セキュリティハンドブック

このハンドブックには、従業者が日々の業務において意識すべき
情報セキュリティのルールが記載されています。

目次

改訂履歴

Ver.	改定日	改定内容	作成	承認
1	2020-04-07	初版発行	西	矢作
1.1	2020-07-28	「私物PCの取り扱い」で、「PCにダウンロードした業務データは、1ヶ月に一回全て削除されていることを確認する。」に変更。（変更前は業務終了時に削除）	西	矢作
（以降、バージョンと改定日の表記のみで良い）				
1.2	2021-07-20	(p1522946)		

1　情報を適切に取り扱う

■　情報資産の分類

- 社内の情報は、以下の表に従って分類する。

区分	定義	例
A情報	社外に漏えいした場合に、当社の存続が危機にさらされる情報	顧客の個人情報、お客様に所有権があるデータ など
B情報	社外に漏えいした場合に、当社に悪影響や被害が想定される情報	従業者の個人情報、取引先情報、業務ノウハウ など
C情報	社外に漏えいしても、当社に悪影響や被害がない、もしくはすでに公開されている情報	会社パンフレット、公開後のプレスリリース など

■　紙媒体の整理・ラベル付け

- A情報およびB情報は、原則、鍵付きキャビネットなどを用いて施錠管理を行う。
- 紙媒体をキャビネットや机の引き出しに保管する場合は、平積みにせず、ファイリングして整理する。
- ファイリングされた紙媒体の背表紙には、識別を容易にするため、内容を記入する。

■　電子データの整理・ラベル付け

- A情報およびB情報は、適切なアクセス権を設定した共有フォルダ等で保管する。
- 電子データには、識別を容易にするため、内容が分かるようなファイル名・フォルダ名を付ける。
- ファイル名・フォルダ名には、「その他」「引き継ぎ」などの中身がわかりにくい名前を付けない。
- PCの破損・紛失時に備え、電子データは共有フォルダへの保管を心がけ、PCローカルのみの保管は最小限とする。

■　個人情報の取り扱い

- 業務で個人情報を扱う場合は、個人情報保護法をはじめとする法令や、ガイドラインを遵守する。

2　機器や媒体を適切に取り扱う

■　会社支給PCの取り扱い

- デスクトップ画面には、可能な限り作業用の一時ファイル、ショートカット、ゴミ箱以外のアイコンを置かない。
- ウィルス対策ソフトを導入し、自動更新の設定を行う。
- 帰宅時や、社外への持ち出し時には、必ずシャットダウンを行う。
- パスワード付きのスクリーンセーバーが5分以内に起動するよう設定する。
- PCから一時的に離れる場合は、画面ロックを手動で実施する。

■　私物PCの取り扱い

- 利用方法については、上記「会社支給PCの取扱い」を遵守する。
- 利用する際は、事前に情報セキュリティ管理者に申請する。
- 業務で用いる私物PCのOSアカウントは、家族や友人などの第三者と共有しない。
- PCにダウンロードした業務データは、1ヶ月に一回全て削除されていることを確認する。

■　私物モバイル端末の取り扱い

- パスワードか、もしくは生体認証(指紋認証 など)を設定する。
- リモートワイプの設定を行う。
- サポートが終了したバージョンのOSしか動作しない端末を使用しない。
- 公式のストア(App StoreやPlayストアなど)以外から、アプリをダウンロードしない。
- アプリやOSは、定期的なアップデートを行い、常に最新のバージョンを利用するよう心がける。
- ロック画面に表示されるアプリの通知に、A情報及びB情報が含まれないように設定する。
- 業務データを端末内に保存(ダウンロード)しない。

■　紙媒体の取り扱い

- A情報およびB情報が記載された裏紙は利用しない。
- A情報およびB情報が記載された紙媒体の利用が終わったら、速やかにシュレッダーで破砕する。
- 社外(コンビニ、自宅　など)で、紙媒体を印刷・コピーすることは禁止する。ただし、情報セキュリティ管理者から許可を得た者は利用してもよいものとする。

■　名刺の取り扱い

- 交換した名刺は、スキャンにより電子データ化し保管する。
- スキャンが終わった名刺の原本は、シュレッダーにて破棄する。

■　機器・媒体の輸送

- A情報及びB情報を含む機器・媒体(契約書など)を物理的に輸送する場合には、盗難に備え、データにパスワードをかける、暗号化するなどの対策を施し、パスワードは別の方法(電話、メールなど)で伝達する。

3　強固なパスワードを設定し、管理する

■　パスワードポリシー

- パスワードは本人が作成したものを利用することとし、初期パスワードは、利用者本人で変更する。
- パスワードの文字列には、辞書に載っている一般的な単語は利用しない。
- パスワードの文字列は、8桁以上とする。
- パスワードの文字列には、英語文字・数字をそれぞれ必ず1文字以上は含める。
- プライベートで利用しているパスワードと同じパスワードを利用しない。
- サービス毎にパスワードが異なるようにする。
- 以下に該当するサービスのパスワードは、個別の利用方針に従う。

サービス名	個別の利用方針
スマートフォン	✔ 数字4桁などの簡単なパスワードを利用してもよいが、「0000」などの単純な数字列は設定しない。 ✔ 可能な限り、生体認証を利用する。

■　パスワードの管理

- パスワードを紙媒体に記載してもよいが、第三者に見られた場合に、簡単にログインされないように工夫する（サービス名, ID, パスワードの3つの情報をセットで同じ場所に記載しない等）。
- パスワードが外部に流出した可能性がある場合は、即座にパスワードを変更する。

4 安全なソフトウェア・Webサービスを利用する

■ 利用可能なソフトウェア・Webサービス

- 業務では、基本的には以下に該当するソフトウェア・Webサービスは利用してはならない。
  - P2Pの仕組みを利用したWebサービス、ソフトウェア
  - SSL通信による保護がなされていないWebサービス
  - プライベートで利用しているWebサービスのアカウントの業務利用
  - 商用利用が有償であるWebサービス、ソフトウェアを無償で利用する行為
  - 個人提供、または提供元が不明のWebサービス、ソフトウェア
- 業務において、上記に該当するソフトウェア・Webサービスを利用する場合は、情報セキュリティ管理者に相談し、許可を得る。

■ クラウドストレージの利用方法

- A情報及びB情報は、適切なアクセス制御がかけられたフォルダに保管する。
- 外部とフォルダを共有していた場合、利用終了後に適切なアクセス権にする。

■ 電子メールの利用方法

- A情報及びB情報は、電子メールに添付して送らない。
- 会社のメールを、個人のメールアドレスに転送しない。
- 互いに知られてはいけない社外の相手に一斉送信をする場合は、BCCを活用し、宛先が外部に流出しないよう注意する。

■ チャットの利用方法

- チャットは会社で指定されたサービスを利用する。
- 業務に関するチャットは、各チャンネル(チャットルーム)を利用しダイレクトチャットでは業務内容のやり取り極力行わない。

■ SNSの利用方法

- FacebookやLINEなどのSNSの私用アカウントを用いて、情報をやり取りすることは最小限に抑える。私用アカウントを用いての、業務ファイルの送付は行わない。
- 社内外で入手した非公開情報は、個人で利用しているSNS等には投稿しない。
- 会社の執務エリア敷地内で撮影した写真や動画などの投稿は避ける。
- 顧客や取引先との懇親会などの画像をアップする場合は、あらかじめ先方の許可を得るようにする。
- 業務で利用しているIDやパスワードを、個人のSNSで再利用はしない。
- 親しみやすい内容の投稿を心がけ、極端な表現の利用や、喧嘩腰の態度を取ることは避け、会社のブランディングに寄与する。
- 他者が作成した画像や文章などの著作物を、許可なく無断でSNSに投稿、プロフィール画像に利用することは禁止とする。
- 従業員や取引先相手の社員、及び一般人など、他者が写り込んだ写真・画像は、無断で投稿しないようにする。

5　働く場所のセキュリティについて

■　セキュリティエリア

- オフィスは、以下のセキュリティエリアに分ける。各エリア内では、以下の事項を守る。

エリア名	入退室管理	遵守事項
休憩スペース	(誰でも入室可能)	✔ PCや業務資料を放置しない。
来客・会議スペース	(誰でも入室可能)	✔ PCや業務資料を放置しない。 ✔ ホワイトボートは、利用が終わるとすぐに内容を消去する。
執務スペース	✔ 来客が入室する場合は、従業者が帯同する。	✔ ホワイトボートは、利用が終わるとすぐに内容を消去する。 ✔ キャビネットは、利用が終わると都度施錠する。

※セキュリティエリアの割り当ては「オフィスレイアウト図」に記載されている。

- 荷物の受取は、来客スペースで行う。宅配員が執務エリアに入る必要がある場合は、必ず従業者が帯同する。
- キャビネットのスペアキーは管理部長が管理する。

■　クリアデスク

- 情報資産を紛失した際にすぐに気づくことができるように、机上は常に整理し、作業中の資料やPC以外は、机上に放置しない。
- 個人の袖机には、他の人が利用する可能性のある会社の情報(書類など)を保管しない。

■　社外での業務

- 新幹線やカフェなど、背後に人が居る環境での作業は、常に盗み見に注意し、A情報及びB情報は開かない。可能であれば、覗き見防止フィルターを用いて画面を保護する。
- 提供元が不明のWi-Fiや、暗号化が行われていないWi-Fiに接続しない。ネットワークに接続する場合は、WPA2以上の強度により暗号化されたWi-Fi、会社が貸与するポケットWi-Fi、もしくはテザリングを利用する。
- 社外(自宅、コンビニなど)での、A情報やB情報の印刷は禁止する。ただし、情報セキュリティ管理者に許可を得た者は利用してもよい。
- 利用する機器(PC、スマートフォンなど)は、盗難を防ぐため、常に肌身離さず持ち歩く。

6 情報セキュリティ事故が発生したときの対応

■ 情報セキュリティ事象

- 情報セキュリティ事象を発見した従業者は、すみやかに情報セキュリティ管理者にチャットまたは電話にて、報告する。
- 情報セキュリティ事象の例として、以下が考えられる（ただし、これらに限らない）。
  - ✔ 業務資料や業務データが入った媒体(PC、スマートフォンなど)を紛失した
  - ✔ メールを誤送信した
  - ✔ パソコンがウィルス(マルウェア)に感染した
  - ✔ 不明な差出人からの添付ファイルを開いた
  - ✔ 外部から情報漏えいに関する連絡があった
  - ✔ 利用システム(Google Workspace等)のサービスのアカウントが乗っ取られた