第二回ITトレンド勉強会　【WEB】

プログラム

16:00～17:00　第一部　講演

2021年6月、情報処理推進機構が公開したサイバーセキュリティお助け隊の報告書で、
中小企業約1,100社に対し18万件超の不審なアクセスが行われていたことが判明しています。

決して他人事ではなくなっている事業継続までも脅かすサイバー攻撃の脅威に、どのように
備え対策していくべきか？
株式会社YONA 三国氏より、実際のインシデント発生現場の事例を交えてご紹介頂きます。

17:10～18:00　第二部　ディスカッション

セキュリティインシデントに関するお悩みを共有・ディスカッションしながら、解決策を模索
します。

18:10～19:00　第三部　座談会

第一部、第二部で「聞き足りない」「語り足りない」という方向けに交流の場をご提供します。

進行メンバー

		
大石 （座長@東京）	吉崎 （座長@大阪）	関 （PCNW事務局）

Zoom操作・音声ガイダンス

クオリティソフト社　PCNW事務局　川合（かわい）

第一部：講演

株式会社YONA　代表取締役社長

三国 貴正 氏

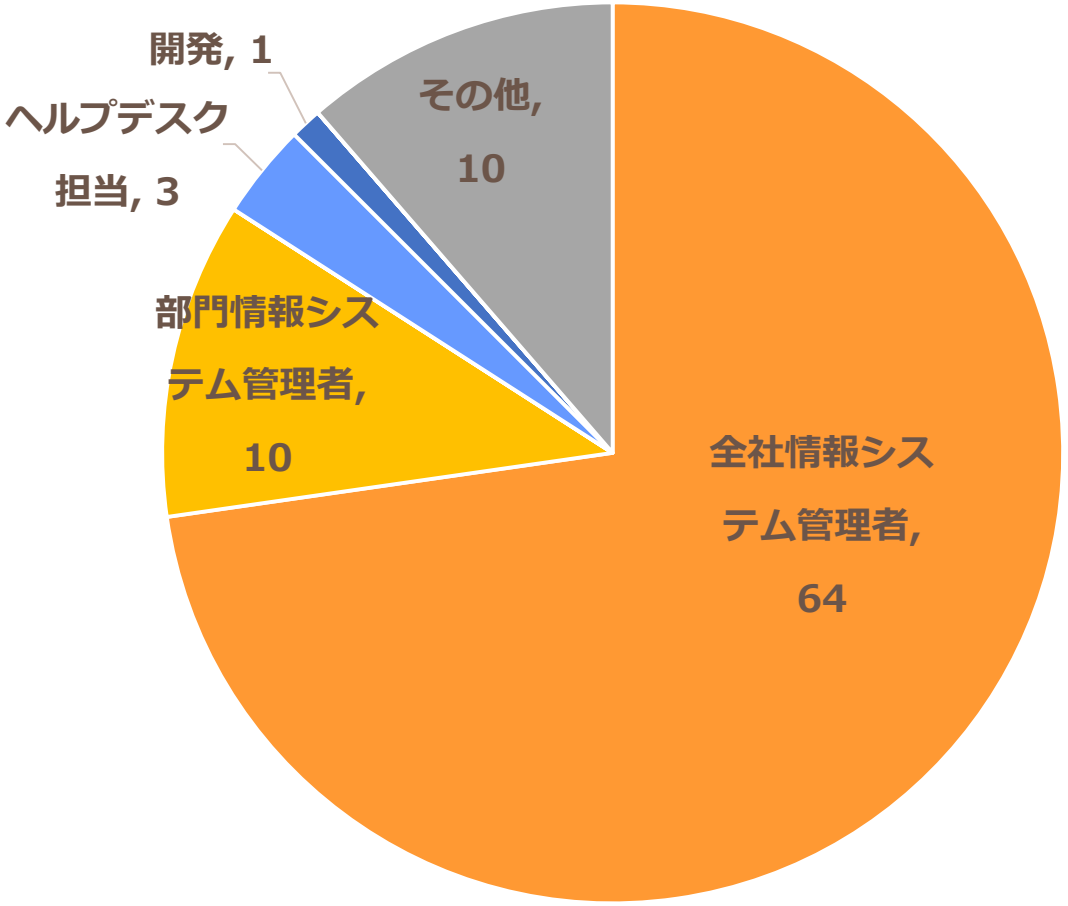
※講演資料については 今回は非公開※

第二部：ディスカッション

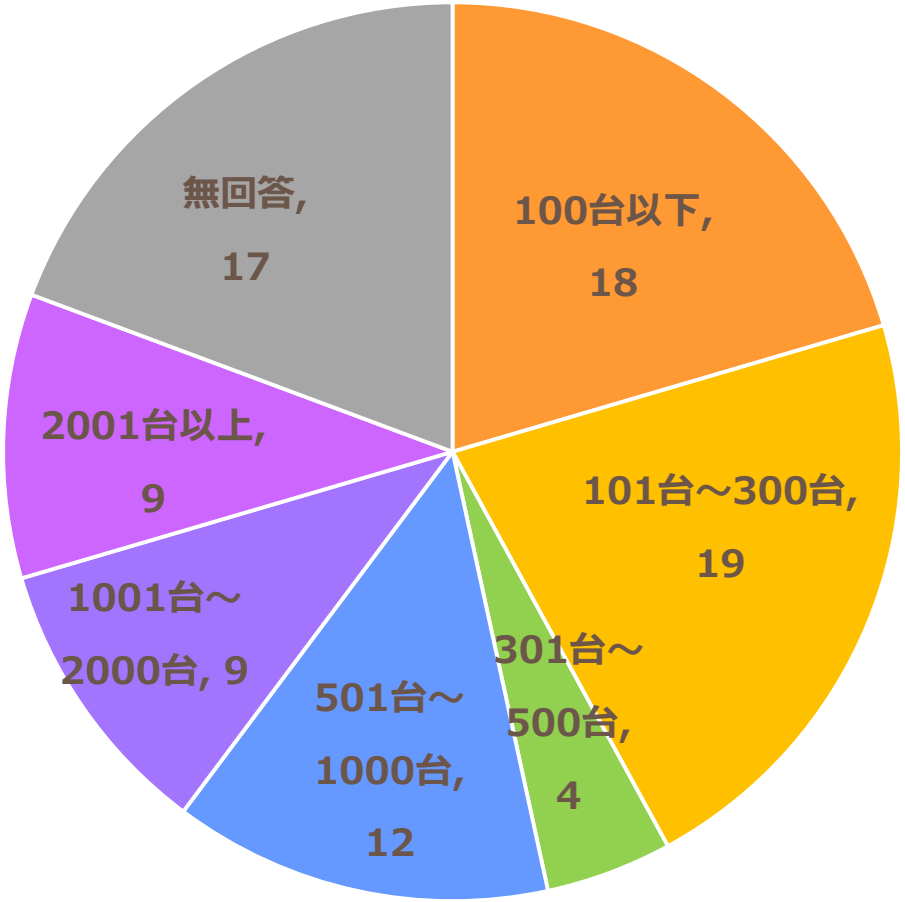
事前アンケート結果

お申込者属性

【職種】

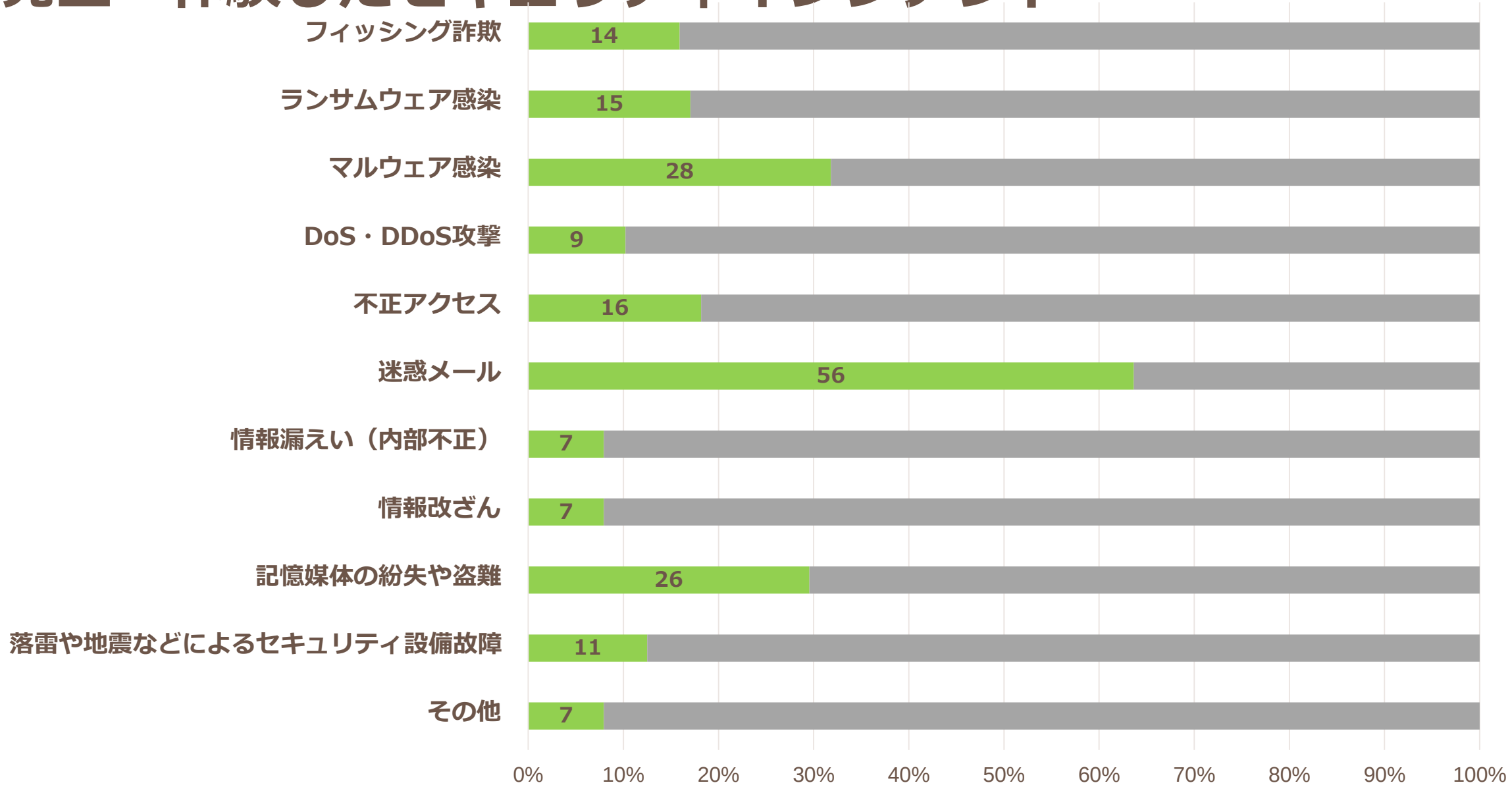


【PC管理台数】



2022/01/24 10:00時点の申込情報で集計：回答者88名

発生・体験したセキュリティインシデント



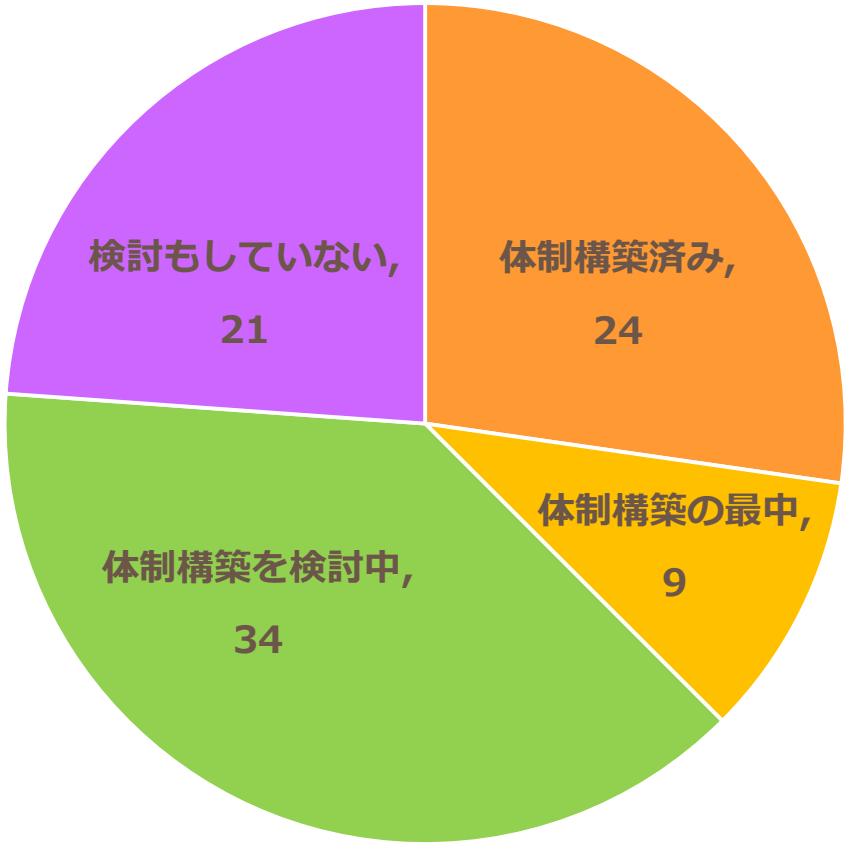
2022/01/24 10:00時点の申込情報で集計：回答者88名

発生・体験したセキュリティインシデント：その他

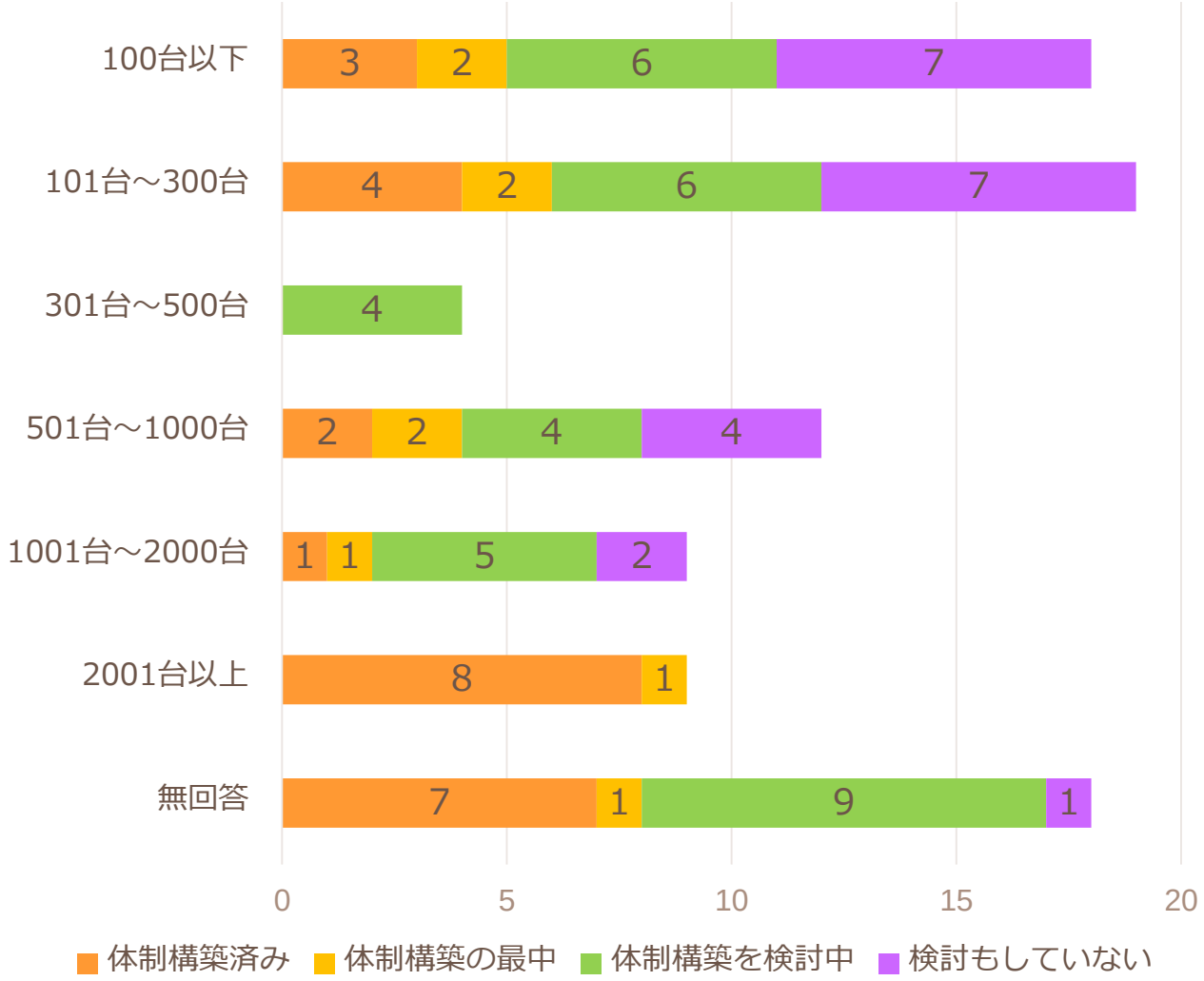
偽サイトの出現
会社貸与PC/スマートフォンの紛失
海外でのPC盗難とその後VPNサーバーへのアタック
そもそも基幹系が古いのでどこまでやられているのか不明
各種メールサーバートラブル（メールループ、Spamメールなど）
マルウェアメールの偽物(メールのURLをクリックしてしまったが、怪しいWebサイトが表示されただけで何も起きなかった)

2022/01/24 10:00時点の申込情報で集計：回答者88名

インシデント対応体制（CSIRT）の状況

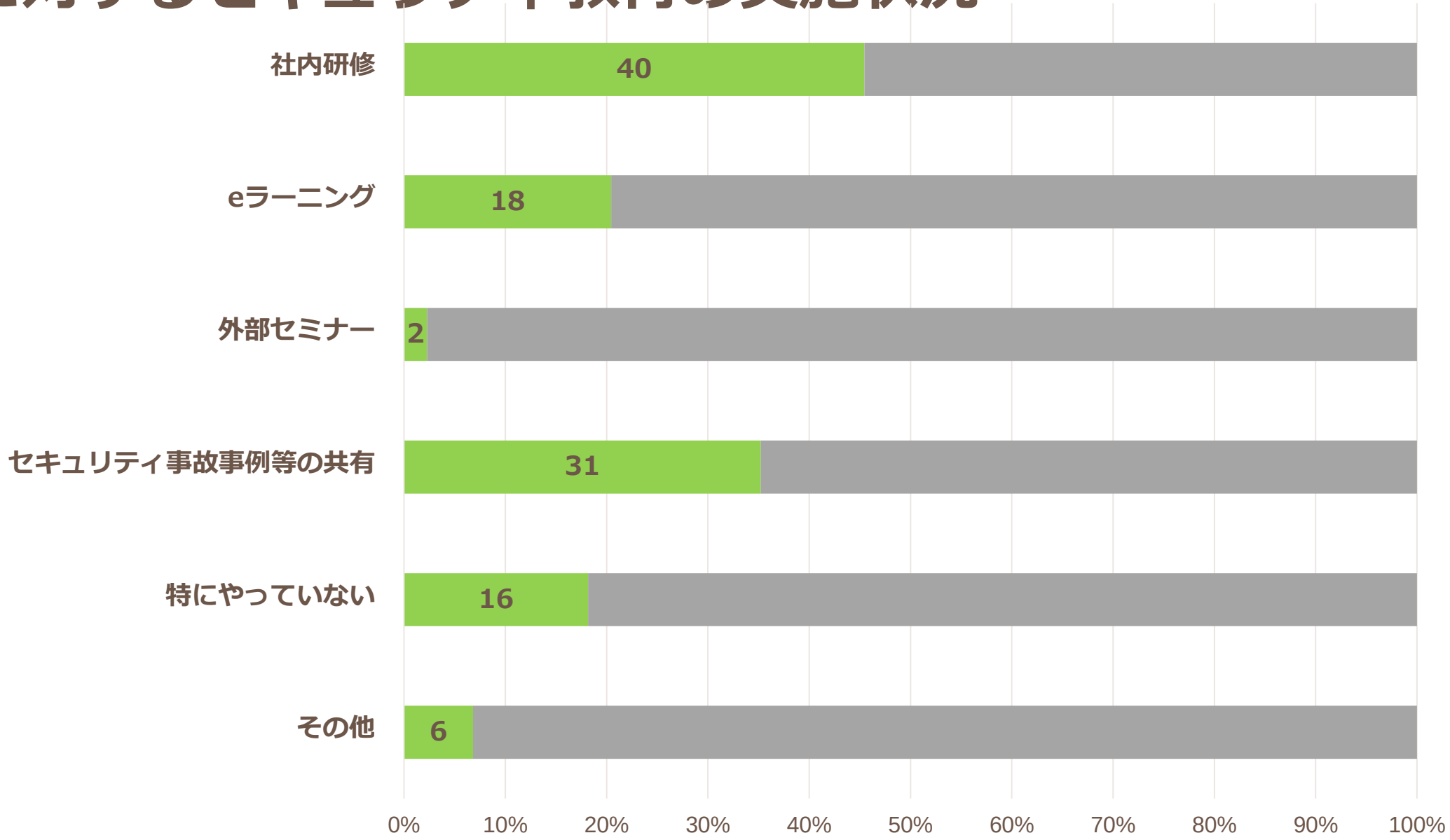


【PC管理台数別 回答状況】



2022/01/24 10:00時点の申込情報で集計：回答者88名

社員に対するセキュリティ教育の実施状況



2022/01/24 10:00時点の申込情報で集計：回答者88名

社員に対するセキュリティ教育の実施状況：その他

メール訓練
標的メールテスト
メールでの案内、注意喚起
年1回ISO27001の研修(ペーパーテスト)
標的型攻撃メール訓練・インシデント訓練（NCA）
2か月に1回のセキュリティクイズ、年1回のメール訓練
社内にばらまき型迷惑メールがきたら、グループウェア上にサンプル文とともに注意を促すインフォメーションを掲示する

2022/01/24 10:00時点の申込情報で集計：回答者88名

セキュリティ対策としてどんな取り組みをしているか①

審査	ISO27001を取得し年1回審査を受けている
	毎年時ごとに内部監査等を実施している
制度・体制	CSIRT構築
	情報セキュリティ規程を策定中。
	サイバーセキュリティ経営ガイドラインの活用
	情報資産台帳の作成更新・ISMS準拠（取得を目標）
	社長直轄の組織(情報セキュリティ委員会）を中心に活動
	PCIDSSとプライバシーマーク、クレジットカード番号等取扱契約締結事業者の規格等に準じた形で。
教育・テスト	年に数回、セキュリティ講習会を実施
	標的型攻撃メール訓練およびeラーニング実施予定
	年に1度社内に情報管理に関するテスト形式の教育を実施
	附属の専門学校の卒業生の大半が就職することから、学生向けのセキュリティ教材、啓発の強化を行っている。
注意喚起	委員会を設置し毎月啓蒙活動を実施
	ITリテラシー強化のため、システム部門から月次でニュースレターを発行。
	年末・年度末など迷惑メールが増える時期に、少しでも不信感を持ったメール本文のURLはクリックしないように呼びかけをしている。
	ソーシャル側に気をつけて、都度の注意アナウンスに加え、年一回行う個別面談時にセキュリティ関連の情報を共有することにしています。

2022/01/24 10:00時点の申込情報で集計：回答者88名

セキュリティ対策としてどんな取り組みをしているか②

仕組み・システム等	リモートが主流のためMDM導入など
	EDR、WAF、クライアントセキュリティソフト、UTMの導入など
	ほとんどUTMやエンドポイントのウイルス対策に頼っています。
	ウィルス対策ソフトの導入、WSUSでのアップデート管理程度
	ゼロトラストネックワークアーキテクチャを採用したITインフラの導入
	ファイアウォール、IPS等の設置、暗号化機能付USBメモリの利用
	PCセキュリティ製品の検討と導入、クラウドサービスの権限管理
	UTMの導入、不正接続防止、USBメモリ使用制限、セキュリティ監査
	エンドポイントセキュリティ導入 WiFi/有線LAN接続のRADIUS認証
	・エンドポイント、UTM等のセキュリティ機器・ソフトの導入 ・ISMSテストを年1回実施
	クラウド型のEDR+NGAVの導入とMDRサービスアウトソース、Bitlocker適用、URLフィルタリング導入、QNDによる脆弱パッチ配信等
	Endpointセキュリティソフトの導入、メールサーバーのセキュリティ対策（CAS） ファイヤーウォールの不正通信、不正アクセスレポート（月次） また、上記それぞれのエラー報告に沿って対策
	ファイアウォール、IDS/IPS、WEBフィルタリング、アンチウイルス、アンチスパム、アプリケーション制御、エンドポイントセキュリティ、クライアントの暗号化(FES/EFS)、Socの活用、クライアント操作ログ監視、ログ監視していることを周知、記憶媒体の利用制御、パスワードのポリシーの強制適用、適時最新の情報を展開、社員教育など

2022/01/24 10:00時点の申込情報で集計：回答者88名

他の参加者に聞いてみたいこと、共有したい課題①

緊急対応	1	委託先などで個人情報が流出してしまう事も考えられると思います。 委託元として、委託先のインシデントが判明したタイミングで取るべき対応について知りたいです。 特にBtoCのサービス展開をしている場合、エンドユーザは委託先などの区別はつかないので、対応の方法を間違えると、大きな被害が発生するのではないかと思っています。
事前対策	1	中小企業＆一人情シスで現実的なセキュリティ対策があれば伺いたい。
	2	セキュリティ対策はありすぎて、自社でどれを優先して取り入れていったらよいか判断が難しい。最低限取り組むべき（皆さんが取り組んでいる）対策を聞いておきたい
	3	実際にはめったに発生しないので、慌てて対応に失敗しそうな気がします。疑似的な標的メール練習等、なにか実用的な対策をしたことがあれば、教えていただけると嬉しいです。
	4	利用者の利便性を下げない状態でのフィッシングメール対策について。最近のフィッシングメールはSPFを設定しているため、迷惑メールトレイでなく受信トレイに受信しています。
	5	ログ取得してもチェックする人員がいないので、ルーターやサーバーの操作ログを積極的に取得していません。最低限これぐらいはやるべきですというアドバイスがあればお願いします。
	6	インシデントレスポンス手順書に関して、あらかじめ対応フローやチェックリスト等を準備していきたいと思っていますが、パターンも多く具体的にどういった内容のものを用意すれば良いか悩んでいます。何かアドバイス頂ければと思います。
	7	クラウドサービスの利用が主流になり、境界型防御からゼロトラスト環境に移行しつつある中、セキュリティインシデントにどの様に気づき、どう対応すればよいのか。他社さんはどうされているのか。中小企業ではど程度投資すればよいのか。
	8	・ベンダーで解決できないようなセキュリティ事案（ランサムウェア被害）などあった場合の備えはどこまですべきか？ ・インフラ管理のベンダーの即応性が弱い場合に、導入業者以外へ運用委託することは可能なのか？

2022/01/24 10:00時点の申込情報で集計：回答者88名

他の参加者に聞いてみたいこと、共有したい課題②

投資・コスト	1	セキュリティ管理と費用のバランス
	2	低予算で効果を発揮する方法・事例があれば（社員への啓蒙活動ではなくシステムレベル）
	3	脅かし商法的な言葉とともに「是非これを」と機器の営業様が来られますが、なかなか導入には至りません。 皆様は何にどれくらい投資されているのでしょうか。
教育・訓練	1	・インシデントに関する一般従業員の意識が低い
	2	社員のITリテラシー（セキュリティ知見向上）をどのようにされているか気になります。
	3	インシデント訓練をやりたいが、シナリオをどのように策定したらよいかがわからない
	4	特に考えていないが、会社にセキュリティの重要性を認知させる手立てがあれば教えてほしい
	5	社員に対するセキュリティ教育の取り組みについて、社員それぞれでITスキルが一定ではないため、どのように進めるべきか、悩んでいます。
	6	社員教育について、外注か社内作成のどちらかを採用しているのかという事とその理由について聞きたい。 比較的手が余っているので、これを機に社内教育を始めたいと思っており、両方の意見を聞きたい。
	7	（社外活動として）現在、九州大学でIT技術者向けにサイバー攻撃と関連したBCP演習の指導にあたっていますが、講義（主に演習）の中でも、CSIRTから見た「インシデントレスポンス」とBCPの観点からの「インシデント対応」の違いと関連を理解してもらうのが難しいと感じています。 実際のインシデント対応の業務の中で、IT部門の認識と、業務部門の認識のギャップを埋めるのに、普段使われている方法や、ポイントがあれば教えて欲しい（なお、希望者には大学での教材提供可）

2022/01/24 10:00時点の申込情報で集計：回答者88名

他の参加者に聞いてみたいこと、共有したい課題③

制度・体制	1	中小企業でのCSIRTの活動実態を知りたい。
	2	・サイバーセキュリティ経営ガイドラインは利用されているでしょうか？ ・CSIRT組織は作られているでしょうか？ ・ISACAやISC2のセキュリティ専門資格取得を社内で推奨・重視しているでしょうか？
他	1	他社事例と傾向・対策
	2	弱い立場（仕組みを矯正できない立場）からの脱PPAP対策
	3	社員や退職者による故意の情報持ち出しに対する効果的な対策はありますか？

2022/01/24 10:00時点の申込情報で集計：回答者88名