第８回宇宙産業 SWG
参考資料４

民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン　添付資料3

情報セキュリティ関連規程（サンプル）

民間宇宙事業者向けの情報セキュリティ関連規程のサンプルです。本サンプルは IPA「中小企業の情報セキュリティ対策ガイドライン」の付録 5「情報セキュリティ関連規程（サンプル）」[1]をベースに作成しています。本文書は、事業者のセキュリティ基本方針や事業者が対応すべきリスクを踏まえ、事業者が実施する対策を示す規程のサンプルであり、自社の状況に応じて必要な対策を選択し、編集することで、規程を作成・見直しする際に活用することができます。なお本サンプルは、民間宇宙システムにおけるサイバーセキュリティ対策ガイドラインを補足する資料であることから、調達要件に活用することは適当ではなく、具体的な対策立案に当たっては、ガイドライン本編を参照してください。
※**赤字箇所**は、自社の事情に応じた内容（役職名、担当者名など）に書き換えてください。
※青字箇所は、自社の事情に応じた文言を選択してください。
※緑色蛍光箇所は、「中小企業の情報セキュリティ対策ガイドライン第 3 版」から宇宙事業者向けにカスタマイズした箇所を表しております。

目　次

[1] https://www.ipa.go.jp/security/guide/sme/about.html

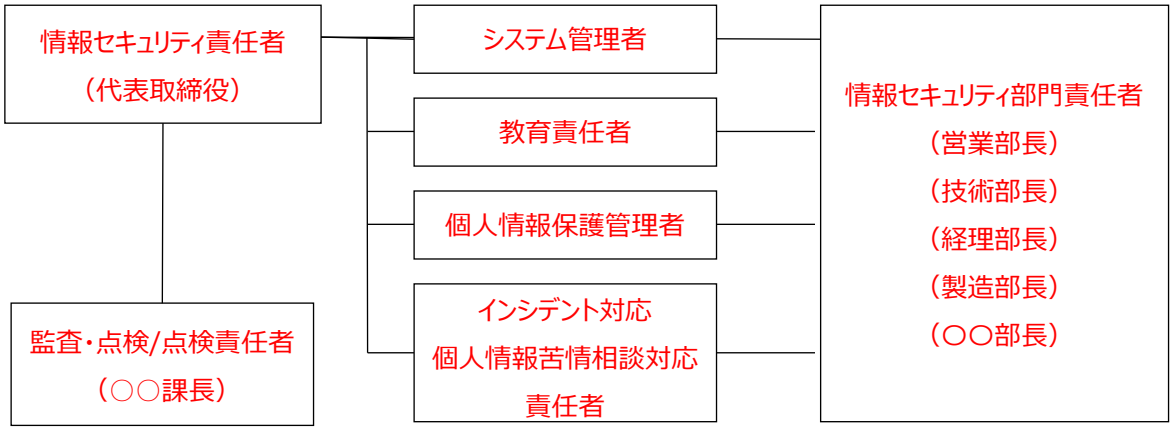
1	組織的対策	改訂日	20yy.mm.dd
適用範囲	全社・全従業員		

1. 情報セキュリティのための組織

経営者等は自社の情報セキュリティに係る最高かつ最終的な権限及び責任を有し、経営者等のリーダーシップのもと、情報セキュリティリスクの管理体制を構築する。情報セキュリティ対策を推進するための組織として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。

役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者。情報セキュリティ対策などの決定権限を有するとともに、全責任を負う。
情報セキュリティ部門責任者	各部門における情報セキュリティの運用管理責任者。各部門における情報セキュリティ対策の実施などの責任を負う。
システム管理者	社内の情報システムに必要な情報セキュリティ対策の検討・導入を行う。
教育責任者	情報セキュリティ対策を推進するために従業員への教育を企画・実施する。
インシデント対応責任者 個人情報苦情相談対応	事故の影響を判断し、対応について意思決定する。 個人情報の取扱いに関して本人からの苦情・相談に対応する。
個人情報保護管理者	個人情報の取扱いについて関連法令を遵守する責任を負う。
監査・点検/点検責任者	情報セキュリティ対策が適切に実施されているか情報セキュリティ関連規程を基準として検証または評価し、助言を行う。

＜情報セキュリティ委員会体制図＞



2. 情報セキュリティ取組みの監査・点検/点検

監査・点検/点検責任者は、情報セキュリティ関連規程の実施状況について、〇月に点検を行い、監査・点検/点検結果を情報セキュリティ委員会に報告する。情報セキュリティ委員会は、報告に基づき、以下の点を考慮し、必要に応じて改善計画を立案する。

●情報セキュリティ関連規程が有効に実施されていない場合は、その原因の特定と改善

●情報セキュリティ関連規程に定められたルールが、対策として不十分または有効でない場合は、情報セキュリティ関連規程の改訂

●情報セキュリティ関連規程に定められたルールが、関連法令や取引先の情報セキュリティに対する要求を満たしていない場合は、情報セキュリティ関連規程の改訂

3. 情報セキュリティに関する情報共有

情報セキュリティ責任者は、新たな脅威及び脆弱性に関する警戒情報及び個人情報の保護に関する情報を専門機関等から適時に入手し、委員会で共有する。

＜専門機関＞

➢独立行政法人情報処理推進機構（略称：IPA）

[情報セキュリティ]

https://www.ipa.go.jp/security/

[ここからセキュリティ]

https://www.ipa.go.jp/security/kokokara/

➢JVN（Japan Vulnerability Notes）

https://jvn.jp/index.html

➢一般社団法人 JPCERT コーディネーションセンター（略称：JPCERT/CC）

https://www.jpcert.or.jp/

➢個人情報保護委員会

https://www.ppc.go.jp/

2	人的対策	改訂日	20yy.mm.dd
適用範囲	全従業員（取締役、社員、派遣社員、パート・アルバイトを含む）		

1. 雇用条件

従業員を雇用する際には秘密保持契約を締結する。

2. 従業員の責務

従業員は、以下を遵守する。

●従業員は、当社が営業秘密として管理する情報及びその複製物の一切を許可されていない組織、人に提供してはならない。

●従業員は、当社の情報セキュリティ方針及び関連規程を遵守する。違反時の懲戒については、就業規則に準じる。

※当社が営業秘密として管理する情報とは、3 情報資産管理　1.1 情報資産の特定と機密性の評価 に示す「情報資産管理台帳」の機密性評価値が 1 以上のものをいう

※編集時注意：懲戒について規定する場合は、以下を参考にしてください。

（厚生労働省「労働契約法のあらまし」から引用）

(1)趣旨

懲戒は、使用者が企業秩序を維持し、企業の円滑な運営を図るために行われるものですが、懲戒の権利濫用が争われた裁判例もみられ、また、懲戒は労働者に労働契約上の不利益を生じさせるものであることから、権利濫用に該当する懲戒による紛争を防止する必要があります。このため、法第 15 条において、権利濫用に該当するものとして無効となる懲戒の効力について規定したものです。

(2)内容

①法第 15 条は、使用者が労働者を懲戒することができる場合であっても、その懲戒が「客観的に合理的な理由を欠き、社会通念上相当であると認められない場合」には権利濫用に該当するものとして無効となることを明らかにするとともに、権利濫用であるか否かを判断するに当たっては、労働者の行為の性質及び態様その他の事情が考慮されることを規定したものです。

②法第 15 条の「懲戒」とは、労働基準法第 89 条第 9 号の「制裁」と同義であり、同条により、当該事業場に懲戒の定めがある場合には、その種類及び程度について就業規則に記載することが義務付けられているものです。

3. 雇用の終了

●従業員は、在職中に交付された業務に関連する資料、個人情報、顧客・取引先から当社が交付を受けた資料又はそれらの複製物の一切を退職時に返還する。

●従業員は、在職中に知り得た当社の営業秘密又は業務遂行上知り得た技術的機密を利用して、競合的あるいは競業的行為を行ってはならない。

4. 情報セキュリティの教育

教育責任者は、以下の点を考慮し、情報セキュリティに関する周知・教育計画を年度単位で立案す

る。

対象者：経営者等

テーマ：以下は必須とする。

- 組織の内部不正対策に関する方針
- 重要情報の取扱い等の手順

対象者：全従業員

テーマ：以下は必須とする。

- 情報セキュリティ関連規程の説明（入社時、就業時）
- 最新の脅威に対する注意喚起（随時）
- 関連法令の理解（関連法令の公布・施行時）
- 個人情報の取り扱いに関する留意事項

5. 人材育成

教育責任者は、以下に挙げる推奨資格の取得による従業員の情報セキュリティに対する意識向上を年度単位で計画する。計画には関連テキストの配付、公開セミナーの受講、受験費用の予算化を含むこととする。

＜情報セキュリティに関わる推奨資格＞

IPA　情報処理技術者試験・情報処理安全確保支援士試験

- 情報セキュリティマネジメント試験
- システム監査技術者試験
- 情報処理安全確保支援士試験

3	情報資産管理	改訂日	20yy.mm.dd
適用範囲	全社・全従業員		

1. 情報資産の管理

1.1 情報資産の特定と機密性・完全性・可用性の評価

当社事業に必要で価値がある情報及び個人情報（以下「情報資産」という）を特定し、「情報資産管理台帳」に記載する。情報資産の機密性は、以下の基準に従って評価し、特定の情報については、アクセスを認められた者だけがアクセスできるようにする。

機密性 3：極秘	●法律で安全管理が義務付けられている ●守秘義務の対象として指定されている ●限定提供データ（一定の条件を満たす特定の外部者に提供することを目的とする情報）として指定されている ●営業秘密（秘密として管理されているもの）として指定されている ●漏えいすると取引先や顧客に大きな影響がある ●漏えいすると事業の継続及び推進が困難になる。
機密性 2：社外秘	漏えいすると事業の継続・推進に支障を及ぼすおそれがある
機密性 1：公開	漏えいしても事業の継続・推進にほとんど影響はない

『人工衛星等の打上げ及び人工衛星の管理に関する法律』、『衛星リモートセンシング記録の適正な取扱いの確保に関する法律』、『特定秘密の保護に関する法律』等をはじめとし、自社が扱う情報の内、法律や訓令に基づく取扱いが求められる情報等、別途定められる秘匿性の高い非公知の情報については、当該法、運用基準、省庁通達等に則った適切な保護措置等を講じる。

情報資産の完全性は、以下の基準に従って評価し、必要時に必要な情報へのアクセスを可能にする。

完全性 2	改ざん、誤びゅう又は破損により、事業の継続・推進に支障を及ぼすおそれがある
完全性 1	改ざん、誤びゅう又は破損により、事業の継続・推進にほとんど影響はない

情報資産の可用性は、以下の基準に従って評価し、情報へのアクセスを認められた範囲内において必要時に必要な情報へのアクセスを可能にする。

可用性 2	滅失、紛失又は当該情報が利用不可能であることにより、事業の継続・推進に支障を及ぼすおそれがある
可用性 1	滅失、紛失又は当該情報が利用不可能であることにより、事業の継続・推進にほとんど影響はない

1.2 情報資産の分類の表示

情報資産の機密性は以下の方法で表示する。

●電子データ：保存先サーバーのフォルダー名に表示

●書類：保管先キャビネット、ファイル、バインダーに表示

表示が困難な場合は、「情報資産管理台帳」に機密性評価値を表示する。

1.3 情報資産の管理責任者

情報資産の取り扱いに関する情報セキュリティの運用管理責任者は、当該情報資産を主に利用する部門長とする。

1.4 情報資産の利用者

情報資産の利用者の範囲は、「情報資産管理台帳」の利用者範囲欄に示された部門に従事する従業員とする。

1.5 情報資産の適切な利用

関係法令に基づき、特定の記録（例：衛星リモートセンシング記録）を加工する場合において、当該加工を適切に行うために必要な措置を講じる。

2. 情報資産の社外持ち出し

情報資産を社外に持ち出す場合には、以下を実施する。

●社外秘の場合は所属部門長の許可を得る。

●極秘の場合は代表取締役の許可を得る。

●ノートパソコンのハードディスクに保存して持ち出す場合は、ハードディスク/フォルダー/データを暗号化する。

●スマートフォン、タブレットに保存して持ち出す場合は、セキュリティロックを設定する。

●USB メモリ、HDD 等の電子媒体に保存して持ち出す場合は、不要データは全て完全消去専用ツールで消去し、持ち出すデータを暗号化する。

●USB メモリ等の小型電子媒体は、大きなタグを付ける/ストラップで体やカバンに固定する/落としてもすぐに分かるように鈴を付ける。

●屋外でネットワークへ接続して極秘又は社外秘の情報資産を送受信する場合は、暗号化する。

●携行中は常に監視可能な距離を保つ。

3. 媒体の処分

3.1 媒体の廃棄

社外秘又は極秘の情報資産を廃棄する場合は以下の処分を行う。

書類・フィルム	細断/溶解/焼却
USB メモリ・HDD・CD・DVD	破壊/細断/完全消去

	※OS による削除・クイックフォーマットは不可

3.2 媒体の再利用

社外秘又は極秘の情報資産を保存した媒体を再利用する場合は、以下の処分を行う。

書類	裏紙再利用禁止
USB メモリ・HDD・CD-RW ディスク・DVD-RW ディスク	完全消去後再利用 ※OS による削除・クイックフォーマットは不可
CD-R・DVD-R	再利用不可

4.バックアップ

4.1 バックアップ取得対象

システム管理者は、以下の機器で処理するデータのバックアップを定期的に取得する。

機器名	対象	方法	保管先
ファイルサーバー	ユーザーファイル	Windows Server バックアップ	NAS サーバー
給与計算システム	アプリケーションデータ	ファイルコピー	専用外付け HDD(暗号化機能付)
会計システム	アプリケーションデータ	アプリケーションバックアップ機能	クラウドバックアップサービス
○○管理システム	アプリケーションデータ	同期ツール	外付け HDD
Web サーバー	ホームページ	同期ツール	NAS サーバー

4.2 バックアップ媒体の取り扱い

バックアップに利用した機器及び媒体の取り扱いは以下に従う。

＜保管＞

●可搬電子媒体：施錠付きキャビネットに保管

●NAS サーバー：施錠付きサーバーラックに収納

＜廃棄・再利用＞

●「3.媒体の処分」に従う

4.3 クラウドサービスを利用したバックアップ

クラウドサービスを利用し、外部のサーバーにバックアップを保存する場合は、情報セキュリティ責任者の許可を得て導入する。

＜サービス要件＞

●サービス提供者のサービス利用約款、情報セキュリティ方針、セキュリティ対策の実施状況が、当社の情報セキュリティ関連規程やサービス要件に適合している。

●当社事業所がある地域で発生する震災、水害等の影響を受けない地域の施設であること。

●バックアップが保管される国又は地域が、関係法令に基づき、制限されていない国又は地域に所在するよう確認すること。

4	アクセス制御及び認証	改訂日	20yy.mm.dd
適用範囲	情報資産の利用者及び情報処理施設		

1. アクセス制御方針

機密性 3 及び機密性 2 に該当する情報資産を扱う情報システム又はサービスに対するアクセス制御は以下の方針に基づいて運用する。対象となるシステム等は「9.1 アクセス制御対象情報システム及びアクセス制御方法」に記載する。

●データ及びシステムに対する論理的なアクセスの制御を実施するために必要な措置を定めたアクセス制御方針を作成する。

●アクセス制御方針は、システム管理者が作成し、統括者の承認を得るものとする。

●「情報資産管理台帳」の利用者範囲に基づき、利用者の業務・職務の遂行上必要最低限かつ正当な権限を有する者のみにアクセス権を付与する。

●特定の情報資産へのアクセス権が、同一人物に集中することで発生し得る不正行為等を考慮し、複数名に分散してアクセス権を付与する。

●機密性の段階に応じて、本人だけが所有する要素及び本人の持つ生体的要素のうち複数の異なる要素を認証する（多要素認証）等、必要な認証機能を導入する。

『人工衛星等の打上げ及び人工衛星の管理に関する法律』、『衛星リモートセンシング記録の適正な取扱いの確保に関する法律』、『特定秘密の保護に関する法律』等をはじめとし、自社が扱う情報の内、法律や訓令に基づく取扱いが求められる情報等、別途定められる秘匿性の高い非公知の情報については、当該法、運用基準、省庁通達等に則った適切な保護措置等を講じる。

2. 利用者の認証

機密性 3 及び機密性 2 に該当する情報資産を扱う社内情報システムは、以下の方針に基づいて利用者の認証を行う。認証方法等は「9.2 利用者認証方法」を参照のこと。

●利用者の認証に用いるアカウントは、利用者 1 名につき 1 つを発行する。

●同一アカウントの他者との共有および複数の利用者が共有するアカウントの発行を禁止する。

●システムへのログオン試行回数の上限を定める。上限値を超えた場合は、当該ログオン試行を行ったアカウントを自動的にロックし、ロック時から定められた時間が経過するまで、ログオンの再試行が実施できないようにする。

3. 利用者アカウントの登録

利用者の認証に用いるアカウントは、代表取締役又は情報セキュリティ責任者の承認に基づき登録する。アカウント名の設定条件は「9.3 利用者アカウント・パスワードの条件」を参照のこと。

4. 利用者アカウントの管理

機密性３及び機密性２に該当する情報資産を扱うシステムの利用者について、アカウントの利用状況（利用者名及び利用開始日時）を記録する。

また、退職、異動及び職内容の変更などの事由により利用者の認証に用いるアカウントが不要になる場合、システム管理者は、当該アカウントの削除又は無効化を、当該アカウントが不要になった日の翌日までに実施する。

5. パスワードの設定

利用者の認証に用いるパスワードは、以下に注意して設定する。パスワードの設定条件は、「9.3 利用者アカウント・パスワードの条件」を参照のこと。

●十分な強度のあるパスワードを用いる。

●他者に知られないようにする。

6. 従業員以外の者に対する利用者アカウントの発行

当社の従業員以外の者にアカウントを発行する場合は、代表取締役又は情報セキュリティ責任者の承認を得たうえで、秘密保持契約を締結する。

7. 端末の識別による認証

社外秘又は極秘の情報資産を扱う情報システムに、ネットワーク接続によりアクセスする際の認証方式として、端末の識別による認証を用いる。認証方法等は「9.4 端末認証方法」を参照のこと。

8. 端末のタイムアウト機能

社外秘又は極秘の情報資産を扱う情報システムの端末又は情報機器を、アカウントを付与していない者が接触可能な場所に設置する場合は、接続時間制限やタイムアウト等機能を利用する。

9. 標準設定等

9.1 アクセス制御対象の情報システム及びアクセス制御方法

アクセス制御対象システム・サービス	アクセス制御方法
ファイルサーバー	Windows Active Directory
給与計算システム	アプリケーションのユーザー認証
○○管理システム	アプリケーションのユーザー認証
メールサーバー（ホスティングサービス）	ホスティングサービスのユーザー認証
Web サーバー（ホスティングサービス）	ホスティングサービスのユーザー認証
社内無線 LAN	ルーターの端末認証

アクセス制御対象 宇宙システム	サブシステム	アクセス制御方法
衛星運用システム	ネットワーク運用・制御システム	○○○○
	衛星管制システム	○○○○
	○○○○	○○○○
衛星データ利用システム （衛星データ利用サービス）	データ送受信アンテナ制御システム	○○○○
	ネットワーク運用・制御システム	○○○○
	○○○○	○○○○
開発・製造システム	○○○○	○○○○

※自社の業務形態や状況に合わせてテーラリングして利用ください。

9.2 利用者認証方法

情報システム	利用者認証方法
ファイルサーバー	Windows ログオン認証：アカウント名・パスワード
給与計算システム	アプリケーションのユーザー認証：ID・パスワード
○○管理システム	アプリケーションのユーザー認証：ID・パスワード

利用者認証の対象宇宙システム・サービス	サブシステム	利用者認証方法
衛星運用システム	ネットワーク運用・制御システム	・ID・パスワード ・多要素認証 ・（複数間で利用するアカウントによる接続の場合）個人認証
	衛星管制システム	
	○○○○	○○○○
衛星データ利用システム （衛星データ利用サービス）	データ送受信アンテナ制御システム	・ID・パスワード ・多要素認証 ・（複数間で利用するアカウントによる接続の場合）個人認証
	ネットワーク運用・制御システム	
	○○○○	○○○○
開発・製造システム	○○○○	○○○○

※自社の業務形態や状況に合わせてテーラリングして利用ください。

9.3 利用者アカウント・パスワードの条件

	特権アカウント	一般アカウント
アカウント名	●推奨：推測困難であるもの ＜禁止アカウント名＞ WindowsOS：administrator、admin LinuxOS：root ●1 つの特権アカウント名を 2 名以上で共用しない ●Guest 用アカウントは無効化する	●従業員番号 ●従業員コード
パスワード	＜パスワードに使う文字＞ ●12 文字以上 ●当人の名前、電話番号、誕生日等、他者が推測できるものを使わない ●アルファベット大文字･小文字、数字、記号の全てを含む ●辞書に含まれる単純な語を使わない ＜パスワードの管理＞ ●システムにパスワードポリシー設定機能がある場合は本項の条件を設定する ●パスワードを変更する場合は過去 1 年間に使用したパスワードと同一パスワードを使用しない ●ロックアウトのしきい値は 3 回、時間は 6 時間に設定する ●定められた期間以内に変更する ●紙等への記載又は記憶媒体への保存を行わない	＜パスワードに使う文字＞ ●10 文字以上 ●当人の名前、電話番号、誕生日等、他者が推測できるものを使わない ●アルファベット大文字･小文字、数字、記号の全てを含む ●辞書に含まれる単純な語を使わない ＜パスワードの管理＞ ●システムにパスワードポリシー設定機能がある場合は本項の条件を設定する ●パスワードを変更する場合は過去 1 年間に使用したパスワードと同一パスワードを使用しない ●ロックアウトのしきい値は 5 回、時間は 1 時間に設定する

9.4 端末認証方法

情報システム	端末認証方法
社内無線 LAN	Wi-Fi ルーターに端末の MAC アドレスを登録
○○管理システム	パソコンにデジタル証明書をインストール

5	物理的対策	改訂日	20yy.mm.dd
適用範囲	全事業所		

1. セキュリティ領域の設定

当社内で扱う情報資産の重要度に応じて社内の領域を区分する。区分した領域内では以下を実施する。なお、『人工衛星等の打上げ及び人工衛星の管理に関する法律』、『衛星リモートセンシング記録の適正な取扱いの確保に関する法律』、『特定秘密の保護に関する法律』等をはじめとし、自社が扱う情報の内、法律や訓令に基づく取扱いが求められる情報等、別途定められる秘匿性の高い非公知の情報については、当該法、運用基準、省庁通達等に則った適切な保護措置等を講じる。

レベル 1 領域	本社受付・応接スペース・商談室・倉庫
機密性	扱う情報は、漏えいしても事業の継続・推進にほとんど影響はなく公開可能（機密性 1）である。
利用者	従業員、社外関係者、部外者が立ち入り可
施錠	最終退室者による施錠
設置可能情報機器	プロジェクター、ホワイトボード
制限事項	未使用時に社外秘又は極秘の情報資産の放置禁止
部外者管理	従業員の許可を受けて入室可能
管理記録	ー
侵入検知	ー
来客用名札	着用不要
火災対策	火災検知器、消火器設置

レベル 2 領域	本社執務室・社長室・書庫・工場（開発、製造システム）・営業所
機密性	扱う情報は、事業の継続・推進に支障を及ぼすおそれがあり社外秘（機密性 2）である。
利用者	従業員以外の入室は従業員の許可又はエスコートが必要
施錠	最終退室者による施錠及び警備会社への通報装置作動
設置可能情報機器	プロジェクター、ホワイトボード、パソコン、複合機、電話機 LAN ケーブルハブ、無線 LAN 中継器、ルーター、制御ネットワーク機器
制限事項	情報機器・設備の無断操作禁止・無断持出し禁止
部外者管理	従業員/受付守衛/総務部受付の許可を受けて入室可能

管理記録	入退室を所定様式に記録
侵入検知	センサーによる警備会社通報
来客用名札	要着用
火災対策	スプリンクラー、消火器設置

レベル 3 領域	サーバールーム/鍵付きサーバーラック、衛星運用システム（ミッションコントロールシステム等）
機密性	扱う情報は、漏えいすると事業の継続・推進に支障を及ぼすおそれがあり機密性 3（極秘）である。
利用者	あらかじめ許可された者
施錠	常時施錠及び警備会社への通報装置作動、鍵の管理責任者
設置可能情報機器	サーバー、ルーター等のネットワーク機器
制限事項	情報機器・設備の無断操作禁止・無断持出し禁止 スマートフォン、USB メモリ、HDD、CD-R、デジタルカメラその他の情報記憶媒体の無断持込み禁止
部外者管理	保守・点検時等に登録者のエスコート付で入室可能
管理記録	入退室を所定様式に記録、監視カメラによる記録
侵入検知	センサーによる警備会社通報
来客用名札	要着用
火災対策	不活性ガス系消火設備、純水ベース消火器、空調設備

2. 関連設備の管理

情報機器に関連する設備は以下を設置する。

●サーバーは施錠付き専用ラックに収納する。

●LAN ケーブルは回線盗聴防止のため床下配線とする。

衛星運用業務を行う施設・システムは以下を設置する。

●特定設備に対する専用室（サーバ室、計算機室、通信回線装置室等）を設け、入退管理を実施する。

●ハードウェアや記憶媒体は施錠付き専用ラック又はセキュリティワイヤ等により固定・施錠する。

●固定が困難な場合は、業務上使用しないものをロッカー等に保管し施錠する。

●LAN ケーブルは回線盗聴防止のため床下配線とする。

なお、衛星運用システムが他のシステムの一部に所在する場合には、当該システムの管理者との連絡手段と体制を確認・整備する対策を実施する。

3. セキュリティ領域内注意事項

セキュリティ領域では区分にかかわらず以下の点に注意する。

●複合機、プリンタに原稿、印刷物を放置しない。

●複合機、プリンタの運用を終了する際は、電磁的記録を媒体の全てを抹消する。

●FAX 送信時には誤送信防止のため宛先を複数回確認する。

●ホワイトボードは利用後に消去する。

●室内での撮影、録音は禁止する。業務上必要な場合は、情報セキュリティ部門責任者の許可を得ること。

●応接室、会議室内及びエレベータ内では会話の盗み聞きを防止するよう配慮する。

●外線受話時の際に相手が不審な場合は、従業員の個人情報を伝えてはならない。

●部外者を見かけた場合は用件を確認する。

4. 搬入物の受け渡し

郵便物及び宅配便の受取り・受け渡しは、以下を介して行う。

＜本社＞

●郵便物：本社施錠ポスト/書留便の場合は総務部

●宅配便：本社 1 階受付

6	Ｉ Ｔ機器利用	改訂日	20yy.mm.dd
適用範囲	業務で利用する情報機器		

1. ソフトウェアの利用

1.1 標準ソフトウェア

業務に利用するパソコンには、当社の標準ソフトウェアを導入する。当社の標準ソフトウェア以外のソフトウェアを導入する場合は、システム管理者の許可を得たうえで導入する。標準ソフトウェアは「6.1 標準ソフトウェア」を参照のこと。また、『人工衛星等の打上げ及び人工衛星の管理に関する法律』、『衛星リモートセンシング記録の適正な取扱いの確保に関する法律』、『特定秘密の保護に関する法律』等をはじめとし、自社が扱う情報の内、法律や訓令に基づく取扱いが求められる情報等、別途定められる秘匿性の高い非公知の情報については、当該法、運用基準、省庁通達等に則った適切な保護措置等を講じる。

1.2 ソフトウェアの利用制限

システム管理者は、利用者の業務に不要な機能をあらかじめ取除いて提供する。従業員は、業務に不要なシステムユーティリティやインストールされているソフトウェアを利用しない。

＜利用を禁止するソフトウェア＞

●インターネットを利用して、不特定多数のコンピュータ間でファイルをやりとりできるソフトウェア（ファイル共有ソフト）。

●不審なベンダーが提供するソフトウェア。

●正規ライセンスを取得していないソフトウェア。

必要に応じて、インストール・実行してはならないソフトウェアのリスト（ブラックリスト）もしくは、インストール・実行してもよいソフトウェアのリスト（ホワイトリスト）を作成し、リストに基づいてインストール・実行を管理する。

1.3 ソフトウェアのアップデート

従業員は、業務で使用するソフトウェアを最新の状態で利用する。最新の状態で利用する方法は「6.2 ソフトウェアのアップデート方法」を参照のこと。

1.4 ウイルス対策ソフトウェアの利用

1.4.1 ウイルス検知

従業員は、以下の方法でウイルス検知を行う。

●ネットワーク経由で入手するファイルは、自動検知機能を有効にしてウイルス検知を実施する。

●電子媒体を用いてファイルの受け渡しを行う場合は、媒体内のファイルにウイルス検知を実施す

る。

●システム管理者は、必要に応じて EDR 導入を検討する。

EDR の運用や管理にあたってはセキュリティに関する知識が求められることから、自社の状況を踏まえて、外部監視 SOC との契約を検討し、対象のネットワークやサーバー機器などのウイルス検知に関する運用体制を整備する。

1.4.2 ウイルス対策ソフト定義ファイルの更新

従業員は、パソコン・スマートフォン・タブレットに導入したウイルス対策ソフトウェアの定義ファイルを随時更新する。持ち出し用ノートパソコンは利用時に定義ファイルの更新を確認する。定義ファイルの更新方法は「6.3 ウイルス対策ソフトウェアの定義ファイルの更新方法」を参照のこと。

1.4.3 社外機器の LAN 接続

当社が管理するパソコン及びサーバー以外の機器を社内 LAN に接続することを禁止する。業務上必要な場合は、システム管理者の許可を得たうえで、当該機器にインストールされているウイルス対策ソフトの定義ファイルを最新版に更新し、当該機器のフルスキャンを実行し、ウイルスが検知されないことを確認してから接続する。

1.5 ウイルス対策の啓発

システム管理者は、適宜ウイルスに関する情報を収集し、重大な被害を与えるウイルスに対しては、対応策及び対応に必要な修正プログラムを社内に公開及び通知する。従業員は、感染防止策が通知された場合は、速やかに実施完了すること。

2. ＩＴ機器の利用

従業員は、業務に利用するパソコン・タブレット・スマートフォンには、ログインパスワードを設定する。利用するときには以下を実行する。

●ログインパスワードを他者の目に触れる所に書き記さない。

●屋外で利用する場合は、他者が画面を盗み見可能な環境で利用しない。

●退社時又は使用しないときには電源を切り、ノートパソコン・タブレット・スマートフォン・USB メモリ、HDD、CD 等の電子媒体は施錠保管する。

3. クリアデスク・クリアスクリーン

3.1 クリアデスク

従業員は、社外秘又は極秘の書類及び電子データを保存したノートパソコン、USB メモリ、HDD、CD 等の持ち運び可能な機器や媒体の扱いについて、以下のようにクリアデスクを徹底する。

●利用時以外には机上に放置しない。

●離席時に書類を伏せる、引き出しに入れる等する。

●退社時又は使用しないときには机の引き出しに保管し、施錠する。

3.2 クリアスクリーン

従業員は、離席時に以下のいずれかによりパソコンの画面をロックし、クリアスクリーンを徹底する。

●スクリーンセーバー起動時間を 5 分以内に設定し、パスワードを設定する。

●スリープ起動時間を 5 分以内に設定し、解除時のパスワード保護を設定する。

●離席時に［Windows］＋［L］キーを押してコンピュータをロックする。

●ログオフ状態ではシステム操作画面は非表示に設定する。退社時又は使用しないときにはパソコンの電源を切る。

●スマートフォン･タブレットを外出先で利用する場合は、他者が盗み見できる環境で利用しない。

4. インターネットの利用

4.1 ウェブ閲覧

システム管理者は、ウイルス等の悪意のあるソフトウェアに感染するおそれがあると認められる有害ウェブサイトは社内周知/ウェブフィルタリングソフトを使用して、従業員の閲覧を制限する。従業員は、業務でウェブ閲覧を行う場合は以下に注意する。

●公序良俗に反するサイトへのアクセスを禁止する。

●不審なサイトへのアクセス及び社用メールアドレス登録を禁止する。

●パスワードをブラウザに保存しない。業務で特定のウェブサービスを利用する場合で、パスワードをブラウザに保存する必要があるときはシステム管理者の許可を得る。

●業務上、個人情報(メールアドレス、氏名、所属等)を入力する場合は、通信の暗号化、接続先の実在性等を十分に確認したうえで行う。

●信頼できるサイトから署名付きのモバイルコードをダウンロードする場合を除き、モバイルコード(クライアントパソコン側で動作するプログラム)を実行しない。

4.2 オンラインサービス

従業員は、インターネットで提供されているサービスを業務で利用する場合は、システム管理者の許可を得る。利用する際には以下に注意する。

＜インターネットバンキング・電子決済＞

●インターネットバンキングを利用する際には、自分で設定したブックマークや銀行が提供する専用アプリケーションソフトを用いる。

●電子決済を利用する際には、SSL/TLS による通信暗号化を採用しているサイトを利用する。

●電子メールに記載されているリンクや、他のウェブサイト等に設置されているリンクは、偽サイトへの誘導である可能性があるためアクセスしない。

＜オンラインストレージ＞

●社外秘又は極秘の情報資産を保存する場合は、システム管理者の許可を得る。

●メールアドレスの登録が必要な場合は社用メールアドレスを登録する。
●セキュリティポリシーを公表していないサービスの利用は禁止する。
●不審なベンダーが提供しているサービスの利用を禁止する。

4.3 SNS の個人利用

●当社の業務に関わる情報の書き込みは行わない。
●取引先従業者と SNS 上で私的に交流する場合、双方の立場をわきまえ、社会人として良識の範囲で交流する。
●SNS 用のアプリケーションが提供するセキュリティ設定を行い、アカウントの乗っ取りやなりすましに注意する。
●使用するパソコン、スマートフォン、タブレット上のデータ、写真、位置情報が、予期せず公開される可能性のあることに注意する。

4.4 電子メールの利用

従業員は、業務で電子メールを利用する際には以下を実施する。

＜誤送信防止＞

●電子メールソフトの即時送信機能を停止する。

＜メールアドレス漏えい防止＞

●同報メール（外部の多数相手に同時に送信するとき）を送信する場合は、宛先（TO）に自分自身のアドレスを入力し、BCC で複数相手のアドレスを指定する。

＜傍受による漏えい防止＞

●社外秘又は極秘の情報資産を送信する場合は、メール本文ではなく添付ファイルに記載し、ファイルを暗号化して送信する。

＜添付ファイル暗号化の方法＞

●パスワード保護の設定又はパスワード付きの ZIP ファイルにする。/パスワードは先方とあらかじめ決めておくか電話で知らせるなど、パスワードが傍受されないよう配慮する。

＜クラウド型メールの利用＞

●業務でクラウド型メールを利用する場合は、システム管理者の許可を得る。
●システム管理者から許可されたパソコン以外で、メールサーバーからのメールの取り出し及びエクスポートを禁止する。

＜禁止事項＞

●業務に支障をきたすおそれがある使用。
●私用電子メールサーバーへの接続。
●私用メールアドレスへの転送。
●受信メールの HTML 表示（テキスト形式に変換して表示）。
●HTML 形式メールの中に含まれる不正なコードを実行しないようテキスト形式で表示する。

4.5 ウイルス感染の防止

標的型攻撃メール等によるウイルス感染を防止するため、以下の内容に複数合致する場合は十分に注意し、添付ファイルを開く、又はリンクを参照するなどしない。受信した場合は、システム管理者に報告し、システム管理者は社内に注意を促す。

メールのテーマ	①知らない人からのメールだが、メール本文のURLや添付ファイルを開かざるを得ない内容 ·新聞社や出版社からの取材申込や講演依頼 ·就職活動に関する問い合わせや履歴書送付 ·製品やサービスに関する問い合わせ、クレーム ·アンケート調査 ②心当たりのないメールだが、興味をそそられる内容 ·議事録、演説原稿などの内部文書送付 ·VIP 訪問に関する情報 ③これまで届いたことがない公的機関からのお知らせ ·情報セキュリティに関する注意喚起 ·インフルエンザ等の感染症流行情報 ·災害情報 ④組織全体への案内 ·人事情報 ·新年度の事業方針 ·資料の再送、差替え ⑤心当たりのない、決裁や配送通知（英文の場合が多い） ·航空券の予約確認 ·荷物の配達通知 ⑥IDやパスワードなどの入力を要求するメール ·メールボックスの容量オーバーの警告 ·銀行からの登録情報確認
差出人のメールアドレス	①フリーメールアドレスから送信されている ②差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なる
メールの本文	①日本語の言い回しが不自然である ②日本語では使用されない漢字（繁体字、簡体字）が使われている ③実在する名称を一部に含むURL が記載されている ④表示されているURL（アンカーテキスト）と実際のリンク先のURLが異なる（HTML メールの場合） ⑤署名の内容が誤っている ·組織名や電話番号が実在しない

	･電話番号がFAX 番号として記載されている
添付ファイル	①ファイルが添付されている ②実行形式ファイル(exe/scr/cplなど)が添付されている ③ショートカットファイル(lnkなど)が添付されている ④アイコンが偽装されている ･実行形式ファイルなのに文書ファイルやフォルダーのアイコンとなっている ⑤ファイル拡張子が偽装されている ･二重拡張子となっている ･ファイル拡張子の前に大量の空白文字が挿入されている ･ファイル名にRLOが使用されている

5.私有ＩＴ機器・電子媒体の利用

5.1 利用の可否

従業員個人が所有するパソコン、タブレット、スマートフォン、携帯電話等のＩＴ機器及びUSBメモリ、HDD、CD等の電子媒体を業務で利用する場合は、システム管理者の許可を得る/利用することを禁止する。

※編集時注意:利用することを禁止する場合は、5.1～5.3は削除してください。

5.2 利用開始時

利用を開始する前に利用する本人が以下を実行する。

●システム管理者が指定するウイルス対策ソフトウェアをインストールし、定義ファイルを更新する。

●ハードディスク、電子媒体に対してウイルスチェックを行う。

●業務に支障が出る可能性があるソフトウェアを削除する。

●当社で契約したサービス以外のWi-Fiスポットの利用は禁止する。

5.3 利用期間中

利用期間中は、利用するＩＴ機器や電子媒体に以下に該当する機能がある場合には実行する。

●ウイルス対策ソフトウェアの定義ファイルを常に最新版に更新する。

●OSやアプリケーションソフトのアップデートが通知されたら速やかに実施する。

●社内LANへのリモート接続は禁止する/する場合はシステム管理者の許可を得る。

※編集時注意:接続を禁止する場合は、5.1～5.3は削除してください。

●社外から社内LANにリモートで接続する場合は以下を遵守する。

●システム管理者の許可を受け指定された方法で接続する。

●画面の盗み見、不正操作等を防ぐよう、適切な環境で行う。

●端末機器から離れる場合は、端末機器を停止するか他者が利用できないようにする。

●リモート接続で利用する端末機器を紛失した場合は、直ちにシステム管理者に連絡し指示に従う。
●社用メールアドレスで受信したメールを従業員個人のアドレスに転送することを禁止する。
●社内で利用したデータを従業員個人のアドレスに送信することを禁止する。
●社外秘又は極秘の情報資産の保存を禁止する。
●以下のアプリケーションソフトのインストールと利用を禁止する。
·機器ベンダーの公式な公開場所（App Store、Google Playなど）以外から提供されるもの
·不審なベンダーが提供するもの
·正規ライセンスを取得していない違法なもの
●会社で契約したサービス社外の Wi-Fi サービスの利用を禁止する。
●自宅や屋外で利用する場合は以下を遵守する。
●信頼できる通信回線のみを利用する。
●機器は原則として勤務時間のみ稼働させる。
●不審なメールの受信など、情報セキュリティで不安がある場合はシステム管理者に問い合わせる。

5.4 社内での利用

利用期間中にＩＴ機器や電子媒体を社内に持ち込む場合は、システム管理者の許可を得る。社内で利用する場合は以下を実行する。/ことを禁止する。

※編集時注意:社内持ち込みを禁止する場合は、以下の箇条を全て削除してください。

●社内 LAN への接続は禁止する/する場合はシステム管理者の許可を得る。
●充電を除き、社内のパソコンやサーバーへの接続は禁止する。

5.5 利用終了時

利用を終了する際には、システム管理者が指定するツールを使用してＩＴ機器業務で利用したデータを完全に消去し、復元できない状態にしてシステム管理者の了解を得る。

6. 標準等

6.1 標準ソフトウェア

種別	名称	開発・販売元	バージョン
パソコン OS	Windows	Microsoft	○○以降
オフィス系ソフト	Office	Microsoft	○○以降
電子メール	Outlook	Microsoft	○○以降
パソコン用 ウイルス対策	○○○○	○○社	Ver.○以降
スマートフォン用 ウイルス対策	○○○○	○○社	Ver.○以降
ブラウザ	○○○○	○○社	Ver.○以降
シミュレーション	○○○○	○○社	Ver.○以降

種別	名称	開発・販売元	バージョン
ソフト			
○○○○	○○○○	○○社	Ver.○以降

6.2 ソフトウェアのアップデート方法

種別	名称	開発・販売元	アップデート方法
パソコン OS	Windows	Microsoft	Windows Update の自動更新機能を有効にする
業務用ソフト	Office	Microsoft	Windows Update の自動更新機能を有効にする
	Adobe Reader	Adobe	自動アップデートを有効にする。
ブラウザ	○○○○	○○社	○○○○
スマートフォン OS	Android	Google	機種毎の情報を常に調べて必要に応じて対応する。
	iOS	Apple	iOS アップデート

6.3 ウイルス対策ソフトウェアの定義ファイルの更新方法

種別	名称	開発・販売元	アップデート方法
パソコン用ウイルス対策	○○○○	○○社	定義ファイル更新方法を自動に設定する
スマートフォン用ウイルス対策	○○○○	○○社	定義ファイル更新方法を自動に設定する

7	ＩＴ基盤運用管理	改訂日	20yy.mm.dd
適用範囲	サーバー・ネットワーク及び周辺機器		

1. 管理体制

システム管理者は、ＩＴ基盤の運用に当たり情報セキュリティ対策を考慮し製品又はサービスを選択する。ＩＴ基盤の情報セキュリティ対策及び関連仕様は、情報セキュリティ責任者が承認する。

2. ＩＴ基盤の情報セキュリティ対策

2.1 サーバー機器の情報セキュリティ要件

ＩＴ基盤で利用するサーバー機器に求める情報セキュリティ要件は、システム管理者が決定する。新規にサーバー機器を導入する場合は、情報セキュリティ要件を満たす製品を選択し、システム管理者の許可を得て導入する。サーバー機器の情報セキュリティ要件は、「7.1 サーバー機器情報セキュリティ要件」を参照のこと。

『人工衛星等の打上げ及び人工衛星の管理に関する法律』、『衛星リモートセンシング記録の適正な取扱いの確保に関する法律』、『特定秘密の保護に関する法律』等をはじめとし、自社が扱う情報の内、法律や訓令に基づく取扱いが求められる情報等、別途定められる秘匿性の高い非公知の情報については、当該法、運用基準、省庁通達等に則った適切な条件下で IT 基盤を運用また管理する。

2.2 サーバー機器に導入するソフトウェア

ＩＴ基盤で利用するサーバー機器に導入するソフトウェアは、システム管理者が標準ソフトウェアを選定する。新規にソフトウェアを導入する場合は、システム管理者の許可を得て導入する。標準ソフトウェアは、「7.2ＩＴ基盤標準ソフトウェア」を参照のこと。

2.3 ネットワーク機器の情報セキュリティ要件

ＩＴ基盤で利用するネットワーク機器に求める情報セキュリティ要件は、システム管理者が決定する。新規にネットワーク機器を導入する場合は、情報セキュリティ要件を満たす製品を選択し、システム管理者の許可を得て導入する。ネットワーク機器の情報セキュリティ要件は、「7.4 ネットワーク機器情報セキュリティ要件」を参照のこと。

また、IT 基盤で利用するネットワーク機器の内、特定の用途で使用されるネットワーク機器を導入する場合は、特定用途機器に求めるセキュリティ要件を、システム管理者が決定する。当該機器で取り扱う情報の格付けを行った上で、システム管理者の許可を得て導入する。

3. ＩＴ基盤の運用

システム管理者は、ＩＴ基盤の運用を行う際には以下を実施すること。

●システム管理者は、機器の管理画面にログインするためのパスワードは初期状態のまま使わず、

推測不可能なパスワードを設定して運用する。

●以下に従い、ゲートウェイにおける通信ログを取得及び保存する。

➢通信ログの保存期間は 3 年間とする。

➢ログファイルの保存状況について、システム管理者が定期的に確認する。

●システム管理者は、通信ログについて以下の確認を定期的に行う。

➢管理外のインターネット接続がないか

➢許可なく接続された機器や無線 LAN 機器はないか

➢不審な通信が行われていないか

●システム管理者は、必要に応じて業務に不要なウェブサイト閲覧を社内周知/ウェブフィルタリングソフトを使用して制限する。

●遠隔診断ポートの利用は、保守サポートなど必要な場合のみに限定し、認証機能やコールバック機能等を備えるなど、適切なセキュリティ対策を施す。

●システム管理者は、必要に応じて外部監視 SOC との契約を検討し、対象のネットワークやサーバー機器などの監視や検知に関する運用体制を整備する。

4. クラウドサービスの導入

ＩＴ基盤の一部としてクラウドサービス等の外部サービスを導入する場合は、法令やミッション等に適したセキュリティ要件やサービスレベルアグリーメント（SLA）に対応したサービスを選定し導入する。

システム管理者がサービスプロバイダの情報セキュリティ対策をあらかじめ評価したうえで選定する。新規クラウドサービス等の外部サービスを導入する場合は、システム管理者の許可を得て導入する。サービスプロバイダの情報セキュリティ対策の評価基準は、「7.2 クラウドサービスの情報セキュリティ要件」を参照のこと。

5. 脅威や攻撃に関する情報の収集

システム管理者は、最新の脅威や攻撃に関する情報収集を行い、必要に応じて社内で共有する。

6. 廃棄・返却・譲渡

システム管理者は、ＩＴ基盤で利用した機器を返却、廃棄、譲渡を行う場合は、内部記憶媒体の破壊又は専用ツールによりデータを完全に消去し、情報セキュリティ責任者の承認を得たうえ返却、廃棄、譲渡を行う。内部記憶媒体の破壊又はデータの完全消去を、外部に委託する場合は、破壊又はデータの完全消去を実行したことの証明書を取得する。

7. ＩＴ基盤の情報セキュリティ要件及び標準

7.1 機器・ソフトウェアの情報セキュリティ要件及び標準

ＩＴ基盤で利用する機器及びソフトウェアの情報セキュリティ要件と、それに基づく当社標準を以

下とする。

＜機器の情報セキュリティ要件＞

対象機器	セキュリティ要件	利用技術・製品
ファイルサーバー	利用者認証機能	Windows Active Directory
	セキュリティログ取得機能	Windows
	システムログ取得機能	Windows
	ユーザーアクセスログ取得機能	○○○○
	ハードディスク：容量○TB 以上 RAID 構成	○○○○
NAS サーバー	利用者認証機能	
	ディスク暗号化機能	○○○○
	ハードディスク：容量○GB 以上	
データ受付サーバー	データの暗号化	○○○○
	利用者認証機能	○○○○
	ハードディスク：容量○TB 以上	○○○○
SSH サーバー	利用者認証機能	○○○○
	データの暗号化	○○○○
	ハードディスク：容量○GB 以上	○○○○

＜標準ソフトウェア＞

種別	名称	開発・販売元	バージョン
ＯＳ	Windows Server	Microsoft	○○以降
ＲＤＢ	○○SQL	○○社	Ver.○以降
ウイルス対策	○○○○	○○社	Ver.○以降
ブラウザ	○○○○	○○社	Ver.○以降
シミュレーションソフト	○○○○	○○社	Ver.○以降

＜ネットワーク機器の情報セキュリティ要件＞

対象機器	セキュリティ要件	利用技術・製品
ルーター	利用者認証機能	○○○○
	MAC アドレス認証	○○○○
	通信ログ取得	○○○○
	○○○○	○○○○
○○監視ツール	ユーザーアクセス監視	○○○○
	○○○○	○○○○

対象機器	セキュリティ要件	利用技術・製品
ネットワークカメラシステム	○○○○	○○○○
施設管理システム	○○○○	○○○○

＜標準ネットワーク機器＞

種別	名称	開発・販売元	OS バージョン等
ルーター	○○○○	○○社	Ver.○以降
ＵＴＭ	○○○○	○○社	Ver.○以降
監視ツール	○○○○	○○社	Ver.○以降
○○○○	○○○○	○○社	Ver.○以降

7.2 クラウドサービスの情報セキュリティ要件

ＩＴ基盤で利用するクラウドサービスの情報セキュリティ要件を以下とする。

●サービスプロバイダが公表する情報セキュリティ又は個人情報保護への取組方針が、関連法令に準拠していること、ミッションの遂行や処理しようとする情報資産の重要度に照らして適したサービス要件であること。

●サービス仕様に含まれる情報セキュリティ対策が、関連法令に準拠していること、ミッションの遂行や処理しようとする情報資産の重要度に照らして適していること。

●情報セキュリティに関する適合性評価制度の認証・認定を取得していること。

＜適合性評価制度の種類＞

- ➢情報セキュリティマネジメントシステム適合性評価制度（ISMS クラウドセキュリティ認証）
- ➢クラウド情報セキュリティ監査制度
- ➢プライバシーマーク制度
- ➢PCI DSS（クレジットカード業界セキュリティ基準）
- ➢クラウドサービスの安全・信頼性に係る情報開示認定制度
- ➢ISMAP 政府情報システムのためのセキュリティ評価制度

8	システム開発及び保守	改訂日	20yy.mm.dd
適用範囲	当社が独自に開発する情報システム		

1. 新規システム開発・改修

情報システムの開発・改修を行う際には、以下の工程を経て実施し、各工程の完了時にシステム管理者の承認を得る。

『人工衛星等の打上げ及び人工衛星の管理に関する法律』、『衛星リモートセンシング記録の適正な取扱いの確保に関する法律』、『特定秘密の保護に関する法律』等をはじめとし、自社が扱う情報の内、法律や訓令に基づく取扱いが求められる情報等、別途定められる秘匿性の高い非公知の情報については、当該法、運用基準、省庁通達等に則った適切な保護措置等を講じる。

①対象業務の範囲定義
②ハードウェア・ソフトウェア・ネットワーク機能検討※1
③必要なパフォーマンスの検討
④情報セキュリティ要件定義※2
⑤バックアップ/障害復旧要件定義
⑥情報システム運用要件定義
⑦運用体制
⑧移行計画立案

※1 Microsoft 365 や AWS・Azure・GCP 等のクラウドサービスを用いる場合、セキュリティ要件・機能を確認し、開発・改修を行う。

※2 新規システム開発を外部に委託する際は、契約時にセキュリティ要件に関する責任範囲を明確にする。

2. 脆弱性への対処

情報システムのソフトウェア開発を行う際には、当該情報システムの利用環境に応じて設計時に技術的な脆弱性を識別し、対策を講じる。脆弱性に対する対策の有効性はシステム管理者が判断し、承認する。

（参考）IPA　情報セキュリティ　脆弱性対策
https://www.ipa.go.jp/security/vuln/index.html

3. 情報システムの開発環境

情報システムの開発及び改修を行う環境は、運用環境とは分離する。新たに情報システムの開発を行った場合や、情報システムの改修を行った場合は、当該情報システムの運用を開始する前に、必

要な情報セキュリティ対策が講じられていることを確認し、システム管理者の承認を得る。

4. 情報システムの保守

情報システムの保守を、定期的に及び必要な場合にはその都度行う。

開発元又は外部の組織に委託することができない場合、以下に挙げる事項に留意し、情報システムに既知の脆弱性が存在しない状態で運用する。

●開発時に用いたソフトウェアに関する脆弱性が公表された場合には、速やかにその影響が顕在化しないための対策を講じる。

●開発時に用いたソフトウェア及びハードウェアの製造者が提供するサポートの終了が予定されている場合、他のソフトウェアやハードウェアを用いた再構築又は当該情報システムの利用停止を検討し、システム管理者の承認を得る。

5. 情報システムの変更

情報システムのハードウェア又はソフトウェアの変更を行う際には、以下の工程を経て実施する。各工程の完了時にシステム管理者の承認を得る。

①現行システムの問題・課題の把握

②システム変更計画立案

③システム変更計画書に基づくシステム設計

④セキュリティ要求と設計の見直し※

⑤移行計画立案（移行時、運用時の障害対応をあらかじめ検討する。）

⑥変更後の仕様書、操作手順書、運用手順書等の関連文書の作成

※情報システムのハードウェア又はソフトウェアの変更を外部に委託する際は、契約時にセキュリティ要求に関する責任範囲を明確にする。

9	委託管理	改訂日	20yy.mm.dd
適用範囲	情報資産を取り扱う業務の委託		

1. 委託先評価基準

情報セキュリティ部門責任者は「情報資産管理台帳」の重要度が 1 以上である情報資産を取り扱う業務を、外部の組織に委託する場合は、委託先の情報セキュリティ管理について、委託先評価基準に基づいて評価する。

宇宙システムのサプライチェーン対策として、システムの調達から廃棄までのライフサイクルに応じた対策を講じる。

『人工衛星等の打上げ及び人工衛星の管理に関する法律』、『衛星リモートセンシング記録の適正な取扱いの確保に関する法律』、『特定秘密の保護に関する法律』等をはじめとし、自社が扱う情報の内、法律や訓令に基づく取扱いが求められる情報等、別途定められる秘匿性の高い非公知の情報については、当該法、運用基準、省庁通達等に則った適切な保護措置等を講じる。

＜委託先評価基準＞

●一貫した品質管理体制が構築され、管理されている。
●情報セキュリティマネジメントシステム（ISMS）適合性評価制度の認証を取得している。
●個人情報保護マネジメントシステム（PMS）に適合し、プライバシーマーク付与を受けている。
●SECURITY ACTION 一つ星／二つ星に取り組んでいる。
●人的・物理セキュリティ対策を含むセキュリティ管理を実施している。
●情報セキュリティ監査を定期的に実施している。
●情報セキュリティに関する方針を公開している。
●「委託先情報セキュリティ対策状況確認リスト」で全ての対策を実施している。／〇個以上の対策を実施している。／〇個以上の対策を実施する予定を確認している。／取り扱う情報資産に必要な対策を実施している。

2. 委託先の選定

評価結果に基づき委託先を選定し、情報セキュリティ責任者の承認を得る。

3. 委託契約の締結

委託契約書には、下記に関する事項を明記する。

●委託業務に従事する従業員についての事項
●当社の社外秘又は極秘の情報資産及び個人情報の守秘義務
●再委託についての事項
●事故時の責任分担についての事項

●委託業務終了時の当社が提供した社外秘又は極秘の情報資産及び個人情報の返却又は廃棄、消去についての事項
●契約期間中における情報セキュリティ対策の実施状況に関する監査の方法とその権限（追跡調査・立ち入り検査等の原因調査に関する事項）についての事項
●契約内容が遵守されない場合の措置
●委託先における試作品等を廃棄・消去する場合の費用負担、廃棄手順、廃棄証明についての事項
●委託先より納品される製品に対する試験の実施についての事項
●事故発生時の報告方法
●委託先が調達した機器もしくは開発した構成品に関する脆弱性等の問題が発見された場合の対応についての事項

4. 委託先の評価

委託開始後には、「委託先情報セキュリティ対策状況確認リスト」により、委託先における情報セキュリティ対策の実施状況について定期的に評価する機会を設ける。委託先における情報セキュリティ対策の実施に関して不備又は変更が認められた場合は、双方協議のうえ、対処を検討し、書面で合意する。

＜委託先評価の方法＞

➢委託先事業所に訪問して現場を観察する。
➢委託先の管理責任者にインタビューする。
➢委託先に「委託先情報セキュリティ対策状況確認リスト」を送付し、実施状況について回答してもらう。

（参考情報：9-1　委託先情報セキュリティ対策実施状況確認リスト）

5. 再委託

当社が委託する業務を、委託先が他の組織又は個人に再委託する場合には、適切な条件下でセキュリティ管理が実施されているか確認するために、事前に書面による報告を委託先に求める。

報告には必要に応じて以下の提供を含め、当社の「1. 委託先評価基準」「3. 委託契約の締結」「4. 委託先の評価」と同等の管理を再委託先に求めていることを確認し、情報セキュリティ責任者の承認を得たうえで再委託を認める。

●委託先と再委託先との契約書案の写し（情報セキュリティに関連する部分のみ）
●再委託先の選定基準
●再委託先が情報セキュリティに関する適合性評価制度の認証・認定を取得している場合にはその証書の写し
●再委託先において意図しない変更や情報の窃取等が行われないことを保証するための管理体制

9-1　委託先情報セキュリティ対策状況確認リスト

注 1：このサンプルは、委託先の情報セキュリティ対策の実施状況を確認するためのものです。必要な項目を加筆修正してご利用ください。

注 2：『人工衛星等の打上げ及び人工衛星の管理に関する法律』、『衛星リモートセンシング記録の適正な取扱いの確保に関する法律』、特定秘密の保護に関する法律等をはじめとし、自社が扱う情報の内、法律や訓令に基づく取扱いが求められる情報等、別途定められる秘匿性の高い非公知の情報の授受を伴う委託先については、当該法、運用基準、省庁通達等に則った適切な保護措置等が求められます。

区分	No	確認項目	実施状況（○、×）
社内体制	1	情報セキュリティ管理責任者を定めている	
	2	リスクアセスメントを実施し、アセスメント結果に基づいた情報セキュリティに関する規程を整備している	
	3	情報セキュリティへの取り組み方針を従業員や取引先に周知している	
	4	情報セキュリティ事故に対する対応手順を整備している	
	5	定期的に情報セキュリティに関する内部点検を実施している	
	6	情報セキュリティ対策の実施状況に関する監査を実施している。	
	7	製造工程の履歴を記録する管理体制を整備している	
人的管理	8	委託業務に従事する従業員についての規程を整備している	
	9	情報セキュリティに関する教育を定期的に実施し、受講記録を作成している	
	10	従業員と守秘義務契約を交わしている	
物理的管理	11	関係者以外の事務所への立ち入りを制限している	
	12	機密情報の保管について施錠管理をしている	
	13	機密情報を保管している領域に入ることができる人を制限し、入退出記録を取得している	
	14	入退出記録を定期的に確認している	
情報機器・媒体の取り扱い	15	機器・媒体の盗難防止措置を講じている	
	16	媒体の無断複製、不正持出しを防止する措置を講じている	
	17	媒体の移送、受け渡し時の保護措置を講じている	
	18	媒体の安全な消去、廃棄の手順を整備している	
技術的対策	19	システム設計時にリスクアセスメントを実施し、アセスメント結果に基づいた必要なセキュリティ対策を行っている	
	20	業務で使用するサーバー・パソコンのウイルス対策を行っている	

	21	業務で使用するサーバー・パソコンは利用者認証機能を設定している	
	22	業務で使用するサーバー・パソコンに利用制限等を設け管理している	
再委託先管理	23	重要情報の授受を伴う委託先との契約書には、秘密保持条項を規定している	
	24	重要情報の授受を伴う委託先には自社と同等の情報セキュリティ対策を求めている	

10	情報セキュリティインシデント対応 及び事業継続管理	改訂日	20yy.mm.dd
適用範囲	情報資産及び保有する個人データに関わるインシデント		

1. 対応体制

情報セキュリティインシデントが発生した場合には、以下の体制で対応する。

最高責任者	代表取締役
対応責任者	インシデント対応責任者
一次対応者	発見者又はシステム管理者

2. 情報セキュリティインシデントの影響範囲と対応者

情報セキュリティインシデントが発生した場合、以下を参考に影響範囲を判断して対応する。

なお、以下に示すインシデントの影響範囲に加え、『人工衛星等の打上げ及び人工衛星の管理に関する法律』、『衛星リモートセンシング記録の適正な取扱いの確保に関する法律』、『特定秘密の保護に関する法律』等をはじめとし、自社が扱う情報の内、法律や訓令に基づく取扱いが求められる情報等、別途定められる秘匿性の高い非公知の情報を扱う場合、漏洩すると国家の安全保障に甚大な影響を及ぼすことが考えられることから、扱う情報のレベルに応じ、影響範囲を判断して対応する。

事故レベル	影響範囲	責任者
3	●顧客、取引先、株主等に影響が及ぶとき ●個人情報が漏えいしたとき ●事業の継続及び推進が困難になるとき	代表取締役
2	●事業の継続及び推進に影響が及ぶとき	インシデント対応責任者
1	従業員の業務遂行に影響が及ぶとき	インシデント対応責任者
0	インシデントにまでは至らないが、将来においてインシデントが発生する可能性がある事象が発見されたとき	システム管理者

3. インシデントの連絡及び報告

事故レベル１以上のインシデントが発生した場合、発見者は以下の連絡網に従い、対応者または責任者に速やかに報告し、指示を仰ぐ。

対応者または責任者	緊急連絡先
代表取締役	携帯電話：090-****-**** 電子メールアドレス：president@*****.co.jp

インシデント対応責任者	携帯電話：090-****-**** 電子メールアドレス：incident@*****.co.jp
システム管理者	携帯電話：090-****-**** 電子メールアドレス：system@*****.co.jp

4. 対応手順

インシデントを以下のとおりに区分し、それぞれの対応手順を示す。

区分	事件・事故の状況
漏えい・流出	社外秘又は極秘情報資産の盗難、流出、紛失
改ざん・消失・破壊 サービス停止	情報資産の意図しない改ざん、消失、破壊 情報資産が必要なときに利用できない
ウイルス感染	悪意のあるソフトウェアに感染

＜漏えい・流出発生時の対応＞

事故レベル	対応手順
3	①発見者は即座にインシデント対応責任者及び代表取締役社長に報告する。 ②インシデント対応責任者は原因を特定するとともに、二次被害が想定される場合には防止策を実行する。 ③インシデント対応責任者は被害者/本人対応を準備する。 ④インシデント対応責任者は問い合わせ対応を準備する。 ⑤インシデント対応責任者は影響範囲・被害の大きさによっては総務部に報道発表の準備を申請する。 ⑥インシデント対応責任者はサイバー攻撃等の不正アクセスによる被害の場合は都道府県警察本部のサイバー犯罪相談窓口に届け出る。 ⑦インシデント対応責任者は個人データ*または特定個人情報漏えいの場合には個人情報保護委員会に報告する。 ⑧代表取締役は社内及び影響範囲の全ての組織・人に対応結果及び対策を公表する。 *個人データ：個人情報データベース等（特定の個人を検索できるようにまとめたもの）を構成する個人情報
2	①発見者は発見次第、システム管理者に報告する。 ②システム管理者は漏えい先を調査し、インシデント対応責任者に報告する。 ③システム管理者は社内関係者に周知する。
1	※情報漏えい・流出は全て事故レベル 2 以上

＜改ざん・消失・破壊・サービス停止発生時の対応＞

事故レベル	対応手順
3	①発見者は即座にインシデント対応責任者及び代表取締役社長に報告する。 ②システム管理者は原因を特定し、応急処置を実行する。 ③インシデント対応責任者は社内に周知する。 ④電子データの場合はシステム管理者がバックアップによる復旧を実行する。 ⑤機器の場合はシステム管理者が修理、復旧、交換等の手続きを行う。 ⑥書類・フィルム原本の場合は情報セキュリティ部門責任者が可能な範囲で修復する。 ⑦システム管理者は原因対策を実施する。 ⑧代表取締役は社内及び影響範囲の全ての組織・人に対応結果及び対策を公表する。
2	①発見者は発見次第、システム管理者に報告する。 ②システム管理者は原因を特定し、応急処置を実行する。 ③インシデント対応責任者は社内に周知する。 ④電子データの場合はシステム管理者がバックアップによる復旧を実行する。 ⑤機器の場合はシステム管理者が修理、復旧、交換等の手続きを行う。 ⑥書類・フィルム原本の場合は情報セキュリティ部門責任者が可能な範囲で修復する。 ⑦システム管理者は原因対策を実施する。
1	①発見者は発見次第、システム管理者に報告する。 ②システム管理者は原因を特定し、応急処置を実行するとともに必要に応じて社内に周知する。 ③電子データの場合はシステム管理者がバックアップによる復旧又は再作成・入手を実行する。 ④機器の場合はシステム管理者が修理、復旧、交換等の手続きを行う。 ⑤書類・フィルム等の原本の場合は情報セキュリティ部門責任者が可能な範囲で修復する ⑥システム管理者は原因対策を実施する
0	発見者は発見次第、発生可能性のあるインシデントと想定される被害をシステム管理者に報告する。

＜ウイルス感染時の初期対応＞

従業員は、業務に利用しているパソコン、サーバー又はスマートフォン、タブレット（以下「コンピュータ」といいます。）がウイルスに感染した場合には、以下を実行する。

①ネットワークからコンピュータを切断する。

②システム管理者に連絡する。

③ウイルス対策ソフトの定義ファイルが最新の状態でない場合は最新版に更新する。

※他のコンピュータでネットワークに接続し、定義ファイルの最新版をダウンロードしたうえで、感染したコンピュータの定義ファイルを更新する。

④ウイルス対策ソフトを実行しウイルス名を確認する。

⑤ウイルス対策ソフトで駆除可能な場合は駆除する。

⑥駆除後再度ウイルス対策ソフトでスキャンし、駆除を確認する。
⑦システム管理者に報告する。

以下の場合など従業員自身で対応できないと判断される場合はシステム管理者に問い合わせる。
●ウイルス対策ソフトで駆除できない。
●システムファイルが破壊・改ざんされている。
●ファイルが改ざん・暗号化・削除されている。

5.届出及び相談
システム管理者は、インシデント対応後に以下の機関への届け出、報告又は相談を検討する。
＜届出・相談・報告先＞
【独立行政法人 情報処理推進機構セキュリティセンター】
https://www.ipa.go.jp/security/todokede/crack-virus/about.html
➢ ウイルス発見・感染、ランサムウェア被害の届出
E-mail：virus@ipa.go.jp
➢ 不正アクセスの届出
E-mail：crack@ipa.go.jp
➢ ウイルス発見・感染、ランサムウェア被害の届出
E-mail：virus@ipa.go.jp
➢ 情報セキュリティ安心相談窓口
https://www.ipa.go.jp/security/anshin/about.html
E-mail：anshin@ipa.go.jp
TEL:03-5978-7509　FAX:03-5978-7518
〒 113-6591 東京都文京区本駒込 2-28-8 文京グリーンコート センターオフィス 18 階
IPA セキュリティセンター 安心相談窓口

【個人情報保護委員会】
➢ 個人データの漏えい等の事案が発生した場合等の対応
①個人データ（特定個人情報に係るものを除く。）の漏えい、滅失又は毀損
②加工方法等情報（匿名加工情報の加工の方法に関する情報等）の漏えい
③上記①又は②のおそれ
漏えい等事案が発覚した場合は、速やかに下記 UR を参照して個人情報保護委員会等に対し、報告すること
https://www.ppc.go.jp/personalinfo/legal/leakAction/
TEL：03-6457-9685
個人情報保護委員会事務局　個人データ漏えい等報告窓口
➢ 特定個人情報の漏えい事案が発生した場合の対応

①番号法違反又は違反のおそれ

番号法違反又は違反のおそれを把握した場合は、速やかに下記 UR を参照して個人情報保護委員会等に対し、報告すること

https://www.ppc.go.jp/legal/rouei/

②重大事態に該当する事案又はそのおそれ

≪重大事態≫

- 情報提供ネットワークシステム等又は個人番号利用事務を処理するために使用する情報システムで管理される特定個人情報が漏えい等した事態
- 漏えい等した特定個人情報に係る本人の数が 100 人を超える事態
- 特定個人情報を電磁的方法により不特定多数の者が閲覧することができる状態となり、かつ閲覧された事態
- 従業員等が不正の目的をもって、特定個人情報を利用し、又は提供した事態

重大事態が発覚した場合は、直ちに下記 UR を参照して個人情報保護委員会等に対し、報告すること

https://www.ppc.go.jp/legal/rouei/

個人情報保護委員会事務局　特定個人情報漏えい等報告窓口

TEL:03-6457-9680

事業内容に応じて、以下の報告・相談先から選択する。

【内閣総理大臣（内閣府）】

➢ 衛星リモートセンシング装置又はこれを搭載する地球周回人工衛星の故障その他の事情により、終了措置を講ずることなく当該衛星リモートセンシング装置の使用を行うことができなくなり、かつ、回復する見込みがない場合等の対応：

①テレメトリ等から、衛星リモセン装置の故障等により機能の回復が望めないことが把握できるとき

②通信の途絶等、回復の手立てがないとき

『衛星リモートセンシング記録の適正な取扱いの確保に関する法律』に基づき、報告が必要な場合においては、速やかに下記 URL を参照して内閣府宇宙開発戦略推進事務局リモセン法担当に対し、報告すること

https://www8.cao.go.jp/space/application/rs/application.html

➢ 人工衛星の他の物体との衝突その他の事故の発生により、同項の許可に係る終了措置を講ずることなく人工衛星の管理ができなくなり、かつ、回復する見込みがない場合等の対応

『人工衛星等の打上げ及び人工衛星の管理に関する法律』に基づき、報告が必要な場合においては、速やかに下記 URL を参照して内閣府宇宙開発戦略推進事務局宇宙活動法担当に対し、報告すること

https://www8.cao.go.jp/space/application/space_activity/application.html

【総務大臣（総務省）】

➢ 電気通信業務の一部を停止したとき、又は電気通信業務に関し通信の秘密の漏えいその他重大な事故が生じた場合等の対応

①電気通信業務の一部を停止したとき

②報告を要する事由が発生したとき

『電気通信事業法』及び『電気通信事業法施行規則』に基づき、報告が必要な場合においては、速やかに下記 URL を参照して総務省総合通信基盤局安全・信頼性対策課及び総合通信局等の所管部署に対し、報告すること

https://www.soumu.go.jp/menu_seisaku/ictseisaku/net_anzen/jiko/judai.html

➢ 設備に起因する放送の停止、またその他の重大な事故が生じた場合等の対応

①設備に起因する放送の停止その他の重要な事故が発生したとき

『放送法』及び『放送法施行規則』に基づき、報告が必要な場合においては、速やかに下記 URL を参照して総務省情報流通行政局等の所管部署に対し、報告すること

https://www.soumu.go.jp/main_content/000496674.pdf

【各関係省庁】

➢ 宇宙に関連するサービスが起因で重要インフラのサービスに支障が生じる場合等の対応

①電気通信サービスの停止

②放送サービスの停止

各重要インフラ分野の事業法に基づき、報告が必要な場合においては、速やかに下記 URL を参照して関係省庁に対し、報告すること

https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf （P.48～）

6. 情報セキュリティインシデントによる事業中断と事業継続管理

代表取締役は、情報セキュリティインシデントの影響により当社事業が中断した場合に備え、以下を定める。

＜想定される情報セキュリティインシデント＞

以下のインシデントによる事業の中断を想定する。

●情報セキュリティインシデント①：大型地震の発生に伴う設備の倒壊、回線の途絶、停電等による〇〇システム停止

●想定理由：当社の事業は、商品の販売から請求回収までの業務を〇〇システムに依存しているため、停止した場合は事業の継続が困難になり多大な損失が発生

●情報セキュリティインシデント②：△△システムを対象としたサイバー攻撃による自社サービスの停止、機密情報の漏えい

●想定理由：衛星関連システムを対象としたインシデント事例が増加しており、当社の基幹事業である〇〇は、△△システムに依存しているため、停止した場合は、事業の継続が困難になり多大な損失が発生

＜復旧責任者及び関連連絡先＞

被害対象	復旧責任者	関係者連絡先
電源設備 空調機	総務部長	○○電力△△支店 （株）○○設備
（○○システム） ハードウェア ソフトウェア ネットワーク機器 回線サービス バックアップクラウドサーバー	インシデント対応責任者 システム管理者	（株）○○システム開発 （株）△△ネットワークサービス （株）◇◇マネージドサーバー
顧客	営業部長	営業部取引先リスト参照
従業員人的被害	総務部長	従業員名簿参照

7. 事業継続計画

インシデント対応責任者は、想定する情報セキュリティインシデントが発生し、事業が中断した際の復旧責任者の役割認識及び関係者連絡先について、有効に機能するか検証する。復旧責任者は、被害対象に応じて復旧から事業再開までの計画を立案する。

11	テレワークにおける対策	改訂日	20yy.mm.dd
適用範囲	テレワーク勤務者		

1. テレワーク共通ルール

1.1 テレワークで利用する情報システム

テレワークを実施する際には、以下の情報システム・サービスを利用する。他の情報システムやサービスを利用する必要がある場合は、システム管理者の許可を得る。

情報システム・サービス	用途	導入手順・制限事項
電子メールソフト ●●●●	電子メール	・社内 PC にリモートアクセスして利用 ・私有メールアドレス、メーラーの業務利用禁止
クラウド型グループウェア ●●●●	・勤怠管理 ・社内連絡 ・ファイル転送・保存	社内 PC にリモートアクセスして利用または以下の URL に直接アクセスして利用 https://groupware/login/
クラウド型ビジネスチャット ●●●●	プロジェクト管理	●●●●.pdf 参照
オンライン会議システム ●●●●	・社内会議 ・商談	・通信はエンドツーエンド暗号化を利用 ・参加者名の設定機能を利用 ・会議終了後に録音・録画、共有資料。チャット等の会議データをクラウド上から削除 ●●●●.pdf 参照
●●●●シリーズ	・会計 ・給与計算	社内 PC にリモートアクセスして利用 ●●●●.pdf 参照
●●●●CRM システム	顧客管理	以下の URL に直接アクセスして利用 https://groupware/login/ ●●●●.pdf 参照
●●●●	○○○○業務	●●●●.pdf 参照

1.2 テレワークで利用する機器

テレワークで業務を行う際には、以下の情報機器を利用する。他の情報機器を利用する必要がある場合は、システム管理者の許可を得る。

情報機器	社有機器	私有機器
パソコン	・全社貸与テレワーク用 PC を利用 ・社内 PC を持ち出して利用	53 ページ「私有機器を利用する場合」の対策を実施して利用
スマホ・タブレット	●●部員は会社貸与品を利用	●●部員以外は「私有機器を利用する場合」の対策を実施して利用
通信機器（ルーター）	●●部員は会社貸与のモバイルルータを利用	●●部員以外は「私有機器を利用する場合」の対策を実施して利用
USB メモリ・外付け HDD	全社貸与品を利用	私有機器の業務利用禁止
オンライン会議用ヘッドセット	全社貸与品を利用	必要に応じて私有機器を利用
オンライン会議用 Web カメラ	会社貸与テレワーク用 PC 内蔵 Web カメラを利用	必要に応じて私有機器を利用
プリンタ	●●部員は会社貸与品を利用	●●部員以外は私有機器またはコンビニ・レンタルオフィス等のサービスを、「私有機器を利用する場合」の対策を実施して利用
●●●●	●●●●	●●●●

1.3 システム構成別セキュリティ対策

テレワークで利用するシステム構成に応じて、以下のセキュリティ対策を実施する。

方式	詳細	対策
VPN 方式	テレワーク端末から社内ネットワークに通信を暗号化して接続する方式	情報漏えい防止のために、テレワーク端末のハードディスクや SSD など内蔵記録装置の暗号化やデータの遠隔消去等の対策を実施する。
リモートデスクトップ方式	テレワーク端末から社内パソコン等の端末に接続する方式	通信環境によっては処理が遅くなるなど操作性が低下し、業務に著しく影響することがあるため、業務に適した方式かを事前に検討する。

スタンドアロン（持ち帰り）方式	テレワーク端末を社内ネットワークに接続せずに使用する方式	情報漏えい防止に向けて、テレワーク端末のハードディスクや SSD など内蔵記録装置の暗号化やデータの遠隔消去等の対策を実施する。 必要最低限のデータのみ許可を得て持ち出すようにする。 インターネットを利用する場合は、ウイルスや不正アクセスへの対策を実施する。
クラウドサービス方式	インターネット上のクラウドサービスに直接接続する方式	端末から社内ネットワークを経由せず直接インターネットに接続するため、通信の暗号化やサービスにログインするときの認証強化などのネットワーク上の対策を実施する。

2. 情報機器のセキュリティ

2.1 社有機器を利用する場合

社有機器を利用する場合は以下を遵守する。

＜パソコン＞

●OS・ソフトウェアはインターネットに接続した状態で自動更新を有効にして最新の更新プログラムをインストールする

●ウイルス対策ソフトの定義ファイルは自動で更新する。

●社内標準外ソフトウェアのインストールは禁止する。

2.1.2 スマホ・タブレット

●指定された MDM（モバイル機器管理）エージェントをインストールし、データの暗号化や遠隔でのデータ消去等の対策を行う。

●OS は以下を参考にして自動で更新する。

➢Android 端末の場合：機種毎の設定画面で自動システムアップデートを選択する。

➢iPhone の場合：デバイスの自動アップデートを有効にする。

●アプリをインストールする際は、公式のマーケットを利用する。

●社内標準外アプリのインストールは禁止する。

＜USB メモリ＞

●秘密情報または個人情報を保存して外出する場合は、ファイルを暗号化する。

2.2 私有機器を利用する場合

私有機器を利用する場合は以下を遵守する。

＜パソコン＞

●テレワーク専用のアカウントを追加し、ログインパスワードを設定する。

●会社がライセンスを取得したソフトウェアおよびウイルス対策ソフトをインストールする。

●業務で社内標準外ソフトウェアを利用する必要がある場合は、システム管理者に許可を得る。

●利用開始時にウイルス対策ソフトで PC 全体をフルスキャンする。

●OS・ソフトウェアはインターネットに接続した状態で自動更新を有効にして最新の更新プログラムをインストールする。

●ウイルス対策ソフトの定義ファイルは自動で更新する。

＜スマホ・タブレット＞

●OS は以下を参考にして自動で更新する。

●アプリをインストールする際は、公式のマーケットを利用する。

➢Android 端末の場合：機種毎の設定画面で自動システムアップデートを選択する。

➢iPhone の場合：デバイスの自動アップデートを有効にする。

●社内標準のセキュリティソフトをインストールする。

●業務を行うときは以下の社内標準アプリを公式マーケットから入手して利用する。

●業務で社内標準外のアプリを利用する場合は、システム管理者に許可を得る。

●不正な改造を行うことを禁止する（脱獄・root 化）。

2.3 社内標準アプリ

社内標準アプリは、以下を利用する。

セキュリティソフト	●●●●セキュリティ
社内通話・打ち合わせ	●●●●
メール・スケジュール管理システムへのアクセス	●●●●
ビジネスチャットメール	●●●●
●●●●	●●●●

＜公式マーケット＞

アプリをインストールする際は、公式のマーケットを利用する。

➢Android 端末：Google 社「Google Play」

➢iPhone：Apple 社「App Store」

3. ネットワーク機器のセキュリティ：テレワークのネットワーク環境

テレワークで使用する通信機器（ルーター）には、以下の対策を講じる。

利用場所	通信機器サービス	対策
自宅	有線 LAN ハブ	同じハブに他者（家族を含む）も PC を接続する場合は ・スイッチングハブを利用する（リピー

		ターハブは禁止） ・OS の「ネットワークのファイルとフォルダーの共有」を解除する
	無線 LAN ルーター	・同じルーターに他者（家族を含む）も端末を接続する場合は OS の「ネットワークのファイルとフォルダーの共有」を解除する ・暗号化方式は WPA2-PSK または機器が対応している場合は WPA3 を選択する ・暗号化キーに簡単なものが設定されている場合、次の条件を満たすように変更する ➢ 英語の辞書に載っている単語を使わない ➢ 大文字、小文字、数字、記号の全てを含む文字列とする ➢ 文字数を増やし容易に推測できないようにする ・SSID は、使用者氏名、会社名などを想起させないものを使う ・設定画面にログインするためのパスワードは、容易に推測できないものを使う ・ファームウェアは自動更新にする
外出先 ※取引先・レンタルオフィス・カフェ・ホテル・ファーストフード・コンビニ・空港・駅・鉄道・バスなど	モバイル Wi-Fi ルーター（スマホでのテザリングを含む）	・SSID/ネットワーク名は初期値を変更し、ルーター/スマホ機種名、使用者氏名、会社名などを想起させないものを使う ・セキュリティキー/パスワードは、無線 LAN ルーターの暗号化キーと同等の推測できないものを使う
	公衆 Wi-Fi サービス	・メールは社内 PC にリモートアクセスして利用する ・ID・パスワードなどの認証情報、会社の秘密情報、個人情報などの重要情報を入力・表示しない ・重要情報の入力・表示が必要な場合に

		は VPN または SSL/TLS 対応サイトを利用する ・OS の「ネットワークのファイルとフォルダーの共有」を解除する

4. 勤務中のルール

4.1 電子メール・ウェブサイトの利用

テレワーク端末で電子メール、ウェブサイトを利用する場合は以下を遵守する。

●個人のメールアカウントを利用するときには、安易に添付ファイルを開いたリンクを参照しない。

●ウェブサイトからファイルをダウンロードするときには、ブラウザで証明書を確認し（ブラウザの鍵マークをクリックする）、信頼できるサイトを利用する。

●業務に関係がない不審なサイトにアクセスしない。

●メールで重要な情報を添付ファイルで送信する場合はファイルを暗号化し、復号パスワードは SMS 等別の方法で相手に伝える。

4.2 クラウド・SNS の利用

テレワーク端末で個人的にクラウドサービス、SNS を利用する場合は以下を遵守する。

●業務関連データの送受信、保存、共有に利用しない。

●社内、取引先との連絡に利用しない。

●当社の秘密情報の書き込みは行なわない。

4.3 在宅時の注意

在宅勤務では以下に注意する。

●離席時にスクリーンセーバーや画面をロックし他者（家族を含む）にテレワーク用の情報機器を操作させない。

●他者（家族を含む）から見えるところにテレワークで使うパスワードを書き記さない。

4.4 外出時の注意

取引先・レンタルオフィス・カフェ・ホテル・ファーストフード・コンビニ・空港・駅・鉄道・バスなど外出先でテレワークを行うときには、以下に注意する。

●必要な情報以外は持ち出さない。

●機器や書類は目の届く範囲に置き放置しない。

●取引先やレンタルオフィスなどで離席するときはスクリーンセーバーや画面をロックする※2。

●不特定多数の人がいる場所では重要情報を画面に表示せず、のぞき見防止フィルターを利用する。

●外出先で書類や CD・DVD などの媒体を廃棄しない。

●公衆 Wi-Fi を利用するときは以下を遵守する。

●メールは端末から直接メールサーバーにアクセスせず社内 PC にリモートアクセスするか、指定さ

れたセキュアブラウザを利用する。
●その他で公衆 Wi-Fi を使用して業務データを扱うときには VPN または SSL/TLS 対応サイトを利用する。

5. データ・書類の保存
5.1 電子データ保存と消去
業務データの取り扱いに関して以下を遵守する。
●業務関連データのうち秘密情報または個人情報をテレワーク用 PC で処理する場合は、作業後に社内 PC にリモートアクセスし、社内サーバーに転送・保存する。
●転送後には PC 内のデータをシステム管理者の指定するツールで完全消去する。
●秘密情報または個人情報を継続してテレワーク用 PC または会社貸与の USB メモリ、外付け HDD に保存する必要がある場合は、ファイルを暗号化する。

5.2 物理媒体の保管と廃棄
書類・印刷物・CD/DVD 等の物理媒体の取り扱いに関して以下を遵守する。
●秘密情報または個人情報を含む書類・印刷物・CD/DVD などの媒体は、鍵付き引き出し、書類ケースに保管し、利用時以外は施錠する。
●書類・印刷物は、ハサミなどで細断して廃棄する。
●CD/DVD を廃棄する場合は、割る、またはカッターなどで傷を付けて廃棄する。

6. 社内問い合わせ・緊急連絡先
テレワークのことで分からないことがあったら以下に問い合わせてください。
＜問合せ先＞
システム管理者（管理部長）TEL：090- ○○○○-○○○○
Mail：soumu@○○○○.co.jp
ウイルス感染の疑いや、情報機器や書類の紛失・盗難などのセキュリティ事故が起きてしまったら、速やかに以下に連絡してください。
＜緊急連絡先＞※夜間休日を問いません
システム管理者（管理部長）TEL：090- ○○○○-○○○○
Mail：soumu@○○○○.co.jp

NIST の Cybersecurity Framework 2.0 の
フレームワークコア・カテゴリーとの対応関係

各章の内容は、NIST Cybersecurity Framework 2.0（NIST CSF 2.0）における以下のフレームワークコア・カテゴリーに関係するため、必要に応じて参照されたい。

https://www.nist.gov/cyberframework

※ カテゴリーの日本語名称は仮訳であるため、必要に応じて原文を参照のこと。

No.	題目	NIST CSF 2.0 フレームワークコア・カテゴリー
共通	—	・ 統治（Governance：GV） ➢ 組織のコンテクスト（GV.OC） ➢ リスクマネジメント戦略（GV.RM） ➢ 役割、責任、権限（GV.RR） ➢ 方針（GV.PO） ➢ 監督(GV.OV) ➢ サイバーセキュリティサプライチェーンリスク マネジメント（GV.SC）
1	組織的対策	・ 特定（Identify：ID） ➢ リスクアセスメント(ID.RA) ➢ 改善（ID.IM）
2	人的対策	・ 防御（Protect：PR） ➢ 意識向上及びトレーニング(PR.AT)
3	情報資産管理	・ 特定（Identify：ID） ➢ 資産管理（ID.AM） ➢ リスクアセスメント（ID.RA） ・ 防御（Protect：PR） ・ データセキュリティ（PR.DS）
4	アクセス制御及び認証	・ 防御（Protect：PR） ➢ アイデンティティ管理、認証/アクセス制御（PR.AA）
5	物理的対策	・ 防御（Protect：PR） ➢ アイデンティティ管理、認証/アクセス制御（PR.AA） ➢ 技術インフラの回復力（PR.IR） ・ 検知（Detect：DE） ➢ 継続的なモニタリング(DE.CM)
6	IT 機器利用	・ 防御（Protect：PR）

No.	題目	NIST CSF 2.0 フレームワークコア・カテゴリー
		➢ プラットフォーム セキュリティ (PR.PS) ・ 検知 (Detect : DE) ➢ 有害イベント分析 (DE.AE) ➢ 継続的なモニタリング (DE.CM)
7	IT 基盤運用管理	・ 特定 (Identify : ID) ➢ 改善 (ID.IM) ・ 防御 (Protect : PR) ➢ プラットフォームセキュリティ (PR.PS) ➢ 技術インフラの回復力 (PR.IR)
8	システム開発及び保守	・ 特定 (Identify : ID) ➢ リスクアセスメント(ID.RA) ・ 防御 (Protect : PR) ➢ プラットフォームセキュリティ (PR.PS)
9	委託管理	・ 検知 (Detect : DE) ➢ 継続的なモニタリング (DE.CM)
10	情報セキュリティインシデント対応及び事業継続管理	・ 防御 (Protect : PR) ➢ 技術インフラの回復力 (PR.IR) ・ 検知 (Detect : DE) ➢ 有害イベント分析 (DE.AE) ・ 対応 (Respond : RS) ➢ インシデント管理(RS.MA) ➢ インシデント分析 (RS.AN) ➢ インシデントレスポンスの報告とコミュニケーション (RS.CO) ➢ インシデントの緩和 (RS.MI) ・ 復旧 (Recover : RC) ➢ インシデントの復旧計画の実行 (RC.RP) ➢ インシデント復旧コミュニケーション (RC.CO)
11	テレワークにおける対策	・ 防御 (Protect : PR) ➢ データセキュリティ (PR.DS)