セキュリティチェックシート

お客様各位

当社はISMS認証を取得しており、社内で情報セキュリティに関するルールを定め、運用しております。
情報セキュリティレベルを開示することで、お客様の安心と信頼に応えられればと考えております。
弊社サービスのご契約の際や、お客様のISMSやプライバシーマークの外部委託先としてご判断する際に、
必要に応じてお役立ていただけますと幸いです。

株式会社KDDIウェブコミュニケーションズ
2022年 7月 1日
情報セキュリティ委員会
委員長　大縄　陽一

	管理項目	管理実施状況	備考・補足
全社共通			
1. 情報セキュリティに対する基本方針			
1-1	経営陣による個人情報保護方針および情報セキュリティ基本方針を策定し、従業員および外部へ公開しているか	○	
1-2	情報セキュリティ基本方針は予め定められた間隔、または組織内外に重大な変化が発生した場合に、見直しを実施し、組織の状況に応じた最新の情報セキュリティ基本方針として維持しているか。	○	
2. 情報セキュリティに対する組織的な取り組み状況			
順守			
2-1	事業活動に関連する法令・規制、契約上の取り決めを把握し、順守しているか。	○	
2-2	知的財産権および登録商標が存在するソフトウェア製品を利用する場合、関連法令を順守するための手順を定めているか。	○	
2-3	事業活動を行う上で重要な記録を、法令・規制、および契約によって定められたとおり、適切に保護しているか。	○	
2-4	個人データおよび個人情報を個人情報保護法など関連法令を順守し、適切に取り扱っているか。	○	
2-5	暗号化機能を用いた製品などの輸出入など、暗号化機能の取り扱いについて、関連法令を順守しているか。	×	当社は暗号化機能に対する規制の影響を受ける事業、業務がないため
2-6	経営者は情報セキュリティマネジメントシステムについて、定期的なレビューを実施しているか。	○	
2-7	管理者は、各セキュリティ対策について、従業員が正しく実施しているか管理を行っているか。	○	
2-8	情報処理システムに対し、定期的にセキュリティに対する脆弱性検査を実施しているか。	○	
情報セキュリティのための組織			
2-9	情報セキュリティ対策に係る役割および責任を定め、明記しているか。	○	
2-10	情報セキュリティインシデント発生における、被害者への連絡や外部への周知方法、関係当局への連絡方法について定めているか。	○	
2-11	情報セキュリティ環境の理解や、情報セキュリティレベルの維持のため、外部の研究機関や専門組織への参加や、連絡体制を構築しているか。	○	
2-12	プロジェクトにおいて、各プロジェクトの特性に応じた情報セキュリティ対策を明確にし、実施しているか。	○	
2-13	職務と責任範囲を分離し、不正使用や変更などの危険性をの低減を実施してているか。	○	
2-14	モバイル端末利用における方針を定め、セキュリティ対策を講じているか。	○	
2-15	テレワーク利用における方針を定め、セキュリティ対策を講じているか。	○	
従業員の雇用			
2-16	従業員の雇用時に、その資質や能力を見極めるよう選考を実施しているか。	○	
2-17	従業員を雇用する際に、守秘義務契約や誓約書を交わしているか。	○	
2-18	従業員に対し、雇用の終了や契約内容の変更度も、その責任は一定期間有効であることを定めているか。	○	
2-19	経営陣は従業員に対し、情報セキュリティ方針や手順に従ったセキュリティの適用の実施について示しているか。	○	
2-20	従業員に対し、情報セキュリティに関する教育・訓練の機会を定期的に与え、順守すべき事項やその必要性について理解をさせているか。	○	
2-21	情報セキュリティ違反時の懲戒手続きが整備されているか。	○	
3. 情報資産の管理			
情報資産に関する責任			
3-1	情報および情報処理施設を特定し、資産目録として作成し、維持しているか。	○	
3-2	応報資産の管理責任者を定めているか。	○	
3-3	情報資産単位に利用制限を明確に定め、実施しているか。	○	
3-4	従業員の雇用終了時に、従業員の所持する当社の資産を回収しているか。	○	
情報の分類			
3-5	情報を重要度に応じて分類しているか。	○	
3-6	情報に対し、その重要性を認識できるようラベル付を行っているか。	○	
3-7	資産の取り扱い方法を定めているか。	○	
媒体の取扱い			
3-8	モバイルPCやUSBメモリなどの記憶媒体の取り扱いについて、盗難や紛失などに備え、適切なパスワード設定や暗号化などの対策を実施しているか。	○	
3-9	不要な媒体の処分について、処分手順を定め、実施しているか。	○	
3-10	情報資産に対する配送中の紛失や漏洩から、情報を保護するための手順を定めているか。	○	

4.物理的なセキュリティ			
物理的領域に対するセキュリティ			
4-1	接触式電子錠や有人による入退室管理を実施しているか。	○	
4-2	セキュリティを保つ領域への入退室管理手順を定めているか。	○	
4-3	オフィスなどの執務スペースにおけるセキュリティ基準を定めているか。	○	
4-4	地震などによる転倒防止、自動火災報知機の設置、停電時の代替電源の確保等を情報資産の保護のために実施しているか。	○	
4-5	セキュリティ区画での作業に関する、物理的な保護および指針を定め、実施しているか。	○	
4-6	荷物等の受け渡し場所を定め、外部の者の立ち入りを最小限に抑えているか。	○	
装置に対するセキュリティ			
4-7	情報資産を格納する設備は、許可された人だけが入ることができる安全な場所に設置しているか。	○	
4-8	情報資産を格納する設備は、停電や漏水などから保護しているか。	○	
4-9	電源や通信ケーブルなどは、許可されていない他の人が容易に接触できないよう設計してあるか。	○	
4-10	情報資産を格納する設備に対し、完全性、可用性を維持するための保守作業を実施しているか。	○	
4-11	情報資産や装置の持ち出し規定を定め、実施しているか。	○	
4-12	情報資産や装置を利用する場合の規定を定め、実施しているか。	○	
4-13	記憶媒体を内蔵した装置の処分や再利用について手順を定め、実施しているか。	○	
4-14	無人状態で稼働するPCの保護手順を定めているか。	○	
4-15	重要な情報が存在する机上、書庫、会議室などは整理整頓を実施しているか。また、ディスプレイに対するクリアスクリーン方針を適用しているか。	○	
5.情報システムおよび通信ネットワークの運用管理			
暗号の利用			
5-1	情報保護のための暗号化に関する利用方針を定め、実施しているか。	○	
5-2	暗号化に必要な秘密鍵の管理方法について定め、実施しているか。	○	
運用におけるセキュリティ			
5-3	操作手順書を作成し、従業員が利用可能な状態にしているか。	○	
5-4	情報セキュリティに影響を与える、業務プロセス、処理システム等の変更に関する手順を定め、実施しているか。	○	
5-5	情報処理システムの運用状況について点検を行っているか。	○	
5-6	システム試験および開発環境と本番環境は分離して運用を実施しているか。	○	
5-7	マルウェアの感染に関し適切な対処（ウイルス対策ソフトの導入や脆弱性の解消等）を実施しているか。	○	
5-8	重要な情報に対するバックアップの取得を実施しているか。	○	
5-9	情報処理システムにおいて発生した障害、セキュリティ関連イベントについてログを取得しているか。	○	
5-10	取得したログが改ざんや不正アクセスなどの脅威から保護されているか。	○	
5-11	情報処理システムに対する管理者や運用担当者の作業の実施ログを取得しているか。	○	
5-12	情報システム内の時刻は、単一の時刻同期サーバーと同期しているか。	○	
5-13	ソフトウェアの導入において、セキュリティレベルを定義した導入ポリシーを定めているか。	○	
5-14	脆弱性情報や脅威に関する情報の入手方法を定め、実施しているか。	○	
5-15	Winny等、組織で許可されていないソフトウェアのインストールの禁止、あるいは使用制限を行っているか。	○	
5-16	システム監査は業務プロセスの中断を最小限に抑えるよう計画しているか。	○	
通信におけるセキュリティ			
5-17	重要な情報の通信を行う場合は、暗号化通信を用いているか。	○	
5-18	ネットワークサービスに関するセキュリティ上の要求事項を特定し、ネットワークサービスの利用時にこれら要求事項を盛り込んでいるか。	○	
5-19	保護すべき重要な情報が保存されるシステムは、それ以外のシステムが接続しているネットワークから物理的に遮断する、もしくはセグメント分割することによりアクセスできないようにするなどの対策を講じているか。	○	
5-20	通信タイプを問わず、情報の転送や交換に関する利用方針や手順を定めているか。	○	
5-21	外部組織との情報交換において、事前に情報交換の方法を定めているか。	○	
5-22	社外秘以上の情報を電子メールやアップロードサイト等で送信する場合の手順を定め、実施しているか。	○	
5-23	情報保護のために秘密保持契約または守秘義務契約の要件を特定し、定期的にレビューを実施しているか。	○	

6.情報システムのアクセス制御の状況および情報システムの開発、保守におけるセキュリティ対策			
アクセス制御			
6-1	重要な情報に対するアクセス管理方針を定め、明文化しているか。また、その内容のレビューを実施しているか。	○	
6-2	接続可能なネットワークや、ネットワークへの接続許可の承認等、ネットワークを用いた利用に関する利用方針を定め、実施しているか。	○	
6-3	アクセス権の割当について、従業員の登録および削除に関する手順を定め、実施しているか。	○	
6-4	ユーザーIDに対するアクセス権の割当および無効化の手順を定め、実施しているか。	○	
6-5	特権的アクセス権の割当およびその使用について、手順を定めているか。また、割り当てた特権アクセス権について管理をしているか。	○	
6-6	パスワード等の秘密認証情報の割当について、受け渡し方法、作成規則について手順を定め、実施しているか。	○	
6-7	アクセス権の定期的な見直しを実施しているか。	○	
6-8	従業員の雇用終了や、異動にあわせて、アクセス権の削除や修正を実施しているか。	○	
6-9	パスワード等の秘密認証情報の利用方法について、従業員に対し規定に従うよう示しているか。	○	
6-10	情報に対し不必要なアクセスが行われないよう、アクセス制限を実施しているか。	○	
6-11	ログオンの成功や失敗の記録や、パスワードの表示方法など、セキュリティを考慮したログオン手順を定め、実施しているか。	○	
6-12	パスワードの定期的な見直しを行うとともに、適切なパスワード（文字数／文字種の考慮したパスワード）の運用管理を実施しているか。	○	
6-13	アプリケーションやオペレーションシステムの制御を無効化するユーティリティプログラムの使用について、明確な手順を定め、管理を実施しているか。	○	
6-14	プログラムソースコードへのアクセス権限は、制限されているか。	○	
開発および保守			
6-15	情報処理システムの導入や改善時に、情報セキュリティに対する要求事項を含めているか。	○	
6-16	電子商取引等の契約情報について、情報の暗号化やデジタル署名の利用など適切な保護を行っているか。	○	
6-17	電子商取引等の決済情報について、情報の暗号化やデジタル署名の利用など適切な保護を行っているか。	○	
6-18	ソフトウェアおよびシステム開発の規則を定め、適用しているか。	○	
6-19	システムの変更手順を定め、実施しているか。	○	
6-20	ソフトウェアおよびシステムの変更を行う場合、評価試験を実施しているか。	○	
6-21	パッケージソフトウェアの改修は抑止しているか。また、改修箇所を管理しているか。	○	
6-22	システム構築における原則を定め、すべての情報システムへの実装を行っているか。	○	
6-23	セキュリティに考慮した開発環境を構築しているか。	○	
6-24	外部委託によるソフトウェア開発に対しマネジメントを実施しているか。	○	
6-25	リリース前にセキュリティ機能の試験を実施しているか。	○	
6-26	システムの受け入れ手順を定めているか。	○	
6-27	試験結果やログなどの情報を管理しているか。	○	
7.外部組織の管理			
セキュリティレベルの合意			
7-1	外部委託先等が当社情報資産へアクセスする際の規定を定めているか。	○	
7-2	外部委託先等と法的義務およびSLAを含む契約上の義務、制限等に関する取り決めを定めているか。	○	
7-3	再委託先に対する情報セキュリティ要求事項の順守を実施しているか。	○	
サービスレベルの合意			
7-4	第三者サービスの品質について、定期的な監査を実施しているか。	○	
7-5	第三者サービスの変更が、当社が要求するサービス品質から逸脱しないよう管理しているか。	○	
8.情報セキュリティ上の事故対応			
8-1	情報セキュリティインシデントに対する体制および責任を定めているか。	○	
8-2	情報セキュリティ事象発生時の報告経路が整備され、周知されているか。	○	
8-3	システムやサービスに対する情報セキュリティ上の脆弱性を記録し、報告を実施しているか。	○	
8-4	情報セキュリティ事象を情報セキュリティインシデントと分類するフローを定めているか。	○	
8-5	情報セキュリティインシデントに対する手順を定めているか。	○	
8-6	発生した情報セキュリティインシデントを分析し、教育や規程の更新などの予防処置へと役立てているか。	○	
8-7	情報セキュリティインシデントの証拠を収集し、保全するよう定めているか。	○	
9.事業継続			
9-1	事業を中断する可能性のある事象に対処する体制および手順を定めているか。	○	
9-2	事業を中断する可能性のある事象に対処する計画を立案しているか。	○	
9-3	事業を中断する可能性のある事象に対し、計画通りの対処が可能か検証を実施しているか。	○	
9-4	重要な情報処理システムは可用性を考慮した冗長構成などの対策を実施しているか。	○	
10.クラウドサービスの利用			
10-1	クラウドサービス利用に対して経営陣による認可プロセスを定め、実施しているか。	○	
10-2	クラウドサービス上の資産を明確に識別したうえ、重要な資産すべての目録を作成し維持しているか。	○	
10-3	利用するクラウドサービスに対し、その管理責任者を指定しているか。	○	
10-4	クラウドサービス利用者は、個人ごとに一意な識別子（利用者ID）を保有し管理しているか。	○	