アンケート調査票

- **本アンケートは、企業・組織でのテレワークの実施状況、および、関連するセキュリティについてお伺いしております。情報システムのご担当者、テレワークの推進をされている方に回答いただくことを想定しております。**
- **ご不明な設問がありましたら、必要に応じて他部門のご担当者様にご照会いただけますと幸いです。**

本アンケートで使用している表現について

- ✧ 「**現在**」は、2022 年 1 月 31 日時点と想定してお答えください。
- ✧ 「**テレワーク**」は、パソコン(PC)を使って電子データを取り扱う業務を社外で実施(在宅勤務・移動中のモバイルワーク・サテライトオフィス勤務等)することを指します。
- ✧ 「**会社支給 PC**」は、支給・貸与・有償・無償にかかわらず、あなたが属する企業・組織が準備し、社員(従業員・職員)に業務で使用させている PC を指します。
- ✧ 「**個人所有 PC**」は、従業員・職員が個人で準備した PC を指し、個人所有 PC の業務利用は BYOD といわれることもあります。

■テレワークの実施状況(Q1～Q6)

Q1. 貴社では、現在テレワークを実施していますか(または、これまでに実施したことがありますか)。
以下の中から当てはまるもの一つに〇をつけてください。(単一選択)

1. テレワークを実施している(実施していたことがある)
2. テレワークを実施したことはない

Q2. 貴社では、2022 年 4 月以降テレワークを実施しますか。
以下の中から当てはまるもの一つに〇をつけてください。(単一選択)

1. 実施する
2. 実施しない
3. 現在検討中
4. 未定

Q3～Q18 は、Q1 で「1.テレワークを実施している(実施していたことがある)」を選択された組織への設問です。
Q1 で「2.テレワークを実施したことはない」を選択された場合は Q19 へお進みください。

Q3. 貴社ではいつからテレワークを実施していますか(いましたか)。
以下の中から当てはまるもの一つに〇をつけてください。(単一選択)

1. 2020 年 4 月 6 日以前(初回の緊急事態宣言発出より以前)
2. 2020 年 4 月 7 日～2020 年 5 月 25 日(初回の緊急事態宣言中)
3. 2020 年 5 月 26 日～2020 年 9 月 30 日
4. 2020 年 10 月 1 日～2021 年 3 月 31 日
5. 2021 年 4 月 1 日～2021 年 9 月 30 日
6. 2021 年 10 月 1 日以降

Q4. 貴社では現在、全社員*のうちどの程度の割合の社員がテレワークを実施していますか（いましたか）。また、テレワークを実施している社員は、平均でどれくらいの頻度でテレワークを実施していますか（いましたか）。以下の中から、それぞれ当てはまるもの一つに○をつけてください。（割合・頻度それぞれ単一選択）

＊ 社員は、アルバイトやパート、派遣社員などすべてを含む従業員・職員と考えてお答えください。

＜テレワーク実施社員の割合＞

	1. 全社員の80％以上	2. 全社員の50％以上80％未満	3. 全社員の20％以上50％未満	4. 全社員の20％未満	5. 実施していない（実施する予定はない）
ピーク時(*) ⇒	1	2	3	4	5
現在 ⇒	1	2	3	4	5
2022年4月以降(想定) ⇒	1	2	3	4	5

（*） 2020年4月から現在までの間で最もテレワークの割合が高かった時期

＜平均的なテレワーク実施頻度＞

	1. 完全テレワーク（原則テレワーク）	2. 週3～4回程度	3. 週1～2回程度	4. ほとんどテレワークをしていない（原則出社）	5. 実施していない（実施する予定はない）
ピーク時(*) ⇒	1	2	3	4	5
現在 ⇒	1	2	3	4	5
2022年4月以降(想定) ⇒	1	2	3	4	5

（*） 2020年4月から現在までの間で最もテレワークの割合が高かった時期

Q5. 貴社では現在（現在テレワークを実施していない場合は、実施していた時点で）どの場所でのテレワークを認めていますか（いましたか）。以下の中から当てはまるもの全てに○をつけてください。（複数選択可）

1. 自宅（個人が所有する別荘等を含む）
2. サテライトオフィス・コワーキングスペース
3. カフェ・飲食店等
4. 移動時間中（電車、駅、空港等）
5. 自宅・サテライトオフィス以外のリゾート宿泊施設等（ワーケーション）
6. その他（具体的に　　）
7. 場所を限定していない

Q6. 貴社でテレワークのセキュリティ対策を実施するにあたり、現在（現在テレワークを実施していない場合は、実施していた時点で）課題と感じていることはありますか（ありましたか）。
以下に挙げた内容それぞれについて、当てはまるもの一つに〇をつけてください。
（矢印の方向ごとに1.～5.のうち一つずつ選択）（単一選択）

		1. 強く感じる	2. どちらかというと感じる	3. どちらかというと感じない	4. まったく感じない	5. わからない
セキュリティ対策に必要な要員の増強（要員確保）	⇒	1	2	3	4	5
セキュリティ対策に必要な要員の能力向上（人材育成）	⇒	1	2	3	4	5
社員へのルール徹底、順守状況の確認（ガバナンス）	⇒	1	2	3	4	5
機密管理が十分な執務環境の確保（執務環境）	⇒	1	2	3	4	5
セキュリティインシデント発生時の対応（インシデント対応力）	⇒	1	2	3	4	5

■テレワークに関する社内規則・ルール（Q7～Q10）

Q7. 貴社では、緊急事態宣言中またはコロナ禍の影響により特例や例外を認めなければならない
セキュリティ対策の社内規程・規則・手順等はありましたか。
以下に挙げたルールそれぞれについて、当てはまるもの一つに○をつけてください。
（矢印の方向ごとに 1.～5.のうち一つずつ選択）（単一選択）

		1. もともと社内規程・規則・手順等で認めている	2. 一時的にやむを得ず特例や例外を認めたが、その後社内規程・規則・手順を変更した	3. 一時的にやむを得ず特例や例外を認め、現在も認めている	4. 一時的にやむを得ず特例や例外を認めたが、現在は認めていない	5. 特例や例外を認めたことはなく禁止している
機密情報の社外持ち出し（機密情報が含まれる書類・USB メモリ等の電子記録媒体）	⇒	1	2	3	4	5
機密情報の個人所有 PC への保存（メール等での個人所有 PC への情報の転送等）	⇒	1	2	3	4	5
機密情報が保存することができる会社支給 PC の持ち出し	⇒	1	2	3	4	5
機密情報の社外（自宅・サテライトオフィス等）での印刷	⇒	1	2	3	4	5
機密情報のクラウドストレージサービスへの保存	⇒	1	2	3	4	5
個人所有 PC の業務利用（BYOD）	⇒	1	2	3	4	5
会社が許可していないアプリケーション・ソフトウェア・クラウドサービスの業務利用	⇒	1	2	3	4	5

Q8. 貴社では、社員がテレワークに関する社内規程・規則・手順等が守られていることを何らかの方法で確認していますか（いましたか）。

以下の中から当てはまるもの全てに〇をつけてください。（複数選択可）

1. 規定・規則・手順の順守状況について確認（自己申告）している（いた）
2. 規定・規則・手順の順守状況について点検（上司や自分以外の人が）している（いた）
3. 規定・規則・手順の順守状況について監査（第三者(*)が）している（いた）
4. 確認していない（いなかった）

(*) 外部機関だけでなく、業務で直接関わりのない社内の第三者的な組織や人を含む

Q9.貴社では 2020 年 4 月以降現在までに社内規則・ルール違反、過失等が発生しましたか。

以下の中から当てはまるもの全てに〇をつけてください。（複数選択可）

1. 会社で禁止している機密情報の社外持ち出し（機密情報が含まれる書類・USB メモリ等の電子記録媒体）
2. 会社で禁止している機密情報の個人所有 PC への保存（メール等での個人所有 PC への情報の転送等）
3. 会社で禁止している機密情報が保存することができる会社支給 PC の持ち出し
4. 会社で禁止している機密情報の社外（自宅・サテライトオフィス等）での印刷
5. 会社で禁止している機密情報のクラウドストレージサービスへの保存
6. 会社が許可していない個人所有 PC の業務利用（BYOD）
7. 会社が許可していないアプリケーション・ソフトウェア・クラウドサービスの業務利用
8. その他（具体的に　　）
9. 発生していない

Q10.貴社のテレワーク実施に関するセキュリティ対策の社内規程・規則・手順等について、現在（現在テレワークを実施していない場合は、実施していた時点で）課題と感じている点がありますか。

以下の中から当てはまるもの全てに〇をつけてください。（複数選択可）

1. 働き方の変化に対応していない
2. 社員の理解が不十分
3. ルールが周知できていない
4. 曖昧な部分が多い
5. 必要な情報がどこに書かれているか分かりづらい
6. リスクと規則が見合っていない
7. 実現困難なことを求めている
8. 現場に負担がかかっている
9. その他（具体的に　　）
10. 課題と感じている点はない

■テレワーク実施時のインシデント（Q11～Q12）

Q11.貴社では、テレワーク導入後、セキュリティインシデントへの対応体制や手順をチェック(再検討)しましたか。
また、チェックの結果、対応体制や手順を変更しましたか。
以下に挙げたルールそれぞれについて、当てはまるもの一つに○をつけてください。
（矢印の方向ごとに 1.～4.のうち一つずつ選択）（単一選択）

	1. チェックし、変更した	2. チェックしたが、変更はしなかった	3. チェックはしていない	4. もともとセキュリティインシデントへの対応体制や手順の取り決めがなかった
セキュリティインシデント発生時の対応マニュアル ⇒	1	2	3	4
セキュリティインシデント発生時の連絡体制（社外から問い合わせできる連絡先） ⇒	1	2	3	4
システム障害対策を含む IT-BCP の計画・体制 ⇒	1	2	3	4
セキュリティインシデント対応の教育訓練の内容 ⇒	1	2	3	4

Q12.貴社では、緊急事態宣言後(2020 年 4 月以降)、社員のテレワーク実施中にどのようなセキュリティインシデントが発生しましたか。
以下の中から当てはまるもの全てに○をつけてください。（複数選択可）

1. テレワークで利用する PC のマルウェア感染
2. テレワークで利用する PC からの情報漏えい
3. テレワークで利用する PC の紛失・盗難
4. 自宅ルータのマルウェア感染
5. 自宅ネットワークの盗聴
6. Web 会議ツールのセキュリティ上の問題（脆弱性を悪用した攻撃・情報漏えい等）
7. クラウド・SNS のセキュリティ上の問題（機密ファイルの流出、風評被害の発生等）
8. メールの誤送信
9. 紙資料や書類・USB メモリ等の電子記録媒体の紛失・盗難
10. その他（具体的に　　）
11. セキュリティインシデントは発生していない
12. セキュリティインシデントが発生しているか把握できていない

■個人所有 PC の業務利用（BYOD）（Q13～Q18）

Q13.貴社がテレワーク業務で利用を許可している（していた）PC は会社支給 PC ですか、それとも個人所有 PC ですか。

以下の中から当てはまるもの一つに〇をつけてください。（単一選択）

1.	すべて会社支給 PC であり個人所有 PC の利用は認められていない⇒Q19 へお進みください
2.	多くが会社支給 PC だが、一部は個人所有 PC の利用も認めている
3.	個人所有 PC の利用が認められているが、必要であれば会社から支給する場合もある
4.	すべて個人所有 PC である。（個人所有 PC の利用を会社が認めている）
5.	テレワーク業務で PC は利用していない ⇒Q19 へお進みください

Q14～Q18 は、Q13 で「個人所有 PC の利用を認めている（選択肢 2, 3, 4 のいずれか一つ）」を選択された組織への設問です。

Q14.貴社では、現在（現在テレワークを実施していない場合は、実施していた時点で）社員が個人所有 PC のテレワーク業務での利用を減らしていきたい（または増やしていきたい）という意向はありますか（ありましたか）。

以下の中から当てはまるもの一つに〇をつけてください。（単一選択）

1.	今後減らしていきたい	⇒Q15 へお進みください
2.	今後増やしていきたい	⇒Q16 へお進みください
3.	今のままで良い	⇒Q17 へお進みください

Q15 は、Q14 で「1. 今後減らしていきたい」を選択された組織への設問です。

Q15.貴社が個人所有 PC の業務利用を「今後減らしていきたい」と考える理由は何ですか。

以下の中から当てはまるもの全てに〇をつけてください。（複数選択可）

1.	PC のセキュリティ対策が不安である
2.	PC を利用した副業や家族等との共同利用による情報漏えいを防止したい
3.	PC のスペックの違い（処理能力、カメラの有無など）による業務効率の低下を防ぎたい
4.	従業員のプライバシー保護などの問題を減らしたい
5.	個人所有 PC の業務利用の為にルールや規定が複雑になることを防止したい
6.	その他（具体的に ）

Q16 は、Q14 で「2. 今後増やしていきたい」を選択された組織への設問です。

Q16.貴社が個人所有 PC の業務利用を「今後増やしていきたい」と考える理由は何ですか。

以下の中から当てはまるもの全てに〇をつけてください。（複数選択可）

1.	会社支給 PC を管理することが困難(管理する要員やツールなどのリソース不足)
2.	会社支給 PC を準備する予算が確保できない（コスト不足）
3.	従業員の満足度向上（複数の PC を持たなくてよい、使い慣れたものが使える）
4.	その他（具体的に ）

Q17.貴社では、現在（現在テレワークを実施していない場合は、実施していた時点で）個人所有 PC を業務利用する際にどのようなセキュリティ対策を要求(ルール化)していますか（いましたか）。

以下の中から当てはまるもの全てに〇をつけてください。（複数選択可）

1. 個人所有 PC の業務での利用範囲・用途
2. 業務利用する個人所有 PC の情報を会社に登録
3. 個人所有 PC にマルウェア対策ソフトを導入
4. 個人所有 PC にパスワードを設定
5. 盗難防止対策の実施（ワイヤーロック等）
6. 個人所有 PC の OS を常に最新状態にアップデート
7. 複数人（家族等）で共有している PC のテレワークでの利用禁止
8. 不審な電子メールの添付ファイル開封・リンク先クリックの禁止
9. 自宅ルータのパスワード設定ルール
10. フリーメールの利用ルール
11. 個人所有 PC で利用してはいけないクラウドサービスの指定
12. 個人所有 PC への業務データダウンロードの制限
13. 個人所有 PC に保存する業務データの暗号化
14. 個人所有 PC で利用してはいけないソフトウェア・アプリケーションの指定
15. その他（具体的に　　）
16. ルールは定められていない

Q18.個人所有 PC を利用して業務を行うこと(BYOD)について、課題と考えていることはありますか。

以下の中から当てはまるもの全てに〇をつけてください。（複数選択可）

1. PC のマルウェア感染
2. PC からの情報漏えい
3. PC の紛失・盗難
4. 自宅ルータのマルウェア感染
5. 自宅ネットワークの盗聴
6. セキュリティインシデント発生時の対応（状況把握が困難、対応の遅れ等）
7. セキュリティインシデント発生時の PC の証拠保全が困難
8. 会社が把握していない PC の利用
9. PC への社内規則の適用が困難
10. PC を利用した副業や家族等との共同利用
11. その他（具体的に　　）
12. 課題に思うことはない

■委託先企業のテレワーク（Q19～Q23）

Q19.貴社では委託先企業がテレワークを実施することを認めていますか。

以下の中から当てはまるもの一つに○をつけてください。（単一選択）

1. テレワークの実施を認めていない	⇒Q23 へお進みください
2. 機密性の高い情報を扱う場合等に限りテレワークを認めていない	⇒Q20 へお進みください
3. テレワークの実施を制限していない	⇒Q20 へお進みください
4. テレワークを実施している委託先は無い	⇒Q24 へお進みください

Q20～Q22 は、Q19 で「2.機密性の高い情報を扱う場合等に限りテレワークを認めていない」もしくは「3.テレワークの実施を制限していない」を選択された組織への設問です。

Q20.貴社では 2021 年 4 月 1 日から現在までの業務委託契約において、委託先企業との間の契約書・仕様書／利用規約・SLA の中で、以下に示すような情報セキュリティ上の要求事項を取り決めましたか。

以下に挙げた要求事項それぞれについて、当てはまるもの一つに○をつけてください。

（矢印の方向ごとに 1.～4.のうち一つずつ選択）（単一選択）

		1. 取り決めている	2. 取り決めていないが、今後取り決める予定である	3. 取り決めていないが、今後検討する必要がある（検討したい）	4. 取り決めておらず、今後も取り決める予定はない
テレワークの実施可否	⇒	1	2	3	4
テレワークで実施して良い業務、もしくは テレワークで実施してはいけない業務	⇒	1	2	3	4
テレワーク時に利用する PC への ウイルス対策ソフトの導入	⇒	1	2	3	4
テレワーク時に利用する PC への 機密情報の保存禁止	⇒	1	2	3	4
テレワーク環境への電子記憶媒体や紙資料・書類による機密情報の持ち出し禁止	⇒	1	2	3	4
テレワーク環境の限定（自宅、帰省先、サテライトオフィス、移動中など）	⇒	1	2	3	4
個人所有 PC の利用可否	⇒	1	2	3	4
個人所有 PC で実施して良い業務、もしくは 個人所有 PC で実施してはいけない業務	⇒	1	2	3	4

Q21.委託先企業のテレワークのセキュリティ対策状況について、貴社が課題として認識していることはありますか。
以下の中から当てはまるもの全てに〇をつけてください。（複数選択可）

1. テレワーク時に利用する PC にウイルス対策ソフトが導入されているか
2. テレワーク時に利用する PC に機密情報を保存していないか
3. テレワーク環境に電子記憶媒体や紙資料・書類で機密情報を持ち出していないか
4. テレワーク環境が限定されているか（自宅、帰省先、サテライトオフィス、移動中など）
5. セキュリティインシデント発生時の対応が遅れるのではないか
6. その他（具体的に　　）
7. 特に課題はない

Q22. 貴社では委託先企業がテレワークで業務を実施するようになってから、委託先企業に対して不安を感じることはありますか。
以下に挙げた事項それぞれについて、当てはまるもの一つに〇をつけてください。
（矢印の方向ごとに 1.～5.のうち一つずつ選択）（単一選択）

	1. 強く感じる	2. どちらかというと感じる	3. どちらかというと感じない	4. まったく感じない	5. わからない
契約書や仕様書等に定める規則、ルール等の要求事項の順守 ⇒	1	2	3	4	5
ガバナンスの確保 ⇒	1	2	3	4	5
コンプライアンスの確保 ⇒	1	2	3	4	5
セキュリティインシデント発生時の対応体制や対応力 ⇒	1	2	3	4	5
コミュニケーション、情報共有 ⇒	1	2	3	4	5
技術力、提案力等のスキル ⇒	1	2	3	4	5

Q23 は、Q19 で「1. テレワークの実施を認めていない」を選択された組織への設問です。

Q23.貴社が、委託先企業にテレワークを認めていない理由は何でしょうか。

以下の中から当てはまるもの全てに○をつけてください。（複数選択可）

1. 情報セキュリティ上のリスクが高いと考えられているから
2. セキュリティインシデント発生時に現場(オンサイト)の対応者がいてほしいから
3. 契約期間が継続中である業務委託契約の条件が現場(オンサイト)での業務を要求しており、これを変更していないから
4. テレワークでは実施できない業務を委託しているから
5. 社内あるいはグループの規則で定められているから
6. 業界ルールや上位の契約などで定められているから
7. その他（具体的に　　）

■SaaS(*)の選定条件やセキュリティ対策（Q24～Q28）

(*)Software as a Service：インターネットを通じてソフトウェアやアプリケーションを利用するサービス。

Q24.貴社ではどのような SaaS を利用していますか。

以下に挙げたサービスそれぞれについて、当てはまるもの一つに○をつけてください。

（矢印の方向ごとに 1.～4.のうち一つずつ選択）（単一選択）

	1. 2020年4月**以前**から利用している	2. 2020年4月**以降**から利用している	3. SaaSは利用していない（社内システム利用）	4. 利用していない
社内のファイル保管・データ共有 ⇒	1	2	3	4
電子メール ⇒	1	2	3	4
Web 会議 ⇒	1	2	3	4
電子承認 ⇒	1	2	3	4
社内情報共有・ポータル ⇒	1	2	3	4
スケジュール共有 ⇒	1	2	3	4
給与・財務会計・人事（評価／採用など）・勤務管理 ⇒	1	2	3	4
データバックアップ ⇒	1	2	3	4
動画配信・ウェビナー ⇒	1	2	3	4
名刺管理・顧客管理 ⇒	1	2	3	4
e ラーニング ⇒	1	2	3	4
取引先との情報共有 ⇒	1	2	3	4
プロジェクト管理 ⇒	1	2	3	4
受注販売 ⇒	1	2	3	4
システム開発・web サイト構築 ⇒	1	2	3	4
生産・物流・店舗管理 ⇒	1	2	3	4
調達 ⇒	1	2	3	4
セキュリティ（認証システム／WAF／脆弱性診断など） ⇒	1	2	3	4
課金・決済システム ⇒	1	2	3	4
研究・開発関係 ⇒	1	2	3	4
その他（　　） ⇒	1	2	3	4

Q25.貴社で SaaS を選定する際(選定した際)に重要視する(した)セキュリティ対策の内容は何ですか。

以下の中から当てはまるものに〇をつけてください。(最大 3 つまで)

1. SaaS 事業者の信頼性（財務状況、利用者社数、認証制度(*1)の取得状況、外部機関からの評価(*2)など）
2. 稼働率
3. 不正アクセス防止対策
4. 不正ログイン対策
5. 脆弱性対策
6. データ消失対策（データが消失しない対策(冗長化やバックアップなど）が整えられている）
7. 障害検知・復旧対策（障害発生時にできるだけ早く復旧できる環境や体制が整えられている）
8. 災害対策（災害や停電などが発生した場合でも、業務継続できる）
9. ヒューマンエラー対策（人による不注意やプログラムの設定漏れなど、ミスが発生しにくい体制が整えられている）
10. 保守体制（使い方がわからないときの支援（ヘルプデスクや FAQ)が提供されている）
11. SaaS が終了したときのデータの取扱い(完全に消去されることが保証されている）
12. SaaS 事業者の再委託先を含めた管理監督責任
13. 特にない
14. わからない　⇒Q29 へお進みください
15. SaaS は利用していない　⇒Q29 へお進みください

(*1)ISMAP や ISMS などの認証の取得など

(*2)外部機関による受賞歴など

Q26～Q28 は Q25 で 1.～13. を選択された組織への設問です。

Q26.貴社では、SaaS のセキュリティ対策についてどのような意識をもっていますか。

以下の中から当てはまるもの一つに〇をつけてください。(単一選択)

1. SaaS 提供事業者側の責任で実施するべき
2. SaaS 利用者側の責任で実施するべき
3. SaaS 提供事業者と SaaS 利用者が話し合い、双方の責任分界点を決めて実施するべき
4. わからない

Q27. SaaS 利用者側の設定不備が起因で発生した情報漏えい事故をきっかけに貴社で行った事はありますか。
以下の中から当てはまるもの全てに〇をつけてください。（複数選択可）

1. 現状の設定内容の確認や見直し
2. 設定内容について SaaS 提供事業者に問い合わせた
3. 契約内容や約款内容の確認や見直し
4. 契約や約款の内容について SaaS 提供事業者に問い合わせた
5. クラウドセキュリティポスチャ管理（CSPM）を導入もしくは検討
6. 設定確認ルール（タイミング、担当者等）の制定や見直し
7. 利用者への注意喚起
8. サービス利用停止や他のサービスへの移行
9. 対策は実施していない
10. その他（具体的に　　）
11. わからない

Q28.貴社では、SaaS を利用する際に、契約書や約款に記載されている内容を確認していますか（いましたか）。
以下の中から当てはまるもの一つに〇をつけてください。（単一選択）

1. 全て確認している（いた）
2. 一部確認している（いた）
3. 確認していない（いなかった）
4. わからない

■基本情報（Q29～Q32）

Q29.貴社の所在地について、以下の中から当てはまるもの一つに〇をつけてください。（単一選択）
（所在地が複数ある場合は、回答いただいた方の主な勤務地で結構です。）

1. 北海道	2. 青森県	3. 岩手県
4. 宮城県	5. 秋田県	6. 山形県
7. 福島県	8. 茨城県	9. 栃木県
10. 群馬県	11. 埼玉県	12. 千葉県
13. 東京都	14. 神奈川県	15. 新潟県
16. 富山県	17. 石川県	18. 福井県
19. 山梨県	20. 長野県	21. 岐阜県
22. 静岡県	23. 愛知県	24. 三重県
25. 滋賀県	26. 京都府	27. 大阪府
28. 兵庫県	29. 奈良県	30. 和歌山県
31. 鳥取県	32. 島根県	33. 岡山県
34. 広島県	35. 山口県	36. 徳島県
37. 香川県	38. 愛媛県	39. 高知県
40. 福岡県	41. 佐賀県	42. 長崎県
43. 熊本県	44. 大分県	45. 宮崎県
46. 鹿児島県	47. 沖縄県	48. 国外

Q30.貴社の従業員規模について、以下の中から当てはまるもの一つに○をつけてください。（単一選択）

1. ~19 人	2. 20 人～49 人
3. 50 人～100 人	4. 101 人～300 人
5. 301 人～500 人	6. 501 人～1,000 人
7. 1,001 人～5,000 人	8. 5,001 人～10,000 人
9. 10,001 人以上	

Q31.貴社の主たる業種について、以下の中から当てはまるもの一つに○をつけてください。（単一選択）

1. 農業、林業、漁業
2. 鉱業、採石業、砂利採取業
3. 建設業
4. 製造業
5. 電気・ガス・熱供給・水道業
6. 通信業
7. 放送業
8. 情報サービス業__ソフトウェア業
9. 情報サービス業__情報処理サービス業
10. 情報サービス業__情報提供サービス業
11. 情報サービス業__市場調査・世論調査・社会調査業
12. 情報サービス業__その他の情報サービス業
13. インターネット附随サービス業
14. 映像・音声・文字情報制作業
15. 運輸業、郵便業
16. 卸売業、小売業
17. 金融業、保険業
18. 不動産業、物品賃貸業
19. 学術研究、専門・技術サービス業
20. 宿泊業、飲食サービス業
21. 生活関連サービス業、娯楽業
22. 教育、学習支援業
23. 医療、福祉
24. 複合サービス事業
25. サービス業（他に分類されないもの）
26. 公務（他に分類されるものを除く）
27. その他（上記で分類不能の産業）

Q32.貴社では、IT システムの開発・運用や IT サービスの提供を社外に発注していますか。それとも受注していますか。以下の中から当てはまるもの一つに○をつけてください。（単一選択）

1. 主に発注している	⇒終了
2. 主に受注している	⇒Q33 へお進みください
3. 受注することも、発注することもある	⇒Q33 へお進みください
4. どちらもしていない（自社開発・運用している）	⇒終了
5. IT システムや IT サービスを利用していない	⇒終了

Q33.貴社では、現在以下の IT サービスに該当する業務を業として実施・受託していますか。
以下の中から当てはまるもの全てに○をつけてください。（複数選択可）

1. IT 機器（PC や周辺機器等）部品・製品の製造
2. IT 機器（PC や周辺機器等）部品・製品の販売
3. IT 機器（PC や周辺機器等）部品・製品の保守
4. システム・ネットワーク構築
5. システム・ネットワーク保守・運用
6. ソフトウェア・アプリケーション開発・販売
7. ソフトウェアサポートサービス
8. アプリケーション保守
9. Web サイト設計・構築・運用
10. IT 技術者派遣
11. ASP・SaaS 等サービス提供
12. PaaS 等プラットフォーム提供
13. IaaS・ホスティング等インフラ提供
14. データ処理・分析・入力
15. IT 関連コンサルティング
16. フォレンジック
17. セキュリティ関連システムの開発・保守・販売
18. セキュリティ監査
19. 脆弱性診断
20. セキュリティ監視・運用
21. その他（具体的に　　）

調査は以上で終了です。本アンケート調査にご協力いただき、心より感謝申し上げます。