システム利用規程

1.0版

システム利用規程

システム利用規程

１　趣旨

本規程は、システムやネットワーク利用時における可用性・機密性・完全性を確保し、発生し得る各種問題を未然に防ぐことを目的とする。

２　対象者

ＰＣ、システム、ネットワークを利用するすべての従業員。

３　対象システム

当社より支給・貸与するＰＣ、および利用するシステムとネットワーク。

４　遵守事項

４．１　　ＰＣにおけるセキュリティ対策

４．１．１　ＰＣの利用

(A.9.3.1)

当社の業務に利用するＰＣは、以下のものでなければならない。

（１）当社が支給・貸与するＰＣのみとする。

４．１．２　ＰＣで使用できるソフトウェア

(A.12.6.1、A.12.6.2)

当社が支給・貸与するＰＣに導入するソフトウェアは、以下を遵守しなければならない。

（１）ＰＣの利用者は、システム管理者が初期導入したソフトウェアのみ使用すること。

（２）規定されたソフトウェア以外で、業務上やむを得ず使用する必要がある場合、ＰＣの利用者は、情報セキュリティ担当者に申請し、許可を得なければならない。

（３）ＰＣの利用者は、情報セキュリティ担当者が提供するソフトウェア情報をもとに最新の修正プログラム等を適用しなければならない。

４．１．３　ＰＣのパスワード管理

(A.9.4.2、A.9.4.3)

当社が支給・貸与するＰＣの盗難、紛失に備え、以下を遵守しなければならない。

（１）ＰＣの利用者は、支給・貸与を受けた場合、ＰＣログオンの初期パスワードを直ちに変更しなければならない。

（２）ＰＣの利用者は、システム管理者の設定したパスワードポリシーに従い、パスワードを設定し、定期的に変更しなければならない。

（３）ＰＣの利用者は、第三者が容易に推測できないパスワードを選択すること。

４．１．４　ＰＣでの情報の取り扱い

(A.8.2.3、A8.3.1、A.9.3.1、A.10.1.1)

当社が支給・貸与するＰＣでの情報の取扱いは、以下を遵守しなければならない。

（１）ＰＣの利用者は、ＰＣで機密情報を取り扱う場合には、機密情報を取り扱う許可を情報の管理責任者に申請し、許可を得なければならない。許可を得た機密情報は、万一の漏洩に備え、暗号化等の対策を実施しなければならない。

（３）ＰＣの利用者は、情報の管理責任者の許可無く、機密情報を外部媒体に保管してはならない。

（４）ＰＣの利用者は、機密情報取り扱い後には、不必要となった機密情報を直ちにＰＣと外部媒体から削除しなければならない。

４．１．５　ＰＣの使用場所

(A.6.2.2、A.11.1.5)

当社が支給・貸与するＰＣの利用は、利用を許可した以下の場所のみとする。

（１）当社の事務フロア、会議室。

（２）社外では不特定の他人の目にふれない場所。ただし、覗き見防止フィルターにより覗き見が困難な対策を施すＰＣは除く。

４．１．６　ＰＣの利用者の変更

(A.9.2.1)

当社が支給・貸与するＰＣの利用者を変更する場合は、以下を遵守しなければならない。

（１）ＰＣの利用者は、ＰＣの利用者を無断で変更してはならない。

（２）ＰＣの利用者を変更する場合には、情報セキュリティ担当者に返却しなければならない。

４．１．７　ＰＣの利用上の注意事項

(A.6.2.2、A.7.2.2、A.11.2.9、A.12.4.1、A.16.1.2)

当社が支給・貸与するＰＣの利用にあたり、以下を注意する。

（１）ＰＣの利用者は、社外にＰＣを持ち出す場合、盗難・窃盗に注意し取り扱わなければならない。

（２）ＰＣの利用者は、社外でＰＣを利用する場合、情報の盗み見に注意しなければ

ならない。

（３）ＰＣの利用者は、利用環境を整理整頓すると共に、デスクトップを整理し、クリアスクリーンを心がけなければならない。

（４）ＰＣの利用者は、定期的（１年に一回）に、ＰＣ利用に伴う教育を受講しなければならない。

（５）ＰＣの利用者は、ＰＣ利用に伴う、ＰＣ及びそれに付随する機器の紛失・盗難、また情報漏えい等セキュリティインシデントが発生した場合、『セキュリティインシデント報告・対応規程』に従い報告・対応しなければならない。

（６）ＰＣの利用状況は、情報セキュリティ担当者によってモニタリングされていることに留意していなければならない。

４．２　ＰＣや媒体の取り扱いに関するセキュリティ対策

４．２．１　使用機器に関する遵守事項

(A.8.3.1、A.9.3.1)

（１）利用者は、情報システム部が指定したＰＣや媒体を利用しなければならない。

（２）ＰＣや媒体は、盗難に遭わない様に、また紛失しない様に、利用者が管理を行わなければならない。

４．２．２　ＰＣの修理

(A.8.2.3、A.11.2.5)

（１）ＰＣの修理を依頼する場合は、申請書を提出し、情報セキュリティ担当者を通して修理を依頼しなければならない。

（２）ＰＣ等の修理を依頼する利用者は、機密性の高い情報が保管されていないことを確認した上で修理を依頼しなければならない。

故障の状況により、保管されている情報の確認や保護が実施できない場合には、利用者は、情報セキュリティ担当者から指定された方法にて修理を依頼しなければならない。

４．２．３　媒体の保管

(A.10.1.1、A.11.1.1)

（１）利用者が、機密性の高い情報を媒体に保存する時は、保管された情報に権限のない人がアクセスできないよう、データまたは媒体に対して暗号化を行い、媒体を鍵のかかる場所に保管し、鍵を管理しなければならない。

４．２．４　媒体の移動

(A.8.3.3、A.11.2.5)

（１）利用者は、機密性の高い情報を保管している媒体を、その情報の管理責任者の許可なく社外へ持ち出してはならない。

（２）利用者は、機密性の高い情報を保管している媒体を郵送や宅配便等で送付する場合、セキュリティが保たれた郵送や宅配便等を利用すること。

４．２．５　ＰＣと媒体の再利用および廃棄

(A.8.3.2)

（１）ＰＣまたは媒体の再利用および廃棄を行う場合は、情報セキュリティ担当者に廃棄申請を提出し、指定された方法にて再利用および廃棄処理を行う。

４．３　マルウェア対策

４．３．１　マルウェアやサイバー攻撃に関する教育の受講

(A.7.1.2、A.7.2.2)

当社より支給・貸与するＰＣ、およびシステム、ネットワークの利用にあたっては、以下の教育を受講しなければならない。

（１）ＰＣの利用者は、入社時には、マルウェアやサイバー攻撃に関する教育を受講しなければならない。

（２）ＰＣの利用者は、定期的（1 年に一回）に、マルウェアやサイバー攻撃に関する教育を受講しなければならない。

４．３．２　マルウェア対策ソフトの利用

(A.12.2.1)

当社より支給・貸与するＰＣは、マルウェア対策ソフトにより以下の対策をしなければならない。

（１）ＰＣの利用者は、システム管理者が設定したマルウェア対策ソフトの設定を変更してはならない。

（２）ＰＣの利用者は、ドライブ全体に対する定期スキャンを無効化してはならない。また、やむを得ずスキャンを停止した場合は、できるだけ早く定期スキャンを再開しなければならない。

４．３．３　電子メールやインターネット閲覧を介してのマルウェア被害の防止

(A.12.2.1)

電子メールや、インターネット閲覧による被害を招かないため、以下を遵守しなけれ

ばならない。

（１）ＰＣの利用者は、メールの受信にあたっては、メーラやＷｅｂメール上でスパムメールや迷惑メールを分別する機能を有効にしなければならない。

（２）ＰＣの利用者は、送信元不明（特にフリーメール）のメールに添付されたファイルや、実行形式のまま添付されたファイルなど、不審だと疑われるメールの添付ファイルは安易に開いてはならない。また、安易にＵＲＬリンクをクリックしてはならない。不審だと疑われるメールを受信した場合は、即座に情報セキュリティ担当者に報告しなければならない。

（３）ＰＣの利用者は、ファイルを添付してメールを送信する場合、当該ファイルのマルウェア感染が無いことをマルウェア対策ソフトにて確認後、メールを送信しなければならない。

（４）インターネット閲覧によるマルウェア感染を防ぐ為に、ＰＣの利用者は、業務上関係のないサイトの閲覧をしてはならない。

４．３．４　マルウェアに感染した場合、または感染したと疑われる場合

(A.16.1.2、A.16.1.5、A.16.1.7)

マルウェアに感染、もしくは感染が疑われる場合は、利用者は以下を遵守しなければならない。

（１）ＰＣの利用者は、以下の症状などが見受けられた場合には、情報セキュリティ担当者に報告し、対応方法の指示を受け、対応しなければならない。

・マルウェア付のメールが送られたとの連絡が取引先などからあった。

・メールの添付ファイルを開いたが、何も表示されなかった。

・インターネットのサイトを閲覧中に表示される広告などの表示を消すことができなくなった。

（２）ＰＣの利用者は、有線ＬＡＮ接続のＰＣはネットワークケーブルを外し、無線ＬＡＮ接続のＰＣは無線ＬＡＮ機能をＯＦＦにしなければならない。

（３）ＰＣの利用者は、情報セキュリティ担当者の指示に従って、マルウェア駆除をしなければならない。

（４）ＰＣの利用者は、マルウェア被害の影響範囲が社外にまで至っている可能性が認められる場合、その影響について、情報セキュリティ担当者に報告しなければならない。

４．４　電子メール利用におけるセキュリティ対策

４．４．１　電子メールサービス利用端末機器のセキュリティ

(A.9.4.2、A.12.6.2)

（１）電子メールの利用にあたっては、情報システム部が指定した電子メールソフト

ウェアを用いなければならない。また、情報システム部の指示に従い、当該ソフトウェアを最新の状態に保たなければならない。

（２）電子メールの利用者は、電子メールソフトウェアにパスワードを保存してはならない。電子メールソフトウェア起動時にユーザ認証を必要とする設定にしなければならない。

４．４．２　電子メールで送受信される情報の保護

(A.10.1.1、A.13.2.3)

（１）電子メールの利用者は、当社の事業に関わる情報や、顧客・従業員の個人情報などの機密情報をメールにて送受信する場合は、機密情報の内容に応じて暗号化、電子署名などの処置を施さなければならない。

（２）電子メールの利用者は、電子メールの送信にあたっては、送信先のメールアドレスに間違いがないか、確認の上送信しなければならない。

（３）当社のセミナー案内や製品紹介メールなどのように電子メールで同報送信する場合は、送信先メールアドレスが受信者に閲覧できないよう、BCC を利用しなければならない。また、広告メール等の送信にあたっては、法律を遵守しなければならない。

（４）電子メールの利用者は、電子メールを社外の個人的なメールアドレスに転送する場合は、情報セキュリティ担当者に申請をし、許可を得なければならない。

４．４．３　電子メールサービスとネットワーク保護

(A.9.3.1、A.12.2.1、A.13.1.2、A.13.2.2、A.13.2.3)

（１）電子メールの利用者は、業務目的以外に電子メールサービスを利用してはならない。

（２）電子メールの利用者は、スパムメールを受信した場合は、これを転送してはならない。

（３）電子メールの利用者は、社外のメーリングリストに参加する場合は、当該メーリングリストの信頼性、および業務への必要性を充分考慮した上で参加しなければならない。また、参加意義の無くなった場合は、直ちに脱退しなくてはならない。また公序良俗に反する発言をしてはならない。

（４）電子メールの利用者は、電子メールの送信にあたっては、添付するファイルの容量を考慮しなければならない。規定容量以上のファイルを送信せざるを得ない場合は、情報セキュリティ担当者にて指定されたファイル共有サイト・ファイル転送サイトを利用しなければならない。

（５）電子メールの利用者は、その他、無用な電子メールを送受信することにより、ネットワークに負荷をかけてはならない。また、電子メールはテキスト形式で

送信するよう設定しなければならない。

４．５　Ｗｅｂサービス利用におけるセキュリティ対策

４．５．１　Ｗｅｂブラウザ利用端末機器のセキュリティ

(A.9.1.2、A.9.3.1、A.12.6.1)

（１）利用者は、Ｗｅｂブラウザの利用にあたって、情報システム部が指定したＷｅｂブラウザを用いなければならない。また、情報システム部の指示に従い、当該ソフトウェアを最新の状態に保たなければならない。

（２）利用者は、Ｗｅｂブラウザの利用にあたって、情報セキュリティ担当者が指定したＷｅｂブラウザの設定を施さなければならない。

（３）利用者は、社内からインターネットにアクセスするときは、必ず情報セキュリティ担当者が指定するＰｒｏｘｙサーバを使用しなければならない。

４．５．２　Ｗｅｂブラウザの利用

(A.9.1.2、A.9.3.1、A.12.2.1、A.12.6.2、A.18.1.1)

（１）利用者は、社内及びインターネット上のＷｅｂサーバへのアクセスは、業務上必要な場合のみ利用することができる。

（２）利用者は、ＵＲＬリンクをクリックするとき、リンク先のＵＲＬを確認してからクリックしなければならない。この場合、リンク先が、信頼できないＵＲＬである場合は、クリックしてはならない。また、バナー広告についても同様で、業務上必要のないバナー広告はクリックしてはならない。

（３）利用者は、業務上不必要なファイルやソフトウェア、不審なファイルなどをダウンロードしてはならない。

（４）利用者は、署名の無いあるいは信頼できないサイトの ActiveX、Java、JavaScript、VBScript などのコードは実行してはならない。

（５）業務と関連の無い Web メールを利用してメールの送受信を行ってはならない。

（６）利用者は、社内外のＷｅｂサーバに対して、攻撃等不正なアクセスを行ってはならない。また、攻撃や不正なアクセスを目的として社内外のシステムを利用してはならない。

４．５．３　Ｗｅｂサーバの利用

(A.9.3.1、A.13.2.2)

（１）利用者の情報の発信（掲示板、ＳＮＳなどへの書き込み）に関しては、部門長が業務上必要と認めた場合のみ許可される。このとき、情報の正確性を確保し、必要最小限の範囲で発信しなければならない。また、下記に該当する情報の発信は禁止する。また、情報の閲覧に関しても同様とする。

- 著作権、商標、肖像権を侵害するおそれのあるもの
- プライバシーを侵害するおそれのあるもの
- 他者の社会的評価にかかわる問題に関するもの
- 他者の名誉・信用を傷つけるおそれのあるもの
- 会社の信用・品位を傷つけるおそれのあるもの
- 性的な画像や文章に該当するおそれのあるもの
- 不正アクセスを助長するおそれのあるもの
- 差別的なもの
- 虚偽のもの
- 社内の機密情報
- その他公序良俗に反するおそれのあるもの

（２）利用者は、情報セキュリティ担当者の許可なく、インターネット上のサービス、たとえば、ファイル共有サイトやファイル交換サイトを通じて、他社とファイルを送受信するサービスなどを利用してはならない。

４．５．４　アクセス制御されたＷｅｂサイトの閲覧に関して

(A.9.4.2、A.11.1.5)

（１）利用者は、パスワードによってアクセス制御されたＷｅｂサイトの閲覧において、パスワードをＷｅｂブラウザに記憶させる設定を行ってはならない。

（２）利用者は、アクセス制御された社内Ｗｅｂサイトの閲覧時に離席、または閲覧しなくなった場合は必ず、Ｗｅｂブラウザを終了させるか、ＯＳのパスワード付スクリーンロックを実施しなければならない。

４．５．５　Ｗｅｂサイトの閲覧許可

(A.9.1.2)

（１）ＵＲＬフィルタリングにより業務上必要とされるサイトが閲覧できない場合、利用者は、情報セキュリティ担当者に申請し、許可を得た場合のみ、閲覧できるものとする。

４．６　ネットワークの利用

４．６．１　社内ネットワーク及びインターネットの業務目的以外の利用禁止

(A.9.1.2、A.9.3.1、A.9.4.1)

（１）社内ネットワークは、会社の情報資産であり、電子メールやＷｅｂサイトの利用などにおいて、業務目的以外の使用を禁止する。インターネットの利用についても同様である。

（２）情報セキュリティ委員会の許可無く、社内ネットワーク上に、電子メールサー

バや、Ｗｅｂサーバ、ＦＴＰサーバなどを構築してはならない。

（３）他人の利用者ＩＤを用いて、社内ネットワーク及び、社外のネットワーク、インターネット上のサイトへアクセスしてはならない。

（４）利用者は、故意もしくは不注意を問わず、社内ネットワーク及び社外ネットワーク、インターネット上のサーバに対して、許可されたアクセス権限以上のアクセスを行ってはならない。

４．６．２　社内ネットワークで利用可能なサービス

(A.9.3.1、A.9.4.1、A.9.4.2、A.9.4.3、A.10.1.1、A.13.1.2)

（１）業務システム（人事、経営、経理、交通費管理、受発注システム、イントラネットサーバなど）へのアクセスは、許可された利用者以外利用してはならない。

（２）機密情報をネットワークを介して扱う場合は、情報システム部の指示に従い、暗号化、電子署名などの処置を施さなければならない。

（３）利用者は、社内ネットワークにおいて、ネットワークモニターなどの、ネットワーク上を流れるパケットを盗聴できる機器及びソフトウェアを使用してはならない。

（４）利用者は、社内ネットワークサーバへのアクセス用のＩＤ及びパスワード、証明書は適切に管理しなければならない。

４．６．３　社内ネットワークへの接続時の注意事項

(A.6.2.1、A.9.1.2、A.9.3.1、A.12.2.1)

（１）自宅や、他組織のネットワークに接続していたＰＣは、マルウェア対策ソフトを用いて、最新の定義ファイルによりマルウェアチェックを実施し、異常が発見されなかったことを情報セキュリティ担当者が確認した後でなければ、社内ネットワークに接続してはならない。

（２）利用者は、ＩＰアドレスが固定の環境である社内ネットワークの場合、与えられたＩＰアドレス以外のＩＰアドレスを使用してはならない。

（３）利用者は、社内ネットワークに接続中のＰＣを、情報システム部の許可の無いADSL 回線、携帯電話、無線ＬＡＮ（公衆 Wi-Fi スポットなど）、専用線などを利用して、社外のネットワークに接続してはならない。

４．７　リモートアクセスサービス利用時のセキュリティ対策

４．７．１　利用申請

(A.6.2.1、A.6.2.2)

（１）業務上リモートアクセスサービスの利用が必要な者は、部門長の承認を得、情報システム部に申請しなければならない。

４．７．２　使用機器に関する遵守事項

(A.6.2.1、A.9.3.1)

（１）利用者は、社外から社内ネットワークへのアクセスにおいて、情報システム部が指定した機器を利用しなければならない。

（２）利用者は、インターネットから社内ネットワークへの接続手段を、情報セキュリティ委員会の許可を得ることなく設置してはならない。

（３）その他社内ＬＡＮ環境への接続にあたり、利用機器は、本規程に基づいて設定されなければならない。

（４）リモートアクセスで使用するＰＣは、盗難に遭わない様に、また紛失しない様に、利用者が管理を行わなければならない。

４．７．３　物理セキュリティ遵守事項

(A.6.2.1)

（１）リモートアクセスで使用するＰＣや Wi-Fi ルーターは、所有者の目に届く範囲内で管理できるようにし、使用しない時には、セキュリティが確保できる場所に保管しなければならない。

５　運用確認事項

（１）社内で実施される教育の内容を理解する。

（２）メール及びインターネット利用時のリスクを理解する。

（３）社外に情報を持ち出す場合は、その重要度を認識し、適切な管理策が取られていることを確認する。

（４）ＰＣの利用時、マルウェア対策、媒体管理等各種設定および設定が、正しく実施されていることを確認する。

６　例外事項

業務都合等により本規程の遵守事項を守れない状況が発生した場合は、情報セキュリティ担当者に報告し、例外の適用承認を受けなければならない。

７　罰則事項

本規程の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『人的管理規程』に従う。

８　公開事項

本規程は対象者にのみ公開するものとする。

９　改訂

・本規程は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本規程の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本規程は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。