情報セキュリティ規程(情報セキュリティ基本方針)

（目的）

第１条　この規程は、株式会社アキタ保険が業務上取り扱う顧客情報、個人情報、機密情報をサイバー攻撃等の脅威から適切に保護することを目的とする。

２　顧客情報、個人情報、機密情報の漏洩・破損防止、ウイルス感染やサイバー攻撃防止、インターネットやパソコン等を適切に運用・管理・利用するため、情報セキュリティ対策として、損害保険業界推奨の損保クラウドシステムを導入し、当社の基幹システムと位置づけ、運用します。

３　情報セキュリティとは、顧客情報、個人情報、機密情報等の情報資産の「機密性」「可用性」「完全性」を確保し、維持することをいう。機密性とは、情報資産を、アクセス権を持つ者のみに所定の方法にて開示し、アクセス権を持たない者から保護することをいう。可用性とは、情報資産を、アクセス権限を持つものが必要な時に利用できるように保持することをいう。完全性とは、情報資産を、整合性を保ちながら改ざん等がなされることなく、正確に処理し保持することをいう。

４　情報セキュリティポリシーとは、下記の構成要素から成り立っています。

目　　的：情報セキュリティポリシー策定の目的や背景を示すもの。

適 用 範 囲：ポリシーの対象となる組織や情報資産の範囲を明確にする。

基 本 方 針：組織の情報セキュリティに対する基本的な考え方や方針を宣言します。

対 策 基 準：情報資産の分類や管理、アクセス制御、インシデント対応など、情報セキュリティ対策の具体的な基準を定めます。

実 施 手 順：対策基準を実践するための詳細な手順やルールを規定します。

評価・見直し：ポリシーの遵守状況の評価や、定期的な見直しについて定めます。

５　情報セキュリティ対策　損保クラウド　マイクロソフト３６５の構成

マイクロソフト３６５はクラウドサービスのグループウエアで、ＩＩＪによるセキュリティ機能追加、ガーディアンウォールによるメール管理機能により構成されています。マイクロソフト３６５として、主にアウトルック、ワード、エクセル、パワーポイント、シェアポイント、ワンドライブ、チームズを利用します。アウトルックによるメール、シェアポイントやワンドライブによるファイル管理、チームズによるファイル管理・ＷＥＢ会議・チャットは全てセキュリティにより保護されています。

(1)ＩＩＪ(株式会社インターネットイニシアティブ　Internet Initiative Japan inc.)

Microsoft365の{Microsoft365 Exchange Online}というメール機能にセキュリティ機能を追加するためのアプリがIIJです。

(2)Ｇｕｒｄｉａｎ Ｗａｌｌ

メールの送受信ルールを設定・管理するシステム。メール送信後、宛先や内容が誤っていた場合に遅延メールのリンクからメール送信を止めることができます。

(3)Ｍｉｃｒｏｓｏｆｔ　３６５　https://www.office.com

情報共有、ファイル共有、データ保存などを行う、クラウドのグループウエア。

損保クラウド　マイクロソフト３６５の主な機能と当社の対応

①標的型攻撃対策

・悪意のあるURLに対してクリック時の保護をリアルタイムに行う。

・送信された添付ファイルをチェックし危険な場合はブロックします。

・なりすましメールを検知し、管理者に連絡されると共にメールを検疫します。

・クラウドストレージに格納されたファイルは定期的にスキャンされ、ウイルス感染があった場合はブロックされます。

・ウイルス対策ソフトでは検知できない未知のウイルスに対応して、機械学習などで悪意のある動作を検出し無害化します。

②メール・添付ファイル暗号化

・添付ファイルは自動的にＺＩＰ暗号化し、パスワードがかけられるため、万一、盗難に遭っても情報漏えいを防止できます。

・損保クラウドはメールデータ及び通信にも暗号化がかけられているため、情報漏えい、改ざん、盗聴の被害を防ぐことが出来ます。

③メール誤送信防止

・一定期間（当社では５分間）送信を自動的に保留でき、誤り気付いた場合はガーディアンウォールにて送信を止めることが出来ます。

④不正アクセス防止

・アカウントとパスワード、電話による二要素認証により、損保クラウド全体、メール等の第三者の不正な利用を防止できます。

・当社においては、パスワードはアルファベットの小文字と大文字、数字、記号の組み合わせによる４種１０桁以上とし、パスワードを強化する。不正アクセスの疑義が発生した場合等、的確にパスワードを変更すること。二要素認証については、本人の業務用携帯、本人所有の携帯、会社固定電話によるものとする。

・前回の利用日時が確認できるため、不正アクセスをすぐに確認できます。

・セキュリティ事故が起きた際にはログを取得し速やかに状況が確認できます。

・シェアポイントにはアクセス権限を設定しており、社内の情報管理も適切に行います。

⑤端末の対策

・パソコンを監視し、未知のウイルスを検知、隔離します。

・クラウド型で自動アップデートされるため、一般的なウイルス対策ソフトと比較しパソコンの処理に影響が出ません。

（適用範囲）

第２条　本規程は、業務上取り扱う顧客等の情報資産および会社の情報資産すべてに適用する。なお、顧客等の情報資産の管理・取り扱いについて、契約等により特段の運用ルール等を定めている場合には、当該運用ルール等に従うものとする。

２　本規程は、前項の情報資産を利用する全社員に適用する。

（基本方針）

第３条　当社は、業務上取り扱う顧客等の情報資産および会社の情報資産を事故・災害・犯罪などの脅威から守り、お客さまならびに社会の信頼に応えるべく、以下の方針に基づき全社で情報セキュリティに取り組みます。

１　当社は、経営者主導で組織的かつ継続的に情報セキュリティの改善・向上に努めます。

２　当社は、情報セキュリティの維持及び改善のために社内体制を整備し、情報セキュリティ規程を定め、運用します。

３　当社は、すべての社員が情報セキュリティのために必要とされる知識、技術を習得し、情報セキュリティに取り組みます。

４　当社は、情報セキュリティに関わる法令、規制、規範、契約上の義務を遵守するとともに、お客さまの期待に応えます。

（組織体制）

第４条　情報管理責任者は、組織内の情報セキュリティの適切な環境等の整備、点検、組織内における指導、情報セキュリティポリシーを徹底するために必要な措置を講じなければならない。業務上、必要がある時は、代表取締役、または、情報管理責任者の命により、情報セキュリティに関する業務を職員に委任する。

２　教育責任者は、情報セキュリティ規程に定められた事項を理解、遵守するとともに、全社員が情報セキュリティを遵守するための教育を企画、運営します。

（リスクと評価）

第５条　情報管理責任者は、技術の進歩や業務環境の変化等も考慮の上、情報資産のリスク評価を多方面から継続的に実施し、それを情報セキュリティポリシー及び、それに基づく各種施策に反映させることにより、情報セキュリティの維持、向上を図るも

のとする。

（実施手順、遵守事項）

第６条　全社員が会社のパソコン等を利用するにあたって、個人情報・機密情報保護、情報セキュリティの観点から以下の事項を遵守しなければならない。

（１）　パソコン、タブレット等の購入、リースの状況、ウイルス対策ソフトの有効期限、共同ゲートウエイのIDなどをパソコン台帳に登録、管理する。

（２）パソコン等を破損することのないよう適切に使用すること。

（３）電子メール等を介してパソコン等がコンピュータウイルスに感染することのないよう、ウイルス対策ソフトをインストールし、アップデートを行い、常に最新の状態で使用すること。 同様にウインドウズやエッジのアップデートを行い、常に最新の状態で使用し、リアルタイムでの不正検知ができる状態にすること。但し、パソコン、タブレットのOSそのもののバージョンアップについては、保険会社で使用しているアプリケーションが未対応の場合もあるため、事前に保険会社に確認すること。

（４）①パソコンは、起動パスワード、ログインパスワードを設定すること。ログインパスワードはアルファベットの小文字と大文字、数字、記号の組み合わせによる「4種10桁以上」とし、パスワードを強化する。不正アクセスの疑義があった場合等、的確にパスワードを変更すること。

②タブレット、スマートフォン、携帯等はパスワードまたはパスコードを設定すること。

③会社所有のスマートフォン、携帯等についてはパスワードをつけること。アドレス帳登録件数は必要最小限とし、個人が特定されないようフルネームでの入力を行わず、姓のみ、略称、イニシャルや記号などを活用して登録する。携帯等の紛失や盗難発生時は本社に報告し、電話会社へ直ちに連絡して利用停止やデータ削除手続きを行う。本社においては、所属保険会社への報告を行う。業務上、写真を撮影した場合は、T-SHOTフォルダーを利用するなど、遅滞なく、データ削除を行うこと。シェアポイントやワンドライブに保存する場合は、CubePdfを利用して圧縮して容量を小さくし、必要最低限度の保存とし、不要になったら速やかに削除すること。

④無線ＬＡＮ(≒wifi)を利用する場合、提供元が明確でない、または、パスワードが設定されていないwifiには接続しないこと。

（５）業務上の必要からパソコンを社外に持ち出す場合には、持ち出し管理簿に記載、申請し、管理者の承認を得ること。

（６）個人情報、機密情報等を含むファイルについては必ずパスワードをかけること。社内においては会社共通のパスワード等を使用し、社外に送信するファイルは別なパスワードを使用する。

（７）ＵＳＢフラッシュメモリ、ＳＤカード、マイクロＳＤ等は紛失リスクが高いため、原則使用しないこと。

（８）ＵＳＢフラッシュメモリ等を使用する場合は社外に持ち出さず、社内でのみ使用し、施錠できるところに保管し、保管場所を毎日点検すること。

（９）外出する際は机上にある個人情報等を放置せず収納すること。

（１０）メールソフトについては、情報セキュリティの観点から、損保クラウドのアウトルック　オン　ザ　Ｗｅｂ以外使用してはならない。メールを送信する際は、個人が特定される文章は書かないこと。また、個人情報、機密情報等を含む添付ファイルを送信する場合は、パスワードを設定し、２回目のメールでパスワードを送る形とし、情報漏洩防止措置をとること。

ファイルパスワード、ＺＩＰフォルダパスワード

【確認事項】

①複数宛先への一斉送信時のBcc指定（送受信者間の承諾あるときを除く）。「私の個人情報であるメールアドレスを勝手に教えた」と指摘されることが想定されます。

②ファイルのパスワードロック、およびパスワードの電話や別メール等での別途通知。

③スパムメールや標的型攻撃メール等による不審なメールに対して、添付ファイルや本文中のリンクを開かないこと。
サイバー攻撃は、標的型メールの他にも、サポート詐欺、ランサムウエア、フィッシング詐欺、不正ＷＥＢサイト閲覧による攻撃があります。万一の場合は、インターネットから切断し、電源を切らずに社長、総務部長に連絡して下さい。
④初めて送信する宛先の場合、送信先アドレスの内容のダブルチェック、または、テスト送信による正しい宛先の事前確認。送信内容が個人情報、機密情報等がある場合は、特に注意を払うこと。
⑤メール等のデータについては不要なデータを保存せず、適宜削除するように努め、４年を超えたものは削除する。
⑥不審なメールの添付ファイルは開かない、ＵＲＬを不用意にクリックしない。本社に連絡、相談して下さい。
⑦初めて送信するメールアドレス、宛先の場合、送信先アドレスの内容のダブルチェック、またはテスト送信による正しい宛先の事前に確認すること。
（１１）ユーザーＩＤは個人ごとに設定する。
（１２）従業者の入社、退職や異動に伴うＩＤの追加、削除は情報管理責任者が最終確認を行い、アキタ保険募集人入退社点検・特定関係法人・印鑑登録リストに記録、管理する。
（１３）パソコン、タブレット等の情報機器の廃棄については、パソコン台帳で管理し、データ消去ソフトによる消去、不可能な場合は物理的破壊、信頼できる業者への廃棄依頼のいずれかによる方法で確実にデータ廃棄を行う。
（１４）ホームページはホームページ会社に作成、管理を依頼し、ハイパー・テキスト・トランスファー・プロトコル・セキュア(https)で作成し、通信内容を暗号化すること。お客様からの問い合わせについても、セキュリティ・ソケット・レイヤー/トランスポート・レイヤー・セキュリティ（ＳＳＬ／ＴＬＳ）を利用し、情報を暗号化して送信するよう作成する。当社以外のホームページの閲覧時も、不正なＷＥＢサイト(偽サイト　フィッシング詐欺)もあるため、疑いの目で確認し、不審に感じたらアクセスしないこと。公式サイトと書いてあるのに公式サイトではない場合もあります。
（１５）①損保クラウド(マイクロソフト365)の使用にあたっては、機密情報・人事情報・個人情報漏洩を防ぐため、業務上必要な職員のみがアクセスできるよう、アクセス権を設定します。
②パソコンやタブレット等の盗難、紛失による個人情報・機密情報の漏洩を防ぐ、パソコン等のトラブルにより、パソコン等の復旧が困難となり、データが復活できない場合のトラブルに備え、会社全体で共有するファイル等はシェアポイントに保存し、個人で保存するファイル等はワンドライブに保存すること。
③パソコン等の本体のハードディスク（ＳＳＤ含む）へのフォルダ、ファイル等の保存は、業務のために、当座、使用する場合に使用すること。保存が必要なファイルは、個人使用のファイルはワンドライブ、会社で共有使用の場合は、分類のルールに従ってシェアポイントに保存すること。
④タブレットに電子証明書登録などのために、メールを使用する場合は、損保クラウド(Microsoft365)を使用すること。共同ゲートウエイのＴ－ｎｅｔメールなど、各保険会社のメールシステムを使用することも可。
（１６）インシデント(事故)の発生、インシデントの疑いがある場合の本社報告
不正アクセス、盗難、紛失、メール・モバソンチャット・ＦＡＸ誤送信、郵便等のご配送が発生した場合、その疑いがある場合、ウイルス感染、サイバーインシデント(事故)の疑いがある場合は、本社の総務部長、社長に報告すること。
総務部長、社長は状況を確認し、対策検討、所属保険会社への報告を行う。
・事件や事故の種別、重要度
・検知と分析、封じ込め、根絶、復旧、教訓、証拠保全、再発防止策の検討
・損保ジャパンに加入しているサイバー保険の付帯サービス業者に相談、対策案立案

（禁止事項）
第７条　　従業員は、会社のパソコン、タブレット等を利用するにあたって、以下の行為をしてはならない。
（１）会社の業務に関係のない文書を作成するなど、私的な目的でパソコン等を使用すること。
（２）会社のパソコン、タブレット等で、会社の業務に関係のないホームページ閲覧、各種ＳＮＳの閲覧・使用、メールの送受信

を行うこと。また、会社のパソコン、タブレット等を個人の私的利用目的で使用すること。

（３）私用の電子メールを送受信すること、会社のメールを個人のパソコン、タブレット、スマートフォン、携帯等に転送すること。

（４）社外の者に会社のパソコンを使用させること、貸与すること。

（５）パソコンを許可なく社外へ持ち出すこと。

（６）会社の秘密情報を業務以外の目的に使用し、または、社外に漏らすこと、社外に持ち出すこと。

（７）業務ため、社外に持ちだすタブレット、携帯（本体、マイクロＳＤ）は、個人情報、法人情報等は保存せず、空にした状態で携行すること

①会社に戻るまでなど、一時保存する場合はファイル作成時にパスワードをつけ、帰社次第、パソコンやサーバーへ保存し、タブレット等からは速やかに削除すること。

②写真撮影しても、タブレットに情報が残らない「Ｔ－ｓｈｏｔフォルダー」の活用を優先すること。

（８）個人所有のパソコンやタブレット、スマートフォン、携帯等を業務で使用すること。個人所有のメールアドレスを業務で使用すること。

（９）業務用パソコン等におけるファイル交換ソフト（Winny、Share等）をインストール、使用すること、及び、業務に関係のないソフトをインストール、使用すること。

（１０）g-mail、yahooメールなどのフリーメールアドレスを業務で使用すること。

（１１）グーグルドライブ、ヤフーボックスなど、会社で承認していないクラウドサービスを業務で使用すること。（会社で承認しているのは損保クラウドのみ。）

（１２）Ｆａｃｅｂｏｏｋ、Ｔｗｉｔｔｅｒ、ＬＩＮＥなどのＳＮＳを業務で使用すること。

例外１．事故処理など、保険会社の業務に関連して、損保ジャパンのセキュリティつきのＬＩＮＥ(モバソンチャット)を使用は可とする。

例外２．当社の社内のＢＣＰ　ＬＩＮＥについては、緊急時の使用は可とする。但し、顧客に関する情報、個人情報・機密情報については入力しないこと。

その他、前各号に準ずる行為

（報告義務等）

第８条　従業員は、以下の場合には、直ちに会社に連絡し、会社の指示に従って適切な措置を講じなければならない。

（１）　パソコン、タブレット、携帯等が故障・破損した場合

（２）　パソコン、タブレット、携帯、電子記録媒体等が紛失・盗難にあった場合

（３）　パソコン、タブレット等がコンピュータウイルスに感染した場合

（４）　パソコン、タブレット等に対して社外から不正なアクセスがなされた場合

２　従業員は、会社から、自己の送受信した電子メールの内容の開示を求められた場合には、直ちにこれに応じなければならない。

（処分等）

第９条　会社は、この規程に違反する行為を行った従業員に対して、就業規則の定めるところにより懲戒処分を行うことができる。

２　会社は、この規程に違反する行為を行った従業員の上司について監督が不十分であった場合には、その上司について責任を問うことがある。

（施　行）

第１０条　　本規程は、平成27年12月1日から施行する。

附　則　　第２条遵守事項、第３条禁止事項について、令和２年９月１日より改定する。