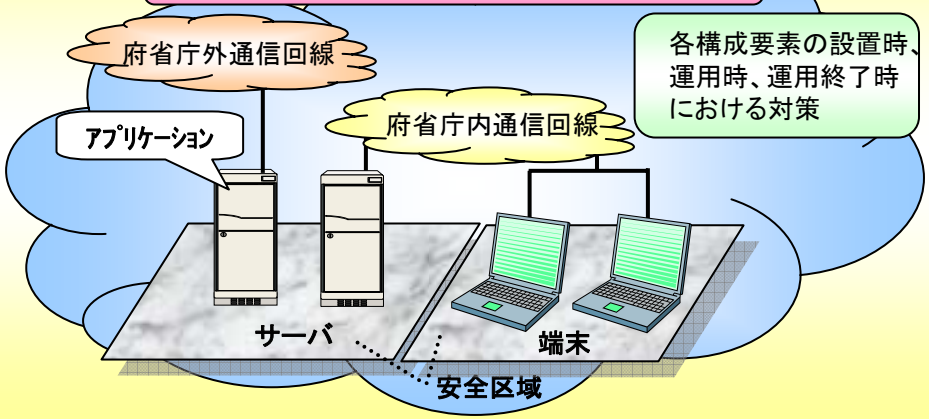
（参考） 政府機関統一基準の概要③

第5部　情報システムの構成要素についての対策

※　主に情報システムの管理者が実施する対策
遵守事項数：126（基本：82、強化：44）

【各構成要素に必要となる対策の検討】



【各構成要素に必要となる主な対策】

- **電子計算機等を設置する安全区域**
  立入り・退出の管理、身分証明書の提示等
- **電子計算機（端末、サーバ）**
  電子計算機関連文書の整備、モバイルPCの取扱い等
- **アプリケーション（電子メール、ウェブ）**
  電子メールの不正な中継の禁止、特殊文字の無害化等
- **通信回線（府省庁内通信回線、府省庁外通信回線）**
  不適切な接続の禁止、通信状況の確認・分析等

各構成要素に必要となる対策を列挙
⇩
検討漏れによる不備の防止

第6部　個別事項についての対策

※　④、⑤については、主に情報システムの利用者が実施する対策
遵守事項数：　74（基本：70、強化：　4）

①　機器等の購入に係る対策

【脅威】セキュリティ対策に不備がある製品の購入　等
【対策】機器等の選定基準の整備
機器等の納入時の確認　等

②　外部委託に係る対策

【脅威】委託先の不適正な情報管理による情報漏えい　等
【対策】委託先の選定基準の整備
委託先に適用する対策の整備　等

③　ソフトウェア開発に係る対策

【脅威】開発したソフトに脆弱性が存在する　等
【対策】ソフトウェア開発手順の整備
設計レビューの実施　等

④　庁舎外での情報処理に係る対策

【脅威】行政情報を保存したモバイルPCの紛失　等
【対策】庁舎外での情報処理に係る手続の整備
安全管理措置規定の整備　等

⑤　私物パソコンの利用に係る対策

【脅威】ウイルスに感染した私物パソコンの利用による情報漏えい　等
【対策】私物パソコンの公務利用に係る手続の整備
安全管理措置規定の整備　等

⑥　その他

- 府省庁外の情報セキュリティ水準の低下を招く行為の防止
- 事業継続計画（BCP）との整合的運用の確保