公益財団法人妻籠を愛する会　情報セキュリティ基本方針

公益財団法人妻籠を愛する会（以下「本財団」という）は多様な情報を保管しており、その多くは公益性優先の見地から原則として広く公開しています。一方で本財団は個人情報や守秘義務を伴う情報も保持しており、これらについては保護し、その信頼性を確保することに社会的責務を負っています。

また、すべての情報は本財団の貴重な資産でもあります。従って、すべての役員・職員は、関連法規、業務における契約事項等を遵守し、本財団の保有する情報資産を適切に取り扱わなければなりません。秘密情報の漏洩、改ざん、紛失、不正利用する行為や許可なく開示する等の行為は、会員及び関係者等から信頼を奪い、本財団に損害も与えます。そのような行為を行った者は、法的処罰の対象となることもあります。

本財団は、情報セキュリティの管理体制を整備し、公益事業ならびに信頼性のさらなる向上を目指していきます。そこで、ここに、すべての職員が情報管理の重要性と責任について当事者感覚を自覚し、情報セキュリティ基本方針を遵守して信義に従い誠実に行動することを求めます。

（目的）

第１条　この情報セキュリティ基本方針（以下「基本方針」という。）は、本財団にとって事業運営上重要であり、かつ、部外に漏洩等した場合に極めて重大な結果を招く情報が多く含まれる情報資産について、機密性、完全性及び可用性を確保し、人的脅威、災害及び事故からの防止、検知並びに回復するため、本財団が組織的、かつ、計画的に取り組むために必要な統一的な方針として、基本的な考え方及び方策を定めることを目的とする。

（適用範囲）

第２条　この基本方針の適用範囲は、本財団定款第４条に規定する事業において、作成、取得及び確立された情報資産及び本財団が保有する情報資産並びに当該情報資産に接する役員及び職員（非常勤職員及び臨時職員を含む。以下「職員等」という。）とする。

（管理体制）

第３条　情報セキュリティを確保するため、本財団に「情報管理担当」を設置する。

２　情報管理担当は、「統括情報管理責任者」「情報管理責任者」「情報管理担当者」をもって構成する。

３　統括情報管理責任者は、理事長が兼任する。

４　統括情報管理責任者の所掌事項は、次の各号に掲げる事項とする。

（１）　情報セキュリティポリシーの発布

（２）　情報セキュリティポリシーに違反した職員等への懲戒処分等の決定

（３）　情報管理責任者は、事務局長が兼任する。

５　情報管理責任者の所掌事項は、次の各号に掲げる事項とする。

（１） 情報セキュリティポリシーの評価
（２） 情報セキュリティに関する監査
（３） 事務局員から発信されるメールの監視
６　情報管理担当者は、事務局・総務担当職員が担当する。
７　情報管理担当者の所掌事項は、次の各号に掲げる事項とする。
（１） 情報セキュリティポリシーの見直し
（２） 情報セキュリティポリシーの遵守状況の確認
（３） 情報セキュリティに関する実施計画の策定
（４） 情報セキュリティの実施及び情報管理責任者への報告
（５） 情報セキュリティに関する教育及び研修の実施

（情報の管理及び分類）
第４条　情報資産については、情報の機密性、完全性及び可用性を踏まえた情報資産の分類を行い、その重要性に応じ、適切な管理を行うものとする。

（情報資産に対する脅威）
第５条　「情報管理担当」は、情報資産に対する脅威について、その発生度合い及び発生した場合の影響を考慮し、情報セキュリティポリシーを策定し、実施する。
２　前項における脅威は、次の各号に掲げるところによるものとする。
（１） アクセス権限を有しない者による故意の不正アクセス又は不正操作による情報資産の持出・盗聴・改ざん・消去、機器及び記録媒体の盗難等
（２） 職員等による意図しない操作、故意の不正アクセス又は不正操作による情報資産の持出・盗聴・改ざん・消去、機器及び記録媒体の盗難等
（３） 誤作動による改ざん・消去・停止等
（４） 地震、落雷、火災等による災害、事故及び故障等

（情報セキュリティ対策）
第６条　情報資産を前条の脅威から守るため、次の各号に掲げる対策を講ずるものとする。
（１）人的セキュリティ対策
情報セキュリティに関する権限、責任及び遵守すべき事項を明確に定め、職員等に周知及び徹底を図るとともに、十分な教育・啓発が行われるよう人的な対策を講ずる。
（２）物理的セキュリティ対策
情報資産を使用及び保管する施設への不正な立入り、情報資産への損害及び利用の妨害等から保護するための物理的な対策を講ずる。
（３）技術的セキュリティ対策
情報資産を不正アクセス等から保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術的な対策を講ずる。

（４）運用等における対策

情報資産へのアクセスの監視、情報セキュリティ対策の遵守状況の確認等の運用における対策を講ずる。

（５）緊急時におけるセキュリティ対策

緊急事態が発生した場合に、迅速、かつ、適切な対応が可能となるような危機管理対策の整備等による緊急時の対策を講ずる。

（情報セキュリティ対策基準の策定）

第７条　このセキュリティ基本方針に基づき、情報セキュリティ対策を実施するに当たっての遵守すべき事項及び判断等の統一的な基準として「情報セキュリティ対応計画」（以下「対応計画」という。）を定めるものとする。

（対応計画の扱い）

第８条　対応計画については、これらを原則非公開とする。

（職員等の義務）

第９条　職員等は、情報セキュリティに関係する法令及び契約等情報セキュリティの重要性について共通の認識を持つと共に、事業の遂行に当たり、情報セキュリティポリシーを遵守する義務を負うものとする。

（職員等に対する処分）

第１０条　情報セキュリティポリシーに違反した職員等については、その重大性又は発生した事案の状況等に応じて、懲戒処分等を行うものとする。懲戒処分等の詳細については、理事会の議を経て統括情報管理責任者が決定する。

（情報セキュリティ意識の啓発）

第１１条　「統括情報管理責任者」は、職員等に対し情報セキュリティ意識の周知徹底のため、計画的な教育・研修などの必要な措置を講ずるものとする。

（評価及び見直し）

第１２条　情報セキュリティ監査の結果等により、必要に応じこの基本方針、対策基準及び実施手順の見直しを行うものとする。

附則

この基本方針は、平成２９年３月２４日より施行する。