自動車産業 セキュリティチェックシート(V2.0)

会社名	●●株式会社	評価範囲	マプルダウンから選択ください
会社分類	マプルダウンから選択ください	会社従業員数	マプルダウンから選択ください

達成条件評価欄に達成条件毎の実施レベルをご記入ください。また、評価の根拠記入欄に対策状況をご記入ください。

分類	ラベル	No.	レベル	達成条件	達成基準	他社事例 (参考事例を列記しており、 すべての遵守を求めているものではありません)	対象	担当領域 (回答者検討時の参考情報)	池田事務器&KISPA 提供サービス	Ｓｋｙ株式会社にて追記 対応内容 ※左記に対し、支援可能な項目のみ記載	SKYSEA Client View Light Edition 対応可否	S1 / S3 Cloud Edition 対応可否	M1 Cloud Edition 対応可否	対応状況 0:未実施	1:対応中	2:対応完了	経産省CPSF 要求事項に関する 対策要件ID
共通	1方針	1	Lv1	**自社の情報セキュリティ対応方針(ポリシー)を策定している**	・自社の情報セキュリティ対応方針を策定し、文書化すること	【情報セキュリティ対応方針の記載事項の例】 ・経営者の責任：当社は、情報セキュリティを確保・維持、改善するための活動を、経営者主導で推進します ・法令遵守： 当社は、情報セキュリティに関連する法令を遵守します 【策定・文書化の責任者の例】 ・経営者 ・取締役会	基本方針および推進体制の確立	情報セキュリティ	Secポリシー策定サービス	–						CPS.BE-2 CPS.GV-1
		2	Lv2	**自社の情報セキュリティ対応方針(ポリシー)の内容を確認し、必要に応じて見直ししている**	【規則】 ・社内外の環境変化を踏まえて、内容を確認し、適宜見直ししていること 【頻度】 ・情報セキュリティ対応方針(ポリシー)の内容を確認、改善 -1回以上/年 ※別途、重大な変化が発生した場合には迅速に対応すること	【見直しの例】 ・会社規則に見直しについて規定している ・定期的にセキュリティ委員会で規定見直し状況を報告施している 【社内外の環境変化の例】 ・自社体制の変更 ・対象となる情報資産の変更 ・新たな脅威の検知・管理対象の変更時 ・情報セキュリティ事件・事故発生後	基本方針および推進体制の確立	情報セキュリティ	Secポリシー策定サービス	–						
		3	Lv1	**情報セキュリティ対応方針(ポリシー)を社内に周知している**	【規則】 ・情報セキュリティ対応方針(ポリシー)を容易に確認できる状態にすること 【対象】 ・役員、従業員、社外要員（派遣社員等） 【頻度】 ・定常的に、かつ、情報セキュリティ対応方針の改正時に周知すること	【容易に確認できることの例】 ・壁にポスター等で掲示している ・社内イントラに掲示している 【周知の例】 ・全社員向け一斉メールで周知している ・朝会等で口頭で周知をしている ・役員、従業員の新規受け入れ時に周知している 【周知の責任者の例】 ・経営者 ・取締役会	基本方針および推進体制の確立	情報セキュリティ	Secポリシー策定サービス	–						
	2機密情報を扱うルール	4	Lv1	**自社の守秘義務のルールを規定し、守らせている**	【規則】 ・自社の守秘義務を策定し、文書化すること ・入社時あるいは社外要員の受け入れ時に守秘義務を説明すること ・退職もしくは期間満了時に会社の機密情報を持ち出さないこと 【対象】 ・役員、従業員、社外要員（派遣社員等）	【守秘義務の記載例】 ・在籍中は、業務上の必要がない限り、会社の情報を他者に伝えない ・社外に機密情報を取り扱う業務を委託する場合、必ず機密保持契約をする ・退職もしくは期間満了時に会社PCや会社の資料を返却させる 【理解させ、守らせることの例】 ・退職もしくは期間満了時の機密情報の回収、退職後の義務の書面または対面での説明をしている ・守秘義務の誓約書の雛型を作成し、入社時に署名している ・従業員の就業規則により、機密情報の守秘義務が明記されている ・守秘義務違反時の罰則を規則に記載している ・退職時マニュアルに守秘義務事項を確認する手順を記載している ・機密管理月間を設けて、守秘義務に関する職場自主点検を実施して	守秘義務	法務／人事	Secポリシー策定サービス	–						CPS.GV-2 CPS.SC-5
		5	Lv2		【規則】 ・守秘義務の誓約書を提出させること（社外要員除く）	【実施事例】 ・全社員入社時及び退職時に誓約書提出、研究開発部門への配属社員は毎年誓約書を提出させている	守秘義務	法務／人事	Secポリシー策定サービス	–							
		6	Lv2	**派遣社員、受入出向社員について、派遣元、出向元の会社と守秘義務を締結している**	【規則】 ・守秘義務には、業務で知り得た情報を外部に漏えいさせない旨の記述があること 【時期】 ※守秘義務の締結時期 ・業務開始前	【実施事例】 ・全社契約書ひな形に守秘義務に関する事項を盛り込んでいる ・守秘義務契約を締結するため、基本契約書以外に機密保持契約（NDA）を締結している	守秘義務	法務	Secポリシー策定サービス	–						
		7	Lv2	**退職や期間満了時には必要な機密情報、情報機器などを回収している**	【基準】 ・回収物一覧のチェックシートまたは帳票を作成すること ・回収漏れが起こらない手順を整備、運用すること ・手順に従い回収しているかを確認し、必要に応じて手順の是正を行うこと [回収物] -情報(印刷物、記憶媒体) -情報機器(PC、スマートデバイス) -アクセス権（ID、鍵） ※上記の他に必要な回収物を各社で判断すること 【規則】 ・回収状況の確認、手順の是正頻度	【実施事例】 ・退職、期間満了時、回収物一覧のチェックシートまたは帳票を作成し、回収漏れ発生を防止している	守秘義務	人事	Secポリシー策定サービス	【SKYSEA Client View Light Edition】 ・稼働している端末の一覧を収集可能 ・利用されているUSBデバイス（記憶媒体）を可能 ・USBデバイス(記憶媒体)の棚卸が可能	○	○	○ ※棚卸は不可			
		8	Lv1	**業務で利用する情報機器の利用ルールを規定し、周知している (個人所有機器(BYOD)含む)**	【規則】 ・情報機器（PC、サーバー、通信機器、記憶媒体、スマートデバイス等）の利用ルールを策定し、このルールには利用開始時、利用終了時の手続き、利用中の遵守・禁止事項、紛失時の手続きを含むこと ・情報機器の利用ルールを容易に確認できる状態にすること 【対象】 ・役員、従業員、社外要員（派遣社員等） 【頻度】 ・定常的に、かつ、ルールの改正時に周知すること	【情報機器の利用ルールの記載事項例】 ・BYODの許可もしくは禁止に関するルール ・社給スマートデバイスではApple Store等は使用禁止とし、業務アプリのみの利用としている 【周知の例】 ・情報機器の利用開始時に利用者に説明している ・役員、従業員、派遣社員等の新規受け入れ時に周知している ・情報機器の利用ルールについて、従業員に年1回eラーニングを受講させている ・社内規則に情報機器を利用する際のルールを明記しており、常時閲覧可能な状態で社内イントラサイトに掲載している ・社内の共通電子申請システムで、情報機器の利用申請を行えるようにしている	守秘義務	IT	・Secポリシー策定サービス LanScope EndPointManager SKYSEA Client View モバイル機器管理機能 (MDM)	【SKYSEA Client View Light Edition】 ・Windows端末に対して各種制限を実施することが可能 ・外部記憶媒体(USBデバイス)の使用条件を設定可能 ・OP：iOS端末のアプリケーションを制御可能	○ OP：MDM Services	○ OP：MDM Services	○ OP：MDM Services			
	3法令順守	9	Lv1	**情報セキュリティに関する法令を考慮し、ルールを策定、教育・周知している**	【規則】 ・情報セキュリティに関連する法令を守るための社内ルールを策定すること ・策定した社内ルールを教育・周知すること 【対象】 ・役員、従業員、社外要員（派遣社員等） 【頻度】 （教育） ・新規受け入れ時、かつ、１回／年 （周知） ・定常的に、かつ、ルールの改正時に周知すること	【規則改定の例】 ・個人情報保護法、GDPR、不正競争防止法等の情報セキュリティに関する法令・規則の情報収集をを行い必要に応じ規則改定を行っている ・法令の変更内容がルールに則っているか関係部署で確認している（１回／年） ・策定したルールに、見直す頻度を記載している 【教育・周知の例】 ・策定したルールに、教育・周知頻度を織り込んでいる ・eラーニングで教育を実施している（年1回）	情報セキュリティ対策フレームワークの構築	情報セキュリティ／法務	・Secポリシー策定サービス セキュリティハンドブックを使用した教育実施 ・学び維新、Formsなど(eラーニング) ・セキュリティ研修サービス ・NI Collabo 360/Microsoft 365（情報共有）	【有償サービス】 ・Ｓｋｙ株式会社で作成した研修資料を用いてセミナーを実施可能(要望により内容のカスタマイズ可能)	有償サービス：セキュリティ研修	有償サービス：セキュリティ研修	有償サービス：セキュリティ研修			CPS.GV-2
		10	Lv2	**個人情報をお持ちの会社については、個人情報に特化した社内ルールの規定があること**	【規則】 ・お客様個人情報の取り扱いにおける社内ルールを策定すること [明確にする内容] -個人情報の管理体制を確立 -取得時に利用目的を通知、明示 -本人の同意の範囲内で利用 -本人の同意なしに第三者提供しないこと -本人による開示・訂正・利用停止・消去などの要望に対応すること -個人情報の取扱いルールを定めること -個人情報保護法、GDPR、不正競争防止法等の情報セキュリティに関する法令・規則の情報収集を行うこと	【規則制定の例】 ・個人情報取り扱いに関する会社規則を制定している ・部署ごとに個人情報管理台帳を作成し１回／年の棚卸を実施している 【教育・周知の例】 ・自社ホームページに個人情報保護に関するポリシーを掲載(GDPR含む)している ・コンプライアンス教育の一環として、個人情報保護についても教育している ・eラーニングで教育を実施している（年1回） ・２回／年の社内連絡会で最新の各国法規動向と合わせ全部署に周知・徹底している	情報セキュリティ対策フレームワークの構築	法務	Secポリシー策定サービス	【有償サービス】 ・Ｓｋｙ株式会社で作成した研修資料を用いてセミナーを実施可能(要望により内容のカスタマイズ可能)	有償サービス：セキュリティ研修	有償サービス：セキュリティ研修	有償サービス：セキュリティ研修			
		11	Lv1	**法令の変更に伴い、ルールを適宜見直ししている**	【頻度】 ・1回／年、もしくは、法令の改正が公布・施行された時	【規則改定の例】 ・個人情報保護法、GDPR(欧州一般データ保護規則)、不正競争防止法等の情報セキュリティに関する法令・規則の情報収集をを行い必要に応じ規則改定を行っている ・法令の変更内容がルールに則っているか関係部署で確認している（１回／年） ・策定したルールに、見直す頻度を記載している	情報セキュリティ対策フレームワークの構築	情報セキュリティ／法務	Secポリシー策定サービス	–						
		12	Lv2		【頻度】 ・社内ルールの遵守状況を確認し、必要に応じて是正すること	【実施事例】 ・eラーニングでの受講状況をもとに、是正要否を検討している ・コンプライアンス委員会で、社員および顧客から寄せられた通報内容をモニタリングしている ・１回／年、個人情報管理台帳の棚卸を実施している	情報セキュリティ対策フレームワークの構築	法務	・Secポリシー策定サービス セキュリティハンドブックを使用した教育実施 ・学び維新(eラーニング) ・Forms(eラーニング) ・セキュリティ研修サービス	–						
	4体制(平時)	13	Lv1	**情報セキュリティ責任者を含む、平時の体制と責任と役割を明確化している**	【規則】 ・情報セキュリティを統括する役員（CISO等）や情報セキュリティ 担当部署の役割・責任を明確化すること ・連絡先リストを整備すること	【実施事例】 ・情報セキュリティ対策基準「管理体制」を制定している ・機密保持委員会を設置・運用している ・体制図、必要な連絡先リストを明文化している	基本方針および推進体制の確立	情報セキュリティ	Secポリシー策定サービス	–						CPS.AE-2 CPS.RA-2 CPS.DP-2 CPS.IM-1 CPS.IM-2 CPS.GV-4 CPS.AE-2
		14	Lv2		【規則】 ・情報セキュリティリスクは、経営に重大な影響を及ぼすことを理解し、 組織的に経営判断できる体制を設置していること	【実施事例】 ・役員レベルの方がCISOに任命されている、または、セキュリティ推進の委員会に役員が入った形で情報セキュリティ体制を整備している ・情報セキュリティを統括するCISOとITを統括するCIOは兼務ではなく、別の方を任命している	基本方針および推進体制の確立	情報セキュリティ	Secポリシー策定サービス	–						
		15	Lv1	**定期的、または必要に応じて、平時の体制を見直ししている**	【頻度】 ・１回／年、もしくは、重大な情報セキュリティ事件・事故が発生した場合 ・または、社内組織改正等にて、お客様情報をはじめとした各種情報の保護・管理部署や責任者に変更が生じた時	【実施事例】 ・重大な情報セキュリティ事件・事故が発生した場合や年2回の組織改正に合わせて、平時の体制を見直ししている	基本方針および推進体制の確立	情報セキュリティ	Secポリシー策定サービス	–						

分類	ラベル	No.	レベル	達成条件	達成基準	他社事例 （参考事例を列記しており、 すべての遵守を求めているものではありません）	対象	担当領域 （回答者検討時の参考情報）	池田事務器&KISPA 提供サービス	Ｓｋｙ株式会社にて追記 対応内容 ※左記に対し、支援可能な項目のみ記載	SKYSEA Client View Light Edition 対応可否	S1 / S3 Cloud Edition 対応可否	M1 Cloud Edition 対応可否	対応状況 0：未実施	1：対応中	2：対応完了	経産省CPSF 要求事項に関する 対策要件ID
		16	Lv1	**サイバー攻撃や情報漏えいの新たな手口を知り、対策を社内部署へ共有している**	【規則】 ・平時の体制に則り、情報セキュリティ事件・事故事例やその対応策を社内部署へ共有していること 【対象】 ・役員、従業員、社外要員（派遣社員等） 【頻度】 ・１回／年、もしくは、社内外で重大な情報セキュリティ事件・事故が発生した時	【実施事例】 ・定期的に情報セキュリティ会議を開催し、事件・事故を共有している ・下記収集元の情報を用いて、大型連休前に社内へ注意喚起している <情報収集元> ・新聞/ニュース ・IPA、JPCERT/CC（日本の代表的セキュリティ機関）	情報セキュリティ対策フレームワークの構築	情報セキュリティ	・Secポリシー策定サービス セキュリティハンドブックを使用した教育実施 ・情報セキュリティ対策セミナー 学び維新(eラーニング) Forms(eラーニング) ・セキュリティ研修サービス ・NI Collabo 360/Microsoft 365（情報共有）	【有償サービス】 ・社内部署へ周知のためセミナーを実施可能 (要望により内容のカスタマイズ可能)	有償サービス：セキュリティ研修	有償サービス：セキュリティ研修	有償サービス：セキュリティ研修				
		17	Lv2	**サイバー攻撃や予兆を監視・分析をする体制を整備している**	【規則】 ・サイバー攻撃や脆弱性に関する公開情報、非公開情報を活用する体制を構築している ・相関分析によりサイバー攻撃や予兆の検知を可能とし、その分析結果から適切な対応が導きだせる体制を構築している ※相関分析： 複合的なログなどで分析して情報セキュリティ事件・事故の予兆や痕跡を見つけ出す手法	【体制構築の例】 ・サイバーセキュリティに対応する体制を構築し、多角的なログ収集、ふるまい検知による異常検知、外部委託SOCからの検知情報の確認等を24h/365日で実施する体制を構築している 【インテリジェンス収集】 ・社内にサイバーインテリジェンス専門要員を配置している ・以下のリスク増加の兆候が検知された場合、各情報の相関分析により、次善策の対応が検討できるスキルレベルを有している体制を構築している 1.攻撃形態、関連する通信の内容 2. 核心となる攻撃コード 3. 被害を受けた後の通信内容 4. サーバやクライアントに残るその他特徴 【ログ分析事例】 ・各種ルールによる分析結果等を毎月報告会にて報告している	情報セキュリティ対策フレームワークの構築	情報セキュリティ	・Secポリシー策定サービス ・LanScope EndPointManage ・SKYSEA Client View ・FortiGate ・SubGate ・ESET	【SKYSEA Client View Light Edition】 ・ログ収集機能にて、ユーザーによるPC操作をログとして収集可能 ・OP1：UTM及びAVの異常検知と連動し端末のネットワーク遮断が可能 ・OP2：他社製品：FFRIセキュリティ社製 FFRI yarai（NGAV）と連携しマルウェアの収集・隔離・他端末への感染有無の確認が可能	OP1：ITセキュリティ対策強化 OP2：EDRプラスパック	○ OP1：S1×　※S3のみ搭載 OP2：S1・S3ともにOP	○ OP1：× OP2：×				CPS.RA-2 CPS.PT-1 CPS.CM-3
	5体制(事故時)	18	Lv1	**情報セキュリティ事件・事故発生時の対応体制と責任と役割を明確化している**	【規則】 ・情報セキュリティを統括する役員（CISO等）や情報セキュリティ担当部署の役割・責任が明確化されていること ・情報セキュリティ事件・事故の基準や社内外組織との連絡先、ルートが明確化されていること	【対応体制の例】 ・機密保持委員会を設置している ・情報セキュリティ事件・事故発生時の対応体制をCSIRTとして設置している 【責任者の例】 ・社長 ・CISO	事件・事故対応	情報セキュリティ	Secポリシー策定サービス	–							CPS.AE-2 CPS.RA-2 CPS.RA-3 CPS.DP-2 CPS.IM-1 CPS.IM-2 CPS.AN-3
		19	Lv1	**発生した情報セキュリティ事件・事故対応が実施され、事故の概要や影響および対応内容の記録がある**	【規則】 ・情報セキュリティ事件・事故発生後の初動対応フローが整備されていること ・情報セキュリティ事件・事故の報告フォーマットが整備されていること	【初動対応フローの記載例】 ・№.24 記載の例を参照すること 【事件・事故発生時の報告フローの例】 ・№.18 記載の例を参照すること 【報告フォーマットの項目例】 ・発生日時 ・現象 ・業務影響 ・原因 ・暫定対応（抑制措置と復旧） ・恒久対策（再発防止） ・完了日時（恒久対策）	事件・事故対応	情報セキュリティ	Secポリシー策定サービス ・LanScope EndPointManage ・SKYSEA Client View	【SKYSEA Client View Light Edition】 ・OP1：UTM及びAVの異常検知と連動し端末のネットワーク遮断が可能 ・OP2：他社製品：FFRIセキュリティ社製 FFRI yarai（NGAV）と連携しマルウェアの収集・隔離・他端末への感染有無の確認が可能	OP1：ITセキュリティ対策強化 OP2：EDRプラスパック	○ OP1：S1×　※S3のみ搭載 OP2：S1・S3ともにOP	×				
		20	Lv1	**定期的、または必要に応じて、事故時の体制を見直ししている**	【頻度】 ・１回／年、もしくは、重大な情報セキュリティ事件・事故が 発生した場合等	【見直しの実施例】 ・プロジェクト発足時や人事異動発生時の他、年度初めに体制を見直し ・情報セキュリティ事件・事故発生時に見直し	事件・事故対応	情報セキュリティ	Secポリシー策定サービス	–							
		23	Lv2	**情報セキュリティ事件・事故として扱う対象範囲を明確にし、周知していること**	【規則】 ・下記対象範囲が明確になっていること ［明確にする内容］ -事件・事故として扱う事象 -事件・事故のレベル 【対象】 ・役員、従業員、派遣社員、受入出向者への周知	【対象範囲の例】 ・会社貸与PCやUSBメモリ、図面・報告書等情報記録媒体の紛失・盗難 ・外部からの攻撃（マルウェア感染・不正アクセス・会社ホームページの改ざん・会社貸与PC操作の乗っ取り等） ・機密情報の電子メール・ファクシミリ・郵便（EMS等も含む）等による誤送信 ・業務委託先による機密情報の漏洩 ・社員証、機密エリアへの入場用IDカードの紛失・盗難 ・その他情報漏洩等につながる、もしくは恐れがある事象で、情報セキュリティ管理の統括責任者が重要であると判断したもの ex.内部犯行 【周知の事例】 ・教育内容に「事件・事故として扱う対象範囲」について含めている	事件・事故対応	情報セキュリティ	・Secポリシー策定サービス ・情報セキュリティ対策セミナー 学び維新(eラーニング) Forms(eラーニング) ・セキュリティ研修サービス ・NI Collabo 360/Microsoft 365（情報共有）	【有償サービス】 ・社内部署へ周知のためセミナーを実施可能 (要望により内容のカスタマイズ可能)	有償サービス：セキュリティ研修	有償サービス：セキュリティ研修	有償サービス：セキュリティ研修				CPS.RP-1 CPS.RP-3
		24	Lv1	**情報セキュリティ事件・事故時の対応手順(初動、システム復旧等)を定めている**	【規則】 ・対応手順には組織の必要に応じて下記の手順を含んでいること ①発見報告、 ②初動、③調査・対応、④復旧、⑤最終報告	【対応手順書の記載項目の例】 ・具体的な対処内容 例：マルウェア感染や不正アクセスの疑いがある場合、発見後ただちにネットワークから切り離す ・対処体制、連絡先 ・情報セキュリティ事件・事故状況の調査方法（対象ログ、操作方法） ・技術的な対策方法の検討業務フロー（原因の一次切り分け） ・社内への報告（書式、業務フロー） ・報告項目の例：発見日時、影響範囲、内容、原因 ・広報部を通じて顧客などへのアナウンス方法（書式、業務フロー） 【対応手順書の取り扱い例】 ・常時閲覧可能な状態で電子媒体に掲示し、紙媒体でも保管している	事件・事故対応		・Secポリシー策定サービス ・Fortigate個別構築 ・ESET ＋ SKYSEA Client View(ネットワーク遮断) ・SubgGate（ネットワーク遮断）	【SKYSEA Client View Light Edition】 ・OP1：UTM及びAVの異常検知と連動し端末のネットワーク遮断が可能 ・OP2：他社製品：ESETと連携しマルウェアの収集・隔離・他端末への感染有無の確認が可能	OP1：ITセキュリティ対策強化 OP2：EDRプラスパック	OP1：S1×　※S3のみ搭載 OP2：S1・S3ともにOP	×				
		26	Lv1	**マルウェア感染時の対応手順を定めている**	【規則】 ・マルウェア感染時用の対応手順には組織の必要に応じて下記の手順を含んでいること ①発見報告、 ②初動、③調査・対応、④復旧、⑤最終報告	【対応手順の例】 ・クライアントPCにおいて、マルウェア感染や不正アクセスの疑いがある場合、発見後ただちにネットワークから切り離した後に、情報セキュリティ事件・事故時の報告窓口へ連絡する手順書を定義	事件・事故対応	IT	・Fortigate個別構築 ・ESET ＋ SKYSEA Client View(ネットワーク遮断) ・SubgGate（ネットワーク遮断）	【SKYSEA Client View Light Edition】 ・ログ収集機能にて、ユーザーによるPC操作をログ収集可能。 ・OP1：UTM及びAVの異常検知と連動し端末のネットワーク遮断が可能 ・OP2：他社製品：ESETと連携しマルウェアの収集・隔離・他端末への感染有無の確認が可能	○ OP1：ITセキュリティ対策強化 OP2：EDRプラスパック	○ OP1：S1×　※S3のみ搭載 OP2：S1・S3ともにOP	○ OP1：× OP2：×				
		27	Lv2	**マルウェア感染時の対応手順は、定期的に確認され、必要に応じて、改定していること**	【規則】 ・世間動向や攻撃のトレンドなどをふまえ、教育・訓練内容の見直しをすること 【頻度】 ・1回/年以上	【実施事例】 ・毎年見直しを行い、必要に応じ関係者へ周知している	事件・事故対応	IT	・Secポリシー策定サービス ・セキュリティ対策セミナー	【SKYSEA Client View Light Edition】 ・メッセージ配信機能にて各端末へ情報周知が可能 【有償サービス】 ・社内部署へ周知のためセミナーを実施可能 (要望により内容のカスタマイズ可能)	○ 有償サービス：セキュリティ研修	○ 有償サービス：セキュリティ研修	× 有償サービス：セキュリティ研修				
	7日常の教育	28	Lv1	**電子メールのマルウェア感染に関する社内への教育を行っている**	【規則】 ・電子メールによるマルウェア感染の予防について、教育資料配布・掲示、eラーニング、集合教育等による教育を実施すること ・教育内容を振返り、次回の教育内容を改善すること 【対象】 ・役員、従業員、社外要員（派遣社員等）における メール利用者 【頻度】 ・新規受け入れ時、かつ、１回／年以上	【教育の例】 ・新入社員教育・中途入社教育・社外要員受け入れ集合教育等 ・eラーニングによる教育 ・自社、IPAやセキュリティベンダー等の提供する映像教育コンテンツの視聴 ・自社、IPAやセキュリティベンダー等の提供する教育資料の配布・掲示 ・利用マニュアル等による電子メール利用のリスクと対処法等の解説 ・標的型メール訓練の実施とその解説 【教育頻度の例】 ・新入社員・中途社員・社外要員受け入れ時 ・1回／年 eラーニング による教育を実施 ・1回／年 更新内容を中心とした教育資料・マニュアル等の再確認の通知	教育・啓発	情報セキュリティ／IT	・Secポリシー策定サービス セキュリティハンドブックを使用した教育実施 ・情報セキュリティ対策セミナー 学び維新(eラーニング) Forms(eラーニング) ・セキュリティ研修サービス ・標的型メール訓練サービス	【有償サービス】 ・社内部署へ周知のためセミナーを実施可能 (要望により内容のカスタマイズ可能)	有償サービス：セキュリティ研修	有償サービス：セキュリティ研修	有償サービス：セキュリティ研修				
		29	Lv1	**インターネットへの接続に関する社内への教育を行っている**	【規則】 ・Web閲覧によるマルウェア感染の予防について、教育資料配布・掲示、eラーニング、集合教育等による教育を実施すること ・教育内容を振返り、次回の教育内容を改善すること 【対象】 ・役員、従業員、社外要員（派遣社員等）における インターネット利用者 【頻度】 ・新規受け入れ時、かつ、１回／年以上	【教育の例】 ・新入社員教育・中途入社教育・社外要員受け入れ集合教育等 ・eラーニングによる教育 ・自社、IPAやセキュリティベンダー等の提供する映像教育コンテンツの視聴 ・自社、IPAやセキュリティベンダー等の提供する教育資料の配布・掲示 【教育頻度の例】 ・新入社員・中途社員・社外要員受け入れ時 ・1回／年 eラーニング による教育を実施 ・1回／年 更新内容を中心とした教育資料・マニュアル等の再確認の通知	教育・啓発	情報セキュリティ／IT	・Secポリシー策定サービス セキュリティハンドブックを使用した教育実施 ・情報セキュリティ対策セミナー 学び維新(eラーニング) Forms(eラーニング) ・セキュリティ研修サービス	【有償サービス】 ・社内部署へ周知のためセミナーを実施可能 (要望により内容のカスタマイズ可能)	有償サービス：セキュリティ研修	有償サービス：セキュリティ研修	有償サービス：セキュリティ研修				
		30	Lv1	**機密区分に応じた情報の取り扱いに関する教育を行っている**	【規則】 ・機密区分の定義と取り扱いについて、教育資料配布・掲示、 eラーニング、集合教育等による教育を実施すること ・教育内容を振返り、次回の教育内容を改善すること 【対象】 ・役員、従業員、社外要員（派遣社員等） 【頻度】 ・新規受け入れ時、かつ、１回／年以上	【教育の例】 ・新入社員教育・中途入社教育・社外要員受け入れ集合教育等 ・eラーニングによる教育 ・自社、IPAやセキュリティベンダー等の提供する映像教育コンテンツの視聴 ・自社、IPAやセキュリティベンダー等の提供する教育資料の配布・掲示 【教育頻度の例】 ・新入社員・中途社員・社外要員受け入れ時 ・1回／年 eラーニング による教育を実施 ・1回／年 更新内容を中心とした教育資料・マニュアル等の再確認の通知	教育・啓発	情報セキュリティ	・Secポリシー策定サービス セキュリティハンドブックを使用した教育実施 ・情報セキュリティ対策セミナー 学び維新(eラーニング) Forms(eラーニング) ・セキュリティ研修サービス	【有償サービス】 ・社内部署へ周知のためセミナーを実施可能 (要望により内容のカスタマイズ可能)	有償サービス：セキュリティ研修	有償サービス：セキュリティ研修	有償サービス：セキュリティ研修				
		31	Lv2	**標的型メール訓練を実施している**	【規則】 ・標的型メール訓練を実施すること ・万が一開封した時の対応も訓練内容に含めること ・訓練内容や方法を振返り、次回の訓練を改善すること 【対象】 ・電子メールの利用者 【頻度】 ・1回以上／年	【訓練の内容】 ・標的型メールやビジネスメール詐欺(BEC)想定のメールを訓練対象に送る ・経営者向け不審メール訓練を実施している 【訓練項目】 ・メールの開封 ・メール内リンクへのクリック ・リンク先サイトへの情報入力 ・添付ファイルの開封有無 ・社内ヘルプデスクオペレーターのエスカレーション 【訓練後のフォロー】 ・結果および振返りはトップ報告し、次年度の訓練に改善点を反映している ・実施結果の考察を行い、結果を社内掲示板の掲載している	教育・啓発	IT	標的型メール訓練サービス	【他社製品】 ・アクモス社製 SYMPROBUS Targeted Mail Training/SYMPROBUS CoTra Enterprise(標的型攻撃メール対応 訓練ソリューション)の販売が可能	–	–	–				
		32	Lv2	**各部署の情報セキュリティ管理者に対して、組織内での対策とマネジメント手法に関する教育を実施している**	【規則】 ・組織内での対策とマネジメント手法に関する教育を実施すること ・教育内容を振返り、次回の教育内容を改善すること 【対象】 ・各部署の情報セキュリティ管理者または推進者 ※情報セキュリティ管理者が任命されてない場合は部門長 【頻度】 ・1回以上／年	【規則制定の例】 ・規則に定期的な教育の実施について規定している 【教育内容】 ・責任者または推進者の役割と権限 例：日常指導・啓発におけるポイント、 各種申請の許可・承認時の注意点 【実施方法の例】 ・実地点検に併せ、部署機密管理担当者(管理者)向け教育を実施している ・管理者研修(新任時、年次)の一環として実施している ・各部署の情報セキュリティ推進者に対する連絡会を開催している	教育・啓発	情報セキュリティ／IT	Secポリシー策定サービス	–						CPS.AT-1 CPS.AT-1 CPS.GV-4
		33	Lv2	**経営層が情報セキュリティに関する役割と責任を理解するための機会を設けている**	【規則】 ・経営層が役割と責任を理解するための説明の場を設けている ・説明内容を振返り、次回の説明内容を改善すること 【対象】 ・経営層や役員 【頻度】 ・1回以上／年	【規則】 ・規則に経営層の役割・責任及び経営層への報告について規定している 【教育内容】 ・役割と責任 例：方針決定や管理者への実行指示、事故発生時の対外説明の方法 ・世間動向 例：最新の攻撃手法、他社の重大なセキュリティ事故事例 【実施方法】 ・情報セキュリティ委員会での報告内容を、上部の内部統制委員会にて経営層へ報告している ・役員研修会にて、社外講師等による情報セキュリティの講演を実施し理解を深める機会を設けている	教育・啓発	情報セキュリティ	《管理者向け》 ・Secポリシー策定サービス セキュリティハンドブックを使用した教育実施 ・情報セキュリティ対策セミナー 学び維新(eラーニング) Forms(eラーニング) ・セキュリティ研修サービス	–						

分類	ラベル	No.	レベル	達成条件	達成基準	他社事例 （参考事例を列記しており、 すべての遵守を求めているものではありません）	対象	担当領域 （回答者検討時の参考情報）	池田事務器&KISPA 提供サービス	Ｓｋｙ株式会社にて追記 対応内容 ※左記に対し、支援可能な項目のみ記載	SKYSEA Client View Light Edition 対応可否	S1 / S3 Cloud Edition 対応可否	M1 Cloud Edition 対応可否	対応状況 0：未実施	1：対応中	2：対応完了	経産省CPSF 要求事項に関する 対策要件ID
		34	Lv2	**全社で啓発活動を実施している**	【規則】 ・全社で情報セキュリティの重要性を再認識する機会を設けること 【対象】 ・役員、従業員、社外要員（派遣社員等） 【頻度】 ・1回以上／年	【実施事例】 ・年1回 強化月間を設け以下を実施している -各部の機密管理帳票の更新や自主点検 -ポスター、標識の掲示 -eラーニングによる教育 -ログインメッセージによる注意喚起 ・朝礼で情報セキュリティの社内ルールをリマインドしている ・教育後、理解度テストを実施し、合格点に達するまでフォローしている ・全社員向けにサイバーセキュリティニュースレターを発行している ・専門委員会におけるセキュリティ最新動向などを社内周知している ・過去事例の情報共有している ・機密管理ニュース配信やポータルサイトに教育コンテンツを掲示～受講促進し啓蒙活動を実施している	教育・啓発	情報セキュリティ	・Secポリシー策定サービス セキュリティハンドブックを使用した教育実施 ・情報セキュリティ対策セミナー 学び維新(eラーニング) Forms(eラーニング) ・セキュリティ研修サービス ・NI Collabo 360/Microsoft 365（情報共有）	【SKYSEA Client View Light Edition】 ・メッセージ配信機能にて、注意喚起メッセージ配信を各端末に配信可能	○	○	×				
		35	Lv2	**各職場で特に重要なリスクやルールについて啓発活動を実施している**	【規則】 ・各社が定める活動単位（部・室など）で特に重要なルールやリスクについて リマインドすること ・啓発内容を振返り、次回の啓発内容を改善すること 【対象】 ・職場特有のリスクの理解、ルールの遵守が重要な従業員、社外要員（派遣社員等） 【頻度】 ・1回以上／1年	【啓発内容】 ・ヒヤリ、事故事例 ・各職場独自の情報セキュリティリスクの注意喚起 ・職場で特に重要な規定・ルールのリマインド 【啓発手段】 ・グループ会社を含めたIT部門社員向けに、年2回のサイバーセキュリティセミナーを開催している ・グループ会社を含めたCSIRT担当者で情報交換会を年に2回実施している	教育・啓発	情報セキュリティ	・Secポリシー策定サービス セキュリティハンドブックを使用した教育実施 ・情報セキュリティ対策セミナー ・学び維新、Formsなど(eラーニング) ・セキュリティ研修サービス ・NI Collabo 360/Microsoft 365（情報共有）	【有償サービス】 ・社内部署へ周知のためセミナーを実施可能 (要望により内容のカスタマイズ可能)	有償サービス：セキュリティ研修	有償サービス：セキュリティ研修	有償サービス：セキュリティ研修				
		36	Lv2	**教育、啓発の実施状況を数値等で具体的に把握している**	【規則】 ・教育・啓発の受講状況、理解度を数値等で具体的に把握すること 【対象の教育、啓発】 ・各社で判断した重要な教育、啓発 【頻度】 ・1回以上/年	【把握する内容】 ・教育、啓発の受講率を確認している ・年１回のeラーニングを実施した際の部署ごとの受講率、正解率 ・理解度テストを実施し、合格点に達するまでフォローする ・メール訓練結果、セミナー、各種情報セキュリティ施策実施状況を情報セキュリティ委員会で報告し、経営レベルで把握している	教育・啓発	法務／ 情報セキュリティ	・Secポリシー策定サービス セキュリティハンドブックを使用した教育実施 ・情報セキュリティ対策セミナー 学び維新(eラーニング) Forms(eラーニング) ・セキュリティ研修サービス ・標的型メール訓練サービス	【有償サービス】 ・セキュリティ研修 eラーニングメニューで理解度チェックが可能 (内容別途相談)	有償サービス：セキュリティ研修	有償サービス：セキュリティ研修	有償サービス：セキュリティ研修				
		38	Lv1	**情報セキュリティ事件・事故発生時の対応について教育・訓練を実施している**	【規則】 ・情報セキュリティ事件・事故発生時の対応について、教育資料配布・掲示、eラーニング、集合教育等による教育や訓練を実施すること 【対象】 ・役員、従業員、社外要員（派遣社員等） 【頻度】 ・新規受け入れ時、かつ、１回／年以上	【教育・訓練の例】 ・新入社員教育・中途入社教育・社外要員受け入れ教育等で下記教育を実施している ・eラーニングによる教育 ・映像教育コンテンツの視聴 ・教育資料の配布・掲示 ・マニュアル等による機密区分の定義と取り扱いについて解説 ・想定される事故シナリオに沿った対応訓練（机上含む）を実施 【頻度の例】 ・新入社員・中途社員・社外要員受け入れ時 ・1回／年 eラーニング による教育を実施 ・1回／年 更新内容を中心とした教育資料・マニュアル等の再確認の通知	事件・事故対応	情報セキュリティ	・Secポリシー策定サービス セキュリティハンドブックを使用した教育実施 ・情報セキュリティ対策セミナー ・学び維新、Formsなど(eラーニング) ・セキュリティ研修サービス ・NI Collabo 360/Microsoft 365（情報共有）	【有償サービス】 ・社内部署へ周知のためセミナーを実施可能 (要望により内容のカスタマイズ可能)	有償サービス：セキュリティ研修	有償サービス：セキュリティ研修	有償サービス：セキュリティ研修				CPS.AT-1 CPS.AT-2 CPS.AT-3 CPS.SC-9 CPS.IP-7 CPS.CO-1
		40	Lv1	**教育・訓練の内容を必要に応じて見直ししている**	【頻度】 ・教育・訓練実施前後、もしくは１回／年以上	【頻度の例】 ・1回/年、社内規程や情報セキュリティのガイドラインのレビューを行い、必要に応じて教育・訓練内容の見直しをしている ・毎年、教育・啓発を実施する前後に、内容の見直しを実施している	事件・事故対応	情報セキュリティ	Secポリシー策定サービス	–							
		44	Lv1	**他社との間で、機密情報の取り扱い方法が明確になっている**	【規則】 ・業務開始前に機密情報の取り扱いについての取り交わしを行うこと 【対象】 ・機密情報を共有する会社	【取り交わしの例】 ・機密情報を取り扱う場合は、機密保持契約を締結している ・責任者の明確化、人的管理（守秘義務）、物理的管理措置、技術的対策、再委託の取り扱い、取引終了時の取り扱い等を含む取り交わしを行っている	パートナー企業のリスク管理	法務	Secポリシー策定サービス	–							CPS.AM-7 CPS.BE-1 CPS.BE-2 CPS.GV-1 CPS.SC-1 CPS.SC-2 CPS.SC-3 CPS.SC-8 CPS.SC-10 CPS.SC-11 CPS.AC-1 CPS.AE-1
		46	Lv1	**情報セキュリティ事件・事故時の他社との役割と責任が明確になっている**	【規則】 機密情報を共有する際、取り扱いとともに、情報セキュリティ事件・事故発生時の、会社ごとの役割と責任を文書化しておくこと	【会社ごとの役割と責任の例】 ・取引契約の中に、事故発生時の委託元への報告、事故対応への協力責任等に関する内容を含めている ・事故発生時の連絡窓口を取り交わしている	パートナー企業のリスク管理	購買・調達	Secポリシー策定サービス	–							
	9アクセス権	49	Lv1	**人の異動に伴うアクセス権(入室権限やシステムのアクセス権)の管理ルールを定めている**	【規則】 ・以下の内容等を含む管理ルールを定めること ・アクセス権の発行・変更・削除は申請・承認制であること ・与える入室許可・アクセス権の範囲は必要な範囲に限定すること ・入室権限やアクセス権の棚卸について定めていること ・与えた入室許可・アクセス権の申請書または台帳を管理していること 【対象】 ・業務で利用するシステムおよびPCログオン時のユーザーID	【管理ルールの例】 ・人事異動の際の事務手続きに、アクセス権の付与・変更・削除の手続きを記載している ・管理ルールに紙面の機密文書の保管場所を定め、施錠することを定めている ・1回／年の棚卸の実施及びその手順を定めている	認証とアクセス権	IT	・Secポリシー策定サービス ・NI Collabo 360(承認フロー) ・LanScope EndPointManage ・SKYSEA Client View	【SKYSEA Client View Light Edition】 ・監査機能はありませんが、利用されているアカウントを記録することが可能	○	○	×				CPS.IP-9
		50	Lv2		【規則】 ・重要情報を扱うシステムは、アクセス権を付与するための条件を 明確にする ・アクセス権の設定は、システム管理者の要件および設定手順を 明確にし、厳格な管理下で実施する。 ・重要情報を扱うシステムは、情報利用者とシステム管理者の権限を 分離するなど、個人に権限が集中しない環境とする。 ・重要情報を扱うシステムは、その運用／利用状況を監視する。	【管理ルールの例】 ・重要情報を扱うシステムへのアクセス権は、一定の基準を満たす社員にのみ付与している ・重要な権限変更は、単一の行為者では実施できない仕組みとなっている （申請者・承認者・作業者を分掌） ・開発部門による重要な情報へのアクセスログは運用部門が監視している ・運用部門による重要な情報へのアクセスは、セキュリティ専任者が監視している ・セキュリティ専任者は、重要な情報へ直接アクセスができない仕組み(開発部門権限)としている	認証とアクセス権	IT	Secポリシー策定サービス ・LanScope EndPointManage ・SKYSEA Client View	【SKYSEA Client View Light Edition】 ・監査機能はありませんが、利用されているアカウントを記録することが可能	○	○	×				
		51	Lv1	**管理ルールに沿ってアクセス権の発行、変更、無効化、削除を実施している**	【規則】 ・No49に定義した管理ルールの順守状況の点検を行っていること	【点検の例】 ・管理ルールの遵守状況を確認するチェックリストを作成し、1回／年チェックリストにより点検し、不備・違反があれば是正を行っている ・申請、承認、設定の記録を確認し、管理ルールに従い行われていることを点検している ・定期人事異動の際、権限設定を確認・修正している	認証とアクセス権	IT	Secポリシー策定サービス ・LanScope EndPointManage ・SKYSEA Client View	–							
		52	Lv1	**アクセス権の棚卸を定期的、または必要に応じて実施している**	【規則】 ・No49により定めたルールに従い、アクセス権の棚卸を定期的、または必要に応じて実施していること	【棚卸の例】 ・1回／年 入室権限やシステム上のアクセス権設定を点検し、権限設定の不備を修正している	認証とアクセス権	IT	Secポリシー策定サービス ・LanScope EndPointManage ・SKYSEA Client View	【SKYSEA Client View Light Edition】 ・棚卸機能はありませんが、利用されているアカウントを記録することが可能	○	○	×				
		53	Lv2	**アクセスログは、安全に保管しアクセス制御された状態で管理されている**	【規則】 ・法規制等により要求される事項を満たす事ができるよう、適切な期間のログを保持する。 ・ログを脅威から保護するため、ログを保存するサーバ、システムにアクセス制御等を適用すること	【取得対象の例】 ・ログ保管対象は情報入手・加工・発信の各システムとしている 【安全な保管の例】 ・アクセスログは自社内には保管せず、機密保持契約、外部サービスセキュリティ要件に合致したサービスを利用している 【アクセス制御の例】 ・重要なログはサイバー攻撃の脅威から保護するため、ログの消去や改ざんが出来ないように制御している 【法規制等への対応の例】 ・重要なログはサイバー攻撃の脅威から保護するため、ログの消去や改ざんが出来ないように制御している ・監査機関や法執行機関等からの要求に応じてログを提供可能な状態で保管している	認証とアクセス権	IT	・LanScope EndPointManage ・SKYSEA Client View（アクセスログ等） ・FortiGateなどUTM（ログ管理） ・NI Collabo 360(承認フロー)	【SKYSEA Client View Light Edition】 ・操作ログは最大10年間保存可能 ・操作ログを別途バックアップすることで、自社以外の環境へ配置することが可能	○	○ ※保存期間は3か月	○ ※保存期間は1年				
	10情報資産の管理(情報)	54	Lv1	**機密区分に応じた情報の管理ルールを定めている**	【規則】 ・以下の内容等を含む管理ルールを定めること ・機密の特定 ・機密区分のレベル判定と表示 ・区分に応じた取り扱い方法 ・取り扱いエリアの区分及び制限 【対象】 ・情報資産（情報）	【管理ルールの例】 ・管理対象は、電子と紙の両方とする ・機密文書に機密であることを明示するスタンプを押す ・文書のリスクアセスメントの実施 ・文書台帳の整備 ・規程で、次の項目につき明文化している ・管理すべき守秘情報、機密情報、情報区分、守秘情報の種類、守秘情報の取扱い、機密情報を取り扱う部署の管理責任 ・機密管理区分を定め、様式にて一覧化するルールを定めている ・規程に機密区分に応じた情報の管理ルールを明記	機密管理	情報セキュリティ	・Secポリシー策定サービス ・文書管理システム	–							CPS.GV-3
		55	Lv2	**機密区分に応じた情報の管理ルールを 定期的、または必要に応じて見直ししている**	【規則】 ・管理ルールの内容を確認し、必要に応じて改善すること 【頻度】 ・1回以上 ／年	【見直しの例】 ・年一回規則の内容を確認し、必要に応じて改訂している。	機密管理	情報セキュリティ	Secポリシー策定サービス	–							
		56	Lv1	**高い機密区分の情報資産(情報)を一覧化している**	【規則】 ・ 一覧には、対象情報、管理者名、部署名、保管場所、保管期限、開示先、連絡先などを含むこと 【対象情報】 ・ No.54で定めた機密区分のうち、高レベルの機密に該当する情報資産	【一覧化の実施例】 ・情報の主管部門毎に高い機密区分の情報資産の一覧表を作成している ・情報資産の一覧を部署毎に作成させて、1回/年 見直している ・専用様式にて一覧化している	情報セキュリティ対策フレームワークの構築	情報セキュリティ	Secポリシー策定サービス	【他社製品】 ・三菱電機ソフトウェア社製　すみずみ君で端末上に保存されている個人情報ファイルを発見することが可能	–	×	×				
		57	Lv2	**高い機密区分の情報資産(情報)の一覧化を 定期的、または必要に応じて見直ししている**	【規則】 ・一覧表の内容を確認し、必要に応じて是正すること 【頻度】 ・1回以上 ／年	【見直しの例】 ・年一回一覧の内容を確認し、必要に応じて改訂している。	情報セキュリティ対策フレームワークの構築	情報セキュリティ	Secポリシー策定サービス	–							
		58	Lv1	**情報資産(情報)は機密区分に応じた管理ルールに沿って管理している**	【規則】 ・ No.54に定義した管理ルールの順守状況の点検を行い、不備・違反があれば是正を行うこと 【頻度】 ・ 1回/年 以上	【点検の例】 ・管理ルールの遵守状況を確認するチェックリストを作成し行う	機密管理	情報セキュリティ	Secポリシー策定サービス	–							

分類	ラベル	No.	レベル	達成条件	達成基準	他社事例 (参考事例を列記しており、 すべての遵守を求めているものではありません)	対象	担当領域 (回答者検討時の参考情報)	池田事務器&KISPA 提供サービス	Ｓｋｙ株式会社にて追記 対応内容 ※左記に対し、支援可能な項目のみ記載	SKYSEA Client View Light Edition 対応可否	S1 / S3 Cloud Edition 対応可否	M1 Cloud Edition 対応可否	対応状況 0:未実施	1:対応中	2:対応完了	経産省CPSF 要求事項に関する 対策要件ID
	11情報資産の管理(機器)	59	Lv1	**重要度に応じた情報機器、OS、ソフトウェアの管理ルールを定めている**	【規則】 ・導入、設置、ネットワーク接続、セキュリティパッチ適用等のルールを含む管理ルールを定めていること	【セキュリティパッチ適用ルールの例】 ・端末管理ツールを利用して、脆弱性対応パッチを自動で適用している ・資産管理システムを活用し、脆弱性のある情報機器を定期的に特定している ・サーバーはパッチ公開後１月以内に適用する ・MS月例パッチは、テストで不具合がなければ、約1週間後に適用している 【ソフトウエアについてのルール例】 ・標準ソフトを決め、それ以外のソフトは許可制としている	機器全般	IT	・Secポリシー策定サービス ・LanScope EndPointManage ・SKYSEA Client View(端末管理)	【SKYSEA Client View Light Edition】 ・インストールされてるアプリケーションの一覧取得 ・脆弱性対応パッチの配信可能 ・ホワイトリスト/ブラックリストでのアプリケーション利用制限可能	○	○	○ ※ブラックリストのみ可能				CPS.AM-1 CPS.DS-13 CPS.CM-6
		60	Lv1	**情報機器、OS、ソフトウェアの情報(バージョン情報、管理者、管理部門、設置場所等)について、一覧を作成している**	【規則】 ・バージョン情報、管理者、管理部門、設置場所等の管理項目を含む情報機器、OS、ソフトウェアの一覧を作成すること	【管理項目の例】 ・機器管理番号、機器名、IPアドレス、設置場所、使用者、連絡先、ソフトウェアバージョン情報 -サーバー、NW機器、プリンタ、TV会議システム 管理番号、ハードウェア名、IPアドレス、ホスト名、設置場所、 管理者(部署名、氏名等) -会社支給のクライアントPCおよびスマートデバイス 管理番号、ハードウェア名、IPアドレス、ホスト名、利用開始日、 利用者(部署名、氏名等) -ソフトウェア 管理番号、ソフトウェア名、バーション、導入ホスト名、 連絡先(部署名、氏名等)	機器全般	IT	・LanScope EndPointManage ・SKYSEA Client View(IT資産管理)	【SKYSEA Client View Light Edition】 ・「管理項目の例」に列挙されている情報を組織単位で閲覧可能	○	○	○ ※ネットワーク機器情報は不可				
		61	Lv2	**情報機器、OS、ソフトウェアの情報(バージョン情報、管理者、 管理部門、設置場所等)の一覧を 定期的、または必要に応じて、見直ししている**	【頻度】 ・1回/年 以上	【見直しの例】 ・年一回一覧の内容を確認し、必要に応じて改訂している	機器全般	IT	・LanScope EndPointManage ・SKYSEA Client View(IT資産管理)	【SKYSEA Client View Light Edition】 ・資産管理機能にて詳細な利用バージョン等の情報を収集・閲覧可能	○	○	○				
		62	Lv1	**情報資産(機器)は重要度に応じた管理ルールに沿って管理している**	【規則】 ・ No59に定義した管理ルールに沿って管理を実施すること。不備・違反があれば是正を行うこと 【頻度】 ・ 1回/年 以上	【管理の例】 ・管理ルールに沿った管理状況の確認を1回／年で実施し、発見された不備の是正などを実施する ・毎週自動収集した情報を元にOSのパッチ適用状況、不適切ソフトの調査を行い是正を指導している。 ・毎週パッチの適用状況を確認し、漏れがあった場合には対応している。	機器全般	IT	・LanScope EndPointManager ・SKYSEA Client View モバイル機器管理機能 (MDM)	【SKYSEA Client View Light Edition】 ・Windows更新プログラムの適用状況把握が可能 ・不適切なソフトウェアのインストール状況を把握可能	○	○	○				
		64	Lv2	**スマートデバイスへのアプリケーションの無断インストールを制限し、定期的にインストール状況を確認している**	【規則】 ・インストール可能なアプリケーションを定義し、定期的にインストール状況を確認している。 【対象】 ・会社支給のスマートデバイス 【確認頻度】 ・1回/年	【制限すべきアプリの例】 -情報漏えいにつながるアプリ -深刻な脆弱性があるアプリ -マルウェア・スパイウェアの疑惑のあるアプリ 【無断インストールの制限】 ・端末管理ソフトにより、インストール可能アプリケーションを制御し、定期的に定義リストを確認している ・一般ユーザーには管理者権限を付与せず、インストールを制限している ・アプリケーションのインストールは申請制にしている ・ルールによりアプリケーションを管理部署に無断でインストールすることを禁止している	スマートデバイス	IT	・LanScope EndPointManager ・SKYSEA Client View モバイル機器管理機能 (MDM)	【SKYSEA Client View Light Edition】 ・OP：iOS端末に対して定義したアプリケーションの配布が可能。iOS端末にインストールされたアプリケーションの情報収集、ハードウェア情報を収集可能 ※Android OSも実装予定	OP：MDM Services	OP：MDM Services	OP：MDM Services				
		65	Lv2	**廃棄時(リース終了時含む)は、記憶媒体のデータを消去している**	【規則】 ・情報資産(機器)の廃棄時(リース終了時含む)はデータを復元できないよう消去すること ・情報資産(機器)の記憶領域の消去を実施した記録または業者の廃棄証明書を保管すること ※ディスクのフォーマットは、データを復旧される可能性があるため不可 ［対象］ -サーバー、会社支給のクライアントPC、スマートデバイス、外部記憶媒体	【消去の例】 ・物理的に破壊している ・専用消去ツールを利用している ・データ消去外部サービスを利用し、廃棄証明等による確認、あるいは、運用状況を監査している	機器全般	IT	・物理破壊、証明書発行	–							
12リスク対応		66	Lv1	**情報資産において 「機密性」「完全性」「可用性」の3要素が確保できなくなった場合のリスクを特定できている**	【規則】 ・ 対象の情報資産に情報セキュリティ事件・事故が発生した時の業務影響を影響範囲や発生頻度を踏まえ把握すること 【対象】 ・ №56で特定した情報資産 【観点】 -外部の脅威 -自社の脆弱性 ※必要に応じて、パートナー企業起因の脅威、脆弱性を考慮すること -情報資産の価値	【業務影響を把握する手法の例】 ・リスクアセスメントを行う 【頻度の例】 ・取り扱うシステム更新時 ・業務プロセスの変更時 ・体制の変更時	情報セキュリティ対策フレームワークの構築	情報セキュリティ／IT	Secポリシー策定サービス	–							CPS.RA-1 CPS.RA-4 CPS.RA-5 CPS.RA-6 CPS.RM-1
		68	Lv1	**必要に応じて経営層へ業務影響及び対策を報告し、セキュリティ業務に関与している社内部署と共有している**	【規則】 ・№66で把握した業務影響に対する対策方法及び計画を策定し、報告・共有すること ・ 報告に際し役員からの指示があった場合、これを関係部門へ共有すること 【対象】 ・ 情報セキュリティの総括責任者、関係部門 【頻度】 ・1回以上／年	【対策方法の例】 ・個人情報を漏えいした場合は、当局（個人情報保護委員会）への届け出が必要になることを経営陣や、個人情報を扱う人・部門へ共有する ・経営陣を含めたセキュリティ会議体を設け、計画報告・対応承認を得ている	情報セキュリティ対策フレームワークの構築	情報セキュリティ／IT	Secポリシー策定サービス	【他社製品】 ・三菱電機ソフトウェア社製　すみずみ君で端末上に保存されている個人情報ファイルを発見することが可能	–	×	×				
		69	Lv1	**業務影響への対策は策定された計画に沿って管理している**	【規則】 ・№68で作成された対策及び計画が適切に実施され、業務影響の低減がされていることを確認し、発見された不備の是正などを 実施すること 【対象】 ・ 情報資産の業務影響 【頻度】 ・ 1回／年 以上	【確認の例】 ・個人情報の漏えい発生の際の対応履歴を調査し、当局への 届出、関連役員への報告が事前に定めた対策方法に沿って行われていたかを検証する ・情報セキュリティ事件・事故の管理表を作成し、計画実施状況や結果を定期的にチェックしている	情報セキュリティ対策フレームワークの構築	情報セキュリティ／IT	Secポリシー策定サービス	–							
13取引内容・手段の把握		70	Lv1	**会社毎に取り交わす情報・手段(受発注の手段等、情報のやり取り)を一覧化している**	【規則】 ・ 一覧表には取引に伴い授受／使用される情報資産とその取り扱いを記載し、取引先と相互に把握すること 【対象】 ・ 重要な情報資産（№54で定められた機密レベルが高い情報資産など）を共有する取引先 【頻度】 ・ 取引開始時／取り交わす情報・手段の変更時	【一覧化の例】 ・取引先毎に、取り交わす情報と利用する手段を記載する 【取り扱いの例】 ・重要な情報を取り交わす取引先とは、契約に機密情報の取り扱いのルールを定める ・取引先へ機密情報を渡す際、それがパワーポイントやエクセル等であれば、ファイルにパスワードを設定する	パートナー企業のリスク管理	IT	・Secポリシー策定サービス ・Canonクラウドストレージサービス Home type-S2 (クラウド活用)	–						CPS.BE-3
14外部への接続状況の把握		74	Lv2	**ネットワーク図・データフロー図を作成し、 関係組織（サプライヤー等含む）との通信を監視している**	【基準】 ・ネットワーク図を作成すること ［対象範囲］ -自社の情報機器が存在するネットワーク ［見直し頻度］ -1回/年以上 <追記> 【基準】 ・データフロー図を作成すること ［対象範囲］ -関係組織間のネットワークでやり取りされる自社内のデータ	【ネットワーク図の例】 ・グループ間ネットワーク図 ・拠点間ネットワーク図 ・事務所内ネットワーク構成図 【データフロー図の記載内容例】 ・関係組織間ネットワークを使用するシステム ・送受するデータの種類、方向等 【通信の監視の例】 ・関係組織間の不審なアクセスを統合脅威管理（UTM）等で監視 ・通信量状況の監視（稼働監視、性能監視） ・インターネットを通じた関係組織間の通信はIDS等で監視	社内ネットワーク	IT	ネットワーク調査	–						CPS.AM-4 CPS.AM-5 CPS.CM-5
		75	Lv2	**ネットワーク図・データフロー図は、定期的、 または必要に応じて、見直ししている**	【頻度】 ・1回/年以上	【見直しの例】 ・年一回内容を確認し、必要に応じて改訂している	社内ネットワーク	IT	ネットワーク調査	–							
		76	Lv1	**自組織の資産が接続している外部情報システムの利用ルールを定めている**	【規則】 ・以下の内容を含む利用ルールを定めること ・外部情報システムの接続先と守秘義務契約を締結する ・外部の情報サービスを利用する際のセキュリティ要件を定めている ・外部の情報サービスの利用時にセキュリティ要件を満たしているかサービス内容を確認し、承認した証跡を保管している	【利用ルールの例】 ・会計情報などの自社の機密情報を扱う外部サービスを利用する際は、利用前にそのサービスの情報セキュリティ仕様を確認する ・パートナー企業とは取引開始前の段階で、必ず守秘義務項目を含む取引基本契約書を締結する社内ルールで運用している ・全社標準「情報システム管理規定」に基づき、委託先の選定・契約を管理している(規定項目:守秘義務契約、情報セキュリティ要件、SLA、BCP対応) ・クラウドサービス利用に関する社内ルールの中で制約事項や利用開始までの一連の手続きを明文化している ・クライドサービスを利用する場合は、申請制にしている	サーバー	情報セキュリティ／IT	・Secポリシー策定サービス ・NI Collabo 360(承認フロー)	–						
		77	Lv1	**利用している外部情報システムを一覧化している**	【規則】 ・外部情報システムの一覧を作成していること	【一覧の項目の例】 ・契約署名、契約相手先、契約日、契約満了日、管理部署を管理項目として一覧化している 【作成の例】 ・表計算シートで台帳化してデータで保管している ・外部システムの利用申請システムで利用システムの一覧を保管している ・利用しているクラウドサービス・EDIを一覧化している	サーバー	IT	・Secポリシー策定サービス ・SKYSEA Client View（情報資産管理）	–						

分類	ラベル	No.	レベル	達成条件	達成基準	他社事例 (参考事例を列記しており、 すべての遵守を求めているものではありません)	対象	担当領域 (回答者検討時の参考情報)	池田事務器＆KISPA 提供サービス	Ｓｋｙ株式会社にて追記 対応内容 ※左記に対し、支援可能な項目のみ記載	SKYSEA Client View Light Edition 対応可否	S1 / S3 Cloud Edition 対応可否	M1 Cloud Edition 対応可否	対応状況 0:未実施	1:対応中	2:対応完了	経産省CPSF 要求事項に関する 対策要件ID
		78	Lv1	**外部情報システムの一覧を定期的、または必要に応じて見直ししている**	【規則】 ・定期的に棚卸を実施するとともに、新規あるいは利用中止するものを一覧に反映すること 【頻度】 ・1回／年以上、かつ、新規開始あるいは利用中止時	【棚卸実施の方法例】 ・社内ルールで利用開始時の報告を義務付けている ・一覧に記載されている外部システムの管理者に、利用状況を1年に1度確認している ・インターネット通信ログを確認して、申請されていない外部情報システムが利用されていないか確認している ・外部システムの利用申請システムに登録された情報に基づき棚卸をしている	サーバー	IT	・Secポリシー策定サービス ・SKYSEA Client View（情報資産管理）	–						
	15社内接続ルール	79	Lv1	**業務で利用する情報機器の自社ネットワークへの接続ルールを定めている**	PCやサーバーなどの機器の接続ルール 【規則】 ・社内ネットワークへの接続に関するルールを定めること 【対象】 ・社内でネットワークに直接接続するすべての機器 ・会社標準機器、社外からの持ち込み機器含む 社外から社内ネットワークへ接続するための追加ルール	【PCやサーバーなどの機器の接続ルールの例】 ・社内ネットワークへの接続は申請・承認制にすることとしている ・接続するPC、サーバーにマルウェア感染防止対策を実施することしている ・申請内容に変更があった場合は、許可を得ること再申請が必要としている ・社内ネットワークに接続できるのは、社有機器かつ定められたセキュリティ対策を満たす情報機器とするしている ・私有デバイスの接続は禁止している許可していない ・接続機器のを台帳管理している ・通信手段は会社提供のみとしている（Wi-Fiルータ持ち込み、デザリング不可） ・外来者が持込みした機器はを自社社内ネットワークに接続することは禁止。とするが、保全業務等でやむを得ず社内ネットワークに接続する場合は、セキュリティ条件を全て実施することに切替えることとするしている	社内ネットワーク	IT	・Secポリシー策定サービス ・SKYSEA Client View(禁止アプリ、無許可機器接続監視）	【SKYSEA Client View Light Edition】 ・必須アプリケーションの未インストールを検知可能 ・不正・無許可機器のネットワークへの接続を検知することが可能 ・OP：指定したネットワーク以外には接続させないことが可能	○ OP：ITセキュリティ対策強化	○ OP：S1×　※S3のみ搭載（遮断機能が不可）	×				CPS.AC-1 CPS.AC-4 CPS.AC-3
		82	Lv2	**リモートワークで使用する情報機器や機密情報の条件についてのルールを定め、運用している**	【規則】 ・リモートワークで使用する情報機器や機密情報の条件についてのルールを定め、周知すること ・ルールの遵守状況を確認し、必要に応じて是正すること ［周知対象］ -リモートワークを行う全ての従業員、派遣社員、受入出向者 ［周知のタイミング］ -リモートワークの開始前 ［ルールの内容］ -リモートワークで使用許可する情報機器 ※必要に応じて申請、承認の方法を含む 個人所有端末にダウンロード可能なファイル	【ルールの例】 ・リモートワークで使用する情報機器（私有デバイス）について、セキュリティ対策状況や機密保持の誓約の確認を含めて、申請・承認制とし、必要に応じて是正している ・機密情報のダウンロード、印刷等は禁止としている（周知徹底もしくは仕組みで禁止） ・リモートワーク時の注意点について周知徹底、eラーニング等での啓発を実施している ・リモートワークは社有機器のみとしている（私有デバイスは禁止） 【見直しの例】 ・年一回ルールの内容を確認し、必要に応じて改訂している。	リモートワーク時の注意喚起	情報セキュリティ／IT	・Secポリシー策定サービス ・NI Collabo 360(承認フロー) ・LanScope EndPointManager ・SKYSEA Client View	【SKYSEA Client View Light Edition】 ・ユーザ操作によるファイル操作(外部記憶媒体への操作含む)ログ、アプリケーションログ、印刷ログ、Webアクセスログの収集が可能 ・リモートワーク時に印刷、記憶媒体利用を禁止させることが可能 ・OP：指定したネットワーク以外には接続させないことが可能	○ OP：ITセキュリティ対策強化	○ OP：S1×　※S3のみ搭載	○ OP：×				
		83	Lv2	**リモートワーク遂行上のルールを定め、運用している**	【規則】 ・リモートワーク遂行上のルールを定め、周知すること ・ルールの内容や遵守状況を確認し、必要に応じて是正すること ［周知対象］ -リモートワークを行う全ての従業員、派遣社員、受入出向者 ［周知のタイミング］ -リモートワークの開始前 ［ルールの内容や遵守状況の確認、是正頻度］ -1回以上/年	【ルールの例】 ・関係者以外に 業務情報を話したりパソコン画面や資料を見せたりしないこと ・のぞき見や音漏れが起こらない環境を確保すること ・会社ルールに従い撮影、録音を行うこと ・ID/ パスワードを人目に付かないように管理すること ・重要な会議では主催者が参加者を確認すること ・リモートワークで使用する情報機器を安全な場所に保管することとしている ・離席時には、スクリーンロックまたはシャットダウンを行うこととしている ・移動時には常に携帯することとしている ・リモートワーク遂行上のルールを周知し、必要に応じて是正している 【見直しの例】	リモートワーク時の注意喚起	情報セキュリティ／IT	・Secポリシー策定サービス ・文書管理システム ・LanScope EndPointManager ・SKYSEA Client View	【SKYSEA Client View Light Edition】 ・ユーザ操作によるファイル操作(外部記憶媒体への操作含む)ログ、アプリケーション実行ログ、印刷ログ、WEBアクセスログの収集が可能 ・リモートワーク時に印刷、記憶媒体利用を禁止させることが可能 ・OP：指定したネットワーク以外には接続させないことが可能	○ OP：ITセキュリティ対策強化	○ OP：S1×　※S3のみ搭載	○ OP：×				
攻撃を防ぐ対策実施（防御）	16物理セキュリティ	84	Lv1	**サーバー等の設置エリアは、入場可能な人を定めている**	【規則】 ・サーバー等の設置するエリアに入場可能な人を定めること	【入場可能な人の例】 ・事前に管理者の承認を得た従業員を入場可能としている ・社内のシステム運用・保守責任者・担当者、メンテナンス業者を入場可能としている ・入退場時に台帳で立ち入り記録をつけ、都度社内責任者の承認を取得するとともに、入場可能な社内担当者の立ち合いを必須としている	サーバー	IT	入退室管理システム	–						CPS.AC-2 CPS.IP-5
		85	Lv1	**サーバー等の設置エリアは、施錠等で入場を制限している**	【規則】 ・サーバー等の設置エリアを施錠すること ・施錠が出来ないエリアにサーバーが設置されている場合、サーバーを専用ラックに入れて施錠すること ・管理者を定めて、施錠管理を行うこと	【施錠の実施例】 ・物理鍵で施錠し、管理者が都度開錠を行っている ・セキュリティカードで施錠し、管理者が権限管理を行っている ・パスワードで施錠し、管理者が都度開錠を行っている ・生体情報で施錠し、入場者の生体情報で開錠を行っている ・施錠が出来ないエリアにサーバーが設置されている場合、サーバーを専用ラックに入れて施錠している	サーバー	IT	入退室管理システム	–						
		86	Lv2	**サーバー等の設置エリアに入場した記録を保管し、定期的にチェックしている**	【規則】 ・サーバー等の設置エリアの入退場記録を取得し、保管すること 【記録する項目】 -入退場日時 -入場者(氏名、所属、連絡先など) -入場目的 -承認者 【保管期間】 ・6ヶ月	【入退場記録の例】 ・台帳に入退場の都度記載し、保管している ・システムで入退場記録を自動取得している	サーバー	IT	入退室管理システム	–						
		87	Lv2	**サーバー等の設置エリアに不正侵入や不審行動を監視している**	【規則】 ・入場時、退場時に持込み・持ち出し物を確認すること ・入場者の行動を監視すること	【監視の例】 ・持ち込み物、持ち出し物を台帳に記載している ・入場時、自身の荷物はロッカーに入れ、透明のバックを利用している ・入場認証エラーが続いた際に管理者へ通知される様にしている ・事前入場許可者の立ち合いを必須としている ・監視カメラを設置している	サーバー	IT	・監視カメラ ・セキュリティロッカーなど什器	–						
		88	Lv2	**入退場に関するルールを定め、周知、運用している**	【規則】 ・自社の入退場ルールを定めること ・入退場ルールを周知すること ・入退場ルールの内容や遵守状況を確認し、必要に応じて改定や再周知を行うこと ［周知対象］ ・自社に出入りする全ての人員 【入退場ルールの内容】 ・入場制限エリアの定義 ・入退場時の申請、承認 ・入退場時の身分証明方法(社員証、入場許可証の着用など) ・入場許可証、通門証の発行規則 【入退場ルールの内容や遵守状況の確認、是	【ルールの例】 ・執務室、会議室、機密情報設置場所を入場制限エリアとしている ・許可されたエリア以外への立ち入り時は申請を行うこととしている ・社員証、入場許可証を見える場所に着用することとしている ・外来者の入場時には受付で記名の上、入場許可証を貸与することとしている ・入退場ルールを社内に周知し、必要に応じて改訂や再周知している	入退場管理	情報セキュリティ／総務	・入退室管理システム ・サーバールームやパーティション設置など什器案件 ・サーバーラック導入	–						
		89	Lv2	**重要なエリア、部屋への入場を制限し、入退場記録を保管している**	【規則】 ・重要なエリア、部屋の入退場を制限すること ・重要なエリア、部屋への入退場記録を取得し、保管すること 【記録する項目】 ・入退場日時 ・入場者(氏名、所属、連絡先など) ・入場目的 ・承認者 【記録の保管期間】 ・6ケ月以上	【入場制限の例】 ・研究、設計エリア、経営陣エリアには、許可された従業員のみ入場可能としている 【入退場記録の例】 ・台帳に入退場の都度記載している ・システムで入退場記録を自動取得している	入退場管理	情報セキュリティ／総務	入退室管理システム	–						
		90	Lv2	**不正侵入や不審行動を監視している**	【規則】 ・自社の重要な場所において、不正侵入や不審行動を監視すること ・監視が正常に機能していることを確認し、必要に応じて是正すること 【監視状況の確認、是正頻度】 ・1回以上/6か月	【監視の例】 ・持ち込み物、持ち出し物を台帳に記載している ・入場認証エラーが続いた際に管理者へ通知される様にしている ・事前入場許可者の立ち合いを必須としている ・監視カメラを設置し、定期的に機能を確認している	入退場管理	情報セキュリティ／総務	監視カメラ	–						
		91	Lv2	**社内への持込みルールを明確にし、運用している**	【規則】 ・社内への持込みルールを定めること ・持込みルールの内容や遵守状況を確認し、必要に応じて是正すること 【対象者】 ・従業員、派遣社員、受入出向者および社外者 【対象の物品】 ・パソコン、タブレット、スマートフォン、カメラ、外部記憶媒体 ※上記の他に記録可能な物品があれば各社で判断すること 【持込みルールの内容】 ・持込み制限の対象とするエリア、物品	【ルールの例】 ・研究、設計エリアには、カメラ・外部記憶媒体・録音機器の持ち込みを禁止している ・禁止されている物品を持ち込む際には、申請書でエリア管理者の承認を得ている ・持ち込み物を管理台帳に記録し、6ヶ月保管している ・社内への持ち込みルールを周知し、定期的に見直しをしている	持込み・持出し制限	情報セキュリティ／総務	・Secポリシー策定サービス ・NI Collabo 360(承認フロー)	–						
		92	Lv2	**社外への持出しルールを明確にし、運用している**	【規則】 ・社外への持出しルールを定めること ・持出しルールの内容や遵守状況を確認し、必要に応じて是正すること 【対象】 ・従業員、派遣社員、受入出向者および社外者 【対象の物品】 ・パソコン、タブレット、スマートフォン、カメラ、外部記憶媒体、 印刷物(図面などの機密書類) ※上記の他に必要な物品を各社で判断すること 【持出しルールの内容】	【ルールの例】 ・社外持ち出し時には、所属長の承認を得ることとしている ・持ち出し物を管理台帳に記録し、6ヶ月保管している ・社内への持ち出しルールを周知し、定期的に見直しをしている	持込み・持出し制限	情報セキュリティ／総務	・Secポリシー策定サービス ・NI Collabo 360(承認フロー)	–						
		93	Lv2	**持込み・持出しルールに関する意識を高める対策を講じている**	【規則】 ・持込み・持出しルールに関する意識を高める対策を講じること 【実施頻度】 ・1回以上/6か月	【対策の例】 ・半年ごとにルールの教育を実施している ・半年ごとに持ち出し点検を実施している	持込み・持出し制限	情報セキュリティ／総務	・情報セキュリティ対策セミナー ・学び維新、Formsなど(eラーニング) ・NI Collabo 360/Microsoft 365（情報共有）	【SKYSEA Client View Light Edition】 ・メッセージ配信機能にて各端末へ情報周知が可能 【有償サービス】 ・社内部署へ周知のためセミナーを実施可能 (要望により内容のカスタマイズ可能)	○ 有償サービス：セキュリティ研修	○ セキュリティ研修	× 有償サービス：セキュリティ研修			
		94	Lv2	**社内における撮影ルールを定め、運用している**	【規則】 ・社内における撮影ルールを定めること ・撮影ルールの内容や遵守状況を確認し、必要に応じて是正すること 【撮影ルールの内容】 ・撮影を制限する対象またはエリア ・撮影の申請、承認手順 ・撮影申請、行為の記録の保管(保管期間:6か月) ※撮影を制限しないエリアを設けることも可能 (例：社外者との打合せエリア) 【撮影ルールの内容や遵守状況の確認、是正頻度】	【ルールの例】 ・研究、設計エリアを撮影制限エリアとしている ・撮影の際は、1週間前までに申請書でエリア管理者に申請し、承認を得ることとしている ・撮影の際は、エリア管理者立ち合いを必須としている ・撮影申請書は6ヶ月保管している	社内撮影制限	情報セキュリティ／総務	Secポリシー策定サービス	–						
		97	Lv2	**PCの標準構成・設定ルールを定め、標準構成・設定ルールに変更がある場合は承認を経て変更している**	【規則】 ・PCの標準構成(ソフトウェアとバージョン)と設定を定めること ・構成、設定の変更は承認制にすること ［対象］ -会社支給のPCのOS、オフィスソフト、ブラウザ、ウイルス対策ソフト	【ルールの例】 ・標準ソフトウエアを定め、運用している ・標準ソフトウェアの構成、設定変更を承認制としている	クライアントPC	IT	・情報セキュリティ対策セミナー ・NI Collabo 360/Microsoft 365（情報共有） ・LanScope EndPointManager ・SKYSEA Client View(情報資産管理)	【SKYSEA Client View Light Edition】 ・ホワイトリスト/ブラックリストでのアプリケーション利用制限可能	○	○	○　※ブラックリストのみ可能			

分類	ラベル	No.	レベル	達成条件	達成基準	他社事例 (参考事例を列記しており、 すべての遵守を求めているものではありません)	対象	担当領域 (回答者検討時の参考情報)	池田事務器&KISPA 提供サービス	Ｓｋｙ株式会社にて追記 対応内容 ※左記に対し、支援可能な項目のみ記載	SKYSEA Client View Light Edition 対応可否	S1 / S3 Cloud Edition 対応可否	M1 Cloud Edition 対応可否	対応状況 0:未実施	1:対応中	2:対応完了	経産省CPSF 要求事項に関する 対策要件ID
		98	Lv2	**PCで利用を許可または禁止するソフトウェアを定め、ソフトウェアの無断インストールを禁止し、違反がないか定期的に確認している**	【規則】 ・社内で利用許可または禁止するソフトウェアの一覧を作成し周知すること ・ソフトウェアの無断インストールを制限すること ・定期的にソフトウェアのインストール状況を確認すること ※システムでインストール制限している場合は確認不要 [対象] -会社支給のクライアントPC [制限すべきソフトウェアの例] -情報漏えいにつながるソフトウェア -深刻な脆弱性があるソフトウェア -マルウェア・スパイウェアの疑惑のあるマカ	【ルールの例】 ・禁止ソフトウエアの一覧を作成し、関係者で共有している ・禁止ソフトウエアは自動でソフトウエアの稼働抑止を実施している ・毎週インストール状況を調査している	クライアントPC	IT	・Secポリシー策定サービス ・LanScope EndPointManager ・SKYSEA Client View（情報資産管理）	【SKYSEA Client View Light Edition】 ・ホワイトリスト/ブラックリストでのアプリケーション利用制限可能 ・利用禁止アプリケーションのインストールを検知可能	○	○	○ ※ブラックリストのみ可能 ×	■			CPS.RA-1 CPS.IP-1 CPS.IP-2 CPS.PT-2
		99	Lv2	**PCからのデータ書き出しを仕組みで制限している**	【規則】 ・データ書き出しを制限する仕組みを導入すること [対象] -会社支給のクライアントPC	【ルールの例】 ・システム対策（Directoryサービス）により、USBの利用制限を実施している ・書き出し制限機能がるソフトを導入している ・物理的なポート閉鎖をしている	クライアントPC	IT	・LanScope EndPointManager ・SKYSEA Client View（デバイス制御）	【SKYSEA Client View Light Edition】 ・外部記憶媒体(USBデバイス)の使用条件を設定可能	○	○	○	■			
		100	Lv2	**マルウェアによる被害(データ暗号化等)を受けた場合に業務に支障をきたす重要データについては、PC以外へ保管するようルールを定め、周知している**	【規則】 ・重要データはクライアントPC以外に保管すること [周知対象] -役員、従業員、派遣社員、受入出向者	【ルールの例】 ・ソフトウエアによってはローカル保存が前提の場合も想定されるため、規則ではなく運用ルールとして周知している。 ・定期バックアップを実施しているサーバーに保存している ・外部記憶媒体に保存している	クライアントPC	IT	Barracuda（クラウド型バックアップ）	–				■			
		101	Lv2	**サーバーの不要な機能を無効化している デフォルトユーザーIDの利用の停止をしている デフォルトパスワードの変更をしている**	【規則】 ・不要サービス、デーモンを無効化すること ・デフォルトユーザーIDの利用を停止すること ・デフォルトパスワードの変更すること	【不要な機能停止運用の例】 ・初期導入時に不要なサービスを無効化している ・デフォルトパスワードは必ず変更している ・定期的(1回/年)にサービス・デーモンの仕様と設定が同一であるか確認している ・機能の追加・変更がある場合、サービス設定を確認している	サーバー	IT	・Secポリシー策定サービス ・サーバー構築委託	–				■			
		102	Lv2	**管理部署がスマートデバイスに対して、機密管理上必要な設定を行っている**	【規則】 ・パスワードを設定すること ・紛失時のデータ削除機能を設定すること	【実施例】 ・モバイルデバイス管理ツール（MDM）により遠隔削除機能を設定している ・システム対策として、パスワードルールを設定している ・スマートデバイスのパスワード・生体認証を必須としている	スマートデバイス	IT	・LanScope EndPointManager ・SKYSEA Client View（MDM）	【SKYSEA Client View Light Edition】 ・OP：iOS端末に対して、遠隔削除、リモートロックが可能。パスワードルールの設定が可能	OP：MDM Services	OP：MDM Services	OP：MDM Services	■			
	17通信制御	103	Lv2	**インターネットと社内ネットワークとの境界にファイアウォールを設置し、通信を制限している**	【規則】 ・社内と社外のネットワーク通信を制限する仕組みを導入すること [導入場所] -社内外ネットワークの境界 [制限する項目] -接続元および接続先のIPアドレス -通信ポート	【実践例】 ・IPアドレス、またはMACアドレスで通信制限を設定している ・パケットフィルタリングを設定して、特定のアプリケーションだけに制限している ・ファイアウォールを設置し接続できるポートを制限している	外部ネットワーク	IT	・Fotigate	–				■			CPS.AC-3 CPS.AC-7 CPS.AC-8 CPS.AC-9 CPS.DS-3 CPS.DS-9 CPS.CM-1
		104	Lv2	**ファイアウォールのフィルタリング設定(通信の許可・遮断設定)を記録し、不要な設定がないか定期的に確認している**	【規則】 ・社内外ネットワーク通信のフィルタリング設定を記録すること ・定期的に不要なフィルタリング設定がないか確認すること ・不要なフィルタリング設定を削除すること 【記録する項目】 ・申請者、接続元および接続先のIPアドレス、通信方向、プロトコル、 ポート番号、利用用途、登録日、有効期限 【確認頻度】 ・1回/年	【実践例】 ・ファイアウォールに重要な変更を行う際には、設定のスナップショットを撮っておき、保存している ・ファイアウォールの設定を台帳で管理し、年1回申請者へ必要性の確認を行っている	外部ネットワーク	IT	・Fotigate	–				■			
		105	Lv2	**リモートアクセスのIDを管理し、不要なIDがないか定期的に確認している**	【規則】 ・リモートアクセスのIDの発行・変更・削除は申請・承認制にすること ・定期的に不要なIDがないか確認すること ・不要なIDを削除すること 【確認頻度】 ・1回/年	【実践例】 ・利用者IDの発行・変更・削除は申請・承認制としている ・利用実績を通知し、不正利用が無いか確認している ・デジタル申請/承認が実施可能なワークフローシステムを導入している ・リモートログインを許可するアクセス元をアクセス制御機器により最小限に設定している ・1回/年　IDの棚卸管理を実施し、不要なIDを削除している	外部ネットワーク	IT	・NI Collabo 360(承認フロー)	–				■			
		106	Lv2	**業務およびデータの重要性に応じてネットワークを分離している。**	【規則】 ・業務内容やデータ重要性でシステムを分類し、専用のネットワークセグメントに設置すること 【対象】 ・社外公開サーバー	【実践例】 ・インターネット公開サーバーはDMZに設置している ・PCとサーバーは、ネットワークセグメントを分離している ・重要情報を取り扱うシステムは専用のネットワークセグメントに設置している ・工場ネットワークは専用のネットワークセグメントとしている	外部ネットワーク	IT	・VLAN構築	–				■			
		107	Lv2	**開発やテストを行う際は、本番環境に影響を与えない構成になっている**	【規則】 ・開発環境やテスト環境が本番環境と分離されていること [対象] -重要な社内サーバー、重要な社外公開サーバー ※対象はリスクに応じて各社で判断	【分離の例】 ・システムの重要度・変更/リリース頻度に応じた開発・テスト・本番環境構成を決め運用している ・重要システムは検証環境を用意し、権限等も分離している	サーバー	IT	・社内サーバー： FortiGate個別構築、法人向けNW構築（NW分割） ・社外公開サーバー：SE個別構築による 社外公開サーバーセキュリティ対策 ※対象が無ければ対策不要	–				■			
		108	Lv2	**不正なWebサイトへのアクセスを制限している**	【規則】 ・不正なWebサイトへのアクセスを制限すること 【対象】 ・クライアントPC/Webゲートウェイ	【実践例】 ・URLフィルタリングを導入し、不正なサイトへのアクセスをブロックしている ・統合脅威管理（UTM）にてWebフィルタリング機能を有効にしている	オフィスツール	IT	・FortiGate　・ LanScope EndPointManager ・SKYSEA Client View	【SKYSEA Client View Light Edition】 ・URL単位で閲覧不可なWEBサイトの制御が可能	○	○	○	■			
		109	Lv2	**インターネットに公開しているWebアプリケーションについてWAF(Web Application Firewall)を導入している**	【規則】 ・WAF(Web Application Firewall)を導入すること 【対象】 ・重要な社外公開Webアプリケーション	【実践例】 ・アプライアンス型のWAFを導入している ・Webサーバーにソフトウェアをインストールするホスト型のWAFを導入している ・インターネット経由サービスとしてクラウド型(DNS切替型)のWAFを導入している ・クラウド連動エージェント型のWAFを導入している	サーバー	IT	・FortiGate ※対象が無ければ対策不要	–				■			
		110	Lv2	**インターネットに公開しているWebサイト、システムについて、DDoS攻撃を受けてもサービスを継続するための対策を実施している**	【規則】 ・DDoS攻撃を受けた際にサービスを継続する仕組みを導入すること 【対象】 ・重要な社外公開Webサイト、DNSサーバー	【実践例】 ・不正侵入検知・防御システム(IDS/IPS)を導入している ・通信事業者によるDDOS対策サービスを利用している	サーバー	IT	・FortiGate ※対象が無ければ対策不要	–				■			
		111	Lv2	**インターネット経由の通信が盗聴、改ざんされないよう、通信を暗号化している**	【規則】 ・社内外ネットワーク通信を暗号化すること 【対象】 ・社外から社内へのリモートアクセス通信 ・ユーザーと社外公開サーバーとの間で認証を伴う通信	【実践例】 ・リモートアクセスはVPNを利用し、暗号化している ・WebサービスはHTTPSを利用し、暗号化している	外部ネットワーク	IT	・FortiGate	–				■			
		112	Lv2	**端末と無線LANアクセスポイントの間の通信を暗号化している**	【規則】 ・端末とアクセスポイントの間の通信を暗号化すること ・政府推奨暗号において危殆化している暗号技術は利用しないこと 【対象】 ・社内無線LAN	【実践例】 ・社内無線LANを利用するPCに電子証明書をインストールし、アクセスポイントの間の通信を暗号化している ・年1回、電子政府推奨暗号リストを確認し、利用している暗号技術が危殆化していないことを確認している	社内ネットワーク	IT	・Aruba ・Meraki	–				■			
	18認証・認可	113	Lv1	**ユーザーIDを個人毎に割り当てている**	【規則】 ・ユーザーIDを共有しないこと ・やむを得ず共有IDが必要な場合は、共有IDを利用したユーザーを特定できるようにすること 【対象】 ・業務で利用するシステムおよびパソコンログオン時のユーザーID	【ルール設定の例】 ・ユーザーIDの共有利用は原則禁止とする　やむを得ず共有する場合は、利用記録を残す 【共有ID利用の例】 ・やむを得ず共有IDを利用する場合、利用者を台帳管理している ・共有IDは利用者が特定できるように、同一時間帯での利用はしない運用にしている	認証とアクセス権	IT	・Secポリシー策定サービス ・SmartOnシリーズ	–				■			

分類	ラベル	No.	レベル	達成条件	達成基準	他社事例 (参考事例を列記しており、 すべての遵守を求めているものではありません)	対象	担当領域 (回答者検討時の参考情報)	池田事務器&KISPA 提供サービス	Ｓｋｙ株式会社にて追記 対応内容 ※左記に対し、支援可能な項目のみ記載	SKYSEA Client View Light Edition 対応可否	S1 / S3 Cloud Edition 対応可否	M1 Cloud Edition 対応可否	対応状況 0:未実施	1:対応中	2:対応完了	経産省CPSF 要求事項に関する 対策要件ID
		114	Lv1	**ユーザーIDとシステム管理者IDの権限を分離している**	【規則】 ・システム管理者と責任者を定めること ・管理者権限を付与する従業員を限定すること ・役割に応じた必要最低限の権限のみ付与すること ・システム開発者が本番環境において、管理者権限で操作できないようにすること ・管理者パスワードを適切に設定すること 【対象】 ・すべてのサーバー、ネットワーク機器	【実践例】 ・システム管理特権IDは、管理行為を行う場合のみ利用し、個々のユーザーIDとは分けて発行している ・OS管理者とDB管理者では、それぞれ必要な権限のみ付与している ・システム管理特権IDを利用する場合は、申請・許可制とし、昔段はログしている ・管理者権限はワークフロー申請により限定された従業員に付与している	認証とアクセス権	IT	・Secポリシー策定サービス ・NI Collabo 360(承認フロー)	–				○			CPS.AC-1 CPS.AC-9 CPS.GV-3 CPS.AC-4 CPS.AC-5 CPS.AC-6 CPS.AC-1
		115	Lv1	**パスワード設定に関するルールを定め、周知している**	【規則】 ・桁数・組み合わせ文字・有効期限を定めること ・英字や数字の連続など容易に推測されるものを避けること ・パスワードの漏えいが判明した場合は、パスワードを変更すること 【対象】 ・業務で利用するシステムおよびパソコンログオン時のパスワード 【周知対象】 -役員、従業員、派遣社員、受入出向者	【パスワード設定ルールの例】 ・8桁以上、英大文字・小文字・記号・数字のうち、3種類以上を組み合わせる ・パスワードの桁数は、10桁以上とし、複雑な文字列に設定されるように制約を設ける ・パスワードは、90日毎に強制的変更を促す設定にする ・パスワード漏えいの疑いが判明した場合は、強制的に変更を行う	認証とアクセス権	情報セキュリティ／IT	・SmartOnシリーズ ・ActiveDirectory構築	–				○			
		116	Lv2	**外部情報システムのパスワード設定ルールを定め、周知している**	【規則】 ・対象のパスワードを社外Webサービスで設定しないこと ※同一の認証基盤(SSO等)の場合は使いまわしに該当しない 【対象のパスワード】 ・PCログオン時のパスワード ・メールシステムのパスワード(Microsoft 365など) 【周知対象】 ・役員、従業員、派遣社員、受入出向者	【パスワード設定ルールの例】 ・社外WEBサービスでパスワードの使いまわしをしない 【周知の例】 ・社内社内電子掲示板（ポータルWebサイト）に1回/年掲載している ・1回/年のユーザー教育を実施している 【Webサービスの例】 ・メールマガジン ・SNS ・会員登録サイト ・クラウドサービス ※業務用/私用双方を含む	認証とアクセス権	情報セキュリティ／IT	・Secポリシー策定サービス セキュリティハンドブックを使用した教育実施 ・情報セキュリティ対策セミナー ・学び維新、Formsなど(eラーニング) ・セキュリティ研修サービス ・NI Collabo 360/Microsoft 365（情報共有）	–				○			
		117	Lv1	**ユーザーID及びシステム管理者IDは定期的、または必要に応じて棚卸しを行い、不要なIDを削除している**	【規則】 ・実施タイミングを明記した棚卸実施ルールを定め、不要なIDを削除すること 【対象】 ・業務で利用するシステムおよびパソコンログオン時のユーザーID、及び、システム管理者のID	【棚卸の実践例】 ・システムごとに年1回以上、ID棚卸を実施し、不要なIDは削除している ・1回/年、全社で定期棚卸を行い、不要なユーザーIDを削除している ・業務委託は3か月に一度責任者が棚卸している ・アカウントが不要になったらドメインアカウント削除申請を起票し、処理している ・退職もしくは期間満了の翌日にID削除実施している	認証とアクセス権	IT	・Secポリシー策定サービス ・SmartOnシリーズ ・SKYSEA Client View（台帳管理）	–				○			
		118	Lv2	**ユーザーIDの発行・変更・削除の手続きを定めている**	【規則】 ・ユーザーIDの発行・変更・削除は申請・承認制にすること 【対象】 ・業務で利用するシステムおよびパソコンログオン時のユーザーID	【実践例】 ・申請・承認については、ユーザーID申請用のシステムを利用している ・申請・承認については、申請書を利用している ・システム主管部署の承認に基づき、作業を実施している	認証とアクセス権	IT	・Secポリシー策定サービス ・NI Collabo 360(承認フロー)	–				○			
		119	Lv2	**管理者権限の付与・変更・削除およびサーバーとネットワーク機器の設定内容の変更については、責任者の承認を得ている**	【規則】 ・管理者権限の付与・変更・削除は申請・承認制にすること ・サーバーおよびネットワーク機器の設定変更は申請・承認制にすること ・サーバーの管理者権限を管理すること（追加、変更、修正） ・ネットワーク機器で管理者権限を利用できる人を管理すること	【実践例】 ・申請・承認については、ユーザーID申請用のシステムを利用している ・申請・承認については、申請書を利用している ・設定変更時は、作業申請書を提出し、管理者の承認を受けてから作業を実施している ・管理者権限を利用できる人は、事前登録制としている	認証とアクセス権	IT	・Secポリシー策定サービス ・NI Collabo 360(承認フロー)	–				○			
		121	Lv2	**重要システムではセッションタイムアウトを実装している**	【規則】 ・重要システムではセッションタイムアウトを実装すること 【対象】 ・社外公開システム、重要な社内システム	【実装例】 ・個人情報を扱うシステムでは、セッションタイムアウトを5分としている ・ネットワーク機器では、セッションタイムアウトを5分としている	サーバー	IT	・Secポリシー策定サービス	–				○			
19パッチやアップデート適用		123	Lv2	**サポート期限が切れたOS、ソフトウェアを利用しないようにしている**	【規則】 ・サポートのあるOS、ソフトウェアを利用すること ・やむを得ずサポート切れのOS、ソフトウェアを利用する場合は、できる限り脆弱性悪用のリスクを低減すること 【対象】 ・会社支給のパソコンのOS、ブラウザ、Officeソフト ・サーバーのOS、ミドルウェア ・会社支給のスマートデバイスのOS、アプリ ・インターネットとの境界に設置されているネットワーク機器の OS、ファームウェア	【実践例】 ・資産管理ソフトでソフトウエアの棚卸を行っている ・ソフトウェア別／バージョン別のサポート情報を定期的に確認し、サポート終了の１年前からバージョンアップあるいは機器の入替計画を検討している ・更新できない場合は、指定のアプリケーションしか動作させないように制御ソフトを導入している（ホワイトリスト制御）	機器全般	IT	・LanScope EndPointManager ・SKYSEA Client View（IT資産管理）	【SKYSEA Client View Light Edition】 ・インストールされてるアプリケーションの一覧取得が可能	○	○	○			CPS.RA-1 CPS.RA-2 CPS.MA-1 CPS.DS-10 CPS.AE-3
		124	Lv1	**情報システム・情報機器、ソフトウェアへセキュリティパッチやアップデート適用を適切に行っている**	【規則】 ・セキュリティパッチやアップデート適用を、規則と期限を定め実施すること ・やむを得ず適用できない場合は、適用対象外の理由を記録すること 【対象】 ・パソコン、スマホ、タブレット、サーバー、ネットワーク機器、ソフトウェア等 -会社支給のクライアントPCのOS、ブラウザ、Officeソフト -サーバーのOS、ミドルウェア -会社支給のスマートデバイスのOS、アプリ -インターネットとの境界に設置されているネット	【適用基準の例】 ・Microsoftの「緊急」レベルを適用している ・Windows Update を毎月適用している ・IPA、JPCERTの「緊急」および「重要」レベルを適用している 【適用期限の例】 ・公開後1ヶ月以内に適用している ・「緊急」レベルは2週間以内、「重要」レベルは1ヶ月以内に適用している ・期限内に適用できなかったセキュリティパッチは、管理表を作成のうえ記録している	機器全般	IT	・LanScope EndPointManager ・SKYSEA Client View (IT資産管理、更新プログラム配布)	【SKYSEA Client View Light Edition】 ・ソフトウェア配布にて、Windows更新プログラムを配布可能	○	○	○			CPS.RA-1 CPS.RA-2 CPS.MA-1 CPS.DS-10 CPS.AE-3
		125	Lv2	**脆弱性の管理体制、管理プロセスを定めている**	【規則】 ・脆弱性情報の収集から対応まで担当部署の役割・責任を明確化すること ・脆弱性情報/脅威情報を収集する情報源、ツール、頻度を定めること ・収集した情報の対応要否判断基準・対応手順を定めること ・対応履歴を記録し、月次でチェックすること	【実践例】 ・情報システム部門にて、IPAやJPCERT等から随時情報収集している ・脆弱性対応のSOCサービスからの定期レポートを確認し、社内システムに該当する脆弱性がないか確認している ・該当する脆弱性がある場合、対策を決定する会議を開催している ・該当した脆弱性は、緊急度およびシステム・業務への影響を確認し、最大2か月以内に対策を実施している ・緊急度に応じた対策実施体制が整っている ・対応状況を記録し、月1回状況を確認している	サーバー	IT	・Secポリシー策定サービス ・LanScope EndPointManager ・SKYSEA Client View	【SKYSEA Client View Light Edition】 ・JVNの脆弱性対策情報ポータルサイトと連携し、脆弱性があるアプリケーションの把握が可能	○	○	×			
		130	Lv2	**外部から受け取ったデータが安全であることを確認している**	【規則】 ・ウイルス対策ソフトのリアルタイムスキャンを実行すること ・外部から受け取ったファイルを安全な仮想環境上で安全性を確認するシステムを導入すること	【安全性確認の例】 ・ウイルス対策ソフトのリアルタイムスキャンを実施している ・サンドボックスと呼ばれる仮想環境で実行してみて怪しい振る舞いを行わないか確認している ・EDR（Endpoint Detection and Response）で不審な振舞いをリアルタイム検知・対処をしている	機器全般	IT	・ESET ・ISM CloudOneなど（ふるまい検知） ・SKYSEA Client View（EDR） ・Sophos MDR（EDR）	–						CPS.RA-2 CPS.MA-1 CPS.DS-1 CPS.DS-2
21オフィスツール関連		131	Lv2	**メール送信による情報漏えいを防止するための対策を実施している**	【規則】 ・機密情報をメール送信する場合は、情報漏えい対策を実施すること	【対策の例】 ・転送禁止などの注記の記載している ・メールCCに上司等のアドレスを含める ・上司の承認を得てメール送信を行っている ・添付ファイルへのパスワード付与またはを暗号化している ・極秘情報については社内であっても、添付ファイルをパスワード付与または暗号化する ・社外メーリングリストへの送信禁止 ・メール文面に禁止語句があった場合、システムで送信遮断しているら送信不可 ・TLSによる暗号通信を可能な限り使用している ・メール本文への機密情報の記載を禁止している	オフィスツール	IT	・M-Filter@Cloud ・FinalCode ・HENGE	【SKYSEA Client View Light Edition】 ・OP：Outlookから送信されたメールログを収集可能 ・OP：Outlookから送信された添付ファイル付きメールの添付ファイルを暗号化することが可能	OP：送信メールログ+外付けデバイス&ファイル暗号化 OP：外付けデバイス&ファイル暗号化	×	×			CPS.RA-2 CPS.MA-1
		132	Lv2	**メールの誤送信を防止する対策を実施している**	【規則】 ・メールの誤送信を防止する対策を実施すること 【対象】 ・社外宛ての送信メール	【対策の例】 ・事故事例の展開や注意喚起などの啓発活動(年1回以上)を行っている ・上司の承認を得てメール送信を行っている ・メールソフトの設定による宛先間違い防止対策を行っている ・送信前に確認を促す仕組みを導入している ・一定時間メール送信を保留し、送信を取り消せる仕組みを導入している	オフィスツール	IT	・M-Filter MailAdviser ・FinalCode ・HENGE E-Mail Security Edition	–						
		133	Lv2	**内部不正対策として社外送付メールの監査を実施し、監査している事をメール利用者に周知している**	【規則】 ・メール監査を実施し、監査している事を周知すること 【対象】 ・社外宛ての送信メール 【周知対象】 ・役員、従業員、派遣社員、受入出向者	【対策の例】 ・システムにより社外宛に送信したメールの一覧及び内容を上司が確認できるようにしている ・全メールをアーカイブし、必要に応じ監査を実施している 【周知の例】 ・下記を定期的に、またはインシデント発生時に実施することを社内電子掲示板（ポータルWebサイト）で周知している -全件調査 -対象絞り込み(キーワード、フリーメール宛先など) -条件抽出による調査 -無作為のサンプリング調査	オフィスツール	IT	・ExchangeOnline構築 ・m-FILTER Archive	【SKYSEA Client View Light Edition】 ・OP：Outlookから送信されたメールログを収集可能	OP：送信メールログ	×	×			CPS.RA-2 CPS.MA-1
		134	Lv2	**WebサイトやWebアプリケーションの利用における禁止事項および制限事項を明確にし、周知している**	【規則】 ・下記を明文化し周知すること -許可なく会社情報をSNSへ掲載しないこと -許可なく業務データをWebサービスにアップロードしないこと 【周知対象】 ・役員、従業員、派遣社員、受入出向者	【対策の例】 ・無許可でのSNSやWebサービスへの投稿・データ保存禁止について規則を作っている ・SNSやWebサービスを利用する場合は上長許可・管理部門への申請制としている 【周知の例】 ・社内電子掲示板（ポータルWebサイト）への掲示・教育等を通じ規則を周知している	オフィスツール	情報セキュリティ／IT	・Secポリシー策定サービス ・NI Collabo 360/Microsoft 365（情報共有）	【SKYSEA Client View Light Edition】 ・メッセージ配信機能にて各端末へ情報周知が可能 【有償サービス】 ・社内部署へ周知のためセミナーを実施可能 (要望により内容のカスタマイズ可能)	○ 有償サービス：セキュリティ研修	○ セキュリティ研修	× 有償サービス：セキュリティ研修			
		135	Lv2	**関係会社やパートナー企業とファイル共有する場合の利用ルールを定め、周知している（クラウドサービス利用も含む）**	【規則】 ・下記を明文化し周知すること -社外とファイル共有する場合は、信頼できる相手とのみ共有すること -送信履歴が残らない方法で、社外へファイル転送することを禁止すること ※ファイル共有：特定の場所にファイルをアップロードし、特定の相手に ファイルのアクセスを許可すること ※ファイル転送：特定の相手にファイルを直接送信すること 【周知対象】	【対策の例】 ・ファイル共有する組織と守秘義務契約を締結している ・コラボレーションするチームのメンバ情報を管理し、適切なメンバであるか定期的に確認している ・ファイル共有ツールの規則を定め利用履歴を取得している ・Web会議でのファイル転送・共有を禁止している ・チャットツールは会社で許可したものを使用し、必要な機能制限を実施している	オフィスツール	IT	・Secポリシー策定サービス ・365Teams ・Canonクラウドストレージサービス Home type-S2 (クラウド活用)	【SKYSEA Client View Light Edition】 ・ユーザ操作によるファイル操作(外部記憶媒体への操作含む)ログ、アプリケーション実行ログの収集が可能 【有償サービス】 ・社内部署へ周知のためセミナーを実施可能 (要望により内容のカスタマイズ可能)	○ 有償サービス：セキュリティ研修	○ セキュリティ研修	× 有償サービス：セキュリティ研修			

分類	ラベル	No.	レベル	達成条件	達成基準	他社事例 （参考事例を列記しており、 すべての遵守を求めているものではありません）	対象	担当領域 （回答者検討時の参考情報）	池田事務器&KISPA 提供サービス	Ｓｋｙ株式会社にて追記 対応内容 ※左記に対し、支援可能な項目のみ記載	SKYSEA Client View Light Edition 対応可否	S1 / S3 Cloud Edition 対応可否	M1 Cloud Edition 対応可否	対応状況 0：未実施	1：対応中	2：対応完了	経産省CPSF 要求事項に関する 対策要件ID
攻撃されたことを迅速に知るため(検知)	22マルウェア対策	136	Lv1	**パソコン、サーバーには、マルウェア感染を検知・通報するソフトウエア(ウイルス対策ソフト)を導入している**	【規則】 ・パソコン、サーバーごとにウイルス対策ソフトを導入すること ・機器に応じた適切なスキャン範囲と頻度を規定し、スキャンを実行すること 【対象】 ・ネットワークに接続している全てのパソコン、サーバー	【実践例】 ・ネットワーク接続するパソコン、サーバーにはウイルス対策ソフトのインストールを必須としている ・既知のパターンをベースに分析し、未知のパターンや亜種などを事前に予測し、検知の精度を高めるビッグデータ活用ディープラーニング型のツールを導入している。 ・ブラウザのセキュリティ設定を高い状態に義務付けている。 ・PC起動時にウイルス対策ソフトの稼働状況を監視している。 【スキャンの実践例】 ・パソコンは1回/日、サーバーは1回/週の定期スキャンをスケジュールしている ・リアルタイムスキャンを有効にしている ・スキャンの範囲は感染リスクの高い特定フォルダに限定している	機器全般	IT	・ESET	【SKYSEA Client View Light Edition】 ・ウイルス対策ソフトウェアのインストールを必須とすることが可能 ・ウイルス対策ソフトウェアのパターンファイル更新日時等を確認することが可能 ・OP：パターンファイル未更新、ウイルス対策ソフトウェア未インストールの検知および本人への通知が可能	○ OP：PC環境診断	○ OP：×	×				CPS.RP-1 CPS.DP-4
		137	Lv1	**ウイルス対策ソフトのパターンファイルは常に最新化している**	【対象】 ・ №136の対象のとおり 【パターンファイルの更新頻度】 ・ 起動し利用する日ごとに１回 以上	【実践例】 ・ウイルス対策ソフトのパターンファイルの更新は1回/日以上行っている ・ユーザーには、長期休み後の業務開始時には、パターンファイルが最新になっていることを促す教育をしている ・仮想デスクトップ基盤上で、統合的に最新化管理をしている 【パターンファイルが最新化できない場合の例】 ・1週間に一度、パターンファイル更新のためのネットワーク接続を実施する ・USB形マルウェアスキャンツールにて、週1回、スキャンを実施する ・パソコンやサーバーをファイアウォールで通信を制限する	機器全般	IT	・Secポリシー策定サービス ・SKYSEA Client View（更新管理） ・LanScope EndPointManager ・SKYSEA Client View	【SKYSEA Client View Light Edition】 ・ウイルス対策ソフトウェアのパターンファイル更新日時等を確認することが可能 ・OP：パターンファイル未更新、ウイルス対策ソフトウェア未インストールの検知および本人への通知が可能	○ OP：PC環境診断	○ OP：×	×				
		139	Lv2	**メールによるマルウェア感染を防止するため、メールゲートウェイでのマルウェアチェックを実施している**	【規則】 ・メールゲートウェイにマルウェアチェック機能を導入すること	【対策例】 ・外部メールサービスの経路上にマルウェアチェック機能を導入している ・社内にメールセキュリティシステムを導入している ・マルウェア付きメールを削除している ・迷惑メールを削除している ・不審メールへ特殊なメールヘッダを付加している ・送信ドメイン認証レコード（SPFレコード）を発行している（送信元詐称迷惑メールの対策） ・送信元詐称メールを隔離している	オフィスツール	IT	・FortiGate ・ExchangeOnline構築	–						
		140	Lv2	**メールの添付ファイルによるマルウェア侵入を防止するため、システムで拡張子制限を実施している**	【規則】 ・メールゲートウェイに特定の拡張子を制限する機能を導入すること	【実践例】 ・特定のファイル拡張子の添付ファイルの受信をメールシステムで遮断している ファイル拡張子の例】 .exe, .pif, .scr, .bat, .com, .lnk, .cmd, .vbs, .cpl, .hta, .shs, .url, .desklink, .mapimail	オフィスツール	IT	・FortiGate ・ExchangeOnline構築	–						
		141	Lv2	**不正なWebサイト閲覧によるマルウェア感染を防止するため、Webゲートウェイでのマルウェアチェックを実施している**	【規則】 ・Webゲートウェイにマルウェアチェック機能を導入すること	【実践例】 ・プロキシサーバーにマルウェアチェックの機能を組込んでいる ・Webゲートウェイサービスにマルウェアチェック機能を付加している	オフィスツール	IT	・FortiGate	–						
	23不正アクセスの検知	142	Lv2	**通信内容を常時監視し、不正アクセスや不正侵入をリアルタイムで検知/遮断および通知する仕組みを導入している**	【規則】 ・不正アクセスをリアルタイム検知・遮断する仕組みを導入すること 【対象】 ・インターネットから社内への通信 ・社内から不正なサーバーへの通信 【導入場所】 ・社内外ネットワークの境界	【実践例】 ・SOCサービスを利用し、外部から内部、内部から外部の通信を24時間365日監視している ・不正侵入検知・防御システム(IDS/IPS)を導入している	外部ネットワーク	IT	・ESET ・Fortigate ＋ SKYSEA Client View(ネットワーク遮断)	–						
		143	Lv2	**インシデント発生時の調査のために必要なログを取得している**	【規則】 ・下記ログを取得、保管している ［取得するログ(保管期間)］ -メールの送受信ログ(6カ月) 取得項目：日時、宛先メールアドレス、送信元メールアドレス -ファイアウォールのログ(6カ月) 取得項目；日時、送信元IPアドレス、送信先IPアドレス -プロキシサーバーのログ(6カ月) 取得項目：日時、リクエスト元IPアドレス、URL -リモートアクセスのログ(6カ月) 取得項目：日時、接続元IPアドレス、ユー	【実践例】 ・保管が必要なログと保管期間を定義し、統合ログ管理システムで保管している ・保管が必要なログと保管期間を定義し、ハードディスクなどオンラインの記憶媒体にログを保管している ・保管が必要なログと保管期間を定義し、バックアップ用テープ、光学ディスク、メモリなどの外部記憶媒体に保管している	事件・事故対応	IT	・LanScope EndPointManager ・SKYSEA Client View	【SKYSEA Client View Light Edition】 ・クライアントの操作ログを最大10年間保存可能	○	○ ※保存期間は3か月	○ ※保存期間は1年				
		145	Lv2	**ログを分析し、サイバー攻撃を検知する仕組みを導入している**	【規則】 ・ログを常時分析し、異常発見時に通知する仕組みを導入すること ［分析対象］ -プロキシサーバー、IPS/IDS、ファイアウォール、エンドポイントのいずれか、または組み合わせ ［監視時間］ -24時間/365日 ［機能要件］ -インシデントアラートが即時発報されること -インシデントの速報レポートが作成され、通知されること	【実践例】 ・SOCサービスを利用し、異常発見時は重大性に基づいて適切なタイミングで通知を受けている ・ログ分析ツールを導入し、検知ポリシーを作成して検知を行っている	外部ネットワーク	IT	・ESET ・FortiGate ・LanScope EndPointManager ・SKYSEA Client View	–						
		146	Lv2	**社内に侵入したマルウェアと不正なサーバーとの通信を遮断する対策を実施している**	【規則】 ・社内から不正なサーバーへの通信を遮断する仕組みを導入すること	【対策例】 ・不正通信先のアドレス情報（URLやIPアドレス等）をブラックリストに登録しておき、通信遮断をしている ・プロキシサーバーにユーザー認証を設定している ・SOCサービスで通信内容を監視し、検知/遮断および通知している	外部ネットワーク	IT	・ESET ・FortiGate	–						
検知被害の対応と修復（対応・復旧）	24バックアップ・復元(リストア)	148	Lv1	**適切なタイミングでバックアップを取得している**	【規則】 ・取得対象、取得頻度を定めてバックアップを取得すること	【取得方法の例】 ・バックアップは外部記録メディアに保管し、ランサムウエア等に暗号化されないようにしている。 【取得対象の例】 ・ファイルサーバーに保存された文書及び設定情報 ・メールサーバー内のメール及び設定情報 【取得頻度の例】 ・日次でデータバックアップ、構成変更時に設定情報（システムイメージバックアップ）バックアップを取得している ・サーバー内のデータおよびサーバーの設定をバックアップ対象とし、頻度は1回/日、過去3世代以上、もしくは法令の定める期間分を保持している	サーバー	IT	・オンプレサーバー＋バックアップシステム構築 ・Barracuda	【SKYSEA Client View Light Edition】 ・サーバ上の資産情報、ログ情報はネットワーク経由や外部記憶媒体に保存可能	○	○	○				CPS.DS-6 CPS.DS-7 CPS.IP-4 CPS.IP-5 CPS.RP-1
		149	Lv1	**復元(リストア)手順を整備している**	【規則】 ・バックアップ対象ごとにリストア手順書を整備すること	【リストア手順書の記載例】 ・対象とする重要度が高いシステムの定義 ・復旧目標時間 ・復旧目標時間を達成するリストア手順 ・リストアテストの実施頻度 【リストア手順書の保管方法の例】 ・障害に備えて、復元手順書を紙面ですぐに利用できる場所に保管する 【リストア手順書の見直し例】 ・年一回リストア手順書を机上・実地でテストを行い、見直しを実施する。 ・内部監査により適切な方式によるバックアップの取得・リストア手順書の整備を確認している	サーバー	IT	・Secポリシー策定サービス ・iTutor、Dojoなど（マニュアル作成ソフト） ・ファイルサーバー構築 ・Barracuda（ストレージ活用）	–						
		150	Lv1	**システムが停止した際も業務が遂行できる代替手段を用意している**	【規則】 ・システム利用不可能時を想定した、実施可能な代替手法を整備すること ［対象］ -高い可用性が求められる(稼働停止許容時間が短い)システム ※対象はリスクに応じて各社判断 ［対策例］ -アナログツールの利用(FAXなど) -クラウドサービスなどの外部情報システムの利用	【代替手法の例】 ・メール等のシステムでのコミュニケーション手段が途絶した際の、緊急電話連絡先を整備している ・生産手配システムが停止した場合は、取引先担当とメールやFAX等で情報を共有し供給を継続する手順を整備している ・生産指示・実行システム停止により安全在庫で納入を補完できない事業所は、マニュアルで生産できる手順・体制を構築している	サーバー	IT	・Secポリシー策定サービス ・Barracuda（ストレージ活用）	–						
		151	Lv2	**重要なデータやシステムについてバックアップの復元(リストア)テストを実施している**	【規則】 ・定めた復元手順により、復元ができることを確認すること 【対象】 ・重要なデータ・システム 【頻度】 ・システム構築時、変更時、定期的（リスク応じて判断）	【リストアテストの例】 ・リストア手順に従いリストアができることを、システム稼働や更新のタイミングで確認している ・バックアップの方式毎にバックアックから復元ができることを年1回確認している ・通常時の担当者以外が、リストア手順に従い復元できることを確認している ・新システム稼働時にリカバリ訓練を必ず実施している	事件・事故対応	IT	・Secポリシー策定サービス ・iTutor、Dojoなど（マニュアル作成ソフト） ・ファイルサーバー構築 ・Barracuda（ストレージ活用）	–						
		152	Lv2	**サーバー等の設置エリアには、設備に災害対策、環境対策を実施している**	【規則】 ・火災、水害、停電に対する対策を行うこと ・温湿度管理を行うこと	【災害対策の例】 ・免震構造のラックを使用している ・建屋の上層階を利用している ・高感度煙センサーを設置している ・外部データセンターを利用している 【環境対策の例】 ・温湿度計を設置している	サーバー	IT	・耐震、免震ラック導入 ・サーバールーム構築など	–						
		153	Lv2	**事業継続上重要なシステムについては、要度に応じて決められた各システムの復旧ポイント、復旧時間を満足するデータと手順が整備されている**	【規則】 ・求められる復旧ポイントへ復帰可能なバックアップ及びトランザクションデータログを保管すること ・求められる復旧時間でリストアできる手順書を整備すること 【対象】 ・事業継続上重要なシステム	【バックアップ設計の例】 ・事業継続上重要なシステムは、求められる復旧ポイント、復旧時間、保管世代・場所を考慮して設計しリストア手順書も整備している	事件・事故対応	IT	・オンプレサーバー＋バックアップシステム構築 ・・Barracuda（ストレージ活用）	–						
合計		153															

分類	ラベル	No.	レベル	達成条件	達成基準	他社事例 （参考事例を列記しており、 すべての遵守を求めているものではありません）	対象	担当領域 （回答者検討時の参考情報）	池田事務器＆KISPA	Ｓｋｙ株式会社にて追記				対応状況			経産省CPSF 要求事項に関する 対策要件ID
									提供サービス	対応内容 ※左記に対し、支援可能な項目のみ記載	SKYSEA Client View Light Edition 対応可否	S1 / S3 Cloud Edition 対応可否	M1 Cloud Edition 対応可否	0：未実施	1：対応中	2：対応完了	