このNPOの情報セキュリティ規程には、いくつかの不足している点や矛盾が見受けられます。以下に主な点を指摘します。
・組織的対策の不足: NPOは常任スタッフがいないとの前提がありますが、情報セキュリティ委員会や役割・責任の定義が常任スタッフを前提としているように見えます。非常勤やボランティアスタッフの役割と責任についても明確にする必要があります。
・基幹ITシステムの不在: 基幹ITシステムがなく、Excelベースでデータ管理が行われているとのことですが、データのバックアップやアクセス制御に関する記述が不足しています。Excelベースの管理におけるセキュリティ対策を具体的に定める必要があります。
・リモート会議のセキュリティ対策: 会議体がほぼリモート会議であるとのことですが、リモート会議のセキュリティ対策に関する記述が見当たりません。リモート会議のためのセキュリティガイドライン（例えば、使用するツールのセキュリティ設定、参加者の認証方法など）が必要です。
・物理的対策の不足: 物理的対策に関する記述が非常に限定的です。特に、NPOがオフィスを持たない場合や、スタッフが自宅で作業をする場合の物理的セキュリティ対策についても言及する必要があります。
・個人デバイスの使用ポリシー: スタッフが個人のデバイスを業務に使用する場合のポリシーが不足しています。BYOD（Bring Your Own Device）ポリシーを設け、個人デバイスのセキュリティ要件やデータ管理方法を明確にする必要があります。
・データ廃棄ポリシーの不足: データの廃棄方法に関する記述が不足しています。特に、電子データの安全な廃棄方法についてのガイドラインが必要です。
・緊急時の連絡体制の不明確さ: インシデント発生時の連絡体制が不明確です。非常時の連絡網や、インシデント発生時の対応フローをより詳細に記述する必要があります。 これらの点は、NPOの情報セキュリティ管理体制を強化するために重要です。特に、非常勤スタッフやリモートワークの増加に伴い、これらの対策を適切に実施することが不可欠です。