# 個人情報セキュリティ実施基準

## 第１章　総則

（目的）
第１条　この基準は、「個人情報取扱規程」第 13 条第 2 項及び「資料の収集、管理及び閲覧規程」第 12 条に基づき、（株）猿橋鑑定システム（以下「弊社」という。）が取り扱う情報及び情報システムの適切な運用を図るために、役員、顧問、相談役並びに職員及び嘱託（以下「従業者」という。）が最低限遵守すべき事項を明らかにし、もって情報の漏えい、き損、滅失等の事故の防止、情報システムの適切な運用、及び万が一の事故の場合の損害を最低限にすることを目的とする。

（他の規程等との関係）
第２条　個人情報の取扱いについては、「個人情報取扱規程」、並びに保存文書については、「保存文書規程」が本基準に優先するものとする。

## 第２章　情報の指定・解除

（情報の指定・解除）
第3条　　弊社が保有する情報のうち、漏えい等が発生した場合、弊社に重大な損害を及ぼすおそれが高い情報を秘密情報として指定する。
２　秘密情報の指定は、各業務の部門責任者がこれを認定し所長の承認を得て決定する。
３　秘密情報が記載された紙の文書を秘密文書という。
４　秘密情報を指定した者又は所長は、その情報が秘密でなくなった場合には、所長の承認を得て秘密情報であることを解除することができる。

（秘密であることの明示）
第４条　秘密情報には、秘密であることを表示する。
２　秘密情報が解除された場合は、秘密の表示を消去又は取り消し線で消す。

## 第３章　秘密情報の取扱い

（保管）
第 5 条　秘密文書を業務時間外に保管する場合は、キャビネット等に保管し、施錠する。
２　前項については、フロッピーディスク、CD-ROM その他の携帯することが可能な電子媒体（以下、「携帯可能媒体」という。）に保存する場合も同じものとする。
３　コンピュータ上に保管する場合は、最低限、ID とパスワードにより認証されるコンピュータ上に保管する。

（作業上の注意点）
第 6 条　業務時間内に一時的に離席する場合、秘密文書を机上等に放置せず、机の引き出しその他目につかない場所に一時的に保管する。
２　コンピュータ等の画面に秘密情報が表示されている場合、スクリーンセーバー等を起動し、秘密情報が画面に表示された状態のまま離席しない。

（持ち出しの制限）
第 7 条　秘密文書、秘密情報を保管した携帯可能媒体又はコンピュータを事務所外に持ち出すときは、所属する部門責任者又は所長の承認を得る。

（郵送、FAX、電子メールの制限）
第 8 条　秘密文書又は秘密情報を保管した携帯可能媒体を郵送する場合は、事前に所属する部門責任者又は所長の承認を得た上で、書留等、受取が確実に行われたことがわかる通信手段により行う。
２　秘密文書を FAX で送信してはならない。
３　電子メールで秘密情報を送信する場合は、事前に所属する部門責任者または所長の承認を得た上で、暗号化又はパスワードによる保護をし、送信する。

（印刷・複写・複製の制限）
第 9 条　秘密情報を印刷、複写、複製する場合は、所属する部門責任者または所長の承認を得る。

（廃棄・返却）
第 10 条　秘密情報が保管された保存文書の廃棄は、別に定める保存文書規程に指定する方法による。
２　携帯可能媒体を廃棄する場合は、専用ソフトによる上書消去、携帯可能媒体の細断、焼却、溶解等復元できない方法による。
３　コンピュータを廃棄又はリース会社へ返却する場合は、廃棄又は返却する前に専用ソフトによる上書消去をする。この作業は、守秘義務契約を結んだ第三者に委託することが

できる。

## 第４章　認証及びアクセス管理

（ID の登録・休止・廃止）
第 11 条　弊社のコンピュータを利用する場合、所長又は部門責任者は事前に利用者に対し ID を付与する。
２　ID を付与された者は、ID を適切に管理する。
３　ID を付与された者が長期休暇、休職等一ヶ月以上弊社のコンピュータを利用することがないと想定される場合、速やかに ID の利用を停止する。
４　ID を付与された者が退会等、弊社のコンピュータを利用する必要がなくなった場合、速やかに ID の利用を停止する。

（パスワード等による認証）
第 12 条　弊社のコンピュータを利用する者は、パスワード等により認証する。

（パスワードの条件）
第 13 条　パスワードは 8 文字以上とする。
２　パスワードは、英数字、数字及び特殊文字の組み合わせとする。
３　パスワードは 3 ヶ月に一度以上変更する。

（利用者のパスワード等の管理）
第 14 条　パスワードにより本人を認証する場合、コンピュータの利用者は、他人に推測されにくいパスワードをつけ、他人に漏れないように適切に管理する。
２　ID カード等のパスワード以外の認証手段を用いる場合、ID カード等を付与された者は、ID カード等を紛失しないように適切に管理すること。紛失した場合は、総務部門責任者又は所長に速やかに連絡する。

（アクセス権の管理）
第 15 条　秘密情報をコンピュータに保存する場合、秘密情報を閲覧する権限がない者が閲覧できない状態となるようにアクセス権を設定する。
２　業務が変更になる等、アクセス権を付与されていた者にアクセス権を付与する必要がなくなった場合は、速やかにアクセス権を削除する。

## 第５章　コンピュータの適正利用

（弊社のコンピュータの利用の前提）
第 16 条　弊社のコンピュータを利用するに当たり、自らのコンピュータ利用状況が記録され、確認される可能性があることに同意した者のみに、弊社のコンピュータの利用を認める。

（私的利用の禁止）
第 17 条　弊社のコンピュータ利用者は、弊社業務の目的のみにコンピュータを利用し、私的な利用をしてはならない。
２　弊社のコンピュータ利用者は、弊社業務の目的のみに電子メールを利用し、私的な利用をしてはならない。
３　弊社のコンピュータ利用者は、弊社業務の目的のみに、インターネットのホームページを閲覧し、私的な利用をしてはならない。
４　総務部門責任者又は所長は、必要に応じ、不必要なインターネットホームページへのアクセスを制限するソフトを導入することができる。
５　総務部門責任者又は所長は、必要に応じ、弊社コンピュータ利用者のコンピュータ利用状況を確認することができる。
６　総務部門責任者又は所長は、上記の確認の結果、第 1 項から第 3 項に違反している可能性があると判断した場合は、本人から事情を聴取し、違反があればコンピュータの利用を停止することができる。

（ソフトウェアライセンスの管理）
第 18 条　総務部門責任者は、弊社のコンピュータに標準的にインストールするソフトウェアを定め、ライセンスを適切に管理しなければならない。

（ソフトウェアの無断インストールの禁止）
第 19 条　弊社のコンピュータ利用者は、弊社が認めたソフトウェアのみをインストールして利用し、その他のソフトウェアを無断でインストールしてはならない。
２　弊社のコンピュータ利用者は、業務上の理由によりソフトウェアをインストールする必要が生じた場合、総務部門責任者又は所長に承認を得て、当該ソフトウェアをインストールしなければならない。
３　総務部門責任者は、無断でインストールしたソフトウェアを発見した場合、弊社のコンピュータ利用者に対し、そのソフトウェアを消去することを指示しなければならない。

（コンピュータウィルス対策ソフトの導入）

第 20 条　総務部門責任者は、弊社で利用する全てのコンピュータにコンピュータウィルス対策ソフトをインストールしなければならない。
２　弊社のコンピュータ利用者は、コンピュータウィルス対策ソフトが起動している状態でコンピュータを利用しなければならない。
３　コンピュータウィルスのパターンファイル又はソフトウェアは、常に最新に保たれるように設定されるものとする。

（システム上の脆弱性の管理）
第 21 条　総務部門責任者は、弊社で利用するコンピュータについて、オペレーティングシステムのバグその他のシステム上の脆弱性の存在を知った場合、セキュリティパッチソフトの導入その他の対策を検討しなければならない。
第 22 条　弊社のコンピュータ利用者は、総務部門責任者の指示によりセキュリティパッチソフトの導入が指示された場合、速やかに導入を行わなければならない。

## 第 6 章　ネットワーク及びサーバの管理

（管理者の設置と役割）
第 23 条　弊社のネットワーク機器、サーバ及びクライアについて、システム管理者を設置する。
２　システム管理者は、ネットワーク機器、サーバについての運用管理を行う。

（サーバの管理）
第 24 条　弊社のサーバのシステム管理者は、サーバに対するアクセス制御方針を定め、外部、内部からの無権限アクセスを防止する。

（ネットワークの管理）
第 25 条　弊社のネットワーク機器のシステム管理者は弊社のネットワークと外部のネットワークの接続についてのアクセス制御方針を定め、外部からの無権限アクセスを防止する。

（アクセスログの採取と検査）
第 26 条　ネットワーク機器及びサーバのシステム管理者は、アクセスログ採取及び検査についての方針を定め、アクセスログの採取及び検査を行う。

（個人情報を用いたテストの禁止）
第 27 条　システム開発に関連し、システム開発テストを実施する場合、個人情報を用いて

はならない。

（データのバックアップおよびリカバリーテストの実施）
第 28 条　システム管理者は、サーバに保管されているデータのバックアップ及びリカバリー方針を定めなければならない。
２　システム管理者は、サーバのデータバックアップを、方針に従い定期的に実施しなければならない。
３　システム管理者は、方針に従い定期的にリカバリーテストを実施しなければならない。
４　システム管理者は、リカバリーテストの結果を踏まえて、バックアップ及びリカバリー方針を変更しなければならない。

## 第７章　物理的・環境的対策

（セキュリティ区画の設定）
第 29 条　弊社の施設を、外部者が入室できる区画（以下、「レベル１区画」という。）と、事前に承認された者が入室できる区画（以下、「レベル２区画」という。）、レベル２の区画にあり、特定の権限を与えられた者だけがアクセス（入室を含む）できる区画（以下、「レベル３区画」という。）に区分する。

（入室管理）
第 30 条　外部者がレベル１区画に入室する場合は、弊社の役職員が必ず同席する。
２　外部者がレベル２区画に入室する場合は、弊社の役職員が必ず同伴し、役職員の指示に従い行動してもらうように依頼する。
３　外部者がレベル３区画にアクセスする場合は、レベル３区画にアクセスすることができる役職員が必ず同伴し、当該役職員の指示に従い行動してもらうように依頼する。

（キャビネット、コンピュータ等の設置）
第 31 条　秘密文書を保管するキャビネットは、レベル２区画に設置する。
２　サーバ及びクライアントコンピュータは、レベル２区画に設置する。
３　ネットワーク機器は、レベル２区画に設置することを原則とする。
４　レベル１区画に設置するネットワーク機器は盗難又は外部者の事故等による破損を防止するために、施錠管理その他の適切な物理的対策を実施する。

## 第８章　教育・訓練

（教育・訓練）
第 32 条　情報セキュリティに関する教育を定期的に実施する。
２　技術的対策が確実に実施できるように、必要に応じ、訓練を実施する。

（教育・訓練の記録）
第 33 条　情報セキュリティに関する教育・訓練を実施した記録を保持する。

## 第９章　委託管理

（委託先の選定）
第 34 条　弊社の業務を外部に委託する場合、委託先を選定するための条件として、委託先の情報管理についても考慮する。

（契約書の締結）
第 35 条　弊社の業務を外部に委託する場合、委託先と業務委託契約を締結し、両者の責任の範囲及び実施する業務を明確にする。
２　契約書又はその覚書に次条の委託先に要求すべき情報セキュリティに関する事項を含めるように努める。

（委託先に要求すべき情報セキュリティに関する事項）
第 36 条　委託先に要求すべき情報セキュリティに関する事項として、以下の事項を要求する。
１）弊社で要求している情報セキュリティに関する事項の遵守。
２）委託先の業務の遂行における情報セキュリティ関連事項について弊社に対する定期的な報告。
３）弊社の役職員又は弊社が委託した者等が、委託先の業務の遂行における情報セキュリティ関連事項の遵守状況を検査又は監査による確認。

（委託先からの報告）
第 37 条　業務委託を行った部門責任者は、業務の遂行におけるセキュリティ関連事項について、委託先から定期的な報告をうけなければならない。
２　必要に応じ、委託先との間で定期的な報告会を開催するよう努めることとする。

（委託先への確認）
第 38 条　業務委託を行った部門責任者は、委託先の情報セキュリティ関連事項の契約事項の遵守状況を検査又は監査により年に１度以上確認する。
２　前項の確認は、外部の専門家に委託することができる。

## 第１０章　事件・事故への対応

（事件・事故への対応）
第 39 条　ネットワーク機器及びサーバのシステム管理者は、アクセスログの検査の結果、不正なアクセスを発見又はそのおそれを発見した者は、総務部門責任者及び契約しているシステム運用委託先に連絡しなければならない。
２　前項の場合、総務部門責任者は、システム管理者及びシステム運用委託先と相談し、対応を決めなければならない。
３　個人情報の漏えい事故の場合は、別途定める事故に関する規定に従い対応する。

## 第１１章　情報セキュリティ実施状況の確認

（監査人の選任）
第 40 条　所長は、情報セキュリティ監査を実施する者を選任する。
２　情報セキュリティ監査を実施する者を外部の専門家に委託することができる。

（監査の実施と報告）
第 41 条　情報セキュリティ監査を実施する者は、情報セキュリティに関する規程等が遵守されていることを年に１度以上、監査により確認しなければならない。
２　上記の監査は、第 38 条に規定する委託先への検査又は監査による確認を含む。

（監査の報告）
第 42 条　所長は、情報セキュリティ監査の報告を受ける。
２　所長は、監査の結果、重大な問題が発見された場合は、役員会に報告しなければならない。

（監査結果に基づく改善）
第 43 条　役員会は、必要に応じて情報セキュリティ監査の結果に基づく改善を指示しなければならない。