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

2017 年 12 月

株式会社クボタ

1. はじめに

本対策基準は、CSR 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 CSR 調達ガイドライン」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

情報セキュリティは、“組織的”、“人的”、“技術的”、“物理的”の 4 つの観点で対策状況を確認し、継続的に改善に繋げることが重要です。

お取引先様に求める情報セキュリティ対策基準を以下に示します。

お取引先様に求める情報セキュリティ対策基準

[組織的対策]

項目		基準
1	情報セキュリティ管理体制	情報セキュリティ管理体制を構築し、責任と役割が明確になっており、それが明文化され、従業員に周知している
2	情報セキュリティ関連規程類	情報セキュリティ関連の基本方針（ポリシー）や対策基準等が整備されており、それが明文化され、従業員に周知している

項目		基準
3	委託先管理（再委託）	貴社が委託先に機密情報を共有する場合、貴社が当社に負うのと同じ秘密保持義務を委託先に負わせている
4		貴社が委託先に機密情報を共有する場合、受け渡しを記録し、管理している
5	機密情報の明確化	機密情報（機密情報を複製・複写したものも含む）が台帳管理されており、明確になっている
6		機密情報は他の情報と区別して保管している
7	機密情報の持出し管理	① 原則、機密情報の社外持出し（メールのようなネットワーク経由の送付等も含む）を禁止している ② 業務上社外持出しが必要な場合は、以下の全ての対応を含めた、持出しルールを策定している 1）機密情報を持出す場合は、管理責任者の承認を得たうえで、台帳管理する 2）電子化されている場合は、暗号化等の情報漏えい対策を実施する 3）部外者の目に触れないように注意するとともに、常に傍を離れないようにする
8	社外への情報発信	社外発信する情報について、審査・承認するプロセスを定めている
9	社外サービスの利用	レンタルサーバやクラウドサービス等の社外サービスを利用する場合の選定基準を定めており、社内の情報セキュリティ基準と同等、もしくはそれ以上であることを確認している
10	情報セキュリティ事故・事件対応	ウイルス感染や機密情報の漏えい・流出等の情報セキュリティ事故・事件発生時の対応手順や対応体制が明確になっており、それが明文化され、従業員に周知している
11	監査	情報セキュリティ監査等を実施し、定期的（年１回以上）に情報セキュリティ管理状況を確認しており、確認された問題点については、適切に改善している
12		貴社が委託先に機密情報を共有する場合、委託先に対しても貴社と同等の情報セキュリティ管理を要請している
13		委託先を訪問し、実地確認を実施している

［人的対策］

項目		基準
14	教育・研修	全従業員に対して情報セキュリティ教育や研修が定期的（年１回以上）に実施されており、その受講状況を記録・保管している
15		貴社が委託先に機密情報を共有する場合、委託先に対しても貴社と同等の情報セキュリティ教育や研修が定期的（年１回以上）に実施されるように要求している
16	機密保持誓約書の取得	就業規則等に機密保持の項目を設け、従業員から機密保持の誓約書を取得している
17		貴社が委託先に機密情報を共有する場合、委託先に対しても、委託先従業員から貴社と同等の機密保持の誓約書を取得することを要求している

［技術的対策］

項目		基準
18	アカウント・パスワード管理	機密情報には、適切なアクセス権を設定する等し、業務上情報を知る必要がある人のみが取り扱えるようにしている
19		アカウント(システム、サーバのユーザ ID 等)は個人ごとに付与され、推測されにくい十分長いパスワード（8 桁以上）が設定されるような仕組みになっている
20		従業員の入社、退職、異動等に伴うアカウントの発行・登録・削除や定期的な棚卸(年 1 回以上)等に関するルールや手順が明確になっており、それが明文化されていると同時に適切に運用している
21	ネットワークセキュリティ	社内ネットワークは、ファイアウォール等のネットワーク機器により、インターネット等の社外ネットワークと分離しており、かつ社外ネットワークから社内ネットワークに接続できないよう、適切なアクセス制限を実施している
22	ぜい弱性対策	パソコンやサーバ、スマートデバイス（スマートフォンやタブレット）等で使用する OS に対して、常に最新のセキュリティ更新プログラム（セキュリティパッチ）を適用している
23		パソコンやサーバ、スマートデバイス等で使用するソフトウェアに対して、常に最新のセキュリティ更新プログラムを適用している
24	不正プログラム対策	パソコンやサーバ、スマートデバイス等にウイルス対策ソフトウェアを導入しており、常に最新のパターンファイル（検知・防御ルール）で防御可能な状態になっている
25		パソコンやサーバ、スマートデバイス等に保管されている全てのファイルに対して、ウイルス対策ソフトウェアによる検査（フルスキャン）が定期的（週 1 回以上）に実施している
26		ウイルス感染時の被害を最小化するための対応手順（ネットワークからの切断等の初動対応や報告方法等）が明確になっており、それが明文化され、従業員に周知している
27		情報漏えいリスク等の観点から使用を禁止するソフトウェアが明確になっており、それが明文化され、従業員に周知している
28		情報漏えいリスク等の観点から使用を禁止するソフトウェアを使用していないことを定期的（毎日）に確認している
29		Winny（ウィニー）等のファイル共有・交換ソフトの使用を禁止にしている
30	インターネット・メール利用	業務上関係のないウェブサイトへのアクセスを制限する仕組みを導入している
31		会社が許可していないメールアドレスやオンラインストレージサービス※等の使用を禁止している ※インターネット上のファイル共有サービス(Google ドライブ、OneDrive 等)
32	私有機器の利用制限	私有パソコンや私有スマートデバイス、私有情報記憶媒体（USB 等）等を業務で使用させず、会社が貸与した許可された情報機器のみ使用させている
33	情報記憶媒体の利用	業務で使用してもよい情報記憶媒体を指定し、使用状況を管理台帳等で管理している
34	機密情報の管理	機密情報は、所定のサーバやシステム等でのみ管理し、アクセス制御等の適切なセキュリティ管理を実施している

項目		基準
35	機密情報の消去	パソコンやサーバ、スマートデバイス、情報記憶媒体を廃棄する場合は、保存されたデータの復元が不可能になるよう、内部の情報を完全に消去するデータ消去ツール等を使用している。または、物理的に破壊している。
36		廃棄を産業廃棄物業者等の外部業者に委託する場合、その外部業者と機密保持契約を締結している
37		当社からの依頼に基づき、当社へ廃棄証明を提出できる
38	ログ管理	機密情報へのアクセスログ（いつ・誰が・どのような操作を実施したのか等）を取得し、貴社で定めた期間で適切に保管している
39	バックアップ	機密情報は適切にバックアップを取得しており、かつ取得したバックアップについても、アクセス制御等の適切なセキュリティ管理を実施している

［物理的対策］

項目		基準
40	入退室管理	機密情報を保存するサーバやシステム等の設置場所に出入り可能な人を制限する施錠等の物理的な対策が備わっている
41		機密情報を保存するサーバやシステム等の設置場所への出入りを管理台帳等で管理している
42		機密情報を保存するサーバやシステム等の設置場所へ持ち込む機器については、事前に必要性や妥当性を確認している
43	機密情報の施錠管理	印刷された機密情報（設計図面情報等）や機密情報から作成された物（金型等）は、業務上情報を知る必要がある人のみが取り扱えるように、施錠保管している

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、改訂を行います。

以上

2017 年 12 月初版