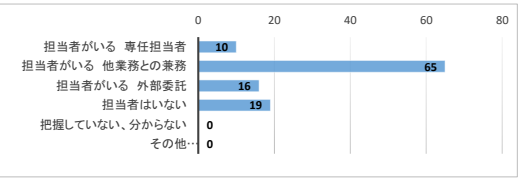
令和６年　サイバー防犯診断　アンケート調査結果

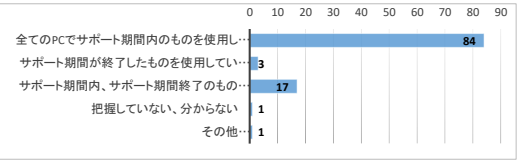
愛知県警察本部生活安全部サイバー犯罪対策課

令和６年に実施したサイバー防犯診断でのアンケートの集計結果です。
製造業、卸・小売業、サービス業、建設業、運輸業、医療機関等、106の中小事業者を対象に実施しました。

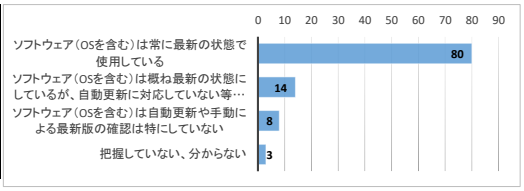
1	情報セキュリティ担当者の有無について　※複数選択可	
①	担当者がいる　専任担当者	10
②	担当者がいる　他業務との兼務	65
③	担当者がいる　外部委託	16
④	担当者はいない	19
⑤	把握していない、分からない	0
⑥	その他【　　】	0



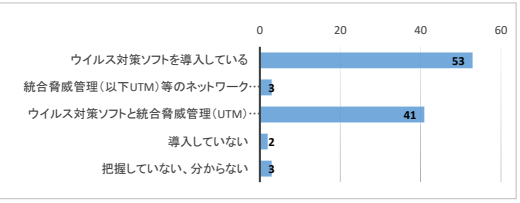
2	社内ネットワークに接続できるPCで使用しているOSについて	
①	全てのPCでサポート期間内のものを使用している　例）Windows11、10など	84
②	サポート期間が終了したものを使用している　例）Windows8.1、7、Vista、XP	3
③	サポート期間内、サポート期間終了のものが混在している	17
④	把握していない、分からない	1
⑤	その他【　　】	1



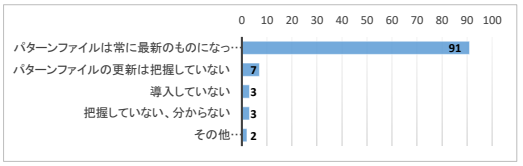
3	社内ネットワークに接続できるPCで使用しているソフトウェアについて	
①	ソフトウェア（OSを含む）は常に最新の状態で使用している	80
②	ソフトウェア（OSを含む）は概ね最新の状態にしているが、自動更新に対応していない等一部実施できていない	14
③	ソフトウェア（OSを含む）は自動更新や手動による最新版の確認は特にしてい	8
④	把握していない、分からない	3
⑤	その他【　　】	1



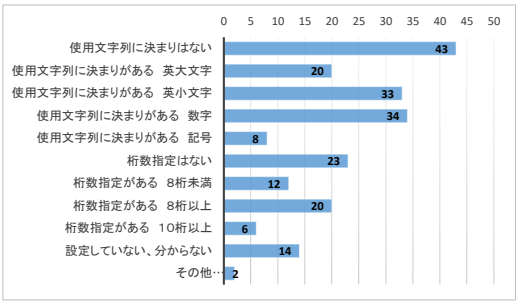
4	ウイルス対策ソフト・ネットワークセキュリティ機器の導入状況について	
①	ウイルス対策ソフトを導入している	53
②	統合脅威管理（以下UTM）等のネットワークセキュリティ機器を導入している	3
③	ウイルス対策ソフトと統合脅威管理（UTM）等のネットワークセキュリティ機器を両方導入している	41
④	導入していない	2
⑤	把握していない、分からない	3
⑥	その他【　　】	4



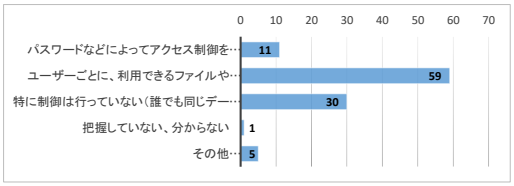
5	ウイルス対策ソフトの管理状況について	
①	パターンファイルは常に最新のものになっている	91
②	パターンファイルの更新は把握していない	7
③	導入していない	3
④	把握していない、分からない	3
⑤	その他【　　】	2



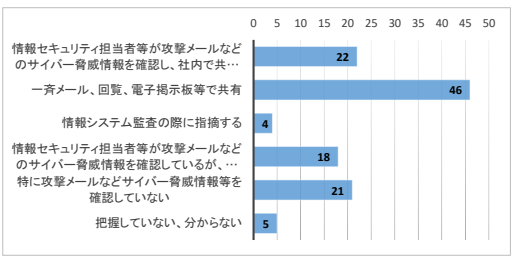
6	パスワードについて　※複数選択可	
①	使用文字列に決まりはない	43
②	使用文字列に決まりがある　英大文字	20
③	使用文字列に決まりがある　英小文字	33
④	使用文字列に決まりがある　数字	34
⑤	使用文字列に決まりがある　記号	8
⑥	桁数指定はない	23
⑦	桁数指定がある　８桁未満	12
⑧	桁数指定がある　８桁以上	20
⑨	桁数指定がある　１０桁以上	6
⑩	設定していない、分からない	14
⑪	その他【　　】	2



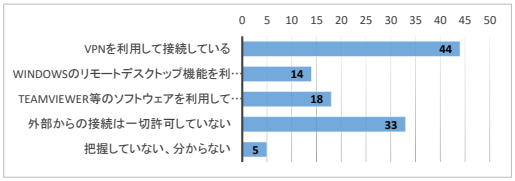
7	共有設定について	
①	パスワードなどによってアクセス制御を行っている（業務内容等によってアクセスできるファイルが異なる）	11
②	ユーザーごとに、利用できるファイルやフォルダや業務システムを制御してい	59
③	特に制御は行っていない（誰でも同じデータにアクセスできる）	30
④	把握していない、分からない	1
⑤	その他【　　】	5



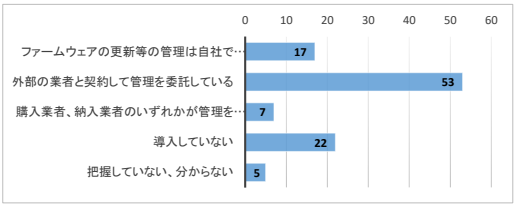
8	サイバー脅威情報の収集と社内共有について　※複数選択可	
①	情報セキュリティ担当者等が攻撃メールなどのサイバー脅威情報を確認し、社内で共有している　集合研修を実施	22
②	一斉メール、回覧、電子掲示板等で共有	46
③	情報システム監査の際に指摘する	4
④	情報セキュリティ担当者等が攻撃メールなどのサイバー脅威情報を確認しているが、社内で共有はできていない	18
⑤	特に攻撃メールなどサイバー脅威情報等を確認していない	21
⑥	把握していない、分からない	5
⑦	その他【　　】	0



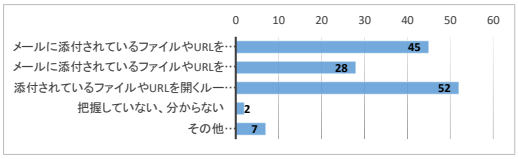
9	外部から社内ネットワークへのアクセスについて　※複数選択可	
	① VPNを利用して接続している	44
	② Windowsのリモートデスクトップ機能を利用して接続している	14
	③ TeamViewer等のソフトウェアを利用して接続している	18
	④ 外部からの接続は一切許可していない	33
	⑤ 把握していない、分からない	5
	⑥ その他【　　】	5



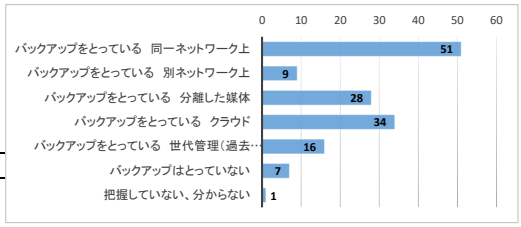
10	ネットワークセキュリティ機器（UTM等）、リモート接続機器（VPN対応ルーター等）の管理状況について	
	① ファームウェアの更新等の管理は自社で行っている	17
	② 外部の業者と契約して管理を委託している	53
	③ 購入業者、納入業者のいずれかが管理をしていると思うが契約内容を把握してい	7
	④ 導入していない	22
	⑤ 把握していない、分からない	5
	⑥ その他【　　】	2



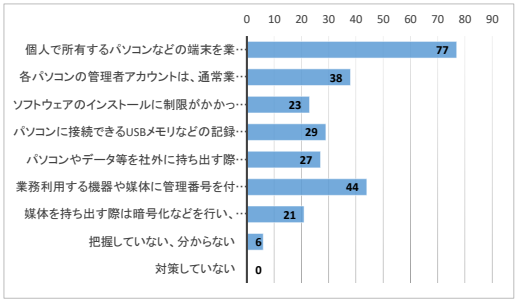
11	メール対策について　※複数選択可	
	① メールに添付されているファイルやURLを開くルールがある　添付ファイル	45
	② メールに添付されているファイルやURLを開くルールがある　URL	28
	③ 添付されているファイルやURLを開くルールは特にない	52
	④ 把握していない、分からない	2
	⑤ その他【　　】	7



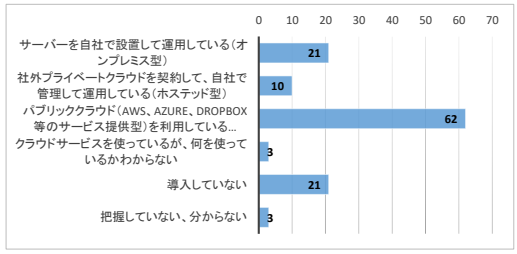
12	データのバックアップについて　※複数選択可	
	① バックアップをとっている　同一ネットワーク上	51
	② バックアップをとっている　別ネットワーク上	9
	③ バックアップをとっている　分離した媒体	28
	④ バックアップをとっている　クラウド	34
	⑤ バックアップをとっている　世代管理（過去のバックアップデータを保存してい	16
	⑥ バックアップはとっていない	7
	⑦ 把握していない、分からない	1
	⑧ その他【　　】	2



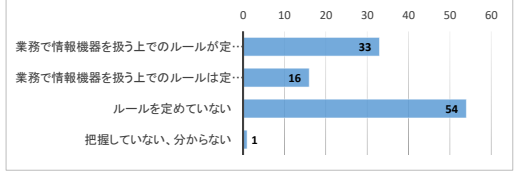
13	端末のセキュリティ対策について　※複数選択可	
	① 個人で所有するパソコンなどの端末を業務で使用させない	77
	② 各パソコンの管理者アカウントは、通常業務には使用しない	38
	③ ソフトウェアのインストールに制限がかかっている	23
	④ パソコンに接続できるUSBメモリなどの記録媒体を制限している	29
	⑤ パソコンやデータ等を社外に持ち出す際は、管理者に許可を求めるなどのルールを定めている	27
	⑥ 業務利用する機器や媒体に管理番号を付けて一覧表を作成し、管理者と種類・数を明確化している	44
	⑦ 媒体を持ち出す際は暗号化などを行い、盗難や紛失の対策をしている	21
	⑧ 把握していない、分からない	6
	⑨ 対策していない	0



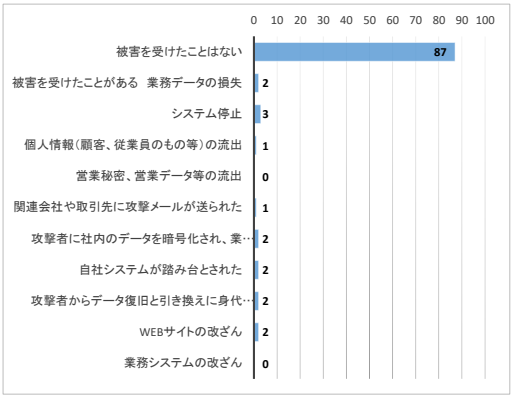
14	クラウドサービスの利用状況について　※複数回答可	
	① サーバーを自社で設置して運用している（オンプレミス型）	21
	② 社外プライベートクラウドを契約して、自社で管理して運用している（ホステッド型）	10
	③ パブリッククラウド（AWS、Azure、Dropbox等のサービス提供型）を利用している(IaaS/SaaS/PaaS型)	62
	④ クラウドサービスを使っているが、何を使っているかわからない	3
	⑤ 導入していない	21
	⑥ 把握していない、分からない	3
	⑦ その他【　　】	2



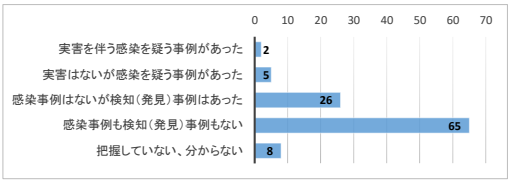
15	情報セキュリティに対するルールについて（例：情報セキュリティ5か条（IPA提唱）やセキュリティポリシーなど）	
	① 業務で情報機器を扱う上でのルールが定められ、従業員に示されている	33
	② 業務で情報機器を扱う上でのルールは定めてあるが、従業員へ示されていない	16
	③ ルールを定めていない	54
	④ 把握していない、分からない	1
	⑤ その他【　　】	2



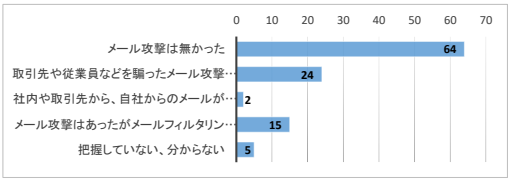
16	サイバー攻撃（コンピュータウィルス、マルウェア、メール攻撃、ランサムウェアなどを含む）により生じた被害について（過去３年間）　※複数回答可	
①	被害を受けたことは**ない**	87
②	被害を受けたことが**ある**　業務データの損失	2
③	システム停止	3
④	個人情報（顧客、従業員のもの等）の流出	1
⑤	営業秘密、営業データ等の流出	0
⑥	関連会社や取引先に攻撃メールが送られた	1
⑦	攻撃者に社内のデータを暗号化され、業務が停滞した	2
⑧	自社システムが踏み台とされた	2
⑨	攻撃者からデータ復旧と引き換えに身代金を要求された	2
⑩	Webサイトの改ざん	2
⑪	業務システムの改ざん	0
⑫	その他	2
⑬	把握していない、分からない	1
⑭	その他【　　】	1



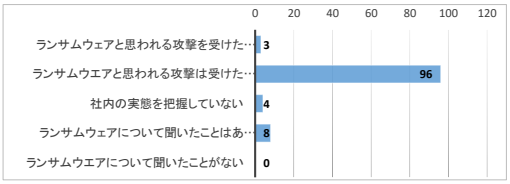
17	マルウェア（コンピュータウイルス等）について（過去3年間）	
①	実害を伴う感染を疑う事例があった	2
②	実害はないが感染を疑う事例があった	5
③	感染事例はないが検知（発見）事例はあった	26
④	感染事例も検知（発見）事例もない	65
⑤	把握していない、分からない	8
⑥	その他【　　】	0



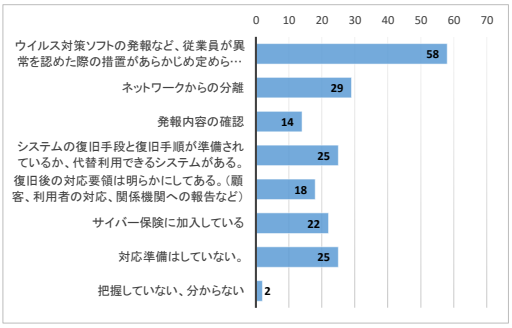
18	メール攻撃について（過去3年間）　※複数回答可	
①	メール攻撃は無かった	64
②	取引先や従業員などを騙ったメール攻撃を受けたことがある	24
③	社内や取引先から、自社からのメールがウイルスに感染しているなどと指摘され	2
④	メール攻撃はあったがメールフィルタリングで排除した	15
⑤	把握していない、分からない	5
⑥	その他【　　】	1



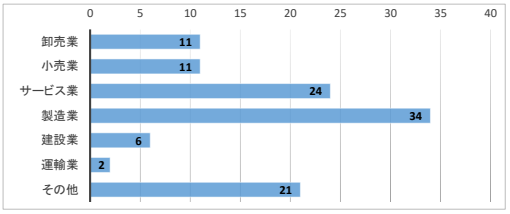
19	ランサムウェアについて（過去3年間）　※複数回答可	
①	ランサムウェアと思われる攻撃を受けたことが**ある**	3
②	ランサムウエアと思われる攻撃は受けたことが**ない**	96
③	社内の実態を把握していない	4
④	ランサムウェアについて聞いたことはあるがよく知らない	8
⑤	ランサムウエアについて聞いたことがない	0
⑥	その他【　　】	0



20	サイバー攻撃（コンピュータウィルス、マルウェア、メール攻撃、ランサムウェアなどを含む）被害発生時の対応準備について　※複数回答可	
①	ウイルス対策ソフトの発報など、従業員が異常を認めた際の措置があらかじめ定められている。セキュリティ担当者への連絡	58
②	ネットワークからの分離	29
③	発報内容の確認	14
④	システムの復旧手段と復旧手順が準備されているか、代替利用できるシステムが	25
⑤	復旧後の対応要領は明らかにしてある。（顧客、利用者の対応、関係機関への報告など）	18
⑥	サイバー保険に加入している	22
⑦	対応準備はしていない。	25
⑧	把握していない、分からない	2
⑨	その他【　　】	1



21	業種　※複数回答可	
①	卸売業	11
②	小売業	11
③	サービス業	24
⑤	製造業	34
⑥	建設業	6
⑦	運輸業	2
⑩	その他	21



22	事業規模（従業員数）	
①	５人以下	11
②	６人以上、20人以下	32
③	21人以上、50人以下	19
④	51人以上、100人以下	15
⑤	101人以上、300人以下	15
⑥	301人以上	14