出典:実教出版社「情報セキュリティ読本(IPA)」 文責:河東岩夫 (平成25年10月31日)

【セキュリティサービスと製品】

<table>
<tr><td rowspan="3">セキュリティサービス</td><td colspan="7">情報セキュリティポリシー策定 (リスク分析・情報セキュリティ基本方針・対策基準・実施手順)</td></tr>
<tr><td colspan="7">情報漏洩防止強化対策</td></tr>
<tr><td colspan="7">セキュリティ診断/侵入テスト/脆弱性検査/セキュリティ監査/セキュリティ教育</td></tr>
<tr><td>セキュアな環境・施設・オフィス</td><td colspan="7">セキュアゾーニング,セキュアオフィス・施設・設備・什器(入退出管理,監視カメラ,バイオメトリクス認証/盗難・紛失防止備品)</td></tr>
<tr><td rowspan="3">ネットワークセキュリティ</td><td colspan="4">ファイアウォール/WAF/ゲートウエイウイルス対策</td><td colspan="3">VPN(IPsec/IP-VPN/SSL-VPN)</td></tr>
<tr><td colspan="5">侵入検知システム(ネットワーク型IDS)/侵入、防止システム(IPS)</td><td colspan="2" rowspan="2">PKI関連製品</td></tr>
<tr><td colspan="4">アクセス制御/デバイス認証</td><td colspan="2">暗号化/デジタル署名</td></tr>
<tr><td></td><td colspan="3">セキュリティパッチ/脆弱性検査</td><td>フィッシング対策</td><td>コンテンツフィルタリング</td><td>データ暗号化</td></tr>
<tr><td rowspan="3">クライアントセキュリティ</td><td>個人認証</td><td>パーソナルファイアウォール</td><td rowspan="2">端末ウイルス対策</td><td rowspan="2">スパイウェア対策</td><td colspan="2">資産管理/端末構成管理</td></tr>
<tr><td colspan="2">メールセキュリティ(暗号化・監視)</td><td colspan="2">持出制限/文書保護ソフト</td></tr>
<tr><td colspan="6">検疫システム/不正PC監視・検知/シンクライアント</td><td>スパム対策</td></tr>
<tr><td rowspan="3">サーバセキュリティ</td><td>主体認証</td><td colspan="3">アクセス制御/権限管理</td><td>バックアップ</td><td>負荷分散</td></tr>
<tr><td colspan="3">セキュリティパッチ(適用・更新)・セキュアプログラミング</td><td rowspan="2">ログ管理</td><td>メールスキャン</td><td rowspan="2">フォレンジック</td></tr>
<tr><td>ホスト型IDS</td><td>サーバウイルス対策</td><td>完全性チェックルール</td><td>PKI関連製品</td></tr>
</table>

注)ウイルス対策:
1)ゲートウエイ:ネットワーク(ワーム)・ゲートウエイ対策　2)端末・サーバ:グループウエア・ファイルサーバ・クライアント
スパム:迷惑メール・フィッシング(情報盗取行為)、ワーム:ネットワークを介して自己増殖する機能を持った不正プログラムで
システムに侵入してディスク容量や処理時間を占有することでトラブルを引き起こすことも多い。

【施設や環境に関する対策例】

対策	具体的例
物理的な区域のレベル	セキュリティレベルを設定(ゲート・間仕切り) レベル１:誰でも立入可能な区域(受付,ロビー等) レベル２:許可された人のみ立入可能な区域(執務室,会議室等) レベル３:特定の人のみ立入可能な区域(サーバ室,重要資料室等)
アクセスできる区域の制限と入退室管理	職務・職階によりアクセス可能ゾーンを制限,安全区域(レベル２,３)への立入承認(手続の整備,申請書の記入管理),入退室の管理(ICカード,指紋認証,警備員による目視確認,供連れ防止,入退室の記録),入退室の監視(監視カメラ),不審者撃退(衝撃音波)
訪問者や受渡し業者の管理	訪問者対応(会議室で対応,ネームプレート,訪問相手の付添い,入退室の記録),受渡し業者の管理(レベル１区域での受渡し),安全区域内の限定立入り,職員の立会い)
コンピュータや通信装置の保護	情報システムの盗難,持出し防止(セキュリティワイヤー,サーバラック・キャビネットへの施錠収納),不正操作や盗み見防止(主体認証,離席時のログアウト・スクリーンロック,偏向フィルタ),配線保護(床下への埋設,ナンバリング),電磁波による情報漏洩防止(電磁波軽減フィルタ),端子盤の管理
安全区域内の(セキュリティ管理)	手続きの整備,身分証明書の携帯,小型カメラの使用禁止,持込み持出しの管理(手順の整備,記録保存),重要書類や記録媒体の管理(整理整頓,机・キャビネットの施錠,郵便受け・非常口内部の施錠,FAX資料・プリント出力の放置禁止,粉砕廃棄,消去ソフト,シュレッダ,溶解処理,裏紙使用禁止)
災害や障害への対策	サーバラックの固定,消火設備,無停電電源装置(UPS),空調設備,耐震・免震設備,非常口,非常灯設備,電源遮断装置