アクセス管理規則

第１章　総　　則

（目　的）

第１条　この規則は、ジーダブルテクノロジー株式会社（以下「会社」という。）におけるコンピュータシステムへの不正アクセスを防止し情報資産を保護するため、必要な事項を定め、もって企業情報の適正な活用および企業秘密漏えいの防止を図ることを目的とする。

（適用範囲）

第２条　この規則は、会社内のすべてのコンピュータシステムに適用される。また、そのシステムを利用する会社の役員および従業員（以下「役職員」という。）に適用されるものとする。

（定　義）

第３条　アクセスの対象となるのは、社内情報資源の存在するところすべて、すなわちコンピュータシステムおよび記憶媒体の存在する場所（以下「媒体保管場所」という。）である。この規則においてコンピュータシステムとは、社内・社外ネットワーク、ハードウェア、ソフトウェアから構成されるシステム全体を指す（社内・外ネットワークの定義については、「ネットワークセキュリティ規則」を参照のこと）。

２　この規則において、アクセス管理とは、アクセス権限の設定、アクセス認証、アクセス制御、アクセス監視を指す。

（１）アクセス権限の設定とは、各種情報資産に関してアクセス権限の内容を明確化することをいう（閲覧のみか、編集可能か、などまで含む。）。

（２）アクセス認証とは、情報の利用者がその利用を許可された本人であることを確認することである。

（３）アクセス制御とは、情報の利用者が当該情報を利用する権限のある役職員であることを確認し、かつその利用方法が当該役職員の権限の範囲内であることを確認することによって、権限のない役職員あるいは第三者などからの不正なアクセスを排除するために実施する施策である。

（４）アクセス監視とは、コンピュータネットワークへのアクセス履歴を記録し、定期的に調査することで、不正アクセスの防止・発見に役立てることである。

第２章　アクセス管理体制

（アクセス管理主体）

第４条　コンピュータシステムについては、別に定める情報管理統括責任者（以下「統括責任者」という。）をリーダーとする情報管理統括部署（以下「統括部」という。）がこれを主管することとする。

２　記憶媒体保管場所に関しては、「情報管理規程」に従って厳重に管理するとともに、当該場所を管理している部署がその管理責任を負う。

第３章　アクセス管理手順

（アクセス権限設定）

第５条　各部署の情報管理責任者（以下「管理責任者」という。）は、「情報管理規程」で規定される企業情報の機密性に関する等級を考慮して、各情報資産についてアクセス権限を設定することとする。また、利用者ごとのアクセス権限内容を文書化し、保管管理する。なお、管理責任者は自らの管理者権限を悪用し、情報資産を盗用などすることがあってはならない。

２　アクセス権限は随時、事業の推移に合わせて管理責任者が見直すこととする（変更の際は本規則第７条（２）を参照のこと。）。

（アクセス認証）

第６条　統括部は、アクセス管理されるコンピュータシステムおよび媒体保管場所について、利用者のアクセス認証をするためのしくみを設ける。アクセス認証は、各種情報資産の不正利用・流出を防止するためにも重要であるので、コンピュータシステムについては個人 ID およびパスワードにより、媒体保管場所については施錠と鍵の管理の徹底などによって、厳重に行う。

（アクセス制御の手順）

第７条　アクセス制御を行うにあたっては、ネットワークの設計段階から運用に至るまで段階的に行う。

（１）ネットワークの設計にあたり、設計担当者はネットワークおよびネットワークに接続されるハードウェアについて物理的・論理的にアクセス制御ができるようにする。

（２）ネットワーク運用担当者は、運用開始後、コンピュータネットワークおよび記憶媒体に対して適切にアクセス制御がなされているかどうかを定期的に検査し、不適切なものは主管部署の管理責任者と協議のうえ、これを変更する。

（３）特に重要な機密情報が存在するコンピュータネットワークについては、ID とパスワードによるアクセス制御以上に強固なものを利用するなどして（たとえば使い捨てパスワードなど）厳重にアクセス制御を行う。

（４）媒体保管場所については、当該情報の利用を許可されていないものの侵入を防ぐための措置を講じる。たとえば、部屋に施錠し、鍵は厳重に管理し、鍵の管理部署において入退出者の氏名・部署・連絡先などを記録し、保管するなどである。

（利用者側の留意事項）

第８条　利用者はコンピュータシステムを利用するにあたり、各部署の管理責任者に対して利用者登録を申請する。管理責任者は、個人情報についての情報漏えいに注意し、IDおよびパスワードなど、別に規定する方法で登録を行う。

２　各利用者は、自らに与えられた権限が第三者に悪用されないよう、細心の注意を払う。たとえば、自らが権限のある情報資産にログインしたまま、席を離れるなどして、第三者への情報漏えいの可能性がある行為は行わないこと。

３　利用者は退職・転部その他の理由により、当該情報資産を利用する権限を持たなくなった場合、各部署の管理責任者に対して登録抹消手続の申請を行う。

４　利用者はアクセス権限を持たなくなった場合、原則として、権限保有中に知り得た情報を他人に漏らしたり盗用してはならない。

５　利用者は、許可されていない情報資産に対して不正にアクセスしてはならない。

（アクセス監視）

第９条　統括部は共同利用のコンピュータシステムについて、動作履歴とアクセス履歴をとる機能を構築する。媒体保管場所については、入退出管理を徹底する。

２　統括部は、蓄積された履歴を定期的に調査し、不正の疑いがあるものについてはそれを究明し、再発を防止する。

３　統括部は、蓄積された履歴の紛失・改ざんなどに注意し、厳重に保管する。

第４章　トラブル発生時の対応

（トラブル発生時の対応）

第 10 条　「ネットワークセキュリティ規則」第 4 章に準じて行うものとする。

付　　則

この規程は、平成２５年１０月１日より施行する。