Cloudflare 設定防呆 Checklist

從 DNS 串接、SSL 強制加密到快取隔離，跟著逐項打勾，把上線 SOP 變成不踩雷的一頁清單。

使用方式：依階段順序由上往下做；標有「地雷」的項目一錯就可能全站中招，務必看清下方灰字的「為什麼」。此為靜態清單，請直接列印後逐項打勾。

01 事前準備與盤點

沒盤點就上線，後面每一步都在補洞

- [ ] 備妥網域註冊商（GoDaddy、Namecheap 等）的登入帳號與密碼。
- [ ] 盤點目前所有子網域（www、blog、mail、ftp …），逐一列出。
- [ ] 記下源站真實 IP（A 紀錄）——這是稍後要「藏起來」的東西。
- [ ] 確認源站主機是否已安裝 SSL 憑證——它決定階段三該選哪種加密模式。

02 Cloudflare 基礎串接

把網域的解析大權交給 Cloudflare

- [ ] 註冊 Cloudflare 帳號、新增網站網域，選擇方案（免費起步即可）。
- [ ] 讓 Cloudflare 自動掃描既有 DNS 紀錄，逐筆核對無漏再繼續。
- [ ] 複製 Cloudflare 指派的 2 組專屬 Nameservers。
- [ ] 到網域註冊商後台，把名稱伺服器換成 Cloudflare 那 2 組並儲存。
- [ ] 等待 DNS 傳播生效（用 whatsmydns.net 檢查全球是否同步）。

03 核心安全與效能設定 極重要

三大致命地雷都埋在這一段

- [ ] 主要紀錄（根網域 + www）開啟橘色雲朵（已代理）。
  → 灰色雲朵 = 只做 DNS 解析，完全沒有加速與防護。
- [ ] 地雷一 SSL/TLS 模式強制設為 Full (Strict)；源站已有憑證就絕不能用 Flexible。
  → Flexible 下 Cloudflare 到源站是明文（假性加密），還會觸發無限重導迴圈讓網站超慢。
- [ ] 開啟自動 HTTPS 重寫（Automatic HTTPS Rewrites）。
- [ ] 到「安全性 > 設定」開啟 Bot Fight Mode（機器人對抗模式）。
- [ ] 地雷二 裸 IP 清查：MX、ftp 及舊子網域不得指向源站真實 IP。
  → 殘留裸 IP 會被 Shodan／Censys 一搜就中，駭客直接繞過 Cloudflare 打源站，WAF 形同虛設。
- [ ] 主機防火牆只放行 Cloudflare 官方 IP 白名單（cloudflare.com/ips），封掉其他來源。
- [ ] 地雷三 Cache Rules 絕不要對「所有請求」設 Cache Everything。
  → 會把會員後台、購物車整頁快取，A 登入後 B 直接看到 A 的個資——嚴重外洩、觸法。
- [ ] 只對靜態路徑（/blog/*、圖片、CSS/JS）設 Cache Everything。
- [ ] 動態路徑（/wp-admin/、/checkout/、/my-account/、API）建立最高優先級「略過快取」。
- [ ] 進階：偵測到登入 Cookie 時 Bypass Cache（依 Cookie 略過快取）。

04 進階效能與安全優化

基礎穩了，再往上加一層

- [ ] 「快取 > Tiered Cache」開啟分層快取，減少回源請求、省頻寬。

- [ ] 「速度 > 最佳化」確認 Brotli 壓縮已開啟（比 Gzip 更省）。
- [ ] 「安全性 > WAF」建第一條規則，例如 URI 含 /wp-admin 且國家不是台灣就 Block。

05 上線驗證與監控

沒驗證 = 不知道到底有沒有生效

- [ ] F12 > Network > Headers 看到 cf-ray 或 server: cloudflare = 已生效。
- [ ] 靜態資源（圖片、CSS）的 cf-cache-status 出現 HIT。
- [ ] 實測聯絡表單、會員登入、購物車等動態功能正常，未被錯誤快取。
- [ ] 若上線後反而變慢：查（1）SSL 是否誤設 Flexible 造成重導迴圈（2）是否全站 BYPASS 沒快取到（3）多餘 Page Rules 衝突。
- [ ] 開啟 Always Online，源站短暫故障時仍能提供快取版頁面。
- [ ] 排定定期回檢：威脅天天進化，每季或每次改版後重跑這份清單。

3 大致命地雷速查（錯誤 → 惡果 → 正解）

1 假性加密的 SSL/TLS 悲劇

錯誤 源站已裝憑證跑 HTTPS，Cloudflare 卻用 Flexible 模式。
惡果 訪客到 Cloudflare 有加密、Cloudflare 到源站卻是明文，中間人可竊聽；還會無限重導、網站超慢。
正解 只要源站有憑證，一律設 Full (Strict)——真正的全程加密，沒有妥協空間。

2 繞道攻擊的裸 IP 洩漏

錯誤 忘了處理舊的 MX／ftp 紀錄，它們仍指向源站真實 IP。
惡果 駭客用 Shodan／Censys 一搜就拿到 IP，直接繞過 Cloudflare 對源站發動 DDoS。
正解 審核所有 DNS 紀錄不露源站 IP，並把 Cloudflare 官方 IP 加入主機防火牆白名單。

3 Cache Everything 全站快取災難

錯誤 為追速度，對「所有傳入請求」直接設 Cache Everything。
惡果 會員後台、購物車被整頁快取，使用者 A 的個資被使用者 B 看到，面臨隱私法規開罰。
正解 只快取靜態路徑；動態路徑（後台／結帳／API）與帶登入 Cookie 者一律 Bypass。