**不正アクセス行為対策等の実態に関するアンケート調査**

1. **組織的対策**

**【貴社・団体について伺います】**

**問１.　貴社・団体は、どの業種に該当しますか。（○は一つ）**



（太枠線内にご回答ください）

**問２.　貴社・団体の従業員は、どのくらい在籍されていますか。（○は一つ）**

|  |  |
| --- | --- |
| １．100人未満 | ５．1,000人以上5,000人未満 |
| ２．100人以上300人未満 | ６．5,000人以上１万人未満 |
| ３．300人以上500人未満  ４．500人以上1,000人未満 | ７．1万人以上 |

**問３.　貴社・団体の売上げ、予算の総額は、どれくらいの規模ですか。（○は一つ）**

|  |  |
| --- | --- |
| １．10億円未満 | ５．1,000億円以上～5,000億円未満 |
| ２．10億円以上～50億円未満 | ６．5,000億円以上～1兆円未満 |
| ３．50億円以上～100億円未満 | ７．1兆円以上 |
| ４．100億円以上～1,000億円未満 | ８．適切な指標がない |

**【情報システム等の環境について伺います】**

**問４.****貴社・団体支給の端末装置（パソコン、スマートフォン等）の整備環境は、どのようになっていますか。  
（○は一つ）**

|  |  |
| --- | --- |
| １．１人当たり１台以上 | ４．事業所や拠点で共有 |
| ２．数人で共有 | ５．その他（　　　　　　 ） |
| ３．部・課で共有 | ６．端末装置は利用していない |

**問５.　貴社・団体では業務における個人所有端末装置（パソコン、スマートフォン等）の扱いをどうしていますか。  
（○は一つ）**

問６へ  
お進みください

|  |  |  |
| --- | --- | --- |
| １．全て許可（２及び３を許可）している |  | ４．許可していない |
| ２．パソコン・タブレット（タブレット  ＰＣを含む）を許可している |  | ５．把握していない  問5-1へお進みください |
| ３．スマートフォンを許可している |  |

**問5-1.　問５で個人所有端末装置の使用を許可している（１～３）と回答された方に伺います。個人所有端末装置のセ  
 キュリティ対策（ウイルス対策ソフトの導入など）を義務づけていますか。（○は一つ）**

|  |  |
| --- | --- |
| １．義務づけている | ２．義務づけていない |

**問６.　昨今の新型コロナウイルス感染拡大防止策等により、テレワーク業務が急激に普及していますが、貴社・団体においてテレワークを行っていますか。（○は一つ）**

|  |  |
| --- | --- |
| １．行っている | ２．行っていない |
| 問6-1～6-2へお進みください | 問6-3へお進みください |

**問6-1.　問６で「１．行っている」と回答された方に伺います。いつ頃からテレワークを行っていますか。（○は一つ）**

|  |
| --- |
| １．新型コロナウイルス感染対策に伴い開始した |
| ２．貴社・団体の業務の運用として、以前から行っていた |
| ３　その他（　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　） |

**問6-2.　問６で「１．行っている」と回答された方に伺います。テレワーク業務を行う際の端末装置（パソコン、スマートフォン等）の利用環境はどのようになっていますか。（○は一つ）**

|  |  |
| --- | --- |
| 1. 貴社・団体支給の端末装置のみ利用 | ３．貴社・団体支給及び個人所有端末装置のどちらでも利用可能 |
| ２．個人所有端末装置のみ利用 | ４．端末装置を利用しない |

**問6-3.　問６で「２.行っていない」と回答された方に伺います。テレワークを行っていない理由はなぜですか。  
（○はいくつでも）**

|  |  |
| --- | --- |
| １．行う必要がない | ５．技術不足のためできない |
| ２．業務の特性上行えない | ６．資金不足のためできない |
| ３．以前行っていたがやめた  （必要性がなくなった） | ７．ルール作りや教育ができない ８．今後導入を計画している |
| ４．以前行っていたがやめた  　（セキュリティ上の問題でやめた） | ９．その他（　　　　　　　　　） |

**問７.　貴社・団体内LANには、有線、無線のいずれかのネットワークを利用していますか。（○は一つ）**

|  |  |
| --- | --- |
| １．有線ネットワークと無線ネットワークを併用 | ３．全て有線ネットワークで構築 |
| ２．全て無線ネットワークで構築 | ４．LANを敷設していない |

**問８.　クラウドサービスを利用していますか。（○は一つ）**

|  |  |  |
| --- | --- | --- |
| １．利用している | ２．利用していない | ３．わからない |

**問９.　外部から内部ネットワークへの接続を許可していますか。（○は一つ）**

|  |  |
| --- | --- |
| １．許可している | ２．許可していない |

**【情報セキュリティの運用・管理体制について伺います】**

**問10.　情報セキュリティ対策の必要性を感じるのは、どのような理由からですか。（○はいくつでも）**

問10-1～10-5へ  
お進みください

問11へ

お進みください

|  |
| --- |
| １．過去1年間に不正アクセス等の攻撃・被害にあったため |
| ２．ウイルス等のマルウェアの感染を防ぐため |
| ３．DDoS攻撃等によるシステムダウンを防ぐため |
| ４．システムの乗っ取り等により犯罪等へ悪用されるのを防ぐため |
| ５．顧客等との取引を万全なものとするため |
| ６．インターネット上に顧客情報等の部内情報が漏れるのを防ぐため |
| ７．セキュリティ事故がブランドイメージや業績に与える影響を避けるため |
| ８．事業を行う上で必要不可欠なため |
| ９．顧客等から要請があるため |
| 10．社会情勢や国際的行事等から、攻撃が増えることが予想されるため  11．新型コロナウイルス感染対策として |
| 12．不正アクセスの加害者にならないため |
| 13．その他（ 　　　　 ） |

**問10-1.　過去1年間に攻撃・被害を受けられた方にお伺いします。それは、どのような被害であり、また、攻撃手段   
でしたか。（○はいくつでも）**

|  |  |
| --- | --- |
| 【→被害は？】 | 【→攻撃手段は？】 |
| １．ホームページの改ざん | １．DDoS攻撃 |
| ２．システム損壊等による業務妨害 | ２. 踏み台（バックドア設置等） |
| ３．ウイルスによる情報流出 | ３. 部外からの不正アクセス |
| ４．ウイルス以外の情報流出 | ４. ウイルス等の感染 |
| ５．ネットワーク利用詐欺 | ５. システム損壊、データ改ざん |
| ６．偽サイト等模倣サイトの開設 | ６. 内部の者のネットワーク悪用 |
| ７．フィッシングサイトの開設 | ７. 関連会社や取引先等を経由 |
| ８．電子メールの不正中継（不正送信） | ８. 不明 |
| ９．Web等での誹謗・中傷被害 | ９．不正なメール（フィッシング含む） |
| 10. 端末機器（パソコン、スマートフォン等）の盗難 | 10．その他（　　　　　　　　　　） |
| 11. 外部記録媒体の盗難  12．インターネットバンキング不正送金  13．ランサムウェア |  |
| 14. その他データ盗用（キーロガー含）  15. その他（　　　　　　　　　　　）  16. 実質的な被害はなかった |  |

**問10-2.　過去1年間に攻撃・被害を受けられた方にお伺いします。攻撃・被害を受けた結果、関連会社や取引先等に  
被害を与えてしまったことはありますか。与えてしまった場合はどのような被害を与えてしまいましたか。（○は一つ）**

|  |
| --- |
| １．与えてしまった（　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　） |
| ２．与えていない |

**問10-3. 過去１年間に攻撃・被害を受けられた方にお伺いします。攻撃・被害を受けた結果、実際に講じられた  
対応策はどういったものですか。（○はいくつでも）**

|  |  |
| --- | --- |
| １．ファイアウォールの設置・強化  ２．ウイルス等対策製品の導入・強化 | 12．システム上にセキュリティホールがない  　　かどうか検査、診断 |
| 1. 最新パッチの適用   ４．ソフトウェアのバージョンアップ | 13．セキュリティコンサルティングの利用  14．セキュリティ監査の実施 |
| ５．認証機能の導入・強化 | 15．弁護士への相談 |
| ６．ネットワークの再構築 | 16．関連会社や取引先等に対応するよう求めた |
| ７．不必要なサービスの停止 | 17. クラウドの設定を見直した |
| ８．セキュリティポリシーの策定・見直し | 18．不明 |
| ９．セキュリティ教育の実施・強化 | 19．その他（　　　　　　　　　　　　　） |
| 10．不正アクセスが行われていないかどうか  　　ネットワークの監視 | 20．特に何も対策を講じていない |
| 11．クラウド等の外部セキュリティサービスの利用 |  |

**問10-4.　過去1年間に攻撃・被害を受けられた方にお伺いします。どこに届出・相談をなされましたか。また、その理由は何ですか。（○はいくつでも）**

**〈届出・相談先機関等〉**

|  |  |
| --- | --- |
| １．警察 | ６．個人情報保護委員会 |
| ２．IPA（情報処理推進機構） | ７．その他（　　　　　　　　　　　　　） |
| ３．JPCERT/CC | ８．届け出なかった |
| ４．国民生活センター・消費生活センター |  |
| ５．監督官庁 | 問10-5へお進みください |

〈届出・相談した理由〉へお進みください

**〈届出・相談した理由〉**

|  |  |
| --- | --- |
| １．届出義務があるため | ７．法律職（弁護士等）からの意見により |
| ２．事案解決を求めて | ８．解決方法を知るため |
| ３．被害拡大を阻止するため | ９．行政機関からの指導により |
| ４．関係者（株主等）への説明責任を果たすため | 10．利用者からの指摘により |
| ５．報道されたため | 11．その他（　　　　　　　　　　　　　） |
| ６．情報セキュリティ事業者からの意見により |  |

**問10-5.　過去1年間に攻撃・被害を受けられたが、届け出なかった方にお伺いします。届出・相談を躊躇させる要因としては、どういったことがあげられますか。（○はいくつでも）**

|  |  |
| --- | --- |
| １．自社・団体の信用が低下するので | ７．面倒なので |
| ２．社・団体内で対応できたので | ８．競合他社に知られたくないので |
| ３．届出義務がないので | ９．届出するべきなのかわからなかった |
| ４．自社内だけの被害だったので | 10．どこに届ければいいかわからなかった |
| ５．実質的な被害が無かったので  ６．問題解決にならないので | 11．関連会社や取引先等が届け出たため  12．その他（ 　　　　） |

**問11.　不正アクセス等の攻撃・被害に遭われた場合の届出先を知っていますか。それはどこですか。（○は一つ）**

|  |
| --- |
| １．具体的な届出先（　　　　　　　　　　　　　　　　） |
| ２．わからない |

**問12.　不正アクセス禁止法では第８条において、アクセス管理者による防御措置について《努力義務》が規定されて**

**いますが、そのことを知っておられましたか。（○は一つ）**

|  |  |
| --- | --- |
| １．知っている | ２．知らなかった |

**問13.　情報セキュリティ対策を行っていますか。（○は一つ）**

|  |  |
| --- | --- |
| １．行っている  問13-1～13-7へお進みください | ２．行っていない又は把握していない  問13-8へお進みください |
|  |  |

**問13-1.** **問13で「１．行っている」と回答された方に伺います。情報セキュリティに関して、その運用、管理を  
専門に行う部署はありますか。（○は一つ）**

|  |  |  |
| --- | --- | --- |
| １．ある | ２．ない | ３．今後設置予定 |

**問13-2.　 問13で「１．行っている」と回答された方に伺います。情報セキュリティに関する管理体制は、どのよう  
になっていますか。（○はいくつでも）**

|  |  |
| --- | --- |
| １．情報セキュリティ担当役員（CISO等）を設置  ２．専従の担当者を設置 | ４．情報システム運用管理者以外の者が 情報セキュリティについて兼務 |
| ３．情報システム運用管理者が情報セキュリティに ついて兼務 | ５．設置していない |

**問13-3.　 問13で「１．行っている」と回答された方に伺います。情報セキュリティポリシー等は、策定されて  
いますか。（○は一つ）**

|  |  |
| --- | --- |
| １．策定している | ４．今のところ、策定する予定はない |
| ２．現在、策定作業中である | ５．策定しない |
| ３．今後、策定する予定である。 | ６．非公開情報のため、答えられない |

問13-3-1へお進みください

問13-4へお進みください

**問13-3-1.　 問13-3で「１．策定している」と回答された方に伺います。新型コロナウイルス感染対策又はテレワー  
ク業務の開始により、情報セキュリティポリシー等を変更しましたか。（○は一つ）**

|  |  |
| --- | --- |
| １．変更した | ３．変更することを検討している |
| ２．変更していない | ４．その他（ 　　　　） |

**問13-4.　 問13で「１．行っている」と回答された方に伺います。不正アクセス等の侵害事案が発生した場合のため  
に、現在、対応マニュアルや要領等を策定しておられますか。（○は一つ）**

|  |  |
| --- | --- |
| １．策定している | ４．策定する必要はない |
| ２．策定していないが、策定作業中 | ５．非公開情報のため、答えられない |
| ３．策定することを検討 |  |

**問13-5.　 問13で「１．行っている」と回答された方に伺います。情報システムのセキュリティ対策について、認証  
制度等を利用していますか。（○はいくつでも）**

|  |  |
| --- | --- |
| １．ISMS | ５．ISO 27017：クラウドセキュリティ認定 |
| ２．Pマーク | ６．IEC 62443：産業セキュリティ系認定 |
| ３．PCI DSS | ７．その他（ 　　　　 ） |
| ４．IPA セキュリティアクション宣言（二つ星） | ８．特に利用していない |

**問13-6.　 問13で「１．行っている」と回答された方に伺います。次年期（年単位）の情報セキュリティ対策の投資  
総額については、今年期（年単位）と比較してどのようになりますか（未定の場合は見込みでご回答ください）。（○は一つ）**

|  |  |
| --- | --- |
| １． 増額する予定 | ３． 減額する予定 |
| ２． 現状どおりの予定 | ４． 把握していない |

**問13-7.　 問13で「１．行っている」と回答された方に伺います。これらの経費に関しては、どういった問題点が考えられますか。（○はいくつでも）**

|  |  |
| --- | --- |
| １．コストがかかりすぎる | ７．トップの理解が得られない |
| ２．費用対効果が見えない | ８．情報を資産として考える習慣がない |
| ３．教育訓練が行き届かない | ９．最適なツール・サービスがない |
| ４．従業員への負担がかかりすぎる | 10．特に問題はない |
| ５．対策を構築するノウハウが不足している | 11．その他（ 　　　　 ） |
| ６．どこまで行えば良いのか基準が示されていない |  |

**問13-8.　問13で「２．行っていない又は把握していない」と回答された方に伺います。なぜ、情報セキュリティ対策  
を行っていませんか。（○はいくつでも）**

|  |
| --- |
| １．どのような対策を行えば良いか分からない |
| ２．情報セキュリティ対策の運用・管理を行う体制が確保できない |
| ３．情報セキュリティ対策を行う予算が確保できない |
| ４．情報セキュリティ対策を行うという概念がなかった |
| ５．情報セキュリティ対策は各職員に任せている |
| ６．情報セキュリティ対策は必要ないと考えている |
| ７．把握していない |
| ８．その他（　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　） |

**問14.　サプライチェーンリスク対策として、関連会社や取引先に情報セキュリティ対策を求めるなど何らかの対策を  
行っていますか。行っている場合はどのようなことを行っていますか。（○は一つ）**

|  |
| --- |
| １．行っている（　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　） |
| ２．行っていない |

**問15.　今後、どのようなことに重点をおいて、情報セキュリティ対策を行うべきだと考えておられますか。**

**下表の各行に考え方①、②の内容を比較し、より考え方が近いものをお選びください。（○は各項目一つ）**



1. **技術的対策**

**【端末装置（パソコン、スマートフォン等）やサーバ機器に対するセキュリティ対策について伺います】**

**問16.　 OSやアプリケーションのセキュリティ・パッチの適用や更新状況をお答えください。（○は一つ）**

|  |
| --- |
| １．頻繁（１か月に１回以上）にセキュリティ関連サイトを確認し、常に最新のパッチを適用している |
| ２．定期的（四半期～半年に１回程度）にセキュリティ関連サイトを確認し、必要なパッチを適用している |
| ３．定期的に確認はしていないが、サーバの管理者等の裁量で適用している |
| ４．パッチを適用していない |
| ５．問題が発生するまでパッチは適用しない |
| ６．わからない |
| ７．その他（ ） |

**【情報セキュリティサービスの利用状況について伺います】**

**問17.　現在、どのようなサービスを利用されていますか。（○はいくつでも）**

問18へお進みください

|  |  |
| --- | --- |
| １．Webアプリケーション診断 | 11．社外での研修による教育の実施 |
| ２．プラットフォーム診断 | 12．セキュリティ運用・監視 |
| ３．リスク分析 | 13．ウイルス等監視 |
| ４．ポリシー策定 | 14．セキュアシステム構築 |
| ５．セキュリティ監査 | 15．フォレンジックサービス |
| ６．ログ解析 | 16．ペネトレーションテスト |
| ７．パッチマネジメント | 17．緊急対応 |
| ８．ハウジングサービス | 18．損害保険（不正アクセス等対応） |
| ９．DDoS対策 | 19．その他（　　　　　　　　　　　　　　　　） |
| 10. 標的型攻撃対策 | 20．利用していない |

問17-1へお進みください

**問17-1.　問17で「20．利用していない」と回答された方に伺います。その理由は何故ですか。**

**（○はいくつでも）**

|  |
| --- |
| １．社・団体内に高い専門性やノウハウ、技術力があり、必要性がない |
| ２．社・団体内の担当者だけで必要な人員が確保されているため、必要性がない |
| ３．社・団体内にノウハウの蓄積を行いたい |
| ４．予算がない |
| ５．価格が見合わない |
| ６．要求に合致するサービスが提供されていない  （求める具体的なサービス例：　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　） |
| ７．機密情報の漏えいにつながることが懸念される |
| ８．その他（ 　　　　　　　　　　　　　　　　　　　　　　　　） |

**【ネットワークに対する情報セキュリティ対策について伺います】**

**問18.** **安全なアクセス環境を維持するために、どのような対策をされていますか。（○はいくつでも）**

|  |  |
| --- | --- |
| 1. ID、パスワード等による認証   ２．ファイアウォールの導入 | ９．アクセスログ収集の強化・充実  10．クラウドサービスの利用 |
| ３．ルータによるプロトコル制御 | 11．外部からの接続を伴うサービス等を |
| ４．PROXYサーバの設置 | 提供していない |
| ５．侵入検知・防御システム | 12. バックアップの取得 |
| （IDS・IPS）の導入 | 13. 常に最新のパッチを適用 |
| ６．検疫ネットワークシステムの利用 | 14．その他（　　　　　　　　　　） |
| ７．非武装地帯（DMZ）の構築 | 15．特に行っていない |
| ８．VPNの利用 |  |

問18-1へお進みください

問19へお進みください

**問18-1.　問18で「８．VPNの利用」と回答された方に伺います。VPN機器のセキュリティ対策として、どのような  
対策を行っていますか。（○はいくつでも）**

|  |
| --- |
| １．OS/ファームウェアの最新パッチを常に適用している |
| ２．不正アクセス、ランサムウェア等の被害に遭ったのでパッチを適用した |
| ３．報道等によりランサムウェア等の被害の原因になることを知ったのでパッチを適用した |
| ４．VPN機器への接続認証について、複雑なパスワード、ワンタイムパスワード、多要素認証などを設定している |
| ５．VPN機器への接続端末について、IPアドレスなどで規制している |
| ６．実施していない |

**問19.　問８でクラウドサービスを「１．使用している」と回答された方に伺います。**

**クラウドサービスを使用することになった理由は何ですか。（○はいくつでも）**

|  |
| --- |
| １．セキュリティ強化のため |
| ２．管理する技術が不足している、又は負担軽減のため |
| ３．管理する人的リソースが不足している、又は負担軽減のため |
| ４．管理する費用が不足している、又は負担軽減のため |
| ５．外出先（テレワーク先）から利用するため |
| ６．わからない |
| ７．その他（ 　　　　　　　　　　　　　　　） |

**問20.　問９で外部から内部ネットワークへの接続を「１．許可している」と回答された方に伺います。どのような報セキュリティ対策を講じておられますか。通信路に対する対策は、回答群Ａから、端末に対する対策は、回答群Ｂからそれぞれ選択してください。（○はいくつでも）**

|  |
| --- |
| **【回答群Ａ（通信路に対する対策）】**  １．ID・パスワード等による認証 |
| ２．MACアドレス、クライアント証明書等使用する端末機器の固有情報を用いた認証  ３．通信の暗号化 |
| ４．専用ネットワークセグメントの設定 |
| ５．ネットワークトラフィックの監視 |
| ６．クラウドサービスの利用  ７．その他（　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　） |
| **【回答群Ｂ（端末に対する対策）】**  １．ウイルス対策ソフト等の導入  ２．OS、アプリケーション等をアップデートする仕組みの導入  ３．使用するアプリケーションの制限（外部の端末機器に業務データが残らないアプリに限定等）  ４．内部データの暗号化  ５．各種ログの保管  ６．盗難対策（端末ロック、内部データの遠隔消去等）  ７．のぞき見防止  ８．その他（　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　） |

**問21.　問９で外部から内部ネットワークへの接続を「１．許可している」と回答された方に伺います。**

**従業員等が社外等からインターネット接続経由で業務アクセスを行う場合に利用しているのはどういった認証  
方法ですか。（○はいくつでも）**

|  |  |
| --- | --- |
| １．ID・パスワード等による認証 | ６．ＳＭＳ認証 |
| ２．ワンタイムパスワード  問21-1～21-2へお進みください | ７．その他（　　　　　　　　　　） |
| ３．ICカード・トークンデバイス型認証ツール | ８．認証なし |
| ４．電子証明書（PKI） |  |
| ５．バイオメトリクス（指紋等での認証） | 問21-2へお進みください |

**問21-1.****問21で「１．ＩＤ・パスワード等による認証」と回答された方に伺います。ＩＤ・パスワード等の管理を  
徹底するために、どのような対策をされていますか。(○はいくつでも）**

|  |
| --- |
| １．パスワード長を一定以上に定める |
| ２．定期的にパスワードを変更させる |
| ３．パスワードの複雑性をチェックし、簡単すぎるものは変更させる |
| ４．異動等で使用しなくなったIDはすぐに削除する |
| ５．IDをメールアドレス等の他の用途で流用しない |
| ６．IDを複数ユーザで使わせない |
| ７．ID・パスワードは利用者側の端末に保存されない |
| ８．会社等の組織が指定したパスワード管理ツールを使う |
| ９．その他（　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　） |
| 10．特に行っていない |

**問****21-2.　不正ログイン（他人のＩＤ・パスワードを無断で入力する不正アクセス行為）を防止するために、どのよう  
な対策をされていますか。（○はいくつでも）**

|  |
| --- |
| １．同一ID、パスワードを固定した繰り返し入力の規制 |
| ２．同一IPアドレスからの誤ったID・パスワードの繰り返し入力の規制 |
| ３．正規の利用者が使用する通信端末機器の事前登録 |
| ４．CAPTCHA（プログラムでは読み取り・入力が困難な符号の入力要求） |
| ５．多要素認証の導入 |
| ６．リスクベース認証の導入 |
| ７．その他（　　　　　　　　　 　　） |
| ８．特に行っていない |

**問22.　お客様などがフィッシング被害に遭わないための対策として、どのような対策をされていますか。  
（○はいくつでも）**

|  |
| --- |
| １．顧客に対する注意喚起 |
| ２．フィッシングサイトの監視 |
| ３．フィッシングサイト発見時の関係機関への通報 |
| ４．送信ドメイン認証（SPF、DKIM、DMARC）等の電子メールなりすまし対策 |
| ５．その他（　　　　　　　　 　　　） |
| ６．特に行っていない |
|  |

**【各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）に対するセキュリティ対策について伺います】**

**問23.　各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）を利用していますか。（○は一つ）**

|  |  |
| --- | --- |
| １．使用している | ２．使用していない |

問24へお進みください。

問23-1へお進みください。

**問23-1.　当該サービスは、どのように管理されていますか。（○は一つ）**

問24へお進みください。

|  |  |
| --- | --- |
| １．自社管理 | ３．全て外部業者に委託 |
| ２．一部外部業者に委託 |  |

問23-2～23-4へお進みください。

**問23-2.　 問23-1で「１．自社管理」「２．一部外部業者に委託」と回答された方に伺います。セキュリティ対策は、  
どのような取組みをされていますか。（○はいくつでも）**

|  |
| --- |
| １．常に最新のパッチを適用 |
| ２．管理者用アカウントのパスワードの複雑化 |
| ３．デフォルトアカウントを利用停止、または利用制限 |
| ４．セキュアコーディングの適用  ５．リモートアクセスの接続元を限定 |
| ６．Webコンテンツの変更履歴を定期的に確認 |
| ７．Webシステムの設定状況を定期的に確認 |
| ８．IDS,IPS,WAF等のセキュリティ機器やサービスを利用 |
| ９．その他（　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　） |

**問23-3.　 問23-1で「１．自社管理」「２．一部外部業者に委託」と回答された方に伺います。過去1年間にシステム  
のぜい弱性検査（ぺネトレーションテスト等）を実施しましたか。（○はいくつでも）**

|  |
| --- |
| １．定期点検のため実施 |
| ２．外部からの攻撃を受けた（可能性を含む）ため実施 |
| ３．関係業者、団体が被害に遭ったことを知ったため実施 |
| ４．その他（　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　） |
| ５．実施していない（理由：　　　　　　　　　　　　　　　　　　　　　　　　　　） |

**問23-4.　 問23-1で「１．自社管理」「２．一部外部業者に委託」と回答された方に伺います。ログは取得後、どれく  
らいの期間保管されていますか。また、どの様な方法で行っておられますか。（下表の各欄に、取得しているログの種類は該当する番号に〇を、ログの保管期間及び方法は回答群Ａ（保管期間）・Ｂ（方法）からそれぞれ回答を選び、番号をご記入ください。）**

**※　回答が複数あるときは、最も長い期間を選んでご記入ください。**

該当する選択肢の番号に〇

各解答欄に該当する回答群から当てはまる番号を記入

|  |  |  |
| --- | --- | --- |
| ログの種類 | 回答群Ａ | 回答群Ｂ |
| **回答例** |  |  |
| ４．プロキシサーバのログ | 5 | 1 |
| １．ファイアウォール・侵入検知システム等（IDS、IPS等）のログ |  |  |
| ２．ウェブサーバへのアクセスログ |  |  |
| ３．メールサーバのログ |  |  |
| ４．プロキシサーバのログ |  |  |
| ５．情報システムへの認証ログ |  |  |
| ６．データベースのログ |  |  |
| ７．クライアントPCのログ |  |  |
| ８．その他（　　　　　　　　　　　　　　　　　　　　） |  |  |
| ９．全く取得していない　　　　　　問24にお進みください。 |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **回答群　Ａ** | |  | **回答群　Ｂ** | |
| １．１週間以下  ２．１か月間  ３．３か月間  ４．６か月間  ５．１年間  ６．１年を超える | ７．決めていない  ８．その他  （　　　　　　　 ）  ９．保管していない  10．運用していない | １．自社  ２．外部委託  ３．その他  　（　　　　　　） |  |

問23-4-1へお進みください

**問23-4-1．問23-4で１～８の選択肢を回答された方に伺います。ログを取得・保管されているのは、どのような理由  
からですか。（○はいくつでも）**

|  |
| --- |
| １．不正アクセス等外部からの不正行為を記録するため |
| ２．従業員等内部の不正行為を記録するため |
| ３．システムの管理、改善等に役立てるため |
| ４．サービスその他業務に反映させるため |
| ５．料金請求に活用するなど、業務に必要であるため |
| ６．法令等により記録が義務づけられているため |
| ７．その他（　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　） |
| ８．特に目的はない |

**【電子メールに対する情報セキュリティ対策について伺います】**

**問24.　電子メールに関するセキュリティ対策では、どのような取組みをされていますか。（○はいくつでも）**

|  |
| --- |
| １．常に最新のパッチを適用  ２．不正中継の防止 |
| ３．フィルタリング（特定の条件を満たすメールの配信をしない） |
| ４．ウイルスチェック |
| ５．特定ドメイン・アドレスからのメールのみ送・受信 |
| ６．特定の拡張子を持つファイルが添付されている場合に送・受信を拒否 |
| ７．利用メールソフトの指定・制限 |
| ８．メール利用の制限  （利用可能者の限定、利用端末の限定、組織内は別のツールで連絡を行う　等） |
| ９．SPF（Sender　Policy　Framework）の導入 |
| 10．DKIM（DomainKeys Identified Mail）の導入 |
| 11．DMARC（Domain-based Message Authentication Reporting and Conformace）の導入 |
| 12．その他送信者認証 |
| 13．電子署名の利用 |
| 14. クラウドサービスの利用 |
| 15．無害化処理を実施 |
| 16．標的型メール受信訓練の実施 |
| 17．電子メールセキュリティ対策に関する教養 |
| 18．その他（ ） |
| 19．わからない |

**問25.　電子メールに添付されたファイルは、どのように取り扱っておられますか。（○はいくつでも）**

|  |
| --- |
| １．ウイルスチェックをしてから受信  ２．無害化、振る舞い検知等をしてから受信 |
| ３．パスワード設定の添付ファイルのみ受信 |
| ４．特定の拡張子を持つファイルが添付されている場合に受信を拒否 |
| ５．添付ファイル付きの電子メールは一切受信しない |
| ６．パスワード付き添付ファイルの禁止 |
| ７．特にチェック等はしていない  ８．その他（ ） |

**【不正アクセス、情報漏えい等に対する情報セキュリティ対策について伺います】**

**問26.　重要なシステム（基幹業務、製造　等に関わるシステム）への侵入阻止や侵入時における被害軽減に向けて、  
どのような対策を導入されていますか。（○はいくつでも）**

|  |
| --- |
| １．外部のネットワークに接続していない |
| ２．重要な基幹業務システムは他のネットワークと分離した専用ネットワークを構築している |
| ３．基幹業務システム専用のファイアウォール・ルータ（ネットワークアクセス制御機能）を導入している |
| ４．システムの冗長化（ネットワークの冗長化を含む）を行っている |
| ５．データのバックアップを行っている |
| ６．緊急時にはシステムを自動停止する仕組みを導入している |
| ７．指定回数以上のログイン失敗時のアカウント失効等、不正操作に対して自動的に制限をかける機能を導入している |
| ８．重要なシステムへの個人所有端末装置（パソコン、スマートフォン等）の接続制限を行っている |
| ９．無線LANの使用制限を行っている |
| 10．多要素認証を導入している |
| 11．その他（ 　　　　　　　　） |
| 12．上記1.～11.のような対策は行っていない |

**問27.　不正アクセス、データ改ざん、情報漏えい等の行為に対して、どのような対策を実施されていますか。  
（○はいくつでも）**

|  |  |
| --- | --- |
| １．情報資産へのアクセス権の設定 | 12．情報資産の暗号化 |
| ２．定期的なパスワード変更 | 13．内部ネットワークのファイアウォール、  侵入検知システム（IDS）の導入 |
| ３．許可していないソフトウェアの制限 |
| ４．ユーザアカウントの定期的なチェック  ５．アクセスログの取得、ログの分析 | 14．メールのフィルタリング  （添付ファイルの利用制限等） |
| 1. 個人認証のためのシステム導入 | 15. 外部Webサイトへのアクセス制限 |
| ７. 定期的なバックアップ  ８．バックアップの履歴管理 | 16. 端末装置等のエンドポイントセキュリティ製品  （EDR等）の導入 |
| ９．印刷物、電子媒体の持出し、廃棄管理 | 17．その他（ 　　　　 ） |
| 10． 端末装置（パソコン、スマートフォン等）廃棄時の適正なデータ消去 | 18．特に何も行っていない |
| 11．共有ID・パスワードの禁止 |  |

**問28.　ウイルスやマルウェア等の不正プログラムに対して、どのような対策を実施されていますか。  
（○はいくつでも）**

|  |  |
| --- | --- |
| １．ウイルス対策ソフト（クライアント）の使用 | ９．許可されていないソフトウェアのインストール制限 |
| ２．ウイルス対策ソフト（サーバ）の使用 | 10．ファイル等のダウンロード制限 |
| ３．パターンファイルを定期的に更新する （社員自らが更新） | 11．プロバイダのウイルス等駆除サービスの利用 |
| ４．パターンファイルを定期的に更新する （自動更新システムを利用） | 12．メールの添付ファイルの削除または実行制限 |
| ５．パターンファイルを定期的に更新する （管理者が手動で更新） | 13．USBメモリ等の外部記録媒体の使用禁止 |
| ６．パッチによるOS等のバージョンアップ （社員自らが更新） | 14. 検疫システムの導入 |
| ７．パッチによるOS等のバージョンアップ （自動更新システムを利用） | 15.その他（ ） |
| ８．パッチによるOS等のバージョンアップ （管理者が手動で更新） | 16. 実施していない |

**３．人的対策**

**【情報セキュリティ教育に関する取り組みについて伺います】**

**問29.　 現在、情報セキュリティ教育を行っておられますか。（○は一つ）**

問29-1～29-2へお進みください

問29-3へお進みください

|  |
| --- |
| １．実施している |
| ２．実施を予定している（具体的に実施計画を立てている） |
|  |
| ３．実施していない |

**問29-1.　 問29で「１．実施している」「２．実施を予定している」と回答された方に伺います。情報セキュリティに  
関する教育では、どのような内容を行っておられますか。（○はいくつでも）**

|  |  |
| --- | --- |
| １．情報セキュリティポリシー | ９．緊急時の対応 |
| ２．情報システム利用に係るモラル | 10．ソーシャルエンジニアリング対策 |
| ３．個人情報の保護・管理 | 11．技術的なセキュリティ対策 |
| ４．機密情報の保護・管理 | （システムぜい弱性、堅牢化設定等） |
| ５．ウイルス等のマルウェア対策 | 12．サイバー犯罪の防止 |
| ６．情報へのアクセス管理（パスワード管理等） | 13. クラウドの利用方法 |
| ７．社外ネットワークへの接続 | 14. テレワーク（リモート接続）関係 |
| ８．文書の管理 | 15．その他（ ） |

**問29-2.　 問29で「１．実施している」「２．実施を予定している」と回答された方に伺います。情報セキュリティに  
関する教育は、どのくらいの頻度で行われていますか。（○はいくつでも）**

|  |  |
| --- | --- |
| １．月に１回以上 | ４．２、３年に１回 |
| ２．年に数回 | ５．採用、異動時等に実施 |
| ３．年に１回 | ６．その他（ ） |

問29-2を回答後、問30へお進みください。

**問29-3.　 問29で「３．実施していない」と回答された方に伺います。なぜ実施しないのですか。（○はいくつでも）**

|  |  |
| --- | --- |
| １．指導できる者が社内にいない | ５．必要性が理解されない |
| ２．必要な資金がない | ６．何をしてよいかわからない |
| ３．環境的に必要ない | ７．その他（ ） |
| ４．必要な時間がない |  |

**問30．　セキュリティ人材（専門家）を確保するための施策を行っておられますか。（○はいくつでも）**

|  |  |
| --- | --- |
| １．社内勉強会の実施 | ５．セキュリティ人材のキャリアパス検討 |
| ２．セキュリティ関連の試験・資格の活用 | ６．専門人材の登用 |
| ３．部外セミナー等の受講 | ７．社内では人材育成しない（外部人材等の活用） |
| ４．セキュリティ団体(コミュニティ)への参加 | ８．その他（ ） |

**問31.　情報セキュリティ対策を実施するに当たって、困難に感じていることや、不正アクセス行為対策に対する不安  
等、または、本アンケート調査に対するご意見等がございましたら、次の空欄に記載してください。**

**アンケートはこれで終わりです。ご協力ありがとうございました。**

**お手数ですが、令和 ４年 ９月 ３０日(金) までに、ご返送ください。**

◆郵送での回答：同封の返信用封筒をご利用ください（切手は不要です）

◆電子メールでの回答：「cyber@researchworks.co.jp」 までお送りください