

企業における営業秘密管理に関する実態調査2024

【回答形式】SA=シングルアンサー(単一回答)/MA=マルチアンサー(複数回答)/NUM=数値入力		
設問番号	回答形式	設問文
■スクリーニング		
調査項目		

回答者:全員

F1	SA	あなたの性別をお答えください。	回答者の性別
		1 男性 2 女性	
F2	NUM	あなたの年齢をお答えください。	回答者の年代
		歳	
		→19歳以下、70歳以上は調査終了	
F3	SA	あなたのお住まいの地域をお答えください。	回答者の居住地域
		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 海外	→調査終了

設問番号	回答形式	設問文	調査項目
回答者:全員			
SC1	SA	あなたが所属する組織の主要業種についてお教えてください。なお、複数の事業がある場合は、直近の決算で売上高が最も大きいものをお選びください。 売上高が等しい場合も、1事業だけ選んでお答えください。	回答者の所属組織の業種
		1 農林業	
		2 漁業	
		3 鉱業、採石業、砂利採取業	
		4 建設業	
		5 製造業	←※割付で製造業
		6 電気・ガス・熱供給・水道業	
		7 情報通信業	
		8 運輸業	
		9 卸売業	
		10 小売業	
		11 金融業、保険業	
		12 不動産業、物品賃貸業	
		13 専門・技術サービス業	
		14 宿泊業	
		15 飲食サービス業	
		16 生活関連サービス業、娯楽業	
		17 教育、学習支援業	
		18 医療、福祉	
		19 サービス業（他に分類されないもの）	
		20 その他（ ）	
回答者:SC1=5を選択された方に表示			
SC2	SA	あなたが所属する組織の主要業種(中分類)についてお教えてください。売上高が等しい場合も、1事業だけ選んでお答えください。	回答者の所属組織の業種（中分類）
		1 食料品	
		2 繊維工業	
		3 家具・装備品	
		4 パルプ・紙・紙加工品	
		5 化学	
		6 プラスチック製品	
		7 ゴム製品	
		8 窯業・土石製品	
		9 鉄鋼	
		10 非鉄金属	
		11 金属製品	
		12 電機・情報通信機械・電子部品	
		13 汎用、生産・業務用機械	
		14 輸送用機械	
		15 その他（ ）	

設問番号	回答形式	設問文	調査項目
回答者:全員			
SC3	SA	あなたが所属する組織の従業員数について教えてください。	回答者の所属組織の従業員数
		1 1～4人	
		2 5～30人	
		3 31～100人	
		4 101～300人	
		5 301～1,000人	
		6 1,001～3,000人	
		7 3,001人以上	
回答者:全員			
SC4	SA	あなたが所属する組織の資本金について教えてください。	回答者の所属組織の資本金
		1 1,000万円以下	
		2 1,000万円超～5,000万円以下	
		3 5,000万円超～1億円以下	
		4 1億円超～3億円以下	
		5 3億円超～5億円以下	
		6 5億円超～10億円以下	
		7 10億円超～100億円以下	
		8 100億円超～	
		9 その他()	
回答者:全員			
SC5	SA	あなたが所属する組織の売上高(2023年度)について教えてください。	回答者の所属組織の売上高
		1 10億円以下	
		2 10億円超～100億円以下	
		3 100億円超～1,000億円以下	
		4 1,000億円超～5,000億円以下	
		5 5,000億円超	
回答者:全員			
SC6	SA	あなたは所属する組織内で、以下の「企業の情報システム部門、セキュリティ・リスク管理部門」のうち、所属している部門を教えてください。	回答者の所属部門
		1 企業における情報システム関連部門	
		2 企業のリスクマネジメント計画・実践に関わる部門	
		3 企業のサイバーセキュリティに関わる部門	
		4 経営企画部門	
		5 経営層	
		6 その他セキュリティやリスクマネジメントに関する業務を実施している部門	
		7 上記にあてはまる部門に所属はしていない	→調査終了

設問番号	回答形式	設問文	調査項目																																																		
■本調査																																																					
回答者:全員																																																					
Q1	SA	あなたが所属する組織において、過去5年以内で営業秘密の漏えい事例はありましたか。 1 明らかに情報漏えい事例と思われる事象が複数回あった 2 明らかに情報漏えい事例と思われる事象が1度あった 3 おそらく情報漏えいではないかと思われる事象があった 4 情報漏えいの事例はない 5 わからない・認識できていない	過去5年以内の営業秘密の漏えい事例の有無																																																		
回答者:Q1=1〜3を選択された方に表示(情報漏えい事例と思われる事象があった)																																																					
Q2	SA	漏えいした営業秘密は、具体的にどのようなものでしたか。 また、流出したそれぞれの営業秘密はあなたが所属する組織の事業においてどの程度重要な情報でしたか。複数流出している場合は、最も重要な情報について記載してください。 「その他」にあたる情報がない場合は、「なし」と記入いただき「無」を選択ください。	漏えいした情報の種類																																																		
		<table><tr><td></td><td>有</td><td>可能性有</td><td>無</td><td>不明</td></tr><tr><td>製造に関するノウハウ、成分表等</td><td>→</td><td></td><td></td><td></td></tr><tr><td>生産プロセス等の工程</td><td>→</td><td></td><td></td><td></td></tr><tr><td>製品・部品・金型等の設計図</td><td>→</td><td></td><td></td><td></td></tr><tr><td>施設（製造プラント、工場設備等）のレイアウト</td><td>→</td><td></td><td></td><td></td></tr><tr><td>経営戦略・事業戦略に関する情報</td><td>→</td><td></td><td></td><td></td></tr><tr><td>サービス提供上のノウハウ</td><td>→</td><td></td><td></td><td></td></tr><tr><td>顧客情報</td><td>→</td><td></td><td></td><td></td></tr><tr><td>従業員の個人情報（生年月日、氏名、メールアドレス、その他アカウント情報 等）→</td><td></td><td></td><td></td><td></td></tr><tr><td>その他（ない場合はなしと記入、無を選択ください）（ ）→</td><td></td><td></td><td></td><td></td></tr></table>		有	可能性有	無	不明	製造に関するノウハウ、成分表等	→				生産プロセス等の工程	→				製品・部品・金型等の設計図	→				施設（製造プラント、工場設備等）のレイアウト	→				経営戦略・事業戦略に関する情報	→				サービス提供上のノウハウ	→				顧客情報	→				従業員の個人情報（生年月日、氏名、メールアドレス、その他アカウント情報 等）→					その他（ない場合はなしと記入、無を選択ください）（ ）→					
	有	可能性有	無	不明																																																	
製造に関するノウハウ、成分表等	→																																																				
生産プロセス等の工程	→																																																				
製品・部品・金型等の設計図	→																																																				
施設（製造プラント、工場設備等）のレイアウト	→																																																				
経営戦略・事業戦略に関する情報	→																																																				
サービス提供上のノウハウ	→																																																				
顧客情報	→																																																				
従業員の個人情報（生年月日、氏名、メールアドレス、その他アカウント情報 等）→																																																					
その他（ない場合はなしと記入、無を選択ください）（ ）→																																																					
回答者:Q1=1〜3を選択された方に表示(情報漏えい事例と思われる事象があった)																																																					
Q3	SA	漏えいした営業秘密は、具体的にどのようなものでしたか。 また、流出したそれぞれの営業秘密はあなたが所属する組織の事業においてどの程度重要な情報でしたか。複数流出している場合は、最も重要な情報について記載してください。	漏えいした情報の重要度																																																		
		<table><tr><td>↓ Q2で「有」及び「可能性有」を選択したものを表示</td><td>非常に重要</td><td>重要</td><td>あまり重要でない</td><td>わからない</td></tr><tr><td>製造に関するノウハウ、成分表等</td><td>→</td><td></td><td></td><td></td></tr><tr><td>生産プロセス等の工程</td><td>→</td><td></td><td></td><td></td></tr><tr><td>製品・部品・金型等の設計図</td><td>→</td><td></td><td></td><td></td></tr><tr><td>施設（製造プラント、工場設備等）のレイアウト</td><td>→</td><td></td><td></td><td></td></tr><tr><td>経営戦略・事業戦略に関する情報</td><td>→</td><td></td><td></td><td></td></tr><tr><td>サービス提供上のノウハウ</td><td>→</td><td></td><td></td><td></td></tr><tr><td>顧客情報</td><td>→</td><td></td><td></td><td></td></tr><tr><td>従業員の個人情報（生年月日、氏名、メールアドレス、→</td><td></td><td></td><td></td><td></td></tr><tr><td>その他（Q2「その他」の回答を表示）</td><td>→</td><td></td><td></td><td></td></tr></table>	↓ Q2で「有」及び「可能性有」を選択したものを表示	非常に重要	重要	あまり重要でない	わからない	製造に関するノウハウ、成分表等	→				生産プロセス等の工程	→				製品・部品・金型等の設計図	→				施設（製造プラント、工場設備等）のレイアウト	→				経営戦略・事業戦略に関する情報	→				サービス提供上のノウハウ	→				顧客情報	→				従業員の個人情報（生年月日、氏名、メールアドレス、→					その他（Q2「その他」の回答を表示）	→				
↓ Q2で「有」及び「可能性有」を選択したものを表示	非常に重要	重要	あまり重要でない	わからない																																																	
製造に関するノウハウ、成分表等	→																																																				
生産プロセス等の工程	→																																																				
製品・部品・金型等の設計図	→																																																				
施設（製造プラント、工場設備等）のレイアウト	→																																																				
経営戦略・事業戦略に関する情報	→																																																				
サービス提供上のノウハウ	→																																																				
顧客情報	→																																																				
従業員の個人情報（生年月日、氏名、メールアドレス、→																																																					
その他（Q2「その他」の回答を表示）	→																																																				

設問番号	回答形式	設問文	調査項目
回答者:Q1=1~3を選択された方に表示(情報漏えい事例と思われる事象があった)			
Q4	MA	どのようなことから漏えい事例を認識しましたか。	漏えい事例を認識したきっかけ
		1 貴社しか知り得ない情報がインターネットや文献等に掲載されているのを偶然発見した	
		2 貴社しか知り得ない情報を他社が使用しているのを偶然発見した	
		3 貴社製品の類似品が市場に出回った	
		4 競合他社の研究開発のスピードが速まった	
		5 第三者(取引先、貴社製品ユーザー、匿名電話等)から、貴社の情報が漏えいしているのではないかと指摘を受けた	
		6 漏えいを察知できるような自発的な活動(外部への発信メールのチェック、ログのモニタリング等)により流出したことが発覚した	
		7 貴社の役員・従業員等からの報告があった	
		8 貴社の役員・従業員等が競合他社と接触している事実から調査したところ発覚した	
		9 電子メールや物流上のトラブル(郵便の誤配送等)が生じた	
		10 その他()	
		11 特に根拠はない	
回答者:Q1=1~3を選択された方に表示(情報漏えい事例と思われる事象があった)			
Q5	SA	営業秘密の漏えいによって、どの程度の損害(2回以上流出している場合はその合計)が生じていると考えていますか(大まかな推定で構いません)。	漏えいによる推定損害額
		1 1,000万円未満	
		2 1,000万円以上1億円未満	
		3 1億円以上10億円未満	
		4 10億円以上100億円未満	
		5 100億円以上1,000億円未満	
		6 1,000億円以上	
		7 わからない	
回答者:Q1=1~3を選択された方に表示(情報漏えい事例と思われる事象があった)			
Q6	MA	営業秘密はどこに漏えいしましたか(したと思います)。 (外国の競合他社・外国の競合他社以外の企業を選択した方で、国名・地域が不明な場合は「不明」と記入してください)	漏えい先
		1 国内の競合他社	
		2 国内の競合他社以外の企業	
		3 外国の競合他社(国名・地域)	
		4 外国の競合他社以外の企業(国名・地域)	
		5 その他()	
		6 わからない	

設問番号	回答形式	設問文	調査項目
回答者: Q1=1〜3を選択された方に表示(情報漏えい事例と思われる事象があった)			
Q9	MA	営業秘密の漏えい後、以下の不審な現象は観察されましたか。	営業秘密の漏えい後に観察された不審な事象
		1 ネットワークが遅くなったり、頻繁に切断されたりした。 2 不明なプロセスが多数実行されていた 3 通常とは異なるIPアドレスやポートへの通信が頻繁に発生した。 4 大量のデータが外部に送信されていた。 5 特定の時間に集中して通信が発生した。 6 パスワードが変更された形跡があった。 7 普段利用しないサービスにログインされた形跡があった。 8 不審なメールやメッセージが届いた。 9 重要なファイルが暗号化されていた。 10 不明なエラーメッセージが表示されていた。 11 ウイルス対策ソフトが頻繁に警告を出していた。 12 漏えいが発覚する前に、社外秘情報が外部に漏えいしたという情報が入っていた。 13 漏えいが発覚する前に、社員の不正な行為が疑われていた。 14 社員になりましたメールが届いた。 15 マルウェアに感染したファイルが送り付けられてきた。 16 その他() 17 わからない	
回答者: 全員			
Q10	MA	自社の営業秘密の漏えいに関して、現在脅威と感じ、対策が必要と考えているものを、最大3つまで選択してください。	営業秘密の漏えいに関して必要な対策
		1 自社の営業秘密を狙う外部からの標的型攻撃 2 自社の情報管理やサイバーセキュリティ対策に関する体制の不備や担当者のスキル不足 3 自社の秘密情報管理に関するルールの不備 4 自社で利用するシステムやサービスの設定ミスや対策の不徹底（例：脆弱性の放置等） 5 従業員、退職者や委託先等による意図的な内部不正 6 従業員に対する悪意の第三者（競合企業のスパイ等）の接触 7 自社で契約していないクラウドサービスや個人で利用している電子メール（フリーメール含む）やストレージサービス、私物端末等を用いて従業員が営業秘密を扱うこと 8 テレワーク環境、ビデオ会議システム等、新たな環境において従業員等が営業秘密情報を扱うこと 9 国内の協業先・共同研究先からの自社秘密情報の漏えい 10 海外の拠点・取引先・連携先等を通じた自社秘密情報の漏えい 11 その他() 12 脅威と感じているものはない	

設問番号	回答形式	設問文	調査項目
回答者:全員			
Q11	MA	内部不正を誘発する環境や状況として以下が例として挙げられます。あなたが所属する組織またはあなたの身の回りに当てはまるものはありますか。	内部不正を誘発する環境や状況
		1 同じ仕事・業務を同じ人が長く続けている 2 少ない人数で業務を回している 3 人間関係、コミュニケーション、上司や会社への恨みが大きい 4 借金がある人が、営業秘密等を業務で取扱っている 5 なんらかの弱みを握られて脅迫されている 6 上記に当てはまるものはないと思う 7 回答したくない	
回答者:全員			
Q12	SA	あなたが所属する組織の保有する情報について、営業秘密とそれ以外の情報とを区分していますか。 また、営業秘密をその秘密性のレベルに応じて格付け（「極秘」、「秘」など）していますか。	営業秘密の区分及び格付け実施の有無
		1 営業秘密とそれ以外の情報とを区分しており、営業秘密に関してはさらに秘密性のレベルに応じて区分している 2 営業秘密とそれ以外の情報とを区分しているが、秘密性のレベルに応じた区分はしていない 3 営業秘密とそれ以外の情報とを区分していない 4 わからない	
回答者:全員			
Q13	SA	あなたが所属する組織の保有する営業秘密について、社内規程として定められた管理ルールはどの程度厳密に運用されているとお考えですか （例:エビデンスを残す、定期的な内部監査・アセスメントの実施等）。	営業秘密の管理ルールの運用状況
		1 全社において厳密な運用が徹底されている 2 ある程度厳密に運用されている（部署やチーム等によって事情が異なる場合も含む） 3 厳密な運用を目指して改善の途上にある 4 厳密な運用とはいえない 5 管理ルールを制定したのみ 6 わからない	

設問番号	回答形式	設問文	調査項目
回答者:全員			
Q14	MA	営業秘密情報の保護対策を実践する上で問題と感じる事項を選択してください。 1 対策投資に関する経営層の承認を得ることに苦勞すること 2 対策のための人的リソースを割くことが難しいこと 3 技術的対策に要するコストが高額なこと 4 対策の費用対効果を明示しにくいこと 5 電子メールで授受される営業秘密の管理が徹底されていないこと 6 テレワーク（在宅勤務等）やビデオ会議、クラウドサービスの利用、コラボレーションツールの利用等、新たな業務環境における適切な対策の見極めができていないこと 7 従業員に秘密情報管理のルール遵守を徹底させることが難しいこと 8 従業員の私物端末における対策の徹底が難しいこと 9 海外の拠点等で秘密情報管理のルール遵守を徹底させることが難しいこと 10 顧客・取引先から提供された営業秘密情報の管理にあたり、顧客等から過剰に厳しい対策を要求されること 11 自社の営業秘密情報を委託先や協業先に提供する場合に、秘密保持契約を締結しても効果が不明なこと 12 自社で利用する情報システムやサービスの特権管理者による内部不正を完全に防ぐのが難しいこと 13 自社の役員による内部不正を完全に防ぐのが難しいこと 14 退職者の追跡が難しいこと 15 その他（ ） 16 わからない 17 問題は特にない	営業秘密管理を実践する上での問題
回答者:全員			
Q15	SA	あなたが所属する組織では、営業秘密のほか、限定提供データに相当する情報を保有しており、ビジネスで活用していますか。 1 限定提供データを保有しているが、ビジネスで活用はしていない 2 限定提供データを保有しており、ビジネスで活用している 3 保有していない 4 わからない（理由：）	限定提供データの保有と活用
回答者:全員			
Q16	SA	あなたが所属する組織において、サーバーのアクセスログの確認やメールのモニタリング等、営業秘密の漏えいに気付くことができるような技術的対策は実施されていますか。 1 実施しており、従業員等にも周知されている 2 実施しているが、従業員等には周知されていない 3 実施することを検討中 4 実施しておらず、今後の予定もない 5 わからない	営業秘密の漏えいに気付くための技術的対策の実施

設問番号	回答形式	設問文	調査項目
回答者:Q16=1〜3を選択された方に表示(技術的対策を実施、または検討している)			
Q17	MA	技術的対策を実施している、あるいは実施することを検討している場合、具体的な内容をご回答ください。 - ファイアウォールやDMZ、IDS/IPSなどの設置・構築 - ウイルス対策ソフトの導入 - ログ監視ツールによる不正アクセスや不審な動きへの監視 - アクセス制御ツール・サービスによる権限管理 - PCのディスク暗号化や暗号化機能付きUSBの使用 - その他()	実施しているあるいは実施することを検討している技術的対策
回答者:全員			
Q18	MA	営業秘密情報(紙と電子媒体の両方)への不正なアクセスを防ぐための対策として、実施しているものを選択してください。 - 営業秘密を一般情報と分離して保管 - 営業秘密の保管場所への入室制限 - 営業秘密の保管場所の施錠管理 - 営業秘密の破棄時、復元不可能な方法を適用 - 部門単位で、営業秘密の電子データ保存場所へアクセス権を設定 - 個人単位で、営業秘密の電子データ保存場所へアクセス権を設定 - 営業秘密の電子ファイルへのパスワード設定 - 業務使用PC等へのアンチウイルスソフト導入 - 業務使用PC等のOS、アプリ等の常時更新 - ファイアウォール(ソフトや機器)等の導入 - その他() - 特に何もしていない	営業秘密情報への不正アクセス防止策として実施している対策

設問番号	回答形式	設問文	調査項目
回答者:全員			
Q19	MA	営業秘密情報の社外への不正な持出を防ぐための対策として、実施しているものを選択してください。	営業秘密情報の社外への不正持出防止策として実施している対策
		1 営業秘密記載資料の提示後回収	
		2 業務使用PC等のワイヤー等での固定	
		3 USBメモリ、撮影機器等の持ち込み・持ち出し制限	
		4 紙資料、IT機器、記録媒体等の採番・台帳管理	
		5 紙資料、IT機器、記録媒体等の施錠保管	
		6 従業員IDカードでの印刷・複写制限	
		7 業務使用PC等のローカルドライブへの保存制限	
		8 業務使用PC等でのUSBメモリ等への書き出し制御	
		9 USBメモリやDVD等の複製制限	
		10 遠隔データ消去機能を有するPCや端末の利用	
		11 電子メールの添付ファイルの制限・または禁止	
		12 電子メール送信時の上長確認フローを運用（必ず上司等がCCに追加される設定を行っている等）	
		13 コンテンツフィルタによるオンラインストレージ等へのアクセス制限	
		14 その他（ ）	
		15 特に何もしていない	
回答者:全員			
Q20	MA	営業秘密の漏えいを生じさせにくい環境をつくるための対策として、実施しているものを選択してください。	営業秘密の漏えいを生じさせにくい環境をつくるために実施している対策
		1 「関係者以外立入禁止」「撮影禁止」等の警告表示	
		2 従業員への社員証や名札等の着用義務付け	
		3 防犯カメラの設置と周知	
		4 職場の整理整頓、不要文書廃棄	
		5 従業員による不正検知が容易な座席レイアウトの工夫	
		6 情報システムのログの記録・保管と周知	
		7 不自然なアクセス発生時の上司への警告・通知と周知	
		8 不自然なアクセス発生時の本人への警告・通知	
		9 外部への電子メール送信時のチェック機能導入	
		10 その他（ ）	
		11 特に何もしていない	

Q21	MA	転職者・出向者の受け入れや、共同研究・研究受託等によって、自社の情報と他者の情報との混在（コンタミネーション）が生じることがあります。	情報のコンタミネーション対策
-----	----	---	----------------

1	転入者が転入元との関係で負っている秘密保持契約や競業禁止義務といった義務の有無や内容を確認している
2	共同研究の際、自社開発と共同研究開発の担当者を分けている
3	共同研究で出入りする人に対し、「当該情報を共同研究開発目的以外で使用しない」という誓約書を取得している
4	共同研究の際、取得した他社情報の内容、日時、経緯を記録するようにしている
5	共同研究の際、他社情報の電子データは別フォルダで分離し、ID、パスワード等でアクセス制限をする
6	共同研究の際、物理的な実体を持つ物が他社の秘密情報の場合、当該他社専用のキャビネットや倉庫等で分離管理している
7	その他（ ）
8	該当するものはない

Q22	SA	就業規則以外に役員・従業員と秘密保持契約(それに準じるような誓約書を含む)を締結していますか。締結している場合は、秘密保持の期間についてもお答えください。	秘密保持契約の締結状況
-----	----	---	-------------

		締結していない	締結している／在職中	締結している／兼業または副業をしている期間中	締結している／退職後1年未満	締結している／退職後1年～3年未満	締結している／退職後3年以上	締結している／退職後期間の定め無し	わからない
役員	→								
従業員	→								

回答者:全員

なお、就業規則のみで対応している場合は「締結していない」を選択ください。

		締結して いない	締結しよう としたが拒 否されたこ とがある	締結してい る／退職後 1年未満	締結してい る／退職後 1年～3年 未満	締結してい る／退職後 3年以上	締結してい る／退職後 期間の定め 無し	わからない
役員	→							
従業員	→							

設問番号	回答形式	設問文	調査項目
回答者: 全員			
Q24	MA	役員・従業員との競業避止義務契約（それに準じるような誓約書を含む）の中では、競業避止の期間以外に、どのような内容を取り決めていますか。	競業避止義務契約の対象とする内容の範囲
		1 競業避止対象となる「期間」のみを取り決めている	
		2 競業避止対象となる「地域・場所」を限定して取り決めている	
		3 競業避止対象となる「地域・場所」を限定せずに取り決めている	
		4 競業避止対象となる「業務内容・職種」を限定して取り決めている	
		5 競業避止対象となる「業務内容・職種」を限定せずに取り決めている	
		6 競業避止義務の「対価や代償措置」を取り決めている	
		7 その他（ ）	
		8 わからない	
回答者: 全員			
Q25	MA	競業避止義務に違反した役員・従業員に対してどのような対応をとりましたか。	競業避止義務に違反した役員・従業員への対応
		1 違反者に対し警告を行った	
		2 違反者の就職した企業に対し警告を行った	
		3 民事訴訟の提起（仮処分命令の申立てを含む）	
		4 その他（ ）	
		5 何も措置はとらなかった	
		6 違反事例が存在しない（把握できていない場合を含む）	
		7 わからない（関係者外秘の場合を含む）	
回答者: 全員			
Q26	SA	子会社、関連会社、取引先、共同研究先など、あなたが所属する組織事業のサプライチェーンにおける営業秘密の管理状況について、どこまで把握していますか。 最も近いものを選択してください。	サプライチェーンにおける営業秘密の管理状況の把握
		1 直接の取引先の管理状況を把握していない	
		2 直接の取引先の管理状況を把握しているが、再委託先等への営業秘密提供について条件を定めていない	
		3 直接の取引先の管理状況を把握し、再委託先等への営業秘密提供の条件を定め、管理状況の把握は取引先に行わせている	
		4 営業秘密を提供する直接の取引先の管理状況を検査や報告により把握するとともに、取引先から再委託先等への営業秘密提供の条件を定め、再委託先の管理状況の把握も自ら実施している	
		5 営業秘密のやりとりを行う相手先がない	

設問番号	回答形式	設問文	調査項目
回答者:全員			
Q27	SA	あなたが所属する組織では、クラウドサービスを使って、社内・社外を問わず、営業秘密の共有や参照を行っていますか。	クラウドサービスを使用した営業秘密の共有や参照
	1	社内・社外を問わず、共有を行っている	
	2	社内に関り共有を行っており、社外では共有を行っていない	
	3	社内では共有を行っておらず、社外に関り共有を行っている	
	4	過去には共有していたが、現在は行っていない	
	5	現在は行っていないが、将来行うことを検討している	
	6	行ったことがなく、今後の予定もない	
回答者:全員			
Q28	MA	クラウドサービスにおける営業秘密に関する不正使用リスクを想定した対策として、実施しているものを選択してください。	クラウドサービスにおける営業秘密の不正使用リスク対策
	1	クラウドサービス上でアクセス権限が適切に設定されているかどうかを定期的に確認	
	2	クラウドサービスの認証情報（パスワード等）が適切に設定されているかどうかを定期的に確認	
	3	アクセスログを参照可能なクラウドサービスにて、ログ分析を実施	
	4	クラウド利用に関する監査を実施	
	5	管理者権限を役割別に分けること（ロールベースのアクセス制御等）による不正の抑制	
	6	管理者権限を複数名に割当てることによる相互牽制の実施	
	7	秘密情報の流出検知機能（ダミーデータの格納等）の利用	
	8	秘密情報を格納した電子データの開封確認機能（Webビーコン等）の利用	
	9	その他（ ）	
	10	クラウドサービスを利用していない、または上記のいずれも実施していない	
回答者:全員			
Q29	SA	あなたが所属する組織では、「シャドークラウド」（あなたが所属する組織のセキュリティ担当者が把握していない、個人や部署が勝手に利用しているようなクラウドサービス）が生ずることを防止する対策を講じていますか。	「シャドークラウド」が生ずることを防止する対策の実施状況
	1	クラウド利用に関するルールを設けるとともに、検知する仕組み（CASB等）も運用している	
	2	クラウド利用に関するルールを設けているのみ	
	3	クラウド利用に関するルール策定を検討している	
	4	何も講じていない	

設問番号	回答形式	設問文	調査項目
回答者: 全員			
Q30	SA	近年、生成AIの技術が急速に発展し、情報検索から画像編集に至るまで、さまざま分野で活用が進んでいます。 生成AIを業務に利用する際、秘密情報を誤って生成AIに入力してしまう可能性が想定されます。 あなたが所属する組織における生成AIの業務利用について、秘密情報を保護する観点でどのような対策を行っていますか。当てはまるものを選んでください。 1 業務環境から生成AIを強制的に利用できなくしている 2 ルールを定め、業務では、一切生成AIを利用してはならないことになっている 3 ルールを定め、業務では、外部にもオープンな生成AIに、公開情報のみ生成AIに入力して、取扱ってよいことになっている 4 ルールを定め、業務では、組織内に情報開示を閉じた生成AI環境で、秘密情報を含めすべての情報を取扱ってよいことになっている 5 ルールはなく、業務では、自由に組織内外の生成AIを利用できる 6 上記以外の手段を用いて、生成AIによる秘密情報漏えいの対策を実施している（実現例 ※自由記述） 7 わからない	生成AIの業務利用に関してルールを定めている割合
回答者: 全員			
Q31	SA	営業秘密を含む技術情報や物品の海外への持ち出しに際しては、不正競争防止法に加え、外国為替及び外国貿易法（外為法）が定めるリスト規制やキャッチオール規制等にも対応する必要があります。外為法を遵守するための社内の輸出管理体制は整備されていますか。 1 該非判定（当該技術や物品が、規制に該当するかどうかの判断）によって、外為法で定められた事前許可が必要かどうか判断する規程やマニュアルが整備され、その周知・教育も行っている 2 該非判定によって、外為法で定められた事前許可が必要かどうか判断する規程やマニュアルを整備しているが、その周知・教育はできていない 3 外為法を遵守するための規程やマニュアル整備の必要は認識しているが、整備中である 4 当社では整備する必要を認めず、特に整備していない 5 わからない	外為法を遵守するための社内の輸出管理体制の整備状況
回答者: 全員			
Q32	MA	メール等による情報のやり取りを含め、海外の拠点や取引先に対して秘密情報の提供等を行う際、他国の法令について配慮することはありますか。 1 個人情報を含む秘密情報提供に際して、EUの一般データ保護規則（GDPR）に配慮している 2 米国の輸出管理規則（EAR）の適用範囲・規制対象・禁止事項等に沿うよう配慮している 3 上記以外の国の法令についても配慮している（国・法令名 ） 4 日本国外の法令についても配慮する必要があると感じているが、まだ配慮できていない 5 当社では配慮する必要を認めていないため、配慮していない 6 わからない	海外の拠点や取引先に対する秘密情報の提供等の際に配慮する他国の法令

設問番号	回答形式	設問文	調査項目
回答者:全員			
Q33	SA	秘密情報の漏えい時におけるあなたが所属する組織の組織体制について、選択してください。	秘密情報の漏えい時の組織体制
		1 経営層がリーダーシップを取る横断的組織等が主導して対策を検討・実施する体制である	
		2 特定の部署等が主導して対策を検討・実施する体制である	
		3 部署ごとに対策を検討・実施する体制である	
		4 その他()	
		5 特にない	
回答者:全員			
Q34	SA	秘密情報の漏えい時に対応を主導する部署・担当はどこですか。	秘密情報の漏えい時に対応を主導する部署・担当
		1 情報システム部門・システム担当者	
		2 サイバーまたは情報セキュリティ対策部門・サイバーまたは情報セキュリティ対策担当者	
		3 法務部門・法務担当者	
		4 知財部門・知財担当者	
		5 コンプライアンス部門・コンプライアンス担当者	
		6 リスク管理部門・リスク管理担当者	
		7 総務部門・業務管理担当者	
		8 経営者・経営者直轄チーム	
		9 その他()	
		10 決まっていない	
回答者:全員			
Q35	MA	テレワーク(在宅勤務等)の環境で営業秘密を扱う場合のルールの内容として、あてはまるものを選択してください。	テレワーク環境で営業秘密を扱う場合のルール
		1 家族や第三者が秘密情報にアクセスしないようにするための対策の実施に関すること	
		2 通信ネットワークを通じて秘密情報を送受するときの情報の保護対策(VPN利用、暗号化等)に関すること	
		3 私物の端末で秘密情報を扱う場合の情報漏えい防止対策に関すること	
		4 無料のインターネットサービス(メール、ファイル授受、ストレージ等)の業務利用に関すること(営業秘密を扱うかどうかに限らず)	
		5 ビデオ会議やコラボレーションツールで秘密情報を扱う場合の対策の実施に関すること	
		6 クラウドサービス(ビデオ会議を除く、職場で許可されているもの)で秘密情報を扱う場合の対策の実施に関すること	
		7 自宅や社外から顧客等との間で秘密情報を送受や共有するときの対策の実施に関すること	
		8 秘密情報が保存されているサーバー等へのアクセスに用いる認証情報(パスワード、ICカード等)の管理に関すること	
		9 ソーシャルメディア(SNS等)の利用に関すること	
		10 書類の持出しに関すること	
		11 その他()	
		12 テレワークにおける情報管理のルールはない	

設問番号	回答形式	設問文	調査項目
回答者: 全員			
Q36	MA	経済産業省が2016年に公表した「秘密情報の保護ハンドブック」(以下、「ハンドブック」)(※)を、あなたが所属する組織の対策における参考として活用している場合、今後の改定で実施してほしい内容を選んでください。 ※公表URL https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html 1業種に固有の内容を入れてほしい 2企業が取引先に実際に求めているルールや対策の事例を紹介してほしい 3テレワーク(在宅勤務等)における営業秘密の保護に関する内容を増やしてほしい 4クラウドサービスで営業秘密を管理する際の対策に関する内容を増やしてほしい 5認証を強化する方法に関する内容を増やして欲しい(ゼロトラストモデルの導入等も含む) 6特権の悪用対策に関する内容を増やしてほしい 7規程等のサンプルをもっと増やしてほしい(具体的な希望内容) 8各規程のサンプルの解説を充実させてほしい 9分厚いので内容別に分冊にするなどしてほしい 10その他の要望() 11特に見直しの必要は感じない 12ハンドブックを入手しているが、利用していない 13ハンドブックのことは知っているが、入手していない 14ハンドブックがあることを知らなかった	「秘密情報の保護ハンドブック」の今後の改定で実施してほしい内容
回答者: 全員			
Q37	MA	営業秘密の保護にあたり、企業等が対策を講じる時、以下の行政サービス、ガイドライン等が利用できます。知っているものを全てお選びください。 1不正競争防止法テキスト(経済産業省 https://www.meti.go.jp/policy/economy/chizai/chiteki/shiryouhaifu.html) 2啓発・解説パンフレット「知っておきたい営業秘密～予期せぬトラブルに巻き込まれないために～」(経済産業省 https://www.meti.go.jp/policy/economy/chizai/chiteki/shiryouhaifu.html) 3秘密情報の保護ハンドブック(経済産業省 https://www.meti.go.jp/policy/economy/chizai/chiteki/shiryouhaifu.html) 4情報管理も企業力 秘密情報保護ハンドブックのてびき(経済産業省 https://www.meti.go.jp/policy/economy/chizai/chiteki/shiryouhaifu.html) 5限定提供データに関する指針(経済産業省 https://www.meti.go.jp/policy/economy/chizai/chiteki/shiryouhaifu.html) 6データ利活用のポイント集(経済産業省 https://www.meti.go.jp/policy/economy/chizai/chiteki/shiryouhaifu.html) 7データ利活用のてびき(経済産業省 https://www.meti.go.jp/policy/economy/chizai/chiteki/shiryouhaifu.html) 8技術情報管理 自己チェックリスト(経済産業省 https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/page03.html) 9営業秘密管理指針(経済産業省https://www.meti.go.jp/policy/economy/chizai/chiteki/shiryouhaifu.html) 10営業秘密支援窓口(独立行政法人工業所有権情報・研修館 https://www.inpit.go.jp/katsuyo/tradesecret/madoguchi.html) 11組織における内部不正防止ガイドライン(独立行政法人情報処理推進機構 https://www.ipa.go.jp/security/guide/insider.html) 12あてはまるものはない	行政サービス、ガイドライン等で知っているもの