情報セキュリティに関するアンケート調査

Q1
自社の事業特性をふまえてセキュリティリスクを特定し、リスクが顕在化した場合に事業におよぼす影響を評価していますか。
以下の中から、最もあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：自社のセキュリティリスクを特定している
- ○ 実施済：特定した自社のセキュリティリスクが顕在化した場合に事業におよぼす影響を評価している
- ○ 定期的に見直し：定期的にセキュリティリスクの特定、評価を実施している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q2
リスクに対する具体的なセキュリティ対策の実施計画を立てていますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 中長期（３年程度）計画を立て、年単位で適宜見直ししている
- ○ 中長期計画を立てているが、見直ししていない
- ○ 直近 1 年以内の計画を立て、適宜見直ししている
- ○ 直近 1 年以内の計画を立てているが、見直ししていない
- ○ 今後計画を立てる予定である
- ○ 計画を立てる予定はない
- ○ その他（具体的に記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
- ○ わからない

Q3
定期的にセキュリティ対策の実施状況を評価し、足りていない対策を把握していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ セキュリティベンダや監査法人等の第三者評価を定期的に実施している
- ○ 自己評価を定期的に実施している
- ○ 第三者評価および自己評価をいずれも定期的に実施している
- ○ 今後定期的に評価を実施する予定である
- ○ 不定期に評価を実施している
- ○ いずれも実施する予定はない
- ○ その他（具体的に記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
- ○ わからない

Q4
直近 1 年に実施した情報セキュリティ対策の実施のきっかけや理由は何ですか。
以下の中から、最もよくあてはまるものを最大 3 つお選びください。

- ☐ 経営層のトップダウン指示
- ☐ 監督省庁からのセキュリティ対策強化の要請 (自治体からの要請を含む) （具体的な要請内容を記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
- ☐ 関連法規の改定（具体的な関連法規を記載）
＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
- ☐ 自社でのセキュリティインシデント
- ☐ 他社でのセキュリティインシデント事例
- ☐ 株主や取引先からの要請
- ☐ 持株会社や親会社からの要請
- ☐ 競合他社の実施状況との比較
- ☐ 外部監査・第三者評価の結果
- ☐ 内部監査・内部有識者からの指摘
- ☐ COVID-19 に伴うテレワーク対応
- ☐ 東京 2020 大会（オリンピック・パラリンピック）に伴う対応
- ☐ DX 化推進に伴う対応
- ☐ その他（具体的に記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
- ☐ わからない

Q5
情報セキュリティに関する脅威について、対策実施状況に関わらず、自社で最も脅威となる事象は何ですか。
以下の中から、最もよくあてはまるものを最大３つお選びください。

- ☐ 標的型攻撃による情報漏えい
- ☐ ランサムウェアによる被害（情報消失、金銭被害）
- ☐ サービス妨害攻撃（DDoS 攻撃等）によるサービス停止
- ☐ ビジネスメール詐欺（BEC）による金銭被害
- ☐ Web サイトの改ざん
- ☐ 自社 Web サービスへのリスト型アカウントハッキングによる被害（情報漏えい、サービス停止）
- ☐ 内部不正による被害（情報漏えい、業務停止）
- ☐ 退職者、転職者による在職時に利用していた情報の使用
- ☐ メールの誤送信・誤配信
- ☐ 情報機器、社員証等の置き忘れ、棄損による情報漏えい
- ☐ SaaS(ストレージサービス、チャット、web 会議ツール等)利用からの情報漏えい
- ☐ 顧客向けに提供している自社製品のセキュリティ侵害
- ☐ サプライチェーンからの情報漏えい
- ☐ クラウドサービス（IaaS/PaaS/SaaS）の設定ミスによる情報漏えい
- ☐ その他（具体的に記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
- ☐ わからない

Q6
セキュリティリスクへの対応計画を策定し、対策の実施状況を管理していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：対策の実施優先順位を決めている
- ○ 実施済：対策実施計画を策定し、計画の遂行状況を管理している
- ○ 定期的に見直し：定期的に対策実施計画を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q7
企業としてセキュリティリスクを管理する体制を構築し、役割と責任を定めていますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：セキュリティリスクを管理する担当者を任命、あるいは体制を構築している
- ○ 実施済：セキュリティリスクを管理する担当者や体制の役割と責任を定めている
- ○ 定期的に見直し：定期的にセキュリティリスクを管理する担当者や体制の役割と責任を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q8
サイバー攻撃の防御・検知に必要な情報を適宜収集・分析し、担当者に連携していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

○ 未実施

○ 一部実施：サイバー攻撃の防御・検知に必要な情報を収集し、分析可能な状態に加工している

○ 実施済：加工したサイバー攻撃の防御・検知に必要な情報を分析し、必要に応じて担当者に連携している

○ 定期的に見直し：定期的にサイバー攻撃の防御・検知に必要な情報の収集・分析・連携方法を見直している

○ 該当なし：実施する必要がない、実施しないことを決定した

Q9
セキュリティリスクへの対応方針と対策状況を開示すべき相手を定め、適切な方法で開示していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

○ 未実施

○ 一部実施：セキュリティリスクへの対応方針と対策状況を、求められた場合に都度開示している

○ 実施済：セキュリティリスクへの対応方針と対策状況を開示すべき相手を定め、適切な方法で開示している

○ 定期的に見直し：定期的に開示する内容を見直している

○ 該当なし：実施する必要がない、実施しないことを決定した

Q10
セキュリティインシデントの各種損害を補償する保険への加入を検討していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

○ 未実施

○ 一部実施：セキュリティインシデントの各種損害を補償する保険に関する情報を収集し、加入を検討している

○ 実施済：セキュリティインシデントの各種損害を補償する保険へ加入している、あるいは加入しないことに決めている

○ 定期的に見直し：定期的に契約内容や加入是非を見直している

○ 該当なし：実施する必要がない、実施しないことを決定した

Q11
セキュリティインシデントに関する保険の加入を決めた理由は何ですか。
以下の中から、最もよくあてはまるものを最大３つお選びください。

- ☐ 自社の対応だけでは被害を防ぎきれない可能性があるため
- ☐ 補償内容に対し、保険料が妥当だと感じたため
- ☐ 付帯サービスに魅力を感じたため（具体的な付帯サービスを記載）
  _____
- ☐ 事故発生時の見舞金等、支払う可能性がある金銭を補うため
- ☐ 事故発生時に迅速に対応するためのコストを捻出したいため
- ☐ 残留セキュリティリスクも適切に管理していることを株主・取引先にアピールするため
- ☐ 取引先や業務委託元等から加入の要請があったため
- ☐ トップダウン指示があったため
- ☐ 法制度改正等による処罰や制裁金が厳しくなっているため
- ☐ 関連企業、同業他社が加入しているため
- ☐ セキュリティリスクの高いビジネスを立ち上げたため
- ☐ サイバーセキュリティ経営ガイドラインで加入を推奨する記載があるため
- ☐ 情報漏えいなど、セキュリティ事件・事故のニュースを見聞きする機会が増えたため
- ☐ DX 化に伴い取り扱う情報やサービスが増えたため
- ☐ 加入していない
- ☐ その他（具体的に記載）_____
- ☐ わからない

Q12
企業のセキュリティ担当者として、最も対応に困っていることは何ですか。
以下の中から、最もよくあてはまるものを最大３つお選びください。

- ☐ セキュリティ業務の状況・進捗に関する経営層への報告
- ☐ セキュリティ脅威・事故に関する情報収集と関係者共有
- ☐ セキュリティ対策のトレンド・他社動向の把握
- ☐ セキュリティインシデント発生時の緊急対応
- ☐ サイバー攻撃の高度化への対応
- ☐ 東京 2020 大会（オリンピック・パラリンピック）に伴うサイバー攻撃の増加
- ☐ 自社セキュリティ対策の遅れ（最新技術・動向の未反映）
- ☐ グループ会社・国内外拠点のセキュリティ統制・管理
- ☐ 業務委託先や取引先のセキュリティ統制・管理
- ☐ テレワーク環境におけるセキュリティの確保
- ☐ DX 化に伴うデジタルサービスのリスク分析・把握
- ☐ セキュリティ人材の育成
- ☐ その他（具体的に記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
- ☐ 困っていることはない

Q13
IT 関連予算（情報セキュリティ関連予算を含む）は、どの程度を見込んでいますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 500 万円未満
- ○ 500 万円～１千万円未満
- ○ １千万円～３千万円未満
- ○ ３千万円～５千万円未満
- ○ ５千万円～１億円未満
- ○ １億円～５億円未満
- ○ ５億円～１０億円未満
- ○ １０億円～５０億円未満
- ○ ５０億円以上
- ○ 不明

Q14
IT 関連予算に対する情報セキュリティ関連予算は、どの程度を見込んでいますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 0%
- ○ 1%～5%未満
- ○ 5%～10%未満
- ○ 10%～15%未満
- ○ 15%～30%未満
- ○ 30%～45%未満
- ○ 45%～60%未満
- ○ 60%以上
- ○ 不明

Q15
情報セキュリティ関連予算のうち新規セキュリティ対策に投資する予算は昨年度と比べて変化はありますか？

	減額した、または減額する見込み	増額した、または増額する見込み	変化はない	不明
コーポレート IT*1 への新規セキュリティ対策投資　*1 自組織の業務プロセスで利用する内部向けの IT システム（基幹業務、経理、人事システム等）	○	○	○	○
ビジネス IT*2 への新規セキュリティ対策投資 *2 自組織の事業やビジネスで利用する外部向けの IT システム（オンラインショッピングサイトやスマホアプリ等	○	○	○	○

Q16
情報セキュリティの管理や、社内システムのセキュリティ対策に従事する人材の充足状況はいかがですか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 人材が過剰な状態
- ○ 充足している（最適な状態）
- ○ どちらかといえば充足している
- ○ どちらかといえば不足している
- ○ 不足している
- ○ わからない

Q17
人材が充足していると考える理由は何ですか。
以下の中から、最もよくあてはまるものを最大３つお選びください。

- ☐ セキュリティ業務が標準化されており、役割分担が明確化されているため
- ☐ セキュリティ業務の量が少ないため
- ☐ 想定していたほどの有事が少ないため
- ☐ セキュリティ業務がシステム等により自動化・省力化されているため
- ☐ セキュリティ業務は経験豊富な一部のメンバーで対応しているため
- ☐ セキュリティ業務を外部委託しているため
- ☐ 外部から経験豊富な人材を採用し、補充しているため
- ☐ 社内のセキュリティ人材を育成する仕組みを整備しているため
- ☐ 社内・グループ内異動等で、人員を補充しているため
- ☐ その他（具体的に記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
- ☐ わからない

Q18
人材が不足していると考える人材種別は何ですか。
以下の中から、最もよくあてはまるものを最大３つお選びください。

- ☐ セキュリティ戦略・企画を策定する人
- ☐ セキュリティリスクを評価・監査する人
- ☐ 経営層に対して適切な表現で、現状や対策内容等を説明・報告できる人
- ☐ 関係部署との調整をしながら、セキュリティ対策を推進・統括できる人
- ☐ セキュアなシステム設計ができる人
- ☐ セキュアなプログラミングができる人
- ☐ セキュリティインシデントへの対応・指揮ができる人
- ☐ ログを監視・分析して、危険な兆候をいち早く察知できる人
- ☐ ビジネス・事業部門側のセキュリティ担当者
- ☐ その他（具体的に記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
- ☐ わからない

Q19
自社が準拠すべき法令や基準、ガイドラインを認識し、セキュリティに関する要求事項に対応していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

○ 未実施

○ 一部実施：準拠すべき法令や基準、ガイドラインを把握している

○ 実施済：準拠すべき法令や基準、ガイドラインの要求事項を把握し、対応方針を決めている

○ 定期的に見直し：準拠すべき法令や基準、ガイドラインの改定箇所などを定期的に確認し、対応方針を見直している

○ 該当なし：実施する必要がない、実施しないことを決定した

Q20
情報セキュリティに係る戦略策定や自社・グループ会社のルール・ガイドライン策定の際に利用するフレームワーク、ガイドラインを教えてください。
以下の中から、あてはまるものを全てお選びください。

- [ ] ISO27001，2（ISMS JIS Q 27001，2）
- [ ] PCI DSS
- [ ] NIST Cyber Security Framework
- [ ] NIST SP800-171
- [ ] Cybersecurity Maturity Model Certification (CMMC)
- [ ] CIS Controls
- [ ] 業界特有の規制(HIPAA、 FFIEC CAT 発行の各種ガイドライン)
- [ ] サイバーセキュリティ経営ガイドライン
- [ ] IoT セキュリティガイドライン
- [ ] フレームワーク・ガイドラインは利用していない
- [ ] その他（具体的に記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
- [ ] わからない

Q21
2022 年 4 月の「改正個人情報保護法」の全面施行に向けた準備・対応状況についてお答えください。

	未対応	対応予定	全面施行前に対応完了予定	全面施行後に対応完了予定	分からない
個人情報保護関連ポリシーのアップデート	○	○	○	○	○
漏えい時の対応手順の整備	○	○	○	○	○
システム・技術的な対策	○	○	○	○	○

Q22
東京 2020 大会（オリンピック・パラリンピック）に向けたサイバーセキュリティ観点での対応についてお答えください。

	実施して、効果があった	実施したが、効果はなかった	実施したが、効果は不明	検討したが、実施していない	検討していない
大会の開催前に、インターネットに公開する web サイトやシステムのセキュリティ診断	○	○	○	○	○
大会開催前に、サイバーセキュリティ観点でのインシデント対応訓練や演習	○	○	○	○	○
大会期間中、セキュリティ担当者リソースを一時的に増強	○	○	○	○	○
大会期間中、セキュリティ監視のモニタリングレベルの強化	○	○	○	○	○

Q23
企業におけるセキュリティポリシーを定め、全従業員に周知していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：セキュリティポリシーを定めている
- ○ 実施済：セキュリティポリシーを定め、全従業員に周知している
- ○ 定期的に見直し：定期的にセキュリティポリシーの内容を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q24
人材雇用開始から終了までのセキュリティに関する責任と義務を定めて周知し、契約締結および義務の遂行を要求していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：在職中および退職後のセキュリティに関する責任と義務を定めている
- ○ 実施済：在職中および退職後のセキュリティに関する責任と義務を対象者に説明している
- ○ 定期的に見直し：定期的に責任と義務を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q25
グループ全体のセキュリティ対策実施状況を把握し、共通の対策を実施するなどしてグループ全体でセキュリティリスクを低減していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：グループ各社のセキュリティ対策状況を把握している
- ○ 実施済：グループ各社のセキュリティ対策状況を把握し、施策を実施している
- ○ 定期的に見直し：定期的にグループ全体のセキュリティ対策状況を把握し、施策を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q26
顧客や委託先との契約内容におけるセキュリティに関する責任分界点を契約書や仕様書で明確にしていますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：顧客や委託先との契約に求める双方の責任を把握している
- ○ 実施済：責任分界点を契約書や仕様書などで明記している
- ○ 定期的に見直し：定期的に記載内容を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q27
サプライチェーンのビジネスパートナーや委託先企業のセキュリティ対策状況を把握し、自社が定める水準を満たすよう適宜改善を求めていますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：サプライチェーンのセキュリティ対策状況を把握している
- ○ 実施済：サプライチェーンのセキュリティ対策状況を把握し、自社の水準を満たすために改善を要求している
- ○ 定期的に見直し：定期的にサプライチェーンの企業においてセキュリティ対策状況が改善されていることを確認している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q28
サプライチェーンにおけるセキュリティの対応状況についてお答えください。

	セキュリティ対策状況を把握している	セキュリティ対策状況を把握し、自社の水準をみたすため改善を要求している	セキュリティ対策状況が改善されていることを定期的に確認している	セキュリティ対策状況を把握していない	該当なし
国内の委託先企業やビジネスパートナー	○	○	○	○	○
海外の委託先企業やビジネスパートナー	○	○	○	○	○
国内の関連子会社やグループ会社	○	○	○	○	○
海外の関連子会社やグループ会社	○	○	○	○	○

Q29
サプライチェーンにおけるセキュリティの実態調査方法についてお答えください。
以下の中から、あてはまるものを全てお選びください。

- ☐ Excel ベースのアンケートやチェックシートによる調査
- ☐ Web ベースのアンケートによる調査
- ☐ TV 会議によるヒアリング調査・監査
- ☐ 現地監査
- ☐ インターネット接続機器や棚卸しや設定査定（アタックサーフェスマネジメント）
- ☐ 脅威情報の収集（スレットインテリジェンス）
- ☐ ベンダーリスクの継続的な管理（ベンダーリスクマネジメント）
- ☐ その他（具体的に記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

Q30
サプライチェーンに対するセキュリティ対応における課題についてお答えください。
以下の中から、あてはまるもの全てお選びください。

- [ ] サプライチェーン管理向けのセキュリティ予算を確保できない（本社・自社向けの対策予算がメイン）
- [ ] サプライチェーンの対象数（拠点や取引先）が多い
- [ ] 何から手をつければよいか分からない
- [ ] セキュリティ対応のリソースが自社向けで手一杯
- [ ] 取引先や委託先からセキュリティ対応の理解・協力が得られない
- [ ] アンケートでセキュリティを確認しているが、実効性の観点で不安がある。
- [ ] アンケートでセキュリティを確認しているが、確認内容を更新できていない
- [ ] 特に無し
- [ ] その他（具体的に記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

Q31
情報資産を重要度に応じて分類し、保管・廃棄方法などを定めていますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：情報資産の重要度分類を定義している
- ○ 実施済：資産の重要度別に保管・廃棄方法を定めている
- ○ 定期的に見直し：定期的に情報資産の重要度や管理方法を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q32
情報資産を方針に従って管理し、適切に管理されていることを確認していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：管理方針に従い情報資産を管理している
- ○ 実施済：情報資産の参照・変更・廃棄記録を取得している
- ○ 定期的に見直し：定期的に情報資産が適切に保管されているか確認している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q33
情報システムおよび情報セキュリティを統括する人材の設置状況についてお答えください。

	経営層が専任で就任	経営層が兼務で就任	非経営層が専任で就任	非経営層が兼務で就任	社外有識者が就任	未設置	わからない
CIO（最高情報システム責任者）	○	○	○	○	○	○	○
CISO（最高情報セキュリティ責任者）	○	○	○	○	○	○	○
CRO（最高リスク管理責任者）	○	○	○	○	○	○	○
CTO（最高技術責任者）	○	○	○	○	○	○	○
CDO(最高デジタル責任者)	○	○	○	○	○	○	○

Q34
セキュリティ業務にかかわる人材に必要な資質やスキルを整理し、獲得に必要な教育を実施していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：セキュリティ業務にかかわる人材に教育を実施している
- ○ 実施済：必要な資質やスキルを整理した上で教育を実施している
- ○ 定期的に見直し：定期的に必要な資質やスキル、および教育内容を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q35
セキュリティ業務を担当しない一般従業員に対し、必要なセキュリティ教育を実施していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：一般的なセキュリティに関する教育を実施している
- ○ 実施済：教育計画を立て、計画に従って教育を実施している
- ○ 定期的に見直し：定期的に身につけるべき知識、および教育内容を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q36
セキュリティ担当者向けに推奨している関連資格はありますか。
以下の中から、あてはまるものを全てお選びください。

- [ ] 情報セキュリティマネジメント
- [ ] 情報処理安全確保支援士
- [ ] CISSP(Certified Information Systems Security Professional)
- [ ] SANS GIAC(Global Information Assurance Certification)
- [ ] 公認情報セキュリティマネージャー（CISM）
- [ ] ネットワーク情報セキュリティマネージャー（NISM）
- [ ] 公認情報セキュリティ監査人(CAIS)
- [ ] 公認情報システム監査人(CISA)
- [ ] CompTIA Security+
- [ ] CEH (Certified Ethical Hacker)
- [ ] その他（具体的に記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
- [ ] 特に無し

Q37
メールを使ったサイバー攻撃を模した訓練メールを役職員へ送付して対応能力を測り、訓練結果をふまえて対策を実施していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：メールを使ったサイバー攻撃を模した訓練を実施している
- ○ 実施済：メールを使ったサイバー攻撃を模した訓練結果を元に、必要な対策を実施している
- ○ 定期的に見直し：定期的に訓練内容を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q38
場所毎に必要な物理セキュリティのレベルを定めて場所を区分し、重要な場所はモニタリングしていますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：場所毎に必要な物理セキュリティのレベルを定めて場所を区分している
- ○ 実施済：重要な場所は、入室後の挙動を監視している
- ○ 定期的に見直し：定期的に物理セキュリティレベルや場所の範囲を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q39
場所毎の物理セキュリティのレベルに応じて入退室時に最適な認証を実施し、認証の記録を取得していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：物理セキュリティのレベルに応じて、IC カード認証や生体認証などの認証方式を導入している
- ○ 実施済：入退室の記録を取得している
- ○ 定期的に見直し：定期的に認証方式を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q40
端末管理のルールを定め、離席時には PC をスクリーンロックし紛失防止のためにワイヤーロックや格納場所を施錠管理していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：端末管理のルールを定め、全従業員に周知する
- ○ 実施済：ルールをシステム的に強制、あるいは実施状況を確認している
- ○ 定期的に見直し：定期的にルールやソリューションを見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q41
ハードウェア資産をルールに則って調達・廃棄し、一覧管理していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：ハードウェア資産の調達・廃棄などのルールを定めている
- ○ 実施済：ハードウェア資産の調達・廃棄などのルールを定めて一覧管理している
- ○ 定期的に見直し：定期的にハードウェア資産の棚卸を実施している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q42
ソフトウェア資産を構成情報とライセンス情報を含めて一覧管理していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：管理対象のソフトウェアを把握している
- ○ 実施済：管理対象のソフトウェアを構成情報とライセンス含め一覧で管理している
- ○ 定期的に見直し：定期的にソフトウェア資産の棚卸を実施している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q43
システムやサービスを構成するハードウェアとソフトウェアの品目とバージョンを管理していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：管理対象のシステムやサービスを把握している
- ○ 実施済：管理対象のシステムやサービスを構成情報を含めて一覧で管理している
- ○ 定期的に見直し：定期的に構成情報が最新化されていることを確認し、管理対象を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q44
システムやアプリケーションの脆弱性を特定・評価し、対処するプロセスを整備していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：発見できた一部の脆弱性は対処している
- ○ 実施済：脆弱性情報の収集先を定め、収集した情報を評価した上で適時対処してる
- ○ 定期的に見直し：定期的に情報ソースや、脆弱性適用の判断基準を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q45
端末に対するセキュアな設定を標準化していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：端末に対する標準のセキュリティ設定を定めている
- ○ 実施済：標準化したセキュリティ設定を展開している
- ○ 定期的に見直し：定期的にセキュリティ設定を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q46
端末において未許可ソフトウェアのインストールや実行を制限していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：利用を許可する、あるいは許可しないソフトウェアを定めている
- ○ 実施済：未許可ソフトウェアのインストール制限、実行制限をしている
- ○ 定期的に見直し：定期的に許可する、あるいは許可しない対象のソフトウェアを見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q47
ネットワーク機器のバージョンを管理し、更新があった場合は最新の安定したバージョンをインストールしていますか。
以下の中から、最もよくあてはまるものを１つお選びください。

○ 未実施

○ 一部実施：管理対象のネットワーク機器を把握している

○ 実施済：管理対象のネットワーク機器のバージョンを管理し、最新のバージョンにアップデートしている

○ 定期的に見直し：定期的に情報が最新化されていることの確認、管理対象の見直しを実施している

○ 該当なし：実施する必要がない、実施しないことを決定した

Q48
自社のネットワーク構成図を作成し、業務に関わるすべての通信とデータを把握していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

○ 未実施

○ 一部実施：ネットワーク構成図は作成しているが、すべての通信とデータは把握できていない

○ 実施済：自社のネットワーク構成図を作成し、業務に関わるすべての通信とデータを把握している

○ 定期的に見直し：実態と構成図に差分がないか定期的に確認している

○ 該当なし：実施する必要がない、実施しないことを決定した

Q49
業務内容に応じてネットワークを分離（VLAN など）していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：重要度や業務内容に応じてネットワークを分離している
- ○ 実施済：定義した通りに分離されていることを確認している
- ○ 定期的に見直し：定期的に定義した通りに分離されていることを確認している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q50
リモートアクセス利用を許可するユーザや利用ルールを定め、周知していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：リモートアクセスを許可するユーザや利用に関するルールを定めている
- ○ 実施済：リモートアクセスを許可するユーザにルールを周知している
- ○ 定期的に見直し：定期的にリモートアクセスを許可するユーザやルールを見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q51
リモートアクセスを安全に利用するための対策を導入していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：リモートアクセスを安全に利用するために必要な対策を定義している
- ○ 実施済：定義した対策を導入し、安全に利用されていることを確認している
- ○ 定期的に見直し：定期的にリモートアクセスを安全に利用するための対策を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q52
外部からの不正な通信を検知し、必要に応じて遮断（IDS/IPS の導入など）していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：外部からの不正な通信を検知している
- ○ 実施済：検知した不正な通信を、必要に応じて遮断するか、あるいは代替手段で対処している
- ○ 定期的に見直し：検知傾向を分析し、定期的に不正な通信の定義や対処方法を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q53
テレワークの実施状況を教えてください。
以下の中から、最もよくあてはまるものを１つ選択してください。

- ○ COVID-19 以前より、テレワークを実施していた
- ○ COVID-19 の影響を受け、テレワークを実施し始めた
- ○ COVID-19 の影響を受け、テレワークの実施を検討している
- ○ テレワークは実施していない
- ○ その他（具体的に記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

Q54
テレワーク環境に関する今後の構想や見通しについて教えてください。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ COVID-19 が落ち着いた後も、原則テレワークを続ける予定
- ○ COVID-19 が落ち着いた後は、テレワークとオフィス出社を組み合わせる予定
- ○ COVID-19 が落ち着いた後は、オフィス出社に戻る予定
- ○ テレワーク環境の今後構想や見通しを検討していない
- ○ その他（具体的に記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

Q55
テレワークへの取り組みを進めるにあたって、阻害要因はありますか。
以下の中から、あてはまるものを全て選択してください。

- [ ] ビジネスの性質上、テレワークを行えない
- [ ] 予算配分や投資判断
- [ ] 情報セキュリティに関わる対応
- [ ] 労務管理
- [ ] テレワーク用端末の調達
- [ ] 自宅の業務環境の整備
- [ ] コミュニケーション不足
- [ ] 契約書の押印処理・送付業務
- [ ] 社内制度の整備
- [ ] その他（具体的に記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
- [ ] 課題はない
- [ ] わからない

Q56
テレワーク実施に伴う、セキュリティへの対応状況を教えてください。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ テレワークに伴うセキュリティ要件を把握し、対策を行っている
- ○ テレワークに伴うセキュリティ要件を把握しているが、対策を行えていない
- ○ テレワークに伴うセキュリティ要件を把握していない
- ○ わからない
- ○ その他（具体的に記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

Q57
ゼロトラスト*1 への取り組み状況について教えてください。
以下の中から、最もよくあてはまるものを１つお選びください。
*1 ネットワークの内部と外部を区別することなく、守るべき情報資産やシステムにアクセスするものは全て信用せずに検証することで、脅威を防ぐという新しいセキュリティの考え方

- ○ ゼロトラストを実装している
- ○ ゼロトラストを検討している
- ○ ゼロトラストを検討していない
- ○ 分からない
- ○ その他（具体的に記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

Q58
ゼロトラストの実装・検討目的について教えてください。
以下の中から、最もあてはまるものを最大 3 つお選びください。

- [ ] ニューノーマルな流れでテレワーク化が進展したため
- [ ] DX の進展に伴い、IT・セキュリティ戦略を見直すため
- [ ] 老朽化したインフラ・セキュリティを更改するため
- [ ] クラウドサービスを複数利用する環境になったため
- [ ] シャドーIT の利用に対する不安があったため
- [ ] 自社でセキュリティインシデントが発生したため
- [ ] 世間でセキュリティインシデントが多発しているため
- [ ] 同業他社がゼロトラストへの取り組みを行っているため
- [ ] 取引先やビジネスパートナーとのコラボレーションを活性化させるため
- [ ] ベンダーから推奨されたため
- [ ] その他（具体的に記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

Q59
無線通信の利用方針を定め、無線通信を許可するデバイスを管理し、無線通信データは暗号化や強固な認証方式を選択して保護していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：無線通信の利用方針を定めている
- ○ 実施済：利用方針に従い、無線通信を保護している
- ○ 定期的に見直し：定期的に無線通信の利用方針や保護策を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q60
自組織のネットワークに接続を許可する無線アクセスポイントを管理し、許可しない無線アクセスポイントが接続されていないことを確認していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：ネットワークに接続を許可する無線アクセスポイントを管理している
- ○ 実施済：許可しない無線アクセスポイントが接続されていないことを検知、対処している
- ○ 定期的に見直し：定期的に無線アクセスポイントの設置、管理方法について見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q61
外部に送信する情報や通信データを暗号化していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：外部に送信する情報や通信データの暗号化のポリシー・ルールを定義している
- ○ 実施済：外部に送信する情報や通信データをシステムで強制的に暗号化している
- ○ 定期的に見直し：定期的に暗号化方式が危殆化していないか確認している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q62
端末やサーバに保管するデータを暗号化していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：保存データの暗号化ポリシー・ルールを定義している
- ○ 実施済：保存データを強制的に暗号化している
- ○ 定期的に見直し：定期的に暗号化方式が危殆化していないか確認している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q63
重要なデータのバックアップを取得・保護し、リストアテストを実施していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：バックアップを取得し、保護している
- ○ 実施済：バックアップを定期的に取得し、保護している
- ○ 定期的に見直し：定期的にリストアテストを実施している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q64
アカウント管理のプロセスを整備し、定めたプロセスに従い管理していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：セキュリティ要件レベルに応じてアカウントを作成している
- ○ 実施済：プロセスを定めた上で、アカウントを作成・棚卸している
- ○ 定期的に見直し：定期的にアカウントを棚卸している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q65
ユーザが業務で利用するシステムにアクセスする際に、適切な方式で認証していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：ユーザが業務で利用するシステムにアクセスする際に認証している
- ○ 実施済：業務のセキュリティリスクに応じて適切な認証方式を選択している
- ○ 定期的に見直し：定期的に認証方式を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q66
アカウントのアクセス権限の割り当て方針を定め、アクセス権を管理していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：方針に従いアクセス権を割り当てている
- ○ 実施済：アクセス権を必要に応じて変更している
- ○ 定期的に見直し：定期的にアクセス権が正しく割り当てられていることを確認している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q67
各システムに求めるパスワードの強度や変更頻度を定め、適用していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：パスワードポリシーを定めている
- ○ 実施済：定めたポリシー通りにシステム的に制御、あるいはポリシーを徹底させている
- ○ 定期的に見直し：パスワードポリシーを定期的に見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q68
夜間ログインなど、通常と異なるアカウントの挙動を監視し、必要に応じて利用停止を含む是正処置を実行していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：通常と異なるアカウントの挙動を定義し、定期的にアカウントの利用状況を確認している
- ○ 実施済：通常と異なるアカウントの利用をリアルタイムで監視し、必要に応じて利用を停止するなど対処している
- ○ 定期的に見直し：定期的に通常と異なるアカウントの挙動の定義を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q69
受信メールの添付ファイルのマルウェア検知や、スパムチェックを実施していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：受信メールのセキュリティチェック観点を定める
- ○ 実施済：定めた観点に従い受信メールをチェックし、必要に応じて受信を制限している
- ○ 定期的に見直し：定期的にセキュリティチェック観点を見直す
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q70
メール送信時の宛先誤送信防止機能や、添付ファイル付きメール送信時の保留・承認機能を導入していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：送信メールのセキュリティチェック観点を定める
- ○ 実施済：定めた観点に従い送信メールをチェックしている
- ○ 定期的に見直し：定期的にセキュリティチェック観点や導入する機能を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q71
パターンマッチングによりマルウェア検知をする製品を端末やネットワーク機器に導入し、定期的にパターンファイルを最新化していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：パターンファイルとのマッチングによりマルウェア感染を検知している
- ○ 実施済：定期的にパターンファイルを最新化している
- ○ 定期的に見直し：定期的に検知方法を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q72
異常な挙動からマルウェアを検知する振る舞い検知型の製品を端末やネットワーク機器に導入していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：振る舞い検知型のエンジンによりマルウェア感染を検知している
- ○ 実施済：定期的にスキャンエンジンを更新している
- ○ 定期的に見直し：定期的に検知方法を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q73
端末ログを常時収集、不審な挙動をリアルタイムで可視化し、マルウェアに感染した場合に即時対応可能な製品を導入（EDR の導入など）していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：端末のログを取得・相関分析し、マルウェアの挙動を確認できる状態に可視化している
- ○ 実施済：可視化された内容から即時に対応できる状態にしている
- ○ 定期的に見直し：定期的に対応内容・方法を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q74
許可しない IP アドレスやポートを介した内外からの通信を拒否（FW の導入など）していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：許可しない IP アドレスやポートを介した内外からの通信を拒否している
- ○ 実施済：許可しない通信を拒否できていることを定期的に確認している
- ○ 定期的に見直し：定期的に許可しない通信の定義を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q75
すべてのインターネットアクセスのログを漏れなく取得できるように接続経路を集約（プロキシサーバの導入など）していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：一部のインターネット接続ログを取得している
- ○ 実施済：すべてのインターネット接続ログを漏れなく取得している
- ○ 定期的に見直し：定期的に通信内容を監査している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q76
アクセスを許可・禁止する Web サイトやカテゴリを定義・制限（コンテンツフィルタリングソフトウェアの導入など）していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：アクセスを許可・禁止する Web サイトやカテゴリを定義している
- ○ 実施済：定義通りに Web サイトへのアクセスを制限している
- ○ 定期的に見直し：定期的にアクセスを許可・禁止する Web サイトやカテゴリを見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q77
Web アプリケーションへの外部からの攻撃や侵入を検知・防止（WAF の導入など）していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：Web アプリケーションへの外部からの攻撃や侵入を検知している
- ○ 実施済：検知した Web アプリケーションへの外部からの攻撃や侵入を即時遮断するなど、防御している
- ○ 定期的に見直し：定期的に検知の条件や内容を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q78
通信量が異常に増加した際の、検知・対応方針を整備していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：通信量を監視している
- ○ 実施済：閾値を超えた通信量を検知した際の対応方針を定めている
- ○ 定期的に見直し：定期的に検知状況を確認している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q79
端末のアプリケーション単位での挙動や通信を検知し、不正な挙動や通信を検知・制御していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：端末の不正な挙動や通信を検知している
- ○ 実施済：検知内容に応じて端末の実行制限や通信遮断を実施している
- ○ 定期的に見直し：検知対象と制限条件を定期的に見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q80
クラウドサービス利用のポリシーを定め、周知していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：クラウドサービスを安全に利用するための方針やルールを定めている
- ○ 実施済：クラウドサービスの利用者に方針やルールを周知している
- ○ 定期的に見直し：定期的に方針やルールの内容を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q81
クラウドサービス利用のための申請や利用後の報告など、一連のプロセスを整備していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：クラウドサービス利用のプロセスを整備している
- ○ 実施済：定めたプロセスに従いクラウドサービス利用を管理している
- ○ 定期的に見直し：定期的にプロセスを見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q82
クラウドサービスの利用者側に求められるセキュリティ管理責任を理解し、適切に利用設定していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：クラウドサービスの利用者側で設定可能なセキュリティ対策を実施している
- ○ 実施済：利用者側のセキュリティ管理責任を理解した上で網羅的に設定を実施している
- ○ 定期的に見直し：定期的に適切なセキュリティ設定が実施されていることを確認している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q83
クラウドサービスへのアクセスを検査して利用状況を把握し、許可しないサービスの利用を制御していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：クラウドサービスへのアクセスを検査して利用状況を把握している
- ○ 実施済：許可しないサービスの利用をシステム的に制御している
- ○ 定期的に見直し：許可する、あるいは許可しないサービスを定期的に見直し、利用を制御できていることを確認している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q84
取得する対象や方法を定め、ログを取得していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：定めた方針に従いログを取得している
- ○ 実施済：定めた要件を満たすログが取得されていることを定期的に確認している
- ○ 定期的に見直し：定期的にログの取得対象や取得方法を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q85
ログを必要期間保管し、許可しないアクセスから保護していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：取得したログを必要な期間保管している
- ○ 実施済：ログを外部や遠隔地に保管するなど許可しないアクセスや災害から保護している
- ○ 定期的に見直し：ログが適切に保護され、不正なアクセスがないことを定期的に確認している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q86
ログを分析し、不審な挙動があった場合は担当者に通知するなどの対応をしていますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：ログを分析し、セキュリティイベントを検知している
- ○ 実施済：検知したイベントを内容に応じて通知、対応している
- ○ 定期的に見直し：定期的に分析手法や観点および対応方法を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q87
複数の情報源からログやデータを収集し、相互に関連付けて分析・可視化（SIEM の導入など）していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：複数のログを相関付けて分析し、セキュリティイベントを検知している
- ○ 実施済：相関分析により検知したイベントを内容に応じて通知、対応している
- ○ 定期的に見直し：相関分析するログやデータおよび分析手法を定期的に見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q88
特権アカウント発行の申請・承認のプロセスを整備していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

○ 未実施

○ 一部実施：特権アカウントを発行する際には記録を残しているが、申請・承認プロセスは整備されていない

○ 実施済：申請・承認プロセスを整備し、特権アカウントを発行する際の記録を適切に保管、管理している

○ 定期的に見直し：適切に管理されていることを定期的に確認し、プロセスを定期的に見直している

○ 該当なし：実施する必要がない、実施しないことを決定した

Q89
特権作業は作業者を特定できるアカウントを利用し、事前申請内容と実際の操作ログを突合していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

○ 未実施

○ 一部実施：特権作業者を特定できるようにしている

○ 実施済：事前申請内容と作業後の操作ログを突合して確認している

○ 定期的に見直し：作業確認・突合プロセス自体を見直している

○ 該当なし：実施する必要がない、実施しないことを決定した

Q90
システム開発におけるセキュリティを考慮した設計・実装・運用のポリシーを定め、周知していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：システム開発におけるセキュリティを考慮したポリシーを定めている
- ○ 実施済：定めたポリシーを担当者に周知している
- ○ 定期的に見直し：ポリシーを定期的に見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q91
セキュリティを考慮してシステムを設計していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：システム設計時に考慮すべきセキュリティ観点を整理している
- ○ 実施済：整理した観点に従ってシステムを設計している
- ○ 定期的に見直し：定期的にシステム設計時のセキュリティ観点を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q92
セキュリティを考慮してシステムの実装やテストを実施していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：システム実装時やテスト時に考慮すべきセキュリティ観点を整理している
- ○ 実施済：整理した観点に従ってシステム実装やテストしている
- ○ 定期的に見直し：定期的にシステム実装・テスト時のセキュリティ観点を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q93
セキュリティを考慮してシステムを運用していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：システム運用時に考慮すべき観点を整理している
- ○ 実施済：整理した観点に従ってシステムを運用している
- ○ 定期的に見直し：システム運用時のセキュリティ観点を定期的に見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q94
ソースコードをレビュー、あるいはスキャンツールを利用して脆弱性を発見していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：ソースコードレビューやスキャンを実施している
- ○ 実施済：リリース前に毎回、ソースコードレビューやスキャンを実施している
- ○ 定期的に見直し：定期的にソースコードレビューやスキャンを実施している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q95
侵入テスト（ペネトレーションテスト）を実施していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：侵入テストを実施している
- ○ 実施済：定期的に侵入テストを実施している
- ○ 定期的に見直し：最新の脅威に対抗できるよう侵入テストの観点を定期的に見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q96
開発案件のうち、「Agile 型」もしくは「DevOps 型」の開発手法の採用状況はいかがですか。
以下の中から、最もよくあてはまるものを 1 つお選びください。

- ○ 自社では開発をおこなっていない
- ○ Agile/DevOps 型以外（ウォーターフォール型等）で開発しており、Agile/DevOps 型の採用予定はない
- ○ Agile/DevOps 型以外（ウォーターフォール型等）で開発しているが、Agile/DevOps 型の採用を検討中
- ○ Agile/DevOps 型の採用しているが、拡大予定はない
- ○ Agile/DevOps 型の採用しており、今後拡大予定
- ○ 自社のほとんど全てのプロジェクトが Agile/DevOps 型

Q97
デジタルトランスフォーメーションの取り組み状況を教えてください。
以下の中から、最もよくあてはまるものを 1 つお選びください。

- ○ DX には取り組んでいない
- ○ DX への取り組みを検討している
- ○ コーポレート IT の DX に取り組んでいる
- ○ ビジネス IT の DX に取り組んでいる
- ○ コーポレート IT とビジネス IT に取り組んでいる
- ○ その他（具体的に記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

Q98
デジタルトランスフォーメーションの取り組みを進めるにあったって、阻害要因はありますか？
以下の中から、あてはまるものを全てお選びください。

- [ ] DX に対する経営の理解
- [ ] 縦割りの組織構造
- [ ] 新技術に対する理解や実装する能力を有した人員やリソースの確保
- [ ] 変化を受け入れる企業風土がない
- [ ] 情報セキュリティへの対応
- [ ] その他（具体的に記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
- [ ] 課題はない

Q99
デジタルトランスフォーメーションの取り組みを進めるにあたって、自社のセキュリティ戦略やルール、プロセスの見直しを行っていますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 検討中
- ○ 一部実施
- ○ 実施済
- ○ 見直しは不要
- ○ その他（具体的に記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

Q100
デジタルトランスフォーメーションの取り組みを進めるにあたって、どのようなプロセスの見直しを行っていますか？
以下の中から当てはまるものを全て答えてください。

- [ ] サービス企画段階でのリスク分析プロセスやルールの整備
- [ ] クラウドやマイクロサービスなどの技術に対応したガイドラインの整備
- [ ] クラウドを利用した開発環境でのセキュリティルールの見直し
- [ ] Agile 開発や DevOps に適した設計・開発・運用のセキュリティルールの整備
- [ ] サプライチェーン、サードパーティのリスクに対するルールの見直し
- [ ] その他（具体的に記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

Q101
導入済み、または関心のあるセキュリティ対策の新技術についてお答えください。

	導入済み・利用している	検証している/していた	検討中・関心がある	未検討・関心がない	知らない
UEBA (ユーザ行動に関わるログの統合分析とアラート)	○	○	○	○	○
SOAR (セキュリティアラート等への対応自動化)	○	○	○	○	○
EDR (遠隔での端末内潜伏脅威探索(スレットハンティング)とNW 隔離、フォレンジック対応)	○	○	○	○	○
CASB (クラウド利用の可視化・制御)	○	○	○	○	○
TLPT (脅威ベースのペネトレーションテスト)	○	○	○	○	○
IDaaS(クラウド型 ID・アクセス管理)	○	○	○	○	○
DMARC(電子メールの送信者なりすましといった不正を防ぐことを目的とした送信ドメイン認証)	○	○	○	○	○

脅威インテリジェンス(ダークウェブ監視および攻撃予兆・フィッシング・偽アプリ等の外部脅威情報の可視化・対策)	○	○	○	○	○
SAST(ソースコード解析ツール等によるアプリケーションセキュリティの静的テスト)	○	○	○	○	○
DAST(アプリケーションセキュリティの動的テスト)	○	○	○	○	○
IAST(アプリケーション稼働環境へのセキュリティテストの組み込み)	○	○	○	○	○
RASP(アプリケーション稼働環境に組み込み異常検出・防御する仕組み)	○	○	○	○	○
CSPM(クラウドセキュリティ態勢管理)	○	○	○	○	○

Q102
自社にとって重要な IT サービスを定め、事故や災害時に継続・早期復旧させるための準備態勢を整備していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：事故・災害時に継続、早期復旧が求められる重要な IT サービスを把握している
- ○ 実施済：事故・災害発生時に実施すべき手順書や連絡先一覧を作成するなど、準備態勢を整備している
- ○ 定期的に見直し：定期的に事故・災害を想定した訓練を実施し、準備態勢を見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q103
インシデント発生時の対応方針を定め、経営者の承認を得た上で周知していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：インシデント発生時の対応方針を定めている
- ○ 実施済：インシデント発生時の対応方針を定め、経営層の承認を得た上で周知している
- ○ 定期的に見直し：対応方針を定期的に見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q104
インシデント発生時の具体的な対応手順を定め、周知していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：インシデント発生時の連絡先や初動対応手順を定めている
- ○ 実施済：インシデント種別ごとの対応手順を定めている
- ○ 定期的に見直し：対応手順を定期的に見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q105
インシデント対応専門のチームを組成し、有事や平時の役割を定めていますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：インシデント対応専門のチームを組成している
- ○ 実施済：インシデント対応チームの有事と平時の役割と責任を定めている
- ○ 定期的に見直し：組織のメンバ、および役割と責任を定期的に見直している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q106
CSIRT の構築状況はいかがですか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 専任組織を構築済みで、有効に機能している
- ○ 専任組織を構築済みだが、有効に機能していない
- ○ 兼任組織(情報システム部門等)が類似機能を果たしており、有効に機能している
- ○ 兼任組織(情報システム部門等)が類似機能を果たしているが、有効に機能していない
- ○ CSIRT 運営は外部の業者に委託しており、有効に機能している
- ○ CSIRT 運営は外部の業者に委託しているが、有効に機能していていない
- ○ 現在、検討中もしくは構築中である
- ○ 検討していない
- ○ その他（具体的に記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
- ○ 分からない

Q107
インシデント対応チームを対象に訓練を実施していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：インシデント対応チームを対象に机上訓練を実施している
- ○ 実施済：インシデント対応チームを対象に実機訓練を実施している
- ○ 定期的に見直し：訓練内容を見直し、定期的に訓練を実施している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q108
インシデント対応チームだけでなく、関係各所や役職員も対象としたインシデント対応訓練を実施していますか。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 未実施
- ○ 一部実施：組織横断的に机上訓練を実施している
- ○ 実施済：組織横断的に実機訓練を実施している
- ○ 定期的に見直し：訓練内容を見直し、定期的に訓練を実施している
- ○ 該当なし：実施する必要がない、実施しないことを決定した

Q109
過去 1 年間で発生した情報セキュリティに関する事件・事故はありますか。
以下の中から、あてはまるものを全てお選びください。

- [ ] システム基盤（ミドルウェア、OS プラットフォーム 等）の脆弱性を突いた攻撃
- [ ] Web アプリケーションの脆弱性を突いた攻撃（例：バッファオーバーフロー、SQL インジェクション、ディレクトリトラバーサル、XSS 等）
- [ ] DoS 攻撃／DDoS 攻撃【※ Denial of Service attack の略。ネットワーク経由で大量のパケットの送信や不正な入力をし、サービスを停止に追い込む攻撃 ／ Distributed Denial of Service attack の略。ネットワーク上に分散したコンピュータを踏み台として行う DoS 攻撃】
- [ ] 自社サービスへのリスト型アカウントハッキング【※複数のサービスで同一 ID とパスワードを設定していることを悪用し、パスワード流出したサービスのパスワードリストで他のサービスへの不正アクセスを行う攻撃】
- [ ] 標的型メール攻撃【※特定の企業や組織を狙い、巧妙に偽装されたメールを送り、マルウェアに感染させることで情報を漏えいさせる攻撃】
- [ ] 水飲み場型攻撃【※攻撃対象のユーザがよくアクセスする Web サイトを改ざんし、その Web サイトにアクセスするだけでマルウェア感染させる攻撃】
- [ ] ランサムウェア【※PC 上のデータやシステムへのアクセスを制限し、その制限の解除に金銭を要求するマルウェア】による金銭等の要求
- [ ] マルウェア感染
- [ ] データ通信、音声通信等の盗聴・傍受
- [ ] 情報機器、電子記憶媒体、紙媒体等の盗難・紛失
- [ ] 廃棄された電子記憶媒体等からのデータ復元による情報漏えい

- [ ] システム管理者（特権ユーザ）等による不正アクセスや持出
- [ ] 業務アクセスが可能な一般ユーザによる不正アクセスや持出
- [ ] 退職者、転職者による在職時に利用していた情報の使用
- [ ] ショルダーハックによる盗み見
- [ ] サプライチェーン攻撃
- [ ] 電子メール、FAX 等の誤送信
- [ ] 社員証、業務書類等物品の紛失・置き忘れ・棄損
- [ ] 情報機器・外部記憶媒体の紛失・置き忘れ・棄損
- [ ] Web（SNS、掲示板等）への重要情報のアップロード
- [ ] システム設定ミス、誤操作
- [ ] クラウドサービスの設定ミスによる情報漏洩
- [ ] その他（具体的に記載）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
- [ ] 特になし
- [ ] わからない

Q110
過去 1 年間で、貴社に偽の送金指示メール・金銭の詐取を目的としたメールが届き、金銭被害にあいましたか？
以下の中から、最もよくあてはまるものを 1 つお選びください。

- ○ 会社に届いていないため、金銭被害にはあっていない
- ○ 役員・従業員に届いていたが、金銭被害にはあっていない
- ○ 金銭被害総額が、100 万円未満
- ○ 金銭被害総額が、100 万円～500 万円未満
- ○ 金銭被害総額が、500 万円～1000 万円未満
- ○ 金銭被害総額が、1000 万円～5000 万円未満
- ○ 金銭被害総額が、5000 万円～1 億円未満
- ○ 金銭被害総額が、1 億円以上（具体的に記載）

_____

- ○ わからない

Q111
ランサムウェアによる金銭被害についてお答えください。

	100 万円未満	100 万円～500 万円未満	500 万円～1000 万円未満	1000 万円～5000 万円未満	5000 万円～1 億円未満	1 億円以上	なし	分からない
身代金の要求額	○	○	○	○	○	○	○	○
身代金の支払額	○	○	○	○	○	○	○	○
ランサムウェアでの被害額（身代金の支払額は含まない）	○	○	○	○	○	○	○	○

Q112
あなたの所属する部署をお教えください。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 情報セキュリティ部
- ○ 情報システム部
- ○ その他の IT 部門（具体的に記載）
  _____
- ○ 総務部
- ○ 人事部
- ○ 法務部
- ○ コンプライアンス
- ○ 財務
- ○ 広報
- ○ リスク管理
- ○ 営業・販売
- ○ 研究開発
- ○ 事業部
- ○ 経営企画・事業開発
- ○ CIO (Chief Information Officer)
- ○ CISO (Chief Information Security Officer)
- ○ 役員・取締役
- ○ その他（具体的に記載） _____

Q113
貴社の業種をお教えください。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 機械・電気製品
- ○ 輸送機器・部品製造
- ○ 金属
- ○ 化学
- ○ バイオ・医薬品
- ○ 繊維・アパレル
- ○ 食品
- ○ 紙・パルプ
- ○ その他製品製造
- ○ その他素材・素材加工品
- ○ 銀行
- ○ 証券
- ○ 保険
- ○ その他の金融
- ○ 小売
- ○ 商社・卸売
- ○ 運輸
- ○ システム・ソフトウェア開発

- ○ メディア・広告
- ○ 通信
- ○ その他情報処理
- ○ エネルギー
- ○ 鉄道・航空
- ○ 建設
- ○ 不動産
- ○ 法人
- ○ 消費者
- ○ 医療
- ○ 教育
- ○ 飲食
- ○ その他（具体的に記載） _____

Q114
貴社の売上高（今期の予想）について教えてください。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 1 億円未満
- ○ 1 億円～10 億円未満
- ○ 10 億円～50 億円未満
- ○ 50 億円～100 億円未満
- ○ 100 億円～1000 億円未満
- ○ 1000 億円～5000 億円未満
- ○ 5000 億円～1 兆円未満
- ○ 1 兆円以上

Q115
貴社の従業員数について教えてください。
以下の中から、最もよくあてはまるものを１つお選びください。

- ○ 50 人未満
- ○ 50 人～100 人未満
- ○ 100 人～300 人未満
- ○ 300 人～1 千人未満
- ○ 1 千人～2 千人未満
- ○ 2 千人～5 千人未満
- ○ 5 千人～1 万人未満
- ○ 1 万人以上