AISEL

個人情報マネジメントシステム

（JIS Q 15001：2023）

ＰＭＳユーザーズガイド

2024年4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～

AISEL
顧客満足の一歩先へ

1．個人情報保護法について

AISEL
顧客満足の一歩先へ

【個人情報保護法制定の目的】

個人情報を活用することで、様々な分野での業務の効率化やサービス向上を図ることができますが、個人情報は、個人のプライバシーにもかかわる大切な情報です。

そのため、個人情報の保護と、適切な活用を図る事を目的として制定されたのが「個人情報の保護に関する法律」（通称：「個人情報保護法」）です。

【個人情報保護法制定の沿革】

「個人情報保護法」は平成15年（2003年）5月に成立、平成17年（2005年）4月に全面施行されました。

当初は、大規模な個人情報を保有する事業者を対象に適用されていましたが、その後の社会環境の変化等を踏まえて改正され、最新のものは令和6年4月に施行されています。

現在では「個人情報取扱事業者」とは、個人情報の数にかかわらず「個人情報をデータベース化して事業に利用している事業者」すべてが法律の適用対象とされています。

従って、アイセルもこの法律が適用される対象です。

2．プライバシーマークとは

AISEL
顧客満足の一歩先へ

【法律ではない情報セキュリティの規格】

2005年の個人情報保護法以前、1999年に財団法人日本規格協会により個人情報保護に関する産業規格JIS Q 15001:1999が定められました。

この規格は、海外の個人情報の活用に対する個人情報保護の取り組みを先例として、企業の自主的な取り組みの基準として活用するための、体系的で全経営活動に統合されたマネジメントシステムの最低限の要求事項が規定されています。

同規格は個人情報保護法とは異なる観点から個人情報を保護する取り組みの規格であり、個人情報保護法とは領域において相互に補完しあうものであると同時に、全般的に個人情報保護法よりも高い水準の個人情報保護のスキームを提示するものとなっています。

【規格の改定】

JIS Q 15001:1999 → JIS Q 15001:2006 → JIS Q 15001:2017 → JIS Q 15001:2023

規格は改定が行われており、現JIS Q 15001:2023は改正個人情報保護法に対応したバージョンであり、より強固な個人情報保護マネジメントシステム構築の指針となっています。

【プライバシーマークとは】

プライバシーマーク、略してＰマークとも言われているこのマークは、国内規格JIS Q 15001に従った組織ルールを定め、規格の要求に適合した個人情報保護ルールの運用を行っていることを第三者機関から認定を受けることで利用を許可されるマークです。

◀ 名刺やアイセルホームページに掲載されているプライバシーマーク。
自主的に適切な個人情報運用を推進する組織であることを消費者、取引先企業、また採用応募検討者等にアピールできる。

アイセルではPMS(※)を定め、 2007年から一般財団法人日本情報経済社会推進協会（JIPDEC)の審査を受けてプライバシーマーク認定の継続的更新を続けています。

アイセルはプライバシーマークの認定を維持することで、全事業者の責務である個人情報保護法の遵守のみならず、企業の自主的な取り組みとしてより高いレベルでの個人情報保護を目指しています。

※ JIS Q 15001の規格に準拠した個人情報保護の社内ルールを
PMS(Personal Information Protection Management Systems)と呼びます。

3．個人情報保護方針(プライバシーポリシー)とは

AISEL
顧客満足の一歩先へ

個人情報保護方針はアイセルの個人情報保護に対する基本理念にあたり、個人情報の取り扱いの考え方を社内外に宣言するものです。

同宣言はJIS Q 15001の要求事項としてマネジメントシステムに盛り込み実施しなければならないものです。

【宣言内容】

- 代表者の氏名
- アイセルが個人情報の取り扱いを重大な責務と捉え、個人情報を保護する体制をととのえている事
- 個人情報の取得・利用・提供を利用目的開示して、同意を得て利用する事
- 取得する個人情報の種類と目的
- JISQ15001規格、法令・規範を遵守する事
- 安全対策実施の宣言
- 個人情報保護マネジメントシステムの継続的改善を行っていく事
- 個人情報に関する苦情及び相談(開示・削除請求等)の連絡先
- 個人情報の開示手続きの方法

アイセルでは、これらを明らかにして個人情報に取り組むことを**アイセルホームページ及び社内に掲示**しています。

次ページにアイセルの個人情報保護方針を掲載しています。

４．アイセルの個人情報保護方針 本文

顧客満足の一歩先へ

株式会社アイセル（以下、当社）は、システム開発事業及び関連する社内業務を行っていく上で、「個人情報」の保護はお客様にとっても、取り扱う当社にとっても重要な情報資産であり、確実に保護することは重要な責務であります。

そのために、以下の方針に基づく取り組みとして、個人情報保護マネジメントシステムを構築し、従業員への教育・実践を徹底するとともに、個人情報保護マネジメントシステムの継続的改善を行っていきます。

１．個人情報の取得・利用・提供について

当社は、適正かつ公正な手段によって個人情報を取得いたします。取得にあたっては、利用目的を特定し、その利用目的の達成に必要な範囲内で個人情報を利用いたします。

また、特定された利用目的の達成に必要な範囲を超えた個人情報の取り扱いを行わないための適切な措置を講じ、利用目的を超えて利用する場合には、ご本人に新たな利用目的を通知し、同意を得ます。

当社は、以下のいずれかに該当する場合を除き、あらかじめご本人の同意を得ることなく、個人情報の目的外利用はいたしません。

(1) 本人の事前の同意、承認を得ている場合
(2) 法令に基づく場合

２．法令・規範の遵守について

当社は、確実な個人情報保護の実現のため、JISQ15001に準拠した個人情報保護マネジメントシステム、個人情報に関連する法令、国が定める指針及びその他の規範を遵守します。

３．安全対策の実施について

当社は、取扱う個人情報（当社が取得し、又は取得しようとしている個人情報を含む）の漏えい、滅失または毀損の防止及び是正のための規程と体制の整備を行い、十分なセキュリティ対策を講じるとともに、利用目的の達成に必要な正確性、最新性を確保するための適切な措置を講じます。

４．個人情報保護マネジメントシステムの継続的改善について

当社は、内部監査や代表者による個人情報保護マネジメントシステムの見直しの機会を通じて個人情報保護マネジメントシステムを継続的に改善し、常に最良の状態を維持します。

５．苦情及び相談について

当社の個人情報の取扱いに関する苦情及び相談等があった場合は、迅速かつ誠実に、適切な対応を致します。

株式会社アイセル
代表取締役社長 草川 麗子

平成17年11月 1日制定
令和 6年 4月19日改訂

＜ アイセルホームページ(https://www.aisel.ne.jp/privacy/)より引用 ＞
ホームページでは上記のほか、利用目的や手続き方法、連絡先情報などを掲示しています。

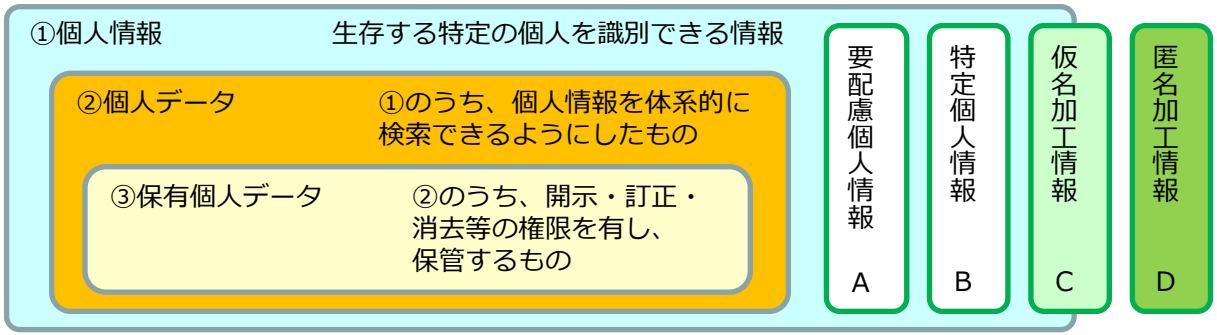
5．個人情報について

AISEL
顧客満足の一歩先へ

1．個人情報の定義

生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。

個人情報の保護に関する法律　第二条 より引用



A：本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報

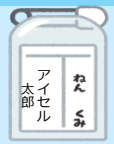
B：個人番号（マイナンバー）を含んだ個人情報
（マイナンバー法に定められた個人番号を含む個人情報で、取り扱いが限定される）

C：他の情報と照合しない限り特定の個人を識別できないように個人情報を加工して得られる個人に関する情報

D：特定の個人を識別できないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元できないようにしたもの

個人情報の例

氏名(フルネーム)　本人と特定できる写真　本人と特定できる音声

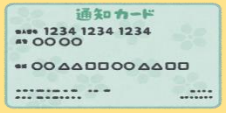


本人と特定できる動画

名刺

運転免許証

《マイナンバー》



取扱注意！

マイナンバーは特に重要な情報として「特定個人情報」に該当し慎重な運用が義務付けられています。

特定個人情報の保護管理については、「個人情報保護法」に加えて「行政手続における特定の個人を識別するための番号の利用等に関する法律」（通称「マイナンバー法」）に定められています

5．個人情報について

2．要配慮個人情報

個人情報の中でもその情報が流通することで本人に精神的、社会的不利益・差別を及ぼす恐れのある情報を特に要配慮個人情報としています。

【要配慮個人情報の例】

- 人種
- 信条
- 社会的身分
- 病歴
- 犯罪の経歴
- 犯罪により害を被った事実
- 身体障害、知的障害、精神障害等の障害があること
- 健康診断等の結果
- 保険指導又は診療若しくは調剤が行われたこと
- 逮捕、差押え、勾留、その他の刑事事件に関する手続が行われたこと
- 少年の保護事件に関する手続が行われたこと

※ 個人情報の保護に関する法律についてのガイドライン（通則編）（令和4年9月一部改正）から抜粋

また、改正個人情報保護法において要配慮個人情報は、
「本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報」
と明確に定義づけられ、慎重な取り扱いをするよう定められています。
（個人情報保護法第二条2項）

要配慮個人情報は、情報の取得や提供など取り扱いに制限があり、また個人情報保護委員会が報告要求や立入検査の権限を持ち行政指導が可能であるなど、厳密な取り扱いが求められます。

労働安全衛生法に基づく、ストレスチェックの検査結果データや産業医の面接指導結果も要配慮個人情報にあたります。慎重な取り扱いが必要です。

5．個人情報について

3．個人情報一覧

アイセルが取り扱う個人情報の詳細情報が記載された一覧であり、これらは個人情報保護の出発点にあたる。
（「取り扱う個人情報」はアイセルが取得した、または取得しようとしている個人情報を含みます。）
個人情報一覧には以下のことが示されている。

◇個人情報の種類
◇個人情報の利用目的
◇個人情報の内容(氏名、住所等具体的情報)
◇個人情報の保有件数(累積及び都度の入手件数)
◇個人情報の入手方法
◇個人情報の媒体（紙、電子データ）
◇個人情報の作成者
◇個人情報の管理責任者
◇個人情報のアクセス権限範囲
◇個人情報の委託、提供の有無
◇個人情報の保管場所
◇個人情報の保管期間
◇個人情報の廃棄方法
◇開示対象に該当するか否かの判断

これらはアイセルが守るべき個人情報の「対象」であり、各項目のリスク分析、運用マニュアルを作成するための判断材料となっています。
そのため、管理責任者、業務責任者はこの一覧を把握し、日々の現場業務における個人情報の取扱いを管理しなければなりません。また、一覧記載の各種取引先に対する監督管理も実施しなければなりません。

この個人情報一覧は**常に最新である必要がある**ため、管理する個人情報の件数の顕著な増減や業務(事業)内容の変更、当該情報を管理する外部機関との契約が変更になる等の場合には随時更新することを求められます。

アイセルでは、**一覧をアイセルポータル(aipo)上で公開**しています。　→「情報資産一覧（個人情報）」

5．個人情報について

AISEL
顧客満足の一歩先へ

4．アイセルで取り扱っている主な個人情報

1. 従業員情報（**あなた自身の情報も該当します**）

社員名簿、緊急連絡先、身元保証情報、人事情報、給与データ、顔写真、社員の(自分の)名刺等、（マイナンバー）

2. 採用情報

履歴書、職務経歴書、顔写真等

3. 株主情報

株主名簿等

4. お客様情報

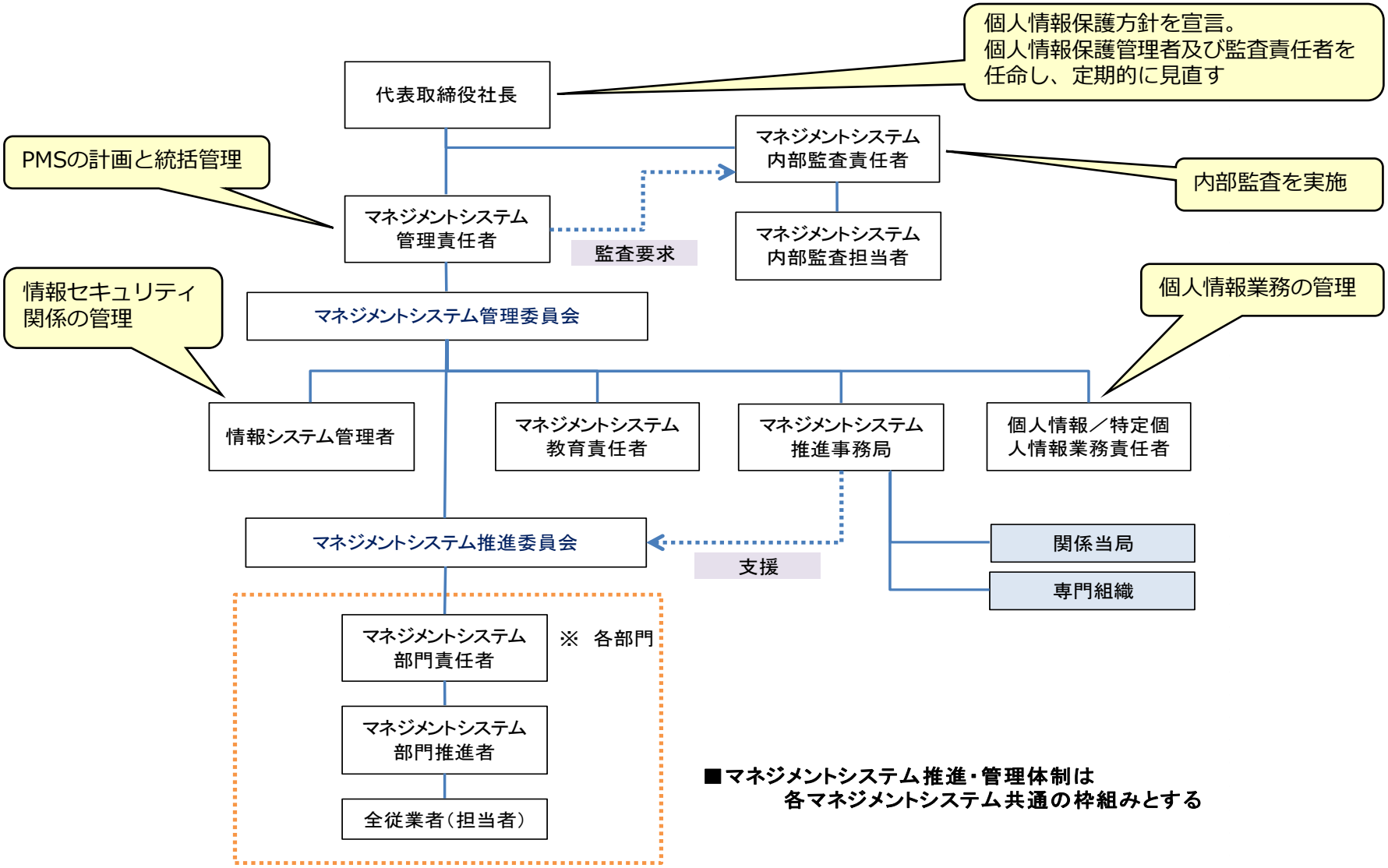
取引先企業の担当者情報、名刺等（他、委託業務で個人情報の委託/預託を受けた場合はその内容が該当）
受託した業務で取り扱うエンドユーザからの申し込み情報等

5. パートナー情報

職務経歴書、顔写真等

このようにアイセルでは多岐に及ぶ個人情報を取り扱っており、自分自身の情報も個人情報に該当することから、
個人情報を持たない部署は存在しないことに注意しなければなりません。

6．PMS推進体制



この体制は、情報セキュリティマネジメントシステム（ISMS）と共通の体制となっています。

7．個人情報関連規程

以下の文書はアイセルのPMSを形作る主な文書であり、これらは全てポータル(aipo)に掲載されています。

文書名称	概　　要
マネジメントシステム統合規程	ＰＭＳマニュアルの上位規程となる、マネジメントシステムの共通規程
個人情報保護方針	アイセル社としての個人情報保護の考え方を社内外に示す文書
ＰＭＳマニュアル	個人情報保護法およびJIS Q 15001に準拠した個人情報の保護に関するマニュアル
施設入退管理規則	事業所として使用する施設の入退室管理を定めた規則　<ISMSと共有>
情報セキュリティ対策規則 情報システム管理規則	情報セキュリティに関する安全措置を定めた規則　<ISMSと共有>
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まとめ定めた規則　<ISMSと共有>
情報資産管理規則	情報資産（ソフト、ハードウェア、媒体）に関する取扱いを定めた規則　<ISMSと共有>
個人情報マネジメントシステム （PMS）ユーザーズガイド	PMSに関する規則をユーザー向けに整理したガイド（本書）

注）これらの各種文書については、JIS Q 15001や個人情報保護法の改正に倣って改定を行っております。
各文書について不明な点は、マネジメントシステム推進事務局にお問い合わせください。

8．個人情報取扱に関する手続き

8-1．申請書の一覧

以下の文書は個人情報取扱において各種手続きを行う場合に必要になる申請書となっており、
次ページ以降に必要になる場合を個別に記載しています。

個人情報取扱申請書	新規で個人情報を取り扱う際の手続き 個人情報を取り扱う際、ただし書き適用する場合の手続き 個人情報を目的外に利用する際の手続き 個人情報を外部へ委託する際の手続き
個人情報授受の記録の作成	個人情報を委託先と授受する際の手続き
個人情報開示等依頼書	保有個人データまたは第三者提供記録の開示、内容の訂正、追加または削除、利用の停止、消去及び第三者への提供の停止の問合せ対応の際の手続き
個人データの第三者提供及び受領に係わる記録	個人データを第三者に提供する、または第三者から受領する際の手続き

注）先に記載の通り、規程類の改定に伴って申請書等のフォームが変更されている場合があります。
申請の際にはaipoに掲載されているフォームをご利用ください。
不明な点は、マネジメントシステム推進事務局にお問い合わせください。

8．個人情報取扱に関する手続き

AISEL
顧客満足の一歩先へ

8-2．個人情報一覧の項目の新規追加

個人情報一覧に登録済の内容の他に、新たに個人情報を取り扱う場合は「個人情報取扱申請書」が必要になります。
併せて対象個人情報を「情報資産一覧（個人情報）」に追加のうえ「個人情報プロセス調査表」「個人情報リスク対策一覧表」の作成が必要になります。

8-3．個人情報授受の記録の作成

取引先・委託先と**個人情報を受け渡しする場合は、授受の記録が必要**になります。
※フォーマット「個人情報授受記録」
預託の場合は渡す時だけでなく、返還あるいは廃棄したかについても確認が必要になります。
受け渡しにおいては、相手先の確認方法、安全な受け渡し方法について留意が必要です。

8-4．問合せ・開示・訂正・削除・利用停止の受付

当社は保有個人データや第三者提供記録に関して「本人から開示等の請求等を受け付けた場合、規定に従い遅滞なく応じる」としています。受付窓口は個人情報保護事務局、対応実施は個人情報業務責任者・個人情報業務担当者です。

[本人確認の方法]
1）社員（退職者含む）からの問合せの場合･･･社員番号/登録先住所
2）株主からの問合せの場合･･･株主番号/登録先住所
3）応募者からの問合せの場合･･･学校名・各部名/氏名/受験場所/受験日
4）顧客・外注からの問合せの場合･･･登録先住所

本人より開示等の申し出があった場合は、本人確認を確実に行うため、「個人情報開示等依頼書」を提出してもらい、郵送にて対応を行う事としてください。（口頭での対応は禁止）
代理人の場合は本人の委任状及び代理人の身分証明書が必要になります。

※本人確認や問合せ対応管理のために、特定個人情報（マイナンバー）を記録することは禁止されています。

８．個人情報取扱に関する手続き

AISEL
顧客満足の一歩先へ

８-５．ただし書き適用する場合

個人情報運用においては、本来的に個人情報を預かる本人の同意を基に取得、利用、開示等を行うのが原則ですが、例えば**緊急性の伴う場合(人命にかかわる場合)や法律など拘束力を伴う場合(行政機関の要請や警察の捜査に協力するなど)** は「ただし書き適用」というルールを利用する事で、本人の同意なく個人情報を運用することが認められています。ただし書き適用の対象となるのは以下の表に示された内容です。

ただし書きに関する詳細内容は、「ＰＭＳマニュアル」を参照してください。

①要配慮個人情報の取得、利用及び提供の制限
②個人情報を取得した場合の措置
③本人から直接書面によって取得する場合の措置
④利用に関する措置
⑤本人に連絡又は接触する場合の措置
⑥個人データの提供に関する措置

※ただし書き適用には「個人情報取扱申請書」による手続きが必要。

8．個人情報取扱に関する手続き

AISEL
顧客満足の一歩先へ

8-6．利用目的外の利用

公表している利用目的以外で個人情報を利用する場合は、
速やかに本人へ通知を行い、同意を得なければなりません。

利用目的は aipo ならびにアイセルホームページで公表しています。

当社が取り扱う個人情報は以下の利用目的の範囲内で利用いたします。

[1] 採用応募者情報
・必要書類の送付、ご連絡など、当社採用に係わる業務管理のため

[2] 従業員情報
・人事、給与、福利厚生など雇用管理のため

[3] お客様情報
・当社サービス、システム開発/保守/運用などの受託開発業務ならびにご要望、お問い合わせに関する対応のため

[4] ビジネスパートナー（個人事業主）情報
・弊社業務の委託管理のため

[5] 株主情報
・各種ご連絡、IR情報提供、その他株式に関する事務処理のため

[6] PMS運用情報
・個人情報保護マネジメントシステム運用情報記録の処理のため

８．個人情報取扱に関する手続き

AISEL
顧客満足の一歩先へ

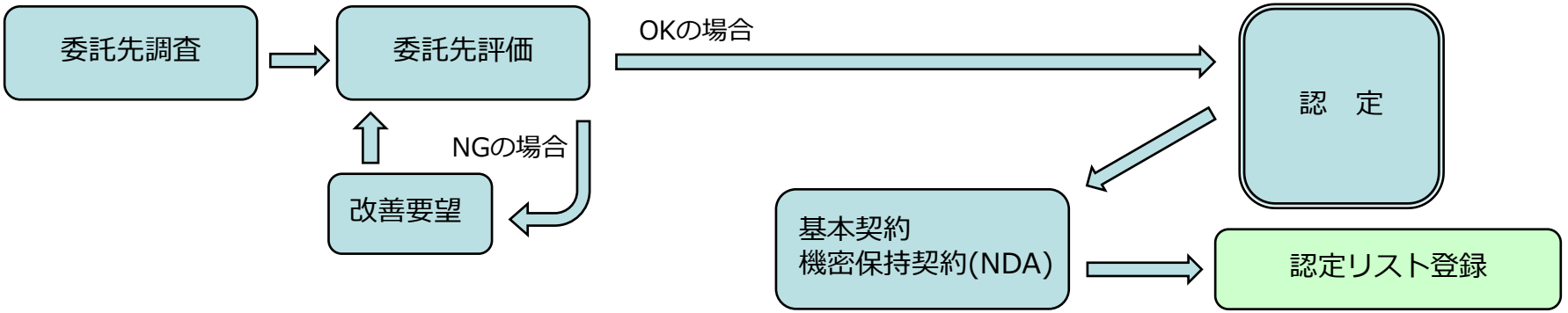
８-７．個人情報取扱に関する各担当窓口

社員情報	管理部　人事総務課	電話番号 03-5652-5236 メール（コンタクトフォーム） https://www.aisel.ne.jp/contact/
採用情報	管理部　採用課	
取引先情報/ パートナー情報	管理部　業務課	
株主情報	管理部　業務課	
その他	個人情報保護事務局	

8．個人情報取扱に関する手続き

8-8．委託先運用方法

・新規委託先と取引を開始する場合は事前の社内審査が必要
・個人情報を取り扱う業務については、一定の個人情報保護水準を満たしている業者のみ発注可能



※ 委託先の認定は最大1年間を有効とし、毎年定期的に認定を継続するか否かを再評価することとなっています。

委託先の認定・更新時による基準は、以下の観点から評価する

1．経営状態
2．情報セキュリティ及び個人情報保護能力

「委託先調査票」「個人情報保護・情報セキュリティ関係チェック」「クラウドサービスセキュリティチェックリスト」及び「委託先評価シート」を用いて記録、評価する。

・経営状態が不良となった委託先への発注はできない。
・評価NGの委託先利用が必要な場合は、改善依頼の後、再評価が必要となる。

- サプライチェーンの弱点を悪用する情報セキュリティの脅威に注意

  情報セキュリティの脅威は自組織だけでなく、調達から販売や業務委託先など一連の繋がりの中で、セキュリティ対策が甘い組織が攻撃の足掛かりとなることがあります。
  また、取引先や業務を委託する外部組織からの情報漏洩も発生し得ます。

  業務委託に関する規則の遵守や**契約内容の確認**、および**委託先組織の定期監査**等の確認の実施をお願いいたします。

8．個人情報取扱に関する手続き

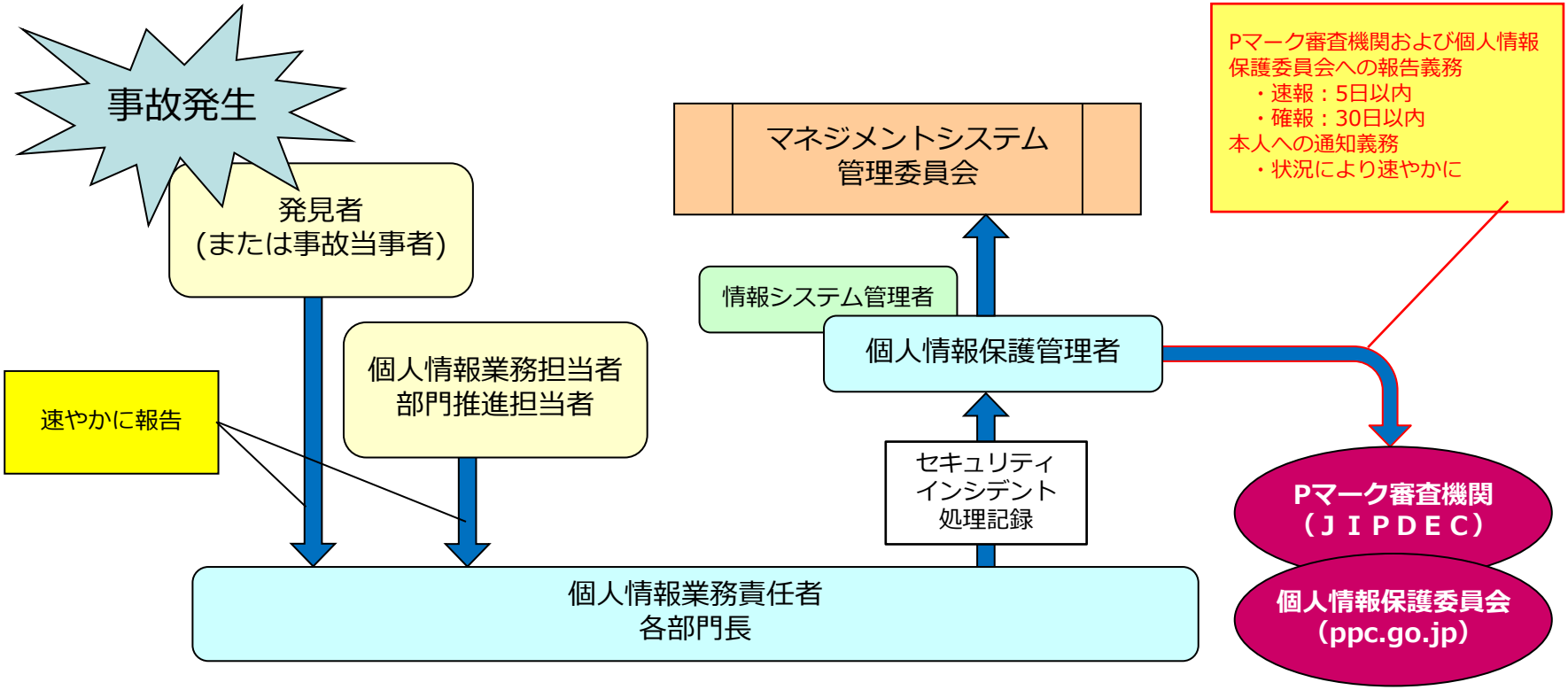
8-9．緊急事態の対応

個人情報を含むPC機器、モバイル機器、電子媒体、紙文書等の紛失、漏洩、毀損が発覚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。

原則的にISMSと共通の推進体制のため、社員は各部門長に報告、各部門長から個人情報保護管理者及び、情報システム管理者に報告を行います。部門長と連絡がつかない場合は発見者が直接個人情報保護管理者及び、情報システム責任者に報告を行うこととなります。

対応者は個人情報保護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「個人情報事故対応計画」を参照してください。



８．個人情報取扱に関する手続き

AISEL
顧客満足の一歩先へ

８-９．緊急事態の対応（続き）

個人情報の事故が発生した場合の、報告義務の要件は以下のとおりです。
また、当社が利用しているサービスや業務委託先に対する不正行為による、当社が取得しようとしている個人情報の事故も報告対象です。
影響の拡大を防止する目的があり速やかな対応が必要ですので、遅滞なくエスカレーションしてください。

1. 事故等が発生した個人情報にマイナンバーが含まれる場合
    - 情報提供ネットワークシステム等からの漏えい、滅失、毀損
    - 不特定多数の者に閲覧された
    - 不正の目的による漏えい、滅失、毀損
    - １００人を超える場合
2. 事故等が発生した個人情報にマイナンバーが含まれない場合
    - 要配慮個人情報を含んだ事故等
    - クレジットカード情報など、不正に利用されることにより財産的被害が生じるおそれがある事故等
    - 不正の目的をもって行われたおそれがある事故等
    - 個人情報に係る本人の数が１０００人を超える場合

- 上記１．または２．に該当する事故が発生した場合は、Pマーク審査機関および個人情報保護委員会に以下の事故報告が必要です。
    - 速報 ： 事故発覚から３～５日以内（暦日）※営業日ではない
    - 確報： 事故発覚から３０日以内（暦日）※営業日ではない
- 上記以外の個人情報の事故が発生した場合は、Pマーク審査機関に以下の事故報告が必要です。
    - 確報： 事故発覚から３０日以内（暦日）※営業日ではない

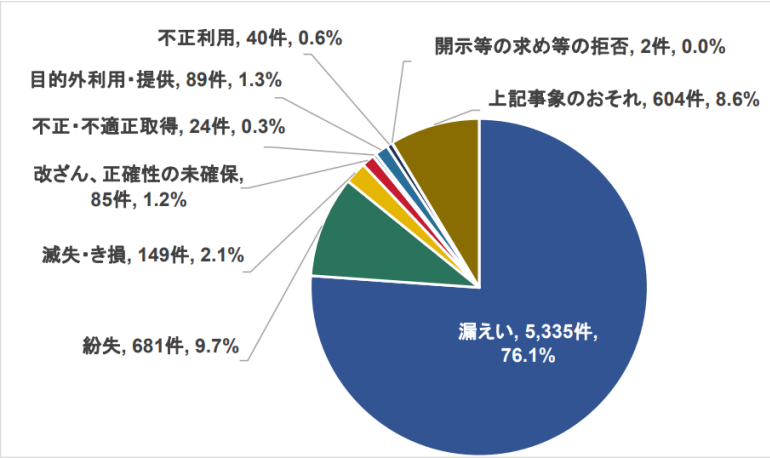
個人情報の取扱いに関する事故等の報告について（ https://privacymark.jp/system/accident/index.html ）

9．安全管理について

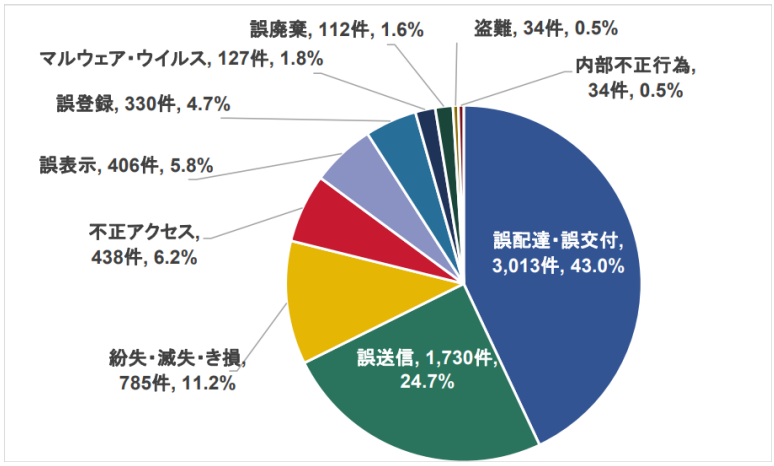
9-1．個人情報の取扱いにおける事故の原因

※出展 JIPDEC「2022年度個人情報の取扱いにおける事故報告集計結果」
https://privacymark.jp/system/reference/index.html

JIPDEC（日本情報経済社会推進協会）による集計では、2022年度の個人情報の取り扱いにおける事故報告件数は、プライバシーマーク付与事業者の 1,460社 から 7,009件でした。



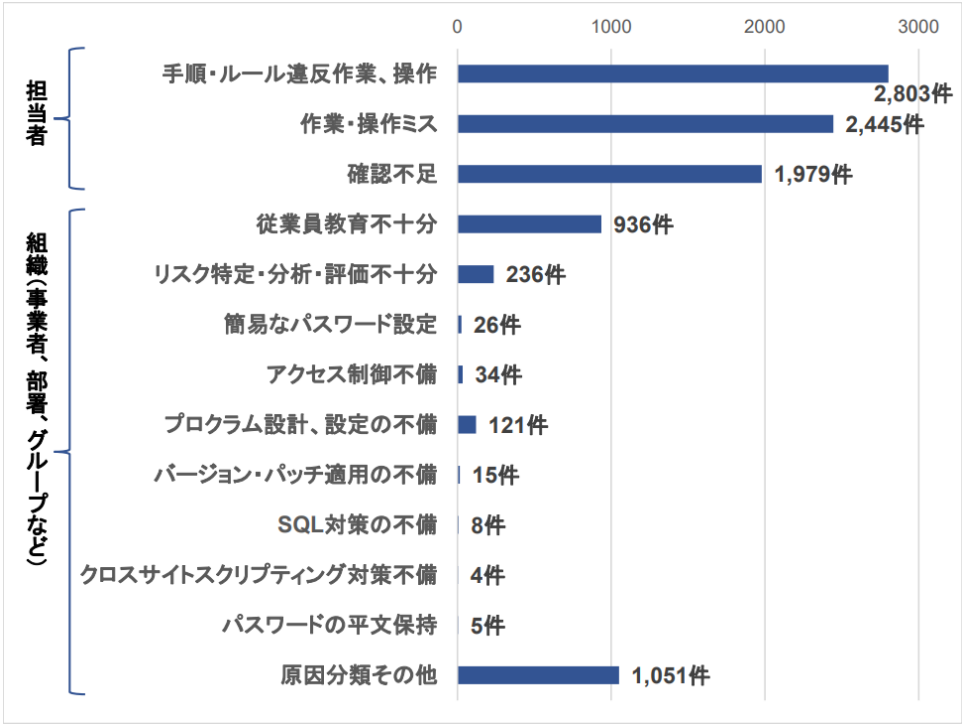
発生事象別の事故報告件数



事象分類別の事故報告件数

発生した事象別には「漏えい」が76%と最も多く、分類別には宛先ミスと思われる「誤配達,誤交付,誤送信」が67%を占めます。

原因別には “ルール違反” や “操作ミス”、“確認不足” となっており、企業の情報管理の安全性は、社員一人一人の手にかかっていると言えます。



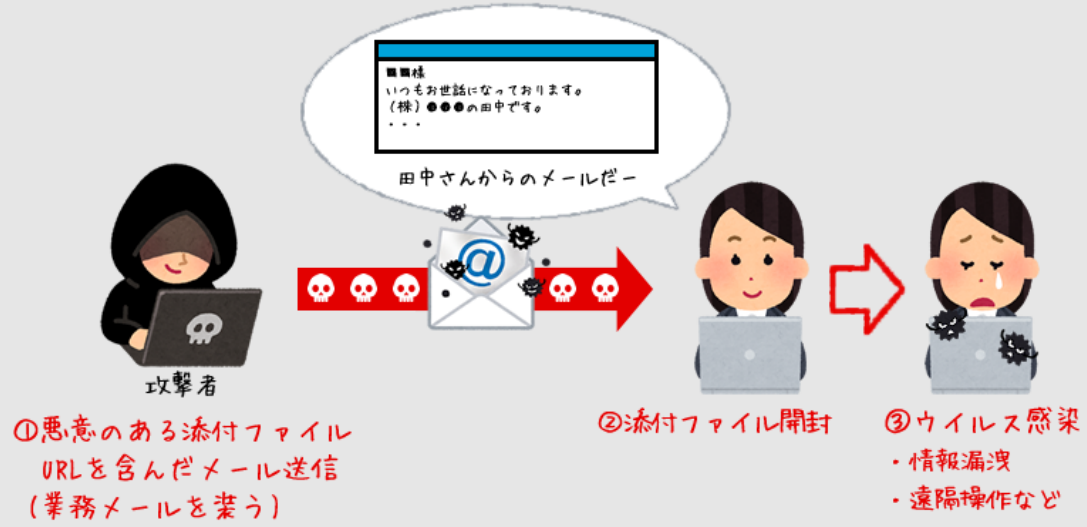
原因別集計

9．安全管理について

AISEL
顧客満足の一歩先へ

9-2．標的型メール攻撃

標的型攻撃とは、ターゲットを特定の組織やユーザー層に絞って行うサイバー攻撃です。そのターゲットに関して知り合いや取引先のふりをして悪意のあるファイルを添付したり、悪意のあるサイトに誘導するためのURLリンクを貼り付けたメールを送信し、パソコンやスマートフォンなどの端末をマルウェアに感染させようとする攻撃です。



送信元アドレスが紛らわしく偽装されたもの

・・・@rnicrosoft.com　など
（ ”m”ではなく “r”と“n” になっている）

だけでなく、
・知り合いからの脈絡のない確認依頼や、
・上司からの急な送金指示、
・添付ファイルを指定フォルダに保存せよ、
など、よくわからないものはメール以外の手段で送信元に確認してください。

アドレスが画像コードで通知されるなど、

← 視認できないため、
正当性が確認できない。

確認できない物はアクセスしないでください。

- 標的型攻撃されると

  標的型攻撃は大半が金銭や機密情報の奪取を目的としているため、何らかの経済的な損失が生じる場合が多くあります。
  また、攻撃者によってはデータベースに侵入した際に、マルウェアを設置することでバックドアを開設し、内部に何度も継続的に不正アクセスし情報を盗み出される可能性もあります。

- 標的型攻撃の原因

  ある調査によると、標的型攻撃はその9割以上がスパムメールによるものとされています。
  「業務連絡」や「お問い合わせの件」などの件名に偽装されたメールを、標的となった企業関係者が開封してしまった結果、事件に発展しているのです。

- 感染が疑われるような行動をしてしまった場合
  - 怪しいメールから変なサイトを見てしまった。
  - 怪しい添付ファイルを開いてしまった。

  など、標的型攻撃によるマルウェアの感染が疑われる場合は、すぐにマルウェアに感染していないかチェックしましょう。

サイバーセキュリティ（ https://cybersecurity-jp.com/security-measures/18646 ）より引用

9．安全管理について

AISEL
顧客満足の一歩先へ

9-3．毎日の業務で気をつけること

毎日の業務では、自分が取り扱う情報について、それを適切に管理する習慣を身につけること。
また、何が情報として保護しなければならない対象かと合わせて確認すること。

【クリアデスク】

キャビネット・袖机の鍵の管理方法	鍵は放置せず携帯すること
印刷物の管理	重要な印刷物はプリンタに放置せず、出力後速やかに回収すること
机上の情報管理	重要情報の記載の書類等を出したままにしない また、パスワード類をモニタなどに貼付しない

【クリアスクリーン】

スクリーンセーバの設定	パスワード付で10分以内で設定する AD管理下のPCについては自動的に設定される
パスワードについて	安全性の高いパスワードにすること 英大文字小文字+数字+記号で10桁以上が望ましい（ISMSユーザーズガイド） 最低6ヶ月以内に一度は変更すること
ファイルの暗号化について	暗号化ソフト、パスワード化を確実にすること
持出PCの暗号化について	暗号化ソフトの導入を実施する事

※　これらは「ユーザー遵守事項規則」にも明記されています。

9．安全管理について

9-4．日々の生活で気をつけること

個人情報保護のルールについて、よくある気を付けたい点について記載している。ISMSとも重なるが、個人情報を含む場合は特に取り扱いに注意を払うようにしたい。

【個人情報預託、取り扱いのイレギュラー発生】

・プロジェクトの開始段階で預かる予定のなかった個人情報を預かる必要が出た場合は、契約書を確認し、リスクがないか法務を交えて確認を行う。個人情報の新たな取り扱いが確定したら取扱申請の上、個人情報一覧に反映すること。法務では契約上のリスクを把握し、必要に応じて契約に覚書を追加するなどの対応を行うこと。

・個人情報は目的を開示し、本人の同意を得て、必要な都度、必要なだけの取得にとどめなければならない。
不必要な個人情報の取得や蓄積はそれ自体がリスクであり、道義的にも慎まなければならない。

→業務遂行の流れを止める可能性があってもリスクをそのまま放置しないこと。希望的観測で行動せず、最悪のケースを想定してリスクの管理、軽減を心がけること

【SNS利用の最低限のルール】

・会社からはSNSサイト、サービスに接続しない (目的外利用でもあり、行ってはいけない)

・会社内の様子がわかる写真をアップロードしない

・社員の氏名や個人情報や業務内容などを記載しない

→常識的に考えて、その行動がどのような影響を及ぼすかを念頭に置いて行動すること

【職場外の情報管理】

・飲食店などでのランチ、飲み会の場、電車などでの移動中に、会社の機密や個人情報について具体的に言及しないように注意すること。利害関係者(取引先)や情報を悪用できる人物が居合わせた場合に、情報が漏洩するなどアイセルの業務に支障をきたす危険性があることに留意すること。

→社外では酒席など含め、開放感から過度な油断をしないこと。常識的に聞かれてはいけない話をしないこと。

１０．個人情報漏えいの影響

AISEL
顧客満足の一歩先へ

もし個人情報の漏えいが発生したらどんな影響が起こりうるのか・・・

1.直接的被害

情報漏えいの結果、漏えい対象である個人や法人に対して賠償責任(クレジットカード情報の悪用などの被害)が発生した場合は、**損害賠償対応への手間・コスト**が生じる。直接被害が発生しなくとも、被害者にお詫び金を支払う事例もある。

１人あたりの損害賠償金額は、、、

・宇治市住民基本台帳データ大量漏洩事件
　15,000円
・東京ビューティーセンター（TBC）情報漏えい事件
　35,000円（※センシティブ情報を含む）

2.間接的被害

「直接的な金銭被害」の他に、「収益機会の損失」、「ブランドへのダメージ」、「顧客信用の失墜」等を指摘している企業が多く、情報漏えい発生時には、中小企業でもかかる間接被害が発生することはある程度避けられない。
一方で、**初動対応の出来不出来が企業イメージの低下等間接損害に大きな影響を与える**ことに留意が必要である。

１１．最後に

AISEL
顧客満足の一歩先へ

個人情報保護法及び当社規程やルールを違反した場合、
社会・取引先及び個人への信頼を失うことになり、アイセルへの影響は想定できないくらい大きな損害になります。

もう一度確認してください 「情報漏洩の影響」

個人情報漏洩は　**直接的被害**と**間接的被害**に分けられる。

直接的被害は被害者に対する**企業の自主的なお詫び金**と、**民事裁判の判決による損害賠償**からなり、漏洩件数とその内容、被害状況次第では**企業の倒産につながるような巨額の損害**となるケースもある。

間接的被害は**企業の信用が毀損される**ことにより、情報漏洩発生以降の**既存取引先との取引停止**や、**新規顧客案件の失注**の要因になりうる。

目に見えないが故にその影響は計り知れず、**企業経営の先行きに大きく影を落とす危険性**がある。

そうならない為に社員の皆さん1人1人の心がけが重要ですので、ご協力をお願いいたします。

プライバシーマーク（Ｐマーク）は取得してしまえば終わりというものではありません。
構築したPMS（個人情報保護マネジメントシステム）を維持して、定期的な教育や監査などを実施し問題点があれば見直し改善するなど、個人情報保護体制を継続して実施していきます。

変更履歴

改編日	改編項	改編内容
2009年3月27日	⑧個人情報取扱に関する手続き <問合せ先> ⑧個人情報取扱に関する手続き <緊急事態の対応>	組織変更に伴う担当窓口の変更 PMS管理責任者の変更
2010年７月1日	⑧個人情報取扱に関する手続き <緊急事態の対応>	PMS管理責任者の変更
2010年3月25日	②プライバシーマークとは ⑧個人情報取扱に関する手続き <問合せ先> ⑧個人情報取扱に関する手続き <緊急事態の対応>	再認定取得日記入 組織変更に伴う担当窓口の変更 PMS管理責任者の変更
2011年1月11日	②プライバシーマークとは ⑥組織体制 ⑧個人情報取扱に関する手続き <緊急事態の対応>	更新の為の申請日記入 組織変更に伴う最高責任者の役職の変更 ＰＭＳ管理責任者→個人情報保護管理者へ役職変更 PMS管理責任者→個人情報保護管理者へ役職変更
2011年10月26日	②プライバシーマークとは ⑧個人情報取扱に関する手続き <緊急事態の対応>	再認定取得日記入 PMS管理責任者の変更
2014年5月2日	②プライバシーマークとは ④JIS Q 15001：2006 ⑥組織体制（役割と責任） ⑧個人情報取扱に関する手続き ⑧個人情報取扱に関する手続き <問合せ先> <緊急事態の対応>	再認定取得日記入 最新改訂版に日付修正 体制を最新組織に変更 組織変更に伴う担当窓口の変更
2017年8月25日	②プライバシーマークとは ④JIS Q 15001：2006 ⑥組織体制（役割と責任） ⑧個人情報取扱に関する手続き ⑧個人情報取扱に関する手続き <問合せ先> <緊急事態の対応> ⑨安全管理について	再認定取得日記入 最新改訂版に日付修正 体制を最新組織に変更 組織変更に伴う担当窓口の変更 事故情報を最新版に変更

変更履歴

改編日	改編項	改編内容
2018年3月13日	②プライバシーマークとは	再認定取得日記入
	④個人情報保護方針	加筆
	⑤個人情報について	加筆、タイトル変更
	⑧個人情報取扱に関する手続き＜緊急事態の対応＞	PMSシステム管理責任者の変更
	⑩個人情報漏えいの影響	項目追加
	⑪PMSの継続的取り組みについて	項目追加
2019年7月23日	全般的に改定	全般的に改定
2019年8月1日	⑬最後に・・・	理解度テスト内容に即して加筆
2020年11月１日	全体的に内容の見直し	ＰＭＳ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	全体的に内容の見直し	改訂PMS規程類に沿わない部分があった為、関連個所修正
2021年7月7日	⑦個人情報関連規定	ISMS規程整備に伴う文言の変更
2021年8月23日	⑦⑧⑨	⑦⑨文言訂正　⑧申請書、但し書き適用項目、手続き見直し
2022年2月	２．プライバシーマークとは	マークを最新化
	９．安全管理について	情報漏えい事故発生の統計情報を最新化 最近の情報漏えい事故の発生状況を最新化
	１１．PMSの継続的取り組み	項目削除
	１２．標的型メール攻撃について	内容を縮小して、項番９．に移動
2023年1月	8-9.緊急事態の対応	Pマーク審査対応 公的機関への報告手順を追記、および報告要件を追記
2023年2月	目次	リンク設定
	6.PMS推進体制	タイトル変更、ISMSと共通の明示
	8-4.開示等請求の受付	規程改訂に応じた文章と役割記載の更新
	8-6.利用目的外の利用	タイトル変更
	8-7.個人情報取扱の各担当窓口	窓口情報（コンタクトフォーム）の最新化
	9-2.個人情報の取扱事故の原因	事故報告の統計情報にページを見直し
2023年10月	7. 個人情報関連規程	文書名称の変更に伴う修正

変更履歴

改編日	改編項	改編内容
2024年2月	8-8.委託先運用方法	サプライチェーンを悪用するセキュリティ脅威について追記
	9-1.情報漏えい事故の原因	上場企業のみの統計情報ページを削除
	9-1.個人情報の取扱い事故の原因	項番変更　個人情報事故報告の統計情報を最新化
	9-2.標的型メール攻撃	項番変更
2024年4月	JIS規格の版数	JIS Q 15001:2023に変更
	4.個人情報保護方針	改訂による変更（安全管理措置対象の追記）
	5-3.個人情報一覧	取得しようとしている個人情報を明示
	8-9.緊急事態の対応	報告対象に「当社が取得しようとしている個人情報」を追記