ユーザ遵守事項規則

－マネジメントシステム共通の

情報セキュリティ対策のために従業者が遵守すべき事項－

2020/10/01 制定
＜修正履歴＞

2021/4/1	記述内容・文言に関する Aisel 現状に合わせた見直し、修正
2021/7/7	5.3(4)電子メール添付ファイルの取り扱いを追記
2022/2/17	2.6 文言修正
	3.1 管理者呼称、申請書名変更
	9.4(1)補足追記、(2)管理者追加
	10.3(11)(12)教育資料見直しに合わせ当該箇所の記述削除
2023/2/1	終了済サービス記述削除など現状に合わせた見直し、修正
	1.1 誤字修正
	5.3(5)例外追記
	6.2 項番修正
	10.2(3)個人情報の送付禁止、(6)参照先規程追記
	10.5(7)重複記載削除、項番更新
2023/10/01	マネジメントシステム文書管理規則の改訂に伴う文書名の変更
	3.1 持出持込申請書の申請先を変更
	8.1 パスワードの要件を変更
2024/2/1	5.4(2)電子メールで示されるリンク先の事前確認を追加
2025/2/1	10.5 消去・廃棄(9) 誤廃棄防止の再確認を追記
	10.5 消去・廃棄(10) 保管期限超過の定期確認を追記

株式会社アイセル

目次

1 総則

1.1 規則の位置付け

本規則は、「情報セキュリティ対策規則」における組織的、人的、物理的、技術的安全管理措置のうち、物理的安全管理措置について定めるものである。

1.2 目的

本規則は社員など当社の情報システムのユーザが情報漏えい等のセキュリティ事故を防止するために遵守すべき事項を定める。

1.3 適用範囲

「情報セキュリティ対策規則」中の以下の事項について適用される。

・ 4 物理的安全管理措置

1.4 対象者

「情報セキュリティ対策規則」で定められた対象者に示されたとおりとする。

1.5 引用規格

「情報セキュリティ対策規則」で定められた引用規格に示されたとおりとする。

1.6 用語の定義

「情報セキュリティ対策規則」で定められた用語の定義に示された通りとする。

2 職場環境におけるセキュリティ

2.1 クリアデスクポリシー

(1) 使用していない書類や媒体をキャビネット等へ収納し、机上等に放置してはならない。
(2) 重要度の高い書類や媒体を施錠保管し、特に必要な場合は耐火金庫・耐熱金庫に保管しなければならない。

2.2 クリアスクリーンポリシー

不正な操作や盗み見防止するため、離席時にはログオフするか、画面・キーボードロック等の保護機能を使用しなければならない。

2.3 事務・通信機器の取り扱い

(1) ホワイトボード等への書き込み内容を使用後に必ず削除し、放置してはならない。
(2) コピー機、FAX、プリンタ等の入出力書類を放置してはならない。特に重要度の高い書類は印刷および送受信の間、従業員が常に機器に(FAX の場合は送受信の両側とも)立ち会うようにしなくてはならない。
(3) FAX 送信時には必ず宛先を確認し、誤送信を防止しなければならない。

2.4 盗み聞きによる情報漏えい防止

電話や立ち話、オープンな会議スペースでの発言について、盗み聞きを防止するよう配慮しなければならない。

2.5 なりすまし侵入への注意

事務所への訪問や電話での顧客応対では「問い合わせ受付シート」に記録するとともに、登録されている電話にかけ直す、メールで回答するなど本人確認に十分注意すること。

2.6 廃棄時における再生防止

個人情報を含む紙資料の廃棄を行う者はシュレッター処理を、磁気媒体資料の廃棄を行う者はメディアシュレッダー等による破壊又は初期化処理を必ず行わなければならない。

3 パソコン等におけるセキュリティ対策

3.1 私物パソコンの使用禁止

(1) ISMS 管理責任者並びに情報システム管理者が許可する場合以外は、当社システム環境に私物パソコンを接続・利用してはならない。
(2) 当社システム環境に私物パソコンを接続・利用する必要がある従業員は「持出・持込申請書」「ネットワーク利用申請書」によって部門責任者に申請し、許可を得なければならない。

3.2 パソコンに導入するソフトウェア

(1) 会社が支給・貸与するパソコンには私的なソフトウェアやハードウェアを組み込むことを禁ずる。
(2) 業務上やむを得ず導入しなければならないソフトウェアは、情報システム管理者に利用の可否を仰いだ上で、部門責任者管理の元、導入しなければならない。

3.3 パソコンの他者利用の制限

席を離れる場合、他者が無断でパソコンを利用できないようにパソコンにロックを掛けなければならない。

3.4 パソコンでの情報の取り扱い

パソコンで一時的に個人情報や機密情報を取り扱う場合、取り扱い後には不必要となった情報を削除し、保持し続けてはならない。

3.5 ウイルス対策の徹底

パソコンを利用するすべての従業員は、パソコンを利用する上でウイルス対策を徹底しなければならない。

3.6 パソコンの移設

パソコンを利用するすべての従業員は、パソコンを勝手に移設してはならない。
（※ 移設とは、部門間の移動、社外への持出）

3.7 ノートパソコンの利用上の注意事項

(1) 社外へのパソコンの持ち出しは、原則禁止とする。但し、業務上必要な場合は持ち出しを認めるものとするが、その場合、部門責任者の許可を得なければならない。
(2) 部門責任者は、情報資産の持ち出しとして、当該パソコンの持ち出し管理をしなければならない。
(3) 社外にパソコンを持ち出す場合、盗難・窃盗に注意し取り扱わなければならない。
(4) 社外でパソコンを利用する場合、情報の盗み見に注意し利用しなければならない。

4 社内ネットワーク利用

4.1 社内ネットワーク及びインターネットの業務目的以外の利用禁止

(1) 社内ネットワークは会社の情報資産であり、電子メールやWebなどのサービス利用において、業務目的以外の使用を禁止する。
(2) 情報システム管理者の許可無く、社内ネットワーク上に、電子メールサーバや Web サーバ、FTP サーバなどを構築してはならない。
(3) 他人の利用者IDを用いて、社内ネットワーク及び社外ネットワーク、インターネット上のサービスへアクセスしてはならない。
(4) ネットワーク利用者は、故意もしくは不注意を問わず、社内ネットワーク及び社外ネットワーク、インターネット上のサービスに対して、許可された権限以上のアクセスを行ってはならない。

4.2 ネットワークを利用した機密情報の送受信

(1) ネットワーク利用者は、当社の事業に関わる情報や、顧客や従業員のプライバシーに関わる情報など機密性の高い情報が社外へ漏洩することを防ぐために、部門責任者の許可なくファイルのアップロードや社外への送信を行ってはならない。
(2) 出所が不明なファイルや内容の確証が得られないファイルの入手や実行をしてはならない。

4.3 インターネットで利用可能なサービス

(1) ネットワーク利用者は、インターネットの利用において、電子メール及び Web 閲覧など、情報システム管理者により許可されている機能以外のサービスを使用してはならない。
(2) 暗号通信を用いたインターネットへのアクセスをする場合は情報システム管理者の許可を得たサービスのみとすること。

4.4 電子メールサービス

ネットワーク利用者は、社内ネットワークに接続したパソコンにおいて、自社の電子メールサービス以外の電子メールサービスを利用してはならない。尚、業務上必要な場合は、情報システム管理者に利用の可否を仰いだ上で、部門責任者の許可を得て利用しなければならない。

4.5 ネットワークモニター

ネットワーク利用者は、社内ネットワークにおいて、ネットワークモニターなどの、ネットワーク上を流れるパケットを盗聴できる機器及びソフトウェアを使用してはならない。
但し、情報セキュリティマネジメントシステム管理責任者が許可した調査及び監視目的のネットワーク調査は実施できるものとする。

4.6 ID及びパスワード、証明書の管理

ネットワーク利用者は、社内ネットワークや各種サービスの利用者ID及びパスワード、証明書を適切に管理しなければならない。

4.7 社内ネットワークへの接続時の注意事項

(1) 自宅や他組織のネットワークへ接続したパソコンは、ウイルスチェック等のセキュリティ検査を実施し、異常が発見されなかったことを確認した後でなければ、社内ネットワークに接続してはならない。
(2) ネットワーク利用は、与えられたIPアドレス以外のIPアドレスを使用してはならない。
(3) ネットワーク利用者は、社内ネットワークに接続中のコンピュータを、許可されていない電話回線、携帯電話、無線LAN、専用線などを利用して、社外のネットワークへ接続してはならない。

※ テレワークに関わる事項に関しては、「11.テレワークにおけるセキュリティ」に基づいて運用すること。

5 電子メールサービス利用

5.1 電子メールサービス利用端末機器のセキュリティ

(1) 電子メールの送受信にあたっては、許可されていない電子メールソフトウェアを用いることを禁ずる。
(2) 電子メールアドレスは初期パスワードとともに発行される。初期パスワードは直ちに変更しなければならない。また、パスワードは最低6ヶ月（推奨 3 か月）に 1 度定期的に変更しなければならない。（社内システムにおいて定めのある場合は、それに従う）
(3) 電子メールの利用者は、電子メールソフトウェアにパスワードを保存してはならない。

5.2 電子メールで送受信される情報の保護

(1) 当社の事業に関わる情報や、顧客、従業員のプライバシーに関わる情報などの機密情報は、原則として電子メールを用いて送信してはならない。
(2) 電子メールの送信にあたっては、送信先のメールアドレスに間違いがないか、確認の上送信しなければならない。
(3) 当社のセミナー案内や製品ご紹介メールなどのように、社外の複数のドメインが混在するメールアドレスに対して 1 通の電子メールで同報送信する場合は、送信先メールアドレスが受信者間で閲覧できないよう、設定しなければならない。
また、広告メール等の送信にあたっては、国内法を遵守しなければならない。
(4) ファイルの添付については、行わない事が望ましい。添付の必要がある場合は、展開時にパスワードを求める暗号化設定を行わなければならない。

5.3 電子メールサービスとネットワーク保護

(1) 業務目的以外に電子メールサービスを利用してはならない。
(2) スパムメールを受信した場合は、これを転送してはならない。
(3) 社外のメーリングリストに参加する場合は、当該メーリングリストの信頼性、および業務への必要性を充分考慮した上で参加しなければならない。また、参加意義の無くなった場合は、直ちに脱退しなくてはならない。メーリングリストでは会社に不利益となる発言や、公序良俗に反する発言をしてはならない。
(4) 電子メールの送信にあたっては、送信するメールサイズを考慮しなければならない。メールサイズが大容量となる場合は、ネットワーク負荷の観点から、代替の送信手段を講じなければならない。

(5) 無用な電子メールを送受信することにより、ネットワークに負荷をかけてはならない。また、電子メール送信時に、必要時以外はテキスト形式で送信するように電子メールソフトウェアを設定しなければならない。

5.4 電子メールを介したウイルス被害の防止

(1) 送信元不明のメールに添付されたファイルや、マクロや実行形式のまま添付されたファイルなど、不審な添付ファイルに対してはこれに操作を加えてはならない。
(2) 受信したメールで示されるリンクについて、目視や文字列検索でリンク先を事前に確認しなければならない。
なお、QR コード画像などの場合でも、事前にリンク先を確認すること。
(3) ファイルを添付してメールを送信する場合、当該ファイルのウイルス感染が無いことを必ず確認しなければならない。

6 Web サービス利用

6.1 業務目的以外の利用禁止

(1) 社内ネットワーク利用者は、社内及びインターネット上の Web サービスは、業務上必要な場合のみ利用できる。
(2) 社内ネットワーク利用者は、Web サーバを利用した電子メールの送受信を行ってはならない。
(3) 社内ネットワーク利用者は、信頼できない Web サービスを利用してはならない。
(4) 社内ネットワーク利用者の情報の発信(掲示板などへの書き込み)に関しては、部門長が業務上必要と認めた場合のみ許可される。このとき、情報の正確性を確保し、必要最小限の範囲で発信するものとする。また、下記に該当する情報の発信や閲覧は禁止する。
・著作権、商標、肖像権を侵害するおそれのあるもの
・プライバシーを侵害するおそれのあるもの
・他者の社会的評価にかかわる問題に関するもの
・他者の名誉・信用を傷つけるおそれのあるもの
・会社の信用・品位を傷つけるおそれのあるもの
・性的な画像や文章に該当するおそれのあるもの
・不正アクセスを助長するおそれのあるもの
・差別的なもの
・虚偽のもの
・社内の機密情報

(5) 社内ネットワーク利用者は、社内外の Web サービスに攻撃等不正なアクセスを行ってはならない。また、攻撃や不正アクセスを目的として社内外のシステムを利用してはならない。
(6) 社内ネットワーク利用者は、社内外の Web サービスに対して、他人の利用者IDやパスワードなどの認証情報を利用してアクセスしてはならない。

6.2 Web ブラウザ利用端末機器のセキュリティ

(1) 社内ネットワーク利用者は、Web ブラウザの利用にあたって、許可されていない Web ブラウザを用いてはいけない。
(2) 社内ネットワーク利用者は、署名の無い ActiveX や Java、JavaScript、VBScript などのコードは実行してはならない。
(3) 社内ネットワーク利用者は、許可されていないソフトウェアもしくはファイルを入手して、実行や閲覧をしてはならない。
(4) 社内ネットワーク利用者は、リンクをクリックするとき、リンク先を確認してからアクセスしなければならない。この場合、リンク先が信頼できないアドレスである場合は、アクセスしてはならない。また、バナー広告についても同様で業務上必要のないバナー広告はクリックしてはならない。

6.3 社内ネットワークでの Web 閲覧

(1) 社内ネットワーク利用者は、情報システム管理者の許可を得ないで Web サービスや情報を他部門や子会社へ公開する目的のサーバは立ち上げてはならない。
(2) 社内ネットワーク利用者は、業務上不必要なファイルやソフトウェア、不審なファイルなどを、入手してはならない。必要なファイルやソフトウェアであっても、Web から直接実行せず、必ず保存後にウイルスチェックを実施してから表示、実行しなければならない。

6.4 アクセス制御された Web サイトの閲覧に関して

(1) 社内ネットワーク利用者は、パスワードを Web ブラウザに記憶させる行為を行ってはならない。
(2) 社内ネットワーク利用者は、離席する場合は必ず、Web ブラウザを終了させるか、OS のパスワード付スクリーンロックを実施しなければならない。

7 媒体の取り扱い

7.1 パソコン（IT 製品）の修理

パソコン等の修理を依頼する者は、機密性の高い情報が読み出し可能な状態で保管されていないことを確認した上で修理を依頼しなければならない。故障の状況により、保管されている情報の確認や保護が実施できない場合には、ハードディスク等の情報が保管されている装置を取り外して修理を依頼しなければならない。

7.2 媒体の保管

個人情報など機密性の高い情報を媒体に保存する者は、権限のない者が保管された情報にアクセスできないよう暗号化を行うか、媒体を鍵のかかる場所に保管し、鍵は容易に持ち出しができない場所に保管しなければならない。

7.3 媒体の移動

すべての従業者は、機密性の高い情報を保管した媒体を、その情報の管理責任者の許可なく社外へ持ち出してはならない。

7.4 媒体の再使用

すべての従業者は、機密性の高い情報が保存されている媒体を再利用する前に、保存されていた情報を、再生できない方法で消去しなければならない。

7.5 パソコン（IT 製品）と媒体の廃棄

パソコン（IT 製品）の廃棄を行う者は、ハードディスク等記憶装置を再生不能な状態に破壊してから指定された事業者を通じて廃棄しなければならない。

8 パスワード管理

8.1 パスワード長

パスワードは安全性の高いものにすること。具体的な基準は ISMS ユーザーズガイドに記載する。

8.2 推測回避

一般に使われている単語や本人の趣味、プライベートなどから、他人に推測されやすいパスワードを使用してはならない。

8.3 パスワード変更

パスワードは 6 か月に1度（推奨は 3 か月）を目安に更新すること。
（社内システムにおいて定めのある場合は、それに従う）

8.4 パスワードヒント

パスワードは口外してはならない。また、ヒントとなるような物品を身の回りに置いてはならない。

8.5 パスワードの連続使用禁止

一度使用したパスワードを連続で使用してはならない。

9 ウイルス対策

9.1 アンチウイルスソフトの利用

(1) パソコンに導入されたアンチウイルスソフトを常駐設定にし、ファイルのアクセスおよび電子メールの受信時には、常時スキャンできるように設定しなければならない。
(2) 常時スキャンだけではなく、一週間に一度ファイル全体に対するスキャンを実施すること。
(3) 定義ファイルを毎日一度は更新するように設定しなければならない。

9.2 パソコンのセキュリティ対策

パソコンに導入されているソフトウェアを最新状態に維持しなければならない。

9.3 パソコンにおける電子メールを介したウイルス被害の防止

電子メールの利用にあたっては、電子メール保護機能を有効にしなければならない。
また、前項 5.4 の対策実施に努めること。

> **5.4 電子メールを介したウイルス被害の防止**
>
> (1) 送信元不明のメールに添付されたファイルや、マクロや実行形式のまま添付されたファイルなど、不審な添付ファイルに対してはこれに操作を加えてはならない。
> (2) 受信したメールで示されるリンクについて、目視や文字列検索でリンク先を事前に確認しなければならない。
> なお、QR コード画像などの場合でも、事前にリンク先を確認すること。
> (3) ファイルを添付してメールを送信する場合、当該ファイルのウイルス感染が無いことを必ず確認しなければならない。

9.4 アンチウイルスソフトがウイルスを検知した場合

(1) ウイルスを発見した場合は、アンチウイルスソフトの駆除機能を使用してウイルスを駆除しなければならない。(「緊急事態対応計画」に基づくインシデント処理を実行する)
(2) 駆除した結果は、ISMS 管理責任者並びに情報システム管理者に報告しなければならない。

9.5 ウイルスに感染した場合

(1) 使用中のパソコンで、以下のような異常が疑われる症状が発生した場合には、当該機器をネットワークから切り離した上で情報システム管理者に報告し、対処について指示を仰がなければならない。
- パソコンの動作が異常に重くなった。
- ウイルス付のメールが送られたとの情報を得た。
- 突然、画面上に予期しない表示が行われた。(花火、うず巻きなど)
- ファイルを開こうとしたら、予期しないマクロの警告ポップアップが出た。

(2) ウイルスが検知された場合は、そのウイルスの特性上どのような挙動を示すかを予測し、影響範囲の特定を実施しなければならない。ウイルスが検知されない場合は、ファイアウォールのログを確認し、疑わしいログが残っていないか確認するなど、可能な限り原因を特定しなければうならない。

10 個人情報の取り扱い

10.1 取得・入力の対策

(1) 個人情報の入力画面では必ず暗号化を行うものとする。
(2) Web 上での個人情報収集について新たに安全対策を行なう場合は、その有効性について評価を行い、結果を管理責任者に報告すること。
(3) 個人情報の本人に、個人情報を提供することの任意性、および個人情報を提供しない場合に生じる結果について明示し、Web 上で本人の同意を得る仕組みをつくること。
(4) 書類を回収する際は、回収もれや紛失のない様、受領チェックを行うこと。
(5) 誤入力を防ぐため、入力チェックを別の人間が行うこと。
(6) 作業中の誤操作や消失に備えて、対象データの退避やバックアップを定期的に行うこと。

10.2 移送・送信の対策

(1) 個人情報を郵送する場合は、書留を利用するなど追跡可能な方法で行うものとする。
(2) メール送付する場合は、送信実行前に見直しを行うなど、宛先を再確認しなければならない。
(3) メールによる個人情報の送付は禁止する。やむを得ず対応する場合は暗号化情報にして送付する。暗号解除するパスワードは、相手方担当者へ電話など、別の手段で連絡する。
(4) FAX で送信する場合は、送信前に宛先を再確認しなければならない。また送信レポートにて宛先を再度確認するものとする。
(5) 宅配を利用して送付する場合は、梱包材や封緘に剥がすと印の残るシールを利用するなどの開封確認可能な措置を行うものとする。
(6) ノートパソコンを社外へ持出する場合は、起動時パスワードなど「情報セキュリティ対策規則」に則った設定を行い、鞄に入れるなどして安全に持ち運ぶこと。
(7) ノートパソコンを社外へ持出する場合は、電車の棚に置いたり、店内でノートパソコンをテーブルに置いたまま席を離れたりなど、手元から離れる行動を行わない。
(8) 携帯電話を持出しする場合は、ストラップを使用する等、盗難・紛失対策を行うこと。
(9) 記憶媒体にデータを保存する場合は、アクセスパスワードの設定や暗号化などを行うこと。
(10) 訪問で手渡しする場合は、移動中に書類を電車の棚に置いたり、車内に置いたまま車から離れたりなど、手元から離してはいけない。また、提出前に、渡すべき書類に間違いないかを必ず再確認すること。

10.3 利用・加工の対策

(1) 個人情報の一時保管は専用のトレイに分け、帰宅時には、鍵のかかる棚に保管する。
(2) 個人情報や機密情報が印刷された紙の、裏紙使用を禁ずる。
(3) 個人情報を記録する記録媒体には必ず、データ名と個人情報である事を記載すること。紙媒体の場合は、ファイル等に個人情報である事を記載する。
(4)「個人情報授受記録」が必要とされる個人情報の受け渡しについては、各業務担当部署で記録を残すこと。
(5) コピー、プリンタを使用した際は、速やかに使用した者が印刷物を回収すること。
(6) FAX が届いたら、速やかに印刷物を回収すること。
(7) 個人情報の複製は、管理責任者が許可した範囲内で行なうこと。
(8) ビルの中であっても、社外(扉の外)では個人情報の口外は厳禁とする。
(9) 携帯電話での会話、ビル内のトイレ、エレベータ内、道中の会話、喫茶店などでの会話では、周囲に個人情報や機密情報が漏洩しないように注意すること。
(10) 自宅での業務は原則禁止し、管理責任者が許可した場合のみ可能とする。

10.4 保管・バックアップの対策

(1) 個人情報を棚に保管する場合は、鍵つき棚に保管すること。
(2)「入退室管理記録」の項目に、棚の施錠をチェックする項目を含め、最終退社者が施錠を確認すること。
(3) 情報セキュリティマネジメントシステム管理責任者は鍵の保管場所、配布状況、スペアキーの作成状況を把握する。
(4) 個人情報を机の引出しに保管する場合は、鍵つきの引出しに保管すること。
(5) 各自が使用している棚や引出しは、各自で帰宅時に施錠すること。
(6) クリアデスクを徹底すること。
(7) 帰宅時や離席時には、机上に個人情報が見える状態で残さないこと。

10.5 消去・廃棄の対策

(1) 紙媒体の個人情報は、全てシュレッダー処理を行なう。
(2) シュレッダー機を設置し、その日のうちに各自がシュレッダー処理を行う事とする。
(3) 処理対象が大量な場合は、情報セキュリティマネジメントシステム管理責任者の承認を得た上で廃棄業者へ依頼する。
(4) 廃棄業者と機密保持契約書を締結し、廃棄処理の実施毎に、廃棄証明を取得する。
(5) 廃棄する場合は、データの削除だけでなく、媒体を物理的に破壊してから廃棄する。
(6) 業者へ引き渡す前に、ディスク消去ソフトを使用し、データの完全消去を実施する。

(7) 借用資産を返却する前に、データの完全消去を実施する。
(8) 加工途中でデータを削除する場合は、必ず2度確認を行い、注意を徹底する。また、サーバ上に、バックアップデータを残すようにする。
(9) 保管期限内の個人情報を誤って消去・廃棄しないか、再確認や別人格によるダブルチェックなど、複数回確認すること。
(10) 保管期限を超過した個人情報を保管したままになっていないか、定期的に棚卸確認を実施すること。

11 テレワークにおけるセキュリティ

当社における技術的安全管理措置は、「セキュリティーガイドライン（テレワーク版）」において定めるものとする。