

# 情報セキュリティ基本方針

第三版

2011年9月

富士通中国システムズ

# 目次

1. はじめに
2. 情報資産と取扱い
3. 情報セキュリティ管理体制と役割

# 1. はじめに

富士通中国システムズ(以下当社と呼ぶ)は、富士通グループの一員として、お客様の視点に立ったプロダクト・サービスによる最適なソリューションを提供しています。当社は、社会・経済活動の基盤をなす情報システムを提供する者として、自社、およびお客様の情報資産/情報システムを適切に取り扱うことが社会的責務であると深く認識しており、情報セキュリティに関する法令、富士通グループ内規程に基づく基本方針/運用手順をマネジメントシステムとして定義し、実践することで、情報資産を適正に取り扱い、保護することをお約束します。

## 富士通中国システムズの情報セキュリティマネジメント

**情報セキュリティ基本方針**  
情報資産・システムを適切に扱うための情報セキュリティにおける「目的」「方針」「守るべきルール」に関する宣言書

**全社情報セキュリティ運用手順**  
情報セキュリティ基本方針に則った組織活動を遂行するための実施手順

**部門情報セキュリティ運用手順**  
情報セキュリティ基本方針に則った部門運営するための実施手順

**各プロジェクトマネジメント手順**  
情報セキュリティ基本方針に則ったプロジェクトを運営するための実施手順

**プロジェクト計画書セキュリティマネジメント**  
プロジェクト情報セキュリティ運用手順、及びお客様のルールを守るためにプロジェクトメンバーが実践すべきことを記述した文書

← 遵守

富士通規程

遵守 →

## 法令

- 個人情報保護法
- 経済産業省ガイドライン
- コンピュータ犯罪防止法
- 不正競争防止法
- 不正アクセス禁止法
- 著作権法

### 適用範囲

本基本方針は当社が執り行なう事業の全組織と作業場所に適用します。対象の人員は当社従業員(非正規社員含む)と当社事業に参画するビジネスパートナー要員です。

## 2. 情報資産と取扱い

情報資産は、企業活動の基本的な財産です。当社は、情報の漏えい、滅失、アクセス不能等の情報資産に関する事故が富士通グループの経済的損失、および社会的信用の失墜に繋がることを認識し、常にこれを適切に取扱います。

### 2.1 情報資産

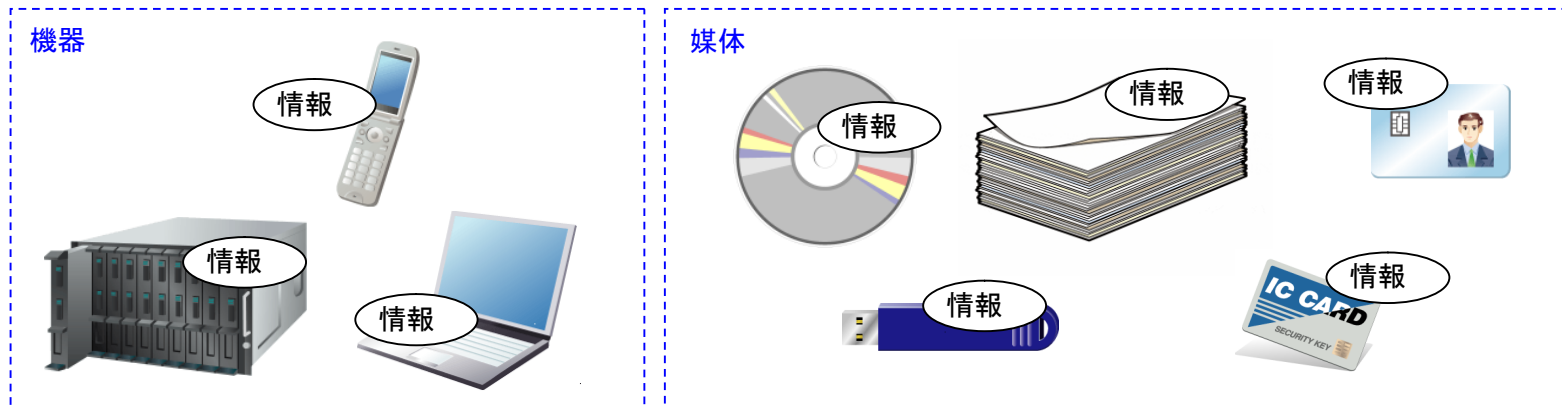
情報資産とは社内、ビジネスパートナー様やお客様先で使用する「情報」および「情報を格納/処理する機器や媒体」を指します。

#### 1) 情報

- ・他社秘密情報、関係者外秘、社外秘、公開情報

#### 2) 機器・媒体

- ・機器 パソコン、サーバー、携帯電話など
- ・媒体 紙、USBメモリ、CDなど
- ・カード 顧客先入館証、IDカードなど



### 2.2 情報資産の取扱い

情報資産を適切に扱い保護するために①情報の分類毎、②媒体毎に取扱い方法を決定します。

①情報の分類				
②機器・媒体 紙 パソコン・サーバー ポータブルハードディスク USBメモリ CD-R/DVD 携帯電話/PHS ICカード	他社秘密情報	関係者外秘情報	社外秘情報	個人情報

## 2.3 情報の分類

情報を適切に保護するために、情報を以下のカテゴリで分類し取扱います。

秘密情報	他社秘密情報	個人情報
	関係者外秘情報	
	社外秘情報	
公開情報		

分類	定義	取扱い
他社秘密情報	他社から当社が受領した情報のうち、秘密表示されている情報、もしくは秘密と言われた情報	アクセス管理又は施錠管理必須 作成時、入手時・持出時・廃棄時に情報資産管理台帳に記入要
関係者外秘情報	他社から当社が受領した情報のうち秘密表示されていない情報および、当社の秘密情報のうち特定の案件に関わる関係者以外に知られてはならない情報	セキュリティが確保された場所に保管
社外秘情報	当社の秘密情報のうち、関係者外秘情報以外の情報	
個人情報	個人を識別できる、住所、氏名、年齢、生年月日、性別、電話番号、会員ID、E-mailアドレス、銀行口座番号、クレジットカード番号、アンケート回答等の情報であって、かかる情報に含まれる氏名、生年月日、その他の記述または個人別に付された番号、記号その他の符号もしくは音声、画像により特定の個人を識別できるもの(ある情報のみでは特定の個人を識別できないが、他の情報と容易に照合でき、それにより個人を識別できる当該情報を含む)	有資格者以外はアクセス不可 アクセス管理又は施錠管理必須 作成時、入手時・持出時・廃棄時に情報資産管理台帳に記入要 個人情報リスク管理台帳で作成時、入手時・持出時・廃棄時におけるリスクの分析と施策立案を実施
公開情報	社内・外を問わず、カタログ、パンフレット、ニュースリリース等により、一般に公開されている情報	特に注意点無し

2.4 機器・媒体の管理

2.4.1 機器・媒体の取扱いルール

機器・媒体の盗難/紛失による情報漏えいを防止するため、機器・媒体の特性に応じた取扱いルールを定めています。

また、機器・媒体について、実施すべき技術的なセキュリティ対策をレベル分けして定めております。持出しやすいノートパソコンについては、盗難/紛失のリスクを考慮し、セキュリティ対策状況が視覚的にわかるシールを貼り付けることで「見える化」を図り、管理を強化しております。

情報の処理を行う従業員用パソコンの管理の詳細については 2.4.2 にてご説明しています。

媒体・機器		個人所有の媒体・機器の利用	利用終了時の情報消去	セキュリティ対策の実施レベル	盗難/紛失の防止対策	盗難/紛失に備えた情報漏えい防止対策	
媒体	紙	/	・セキュリティボックスに廃棄 ・返却	/	・プリンタに印刷物を放置しない ・適切なラベル付け ・施錠付ロッカーなどに保管 ・セキュリティが確保された場所でのみ利用し持出しルールを遵守 ・FAX利用時のルール遵守	・離席時など資料を放置しない ・セキュリティボックスを設置 ・持ち運びはケースに入れて行う ※ケースは警察で捜索依頼可能だが、紙は不可のため	
	USBメモリ ポータブルHDD	禁止	データ上書きによる消去	レベル3必須	・施錠付ロッカーなどに保管 ・持出し持込みルール遵守(不要な持出し禁止)	・指定された社給品のみを利用 ・機器利用時のパスワード設定 ・媒体の自動暗号化(レベル3)	
	CD-R、 DVDなど		破壊	/	・格納情報の情報の分類に応じて定めた所定の方法(施錠ロッカーなど)に保管 ・情報管理ルールの遵守	・機密度に応じ、ファイル単位でパスワード設定や暗号化を行う	
機器	サーバー/HDD	ラックマウント	データ上書きによる消去	レベル1必須	・セキュリティが確保された場所に設置 ・ラックに固定	・機器利用時のパスワード設定	
		据置			レベル2、3は推奨	・セキュリティが確保された場所に設置 ・セキュリティワイヤーで固定	・機器利用時のパスワード設定 ・ディスク自動暗号化(レベル3)推奨
	PC	タワー/デスクトップ		禁止	レベル1、2、3すべて必須	・セキュリティが確保された場所に設置 ・機/ロッカーなどに施錠保管 ・持出し持込みルール遵守(不要な持出し禁止)	・機器利用時のパスワード設定 ・BIOS/HDDパスワードの設定(レベル2) ・ディスク自動暗号化(レベル3)
		ノート				レベル3推奨	・セキュリティが確保された場所に設置 ・セキュリティワイヤーで固定
	卓上型HDD	禁止		/	・紛失のないよう個人で保管 ・社給携帯電話はストラップをつける ・社給携帯電話のアドレス帳ではフルネーム登録禁止、役職は記号化、PCメールアドレス登録禁止	・セキュリティロックを設定し、機器利用時のパスワード設定 ・メール、添付ファイルなどの業務データは保管禁止	
	携帯電話、PHS	可		データ消去	/	・おお客様よりの常時借用は最低限とする ・施錠付ロッカーなどに保管 ・持出し持込みルール遵守 ・ストラップなどで放置を回避	/
その他	顧客先入館証、IDカード、鍵、セキュリティカード等	/	返却	/	/	/	

## 2.4.2 従業員用パソコンの管理について

パソコンのセキュリティ対策を定めるだけでなく、セキュリティソリューションの導入により効率的にチェックを行うことで人為的なミス除去し、従業員が利用するパソコンの安全を確保しています。



### セキュリティ強化のための追加対策

#### (ウイルス対策)

- ・WSUSによるWindows、Officeパッチの自動配布
- ・ウイルス完全スキャンを1回/週以上の頻度で実施
- ・Winnyなどのファイル交換ソフトのインストール禁止

#### (秘密情報の保護)

- ・パスワード付きスクリーンセーバーによる、離席時のパソコン画面の保護

#### (媒体利用時の対策)

- ・USBメモリは利用申請を行い許可を得て利用する
- ・媒体受領/受渡し前の手動ウイルススキャン
- ・USBメモリによるウイルス感染防止(Windowsの自動再生機能の無効化)

#### (電子メール利用時の対策)

- ・電子メール利用時、宛先を再確認
- ・未知のウイルスによる被害を回避するため、実行形式の拡張子のファイル添付禁止

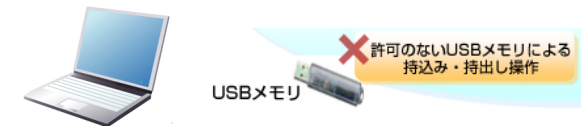
### DOEXPRESS Security 情報セキュリティ対策診断

#### セキュリティ対策設定状況を自動診断



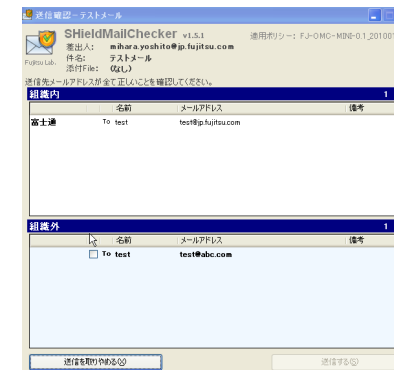
### Desktop Keeper 情報漏えい防止

#### 利用許可がないUSBメモリの接続拒否



### ShieldMailChecker メール誤送信防止

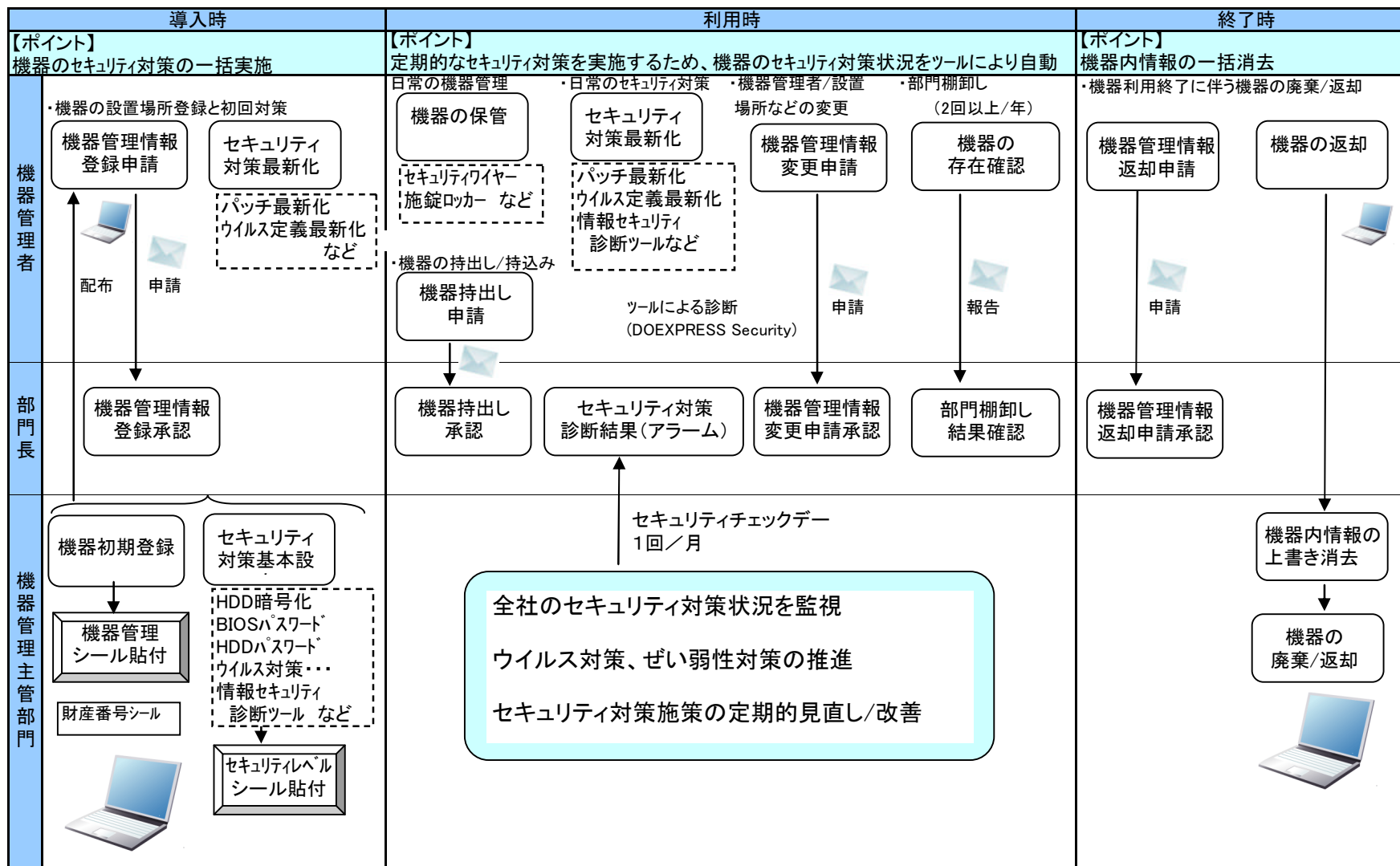
#### 社外メール発信前に送付先を再度確認



### 2. 4. 3 従業員用パソコンの管理フロー

「機器管理主管部門」を設置し、部門長・機器管理者が連携することで「従業員用パソコンの導入から廃棄まで」を管理しています。

ワークフローによる申請により階層別にマネジメントするとともに、セキュリティ対策診断ツール(DOEXPRESS Security)の自動診断機能を導入することで、セキュリティ対策の実施状況を可視化しています。セキュリティ対策の客観的な管理が可能となり、セキュリティ意識の向上と問題発生リスクの軽減を実現しています。



### 3. 情報セキュリティ管理体制と役割

#### リスク管理委員会

情報セキュリティに関する専門化体制をとり、顕在化したリスクの専門委員への情報の集約とお客様および富士通グループ全体の影響を極小化するための対策をとる

#### リスク管理委員長

#### 情報セキュリティ管理責任者

情報セキュリティに関する責任と権限を持つ  
情報セキュリティに関するリスク情報の収集  
(4. リスク情報収集を参照)

専門委員

#### 情報セキュリティ監査責任者

情報セキュリティ監査に関する責任と権限を持つ

監査室

内部監査人

#### 各事業部

#### 部長

情報資産の管理及びセキュリティ施策の遵守に関する権限と責任を持つ

#### 情報セキュリティ担当幹部社員

情報機器の管理及びセキュリティ施策の推進を委任された幹部社員

#### 情報セキュリティ担当者

情報装備担当幹部社員を補佐する要員

#### 各プロジェクト

#### 情報資産管理責任者(プロジェクト責任者)

プロジェクトにおける情報資産の管理及びセキュリティ施策の遵守に関する権限と責任を持つ

#### 情報資産管理者(プロジェクト管理者)

プロジェクトにおける情報資産の管理及びセキュリティ施策の実施

#### 事業管理部

当社全体の情報セキュリティ施策管理、推進  
お客様・ビジネスパートナー様対応、富士通グループ窓口

#### 品質マネジメント推進室

情報セキュリティマネジメントシステム維持・管理

#### 総務部

総務関連事項の対応、マスコミ対応窓口

富士通中国システムズ情報セキュリティマネジメントでは  
下記ソフトを利用しております。

- 情報漏えい防止、印刷量の見える化  
Systemwalker Desktop Keeper V14g  
[http://systemwalker.fujitsu.com/jp/desktop\\_keeper/](http://systemwalker.fujitsu.com/jp/desktop_keeper/)
  
- マネジメントシステム文書管理  
PRODocumalシリーズ最新版「Documal V4」  
<http://www.fcy.co.jp/pkg/documal/>
  
- アンケートの作成/実施/集計/分析ツール  
@Researcher  
<http://www.fcy.co.jp/pkg/researcher/>
  
- パソコンの資産管理、セキュリティと省電力対策  
Systemwalker Desktop Patrol V14g  
[http://systemwalker.fujitsu.com/jp/desktop\\_patrol/](http://systemwalker.fujitsu.com/jp/desktop_patrol/)
  
- 情報セキュリティ対策診断ツール  
DOEXPRESS Security  
<http://jp.fujitsu.com/group/shikoku/services/packages/doexpress/>