ショッピングセンター（ＳＣ）のリスクマネジメント・ガイドラインその１

「ＳＣの情報リスク」

7月27日

社団法人 日本ショッピングセンター協会

＜序文＞

公共政策委員会では、ＳＣが事業活動を行っていく過程で発生する可能性があるリスク（災害や事故）を、あらかじめ予測し、どう管理・制御をするかという「リスクマネジメント」について研究し、提言してきました。

2009 年 10 月には、新型インフルエンザ対策として「ショッピングセンター業界における新型インフルエンザ対策ガイドラインとＢＣＰ（事業継続計画）策定のポイント」を作成・公表しました。

平成 23 年度、公共政策委員会では、改めて、ＳＣを取り巻くリスクを整理すると共に、近年その利用や重要度が増しているＩＴ等を活用した“情報”に係るリスクマネジメントを研究テーマとして取り上げました。

公共政策委員会（委員長：小久保　正明）

Ⅰ．ＳＣのリスクマネジメント

１．リスクとリスクマネジメントとは

①ＳＣ事業の目的である利潤追求や地域インフラとしての役割追求を阻害し､むしろ損失に変えてしまう恐れのある**“不確実性”**をリスクといいます。

②リスク（不確実性）を分析、発見、評価し、どう管理・制御するかがリスクマネジメントです。

③リスクマネジメントがきちんと出来るかどうかで、ＳＣ事業の継続的な発展・成長が左右されます。

２．ＳＣのリスクとは

大分類	中分類	リスク項目
Ⅰ.基幹プロセスリスク	Ⅰ-1　製品・品質	Ⅰ-1-①商品欠陥による顧客怪我 Ⅰ-1-②商品による食中毒・健康被害
	Ⅰ-2　物流	Ⅰ-2-①配送中車両の交通事故 Ⅰ-2-②取扱ミスによる商品損壊
	Ⅰ-3　営業・販売	Ⅰ-3-①貸倒れ Ⅰ-3-②顧客対応不備 Ⅰ-3-③デベ・テナントの共同責任（例えば：名板貸し）
	Ⅰ-4　施設設備管理	Ⅰ-4-①設備･機械の損傷･故障 Ⅰ-4-②火災による来店客死傷・営業停止 Ⅰ-4-③停電・断水等による営業一時停止 Ⅰ-4-④漏水事故による商品水濡れ Ⅰ-4-⑤施設管理ミスによる来店客の怪我
	Ⅱ-1　情報システム	Ⅱ-1-①仕入・流通情報システムの障害･破壊 Ⅱ-1-②通信回線の障害・断絶 Ⅱ-1-③データの消去・改ざん
	Ⅱ-2　情報・技術漏洩	Ⅱ-2-①顧客個人情報漏洩
	Ⅱ-3　知的財産	Ⅱ-3-①商標権侵害・被侵害 Ⅱ-3-②意匠権侵害・被侵害
	Ⅱ-4　法務・倫理	Ⅱ-4-①不当表示･偽装表示 Ⅱ-4-②不当返品や協賛金要求等の独禁法違反

	Ⅱ-5　安全衛生	Ⅱ-5-①労働災害 Ⅱ-5-②違法残業 Ⅱ-5-③社員交通事故（自動車、列車、飛行機） Ⅱ-5-④集団感染症・疾病
	Ⅱ-6　環境	Ⅱ-6-①騒音・臭気・近隣問題等に関するクレーム Ⅱ-6-②土壌汚染
	Ⅱ-7　人事・労務	Ⅱ-7-①人権問題・差別（セクハラ･パワハラ・国籍・宗教・年齢）
	Ⅱ-8　経理・財務	Ⅱ-8-①資金繰り悪化・支払遅延
	Ⅱ-9　社内不正	Ⅱ-9-①横領・背任
	Ⅱ-10　総務	Ⅱ-10-①近隣住民とのトラブル
Ⅲ．外部環境リスク	Ⅲ-1　自然災害	Ⅲ-1-①地震・津波 Ⅲ-1-②台風・集中豪雨 Ⅲ-1-③天候不順･異常気象
	Ⅲ-2　対企業犯罪	Ⅲ-2-①盗難・万引き Ⅲ-2-②放火 Ⅲ-2-③脅迫・テロ Ⅲ-2-④危険物混入犯罪 Ⅲ-2-⑤強盗 Ⅲ-2-⑥風評被害（インターネット、ツイッターなど）
	Ⅲ-3　政治	Ⅲ-3-①法規制の変更・強化
	Ⅲ-4　経済	Ⅲ-4-①人手不足･採用困難
	Ⅲ-5　マーケット	Ⅲ-5-①個人消費の低迷 Ⅲ-5-②為替変動 Ⅲ-5-③少子高齢化
Ⅳ．経営プロセスリスク	Ⅳ-1　ビジネス戦略	Ⅳ-1-①設備投資失敗
	Ⅳ-2　経営者・経営権	Ⅳ-2-①敵対的被買収・株式買占め

Ⅱ．本ガイドラインで取り上げるリスク

今回のガイドラインその１で取り上げるリスクは“ＳＣの情報リスク”です。

ＳＣの主要な情報には、

・顧客情報

・テナント売上情報

・ディベロッパー、テナント従業員情報

・賃貸借契約情報　　等があります。

⇩

１．本ガイドラインでは、情報全体のリスク管理を考える“**情報セキュリティ**”

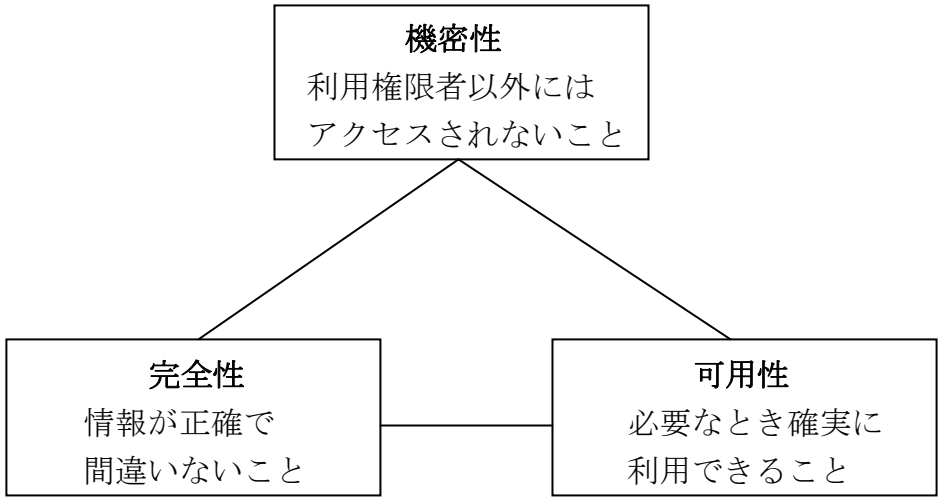
２．主要な情報の中でもＳＣのコンプライアンスとして大切な　**“顧客情報と個人情報保護法”**

の２点を取り上げます。

Ⅲ．情報セキュリティ

１．情報セキュリティとは

①情報セキュリティの三要素



【機密性とは】

正規の利用権限を持つ人にしか利用させないこと。
具体的には、ＩＤ、パスワードなどの認証システムによるアクセス制御、
情報の暗号化などによる無権限者の閲覧防止などの対策が求められる。

【完全性とは】

情報の改ざん、入力・更新時の入力ミスを防ぎ、情報を正確に保つこと。
不正アクセスの防止、入力・更新時のチェック体制の強化、電子署名による
情報改ざん防止などの対策が求められる。

【可用性とは】

システム障害などで必要なときに情報が利用できなくならないようにすること。
設備の災害対策、システムや情報の二重化、データのバックアップ対策が求められる。

２．情報セキュリティ対策

１）セキュリティ対策その１－制度面・物理面－

①重要な情報は、原則、社内や事業所外への持ち出しを禁止とします。

②保管・管理の徹底を図ります。

➢紙媒体情報は、ファイリングし施錠できるロッカーなどに保管することを徹底させます。

➢電子情報は、アクセス制御ができる所定のサーバに保管することを徹底させます。
（ＰＣのハードディスクやＵＳＢメモリーでの保管は原則禁止とします）

③不必要となった情報は、廃棄または消去させることを徹底させます。（法律で保管が定められたものを除く）

④重要情報を扱う場所の入退館管理やゾーン分離を行います。

⑤業務用ＰＣの管理の徹底

➢業務用ＰＣを事業所以外に持ち出す場合には許可制とします。

➢業務用ＰＣを使って出張先等でネットワーク接続を業務用に限定する、また、接続方法を徹底するなどの手段を講じます。（ウイルス感染、情報漏えいの防止）

２）セキュリティ対策その２－人材面－

①従業員に対する啓発・研修・訓練などの教育活動を定期的に行います。

②情報漏えい、紛失などが発生した場合は、直ちにリスク管理責任者に報告することを徹底させます。

Ⅳ．個人情報保護

１．個人情報保護の必要性

１）ＳＣが取り扱う個人情報には、

主として、
①お客様情報
②従業員情報　があります。

その中でも、**“お客様の情報はＳＣの財産”**です。
この貴重な財産である、お客様の情報を紛失、又は漏えいした場合にはＳＣはお客様の信頼を失います。

２）個人情報の取扱いについては**「個人情報保護法」**（2005 年 4 月施行）によって、規定されています。
法律に違反した場合には、罰則が科せられます。

２．個人情報保護法とは

１）個人情報保護法の概要

①ポイント１
・個人情報保護法は、個人情報の有用性に配慮しながら、個人の権利や利益を保護することを目的としています。

②ポイント２

・この法律は、民間の事業者の個人情報の取扱いに関して共通する必要最小限のルールを定めています。

・この法律の仕組みは、事業者が、事業等の分野の実情に応じ、自立的に取り組むことを重視しています。

（経済産業省ＨＰより）

２）法律を守らなければいけない事業者

➢５千件の個人情報データを所有し、事業に使用している事業者＝**“個人情報取扱事業者”**

３）個人情報とは？

➢特定の個人を識別できる情報やデータ

具体的には、

①本人の氏名

②生年月日、連絡先（住所・居所・電話番号・メールアドレス)、会社における職位又は所属に関する情報（本人の氏名と一体となった情報）

③防犯カメラに記録された情報等で個人が判別できる映像情報

３．個人情報保護法の実務

１）個人情報の管理サイクル（「取得」から始まって「廃棄」までは個人情報の管理サイクルです。）

２）取得時における留意点

①利用目的の特定と明示

➢個人情報を取得する際には、出来る限り利用目的を特定します。

ex.「サービス向上のため」というような抽象的な表現ではなく、「バーゲンやイベントのご案内のため」というように具体的に特定します。

➢個人情報を取得する際には、利用目的を明示し、原則として同意を得て下さい。

・書面による同意文を得ておくことが望まし。

・同意文には、利用目的、問合せ先、第三者提供がある場合は、その詳細を盛り込んでおきます。

３）利用・保管時における留意点

①利用目的以外の利用を厳禁します。

➢利用目的を拡大解釈してはいけません。

②従業員の方々に、個人情報保護の大切さや保護のための体制・規程などの教育の徹底を図ることを制度化します。
➢ＳＣの場合、個人情報の取得過程で、テナント従業員さんが係るケース（ポイントカードやクレジットカードの申し込み）があります。したがって、テナント従業員さんを含めた体制・規程の整備や教育が必要となります。

③不特定多数の人が多く出入りするＳＣでは、入退館（室）の管理、個人データの盗難の防止等の措置を講じなければいけません。

イ．個人データを取り扱う業務室を、施錠またはＩＣカードなどによって厳重に管理

ロ．個人データを記した書類、媒体、携帯可能なコンピュータ等の机上及び車内等への放置の禁止

ハ．離席時にパスワード付きスクリーンセイバ等の起動によるのぞき見等の防止策

ニ．個人データを含む媒体の施錠保管

ホ．氏名、住所、メールアドレス等を記載した個人データとそれ以外の個人データの分離保管

④個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理策を講じなければなりません。

イ．個人データにアクセスする権限の有無を識別、認証する方法を確立します（例えば、ＩＤとパスワードによる認証、生体認証等）。

ロ．個人データへのアクセス権限を付与する人を必要最低限とします。
ハ．個人データを格納した情報システムの利用時間の制限（休業日や業務時間外等の時間帯には情報システムにアクセスできないようにする）。

ニ．ウイルスなどの不正ソフトウェア対策を講じます。

ホ．移送時における紛失・盗難が生じた際の対策を講じます。
（例えば、媒体に保管されている個人データの暗号化等の秘匿化）

ヘ．盗聴される可能性のあるネットワーク（例えば、インターネットや無線ＬＡＮ等）で個人データを送信する際の、個人データの暗号化等の秘匿化を講じます。

ト．個人データを取り扱う情報システムの使用状況や個人データのアクセス状況の定期的な監視を行います。

４）廃棄時の留意点

①個人情報を長期間保有することはリスクの拡大となります。不要となった情報は即廃棄とします。

➢個人情報が、紙媒体の場合には、シュレッダー等で破砕します。個人情報が記載されたコピー用紙は再利用してはいけません。

➢個人情報が、データの場合には、完全消去します。なお、メールでデータを受信した場合には、添付ファイルなど忘れずに消去します。

5）その他の留意点

（1）個人データを委託する場合の留意点

➢個人データの取扱いを外部に委託する場合には、データの安全管理が図られるよう、契約締結や常日頃の取扱い状況を把握する必要があります。

個人情報の漏えいなどが発生した場合、その責任は個人情報取扱事業者に生じます。

①個人データの取扱いを委託する場合に契約に盛り込む項目

イ．個人データの漏えい防止、盗用禁止に関する事項
- 委託契約範囲外の加工、利用の禁止
- 委託契約範囲外の複写、複製の禁止
- 委託契約終了後の個人データの返還・消去・廃棄に関する事項

ロ．個人データの取扱状況に関する委託元への報告の内容及び頻度

ハ．契約内容が尊守されていることの確認と尊守されなかった場合の措置

ニ．事件・事故が発生した場合の報告・連絡に関する事項

（2）個人データの第三者提供について

➢個人データを、あらかじめ本人の同意を得ないで、第三者に提供してはいけません。

①第三者提供とされる事例

イ．ディベロッパーとテナントの間で個人データを交換する場合

ロ．親子兄弟会社、グループ会社の間で個人データを交換する場合

ハ．フランチャイズ組織の本部と加盟店の間で個人データを交換する場合

ニ．同業者間で、特定の個人データを交換する場合

（３）個人データの共同利用について

➢個人データを共同利用する場合には、下記の情報をあらかじめ本人に通知しておく必要があります。
この場合は、第三者提供とはなりません。

①共同して利用する個人データの項目（氏名、住所、電話番号、商品購入履歴等）

②共同利用者の範囲

③利用する者の取得時の利用目的（共同して利用する個人データのすべての利用目的）

④個人データの管理責任者の氏名又は名称

６）個人データ情報を紛失、漏えいなどの事故を起こした場合

①紛失、漏えいした個人データ情報対象者への説明・謝罪を迅速に行う必要があります。

②経済産業省など監督官庁に報告します。

③警察に通報します。

④ホームページなどで事故の内容等を公表します。

⑤再発防止のための改善をします。

以上