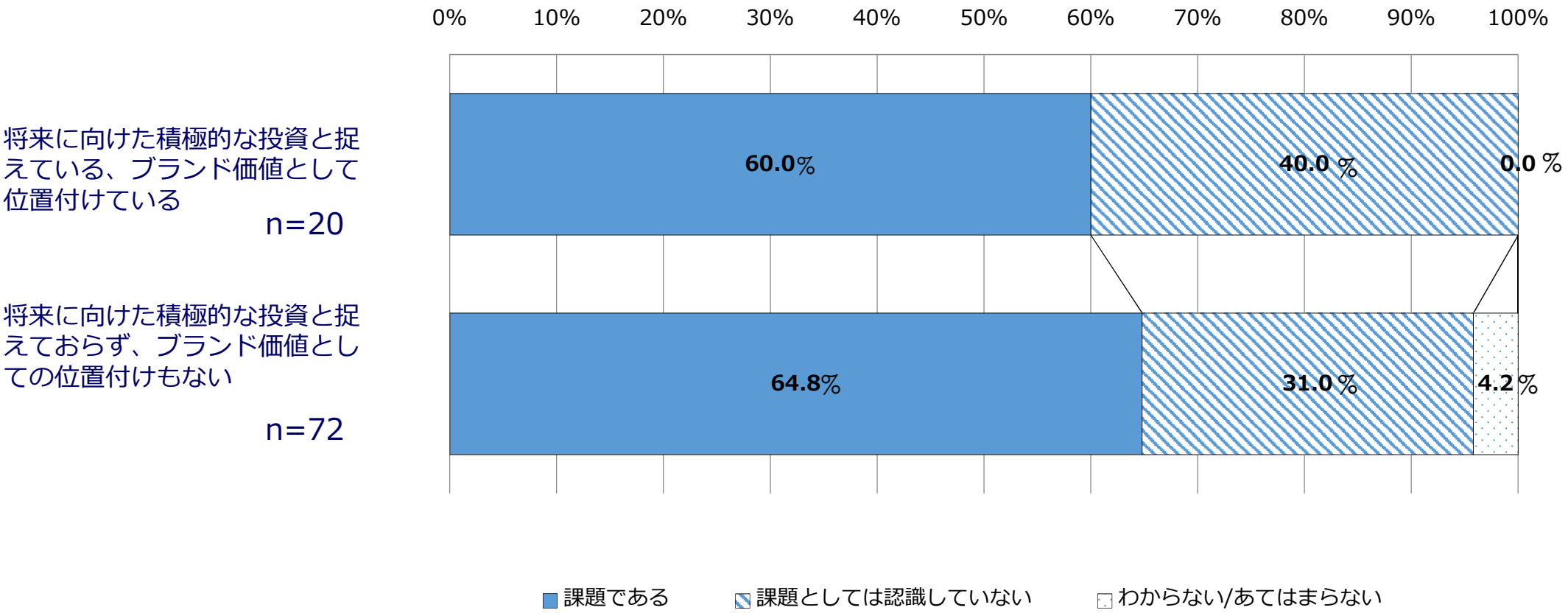
サイバーセキュリティを将来に向けた積極的な投資ととらえ、ブランド価値として位置づけている企業は、経営層がサイバーセキュリティを特に重要な問題として日ごろから関与している。



Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

サイバーセキュリティを投資と捉えブランド価値として位置づけている企業とそれ以外の企業の、経営層の理解と対策の推進に対する課題認識

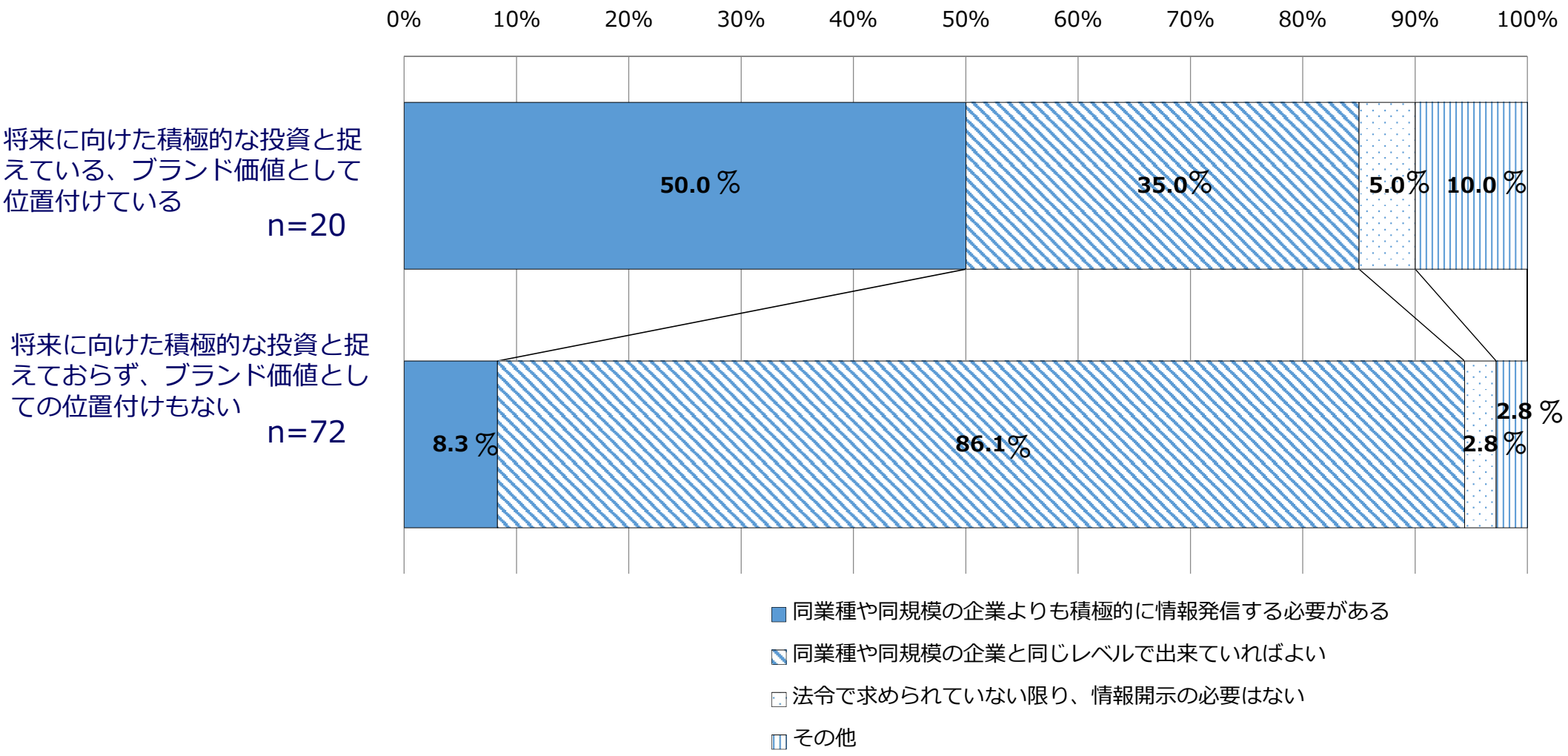
経営層のサイバーセキュリティに対する理解と対策の推進は、サイバーセキュリティを投資・ブランド価値と位置付けている企業でも、そうでない企業でも共通の課題



Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

サイバーセキュリティを投資と捉えブランド価値として位置づけている企業と情報発信の関係

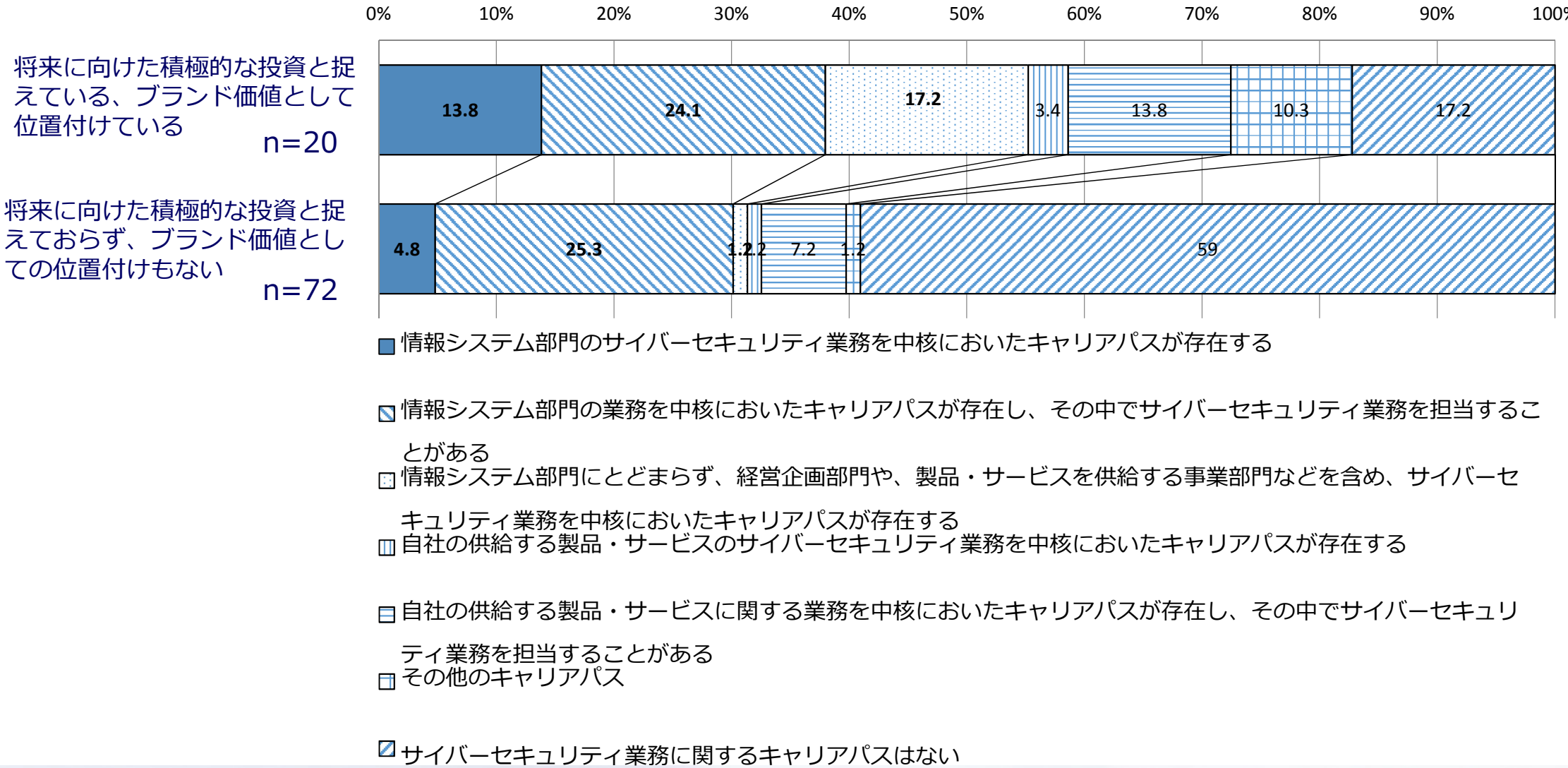
サイバーセキュリティの情報発信の必要性の認識は全体的に高いが、サイバーセキュリティを投資・ブランド価値として位置付けている企業の方が、より積極的な情報発信の必要性を認識している。



Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

サイバーセキュリティを投資と捉えブランド価値として位置づけている企業とキャリアパスとの関係

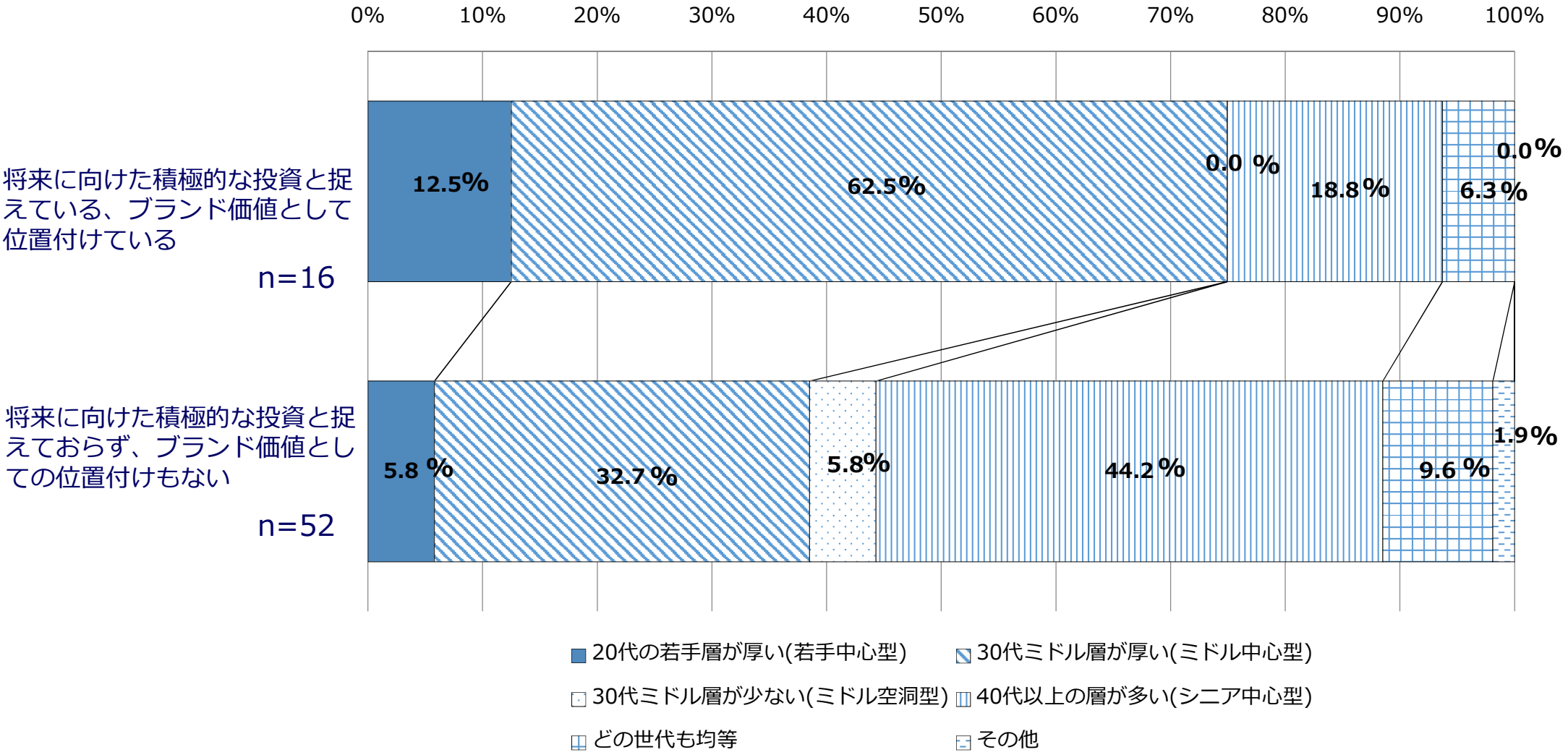
サイバーセキュリティを投資・ブランド価値として位置付けている組織は、サイバーセキュリティ業務に関するキャリアパスが無い割合が低く、何らかのキャリアパスが存在する割合が高い。



Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

サイバーセキュリティを投資と捉えブランド価値として位置づけている企業と情報システム部門（実務者）の年齢層の関係

サイバーセキュリティを投資・ブランド価値として位置づけている企業は、情報システム部門の年齢層がそうでない企業よりも若い（３０代ミドル層が厚い）。



Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

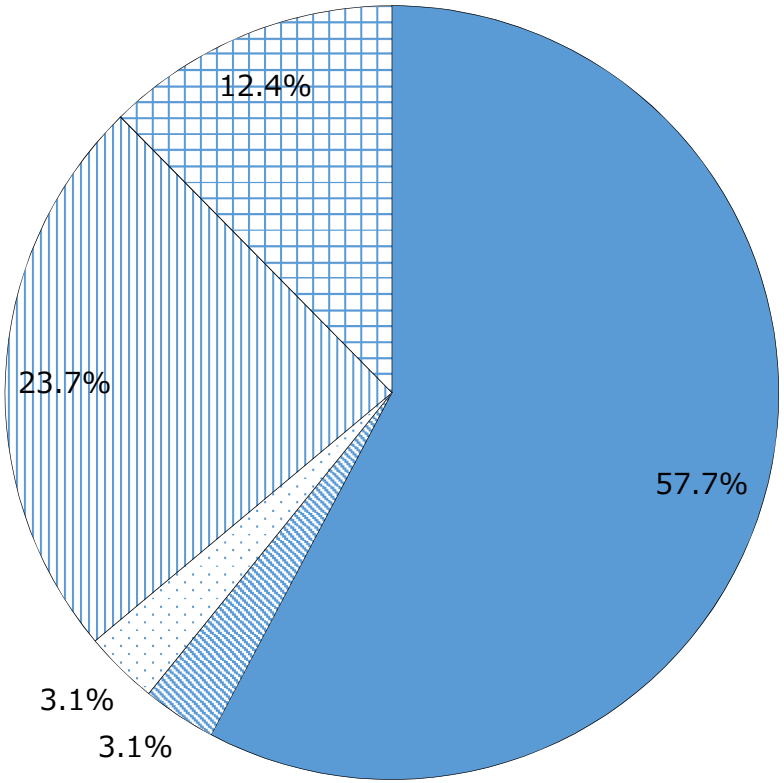
２．サイバーセキュリティを推進する経営層・実務者層間の橋渡し人材（旗振り役）について

Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

橋渡し人材の配置

6割の企業が、橋渡し人材を配置している。

n=97



- サイバーセキュリティの担当者がいる
- サイバーセキュリティの担当者はいない。ただし、今後配置する予定
- サイバーセキュリティの担当者はいない。外部委託のため、今後も配置する予定はない
- サイバーセキュリティの担当者はいない。需要がないため、今後も配置する予定はない
- わからない

質問：経営・企画・セキュリティ総括部門のサイバーセキュリティ人材（橋渡し人材）の配置状況は？

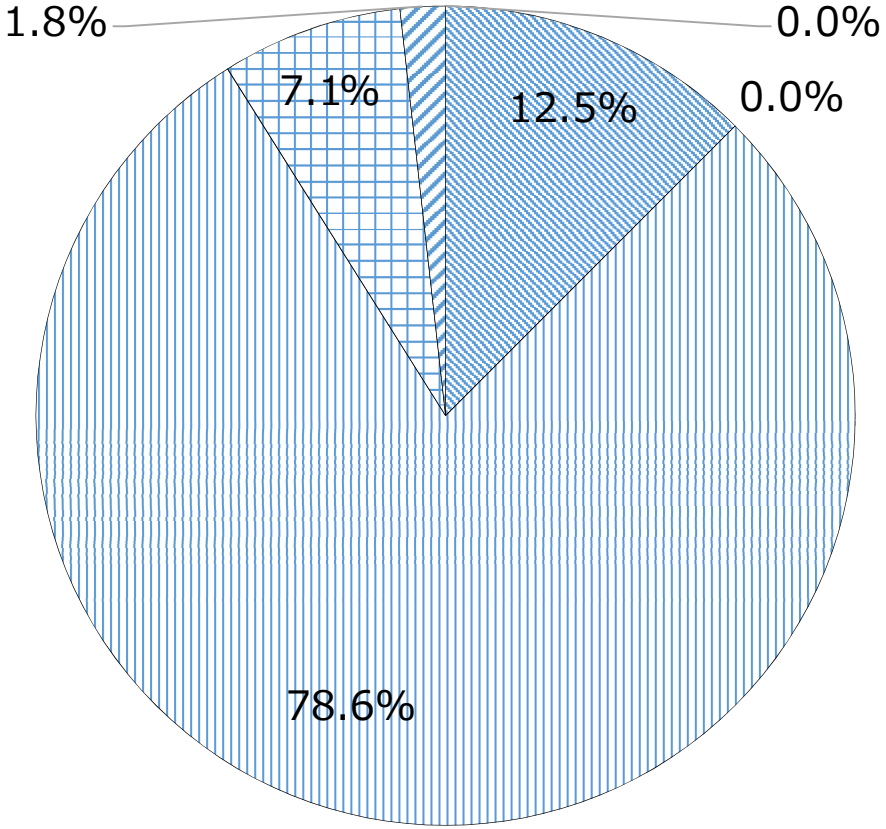
※橋渡し人材＝経営層の示す経営方針に基づくサイバーセキュリティ対策を実践し、実務課題を踏まえた経営戦略を提示し、さらには組織内の関係部局間の総合調整や実務者層をまとめリードできる人材

Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

橋渡し人材の配置

橋渡し人材は、４０代以上の層が多い

n=56



- 20代の若手層が厚い（若手中心型）
- 30代ミドル層が厚い（ミドル中心型）
- 30代ミドル層が少ない（ミドル空洞型）
- 40代以上の層が多い（シニア中心型）
- どの世代も均等
- その他

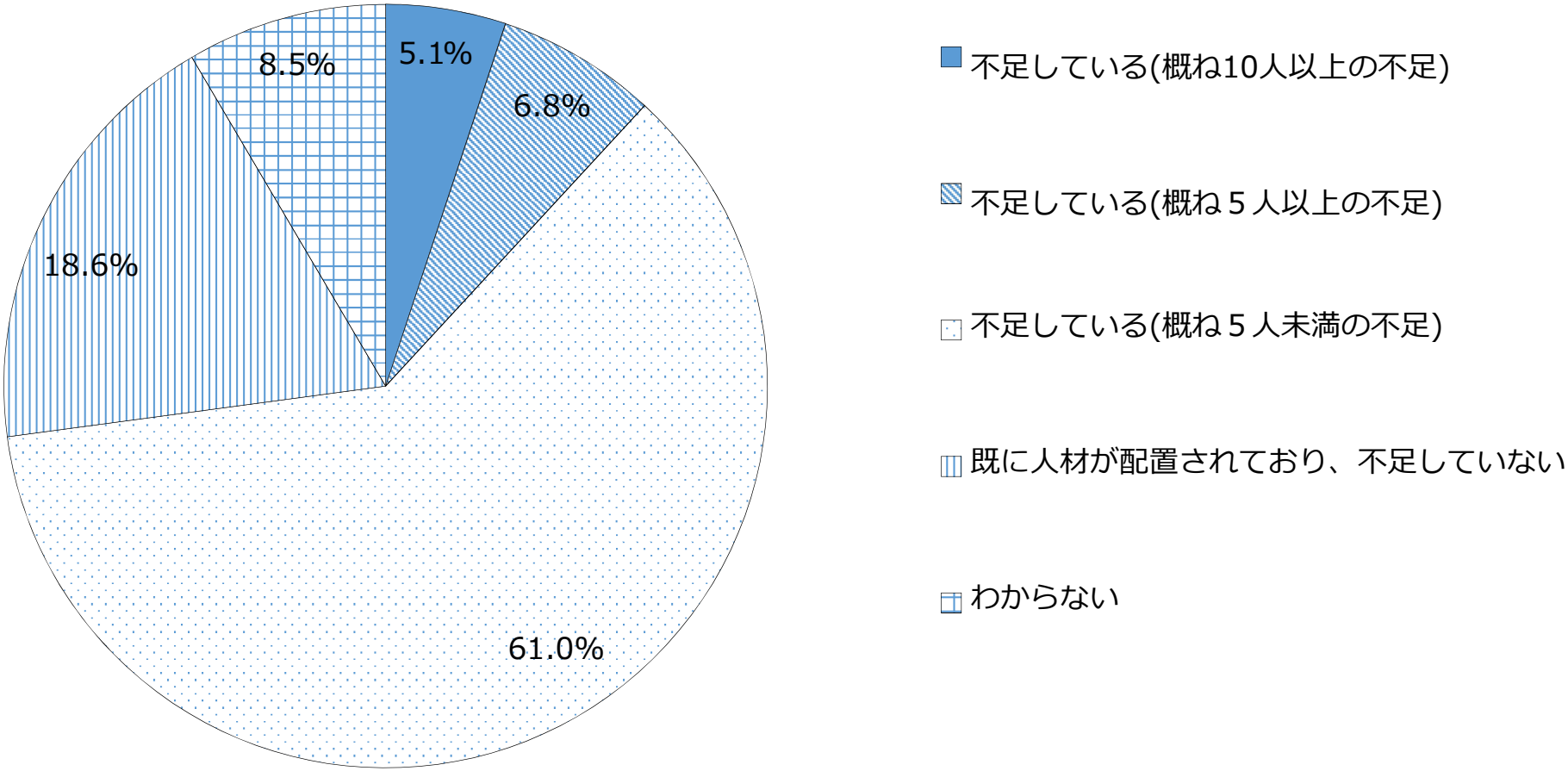
質問：経営・企画・セキュリティ総括部門のサイバーセキュリティ人材（橋渡し人材）の年齢層は？

Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

橋渡し人材の不足

橋渡し人材は、５人未満の不足と回答した企業が６割。

n=59

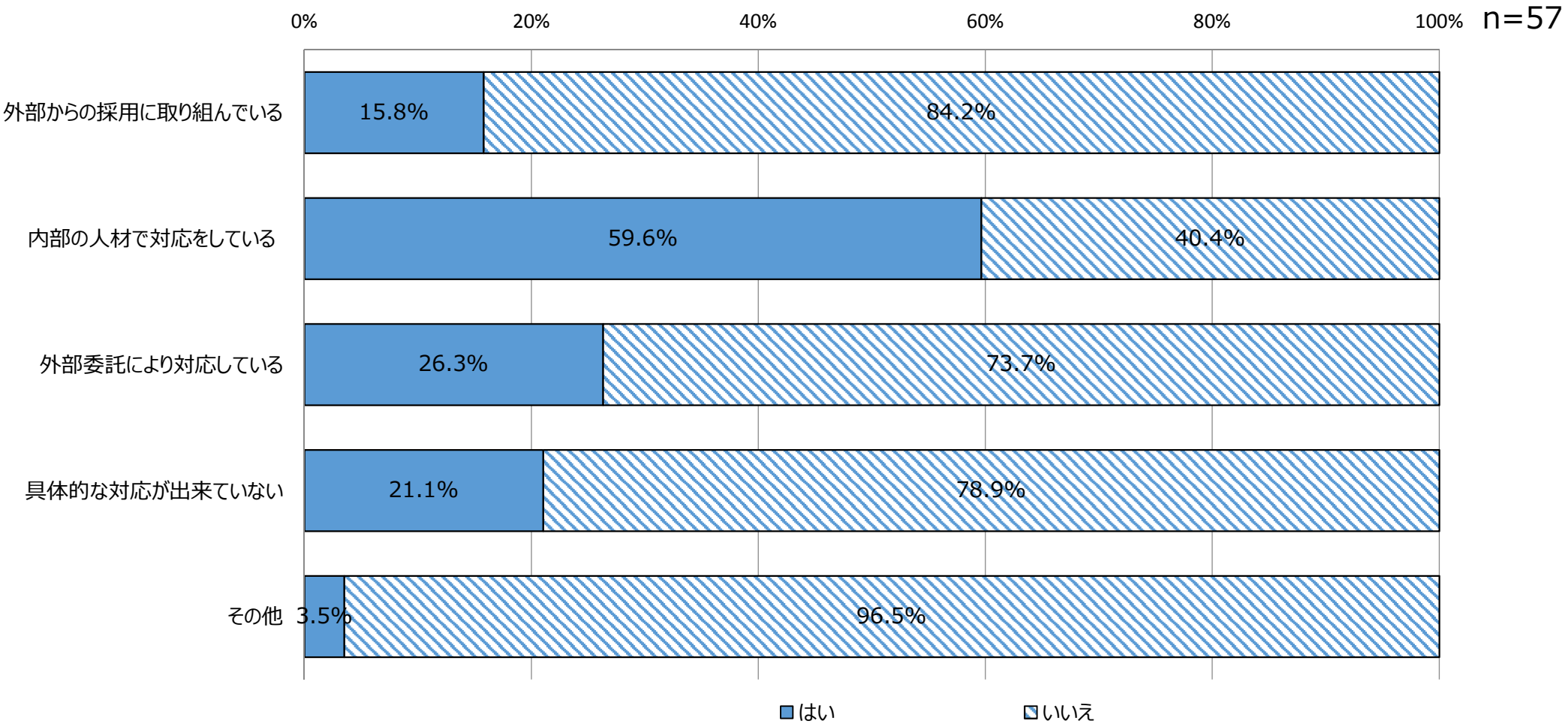


質問：経営・企画・セキュリティ総括部門のサイバーセキュリティ人材（橋渡し人材）の不足状況は？

Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

橋渡し人材の不足への対応

6割の企業は、橋渡し人材の不足への対応として、内部の人材を活用している。



質問：経営・企画・セキュリティ総括部門のサイバーセキュリティ人材（橋渡し人材）不足への対応状況は？

Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

サイバーセキュリティを投資・ブランド価値と位置付けている企業の組織

サイバーセキュリティを「費用」ではなく「投資」ととらえ、品質の高さをブランド価値として位置づけている企業の方が、企業全体のサイバーセキュリティを横断的に見ることができる組織（「旗振り」を行うと思われる組織）を設ける傾向にある。

	サイバーセキュリティを「費用」ではなく「投資」ととらえ、品質の高さをブランド価値として位置づけている企業（n=20）	（参考）企業全体（n=114）
様々な部門のサイバーセキュリティ全体を総括する部門がある	40%	23%
経営企画部門にサイバーセキュリティを担当する組織がある	25%	12%

Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

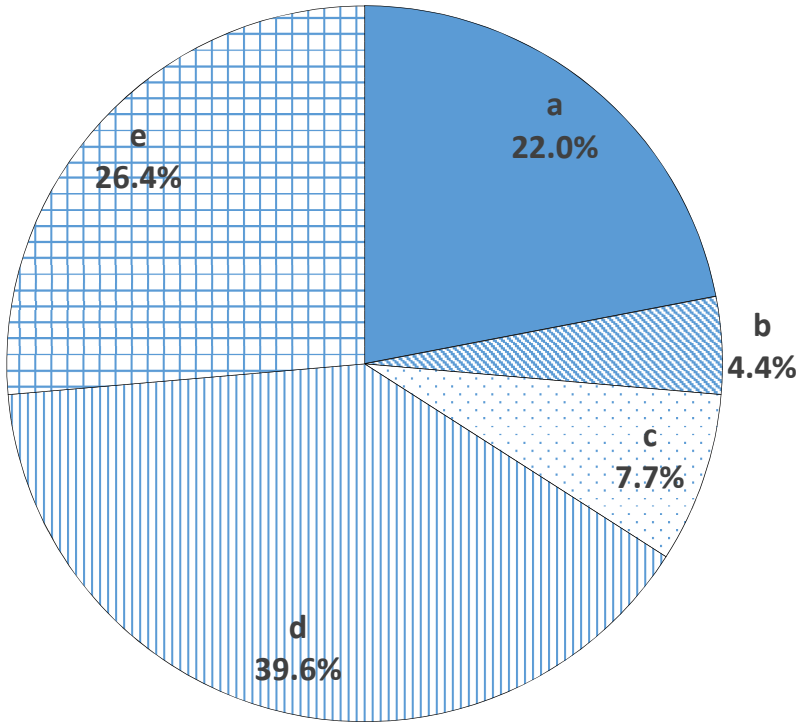
３．企業内の様々な部門のサイバーセキュリティ人材について（組織面について）

Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

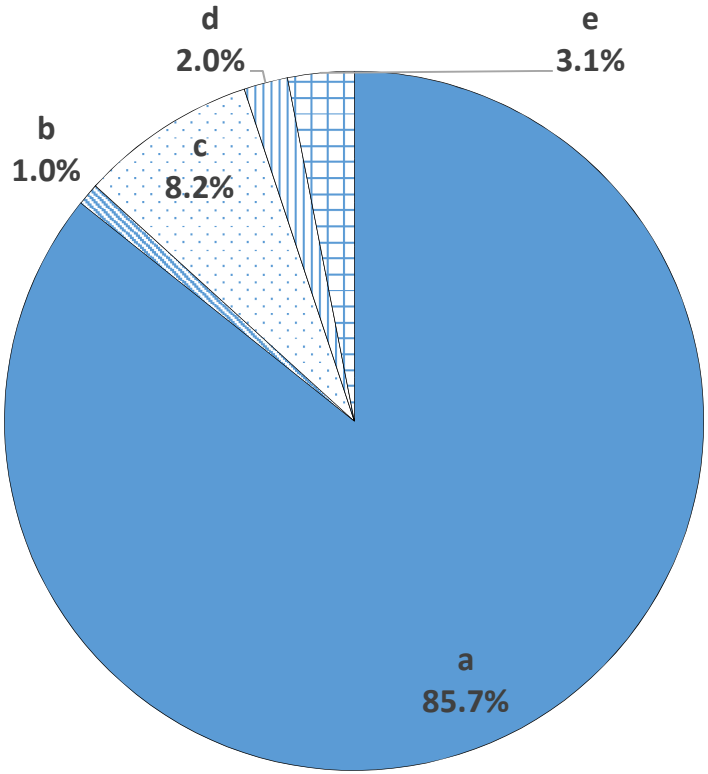
事業部門におけるサイバーセキュリティ人材

事業部門においてサイバーセキュリティの担当者がいる、ないしは、今後配置する予定と回答した企業は、全体の２５％に留まっている。

n=91



事業部門



情報システム部門（実務者）

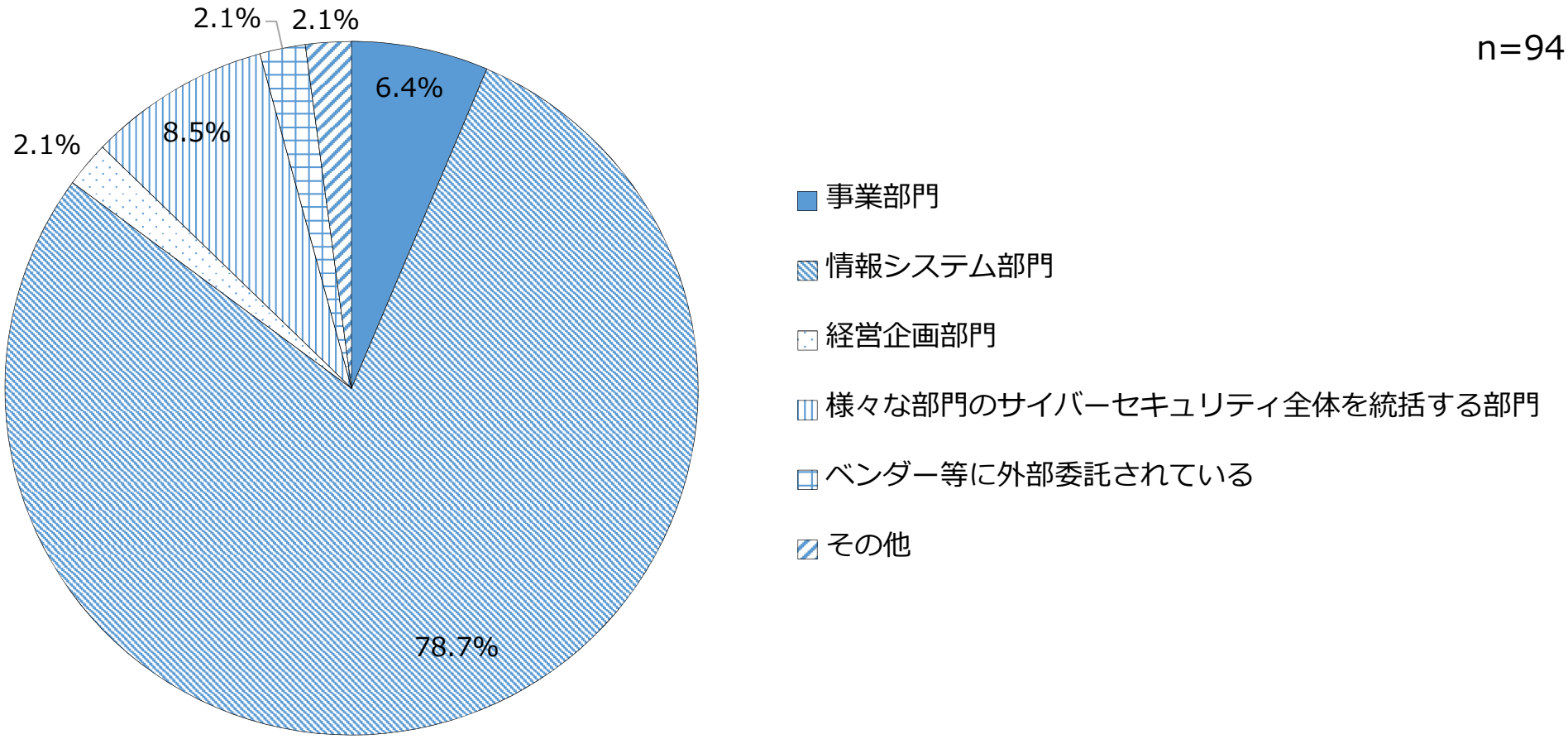
a. サイバーセキュリティの担当者がいる
b. サイバーセキュリティの担当者はいない。ただし今後配置する予定
c. サイバーセキュリティの担当者はいない。外部委託のため、今後配置する予定はない
d. サイバーセキュリティの担当者はいない。需要がないため、今後配置する予定はない
e. わからない

質問：事業部門におけるサイバーセキュリティ人材の配置状況は？

Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

事業で攻めるためのサイバーセキュリティを担う組織

約８割の企業が、事業で攻めるためのサイバーセキュリティを情報システム部門が担っている

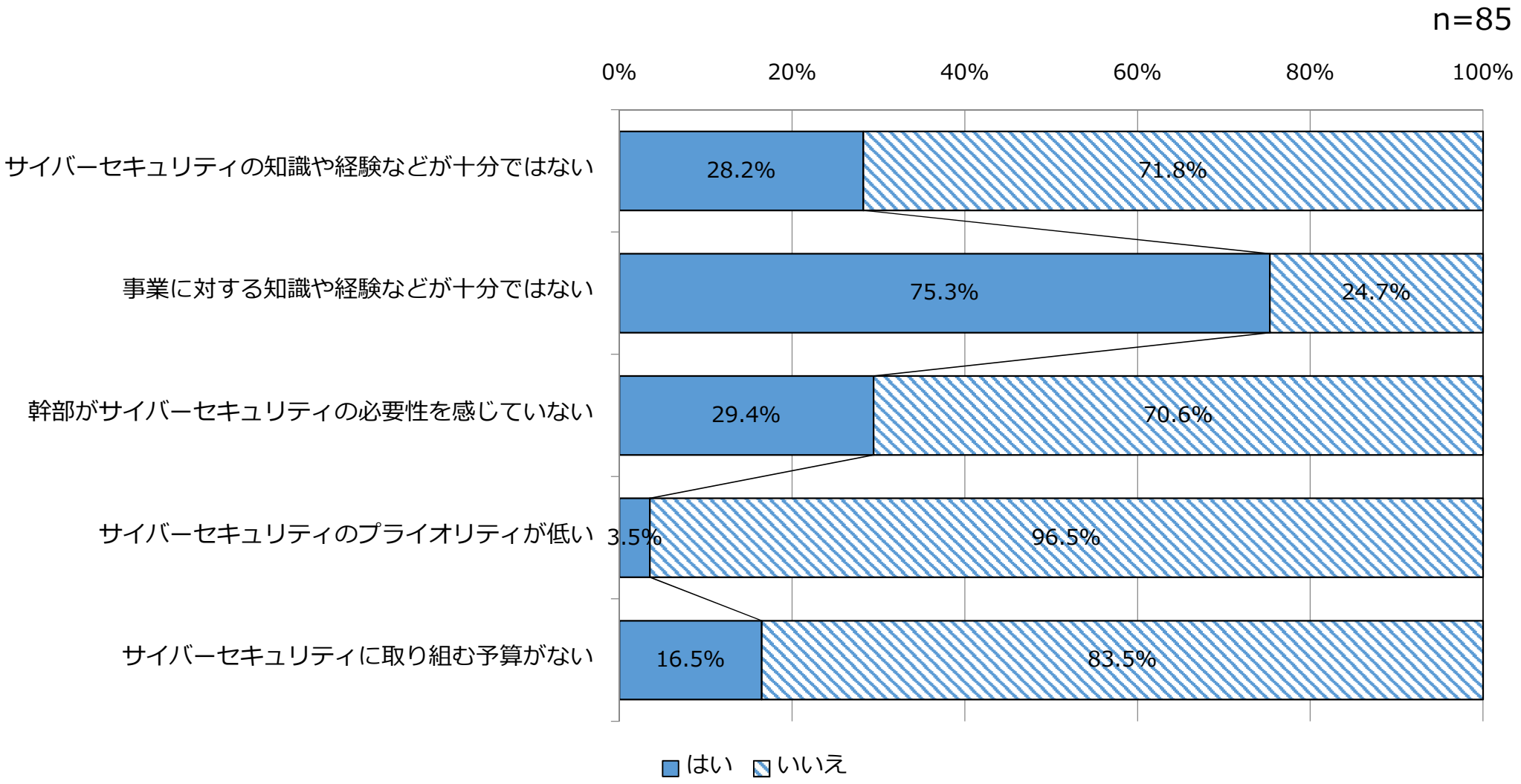


質問：事業でITを利活用して「攻める」際のサイバーセキュリティを担当する主な部門は？

Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

情報システム部門が事業でITを利活用して「攻める」際に抱えている課題

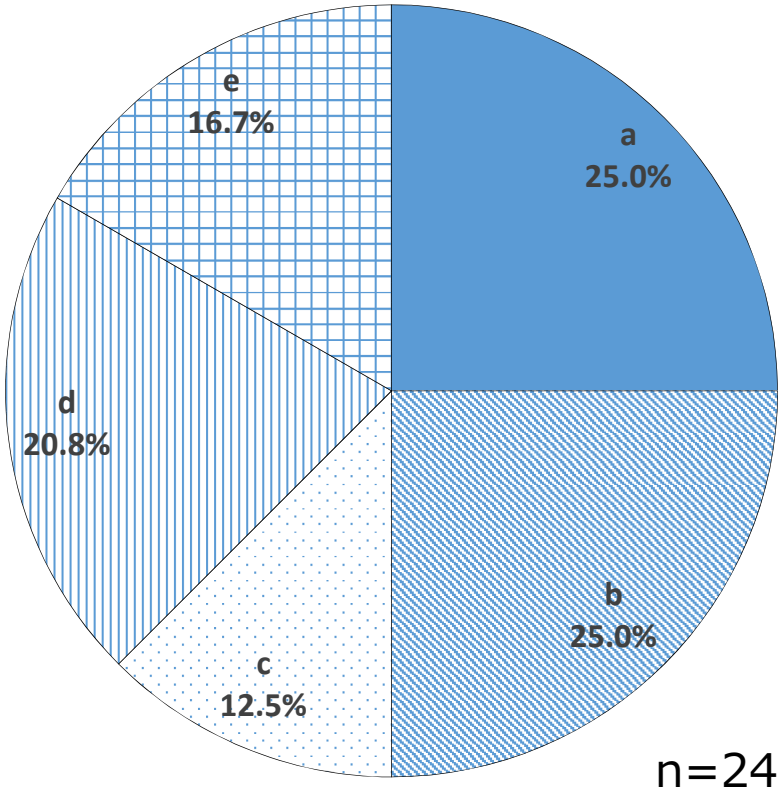
情報システム部門が事業で攻める際のサイバーセキュリティで抱えている課題として、７５%の企業が事業に対する知識や経験が十分ではないと回答。



Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

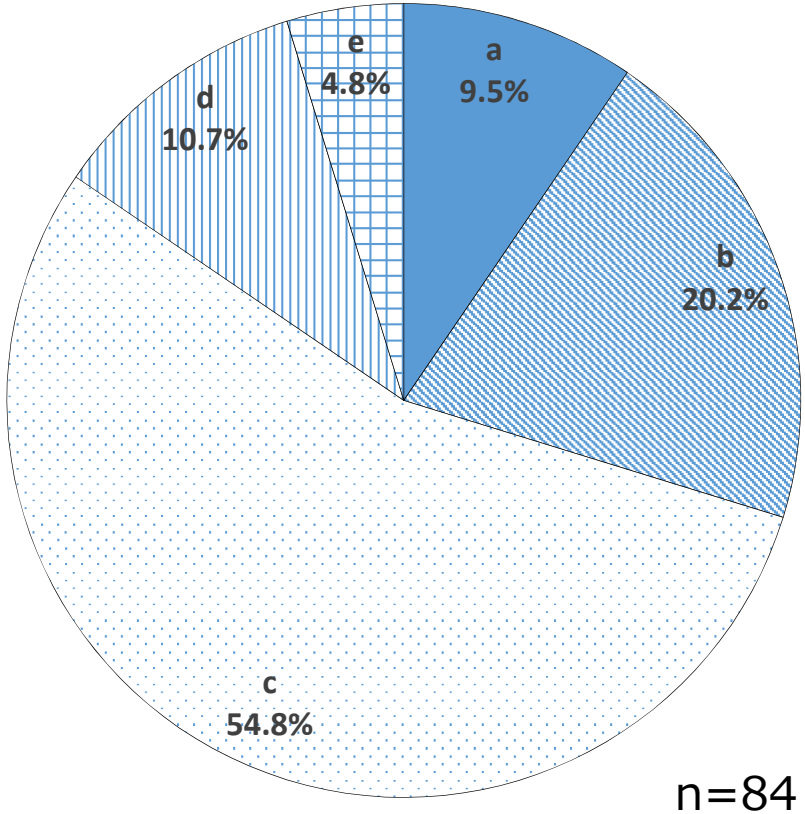
事業部門の人材の不足（情報システム部門との比較）

事業部門のサイバーセキュリティ人材が不足していると回答している企業は、情報システム部門よりも不足人数が多い傾向にある。



n=24

事業部門



n=84

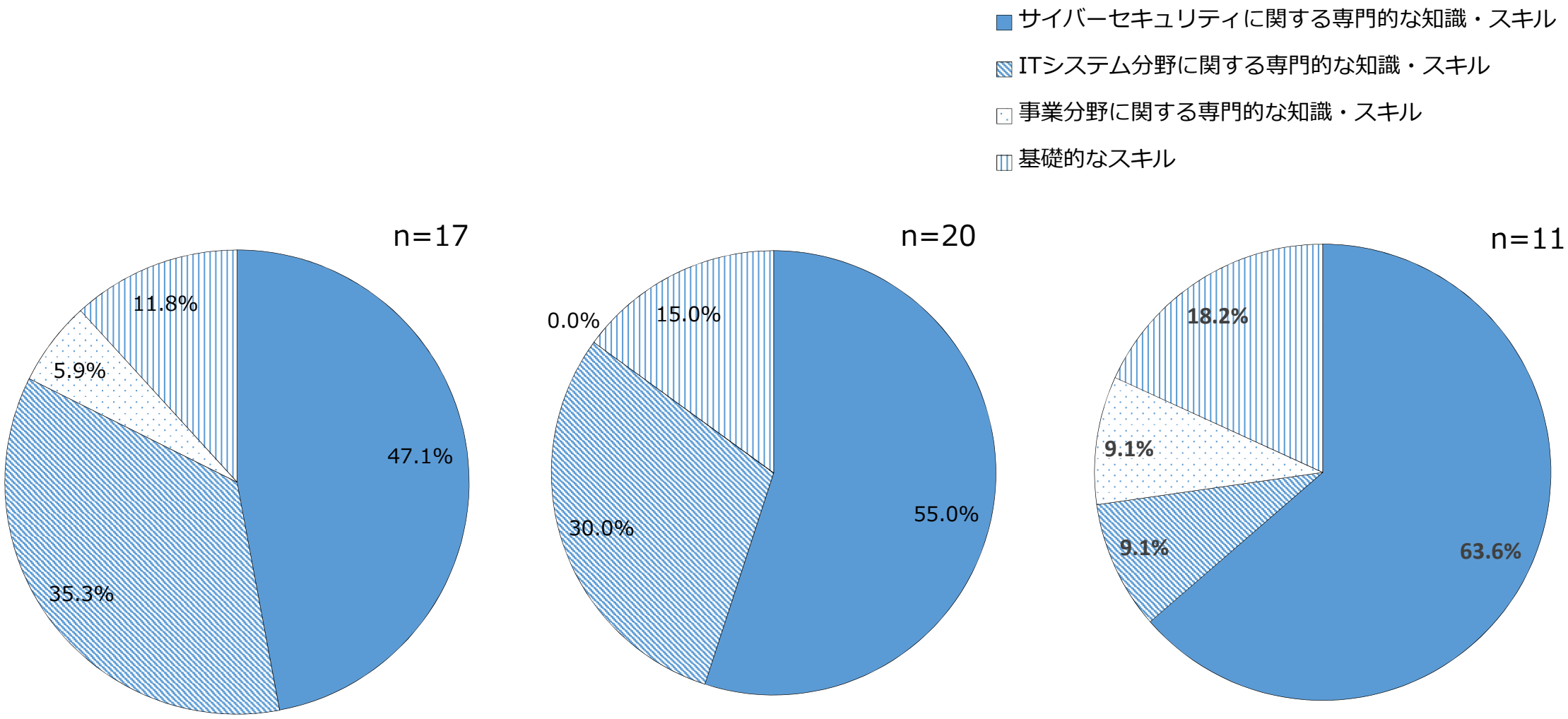
情報システム部門

a.不足している（概ね１０人以上の不足）
b.不足している（概ね５人以上の不足）
c.不足している（概ね５人未満の不足）
d.既に人材が配置されており、不足していない
e.わからない

Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

中途採用時に最も重視したスキル

中途採用時に重視するスキルとして、基礎力や事業に対する知識といったIT・サイバーセキュリティ以外を選択する企業も一定程度（１５％以上）存在。



情報システム部門（マネージャークラス）

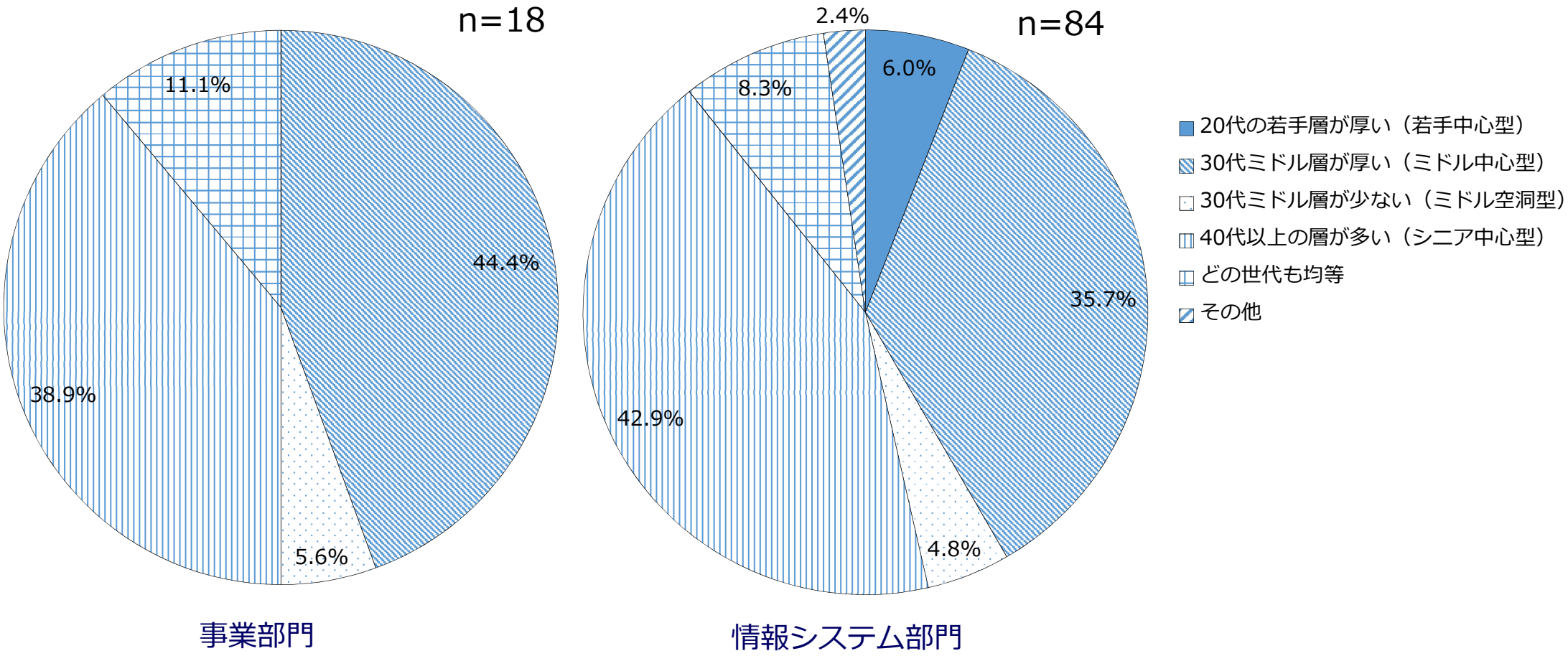
情報システム部門（実務者）

経営・企画・セキュリティ総括部門

Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

事業部門と情報システム部門のサイバーセキュリティ人材の年齢

事業部門のサイバーセキュリティ人材は、３０代ミドル層が厚い企業が多いが、情報システム部門のサイバーセキュリティ人材は、40代以上の層が多い企業が多い。

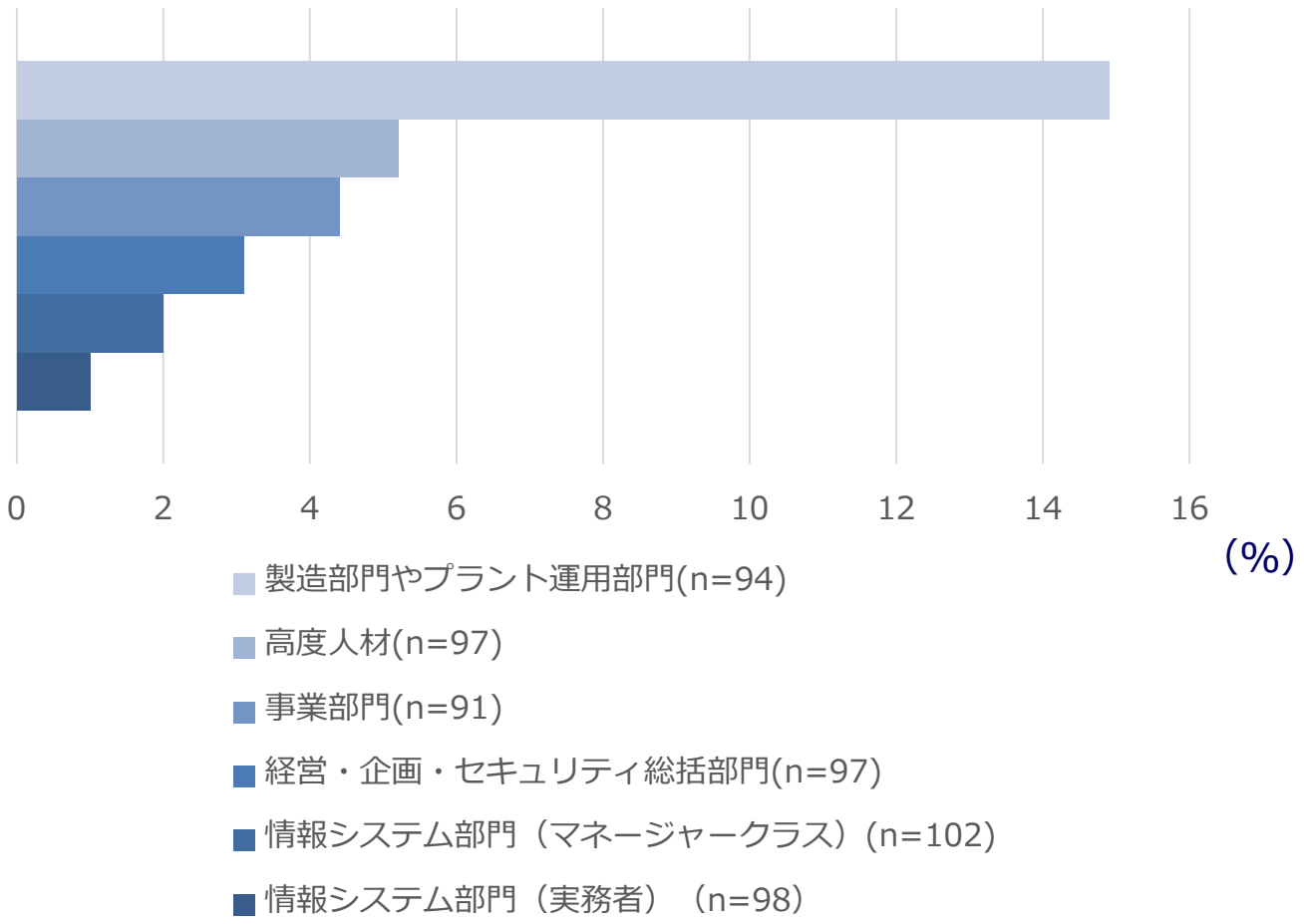


Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

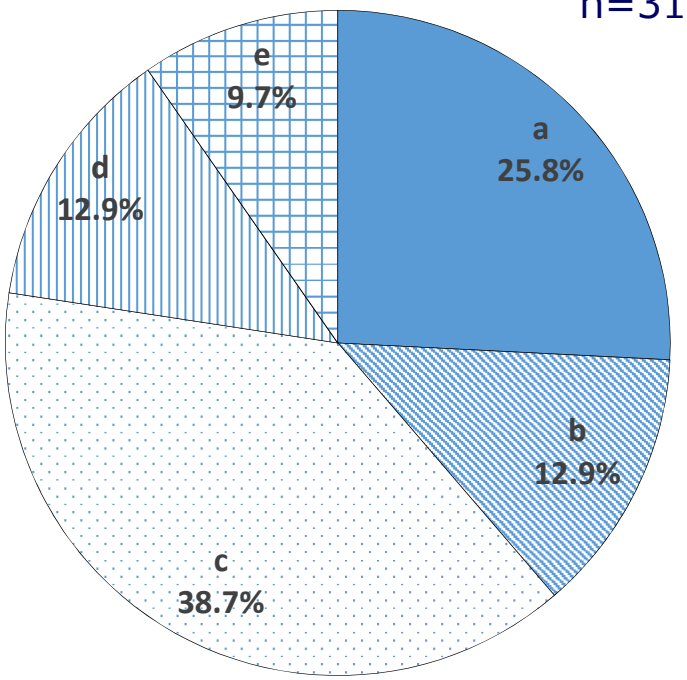
製造部門やプラント運用部門（制御システムを運用・管理する部門の人材）

製造部門やプラント運用部門のサイバーセキュリティ人材は、現在いないものの、今後配置する予定と回答した割合が他の人材に比べて高く、概ね１０人以上の不足と回答した企業は約２６％。

サイバーセキュリティの担当者はいないが、今後配置する予定と回答した割合



n=31



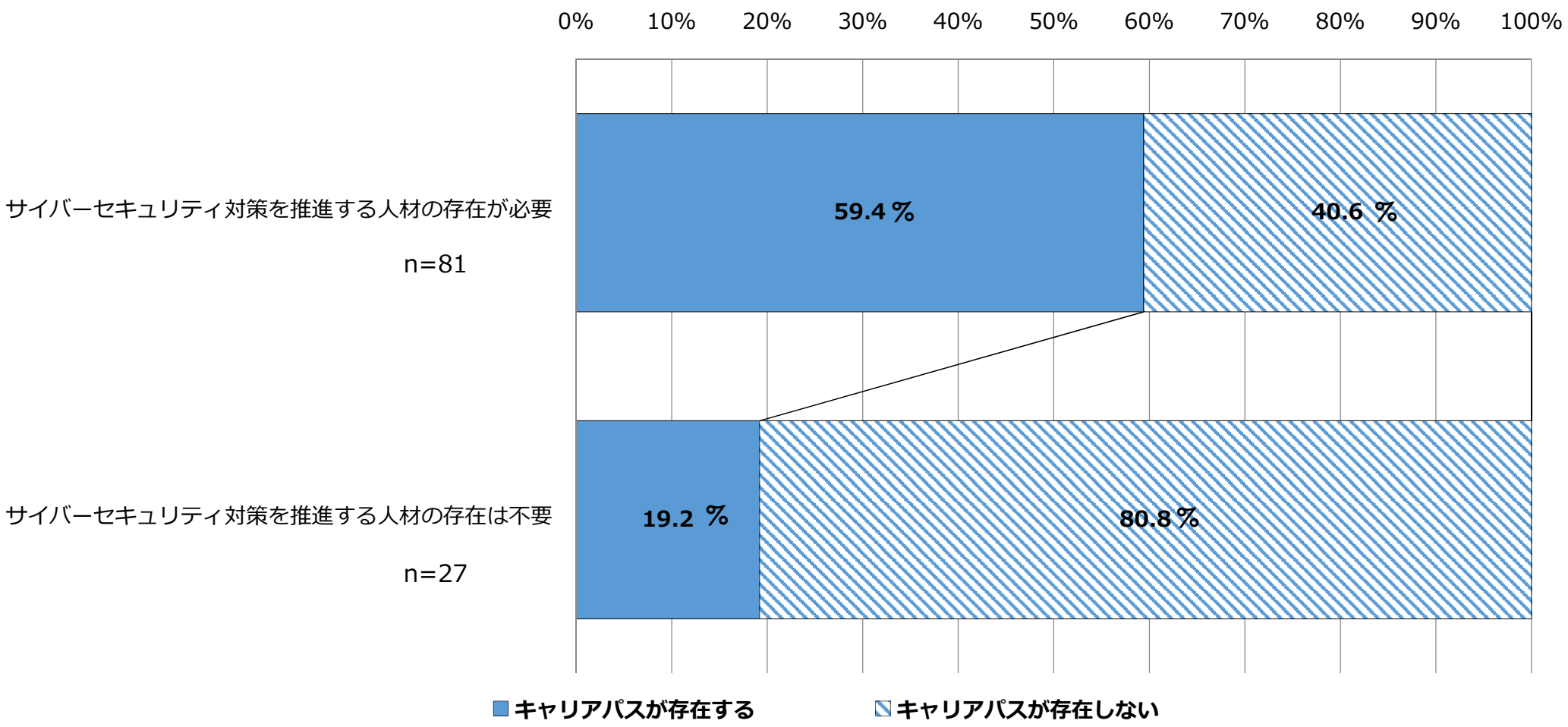
製造部門やプラント運用部門

a.不足している（概ね１０人以上の不足）
b.不足している（概ね５人以上の不足）
c.不足している（概ね５人未満の不足）
d.既に人材が配置されており、不足していない
e.わからない

Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

人材の必要性の有無とキャリアパスの存在

積極的にサイバーセキュリティに取り組む上で必要と思われることとして、「サイバーセキュリティ対策を推進する人材の存在」であると回答した企業は、約6割の企業でキャリアパスが存在する。



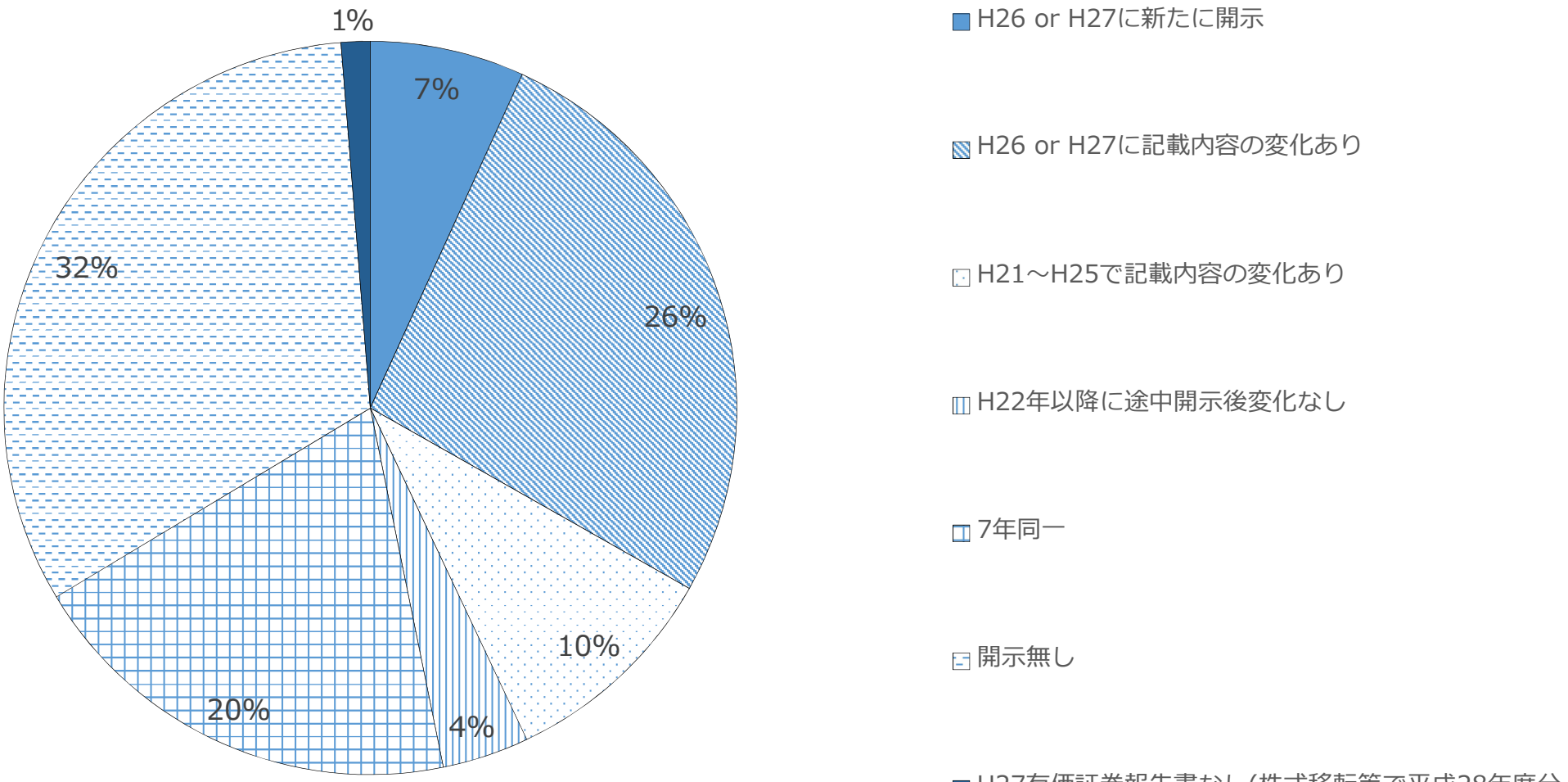
Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

４．その他（情報発信の状況等）

Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

サイバーセキュリティをリスクと認識している状況(全体)

有価証券報告書において、情報開示なしの組織が32%を占めており、次いで平成26年度、27年度に記載内容を更新した企業も26%存在する

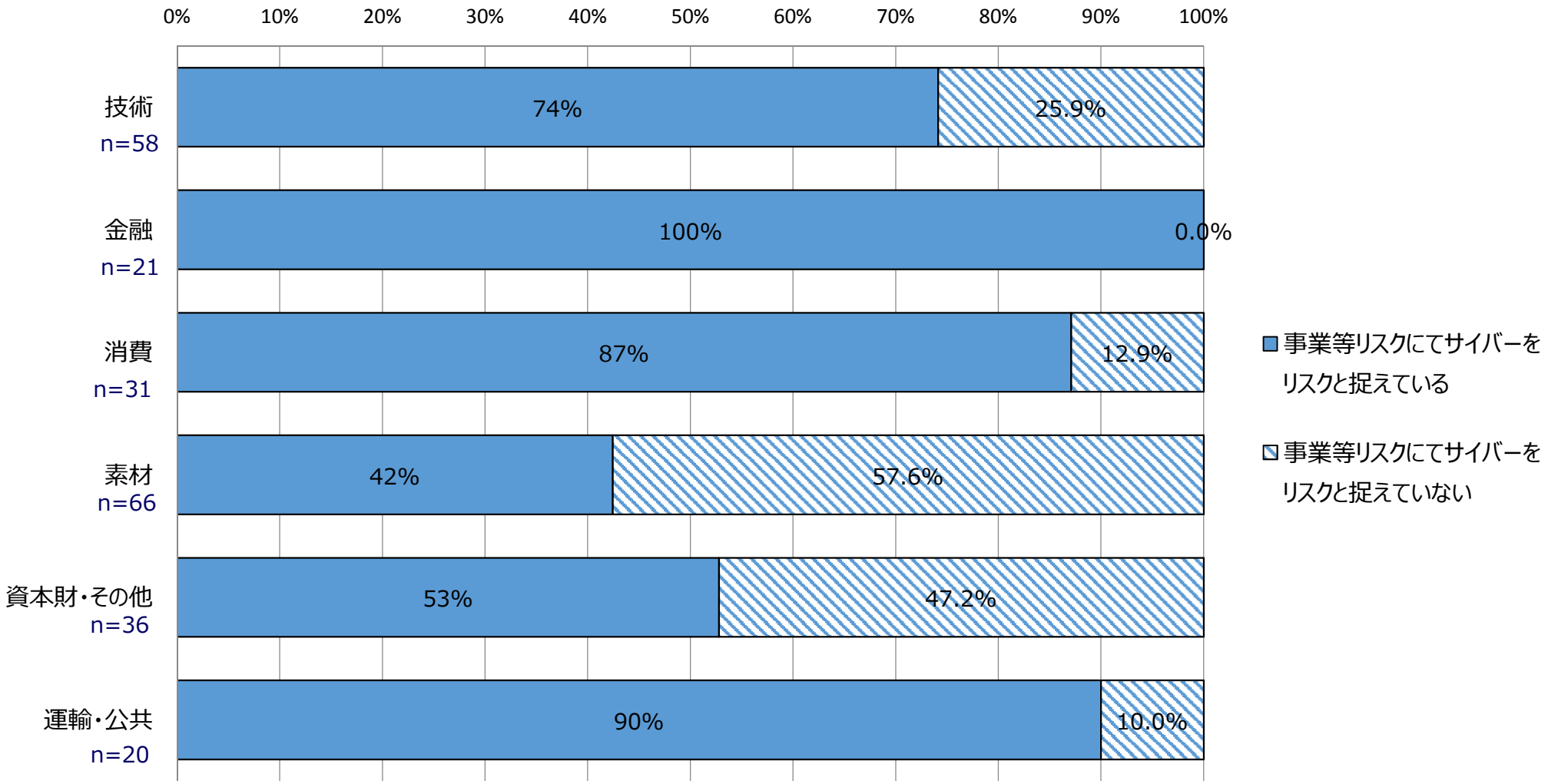


n=232
（日経225の入れ替えのため）

Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

サイバーセキュリティをリスクと認識している状況(業種毎)

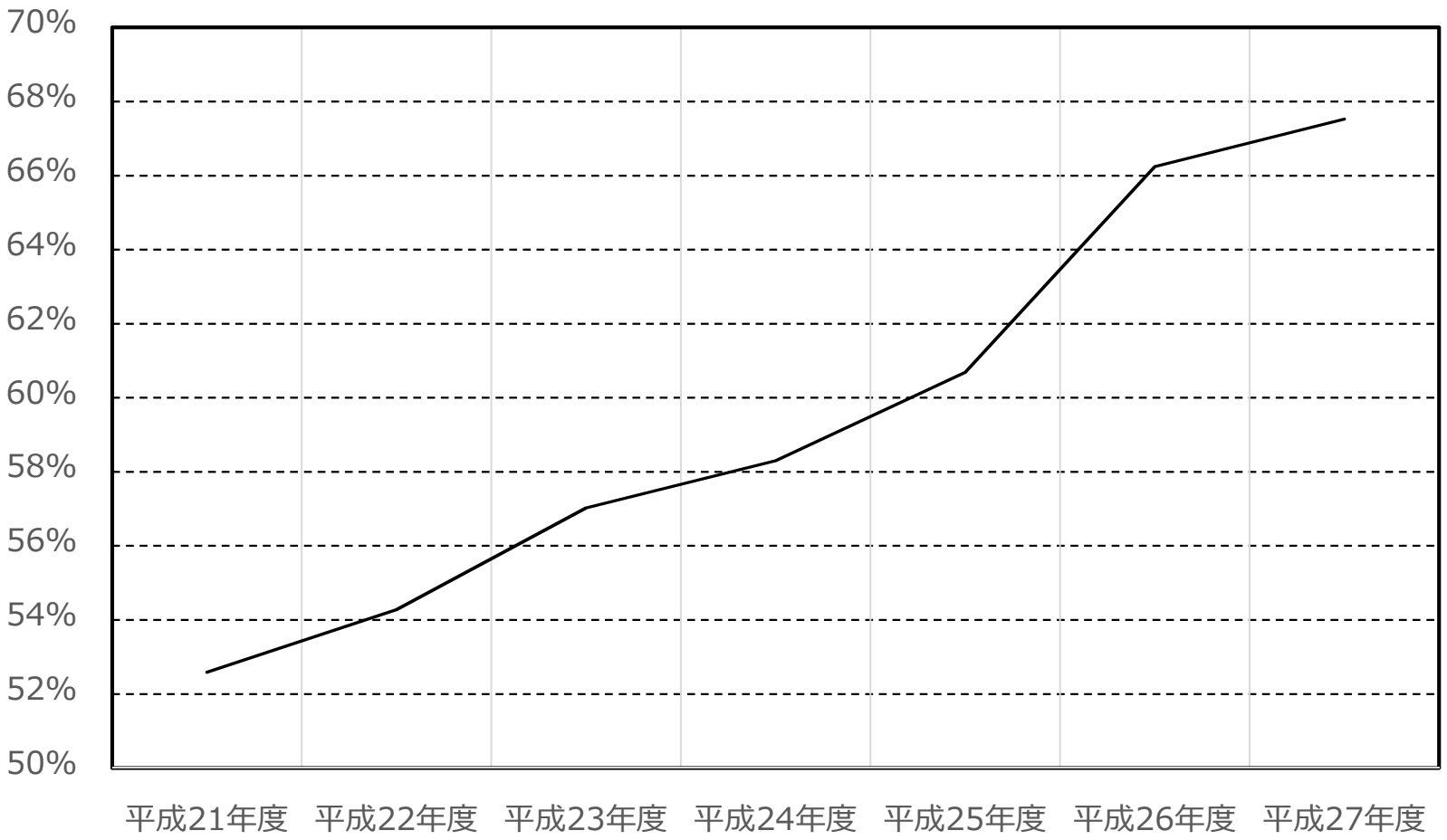
業種毎に見ると、金融業界の開示率は100%となっており、運輸・公共も9割が開示している。



Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

近年の情報発信の動向

有価証券報告書において、情報・サイバーセキュリティリスクを開示する企業の割合は年々増加傾向にある

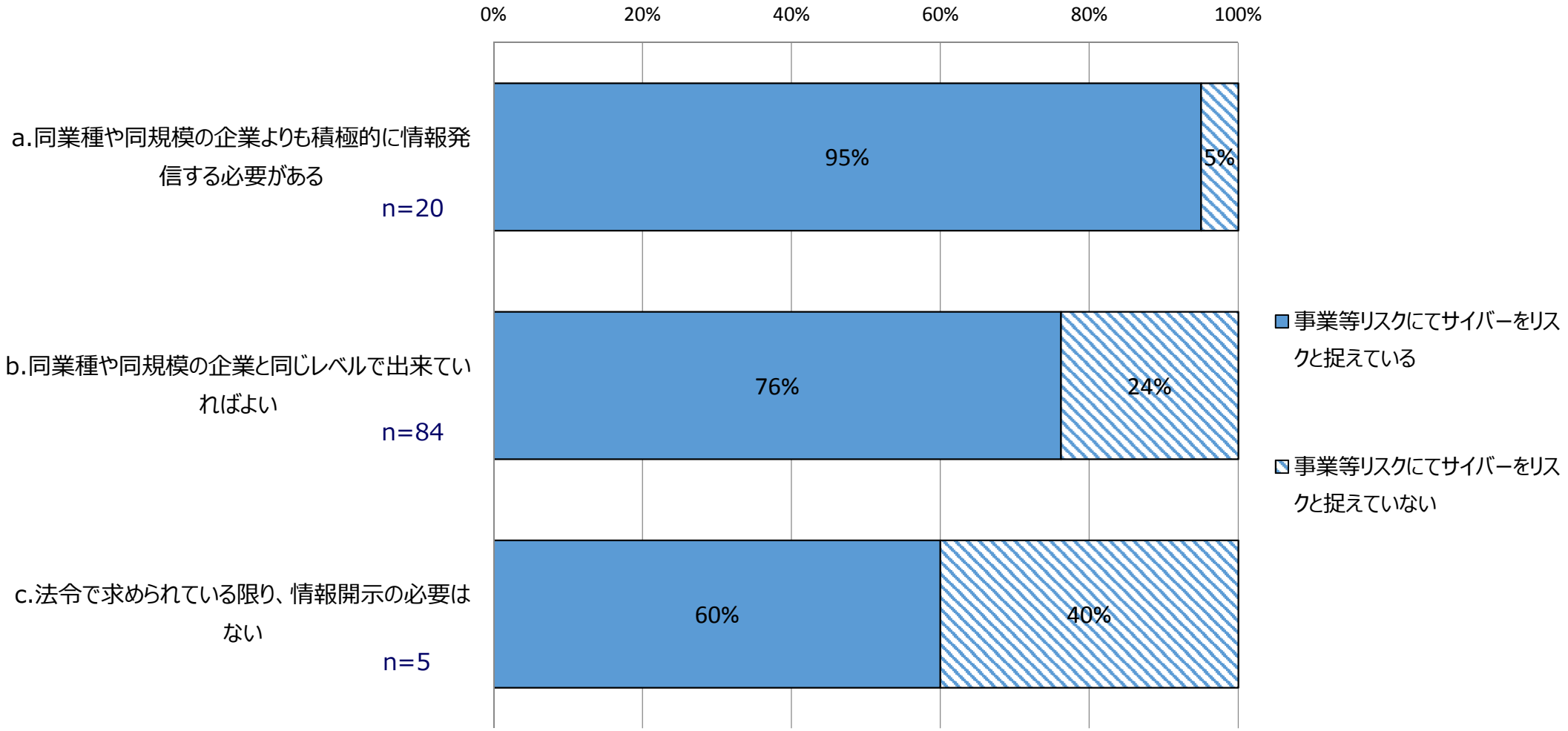


日経２２５企業の有価証券報告書での事業等リスクの項目において、情報・サイバーセキュリティリスクについて開示している企業の割合

Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

情報発信に関するアンケート設問と有価証券報告書でのサイバーリスク認識状況

アンケートにて、積極的に情報発信する必要があると答えた企業ほど、有価証券報告書での開示率も高い。



Copyright (c) 2016 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.