経済産業省
Ministry of Economy, Trade and Industry

DBSCセミナー講演

東日本大震災の経験を踏まえた情報セキュリティ対策

平成２４年２月１７日

経済産業省商務情報政策局
情報セキュリティ政策室長
江　口　純　一

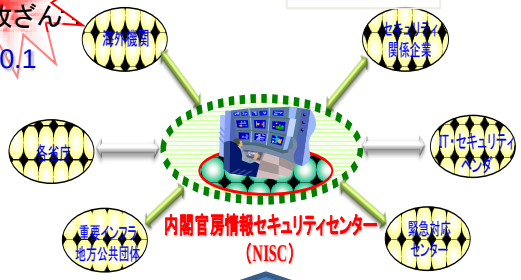
これまでの情報セキュリティ政策（政府全体）

経済産業省
Ministry of Economy, Trade and Industry

年度 2000 2005 2006 2008 2009 2010 2012

省庁HP連続改ざん
2000.1

NISC設置



米韓へのサイバー攻撃
2009.7

スタックスネット
2010

第１次情報セキュリティ基本計画

政府機関・地方公共団体、重要インフラ、企業、個人の情報セキュリティ対策に係る各種対策の強化のための基本計画を策定。
【2006年度から2008年度】

第２次情報セキュリティ基本計画

第１次情報セキュリティ基本計画の取組を持続的に推進するとともに、事前対策は当たり前のこととし、問題が生じても、冷静・迅速に事後対応・復旧活動を推進できる体制を整備。【2009年度から2011年度】

協力

4省庁
警察庁 総務省 経済産業省 防衛省

国民を守る情報セキュリティ戦略

第２次情報セキュリティ基本計画を包含した戦略として、新たに、重点的な取組として、大規模サイバー攻撃事態等への対処等を位置付けた。
【2010年度から2013年度】

政府機関・地方公共団体

「政府機関統一基準」等により情報セキュリティを確保

【主な施策】
① サイバー攻撃等への緊急対応
②情報セキュリティ体制の整備
（最高情報セキュリティ責任者（CISO）の設置など）
③政府機関統一基準の策定
（各省庁が守るべき最低限の対策水準を規定）
④政府機関におけるPDCA

重要インフラ

「重要インフラ行動計画」に基づく官民連携による重要インフラ防護

【主な施策】
① 安全基準等の整備
② 情報共有体制の強化
③ IT障害の波及の最小化
（共通脅威分析、演習等）

※重要インフラ（10分野）
●情報通信 ●金融 ●航空 ●鉄道 ●電力 ●ガス
●政府・行政サービス ●医療 ●水道 ●物流

企業・個人

普及啓発、ガイドライン等

【主な施策】
①「情報セキュリティ月間」の実施
②情報セキュリティガバナンス確立の支援（各種ガイドライン）
③人材育成、製品評価・認証等

経済産業省「情報セキュリティ総合戦略」

経済産業省
Ministry of Economy, Trade and Industry

- 2003年制定
- 我が国で初めて策定された総合的な情報セキュリティに関する戦略
- 戦略の基本目標を、経済・文化国家日本の強みを活かした世界最高水準の高信頼性社会の構築と位置付けた

経済産業省「グローバル情報セキュリティ戦略」

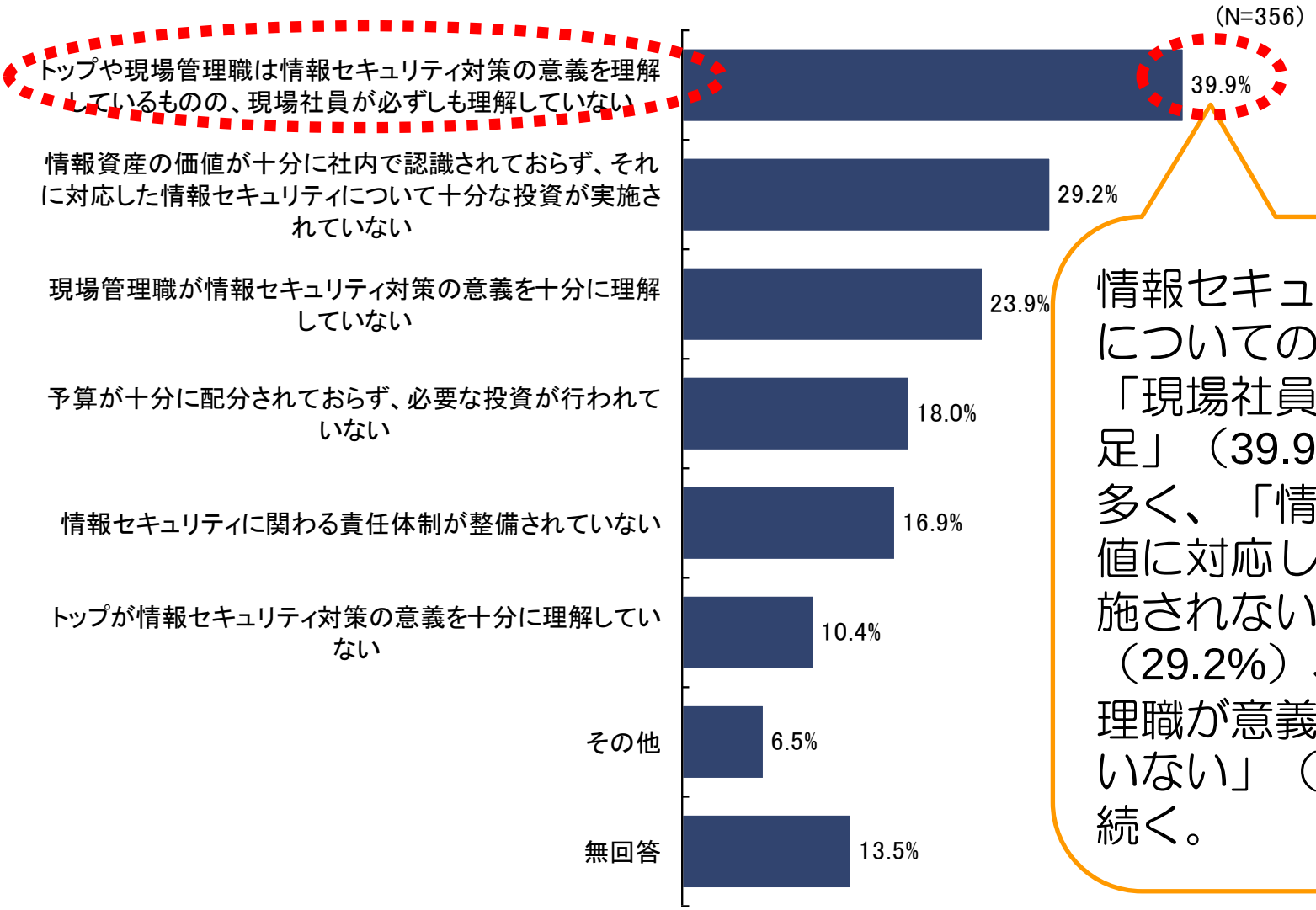
経済産業省
Ministry of Economy, Trade and Industry

- 2007年制定
- ITが国内外の経済社会システムに融合化し、情報セキュリティに関する脅威も国際化傾向にある中、産業構造審議会情報セキュリティ基本問題委員会にて、次の３つの戦略からなる「グローバル情報セキュリティ戦略」を取りまとめた。
  - 戦略１ 我が国を真に情報セキュリティ先進国とするための取組み
  - 戦略２ 国際化する脅威に対応し、我が国の国際競争力を強化していく観点からの情報セキュリティ政策のグローバル展開
  - 戦略３ 国内外の変化に対応するためのメカニズムの確立

情報セキュリティ対策についての現状把握①

経済産業省
Ministry of Economy, Trade and Industry

情報セキュリティ対策についての課題



情報セキュリティ対策についての課題は、「現場社員の理解不足」（39.9%）が最も多く、「情報資産の価値に対応した投資が実施されない」（29.2%）、「現場管理職が意義を理解していない」（23.9%）と続く。

出所：経済産業省調査（2010年）

情報セキュリティ対策についての現状把握②

経済産業省
Ministry of Economy, Trade and Industry

情報セキュリティ人材の不足状況

情報セキュリティ人材については、
半数以上が「質・量ともに不十分」
と回答している。

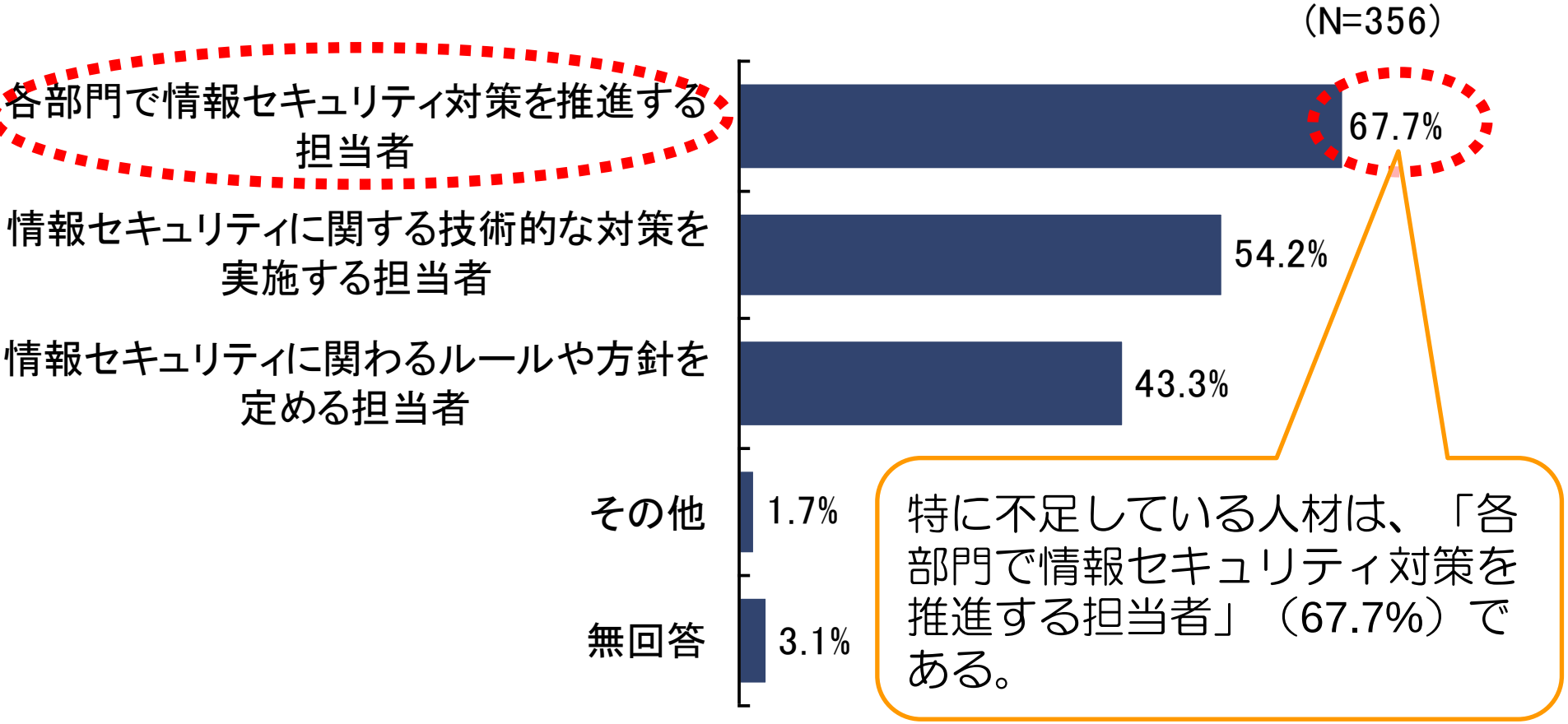
（N=356）

出所：経済産業省調査（2010年）

情報セキュリティ対策についての現状把握③

経済産業省
Ministry of Economy, Trade and Industry

不足している情報セキュリティ人材



特に不足している人材は、「各部門で情報セキュリティ対策を推進する担当者」（67.7%）である。

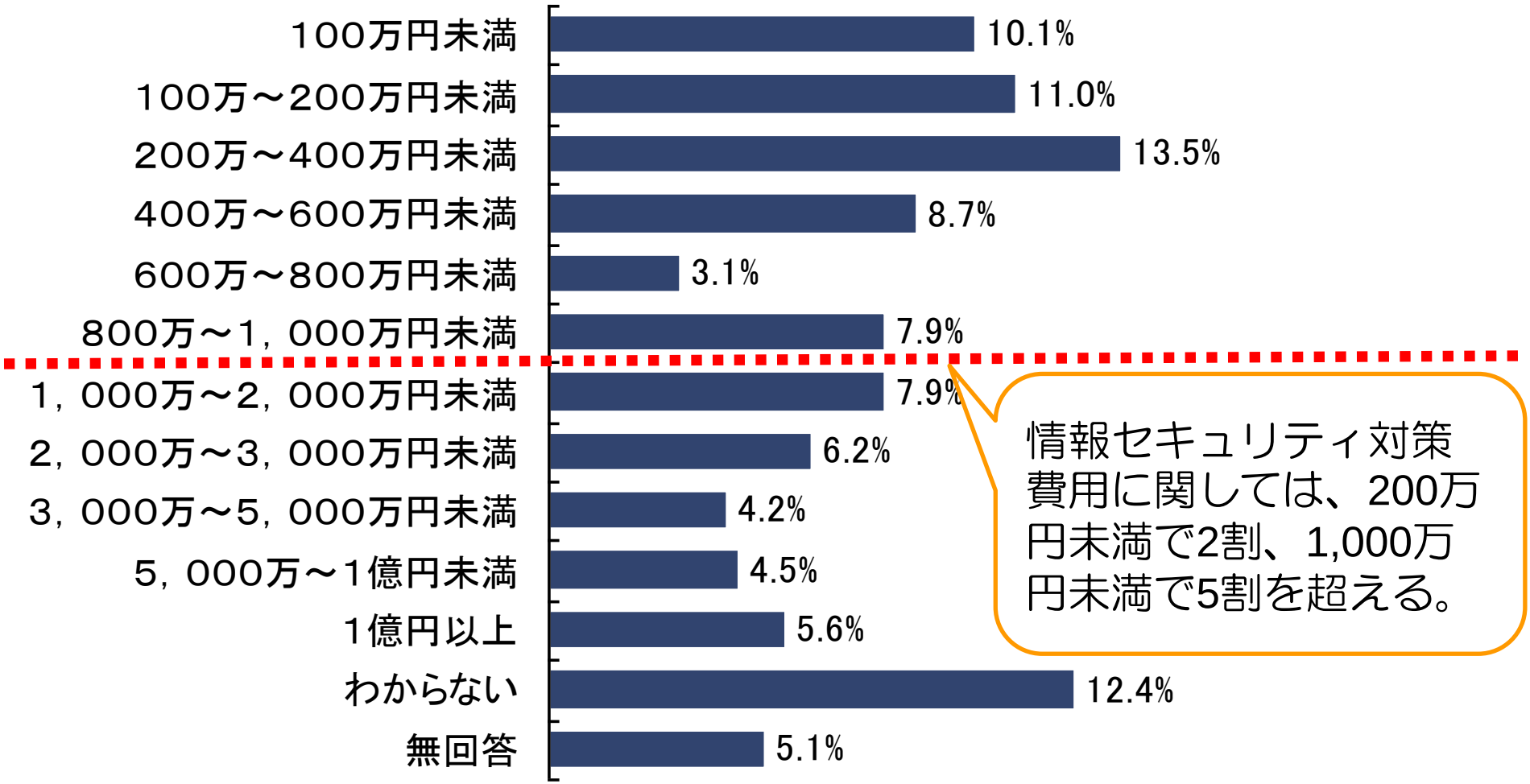
出所：経済産業省調査（2010年）

情報セキュリティ対策についての現状把握④

経済産業省
Ministry of Economy, Trade and Industry

対策費用

（N=356）



情報セキュリティ対策費用に関しては、200万円未満で2割、1,000万円未満で5割を超える。

出所：経済産業省調査（2010年）

- これらの課題に対応するため、企業の情報セキュリティガバナンスを構築することが必要。

情報セキュリティガバナンスとは何か①

経済産業省
Ministry of Economy, Trade and Industry

定義

様々なリスクのうち、情報資産に係るリスクの管理を狙いとして、情報セキュリティに関わる意識、取組及びそれらに基づく業務活動を組織内に徹底させるための仕組みを構築・運用する取組み

情報セキュティガバナンスの適用対象

- 個別企業
- 連結ベースの企業グループ
- バリューチェーンを形成する企業グループ

情報セキュリティガバナンスとは何か②

経済産業省
Ministry of Economy, Trade and Industry

これまでの成果物

企業の情報セキュリティに関する制度等

•2001年 情報セキュリティマネジメントシステム(ISMS)適合性評価制度を開始
((財)日本情報処理開発協会(JIPDEC))
•2003年 情報セキュリティ監査制度開始((NPO日本セキュリティ監査協会(JASA))
•2005年 情報セキュリティ対策ベンチマークのサービス開始((独)情報処理推進機構(IPA))
•2008年 民間の情報セキュリティ格付機関設立

制度・規定・ガイダンス等

•2001年 ISMS国際標準規格 ISO/IEC 17799:2000 に対応したISMS認証基準策定(JIPDEC)
•2003年 情報セキュリティ管理基準、監査基準(経済産業省告示)
•2005年 情報セキュリティ報告書モデル、事業継続計画(BCP)策定ガイドライン
•2006年 財務報告書に係るＩＴ統制ガイダンス　(J-SOX対応版)
•**2008年** 情報セキュリティ管理基準、監査基準(改正)、**ITサービス継続ガイドライン**
•2009年 中小企業の情報セキュリティガイドライン(IPA)

シンポジウムによる普及啓発

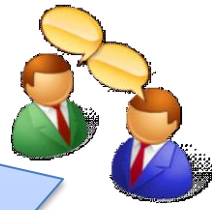
•2005年度,2007年度から2009年度まで情報セキュリティガバナンスシンポジウムを
年１回東京にて開催。

情報セキュリティガバナンス確立に向けた取組(平成２３年度)

経済産業省
Ministry of Economy, Trade and Industry

課題

•東日本大震災の発生により、企業におけるITサービスの継続やサプライチェーンの破綻といったトラブルが発生し、日本経済全体の停滞にもつながりかねない大きな問題となった。



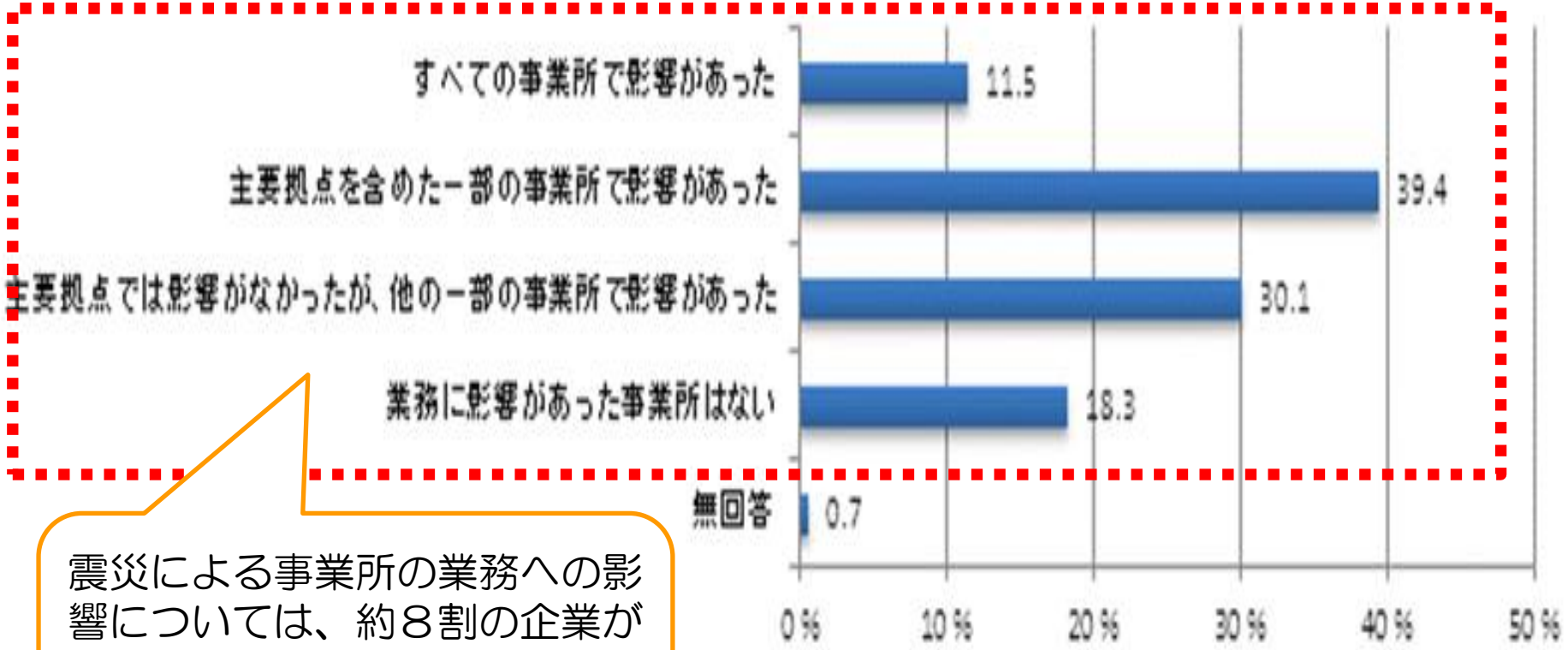
解決策としての当省の取組み

➢東日本大震災の影響及び国際標準(IEC27031)等の内容を踏まえ、2008年度に策定したITサービス継続ガイドラインを改訂する。

震災における被災状況把握①

経済産業省
Ministry of Economy, Trade and Industry

業務に影響があった事業所の有無



震災による事業所の業務への影響については、約８割の企業が事業所の業務に何らかの影響を受けている。

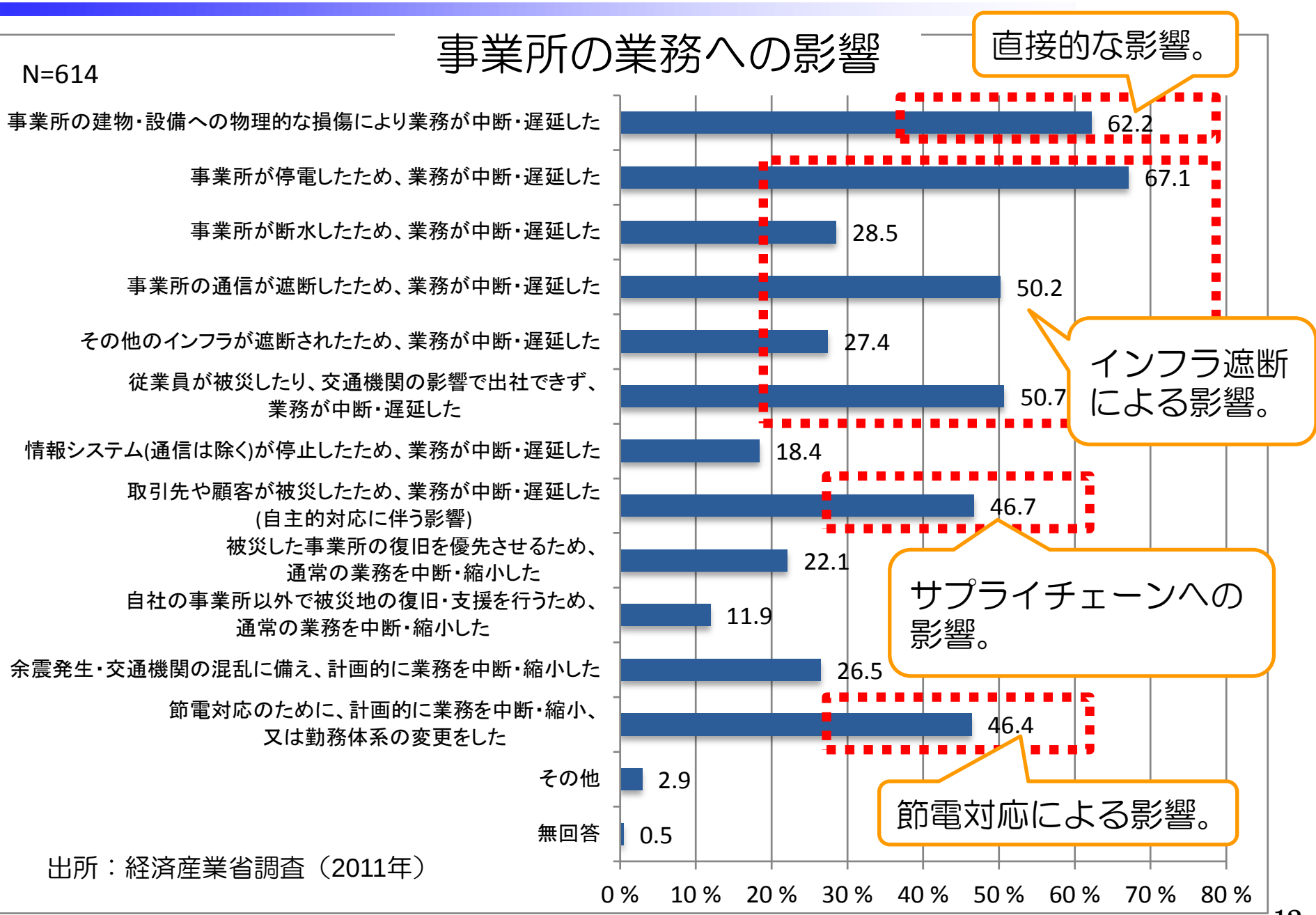
出所：経済産業省調査（2011年）

震災における被災状況把握②

経済産業省
Ministry of Economy, Trade and Industry

事業所の業務への影響

N=614



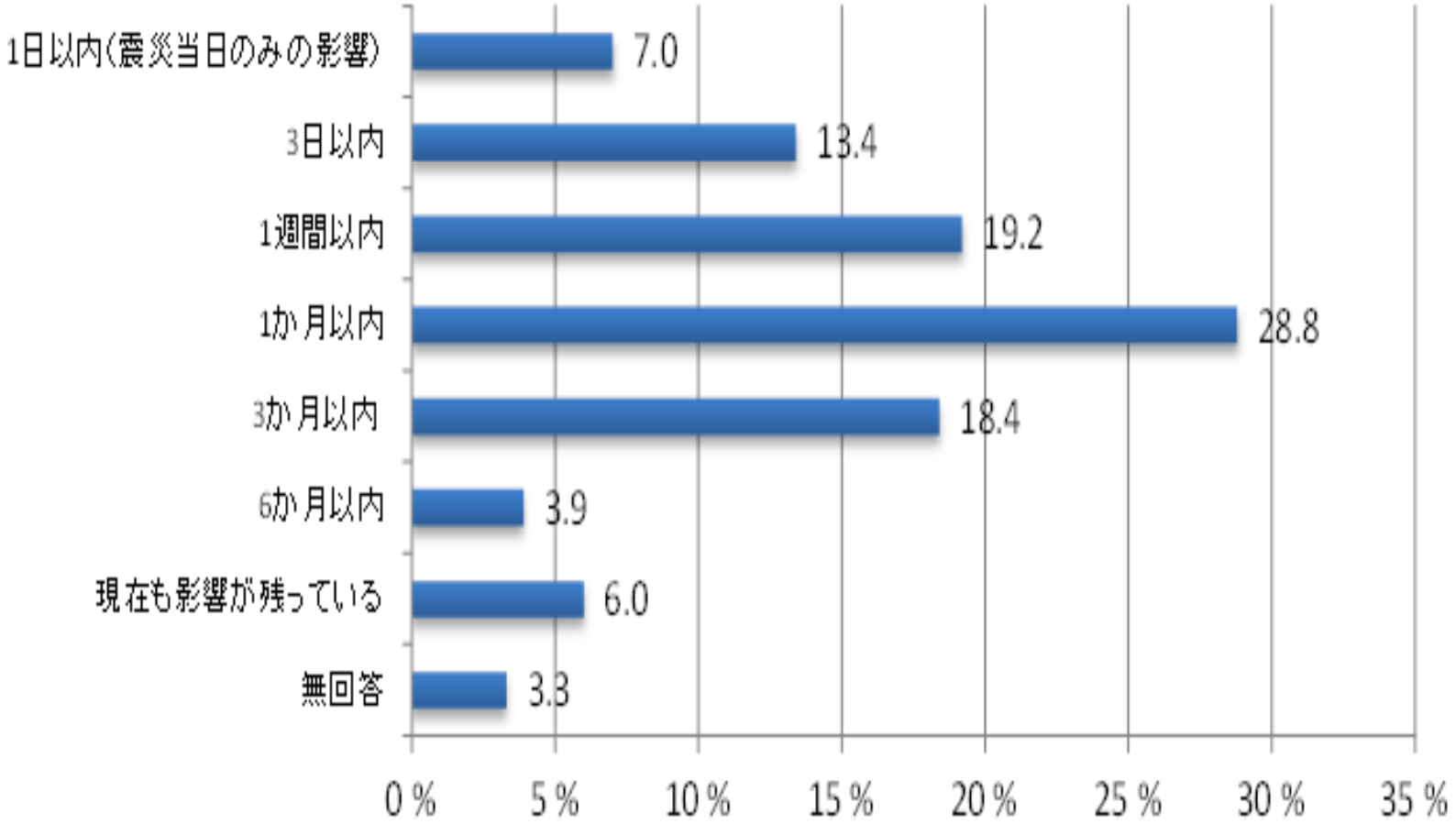
出所：経済産業省調査（2011年）

震災における被災状況把握③

経済産業省
Ministry of Economy, Trade and Industry

N=614

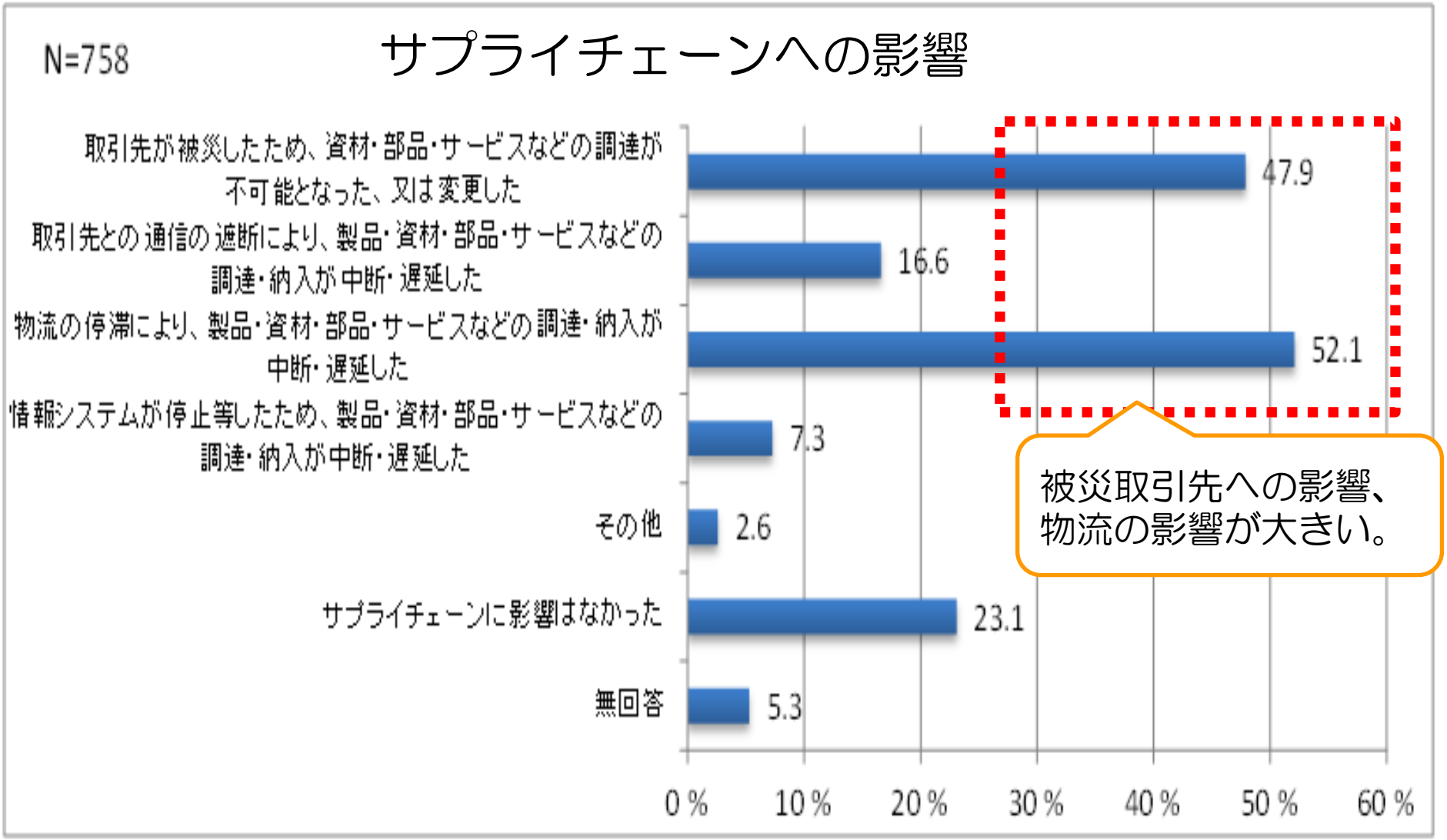
業務への影響があった期間



出所：経済産業省調査（2011年）

震災における被災状況把握④

経済産業省
Ministry of Economy, Trade and Industry



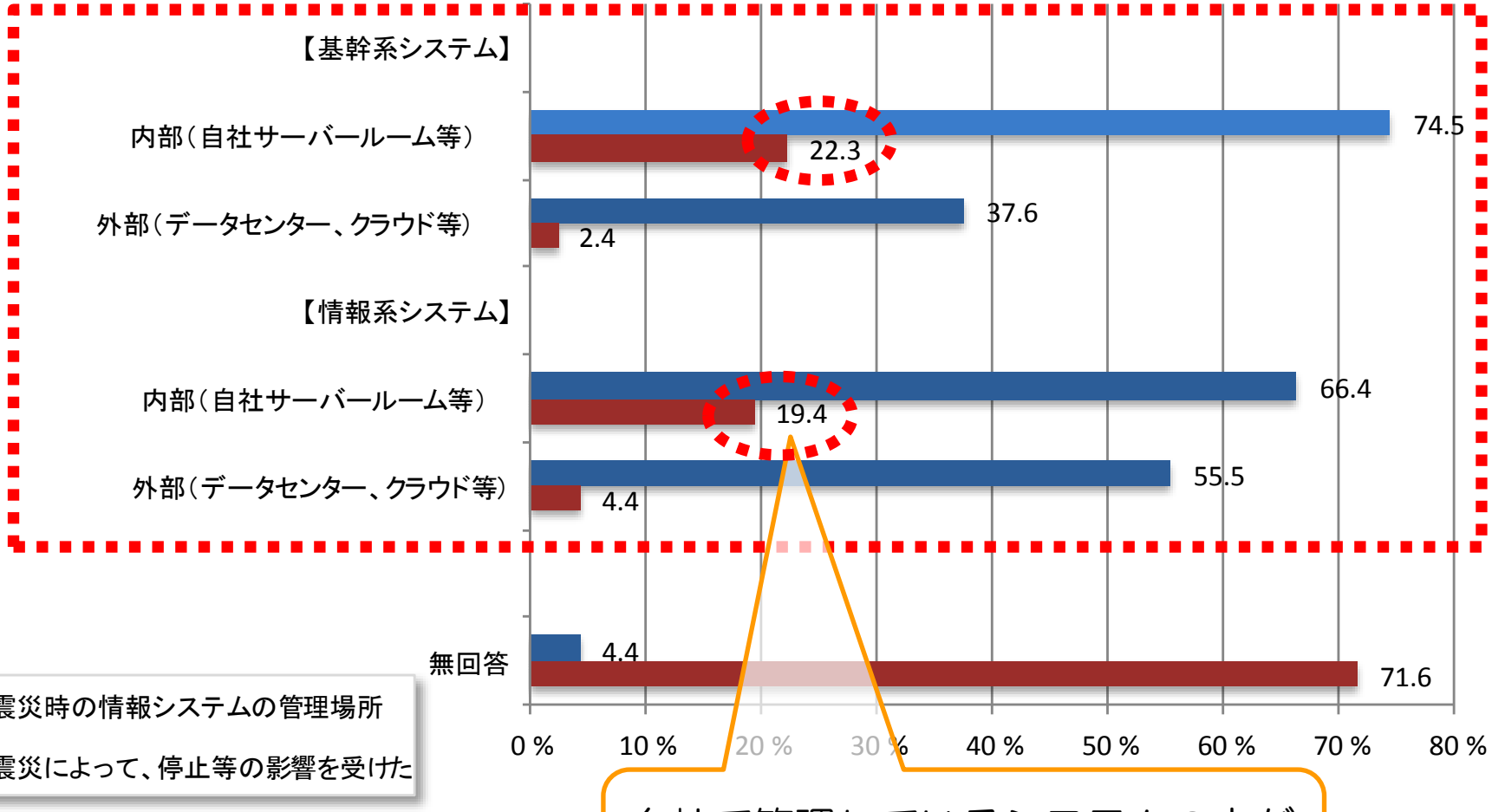
出所：経済産業省調査（2011年）

情報システムが受けた影響①

経済産業省
Ministry of Economy, Trade and Industry

N=758

震災時運用していた情報システムの管理場所／情報システムへの影響の有無



自社で管理しているシステムの方が影響を受けやすい。

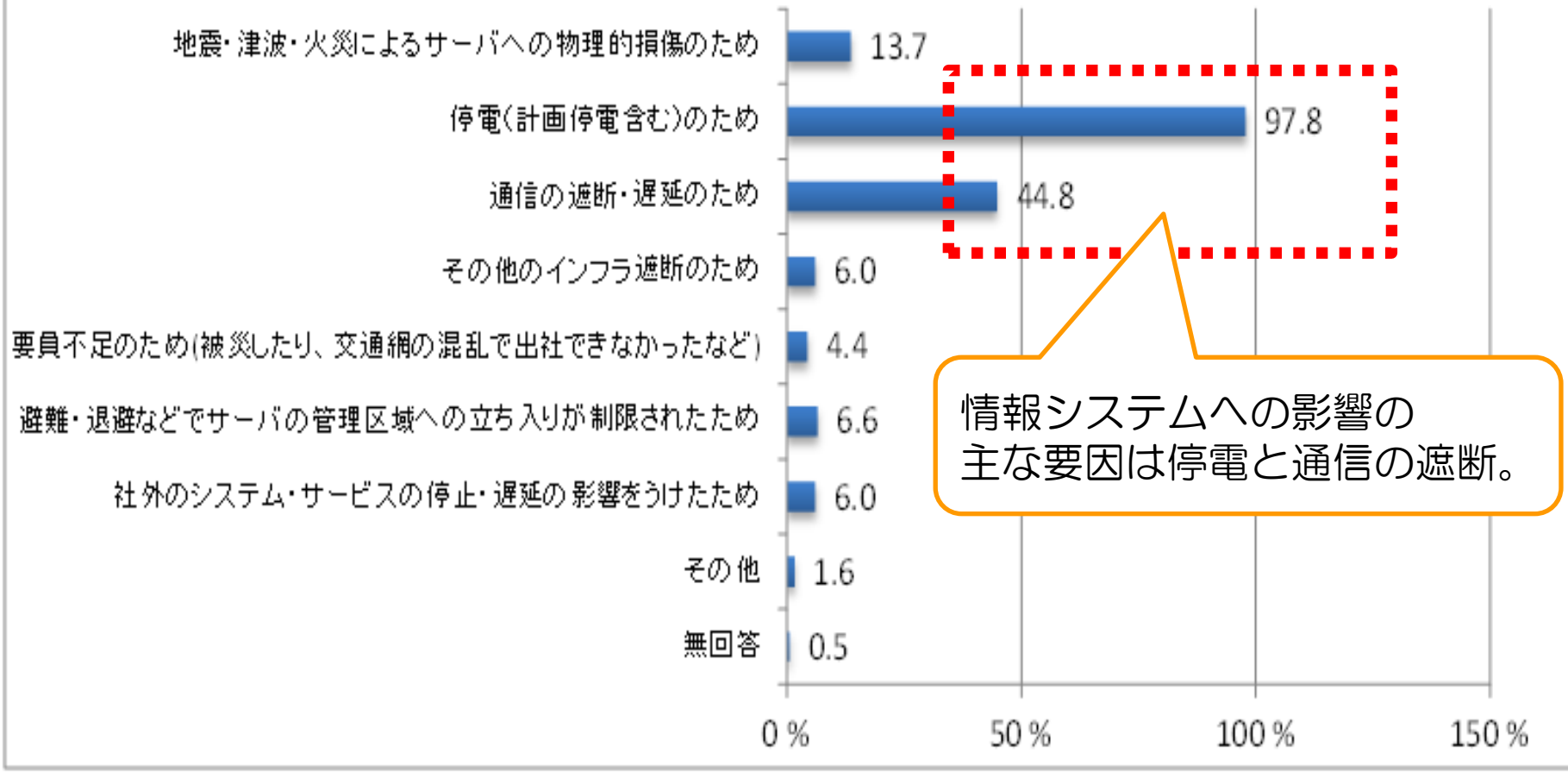
出所：経済産業省調査（2011年）

情報システムが受けた影響②

経済産業省
Ministry of Economy, Trade and Industry

N=215

情報システムに影響を与えた要因

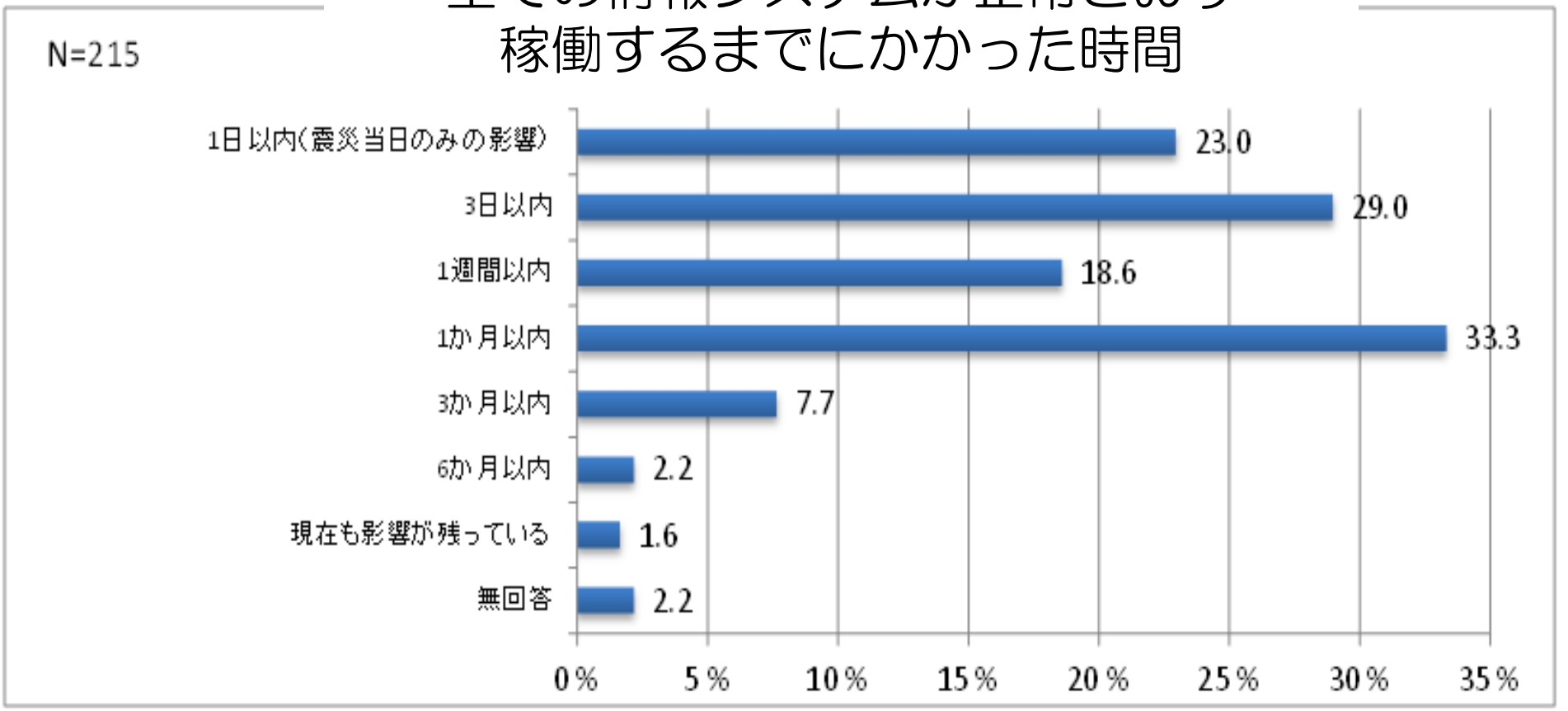


出所：経済産業省調査（2011年）

情報システムが受けた影響③

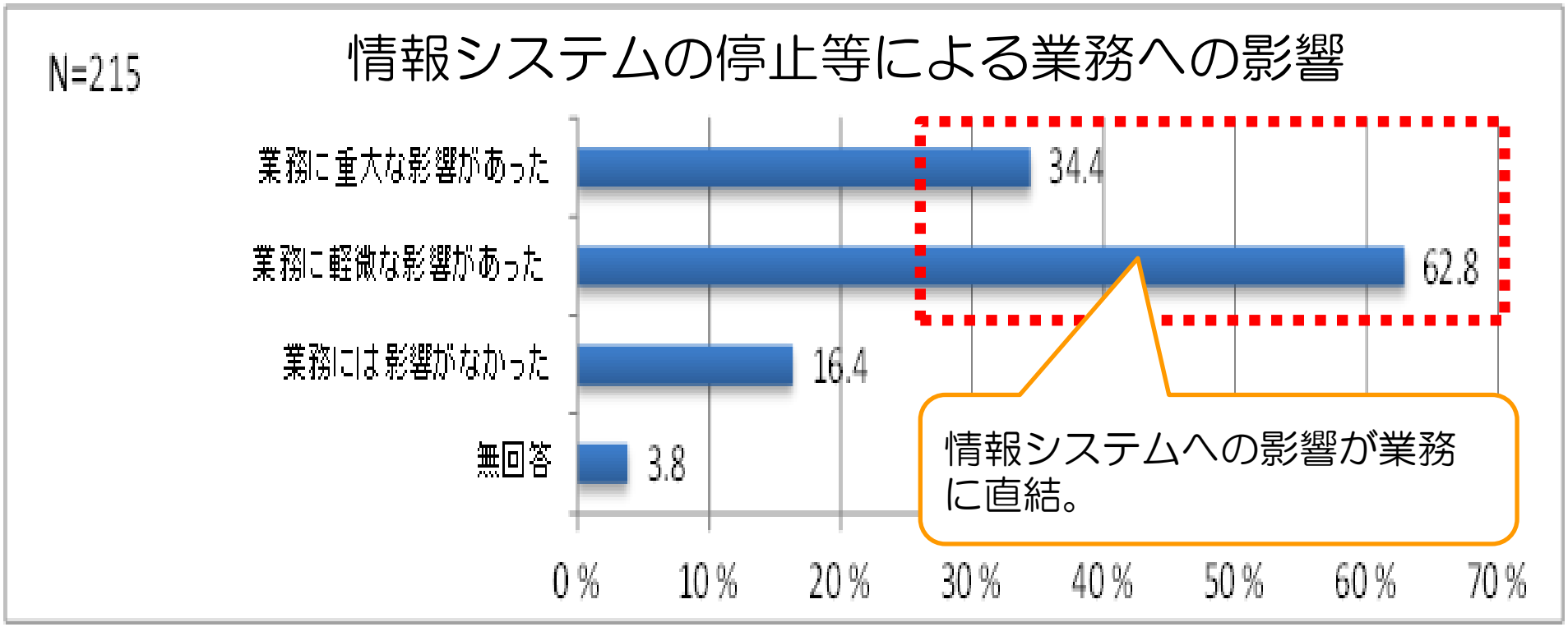
経済産業省
Ministry of Economy, Trade and Industry

全ての情報システムが正常どおり稼働するまでにかかった時間



出所：経済産業省調査（2011年）

情報システムが受けた影響④



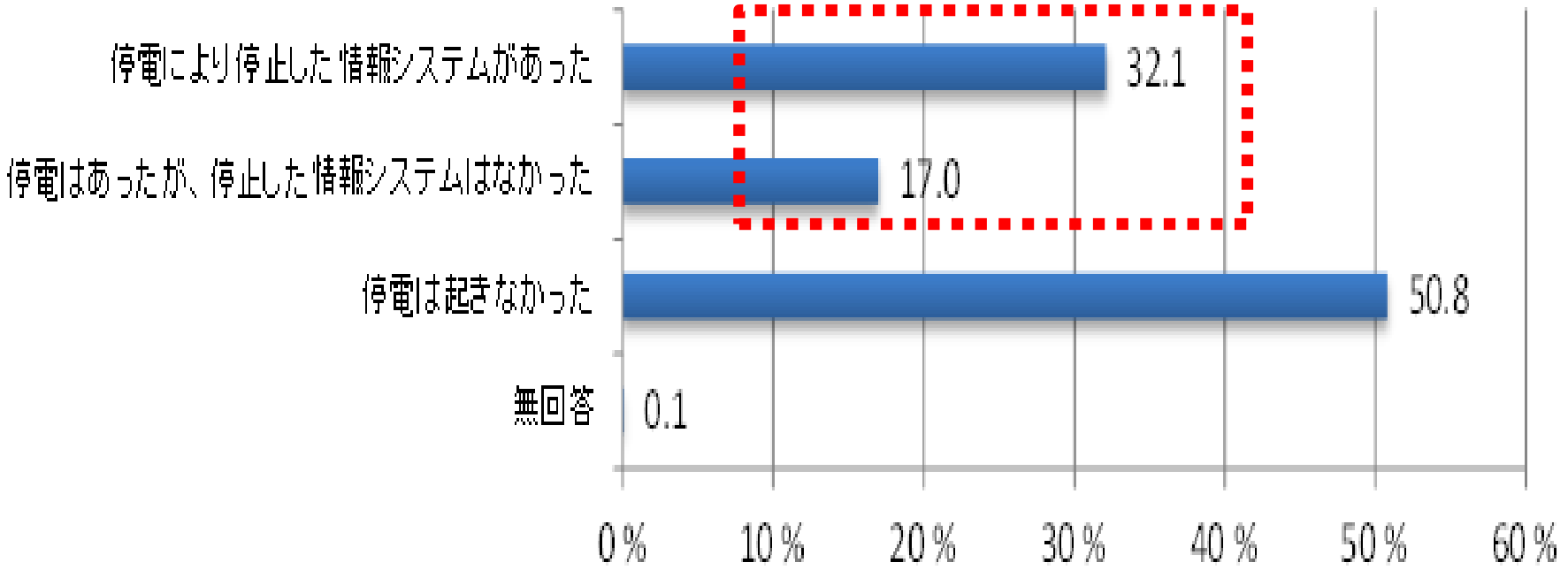
出所：経済産業省調査（2011年）

情報システムが受けた影響⑤

経済産業省
Ministry of Economy, Trade and Industry

N=758

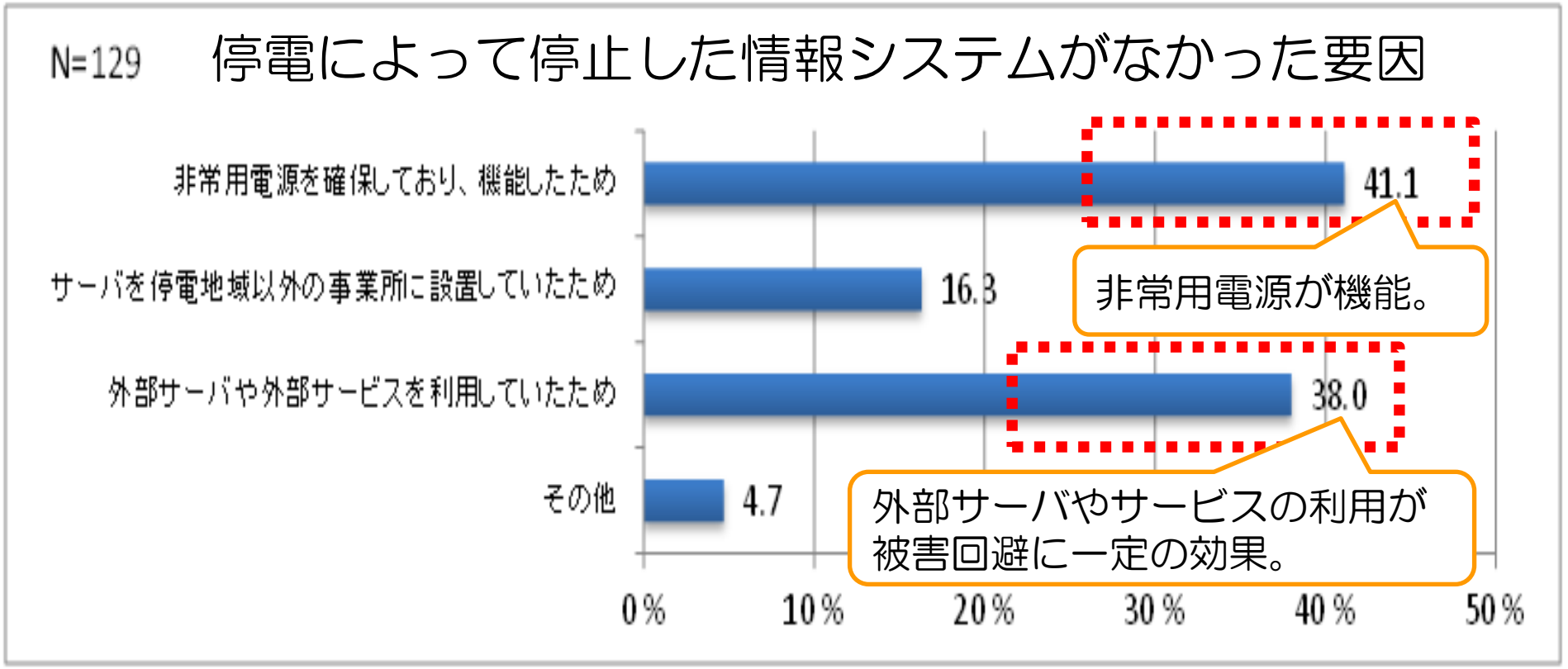
震災時の停電により、停止したシステムの有無



出所：経済産業省調査（2011年）

情報システムが受けた影響⑥

経済産業省
Ministry of Economy, Trade and Industry



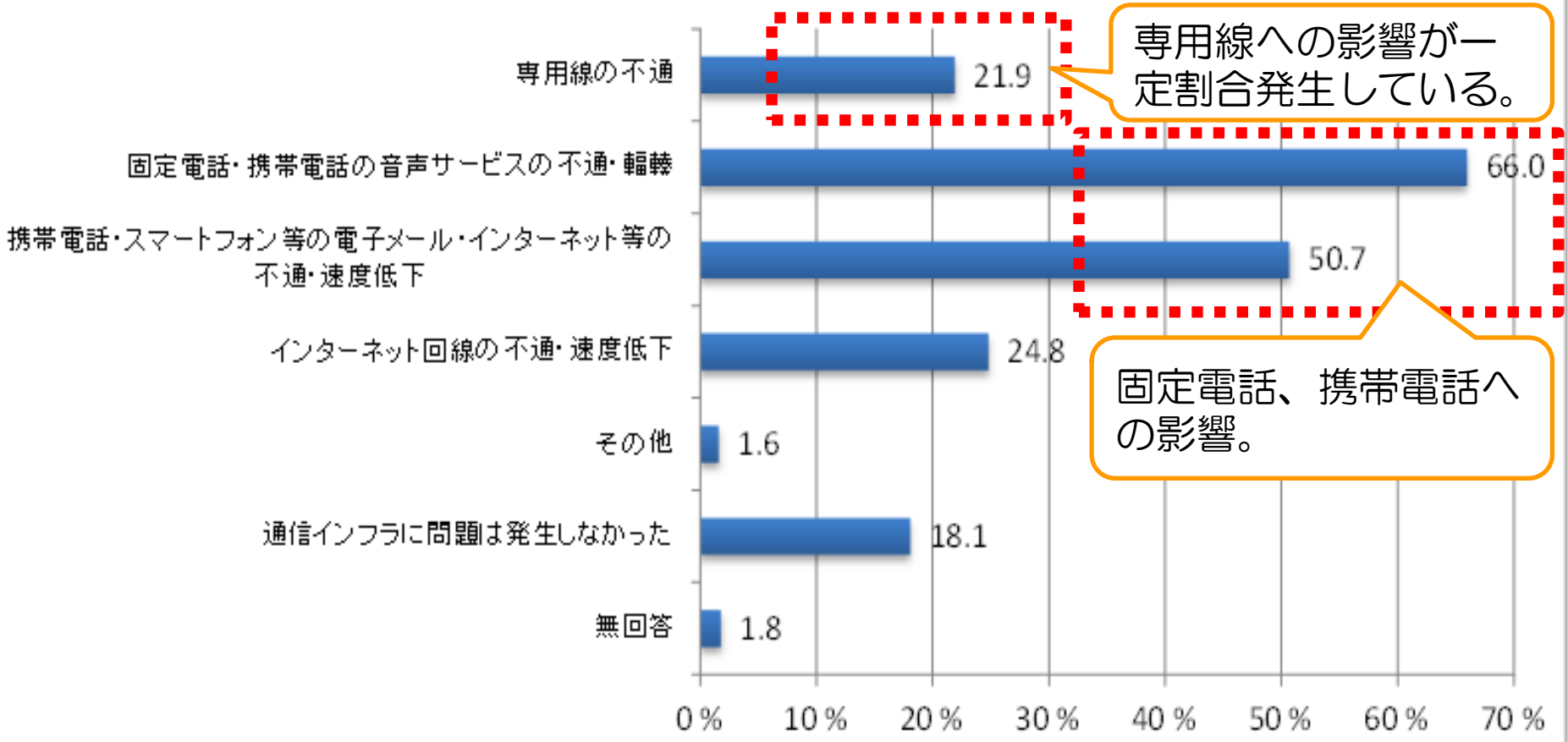
出所：経済産業省調査（2011年）

情報システムが受けた影響⑦

経済産業省
Ministry of Economy, Trade and Industry

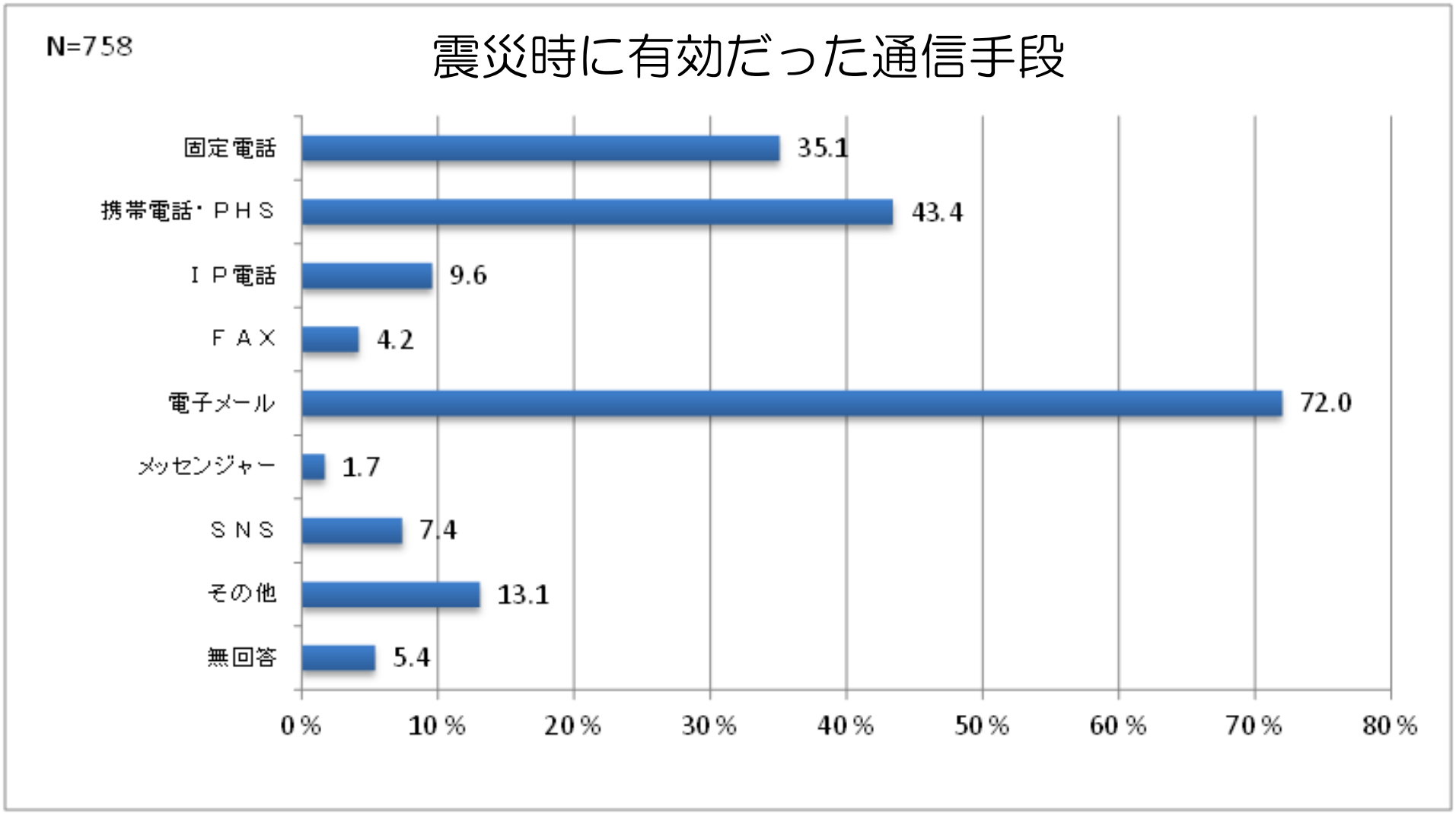
N=758

震災時に影響があった通信インフラへの影響



出所：経済産業省調査（2011年）

情報システムが受けた影響⑧



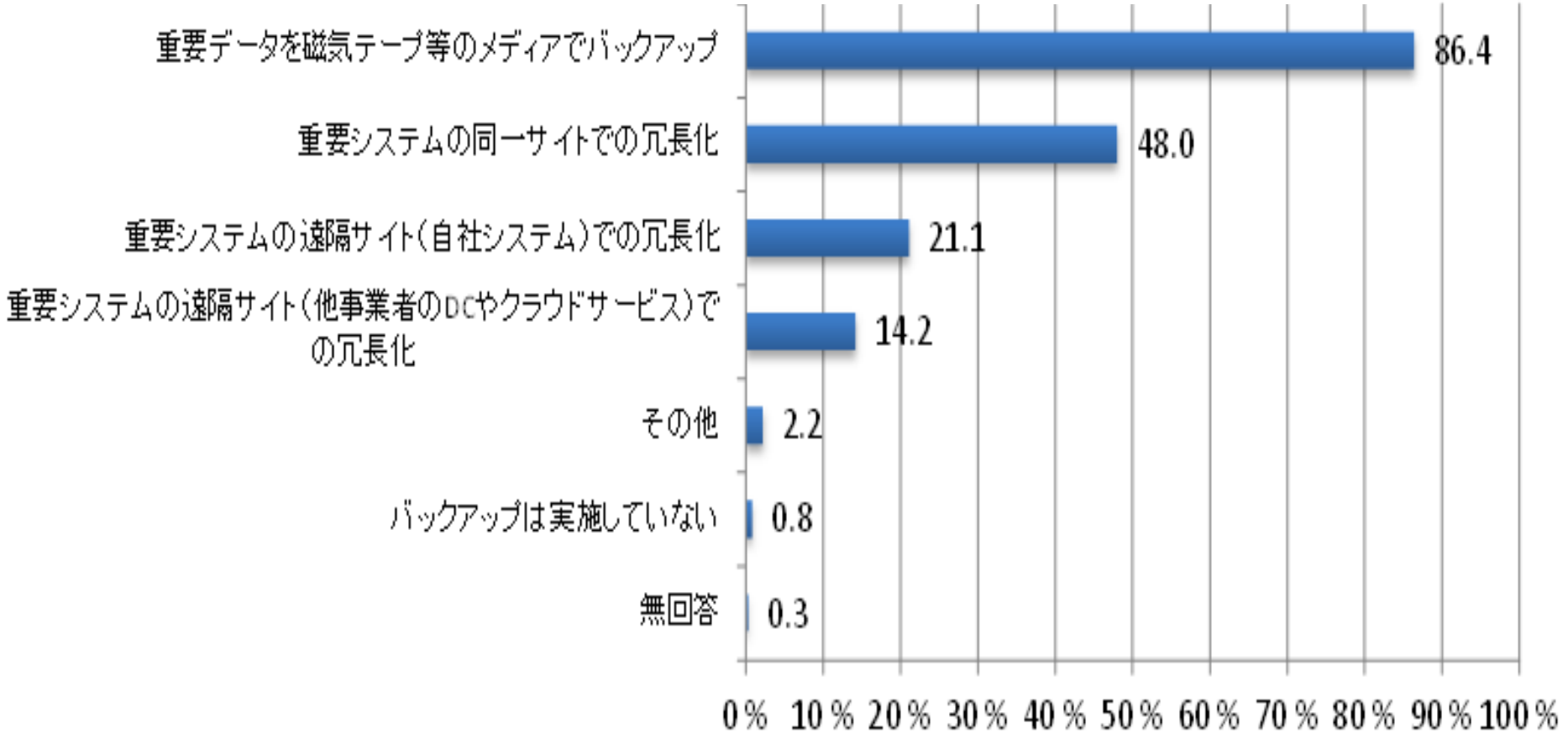
出所：経済産業省調査（2011年）

情報システムが受けた影響⑨

経済産業省
Ministry of Economy, Trade and Industry

情報システム等のバックアップ形態として利用されているもの

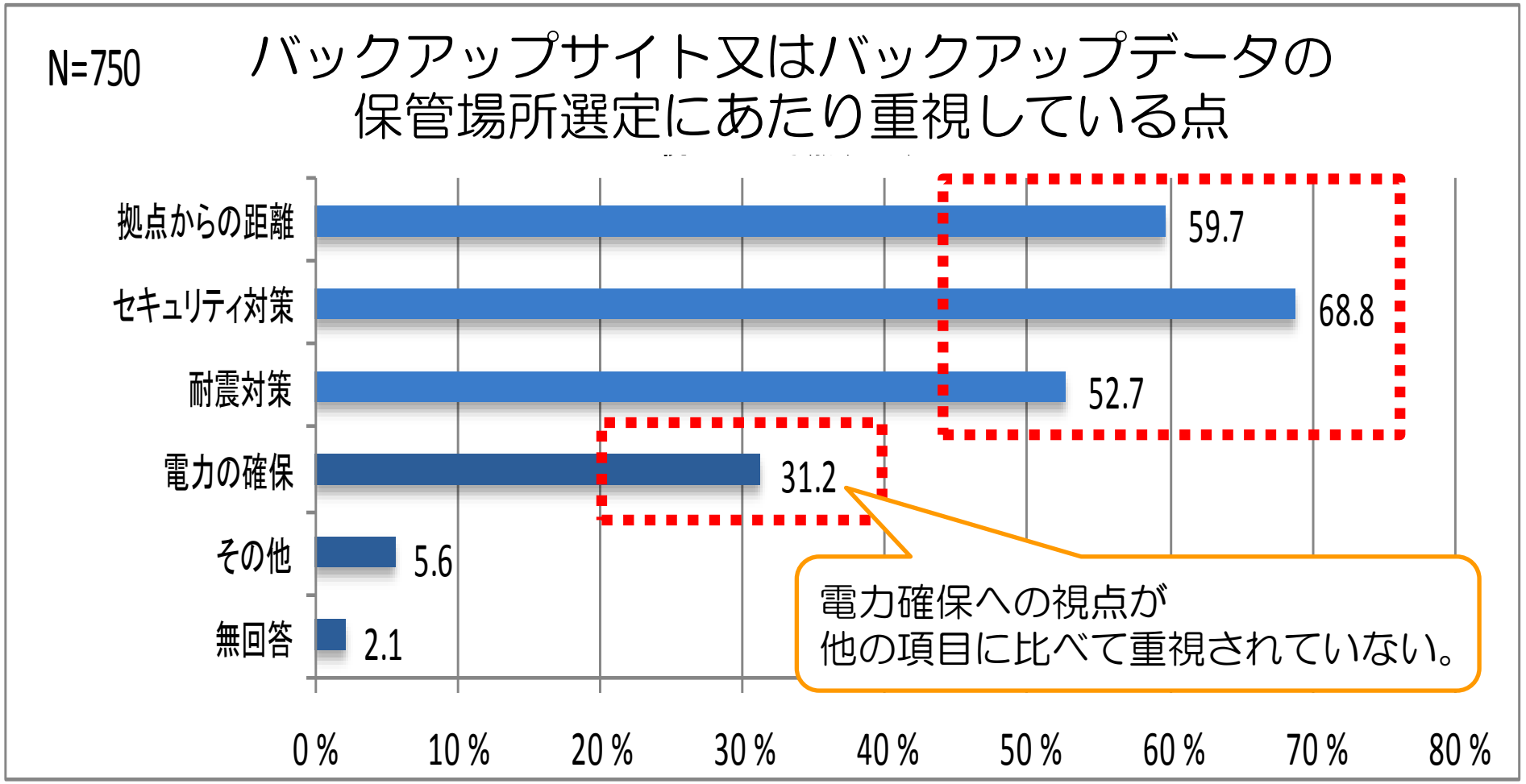
N=758



出所：経済産業省調査（2011年）

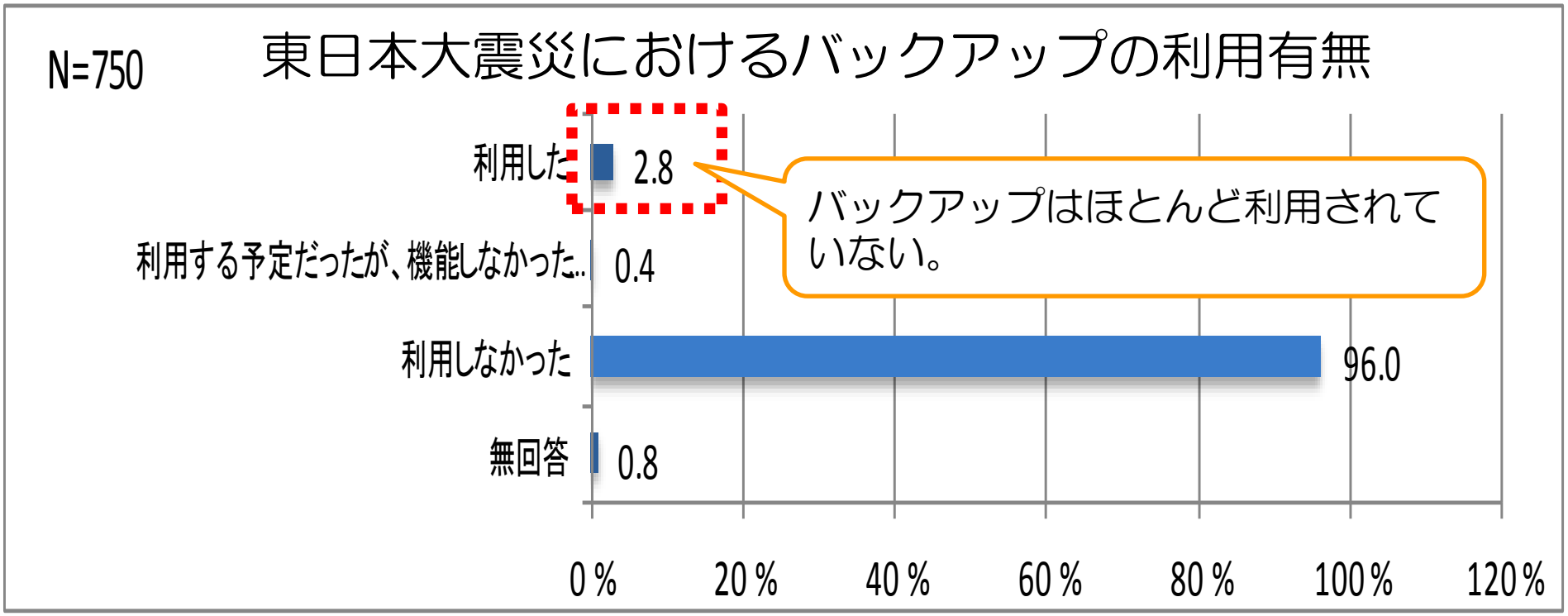
情報システムが受けた影響⑩

経済産業省
Ministry of Economy, Trade and Industry



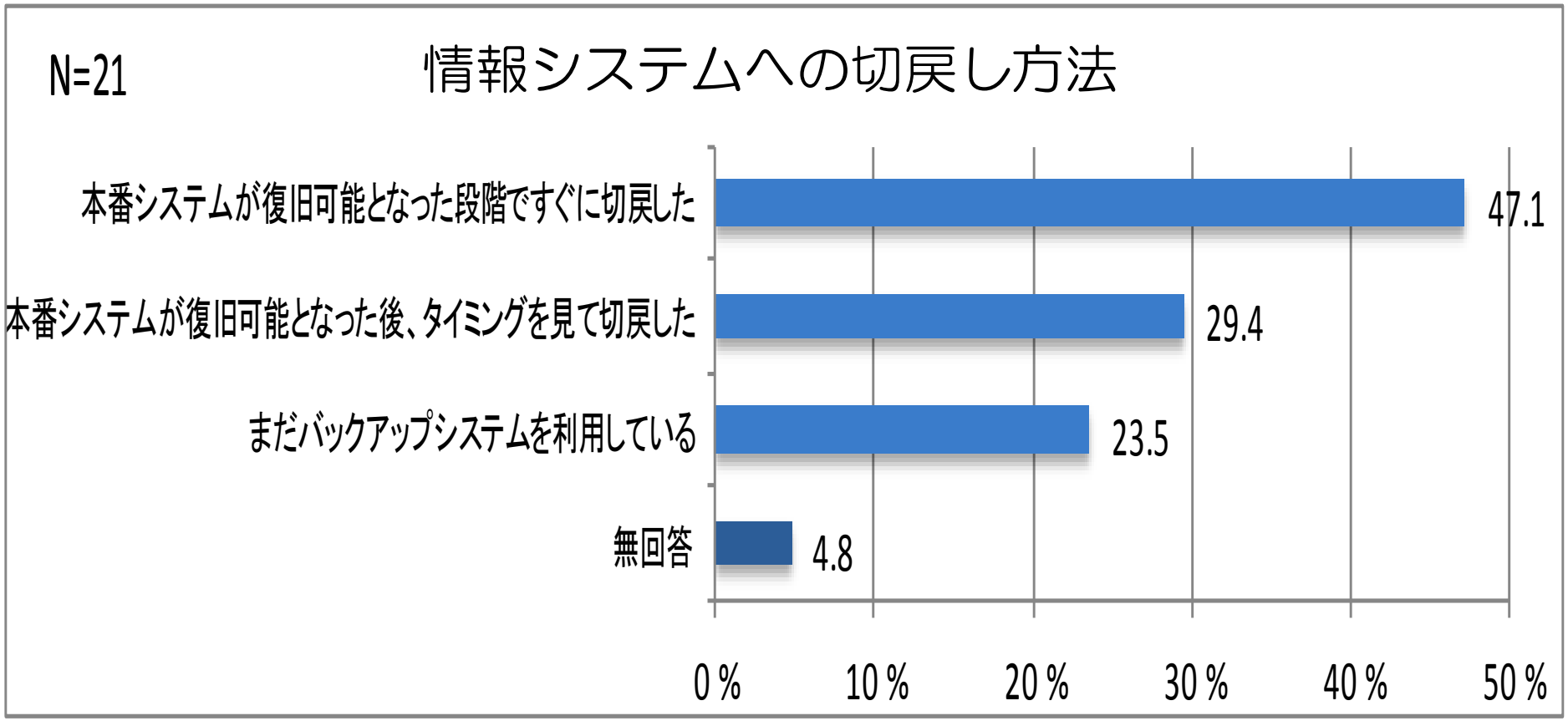
出所：経済産業省調査（2011年）

情報システムが受けた影響⑪



出所：経済産業省調査（2011年）

情報システムが受けた影響⑫



出所：経済産業省調査（2011年）

情報セキュリティとITサービス継続との位置づけ

経済産業省
Ministry of Economy, Trade and Industry

位置づけ

- 情報セキュリティは、情報の機密性、完全性及び可用性を維持することとして一般的に定義されている。IT サービス継続は、主に可用性の維持に関係するものとして位置づけることができる。
- 情報セキュリティとIT サービス継続とは、どちらかが他方を包含する関係というよりも、相互に関係するものとして位置づけられる。

ITサービスとは

経済産業省
Ministry of Economy, Trade and Industry

定義

- ITサービスとは、組織 における業務の遂行に際して必要となるITおよびそれに関連する体制の組み合わせによって提供される機能であり、その機能が組織外部により提供されるものであるか否かは問わない。
- 具体的には、財務会計システム、生産管理システム、在庫管理システム、顧客管理システムなどの基幹システムに加え、電子メールシステム、入館システム、スケジューラー、部門等で作成・提供されている表計算等の基幹システムではないものも含む。

ITサービス継続とは

経済産業省
Ministry of Economy, Trade and Industry

定義

- ITサービス継続とは、事業継続の一部であり、ITサービスの中断・停止による事業継続に与える影響を求められる品質レベルに応じて最適化するための取り組みである。
- ITサービス継続を実現するためには、中長期にわたるITに係る投資計画や体制面の整備が必要となるため、必然的にITサービス継続はIT戦略の一部ないしIT戦略の下位に整合的に位置づけられる。

ITサービス継続戦略の要件定義

経済産業省
Ministry of Economy, Trade and Industry

■IT サービスの中断・停止につながる事象が発生した場合、経営者、業務部門、IT 部門、社外の取引先といった関係者間での共通理解を醸成するため、そのITサービスを復旧させる活動の目標を設定する。

ITサービスを復旧させる活動の目標

目標復旧時間（RTO：Recovery Time Objective)：
事故後、業務を復旧させるまでの目標期間（時間）

目標復旧ポイント（RPO：Recovery Point Objective)：
事故後に事故前のどの時点までデータを復旧できるようにするかの目標時点（時間）

目標復旧レベル（RLO：Recovery Level Objective)：
事故後、業務をどのレベルまで復旧させるか、あるいは、どのレベルで継続させるかの指標

ITサービス継続計画の構成例

経済産業省
Ministry of Economy, Trade and Industry

■IT サービス継続戦略により定められたサービス継続のための要件（組織にとって重要なIT サービスの明確化及び目標とすべき復旧時間・レベル）を踏まえ、これを実現するために必要な、事前対応計画及び緊急事態発生時における具体的な対応方法・計画等を取りまとめる。

事前対応計画

対策実施計画

戦略を実現するための具体的な対策内容を決定し、組織の行動計画として経営者の承認を得る。

【記載項目例】

a) IT サービスの継続要件

b) 実現方法

c) 実施スケジュール

d) 必要な投資

教育訓練計画

IT サービス継続計画の組織内定着化、緊急時における対応能力向上のための教育訓練計画を定める。全体教育、情報システムの切り替えテスト、業務担当者を含めた総合演習などを実施する。

【記載項目例】

a) 教育訓練の対象者と達成目標

c) 教育カリキュラムと実施スケジュール

維持改善計画

IT サービス継続性の継続的な改善に向けた管理プロセスを明確化する。

【記載項目例】

a) 維持改善の目的

b) 維持改善の体制

c) 維持改善方法

（点検時期、点検項目、点検主体）

事後対応計画

緊急時対応計画

緊急事態発生時における情報システムの迅速な復旧・再開に向けた体制及び対応方法を定める。

【記載項目例】

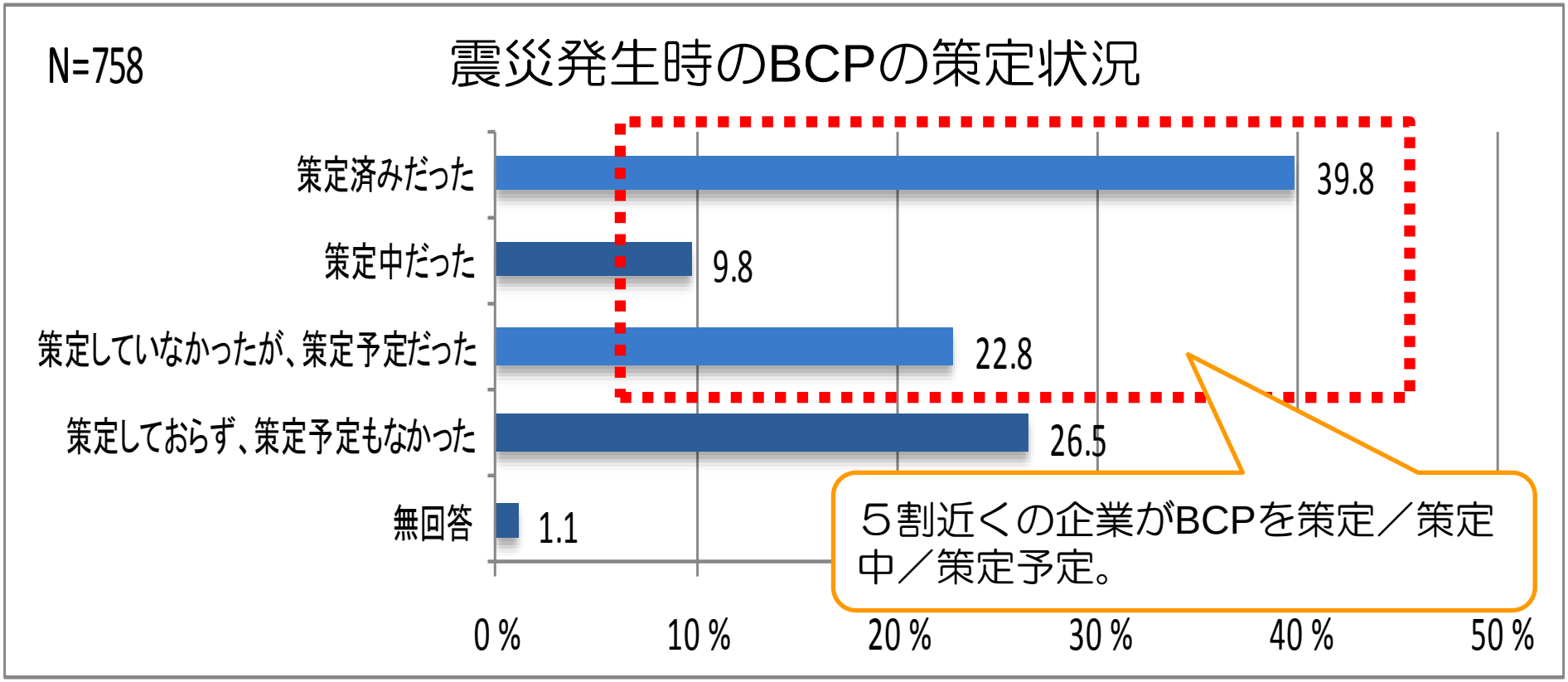
a) 緊急時対応体制

b) 緊急時対応プロセス

c) 緊急時対応手順

震災以前のBCPの策定状況、震災時のBCPの発動状況①

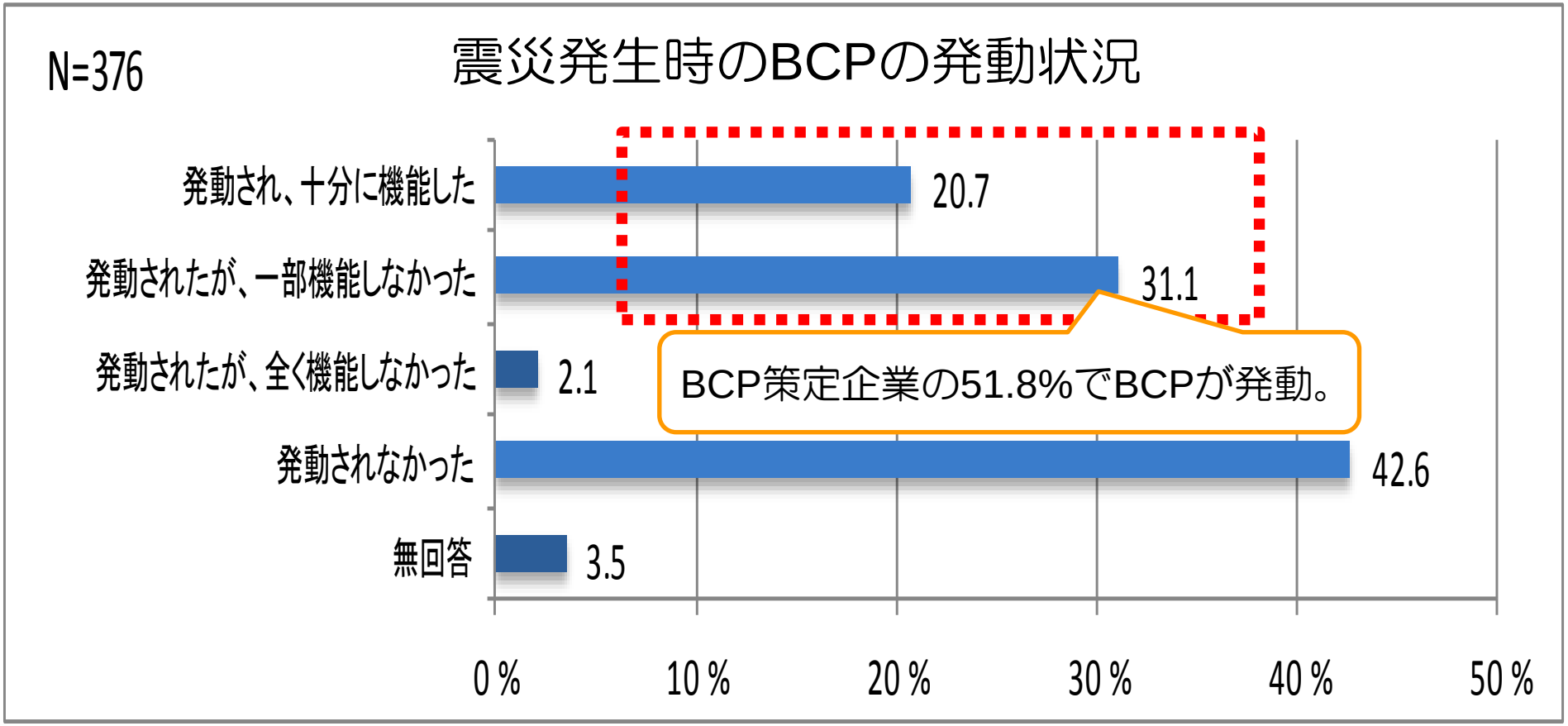
経済産業省
Ministry of Economy, Trade and Industry



出所：経済産業省調査（2011年）

震災以前のBCPの策定状況、震災時のBCPの発動状況②

経済産業省
Ministry of Economy, Trade and Industry



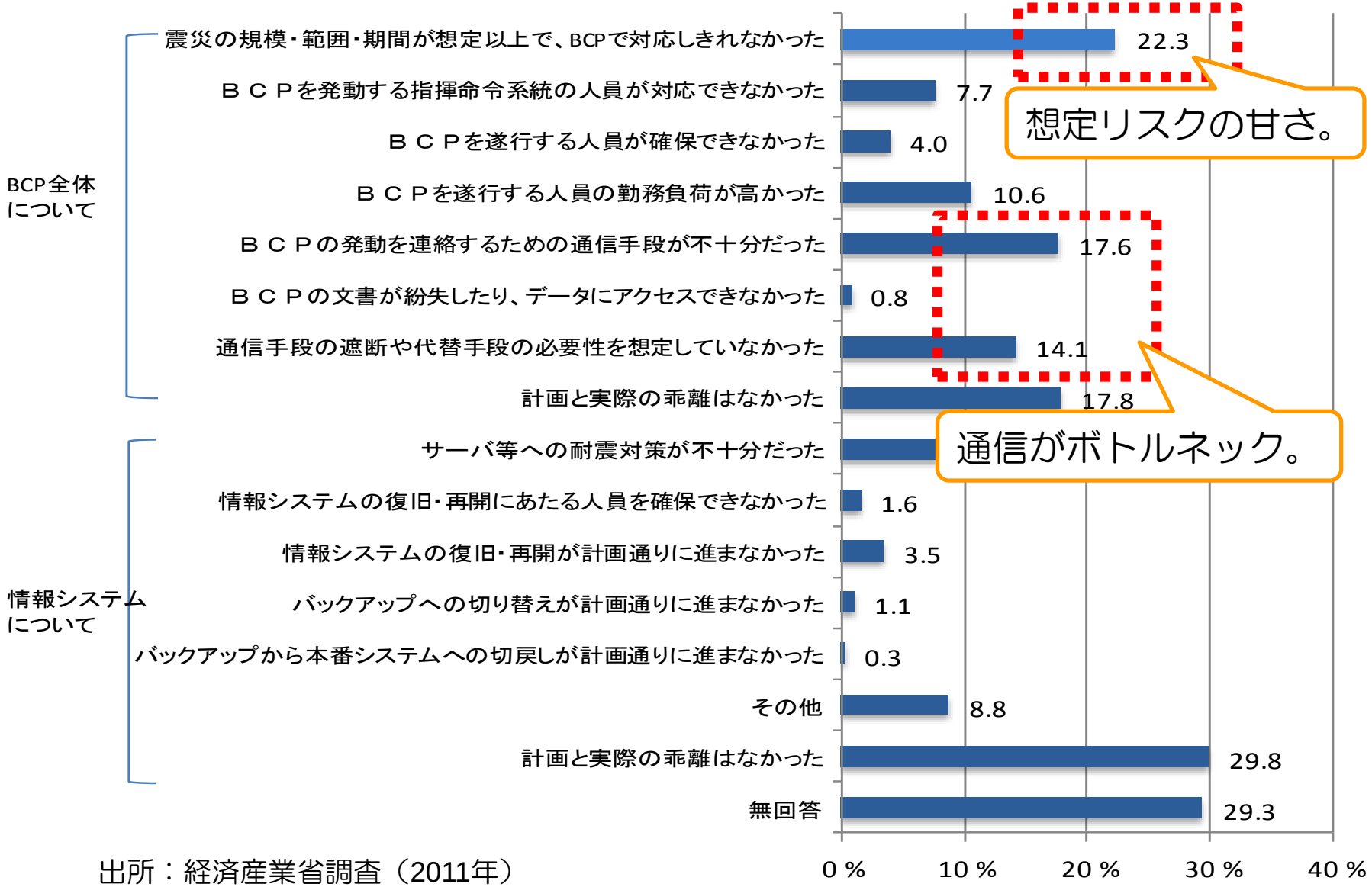
出所：経済産業省調査（2011年）

震災以前のBCPの策定状況、震災時のBCPの発動状況③

経済産業省 Ministry of Economy, Trade and Industry

BCP策定～発動における、計画と実際の乖離

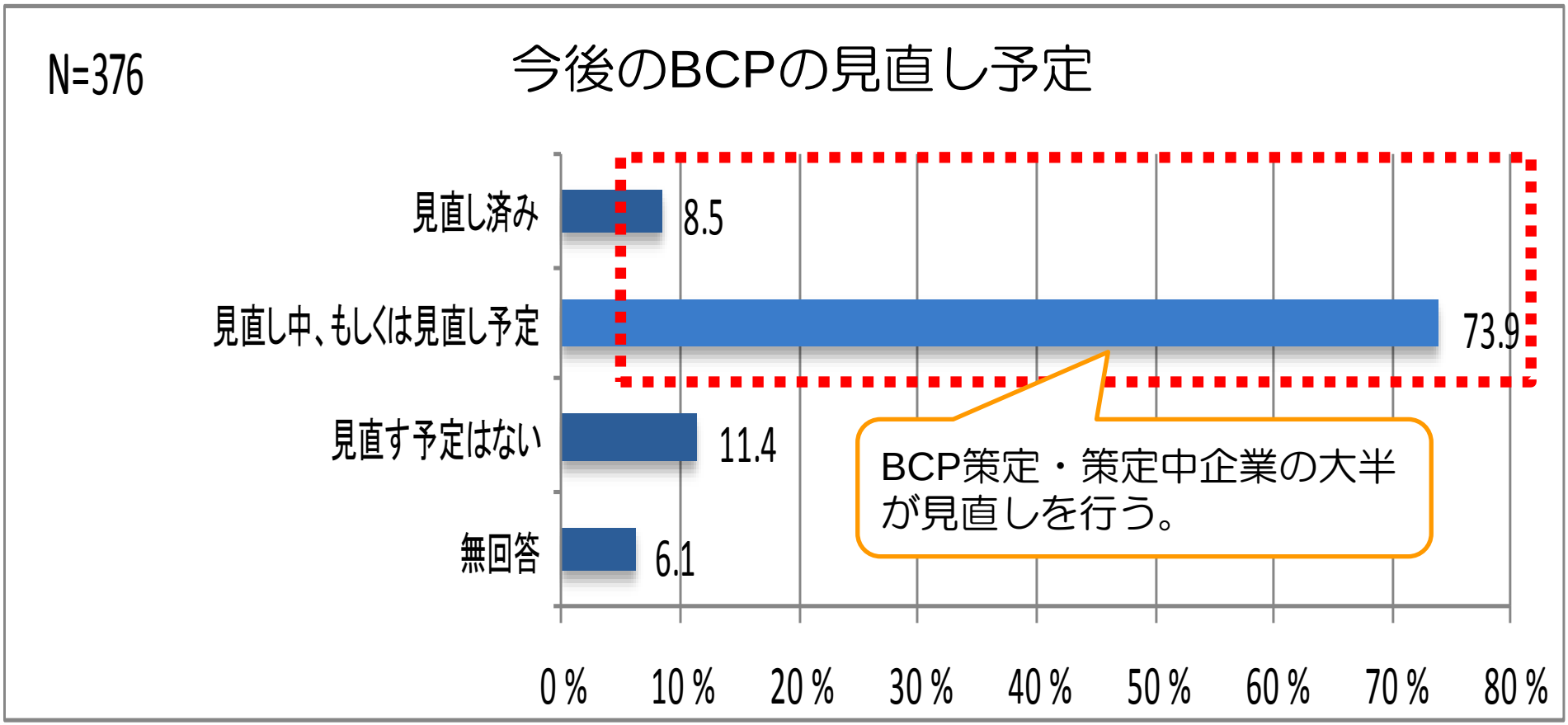
N=376



出所：経済産業省調査（2011年）

震災以前のBCPの策定状況、震災時のBCPの発動状況④

経済産業省
Ministry of Economy, Trade and Industry



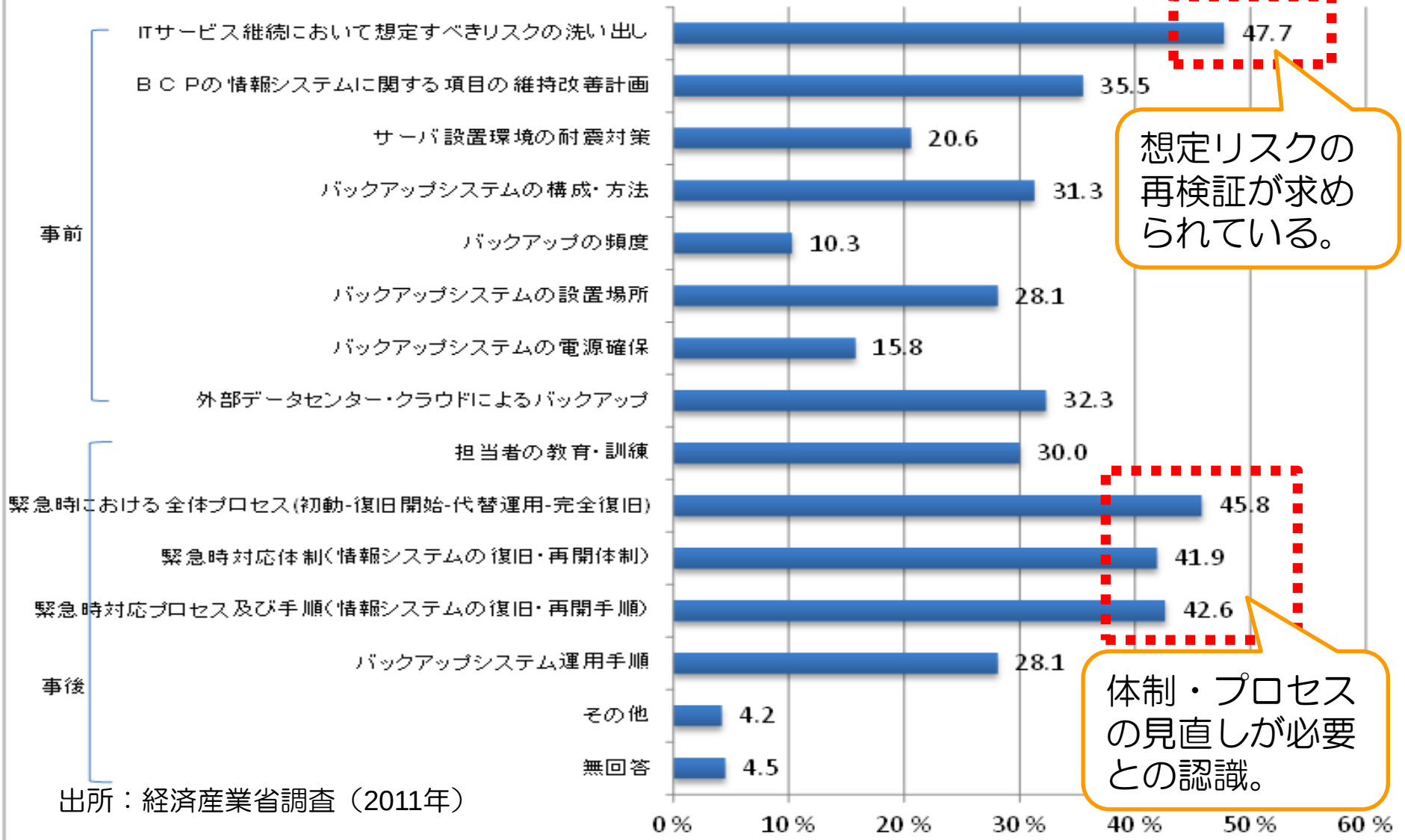
出所：経済産業省調査（2011年）

震災以前のBCPの策定状況、震災時のBCPの発動状況⑤

経済産業省 Ministry of Economy, Trade and Industry

N=310

情報システムに関し、BCPの見直しが必要なもの



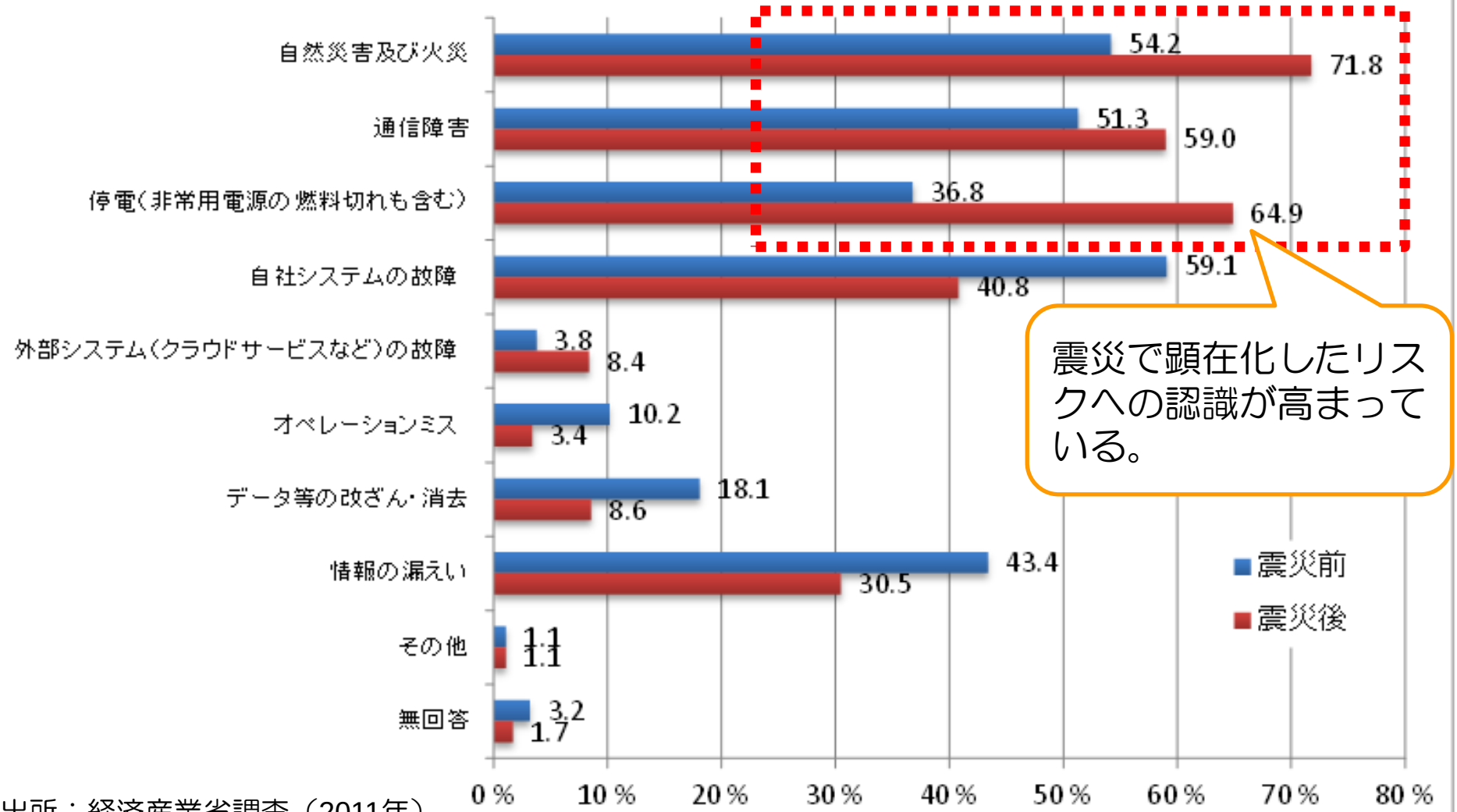
出所：経済産業省調査（2011年）

震災以前のBCPの策定状況、震災時のBCPの発動状況⑥

経済産業省
Ministry of Economy, Trade and Industry

BCPの中で情報システムに関するリスクのうち重視するもの

N=758



震災で顕在化したリスクへの認識が高まっている。

出所：経済産業省調査（2011年）

東日本大震災における教訓(アンケート結果)の反映

経済産業省
Ministry of Economy, Trade and Industry

■IT-BCPの位置づけの整理
⇒BCPの目的、企業が守るべきものを明確にする(企業の業態や規模により、BCPの目的が異なる)
⇒BCPの中のIT-BCPとして体系化

■BIAの重要性
⇒これまでBIAの視点が足りない点を明確にし、想定外の事象はBIAで吸収させる。

■計画停電、長期間にわたる停電への対応
⇒守るシステム、止めてよいシステムの優先度分け
⇒停電対策は技術的対策よりは、ユーティリティや運用の観点で記述

■セキュリティレベルの低下
⇒単なる低下ではなく、機密性、完全性、可用性のバランスを取った対応を提示する。

■その他
⇒安否確認システム、外部サービス利用等のトピックも適宜含める。

国際標準との整合性確保の観点

経済産業省
Ministry of Economy, Trade and Industry

ISO/IEC 27031	ITサービス継続ガイドライン(現行)	対応案
ICT Readiness for Business Continuity (IRBC)に焦点を当てている。	ビジネス継続を重視し、リスクの洗い出しから詳しく記述している。	基準ではICT Readinessに焦点をあてるが、ガイドラインではリスクの洗い出しから記述する。
情報セキュリティインシデントも脅威に上げている。	あまり考慮していない。一方で、セキュリティ対策との矛盾点について若干の考察を行っている。	情報セキュリティインシデントも含めるが、基本的には深堀せず27001を参照するにとどめる。
リスク分析手法としてはBusiness Impact Analysys(BIA)を示しているが詳細は記載されていない。	リスクの例示はされているが、分析手法については特に明示していない。	BIA等を含めリスク分析手法を例示する。
インシデント発生時のプロセスとしてDetectionが追加されている。	インシデント発生時のプロセスに関する記載はなく、Detectionは記載されていない。	インシデント発生時のプロセスを追加しDetectionを記載する。もしくは現行案ママ。
技術的対策についての記述が少ない。	技術的対策についての細かい記述がある。	技術的対策についてガイドラインでは記述するが、基準からは削除する。

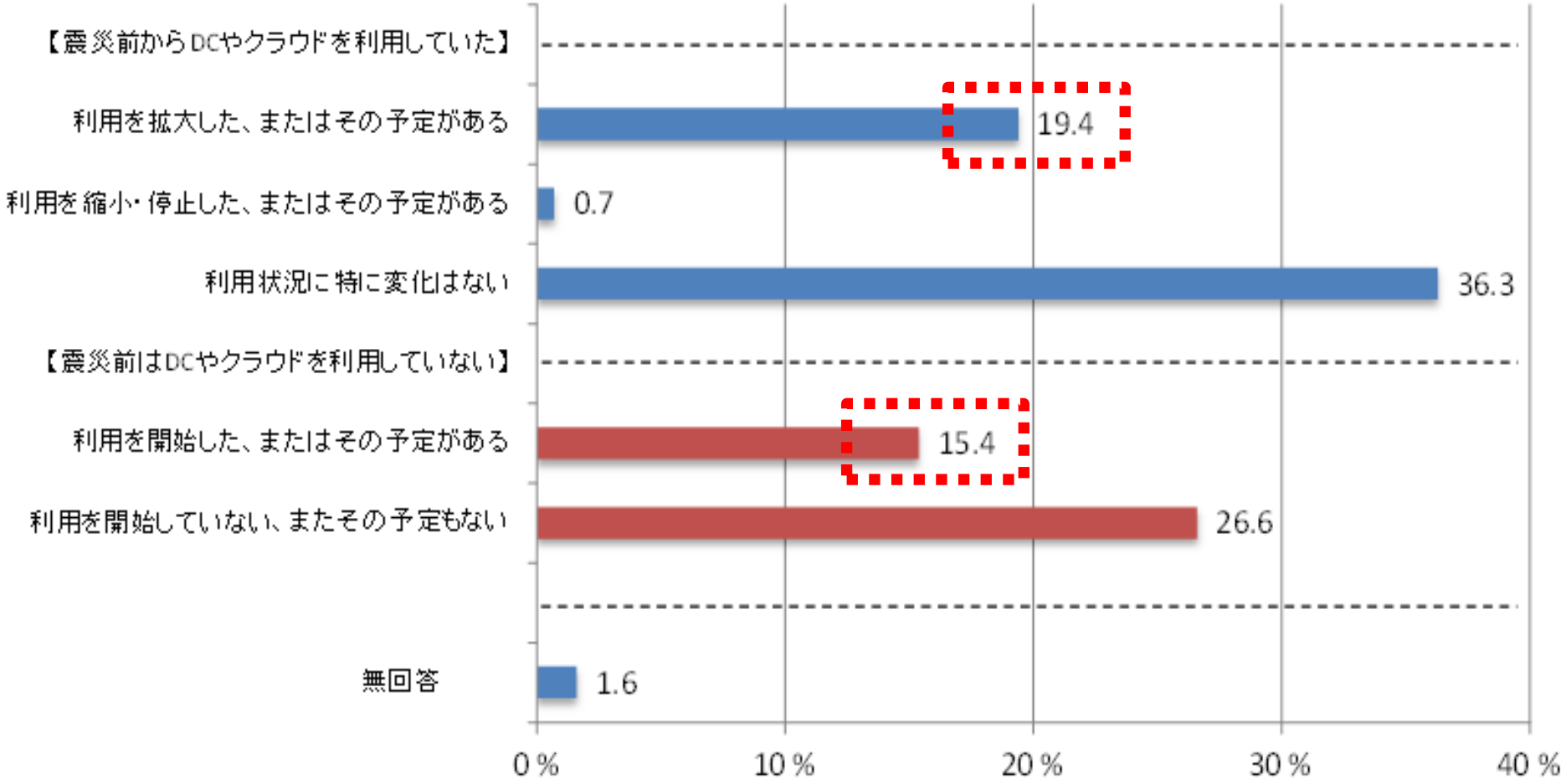
ITサービス継続マネジメントガイドライン整備の効果

- 組織におけるITサービスの企画、開発、調達、導入、運用、保守などに携わる部門や担当者が、ITサービス継続ガイドラインを用いる事で、事業継続マネジメントに必要なITサービス継続を確実にするための枠組みを構築でき、「想定外」の事態が発生したとしても、適切な対応を取ることが可能となる。

外部データセンターやクラウドの利用について①

経済産業省
Ministry of Economy, Trade and Industry

N=758　外部データセンターやクラウドの利用状況・利用意向



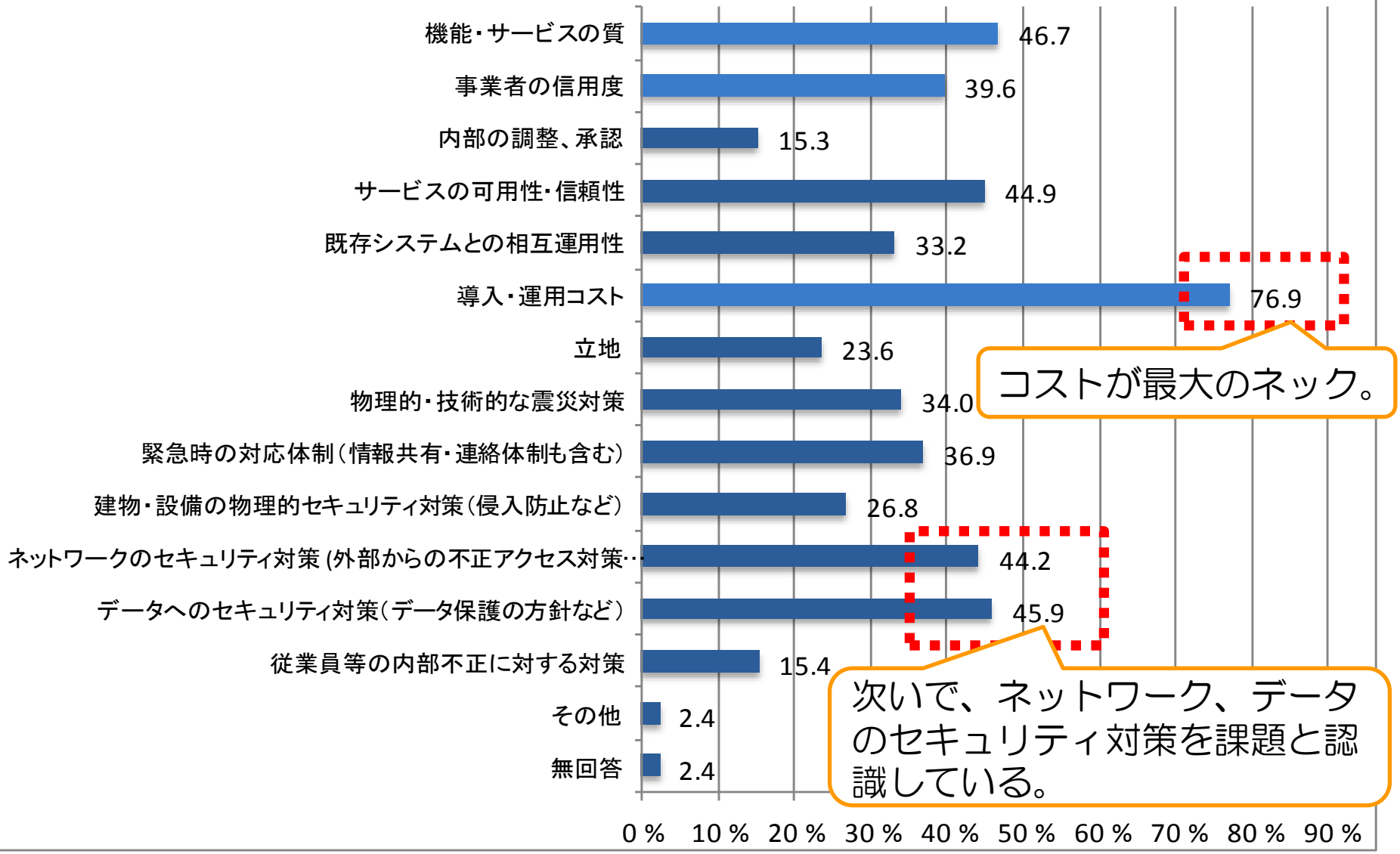
出所：経済産業省調査（2011年）

外部データセンターやクラウドの利用について②

経済産業省
Ministry of Economy, Trade and Industry

外部データセンターやクラウドの利用の課題

N=758

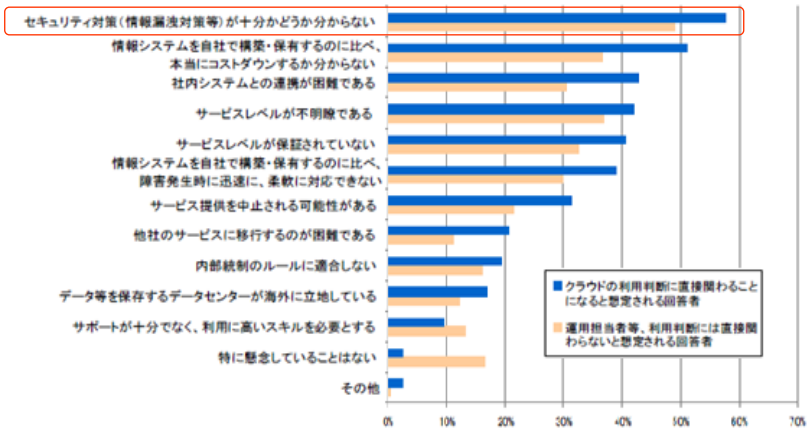


出所：経済産業省調査（2011年）

クラウドセキュリティマネジメントガイドライン策定の背景

経済産業省 Ministry of Economy, Trade and Industry

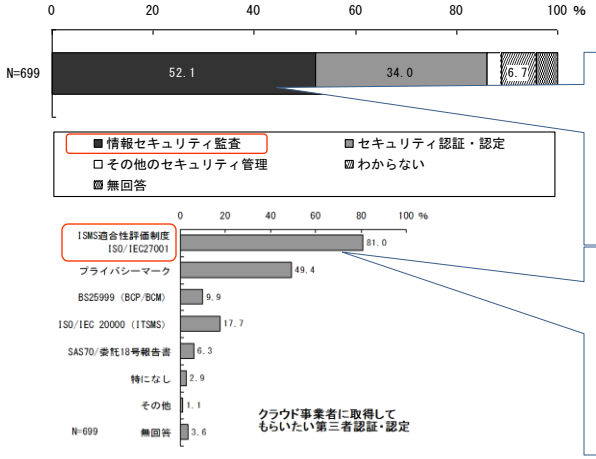
クラウド利用者の不安



＊「高度情報化社会における情報システム・ソフトウェアの信頼性及びセキュリティに関する研究会」（経済産業省2009年3月）

クラウド利用においてセキュリティ上の不安が払拭できていない

クラウド事業者への要求



半数の利用者が，クラウド事業者には情報セキュリティ監査による，具体的な報告を望んでいる

利用者が事業者にJIS Q 27001ベースのセキュリティ管理を望むのは，利用者組織と同様のセキュリティ体制を望んでいるため

＊「クラウドサービスの情報セキュリティ監査に関するアンケート調査報告書」（経済産業省2010年1月）

クラウド利用者はクラウド事業者に，情報セキュリティ監査及びJIS Q 27001ベースのセキュリティ管理を望んでいる。

「情報セキュリティ」および「事業者におけるシステム運用」が見えないことに関する不安を「見える化」する

クラウド利用者のための情報セキュリティマネジメントガイドラインの策定

- 利用者視点による セキュリティリスクの 共通認識の形成
- 事業者選択における 基準として利用できる 対策標準
- 情報セキュリティ監査による利用者と事業者の 信頼関係の構築

クラウドセキュリティマネジメントガイドラインについて

経済産業省
Ministry of Economy, Trade and Industry

目的

◆本ガイドラインを情報セキュリティ管理，及び情報セキュリティ監査に活用することにより，クラウド利用者とクラウド事業者における信頼関係の強化に役立てることを目的とする。

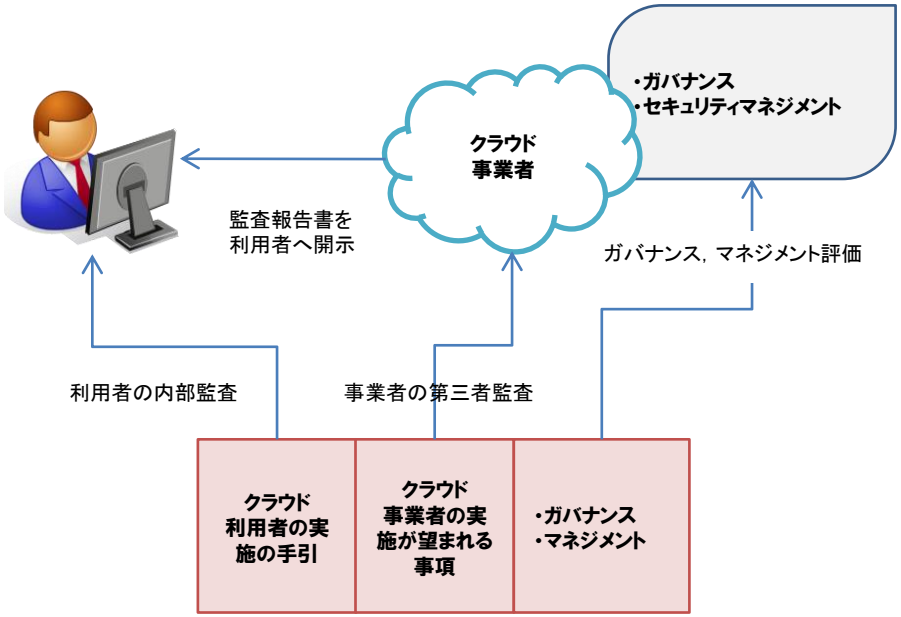
適用範囲

◆本ガイドラインは，組織事業の基礎を成す情報資産の多くを，外部組織であるクラウド事業者が提供するクラウドサービスに委ねようとする組織が，JIS Q 27002（実践のための規範）に規定された管理目的を達成するための管理策を実施しようとする場合を想定している。

特徴

◆全面的にクラウドサービスを利用する際のJIS Q 27002（実践のための規範）の管理目的達成という究極的な状況を想定することにより，クラウドサービスの利用において変化するシステム環境，責任の所在，事故や事象の判断基準を明確にする。

◆クラウドサービスを全面的に利用することにより生ずるリスクの変化に対応するため，JIS Q 27002（実践のための規範）の管理策に，「クラウド利用者のための実施の手引」と，「クラウド事業者の実施が望まれる事項」を追加している。



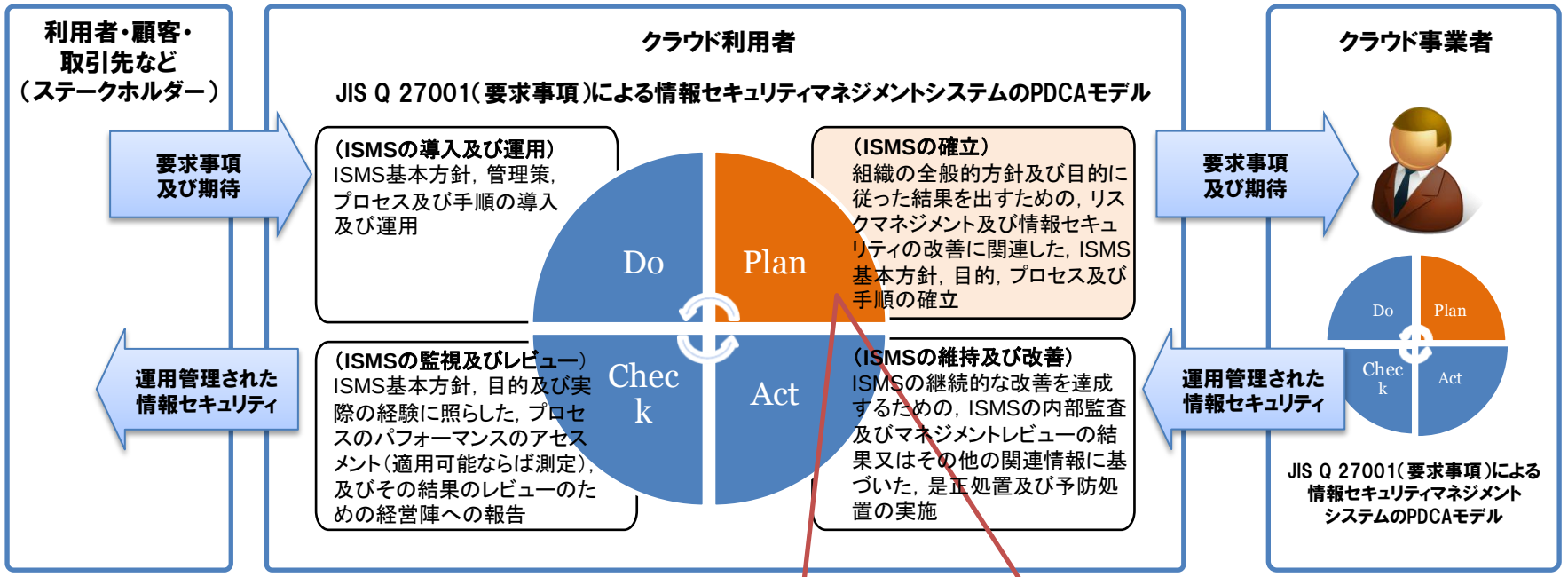
目次構成

経済産業省
Ministry of Economy, Trade and Industry

•本ガイドラインの箇条5～15は，クラウド利用者がJIS Q 27002（実践のための規範）の箇条5～15の管理策を実施するための補足として活用できる。
•参考として附属書Aは，クラウドサービス利用に係るリスクを例示し，附属書Bは，クラウドサービス利用におけるリスクアセスメントの実施例の一つを示す。

クラウドサービス利用に係る管理策の選択

経済産業省
Ministry of Economy, Trade and Industry

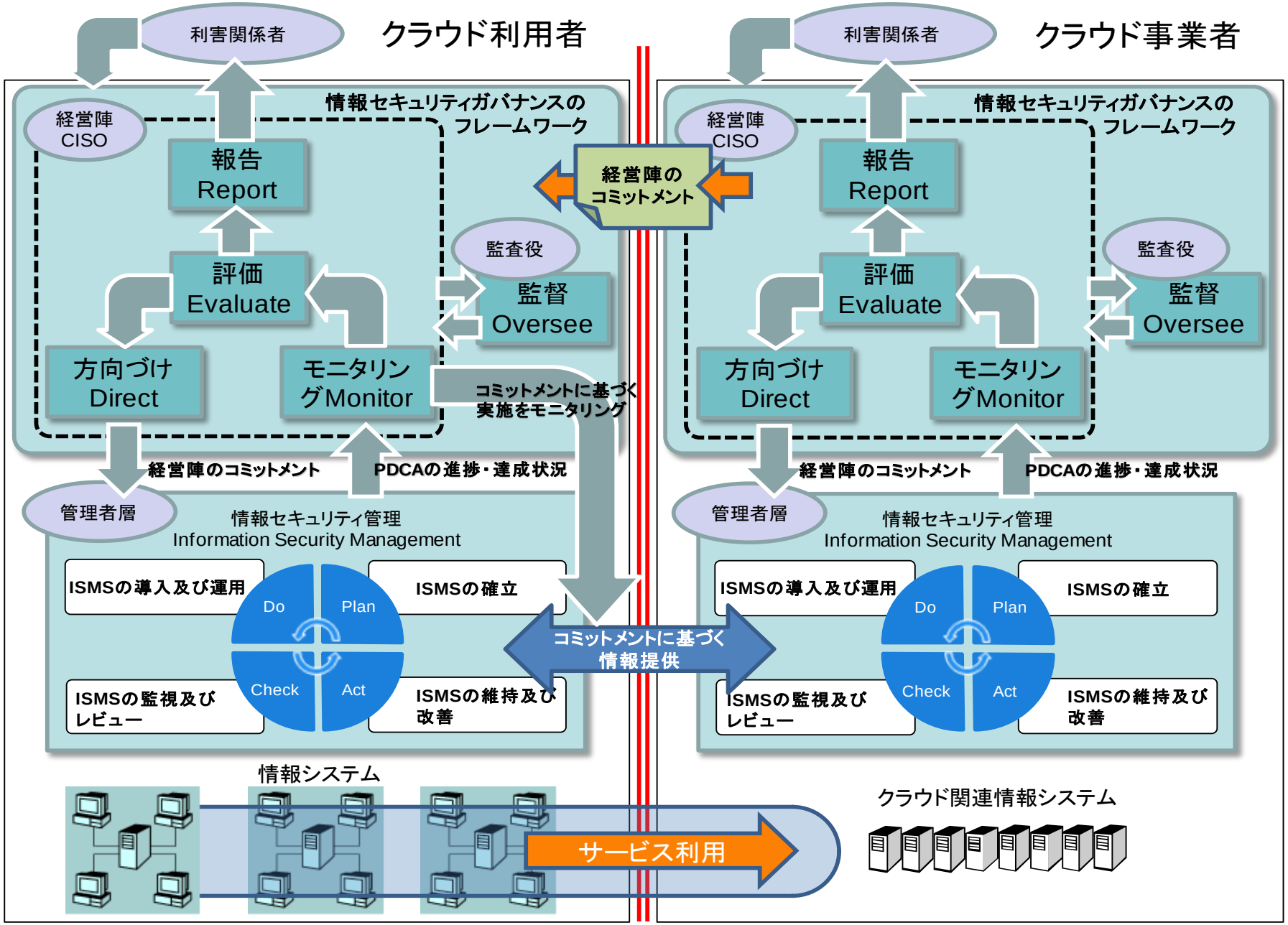


リスクアセスメント	クラウドコンピューティング環境における管理と責任の変化の検討
リスク受容レベル	組織のリスク受容レベルとの比較
管理策の選択	JIS Q 27002（実践のための規範）などから選択
責任の明確化	クラウド利用者と事業者双方による管理策の実施

クラウドサービス利用のための管理策の実施の手引があれば，マネジメントシステムを維持しながら，クラウドサービスを利用した適切な情報セキュリティ管理が容易に行える

クラウドサービス利用における情報セキュリティガバナンス及び情報セキュリティマネジメント

経済産業省
Ministry of Economy, Trade and Industry



国際規格化の経緯

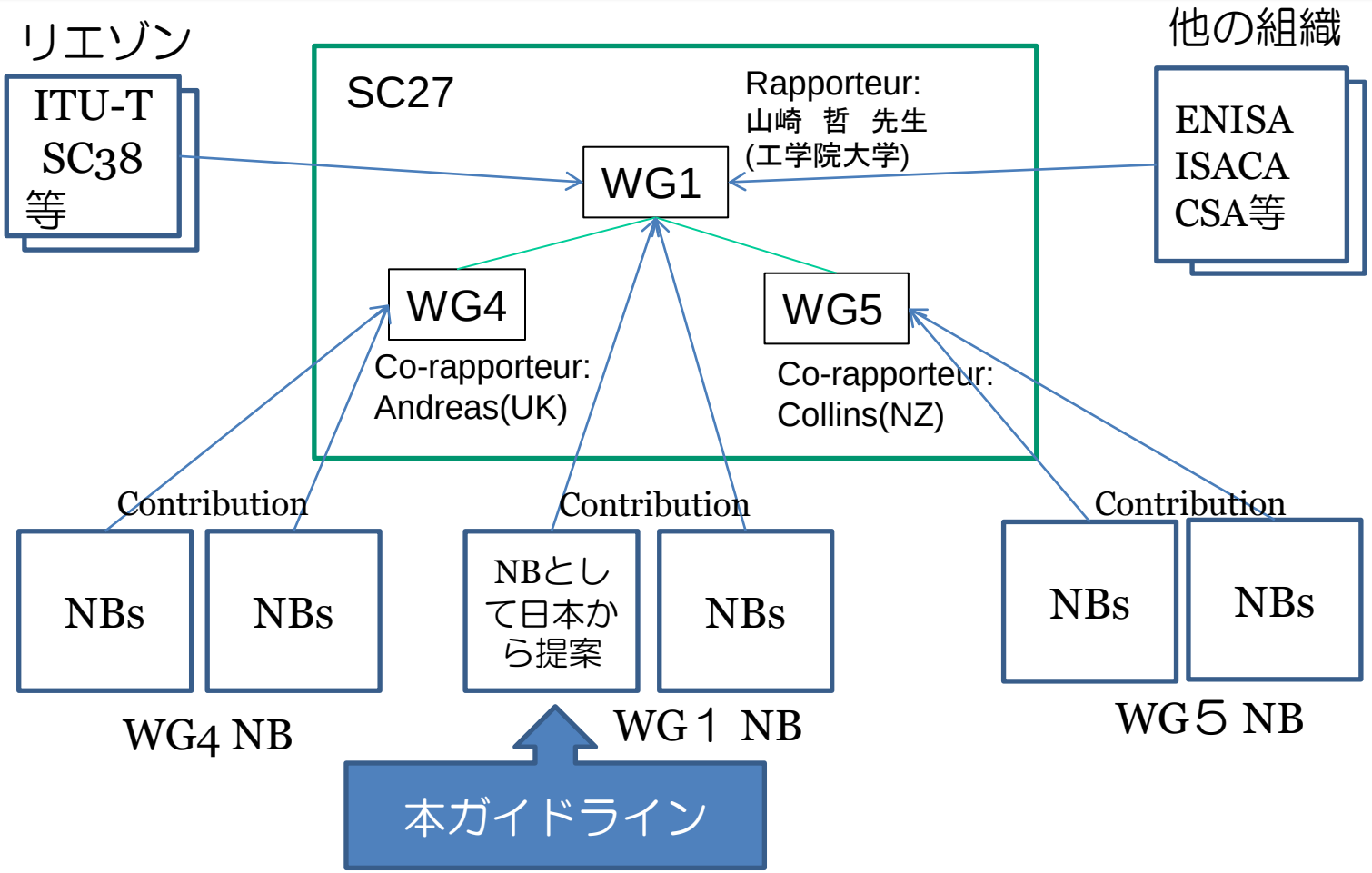
経済産業省
Ministry of Economy, Trade and Industry

1. 日本よりCloud computing servicesにおける情報セキュリティマネジメントを提案
   （1）本ガイドラインを基本に提案
   （2）SC27/WG1のBerlin会議（2010年10月）におけるプレゼンテーションにより各国への理解を求める
2. Cloud computing servicesにおけるSecurity and Privacyプロジェクトの Study period開始が決定
   （1）WG1のInitiateによりStudy periodを開始
   （2）WG4のSecurity Technology及びWG5のPrivacy Technology との協力
3. 情報セキュリティマネジメント分野の日本初プロジェクト開始
   （1）SG27/WG1,WG4,WG5のSingapore会議（2011年4月）においてStudy period結果を審議
   （2）SC27/WG1は、提案した27017　NWIP(New Work Item Proposal)（N10029）として承認

Cloud Computing Security and Privacyプロジェクトの体制

経済産業省
Ministry of Economy, Trade and Industry

- WG1が6ヶ月間のStudy periodを主導し、ラポーター（取り纏め役）は日本人が担当
- Wg4のSecurity technology及びWG5のPrivacy Technologyが参加して実施
- ＩＴＵ－Ｔ，ＳＣ３８，ＥＮＩＳＡ，ＩＳＡＣＡ，ＣＳＡ等ともリエゾン関係



今後のスケジュール

経済産業省
Ministry of Economy, Trade and Industry

- Base ISO/IEC 27002
  - –ISO/IEC 27002 New Revised Version
- Project Editors
  - –Japan : Satoru Yamasaki
  - –US:　Marlin Pohlman (CSA)
- Schedule
  - –WD (Working Draft) 2011-10
  - –CD(Commitee Draft)　2012-10
  - –DIS (Draft International Standards) 2013-04
  - –IS (International Standards)　2013-10

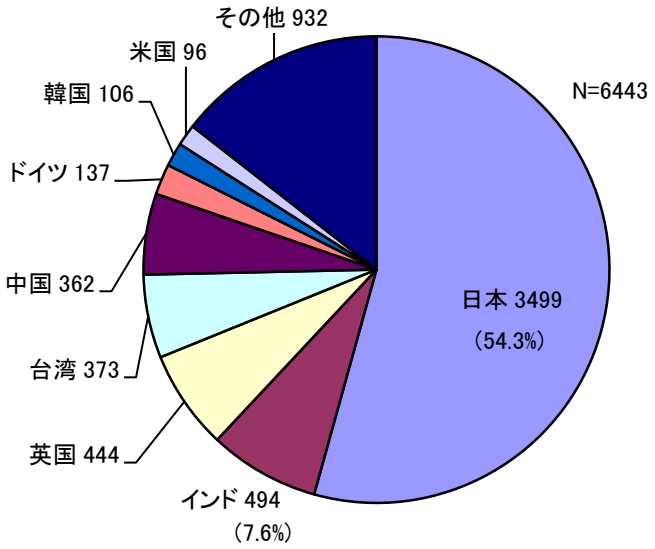
日本企業にとってのメリット

経済産業省
Ministry of Economy, Trade and Industry

- 本ガイドライン※は、ISO/IEC27001Annexに準拠して作成。
  - →目次等の構成を合わせ、管理目的等はISO/IEC27001Annexをそのまま準用。
  - →全面的にクラウドサービスを利用する際の管理目的達成という究極的な状況まで想定。
  - →差分のみの情報セキュリティ監査が可能となるため、クラウド環境における セキュリティ確保コストが削減できる。
- ISMS(ISO/IEC27001)の取得は日本が世界の取得数の半数以上を占める。
  - →すでにISMSを多数取得している我が国企業にとっては、現状のISMS(ISO/IEC27001) に準拠した基準ができる方が有利になる。

※本ガイドラインは、以下のURLからダウンロードできます。
http://www.meti.go.jp/policy/netsecurity/downloadfiles/cloud_security_guideline.pdf

世界のISMS取得状況



（出所：JIPDEC資料より）　（2010年6月時点）

クラウドセキュリティの不安を払拭し、安全なクラウド利用時代へ

- 本ガイドラインを利用することにより、クラウド利用者とクラウド事業者間のセキュリティを確保するためのコミュニケーション手段の提供

クラウド時代における情報セキュリティ監査制度の強化

- クラウドコンピューティングの利用視点に立ったセキュリティリスクの明確化

クラウドセキュリティマネジメントガイドライン整備の効果

- クラウド利用者が、クラウドサービス利用の際に、情報セキュリティ対策の観点から本ガイドラインを活用することで、より一層のクラウドサービスの利用を促進する。

経済産業省
Ministry of Economy, Trade and Industry

ご清聴ありがとうございました。