付録１．リスク分析の別アプローチ

詳細リスク分析

ＩＳＭＳ認証基準のためのガイドである『ISMS ガイド Ver.1.0』(JIPDEC 発行)でのリスク値の算出を参考としてリスク評価を行ってみた。

当ガイドでは情報資産のリスク評価を下記のようにおこなっている。なおベースはGMITS(ISO/IEC TR 13335 Guideline for the management of IT Security)の詳細リスク分析である。

(1)範囲の設定と情報資産の洗い出し

一定の分類基準にしたがって適用範囲中の全ての情報資産を洗い出して表にする。

(2)情報資産価値の評価

情報資産の価値は下記の通りに算出し、４段階で数値化している。

価値＝機密性（Confidentiality）×完全性（Integrity）×可用性（Availability）
例　　４　　×　３　　×　３　　=>　３６

機密性は１～４の４段階、他は１～３の３段階
したがって最低１～最高３６となる
この計算結果から情報価値を４段階に分けるようにしている。
分け方は組織の考え方による。

○数値でわけると、
１～9⇒1、１０～１８⇒2、１９～２７⇒3、２８～３６⇒4
○密度で分けると、1,2,3,4 | 6,8,9 | 12,16,18 | 24,27,36
１～4⇒1、６～9⇒2、１２～１８⇒3、２４～３６⇒4

(3)脅威・脆弱性分析とリスク値算出

同様に上記について各々１～３で数値化し、価値との積をとってリスク値を算出する。

リスク値　＝　資産価値　×　脅威　×　脆弱性
例　　４　×　３　×　３　=>　３６

(4)リスクの管理

リスクには次の４つの方針で対処する。

- 許容：リスクの影響が無視できるとみなして対策をとらない
- 低減：対策を実施することによりリスクを許容範囲まで減少させる
- 移転：保険などによりリスクを他者へ移転する
- 回避：まったく別の手段に切り替えることによりリスクの元をなくす

許容はリスク値の基準をもうけて判断する。（例：基準リスク値を９とすると、９未満はリスクを許容できると判断する。これは残存リスクとなる）

(5)当研究会での試算

当研究会ではＩＳＭＳ自体がテーマではないため、簡易的にリスク値を算出。

資産価値	×	発生頻度		リスク値
１～３		１～３	=>	９

発生頻度⇒脅威×脆弱性

作業では各担当（５名）が手分けしてリスク評価をおこない、後に別の人がその内容をレビューした。ここでモデル企業のセキュリティポリシーが明確でないことから、評価にばらつきが出た。

例えばホームページの不正改竄に対する評価は、以下のようになった。

	資産価値	×	発生頻度			
A氏	３	×	３	＝	９	（最高点）
B氏	２	×	２	＝	４	（中位）

この場合の評価の分かれ目となるのはＨＰの改竄が与える会社の信用への影響度が挙げられる。A氏はきわめて影響が大きいと見、B氏は内部ＤＢと独立で、比較的簡単に復旧できるので、価値、リスクともに相対的に低いとみた。そこでリスク評価には、『この会社（モデル会社）がどんな会社なのか』という点が意外に大きく影響してくるということが明らかになってきた。これはモデル作成の過程で自明になるものではなく、明示的に情報セキュリティポリシー（最上位）を記述すべきものである。

付録２．リスク分析一覧表

リスク分析一覧表(1/9)

	資産	所在地	資産価値	脅威	対象	攻撃者	手段	脅威	発生頻度	リスク値	検知	防止	復旧	残存リスク
1	ﾃﾞｰﾀ	基幹DB	3	第3者がｲﾝﾀｰﾈｯﾄ経由でシステムに侵入しﾃﾞｰﾀを書き換えた	ﾃﾞｰﾀ	第三者	ｲﾝﾀｰﾈｯﾄ	改竄	2	6	○ ログ収集及び定期的チェック ○ IDS	○ F／W設置 ○ ｾｷｭﾘﾃｨﾎｰﾙに対しﾊﾟｯﾁ適用 ○ ｱｸｾｽｺﾝﾄﾛｰﾙの強化 ○ ﾊﾟｽﾜｰﾄﾞ保護（ｻｰﾊﾞｰ･ﾌｧｲﾙetc） × 接続形態の変更（→RAS）	ﾃﾞｰﾀﾊﾞｯｸｱｯﾌﾟ	未知のウィルスセキュリティホール パッチ未発行のセキュリティホール
2	ﾃﾞｰﾀ	基幹DB	3	第3者がｲﾝﾀｰﾈｯﾄ経由でシステムに侵入しﾃﾞｰﾀを盗み出した	ﾃﾞｰﾀ	第三者	ｲﾝﾀｰﾈｯﾄ	窃取	2	6	○ ログ収集及び定期的チェック ○ IDS	○ F／W設置 ○ ｾｷｭﾘﾃｨﾎｰﾙに対しﾊﾟｯﾁ適用 ○ ｱｸｾｽｺﾝﾄﾛｰﾙの強化 ○ ﾊﾟｽﾜｰﾄﾞ保護（ｻｰﾊﾞｰ･ﾌｧｲﾙetc） × 接続形態の変更（→RAS） × 暗号化		未知のウィルスセキュリティホール パッチ未発行のセキュリティホール
3	ﾃﾞｰﾀ	基幹DB	3	第3者が協力会社の名前を語って社屋に侵入しすでに接続されている社内端末経由でシステムに侵入しﾃﾞｰﾀを書き換えた	ﾃﾞｰﾀ	第三者	無断侵入	改竄	1	3		○ ICｶｰﾄﾞ化＜入室＞ × 指紋（角膜）照合＜入室＞ ○ 入館許可書（写真入）の着用 × 監視カメラ設置 × ICｶｰﾄﾞ化＜端末使用＞ ○ 離席時にﾊﾟｽﾜｰﾄﾞ付スクリーンセーバーを活用 ○ 第三者の入館時に社員が同行する ○ 社員のセキュリティ教育 × 暗証番号化	ﾃﾞｰﾀのバックアップ	ICカード／許可証の盗難・偽造
4	ﾃﾞｰﾀ	基幹DB	3	第3者が協力会社の名前を語って社屋に侵入しすでに接続されている社内端末経由でシステムに侵入しﾃﾞｰﾀを盗み出した	ﾃﾞｰﾀ	第三者	無断侵入、社内端末の不正使用	窃取	1	3	× 外部者の持ち込み検査	○ ICｶｰﾄﾞ化＜入室＞ × 指紋（角膜）照合＜入室＞ ○ 入館許可書（写真入）の着用 × 監視カメラ設置 × ICｶｰﾄﾞ化＜端末使用＞ ○ 離席時にﾊﾟｽﾜｰﾄﾞ付スクリーンセーバーを活用 ○ 第三者の入館時に社員が同行する ○ 社員のセキュリティ教育 × 暗証番号化		ICカード／許可証の盗難・偽造

リスク分析一覧表(2/9)

	資産	所在地	資産価値	脅威	対象	攻撃者	手段	脅威	発生頻度	リスク値	検知	防止	復旧	残存リスク
5	ﾃﾞｰﾀ	基幹DB	3	第3者がショールームで誰もいない隙に、すでに接続されている営業端末を利用してシステムに侵入しﾃﾞｰﾀを書き換えた。	ﾃﾞｰﾀ	第三者	営業部社内端末の不正利用	改竄	1	3		× 端末設置場所を隔離	ﾃﾞｰﾀのバックアップ	
												○ 店内を無人にしない		
												○ 離席時にはログオフ		ログオフ忘れ
												○ 監視カメラ設置		カメラ故障
												○ 社員のセキュリティ教育		
6	ﾃﾞｰﾀ	基幹DB	3	第3者がショールームで誰もいない隙に、すでに接続されている営業端末を利用利してシステムに侵入しﾃﾞｰﾀを盗み出した	ﾃﾞｰﾀ	第三者	営業端末の不正利用	窃取	1	3		○ 監視カメラ設置		カメラ故障
												× ICｶｰﾄﾞ化＜端末使用＞		
												○ 離席時にﾊﾟｽﾜｰﾄﾞ付スクリーンセーバーを活用		
												○ 離席時にはログオフ		ログオフ忘れ
												○ 社員のセキュリティ教育		
7	DBファイル	基幹DB	3	・第3者がｻｰﾊﾞ室に侵入してDBファイルを破壊した。	ﾃﾞｰﾀ	第三者	システム部の管理用端末の不正利用	破壊	1	3		○ 暗証番号の定期的変更	ﾃﾞｰﾀのバックアップ	暗証番号の漏洩・解読
												○ ICｶｰﾄﾞ化＜入室＞	予備機の設置	ICカード／許可証の盗難・偽造
												× 指紋（角膜）照合		
												× 監視カメラ設置		
												○ ログインID／ﾊﾟｽﾜｰﾄﾞの定期変更		
												○ 離席時にはログオフ		
												○ 社員のセキュリティ教育		
8	DBファイル	基幹DB	3	・第3者がｻｰﾊﾞ室に侵入してDBファイルを盗み出した	ﾃﾞｰﾀ	第三者	システム部の管理用端末の不正利用	窃取	1	3		○ 暗証番号の定期的変更		暗証番号の漏洩・解読
												○ ICｶｰﾄﾞ化＜入室＞		ICカードの盗難・偽造
												× 指紋（角膜）照合		
												× 監視カメラ設置		
												○ ログインID／ﾊﾟｽﾜｰﾄﾞの定期変更		
												○ 離席時にはログオフ		
												○ 社員のセキュリティ教育		
												○ 管理用端末から外部送信できないようにする（メーラ，FTP）		
												× 管理端末にドライブが接続できないようにする		

リスク分析一覧表(3/9)

	資産	所在地	資産価値	脅威	対象	攻撃者	手段	脅威	発生頻度	リスク値	検知	防止	復旧	残存リスク
9	DBファイル	基幹DB	3 （大）	ｳｨﾙｽ感染した端末経由でDBファイルが破壊された	ﾃﾞｰﾀ	第三者	ｳｨﾙｽ（社内端末）	破壊	3 （多い）	9	○ ウイルスチェック ○ ログ収集及び定期的チェック	○ ｳｨﾙｽ対策ソフトパターンファイルの自動アップデート（起動時） ○ Outlook系メーラーの使用規制（ｾｷｭﾘﾃｨﾎｰﾙが多い為） ○ 外部ﾃﾞｰﾀを持ち込む（FD等）場合はｳｨﾙｽﾁｪｯｸを実施する ○ ﾊﾟｯﾁ適用	ﾃﾞｰﾀのバックアップ	発覚→対処完了までのリスクのみ
10	DBファイル	基幹DB	3 （大）	ｳｨﾙｽ感染した端末経由でDBファイルが盗み出された	ﾃﾞｰﾀ	第三者	ｳｨﾙｽ（社内端末）	窃取	3 （多い）	9	○ ウイルスチェック	○ ｳｨﾙｽ対策ソフトパターンファイルの自動アップデート（起動時） ○ Outlook系メーラーの使用規制（ｾｷｭﾘﾃｨﾎｰﾙが多い為） ○ 外部ﾃﾞｰﾀを持ち込む（FD等）場合はｳｨﾙｽﾁｪｯｸを実施する ○ ﾊﾟｯﾁ適用 ○ データの暗号化（重要データのみ）		発覚→対処完了までのリスクのみ
11	DBファイル	基幹DB	3 （大）	ｳｨﾙｽ感染した端末経由でDBファイルが改ざんされた → 更新、削除を含む	ﾃﾞｰﾀ	第三者	ｳｨﾙｽ（社内端末）	改竄	3 （多い）	9	○ ウイルスチェック ○ ログ収集及び定期的チェック	○ ｳｨﾙｽ対策ソフトパターンファイルの自動アップデート（起動時） ○ Outlook系メーラーの使用規制（ｾｷｭﾘﾃｨﾎｰﾙが多い為） ○ 外部ﾃﾞｰﾀを持ち込む（FD等）場合はｳｨﾙｽﾁｪｯｸを実施する ○ ﾊﾟｯﾁ適用	ﾃﾞｰﾀのバックアップ	発覚→対処完了までのリスクのみ
12	ﾃﾞｰﾀ	基幹DB	3 （大）	社内の内部者がｲﾝﾀｰﾈｯﾄ経由でシステムに侵入しﾃﾞｰﾀを書き換えた	ﾃﾞｰﾀ	内部者（社員、関係会社）	ｲﾝﾀｰﾈｯﾄ	改竄	1 （少ない）	3	○ ログ収集及び定期的チェック ○ IDS	社員のセキュリティ教育	ﾃﾞｰﾀのバックアップ	発覚→対処完了までのリスクのみ
13	DB	基幹DB	3 （大）	営業部の社員が企画部の社員のID/PASSWORDを不正に入手して基幹系DBにｱｸｾｽした。	ﾃﾞｰﾀ	営業部の社員	ID/PASSWORDの不正取得	不正ｱｸｾｽ	1 （少ない）	3	○ ログ収集及び定期的チェック	○ 社員のセキュリティ教育（パスワードの管理方法など） ○ ログインID／ﾊﾟｽﾜｰﾄﾞの定期変更 × ICｶｰﾄﾞ/指紋（角膜）照合		発覚→対処完了までのリスクのみ
14	ﾃﾞｰﾀ	情報系DB	3 （大）	第3者がｲﾝﾀｰﾈｯﾄ経由でシステムに侵入しﾃﾞｰﾀを書き換えた ＜1と同じ＞	ﾃﾞｰﾀ	第三者	ｲﾝﾀｰﾈｯﾄ	改竄	2 （普通）	6	○ ログ収集及び定期的チェック ○ IDS	○ F／W設置 ○ ｾｷｭﾘﾃｨﾎｰﾙに対しﾊﾟｯﾁ適用 ○ ｱｸｾｽｺﾝﾄﾛｰﾙの強化 ○ ﾊﾟｽﾜｰﾄﾞ保護（ｻｰﾊﾞｰ･ﾌｧｲﾙetc） × 接続形態の変更（→RAS）	ﾃﾞｰﾀﾊﾞｯｸｱｯﾌﾟ	発覚→対処完了までのリスクのみ
15	ﾃﾞｰﾀ	情報系DB	3 （大）	第3者がｲﾝﾀｰﾈｯﾄ経由でシステムに侵入しﾃﾞｰﾀを盗み出した ＜2と同じ＞	ﾃﾞｰﾀ	第三者	ｲﾝﾀｰﾈｯﾄ	窃取	2 （普通）	6	○ ログ収集及び定期的チェック ○ IDS	○ F／W設置 ○ ｾｷｭﾘﾃｨﾎｰﾙに対しﾊﾟｯﾁ適用 ○ ｱｸｾｽｺﾝﾄﾛｰﾙの強化 ○ ﾊﾟｽﾜｰﾄﾞ保護（ｻｰﾊﾞｰ･ﾌｧｲﾙetc） × 接続形態の変更（→RAS） × 暗号化		発覚→対処完了までのリスクのみ

リスク分析一覧表(4/9)

	資産	所在地	資産価値	脅威	対象	攻撃者	手段	脅威	発生頻度	リスク値		検知	防止	復旧	残存リスク
16	ﾃﾞｰﾀ	情報系DB	3	第3者が協力会社の名前を語って社屋に侵入しすでに接続されている社内端末経由でシステムに侵入しﾃﾞｰﾀを書き換えた	ﾃﾞｰﾀ	第三者	無断侵入、社内端末の不正使用	改竄	1	3			○ ICｶｰﾄﾞ化＜入室＞	ﾃﾞｰﾀのバックアップ	ICｶｰﾄﾞ・入館許可書の紛失(偽造)時のリスク(入室・機器破壊)のみ
			（大）	＜3と同じ＞					（少ない）				× 指紋(角膜)照合＜入室＞ ○ 入館許可書(写真入)の着用 × 監視カメラ設置 × ICｶｰﾄﾞ化＜端末使用＞ ○ 離席時にﾊﾟｽﾜｰﾄﾞ付スクリーンセーバーを活用 ○ 第三者の入館時に社員が同行する ○ 社員のセキュリティ教育 × 暗証番号化		
17	ﾃﾞｰﾀ	情報系DB	3	第3者が協力会社の名前を語って社屋に侵入しすでに接続されている社内端末経由でシステムに侵入しﾃﾞｰﾀを盗み出した	ﾃﾞｰﾀ	第三者	無断侵入、社内端末の不正使用	窃取	1	3	×	外部者の持ち込み検査	○ ICｶｰﾄﾞ化＜入室＞		ICｶｰﾄﾞ・入館許可書の紛失(偽造)時のリスク(入室・機器破壊)のみ
			（大）	＜4と同じ＞					（少ない）				× 指紋(角膜)照合＜入室＞ ○ 入館許可書(写真入)の着用 × 監視カメラ設置 × ICｶｰﾄﾞ化＜端末使用＞ ○ 離席時にﾊﾟｽﾜｰﾄﾞ付スクリーンセーバーを活用 ○ 第三者の入館時に社員が同行する ○ 社員のセキュリティ教育 × 暗証番号化		
18	ﾃﾞｰﾀ	情報系DB	3	第3者がショールームで誰もいない隙に、すでに接続されている営業端末を利用利してシステムに侵入しﾃﾞｰﾀを書き換えた。	ﾃﾞｰﾀ	第三者	営業端末の不正利用	改竄	1	3			× 端末設置場所を隔離	ﾃﾞｰﾀのバックアップ	特になし
			（大）	＜5と同じ＞					（少ない）				○ 店内を無人にしない ○ 離席時にはログオフ ○ 監視カメラ設置 ○ 社員のセキュリティ教育		
19	ﾃﾞｰﾀ	情報系DB	3	第3者がショールームで誰もいない隙に、すでに接続されている営業端末を利用利してシステムに侵入しﾃﾞｰﾀを盗み出した	ﾃﾞｰﾀ	第三者	営業端末の不正利用	窃取	2	6			○ 監視カメラ設置		ショールームでの人手が少ない頃を見計らって端末から情報を取得
				＜6と同じ＞									× ICｶｰﾄﾞ化＜端末使用＞ × 離席時にﾊﾟｽﾜｰﾄﾞ付スクリーンセーバーを活用 ○ 離席時にはログオフ ○ 社員のセキュリティ教育		

リスク分析一覧表(5/9)

	資産	所在地	資産価値	脅威	対象	攻撃者	手段	脅威	発生頻度	リスク値	検知	防止	復旧	残存リスク
20	DBファイル	情報系DB	3	第3者がｻｰﾊﾞ室に侵入してDBファイルを破壊した。 ＜7と同じ＞	ﾃﾞｰﾀ	第三者	システム部の管理用端末の不正利用	破壊	2	6		○ 暗証番号の定期的変更 ○ ICｶｰﾄﾞ化＜入室＞ × 指紋（角膜）照合 × 監視カメラ設置 ○ ログインID／ﾊﾟｽﾜｰﾄﾞの定期変更 ○ 離席時にはログオフ ○ 社員のセキュリティ教育	ﾃﾞｰﾀのバックアップ 予備機の設置	入室許可をもった内部スタッフによる意図的破壊行為
21	DBファイル	情報系DB	3	第3者がｻｰﾊﾞ室に侵入してDBファイルを盗み出した ＜8と同じ＞	ﾃﾞｰﾀ	第三者	システム部の管理用端末の不正利用	窃取	2	6		○ 暗証番号の定期的変更 ○ ICｶｰﾄﾞ化＜入室＞ × 指紋（角膜）照合 × 監視カメラ設置 ○ ログインID／ﾊﾟｽﾜｰﾄﾞの定期変更 ○ 離席時にはログオフ ○ 社員のセキュリティ教育 ○ 管理用端末から外部送信できないようにする（メーラ，FTP） × 管理端末にドライブが接続できないようにする		入室許可をもった内部スタッフによる意図的破壊行為
22	DBファイル	情報系DB	3	ｳｨﾙｽ感染した端末経由でDBファイルが破壊された ＜9と同じ＞	ﾃﾞｰﾀ	第三者	ｳｨﾙｽ（社内端末）	破壊	3	9	○ ウイルスチェック ○ ログ収集及び定期的チェック	○ ｳｨﾙｽ対策ソフトパターンファイルの自動アップデート（起動時） ○ Outlook系メーラーの使用規制（ｾｷｭﾘﾃｨﾎｰﾙが多い為） ○ 外部ﾃﾞｰﾀを持ち込む（FD等）場合はｳｨﾙｽﾁｪｯｸを実施する ○ ﾊﾟｯﾁ適用	ﾃﾞｰﾀのバックアップ	未確認のウイルスへの感染
23	DBファイル	情報系DB	3	ｳｨﾙｽ感染した端末経由でDBファイルが盗み出された ＜10と同じ＞	ﾃﾞｰﾀ	第三者	ｳｨﾙｽ（社内端末）	窃取	3	9	○ ウイルスチェック	○ ｳｨﾙｽ対策ソフトパターンファイルの自動アップデート（起動時） ○ Outlook系メーラーの使用規制（ｾｷｭﾘﾃｨﾎｰﾙが多い為） ○ 外部ﾃﾞｰﾀを持ち込む（FD等）場合はｳｨﾙｽﾁｪｯｸを実施する ○ ﾊﾟｯﾁ適用 ○ データの暗号化（重要データのみ）		未確認のウイルスへの感染
24	DBファイル	情報系DB	3	ｳｨﾙｽ感染した端末経由でDBファイルが改ざんされた → 更新、削除を含む ＜11と同じ＞	ﾃﾞｰﾀ	第三者	ｳｨﾙｽ（社内端末）	改竄	3	9	○ ウイルスチェック ○ ログ収集及び定期的チェック	○ ｳｨﾙｽ対策ソフトパターンファイルの自動アップデート（起動時） ○ Outlook系メーラーの使用規制（ｾｷｭﾘﾃｨﾎｰﾙが多い為） ○ 外部ﾃﾞｰﾀを持ち込む（FD等）場合はｳｨﾙｽﾁｪｯｸを実施する ○ ﾊﾟｯﾁ適用	ﾃﾞｰﾀのバックアップ	未確認のウイルスへの感染

リスク分析一覧表(6/9)

	資産	所在地	資産価値	脅威	対象	攻撃者	手段	脅威	発生頻度	リスク値	検知	防止	復旧	残存リスク
25	ﾃﾞｰﾀ	情報系DB	3	社員がｲﾝﾀｰﾈｯﾄ経由でシステムに侵入しﾃﾞｰﾀを書き換えた ＜12と同じ＞	ﾃﾞｰﾀ	内部者（社員、関係会社）	ｲﾝﾀｰﾈｯﾄ	改竄	1	3	○ ログ収集及び定期的チェック ○ IDS	社員のセキュリティ教育	ﾃﾞｰﾀのバックアップ	内部犯行
26	情報系DB	情報系DB	3	企画部の社員が営業部の社員のID/PASSWORDを不正に入手して情報系DBにｱｸｾｽした。 ＜13と同じ＞	ﾃﾞｰﾀ	営業部の社員	ID/PASSWORDの不正取得	不正ｱｸｾｽ	1	3	○ ログ収集及び定期的チェック	○ 社員のセキュリティ教育（パスワードの管理方法など） ○ ログインID／ﾊﾟｽﾜｰﾄﾞの定期変更 × ICｶｰﾄﾞ/指紋（角膜）照合		内部犯行
27	ホームページ情報	一般公開HPｻｰﾊﾞ	2	第3者がｲﾝﾀｰﾈｯﾄ経由で公開用ホームページを書き換えた	HPﾃﾞｰﾀ	第三者	ｲﾝﾀｰﾈｯﾄ	改竄	3	6	○ ログ収集及び定期的チェック	○ ﾌｨﾙﾀﾘﾝｸﾞ(F/W)の設定（ポート80のみ許容） ○ 認証／ｱｸｾｽ制御 ○ 改竄摘出ツールの適用 ○ ﾊﾟｯﾁ適用	ﾊﾞｯｸｱｯﾌﾟ	未確認の脆弱性を利用した改竄
28	ｻｰﾊﾞｰ情報	一般公開HPｻｰﾊﾞ	2	第3者がｲﾝﾀｰﾈｯﾄ経由で一般公開HP用ｻｰﾊﾞを踏み台にして他社のｻｰﾊﾞを攻撃	他社ｻｰﾊﾞ	第三者	ｲﾝﾀｰﾈｯﾄ	他ｻｰﾊﾞの攻撃	3	6	○ ログ収集及び定期的チェック	○ ファイアーウォール ○ ｳｨﾙｽﾁｪｯｸ ○ ﾊﾟｯﾁ適用 × 定期的にﾌﾟﾛｸﾞﾗﾑﾁｪｯｸ（有無・ﾀｲﾑｽﾀﾝﾌﾟ・ｻｲｽﾞ）		未確認の脆弱性を利用した改竄
29	DB	一般公開HPｻｰﾊﾞ	2	第3者がｲﾝﾀｰﾈｯﾄ経由でホームページのDBを盗み出した	HPﾃﾞｰﾀ	第三者	ｲﾝﾀｰﾈｯﾄ	窃盗	1	2	影響なしのため不要	影響なしのため対策なし（個人情報なし）	―	なし
30	ユーザID・ﾊﾟｽﾜｰﾄﾞﾌｧｲﾙ	一般公開HPｻｰﾊﾞ	3	第三者がｲﾝﾀｰﾈｯﾄ経由で社員のユーザID・ﾊﾟｽﾜｰﾄﾞﾌｧｲﾙを盗み出して社内システムにアクセスした。	ID/PASSWORD	第三者	ｲﾝﾀｰﾈｯﾄ	窃盗	3	9	○ ログ収集及び定期的チェック ○ IDS	○ ファイアーウォール ○ パッチ適用 ○ 暗号化		未確認の脆弱性を利用した窃取
31	ユーザID・ﾊﾟｽﾜｰﾄﾞﾌｧｲﾙ	一般公開HPｻｰﾊﾞまでの経路	3	第三者がｲﾝﾀｰﾈｯﾄ経由で社員のユーザID・ﾊﾟｽﾜｰﾄﾞﾌｧｲﾙを盗み出して社内システムにアクセスした。	ID/PASSWORD	第三者	ｲﾝﾀｰﾈｯﾄ	窃盗	1	3		○ SSLを使用する		未確認の脆弱性
32	ﾌｧｲﾙ	社内端末	2	社員がWeb閲覧中にパソコンがｳｨﾙｽ感染した。	PC	社員	Web閲覧	ｳｨﾙｽ感染	3	6		○ ｳｨﾙｽ対策ソフトパターンファイルの自動アップデート（起動時） ○ パッチ適用 ○ Webｱｸｾｽの規制		未知のウィルス
33	ﾌｧｲﾙ	社内端末	2	ｳｨﾙｽ感染した社内端末から、社員及び取引会社宛にｳｨﾙｽﾒｰﾙが送信された。	取引会社PC／社内PC	社内端末	ﾒｰﾙ	ｳｨﾙｽ感染	3	6		○ ｳｨﾙｽﾒｰﾙを送信しない機能の導入（サーバ） ○ ｳｨﾙｽ対策ソフトパターンファイルの自動アップデート（起動時） ○ Outlook系メーラーの使用規制（ｾｷｭﾘﾃｨﾎｰﾙが多い為） ○ 外部ﾃﾞｰﾀを持ち込む（FD等）場合はｳｨﾙｽﾁｪｯｸを実施する		未知のウィルス 未確認の脆弱性

リスク分析一覧表(7/9)

	資産	所在地	資産価値	脅威	対象	攻撃者	手段	脅威	発生頻度	リスク値	検知	防止	復旧	残存リスク
34	PC		2	社員がｳｨﾙｽﾒｰﾙを受信し、感染した。	社内PC	第三者	ﾒｰﾙ	ｳｨﾙｽ感染	3	6		○ ｳｨﾙｽﾒｰﾙを受信しない機能の導入（サーバ） ○ ｳｨﾙｽ対策ソフトパターンファイルの自動アップデート（起動時） ○ Outlook系メーラーの使用規制（ｾｷｭﾘﾃｨﾎｰﾙが多い為） ○ 外部ﾃﾞｰﾀを持ち込む（FD等）場合はｳｨﾙｽﾁｪｯｸを実施する		未知のウィルス 未確認の脆弱性
35	PC	本社ビル	2	協力会社の社員がパソコンをネットワークに接続し、そこからｳｨﾙｽﾌｧｲﾙが社内に紛れ込んだ。	本社ビル内PC	第三者	ｳｨﾙｽ	ｳｨﾙｽ感染	3	6	○ ウイルスチェック ○ ログ収集及び定期的チェック	○ PCのビル内持込禁止 ○ 協力会社社員のセキュリティ教育 ○ PCのネットワーク接続の対策強化（許可されたPCの表示）	警戒情報の通知 悪業により生じた問題の除去 全マシンのウイルスチェック	PC持込みチェック漏れ
36	顧客情報	営業マン携帯PC	3	第3者に盗まれて、ハードディスク内の顧客情報が流失した	顧客情報	第三者	物理的に	窃盗	2	6	PCの持ち出し管理	○ 自己管理の徹底 ○ 暗号化ソフトの使用		 暗号解読
37	ﾒｰﾙの内容	営業マン携帯PC	2	ﾒｰﾙの内容が盗聴された	ﾒｰﾙ	第三者	ﾒｰﾙ	窃盗	2	4	（不可）	○ 暗号化ソフトの使用	（不可）	暗号解読
38	ﾒｰﾙ	営業マン携帯PC	2	ショールームに戻って無線LANで接続中にﾒｰﾙが盗聴された	ﾒｰﾙ	第三者	ﾒｰﾙ	窃盗	2	4	（不可）	○ 暗号化ソフトの使用	（不可）	暗号解読
39	ﾊﾟｽﾜｰﾄﾞ	営業マン携帯PC	3	ショールームに戻って無線LANで接続中にﾊﾟｽﾜｰﾄﾞが盗聴された	ﾊﾟｽﾜｰﾄﾞ	第三者	LAN	窃盗	2	6	（不可）	○ 暗号化ソフトの使用	（不可）	暗号解読
40	ﾒｰﾙ	営業マン携帯PC	2	PHSでｲﾝﾀｰﾈｯﾄ接続中にﾒｰﾙが盗聴された	ﾒｰﾙ	第三者	ﾒｰﾙ	窃盗	2	4	（不可）	○ 暗号化ソフトの使用	（不可）	暗号解読
41	ﾊﾟｽﾜｰﾄﾞ	営業マン携帯PC	3	PHSでｲﾝﾀｰﾈｯﾄ接続中にﾊﾟｽﾜｰﾄﾞが盗聴された	ﾊﾟｽﾜｰﾄﾞ	第三者	ｲﾝﾀｰﾈｯﾄ	窃盗	2	6		○ 暗号化ソフトの使用		暗号解読
42	社内機密文書（紙）	本社ビル	3	本社社員が社内文書（紙）を不正に持ち出した。	社内文書	本社社員	物理的に	窃盗	1	3		○ 機密文書管理の徹底（番号管理・廃棄方法）（机上整理・機密情報の鍵管理） ○ 社員のセキュリティ教育		悪意による持ち出し
43	社内一般文書（紙）	本社ビル	2	協力会社の社員が社内文書（紙）を不正に持ち出した	社内文書	協力会社社員	物理的に	窃盗	1	2		○ 文書管理の徹底（机上整理・機密情報の鍵管理） ○ 協力会社社員のセキュリティ教育		悪意による持ち出し
44	社内一般文書（紙）	本社ビル	2	第三者が社内文書（紙）を不正に持ち出した。	社内文書	来客者	物理的に	窃盗	1	2		○ 文書管理の徹底（机上整理・機密情報の鍵管理） ○ 第三者の入室規制		悪意による持ち出し
45	社内ﾃﾞｰﾀ	基幹DB	3	企画部の社員が社内ﾃﾞｰﾀを不正に電子ﾒｰﾙで社外に持ち出した。	社内ﾃﾞｰﾀ	本社社員	ﾒｰﾙ	窃盗	1	3	○ ログ収集及び定期的チェック	○ 社員のセキュリティ教育 ○ ﾃﾞｰﾀｱｸｾｽログの記録 × 社外へのメールは上司にCC × 社外へのメール規制		 事後対処となる可能性

リスク分析一覧表(8/9)

	資産	所在地	資産価値	脅威	対象	攻撃者	手段	脅威	発生頻度	リスク値	検知	防止	復旧	残存リスク
46	社内ﾃﾞｰﾀ	基幹DB	3	協力会社の社員が社内ﾃﾞｰﾀを不正に電子ﾒｰﾙで社外に持ち出した。	社内ﾃﾞｰﾀ	協力会社社員	ﾒｰﾙ	窃盗	1	3	○ ログ収集及び定期的チェック	○ 協力会社用IDの設定 ○ 協力会社社員のセキュリティ教育 ○ ﾃﾞｰﾀｱｸｾｽﾛｸﾞの記録 ○ ﾃﾞｰﾀｱｸｾｽの規制 × 協力会社社員のメール使用禁止		事後対処となる可能性
47	社内ﾃﾞｰﾀ	基幹DB	3	企画部の社員が社内ﾃﾞｰﾀを不正にFDで社外に持ち出した。	社内ﾃﾞｰﾀ	本社社員	FD	窃盗	1	3	○ ログ収集及び定期的チェック	○ 社員のセキュリティ教育 ○ ﾃﾞｰﾀｱｸｾｽﾛｸﾞの記録 × FDドライブを本体より撤去		事後対処となる可能性
48	社内ﾃﾞｰﾀ	基幹DB	3	協力会社の社員が社内ﾃﾞｰﾀを不正にFDで社外に持ち出した。	社内ﾃﾞｰﾀ	協力会社社員	FD	窃盗	1	3	○ ログ収集及び定期的チェック	○ 協力会社用IDの設定 ○ 協力会社社員のセキュリティ教育 ○ ﾃﾞｰﾀｱｸｾｽﾛｸﾞの記録 ○ ﾃﾞｰﾀｱｸｾｽの規制 × FDドライブを本体より撤去		事後対処となる可能性
49	顧客ﾃﾞｰﾀ	基幹DB	3	協力会社の社員が管理用端末を使用して顧客ﾃﾞｰﾀを持ち出した。	顧客ﾃﾞｰﾀ	協力会社社員	システム部の管理用端末の不正利用	窃盗	1	3	× 監視カメラ設置 ○ ログ収集及び定期的チェック	○ 協力会社用IDの設定 ○ 協力会社社員のセキュリティ教育 ○ ﾃﾞｰﾀｱｸｾｽﾛｸﾞの記録 × データの暗号化 × 暗号化、文書管理ツール（ID、パスワード要）の導入		事後対処となる可能性
50	社内ﾃﾞｰﾀ	情報DB	3	第3者がショールームの社内端末で社内情報を盗み見た。	社内ﾃﾞｰﾀ	第三者	目	窃盗	1	3	○ 監視カメラ設置	○ ﾊﾟｽﾜｰﾄﾞ付きスクリーンセーバー ○ 離席時はログオフ × 端末設置場所を隔離 × データの暗号化 × 暗号化、文書管理ツール（ID、パスワード要）の導入		ログオフ忘れ
51	一般公開HPｻｰﾊﾞ	一般公開HPｻｰﾊﾞ	2	第3者からPING攻撃	一般公開HP	第三者	ｲﾝﾀｰﾈｯﾄ	不正ｱｸｾｽ	2	4 0	○ ログ収集及び定期的チェック	○ ファイアーウォール ○ パッチ適用 ○ 不要サービスの停止		未知のウィルスセキュリティホール パッチ未発行のセキュリティホール
52	一般公開HPｻｰﾊﾞ	一般公開HPｻｰﾊﾞ	2	第3者からDoS攻撃	一般公開HP	第三者	ｲﾝﾀｰﾈｯﾄ	不正ｱｸｾｽ	2	4	○ ログ収集及び定期的チェック	○ ファイアーウォール ○ パッチ適用		未知のウィルスセキュリティホール パッチ未発行のセキュリティホール

リスク分析一覧表(9/9)

	資産	所在地	資産価値	脅威	対象	攻撃者	手段	脅威	発生頻度	リスク値		検知	防止	復旧	残存リスク
53	ノートパソコン	本社ビル	2	社員がノートパソコンを不正に持ち出した。	ノートパソコン	本社社員	物理的に	窃盗	1	2	×	監視カメラ設置	○ PCのビル外持出禁止 ○ 社員のセキュリティ教育		悪意による持出し
54	社内機密文書	本社ビル	3	第3者が社員証を不正に取得し本社に入り込み社内文書を持ち出した。	社内	第三者	社員証の不正取得	侵入	1	3	○	監視カメラ設置	○ IC内蔵社員証(写真入)への移行		悪意による持出し

付録３．セキュリティポリシー

情報セキュリティ基本方針

豊日システムキッチン株式会社（以下「当社」という）は業界に先駆けてインターネットをビジネスに活用し、情報システムを構築，整備してきた。しかし情報資産の漏洩や改竄といったリスクも確実に増加しており、問題発生を未然に防ぐと共に、発生時の影響を最小限に抑え迅速な回復をはからなければならない。

当社は情報資産を適切に保護，管理するため「セキュリティポリシー」を策定し、セキュリティ対策に関する遵守すべき事項を定める。これによりセキュリティ水準を高位に保ち、必要な情報資産が常に正常に使用できることを保証する。

豊日システムキッチン株式会社　代表取締役社長　凸山　凹郎

情報セキュリティ対策標準

当社は情報資産の保護のため、情報セキュリティ対策標準を定める。なお、本標準の制限は業務の効率化に優先して実行されなければならない。

(1) セキュリティポリシー

①「情報セキュリティ基本方針」ならびに「情報セキュリティ対策標準」を当社のセキュリティポリシーとする。
②「情報セキュリティ基本方針」は、幹部会議の承認により制定される。

(2)対象範囲

本標準の対象範囲は情報資産に関する全ての人的・物理的・環境的リソースを含む。

(3)情報資産の分類および管理

情報資産の分類基準および管理責任者を定め、情報資産価値および重要度に応じた保護対

策を実施する。

(4)体制

セキュリティ担当役員を委員長とする情報セキュリティ委員会を設置し、積極的にセキュリティ対策に取り組む。

(5)教育

社員（協力会社社員を含む）に情報セキュリティ教育を十分に行い、情報セキュリティの理解を深め本標準の遵守を確実にする。また、違反時の罰則を規定し不正行為を防止する。

(6)法令の遵守

当社の事業に関連する社会の法規を遵守する。

(7)例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

(8)改訂

①本標準は平成 15 年 xx 月 xx 日に情報セキュリティ委員長によって承認され、平成 15 年 xx 月 xx 日より施行する。
②本標準は情報セキュリティ委員会で必要と認められた場合、変更することができる。
③本標準に変更が生じた場合、情報セキュリティ委員会はその内容を速やかに適用者に対し通知しなければならない。