個人情報の適切な管理のための措置に関する規則

１７－一般－１００７０
２０１７年　４月　１日
改正１７－一般－１０１８３
２０１７年　６月１３日
改正１９－一般－０００４３
２０１９年　２月　１日
改正２１－一般－０００４５
２０２１年　４月　１日
改正２２－一般－０００９８
２０２２年　４月　１日
改正２４－一般－０００７４
２０２４年　３月２７日

第１章　総則

（目的）

第１条　この規則は、株式会社日本貿易保険（以下「会社」という。）の保有する個人情報の管理に関する基本的事項及び行政機関等匿名加工情報（以下「匿名加工情報等」という。）の適切な管理に関する事項を規定することにより、事務及び事業の適正かつ円滑な運営を図りつつ、個人の権利利益を保護することを目的とする。

（定義）

第２条　この規則における用語の定義は、「個人情報の保護に関する法律」（平成１５年法律第５７号。以下「法」という。）において使用する用語の例による。

第２章　管理体制

（総括保護管理者）

第３条　会社に、総括保護管理者を一人置くこととし、総務部長をもって充てる。

２　総括保護管理者は、会社における保有個人情報及び匿名加工情報等（以下「保有個人情報等」という。）の管理に関する事務を総括する任に当たる。

（保護管理者）

第４条　本店に置かれる部、大阪支店及びシンガポール支店に保護管理者を一人置くこととし、当該部及び支店の長をもって充てる。

２　本店に置かれる部は、組織規則の定めるところによる。

３　保護管理者（総務部にあっては、総括保護管理者。以下同じ。）は、各部及び支店における保有個人情報等の適切な管理を確保する任に当たる。保有個人情報等を情報システムで取り扱う場合、保護管理者は、当該情報システムの管理者と連携して、その任に当たる（注）。

（注）例えば、第５章、第６章、第９章第４２条、第４３条その他保有個人情報を情報システムで取り扱う場合、保護管理者は、情報システムの管理者と連携して、それぞれの措置を講ずる。

（保護担当者）

第５条　保有個人情報等を取り扱う各グループ（以下「各グループ」という。）に保護担当者を一人置くこととし、各グループの長（シンガポール支店にあっては、次長）をもって充てる。

２　保護担当者は、保護管理者を補佐し、各グループ又はシンガポール支店における保有個人情報等の管理に関する事務を担当する。

（監査責任者）

第６条　会社に、監査責任者を一人置くこととし、監査役をもって充てる。

２　監査責任者は、保有個人情報等の管理の状況について監査する任に当たる。

（個人情報管理委員会の開催）

第７条　総括保護管理者は、保有個人情報等の管理に係る重要事項の決定、連絡・調整等を行うため必要があると認めるときは、関係職員を構成員とする個人情報管理委員会を設け、随時に開催する。

第３章　職員の責務と教育研修の実施

（職員の責務）

第８条　職員は、法の趣旨に則り、関連する法令及び規程等の定め並びに総括保護管理者、保護管理者及び保護担当者の指示に従い、保有個人情報等を取り扱わなければならない。

（保有個人情報等の取り扱いに従事する職員への教育研修）

第９条　総括保護管理者は、保有個人情報等の取扱いに従事する職員（派遣労働者（注）を含む、以下同じ。）に対し、保有個人情報等の取扱いについて理解を深め、個人情報及び匿名加工情報等の保護に関する意識の高揚を図るための啓発その他必要な教育研修を行う。

（注）派遣労働者についても、従事者の義務（法第６７　条）が適用されるところであり、保有個人情報の取扱いに従事する派遣労働者についての労働者派遣契約は、保有個人情報の適切な取扱いを行うことに配慮されたものとする必要がある。

２　総括保護管理者は、保有個人情報等を取り扱う情報システムの管理に関する事務に従事する職員に対し、保有個人情報等の適切な管理のために、情報システムの管理、運用

及びセキュリティ対策に関して必要な教育研修を行う。

３　総括保護管理者は、保護管理者及び保護担当者に対し、各グループの現場における保有個人情報等の適切な管理のための教育研修を実施する。

４　保護管理者は、当該部又は支店の職員に対し、保有個人情報等の適切な管理のために、総括保護管理者の実施する教育研修への参加の機会を付与する等の必要な措置を講ずる。

第４章　保有個人情報等の取扱い

（アクセス制限）

第１０条　総括保護管理者は、保有個人情報等の秘匿性等その内容に応じて、当該保有個人情報等にアクセスする権限を有する職員とその権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限る。

２　アクセス権限を有しない職員は、保有個人情報等にアクセスしてはならない。

３　職員は、アクセス権限を有する場合であっても、業務上の目的以外の目的で保有個人情報等にアクセスしてはならず、アクセスは必要最小限としなければならない。

（複製等の制限）

第１１条　職員が業務上の目的で保有個人情報等を取り扱う場合であっても、保護管理者は、次に掲げる行為については、当該保有個人情報等の秘匿性等その内容に応じて、当該行為を行うことができる場合を必要最小限に限定し、職員は、保護管理者の指示に従い行う。

一　保有個人情報等の複製

二　保有個人情報等の送信

三　保有個人情報等が記録されている媒体の外部への送付又は持出し

四　その他保有個人情報等の適切な管理に支障を及ぼすおそれのある行為

（誤りの訂正等）

第１２条　職員は、保有個人情報等の内容に誤り等を発見した場合には、保護管理者の指示に従い、訂正等を行う。

（媒体の管理等）

第１３条　職員は、保護管理者の指示に従い、保有個人情報等が記録されている媒体を定められた場所に保管するとともに、必要があると認めるときは、金庫への保管、施錠等を行う。また、保有個人情報が記録されている媒体を外部へ送付し又は持ち出す場合には、原則として、パスワード等（パスワード、ＩＣカード、生体情報等をいう。以下同じ。）を使用して権限を識別する機能（以下「認証機能」という。）を設定する等のアクセス制御のために必要な措置を講ずる。

（誤送付等の防止）

第１４条　職員は、保有個人情報を含む電磁的記録又は媒体（注）の誤送信・誤送付、誤

交付、又はウェブサイト等への誤掲載を防止するため、個別の事務・事業において取り扱う個人情報の秘匿性等その内容に応じ、複数の職員による確認やチェックリストの活用等の必要な措置を講ずる。

（注）文書の内容だけでなく、付加情報（ＰＤＦファイルの「しおり機能表示」やプロパティ情報等）に個人情報が含まれている場合があることに注意する。

（廃棄等）

第１５条　職員は、保有個人情報等又は保有個人情報等が記録されている媒体（端末及びサーバに内蔵されているものを含む。）が不要となった場合には、保護管理者の指示に従い、当該保有個人情報の復元又は判読が不可能な方法により当該情報の消去又は当該媒体の廃棄を行う。

特に、保有個人情報の消去や保有個人情報が記録されている媒体の廃棄を委託する場合（二以上の段階にわたる委託を含む。）には、必要に応じて職員が消去及び廃棄に立ち会い、又は写真等を付した消去及び廃棄を証明する書類を受け取るなど、委託先において消去及び廃棄が確実に行われていることを確認する。

（保有個人情報等の取扱状況の記録）

第１６条　総括保護管理者は、保有個人情報等の秘匿性等その内容に応じて、台帳を整備して、当該保有個人情報等の利用及び保管等の取扱いの状況について記録する。

（外的環境の把握）

第１７条　保有個人情報が、外国（※）において取り扱われる場合、当該外国の個人情報の保護に関する制度等を把握した上で、保有個人情報の安全管理のために必要かつ適切な措置を講じなければならない。

（※）近年、行政機関等においても民間事業者が提供するクラウドサービスを利用する場合があり得るところであり、こうした場合においてはクラウドサービス提供事業者が所在する外国及び個人データが保存されるサーバが所在する外国が該当する。

第５章　情報システムにおける安全の確保等

（アクセス制御）

第１８条　保護管理者は、保有個人情報等（情報システムで取り扱うものに限る。以下第５章（第２９条を除く。）において同じ。）の秘匿性等その内容に応じて、指紋認証を使用して権限を識別する機能を設定する等のアクセス制御のために必要な措置を講ずる（注）。

（注）アクセス制御の内容は、第１０条第１項により設定した必要最小限のアクセス制限を具体化するものである必要がある。

（アクセス記録）

第１９条　総括保護管理者は、保有個人情報等の秘匿性等その内容に応じて、当該保有個

人情報等へのアクセス状況を記録し、その記録（以下「アクセス記録」という。）を一定の期間保存し、及びアクセス記録を定期的に分析するために必要な措置を講ずる。

２　保護管理者は、アクセス記録の改ざん、窃取又は不正な消去の防止のために必要な措置を講ずる。

（アクセス状況の監視）

第２０条　総括保護管理者は、保有個人情報等の秘匿性等その内容及びその量に応じて、当該保有個人情報等への不適切なアクセスの監視のため、保有個人情報等を含むか又は含むおそれがある一定量以上の情報が情報システムからダウンロードされた場合に警告表示がなされる機能の設定、当該設定の定期的確認等の必要な措置を講ずる。

（管理者権限の設定）

第２１条　総括保護管理者は、保有個人情報等の秘匿性等その内容に応じて、情報システムの管理者権限の特権を不正に窃取された際の被害の最小化及び内部からの不正操作等の防止のため、当該特権を最小限とする等の必要な措置を講ずる。

（外部からの不正アクセスの防止）

第２２条　総括保護管理者は、保有個人情報等を取り扱う情報システムへの外部からの不正アクセスを防止するため、ファイアウォールの設定による経路制御等の必要な措置を講ずる。

（不正プログラムによる漏えい等の防止）

第２３条　総括保護管理者は、不正プログラムによる保有個人情報等の漏えい、滅失又はき損（以下「漏えい等」という。）の防止のため、ソフトウェアに関する公開された脆弱性の解消、把握された不正プログラムの感染防止等に必要な措置（導入したソフトウェアを常に最新の状態に保つことを含む。）を講ずる。

（情報システムにおける保有個人情報等の処理）

第２４条　職員は、保有個人情報等について、一時的に加工等の処理を行うため複製等を行う場合には、その対象を必要最小限に限り、処理終了後は不要となった情報を速やかに消去する。保護管理者は、当該保有個人情報等の秘匿性等その内容に応じて、随時、消去等の実施状況を重点的に確認する。

（暗号化）

第２５条　総括保護管理者は、保有個人情報等の秘匿性等その内容に応じて必要と認める場合には、その暗号化のために必要な措置を講ずる。

２　職員（注）は、これを踏まえ、その処理する保有個人情報等について、当該保有個人情報等の秘匿性等その内容に応じて、適切に暗号化を行う。

（注）職員が行う暗号化には、適切なパスワードの選択、その漏えい防止の措置等が含まれる。

（記録機能を有する機器・媒体の接続制限）

第２６条　保護管理者は、保有個人情報等の秘匿性等その内容に応じて、当該保有個人情報等の漏えい等の防止のため、スマートフォン、ＵＳＢメモリ等の記録機能を有する機器・媒体の情報システム端末等への接続の制限（当該機器の更新への対応を含む。）等の必要な措置を講ずる。

（端末の限定）

第２７条　総括保護管理者は、保有個人情報等の秘匿性等その内容に応じて、その処理を行う端末を限定するために必要な措置を講ずる。

（端末の盗難防止等）

第２８条　総括保護管理者は、端末の盗難又は紛失の防止のため、執務室の施錠等の必要な措置を講ずる。

２　職員は、総括保護管理者が必要があると認めるときを除き、端末を外部へ持ち出し、又は外部から持ち込んではならない。

（第三者の閲覧防止）

第２９条　職員は、端末の使用に当たっては、保有個人情報等が第三者に閲覧されることがないよう、使用状況に応じて情報システムからログオフを行うことを徹底する等の必要な措置を講ずる。

（バックアップ）

第３０条　保護管理者は、保有個人情報等の重要度に応じて必要と認める場合には、バックアップを作成し、分散保管するために必要な措置を講ずる。

（情報システム設計書等の管理）

第３１条　総括保護管理者は、保有個人情報等に係る情報システムの設計書、構成図等の文書について外部に知られることがないよう、その保管、複製、廃棄等について必要な措置を講ずる。

（入力情報の照合等）

第３２条　保護担当者は、情報システムで取り扱う保有個人情報等の重要度に応じ、必要と認める場合は、入力原票と入力内容との照合、処理前後の当該保有個人情報等の内容の確認、既存の保有個人情報等との照合等を行う。

第６章　情報システム室等の安全管理

（入退管理）

第３３条　総括保護管理者は、保有個人情報等を取り扱う基幹的なサーバ等の機器を設置

する室その他の区域（以下「情報システム室等」という。）に立ち入る権限を有する者を定めるとともに、用件の確認、入退の記録、部外者についての識別化、部外者が立ち入る場合の職員の立会い又は監視設備による監視、外部電磁的記録媒体等の持込み、利用及び持ち出しの制限又は検査等の措置を講ずる。また、保有個人情報等を記録する媒体を保管するための施設を設けている場合においても、必要があると認めるときは、同様の措置を講ずる。

２　保護管理者は、必要があると認めるときは、情報システム室等の出入口の特定化による入退の管理の容易化、所在表示の制限等の措置を講ずる。

３　総括保護管理者は、情報システム室等及び保管施設の入退の管理について、必要があると認めるときは、立入りに係る認証機能を設定し、及びパスワード等の管理に関する定めの整備（その定期又は随時の見直しを含む。）、パスワード等の読取防止等を行うために必要な措置を講ずる。

（情報システム室等の管理）

第３４条　総括保護管理者は、外部からの不正な侵入に備え、情報システム室等に施錠装置、警報装置、監視設備の設置等の措置を講ずる。

２　総括保護管理者は、災害等に備え、情報システム室等に、耐震、防火、防煙、防水等の必要な措置を講ずるとともに、サーバ等の機器の予備電源の確保、配線の損傷防止等の措置を講ずる。

第７章　保有個人情報等の提供及び業務の委託等

（保有個人情報の提供）

第３５条　総括保護管理者は、法第６９条第２項第３号及び第４号の規定に基づき行政機関等以外の者に保有個人情報を提供する場合には、原則として、提供先における利用目的、利用する業務の根拠法令、利用する記録範囲及び記録項目、利用形態等について書面を取り交わす。

２　総括保護管理者は、法第６９条第２項第３号及び第４号の規定に基づき行政機関等以外の者に保有個人情報を提供する場合には、安全確保の措置を要求するとともに、必要があると認めるときは、提供前又は随時に実地の調査等を行い、措置状況を確認してその結果を記録するとともに、改善要求等の措置を講ずる。

３　総括保護管理者は、法第６９条第２項第３号の規定に基づき行政機関等に保有個人情報を提供する場合において、必要があると認めるときは、第１項及び第２項に規定する措置を講ずる。

（匿名加工情報等の提供）

第３６条　保護管理者は、法第１０９条第２項の規定により、法令に基づく場合を除き、利用目的以外の目的のために匿名加工情報及び削除情報（保有個人情報に該当するものに限る。）を自ら利用し、又は提供してはならない。

２　保護管理者は、法第１０９条第１項及び第１１５条の規定（第１１８条の規定により

第１１５条の規定を準用する場合を含む。）により、匿名加工情報の利用に関する契約を締結した者（以下「契約相手方」という。）から法第１１２条第２項第７号の規定に基づき当該契約相手方が講じた非識別加工情報の適切な管理に支障を及ぼすおそれがある旨の報告を受けたときは、直ちに総括保護管理者に報告するとともに、当該契約相手方がその是正のために講じた措置を確認しなければならない。

（業務の委託等）

第３７条　総括保護管理者は、保有個人情報等の取扱いに係る業務又は作成に係る業務を外部に委託する場合には、個人情報及び匿名加工情報等の適切な管理を行う能力を有しない者を選定することがないよう、必要な措置を講ずる。また、契約書に、次に掲げる事項を明記するとともに、委託先における責任者及び業務従事者の管理及び実施体制、個人情報及び匿名加工情報等の管理の状況についての検査に関する事項等の必要な事項について書面で確認する。

一　個人情報及び匿名加工情報等に関する秘密保持、目的外利用の禁止等の義務

二　再委託（再委託先が委託先の子会社（会社法（平成１７年法律第８６号）第２条第３号に規定する子会社をいう。）である場合も含む。本号及び第３項において同じ。）の制限又は事前承認等再委託に係る条件に関する事項

三　個人情報及び匿名加工情報等の複製等の制限に関する事項

四　個人情報の安全管理措置に関する事項

五　個人情報及び匿名加工情報等の漏えい等の事案の発生時における対応に関する事項

六　委託終了時における個人情報及び匿名加工情報等の消去及び媒体の返却に関する事項

七　違反した場合における契約解除、損害賠償責任その他必要な事項

八　契約内容の遵守状況についての定期的報告に関する事項及び委託先における委託された個人情報の取扱状況を把握するための監査等に関する事項（再委託先の監査等に関する事項を含む。）

２　保有個人情報の取扱いに係る業務を外部に委託する場合には、取扱いを委託する個人情報の範囲は、委託する業務内容に照らして必要最小限でなければならない。

３　保有個人情報等の取扱いに係る業務を外部に委託する場合には、委託する業務に係る保有個人情報等の秘匿性等その内容やその量等に応じて、委託先における管理体制及び実施体制や個人情報及び非識別加工情報等の管理の状況について、少なくとも年１回以上、原則として実地検査により確認する。

４　委託先において、保有個人情報等の取扱いに係る業務又は作成に係る業務が再委託される場合には、委託先に第１項の措置を講じさせるとともに、再委託される業務に係る保有個人情報等の秘匿性等その内容に応じて、委託先を通じて又は委託元自らが第３項の措置を実施する。保有個人情報等の取扱いに係る業務又は作成に係る業務について再委託先が再々委託を行う場合以降も同様とする。

５　保有個人情報等の取扱いに係る業務又は作成に係る業務を派遣労働者によって行わせる場合には、労働者派遣契約書に秘密保持義務等個人情報及び非識別加工情報等の取扱いに関する事項を明記する。

６　保有個人情報等を提供又は業務委託する場合には、漏えい等による被害発生のリスクを低減する観点から、提供先の利用目的、委託する業務の内容、保有個人情報等の秘匿性等その内容などを考慮し、必要に応じ、特定の個人を識別することができる記載の全部又は一部を削除し、又は別の記号等に置き換える等の措置を講ずる。

（サイバーセキュリティに関する対策の基準等）

第３８条　個人情報を取り扱い、又は情報システムを構築し、若しくは利用するに当たっては、サイバーセキュリティ基本法第２６条第１項第２号に掲げられたサイバーセキュリティに関する対策の基準等（例；政府機関等のサイバーセキュリティ対策のための統一基準群）を参考として、取り扱う保有個人情報の性質等に照らして適正なサイバーセキュリティの水準を確保する。

第８章　安全確保上の問題への対応

（事案の報告及び再発防止措置）

第３９条　保有個人情報等の漏えい等安全確保の上で問題となる事案又は問題となる事案の発生のおそれを認識した場合に、その事案等を認識した職員は、直ちに当該保有個人情報等を管理する保護管理者に報告する（注）。

（注）職員は、当該事案の発生（事案発生のおそれを含む。）を認識した場合、時間を要する事実確認を行う前にまず保護管理者に報告する。

２　保護管理者は、被害の拡大防止又は復旧等のために必要な措置を速やかに講ずる。ただし、外部からの不正アクセスや不正プログラムの感染が疑われる当該端末等のＬＡＮケーブルを抜くなど、被害拡大防止のため直ちに行い得る措置については、直ちに行う（職員に行わせることを含む。）ものとする。

３　保護管理者は、事案の発生した経緯、被害状況等を調査し、直ちに総括保護管理者に当該事案の内容等について報告する。

４　総括保護管理者は、特に重大と認める事案が発生した場合には、当該事案の内容、経緯、被害状況等を社長に速やかに報告する。

５　総括保護管理者は、事案の内容等に応じて、当該事案の内容、経緯、被害状況等を経済産業省に速やかに情報提供を行う。

６　総括保護管理者及び保護管理者は、事案の発生した原因を分析し、再発防止のために必要な措置を講ずる。

（法に基づく報告及び通知）

第４０条 漏えい等が生じた場合であって法第６８条第１項の規定による個人情報保護委員会への報告及び同条第２項の規定による本人への通知を要する場合には、前条第１項から第５項までと並行して、速やかに所定の手続を行うとともに、個人情報保護委員会による事案の把握等に協力する。

（参考：施行規則第４３条第１項関連部分）

(1) 要配慮個人情報が含まれる保有個人情報（高度な暗号化その他の個人の権利利益を

保護するために必要な措置を講じたものを除く。以下この条において同じ。）の漏えい、滅失若しくは毀損（以下この条において「漏えい等」という。）が発生し、又は発生したおそれがある事態

(2) 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保有個人情報の漏えい等が発生し、又は発生したおそれがある事態

(3) 不正の目的をもって行われたおそれがある当該行政機関の長等の属する行政機関等に対する行為による保有個人情報（当該行政機関の長等の属する行政機関等が取得し、又は取得しようとしている個人情報であって、保有個人情報として取り扱われることが予定されているものを含む。）の漏えい等が発生し、又は発生したおそれがある事態

(4) 保有個人情報に係る本人の数が 100 人を超える漏えい等が発生し、又は発生したおそれがある事態

（公表等）

第４１条　法第６８条第１項の規定による委員会への報告及び同条第２項の規定による本人への通知を要しない場合であっても、事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る保有個人情報等の本人への対応等の措置を講ずる。

国民の不安を招きかねない事案（例えば、公表を行う漏えい等が発生したとき、個人情報保護に係る内部規程に対する違反があったとき、委託先において個人情報の適切な管理に関する契約条項等に対する違反があったとき等）については、当該事案の内容、経緯、被害状況等について、速やかに委員会へ情報提供を行う。

第９章　監査及び点検の実施

（監査）

第４２条　監査責任者は、保有個人情報等の適切な管理を検証するため、第２章から第８章に規定する措置の状況を含む会社における保有個人情報等の管理の状況について、定期に及び必要に応じ随時に監査（外部監査を含む。以下同じ。）（注）を行い、その結果を社長及び総括保護管理者に報告する。

（注）保有個人情報等の秘匿性等その内容及びその量に応じて、実地監査を含めた重点的な監査として行うものとする。

（点検）

第４３条　保護管理者は、各グループ等における保有個人情報等の記録媒体、処理経路、保管方法等について、定期に及び必要に応じ随時に点検を行い、必要があると認めるときは、その結果を社長及び総括保護管理者に報告する。

（評価及び見直し）

第４４条　総括保護管理者、保護管理者等は、監査又は点検の結果等を踏まえ、実効性等の観点から保有個人情報等の適切な管理のための措置について評価し、必要があると認めるときは、その見直し等の措置を講ずる。

第１０章　その他

（規則の改正）

第４５条　この規則は、取締役会の決議を経て、随時改正することができる。ただし、組織名変更等による改正については、取締役会の決議を要しない。

（主管部）

第４６条　この規則の主管部署は、総務部総務・広報グループとする。

附　則

この規則は、２０１７年４月１日から施行する。

附　則

この規則は、２０１７年６月１３日から施行する。

附　則

この規則は、２０１９年２月１日から施行する。

附　則

この規則は、２０２１年４月１日から施行する。

附　則

この規則は、２０２２年４月１日から施行する。

附　則

この規則は、２０２４年４月１日から施行する。