日本リモートセンシング学会（RSSJ）情報セキュリティポリシー

第 1 章　目的

本ポリシーは、日本リモートセンシング学会（以下「本学会」という。）において取り扱う情報資産を適切に保護し、情報漏えい、不正アクセス、改ざん等のリスクを防止することを目的とする。

第 2 章　適用範囲

本ポリシーは、本学会に関連する以下の者及び第 3 章に定める情報資産に適用する：

- 役員（会長、副会長、理事、監事等）
- 事務局職員および委託先
- 委員会および学会活動に関与する関係者
- 学会が管理する情報システム・データを利用する全ての者

第 3 章　情報資産の定義と分類

3.1 情報資産の定義

本学会が管理または利用する以下を情報資産とする：

- 会員情報（個人情報含む）
- 講演会・論文投稿・査読情報
- 会議資料、議事録
- 学会運営に関する各種文書
- 学会刊行物
- IT システム・クラウドサービス上のデータ

3.2 情報の分類

情報は以下の区分で管理する：

区分	内容例	管理レベル
公開情報	公開済論文、Web 掲載情報	制限なし
内部情報	会議資料、一般的な事務情報	関係者限定
機密情報	会員情報、査読情報、未公開資料	厳格管理

第 4 章　基本方針

本学会は以下の基本方針に基づき情報セキュリティを確保する：

1. 法令および関連規程の遵守
2. 情報資産の機密性・完全性・可用性の確保
3. 適切なアクセス制御の実施

4. 継続的な改善および教育・啓発

第 5 章　情報の管理

5.1 アクセス管理

- 情報へのアクセスは業務上必要な範囲に限定する
- ID・パスワードは個人単位で管理し、共有を禁止する
- 強固なパスワードを使用する

5.2 保存・管理

- 機密情報は適切な場所（アクセス制限された環境）で管理する
- 外部クラウド利用時は機密情報の取扱いに十分注意する
- 必要に応じてバックアップを取得する

5.3 外部提供

- 第三者への提供は必要性を確認し、責任者の承認を得る
- 個人情報や機密情報は原則として外部共有を禁止する

第 6 章　情報システム・メール利用

6.1 メール利用

- 宛先・添付ファイルの誤送信防止措置を講じる
- 一斉送信時は BCC の活用などにより個人情報保護を徹底する
- 機密情報送信時は適切な暗号化措置を検討するとともに、必要最低限の宛先とする

6.2 クラウド・外部サービス

- 利用規約・セキュリティ条件を確認した上で利用する
- 機密情報の入力・保存は最小限とする
- 個人アカウントの業務利用は原則禁止する

第 7 章　インシデント対応

以下の事象が発生した場合、速やかに事務局長、情報管理担当者に報告する。事務局長が必要と判断した場合は、会長、副会長に報告する

- 情報漏えいまたはその疑い
- 誤送信・誤共有
- 不正アクセスやマルウェア感染

対応方針：

1. 影響範囲の特定
2. 関係者への通知
3. 再発防止策の策定

第８章　教育・啓発

- 役員・関係者に対し、定期的に情報セキュリティに関する注意喚起を行う
- 事例（誤送信等）を共有し、再発防止に活用する

第９章　見直し

本ポリシーは、以下の場合に見直しを行う：

- 法令・環境の変化
- インシデント発生時
- 必要に応じた定期見直し