AISEL
【ISMS】ユーザーズガイド

2024年2月版

マネジメントシステム推進事務局

AISEL

顧客満足の一歩先へ

～目次～

1．ISMSの目的

AISEL
顧客満足の一歩先へ

【概略】

アイセルでは、国際規格ISO 27001及び日本国内規格JIS Q 27001に規定される組織における情報セキュリティ管理のスキームを活用し、社内の情報セキュリティマネジメントシステム(ISMS)を策定しています。

ISMSはアイセルの社内ルールとして情報資産の取り扱いやリスク対策、社員の意識向上などを目的として運用され、毎年PDCAを回すことによってマネジメントシステムの継続的な取り組み、継続的な改善を目指すものとなっています。

また、アイセルのISMSは外部の第三者審査機関によって定期的に審査を実施し、これに合格することでアイセルのマネジメントシステムが規格に沿った運用を実現できていることを示す認証マークを利用することが許されています。

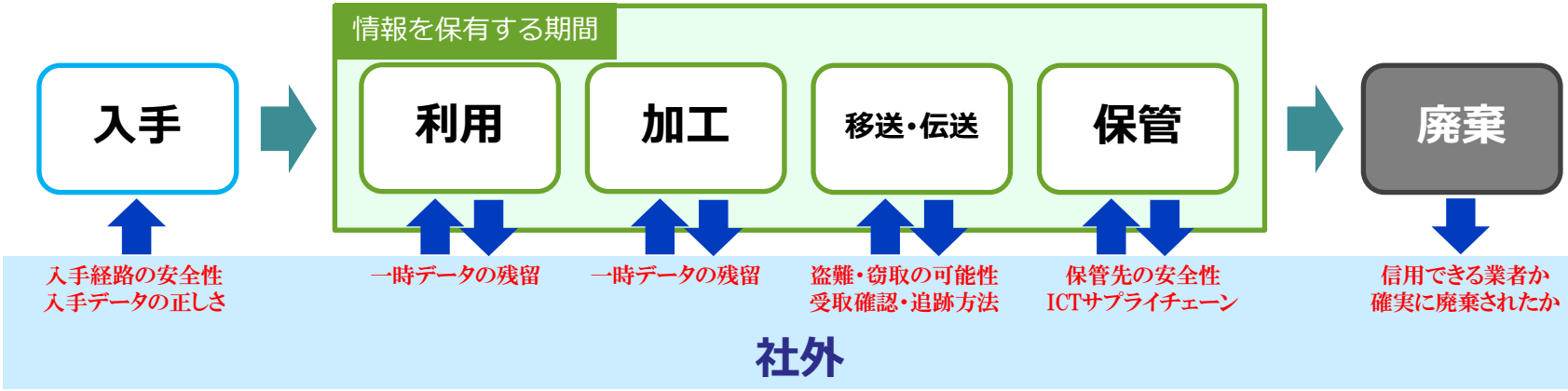
ANAB ANSI National Accreditation Board ACCREDITED ISO/IEC 17021-1 MANAGEMENT SYSTEMS CERTIFICATION BODY
bsi
ISMS-AC ISMS ISR004

IS 533103
ISO/IEC 27001:2013 & JIS Q 27001:2014

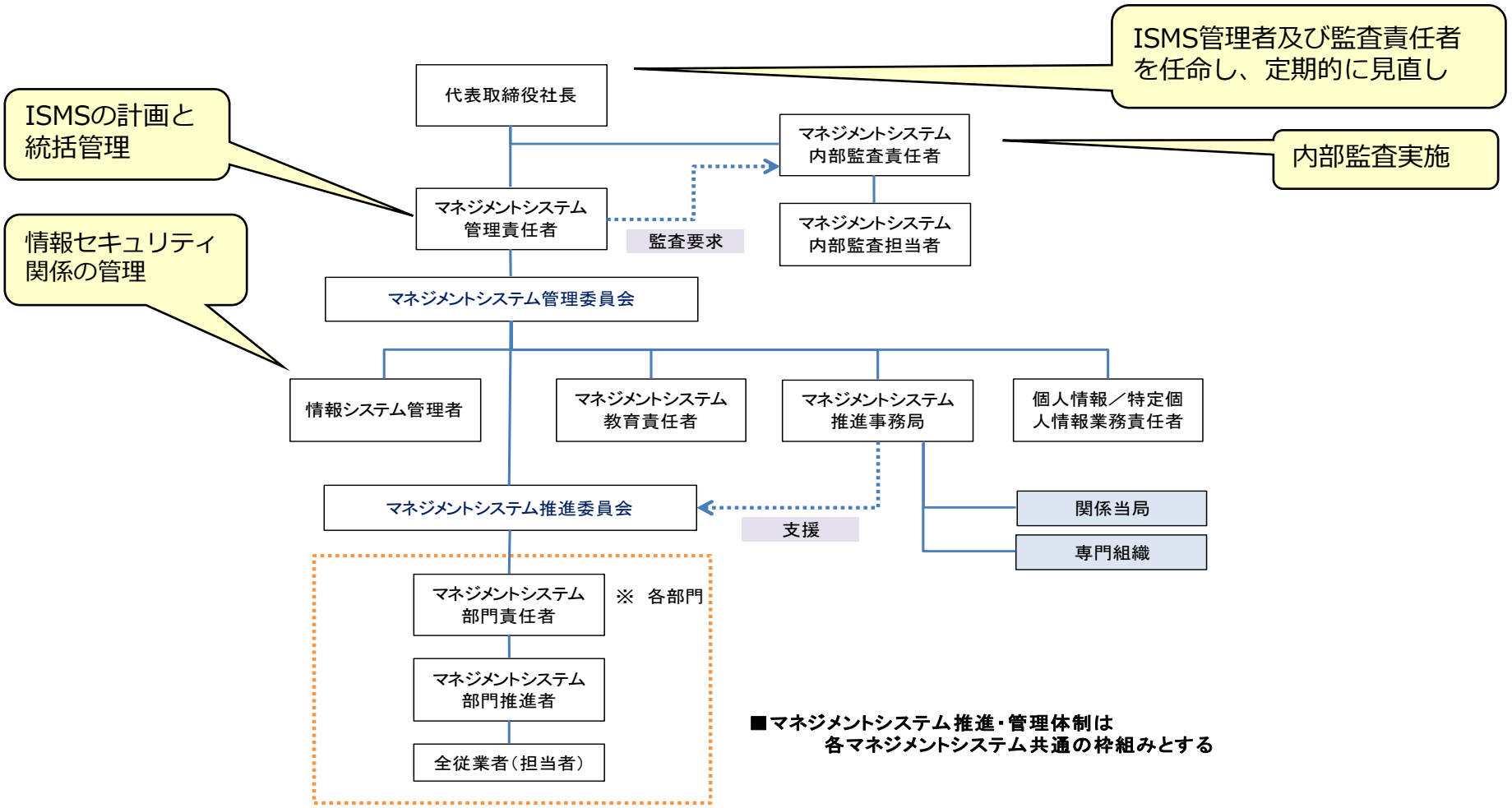
◀ 社員の名刺、アイセルホームページに掲載されている、
外部機関によるISMSの認証マーク。
認証マークの有無は企業の信頼性を表す指標として利用されるが、認証があるから情報を守れているのではなく、あくまで**社員全員による情報セキュリティへの取り組みこそが情報を守る**ものである。

【情報資産保護のライフサイクル】

情報セキュリティ保護対象となる情報資産は次のサイクルでライフサイクルを大別することができ、各段階に応じたリスクの洗い出しと対策が必要です。併せて、外部(取引先会社、サービス利用先、その他利害関係者等)との情報の流通局面が大きなリスク源となるため、特に注意することが必要です。



2．アイセルのISMS推進体制



アイセルでは、社長の指示のもと全社で当社のISMS体制を構築しています。
この体制は情報セキュリティが適切に運用しているかの管理監督を担う機構として、
またISMSを継続的に改善するためのフロー、緊急時に適切な対応を取るためのフローとして機能しています。

※この体制は、個人情報保護マネジメントシステム(PMS)と共通の体制となっています。

3．ISMSの文書体系

AISEL
顧客満足の一歩先へ

No	文書名	内容	掲載場所
1	情報セキュリティ基本方針	アイセルとしての情報セキュリティの考え方を示す文書	ホームページ、 アイセルポータル
2	マネジメントシステム統合規程	ＩＳＭＳマニュアルの上位となるマネジメントシステムの共通規程	アイセルポータル
3	ＩＳＭＳマニュアル	ISMSの主となるセキュリティ全般に関するマニュアル	
4	情報セキュリティ対策規則	ISMS運用に関する技術的管理策を定めた規則	
5	情報システム管理規則	技術的管理策の詳細規則	
6	ユーザー遵守事項規則	情報セキュリティ対策の為に従業者が遵守すべき事項を示す文書	
7	事業継続管理規則	事業継続に関する規則	
8	ISMSユーザーズガイド	ISMSに関する規定をユーザ向けに整理したガイド（本書）	
9	セキュリティガイドライン （テレワーク版）	テレワーク（リモート勤務）におけるセキュリティに関する事項	

これらは、 ISMS運用に関わる主な文書です。
ISMSユーザガイド（本書）は特に皆さんの日々の業務上での注意点について記載しています。
業務で情報の管理・取扱いに困ったら参照するようにしてください。

4．情報資産の管理

AISEL
顧客満足の一歩先へ

- 紙媒体の機密区分

当社の取扱う情報の管理レベルとして**「極秘」**、**「部外秘」**、**「社外秘」**、**「公開」**の4種類が設定されています。
管理レベルの決定及び変更は、情報セキュリティの管理者が行い、「情報資産台帳」を随時更新してください。

- 紙等の媒体の場合、ファイルフォルダーの中に綴じられている最高レベルの情報区分表示を表紙又は背表紙にすることにより、綴じられている用紙への表示を省略して簡素化できるものとする。
- 電子ファイルの場合は、アクセス制御がされたサーバ、フォルダーに保管するものとし、それ以外に保管する場合はフォルダーおよびファイル単位に暗号化、アクセスパスワードなどによるアクセス制御を施すこととする。

○　複数の管理レベルのものが含まれる場合は、最高レベル情報のアクセス制御を施すこととする。

表１　情報の分類および取扱い方法（紙など）

<table>
<tr><th colspan="2">情報分類区分</th><th>極　秘</th><th>部外秘</th><th>社　外　秘</th><th>公開</th></tr>
<tr><td colspan="2">管理責任者</td><td colspan="2">・部門長</td><td>・担当者</td><td>・指定なし</td></tr>
<tr><td rowspan="2">保管形態</td><td>書類ケース、バインダー等の場合</td><td>・ラベル付け（赤色）</td><td>・ラベル付け（黄色）</td><td>・ラベル付け（青色）</td><td>・指定なし</td></tr>
<tr><td>単体の場合</td><td>・confidentialと記載</td><td>・バインダー等で保管</td><td>・規制なし</td><td rowspan="6">・規制なし</td></tr>
<tr><td colspan="2">保管場所</td><td colspan="3">・鍵付きキャビネット</td></tr>
<tr><td colspan="2">複製及びバックアップ</td><td rowspan="2">・原則禁止</td><td rowspan="2">・管理責任者の許可</td><td rowspan="2">・上長の許可</td></tr>
<tr><td colspan="2">持出</td></tr>
<tr><td colspan="2">FAX利用</td><td colspan="3">・送信前または送信後電話連絡</td></tr>
<tr><td colspan="2">媒体の再利用</td><td colspan="3">・不可</td></tr>
<tr><td colspan="2">廃棄</td><td colspan="3">・シュレッダー、または溶解</td></tr>
</table>

4．情報資産の管理

AISEL
顧客満足の一歩先へ

- 電子ファイルの機密区分

電子ファイルの場合情報の管理レベルごとに保管先を分け、管理レベルに応じてアクセス可能な社員が割り当てられていることを確認してください。

複数名で一つのアカウントを共有すると、特定の情報とかかわりのない社員が閲覧・編集などができてしまう場合があります。それが事故の発生につながったり、事故原因の調査に支障を与える可能性があるため、アカウントは各社員に個別に作成、付与するようにしてください。

媒体の廃棄については現場で判断がつかない場合がありますので、廃棄方法が明確に決定できない場合は情報システム管理者まで問い合わせるようにしてください。なお、情報システム部門ではHDDについては外部の業者に破壊を依頼し、破壊されたことを証明する写真を残すようにしています(プラッタの破壊など)

表２　情報の分類および取扱い方法（データ）

<table>
<tr><th>情報分類区分</th><th>極　秘</th><th>部外秘</th><th>社外秘</th><th>公開</th></tr>
<tr><td>管理責任者</td><td colspan="2">・部門長</td><td>・担当者</td><td>・指定なし</td></tr>
<tr><td>保管場所</td><td colspan="3">・アクセス制御されたサーバ、またはＰＣ
・常時施錠の鍵付きキャビネット</td><td rowspan="5">・規制なし</td></tr>
<tr><td>複製の作成</td><td rowspan="2">・原則禁止</td><td rowspan="2">・管理責任者の許可</td><td rowspan="2">・上長の許可</td></tr>
<tr><td>持出</td></tr>
<tr><td>バックアップ</td><td colspan="3">・アクセス制御されたサーバへ保存</td></tr>
<tr><td>メール添付</td><td colspan="2">・暗号化、またはパスワード</td><td>・社内メールは、規制なし
・社外メールは、同左</td></tr>
<tr><td>媒体の再利用
および廃棄</td><td colspan="3">・完全消去ソフトによる削除、または媒体の破壊</td></tr>
</table>

5．セキュリティ区画と入退館

AISEL
顧客満足の一歩先へ

【物理的セキュリティ境界線とセキュリティ区画】

当社のオフィスは、外壁およびカードで制御された入り口で外部からの無断進入を防ぎ、許可された者のみが入室できる設備を設けるものとし、以下のセキュリティ区画の各レベルを設定する。

＜セキュリティ区画＞

レベル1　：　訪問者が出入り可能　東京本社…受付、会議室　大阪支社…なし　佐賀SC…受付

レベル2　：　カード認証により入室が可能　※部外者が入室する場合は、立会いが必要

◇東京本社はレベル2エリア内にアイセルグループ会社のファーストステップ社が入居しているため、物理的セキュリティ境界を示す看板を境界部に設置しています。

レベル3　：　サーバ室　　特別に許可された者のみ認証カードによりドアを開閉する。
※部外者が入室する場合は立会いが必要

◇カード認証扉についての注意◇

認証カードを用いて入退室するときは他の人物が開いた隙に**カード無しで扉を通り抜ける（共連れ）行為がないよう**注意してください。

【一般の人の立ち寄り場所および受け渡し場所】

- 品物の受け渡しはオフィスの受付にて行い、オフィスへの入室はさせないようにする。
- やむを得ずオフィスに入室させる場合は必ず社員が立会い、目的以外の行動をしないように監視する。

※社員、BP以外の外部来客はレベル2以上の区画で一人にしないこと！立ち入りの場合は周囲に声がけを行うこと！

【不審な人物を見かけた場合は】

- セキュリティ区画内で不審な人物を見つけた場合は、声をかけて目的を確認すること。
声をかけることに危険性を感じた場合は管理部に報告を行い、管理部が対応を引き継ぐこととする。

【会議室利用についての注意】

- 会議室は訪問者が入室可能な区画（レベル1）であるため、貴重品、機密資料等を放置して無人状態にしないこと。
- 上記と同じ理由で、打合せ時に使用したホワイトボードに書かれた情報は確実に消去して退室すること。

6．社内ネットワークの利用

AISEL
顧客満足の一歩先へ

■私物の機器(ノートPC、スマートフォン、タブレット等)の接続は**有線・無線ネットワーク共に禁止**とする。
■ネットワーク全体が利用不能になる恐れがあるので、個人や部署の判断でネットワークスイッチや、無線アクセスポイント等、情報システム部門の把握していない機器を接続してはいけない。
→**全社の業務に悪影響が出る可能性があるため、絶対にしないこと。**

【有線ネットワークの利用】

＜東京本社＞

◇ネットワーク利用のみの場合

執務エリアの青いLANケーブルに機器を接続するとDHCPサーバによって自動的にIPアドレスが割り当てられる。

◇ネットワーク利用に加えてクライアントPCで固定IPが必要な場合

社内ネットワークへの接続は、情報システム管理者の承認により、発行されたIPアドレスを利用するものとする。なお、利用を停止する場合は、情報システム管理者へ報告し、IPアドレスを解放する。

＜大阪支社、佐賀SC＞

社内ネットワークへの接続は、各拠点の情報システム管理者の承認により、発行されたIPアドレスを利用するものとする。なお、利用を停止する場合は、情報システム管理者へ報告し、IPアドレスを解放する。

（利用時の注意点）

- ウイルス対策ソフトなどの強制ソフトウェアが導入されていること。
- IPアドレスの転貸（又貸し）は行わないこと。

【無線ネットワーク(wifi)の利用】

＜東京本社＞

ネットワーク利用申請を記入し、無線LANパスワードの入力を情報システム部門に依頼すること。

＜大阪支社、佐賀SC＞

ネットワーク利用申請を記入し、無線LANアクセスポイントへのMACアドレス登録を情報システム部門に依頼すること。その後、各拠点の情報システム管理者からIPアドレスの割当と設定方法について指示を受けること。

7．サーバの設置と管理

AISEL
顧客満足の一歩先へ

【サーバの設置】

サーバの設置を行う場合、サーバ調査票を記入し、ISMS部門責任者および情報システム管理者の承認を得た上で設置するものとする。

サーバ管理者は、不要なサービスの停止やアカウントの削除を行い、不正アクセス防止に努めること。

サーバ管理者は、サーバ調査票に記載されているバックアップ、ログ監視、サービス提供、アカウント管理を行い、定期的に監視結果の報告及び設定の見直しを行うこと。

（注意点）
- サーバとは、個人に割り当てられた事務用PCを除き、開発やサービス提供を目的とした共同利用マシンを意味します。
- サーバと認定されたマシンは、IPアドレス一覧にサーバ区分を設定して管理します。

8．アクセス方針とアカウント申請

AISEL
顧客満足の一歩先へ

【アクセス方針マトリックス】

業務システム	役員	執行役員/部長	一般社員	業務担当者	業務管理者	マシン管理者
社内Webシステム	利用権限	利用権限	利用権限	変更権限	–	ＯＳの管理者権限
Microsoft 365	利用権限	利用権限	利用権限	利用権限	ＡＰの管理者権限	ー
給与会計（PCA）	–	–	–	利用権限	ＡＰの管理者権限	ＯＳの管理者権限
事業部共通ファイルサーバ （事業部内サーバ）	変更権限	変更権限	変更権限	–	–	ＯＳの管理者権限
部門共通ファイルサーバ （部門内サーバ、開発サーバなど）	参照権限	変更権限	変更権限	–	–	ＯＳの管理者権限
業務共通ファイルサーバ （予算管理サーバなど）	変更権限	変更権限	–	–	–	ＯＳの管理者権限
TKC	–	–	–	利用権限	ＡＰの管理者権限	ＯＳの管理者権限

※ファイルサーバとは物理マシンのことではなく、アクセス権を付与するサービスを指す
※利用権限、変更権限、参照権限では、権限が付与できる範囲は、職務分掌に定められた業務範囲に限る

【アカウント申請手続き】

○手続きフロー・・・人事担当者又は担当部長 → 各サーバ管理者

9．パスワード管理、スクリーンロック

AISEL
顧客満足の一歩先へ

【パスワード作成基準】

パスワードは以下の規則に従って設定を行うこと。

1. 英大文字小文字＋数字＋記号で10桁以上が望ましい。
   （内閣サイバーセキュリティセンターの「インターネットの安全・安心ハンドブック ver.5.00」より）
2. 設定されたパスワードは3ヶ月に一度を目安にパスワードを更新することが望ましく、**6ケ月に一度、必ず更新**すること。
   但し、社内利用のサービス（アイセルポータル、MA-EYES、Windows AD、等）ごとにパスワードの有効期限が定められているため、期限切れのメッセージが出た場合はその都度指示に従ってパスワードの変更を行うこと。
3. 設定したパスワードは紙などに書き留めてもよいが、対象システムが特定できたり、パスワードの文字列そのものを「あらわに」表示してはならない。
4. パスワードを口外すること、ヒントとなるような物品を身の回りに置いておいてはならない。
   特にノートPC本体やモニタ等にパスワードの貼り付けを行うことは厳禁とする。
5. 一度使用したパスワードを連続で使用してはならない。

【スクリーンロック】

＜workgroup運用のPCの場合＞

貸与された事務用PCは急な離席の発生に備えてあらかじめスクリーンセーバー設定を行うこと。
画面復帰時にWindowsログオンを求める設定にし、前項パスワード作成基準に従ってパスワード設定を行うこと。
スクリーンセーバー起動までの時間は5～10分で設定すること。

＜AD参加PCの場合＞

AD参加PCはADサーバによってセキュリティ設定が配布されるため、設定作業は発生しない。

- PCから離席するときは「ctrl」+「alt」+「del」や、Windowsキー +「L」で画面のロックを行うこと。
- 画面のスクリーンショット取得は、動作検証など業務遂行に必要な場合のみとすること。
- カメラ画像（写真や動画）を撮影する場合に、機密事項や会話、個人情報が映り込まないようにすること。

１０．ウイルス対策

AISEL
顧客満足の一歩先へ

【ウイルス対策ソフトの管理】

- 指定されているウイルス対策ソフトを入れウイルス対策を講じること。
  (基本的には情報システム部門でインストール済みの状態で貸与されるので、その状態を維持する)
- OSのセキュリティパッチの情報に注意し、必要に応じ最新のパッチをインストールすること。
- ウイルス感染を早期に発見するため、常にウイルスチェックを稼働し、ウイルス対策ソフトを最新の状態にアップデートして定期的にウイルス検査を行わなければならない。
- ウイルスの被害に備えるため、ファイルのバックアップを定期的に行い一定期間保管しなければならない。
- 外部より入手したファイルおよび共用するファイル媒体は、ウイルス検査後に利用しなければならない。

★ もし、ウイルスに感染してしまったら・・

ウイルスに感染したマシンをネットワークから隔離し、すぐにISMS部門責任者に連絡し指示を仰ぐこと。
ISMS部門責任者からの指示があるまでネットワークへつなげてはならない。

※詳細は「１９．緊急事態の対応」を参照し、処置すること

【社外に持出したPCを社内ネットワークに接続する場合】

社外で外部と接続したPCを持ち帰って社内ネットワークに接続する場合は、必ず、ウイルスチェックをかけること。

※持込PCに関しての詳細は「１４．PC等の情報資産の持込、持出」を参照すること

１１．メールの利用

AISEL
顧客満足の一歩先へ

社員は業務の遂行を目的として、以下の注意点に留意して電子メールを利用することができる

- 添付ファイルの大きさは、ネットワーク利用のマナー、サーバ負荷増大を防ぐ観点から常識の範囲内(数MB)程度までとし、それ以上の容量の送受信を行う場合は別の手段を検討すること
- WEBメールの利用は、会社が認め、事業部が有償で外部と契約しているクラウドサービスに限って許可する
- メールの自動転送は、原則禁止とする。但し、業務上やむを得ず、個人しか見られない環境にあるPCで使用する場合に限り、常駐先の了解、および情報システム管理者の承認を得ること
- メール送受信先のアドレスに注意すること。送信前にもう一度宛先をチェックするなど、アドレス間違いによる誤送信の防止に努めること。
  ※ 第三者確認やチェックリストの運用、Outlook誤送信防止アドイン(※紹介記事) など、再度確認を徹底すること。

メールの添付ファイルの取り扱いの注意点

- 見知らぬ相手から届いた添付ファイル付きのメールは原則無条件に削除すること(フィッシング詐欺・ウィルス感染防止)
- メーラー特有の添付ファイルの取り扱いに注意する
  → 自動的に保存されたファイルの削除忘れに注意すること(情報漏洩防止)
- デフォルト値の設定変更をする
  → HTMLメールを自動表示しない、プレビューを表示しない(ウィルス感染防止)
- パスワード付き圧縮ファイルは、内容ファイル展開後にウィルススキャンなどのチェックを行うこと

重要情報のメール送信の禁止

電子メールにおいて**個人情報や企業の機密を含む情報は送信しない**こと

添付ファイルの暗号化

- 電子メールにファイルを添付する場合は、ファイルの展開にパスワードを求める暗号化設定を行うこと
- 展開用パスワードは、電子メール以外の方法で通知することが望ましい

１２．インターネットの利用

業務に関係のない目的で利用することは禁止する。
◆以下の疑いがあるウェブサイトへのアクセスは禁止とする。

- 悪意のあるウェブサイト
- 違法コンテンツを供給するウェブサイト

◆SNSサービスその他、私的なクラウドサービスのアカウントの利用、また業務への利用は禁止とする。
業務に利用する必要がある場合は、ISMS部門責任者を通じて情報システム管理者に判断を仰ぐこと

１３．ソフトウェアの管理

【ソフトウェア及びライセンス管理方法】

ソフトウェアは、購入した部門がライセンス及び貸与の管理を行うこと。なお、全社で保有するソフトウェアは情報システム部門が管理する。

貸与を受けたソフトウェアは貸し出しの期間内で利用を終了し、アンインストール対応を行う。
もし期限を超えて利用を継続したい場合は、その旨を期限内に情報システム部門に申請を行うこととする。

【インターネット上のソフトウェア利用】

◆P2Pファイル交換ソフト(bittorrent等)の利用は禁止する。

- フリーウェアの利用は個人判断でなく、組織内で利用のリスク、ライセンスの適正利用について相談したうえで利用する。判断がつかない場合は情報システム管理者またはISMS事務局に相談すること
- シェアウェア等の有償ソフトウェアについては有効な正規ライセンスを保有していることを確認すること。
不正に入手したシリアルキー等については一切利用禁止とする。

１４．PC等の情報資産の持出・持込

AISEL
顧客満足の一歩先へ

【PC等の情報資産の持出・持込】

PC等の**情報資産の持出及び持込は禁止**とする。
但し、業務上やむを得ないと認められた場合のみ、ISMS部門責任者の承認を得て許可する。
PC等の持出・持込期間は最長１年とする。
１年を超えた場合は、再度、持出・持込申請書を提出して、ISMS部門責任者の承認を得て許可する。

＊PC等とは・・・PC、サーバ、プリンター、ネットワーク機器、外部記憶装置

（持出時の注意点）
- ノートPCには指定のHDD暗号化をかけて情報を保護すること
- 紛失・盗難に注意すること。万が一盗難・紛失した場合は、早急にISMS部門責任者に報告すること

（持込時の注意点）
- 持出・持込申請は社内ネットワークに接続するかどうかにかかわらず、借り受けた機器等を執務エリアに持ち込む場合に必要となる

１５．モバイル機器の管理と社外からの接続

AISEL
顧客満足の一歩先へ

モバイルとは・・・ 携帯して使用可能な情報機器を指す
ノートPC、スマートフォン、タブレット、携帯電話(ガラホ)、モバイルルータなど

【モバイル機器の管理】

- ノートPCは、BIOS・HDDのパスワードをかけ、鍵付きキャビネット等に保管すること。
- 持ち出す可能性のあるノートPCは情報システム部門に依頼してHDD暗号化をかけ、鍵付きキャビネットに保管すること。
- スマートフォン,タブレット,携帯電話(ガラホ)は、第三者が利用できないよう確実にパスワード付きロックをかけること。
- 盗難・紛失に注意すること。万が一盗難・紛失した場合は、早急にISMS部門管理者に連絡し指示を仰ぐこと。
- iOS,Androidのストアアカウントに関しては勝手に端末の設定を変更せず、貸与時に設定されたものを使用すること。
  開発用のアカウントがあるなど、何らかの事情があってそれ以外のアカウントを使用する必要がある場合は
  情報システム部門に相談すること。

【私物のモバイル機器の管理について】

- 個人使用の私物のモバイル機器については充電を目的とする場合を含め、会社貸与のPCに接続することを禁止する。

【社外からの接続(モバイルVPN接続)】

- 社内の情報共有はMicrosoft Teamsを用いて行う。
- 社外からのVDIによる業務実施や、社内業務システムを必要するなど、業務上やむを得ない事情がある場合に限り、
  専用ソフトによるモバイルVPN接続を認める。
- モバイルVPN接続情報の共有は禁止とし、接続も最小限にとどめること。接続元PCのローカルに残留する情報も
  利用が終了次第適時削除を行い、情報漏洩のリスクを低減すること。
- VPNアカウントが業務上不必要になった場合は直ちに情報システム部門に報告し、VPNソフトを削除し、
  アカウントを返却すること。

※テレワーク（リモート勤務）における安全管理措置については、別途定める「セキュリティガイドライン
（テレワーク版）」に基づき管理されることとなります。

１６．媒体の処分

AISEL
顧客満足の一歩先へ

【媒体の処分】

1. 紙媒体
   個人情報および機密情報が印刷された紙媒体は、シュレッダーにかけて処分するものとする。
2. USBメモリ、SD等メモリカード、CD／DVD、磁気フィルム／テープ、光磁気ディスクなど
   データを復元できない形で完全消去を行うか、破壊して廃棄する。
3. その他
   完全な廃棄方法が確保できない媒体については、指定業者を利用して廃棄処分するものとする。

【処分のタイミング】

媒体を含む情報資産を処分するタイミングは、不要になった場合に即時おこなうこと。
また、定期的に実施される情報資産一覧の更新タイミングで再度確認すること。

【廃棄の記録、廃棄証明の取得】

媒体を含む情報資産の処分については可能な限り破壊処理時の写真などの映像記録を取得すること。
また、預かり資産やリース資産の廃棄等で廃棄証明が必要な場合は確実に廃棄証明を取得し、
控えをISMS事務局に報告すること。

１７．協力会社SEの管理

- 当社に常駐してプロジェクト業務を遂行する、就業規則の効力が及ばない外部利用者については、機密保持契約書等に定める、または関連法規に従い罰則及び損害賠償の義務を負うものとする。
- ISMS部門責任者は、情報セキュリティに関連するガイドライン等の教育を実施し、指導と管理をすること。
- ISMS部門責任者は「常駐証発行申請書」を作成し、情報システム管理者に提出し、常駐証、セキュリティカード等の発行を行うものとする。
- 業務が終了した場合は、速やかに情報システム管理者および利用しているサーバ管理者に連絡し、付与したアクセス権等の停止を申し出ること。

１８．常駐先でのセキュリティ

（顧客先等に常駐する社員が遵守すべきセキュリティ規則について）

- 顧客、契約先の情報セキュリティにかかわる規則を優先して遵守する。
- 顧客、契約先の管理施設以外の場所においては、特に指定がない場合は当社の規程に従うものとする。

（顧客先等に常駐する場合のセキュリティ管理手順）

- ISMS部門責任者は、顧客、契約先の情報セキュリティに関連するガイドライン等の教育を実施し、定期的に指導と管理をしなければならない。
- 顧客、契約先より貸与される情報資産類がある場合は、顧客、契約先の手順に従い申請手続きを行い、ISMS部門責任者はそれらの資産類を管理する一覧表を作成し、貸与、返却などを管理しなければならない。
  （例：ユーザID登録、入管証、機器、仕様書、テストデータ等）

１９．セキュリティ事故の対応

AISEL
顧客満足の一歩先へ

情報セキュリティに関する事件や事象とは

コンピュータセキュリティに関係する人為的事象で、意図的および偶発的なもの（その疑いがある場合）を含む。
例えば、データの破壊、サービス妨害行為、意図しない情報の開示や、さらにそれらに至るための行為（事象）などがある。
（JPCERT/CCより）

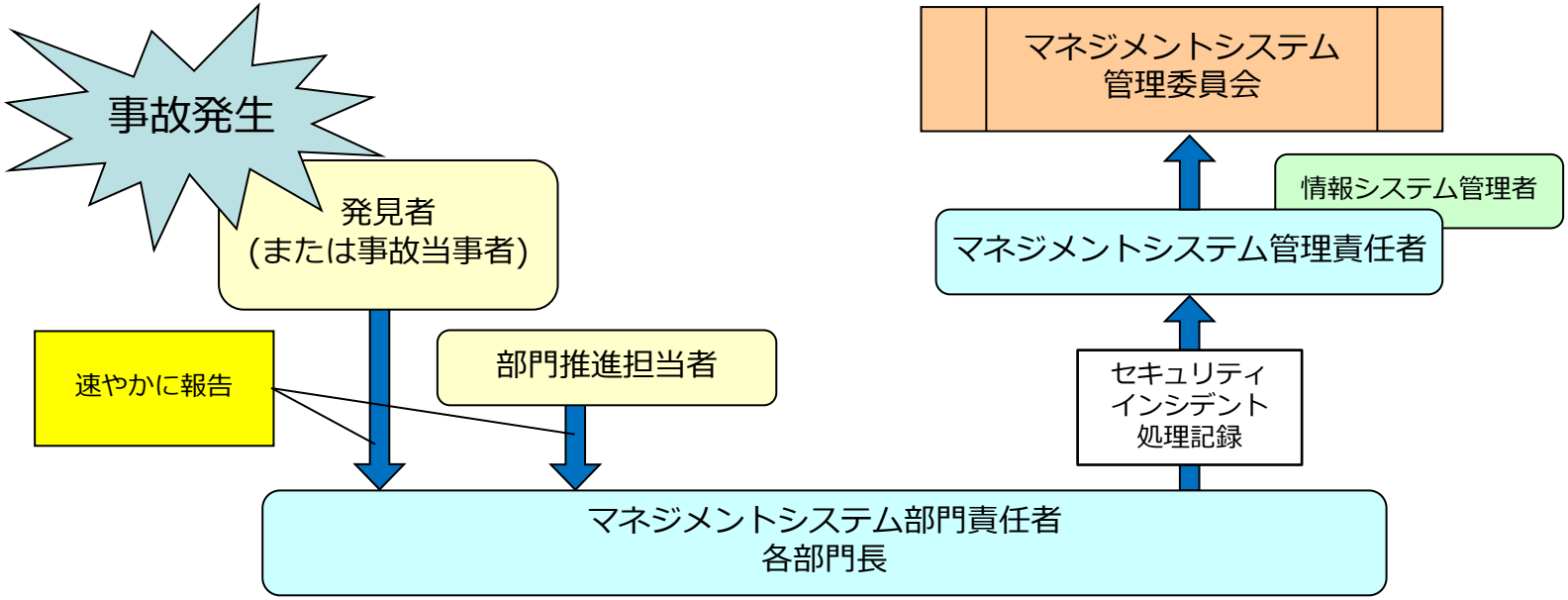
【セキュリティ事故の対応手順】

セキュリティ事故を認識した場合は以下のフローで速やかに報告を行ってください。

社員はマネジメントシステム**部門責任者に報告**、マネジメントシステム部門責任者からマネジメントシステム管理責任者及び、情報システム管理者に報告を行います。マネジメントシステム部門責任者と連絡がつかない場合は発見者が直接マネジメントシステム管理責任者及び、情報システム責任者に報告を行うこととなります。

対応者はマネジメントシステム部門責任者及び情報システム管理者の指示に従って対応を行うものとし、指示のない対応は行ってはいけません。

詳細は、緊急事態対応計画の「セキュリティ事象・事故対応計画」を参照してください。



２０．教育・訓練

ISMS教育責任者は以下により、従業者のセキュリティ教育を実施する。また、ISMS教育責任者は、必要に応じ適用範囲組織以外の従業者、委託先社員等に対しても教育を実施する。

区分	実施時期	対象者	教育内容
自覚教育	適時 (毎年1回以上)	適用範囲従業者全員	1. 情報セキュリティ活動の意味と、目標達成には社員全員のセキュリティに対する役割と責任に対する自覚が最も重要であることの周知。 2. セキュリティインシデントが組織に重大な影響を及ぼすことを周知。 3. 情報セキュリティ基本方針の周知・徹底。
	新入社員配属時	新入社員	
手順教育	ISMS構築時	適用範囲従業者全員	1. ISMSマニュアル、手順書類の内容を周知する。 2. 事業継続計画の教育・訓練。
	新入社員配属時	新入社員	
	手順の大幅な変更時	手順にかかわる従業者全員	1. 変更のあった手順の周知。
	適時	適用範囲従業者全員	1. 再教育の必要性が判断されたとき、再度規定・手順の徹底を図る。 2. 事業継続計画の教育・訓練。
専門教育	適時	専門の力量を必要とする社員	1. 社員にセキュリティの維持、改善に必要な力量を習得させる。 （例）内部監査員教育、情報システム管理者教育

※ 上記とは別に、3月、6月、9月、12月に部門におけるセキュリティセルフチェックを定例化しています。

※ 協力会社社員については、契約開始時、並びに、上記同等のタイミングで、最低1年に1回のアイセル社員同等の教育、理解度テストを実施するものとします。

２１．入退職時の手続きと懲罰

AISEL
顧客満足の一歩先へ

アイセル社員について

【入社時】

社員は、機密保持契約について就業規則の定める規則に従い、雇用条件の一部としてこのような契約書に署名しなければならない。

【退職時等アクセス権の削除及び変更】

すべての社員等の情報及び情報処理施設に対するアクセス権は、終了時には削除し、また、変更に合わせて修正しなければならない。

マネジメントシステム管理責任者は、人事部門および情報システム管理者と連携をとり、システムにかかわる個人のアクセス権を見直し、適切に削除または変更を行う。

【懲罰】

社員は、入社時に提出した誓約書に基づき、情報セキュリティ違反を犯した場合には、就業規則の「懲戒」に定める手順に従い、これらの規則に定める懲戒および損害賠償の義務を負うものとする。

協力会社社員について

【契約時】

委託、協力会社社員は、定められた契約条件に基づき、セキュリティ・個人情報保護の遵守に関して、誓約書を提出しなければならない。

【契約終了時等アクセス権の削除及び変更】

すべての協力会社社員の情報及び情報処理施設に対するアクセス権は、終了時には削除し、また、変更に合わせて修正しなければならない。

マネジメントシステム管理責任者は、人事部門および情報システム管理者と連携をとり、システムにかかわる個人のアクセス権を見直し、適切に削除または変更を行う。

【懲罰等】

協力会社メンバーは、契約時に提出した誓約書及び所属会社との契約に基づき、情報セキュリティに関する順守義務を負うものとする。

当該義務に違反した場合は、所属会社との契約、または関連法規に従い、所属会社において罰則並びに、損害賠償等の責任が生ずる場合がある。

２２．預かり資産の確認と管理

請負開発、客先常駐共に取引先から物品又はサービスアカウントの貸与を受ける場合は、**貸与を受けた部門で預かった資産についての台帳を作成**し、適切な管理及び外部からの管理状況の照会に応じることができるように備えること。

- 物品の例
  入館証、ノートPC、スマートフォン、タブレット、USBメモリ等の媒体類
- アカウントの例
  勤怠入力システム、クラウドストレージ、請求・支払システム、ファイルサーバアカウント、VPNアカウント等
- その他の情報資産
  プログラムソースやテストデータなどの電子ファイル

借り受けた資産を適切に管理し、紛失等に十分注意する。また利用期限を明記し、台帳の管理者は部内の社員が放置していないか監督すること。

２３．外部(クラウド)サービスの利用

外部(クラウド)サービスについては、有償無償を問わず、個人アカウントの利用は禁止とする。

組織で利用する場合は、開発に必要なサービスの利用として組織内で検討の上、マネジメントシステム管理責任者及び情報システム管理者にサービスの利用を申請し、許諾を受けること。
また、情報資産一覧上に列挙し、どのような情報を当該サービスに預託するか、ないしは蓄積するかを明確化し、発生するリスクとリスク対策を検討すること。

原則としてデータの改ざん、消失等に対する一定の保障を契約書又は約款などで明確化し、アイセルが会社として当該サービス上に蓄積されたデータ及びアクセス・操作ログ等に対する監査を実施可能な状態にあるものについてその利用を許諾する。

- 個人で判断をせず、必ず上長、情報システム管理者に相談の上で業務へ取り入れることを検討すること。

２４．資料印刷、FAXの利用

重要な印刷物については印刷を実行したまま複合機等に印刷物を放置しないこと。印刷実施時は出力完了後速やかに印刷物を持ち帰ること。

FAXについては宛先をよく確認し、間違った電話番号に送付することがないよう留意する。不慣れな場合は複数名で宛先や送付物等を確認したうえで送付すること。

２５．飲酒時の注意

顧客満足の一歩先へ

飲酒は社員同士のコミュニケーションの手段であると同時に注意力を低下させ情報の滅失・漏洩・毀損の原因となるリスクを発生させる。
被害が発生しないように普段からの注意に加えて、以下の対策を講じなければならない。

【飲酒前の対策】

・飲酒時に無くす可能性のある、機密に相当する「飲酒時の所持禁止品」をリスト化する

■お客様発行の入館証やセキュリティカード類
■お客様情報（データ・書類）
■お客様からの預かり品（電子機器、記録媒体等）
■お客様情報、機密情報などが第三者に読み取れるノートやメモ帳
■PC,USBメモリ等の電子機器又は電子媒体
■社内情報（個人情報、取引先情報、外部に非公開の会社情報）
■社内資料（提案書、見積書など）

・飲酒は計画を立てて予め「飲酒時の所持禁止品」を持たない日にする
・突発的な飲酒が起こった場合は情シスにサーバルーム保管を依頼する
・所持を避けられない以下所持品の所在と状態を飲酒前に確認する

■社員証／従業員証
■会社貸与の携帯電話（スマホ）のセキュリティロック状態
■（社員証や携帯電話の）ネックストラップの物理的状態
■会社支給の名刺
■バッグの置き場所（他人の往来する場所に置かない）

【飲酒後の対策】

- 飲酒時に同席者で酩酊者がいないか相互確認、いる場合は責任をもって送っていく
  → １人になったときに紛失・盗難の危険大
- 退店時に忘れ物がないか確認する（相互確認・幹事確認）
- 帰り道はバッグを電車の網棚等に置いたりせず、肌身離さず所持し、紛失・盗難防止に努める
- 飲酒後は特に「歩きスマホ」しないように気を付ける
  → 人や物に衝突して物を落としたり、バッグの内容物が毀損する
- 危険性大 飲酒後は特に注意力が散漫になる為、普段よりも警戒が必要

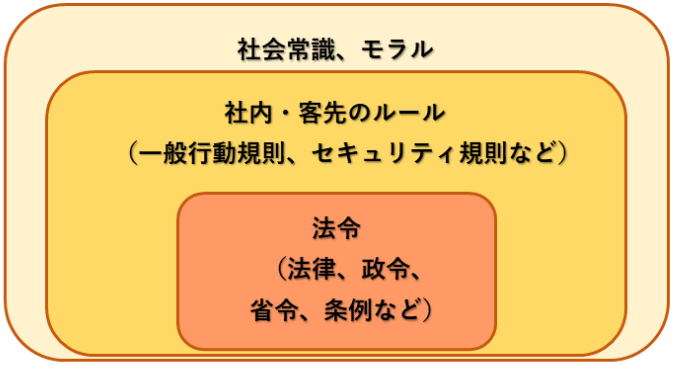
事前準備と相互確認を怠らないようにすることで
事故発生を防ぐことができる。

設定されたルールだけでなくアイセル社員として、
社会人として節度をわきまえた行動を心掛けること

２６．コンプライアンスについて

AISEL
顧客満足の一歩先へ

アイセルの業務に携わるすべての従業者は、当ガイドの遵守はもちろんですが、右記の図に示した内容を守ることが求められています。



コンプライアンスとは、一般的に法令遵守とされていますが、現在は、法令等の遵守として、社内・客先のルール順守、社会常識、モラルを守ることも含めた内容となっています。

従って、法律だけではなく、会社の各種規則や約束事を守ること、あるいは、社会におけるルール、モラルといった成文化されていない道徳観のようなものも守ることが必要です。

常に、何が正しい行いなのか、判断を求められているのです。

社会常識　：　社会を構成する上で当たり前のものとなっている、社会的な価値観

モラル　：　物事の善悪を判断する基準（倫理観、道徳観）

尚、ソフトウェア開発に携わる皆さんには、特許法，著作権法，不正競争防止法、輸出関係法令等に関する必要な知識を持って、業務を行う事が必要です。

開発したソフトウェアが、いったい誰の所有物なのかを考えて取り扱う事は、自分を守る、会社を守るという観点から、とても大切です。

なお、ソフトウェアの所有権に関しては、皆さんと会社の契約、会社同士の契約などにより、その帰属も変わってきます。つねにその事を意識して誤った行動をとらない様にしてください。

最後に自分を守れるのは、自分自身です。

上記に関連して不明なことがあれば、社内の適切な部署（法務等）に問い合わせて判断を仰いでください。

２７．権利侵害の防止について

アイセルでは、企業理念に則り、コンプライアンスに反して自社の利益を求めることはありません。
他者が権利を有する知財を無断で使用するといった権利侵害は明らかな違反行為であり、企業理念に反します。

参照 – 権利侵害とは（特許庁 ： https://www.jpo.go.jp/support/ipr/kenrishingai.html ）

外部のソフトウェアのライセンス

公開されているソフトウェアであっても、ライセンス条項を確認してから利用することとしてください。

制限なくコピーや流用可能とされているものもありますが、**ライセンスや利用規約が提示されていないソフトウェアは利用してよいものではない**ため使用を許可しません。

ネット上で見つかるサンプルコードも同様です。サイトの利用規約や条件を確認することが必要であり、また、成果物に脆弱性などを作り込むことにならないか、十分な精査や検討も必要です。

他社のロゴやサービスのシンボルマーク

無断使用は著作権違反となります。対象がどのような知的財産権で保護されているかを確認してから利用することが重要です。

ロゴやシンボルマークなどを利用する前に対象の公式サイトなどを参照して、利用規約や条件が提示されているかを確認のうえ、許可されている範囲内で利用してください。
利用規約が確認できないロゴやマークは利用しないでください。

２８．ランサムウェア対策

AISEL
顧客満足の一歩先へ

JPCERT/CC ランサムウェア対策特設サイト(https://www.jpcert.or.jp/magazine/security/nomore-ransom.html)より

特設サイトでは、以下に抜き出した記載のほか、感染した場合の対処法などが紹介されています。

対応策は、バックアップの取得やメールの開封、ソフトウェア更新、パスワードの見直しなど、すでに広く一般に知られている方法とされています。
毎日の業務で、つねに気をつけ注意を払うようにしてください。

1．ランサムウエアとは

マルウエアの一種であり、感染したデバイスをロックしたり、ファイルを暗号化したりすることによってユーザによるアクセスを制限し、「元に戻して欲しければ」とランサム（身代金）の支払いを要求します。

2．考えられる感染経路

- 攻撃者からのEメールを受信して添付ファイルを開く
- メール本文中に記載されているURLリンクをクリックする
- 改ざんされたWebサイトからドライブバイダウンロード攻撃を受ける
- 攻撃目的で細工されたサービス要求が送られる
- その他、VPNやRDPの脆弱性や設定ミスを攻撃する侵入型など

3．ランサムウェアの対策

- ファイルやシステムの定期的なバックアップを実施する
- メールの添付ファイルの開封やウェブ・ページ等のリンクをたどる際には注意する
- ファイアウォールやメールフィルタを適切に設定し、不審な通信をブロックする
- OSやアプリケーション・ソフトウエアを最新の状態にアップデートする
- セキュリティソフトを導入し、定義ファイルを常に最新の状態に保つ
- パスワードの設定を見直す

情報漏洩や滅失・既存は、バックアップや暗号化などの対策を行っても、必ずインシデントは発生します。
インシデント対応の遅れは、被害の拡大や個人の権利侵害などをもたらし、また、風評評価の中では最も批判される点です。対応事項の発生時には、速やかな対応をお願いいたします。

２９．脅威に関する情報と対策知識

AISEL
顧客満足の一歩先へ

情報セキュリティに関する事故や脆弱性情報は、日々あらたな報道や発表が行われています。
それらの情報は、公的な団体や機関によって収集し分析された結果が公開されています。
自分で実施可能な対策はなにか、何に注意をはらう必要があるかといった情報を入手して、事象発生の可能性や影響範囲を低減することを検討してください。
以下に情報公開しているサイトを示します。

IPA 情報セキュリティ10大脅威（ https://www.ipa.go.jp/security/10threats/index.html ）

- 毎年、直近に発生した社会的に影響が大きかったと考えられる事案が選出され、事例の紹介や発生した原因、考えられる対策が資料にまとめられています。
- 過去の10大脅威は発生しなくなったわけではありませんので、継続して対策が必要です。

JPCERT/CC 注意喚起（ https://www.jpcert.or.jp/ ）

- 日別に、先頭ページで情報セキュリティ上の脅威など最新の情報を注意喚起されています。
- 「Weekly Report」に、重要と判断された情報がまとめられています。

IPA 重要なセキュリティ情報（ https://www.ipa.go.jp/security/security-alert/index.html ）

- 日別に、危険性が高いと判断されたセキュリティ上の問題と対策について、新しいものから掲載されています。

JVN（"Japan Vulnerability Notes"） 新着情報（ https://jvn.jp/index.html ）

※ 上記の「JPCERT/CC 注意喚起」や「IPA」のサイトで ”脆弱性関連情報” として情報表示されています。

- 製品ベンダーから報告され公表手続きを経た脆弱性情報で、対象製品のバージョンや脆弱性の詳細情報があります。
- パッチなどの対策方法や回避策が掲載されることもあります。

３０．新しい外部サービスの利用について

AISEL
顧客満足の一歩先へ

ChatGPTのような生成AIに限らず、古くはWebメールやオンラインファイル共有、クラウドVPNといった新しい形態で提供されるサービスが発生します。
私的利用は厳禁ですが、技術検証や業務利用を行うにあたっては、サービスの内容や利用方法を情報セキュリティ要件も含めて確認のうえで利用する必要があります。

加えて、当該サービスで扱う機能や情報を必要最小限とすることが、セキュリティリスク対策となります。
＜例＞　（日本ディープラーニング協会『生成AIの利用ガイドライン』）

- 生成系AIにデータを入力する際に注意すべき事項
    1. 第三者が著作権を有しているデータ(他人が作成した文章など)
    2. 登録商標・意匠(ロゴやデザイン)
    3. 著名人の顔写真や氏名
    4. 個人情報
    5. 他社から秘密保持義務を課されて開示された秘密情報
    6. 自組織の機密情報
- 生成系AIが作成した生成物を使用するに際して注意すべき事項
    1. 生成物の内容に虚偽が含まれている可能性がある
    2. 生成物を利用する行為が誰かの既存の権利を侵害する可能性がある
    3. 生成物について著作権が発生しない可能性がある
    4. 生成物を商用利用できない可能性がある
    5. 生成AIのポリシー上の制限に注意する

上の例から、利用時には以下のリスクがないかなど常に確認をしてください。

- ✓ サービス利用のために提供する情報は、結果利益を享受するために**本当に必要なものだけ**になっていますか？
  利害関係者の個人情報や営業情報、成果物やソースコードなど、外部公開すべきでない情報の投入はNGです。
- ✓ 入力や送信した情報は、クラウド上や相手側で**学習利用や保存されないこと**になっていますか？
  制作過程のログは利用者が記録しておいてください。
- ✓ 取り扱う情報が著作権や不正競争防止などの**法令に抵触しません**か？
- ✓ 潜在バグや悪意のあるコード生成により、外部攻撃の危険や脆弱性などの**欠陥を作り込んでいません**か？
  制作結果の根拠や裏付けの確認は利用者が実施してください。

３１．災害時の緊急連絡

- 災害発生時には連絡手段の確保が難しくなることが想定されますが、公衆網によるインターネットの利用可能性が高いと考えられるので、Teamsによる連絡・報告を基本とします。
- 事業継続計画（2022/4/1版）に記載がありますが、災害等の緊急時には、個人所有のPCや携帯端末からのTeamsアプリによるアクセスは許可されます。

aipo ＞ ファイル管理 ＞ ISMS･Pマーク関連文書 ＞ ③三次階層
＞ 6.その他 ＞ 1.その他【共通】＞ 事業継続計画　－　「災害時緊急連絡網」

1．緊急連絡・安否確認等の連絡網発動時は、社員それぞれがTeamsの緊急時登録先に、安否、連絡等の必要情報を登録する。
災害発生時に於いては連絡手段の確保が難しくなる事を想定し、利用可能性が高いと考えられるインターネットを通しての連絡を想定し、スマホ等携帯端末からの**Teams**への登録を考えておくものとする。
2．社員からの登録状況については、対策本部メンバーにより確認されるものとし、個別の連絡が必要な場合は、人事保有の社員連絡先一覧(*)により各個に対しアクセスする。
(*)社員連絡先一覧は人事管理とし、常時準備しアクセス権は対策本部メンバー（対策委員一次、二次とも）に付与される
3．Teams上での緊急連絡登録先の運用については下記の通りとする。
① Teamsへのアクセスは個人所有PC、個人所有携帯からのアクセスを許可する。（事前にTeamsアプリ登録が必要）
② 運用方法の詳細（方法・ルール）については、別途社員全員に通知する。
③ 下記連絡方法にて支障の生じる場合は、TEL、メール、SMS、SNS等、可能な手段で会社に連絡する。

変更履歴

改編日時	改編項	改編内容
2012年1月5日（第5.00版）	１．体制	ISMS委員会所属社員変更
2015年1月22日（第5.01版）	１．体制	ISMS委員会所属社員役職変更
2016年5月2日（第5.02版）	１．体制	ISMS委員会所属社員役職変更
2017年4月18日（第5.12版）	１．体制 ２．文書体系 ７．アカウント管理 １２．ソフトウェアの管理	ISMS委員会所属社員役職変更 掲載場所をアイセルポータルに変更 給与会計をPCAに、グループウェアをアイセルポータルに変更 ソフトウェアダウンロード先をアイセルポータルに変更 委任管理者を情報システム部に変更
2018年3月28日（第5.121版）	１．体制	ISMS部門責任者を「各部長」から「各部門長」に変更 内部監査責任者、SMS委員会所属社員変更
2019年5月1日（第5.122版）	１．体制	内部監査責任者を変更
2019年7月17日（第6版）	１～24.全項目	・以下項目を新設 １.ISMSの目的　22.預かり資産の確認と管理 23.外部(クラウド)サービスの利用　24.資料印刷、FAXの利用 25.飲酒時の注意 ・組織変更　2. ・全ページフォーマット統一、誤字修正 ・説明追加、変更　3. 4. 5. 6. 8. 9. 11. 12. 13. 14. 15. 16. 19. ・図表再作成　2. 19. ・図表削除　6. 7. 8. 13. 14. 17.
2020年11月1日（第7版）	全体的に内容の見直し	ISMS規程類改定及び理解度テスト内容に照らして修正
2021年4月1日（第8版）	３．文書体系	第7版の改定規程に関する追加修正
2021年7月7日（第9版）	３．文書体系 １１．メール利用 ２０．教育・訓練	ユーザー遵守事項規程を追加 重要情報、添付ファイルの取り扱い修正 セキュリティセルフチェックの扱い追記
2021年8月23日（第10版）	3.　ISMSの文書体系 20.　教育・訓練 21.1　入退職時の手続きと懲罰 21.2　契約開始・終了時の手続き 26.　コンプライアンスについて	文言訂正 協力会社社員に関する記載を追記 当項目を社員対象に変更 協力会社社員対象の項目定義追記 コンプライアンスに対する考え方追記

変更履歴

改編日時	改編項	改編内容
2022年2月版	3.ISMSの文書体系 4.情報資産の管理 8.アカウント管理 19.緊急事態の対応 23.外部サービスの利用 27.ランサムウェア対策	セキュリティガイドライン（テレワーク版）を追記 ページタイトルを変更 Microsoft 365を追記、終了した業務システムを削除 ページタイトルを変更、緊急事態対応計画を参照する旨を追記 許諾者をマネジメントシステム管理責任者に変更 ページを追加
2023年2月版	目次 1.2.3.10.16.24. 8.アクセス方針とアカウント申請 9.パスワード管理、スクリーンロック 11.メールの利用 19.セキュリティ事故の対応 21.入退職時の手続き 27.権利侵害の防止について 28.ランサムウェア対策 29.災害時の緊急連絡	ページリンクを作成 文体の整形、図表のレイアウト調整 ページタイトルを変更 ページタイトルを変更 誤送信防止確認を記載。パスワード通知は異なる手段を記載 ページタイトルを変更 アクセス権等管理者をマネジメントシステム管理責任者に変更 ページを追加 項番を変更 ページを追加
2023年10月版	9.パスワード管理、スクリーンロック 29.脅威に関する情報と対策知識 30.災害時の緊急連絡先	パスワード構成文字列の要件を変更 スクリーンショットや写真撮影の注意喚起を追記 ページを追加 項番を変更
2024年2月版	30.新しい外部サービスの利用について 31.災害時の緊急連絡先	ページを追加 項番を変更