危機を制する者がビジネスを制する
安全価値の創造が企業価値を高める

Ver.18.0801.1

Office Security & Cyber Security

No.	オフィス空間の情報セキュリティ対策	サイバー空間の情報セキュリティ対策
1	天変地異と人・物による災害の脅威 ①天候災害：台風・豪雨・洪水・落雷・竜巻 ②地震災害：地震・津波 ③人的災害：事故・火事 ④物的災害：停電・ハード障害・ソフト障害	サイバー攻撃による被害の脅威 ①マルウェア　：悪意行為 ②ウイルス　　：破壊工作 ③スパイウェア：情報工作 ④ワーム　　：感染拡散 ⑤トロイの木馬：偽装工作 ⑥スケアウェア：偽装脅迫 …その他（多種多様なソフトの脆弱性を狙った攻撃）
2	社内ルール化された日常的な対策 「内部統制」に基づき、組織の業務目的を効率的・効果的に達成する為の「体制づくり・仕組づくり」の適正化を進めると共に、災害時における「情報資産の機密性・完全性・可用性の確保と維持保全」の最適化に努める。 ①システムの安定稼働とデータの維持保全に備える。 ②災害によるシステム停止とデータ消失に備える。 ③業務停止による利益損失と信頼失墜に備える。	①Webサイトの常時SSL化公開 ②メール添付データの圧縮・暗号化送信 ③不明なWebサイト閲覧やメール開封の禁止 ④攻撃を受けやすい最低限のソフトウェアのアップデート （Microsoft製品・Acrobat製品・Java・主要ブラウザー・主要メーラー・主要セキュリティ対策ソフト）
3	BCP（事業継続計画）とDR（災害復旧）への対策とPDCAによる継続的な改善 ①内的要因と外的要因による、業務上の事故・火事・停電にどう対処していますか？　問題・課題・解決策は？ ②コンピューターのハードウェアとソフトウェアの障害復旧にどう対処していますか？　問題・課題・解決策は？	①様々な脆弱性を攻撃してくるウイルス（破壊工作）・スパイウェア（情報工作）・ワーム（感染拡散）等への防御にどう対処していますか？　問題・課題・解決策は？ ②攻撃によるシステム停止やデータ漏洩にどう対処していますか？　問題・課題・解決策は？
4	設備対策・施設対策（最適化された遠隔地iDC運用） ①NAS（ネットワーク接続式の冗長化共有ディスク） ②UPS（無停電電源装置） ③iDC：サーバーハウジング・・・・・預りサーバー ④iDC：専用＆VPSサーバー・・・・・・貸出サーバー ⑤iDC：遠隔地バックアップ・・・・・定期一括データ保管 ⑥iDC：オンラインストレージ・・・逐次部分データ保管 …その他（利用者独自仕様の運用環境の構築に対応）	設備対策（ソフトウェア／ハードウェア） ①セキュリティ対策ソフト：主要メーカー製品を推奨。 ②ファイアウォール（FW）：外部からの攻撃を防御する。 ③統合脅威管理（UTM）　：外部から内部への攻撃と、内部から外部への不正アクセスを一元管理して防御する。 ▼以下の「機能の特長」と「運用の課題」を参照。
5	ファイアウォール（FW）機能の特長 インターネット経由で社内ネットワークに侵入した外部攻撃によって引き起こされる、内部データの盗聴・漏洩・改竄等の被害を防ぐ為に、一定量集まって有機的に整理されたデータベース（DB）を元に接続の許可や拒否を判断し、拒否と判断された時には管理者に通報が可能な「入口対策システム」です。	ファイアウォール（FW）運用の課題 OSや各種ソフトウェアの脆弱性を狙った攻撃が相次ぎ、より高度な機能を狙った新種のウイルス（破壊工作）・スパイウェア（情報工作）・ワーム（感染拡散）等が大量発生している為に、「後追型」になるセキュリティ対策ソフトやファイアウォールだけでは、機能面でも・性能面でもセキュリティ対策が遅れ気味になるのが「仕組み上の課題」です。
6	統合脅威管理（UTM）機能の特長 OSや各種ソフトウェアの脆弱性を狙ってインターネット経由で社内ネットワークに侵入した、新種のウイルス（破壊工作）・スパイウェア（情報工作）・ワーム（感染拡散）等の「サイバー空間の脅威」を防御する為の、統合的なセキュリティ対策の一元管理が可能な「入口・出口対策システム」です。	統合脅威管理（UTM）運用の課題 従来は単体の機能毎にメーカーや機種の選定が可能でしたが、現在では複数の異なった機能を統合した「一機種」しか選定が不可能な上に、一元管理によって全ての機能をバランス良くフル稼働した時の性能（データ通信の処理能力）の低下を想定した上で、一定年数の利用を前提とした導入の比較検討が必要不可欠なのが「機種選定上の課題」です。