情報システム管理規程

第1章 総　則

（目的）

第1条　本規程は、財務報告の信頼性の確保及び業務の効率的運営を図る過程において、株式会社トゥエンティーフォーセブンホールディングスグループ（以下、「当社グループ」という。）の情報資産が常に盗聴、侵入、破壊、改ざん等の脅威にさらされていること（特に個人情報においては漏えい、滅失及びき損の脅威）を認識し、ネットワークを通じて正確な情報及び安定的な情報サービスの提供を確保することを目的とする。そのためセキュリティを実現し、当社グループのネットワーク及び取り扱う情報資産を適切に保護するための基本事項を定めたものである。

（主管部門及び責任者）

第2条　本規程の主管部門は株式会社トゥエンティーフォーセブンホールディングス（以下、「HD」という。）コーポレート本部とし、責任者はHDコーポレート本部長とする。

2. 本規程の運用にあたっては、HDの親会社であるNOVAホールディングス株式会社（以下、「NH」という。）のシステム部と連携して実施するものとする。

（定義）

第3条　本規程で掲げる用語の定義は、次のとおりとする。

① 利用者とは、当社グループ内で情報システムを利用する者をいう。

② ソフトウェアとは、業務用プログラム、アプリケーションプログラム、ユーティリティプログラム等のプログラムをいう。

③ 情報システムとは、ハードウェア、ソフトウェアもしくはネットワーク又はこれらの複合体をいう。

④ バックアップとは、プログラム、データ等と同一の内容を別の媒体に記録することをいう。

⑤ ファイルとは、記憶装置又は記録媒体上に、電子的又は光学的に記録されているプログラム、データ等をいう。

⑥ 情報機器とは、ハードウェア、通信回線又は通信機器をいう。

⑦ セキュリティ機能とは、プログラム、データ等の機密性、保全性及び可用性を確保するための機能をいう。

⑧ 重要情報とは、「機密情報管理規程」第2条に別途定める社内機密情報（経営情報、営業情報、役員・従業員情報等）、個人情報（社内、取引先、メールアドレス帳等）及びその他、漏えいを禁止すべき情報をいう。

⑨ 情報資産とは、当社が管理運営する情報、情報処理機器・通信装置など情報を取扱う機器、ソフトウェア、用室・電源・空調などの施設・設備、それらを取扱う人材をいう。

（守秘義務）

第4条　情報システムの企画・開発・運用ならびに利用で知り得た情報や当社のセキュリティに関する事項を外部に開示、漏えいしてはならない。ただし、HD コーポレート本部長の承認を得たものはこの限りでない。

（罰則）

第5条　本規程に故意又は重大な過失により違反した役員及び従業員は、就業規則等の定めるところにより懲戒に処するものとする。

第2章 組織・体制・役割

（責任者）

第6条　情報システムの適切な管理を行うため、情報システム責任者を置く。情報システムの管理に関わる事項を統括する者で、HD コーポレート本部長がこれに当たる。

2. 情報システム責任者は、社内の情報システム管理に適切な者を情報システム担当者として 1 名以上指名する。
3. 各部門における情報システムの適切な運用を管理・推進するために、情報セキュリティ部門責任者を置く。部長または課長がこれに当たる。
4. 情報セキュリティ部門責任者は、部門内における情報システムの運用をサポートするために適切な者を情報セキュリティ部門担当者として 1 名以上指名し、その者の氏名を情報システム責任者に報告する。

（情報システム責任者の責務）

第7条　情報システム責任者の責務は、次のとおりとする。

(1) 利用者管理

① サーバを直接利用できる者は、原則として情報システム責任者及び情報システム担当者に限るものとする。

② 個人IDを利用者単位で割り当て、パスワードを必ず設定しなければならない。

③ 利用者ごとのアクセス権限について一覧表等を作成し、管理しなければならない。

④ 利用者の責として、パスワードは容易に推測されないように設定し、その秘密を保たなければならない。

(2) リスク認識

情報システム責任者は、サーバに格納された情報及びその情報の基となる紙、記録媒体について、情報への不正アクセス、情報の漏えい、滅失、破壊及びき損のリスク（以下「リスク」という）が存在することを認識するとともに、当社グループ内に周知徹底しなければならない。

(3) 情報管理

情報システム責任者は、リスクを回避するために、以下の予防措置を講じて情報を管理しなければならない。

① 通信経路上の情報は、漏えいを防止する仕組みを確立しなければならない。
② 重要情報を記録した紙、記録媒体等は、安全な場所に施錠保管しなければならない。
③ 重要情報を記録した紙、記録媒体等を廃棄する場合は、内容が漏えいしない方法で行わなければならない。
④ ファイルのバックアップを随時行い、その記録媒体等を安全な方法で施錠保管しなければならない。特に重要なファイルについては、複数の記録媒体等にバックアップを行い、それぞれ別の場所に安全な方法で施錠保管しなければならない。

(4) サーバ管理

情報システム責任者は、リスクを回避するために以下の予防措置を講じてサーバを管理しなければならない。

① サーバ等（情報機器含む）は、盗難、破壊、破損、漏水、火災、停電、電磁波、地震などの物理的な脅威を予測し、可能な限り物理的保護を考慮したうえで、格納されるデータ又はファイルの機密性に応じた場所に設置し、管理しなければならない。
② 移動可能な機器は、盗難防止策を講じなければならない。
③ ネットワークを介して外部からサーバ管理を行う場合は、認証機能、暗号機能及びアクセス制御機能を設定しなければならない。

(5) 情報機器・媒体管理

情報システム責任者は、情報機器・媒体の紛失、盗難防措置を講じて機器を管理しなければならない。

① 情報機器等は、台帳を作成して管理しなければならない。
② 当社グループ内の情報システムの範囲を、ネットワーク構成図等を作成して管理しなければならない。
③ 記憶媒体は、使用後、データを完全に消去し施錠できるキャビネット等に保管して管理しなければならない。

(6) 情報収集

① セキュリティ対策に関する情報を随時収集しなければならない。
② 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応しなければならない。

(7) 棚卸

情報システム責任者は、次の項目について定期的に棚卸を行わなければならない。

① 情報機器については、各四半期末に棚卸を実施する。
② 個人IDについては、毎年11月に棚卸を実施する。
③ アクセス権限については、毎年11月に棚卸を実施する。

(8) 指示・伝達

情報システム責任者は、上記の責務を効率的かつ円滑に果たすために、情報セキュリティ部門責任者及び情報セキュリティ部門担当者に対して指示・伝達を行うことができる。

第3章 データの取扱・保管

（重要情報廃棄）

第8条　重要情報の廃棄に関しては、紙情報についてはシュレッダーによる廃棄を行う。PC 本体･HDD・メディア等については、機密の漏えいを防止するために必ず判読不能になるまで物理的に破壊するか又は内容を復元不能になるまで消去した後、廃棄しなければならない。

（損壊の防止）

第9条　重要情報の滅失又はき損を防止するために、定期的(毎日)に外部媒体等にバックアップを行い所定期間（1 ヶ月）保管する。

（電子メールのデータ送信）

第10条　重要情報を電子メール等の方法で送信することは原則禁止する。ただし、業務上やむを得ない場合は、暗号化を行う等の措置を講じ、必要最小限とする。

（情報機器のモニタリング・アクセスログ等の取得）

第11条　当社グループは、必要と認める場合には、従業員等に貸与その他の方法で使用を許諾したＰＣ、スマートフォンその他の情報機器及びソフトウェアについて、その挙動についてモニタリングをし、操作ログ並びに情報機器及び情報システム内に蓄積されたデータ等の閲覧・取得をすることができる。

2. 重要情報の作成・変更・削除・閲覧にあたっては、各々のアクセスログを取得できるようにする。
3. 当社グループは、各社・各部門の部長または課長の求めに応じて、HD コーポレート本部長の承認を得たうえで、当該部門の利用者のメッセンジャーアプリ等で受送信されたメッセージの閲覧・取得含むソフトウェア及び情報システムのアクセスログ等の閲覧・取得をすることができる。
4. 前各項のアクセスログ等の閲覧・取得は HD コーポレート本部長、又はその指示を受けた従業員が実施しなければならない。

（アクセス権限の設定）

第12条　重要情報は、アクセス権限を設定するようにし、利用者以外がアクセスできないような措置を講じる。

2. アクセス権限は、必要機器に限定し、利用者の権限を必要最小限に設定するものとする。
3. アクセス権限は、毎年 11 月に見直しを行う。

（暗号化の設定）

第13条　重要情報を外部へ送付する際は、暗号化を行わなければならない。

（保管場所）

第14条　重要情報の保管は、所定の保管棚等に格納し、常に施錠しなければならない。

（ネットワーク上でのデータの授受）

第15条　ネットワークを介して外部との重要データの授受を行う場合は、認証機能、暗号機能及びアクセス制御機能を設定する。また、WEB ホームページ上で重要情報を収集する場合は、必ず SSL 等の暗号化の措置を講じる。

第4章 セキュリティ

（パソコン・記録媒体に対する措置）

第16条　当社グループが所有又は保有するパソコンは、セキュリティを確保するため、次の措置を講じる。

(1)　携帯可能な情報機器は、退社時に施錠可能な引出しに格納する等、盗難防止策を講じる。（チェーン等での固定でもよい）

(2)　各社・各部門が管理している全てのパソコンは台帳を作成し、実態を把握するものとする。

(3)　パソコンが無断で利用されないよう個人認証措置やパスワードによる保護付きスクリーンセーバの対策を講じる。設定時間は 10 分間以内とする。

(4)　重要情報は各クライアントパソコンに保管せず、アクセス制御やバックアップを遂行している部門のファイルサーバに格納する。業務上やむを得ずクライアントパソコンに情報を格納する場合は、ツールによる漏えい、滅失、き損の防止策を講じる。

(5)　個人所有情報機器を社内に持ち込み利用することは禁止とする。

(6)　情報機器を社外へ持ち出すことは、原則禁止とする。ただし、業務上やむを得ない場合は、WF「情報機器社外持出申請」にて申請し承認を得るものとする。

(7)　情報機器に重要情報を格納し社外へ持ち出す場合には、パスワードによるアクセス制御の他にバイオス又は暗号化するなど二重のパスワード設定対策を講じなければならない。

(8)　長期間利用しないパソコンは、ネットワークから切り離す措置を講じる。

(9)　USB ポート等を経由して記憶する外部記憶媒体（ＵＳＢメモリー等）は、原則使用を禁止する。

（サーバに対する措置）

第17条　当社グループが保有するサーバは、セキュリティを確保するため、次の措置を講じる。

(1)　情報資産を全社的規模で集約し格納するようなサーバは、許可を与えられた者以外立ち入れない場所及び施錠可能なマシン収納ラックに設置し、マシン収納ラックの鍵を適切に管理する。

(2)　重要なファイルへのアクセス権限は、担当者以外の者に与えてはならない。

(3)　サーバが無断で利用されないよう、個人認証措置やパスワードによる保護付きスクリーンセーバの対策を講じる。設定時間は 5 分間以内とする。

(4)　部門サーバの持ち出し、持ち込みは禁止する。

(5)　長期間利用しないサーバは、ネットワークから切り離す措置を講じる。

(6)　各社・各部門が管理している全てのサーバは台帳を作成し、実態を把握できるようにする。

(7)　サーバに必要があれば無停電電源装置（UPS）を設置する。

（ネットワーク機器及び配線における措置）

第18条　当社グループのネットワークの機器及び配線は、機密性、完全性及び可用性を踏まえ、次の措置を講じるものとする。

(1)　ネットワークの構成変更は、情報システム責任者に承認を得、情報システム責任者の指示に従って構築する。

(2) 情報システム責任者は、ネットワークの配線、電源ケーブルについて傍受又は損傷を防止するためフリーアクセスフロアーやモール等、外部に露出しない措置を講じるものとする。
(3) 情報システム責任者は、ネットワークに不正な接続を防止する措置を講じるものとする。

（個人IDとパスワードの管理）

第19条　個人 ID は、次の要領で取り扱わなければならない。
(1) 自分の個人 ID は他の人に利用させてはならない。
2. パスワードは次の要領で取り扱わなければならない。
(1) パスワードは英大文字・英小文字と数字の組み合わせで８文字以上としなければならない。
(2) パスワードは他人に推測されにくいものを使用する。
(3) パスワードは対象アカウントが共有・個人利用に関わらず利用者が退職した際に即座に変更しなければならない。また第三者へパスワードが漏洩またはその恐れがある場合は速やかに情報システム部へ報告し、変更を実施しなくてはならない。
(4) パスワードは各個人で管理を行い、他人に知られないように注意する。
3. 情報システム責任者は、一定回数以上連続してログインに失敗したユーザーＩＤに対し、ロックアウトする等の排除措置を取らなければならない。ただし、情報システムの制約により上記要件にて設定できない場合には、その可能な範囲で上記要件にできるだけ近づくよう設定しなければならない。
4. ソフトウェア（アプリケーションプログラム等）毎に個人 ID を設定する必要がある場合は、個別に基準又は手順書にその取り扱い要領を記載し、管理しなければならない。

（個人IDの運営方法）

第20条　個人 ID は、次の要領にて運営する。
(1) 個人 ID の登録・改廃手続きは情報システム職務権限表による。
(2) 情報システム担当者は、個人 ID の登録・改廃について変更履歴を記録し、これを管理する。
(3) 情報システム担当者は、定期的に個人 ID の棚卸しを行い、不要となった個人 ID が無いかを確認する。

（情報システム利用時の禁止項目）

第21条　利用者は、情報システムを利用する際、次の項目を遵守する。
(1) 業務目的以外のデータ交換及び情報の持ち出しを禁止する。
(2) 電子メールやサイトアクセス等のインターネットサービスの不適切な利用を禁止する。
(3) 良識に反する電子メールの利用を禁止する。

（不正アクセスコンピュータウィルス対策）

第22条　コンピュータウィルス対策として次の感染防止策を講じなければならない。
(1) 情報システム責任者は、ウィルス対策ソフトを準備し、最新のバージョン状態に保つためにパターンファイルやセキュリティーパッチ等アップデートができる環境を提供する。
(2) 情報システム責任者は、ネットワークに接続されている情報処理機器について、ウィルス対策ソフトを管理し、利用者に常に最新状態となるよう指示・指導する。
(3) 利用者は、使用する情報処理機器に情報システム責任者が定めたウィルス対策ソフトを必ず導入し、最新バージョンであることを維持する。
(4) 外部ネットワークからファイル及びソフトウェアを取り入れた際、情報処理機器において該当ファイル及びソフトウェアのウィルスチェックを実施する。
(5) 不正ソフトウエアおよびその対策についての最新情報は、独立行政法人情報処理推進機構（IPA）

等のウエブサイトを参考にする。

(6) 「Winny」、「Share」等ファイル交換ソフトウェアをインストールをしない。

(7) 差出人が不明のメール又は不自然な添付メールの添付ファイルは削除する。

第5章 開 発

（起案）

第23条 当社グループの業務で使用するソフトウェア（アプリケーションプログラム）を開発又はプログラムの修正を行う際は、情報システム職務権限表に定める承認及び決裁を得て行うものとする。

（評価テスト及び本番テスト）

第24条 1.開発又は修正されたソフトウェア（アプリケーションプログラム）は、十分な評価テストを行った上で本番登録されなければならない。評価テスト及び本番登録の手続きは、別に定める「ソフトウェア管理基準」又は個別の手順書によるものとする。

2.評価テストに使用するテストデータには、重要情報に該当する情報は使用しない。

（変更履歴の管理）

第25条 情報システム責任者は、プログラムの本番登録について変更履歴を記録し、一定の期間保管管理しなければならない。

第6章 運 用

（情報システムの監視）

第26条 情報システムの監視について以下の項目を行う。

(1) 情報システム責任者は、当社グループの業務に使用するソフトウェア（アプリケーションプログラム）のプログラムの更新状況に異常が無いことを定期的に監視する。

(2) 情報システム責任者は、情報システムへの不審なアクセスがないかをアクセスログを取得するなどして監視する。

(3) 各部門は、情報システムのサーバに不審なファイルが存在していないか又は既存ファイルがき損されていないかを定期的に監視する。

(4) 本規程第 21 条に定められた情報システムの業務目的以外の利用を防止するために、定期的に監視する。

（ログの管理）

第27条 監視により得られたアクセスログ等については、滅失、き損されないために別サーバに自動的に保存するように施し、エラー等が検出された場合はメールなど等で通知されるなど必要な措置を講じ、使用記録等を四半期に 1 度点検する。

（インフラの管理）

第28条　当社グループの業務に使用する情報システムのインフラは、安全性・耐障害性・持続可能性・快適性を踏まえ次の措置を講じるものとする。

(1) ネットワーク機器及び回線の冗長化やクラウドサービスの採用を行い、災害時などにおける業務停止時間を限りなく最小限にするようにする。

(2) PC およびその周辺機器の予備を常に設けておき、不測の事態が発生した際にも、継続的に業務が遂行できる環境にする。

(3)ネットワーク面において業務に適した速度が保たれているかを監視し、業務支障がない様にする。また常に最新の技術情報を収集し業務効率化ツールの導入・検討に努める。

（ソフトウェアの管理と運用）

第29条　当社グループの業務に使用するソフトウェア（アプリケーションプログラム）について、「ソフトウェア管理基準」によって管理・運用する。また、重要なシステムについては、個別の手順書を定めて管理・運用する。

2. 情報システム責任者が認めたもの以外のソフトウェアのインストールを禁止する。

（ソフトウェアとドキュメントの管理）

第30条　情報処理に関わるソフトウェア及びこれらに付随するドキュメントの管理に関する措置を定め、機密保護と安全の確保を的確に行う。

2. 前項のソフトウェアが当社にて開発したものである場合、情報システム責任者は実行モジュールとソースモジュールとの乖離が無いように管理しなければならない。ただし、ソフトウェアが外部委託業者によって開発されたもので、実行モジュールのみを納品されたものである場合はこの限りではない。

（ジョブスケジュール管理）

第31条　情報システムの日常的な管理業務において、バックログ等を利用して自動化する場合は次の項目を遵守するものとする。

(1)　バックログのプロジェクト登録・変更権限は情報システム責任者および情報システム担当者のみに付与すること。

(2)　情報システム責任者は、ジョブの実行結果を適宜に確認すること。

（バックアップの管理）

第32条　データのバックアップについては、次の項目を遵守するものとする。

(1)　取得対象とするデータの重要度や更新頻度等に応じたバックアップに関する方針として、データの論理的な破壊もしくは媒体の物理的破壊の備えたデータ保存策を次の通り実施することとする。

①　論理的な破壊に対する保全策として、意図的な改ざんに耐え、破壊される直前に戻れるように、バックアップを複数世代に渡り取得し、時間的に遡ることができるようにする。

②　物理的な破壊に対する保全策として、オリジナルデータとバックアップデータの保存場

所、保存メディアを別々に分ける。

③　取得対象は、機密情報管理規程に定める機密情報をいう。

(2)　バックアップの手順書等を定め、バックアップ処理結果について確認を取ること。

(3)　リストアの手順書等を定め、定期的にリストアテストを実施してバックアップからデータ復旧できることを確認すること。

（障害発生時の対応）

第33条　情報システムに障害が発生した場合には、次の対応を行うものとする。

(1)　障害が発生した時刻、障害の事象、原因及び実施した障害対策の内容を記録すること。

(2)　情報システム責任者は、障害対策の内容の妥当性について、事前又は事後に確認をすること。

(3)　障害が発生した際の報告、記録の作成等の手続きは「情報システム職務権限表」による。

（脅威発生時の対応）

第34条　脅威が発生した場合には、次の対応を行うものとする。

(1)　不正アクセス、ウィルス等がネットワーク経由で拡大し、重要情報の重大な被害が発生し、情報資産の防護のためにネットワークの切断がやむを得ない場合は、ネットワークを切断する措置を講じる。

(2)　情報資産が深刻な被害を受けている時、災害等で電源供給確保が困難な時等、情報資産の防護のために情報システムの停止がやむを得ない場合は、情報システムを停止する措置を講じる。

（再発防止の措置）

第35条　情報システム責任者は、再発防止に対処するため当該脅威の対応策を検討の上、本規程等の改善を行い、再発の防止策を講ずる。

（機器廃棄の措置）

第36条　情報機器の廃棄については、次の項目を遵守するものとする。

(1)　情報処理機器、通信機器等の機器内に情報資産が格納されている場合、記録媒体をディスク情報消去ツールでの消去又は記録媒体の破壊を行う。

(2)　廃棄を外部業者に委託する場合は、文書により授受を明確にし、廃棄証明書を受領する。

（外部からの接続）

第37条　外部から社内ネットワークへの接続は、次の項目を遵守するものとする。

(1)　情報システム責任者が承認した者のみ行うことができる。

(2)　ユーザーＩＤおよびパスワードは他人に提供してはならない。

(3)　接続する端末には、ウイルス対策および不正アクセス対策が施されているものとする。

（重要情報の移送・通信）

第38条　重要情報の移送・通信については、次の項目を遵守するものとする。

(1)　重要情報を搬送する場合は、情報システム責任者が承認をした運送業者を使用する。

(2)　重要情報を通信する場合は、送信相手と方式や安全上の取り決めを書面で交わし、データの暗号化を施す措置を講じるものとする。

(3)　重要情報の移送・通信を行う場合は、記録を残すものとする。

第7章 データの直接修正

（起案）

第39条　DBMS 等に対するデータ直接修正に関する案件を依頼する際は、利用部門の責任者及び情報システム責任者の承認を受けるものとする。データ直接修正の手続きは、別に定める「ソフトウェア管理基準」又は個別の手順書による。

（評価テスト）

第40条　データ直接修正を実施する場合は、テスト環境にて十分な評価テストを行わなければならない。評価テスト実施の手続きは、別に定めるソフトウェア管理基準又は個別の手順書によるものとする。

（データ直接修正の実施）

第41条　本番環境においてデータ直接修正を実施する場合は、情報システム責任者が修正方法を決定し、これを行う。本番環境におけるデータ直接修正実施の手続きは、別に定める「ソフトウェア管理基準」又は個別の手順書によるものとする。

（修正履歴の管理）

第42条　情報システム責任者は、データ直接修正について修正履歴を記録し、これを管理する。

第8章 評価・見直し

（評価・見直し）

第43条　年度毎に環境の変化や新たな脅威が発生していないかを分析、評価し、本規程の見直しを行うとともに変更内容の妥当性を確認する。

2. 環境の変化や新たな脅威が発生した時は、適宜本規程の見直しを行うとともに変更内容の妥当性を確認する。

（附則）

1. 本規程の変更は、取締役会の決議によるものとする
2. 本規程は、平成 28 年 6 月 29 日より実施する。

平成 28 年 8 月 1 日　改定・実施

平成 28 年 11 月 15 日　改定・実施

平成 29 年 6 月 1 日　改定・実施

平成 29 年 7 月 19 日　改定・実施

平成 30 年 9 月 1 日　改定・実施

令和３年11月１日　改定・実施
令和７年６月１日　改定・実施