Ver 2.0

情報セキュリティ
ハンドブック

２０２５年１２月１日
第１版

アサヒ衛陶　株式会社

改訂履歴

版 数	発行日	改定箇所	改定内容
第1版	2025年12月1日		

目次

OSとソフトウェアのアップデート

自己診断 No.1

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して最新の更新プログラムをインストールした状態にする。WSUSを利用して統合管理。
- 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

- Windowsの更新時WSUSから更新プログラムを配信し、対策を実施する。
- Adobe Reader はアップデートを自動に設定する。
- スマートフォンは、MDMを利用して統合管理を実施する。

ウイルス対策ソフトの導入

自己診断 No.2

- 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。
  - 社内端末：HP Wolf Security（定義ファイル更新方法：自動）

パスワードの管理

自己診断 No.3

- 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。

パスワード必須要件	パスワード禁止要件
社員番号と英文字数で構成されている	名前・愛称・地名・電話番号・生年月日・ 辞書に載っている単語 よく使われるフレーズは使わない
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

アクセス制御

自己診断 No.4

- 複数名が共有する機器には以下のようにアクセス制御を行う。
- アクセス制限の設定・変更は、事業推進部が行う。

機器名	アクセス制御の方法	アクセス許可対象者
共有ファイルサーバー	部署毎にフォルダのアクセス権設定	全従業員
NAS（技術部）	NASのアクセス権設定	技術部
本社無線アクセスポイント	Wi-Fi パスワード設定 WPA3による暗号化	従業員

セキュリティに対する注意

自己診断 No.5

- 事業推進部は毎週月曜日に以下のサイトを参照し、当社で利用するIT製品やサービスに関わる重要なセキュリティ情報、緊急情報などが公表された時には、速やかに社長に報告し、電子メールで対策を全従業員に通知する。
- 通知を受けた従業員は速やかに対策を実行する。

独立行政法人情報処理推進機構（IPA） 重要なセキュリティ情報
https://www.ipa.go.jp/security/

JVN（Japan Vulnerability Notes 脆弱性対策情報ポータルサイト）
https://jvn.jp/

一般社団法人 JPCERTコーディネーションセンター（JPCERT/CC 技術的な立場における日本の窓口CSIRT）
https://www.jpcert.or.jp/

電子メールの利用①

自己診断 No.7・8

- 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。

Gmailの場合

- 右上にある設定アイコン⚙ ⇒「すべての設定を表示」をクリックします。
- 「送信取り消し」の横で、送信を取り消せる時間（送信から経過時間）を5, 10, 20, 30秒から選択します。※30秒を推奨設定
- 下部にある「変更を保存」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、パスワードを使用して暗号化、またはパスワード付き圧縮ファイル（ZIP形式）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、または携帯電話ショートメッセージサービス（SMS）で知らせるなど、パスワードが傍受されないようにする。

電子メールの利用②

自己診断 No.6

- 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)
⑥ ID 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

インターネットの利用

自己診断 No.10

- 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、事業推進部の許可を得る。
  - 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

自己診断 No.11

- 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、事業推進部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
共有ファイルサーバー	システムファイル 共有ファイルデータ	イメージ バックアップ	NAS	毎日
NAS（技術部）				

クリアデスク・クリアスクリーン

自己診断 No.12・14

- 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メモリー、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。
  - 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メモリー、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。
  - 大阪支店は個人ロッカーにノートPCを保管して、退社する。

重要情報の持ち出し

自己診断 No.13

- 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メモリー、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メモリーはタグ、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メモリー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。
  - 自動車内に置いたまま車外に出ない。
  - 作業中離席する場合は携行する。
  - 他者が画面を覗き見できない状態で使用する。

重要情報の保管

自己診断 No.12

- 退社時、未使用時にはモバイル用パソコン、USBメモリー、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。

入退室

自己診断 No.17

- 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

自己診断 No.18

- 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	• 事業推進部がハードディスクを取り出し破壊 • 事業推進部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	• 事業推進部が破壊 • 事業推進部がデータ抹消ツールにより完全消去
CD・DVDなどの光学メディア	• 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	• 事業推進部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 • 大量の場合は事業推進部が溶解処分を専門業者に依頼し、廃棄証明書を取得

私有情報機器の利用

自己診断 No.21

- 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 • 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事業推進部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メモリー、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 • 事業推進部の許可を得て利用する • 業務終了後に業務用データは事業推進部の指定するツールで完全に消去する

クラウドサービスの利用

自己診断 No.23

- 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、事業推進部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. 従業員のみなさまへ

従業員の守秘義務

自己診断 No.19

- 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、このハンドブックに定められたルールを守り、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

自己診断 No.24

- 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. 発見者は事業推進部に速やかに連絡する。

※夜間休日を問いません
事業推進部携帯電話：080-5338-5341（村岡）、080-4929-0036（玉田）
事業推進部内線電話：06-7777-2074

2. 事業推進部は以下を実行する。

＜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
③ 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
③ 復旧策を実施後、影響範囲の全ての組織及び本人に報告

4－1.　利用する情報システム

テレワークで利用する情報システム

- テレワークを実施する際には、以下の情報システム・サービスを利用する。
- 他の情報システムやサービスを利用する必要がある場合は、事業推進部の許可を得る。

＜テレワークで利用する情報システム＞

情報システム・サービス	用　途	導入手順・制限事項
GoogleWorkspace	電子メール Web会議	Gmail GoogleMeat
Zoom	Web会議	社内PCにリモートアクセスして利用 私有メールアドレス、メーラーの業務利用禁止
基幹システム　Smaileα		セキュアモバイルアクセスを利用して接続
共有ファイルサーバ	データ共有	セキュアモバイルアクセスを利用して接続
imageWareDesktop	用途: 注文書受領 部門間データ共有	

4-2. 利用する情報機器

テレワークで利用する情報機器

- テレワークで業務を行う際には、以下の情報機器を利用する。
- 他の情報機器を利用する必要がある場合は、事業推進部の許可を得る。

＜テレワークで利用する情報システム＞

情報機器	社有機器	私有機器
パソコン	会社貸与テレワーク用PCを利用 社内PCを持ち出して利用	私有機器の業務利用禁止
スマホ・タブレット	会社貸与品を利用	私有機器の業務利用禁止
通信機器（ルーター）	会社貸与のモバイルルータを利用	私有機器の業務利用禁止
USBメモリー・外付けHDD	会社貸与品を利用	私有機器の業務利用禁止
オンライン会議用ヘッドセット	会社貸与品を利用	必要に応じて私有機器を利用
オンライン会議用Webカメラ	会社貸与テレワーク用PC内蔵Web カメラを利用	必要に応じて私有機器を利用

4-3. 社有機器の利用

社有機器を利用する場合

＜パソコン＞
- OS・ソフトウェアはインターネットに接続した状態で自動更新を有効にして最新の更新プログラムをインストールする。
- ウイルス対策ソフトの定義ファイルは自動で更新する。
- 社内標準外ソフトウェアのインストールは禁止する。

＜スマホ・タブレット＞
- 指定されたMDM(モバイル機器管理)エージェントをインストールする。
- OSは以下を参考にして自動で更新する。
  - Android端末の場合：機種毎の設定画面で自動システムアップデートを選択する。
  - iPhoneの場合：デバイスの自動アップデートを有効にする。
- 社内標準外アプリのインストールは禁止する。

＜USBメモリー＞
- 秘密情報または個人情報を保存して外出する場合は、ファイルを暗号化する。

私有機器を利用する場合

＜パソコン＞

- テレワークで使用する通信機器（ルーター）は、以下の対策を施して利用する。

＜テレワークで利用する通信機器＞

利用場所	通信機器 サービス	対策
自宅	有線LANハブ	同じハブに他者（家族を含む）もPCを接続する場合は、 • スイッチングハブを利用する（リピーターハブは禁止） • OSの「ネットワークのファイルとフォルダーの共有」を解除する
	無線LANルーター	• 同じルーターに他者（家族を含む）も端末を接続する場合はOSの「ネットワークのファイルとフォルダーの共有」を解除する • 暗号化方式はWPA2-PSKまたは機器が対応している場合はWPA3を選択する • 暗号化キーに簡単なものが設定されている場合、次の条件を満たすように変更する ➢英語の辞書に載っている単語を使わない ➢大文字、小文字、数字、記号の全てを含む文字列とする ➢簡単なものが設定されている場合は文字数を増やし容易に推測できないようにする • SSIDは、使用者氏名、会社名などを想起させないものを使う • 設定画面にログインするための管理者用パスワードは、推測されにくいものにする • ファームウェアは自動更新にする
外出先 ※取引先・レンタルオフィス・カフェ・ホテル・ファーストフード・コンビニ・空港・駅・鉄道・バスなど	モバイルWi-Fiルーター （スマホでのテサリングを含む）	• SSID/ネットワーク名は初期値を変更し、ルーター/スマホ機種名、使用者氏名、会社名などを想起させないものを使う • セキュリティキー/パスワードは、無線LANルーターの暗号化キーと同等の推測されにくいものを使う
	公衆Wi-Fiサービス	• メールは社内PCにリモートアクセスして利用する • ID・パスワードなどの認証情報、会社の秘密情報、個人情報などの重要情報を入力・表示しない • 重要情報の入力・表示が必要な場合にはVPNまたはSSL/TLS対応サイトを利用する • OSの「ネットワークのファイルとフォルダーの共有」を解除する

4-6. 勤務中のルール

電子メール・Webサイトの利用

- テレワーク端末で電子メール、Webサイトを利用する場合は以下を遵守する。
  - 個人のメールアカウントを利用するときには、安易に添付ファイルを開いたり、リンクを参照しない。
  - Webサイトからファイルをダウンロードするときには、ブラウザで証明書を確認し※1、信頼できるサイトを利用する。※1 ブラウザの鍵マークをクリックする
  - 業務に関係がない不審なサイトにアクセスしない。

クラウド・SNSの利用

- テレワーク端末で個人的にクラウドサービス、SNSを利用する場合は以下を遵守する。
  - 業務関連データの送受信、保存、共有に利用しない。
  - 社内、取引先との連絡に利用しない。
  - 当社の秘密情報の書き込みは行なわない。

在宅時の注意

- 在宅勤務では以下に注意する。
  - 他者(家族を含む)にテレワーク用の情報機器を操作させない。
  - 他者(家族を含む)から見えるところにテレワークで使うパスワードを書き記さない。

外出時の注意

- 取引先・レンタルオフィス・カフェ・ホテル・ファーストフード・コンビニ・空港・駅・鉄道・バスなど外出先でテレワークを行うときには、以下に注意する。
  - 必要な情報以外は持ち出さない。
  - 機器や書類は目の届く範囲に置き放置しない。
  - 取引先やレンタルオフィスなどで離席するときはコンピュータをロックする※2。
  - 不特定多数の人がいる場所では重要情報を画面に表示しない。
  - 外出先で書類やCD・DVDなどの媒体を廃棄しない。
  - 公衆Wi-Fiを利用するときは以下を遵守する。
    - メールは端末から直接メールサーバーにアクセスせず社内PCにリモートアクセスするか、指定されたセキュアブラウザを利用する。
    - その他で公衆Wi-Fiを使用して業務データを扱うときには、VPNまたはSSL/TLS対応サイトを利用する。

※2 [Ctrl] と [Alt] キーを押しながら [Delete] キーを押すか[Windows] キーを押しながら [L] キーを押す

4-7. データ・書類の保存

電子データの保存と消去

- 業務関連データのうち秘密情報または個人情報をテレワーク用PCで処理する場合は、作業後に社内PCにリモートアクセスし、社内サーバーに転送・保存する。
  転送後にはPC内のデータを事業推進部の指定するツールで完全消去する。
- 秘密情報または個人情報を継続してテレワーク用PCまたは会社貸与のUSBメモリー、外付けHDDに保存する必要がある場合は、ファイルを暗号化する。

書類・印刷物・CD/DVDの保管と廃棄

- 秘密情報または個人情報を含む書類・印刷物・CD/DVDなどの媒体は、鍵付き引き出し、書類ケースに保管し、利用時以外は施錠する。
- 書類・印刷物は、ハサミなどで細断して廃棄する。
- CD/DVDを廃棄する場合は、割る、またはカッターなどで傷を付けて廃棄する。
  ※光っている読み取り面ではなく、レーベル面の中心から傷を付ける

社内問合せ・緊急連絡先

- テレワークのことで分からないことがあったら以下に問い合わせてください。

  ＜問合せ先＞
  事業推進部　TEL：080-5338-5341（村岡）、080-4929-0036（玉田）
  Mail：jigyosuishin@asahieito.co.jp

- ウイルス感染の疑いや、情報機器や書類の紛失・盗難などのセキュリティ事故が起きてしまったら、速やかに以下に連絡してください。

  ＜緊急連絡先＞※夜間休日を問いません
  事業推進部　TEL：080-5338-5341（村岡）、080-4929-0036（玉田）
  Mail：jigyosuishin@asahieito.co.jp