制定日：2018 年　7月 2日

情報セキュリティ基本方針

株式会社　コスモテック
代表取締役社長 岡田　経

当社は設立以来、ロケット打上げ設備の保全運用や打上げ支援、射場の管理などの宇宙開発関連業務を実施させていただくことにより、わが国の宇宙開発を基盤で支え続け、その発展及び利用に寄与してきました。また、民間の高圧ガス設備の保全や保安検査などの技術サービスの提供を通じて、宇宙開発以外の分野においても幅広く事業を展開することにより企業としての社会的責任を果たし、もって、社会に貢献することを経営理念としております。

当社は、これらの事業を実施するに当たり、お客さまの信頼を得るため、確かな技術力により高品質のサービスを安全確実に提供することは無論のこと、個人情報を含むすべての情報資産の重要性を強く認識し、次のとおり情報セキュリティに関する基本的遵守事項を定め、これに基づき情報の機密保持及び漏洩防止並びに保護に関する施策を実行いたします。

1. 当社に必要な情報セキュリティマネジメントを実施するために ISO27001 に基づくシステムを推進します。

2. 当社が保有する情報資産の価値に応じ、1）機密性、2）完全性及び 3）可用性を勘案して、効果のある人、組織及び技術に関する施策を講じます。

3. 情報セキュリティマネジメントに必要な事項等を周知徹底するため、当社の業務に係る情報資産を取り扱う全ての従業者に対して適切な教育を実施します。

4. 情報セキュリティマネジメントシステムの運用状況を適宜監査し、継続的な改善を行うことにより、情報セキュリティの強化に努めます。

5. 全ての従業者は、情報セキュリティの関連法規、お客さまとのセキュリティに関する契約条項及び社内規定を遵守します。これらに違反した場合は就業規則その他社内規定に基づく罰則を適用します。

6. 経営陣は、情報セキュリティ方針の発行及び維持を通じて、事業目的に沿った明確な情報セキュリティ基本方針を定め、情報セキュリティに対する活動へ支持（意思表明、承認、バックアップ）及び責任を明示します。

情報セキュリティ個別方針

１．情報資産管理

当社の ISMS 適用範囲で使用する情報資産を適切に管理するため、使用する情報資産を洗出し、その重要度に応じた、管理策を選択し、実施する。

管理策を適切に実施するため、対象となる情報資産の責任者を明確にし、重要度に応じたラベリングや取り扱いの許容範囲の設定などを、実施する。

情報資産を ISMS 適用範囲外に持ち出す際の認可プロセスを確立し、実施する。また、持ち出した際の外部での使用におけるリスクを識別し、適切な対策を実施する。

情報資産の処分（廃棄）及び再利用可能な電子媒体、装置等は、その情報資産が不適切に使用されることを防止するため、確実に消去する手順を確立し、実施する。

２．組織的人的セキュリティ対策

組織内の情報セキュリティ活動を確実にするために、全ての関係者の役割・責任を明確にし、関係者間の調整機能や、経営資源導入・変更に関する認可プロセス、リスクコミュニケーション、内部監査などの組織的な対策を確立し、実施する。

全ての関係者に対して、実施する情報セキュリティ対策の内容を理解し、実施することを確実にするための教育・訓練を継続的に実施し、記録を保持する。

全ての関係者は、その関係が変更又は解消される際には、与えられた権限や貸与物が変更・削除又は返却されるように、責任者を明確にし、確実に実施される仕組みを確立し、実施する。

３．アクセス制御

当社の ISMS 適用範囲で管理する情報資産を、不正利用や誤使用などの不適切なアクセスから保護するために、利用者の識別・認証（本人であることを確認）、情報資産へのアクセス権限の適切な設定、不正アクセスの早期発見、アクセス記録の取得などの対策を実施する。

４．暗　号

情報資産の機密性、真正性、完全性を保護するために、情報資産の重要性、可用性及び技術の進歩を考慮して、適切な暗号化技術を適用する。

５．物理的環境的セキュリティ対策

情報資産を保護するために必要な施設及び情報資産に対する不正アクセスを防止するために、物理的セキュリティレベルを定め、そのレベルに従った入退管理策や、火災、洪水、地震、爆発、暴力行為及びその他の自然災害又は人的被害からの物理的な保護対策を実施する。

セキュリティレベルの高い境界内での不正作業や誤作業を防止するための対策を実施する。

パソコンやサーバー等の装置及び装置の稼働を維持するために必要な電源、ケーブル等の設備全般に対して、環境上の脅威、災害、不正アクセスなどから保護するための対策を実施する。

装置を ISMS 適用範囲外に持ち出す際の認可プロセスを確立し、実施する。また、持ち出した際の外部での使用におけるリスクを識別し、適切な対策を実施する。

装置の処分（廃棄）及び再利用可能な装置等は、その情報資産が不適切に使用されることを防止するため、確実に消去する手順を確立し、実施する。

６．通信及び運用管理

重要な情報処理設備の運用においては、不正操作や誤操作を防止するために、職務及び設備の分割、操作手順書の整備などの対策を確立し、実施する。

システムの可用性及び完全性を維持するため、システム容量管理や情報資産のバックアップなどの対策を確立し、実施する。

マルウェア（悪意のあるコード及び認可されないモバイルコードなど）からの保護のために、検出、予防及び回復のための対策（利用者の意識向上の重要性を含めて）を確立し、実施する。

あらゆる情報交換（物理的配送、電子メールなど）において、リスクを認識し、適切な対策を確立し、実施する。

認可されていない情報処理活動の検知及び障害時の対策に使用するため、システム使用状況や作業ログ、障害ログなどを適切に取得し、ログに対する不正アクセスからの保護及び適切な期間の保持を実施する。

７．システムの取得、開発及び保守管理

情報システムの取得、開発及び保守管理のプロセスにおいて、不正行為又は誤作業等に起因する情報セキュリティインシデントの発生を未然に防ぐために、対策方針に従って、環境を整備し、規則を策定して、プロセスを実施する。

情報システムの実装にあたって、情報セキュリティ要件を満たすことを確実にする。

インターネットを介して利用するアプリケーションサービス（電子商取引など）を利用する場合は、そのリスクを認識し、適切な対策を確立し、実施する。

８．供給者関係（外部委託及び第三者の提供するサービス）管理

業務を外部委託する場合及び第三者が提供するサービスを利用する場合に、経営効率の向上を図ると同時に、情報セキュリティを確保するために、供給者に求める情報セキュリティ要求事項を特定し、事前に供給者と合意し、実施する。

また、合意内容の監視及びレビューを適時実施し、必要に応じて合意内容を見直す。

９．情報セキュリティインシデント管理

情報セキュリティ事象（インシデント及びインシデントに繋がるかも知れない弱点）を早期に発見し、適切な対処を迅速に実施するために、情報セキュリティ事象の検知手順、真の原因を除去するための是正処置及び未然防止のための予防処置の手順を明確にし、実施する。

１０．　事業継続管理

当社の ISMS 適用範囲の事業継続に重大な影響を与える情報セキュリティ上の事件・事故が発生した際に、業務を早期に復旧及び継続するための計画（事業継続計画）を策定する。

１１．　順　守

情報セキュリティに関わる法令、規制又は契約上のあらゆる義務、及びセキュリティ上のあらゆる違反を避けるために、関連する事項の洗い出しと対策を実施する。

順守を確実にするために、監査活動に留まらず日常の自主点検や定期的な技術的点検を実施する。

以上