情報セキュリティ及び情報機器取扱い規程

（目的）

第1条　この規程は、当社において守るべき情報セキュリティ及び情報機器の取扱い運用基準の基本となる遵守事項を定め、事業場の損失、社会的信用の失墜を防ぐことを目的とする。

（用語の定義）

第2条　規程中次に掲げる用語はそれぞれ次の意味に用いる。

1　情報システム
当社の管理するコンピュータ（ソフトウェアを含む）、ネットワークなどをいう。

2　個人情報
個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述、又はマイナンバー等個人別に付された番号、記号その他の符号、画像、若しくは音声により当該個人を識別できるもの（当該情報のみでは識別できないが、他の情報と容易に照合することができ、それにより当該個人を識別できるものを含む）をいう。

3　情報資産
当社が作成したか、社外から取得したかに係らず、機密情報、個人情報等すべて含むものとし、以下のものをいう。
①当社の管理する文書
②当社の管理する電子情報
③当社が管理する、若しくは外部業者へ運用管理を委託したコンピュータ及び記憶媒体に記録された電子情報等

4　事業所
当社の本社、支店、事業所、営業所、現場、その他職制等、本規則を適用する組織単位をいう。

5　文書
情報を記録した文書、図面、マイクロフィルム等、人の知覚によって認識できるものをいう。

6　電子情報
電子的方式、磁気的方式その他人の知覚によって認識することが出来ない方式で作られる記録であって、コンピュータ等による情報処理の用に供される情報をいう。

7　機密情報
業務上の内容を社外または関係者以外に対し、機密とすべき情報をいう。「機密情報」には、機密文書及び機密電子情報の他、サンプル、製品、設備等で機密が化体した有体物及び機密とすべき個人の記憶情報を含む。

8　社内ネットワーク
事業所LAN及び事業所LAN間をネットワークで接続したものをいう。

9　アカウント
パソコン利用ID、インターネット接続ID、電子メールID等、利用者を識別するために作成される登録情報をいう。

10　情報事故
故意、過失に係わらず、本来の意図に反して当社の情報資産及び情報システムに関係する事物が他者に漏洩若しくは情報機器等を紛失、または盗取された事象をいい、その疑いがあるものすべてをいう。

11　パソコン等情報機器
パーソナルコンピュータ（形状を問わない）、携帯電話機、スマートデバイス（スマート

フォン，タブレット端末，ウェアラブル端末等）、デジタルカメラなどに加えてこれらに類する通信機能を有した機器、または情報家電全般をいう。

（適用範囲）

第3条　情報資産及び情報システムに関係する役員、すべての従業員（社員、臨時員、パートタイマー及び派遣労働者を含む）に本規則を適用する。

（統括責任者の指名）

第4条　社長は、本規則の運用に関する責任及び権限を持つ、「情報セキュリティ統括責任者」を指名する。（以下、情報セキュリティ統括責任者を「統括責任者」という）

（情報セキュリティ委員会の設置）

第5条　情報資産及び情報システムを管理するために、統括責任者は全社統括組織として、以下から構成される情報セキュリティ委員会を設置する。

(1) 委員長は統括責任者とする。

(2) 委員は委員長が各部署より指名した者とする。

②　委員長は、委員の中から情報システム責任者を指名する。

③　本社工事部及び中国支店の情報セキュリティ委員は、営業所並びに現場規模に応じて情報セキュリティ実行責任者（以下、「実行責任者」という）を指名する。実行責任者は、情報資産管理並びに情報システム責任者の職務の一部を代行するものとする。

（情報セキュリティ委員会の責務）

第6条　全社的な情報セキュリティ及び情報システム取扱いに関する管理及び統括を行うために、情報セキュリティ委員会は下記施策を継続的に講ずる。

(1) 方針展開

(2) リスクマネジメント

(3) 教育計画の立案及び推進

(4) 点検・運用状況の報告の分析及び施策への反映

（事業所における情報セキュリティ管理体制）

第7条　実行責任者は、事業所において各項に定める施策を継続的に講じる。

(1) 情報セキュリティ施策の実施

(2) 情報資産管理施策の実施

(3) 情報セキュリティに関する教育の実施及び記録

（情報事故対応）

第8条　実行責任者は、情報事故が発生した場合、速やかに被害状況を把握し、情報セキュリティ委員会へ報告すると共に対策に当たらなければならない。

（個人所有パソコン等情報機器利用の禁止）

第9条　当社が支給・貸与するパソコン等情報機器以外で業務を行ってはならない。また、個人所有物への情報資産の複写は厳禁とする。

（パソコン等情報機器に導入するソフトウェア）

第10条　当社が支給・貸与するパソコン等情報機器へインストールするソフトウェアについて、事前に情報システム責任者の承認を得なければならない。

（パソコン等情報機器におけるセキュリティ対策の実施）

第11条　通信網を介した社外接続（インターネット、他社ネットワーク）からの不正アクセス及び事業所内のコンピュータウィルス感染を防止するため利用形態に係わらず下記を実施する。

(1) 外部との接続境界には通信のアクセス制御が可能な機器を用いるほか、ファイアウォールによる不要な通信の遮断

(2) パソコン等情報機器を遠隔操作可能なサービス及びソフトウェア等の削除若しくは設定の無効化

(3) ファイル共有機能の停止若しくは設定の無効化

(4) 不要なアカウントの削除

(5) アンチウィルスソフトの導入、常時検知の設定、定義ファイルの最新化、定期的なウィルススキャンの実施

(6) OS、アプリケーションソフトウェアの最新版パッチの適用

(7) 情報システム責任者が承認したソフトウェア以外がインストールされていないことの確認

（パスワード強度と注意事項）

第12条　使用形態に係わらず、パソコン等情報機器を利用する場合は他者が無断で操作できないようパスワード保護を行わなければならない。

(1) 数字、英字（大文字、小文字）、記号などを組み合わせて推測されにくいもの

(2) 桁数は6桁以上とする

(3) 一般に使われている単語や本人の氏名、電話番号、生年月日などから他者に推測されやすい文字列を使用しないこと

(4) パソコン等情報機器（周辺機器含む）若しくは机上などへパスワードを書留めないこと

(5) 他者へパスワードを漏洩させないこと

（パソコン等情報機器の利用形態による注意事項）

第13条　社外へ持ち出さないパソコン等情報機器は、盗難防止チェーン等を使用する。

②　ノートPC等社外へ持ち出すパソコン等情報機器の利用上の注意事項

(1) 原則として社外に持ち出すパソコン等情報機器に、機密文書規定で区分する機密文書を保管してはならない。

(2) 情報資産を社外で利用する場合は、上長の承認を得なければならない。

(3) 他者が無断でパソコン等情報機器を操作できないように保護機能を使用し、情報資産の盗み見に注意して利用しなければならない。

(4) 社外に持ち出すパソコン等情報機器を常時卓上で利用する場合は、盗難防止チェーン等を使用するか、退場時に鍵付き引き出しへの格納を徹底しなければならない。

(5) 社外へ持ち出したパソコン等情報機器を持ち帰り、再度社内ネットワークに接続する場合は、ウィルス感染の有無を確認しなければならない。この際にウィルス感染の事実を確認した場合は、絶対に事業所内ネットワークへ接続してはならない。
また、情報セキュリティ委員会へ迅速に報告するとともに、情報セキュリティ委員会及び情報システム責任者が行う情報事故の調査に協力しなければならない。

③　前号の対策が困難な場合は、情報システム責任者の指示に従い、情報漏洩のリスクを低減する、出来る限りの対策を個別に施さなければならない。

（外部情報記憶媒体の管理）

第14条　持運びが容易な外部情報記憶媒体の業務使用(セキュリティキーとしての使用を除く)は原則禁止とする。但し、デジタルカメラ等で占用的に使用するものについてはこの限りで無いが、用途外使用を禁止し、情報事故に配慮の上、取扱いには充分に注意すること。

尚、保管は情報セキュリティ委員若しくは実行責任者の指示に従うこと。

② やむを得ず外部情報記憶媒体へ情報資産を保存する場合は、理由と使用目的及び期間等を明確にした上で上長の許可を得ること。また、当該記憶媒体はパスワード保護を施さなければならない。実施できない記憶媒体については使用・携帯を禁止する。

③ 外部情報記憶媒体の紛失時は情報事故如何に係わらず、速やかに情報セキュリティ委員会に報告し、指示に従うこと。

（情報記憶媒体の廃棄）

第15条 情報記憶媒体の廃棄を行う際、情報システム責任者が指定したツールによる情報記憶の完全消去、若しくは再生不能な状態に破壊して情報システム責任者の承認を得た上で廃棄しなければならない。

② 情報記憶媒体に機密情報が保管されているかどうかが確認できない場合、その情報が保管されているものとして取り扱わなければならない。

③ 機密情報が保管された情報記録媒体の廃棄を外部業者に委託する場合、情報システム責任者の承認を得なければならない。

（電子メール・インターネットの利用申請）

第16条 電子メール及びインターネットを利用しようとする者は、上長の承認を得て情報システム責任者に申請し、アカウントを取得しなければならない。

（電子メール・インターネット等の利用）

第17条 個人で取得している電子メールアカウント（フリーメール、個人契約プロバイダメール等）で情報資産を送受信してはならない。

② 業務上の利用目的であるものを除く個人情報及び機密文書規定により機密文書区分に定められた情報は電子メールを用いて送信してはならない。

③ 業務上の利用目的である個人情報及び顧客や取引先業者等へ電子メールで送信する添付ファイルは情報セキュリティ委員会の指示に従い暗号化して送信しなければならない。この際に用いるパスワードは『第12条 パスワード強度と注意事項』に準ずるものとする。

（私的利用の禁止）

第18条 パソコン等情報機器及び電子メール・インターネットを私的に利用してはならない。

（Webサービス等への投稿）

第19条 個人情報や<<機密情報>>は公開しないこと。また、違法性のあるコンテンツの投稿、他者に対する誹謗・中傷を含む発言や投稿、顧客情報及び業務に関する情報並びにこれらを類推される可能性がある情報を公開しないこと。

（不正アクセス・他者電子メール等の閲覧の禁止）

第20条 正当な権限無くして、アクセスの制限された他者のコンピュータにアクセスし、又はその設定を変更してはならない。

② 正当な権限無くして、他者の電子メール、コンピュータファイル等を閲覧、変更又は削除してはならない。

（他者の権利侵害の禁止）

第21条 ソフトウェアの違法インストール及び複製を行ってはならない。また、他者が保有する知的情報資産は利用規約の範囲に限り利用可能とする。

② 他者の権利を侵害している恐れのある行為を見かけた際は、実行責任者若しくは情報セキュリティ委員会に報告すると共に、関係者は協議を行い必要な措置を講じなければならない。

（通信回線網に障害を及ぼす行為等の禁止）

第22条 社内外を問わず、通信回線網及びコンピュータサーバ等に障害を与える行為を行ってはならない。

② 業務上の周知事項及び回覧文書等を除き、転送を強要若しくはこれに類する内容のメール送信を行ってはならない。

③ いかなる場合においてもコンピュータウィルスの持込み、頒布、送付を行ってはならない。

（教育の実施）

第23条 情報セキュリティ委員会は教育計画を策定し、教育委員会と連携して本規則の遵守並びに情報事故の防止に関する従業員の知識向上に努める。

（規則に違反した場合の措置）

第24条 当社役員及び従業員が本規則に違反した場合、就業規則に照らして制裁等の処分を受けることがある。

② 派遣労働者等、当社従業員以外の入場者が本規則に違反した場合、入場者の所属する法人の規則による措置を求めるものとする。

（情報事故の対応）

第25条 情報事故が発生した場合、実行責任者若しくは所管情報セキュリティ委員に速やかに報告しなければならない。この際、急報は口頭で差し支えないが、様式：災害・不適合速報により別途書面報告するものとする。

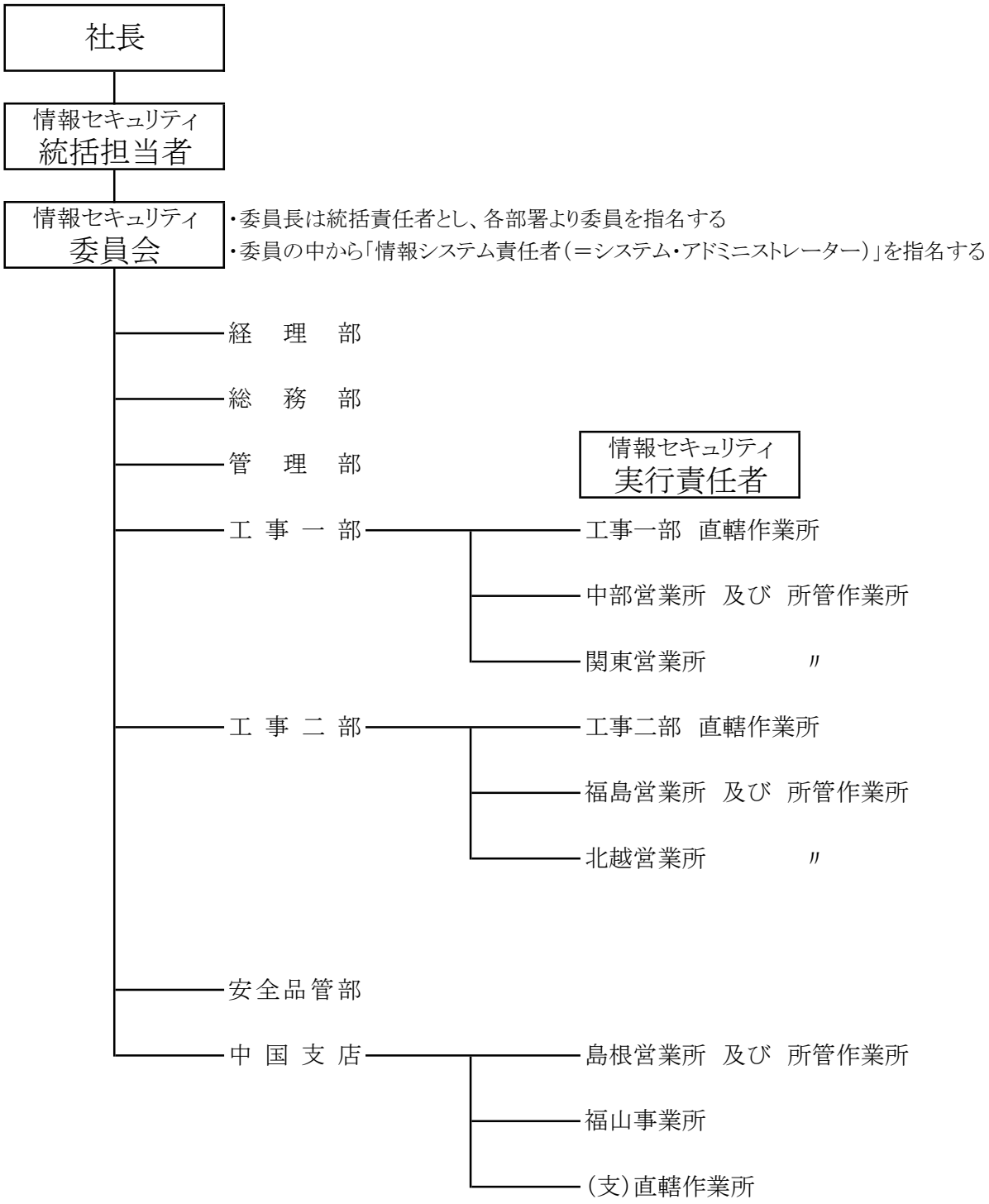
② 情報事故報告を入手した情報セキュリティ委員会は事象を調査・協議し、関係各所への通報及び被害拡大の防止に努め、対応と対策に当たるものとする。

付　　則

第1条 この規程は平成28年12月16日から実施します。

別表

情報セキュリティ管理体制



詳細は「情報セキュリティ管理体制構成名簿」を参照のこと