会社名　　部署名

ご担当者名　　電話番号

メールアドレス　　ID*

* 送付状に印字してあるWebアンケート用のIDをご記入ください。

ITサプライチェーン*における貴社の情報セキュリティに対する取組み（委託先管理・契約・インシデント対応・リスク対応）等についてお伺いします。ご回答可能な範囲で、現在の取組み状況についてご回答いただきますようお願いします。

* ITシステム・サービスに関する業務を外部委託しその委託が連鎖する形態のこと

Ⅰ．貴社及びご回答者についてお伺いします。

S1　貴社の主な業種* をお選びください。（○は1つ）

1　製造業
2　卸売業、小売業
3　不動産業、物品賃貸業
4　学術研究、専門・技術サービス業
5　宿泊業，飲食サービス業
6　生活関連サービス業，娯楽業
7　複合サービス事業
8　サービス業（ 3～7に分類されないもの ）
9　その他（　　）

*業種名は日本産業分類の大分類にもとづいています

→ S1 -1　S1で選択肢「 1製造業」「2卸売業、小売業」を選んだ方にお伺いします。貴社の事業のうち、最も売上高の高い分野をお選びください。（○は１つ）

1　繊維・衣服
2　飲食料品
3　建築材料、鉱物・金属材料
4　印刷・印刷関連製品
5　化学製品
6　電気機械器具、情報通信機械器具
7　輸送用機械器具
8　その他の製品

S2　貴社の総従業員数（正社員、準社員等を含む）*をお選びください。（○は1つ）

1　～50 名
2　51名～100名
3　101名～300名
4　301名～500名
5　501名～1,000名
6　1,001名～5,000名
7　5,001名～10,000名
8　10,001名以上

* 1ヶ月を超える雇用契約者とし、人材派遣業者からの派遣従業者は含めません。

S3　ご回答者の所属部門をお選びください。複数の部門で回答された場合は、主に回答された部門をお選びください。（○は1つ）

1　調達部門
2　総務部門
3　情報システム部門・情報セキュリティ部門
4　法務部門
5　事業部門
6　その他（　　）

S4　ご回答者の役職をお選びください。（○は1つ）

1　取締役・役員クラス
2　事業部長クラス
3　部長クラス
4　課長クラス
5　係長・主任クラス
6　一般社員
7　専門職
8　その他（　　）

Ⅱ．貴社がITシステム・サービスの業務委託（以下、「業務委託」といいます）において行っている情報セキュリティに係る委託先管理等についてお伺いします。なお、以下の設問は、貴社が「委託元」となる取引に関してご回答ください。

＜委託先管理＞

問1　貴社において、昨年度（2017年度）、直接取引のあった委託先の社数をお選びください。（○は１つ）

1　1 社～10 社
2　11 社～50 社
3　51 社～100 社
4　101 社以上
5　わからない

問2　情報セキュリティに関する委託先管理に関し、貴社では、どのような社内ルール・規定類を整備されていますか。当てはまるものを全てお選びください。（○はいくつでも）

1　情報セキュリティ要求事項を含む契約関連文書（仕様書*、契約書等）の雛形
2　委託先に求める情報セキュリティ対策リスト（基準、ガイドライン、規格等を参照する場合も含む）
3　委託先の情報セキュリティ対策状況の確認形式（監査、チェックリスト等）
4　情報セキュリティ対策の評価結果に基づく推奨委託先リスト
5　情報セキュリティに関する項目を含む委託先選定基準
6　その他（　　）
7　特にルールや規定類は整備されていない

*委託する業務の内容を示すための文書で、業務仕様書、発注仕様書等

問3　貴社が参加するITサプライチェーン内で横断的な情報セキュリティ対策はありますか。当てはまるものを全てお選びください。（○はいくつでも）

1　共通の情報セキュリティポリシー・基準等の展開
2　共通の情報セキュリティ要求事項に基づく委託先の適合確認
3　情報セキュリティに関する情報共有の仕組み
4　情報セキュリティの普及啓発、研修等の実施
5　ITサプライチェーン参加企業を対象とするインシデント対応組織（CSIRT*等）の設置
6　その他（　　）
7　特にITサプライチェーン内で横断的な取組みはない

*Computer Security Incident Response Teamの略。 コンピュータセキュリティに係るイシデントに対処するための組織。

問4　情報セキュリティに関する委託先管理において、どのような点が課題だと考えますか。

特に課題と考えるものの選択肢の番号を最大3つまで以下の枠内にご記入ください。

1　経営層の情報セキュリティに関する意識が低い
2　社内に十分な知見・スキルを持った人材が不足している
3　情報セキュリティ対策の確認にかかるコスト負担が大きい
4　再委託先以降の情報セキュリティ対策を確認することが難しい
5　海外の委託先の情報セキュリティ対策を確認することが難しい
6　すべての業務委託に対して統一的な管理体制やルールを適用することが難しい
7　ルールや規定類は存在するが形骸化している
8　その他（　　）

＜契約＞

問5　問2で「1情報セキュリティ要求事項を含む契約関連文書（仕様書、契約書等）の雛形」を選んだ方にお伺いします。契約関連文書に記載する情報セキュリティ要求事項の変更は認められていますか。（○は1つ）

1　情報セキュリティ要求事項の内容は変更できない
2　管理者（法務部門や総務部門の担当者等）からの承認が得られれば、情報セキュリティ要求事項の内容は変更できる
3　情報セキュリティ要求事項の内容は、事業部門の調達担当者の判断だけで変更できる
4　その他（　　）

問6　貴社では、業務委託ごとに契約関連文書（仕様書、契約書等）の内容を確認する専門の部門（法務部等）や専任の担当者を設けていますか。（○は1つ）

1　専門の部門がある
2　専門の部門はないが、総務部門等で専任の担当者がいる
3　専門の部門はなく、専任の担当者もいない
4　その他（　　）

問7　業務委託における情報セキュリティ要求事項の明確化について、役割ごとに所管（関与）する部門をお選びください。1つの役割に対して複数の部門が関与する場合は、関与する部門全てをお選びください。　（✔は各行につき、いくつでも）

	1.調達部門	2.総務部門	3.情報システム部門・情報セキュリティ部門	4.法務部門	5.事業部門	6.貴社のその他の部門	7.委託先
a. 記載項目や手順等ルールを決める							
b. 委託先と内容を調整する。							
c. 要求事項の内容が妥当か確認する							
d. 要求事項を契約関連文書（仕様書、契約書等）に記載する							
e. 要求通りになっていることを確認する							

問8　以下の情報セキュリティ要求事項に関し、業務委託契約において、委託先の責任を明確にしたいと思う度合いについて、当てはまるものをお選びください。（✔は各行につき、1つ）

	強くそう思う	ややそう思う	あまりそう思わない	全くそう思わない	分からない
a.秘密保持					
b.証跡の提示、監査協力等					
c.情報セキュリティに関する契約内容に違反した場合の措置					
d.インシデントが発生した場合の対応					
e. 可用性（稼働率の水準、目標復旧時間等）					
f. 新たな脅威（脆弱性等）が顕在化した場合の情報共有・対応					
g. 再委託の禁止または制限					
h.契約終了後の情報資産の扱い（返却、消去、廃棄等）					

問9　業務委託契約において、情報セキュリティに関する委託元と委託先の責任範囲（責任分界点）が明確にならない理由は何だと思いますか。以下の項目について、理由としての当てはまりの度合いをお選びください。（✔は各行につき、1つ）

	強くそう思う	ややそう思う	あまりそう思わない	全くそう思わない	分からない
a. 自組織の契約関連文書（仕様書、契約書等）の雛形に情報セキュリティ要求事項の記載がないため、何を決めたらいいのかわからない					
b. 情報セキュリティに関する自組織内の専門知識・スキルが不足している					
c. 責任範囲を明確にすることで、見積りに反映され、コスト増となる					
d. 責任範囲を明確にすることで、自組織内の関係者の心理的負担が増える					
e. 責任範囲を明確にするための作業、調整に時間がかかり契約締結が遅くなる。（利用者の不満増大、機会損失の恐れがある。）					
f.責任範囲を明確にすることで、仕様書等に記述されている以外の対応が期待できなくなる					
g. 同じ業者と継続して契約している業務が多く、責任範囲を見直す機会がない					

問10　業務委託契約において、情報セキュリティに関する委託元と委託先の責任範囲（責任分界点）を明確にするためには、どのようなことが有効だと考えていますか。当てはまるものを全てお選びください。（〇はいくつでも）

1　契約関連文書（仕様書、契約書等）の雛形の見直し
2　委託先と協力して行うリスクアセスメント
3　調達担当者向けの情報セキュリティに関するセミナー・教育の実施
4　情報セキュリティに関する委託元と委託先の責任範囲が明確でなかったことで起こったトラブルの事例集
5　国による情報セキュリティに関する委託元と委託先の責任範囲の取り決め方法に関する法律の整備
6　国や業界による情報セキュリティに関する委託元と委託先の責任範囲の取り決め方法に関するガイドラインの整備
7　その他（　　）

問11　業務委託契約における情報セキュリティに関する責任範囲の明確化について、どのような点が課題だと考えますか。

特に課題と考えるものの選択肢の番号を最大3つまで以下の枠内にご記入ください。

1　社内で統一された契約関連文書（仕様書、契約書等）の雛形がない
2　経営層の情報セキュリティに関する意識が低い
3　社内に十分な知見・スキルを持った人材が不足している
4　事業部門の担当者が契約書等の内容を知らずに作業を進めている
5　IoTやAI等の新技術を利用する場合は、責任範囲の考え方について業界指針や判例がない
6　すべての業務委託に対して統一的な管理体制やルールを適用することが難しい
7　その他（　　）

＜インシデント対応・リスク対応＞

問12　過去3年間の業務委託において、以下のような事象が発生したことがありますか。当てはまるものを全てお選びください。（〇はいくつでも）

1　メールの誤送信
2　ビジネスメール詐欺
3　不正アクセス
4　ウイルス感染
5　情報漏えい・暴露
6　システム・サービスの障害・遅延・停止
7　Webページ等の改ざん
8　データの毀損、消失
9　情報システム・機器の不正利用
10　入退出管理用のセキュリティカードの紛失
11　その他（　　）
12　インシデントが発生したかどうかわからない

→ 問12-1 問12の選択肢1～11を選んだ方にお伺いします。発生した事象によって生じた被害の内容と、被害の影響が及んだ範囲（組織・個人）について、当てはまるものを全てお選びください。（✔は各行につき、いくつでも）

	1 自社	2 委託先	3 再委託先以降	4 その他の取引先、関係先	5 個人顧客	6 当該被害はない
a. ITシステム・サービスの障害、遅延、停止による逸失利益						
b. 個人顧客への賠償や法人取引先への補償負担						
c. 原因調査・復旧にかかわる人件費等の経費負担						
d. 裁判、調停等にかかわる人件費等の経費負担						
e. 個人顧客や法人取引先に対する信頼の失墜						

問13 納品後（契約期間外）のITシステムの情報セキュリティに関する未知の脆弱性（契約期間内に明らかでなかったもの）への対応について、どのように考えますか。以下の項目について、当てはまるものをお選びください。（✔は各行につき、1つ）

	強くそう思う	ややそう思う	あまりそう思わない	全くそう思わない	分からない
a. 納品後のITシステムの情報セキュリティに関する未知の脆弱性への対応は、委託先が責任を持つべきだ					
b. 納品後のITシステムの情報セキュリティに関する未知の脆弱性への責任分担について契約書等に定めるべきだ					
c. 納品後のITシステムの情報セキュリティに関する未知の脆弱性への対応は、委託元が検討し、必要に応じて業務委託するべきだ					

問14 以下の情報セキュリティに関する事項について、懸念の度合いをお答えください。（✔は各行につき、1つ）

	非常に懸念している	ある程度懸念している	あまり懸念していない	全く懸念していない	分からない
a.顧客情報や業務情報（機密情報等）が盗まれる（流出する）					
b.Webサイトや業務サーバの内容が改ざんされる					
c.WebサイトやIoT機器が乗っ取られサイバー攻撃に悪用される					
d.サイバー攻撃によってWebサイトの負荷が高まり利用できなくなる					
e.業務サーバ、Webサーバ等がウイルスに感染する					
f.マスメディアで騒がれたりインターネット上で風評被害が広がる					
g.クラウドサービスのサーバが海外にある					
h.委託先で不正なプログラムや機能が埋め込まれる					
i.取引先の脆弱性が原因で自社内に侵入される					

問15 情報セキュリティのリスク低減（移転）策のひとつにサイバー保険がありますが、サイバー保険をご存じですか。当てはまるものをお選びください。（○は1つ）

1 既に加入済み
2 知っており、加入の予定がある
3 知ってはいるが、加入の予定はない
4 知っているが、加入済みか予定があるかはわからない
5 詳細は知らないが、聞いたことはある
6 全く知らない

→ 問15-1 問15で「3知ってはいるが、加入の予定はない」を選んだ方にお伺いします。加入の予定がない理由について、当てはまるものを全てお選びください。（○はいくつでも）

1 個人情報漏洩保険、業務過誤賠償責任保険等の他の保険に加入済み
2 委託先でサイバー保険に加入済み
3 経営層がサイバー保険に関心を持っていない
4 サイバー保険への加入を検討できるほど、情報セキュリティに関する情報を整理できていない
5 サイバー保険に加入する効果がわからない
6 サイバー保険に加入するための予算が取れない
7 その他（ ）

問16　以下にサイバー保険の代表的な補償内容をあげています。これらの補償内容のうち、どれが魅力的であると考えますか。
特に魅力的であると考えるものの選択肢の番号を最大3つまで以下の枠内にご記入ください。

1　法律上の賠償責任が発生した場合の損害賠償金に対する補償
2　損害賠償責任に関する訴訟や示談交渉に関するコストに対する補償
3　行政手続きに要するコストや監督官庁等の課徴金に対する補償
4　セキュリティ事故が発生した場合の応急措置に要するコストに対する補償
5　セキュリティ事故の被害や原因の調査に要するコストに対する補償
6　セキュリティ事故により事業が継続できなくなった場合の喪失利益に対する補償

問17　インシデント対応やリスク対応において、どのような点が課題と考えますか。
特に課題と考えるものの選択肢の番号を最大3つまで以下の枠内にご記入ください。

1　経営層の情報セキュリティに関する意識が低い
2　社内に十分な知見・スキルを持った人材が不足している
3　インシデントが発生した際に何をしたらいいのかわからない
4　インシデントが発生した際に手順どおりに対応できるかわからない
5　マルチベンダーの場合に原因調査が難しい
6　インシデントが委託先からタイムリーに報告されない
7　インシデントが発生した場合に、委託先とのコスト負担の調整が難しい
8　その他（　　）

Ⅲ．ITサプライチェーンにおける情報セキュリティの向上のため、国、IPAに期待する施策についてお伺いします。

問18　ITサプライチェーンにおける情報セキュリティの向上のため、国、IPAに求める施策はありますか。施策として期待するものを全てお選びください。（○はいくつでも）

1　企業向けガイドラインの整備
2　委託先管理で利用できるツール（チェックリスト、ベンチマーク、各種雛形等）の整備
3　ITサプライチェーンのインシデント事例集の整備
4　委託先管理のベストプラクティス集の整備
5　委託先管理者向け普及啓発セミナー・教育の実施
6　その他（　　）

次のページからITシステム・サービスの業務委託に関する具体的な事例についての設問になります。

2017年度以降に回答者がご担当された（または貴社が発注された）ITシステム・サービスに関する業務委託契約の個別の事例について、情報セキュリティ要件の明確化の状況等についてお伺いします。複数の事例についてご回答いただける場合は、お手数ですが、この調査票をコピーしてご記入ください。Webアンケートの場合は、複数事例用の追加のIDを発行しますので調査実施機関にご連絡下さい。

＜事例のプロフィール＞

問19　当該事例に含まれるITシステム・サービスについて当てはまるものを全てお選びください。（○はいくつでも）

1　ソフトウェア開発*
2　システム運用・管理
3　アプリケーション保守
4　ソフトウェアサポートサービス
5　ハードウェア保守
6　Webサイト構築・運用
7　サービス提供（ASP、SaaS等）
8　インフラ提供（IaaS、ホスティング等）
9　データ処理・分析
10　その他（　　）

*貴社固有のアプリケーションソフトウェアを開発する業務を指し、パッケージソフトウェアを利用した事例も含みます。

問20　当該事例のITシステム・サービスの障害発生時の社会的影響度について、当てはまるものをお選びください。（○は１つ）

1　人命に影響、甚大な経済損失が想定される（航空管制，建築構造計算，医療関連機器制御、救急医療NW等）
2　社会的影響が極めて大きい（輸送，通信，金融・証券，プラント制御等）
3　社会的影響が限定される（放送、行政、水道、建設等）
4　社会的影響が殆ど無い（勤怠管理等、影響範囲が事業者内にとどまるもの）

問21　当該事例のITシステム・サービスのネットワークの範囲について、当てはまるものをお選びください。（○は1つ）

1　ネットワークには接続されていない（スタンドアロン）
2　貴社の1事業所の同一の建物内に限定されているネットワーク（LAN）
3　貴社の複数の事業所を結ぶネットワーク（WAN）
4　貴社と貴社の取引先の事業所を結ぶネットワーク（B to B）
5　貴社と貴社の製品・サービスの利用者を結ぶネットワーク（B to C）
6　その他（　　）

問22　当該事例のITシステム・サービスで扱う情報資産について、当てはまるものを全てお選びください。（○はいくつでも）

1　クレジットカード等の個人信用情報や病歴等の要配慮個人情報を含む個人情報
2　クレジットカード等の個人信用情報や病歴等の要配慮個人情報を含まない個人情報
3　営業秘密
4　1～3以外の非公開情報
5　情報資産はない

→ 問22-1　問22で1または2の個人情報を選んだ方にお伺いします。個人情報のデータ件数について、当てはまるものをお選びください。（○は１つ）

1　5,000件未満
2　5,000件～100,000件未満
3　100,000件以上

問23　当該事例の業務委託で扱う情報資産に関して、契約の際に情報セキュリティ上のリスクをどの程度懸念しましたか。それぞれの脅威に対する懸念の度合いとして当てはまるものをお選びください。（✔は各行につき、1つ）

	1 非常に懸念した	2ある程度懸念した	3 あまり懸念しなかった	4全く懸念しなかった	5 わからない
a. 内部不正					
b. 外部攻撃（ウイルス感染や不正アクセス等）					
c. 人的ミス(誤操作等)					
d. システム障害、停止					
e. 災害					

＜委託先＞

問24　当該事例の委託先は、貴社と資本関係のある系列企業・グループ企業ですか。（○は1つ）

1　系列企業・グループ企業
2　系列企業・グループ企業以外

問25　当該事例の委託先はどのようにして決定しましたか。（○は1つ）

1　1社にのみ見積りを徴収して決定
2　2社以上から見積りのみを徴収して決定
3　2社以上から業務提案と見積りを徴収して技術力等を勘案して決定
4　一般公募による入札で決定
5　その他（　　）

問26　委託先には再委託先がありますか。また、再々委託先等の有無を把握していますか。（○は1つ）

1　再委託先はない
2　再委託先はあり、再々委託先はない
3　再委託先はあり、再々委託先以降もある
4　再委託先はあるが、再々委託先があるかどうかわからない
5　再委託先等があるかどうかわからない

＜契約＞

問27　以下の情報セキュリティに係る要求事項について、当該事例の契約関連文書（仕様書、契約書等）にどのように記載されているか、選択肢の番号でご回答ください。

1　当該文書は使用していない
2　当該文書は使用しているが、当該項目は要求事項となっていないので、項目そのものの記載がない
3　当該項目の記載があるが、委託先が責任を負うべき範囲が明示されていない（「都度調整」等）
4　当該項目について、委託先が責任を負うべき範囲が明示されている

	約款	委託先の提案書	仕様書	委託先の見積書	契約書	覚書	その他（SLA*等）
a.秘密保持							
b,証跡の提示、監査協力等							
c.情報セキュリティに関する契約内容に違反した場合の措置							
d.インシデントが発生した場合の対応							
e. 可用性（稼働率の水準、目標復旧時間等）							
f. 新たな脅威（脆弱性等）が顕在化した場合の情報共有・対応							
g. 再委託の禁止または制限							
h.契約終了後の情報資産の扱い（返却、消去、廃棄等）							

*Service Level Agreementの略。委託者とサービス提供事業者の間で結ばれるサービスのレベルに関する合意文書。

→ 問27-1 問27の情報セキュリティ要求事項のいずれかについて「4委託先が責任を負うべき範囲（委託元の免責事項）が明示されている」を選んだ方にお伺いします。情報セキュリティに関する委託先の責任範囲についてどのように明示されていましたか。当てはまるものを全てお選びください。（○はいくつでも）

1 一定の条件において委託先が責任を負わない免責規定を定めていた
2 損害賠償額に業務委託の契約金額等で上限を設定していた
3 ソフトウエア開発等において、瑕疵（契約不適合）に関する項目の中で、業務委託完了後に発覚した未知の脆弱性等を対象としていた
4 その他（ ）を定めていた

問28 当該事例の契約関連文書（仕様書、契約書等）では、委託先が実施すべき組織的な情報セキュリティ対策が明記されていましたか。（○は1つ）

1 明記されていた →問28-1にもご回答ください
2 明記されていなかった

→ 問28-1 問28で選択肢「1明記されていた」を選んだ方にお伺いします。委託先が実施すべき組織的な情報セキュリティ対策として明記されていたものを全てお選びください。（✔はいくつでも）

○情報セキュリティに関する規程類や推進体制の整備	
1 情報セキュリティポリシーや情報セキュリティ管理に関する規程の整備及び実践	
2 全社的な情報セキュリティの推進体制やコンプライアンスの推進体制の整備	
3 重要な情報資産に対する重要性のレベルごとの分類、レベルに応じた表示や取扱方法の規定	
4 重要な情報の利用、保管、持ち出し、消去、破棄等に対する取扱い手順の規定	
5 再委託時の契約における情報セキュリティ要求事項の明記	
○従事者の不正対策	
6 従業者に対する情報セキュリティに関する就業上の義務の明確化（採用、退職時における守秘義務に関する書面の取り交わし等）	
7 従業者に対する情報セキュリティに関する自組織の取組みや関連規程類についての計画的な教育や指導の実施	
8 重要な情報資産のある建物や区画に対する物理的セキュリティ対策、入退室管理の実施	
9 重要な書類、モバイルPC、記憶媒体に対する施錠管理等の適切な管理の実施	
10 従業者ごとの操作ログ等の取得・保存	
11 私物のモバイル機器や記憶媒体に対する持ち込み、持ち出しの管理	
12 単独作業の制限、承認手続き	
13 従業者からの当該業務委託の秘密保持等に関する誓約書の取得	
○技術的な取組み・インシデント対応	
14 重要なデータや関連するシステムのバックアップに関する手順の文書化及び実施	
15 不正プログラム（ウイルス、ワーム、トロイの木馬、ボット、スパイウエア等）への対策実施	
16 情報システムに対する、適切かつ迅速な脆弱性対策の実施	
17 ネットワーク上のデータに対する暗号化等の適切な保護策の実施	
18 モバイルPC、記憶媒体やデータの外部持ち出しに対する、盗難、紛失等を想定した対策の実施	
19 データや情報システムの利用者IDの管理、利用者の識別と認証の実施	
20 データや情報システム、業務アプリケーション等に対するアクセス権の付与とアクセス制御の実施	
21 ネットワークのアクセス制御の実施	
22 インシデント発生時の適切かつ迅速な初動対応、報告の実施	

問29 当該事例において使用した契約書の書式は委託元のものですか、委託先のものですか。当てはまるものをお選びください。（○は1つ）

1 委託元（貴社）の契約書の書式
2 委託先の契約書の書式
3 その他（ ）

問30 当該事例において使用した契約書の書式は、対象業務の情報セキュリティ要求事項に合わせて、情報セキュリティに関する項目を追加したり、内容を修正したりするカスタマイズを行いましたか。当てはまるものを全てお選びください。（○はいくつでも）

1 カスタマイズはしていない（雛形のまま使用）
2 委託元（貴社）の要求で、不足している情報セキュリティ要求事項を追加した
3 委託元（貴社）の要求で、実現できない情報セキュリティ要求事項を削除した
4 委託先の要求で、不足している情報セキュリティ要求事項を追加した
5 委託先の要求で、実現できない情報セキュリティ要求事項を削除した
6 その他（ ）

問31 当該事例において、業務委託契約における情報セキュリティ要求項目に関し、委託先との間で何らかのトラブルが発生したことがありますか。当てはまるものをお選びください。（○は1つ）

1 発生した
2 発生していない

→ 問31-1 問31で選択肢「1発生した」を選んだ方にお伺いします。発生したトラブルをどのように解決したか、自由記入でご回答ください。

（例1）セキュリティの脆弱性が契約終了後に発覚し、委託先に責任があるかどうかでもめた。テストで発見することが可能な脆弱性だったのに、確認が漏れていたことが分かったので委託先に無償で対応させた。
（例2）セキュリティ監査で委託先のデータセンターの現地審査をさせてほしいと依頼したが、契約上それは認めていないといわれた。委託先から公開されている情報セキュリティ報告書を使用した。

ご協力ありがとうございました

このアンケート調査の調査結果は、IPAにより公表されることがありますが，データの特徴から具体的な企業や事例の内容が特定されることがないよう、統計的な処理を行います。ご懸念がある場合は、調査実施機関にお問い合わせください。

会社名　　部署名

ご担当者名　　電話番号

メールアドレス　　ID*

* 送付状に印字してあるWebアンケート用のIDをご記入ください。

ITサプライチェーン*における貴社の情報セキュリティに対する取組み（契約・インシデント対応・リスク対応）等についてお伺いします。ご回答可能な範囲で、現在の取組み状況についてご回答いただきますようお願いします。

* ITシステム・サービスに関する業務を外部委託しその委託が連鎖する形態のこと

Ⅰ．貴社及びご回答者についてお伺いします。

S1　貴社の主な業種をお選びください。（○は1つ）

1　ソフトウェア業
2　情報処理サービス業
3　情報提供サービス業
4　その他の情報サービス業
5　国内・国際電気通信業
6　電気通信に附帯するサービス業
7　民生用電気機械器具製造業
8　電子計算機・同付属装置製造業
9　工業計器製造業
10　発電機・電動機・その他の回転電気機械製造業
11　電気機械製造業
12　その他（　　）

S2　貴社の総従業員数（正社員、準社員等を含む）*をお選びください。（○は1つ）

1　～20 名
2　21名～50名
3　51名～100名
4　101名～300名
5　301名～500名
6　501名～1,000名
7　1,001名～5,000名
8　5,001名～10,000名
9　10,001名以上

* 1ヶ月を超える雇用契約者とし、人材派遣業者からの派遣従業者は含めません。

S3　ご回答者の所属部門をお選びください。複数の部門で回答された場合は、主に回答された部門をお選びください。（○は1つ）

1　営業部門
2　総務部門
3　情報システム部門・情報セキュリティ部門
4　法務部門
5　事業部門
6　品質・リスク管理部門
7　その他（　　）

S4　ご回答者の役職をお選びください。（○は1つ）

1　取締役・役員クラス
2　事業部長クラス
3　部長クラス
4　課長クラス
5　係長・主任クラス
6　一般社員
7　専門職
8　その他（　　）

S5　ITシステム・サービスの取引において、貴社の位置付けとして主要なものをお選びください。（○は1つ）

1　元請け（プライムベンダー）
2　二次請け以降

S6　貴社において、昨年度（2017年度）、直接取引のあった委託元の社数をお選びください。（○は１つ）

1　1 社～10 社
2　11 社～50 社
3　51 社～100 社
4　101 社以上
5　わからない

Ⅱ．貴社が受託するITシステム・サービスに関する業務（以下、「受託業務」といいます）において行っている情報セキュリティ対策等についてお伺いします。なお、以下の設問は、貴社が「受託者」となる取引に関してご回答ください。

＜契約＞

問1　貴社には、情報セキュリティ要求事項を含んだ契約書の雛形がありますか。当てはまるものをお選びください。（○は1つ）

1　サービスの種類に係わらない統一の雛型がある
2　サービスの種類に応じた複数の雛型がある
3　雛型はなく、過去の契約書を流用する等して都度作成している
4　その他（　　）

→ 問1-1　問1で1または2の「雛型がある」を選んだ方にお伺いします。契約書に記載する情報セキュリティ要求事項の変更は認められていますか。（○は1つ）

1　情報セキュリティ要求事項の内容は変更できない
2　管理者（法務部門や総務部門の担当者等）からの承認が得られれば、情報セキュリティ要求事項の内容は変更できる
3　情報セキュリティ要求事項の内容は、営業担当者等の委託元との窓口の判断だけで変更できる
4　その他（　　）

問2　貴社では、受託業務ごとに契約関連文書（契約書等）の内容を確認する専門の部門（法務部等）や専任の担当者を設けていますか。（○は1つ）

1　専門の部門がある
2　専門の部門はないが、総務部門等で専任の担当者がいる
3　専門の部門はなく、専任の担当者もいない
4　その他（　　）

問3　受託業務における情報セキュリティ対策について、役割ごとに所管（関与）する部門をお選びください。1つの役割に対して複数の部門が関与する場合は、関与する部門全てをお選びください。　（✔は各行につき、いくつでも）

	1.営業部門	2.総務部門	3.情報システム部門・情報セキュリティ部門	4.法務部門	5.事業部門	6.品質・リスク管理部門	7.その他の部門
a. 提案時の情報セキュリティ対策の説明							
b. 情報管理・情報セキュリティに関する契約内容確認							
c. 受託業務で扱う情報資産の厳格な管理（授受から廃棄等の一連のプロセス）							
d. 委託元による情報セキュリティ対策の実施状況の確認への対応							
e. インシデントに対する対応体制の整備							

問4　以下の情報セキュリティ要求事項に関し、受託業務の契約において、委託先（貴社）の責任を明確にしたいと思う度合いについて、当てはまるものをお選びください。（✔は各行につき、1つ）

	強くそう思う	ややそう思う	あまりそう思わない	全くそう思わない	分からない
a.秘密保持					
b.証跡の提示、監査協力等					
c.情報セキュリティに関する契約内容に違反した場合の措置					
d.インシデントが発生した場合の対応					
e. 可用性（稼働率の水準、目標復旧時間等）					
f. 新たな脅威（脆弱性等）が顕在化した場合の情報共有・対応					
g. 再委託の禁止または制限					
h.契約終了後の情報資産の扱い（返却、消去、廃棄等）					

問5　受託業務の契約において、情報セキュリティに関する委託元と委託先の責任範囲（責任分界点）が明確にならない理由は何だと思いますか。以下の項目について、理由としての当てはまりの度合いをお選びください。（✔は各行につき、1つ）

	強く そう思う	やや そう思う	あまり そう思わない	全く そう思わない	分から ない
a. 自組織の契約関連文書（契約書等）の雛形に情報セキュリティ要求事項の記載がないため、何を決めたらいいのかわからない					
b. 委託元の情報セキュリティに関する専門知識・スキルが不足している					
c. 責任範囲を明確にすることで、見積りに反映せざるを得ないが、委託元にはコスト増を受け入れてもらえない					
d. 責任範囲を明確にすることで、自組織の関係者の心理的負担が増える					
e. 責任範囲を明確にすることで、調整に時間がかかり契約が遅くなる（工期圧迫、機会損失等）					
f. 契約時点では業務要件自体が未確定であることが多く、情報セキュリティ要求事項のみを明確にすることができない。					
g. 同じ顧客と継続して契約している業務が多く、責任範囲を見直す機会がない					

問6　受託業務の契約にあたり、情報セキュリティ要求事項に関して、委託元と委託先の責任範囲に曖昧さが残る場合に、貴社独自に取られている対策はありますか。（〇はいくつでも）

1　当該受託業務についてのリスクアセスメントを行い、想定されるリスクを洗い出す
2　委託元の提示する条件で受注してよいか、社内で第三者部門や上位責任者が参加する審査を行う
3　請負契約ではなく準委任契約や多段階契約等、責任が限定的になるように契約の方法を変える
4　委託元との情報セキュリティに関する意見交換の場を設定する
5　サイバー保険への加入により、いざという時の経済的影響を最小限にする
6　委託元との協議内容をできるだけ詳細に文書に記録して残すようにする
7　サイバー攻撃や脆弱性の最新情報を入手し、当該受託業務への影響がないかを監視する
8　委託元と事例の共有や合同訓練等インシデントに備えた準備を行う
9　他部署や他社からの支援体制を構築しておく
10　その他（　　）

問7　受託業務の契約において、情報セキュリティに関する委託元と委託先の責任範囲（責任分界点）を明確にするためには、どのようなことが有効だと考えていますか。当てはまるものを全てお選びください。（〇はいくつでも）

1　契約関連文書（契約書等）の雛形の見直し
2　委託元と協力して行うリスクアセスメント
3　営業担当者向けの情報セキュリティに関するセミナー・教育の実施
4　情報セキュリティに関する委託元と委託先の責任範囲が明確でなかったことで起こったトラブルの事例集
5　国による情報セキュリティに関する委託元と委託先の責任範囲の取り決め方法に関する法律の整備
6　国や業界による情報セキュリティに関する委託元と委託先の責任範囲の取り決め方法に関するガイドラインの整備
7　その他（　　）

問8　受託業務の契約における情報セキュリティに関する責任範囲の明確化について、どのような点が課題だと考えますか。
特に課題と考えるものの選択肢の番号を最大3つまで以下の枠内にご記入ください。

1　社内で統一された契約関連文書（契約書等）の雛形がない
2　委託元の情報セキュリティに関する意識が低い
3　営業担当者がセキュリティ要件を確認せずに契約してしまう
4　社内に十分な知見・スキルを持った人材が不足している
5　現場担当者が契約書等の内容を知らずに作業を進めている
6　責任範囲を明確化すると、現場担当者に大きなリスクを背負わせる結果となることが多い
7　すべての受託業務に対して統一的な管理体制やルールを適用することが難しい
8　IoTやAI等の新技術を利用する場合は、責任範囲の考え方について業界指針や判例が無い
9　その他（　　）

＜インシデント対応・リスク対応＞

問9　過去3年間の受託業務において、以下のような事象が発生したことがありますか。当てはまるものを全てお選びください。
（○はいくつでも）

1　メールの誤送信
2　ビジネスメール詐欺
3　不正アクセス
4　ウイルス感染
5　情報漏えい・暴露
6　システム・サービスの障害・遅延・停止
7　Webページ等の改ざん
8　データの毀損、消失
9　情報システム・機器の不正利用
10　入退出管理用のセキュリティカードの紛失
11　その他（　　）
12　インシデントが発生したかどうかわからない

→ 問9-1　問9の選択肢1～11を選んだ方にお伺いします。発生した事象によって生じた被害の内容と、被害の影響が及んだ範囲（組織・個人）について、当てはまるものを全てお選びください。（✔は各行につき、いくつでも）

	1 自社	2 委託元	3 再委託先以降	4 その他の取引先、関係先	5 委託元の個人顧客	6 当該被害はない
a. ITシステム・サービスの障害、遅延、停止による逸失利益						
b. 個人顧客への賠償や法人取引先への補償負担						
c. 原因調査・復旧にかかわる人件費等の経費負担						
d. 裁判、調停等にかかわる人件費等の経費負担						
e. 個人顧客や法人取引先に対する信頼の失墜						

問10　納品後（契約期間外）のITシステムの情報セキュリティに関する未知の脆弱性（契約期間内に明らかでなかったもの）への対応について、どのように考えますか。以下の項目について、当てはまるものをお選びください。（✔は各行につき、1つ）

	強くそう思う	ややそう思う	あまりそう思わない	全くそう思わない	分からない
a. 納品後のITシステムの情報セキュリティに関する未知の脆弱性への対応は、委託先（貴社）が責任を持つべきだ					
b. 納品後のITシステムの情報セキュリティに関する未知の脆弱性への責任分担について契約書等に定めるべきだ					
c. 納品後のITシステムの情報セキュリティに関する未知の脆弱性への対応は、委託元が検討し、必要に応じて業務委託するべきだ					

問11　以下の情報セキュリティに関する事項について、懸念の度合いをお答えください。（✔は各行につき、1つ）

	非常に懸念している	ある程度懸念している	あまり懸念していない	全く懸念していない	分からない
a.顧客情報や業務情報（機密情報等）が盗まれる（流出する）					
b.Webサイトや業務サーバの内容が改ざんされる					
c.WebサイトやIoT機器が乗っ取られサイバー攻撃に悪用される					
d.サイバー攻撃によってWebサイトの負荷が高まり利用できなくなる					
e.業務サーバ、Webサーバ等がウイルスに感染する					
f.マスメディアで騒がれたりインターネット上で風評被害が広がる					
g.クラウドサービスのサーバが海外にある					
h.再委託先で不正なプログラムや機能が埋め込まれる					
i.取引先の脆弱性が原因で自社内に侵入される					

問12　情報セキュリティのリスク低減（移転）策のひとつにサイバー保険がありますが、サイバー保険をご存じですか。当てはまるものをお選びください。（○は1つ）

1　既に加入済み
2　知っており、加入の予定がある
3　知ってはいるが、加入の予定はない
4　知っているが、加入済みか予定があるかはわからない
5　詳細は知らないが、聞いたことはある
6　全く知らない

問13　以下にサイバー保険の代表的な補償内容をあげています。これらの補償内容のうち、どれが魅力的であると考えますか。
特に魅力的であると考えるものの選択肢の番号を最大3つまで以下の枠内にご記入ください。

1　法律上の賠償責任が発生した場合の損害賠償金に対する補償
2　損害賠償責任に関する訴訟や示談交渉に関するコストに対する補償
3　行政手続きに要するコストや監督官庁等の課徴金に対する補償
4　セキュリティ事故が発生した場合の応急措置に要するコストに対する補償
5　セキュリティ事故の被害や原因の調査に要するコストに対する補償
6　セキュリティ事故により事業が継続できなくなった場合の喪失利益に対する補償

問14　インシデント対応やリスク対応において、どのような点が課題と考えますか。
特に課題と考えるものの選択肢の番号を最大3つまで以下の枠内にご記入ください。

1　社内に十分な知見・スキルを持った人材が不足している
2　マルチベンダーの場合に原因調査が難しい
3　契約書等で委託先（貴社）に責任が無いと定めていることでも、委託元から押し付けられてしまうことがある
4　委託元の判断を待っている間に被害が拡大してしまう恐れがあり、やむをえず自社の責任で対応を進めることがある
5　複数のベンダー間での調整が必要なのに、委託元は取り仕切ることができない
6　委託元の情報セキュリティリスクに対する危機意識が希薄である
7　現場担当者がインシデントや情報セキュリティリスクを委託元にぎりぎりまで隠そうとする
8　その他（　　）

Ⅲ．ITサプライチェーンにおける情報セキュリティの向上のため、国、IPAに期待する施策についてお伺いします。

問15　ITサプライチェーンにおける情報セキュリティの向上のため、国、IPAに求める施策はありますか。施策として期待するものを全てお選びください。（○はいくつでも）

1　企業向けガイドラインの整備
2　委託先管理で利用できるツール（チェックリスト、ベンチマーク、各種雛形等）の整備
3　ITサプライチェーンのインシデント事例集の整備
4　委託先管理のベストプラクティス集の整備
5　委託先管理者向け普及啓発セミナー・教育の実施
6　その他（　　）

2017年度以降に回答者がご担当された（または貴社が受注された）ITシステム・サービスに関する受託業務の契約の個別の事例について、情報セキュリティ要件の明確化の状況等についてお伺いします。複数の事例についてご回答いただける場合は、お手数ですが、この調査票をコピーしてご記入ください。Webアンケートの場合は、複数事例用の追加のIDを発行しますので調査実施機関にご連絡下さい。

＜事例のプロフィール＞

問16　当該事例の委託元の業種をお選びください。（○は1つ）

1　農林漁業・同協同組合、鉱業
2　建設業
3　製造業
4　電気・ガス・熱供給・水道業
5　情報通信業
6　運輸業、郵便業
7　卸売業、小売業
8　金融業、保険業
9　その他のサービス業
10　教育、学習支援業
11　医療、福祉
12　その他（　　）

問17　委託元の企業規模（総従業員数）をお選びください。（○は1つ）

1　～50 名
2　51名～100名
3　101名～300名
4　301名～500名
5　501名～1,000名
6　1,001名～5,000名
7　5,001名～10,000名
8　10,001名以上
9　わからない

問18　当該事例の委託元は、貴社と資本関係のある系列企業・グループ企業ですか。（○は1つ）

1　系列企業・グループ企業
2　系列企業・グループ企業以外

問19　当該事例のITサプライチェーンにおける、貴社の位置付けをお選びください。（○は1つ）

1　元請け（プライムベンダー）
2　二次請け以降

問20　当該事例に含まれるITシステム・サービスについて当てはまるものを全てお選びください。（○はいくつでも）

1　ソフトウェア開発*
2　システム運用・管理
3　アプリケーション保守
4　ソフトウェアサポートサービス
5　ハードウェア保守
6　Webサイト構築・運用
7　サービス提供（ASP、SaaS等）
8　インフラ提供（IaaS、ホスティング等）
9　データ処理・分析
10　その他（　　）

*顧客固有のアプリケーションソフトウェアを開発する業務を指し、パッケージソフトウェアを利用した事例も含みます。

→ 問20-1　問20で「1ソフトウェア開発」を選んだ方にお伺いします。委託された開発工程について、当てはまるものを全てお選びください。（○はいくつでも）

1　システム・ソフトウェア要件定義
2　基本設計
3　詳細設計
4　ソフトウェア構築
5　結合テスト
6　総合テスト(ベンダー確認)
7　総合テスト(ユーザ確認)
8　移行
9　その他（　　）

問21　当該事例のITシステム・サービスの障害発生時の社会的影響度について、当てはまるものをお選びください。（○は１つ）

1　人命に影響、甚大な経済損失が想定される（航空管制，建築構造計算，医療関連機器制御、救急医療NW等）
2　社会的影響が極めて大きい（輸送，通信，金融・証券，プラント制御等）
3　社会的影響が限定される（放送、行政、水道、建設等）
4　社会的影響が殆ど無い（勤怠管理等、影響範囲が事業者内にとどまるもの）

問22　当該事例のITシステム・サービスのネットワークの範囲について、当てはまるものをお選びください。（○は1つ）

1　ネットワークには接続されていない（スタンドアロン）
2　委託元の1事業所の同一の建物内に限定されているネットワーク（LAN）
3　委託元の複数の事業所を結ぶネットワーク（WAN）
4　委託元と委託元の取引先の事業所を結ぶネットワーク（B to B）
5　委託元と委託元の製品・サービスの利用者を結ぶネットワーク（B to C）
6　その他（　　）

問23　当該事例のITシステム・サービスで扱う情報資産について、当てはまるものを全てお選びください。（○はいくつでも）

1　クレジットカード等の個人信用情報や病歴等の要配慮個人情報を含む個人情報
2　クレジットカード等の個人信用情報や病歴等の要配慮個人情報を含まない個人情報
3　営業秘密
4　1～3以外の非公開情報
5　情報資産はない
6　情報資産の内容はわからない

→ 問23-1　問23で1または2の個人情報を選んだ方にお伺いします。個人情報のデータ件数について、当てはまるものをお選びください。（○は１つ）

1　5,000件未満
2　5,000件～100,000件未満
3　100,000件以上
4　データ件数はわからない

問24　当該事例の業務で扱う情報資産に関して、契約の際に情報セキュリティ上のリスクをどの程度懸念しましたか。それぞれの脅威に対する懸念の度合いとして当てはまるものをお選びください。（✔は各行につき、1つ）

	1 非常に懸念した	2ある程度懸念した	3 あまり懸念しなかった	4全く懸念しなかった	5わからない
a. 内部不正					
b. 外部攻撃（ウイルス感染や不正アクセス等）					
c. 人的ミス(誤操作等)					
d. システム障害、停止					
e. 災害					

＜契約＞

問25　以下の情報セキュリティに係る要求事項について、当該事例の契約関連文書（仕様書、契約書等）にどのように記載されているか、選択肢の番号でご回答ください。

1　当該文書は使用していない
2　当該文書は使用しているが、当該項目は要求事項となっていないので、項目そのものの記載がない
3　当該項目の記載があるが、委託先（貴社）が責任を負うべき範囲が明示されていない（「都度調整」等）
4　当該項目について、委託先（貴社）が責任を負うべき範囲が明示されている

	約款	提案書	委託元の仕様書	貴社の見積書	契約書	覚書	その他（SLA*等）
a.秘密保持							
b,証跡の提示、監査協力等							
c.情報セキュリティに関する契約内容に違反した場合の措置							
d.インシデントが発生した場合の対応							
e. 可用性（稼働率の水準、目標復旧時間等）							
f. 新たな脅威（脆弱性等）が顕在化した場合の情報共有・対応							
g.再委託の禁止または制限							
h.契約終了後の情報資産の扱い（返却、消去、廃棄等）							

*Service Level Agreementの略。委託者とサービス提供事業者の間で結ばれるサービスのレベルに関する合意文書。

→ 問25-1　問25の情報セキュリティ要求事項のいずれかについて「4委託先（貴社）が責任を負うべき範囲が明示されている」を選んだ方にお伺いします。情報セキュリティに関する委託先（貴社）の責任範囲についてどのように明示されていましたか。当てはまるものを全てお選びください。（○はいくつでも）

1　一定の条件において委託先（貴社）が責任を負わない免責規定を定めていた
2　損害賠償額に受託業務の契約金額等で上限を設定していた
3　ソフトウエア開発等において、瑕疵（契約不適合）に関する項目の中で、業務委託完了後に発覚した未知の脆弱性等を対象としていた
4　その他（　　）を定めていた

問26　当該事例の契約関連文書（仕様書、契約書等）では、委託先（貴社）が実施すべき組織的な情報セキュリティ対策が明記されていましたか。（〇は1つ）

1　明記されていた　→問26-1にもご回答ください
2　明記されていなかった

→ 問26-1　問26で選択肢「1明記されていた」を選んだ方にお伺いします。委託先（貴社）が実施すべき組織的な情報セキュリティ対策として明記されていたものを全てお選びください。（✔はいくつでも）

〇情報セキュリティに関する規程類や推進体制の整備	
1 情報セキュリティポリシーや情報セキュリティ管理に関する規程の整備及び実践	
2 全社的な情報セキュリティの推進体制やコンプライアンスの推進体制の整備	
3 重要な情報資産に対する重要性のレベルごとの分類、レベルに応じた表示や取扱方法の規定	
4 重要な情報の利用、保管、持ち出し、消去、破棄等に対する取扱い手順の規定	
5 再委託時の契約における情報セキュリティ要求事項の明記	
〇従事者の不正対策	
6 従業者に対する情報セキュリティに関する就業上の義務の明確化（採用、退職時における守秘義務に関する書面の取り交わし等）	
7 従業者に対する情報セキュリティに関する自組織の取組みや関連規程類についての計画的な教育や指導の実施	
8 重要な情報資産のある建物や区画に対する物理的セキュリティ対策、入退室管理の実施	
9 重要な書類、モバイルPC、記憶媒体に対する施錠管理等の適切な管理の実施	
10 従業者ごとの操作ログ等の取得・保存	
11 私物のモバイル機器や記憶媒体に対する持ち込み、持ち出しの管理	
12 単独作業の制限、承認手続き	
13 従業者からの当該受託業務の秘密保持等に関する誓約書の取得	
〇技術的な取組み・インシデント対応	
14 重要なデータや関連するシステムのバックアップに関する手順の文書化及び実施	
15 不正プログラム（ウイルス、ワーム、トロイの木馬、ボット、スパイウエア等）への対策実施	
16 情報システムに対する、適切かつ迅速な脆弱性対策の実施	
17 ネットワーク上のデータに対する暗号化等の適切な保護策の実施	
18 モバイルPC、記憶媒体やデータの外部持ち出しに対する、盗難、紛失等を想定した対策の実施	
19 データや情報システムの利用者IDの管理、利用者の識別と認証の実施	
20 データや情報システム、業務アプリケーション等に対するアクセス権の付与とアクセス制御の実施	
21 ネットワークのアクセス制御の実施	
22 インシデント発生時の適切かつ迅速な初動対応、報告の実施	

問27　当該事例において使用した契約書の書式は委託元のものですか、委託先のものですか。当てはまるものをお選びください。（〇は1つ）

1　委託元の契約書の書式
2　委託先（貴社）の契約書の書式
3　その他（　　）

問28　当該事例において使用した契約書の書式は、対象業務の情報セキュリティ要求事項に合わせて、情報セキュリティに関する項目を追加したり、内容を修正したりするカスタマイズを行いましたか。当てはまるものをお選びください。（〇はいくつでも）

1　カスタマイズはしていない（雛形のまま使用）
2　委託元の要求で、不足している情報セキュリティ要求事項を追加した
3　委託元の要求で、実現できない情報セキュリティ要求事項を削除した
4　委託先（貴社）の要求で、不足している情報セキュリティ要求事項を追加した
5　委託先（貴社）の要求で、実現できない情報セキュリティ要求事項を削除した
6　その他（　　）

問29　当該事例において、受託業務の契約における情報セキュリティ要求項目に関し、委託元との間で何らかのトラブルが発生したことがありますか。当てはまるものをお選びください。（○は1つ）

1　発生した
2　発生していない

→ 問29-1　問29で選択肢「1発生した」を選んだ方にお伺いします。発生したトラブルをどのように解決したか、自由記入でご回答ください。

（例1）セキュリティの脆弱性が契約終了後に発覚し、当社に責任があるかどうかでもめた。テストで発見することが可能な脆弱性だったのに、確認が漏れていたことが分かったので当社で無償で対応した。

（例2）委託元のセキュリティ監査で、再委託先のデータセンターの現地審査をさせてほしいと依頼された。契約の際には求められていなかったので、断ったところもめた。再委託先から公開されている情報セキュリティ報告書を使用した。

ご協力ありがとうございました

このアンケート調査の調査結果は、IPAにより公表されることがありますが，データの特徴から具体的な企業や事例の内容が特定されることがないよう、統計的な処理を行います。ご懸念がある場合は、調査実施機関にお問い合わせください。