ペライチ

2024年9月26日

本資料は株式会社ペライチのセキュリティ状況についてまとめ、そのセキュリティ対策を記載したものです。
ペライチ株式会社は情報セキュリティマネジメントシステムSO/IEC27001 認証登録番号 IS 790026 を保有しています。

外部認証		備考
1	外部認証機関の認証(Ｐマーク、ＩＳMS、ＳＡＳ70等)がある。	株式会社ペライチはISMS認証(ISO 27001)を取得しています。認証番号：IS 790026
力量管理		**備考**
2	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、全社に共有されている。	情報セキュリティに関する基本方針やポリシーを策定し、全社に共有しています。詳細はポリシーページにて公開されています。URL：https://peraichi.com/pages/security https://peraichi.com/pages/policy
3	業務従事者に対し、機密情報保護・情報セキュリティに関する教育・訓練を継続的(1年に1回以上等)に実施している。	定期的な情報セキュリティ教育を対象従業員を定め、対象従業員に対して実施しています。特にISMSの範囲に含まれる者には年1回以上の教育が義務付けられています。
ソフトウェア管理		**備考**
4	悪意ある外部サイトへの社内からの通信を遮断するために、ファイアウォールを設置している	ネットワーク内の機器及びサーバに対して、ファイアウォールが設定されています。
5	ファイルサーバ等に保管する情報の重要度に応じて、機密情報へのアクセスを適切に制御している。	機密情報へのアクセスは、業務上必要な者だけに権限が設定されており、必要なアクセス権限の見直しも行われています。
6	ソフトウェアを利用する場合は、事前に利用規約などを確認し、規約に違反する利用を防止している。	
情報管理		**備考**
7	機密情報は、他の情報と区別して保管している。	機密情報は、厳格なアクセス制御の下で、他の情報と区別して保管されています。また、保管方法については定期的に見直しが行われています。
8	機密情報を記録する可搬媒体や紙媒体は、施錠された書庫等に保管している。	機密情報が記録された可搬媒体や紙媒体は、施錠された書庫に保管されることを義務付けています。また、廃棄時にはシュレッダーやデータ消去後の物理破壊を実施しています。
9	情報セキュリティに関するインシデントが発生した際の検知・報告・通報の仕組みを整えている。	情報セキュリティインシデント発生時には、速やかに担当部署に報告し、適切な対応が取られる仕組みが整えられています。
10	監視・測定を実施し、情報セキュリティに関する規程の遵守状況の確認を行う。	定期的な監査が実施され、情報セキュリティ規程の遵守状況を確認しています。また、監査結果は適切に記録され、見直しを行っています。
11	業務で用いるパスワードの桁数は14桁以上とし、複数の文字種(数字、アルファベット、記号)を混在させる。	業務で用いるパスワードは14桁以上とし、複数の文字種を混在させるパスワードポリシーを設定しています。
12	故障に備え、情報は、社が指定するクラウドサービスへ保存する。	重要な情報は定期的にクラウドサービスにバックアップされており、バックアップの世代管理も行っています。
13	自社に関連する法令や規制を洗い出し、法規制リストにまとめる。	自社に関連する法令や規制を定期的に洗い出し、法規制リストとして管理しています。
14	情報セキュリティインシデント(もしくはその疑い)を発見した場合は、速やかにISMS担当者に報告する。	情報セキュリティインシデント発生時には、速やかにISMS担当者に報告し、対応が行われるような仕組みを整えています。
15	情報セキュリティインシデントに対する対応の結果や、インシデントの証拠となるようなログは、記録して保管する。	対応の結果や証拠となるログは適切に記録され、定められた期間保管しています。

16	情報セキュリティに関する規程を作成し、トップマネジメントの承認を得る。	情報セキュリティに関する規程は、トップマネジメントの承認を経て策定され、全社に共有されます。
17	情報セキュリティの推進のために、「トップマネジメント」「ISMS責任者」「ISMS担当者」「内部監査責任者」「内部監査員」を選任する。	情報セキュリティの推進及び管理のために、明確な役割を持つ担当者を選任しています。
18	年1回、内部監査を実施し、情報セキュリティに関する規程の遵守状況の確認を行う。	情報セキュリティに関する内部監査は年1回以上実施され、規程の遵守状況を確認しています。また、監査結果は適切に記録され、次回の監査に反映されます。
19	パスワードが不要なフリーWi-Fiや、提供元がわからないWi-Fiに接続しない。	業務上、パスワードが不要なフリーWi-Fiや提供元が不明なWi-Fiへの接続は禁止しています。
20	執務エリア内での写真撮影は、情報の映り込みに十分に注意する。	写真撮影時の情報の映り込みは十分に注意をしています。
端末管理		**備考**
21	運用を行う端末(クライアントPC)でウイルス対策アプリケーションの随時更新を実施している。	運用端末にはウイルス対策ソフトが導入されており、随時更新が実施されています。
アクセス権限の管理とレビュー		**備考**
22	機密情報およびそれを扱う情報システムは、最小権限の原則に基づき、業務上必要な人のみにアカウント付与・アクセス権限の限定を行う。	情報システムへのアクセスは、最小権限の原則に基づいて厳格に管理されており、業務上必要な人にのみアカウントやアクセス権限が付与されています。
23	特権的アクセス権(管理者権限や、管理者ユーザーを含む)の付与は、必要最小限とする。	特権的アクセス権の付与は必要最小限に留められており、定期的な見直しが行われています。また、権限の付与・変更・削除は厳格に管理されています。
暗号化		**備考**
24	インターネットブラウザを介して情報を送信する場合は、暗号化された通信(https通信など)を利用する。	ブラウザを介しての情報送信には暗号化された通信を利用しています。
ユーザー認証とアクセス権限の管理		**備考**
25	開発者の本番環境へのアクセスを制限している。	開発者の本番環境へのアクセスは厳格に制限されており、不必要なアクセスが発生しないように管理されています。
26	2要素認証を使用している。	システムへのアクセスには2要素認証が導入されています。
27	アカウントは一元的に管理されている。	ユーザーアカウントは一元的に管理されており、アカウントの作成、変更、削除が適切に行われています。
28	退職者のアクセス権限は適切に管理、削除されている。	退職者のアクセス権限は速やかに削除されており、これにより不要なアクセスが発生しないように管理されています。
パスワードポリシーと認証方法の適用		**備考**
29	サービス環境へのログインにパスワードポリシーを設定している。	サービス環境へのログインにはパスワードポリシーが設定されており、複雑なパスワードの使用が義務付けられています。
データの暗号化と伝送時のセキュリティ		**備考**
30	データベースのデータは暗号化して保管されている。	データは暗号化されて保管されており、これによりデータの安全性が確保されています。
31	不正なアクセスを検知するようなシステムを導入している。	不正なアクセスを検知するためのシステムが導入されており、異常が検出された場合には迅速な対応が可能です
クラウドストレージのデータ保護		**備考**
32	データについて、障害時やサイバー攻撃に備え適切なバックアップを取得している。	重要なデータは定期的にバックアップが取得されており、障害時やサイバー攻撃からの復旧が迅速に行える体制が整えられています。

33	バックアップからのレストア手順は確立されている。	適切に保存されたバックアップデータからのレストア手順については確率されています。
パッチ管理とソフトウェアアップデート		**備考**
34	システムの変更は適切にテストされ、承認されている。	変更管理プロセスは定期的に見直されています。
35	システムの変更について証跡をとり、適切に管理している。	システムの変更はすべて記録され、証跡が適切に管理されています。
ログ記録と監視		**備考**
36	アクセスログは適切の管理し、一定期間保管している。	アクセスログは適切に管理され、定められた期間保管されています