

## 情報セキュリティポリシー

実施	2005年	2月21日
改定	2006年	3月29日
改定	2007年	4月1日
改定	2008年	8月1日
改定	2011年	1月7日

### 第1条 目的

企業が保有する情報資産を適切に保護することは企業の社会的責任であり、情報資産を適切に利用することは企業の競争力の源泉である。

株式会社みずほトラストシステムズ（以下、当社という）にとって、情報資産の適切な保護と利用は極めて重要である。

この情報セキュリティポリシー（以下、本ポリシーという）は、当社の「情報管理に関する基本的考え方」に基づき、当社の情報資産の適切な保護と利用についての基本的な取組方針を定めるものである。

本ポリシーが有効に機能するよう、経営者を含め全ての役員および社員がこれに関与し、これを支持しなければならない。

外部委託先等関係者より、当社の情報管理に関する基本方針文書の開示を求められた場合は、本ポリシーを交付することができる。

### 第2条 定義

#### 1. 情報

本ポリシーにおいて「情報」とは、当社が保有または作成する全ての情報をいい、公開・非公開の別や形態（紙文書や電子データ上の情報、映像・音声情報等）を問わない。

#### 2. 情報資産

本ポリシーにおいて「情報資産」とは、「情報」、「情報」の取扱いに係る当社のシステム・機器類・記録媒体等、およびシステム・機器類・記録媒体等を保護し正常に稼働させるために必要な施設・設備等の全てをいう。

上述の「システム」とは、コンピュータ関連のハードウェア、ソフトウェアおよびネットワーク等をいい、「機器類」とは、情報の記録・保存・伝送等を行うために使用する機器類（システムを除く）をいい、「記録媒体等」とは、紙媒体（情報を記録・保存している帳票等の紙）および記録媒体（情報を記録・保存する媒体で、紙媒体以外のもの）をいう。

本ポリシーにおいて「システム等」とは、システムおよび機器類をいう。

#### 3. 情報セキュリティ

本ポリシーにおいて「情報セキュリティ」とは、当社の「情報資産」を様々な脅威（災害、故障、誤処理、漏えい、盗難、不正使用、破壊、改ざん等）から保護することをいう。

#### 4. 情報管理

本ポリシーにおいて「情報管理」とは、「情報セキュリティ」対策の実施等を通じた「情報資産」の機密性・完全性・可用性の確保、個人情報に係る情報主体からの開示等の請求等への

対応など、当社の「情報資産」の適切な保護と利用に係る全ての行為をいう。

上述の「機密性」とは、アクセスを認可された者だけが情報資産にアクセスできることを確実にすることをいい、「完全性」とは、情報および処理方法が、正確であることおよび完全であることを保護することをいい、「可用性」とは、認可された利用者が、必要なときに、情報資産にアクセスできることを確実にすることをいう。

#### 5. 情報セキュリティに係るリスク

本ポリシーにおいて「情報セキュリティに係るリスク」とは、当社の「情報資産」に対する様々な脅威により、お客さまへのサービスに混乱をきたす、またはお客さまの決済システムに重大な影響を及ぼす等、お客さまに損失が発生するリスクおよび当社が有形無形の損失を被るリスクのことをいい、システムリスク、事務リスク等から構成される。

#### 6. 情報セキュリティに係るリスク管理

本ポリシーにおいて「情報セキュリティに係るリスク管理」とは、情報セキュリティに係るリスクの所在・規模・性質を適時かつ正確に把握し、適切な対応を行うことをいう。

### 第3条 適用範囲

本ポリシーの適用対象は、当社内の全組織および全ての役員および社員とする。

当社は、外部委託先社員や派遣社員等、当社と直接雇用契約がない者に対しても、外部委託契約や守秘義務契約等の締結や誓約書の徴求等により、本ポリシーに準拠した行動を求めることとする。

### 第4条 情報資産の分類等

当社は、当社の情報資産について、その重要性や利用状況等に応じた適切な管理を行うことを通じて機密性・完全性・可用性を確保するため、以下の通り重要度の分類を設定する。

#### 1. 情報の分類

##### (1) 最重要

漏えい等が生じた場合、顧客等の情報主体、あるいは当社の経営や業務に対して極めて重大な影響を及ぼす恐れがあるため、特に厳格な管理を要する情報

##### (2) 重要

漏えい等が生じた場合、顧客等の情報主体、あるいは当社の経営や業務に対して重大な影響を及ぼす恐れがあるため、厳格な管理を要する情報

##### (3) 一般

漏えい等が生じた場合、顧客等の情報主体、あるいは当社の経営や業務に対して影響を及ぼす恐れがあるため、管理を要する情報

##### (4) 公開

当社が作成し、当社の外部に公開している情報

上述の「漏えい等」とは、漏えい（情報資産が外部に流出すること）、滅失（情報資産の内容が失われること）、き損（情報資産の内容が意図しない形で変更されること、あるいは内容を保ちつつも利用不能な状態となること）をいう。

記録媒体等は、そのなかに記録・保存されている情報の分類に応じて分類することを原則と

するが、下記2のシステム等と一体のものとして分類することも可とする。

## 2. 情報以外の情報資産（システム等）の分類

### （1）最重要

システム等が使用不能、またはシステム等の処理内容・出力結果に誤り等が発生した場合に、影響が当社外部・内部の極めて広範囲に渡り、かつ、代替手段・修復手段が限定されていることから、業務継続のためには当該システム等の速やかな復旧が必要になるシステム等

### （2）重要

システム等が使用不能、またはシステム等の処理内容・出力結果に誤り等が発生した場合に、影響が当社外部・内部の広範囲に渡り、かつ、代替手段・修復手段により、当面は主要業務を継続することが可能であるが、短期間の内に当該システム等の復旧が必要になるシステム等

### （3）一般

上記以外のシステム等

## 3. その他の情報の区分

当社は、上記1、2の分類とは別に、情報主体の区別や法令等の要請等に応じて、「顧客情報」「個人情報」「センシティブ情報」「生体認証情報」「インサイダー情報」等の区分を制定し、必要に応じて個別の管理方法を定める。

## 第5条 情報管理の原則

### 1. コンプライアンス（法令等遵守）

当社は、業務の遂行において使用する情報管理に係る関係法令等を遵守する。

役員および社員は、情報管理に係る関係法令等および本ポリシー等の社内規程に従わなければならない。また、役員および社員は、他の者に対して関係法令等および本ポリシー等の社内規程に違反する行為を誘動、命令してはならない。

役員および社員は、違反行為や漏えい等の事実またはその発生の兆候、情報セキュリティに係る問題点等を発見した場合には、速やかに情報管理責任者等の適切な権限者に報告し、その指示に従わなければならない。

### 2. 情報資産の外部持出し等・漏えい等の禁止

当社の情報資産（公開情報を除く）については、本ポリシー等の社内規程に基づき定められた承認手続等を経た場合を除き、当社の外部への持出しを禁止する。

役員および社員は、転勤・異動等に際しては、本ポリシー等の社内規程に基づき定められた承認手続等を経た場合を除き、元の所属部室から情報資産を持出してはならない。

役員および社員は、在任・在職中、退任・退職後、職務上・職務外を問わず、当社の情報について漏えい等を行ってはならない。

### 3. 情報資産の管理方法

当社は、当社の情報の各管理段階（取得・入力、利用・加工、保管・保存、移送・送信、消去・廃棄）において、情報資産の分類や記録媒体等の性質等に応じた適切な安全管理措置（組

織的・人的・物理的・技術的)を講じる。

管理の具体的方法については、本ポリシー等に基づいて各管理段階毎の安全管理に係る取扱規程を別途定めることとする。

## 第6条 組織的安全管理措置

当社の情報管理を適切に実施・推進するため、組織体制・規程等の整備等、適切な組織的安全管理措置を講じる。

### 1. 情報管理統括責任者の設置

当社の情報管理全般に係る企画、立案および推進を統括する役員として、情報管理統括責任者を設置する。

情報管理統括責任者は、情報管理に係る諸施策の実施について、関係部署の担当役員等と協議のうえ必要な措置を講ずる。

情報管理統括責任者はその職務を補佐するものとして「情報管理統括管理責任者」を任命することができる。

情報管理統括責任者は、情報管理統括管理責任者、および情報管理責任者等より報告・提言を受けるとともに、必要に応じて情報管理の観点から提言を行う。

### 2. 情報管理委員会の設置

当社の情報管理全般に関する事項について、組織横断的な審議を行うため、情報管理委員会を設置する。

情報管理委員会は、当社の情報管理に関する各種施策の推進状況、情報セキュリティに係るリスクの管理、個人情報保護法等の関係法令等への対応、情報管理に関する各種規程類等について審議を行う。

### 3. 組織の体制と役割

当社の情報管理を適切に実施・推進するため、以下の組織体制を構築する。

リスク管理部は、情報管理全般に関する企画、立案および推進を行い、コンプライアンス・プログラム等の策定・実施等を通じた適切な情報管理の実施を図る。

各部は、情報管理に係る事項について、定期的および必要に応じて都度、情報管理統括責任者や情報管理委員会等に報告を行う。

業務監査部は、情報管理に係る本ポリシー等の社内規程の遵守状況等の監査を行う。

### 4. 情報セキュリティに係るリスク管理の運営と管理方法

当社は、「オペレーショナルリスク管理の基本方針」に則り、複合的なリスクとして情報セキュリティに係るリスクを適時かつ正確に把握・モニタリングすることにより適切に管理する。

リスク管理部は、各種リスクが当社の情報セキュリティに与える影響等について、システムリスクは「システムリスク管理の基本方針」に従い、事務リスクは「事務リスク管理の基本方針」に従って適切な管理を行う。

リスク管理部は、情報セキュリティに係るリスク管理の企画運営に関する基本的事項を所管し、情報セキュリティに係るリスクを一元的に把握する。その管理の状況等について必要に応じ取締役会、経営会議および社長に報告を行うとともに、必要に応じ情報セキュリティに

係るリスク管理の観点からリスク管理担当役員に対して提言を行う。また、関係する各部と協議の上、情報セキュリティに係るリスク管理に関する基本的施策の立案・推進を行う。

#### 5. 各部における情報管理責任者の設置

情報管理責任者は、各部における情報管理について責任を負うとともに、従業員に対して、本ポリシーの周知徹底を図る。

情報管理責任者は、その職務を補佐する者を別途任命することができる。

情報管理責任者は、各部における従業員の役割等の明確化、情報の取扱状況の把握、本ポリシー等の社内規程の遵守状況に関する点検体制の整備等を行う。

情報管理責任者は、個人情報保護法に定義される個人データの安全管理に係る業務を遂行する個人データ管理者としての役割を合わせ担うものとする。

本ポリシーにおいて「従業員」とは、「役員および社員」、および外部委託先社員や派遣社員など、当社の組織内にあって直接または間接に当社の指揮監督を受けて当社の業務に従事している者全てをいう。

#### 6. 情報セキュリティスタンダードの策定と適用

当社は、本ポリシーに基づき、当社の情報管理の具体的な基準として情報セキュリティスタンダードを策定する。

情報セキュリティスタンダードの策定に際しては、関係法令等およびみずほ信託銀行株式会社他システムサービス提供先の「情報セキュリティスタンダード」を参照することとする。

当社の全ての社内規程やシステム等は、情報管理については本ポリシーおよび情報セキュリティスタンダードに従って規定・運用されるとともに、取扱う情報資産の分類等に応じた適切な情報セキュリティ対策を講じなければならない。

#### 7. 漏えい等への対処

当社は、当社において情報資産の漏えい等の事案が生じた場合、迅速かつ適切な対応を講じることができるよう、対応部署の確定、みずほ信託銀行他システムサービス提供先、顧客、監督当局をはじめ関係各所への連絡・報告、本人への通知、調査・再発防止策等の検討体制および対外公表等について体制を整備するとともに、具体的な対処方法を定めたマニュアル等を予め策定し、従業員に周知徹底する。

#### 8. 業務継続対策

当社は、災害や事故・障害等の発生等に際して、当社の重要な情報資産に対する損害の範囲および業務への影響を極小化するとともに、迅速かつ効率的な業務の復旧を行うため、適切な対策を講ずるとともに、その対策を定期的に確認し、必要な見直しを行う。

#### 9. 監査体制

当社は、各部において情報管理に係る関係法令等や本ポリシー等の社内規程が遵守されていることを検証するため、業務監査部において必要な体制の整備や監査計画の立案等を行い、定期的および必要に応じて都度、監査を実施する。

業務監査部は、監査結果について情報管理統括責任者及び社長に通知する。

### 第7条 人的安全管理措置（従業員の監督）

当社は、従業者による当社の情報資産の漏えい等や不適切な利用等を未然に防止するため、従業者に対して適切な監督を実施する。

1. 非開示契約等の締結等

当社は、個々の従業者との間で、採用・異動・退職時等において、業務上知り得た秘密に関する守秘義務を含む非開示契約の締結または誓約書の取得等を行う。

当社は、業務上知り得た秘密に関する守秘義務や、情報管理に係る関係法令等や本ポリシー等の社内規程に違反した場合に適用されうる処分を就業規則等に定める。

2. 従業者の役割・責任等の明確化

当社は、情報管理に関し、従業者の職務・権限や情報資産の分類、情報の各管理段階等に応じた適切な従業者の役割・権限・責任を定めて明確化する。

3. 教育・研修

当社は、従業者に対して、情報管理に係る関係法令等や本ポリシー等の社内規程の周知徹底と情報セキュリティ意識の向上を図る内容の教育・研修を計画的に実施する。

当社は、教育・研修の担当部門の明確化等、従業者に対する適切な教育・研修を行うための体制を整備する。

4. 遵守状況の確認

当社は、従業者による本ポリシー等の社内規程等の遵守状況について、定期的に記録・確認および点検・監査を実施する。

5. 懲戒等

当社は、情報管理に係る関係法令等や本ポリシー等の社内規程等への違反行為に対して厳正に対応する。

当社は、それらの違反行為を行った従業者、および当該違反行為に関係した従業者については、関係法令等や就業規則等に照らして懲戒等の処分や損害賠償の請求等を行うことがある。

## 第8条 物理的安全管理措置

当社は、正当なアクセス権限を有しない者による当社の情報資産へのアクセスや、漏えい等を防ぐため、施設等、システム等および記録媒体等について適切な物理的安全管理措置を講じる。

1. 施設等の管理

当社は、防犯・防災対策を講じる等、情報資産の分類等に応じて、施設の管理、入退館（室）の管理、鍵の管理を適切に実施する。

2. システム等の管理

当社は、情報を取扱うシステム等の不正使用、破壊、盗難等の防止や、漏水、火災、停電等の環境上の脅威による被害の回避または低減のため、部外者によるシステム等への接近の防止、盗難防止策等により、情報資産の分類等に応じて適切なシステム等の物理的な保護を講じる。

3. 記録媒体等の管理

当社は、記録媒体等の漏えい等や不正使用等を防止するため、記録媒体等の取得・入力、利用・加工、保管・保存、移送・送信、消去・廃棄の各段階における物理的な保護を社内規程

に定めてそれに従った運用を行う。

## 第9条 技術的安全管理措置

当社は、情報資産の適正な稼働等を確保するため、システム等および記録媒体等について適切な技術的安全管理措置を講じる。

### 1. 情報資産へのアクセスの管理

当社は、当社の情報資産への無資格者によるアクセスや許可された範囲を越えるアクセス等を防止するため、当社が承認した有資格者にのみアクセスを許可するとともに、その付与権限の管理、情報資産の分類ならびに有資格者の職務と権限等に応じたアクセスの制限、ユーザID等の管理など、適切なアクセス管理を実施する。

当社は、上記不正アクセス等の防止や、本ポリシー等に基づく情報管理の実施状況の確認等のために、情報資産の分類等に応じて情報資産へのアクセス等の記録および分析を適切に実施する。

### 2. システムの運用管理等

当社は、システムの適正な稼働を確保するため、システムの開発・運用・利用部門の分離等、情報資産の分類等に応じて適切な運用管理を実施する。

当社は、システムの適正な稼働の確保や情報資産の漏えい等を防止するため、ソフトウェアの適正なライセンス管理と使用、無認可のソフトウェアの導入・使用の禁止、サイバーテロ対策やコンピュータウイルス防御対策等の実施など、情報資産の分類等に応じて適切な不正ソフトウェア対策等を実施する。

当社は、情報の移送・通信時等における情報セキュリティを確保するため、情報資産の分類等に応じて適切なネットワーク等の管理を実施する。

当社は、システムの適正な稼働を確保するため、電源・空調等の建物付帯設備の供給能力を確保するとともに、障害の予防対策や障害発生時の迅速かつ正確な復旧のための対応等、情報資産の分類等に応じて適切な障害時対策を整備し、その対策を定期的に確認し、必要な見直しを行う。

### 3. システムの開発とメンテナンス

当社は、システムが本ポリシー等に定める情報セキュリティに係る諸要件を満たすものであることを維持するため、その開発や変更に際して開発・本番環境を分離する等、情報資産の分類等に応じて適切な開発・メンテナンスを実施する。

## 第10条 外部委託管理

当社は、情報資産の取扱いに係る業務の一部または全部を外部に委託することによる漏えい等を防止するため、委託先における情報管理の状況の確認等、情報資産の分類等に応じて適切な外部委託管理を行う。

### 1. 委託先の選定基準

当社は、委託先における情報管理に係る方針・取扱規程等の整備状況等、委託先の選定基準を定め、取扱う情報資産の分類等に応じて、その基準に従った委託先の選定を実施する。

2. 適切な委託契約の締結

当社は、守秘義務など漏えい等の防止に係る事項や再委託に係る事項等、取扱う情報資産の分類等に応じて適切な内容の委託契約を締結する。

3. 委託先に対する適切な監督等

当社は、委託先における義務の履行状況について、定期的および必要に応じて都度報告を受ける等、適切な委託先の監督等を実施する。

**第11条 個人情報保護に関する方針**

当社は、個人情報の適切な保護と利用を重要な社会的責任と認識し、利用目的の特定とその範囲内での利用、適正な取得、第三者提供の制限、保有個人データ事項の公表、開示・訂正等の請求への適切な対応等を講じることにより、個人情報の保護に努めることとする。

当社は、個人情報の取扱い等に関する事項を含むプライバシーポリシーを別途定めて公表する。

**第12条 グループ内における顧客情報の共同利用**

当社は、グループ内における顧客情報の共同利用に関する手続を定め、厳格な運営・管理態勢を整備し、顧客情報の適切な保護と利用の実現、「個人情報の保護に関する法律」をはじめとする関係法令の遵守に努める。

**第13条 本ポリシーの改廃**

本ポリシーは、原則として年1回、必要な場合は都度見直しを行い、その改廃に当たってはみずほ信託銀行に申請し、承認を得たうえで取締役会の承認を得るものとする。ただし、組織、呼称等の変更に伴う修正で、本ポリシーの内容の実質的な変更を伴わないものは、情報管理統括責任者の承認で行うことができる。その場合、みずほ信託銀行に報告を行う。

以上