

## 簡介

---

### 概觀

由保護模式的名稱，就可以看出保護機制的重要性。保護機制可以減少系統當機，加強作業系統的穩定性，還可以幫忙找出程式的問題。IA-32 的保護機制，基本上是架構在「特權等級」上（在 segment 有四個等級，而在 page 有兩個等級）。因此，作業系統可以把重要的核心、系統程式、服務等等部分，放在具較高的特權等級的 segment 中；而把一般的應用程式放在特權等級最低的 segment 中。處理器會阻止等級較低的 segment 任意對等級較高的 segment 進行存取。這樣一來，就可以避免一個不正常的應用程式，破壞了整個系統。

在存取一記憶體位址之前，就會開始進行檢查。如果有任何違反保護規則的情形，就會發出例外（exception）。保護的規則包括：邊界檢查、型態檢查、特權等級檢查、可定址空間限制、程序進入點限制、和指令集限制。這些檢查和位址轉換是同時進行的，所以對執行效能不會有影響。

要進入保護模式，只要把 CR0 的 PE（protection enable，第 0 bit）設為 1 就可以開啟 segment 保護。在保護模式中，並沒有什麼方法可以把保護機制暫時開啟或關閉。如果不想使用任何保護功能，可以把所有的 segment 的特權等級都設定為 0（最高的等級），這樣會取消 segment 和 segment 之間的檢查動作。不過，邊界檢查和型態檢查還是會有作用。

分頁的保護，也是在開啟分頁功能之後，就會自動作用。同樣的，也沒有特別的方法可以暫時關閉或開啟分頁的保護機制。不過，就像 segment 一樣，可以把 CR0 的 WP（write protect，第 16 bit）設為 0，再把所有的分頁的 U/S 和 R/W 旗標都設為 1（參考「記憶體管理」的「[分頁機制](#)」）。這樣會把所有的分頁設定成可寫入、且在 user level 中，如此一來，分頁的保護機制就等於沒有作用了。