Ver 1.3

情報セキュリティハンドブック

（ひな形）

ハンドブックの使い方

本ハンドブック（ひな形）は、従業員に配付し自社のセキュリティルールを確認してもらうためのものです。５分でできる！情報セキュリティ自社診断に連動しています。赤字で記載した箇所は記載例になりますので、自社のルールにあわせて赤字を中心に修正し、また必要に応じて項目を加筆して、ご利用ください。

株式会社〇〇〇〇

1－1 全社基本ルール

OSとソフトウェアのアップデート

＜OSのアップデート＞

●パソコンのOSはWindows Updateの自動更新を有効にする。

●業務に利用するスマートフォンのOSは以下を参考にして手動で更新する。

- Android端末の場合：機種毎の情報を常に調べて必要に応じて対応する。
- iPhoneの場合：iPhone本体（Wi-Fiを利用）でiOSアップデートを行う。
  ※アップデート後は元のバージョンに戻せないので、事前にデータのバックアップを取得する。

＜ソフトウェアのアップデート＞

●Microsoft Office は自動更新設定を設定する。

●Adobe Flash Player、Adobe Reader は自動更新設定を設定する。

業務でスマートフォンを使う場合は、スマートフォンのOS、ウイルス対策ソフトもアップデートしてください。やりかたが分からない人は、総務部システム担当までお問い合せください。

ウイルス対策ソフトの導入

●業務で利用する機器には以下のウイルス対策ソフトを導入し、定義ファイルを随時更新する。持ち出し用ノートパソコンは利用時に定義ファイルの更新を確認する。

- パソコン：〇〇〇〇ウイルス対策ソフト（定義ファイル更新方法　自動）
- タブレット端末：〇〇〇〇ウイルス対策ソフト（定義ファイル更新方法　自動or手動）

パスワードの管理

●ログインやファイル暗号化に使うパスワードは、以下に従って設定・利用する。

◎必須	×禁止
10文字以上で制限範囲の最大文字数	名前・電話番号・誕生日は使わない
アルファベットの大文字と小文字、数字や「@」「%」などの記号を組み合わせる	同じ文字・数字を連ねただけにしない
ID・パスワードの使い回しをしない	他者に見えるところに記さない/教えない

1-2 全社基本ルール

アクセス制限

●複数名が共有する機器には以下のようにアクセス制限を行う。
●アクセス制限の設定・変更は、総務部システム担当が行う。

機器名	アクセス制限の方法	アクセス権限付与対象者
○○ファイルサーバー	NAS ○○ACL	社長/○○部従業員
設計図保存サーバー	Windows Active Directory	社長/技術部従業員
○○部複合機HDD	複合機アクセス権設定機能	社長/経理部従業員
本社無線LANルーター	Wi-Fi パスワード設定 WPA2による暗号化	社長/取締役/従業員

セキュリティに対する注意

●総務部システム担当は毎週月曜日に以下のサイトを参照し、当社で利用する製品やサービスに関わる緊急情報が公表された時には、即座に社長に報告し、電子メールで対策を全従業員に通知する。

- 独立行政法人情報処理推進機構（略称：IPA） 重要なセキュリティ情報
  https://www.ipa.go.jp/security/
- JVN（Japan Vulnerability Notes）
  https://jvn.jp/
- 一般社団法人 JPCERT コーディネーションセンター（略称：JPCERT/CC）
  https://www.jpcert.or.jp/

2-1 仕事中のルール

電子メールの利用

●メールソフトを以下のように設定し、宛先のアドレスが間違っていないか確認してから送信する。

（Microsoft Outlookの場合）

- [ファイル]→[オプション]→[詳細設定]→[送受信]の項目にある「接続したら直ちに送信する」チェックを外す→「OK」
- 送信トレイに保存されたメールをもう一度確認して「送受信タブ」から[すべてのフォルダーを送受信]をクリックする。

●複数の外部の人に同時に同じメールを送る場合には、宛先（TO）に自分自身のアドレスを入力し、BCCで複数相手のアドレスを指定する。

●重要な情報または個人情報を送信する場合は、本文に記入せず、以下の方法で行う。

- 重要な情報または個人情報を添付ファイルに記載して、パスワードの設定、またはパスワード付きのZIPファイルにして暗号化する。
- パスワードは先方とあらかじめ決めておく、または電話で知らせるなどパスワードが傍受されないよう配慮する。

2-2 仕事中のルール

電子メールの利用

●標的型攻撃メールによるウイルス感染を防止するため以下の内容に複数合致する場合は十分に注意し、安易に添付ファイルを開いたり、リンクを参照したりしない。

- **メールのテーマ（件名・見出し）**
  ①知らない人からのメールだが、メール本文のURLや添付ファイルを開かざるを得ない内容
  ②心当たりのないメールだが、興味をそそられる内容
  ③これまで届いたことがない公的機関からのお知らせ
  ④組織全体への案内
  ⑤心当たりのない決済や配送通知 （英文の場合が多い）
  ⑥ID やパスワードなどの入力を要求するメール
- **差出人のメールアドレス**
  ①フリーメールアドレスから送信されている
  ②差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なる
- **メールの本文**
  ①日本語の言い回しが不自然である
  ②日本語では使用されない漢字（繁体字、簡体字）が使われている
  ③実在する名称を一部に含むURL が記載されている
  ④表示されているURL（アンカーテキスト）と実際のリンク先のURL が異なる（HTML メールの場合）
  ⑤署名の内容が誤っている
- **添付ファイル**
  ①ファイルが添付されている
  ②実行形式ファイル（exe / scr / cpl など）が添付されている
  ③ショートカットファイル（lnk など）が添付されている
  ④アイコンが偽装されている
  ⑤ファイル拡張子が偽装されている

2-3 仕事中のルール

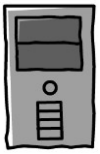
インターネットの利用

●ウェブサイト利用時には以下に注意する。
- 不審なサイトへのアクセス及び社用メールアドレス登録を禁止する。
- パスワードをブラウザに保存しない。

●業務でオンラインストレージサービスを利用する際には以下を順守する。
- 業務でオンラインストレージサービスを利用する場合は、総務部システム担当の許可を得る。
- 従業員、もしくは取引先以外との業務関連情報の共有を禁止する。
- メールアドレスの登録が必要な場合は社用メールアドレスを登録する。

●業務でSNSを利用する際には以下を順守する。
- 当社の秘密情報の書き込みは行わない。
- 取引先従業者とSNS上で私的に交流する場合、双方の立場をわきまえ、社会人として良識の範囲で交流する。
- セキュリティ設定を行い、アカウントの乗っ取り、なりすましに注意する。
- 使用するスマートフォン、タブレット端末上のデータ、写真、位置情報が、予期せず公開される可能性のあることに注意する。

データのバックアップ



●重要なデータは以下に指定したサーバーに保存する。
●重要なデータを保存したサーバーのバックアップは、総務部システム担当が以下の要件に従い取得する。

機器名	対象	方法	保管媒体	頻度
○○サーバー	システムファイル ユーザーファイル	Windows バックアップ	外付けHDD	毎週
設計図保存 サーバー	ファイルバックアップ	○○同期ツール	外付けHDD	毎日

2-4 仕事中のルール

クリアデスク・クリアスクリーン

●重要書類、スマートフォン、携帯電話、重要な情報を保存したUSBメモリ、小型ハードディスク、CD等の電子媒体などを業務利用時以外は机上に放置せず、クリアデスクを徹底する。
●離席時には以下のいずれかによりパソコンの画面をロックし、クリアスクリーンを徹底する。
- スクリーンセーバー起動時間を5分以内に設定し、パスワードを設定する。
- スリープ起動時間を5分以内に設定し、解除時のパスワード保護を設定する。
- [Windows]＋[L]キーを押してコンピュータをロックする。

●退社時、未使用時にはノートパソコン、USBメモリ、小型ハードディスク、CD等の電子媒体及び重要書類を机の引き出しに保管し、施錠する。

重要情報の持ち出し

●ノートパソコン、タブレット端末、重要な情報を保存したUSBメモリ、小型ハードディスク、CD等の電子媒体及び重要書類を社外に持ち出すときには以下を徹底する。
- ノートパソコンまたはタブレット端末に保存するデータは必要最小限にする。
- 電子媒体はケースに入れ、USBメモリはタグ、ストラップ、鈴などを付け紛失を防止する。
- 書類はひも付き封筒に入れる。
- ノートパソコンはBIOSパスワードとWindowsログインパスワードを設定する。
- 電子データはファイル暗号化、またはUSBメモリ暗号化機能により暗号化する。

●携行時には以下に注意する。
- 電車内では網棚に置かない。
- 自動車内には保管しない。
- 作業中離席する場合は携行する。
- 他者から覗き見できない状態で扱う。

重要情報の保管

●退社時、未使用時にはモバイル用パソコン、USBメモリ、小型ハードディスク、CD等の電子媒体及び重要書類を机の引き出しまたは所定のキャビネットに保管し施錠する。

2-5 仕事中のルール

入退室

●取引先または関係者以外が入室した場合、発見者は声をかけ用件を確認する。
●最終退室者は以下を行う。
- 全員のパソコンがシャットダウンされ、プリンターなど周辺機器、暖房器具、湯沸かし器など発熱機器の電源が切られているか確認する。
- 全ての出入口の施錠を確認する。
- 退室時刻と退室者氏名を所定様式に記録する。

電子媒体・書類の廃棄

●電子媒体または重要書類の廃棄は以下の手順で行う。

媒体	廃棄方法
サーバー・パソコン ※リース物件返却・売却含む	・総務部システム担当がハードディスクを取り出し破壊 ・総務部システム担当がデータ抹消ツールにより完全消去
外付けハードディスク	・総務部システム担当が破壊 ・総務部システム担当がデータ抹消ツールにより完全消去
CD・DVDなどのディスク	・利用者がシュレッダーで細断 ・利用者がCDのラベル面、DVDのディスク内面にカッターでキズを入れる
USBメモリー	・総務部システム担当がデータ抹消ツールにより完全消去
重要書類	・利用者がシュレッダーで細断 ・大量の場合は総務部システム担当が溶解処分を専門業者に依頼し、廃棄証明書を取得

3-1 全社共通のルール

私有情報機器の利用

●私有の情報機器を業務で利用する場合は以下を順守する。

情報機器の種類	順守事項
パソコン ※自宅のパソコンで業務を行う場合も含む 	• 社内へ無断で持ち込むことを禁止する • 業務利用を禁止する • 社内LANへの接続を禁止する • ウイルス対策ソフト、アプリケーションソフトは総務部システム担当が指定したものを導入し、許可を得たうえで利用する • 業務終了後に業務用データは総務部システム担当の指定するツールで完全に消去する • 従業員個人のメールアドレスに業務用データを添付して送信することを禁止する • 社用メールアドレスで受信したメールを従業員個人のアドレスに転送することを禁止する
スマートフォン タブレット端末 携帯電話など記憶・通信機能を備えた機器 	• 会社で貸与した機器を利用する • 地図検索、路線案内を除き業務利用を禁止する • 充電を除き、社内パソコンへの接続を禁止する • ウイルス対策ソフト、アプリケーションソフトのインストールは総務部システム担当が指定したものを導入し、許可を得たうえで利用する • 取引先アドレスを除く業務用データの保存を禁止する。 • 従業員個人のメールアドレスに業務用データを添付して送信することを禁止する • 社用メールアドレスで受信したメールを従業員個人のアドレスに転送することを禁止する
USBメモリ 外付けHDDなどの記憶機能を備えた機器・媒体	• 会社で貸与した機器を利用する • 私有物の利用を禁止する • 総務部システム担当の許可を得て利用する • 業務終了後に業務用データは総務部システム担当の指定するツールで完全に消去する

3-2 全社共通のルール

クラウドサービスの利用

●クラウドサービスを新たに利用する必要がある場合は以下を入手し、総務部システム担当の許可を得たうえで利用する。

- サービス提供者が公表する情報セキュリティ方針、プライバシーポリシーなど
- サービス提供者の情報セキュリティ上の責任範囲を定めたサービス利用規約など
- サービスにあらかじめまたはオプションで付随する情報セキュリティに関する機能やサービスについて明記したもの
- サービス提供者が情報セキュリティに関わる適合性評価制度の認証を取得している場合はその証拠となるもの
- 専門家による監査を実施している場合はその証拠となるもの

＜参考＞※カッコ内は運営組織

情報セキュリティ対策への取組み自己宣言制度

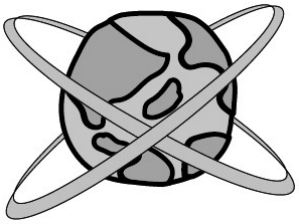
・SECURITY ACTION制度（IPA）

適合性評価制度

・ISMS適合性評価制度（JIPDEC/JAB）
・プライバシーマーク制度（JIPDEC）
・PCI DSS（クレジットカード業界セキュリティ基準）
・クラウドサービスの安全・信頼性に係る情報開示認定制度（ASPIC）
・インターネット接続安全安心マーク（インターネット接続サービス安全・安心マーク推進協議会）
・TRUSTe（JPAC）

独立かつ専門的知識を持った者に対して情報セキュリティ対策の評価を依頼する制度

・情報セキュリティ監査制度（経済産業省/JASA）



3-3 従業員のみなさんへ

従業員の守秘義務

●従業員には当社の就業規則で定められた守秘義務があります。規則を順守し、このハンドブックを情報セキュリティに役立てて情報セキュリティの事故を防ぎましょう。

事故が起きてしまったら

●もしも事故が起きてしまったら、以下の手順に従い、二次被害や事故の影響を最小限に止めましょう。

●情報セキュリティ事故の定義は以下とします。

- 情報の「漏えい」「改ざん」の発生または「利用できない」状態になったときに
- 当社の業務や顧客、取引先、株主、本人（個人情報の場合）に望ましくない影響が及ぶ

1．発見者は社長または総務部システム担当に速やかに連絡する。
※夜間休日を問いません
社長携帯電話：090-〇〇〇〇-〇〇〇〇
社長内線電話：〇〇〇〇
総務部システム担当携帯電話：090- 〇〇〇〇-〇〇〇〇
総務部システム担当内線電話：〇〇〇〇

2．社長/総務部システム担当は以下を実行する。
＜情報漏えい＞
①漏えいした情報の確認
②影響範囲の全ての組織及び本人（個人情報の場合）に事実を報告
影響範囲の全ての組織及び本人（個人情報の場合）に対策案を通知
＜改ざん、利用できない状態＞
①原因の調査
②影響範囲の全ての組織及び本人（個人情報の場合）に事実を報告
復旧策を実施後、影響範囲の全ての組織及び本人に報告