安全管理細則（管理者用）

株式会社＊＊＊＊＊

制　定　平成２６年　９月　１日　初　版

個人情報保護 管理者	安全管理 責任者

目次

第１章　目的

第１条　目的

本細則は、別途定める「安全対策管理規程」によって、当社屋（来客室、執務室及び作業場）及び各拠点の管理を行い、コンピュータ・システム、ネットワーク及びサーバの安定稼働を維持することを目的とする。

第２章　物理的安全対策

第２条　執務室及び作業場の管理者

執務室及び作業場の安全管理は、安全管理責任者が行う。また、各拠点の安全管理は、安全管理責任者の指導の下、各拠点の長が行う。

第３条　安全管理責任者の任務

安全管理責任者は、執務室および作業場の施錠状況の確認及び異常発生時に適切な対処を行う。

２　安全管理責任者は、室内の盗難その他の事故防止及び室内秩序の維持にあたる。

３　安全管理責任者は、室内において盗難その他の犯罪が発生した時及びそれに類する報告を受けた時は、代表取締役に急報してその指揮を受けるほか、臨機応変の措置をとる。

第４条　執務室及び作業場の鍵の管理

各室の鍵の管理は、次に定めるとおりとする。

（１）　当社屋及び各拠点出入口の鍵は、代表取締役が、鍵所有権限があるとして指定された者（以下「鍵所有者」という。）に発行する。具体的な利用方法は、別途「安全管理細則（ユーザ用）」に定める。

（２）　執務室及び作業場は常時施錠し、開閉の鍵は、IC カードキーとし、安全管理者が必要であると認めた者に発行する。

（３）　個人情報及び機密情報を保管するキャビネットは施錠管理する。キャビネットの開錠施錠は「キャビネット開施錠記録簿」に記録し、安全管理責任者、又は安全管理責任者が指名したものが、毎月初めに先月分について異常が無いか確認を行う。

第５条 入室資格の付与

安全管理責任者は、当社の従業者に、身分証明書「社員証」の交付を行う。ただし、「社員証」の交付が間に合わない場合は、「ゲストカード」で一時的に代替えすることができる。

第６条 入室資格の特定

執務室及び作業場への入室資格は、原則として安全管理責任者が指定した「社員証」や「ゲストカード」の交付を受けた者に限る。

第７条 入室資格者の確認

各部門の責任者は、社員が「社員証」を着用している事の確認を適宜行う。

２　各部門の責任者は、特に不審と思われる訪問者に対して入室を拒否し、総務部門の責任者に連絡するとともに、適切な措置をとる。

第８条 訪問者の入室資格

訪問者が来客室以外の執務室などに入室する際は、「ゲストカード」を交付し、それを見やすい位置に着用していただく。

２　原則として、訪問者が入室する場合は、社員が同行しなければならない。ただし、当社の代表者から特に指名されたものを除く。

第９条　入室及び施錠記録の確認

別途「安全管理細則（ユーザ用)」で定める「最終退出点検表」及び「入退受付票」の記録は、安全管理責任者、又は安全管理責任者が指名したものが、毎月、前月分について異常ないか確認し、異常が発見された場合その原因を速やかに追求する。

第３章　ネットワーク・サーバ・PC 管理

第１０条　情報システムの管理原則

システム管理者は、当社の情報システムが、安定して稼動するよう維持し、かつ、更新する。

（１）　システム管理者は、社員等の増減やその要求に応じて、ネットワーク及びサーバに適切な変更を加える。

（２）　システム管理者は、ネットワーク及びサーバが、安定して稼動し、かつ、適切に変更するための必要な資源を、当社及び外部環境に応じて適切と認められる範囲で確保する。

（３）　システム管理者は、セキュリティに関する情報を随時収集し、収集した情報を分析し、重要な情報については速やかに対処する。

（４）　システム管理者は、ユーザがセキュリティ対策を行う場合に必要な情報を収集し、ユーザに対する教育が必要と判断した場合は、安全管理責任者と相談してセキュリティ教育を行う。

（５）　システム管理者は、ユーザのアクセスを必要最小限な範囲に設定する。

（６）　当社社員に携帯端末を貸与する場合について、別途「携帯端末取扱マニュアル」に定める。

第１１条　クライアント PC 管理

サーバにアクセスできるクライアント PC は、システム管理者が承認したものとし、以下の仕様を満たさなければならない。

（１）　ログイン･ログアウトの機能を有し、ログインしている個人が特定でき、サーバへのアクセス記録を取る事ができること。

（２）　ウィルス検知･駆除ソフトがインストールされており、最新のウィルスパターンを利用可能なもの。

（３）　PC のディスプレイは、外部から画面が見える位置に設置してはならない。但しどうしても外部から見える位置にて使用する必要がある場合は、覗き見防止の処置を施し、十分に注意して取り扱うこと。

（４）　パスワードつきのスクリーンセーバーが 10 分以内で起動するよう設定する。

（５）　移動可能な機器は盗難防止措置を講じる。ノート PC や USB メモリ等の可搬媒体は、総務で施錠された書庫にて管理し、持ち出し時には「ノート PC、可搬媒体持ち出し記録」により記録をとる。

第１２条　ネットワーク管理

システム管理者は、リスクを回避するために、以下の予防措置を講じて当社ネットワークを管理しなければならない。

（１）本社及び拠点間の通信経路上の情報は、漏洩が防止する仕組みを確立する。極めて高度な機密性が要求される場合は、通信経路上で情報の盗聴が行われても内容が解析できない機密保持機能を用いる。また、何らかの理由で通信経路上の機密保持機能を確保できない場合は、残存リスクとして認識し利用者にはリスクがある旨を伝えること。

（２）原則として無線 LAN は使用しない。ただし、無線 LAN を使用する必要が発生した場合は、通信内容を暗号化して利用すること。暗号化のレベルは、脆弱性を考慮してシステム管理者が設定する。

第１３条　サーバ管理

システム管理者は、リスクを回避するために、以下の予防策を講じてサーバを管理しなければならない。

（１）　サーバは、地震、火災、盗難、破壊、漏水等の発生可能性を考慮して、可能な限り安全が保たれる場所に設置する、具体的には執務室の一画にて、施錠管理し、その入退室を「サーバルーム入退記録簿」に記録する。「サーバルーム入退記録簿」は、安全管理責任者が、毎月の月初めに前月分を確認する。

（２）　サーバに機器及びソフトウェアを導入する場合は、供給者の連絡先及び更新情報が明確でありセキュリティ仕様が万全であることをあらかじめ確認してから行う。

（３） サーバの設定やシステム構成の変更を行うときは、セキュリティ上の問題が生じないことを確認する。
（４） サーバの機器やネットワークの負荷状況を常に確認し、適切に維持する。
（５） サーバの機器及びソフトウェアの廃棄、返却、譲渡を行うときは、情報漏洩対策をとる。
（６） サーバのシステム関連のファイルは、ユーザがアクセスできないようにする。
（７） ファイルのバックアップを定期的に行い、その磁気媒体などを安全な方法で保管する。その手順を「バックアップ手順書」に定める。

第１４条　履歴管理

システム管理者は、サーバの動作履歴、使用記録等を記録し、その記録の改ざん、削除、破壊及び漏洩の防止策を実施する。
（１）記録したサーバの動作履歴、使用記録等は、異常を発見した際に随時分析する。
（２）記録したサーバの動作履歴、使用記録等は、安全な方法で一定期間保存する。
（３）システム管理者は、毎月の月初めに前月分のサーバの動作履歴、使用記録が確実に取得され保管されていることを確認し、「アクセスログ確認記録」に確認する。

第４章　ユーザ ID・特権 ID の付与、アクセス権の付与及び廃棄

第１５条　特権 ID の付与

システム管理者は、特定の者に、当社の使用するサーバやネットワークの重要機器に、特別な管理を行うことができるユーザとしての管理者特権を有する特権 ID を付与する。特権 ID の付与に当たっては、その資質と適用範囲について十分考慮した上で、安全管理責任者の承認を得る。
２　特権 ID を付与された機器管理者は、ネットワークを管理する上で得た機密情報を外部に漏らしてはならない。
３　特権 ID を付与する機器管理者は、安全性と可用性を考慮して複数のものにすることがのぞましいが、必要最小限にとどめる。

第１６条　ユーザ ID 管理

ネットワークを利用してサーバにアクセスできるユーザ ID は、必要最小限にする。また、アクセスできるユーザがアクセスできる範囲も必要最小限にする。
２　サーバには「guest」など不特定多数が利用する ID を使用しない。
３　新規ユーザ ID の作成は、要求部門の責任者がネットワーク管理者に要請することにより発行する。また、原則として１ユーザ 1ID とする。
４　ユーザ ID のアクセス権は、ユーザごとに設定し登録する。
５　利用しなくなった ID が発生した場合、システム管理者は速やかに ID を削除する。何

らかの理由で速やかに削除できない場合は、削除予定日をあらかじめ定め、それまでは利用停止 ID としてシステム管理者が管理する。

６　管理者特権を有する機器管理者は、管理業務を行うときのみ、管理者特権を使用する。

第１７条　パスワードの設定

ユーザ ID には必ずパスワードを設定することとするが、類推可能なパスワードを使用してはならない。また当該ユーザ以外にパスワードを知らせてはならない。

２　パスワードは、各ユーザが ６ ヶ月に一度、変更するよう設定する。また当該ユーザ以外に知られた可能性があるときは速やかにパスワードを変更しなくてはならない。

第５章　ネットワーク緊急事態対応

第１８条　緊急事態発生時の対応

システム管理者は、当社のコンピュータネットワークシステム及びサーバに、異常が発生した（可能性がある）との報告を受けた場合、又は自ら発見した場合には、関係者と協議して、速やかに講じるべき対策を検討し、必要な対策を講じる。

２　システム管理者は、緊急事態発生時に備え、関係者に速やかに連絡が取れるよう、「緊急連絡体制」を策定し、維持する。当社では、この「緊急連絡体制」は、個人情報保護関連規程で定める「緊急連絡体制」と同一とする。

３　異常の発生には至らないが、異常が起こる（可能性がある）リスクの発生が判明した場合には、関係者と協調して状況を把握し、適切な対応を取り被害発生を防止する。

４　個人情報に関するリスクが発生した場合には、個人情報保護管理者に連絡しその指示に従う。

５　リスクによる被害が発生した場合には、緊急対応策を講じ速やかな復旧に努める。

６　リスク発生の原因を調査分析し、再発防止策を講じる。

規程等の制定及び改廃

本規程の制定及び改廃は、安全管理責任者が、個人情報保護管理者の承認を得て行う。

付則

制定：平成２６年　９月　１日　初　版