\Orchestrating a brighter world NEC

池田糖化グループ

セキュリティハンドブック

２０１９年4月1日 第1版

池田糖化グループ基本ルール～日常業務時

社内LANパソコン、モバイルPC、スマートデバイス使用時の注意事項

- 業務で使用可能なITSが使用を許可した社有品のみ使用可能
- 私有品の業務使用不可
- 許可されたことを示すシール貼付必須
- 修理・返却を依頼する場合は、ITSに連絡、相談する

社内LANパソコン、モバイルPCの使用の注意事項

- 社有のPCに私有品（USBメモリ、スマートフォン等）の接続は不可

マルウェア対策

- マルウェア対策ソフトの常駐、監視、ウイルス定義データベースの最新化
- マルウェアに感染した場合
  - ネットワークから速やかに切り離す
  - LANケーブルの抜線
  - 無線通信機能（Wi-Fi、Bluetooth）および通信事業者が提供する通信（モバイル通信）をオフにする
  - ITSに速やかに連絡し、対応方法について指示を仰ぐ

池田糖化グループ基本ルール～日常業務時

電子媒体使用時の注意事項

- 業務で使用可能なITSが使用を許可した社有品のみ使用可能
  - デジタルカメラの備品として装着している部署で調達したSDカード（micro SDカード含む）、DVD-Rなどのディスクメディアの使用は可能
- 私有品の業務使用不可
- USBメモリ、HDD、SSDの廃棄は各自で行わず、必ずITSへ送付する
- USBメモリ、HDD、SSD以外の重要情報が記録された電子媒体（ディスクメディア等）を廃棄する際は、データが読み出せないようにメディアシュレッダーで処分する
- データが読み出せないように破壊することが困難な場合は電子媒体をITSへ送付する

部門共有の電子媒体使用時の注意事項

- 使用部門にて管理者を決定し、台帳などで管理する
- 使用記録を残すことを推奨する
- 重要情報（電子データ）を保存する際はITSが定めた手段でデータを暗号化する
- ウイルス対策ソフトでスキャンし、問題がないことを確認した上で使用する
- 使用完了後、速やかに保存しているデータを消去し、部門で管理している所定の場所に保管する

池田糖化グループ基本ルール～日常業務時

スマートデバイス使用時の注意事項

- パスコード
  - ITSの指示に従い、各自が設定する（パスコード≠社員番号）
  - 第三者に開示しない
- ロック機能
  - 有効にし、第三者が無断で使用できないようにする
  - 一定時間未使用時に自動的に画面をロックするよう設定する（推奨時間３分）
  - ロック画面上に表示する通知などの情報は最小限にする
  - アプリ自体がロック機能を持っている場合は、それも有効にする
- スマートウォッチ、スマートバンドと会社支給のスマートデバイスの連携
  - 連携に使用するアプリは、App Storeで公開されているアプリのみとする
  - 以下を認識の上使用する
    - スマートウォッチやスマートバンドの中には、収集した情報を外部に送信、保管しているものがある
    - 個人情報保護に対する取り組みが適切ではないベンダーによる製品も存在する
    - 使用に伴い、当社に不利益が生じた場合、使用者に責任を問う可能性がある

池田糖化グループ基本ルール～日常業務時

スマートデバイス使用時の注意事項

- データ転送および充電
  - データ転送は、使用が許可された外部サービス経由で行う
  - 初期設定およびバックアップ・リストア、OSアップデート、充電等を除き、社内LANパソコンへのデータ転送を目的としたケーブル接続は禁止する
  - 社有のスマートデバイスを私有PC等に接続しない
  - ストレージ機能を有するカードリーダー等、社有品であっても許可されていない周辺機器を接続しない

池田糖化グループ基本ルール～日常業務時

社内情報機器使用のためのIDの注意事項

- 社内システム等の使用にIDが必要な場合は申請する
- ID、パスワードはその使用者が適切に管理する必要がある
  - ID使用者は原則として本人だけが知っているパスワードを使用する
  - パスワードは第三者に開示しない
  - パスワードは第三者の目に触れる場所に掲示してはならない
  - 付箋紙に記述しディスプレイに貼る等してはならない
- 異動・退職時は、必ず、所属長に確認の上ITSに連絡する

パスワードの注意事項
・8文字以上を推奨する
・パスワードの文字列は使用するシステムで設定可能な文字種（英大文字、英小文字、数字、記号）のすべてを組み合わせる
・単純なパスワードは類推される可能性があるので使用しない
・名前、生年月日、製品名、会社名、家族の名前、電話番号、社員番号、車のナンバー、キーボードの配列順等あるいはこれらの組み合わせをパスワードにしない
・IDと同じ文字列をパスワードとして設定しない
・異なるシステムで同じパスワードを使い回さない
パスコードの注意事項
・社員番号をパスコードとして設定しない

池田糖化グループ基本ルール～日常業務時

ソフトウェア使用時の注意事項

- ソフトウェアをインストールしたい場合は、「ITSへの依頼書」を使用し、インストールを依頼する
- 許可されたソフトウェア以外のインストールは禁止
  - 許可されたソフトウェアでも、使い方によっては問題を引き起こす場合がある
  - 一部のソフトウェアは条件付きで使用可としているので使用時には条件を確認する

インターネット使用時の注意事項

- インターネットに接続すること自体がリスクであることを理解する
- 業務以外の目的で使用しない
- 危険を感じたら、速やかにネットワークを切断する

ブラウザ使用時の注意事項

- ITSが使用を許可したブラウザ（InternetExplorer Ver11、Chrome、Firefox）以外使用禁止
- ブラウザの設定は勝手に変更してはならない

池田糖化グループ基本ルール～日常業務時

社外メール使用時の注意事項

- 重要情報を電子メールにて送信する場合、以下を確認の上、送信する
  - 「To」「Cc」「Bcc」に入力した宛先は適切か？
  - ダイレクトメールなど不特定多数に電子メールを送信する場合、TOやCCに入れず、BCCに入れているか？
- 添付ファイルを送信する時は、必ずウイルス対策ソフトにより検査を行い、マルウェアに感染していないことを確認した上で送信する
- 重要情報をメールにて送受信する場合は、機密情報を本文に記載せず、添付ファイル内に記載し、添付ファイルは当社指定の圧縮ソフトを用いるか、Officeファイルであれば Officeの機能を用い、適切なパスワードを設定し暗号化する
  - 暗号化のパスワードは、電子メール以外の安全な手段を用いて相手と共有する
- 添付ファイル付き電子メールを受信した時は、サーバに添付ファイルを保存する前に、ウイルスチェックを行う
- 不審な兆候があるメールの添付ファイル、文中のURLは安易に開いたり、クリックしたりしない
- 不審な兆候があるメールを受信した場合は、ITSに連絡する
- メールの削除はITSから削除指示があった場合に実施する
- 手口が巧妙な場合は上記「不審な兆候」がないケースもあるので注意する

池田糖化グループ基本ルール～日常業務時

重要情報（電子データ）の取扱

- 入手時は、取引先と合意した方法でデータを暗号化し、以下の方法で受け取る
  - 許可されたUSBメモリあるいは新品のディスクメディアにコピーし手渡しで受け取るか電子メールで受け取る
- 入手した重要情報は、適切なアクセス制限が施された共有サーバ上およびクラウドシステム上にのみ保管し、以下に留意する
  - 許可なくコピー、持ち出ししない　　・目的外使用をしない
  - 適宜バックアップを取得すること（※共有サーバ上はバックアップ不要）
- 重要情報が保存された媒体（USBメモリ、DVD-Rなど）や電子機器（PC等）を移送する際は、ITSが定めた手段でデータを暗号化する
- 重要情報を電子メールで送信する際は当社指定の圧縮ソフトを用いるか、Officeファイルであれば Officeの機能を用い、適切なパスワードを設定し暗号化する
- 返却時には安全な方法で返却する
  - 入手時に使用したディスクメディアを手渡しで返却する
  - 入手時と同じ方法で返却する
- 使用する必要がなくなった重要情報は削除し、ゴミ箱からも削除する
  - メールで送受信していた場合は、メール削除後、ゴミ箱からも削除する

池田糖化グループ基本ルール～日常業務時

外部サービス（SNSサービス含む）使用時

- 外部サービスは他社によるサービスであるため、情報を社外に預けることになることを理解した上で使用する
- 「使用可能なソフトウェアおよび外部サービス一覧」に記載されている外部サービス以外は使用禁止（条件付きで使用可に注意）
  - 許可された外部サービスでも、使い方によっては問題を引き起こす場合がある
- 外部サービスを使用する際は、使用するIDをITSへ連絡する
  - IDが変更となった場合は、速やかに連絡する
  - 業務で使用が許可された外部サービスのIDを私有機器で使用してはならない
- 広報業務でSNSサービスを使用する際、以下に注意する
  - 重要情報、不正確な情報を投稿しない　　・安易なユーザフォローをしない
  - 私有機器での広報業務用のアカウント使用禁止
  - 他利用者からのクレーム、炎上等がある場合は、ITSに速やかに報告すること
- 業務連絡でSNSサービスを使用する際、以下に注意する
  - 私有機器での業務連絡用のアカウント使用禁止
- SNSサービスの私的利用時の注意
  - 極力、当社所属であることを明かさず、業務に関する情報を発信しない
  - 自らの発言により起こり得る問題の責任を負う可能性があることを意識して使用する

池田糖化グループ基本ルール～持ち出し時

モバイルPC、スマートデバイス、電子媒体持ち出し時の注意事項

- 肌身離さず持ち歩き、放置しない
- 他人に譲渡、貸与しない
- 不要なデータを格納しない
  - 持ち出す前に一度どのようなデータがあるのか確認する
  - 持ち出しが必要なデータがある場合は、使用が許可された外部サービス上に保存することを検討する
  - 重要情報や個人情報を一時的に保存する場合は、使用する必要性がなくなった時点で速やかに消去する
- 盗み見に注意する
- 紛失、盗難時は速やかにITSに連絡する
  - 必要に応じてストラップ等の取り付けなど紛失対策を行うこと

モバイルPC、スマートデバイス持ち出し時の注意事項

- 毎月1回、格納されているデータの確認を行い、不要な情報が保存されている場合は削除する

スマートデバイス持ち出し時の注意事項

- 毎月１回、電子メールデータ（携帯アドレスのメールおよび添付ファイル等）を確認し、不要なものは送受信ボックスおよびゴミ箱からも削除する

池田糖化グループ基本ルール～持ち出し時

モバイルPC、スマートデバイス持ち出し先でのネットワーク接続時の注意事項

- 使用可能なネットワークは下記のみ
  - 通信事業者が提供する通信手段（4G/3G等）
  - 以下のWi-Fi接続方法

原則としてこの3つの方法を推奨	社有のポータブルWi-Fi機器 社有のスマートフォンでのテザリング 拠点に据え置きする会社が用意したWi-Fi機器
使用可能だが遵守事項に従う必要あり	自宅のWi-Fi機器、ホテルが提供するインターネット接続サービス

  - 無料のWi-Fiスポットなどは危険性が高いため、接続することは禁止する

自宅のWi-Fi機器、ホテルが提供するWi-Fi使用時の注意事項

- 暗号化はWPA2を推奨する
- 自宅のWi-Fi機器使用時は、MACアドレスフィルタリングの使用を推奨するとともに、ファームウェアを最新のバージョンに更新する
- 以下はホテルが提供するWi-Fi使用時のみ
  - 不特定多数の利用者が共有しているネットワークであることを常に念頭において使用すること。また、セキュリティが確保されていない可能性があるので、接続するのは「やむを得ない場合のみ」に限ること。

池田糖化グループ基本ルール～例外事象発生時

例外事象（予兆を含む）発生時の対応と報告先

- 例外事象とは主に以下を指す
  - マルウェアに感染した場合、または感染が疑われる場合
  - 情報機器の盗難、紛失
  - 重要情報誤送信（メール、許可されていない外部サービスへのアップロード等）
  - 外部からの不正アクセス、あるいは従業員等の内部不正による重要情報の漏えい
  - ランサムウェア等によるPCまたはサーバ内データの使用不能化
  - 疑わしいメール（フィッシングメール、標的型攻撃メール、ビジネスメール詐欺等）による被害
  - SNS使用における、当社重要情報の漏えい、当社へのクレーム、中傷、炎上等
  - 業務都合等により本基準の遵守事項を守れない状況が発生した場合
- 例外事象を認識した場合、速やかに以下報告先に報告する

電話	**084-957-3380（業務時間内）** **090-9951-3380（業務時間外）** **090-7374-2261（業務時間外）**

- ITSから再発防止策が提示された場合は、その対策を実施する