資料３－２

セキュリティポリシー策定に向けて

一 部 抜 粋

平成１３年３月

社団法人全国信用金庫協会

3.セキュリティポリシー例

(1) 情報資産保護に関する基本方針

○○信用金庫 情報資産保護に関する基本方針
(セキュリティポリシー)

1　総則

1－1　目的

当金庫は金融機関としての社会的責任を果たすため、当金庫が保有する情報資産（以下「情報資産」という。）を適切に保護し管理しなければならない。万が一にも情報資産の漏洩、紛失、不正使用、改ざん（以下「漏洩等」という。）が行われ、または災害、故障その他の理由により情報システムが停止した場合には、当金庫の業務遂行に重大な影響が及ぶことはもとより、企業イメージが低下し信用が失墜することにより当金庫に多大な損失がもたらされ、地域の中小企業者や住民の方々にご迷惑をおかけすることになる。このため当金庫は情報資産の安全対策に関する基本方針として、本情報資産保護に関する基本方針（以下「本基本方針」という。）を定めた。

1－2　本基本方針の位置付け

本基本方針は、情報資産の保護に関する諸規定の最上位に位置するものであり、情報資産保護のための具体的施策に関しては安全対策基準をはじめとする関連規定・規則に定めるものとする。

1－3　役職員の責務

当金庫の役職員（時間労働者、派遣社員、短期労働者を含む。以下において同じ。）は本基本方針が有効に機能するように努めなければならない。

2　情報資産

2－1　情報資産の定義

情報資産とは、当金庫が保有する各種情報と、各種情報を適切に処理しまたは各種情報が正当に保護され、使用されるための情報システムの総称であり、以下のとおり分類する。

①　情報の分類

最重要情報　漏洩等の行為がなされることにより、当金庫の顧客に多大な影響を与え、または当金庫への信頼を著しく失墜させる可能性のある情報

重要情報　漏洩等の行為がなされた場合の影響が、当金庫内に限られると判断できる情報

一般情報　最重要情報、重要情報に該当しない情報

② 情報システムの分類

最重要システム　障害等が発生した場合に、当金庫の顧客や金融システムに多大な影響を与え、または当金庫への信頼を著しく失墜させる可能性のある情報システム

重要システム　障害等の発生が当金庫の業務に及ぼす影響は比較的大きいが致命的大きさにはならないと判断される情報システム

一般システム　障害等の発生による影響が当金庫内に限定されると判断できる情報システム

２－２　情報資産の保護

情報資産の保護に関しては、各情報資産の重要度やそれを取り巻く脅威および脅威の顕在化の可能性を考慮した上で現状での技術水準やコストを認識し、合理的なリスク対策を行う。

３　セキュリティ管理体制

３－１　セキュリティ管理体制の整備

（１）セキュリティ統括責任者として情報セキュリティ担当役員をおく。

（２）情報セキュリティの維持管理を当金庫全体で統一的に行うために、情報セキュリティ統括部門を設置するとともに必要な体制を整備する。

（３）情報セキュリティ統括部門は○○部とし、○○部は関係する部署と連携して情報セキュリティに関する各種規定を確立するとともにその周知徹底に対して責任を負うものとする。

（４）各部門長は、自部門における情報資産の適切な使用と管理に対して責任を負う。また、部門内にセキュリティ担当者を任命する。

３－２　検査体制

当金庫は情報資産が適切に保護・管理されていることを確認するため、検査部門による内部検査時にその検証を行う。検査部門は検証の結果を情報セキュリティ統括責任者に報告する。

４　遵守のための方策

４－１　役職員の遵守

当金庫の役職員は原則として本基本方針に反する行為を行ってはならず、本基本方針に反する行為の命令を行ってはならない。

４－２　外部委託先への協力要請

当金庫は、外部委託先に対し当金庫の役職員が本基本方針を遵守するべきことを説明したうえ、本基本方針が有効に機能するように協力を求めていくものとする。

４－３　例外の扱い

当金庫の役職員は、本基本方針および安全対策基準をはじめとする関連規

定・規則（以下「本基本方針等」という。）に定められていない事象に遭遇した場合や、業務上の諸事情により本基本方針等に反さざるを得ない事象に遭遇した場合には、速やかに情報セキュリティ統括部門に報告し、指示を仰ぐこととする。

４－４　本基本方針等の範囲

４－３の本基本方針等とは、次に掲げる規定等をいう。

① 顧客情報管理規定
② 電子情報管理規定
③ 機器設備管理規定
：
：

５　危機管理

本基本方針等への重大な違反行為があった場合や、当金庫の情報システム等に災害、事故等による危機的状況が発生した場合には、別に定める危機管理計画に基づき事態への対応を行う。

６　権利の制限

本基本方針で定めた情報資産はすべて当金庫の資産である。したがって安全対策のため、それらの内容や記録を検査することがある。

７　本基本方針の検証と改廃

（１）情報セキュリティ統括部門は、ビジネス環境の変化や技術の進展等を考慮して、保護すべき情報資産およびセキュリティ管理体制を見直すものとする。
（２）本基本方針の制定および改廃は、理事会決議をもってこれを行う。

付則

本基本方針は、平成１３年〇月〇日より施行する。

4.セキュリティスタンダード例

（1）情報資産保護に関する規定集

①顧客情報管理規定

1.　目　　的

この規定は、当金庫が業務を通じて接する顧客に関する情報について、金融機関としての社会的信義をまっとうし適切な利用を行うとともに、顧客の権利利益を保護することを目的として定める。

2.　定　　義

この規定で使用する用語は、以下のとおり定義する。

（1）　顧　　客　当金庫の営業活動の対象となる個人または法人をいう。

（2）　顧客情報　顧客に関する情報であり、顧客の住所・所在地、氏名・名称、電話番号や映像、音声など該当顧客を識別できる情報をいう。

3.　適用範囲

この規定は、当金庫役職員の業務活動について適用する。

4.　顧客への周知

4. 1. 顧客情報の収集に当たっては、収集した情報の取り扱いについて当該顧客に周知するものとする。ただし、顧客との日常会話等により偶然知り得た情報に関してはこの限りではない。

4. 2. 前項に規定する周知の方法については店頭、電話、インターネット等、当該顧客との取引に用いられた手法に応じて適切な方法を選択する。

5.　顧客情報の収集範囲

顧客情報の収集は、業務上必要と認められる事項についてのみ収集するものとし、顧客の意に反した情報の収集は行ってはならない。

6.　収集方法の制限

顧客情報の収集は、適法かつ適正な方法によって行わなければならない。

7.　収集情報の制限

顧客情報のうち個人に関するセンシティブな情報（本籍地、思想、保健医療等）については、顧客の明確な同意がある場合または法令に特段の定めがある場合を除き、これを収集、利用してはならない。

8.　利用範囲の制限

顧客情報は、正当な業務の範囲内でのみ利用することとし、一般的に合理的と考えら

れる範囲を超えて利用目的を変更してはならない。

９．　目的外の外部提供の禁止

顧客情報の外部者への提供は、当該情報の収集目的の範囲を超えてはこれを行わないものとする。ただし、予め顧客から文書により同意を得ている場合には、この限りではない。

１０．　目的外の利用

次にあげる場合には、前条の規定にかかわらず、収集目的の範囲外であっても、当該顧客情報を外部者に提供することができるものとする。

（１）　顧客の利益(財産、生命等)を守るために必要な場合。

（２）　当金庫が従うべき法的義務の履行のために必要な場合。

１１．　顧客情報の正確性確保

顧客情報は、利用目的に応じ必要な範囲内において、正確かつ最新の状態で管理するものとする。

１２．　顧客情報の利用の安全性確保

顧客情報への不当なアクセスまたは顧客情報の紛失、破壊、改ざん、漏洩などのリスクに対して、技術面および組織面において合理的な安全対策を講じるものとする。

１３．　従事者の秘密保持に関する責務

当金庫の役職員が顧客情報の収集・利用・提供を行う場合には、この規定のほか当金庫が定める情報セキュリティに関する諸規定および法令に従い、顧客情報の秘密保持に十分な注意を払うものとする。

１４．　顧客情報の処理委託に関する事項

１４－１情報処理を委託するなどのため顧客情報を外部に預託する場合には、顧客情報についての十分な保護水準を維持しうる者を当該委託先として選定するものとする。

１４－２前項に掲げる委託先との契約においては、次の各号に掲げる事項を明確にするものとする。

（１）当該委託先では、管理者の指示を遵守すべきこと

（２）当該委託先では、当金庫が預託する顧客情報に関する秘密を保持すべきこと

（３）当該委託先では、当金庫からの委託事項を第三者に再委託しようとする場合には、予めその旨を当金庫に報告するとともに、当該再委託先との契約において前２号に掲げる事項を明確にすべきこと

１５．　顧客の権利

顧客から、当金庫が保有する当該顧客に関する顧客情報について開示を求められた場合には、原則として合理的な期間内にこれに応じるものとする。また、開示の結果、合理的な理由をもって訂正または削除を求められた場合には、原則として合理的な期間内

にこれに応じるとともに、当該顧客情報の利用者に対して可能な範囲内で訂正または削除の内容を通知するものとする。

１６．　自己情報の利用または提供に関する顧客の拒否権

顧客から自己に関する情報の利用または第三者への提供を拒まれた場合は、原則としてこれに応じるものとする。ただし、法令にもとづく公権力の行使または義務の履行のために必要な場合については、この限りではない。

１７．　規定の遵守

当金庫は、全役職員にこの規定を十分理解させ遵守させなければならない。

附　則

1.　この規定は、　年　月　日より実施する。
2.　この規定の改廃は、セキュリティー委員会の承認を得て行う。
3.　この規定は法制度の変更や社会通念の変化などに応じて見直しを行う。

④外部委託管理規定

1. 目　　的

この規定は、当金庫が業務を行うに際し必要となる情報の処理または情報処理システムの提供（以下「情報の処理等」という。）を外部に委託する場合に、当金庫ならびに当金庫の顧客および取引先などの情報を適切に保護するとともに、当金庫が外部委託先から提供を受ける情報の処理等にかかるサービスのレベルを適切に維持することを目的として定める。

2. 定　　義

この規定で使用する用語は、以下のとおり定義する。

（1）　外部委託先　　当金庫が情報の処理等を委託する外部業者をいう。

（2）　サービスレベル　当金庫が外部委託先から提供を受ける情報の処理等に関するサービスの信頼、安全および効率面での品質をいう。

3. 適用範囲

この規定は、当金庫が重要として位置づける情報の処理等を、信金○○共同事務センターを除く外部業者に委託する場合に適用する。

4. 外部委託先の選定および契約

4.1 外部委託先を選定する場合には、外部委託先が提供するサービスの内容とそのサービスレベルを予め定める。

4.2 外部委託先の選定に際しては、原則として複数の外部業者から当金庫が委託しようとする情報の処理等に関する提案を予め受け、当該提案により示されたサービスの内容、サービスレベルとコストパフォーマンスを比較することにより行うものとする。

4.3 情報の処理等を外部業者に委託する場合には、原則として当該委託に関する契約において当該外部委託先が当金庫のセキュリティポリシーを遵守する旨を明示するものとする。

5. 委託業務のモニタリング

外部に委託した情報サービスを所管する部門は、当該情報サービスの内容やレベルについて定期的に調査し、その結果を審査する。

附　則

1. この規定は、　年　月　日より実施する。
2. この規定の改廃は、セキュリティ委員会の承認を得て行う。