情報セキュリティ個別方針

当社は、情報セキュリティマネジメントシステムの確実な運用を行うために、情報セキュティ個別方針を策定し、ここに提示します。

1．モバイル機器の方針
・会社支給のモバイル機器の利用については、社内利用時、持ち出し時、社外利用時等において、その取扱い手順を定め、管理、運用します。
・私有のモバイル機器の業務利用を禁止します。

2．テレワーキングの方針
・テレワーキングについては、場所、情報の種類及びアクセス方法等のセキュリティに影響を与える項目を考慮し、適切なセキュリティ対策を個別に実施します。
・会社貸与の PC 又はモバイル機器以外での業務を禁止します。
・情報セキュリティインシデントの疑いが発生した場合には、可及的速やかに報告し、インシデント拡大防止策を実施します。

3．アクセス制御方針
・情報資産については、不正利用や誤使用等の不適切なアクセスから保護するため、情報資産の機密レベルと利用者の役割（所属部門、職務及び職位）に応じてアクセス権を適切に設定し、管理、運用します。

4．暗号による管理策の利用方針
・特にセキュリティを要求される業務については、情報の暗号化を図ります。

5．暗号鍵に関する方針
・暗号鍵については、業務担当者とプロジェクトの外部の関係者及び顧客間で秘密に処理し、当事者以外がアクセス出来ないように管理します。

6．クリアデスク・クリアスクリーン方針
・業務情報を含んだ書類や取り外し可能な記憶媒体を机の上や複合機などに放置しません。
・PC の画面上に重要な情報を表示したまま離席しません。
・PC がシステムにサインインした状態のまま離席しません。

7．バックアップ方針
・情報資産の完全性と可用性を保護するため、情報資産の重要性及び機密性を考慮して適切なバックアを実施します。
・バックアップの頻度、保管期間、タイミング及び手順等は、事業上の要求事項を考慮して決定します。
・バックアップデータは他の機密情報と同様に厳重に管理、保管します。
・バックアップが行われているか、定期的に監視します。
・データの復旧が可能か定期的に確認作業を実施します。

8．情報伝送の方針

・情報の伝送方式については、電子メールや郵送等のあらかじめ定めた方式の中から受信者と合意したものを選択します。

・あらゆる情報資産の交換（物理的配送、電子メール及びFAX等）においては、情報漏洩や改竄等のリスクを認識した上で適切な対策を確立、実施します。

9．セキュリティに配慮したシステム開発方針

・セキュリティに配慮したソフトウェア及びシステム開発のための基準を定め、適切な開発を実施します。

１０．供給者関係のための情報セキュリティの方針

・当社の特定の業務の一部または全部を外部委託する場合や第三者が提供するサービスを利用する場合には、情報セキュリティ要求事項について供給者と合意し、文書化します。

１１．技術的ぜい弱性の管理方針

・利用中の情報システムにおけるぜい弱性（セキュリティホール）に係る情報を常に収集、評価し、プログラムのパッチを適用します。

2024年1月29日

公益財団法人日本分析センター

理事長　川原田 信市