電子決済手段関連業務に係る情報の安全管理に関する規則 （2024 年●月●日　制　　定）	「電子決済手段関連業務に係る情報の安全管理に関する規則」に関するガイドライン （2024 年●月●日　制　　定）
第 1 章 総則	
（目的） 第 1 条　本規則は、第一種会員（電子決済手段）が行う電子決済手段関連業務における情報の安全管理のための基本的な事項を定めることを目的とする。	
（情報の安全管理措置） 第 2 条　第一種会員（電子決済手段）は、情報の漏えい、滅失、毀損又は盗難の防止その他の情報の安全管理のために必要な措置を講じなければならない。 2　第一種会員（電子決済手段）は、自らの業務の内容及び方法に応じ、協会が別に定める「電子決済手段関連業務に係るシステムリスク管理に関する規則」に従い、情報の安全管理のためにシステムリスク管理を行わなければならない。	
（緊急時対応等） 第 3 条　第一種会員（電子決済手段）は、協会が別に定める「電子決済手段関連業務に係る緊急時対応に関する規則」に従い、情報の安全を脅かす緊急事態が生じた場合の対応等を定めなければならない。	
（基本姿勢） 第 4 条　第一種会員（電子決済手段）は、情報の安全管理に関する方針を示し、計画的に運用しなければならない。 2　第一種会員（電子決済手段）は、情報の安全管理に要する資源（人的資源を含む。）を適切に配分しなければならない。 3　第一種会員（電子決済手段）は、情報の安全管理の実施状況を把握し、その有効性について評価しなければならない。 4　第一種会員（電子決済手段）は、情報の安全管理上、不適合な状況が生じた場合には、速やかにこれを是正し、情報の安全管理体制を継続的に改善していかなければならない。	
第 2 章 基本方針	
（情報セキュリティ方針等） 第 5 条　第一種会員（電子決済手段）は、以下の内容を含む情報資産の安全管理に関する基本方針（以下、「情報セキュリティ基本方針」という。）を定め、その概要を公衆縦覧に供しなければならない。なお、本規則において、「情報資産」とは、安全管理の対象となる情報及び当該情報を管理又は保管する仕組み（電子機器及び紙の資料を含むがこれに限られない。）をいう。 (1) 情報セキュリティの目標 (2) 目標達成のためにとるべき行動 (3) 情報セキュリティが必要な理由 (4) 対象範囲とセキュリティの程度 (5) 外部委託先における情報資産の安全管理に関する方針 (6) 情報セキュリティの責任者	第 5 条第 1 項関係 情報セキュリティ基本方針の概要を公衆縦覧に供する方法としては、例えば、会員のウェブサイトに掲載する方法が考えられます。公表することにより、情報の安全管理に支障が生じるような内容は、情報セキュリティ基本方針の概要に含めるべきではありません。

2　第一種会員（電子決済手段）は、前項により策定する方針に基づく具体的な実施事項及び体制、役割、責任者を明らかにし、これらを業務活動に組み入れ、機能させるために必要となる社内規定を整備しなければならない。 3　第一種会員（電子決済手段）は、前項の規定を実践するための手順その他具体的な行動を明らかとする情報セキュリティ対策手順書を策定しなければならない。 4　第一種会員（電子決済手段）は、情報セキュリティ対策の遵守、運用状況を記録し、保管しなければならない。	
第 3 章 体制の整備	
（組織体制） 第 6 条　第一種会員（電子決済手段）は、情報の安全管理の目的及び実施体制等の枠組みを示さなければならない。 2　第一種会員（電子決済手段）の経営陣は、業務の仕組みに情報の安全管理のために必要な措置を組み入れ、業務体制を整備しなければならない。 3　第一種会員（電子決済手段）の経営陣は、役職員等（情報の安全管理の対象とする業務の一部を外部に委託する場合にあっては、当該外部委託先を含む。以下、この条において同じ。）を指揮し、情報の安全管理に対する役職員の取り組みを支援しなければならない。 4　第一種会員（電子決済手段）の経営陣は、役職員等に情報の安全管理の重要性を伝達し、かつ、成果達成の意識を高めるために必要な措置の実施に努めなければならない。 5　第一種会員（電子決済手段）の経営陣は、コンピュータシステムの不正使用防止対策、不正アクセス防止対策、コンピュータウィルス等の不正プログラムの侵入防止対策等を実施しなければならない。 6　第一種会員（電子決済手段）の経営陣は、他社における不正・不祥事件も参考に、情報の安全管理体制の PDCA サイクルによる継続的な改善を図らなければならない。	
（情報セキュリティ委員会の設置） 第 7 条　第一種会員（電子決済手段）は、情報の機密性、完全性、可用性を維持するために、次の各号の役割を担う情報セキュリティ委員会を設置しなければならない。 (1) リスク管理の環境整備 (2) 情報の安全管理に関する文書の決定 (3) 情報の安全管理に関する施策の策定及び改訂 (4) 発生したセキュリティ問題の検討 (5) 情報の安全管理の運用評価に基づく改善 2　第一種会員（電子決済手段）は、前項の委員会を管掌する役員を任命しなければならない。 3　第一種会員（電子決済手段）は、第 1 項の委員会が有効に機能するために必要な人員その他の経営資源を配備しなければならない。	第 7 条第 2 項関係 情報セキュリティ委員会を管掌する役員（情報セキュリティ最高責任者）については、会員における情報の安全管理の最高責任者としての権限と責任を有する限り、必ずしも会社法上の役員に限定するものではありません。また、情報セキュリティリスクは、システムリスクの 1 つとして位置付けられるものであるため、会員の規模や業容に応じて、「電子決済手段関連業務に係るシステムリスク管理に関する規則」第 5 条に定めるシステムの統括責任者が情報セキュリティ最高責任者を兼ねることも合理的であると考えられます。
（情報セキュリティ最高責任者） 第 8 条　前条第 2 項により任命された役員は、情報セキュリティ最高責任者として、情報セキュリティ委員会を運営するほか、次の各号の役割を担うものとする。 (1) 情報管理責任者の監督 (2) 取締役会への情報セキュリティに係るリスク管理状況の報告	

(3) 重大インシデント発生時の対応指揮（当局等への外部連絡を含む。） 2　情報セキュリティ最高責任者は、協会が別に定める「電子決済手段関連業務に係るシステムリスク管理に関する規則」第6条に規定するシステム統括管理責任者を兼務することができる。	
（情報管理責任者の設置） 第9条　第一種会員（電子決済手段）は、部署又は業務単位ごとに情報管理責任者を設置しなければならない。 2　情報管理責任者は、部署等に存在する情報資産を把握し、その利用及び保管方法その他日常業務における情報の安全管理に必要とする事項を取りまとめ、管理状況を記録し、管轄する業務に関わる役職員の情報資産の安全管理を指導しなければならない。 3　情報管理責任者は、管理対象とする情報資産の漏えいその他情報の安全管理上の問題が発生した場合には、直ちに情報セキュリティ最高責任者に報告しなければならない。 4　情報管理責任者は、協会が別に定める「電子決済手段関連業務に係るシステムリスク管理に関する規則」第 7 条に規定するシステム管理責任者を兼務することができる。	第9条関係 企業規模にもよりますが、日常の業務管理においても情報の安全管理は必要となることから、部署単位又は業務単位での責任者を設けて、かつ、横断的な監督を図る趣旨です。例えば、一人のみ配置されている部署であれば、当該者を情報管理責任者として指名することになります。
（モニタリング） 第10条 第一種会員（電子決済手段）は、情報資産が適切に管理されていることを定期的にモニタリングし、管理体制を継続的に見直さなければならない。	
（社員教育） 第11条 第一種会員（電子決済手段）は、セキュリティ意識の向上を図るため、全役職員に対するセキュリティ教育（外部委託先におけるセキュリティ教育の実施状況の確認等を含む）を行なわなければならない。	
第 4 章 リスク管理	
（リスク管理プロセス） 第12条　第一種会員（電子決済手段）は、情報の安全管理に影響を及ぼす組織内外の状況を把握し、リスクアセスメントを行わなければならない。 2　第一種会員（電子決済手段）は、前項の結果を踏まえ、情報の安全管理に係るリスクを低減しなければならない。 3　第一種会員（電子決済手段）は、第2項の結果及び前項による低減後のリスクを用いて情報の安全管理の仕組みに期待された成果との差異を特定し、当該仕組みの適切性、妥当性、有効性を検証しなければならない。 4　第一種会員（電子決済手段）は、前項の検証結果を利用し、情報の安全管理の改善を継続して行わなければならない。	
（リスク基準） 第13条 第一種会員（電子決済手段）は、リスク管理を行うため、次の各号を含むリスク基準を定めなければならない。 (1) リスク受容基準（組織として保有することを許容するリスク水準） (2) 情報セキュリティアセスメントを実施するための基準	
（リスク特定） 第14条　第一種会員（電子決済手段）は、情報の安全管理に係るリス	

クとその所有者を特定しなければならない。 2　第一種会員（電子決済手段）は、第 1 項の特定のために情報資産の目録を作成し、以下の各号の事項を明らかとしなければならない。 (1) 資産の重要度又は資産価値 (2) 各情報資産の管理責任者 (3) 各情報資産における脅威 (4) 各情報資産の脅威に対する安全管理上の脆弱性	
（リスク分析） 第 15 条　第一種会員（電子決済手段）は、リスクの発生する可能性及び発生時の結果を分析し、リスクレベルを決定しなければならない。 2　第一種会員（電子決済手段）は、次の各号のいずれか又は組み合わせてリスク分析を行わなければならない。 (1) ベースラインアプローチ（既存の標準や基準をベースラインとして策定し、チェックする方法） (2) 非形式的アプローチ（熟練者の知識や経験に頼ったアプローチ） (3) 詳細リスク分析（情報資産ごとに資産価値、脅威、セキュリティ要件を識別して評価する手法） 3　リスク分析は、他社における不正、不祥事件も参考として行わなければならない。	
（リスク評価） 第 16 条　第一種会員（電子決済手段）は、前条の結果と第 13 条のリスク基準を比較し、リスク対応のための優先順位を決定しなければならない。	
（リスク対応） 第 17 条　第一種会員（電子決済手段）は、リスクを有する情報資産について、次の各号のいずれかの方法又は組み合わせることにより、第 13 条第 1 号により定めるリスク受容基準を満たすための対応方針を決定しなければならない。 (1) リスク低減 (2) リスク回避（リスクに関係する業務及び情報資産の廃止・廃棄） (3) リスク共有（情報資産あるいは安全管理対策の外部委託又は保険によるリスクファイナンスなど契約等）	
（管理策の決定） 第 18 条　第一種会員（電子決済手段）は、前条の対処方針を具体化し、情報の安全管理策を決定しなければならない。 2　第一種会員（電子決済手段）は、前項の管理策と管理策を採用した理由を記載した文書を作成し、保管しなければならない。	
（情報の安全管理計画書の作成） 第 19 条　第一種会員（電子決済手段）は、前条の管理策の実行計画を情報の安全管理計画書として取りまとめなければならない。 2　前項の計画書の作成は情報セキュリティ委員会の管掌とし、当該計画は取締役会決議により決定しなければならない。	
（残留リスクの承認） 第 20 条　第一種会員（電子決済手段）は、情報の安全管理リスク計画	

書に記載する各情報資産に対するリスク所有者に対し、当該計画と受容リスクについて十分に説明を行い、了解を得なければならない。	
第 5 章 利用者の重要情報等	
（洗い出し） 第 21 条　第一種会員（電子決済手段）は、当該会員が責任を負うべき利用者の重要情報を網羅的に洗い出し、把握、管理しなければならない。 2　前項の洗い出しについては、次の各号を含め、業務、システム、外部委託先を 対象範囲として行わなければならない。 (1) 通常の業務では使用しないシステム領域に格納されたデータ (2) 障害解析のためにシステムから出力された障害解析用データ (3) 使用を終え収納された文書	
（利用者の重要情報に係る管理ルール） 第 22 条　第一種会員（電子決済手段）は、利用者の重要情報に関し、それぞれの重要度及びリスクに応じ、次の 各号の情報管理ルールの策定し、管理しなければならない。 (1) 情報の暗号化、ハッシュ化及びマスキングのルール (2) 情報を利用する際の利用ルール (3) 記録媒体等の取扱いルール 等	第 22 条関係 利用者の重要情報とは、業務上収集、蓄積、利用される顧客に関するすべての個人情報（氏名、生年月日、取引内容等）及び法人情報（代表者、決算内容、取引内容等）のうち、漏えい等の問題が起きた場合に顧客に影響を与えるおそれのある情報をいいます。
（重要情報の取扱い） 第 23 条　第一種会員（電子決済手段）は、利用者の重要情報について、次の各号の不正アクセス、不正情報取得、情報漏えい等を牽制、防止する仕組みの導入に努めなければならない。 (1) 職員の権限に応じて必要な範囲に限定されたアクセス権限の付与 (2) アクセス記録の保存、検証 (3) 開発担当者と運用担当者の分離、管理者と担当者の分離等の相互牽制体制 (4) システムテスト等を実施する際のテスト環境と本番環境の分離 等	
（機密情報の取扱い） 第 24 条　第一種会員（電子決済手段）は、利用者の重要情報のうち、利用者に損失が発生する可能性のある情報（機密情報）のうち、次の各号に掲げる情報について、暗号化、ハッシュ化及びマスキング等の管理ルールを定めなければならない。 (1) 暗号鍵等 (2) 暗証番号 (3) パスワード (4) クレジットカード情報 (5) その他利用者に損失が発生する可能性のある情報 2　第一種会員（電子決済手段）は、前項に関し、暗号化プログラム、暗号鍵、暗号化プログラムの設計書等の管理に関するルールを定めなければならない。 3　第一種会員（電子決済手段）は、機密情報の保有・廃棄、アクセス制限、外部持ち出し等について、業務上の必要性を十分に検討し、より厳格な取扱いをしなければならない。	
（個人情報）	第 25 条第 2 項関係

第 25 条　第一種会員（電子決済手段）は、利用者に関する情報管理の適切性を確保する必要性及び重要性を認識 し、適切性を確保するための組織体制の確立、社内規程の策定等、内部管理体制の整備を図らなければならない。 2　第一種会員（電子決済手段）は、利用者の個人情報の取扱いについて、法令、保護法ガイドライン、金融分野ガイドライン、実務指針の規定に従って、取扱基準を定めなければならない。 3　第一種会員（電子決済手段）は、利用者に関する情報へのアクセス管理の徹底、情報の持ち出しの防止に係る対策、外部からの不正アクセスの防御等情報管理システムの堅牢化を図らなければならない。	利用者の個人情報の取扱基準においては、利用者の個人情報の具体的な取扱いを行う際の具体的なルールや手続を定めることが必要となります。これらの内容が適切に定められている限り、名称が「取扱基準」でなくても支障はありません。
（取引時確認等により取得する個人情報の取扱い） 第 26 条　第一種会員（電子決済手段）は、マネー・ローンダリング及びテロ資金供与対策に係る業務により取得した個人情報データの取扱いについては、「電子決済手段関連業務に係るマネー・ローンダリング及びテロ資金供与対策に関する規則」に従い、保管及び廃棄を適切に行わなければならない。	
附則 この規則は、●年●月●日から施行する。	附則 このガイドラインは、●年●月●日から施行する。