2022 年度　プライバシーマーク　教育資料　（スタッフ編）

個人情報保護方針

三幸株式会社（以下、「当社」といいます）は、創業以来、施設総合管理企業として常にお客様の立場に立ち、高品質で低コストのサービスを提供して参りました。当社が安定した経営を続けられることは、ひとえにお客様のご愛顧の賜物と感謝しております。

最近では、これらに加えて「お客様の課題を解決する」「お客様に利益をもたらす」というソリューション提供の考え方のもとに、専門家としてのサービスを提案・提供することを基本方針としております。更には、社会経済の変化に対応して、マーケットを充分把握し、お客様のニーズに対応した弊社独自のサービスを開発することを常に心がけ、実践しております。

当社は、お客様とのお取引を安全かつ確実に進め、より良いサービスを提供させていただくために必要な個人情報を取得させていただいております。

個人情報の取得、利用にあたっては、その利用目的を特定することとし、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扱い（目的外利用）はいたしません。また、目的外利用を行わないために適切な管理措置を講じます。

1. 法令遵守

当社は、すべての事業で取扱う個人情報及び従業者等の個人情報の取扱いに関し、「個人情報の保護に関する法律」及び関連する法令、国が定める指針その他の規範を遵守いたします。さらに、日本産業規格「個人情報保護マネジメントシステム―要求事項」（JIS Q15001）に準拠した個人情報保護マネジメントシステムを策定し、個人情報の保護に取り組んでまいります。

2. 個人情報の管理

当社は、お客様の個人情報を適正に管理及び保護するため以下の安全管理の対策を講じ、個人情報の漏えい、滅失又はき損の防止及び是正に取り組みます。

(1) 体制の整備による個人情報の適正な管理及び保護の推進
(2) 個人情報の取扱いに関する社員への積極的な教育
(3) 情報システムにおける技術的な安全管理方式の強化・推進

3. お客様からのご照会・ご意見・ご要望の受付窓口

個人情報の取扱いに関するご照会・ご意見・ご要望、苦情及び相談については、下記のお問い合わせ先までお申出ください。お申出をいただいたご意見等をもとに、より適切な対応を図るとともに、誠意をもって対応してまいります。

4. 継続的改善

当社は、社会情勢・環境の変化を踏まえて、お客様からの信頼を第一と考え、適正な個人情報の保護を実現するため継続的に個人情報保護マネジメントシステムを見直し、個人情報保護への取り組みを改善してまいります。

制定：平成 17 年4月1日
改定：令和 3 年4月1日

三幸株式会社
代表取締役　橋本　有史

☆三幸ホームページに「個人情報保護方針」、「個人情報の取扱い」、「保有個人データ・第三者提供記録に関する事項の周知など」、「特定個人情報保護方針」、「特定個人情報の取扱い」が掲載されています。必ず閲覧して下さい。

個人情報保護マネジメントシステムに適合することの重要性および利点

個人情報の取扱いについてルールを定め、PDCA サイクルに沿った運用や体制づくりをすることにより社会的信用の確保、リスクマネジメント強化、企業イメージの向上、他社との差別化が図られます。個人情報を扱う企業にとって社内から情報が流出しない体制作りは、最低限の責務です。

個人情報保護マネジメントシステムに適合するための役割および責任

当社の個人情報保護の社内体制は以下のとおりとする。

トップマネジメント：最高位で組織を指揮し、管理する
保護管理者：泉部長　　個人情報の取り扱いの実施、運用に関する責任および権限をもつ
保護監査責任者：東原部長　公平かつ客観的な立場にあり、監査の実施、報告を行う責任・権限をもつ
個人情報苦情・相談窓口担当：総務部　個人情報に関する苦情・相談の受付窓口として、対応にあたる
企画・推進担当：総務部・人事部　個人情報保護管理体制全般の推進を行う
教育担当：総務部　全従業員に対して、教育研修を企画、推進する
運用・管理担当：各部門長　当該部門の従業員に対し適切に個人情報保護に関する業務が遂行されるように指導、管理する

個人情報保護マネジメントシステムに違反した際に予想される結果

個人情報が漏えいした場合、社会的信用の低下・企業イメージの低下によりビジネスへの影響が生じ信用回復には多大な期間と努力が必要となります。

プライバシーマーク制度は、審査機関にて 2 年に一度、個人情報の取扱いが適切に行われているかの審査があります。漏えい以外でも、取扱いが適切でないと判断された場合には、プライバシーマークの剥奪という事態も有り、会社にとっては信頼を失うことになります。

「個人情報の保護に関する法律」の改正（概要）　　2022 年 4 月施行

●短期保有データの保有個人データ化・・・6 か月以内に消去する短期保存データも、「保有個人データ」に含まれる。
●不適正な利用の禁止・・・違法または不当な行為を助長・誘発するおそれ等の不適正な方法により個人情報を利用してはならない旨を明確化した。
●外国の事業者に対する、報告徴収・立入検査などの罰則が追加された。
●保有個人データの開示請求のデジタル化・・・開示請求者は、電磁的記録の提供による方法など個人情報取扱事業者の開示方法を指定でき、原則として本人が請求した方法によって開示する義務を負う。
●第三者提供記録の開示・・・第三者提供記録が、請求者による開示請求の対象となった。
●請求者からの保有個人データの利用停止・消去、第三者への提供禁止の請求権の拡充
　①保有個人データを、事業者が利用する必要がなくなった場合
　②保有個人データの漏えい等が生じた場合
　③その他、本人の権利または正当な利益が害されるおそれがある場合
●漏えい時の報告義務（個人情報保護委員会への報告、および対象者への通知）
●措置命令・報告義務違反の罰則について法定刑が引き上げられた
●仮名加工情報の新設・・・他の情報と照合しない限り特定の個人を識別することが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
●個人関連情報の新設・・・提供元では個人データに該当しないが、提供先が保有している個人データと紐づけると個人データとなることが想定される情報。提供元は、本人同意を得られていることの確認を義務付けられた。

（該当例）①Cookie 等の端末識別子を通じて収集された、個人のウェブサイトの閲覧履歴
　②ある個人の位置情報　　③ある個人の商品購買履歴・サービス利用履歴
　④メールアドレスに結び付いた、ある個人の年齢・性別・家族構成等

2022 年度　プライバシーマーク　教育資料　（スタッフ編）

「情報システム管理規程」より

（ID とパスワードの管理）

第 6 条　情報システム管理者は、許可された利用者に対し ID を付与し、必要な場合には、付与した ID を停止または削除する。

2.　利用者は、付与された ID にパスワードを設定し、他の人に使用させてはならない。パスワードの設定は次のとおりとする。

① 10 桁以上の文字数を設定する。　② 数字、英字、記号などを組み合わせる。

③ 個人に関連する情報を使用しない。　④ 推測されやすいパスワードは設定しない。

⑤ パスワードは各個人で管理を行い、他人に知られないように注意する。

⑥ パスワードは、流出時に速やかに変更する。

（ウィルス対策）

第 8 条　情報システム管理者は、社内ネットワークに接続されたすべてのパソコンについて、ウィルス対策ソフトの導入状況を管理し、利用者に対して最新パターンの適用を指示し指導する。

2.　利用者は、社内ネットワークに接続するパソコンについて、情報システム管理者の指示に従い、ウィルス対策ソフトを導入し、最新パターンを適用する。社内ネットワークに接続しないパソコンについては、情報システム利用責任者の指示に従い同様に対応する。また、差出人不明等の不審なメールに記載されているリンクや添付ファイルは開かずに削除する。

（セキュリティパッチの適用）

第 9 条　情報システム管理者は、社内ネットワークに接続されているすべてのパソコンについて、オペレーションシステム等のセキュリティパッチの適用を、利用者に対して指示し指導する。

2.　利用者は、社内ネットワークに接続するパソコンについて、情報システム管理者の指示に従い、オペレーションシステム等のセキュリティパッチを適用する。社内ネットワークに接続しないパソコンについては、情報システム利用責任者の指示に従い同様に対応する。

（情報機器に対する措置）

第 17 条　当社が所有または保有する情報機器は、セキュリティを確保するため、次の措置をとる。

①　パソコンに対する措置

第 6 条第 2 項の要領で起動用パスワードを設定し、パスワード付スクリーンセーバーを待ち時間 5 分として設定する。

②　スマートフォン、タブレット、携帯電話等の端末に対する措置

利用者は、管理可能な場所に保管または常態的に身に着けるものとし、第 6 条第 2 項、第 9 条第 2 項を準用する。

③　パソコン、記録媒体の措置

社外への持ち出しを禁止する。ただし、業務上やむを得ず、所定の申請書により部門長の承認を得て、申請書に記載された事項を持出者が順守する場合はこの限りではない。

④　部門長は、各部門が管理しているすべてのパソコン、記録媒体の台帳を作成し管理する。

（個人名義の情報機器による当社情報システムの利用）

第 18 条　社内に個人名義のパソコンを持ち込み、社内ネットワークに接続し、当社の情報システムを利用する場合は、所定の申請書により部門長の承認を得るものとし、申請書に記載された事項を順守する。

2.　社外から個人名義のパソコン、スマートフォン、タブレット端末により、当社の情報システムを利用する場合は、所定の申請書により、部門長の確認と情報システム管理責任者の承認を得るものとし、申請書に記載された事項を順守しなければならない。

3.　個人名義の情報機器の通信費用、保守費用、紛失等による再取得費用は個人の負担とする。

「マルウェア（悪意のあるプログラムやソフトウェア）」感染

「Emotet」感染、従業員装うメールが送信 － リコーリース

リコーリースは、パソコンがマルウェア「Emotet」に感染し、従業員を装った「なりすましメール」が送信されたと発表した。同社によれば、同社の一部端末にマルウェア「Emotet」が感染。情報を窃取されたと見られ、同社従業員を装うメールが複数の関係者に対して送信されたという。問題のメールは、パスワードを設定した zip ファイルが添付されており、送信元として同社従業員を名乗っているが、同社のものとは異なるメールアカウントより送信されていた。同社ではドメイン「jp.ricoh.com」「rle.ricoh.co.jp」を含むメールアカウントを利用しているとし、異なるメールアドレスから送信された同社を装うメールについては、添付ファイルや本文中の URL を開かず、削除するよう求めている。　（Security NEXT － 2022/02/09 ）

「対　策」

Emotet への感染を防ぐというためだけにとどまらず、一般的なウィルス対策として、次のような対応をすることを勧めます。

●身に覚えのないメールの添付ファイルは開かない。メール本文中の URL リンクはクリックしない。

●自分が送信したメールへの返信に見えるメールであっても、不自然な点があれば添付ファイルは開かない。

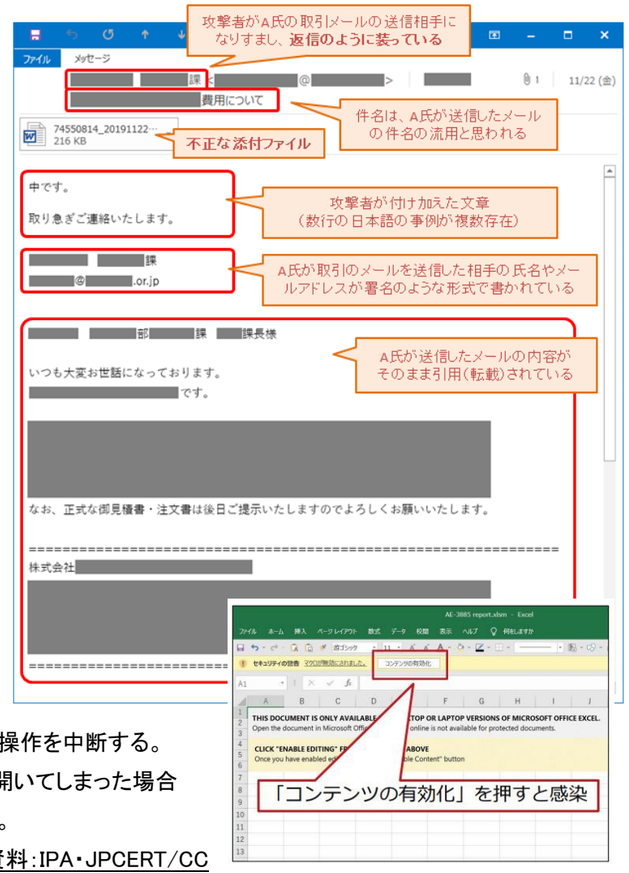
●OS やアプリケーション、セキュリティソフトを常に最新の状態にする。

●信頼できないメールに添付された Word 文書や Excel ファイルを開いた時に、マクロやセキュリティに関する警告が表示された場合、「マクロを有効にする」「コンテンツの有効化」というボタンはクリックしない。

●メールや文書ファイルの閲覧中、身に覚えのない警告ウインドウが表示された際、その警告の意味が分からない場合は、操作を中断する。

●身に覚えのないメールや添付ファイルを開いてしまった場合は、すぐにシステム管理部門等へ連絡する。

「正規のメールへの返信を装う手口」



資料：IPA・JPCERT/CC

漏えい等に対応する組織体制

個人情報の漏えい等が発生した場合、迅速かつ適切な対応を行うために、発生した部署は直ちに部門長に報告、部門長は保護管理者・苦情・相談窓口（総務部）に報告し対応に当たる。

対応として事実関係の調査、原因の究明、影響範囲の特定、対応方法の検討・実施、再発防止策の検討・実施、関係者・関係機関への連絡・対応等を行う。