# クボタグループ
# お取引先様向け
# 情報セキュリティ対策基準

2.1 版

2024 年 11月

株式会社クボタ

## 1. はじめに

本対策基準は、K-ESG 経営を推進するにあたり、株式会社クボタおよび子関連会社（以下、当社）が保有する機密情報を共有するお取引先様に対して実施を要請する情報セキュリティ対策事項を示したものです。

機密情報の適正管理等を通じ、安定した事業継続を実現し、当社やお取引先様、社会の継続的な相乗発展を目指します。

当社の取り組みに対する皆さまのこれまでのご協力に感謝致しますとともに、より一層のご理解とご協力をよろしくお願いいたします。

## 2. 適用範囲

本対策基準の適用範囲は、「クボタグループサプライヤー行動規範」の適用範囲によるものとします。

## 3. 機密情報とは

機密情報とは、一般的に、機密である旨が合意されている文書等（電磁的光学的に記録されたデータ情報を含む）により開示された情報や、機密である旨を告知したうえで口頭にて開示された情報を指します。

## 4. 対象

本対策基準は、当社と共有している機密情報だけではなく、その機密情報を活用して創出された機密情報も対象とします。

また、機密情報の形態としては、紙や電子化されたものだけではなく、機密情報を活用し創出された物（金型等）、ノウハウや技術等の無形資産等も含みます。

## 5. 情報セキュリティ対策の基準

本ガイドラインは、「自工会/部工会・サイバーセキュリティガイドライン」等を参考に、従来の情報セキュリティ事故の発生リスク低減を目的とした対策に加え、発生時の迅速な復旧による影響の軽減などを実現する対策も踏まえ作成いたしました。

お取引先様に求める具体的な情報セキュリティ対策基準を以下に示します。

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| 1 方針 | 会社として、セキュリティに対する基本的な考え方や方針を示し、社内の情報セキュリティ意識を向上させる | 自社の情報セキュリティ対応方針を策定し自組織内に周知していること | 1 | 必須 | 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 |
| | | | 2 | 必須 | 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】<br>・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<br>【頻度】<br>・情報セキュリティ対応方針(ポリシー)の内容を確認、改善<br>-1 回以上/年<br>※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 |
| | | | 3 | 必須 | 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】<br>・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<br>【対象】<br>・役員、従業員、社外要員(派遣社員等)<br>【頻度】<br>・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 |
| 2 機密情報を扱うルール | 機密情報を扱うルールを定め、社内へ周知することにより、機密漏えいを防止する | 機密情報のセキュリティに関する社内ルールを規定していること | 4 | 必須 | 自社の守秘義務のルールを規定し、守らせている | 【規則】<br>・自社の守秘義務を策定し、文書化すること<br>・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<br>・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<br>【対象】<br>・役員、従業員、社外要員(派遣社員等) |
| | | | 5 | 必須 | | 【規則】<br>・守秘義務の誓約書を提出させること(社外要員除く) |
| | | | 6 | 必須 | 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】<br>・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<br>【時期】 ※守秘義務の締結時期<br>・業務開始前 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | | 7 | 必須 | 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】<br>・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<br>・回収漏れが起こらない手順を整備、運用すること<br>・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<br>［回収物］<br>－情報(印刷物)<br>－情報機器(PC、スマートデバイス、USB メモリ等の記憶媒体)<br>－アクセス権（ID、鍵）<br>※上記の他に必要な回収物を各社で判断すること<br>［回収状況の確認、手順の是正頻度］<br>－1 回以上/年 |
| | | | 8 | 必須 | 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<br>(個人所有機器(BYOD)含む) | 【規則】<br>・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<br>・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<br>【対象】<br>・役員、従業員、社外要員（派遣社員等）<br>【頻度】<br>・定常的に、かつ、ルールの改正時に周知すること |
| 3 法令遵守 | 会社として、情報セキュリティに関する法令を遵守する | 情報セキュリティに関する法令を考慮し、社内ルールを策定すること<br>(法令例：個人情報保護法、不正競争防止法) | 9 | 必須 | 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】<br>・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<br>・策定した社内ルールを教育・周知すること<br>【対象】<br>・役員、従業員、社外要員（派遣社員等）<br>【頻度】<br>（教育）<br>・新規受け入れ時、かつ、1回／年<br>（周知）<br>・定常的に、かつ、ルールの改正時に周知すること |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | | 10 | 必須 | 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】<br>・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<br>［明確にする内容］<br>・個人情報の管理体制を確立<br>・取得時に利用目的を通知、明示<br>・本人の同意の範囲内で利用<br>・本人の同意なしに第三者提供しないこと<br>・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<br>・個人情報の取扱いルールを定めること<br>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<br>・情報漏洩した時の対応手順<br>・策定した社内ルールを教育・周知すること<br>【対象】<br>－個人情報を取扱う業務担当者 |
| | | | 11 | 必須 | 法令の変更に伴い、ルールを適宜見直ししている | 【頻度】<br>・1 回／年、もしくは、法令の改正が公布・施行された時 |
| | | | 12 | 必須 | | 【頻度】<br>・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 |
| 4 体制<br>(平時) | 情報セキュリティに関する体制及び役割を明確化し、保護すべきデータの漏洩・サイバーセキュリティ対策の徹底、強化を図る | 平時の情報セキュリティリスクを管理する体制を整備し、事故発生に至らないよう、情報収集と共有を行うこと | 13 | 必須 | 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】<br>・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<br>・連絡先リストを整備すること |
| | | | 14 | 必須 | | 【規則】<br>・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 |
| | | | 15 | 必須 | 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】<br>・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<br>・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 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | | 16 | 必須 | 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】<br>・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<br>【対象】<br>・役員、従業員、社外要員（派遣社員等）<br>【頻度】<br>・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 |
| | | | 17 | 必須 | 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】<br>・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<br>・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<br>※相関分析：<br>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 |
| 5 体制<br>（事故時） | 情報セキュリティに関する体制及び役割を明確化し、事件・事故の発生時に、被害を限定的なものに抑えて最小化し、できるだけ速やかに元の状態へと復旧する | 情報セキュリティ事件・事故発生時の対応体制とその責任者を明確にしていること | 18 | 必須 | 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】<br>・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<br>・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 |
| | | | 19 | 必須 | 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】<br>・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<br>・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 |
| | | | 20 | 必須 | 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】<br>・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 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| 6 事故時の手順 | 同上 | 自社の事業継続計画又は緊急時対応計画の中に情報セキュリティ事件・事故を位置づけること | 21 | 任意 | 情報セキュリティ事件・事故を含めた自社の事業継続計画又は緊急時対応計画を作成している | 【基準】<br>・セキュリティ事件・事故の対応履歴、リスク評価結果に基づき、対策計画を立案すること<br>・対策計画に沿って対策が実行されているか確認すること<br>［対策計画の内容］<br>－対策内容(何に対し、どのような対策を行うか)<br>－スケジュール(開始、終了時期 および 対策の各プロセスに要する期間)<br>［対策の進捗状況の確認］<br>－1 回以上／年 |
| | | | 22 | 任意 | 情報セキュリティ事件・事故を含めた自社の事業継続計画又は緊急時対応計画は、定期的に確認され、必要に応じて改定していること | 【頻度】<br>・1 回以上／年 |
| | | 情報セキュリティ事件・事故発生後に早期に対処する手順が明確になっていること | 23 | 必須 | 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】<br>・下記対象範囲が明確になっていること<br>［明確にする内容］<br>－事件・事故として扱う事象<br>－事件・事故のレベル<br>【対象】<br>・役員、従業員、派遣社員、受入出向者への周知 |
| | | | 24 | 必須 | 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】<br>・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<br>①発見報告、 ②初動、③調査・対応、④復旧、⑤最終報告 |
| | | | 25 | 任意 | 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)は、定期的に確認され、必要に応じて、改定していること | 【頻度】<br>・1回／年及び、重大な事件・事故が発生した場合 |
| | | | 26 | 必須 | マルウェア感染時の対応手順を定めている | 【規則】<br>・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<br>①発見報告、 ②初動、③調査・対応、④復旧、⑤最終報告 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | | 27 | 必須 | 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】<br>・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<br>【頻度】<br>-1 回/年以上 |
| 7 日常の教育 | マルウェアや機密情報についてリスクや正しい取り扱いを理解させ、情報セキュリティ事件・事故を予防する | 従業員として注意することを教育していること | 28 | 必須 | 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】<br>・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<br>・教育内容を振返り、次回の教育内容を改善すること<br>【対象】<br>・役員、従業員、社外要員(派遣社員等)における メール利用者<br>【頻度】<br>・新規受け入れ時、かつ、1回／年以上 |
| | | | 29 | 必須 | 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】<br>・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<br>・教育内容を振返り、次回の教育内容を改善すること<br>【対象】<br>・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<br>【頻度】<br>・新規受け入れ時、かつ、1回／年以上 |
| | | | 30 | 必須 | 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】<br>・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<br>・教育内容を振返り、次回の教育内容を改善すること<br>【対象】<br>・役員、従業員、社外要員(派遣社員等)<br>【頻度】<br>・新規受け入れ時、かつ、1回／年以上 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | | 31 | 必須 | 標的型メール訓練を実施している | 【規則】<br>・標的型メール訓練を実施すること<br>・万が一開封した時の対応も訓練内容に含めること<br>・訓練内容や方法を振返り、次回の訓練を改善すること<br>【対象】<br>　-電子メールの利用者<br>【頻度】<br>　-1回以上／年 |
| | | | 32 | 必須 | 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】<br>・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<br>・教育内容を振返り、次回の教育内容を改善すること<br>【対象】<br>　-各部署の情報セキュリティ管理者または推進者<br>　※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<br>【頻度】<br>　-1 回以上／年 |
| | | | 33 | 必須 | 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】<br>・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<br>・説明内容を振返り、次回の説明内容を改善すること<br>【対象】<br>　-経営層や役員<br>【頻度】<br>　-1 回以上／年 |
| | | | 34 | 必須 | 全社で啓発活動を実施している | 【規則】<br>・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<br>【対象】<br>・役員、従業員、社外要員（派遣社員等）<br>【頻度】<br>　-1 回以上／年 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | | 35 | 必須 | 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】<br>・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<br>リマインドすること<br>・啓発内容を振返り、次回の啓発内容を改善すること<br>【対象】<br>-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）<br>【頻度】<br>-1 回以上／1 年 |
| | | | 36 | 必須 | 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】<br>・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<br>【対象の教育、啓発】<br>-各社で判断した重要な教育、啓発<br>【頻度】<br>-1 回以上/年 |
| | | | 37 | 任意 | 情報システムの調達に係る要員に対して、取引先の指導ができるようセキュリティ教育を実施している | 【規則】<br>取引先の特性に合わせたセキュリティ指導するスキルを得るために、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<br>【対象】<br>・情報システムの調達に係る要員<br>【頻度】<br>・1回／年以上 |
| | 情報セキュリティ事件・事故に迅速かつ適切に対応できるように事前に備え、事故発生時の被害拡 | 自組織内あるいは組織を跨いで影響する情報セキュリティ事件・事故の発生と影 | 38 | 必須 | 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】<br>・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<br>【対象】<br>・役員、従業員、社外要員（派遣社員等）<br>【頻度】<br>・新規受け入れ時、かつ、1回／年以上 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | 大の防止・迅速な復旧を図る | 響を抑制する教育・訓練を行っていること | 39 | 任意 | 組織を跨いだ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】<br>・組織を跨いだ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<br>【対象】<br>・セキュリティ関連部門<br>【頻度】<br>・1回／年以上 |
| | | | 40 | 必須 | 教育・訓練の内容を必要に応じて見直ししている | 【頻度】<br>・教育・訓練実施前後、もしくは1回／年以上 |
| 8 他社との情報セキュリティ要件 | サプライチェーンにおける機密情報の漏洩を防止するとともに、事故発生時の対応を迅速に行えるようにする | サプライチェーン上で発生する情報セキュリティ要件が明確になっていること | 41 | 必須 | サプライヤーとモノ・データの流れを共有できている | 【規則】<br>・重要なサプライヤーを特定できていること<br>・モノ・データの流れを特定できていること<br>・取引の概要を図示して、サプライヤーと共有できていること<br>【対象】<br>・取引のあるサプライヤー |
| | | | 42 | 任意 | 重要な機密情報を取扱うパートナー企業のセキュリティ対策状況を把握している | 【規則】<br>以下の例を参考にパートナー企業の対策状況を把握すること<br>・チェックシートを作成しパートナー企業から回答を受領する<br>・パートナー企業に訪問し点検を実施する<br>【対象会社】<br>－自社の重要な機密情報を提供・共有する子会社、取引先など<br>例:"極秘"の機密情報を共有する会社<br>【頻度】<br>－1 回以上/年 |
| | | | 43 | 必須 | 契約終了時に機密情報やアクセス権などを回収または破棄している | 【規則】<br>・回収すべき機密情報、アクセス権などのチェックシートを作成すること<br>・契約終了時にチェックシートを使用し機密情報、アクセス権などを回収すること<br>・回収、破棄が漏れなく行われていることを確認し、必要に応じて是正すること<br>【対象会社】<br>－機密情報を提供・共有する子会社、取引先など<br>【頻度】<br>－1 回以上/年 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | | 44 | 必須 | 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】<br>・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<br>【対象】<br>・機密情報を共有する会社 |
| | | | 45 | 任意 | 他社との間で、機密情報の取り扱い方法に課題が無いか定期的に確認され、必要に応じて、改定していること | 【頻度】<br>1 回以上/年 |
| | | | 46 | 必須 | 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】<br>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 |
| | | | 47 | 任意 | 情報セキュリティ事件・事故時の他社との役割と責任の文章は、定期的に確認され、必要に応じて、改定していること | 【頻度】<br>1 回以上/年 |
| | | | 48 | 必須 | 自社における他社の重要な機密情報の取扱い状況を把握している | 【規則】<br>・他社の重要な機密情報を自社で取扱った履歴を記録、保管すること<br>・適切に記録、保管されていることを確認し、必要に応じて是正すること<br>【記録、保管状況の確認、是正頻度】<br>-1 回以上/年 |
| 9 アクセス権 | アクセス権設定の不備に起因した、機密エリアやシステムへの不正アクセスを防止する | アクセス権(入室権限やシステムのアクセス権)を適切に管理していること | 49 | 必須 | 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】<br>・以下の内容等を含む管理ルールを定めること<br>・アクセス権の発行・変更・削除は申請・承認制であること<br>・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<br>・入室権限やアクセス権の棚卸について定めていること<br>・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<br>【対象】<br>・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<br>・機密上の配慮が必要な場所や部屋 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | | 50 | 必須 | | 【規則】<br>・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<br>・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。<br>・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。<br>・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。 |
| | | | 51 | 必須 | 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】<br>No49 に定義した管理ルールの遵守状況の点検を行っていること |
| | | | 52 | 必須 | 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】<br>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 |
| | | | 53 | 必須 | 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】<br>・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。<br>・ログを脅威から保護するため、ログを保存するモノ、システムにアクセス制御等を適用すること |
| 10 情報資産の管理(情報) | 情報資産を適切に管理し、機密情報の漏洩を防止する | 情報資産の機密区分を設定・把握し、その機密区分に応じて情報を管理していること | 54 | 必須 | 機密区分に応じた情報の管理ルールを定めている | 【規則】<br>・以下の内容等を含む管理ルールを定めること<br>・機密の特定<br>・機密区分のレベル判定と表示<br>・区分に応じた取り扱い方法<br>・取り扱いエリアの区分及び制限<br>【対象】<br>・情報資産(情報) |
| | | | 55 | 必須 | 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】<br>・管理ルールの内容を確認し、必要に応じて改善すること<br>【頻度】<br>-1 回以上 ／年 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | | 56 | 必須 | 高い機密区分の情報資産(情報)を一覧化している | 【規則】<br>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<br>【対象情報】<br>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 |
| | | | 57 | 必須 | 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】<br>・一覧表の内容を確認し、必要に応じて是正すること<br>【頻度】<br>-1 回以上 ／年 |
| | | | 58 | 必須 | 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】<br>No.54 に定義した管理ルールの遵守状況の点検を行い、不備・違反があれば是正を行うこと<br>【頻度】<br>1 回/年 以上 |
| 11 情報資産の管理(機器) | IT 資産を適切に管理し、情報セキュリティ事件・事故につながるリスクを減ずるとともに、情報セキュリティ事故発生時の対応を迅速化する | 会社が保有する情報機器及び機器を構成する OS や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)を適切に管理していること | 59 | 必須 | 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】<br>・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 |
| | | | 60 | 必須 | 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】<br>・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 |
| | | | 61 | 必須 | 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】<br>・1 回/年 以上 |
| | | | 62 | 必須 | 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】<br>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<br>【頻度】<br>1 回/年 以上 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | | 63 | 任意 | | 【規則】<br>重要度に応じて、機器と搭載ソフトウェアが正規品である事をシリアル番号やハッシュ値を利用して定期的に確認すること<br>【頻度】<br>・1 回/年 以上(資産棚卸時等) |
| | | | 64 | 必須 | 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】<br>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。<br>【対象】<br>-会社支給のスマートデバイス<br>【確認頻度】<br>-1 回/年 |
| | | | 65 | 必須 | 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】<br>・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<br>・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<br>※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<br>[対象]<br>-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 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| 12 リスク対応 | 情報資産のセキュリティリスクを特定し、会社として組織的な対策を行うことにより、業務影響を極小化する | 自組織内(自組織の業務:業務委託も含めて)の情報セキュリティリスクに対する対策を行っていること | 66 | 必須 | 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】<br>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<br>【対象】<br>No.56 で特定した情報資産<br>【観点】<br>-外部の脅威<br>-自社の脆弱性<br>※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<br>-情報資産の価値<br>【方法】<br>-対象の情報、情報システムを定めること<br>-各観点の評価規則、およびそれらを考慮したリスクレベルの規則を定めること<br>-各情報、情報システムについて、各観点の評価からリスクレベルを決定すること<br>【頻度】<br>重要な情報資産を見直した時、または、1回／年 以上 |
| | | | 67 | 任意 | セキュリティの要求事項を記載した開発標準を定め、定期的に見直している | 【規則】<br>・情報システムのセキュリティ開発標準を定めること<br>・開発標準に則って、開発していることをチェックすること<br>・開発標準の内容を定期的に見直すこと<br>【見直し頻度】<br>・1 回/年 |
| | | | 68 | 必須 | 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】<br>No.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<br>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<br>【対象】<br>情報セキュリティの総括責任者、関係部門<br><br>【頻度】<br>-1 回以上／年 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | | 69 | 必須 | 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】<br>No.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<br>【対象】<br>情報資産の業務影響<br>【頻度】<br>1 回／年 以上 |
| 13 取引内容・手段の把握 | どの取引先とどのような情報資産をどのような手段でやり取りするかを明確にし、取引を通じた情報漏えい等を防止する | 取引先毎に、取引で取り交わされる情報資産と、取引に利用している手段を把握していること | 70 | 必須 | 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】<br>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<br>【対象】<br>重要な情報資産(No.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<br>【頻度】<br>取引開始時／取り交わす情報・手段の変更時 |
| | | | 71 | 任意 | 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)の一覧を<br>定期的、または必要に応じて、見直ししている | 【頻度】<br>・1 回/年 以上 |
| | | IT 機器調達における情報セキュリティリスクを管理すること | 72 | 任意 | IT 機器調達に対するセキュリティ要求事項が決められており、社内に周知されていること | 【規則】<br>・機器調達に対するセキュリティ要求事項を一覧化していること<br>・機器調達時に、セキュリティ要求事項を容易に確認できる状態にすること<br>【対象】<br>[機器]<br>・社内ネットワークに接続する IT 機器<br>[周知]<br>・役員、従業員、社外要員(派遣社員等)<br>【頻度】<br>・定常的に、かつ、機器調達時のセキュリティ要求事項の改正時に周知すること |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | | 73 | 任意 | IT 機器調達に対するセキュリティ要求事項を購入先と共有しており、購入時の評価結果を記録し保管している | 【規則】<br>・セキュリティ要求事項が購買契約等に明記されていること<br>・機器調達時に、セキュリティ要求事項の評価を実施し、結果が保管されていること<br>・定期的に確認結果が保管されていることを確認する<br>【対象】<br>社内ネットワークに接続する IT 機器<br>【保管状態の確認頻度】<br>1 回以上/年 |
| 14 外部への<br>接続状況の把握 | 外部情報システム利用における安全性と信頼性の確保、および情報セキュリティ事件・事故発生時の迅速な対応を図る | 関係組織(サプライヤー等含む)との関係において、自組織の通信ネットワーク構成を把握し、他組織との連携状態やデータの流れを監視すること | 74 | 必須 | 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】<br>・ネットワーク図を作成すること<br>[対象範囲]<br>-自社の情報機器が存在するネットワーク<br>[見直し頻度]<br>-1 回/年以上<br>＜追記＞<br>【基準】<br>・データフロー図を作成すること<br>[対象範囲]<br>-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<br>【基準】<br>・関係組織との通信を監視すること<br>[対象範囲]<br>-関係組織間のネットワークでやり取りされるデータ<br>[頻度]<br>-常時 |
| | | | 75 | 必須 | 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】<br>-1 回/年以上 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | 外部情報システム(顧客・子会社・関係会社・外部委託先・クラウドサービス・外部情報サービス等)を明確にし、利用状況を適切に管理していること | 76 | 必須 | 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】<br>・以下の内容を含む利用ルールを定めること<br>・外部情報システムの接続先と守秘義務契約を締結する<br>・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<br>・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 |
| | | | 77 | 必須 | 利用している外部情報システムを一覧化している | 【規則】<br>・外部情報システムの一覧を作成していること |
| | | | 78 | 必須 | 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】<br>・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<br>【頻度】<br>・1 回／年以上、かつ、新規開始あるいは利用中止時 |
| 15 社内接続ルール | 社内ネットワークの利用を適切に管理することにより、情報漏えいやマルウェア感染などの被害を最小化する | 社内ネットワークへの接続時には、情報システム・情報機器の不正利用を抑制する対策を行っていること | 79 | 必須 | 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<br>【規則】<br>・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<br>【対象】<br>・社内でネットワークに直接接続するすべての機器<br>・会社標準機器、社外からの持ち込み機器含む<br>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<br>【規則】<br>・リモートアクセスを利用する場合のルールを定めること<br>【対象】<br>・社外から公衆インターネット経由あるいは専用線経由で社内ネットワークに接続する全ての機器 |
| | | | 80 | 任意 | 許可された機器以外は社内ネットワークに接続できないよう、システムで制限している | 【規則】<br>・許可された機器以外の接続を検知・遮断する仕組みを導入すること<br>【対象】<br>・社内ネットワークに接続する機器 |
| | | | 81 | 任意 | 内部情報漏洩対策として、複数ログを組み合わせて、異常行動を自動検知できる仕組みを導入している | 【規則】<br>・情報持ち出しに関するログを分析して不正な持ち出しが検知できること<br>・不正な持ち出しが発生した場合は、アラートが通知できること |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | リモートワークの環境において、セキュリティ事故(主に情報漏えい、なりすまし)を抑制する対策を行っていること | 82 | 必須 | 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】<br>・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<br>・ルールの遵守状況を確認し、必要に応じて是正すること<br>［周知対象］<br>-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<br>［周知のタイミング］<br>-リモートワークの開始前<br>［ルールの内容］<br>-リモートワークで使用許可する情報機器<br>※必要に応じて申請、承認の方法を含む<br>-個人所有端末にダウンロード可能なファイルの機密区分や種類<br>［ルールの内容、遵守状況の確認頻度］<br>-1 回以上/年 |
| | | | 83 | 必須 | 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】<br>・リモートワーク遂行上のルールを定め、周知すること<br>・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<br>［周知対象］<br>-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<br>［周知のタイミング］<br>-リモートワークの開始前<br>［ルールの内容や遵守状況の確認、是正頻度］<br>-1 回以上/年 |
| 16 物理セキュリティ | サーバー等の重要機器への不正操作による情報漏洩、改ざん、システム停止を防ぐ | サーバー等の設置エリアには、物理的セキュリティ対策を行っていること | 84 | 必須 | 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】<br>・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 |
| | | | 85 | 必須 | 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】<br>・サーバー等の設置エリアを施錠すること<br>・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<br>・管理者を定めて、施錠管理を行うこと |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | | 86 | 必須 | 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】<br>・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<br>【記録する項目】<br>-入退場日時<br>-入場者(氏名、所属、連絡先など)<br>-入場目的<br>-承認者<br>【保管期間】<br>・6ヶ月 |
| | | | 87 | 必須 | 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】<br>・入場時、退場時に持込み・持ち出し物を確認すること<br>・入場者の行動を監視すること |
| | | 社内への入退場において、セキュリティ事故(主に不正侵入、不正持ち出し、情報漏えい、不審行動)を抑制する対策を行っていること | 88 | 必須 | 入退場に関するルールを定め、周知、運用している | 【規則】<br>・自社の入退場ルールを定めること<br>・入退場ルールを周知すること<br>・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<br>【周知対象】<br>-自社に出入りする全ての人員<br>【入退場ルールの内容】<br>-入場制限エリアの定義<br>-入退場時の申請、承認<br>-入退場時の身分証明方法(社員証、入場許可証の着用など)<br>-入場許可証,通門証の発行規則<br>【入退場ルールの内容や遵守状況の確認、是正頻度】<br>-1回以上/年 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | | 89 | 必須 | 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】<br>・重要なエリア、部屋の入退場を制限すること<br>・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<br>【記録する項目】<br>−入退場日時<br>−入場者(氏名、所属、連絡先など)<br>−入場目的<br>−承認者<br>【記録の保管期間】<br>−6 ケ月以上 |
| | | | 90 | 必須 | 不正侵入や不審行動を監視している | 【規則】<br>・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<br>・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<br>【監視状況の確認、是正頻度】<br>−1 回以上/6 か月 |
| | | 持込み・持出し物の制限を行っていること | 91 | 必須 | 社内への持込みルールを明確にし、運用している | 【規則】<br>・社内への持込みルールを定めること<br>・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<br>【対象者】<br>−従業員、派遣社員、受入出向者および社外者<br>【対象の物品】<br>−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<br>※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<br>【持込みルールの内容】<br>−持込み制限の対象とするエリア、物品<br>−社内への持込み申請、承認方法<br>−持込み記録の保管、管理方法(保管期間:6 か月)<br>【持込みルールの内容や遵守状況の確認、是正頻度】<br>−1 回以上/年 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | | 92 | 必須 | 社外への持出しルールを明確にし、運用している | 【規則】<br>・社外への持出しルールを定めること<br>・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<br>【対象】<br>・従業員、派遣社員、受入出向者および社外者<br>【対象の物品］<br>-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、<br>印刷物(図面などの機密書類)<br>※上記の他に必要な物品を各社で判断すること<br>【持出しルールの内容］<br>-社外への持出し申請、承認方法<br>-持出し記録の保管、管理方法(保管期間:6 か月）<br>【持出しルールの内容や遵守状況の確認、是正頻度】<br>-1 回以上/年 |
| | | | 93 | 必須 | 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】<br>・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<br>【実施頻度】<br>・1 回以上/6 か月 |
| | | 社内の撮影・録音において、セキュリティ事故(主に情報漏えい)を抑制する対策を行っていること | 94 | 必須 | 社内における撮影ルールを定め、運用している | 【規則】<br>・社内における撮影ルールを定めること<br>・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<br>【撮影ルールの内容】<br>-撮影を制限する対象またはエリア<br>-撮影の申請、承認手順<br>-撮影申請、行為の記録の保管(保管期間:6 か月）<br>※撮影を制限しないエリアを設けることも可能<br>(例:社外者との打合せエリア)<br>【撮影ルールの内容や遵守状況の確認、是正頻度］<br>-1 回以上/年 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | | 95 | 任意 | 録音に関するルールを定め、運用している | 【規則】<br>・録音に関するルールを定めること<br>・録音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<br>【録音ルールの内容】<br>-録音を制限する会議(面着、リモート含む)やエリアの定義<br>-録音の申請、承認方法<br>※会議の種類やエリアによって、申請、承認の要否を区別することも可<br>【録音ルールの内容、遵守状況の確認、是正頻度】<br>・1 回以上/年 |
| | | | 96 | 任意 | 盗聴による情報漏えいへの対策を行っている | 【規則】<br>・盗聴による情報漏えい対策を行うこと<br>【実施頻度】<br>-1 回以上/年 |
| | | 脆弱性が発見された際の対策対象の把握や外部記憶媒体を用いた情報漏えい等を抑制する対策がおこなえていること | 97 | 必須 | 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】<br>・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<br>・構成、設定の変更は承認制にすること<br>[対象]<br>-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 |
| | | | 98 | 必須 | 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】<br>・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<br>・ソフトウェアの無断インストールを制限すること<br>・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<br>※システムでインストール制限している場合は確認不要<br>[対象]<br>-会社支給のクライアント PC<br>[制限すべきソフトウェアの例]<br>-情報漏えいにつながるソフトウェア<br>-深刻な脆弱性があるソフトウェア<br>-マルウェア・スパイウェアの疑惑のあるアプリ<br>[確認頻度]<br>-1 回/年<br>[周知対象]<br>-役員、従業員、派遣社員、受入出向者 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | | 99 | 必須 | PC からのデータ書き出しを仕組みで制限している | 【規則】<br>・データ書き出しを制限する仕組みを導入すること<br>［対象］<br>－会社支給のクライアント PC |
| | | | 100 | 必須 | 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】<br>－重要データはクライアント PC 以外に保管すること<br>［周知対象］<br>－役員、従業員、派遣社員、受入出向者 |
| | | 重要情報を格納・利用するシステムにおいて、人為的設定ミスによる被害を最小化する対策を実施していること | 101 | 必須 | 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】<br>・不要サービス、デーモンを無効化すること<br>・デフォルトユーザーID の利用を停止すること<br>・デフォルトパスワードの変更すること |
| | | | 102 | 必須 | 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】<br>・パスワードを設定すること<br>・紛失時のデータ削除機能を設定すること |
| 17 通信制御 | | サイバー攻撃、内部情報漏えいを防止するため、情報システム・情報機器や不正な | 103 | 必須 | 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】<br>・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<br>［導入場所］<br>－社内外ネットワークの境界<br>［制限する項目］<br>－接続元および接続先の IP アドレス<br>－通信ポート |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | Web サイトへの通信制御を行っていること | 104 | 必須 | 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】<br>・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<br>・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<br>・不要なフィルタリング設定を削除すること<br>【記録する項目】<br>−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<br>【確認頻度】<br>−1 回/年 |
| | | | 105 | 必須 | 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】<br>・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<br>・定期的に不要な ID がないか確認すること<br>・不要な ID を削除すること<br>【確認頻度】<br>−1 回/年 |
| | | | 106 | 必須 | 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】<br>・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<br>【対象】<br>−社外公開サーバー設置のネットワーク、<br>PC とサーバーのネットワーク、工場ネットワーク／OA ネットワーク等 |
| | | | 107 | 必須 | 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】<br>・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<br>［対象］<br>−重要な社内サーバー、重要な社外公開サーバー<br>※対象はリスクに応じて各社で判断 |
| | | | 108 | 必須 | 不正な Web サイトへのアクセスを制限している | 【規則】<br>・不正な Web サイトへのアクセスを制限すること<br>【対象】<br>−クライアント PC/Web ゲートウェイ |
| | | | 109 | 必須 | 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】<br>・WAF(Web Application Firewall)を導入すること<br>【対象】<br>・重要な社外公開 Web アプリケーション |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | | 110 | 必須 | 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】<br>・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<br>【対象】<br>－重要な社外公開Webサイト、DNSサーバー |
| | | | 111 | 必須 | 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】<br>・社内外ネットワーク通信を暗号化すること<br>【対象】<br>－社外から社内へのリモートアクセス通信<br>－ユーザーと社外公開サーバーとの間で認証を伴う通信 |
| | | | 112 | 必須 | 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】<br>・端末とアクセスポイントの間の通信を暗号化すること<br>・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<br>【対象】<br>・社内無線LAN |
| 18 認証・認可 | 情報システムの不正利用や、情報システムの不正操作・変更を防ぐことで、情報漏洩、改ざんを防ぐとともに、情報システムを安定稼働させる。<br>さらに、情報漏えい、改ざんや情報システム停止の際の | 情報システム・情報機器への認証・認可の対策を行っていること | 113 | 必須 | ユーザーIDを個人毎に割り当てている | 【規則】<br>・ユーザーIDを共有しないこと<br>・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<br>【対象】<br>・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 |
| | | | 114 | 必須 | 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】<br>・システム管理者と責任者を定めること<br>・管理者権限を付与する従業員を限定すること<br>・役割に応じた必要最低限の権限のみ付与すること<br>・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<br>・管理者パスワードを適切に設定すること<br>【対象】<br>－すべてのサーバー、ネットワーク機器 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | 原因調査を可能にする | | 115 | 必須 | 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】<br>・桁数・組み合わせ文字・有効期限を定めること<br>・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<br>・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<br>【対象】<br>・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<br>【周知対象】<br>－役員、従業員、派遣社員、受入出向者 |
| | | | 116 | 必須 | 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】<br>－対象のパスワードを社外 Web サービスで設定しないこと<br>※同一の認証基盤(SSO 等)の場合は使いまわしに該当しない<br>【対象のパスワード】<br>－PC ログオン時のパスワード<br>－メールシステムのパスワード(Microsoft 365 など)<br>【周知対象】<br>－役員、従業員、派遣社員、受入出向者 |
| | | | 117 | 必須 | 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】<br>・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<br>【対象】<br>・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 |
| | | | 118 | 必須 | ユーザーID の発行・変更・削除の手続きを定めている | 【規則】<br>・ユーザーID の発行・変更・削除は申請・承認制にすること<br>【対象】<br>－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 |
| | | | 119 | 必須 | 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】<br>・管理者権限の付与・変更・削除は申請・承認制にすること<br>・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<br>・サーバーの管理者権限を管理すること(追加、変更、修正)<br>・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 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | | 120 | 必須 | インターネットから利用できるシステムには多要素認証を実装している | 【規則】<br>・インターネットを経由した認証において、知識、所持、生体のいずれか 2 つ以上の認証を実装すること<br>【対象】<br>−機密レベルが高い情報を取り扱うシステム<br>−特権アカウント<br>−リモートアクセス |
| | | | 121 | 必須 | 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】<br>・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<br>【対象】<br>社外公開システム、重要な社内システム |
| | | | 122 | 任意 | 認証ログのモニタリングを実施している | 【規則】<br>・認証ログのモニタリングを実施し、不審な認証を検知できること<br>【対象】<br>・パソコン、サーバーの認証ログ、重要システムのデータベースアクセスログ<br>【頻度】<br>・1 回/月以上 |
| 19 パッチやアップデート適用 | 不正アクセスやマルウェア感染のリスクを低減する | サポート期限が切れた機器、OS、ソフトウェアを利用しないようにしていること | 123 | 必須 | 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】<br>・サポートのある OS、ソフトウェアを利用すること<br>・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<br>【対象】<br>−会社支給のパソコンの OS、ブラウザ、Office ソフト<br>−サーバーの OS、ミドルウェア<br>−会社支給のスマートデバイスの OS、アプリ<br>−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（ルーターや VPN 機器など）の OS、ファームウェア |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | 脆弱性を利用した不正アクセスを防止する施策を実施していること | 124 | 必須 | 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】<br>・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<br>・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<br>【対象】<br>・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<br>–会社支給のクライアント PC の OS、ブラウザ、Office ソフト<br>–サーバーの OS、ミドルウェア<br>–会社支給のスマートデバイスの OS、アプリ<br>–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（ルーターや VPN 機器など）の OS、ファームウェア |
| | | | 125 | 必須 | 脆弱性の管理体制、管理プロセスを定めている | 【規則】<br>・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<br>・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<br>・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<br>・対応履歴を記録し、月次でチェックすること |
| | | | 126 | 任意 | 社外へ公開しているサーバーについて、本番稼働前および稼働後に脆弱性診断を実施し、判明した脆弱性に対して対策を行っている | 【規則】<br>・プラットフォームの脆弱性を診断すること<br>・脆弱性に対する対応の要否判断規則とリードタイムを決めること<br>・診断結果と対応結果を保管すること<br>【対象】<br>–社外公開サーバーの OS、ミドルウェア<br>【診断頻度】<br>–本番稼働前：1 回以上<br>–本番稼働後：2 回/年およびシステムの大きな変更時<br>–影響の大きな脆弱性が公開された時 |
| | | | 127 | 任意 | 社内サーバーについて、本番稼働前および稼働後に脆弱性診断を実施し、脆弱性に対応している | 【規則】<br>・プラットフォームの脆弱性を診断すること<br>・脆弱性に対する対応の要否判断規則とリードタイムを決めること<br>・診断結果と対応結果を保管すること<br>【対象】<br>–重要な社内サーバーの OS、ミドルウェア<br>【診断頻度】<br>–本番稼働前：1 回以上<br>–本番稼働後：1 回/年およびシステムの大きな変更時 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | | 128 | 任意 | 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、アプリケーション脆弱性診断を実施している | 【規則】<br>・Web アプリケーションの脆弱性を診断すること<br>・脆弱性に対する対応の要否判断規則とリードタイムを決めること<br>・診断結果と対応結果を保管すること<br>【対象】<br>−重要な社外公開 Web アプリケーション<br>【診断頻度】<br>−本番稼働前:1 回以上<br>−本番稼働後:アプリケーションの大きな変更時 |
| 20 データ保護 | 不正アクセスやマルウェア感染のリスクを低減する | 情報システム・情報機器のデータ保護を行っていること | 129 | 任意 | 情報機器、情報システムのデータを適切に暗号化している | 【規則】<br>・社外に持ち出すパソコン、記憶媒体のデータを暗号化すること<br>・重要システムのデータベースを暗号化すること |
| | | | 130 | 必須 | 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】<br>・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<br>・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 |
| 21 オフィスツール関連 | 不正アクセスやマルウェア感染のリスクを低減する | 情報システム・情報機器のデータ保護を行っていること | 131 | 必須 | 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】<br>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 |
| | | | 132 | 必須 | メールの誤送信を防止する対策を実施している | 【規則】<br>メールの誤送信を防止する対策を実施すること<br>【対象】<br>−社外宛ての送信メール |
| | | | 133 | 必須 | 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】<br>メール監査を実施し、監査している事を周知すること<br>【対象】<br>−社外宛ての送信メール<br>【周知対象】<br>−役員、従業員、派遣社員、受入出向者 |
| | | | 134 | 必須 | 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】<br>下記を明文化し周知すること<br>−許可なく会社情報を SNS へ掲載しないこと<br>−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<br>【周知対象】<br>−役員、従業員、派遣社員、受入出向者 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | | 135 | 必須 | 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】<br>下記を明文化し周知すること<br>-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<br>-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<br>※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<br>※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<br>【周知対象】<br>-役員、従業員、派遣社員、受入出向者 |
| 22 マルウェア対策 | マルウェア感染による情報漏洩、改ざん、システム停止を防ぐ | セキュリティ上の異常を素早く検知するマルウェア対策を行っていること | 136 | 必須 | 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】<br>・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<br>・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<br>【対象】<br>・ネットワークに接続している全てのパソコン、サーバー |
| | | | 137 | 必須 | 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】<br>№136 の対象のとおり<br>【パターンファイルの更新頻度】<br>起動し利用する日ごとに1回 以上 |
| | | | 138 | 必須 | エンドポイントでの詳細な履歴取得およびマルウェア感染後の遠隔対応が可能な行動追跡システムを導入している | 【規則】<br>・エンドポイント対策システム(EDR 型ウイルス対策ソフト または 次世代型ウイルス対策ソフト)を導入すること<br>【対象】<br>-会社支給のクライアント PC<br>-サーバー<br>【機能要件】<br>-AI や機械学習等を活用しファイルの特徴や挙動等からも不審なファイルや兆候を検査できること<br>-端末での検知結果等が一元管理できること<br>-端末の操作履歴、プログラムの実行履歴、レジストリの変更履歴を取得できること<br>-遠隔から端末の調査ができること<br>-遠隔からネットワークからの切断ができること<br>-感染後の復旧対応ができること |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | | 139 | 必須 | 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】<br>・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 |
| | | | 140 | 必須 | 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】<br>・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 |
| | | | 141 | 必須 | 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】<br>・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 |
| 23 不正アクセスの検知 | 不正アクセス・不正侵入による情報漏洩、改ざん、システム停止を防ぐ | ネットワークへの不正アクセスを常時監視する体制を構築すること | 142 | 必須 | 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】<br>・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<br>【対象】<br>・インターネットから社内への通信<br>・社内から不正なサーバーへの通信<br>【導入場所】<br>-社内外ネットワークの境界 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | セキュリティ事件・事故が発生した場合に、侵入経路や漏えい経路の調査が行えるよう、ログが取得されていること | 143 | 必須 | 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】<br>・下記ログを取得、保管している<br>[取得するログ(保管期間)]<br>-メールの送受信ログ(6 カ月)<br>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<br>-ファイアウォールのログ(6 カ月)<br>取得項目 ; 日時、送信元 IP アドレス、送信先 IP アドレス<br>-プロキシサーバーのログ(6 カ月)<br>取得項目 : 日時、リクエスト元 IP アドレス、URL<br>-リモートアクセスのログ(6 カ月)<br>取得項目 : 日時、接続元 IP アドレス、ユーザーID<br>-認証サーバーのログ(6 カ月)<br>取得項目 : 日時、接続元 IP アドレス、ユーザーID、成功/失敗<br>-エンドポイント(パソコン、サーバー)の操作ログ(6 ヶ月)<br>取得項目 : 日時、ホスト名、ユーザーID、IP アドレス、操作内容<br>※クラウドサービスの利用も対象に含む<br>※クラウドサービスを利用しており保管期間の規則を満たせない場合はリスクに応じて期間を各社で判断 |
| | | | 144 | 任意 | 重要なシステムについて、アプリケーション操作ログを取得している | 【規則】<br>・ユーザー、管理者の操作ログを取得すること<br>[対象]<br>-重要なシステム　※対象はリスクに応じて各社判断<br>[取得するログの項目]<br>-ユーザーID、タイムスタンプ、操作内容(ログイン、ログアウト、追加・削除などの操作)<br>[保管期間]<br>-6 カ月<br>※クラウドサービスを利用しており保管期間の基準を満たせない場合はリスクに応じて期間を各社で判断 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | 標的型攻撃など、サイバー攻撃による被害を抑制させるため、サイバー攻撃を速やかに検知、遮断する対策を行っていること | 145 | 必須 | 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】<br>・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<br>［分析対象］<br>−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<br>［監視時間］<br>−24 時間/365 日<br>［機能要件］<br>−インシデントアラートが即時発報されること<br>−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 |
| | | | 146 | 必須 | 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】<br>・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 |
| | | | 147 | 任意 | インターネットに公開しているWebサイトについて、サイトの改ざんを検知する仕組みを導入し、定期的に確認している | 【規則】<br>・Web サイトの改ざんを検知する仕組みを導入すること<br>【対象】<br>−重要な社外公開 Web サイト |
| 24 バックアップ・復元(リストア) | システム停止、データ消失による業務影響を極小化するとともに、早期の業務復旧を実現する | サイバー攻撃に対して重要情報の被害やシステム稼働の影響を最小限に留める対策を行っていること | 148 | 必須 | 適切なタイミングでバックアップを取得している | 【規則】<br>・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<br>・バックアップはランサムウエア等に暗号化されないような安全な場所（外部記録メディア等）で保管すること |
| | | | 149 | 必須 | 復元(リストア)手順を整備している | 【規則】<br>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 |
| | | | 150 | 必須 | 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】<br>・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<br>［対象］<br>−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<br>※対象はリスクに応じて各社判断<br>［対策例］<br>−アナログツールの利用(FAX など)<br>−クラウドサービスなどの外部情報システムの利用 |

| ラベル | 目的 | 要求事項 | No. | 回答対象 | 達成条件 | 達成基準 |
|---|---|---|---|---|---|---|
| | | | 151 | 必須 | 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】<br>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<br>【対象】<br>重要なデータ・システム<br>【頻度】<br>システム構築時、変更時、定期的(リスク応じて判断) |
| | | | 152 | 必須 | 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】<br>・火災、水害、停電に対する対策を行うこと<br>・温湿度管理を行うこと |
| | | セキュリティインシデントを想定し事業継続の要件に沿う復旧に必要なデータを準備できていること | 153 | 必須 | 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】<br>・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<br>・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<br>【対象」<br>事業継続上重要なシステム |

## 6. お取引先様への依頼事項

(1) 情報セキュリティ対策および自己診断の実施

お取引先様には、本対策基準に定める対策の実施および定期的な実施状況の自己診断（別紙「お取引先様向け情報セキュリティ対策チェックシート」を使用）をお願いするとともに、当社からの要請があった場合は、自己診断結果データ（Excel ファイル）の提出にご協力のほどよろしくお願い致します。

なお、本対策基準の実施に関し、お取引先様における対策の実施状況が、当社が定めたレベルに到達しない場合、当該取引先様との機密情報の共有を制限させていただく場合がございます。

(2) 監査への対応

当社は、対策の実施状況を確認するために、監査を実施させていただく場合があります。当社からの要請があった場合は、監査にご協力のほどよろしくお願い致します。

## 7. その他

本基準は、情報セキュリティを取巻く世の中の状況の変化や社内規定の改訂等に伴い、適宜見直し、改訂致します。

以上

2017 年 12 月(V1.0)初版
2022 年 10 月(V2.0)改訂
2024 年 11 月(V2.1)改訂