JPCERT/CC利用者アンケート
調査結果の概要

2002年5月

JPCERT/CC (コンピュータ緊急対応センター)

はじめに

インターネットは、今や我々のビジネスや生活を支える重要な社会インフラに成長しました。その一方、インターネットの役割が不可欠となるにつれて、その脆弱性が問題化しつつあります。クラッカーによる情報システムへの不正侵入や情報詐取、改ざん、コンピュータウイルスによる被害は、従来は企業や行政等の組織内に閉じたものでしたが、最近では取引先や消費者、国をも巻き込んだ大規模なトラブルへと発展する可能性があるのです。

コンピュータ緊急対応センター（JPCERT/CC）は、インターネットを介して発生する、侵入やサービス妨害等のコンピュータセキュリティインシデントについて、日本国内のサイトに関する報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討と助言などを、技術的な立場から行なっています。

JPCERT/CCでは、我が国における今後のCSIRTのあり方を検討するための基本情報として、株式会社三菱総合研究所に委託して、JPCERT/CCの利用者の利用状況やニーズに関するアンケート調査を実施いたしました。本調査の成果を公開することで、本アンケート調査にご協力くださいました皆様へのお礼に代えさせて頂きます。本調査が、有意義かつ発展的な検討のきっかけとなることを祈念いたします。

平成14年5月　コンピュータ緊急対応センター

1.1 調査の枠組み

■調査目的

インターネットの利用環境や利用者層の変化に伴い、JPCERT/CCの発信するセキュリティ関連情報などについて、JPCERT/CC利用者の方々の要望を明らかにする

■調査対象

JPCERT/CCのメーリングリストに登録している、セキュリティ関連情報の利用者層、もしくはそれに準じる層

■調査手法

・Webアンケートを開示し、JPCERT/CCのメールマガジンを通じてアンケート回答者を募集
・回答者は指定のURLにアクセスし、提示されたアンケートに回答

■調査期間

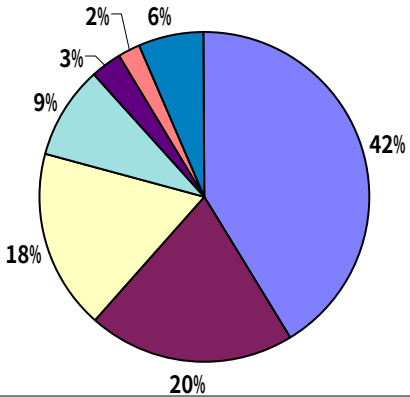
平成14年2月20日（水） ー 3月1日（金） （10日間）

■回答件数

有効回答　　808件

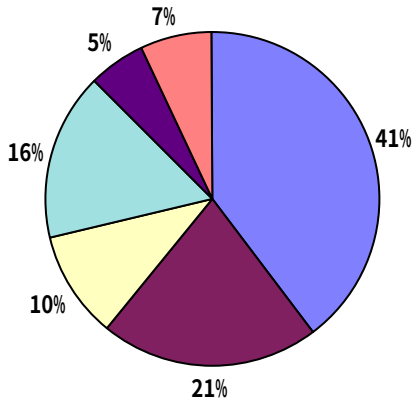
1.2 回答者属性

所属組織の種別



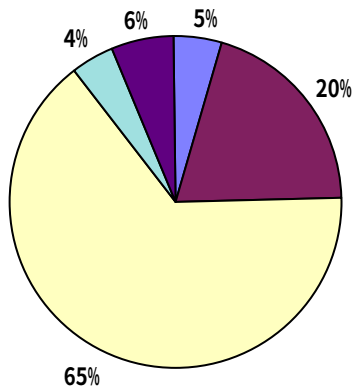
- 情報サービス事業者（ソフトウェアベンダを含む）
- 一般企業
- 教育・研究組織
- 通信サービス事業者
- ハードウェアベンダ
- 行政組織
- その他

所属組織の規模



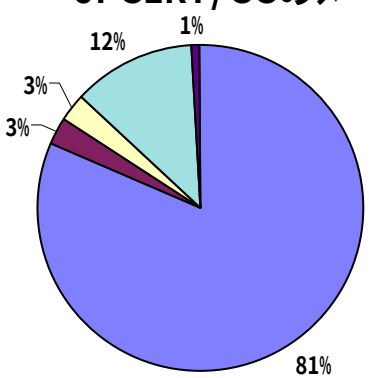
- 100人未満
- 100人－500人未満
- 500人－1,000人未満
- 1,000人－5,000人未満
- 5,000人－10,000人未満
- 10,000人以上

所属組織内での役職



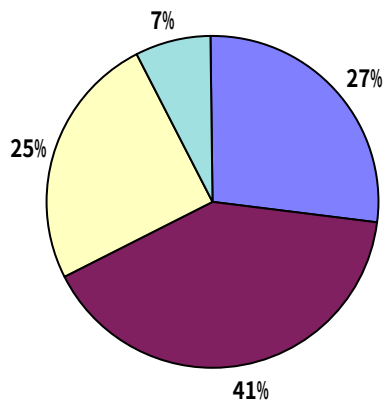
- 経営者
- 管理職
- 一般職員
- 学生
- その他

JPCERT/CCのメーリングリストへの登録



- 自分のメールアドレスで登録している（会社用または個人用）
- グループアドレス（メーリングリスト）で登録している
- 登録していないが、転送されたものを読んでいる
- 登録していない
- わからない

ネットワーク管理への係わり方



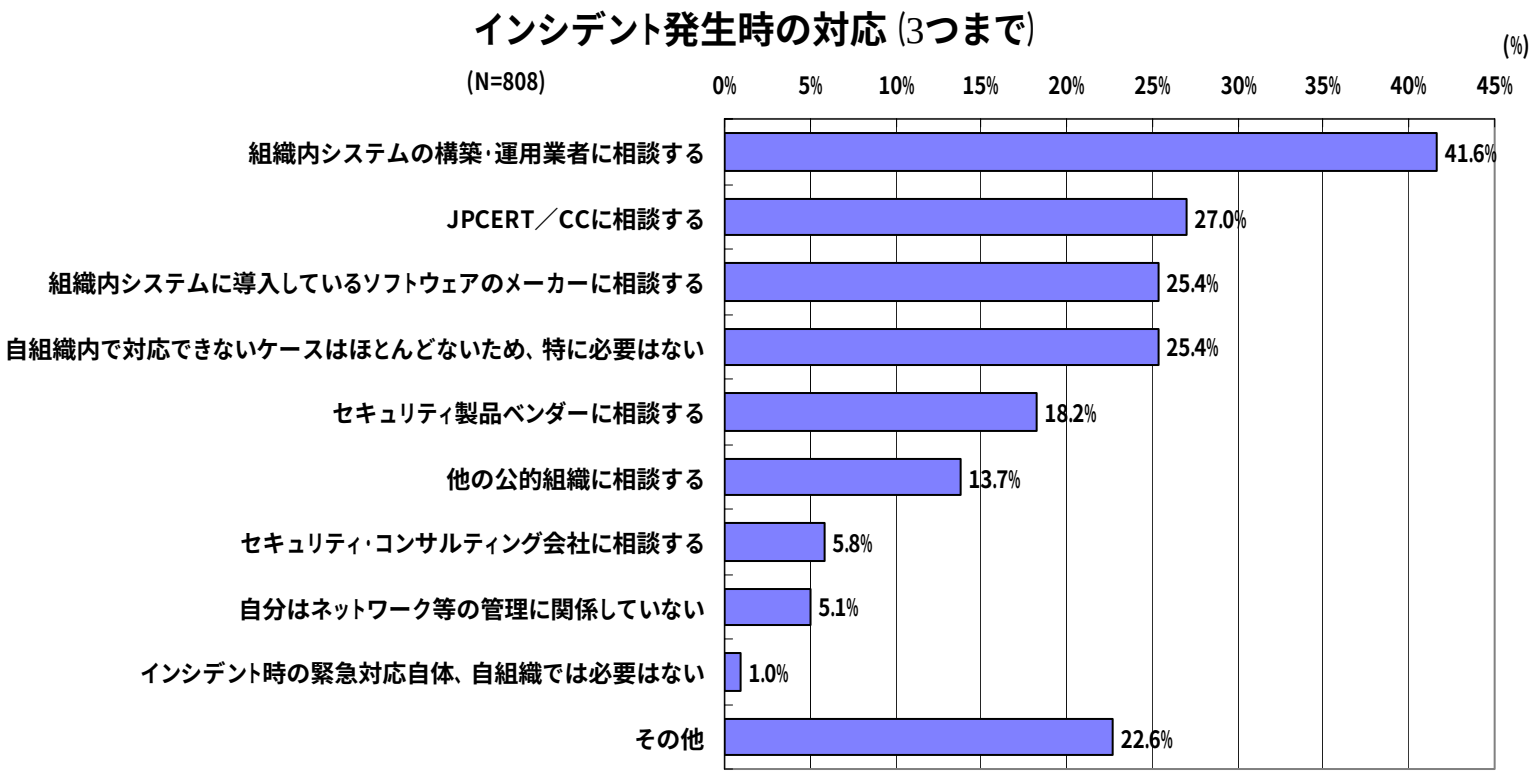
- 責任者をしている
- 業務として担当している
- 業務として担当していないが、係わっている
- 係わっていない

2.1 インシデント発生時の対応

■自らの組織内で対応できないインシデントが発生した時の対応としては、「組織内システムの構築･運用業者に相談する」との回答が突出している。

■JPCERT/CCは、インシデント発生時の相談相手として、組織内システムの構築･運用業者に次ぐ支持を集めており、ソフトウェアのメーカーとほぼ同程度の位置にある。

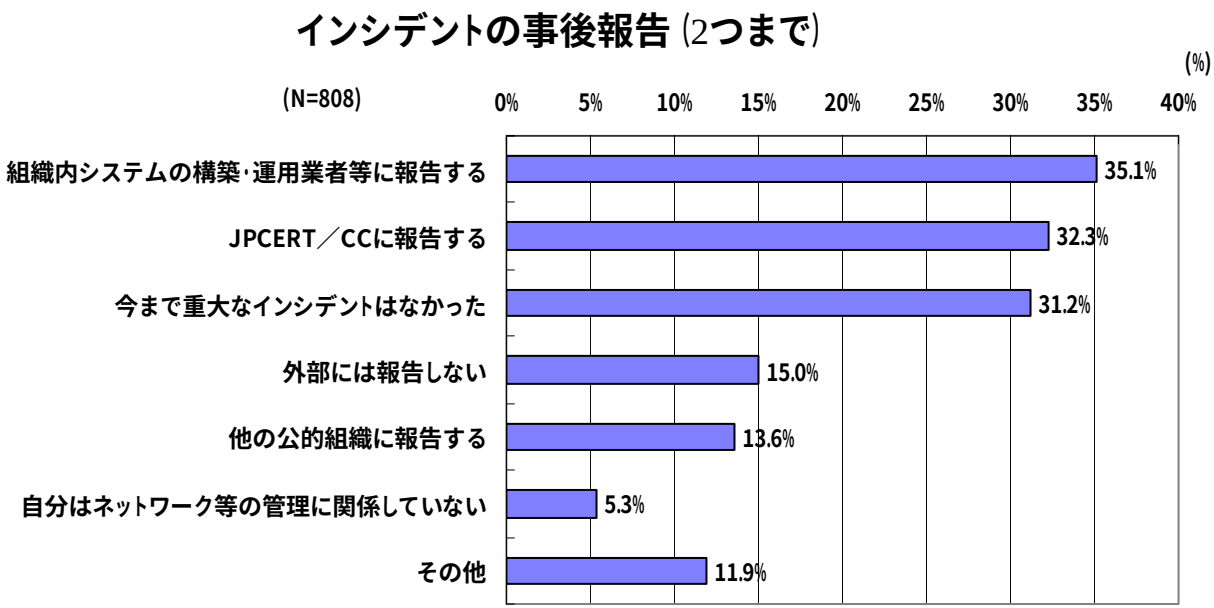
■「自組織内で対応できないケースはほとんどないため、特に必要ない」とする回答も多い。



2.2 インシデントの事後報告

■JPCERT/CCのメーリングリスト登録者を主体とした回答者のうち、インシデントの事後報告先としてJPCERT/CCを挙げた人は3割程度であった。これは、「今まで重大なインシデントはなかった」「自分はネットワーク等の管理に関係していない」とする回答を除くと、半数近くに相当する。

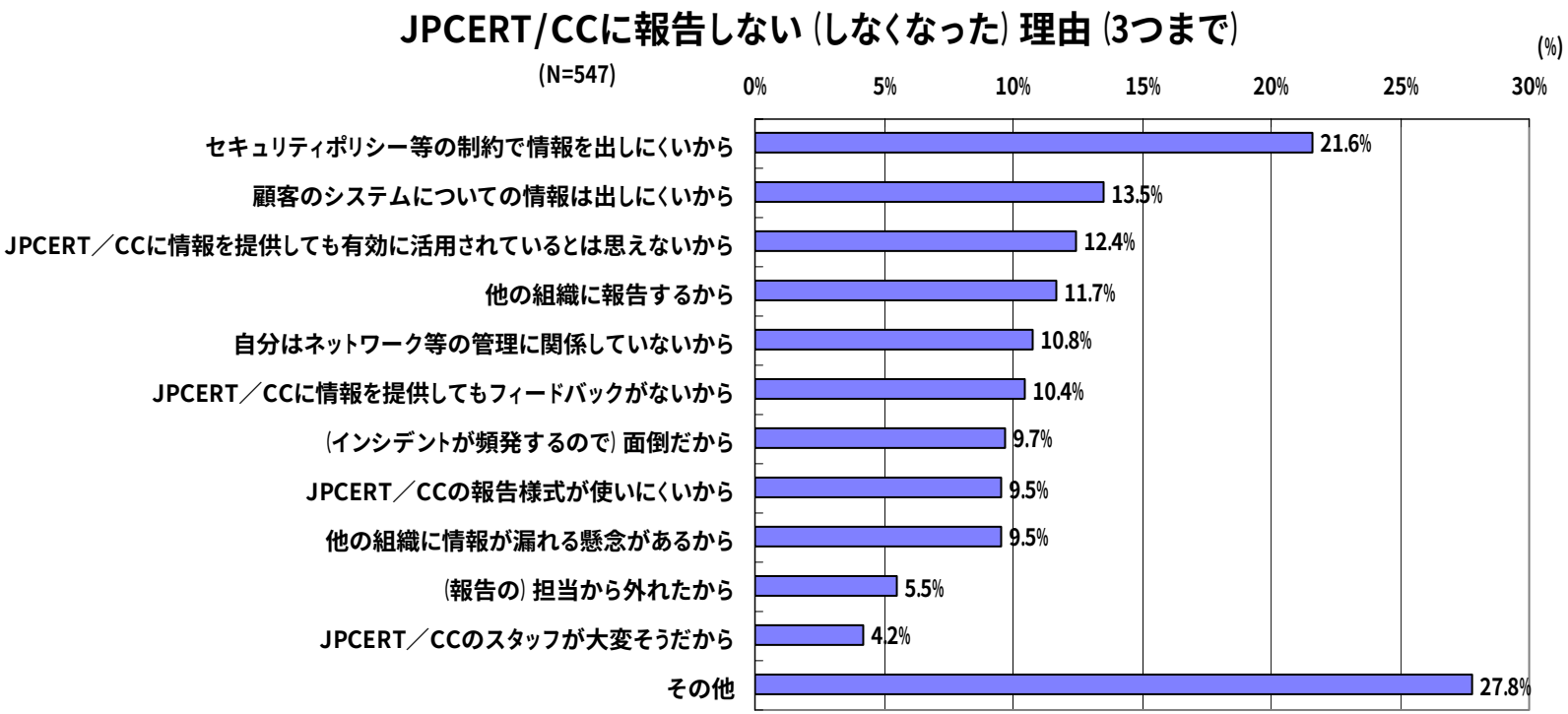
■回答者の所属組織種別に見ると、通信サービス事業者は、他の業種に比べ「今まで重大なインシデントはなかった」とする回答が極端に少なく、インシデントが日常的に発生している現状がうかがえる。



2.3 JPCERT/CCに報告しない（しなくなった）理由

■JPCERT/CCにインシデントの事後報告をしない（しなくなった）理由として、約2割の回答者が「セキュリティポリシー等の制約で情報を出しにくい」を挙げた。この傾向は、今後セキュリティポリシーが普及するとともに、さらに顕著になると予想される。

■「その他」については、「今まで重大なインシデントがなかった」「（回答者自身が）報告する立場にない」「面倒だから」とする回答が多い。また、「JPCERT/CCに報告するということを知らなかった」とする回答も見られた。

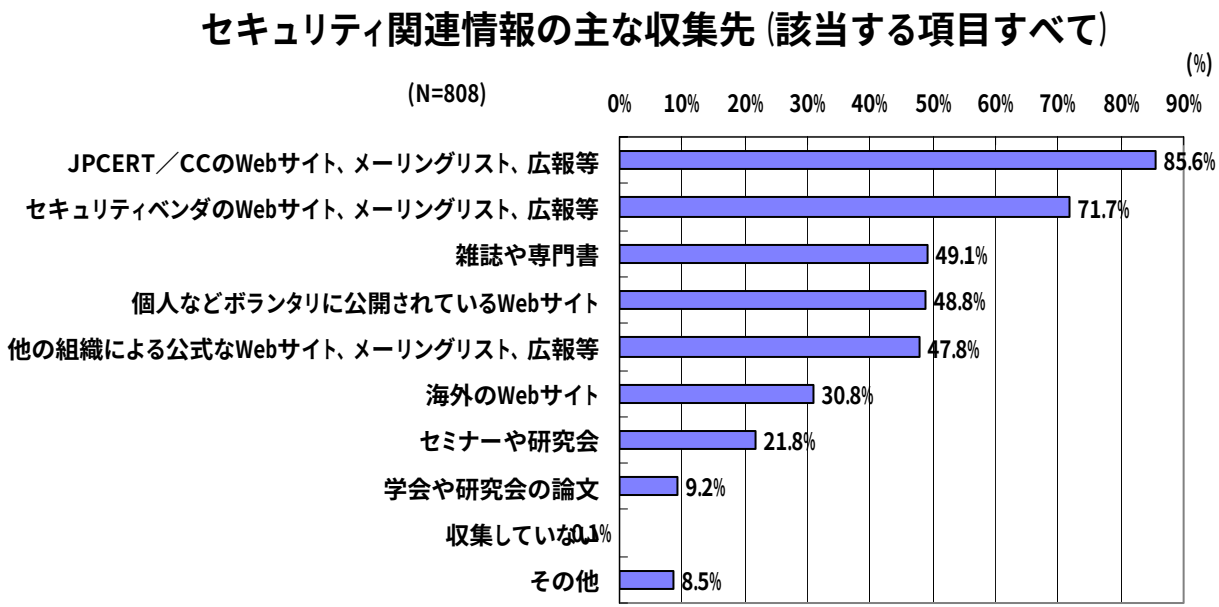


3.1 セキュリティ関連情報の主な収集先

■セキュリティ関連情報の主な収集先としてJPCERT/CCが8割超の支持を集めており、セキュリティ関連情報の情報源として認知されていることがわかる。

■JPCERT/CCのメーリングリスト登録状況別に見ると、登録者の92%、非登録者の47%がJPCERT/CCを主な情報収集先として挙げている。

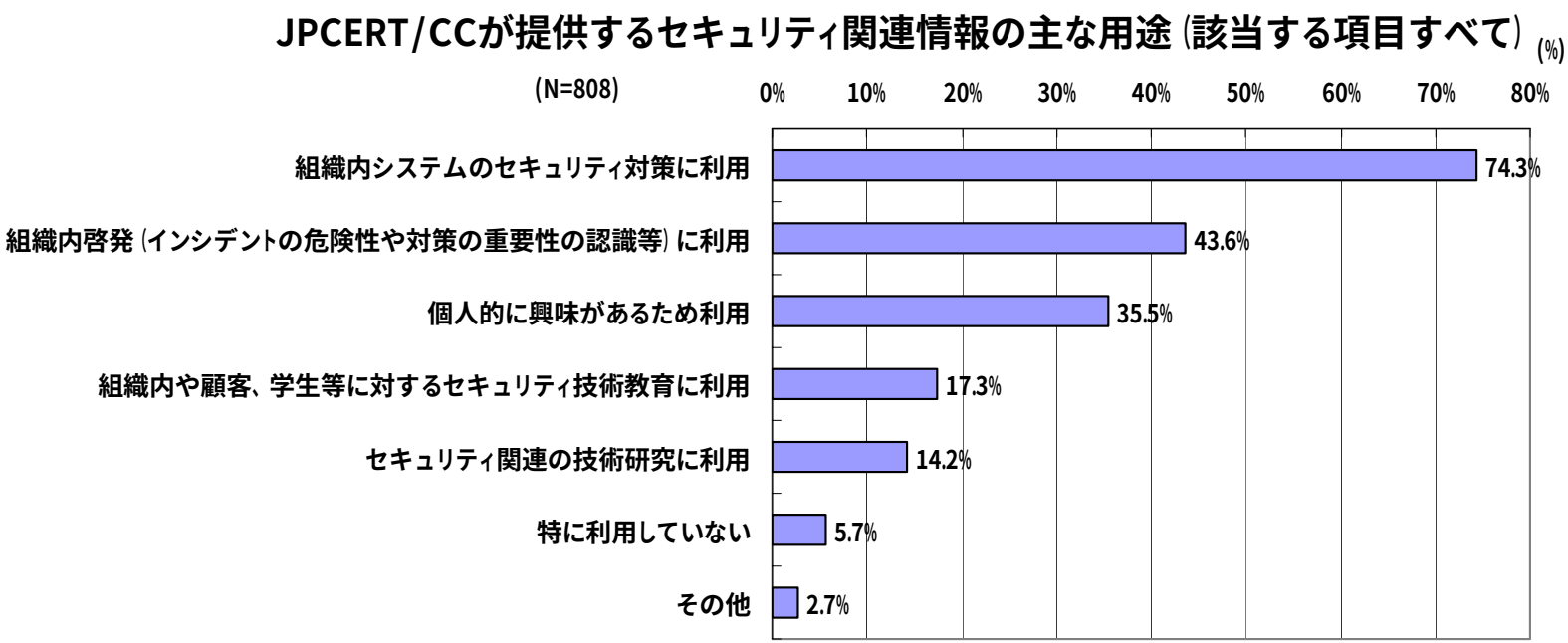
■「個人などボランタリに公開されているWebサイト」を挙げる割合も5割近い。



3.2 セキュリティ関連情報の主な用途

■JPCERT/CCが公開しているセキュリティ関連情報の主な用途として、「組織内システムのセキュリティ対策」が突出している。一方、「セキュリティ技術教育」「セキュリティ関連の技術研究」は比較的支持が少ない。つまり、利用者はJPCERT/CCの情報を実際的な用途に活用している傾向がうかがえる。

■また、「組織内啓発（インシデントの危険性や対策の重要性の認識等）」「個人的に興味がある」も比較的多い。

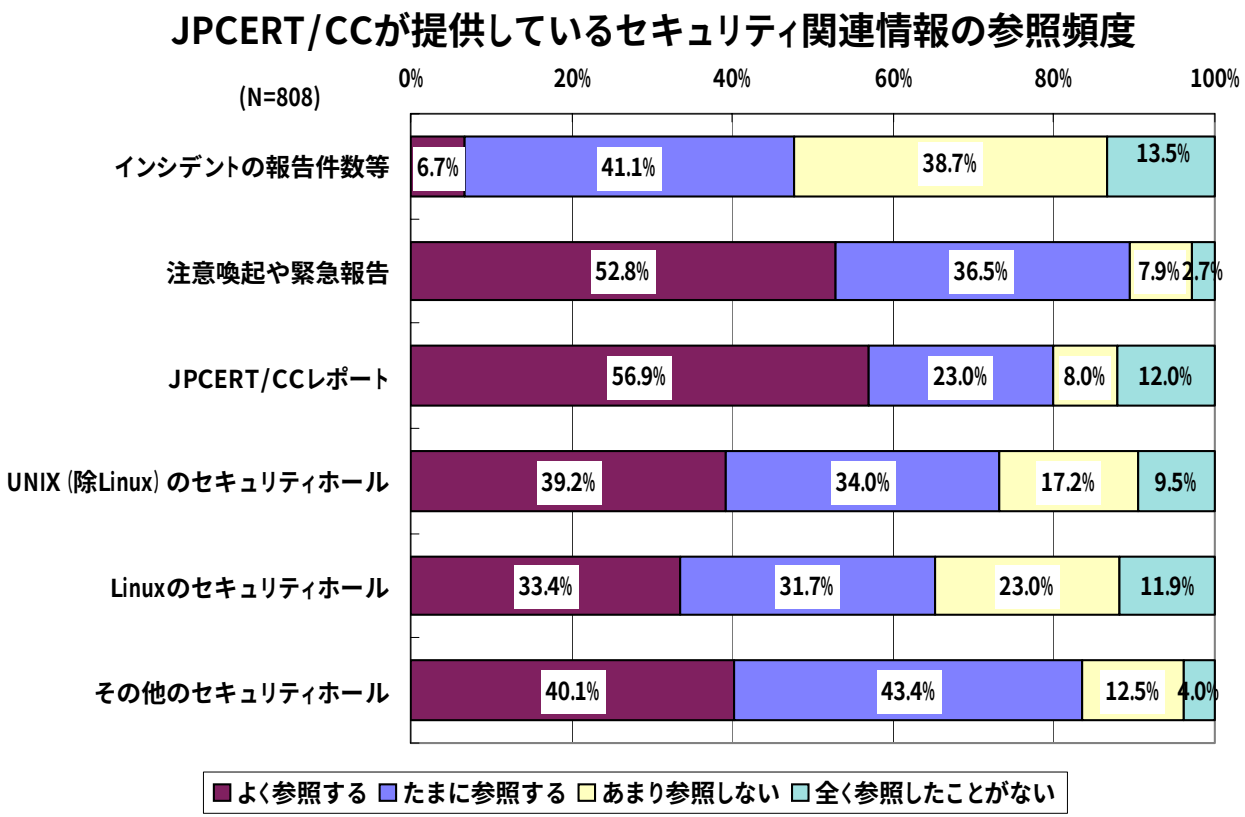


3.3 セキュリティ関連情報の参照頻度

■JPCERT/CCが公開しているセキュリティ関連情報のうち、「JPCERT/CCレポート」「注意喚起や緊急報告」については参照頻度の高い回答が多く、利用者のニーズが高いといえる。

■「UNIXのセキュリティホール」「Linuxのセキュリティホール」についても参照頻度は比較的高いことから、利用者の実際的なニーズがうかがえる。

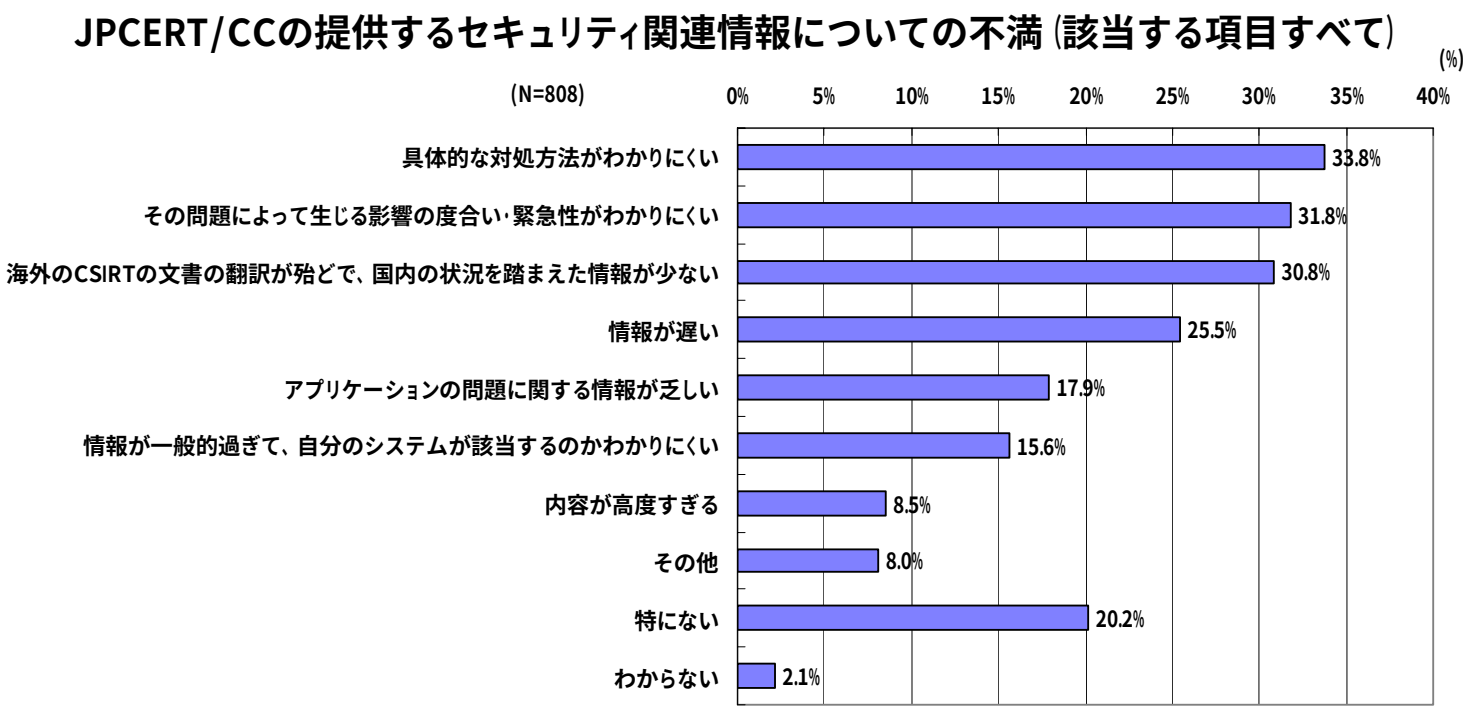
■「インシデントの報告件数等」は、参照頻度の高い回答が少なく、利用者のニーズは低いと考えられる。



3.4 セキュリティ関連情報についての不満

■JPCERT/CCの提供するセキュリティ関連情報についての不満として、「具体的な対処方法がわかりにくい」「その問題によって生じる影響の度合い・緊急性がわかりにくい」「国内の状況を踏まえた情報が少ない」「情報が遅い」とする回答が多い。

■「具体的な対処方法がわかりにくい」という不満は、模倣行為を促すリスクを避けるため、インシデントの詳細を開示していないことが大きく影響している。

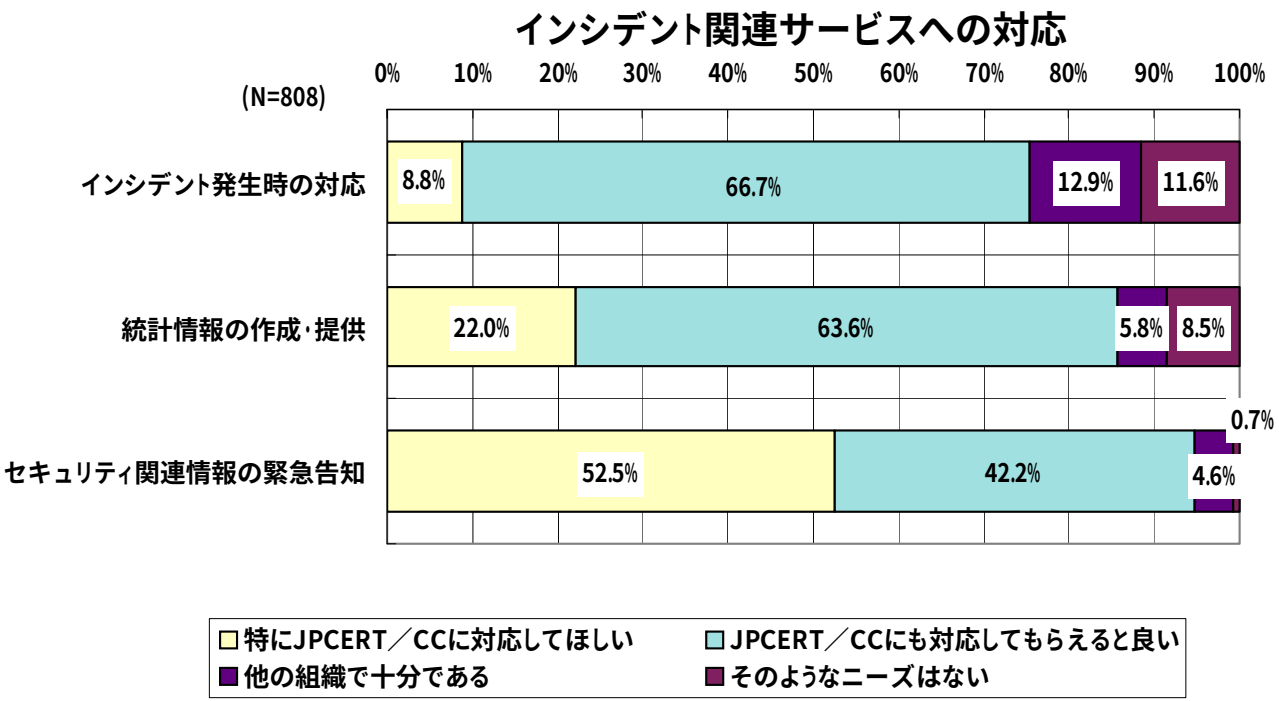


4.1 インシデント関連サービスへの対応

■インシデント関連の各種サービスのうちJPCERT/CCが対応すべきものとして 「セキュリティ関連情報の緊急告知」を支持する割合が高い。つまり、ベンダやユーザの利害に縛られない中立的な組織による対応が求められる。

■「インシデント発生時の対応」については、「JPCERT/CCにも対応してもらえると良い」及び「他の組織で充分である」の合計が約8割、「ニーズがない」を除いた比率では約9割となることから、回答組織の多くは、インシデント発生時の対応先についてJPCERT/CC以外の当てがあると考えられる。

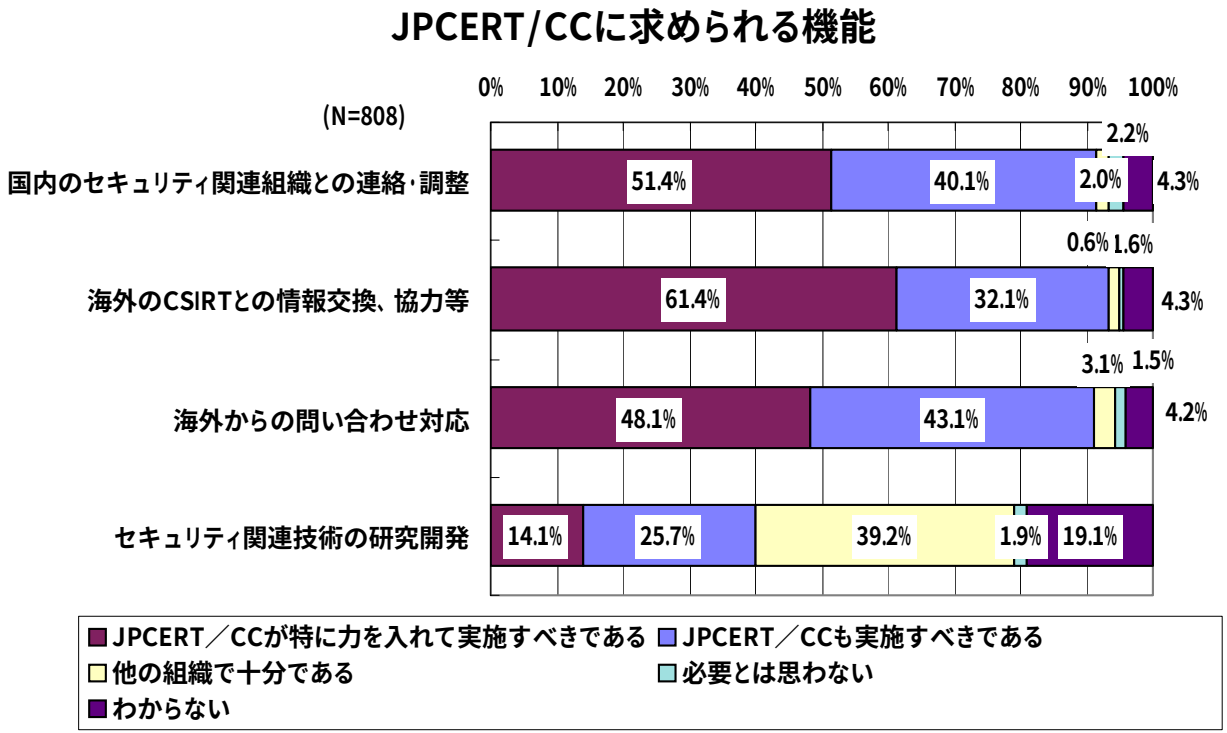
■「統計情報の作成・提供」も、「特にJPCERT/CCに対応して欲しい」とする意見は2割程度にとどまる。



4.2 JPCERT/CCに求められる機能

■JPCERT/CCが実施すべき機能として、「海外のCSIRTとの情報交換・協力等」、「国内のセキュリティ関連組織との連絡・調整」「海外からの問い合わせに応じた国内サイトへの連絡・調整」の支持が多い。いずれも、調整が重要であり、中立であることが前提となる機能といえる。

■「セキュリティ関連技術の研究開発」については、支持が少ない。これは、民間における競争、もしくは国の主導による基盤開発の形で進めることが妥当と見ることができる。



5 まとめ

■JPCERT/CCのメーリングリストに登録している、セキュリティ関連情報の利用者層を中心にWebアンケート調査を行った結果、以下の点が明らかになった。

・JPCERT/CCは、インシデント発生時の相談先として、インシデントの事後報告先として、またセキュリティ関連情報の収集先として活用されている。

・ただし、セキュリティポリシー等の制約があるため、インシデントの事後報告は今後減少する可能性もある。

・JPCERT/CCが提供するセキュリティ関連情報は、組織内システムのセキュリティ対策のように、実際的な用途で活用されている。

・セキュリティ関連情報の緊急告知サービスや、国内外のセキュリティ関連組織との連携機能、海外からの問い合わせに応じた国内サイトへの連絡・調整機能の提供は、JPCERT/CCによる対応が望まれている。

■以上の結果から、 JPCERT/CCに求められているのは、インシデント対応のように営利事業として成立する業務ではなく、セキュリティ関連情報の緊急告知や組織間の調整のように公平・中立性が重視される業務といえる。特に、組織間の調整業務は、JPCERT/CCのような中立的組織に対する期待が高いものと考えられる。

■また、今回の調査がJPCERT/CCのメーリングリスト登録者であること、JPCERT/CCの提供している情報が有用に活用されていることから、JPCERT/CCの概要や業務の周知を図ることにより、一層、多くの利用者に提供情報を活用いただける可能性も期待される。

■従って、JPCERT/CCにおける当面の課題としては、利用者のニーズや不満に応じて、より的確な情報を発信していくこと、JPCERT/CCの認知度を高め、新しい利用者層を開拓していくことが挙げられる。