2022 年度　プライバシーマーク　教育資料　（現場編）

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

個人情報の漏えい事故の原因の多くは、人為的なミスによるものです。また、その大半は従業員の個人情報の重要性に対する認識不足による<u>うっかりミス</u>です。情報漏洩が発生した場合、今まで積み上げてきた企業の信用を一度に失うことになります。

個人情報保護対策の仕組み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

個人情報保護に関して、従業員各人の役割及び責任は、法令、規範などを遵守し、個人情報保護マネジメントシステムの規定に従い、個人情報の保護及び管理のため充分な注意を払いつつ業務を行なうことです。

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。また、漏えいに関与した本人は、社会的な制裁などを受けることも考えられます。

☆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を審査があります。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。

プライバシーマーク付与事業者が実践する 10 の取り組み　　（JIPDEC 資料より）

1、個人情報を取得する際には、その利用目的および第三者に提供するかなどの必要な事項をはっきりと通知する。
2、明示された内容（利用目的および第三者への提供など）について、同意がなければ個人情報は取得しない。また偽りその他不正の手段により取得しない。
3、取得する個人情報は、利用目的を特定してその範囲内で利用する。
4、取得した個人情報の利用目的などを変更する場合は、事前に通知し、同意を取り直す。
5、個人情報の開示、訂正、削除、利用停止などの求めがあれば、それぞれの手続きの要件に基づき対応する。
6、取得した個人情報の漏えい等が生じないよう安全かつ正確に管理する。
7、個人情報の取り扱いの全部または一部を他社に委託して行う場合は、当社と同等の個人情報保護体制ができている事業者を選ぶ。また、委託している間は、適正に管理と監督を行う。
8、他社から個人情報の提供を受ける場合には、適正に取得したものであるかをあらかじめ確認する。
9、問い合わせや苦情などに迅速に対応する。
10、以上のような内容を含む『個人情報保護方針』や『個人情報の取り扱いについて』などをホームページなどで公表する。

2022 年度　プライバシーマーク　教育資料　（現場編）

付与事業者から報告のあった原因別事故報告件数と割合（2020 年度）

（1）原因別事故報告件数　　資料：一般財団法人日本情報経済社会推進協会（JIPDEC）

原　因		漏えい						紛失・盗難			その他	合計
		誤送付					その他漏えい	紛失	盗難			
		宛名間違い等	封入ミス	配達ミス	メール	FAX			車上荒し	置き引き等		
2019 年度	報告件数	400	329	58	590	136	446	421	5	6	152	2,543
	割合（%）	15.7	12.9	2.3	23.2	5.3	17.5	16.6	0.2	0.2	6.0	100.0
2020 年度	報告件数	314	323	137	764	110	454	394	5	3	140	2,644
	割合（%）	11.9	12.2	5.2	28.9	4.2	17.2	14.9	0.2	0.1	5.3	100.0

原因別事故の傾向　：「メール誤送信」（764 件 28.9%）が最も多い

「誤送付」の内訳の原因別割合をみると、2020 年度は「メール誤送信」が増加しているのに対し、紙媒体による「宛名間違い等」「封入ミス」「FAX 誤送信」は減少しています。これは、新型コロナウイルス感染症対策の「テレワーク」導入等による、通信手段・連絡手段の変化によるところと推測されます。

●「その他漏えい」の内訳（件数）

内　容		ウイルス感染	プログラム/システム設計・作業ミス	不正アクセス・不正ログイン	口頭での漏えい	関係者事務処理・作業ミス等	合計
2019 年度	報告件数	9	185	66	48	138	446
2020 年度	報告件数	29	102	54	37	232	454

その他漏えい　：　関係者事務処理・作業ミス等が 2020 年度 232 件で前年の 138 件より大幅に増加した。ウイルス感染 29 件で前年の 9 件より増加した。

●「その他」の内訳

内　容		不正取得	目的外利用	同意のない提供	内部不正行為	誤廃棄	消失・破壊	左記に分類できない内容	評価対象外	合計
2019 年度	報告件数	2	47	12	8	66	9	3	5	152
2020 年度	報告件数	3	37	9	15	38	8	27	3	140

「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。

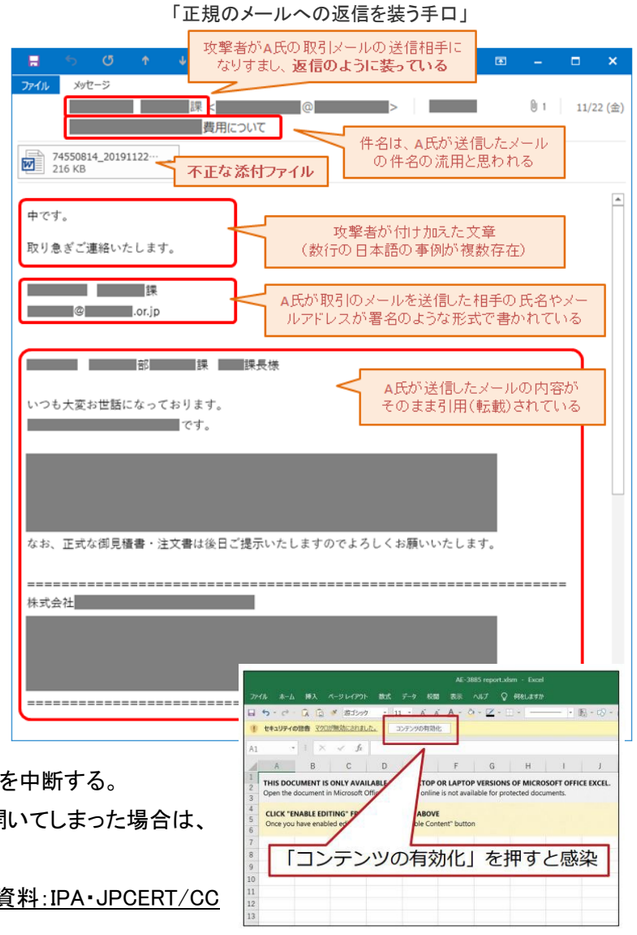
●OS やアプリケーション、セキュリティソフトを常に最新の状態にする。

●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。