永遠走在最前面
Always Ahead

DNS的安全需求與對策

HiNet DNS 林方傑

2022-12-01

中華電信
Chunghwa Telecom

大綱

- **領域背景知識**
  - DNS用途、原理、分類
  - DNS安全議題
- **維運經驗分享**
  - 服務品質相關作為
  - 可用性相關作為
  - 完整性相關作為
  - 機密性相關作為
- **結語**
  (key takeaways)

議程主軸：Spreading and sharing the knowledge required to operate the Internet

Q: Why DNS?

- 骨幹網路的建設與維護
- 路由管理
- …

屬ISP的職責

but

網域名稱

（大家都有）

takes

DNS系統

important

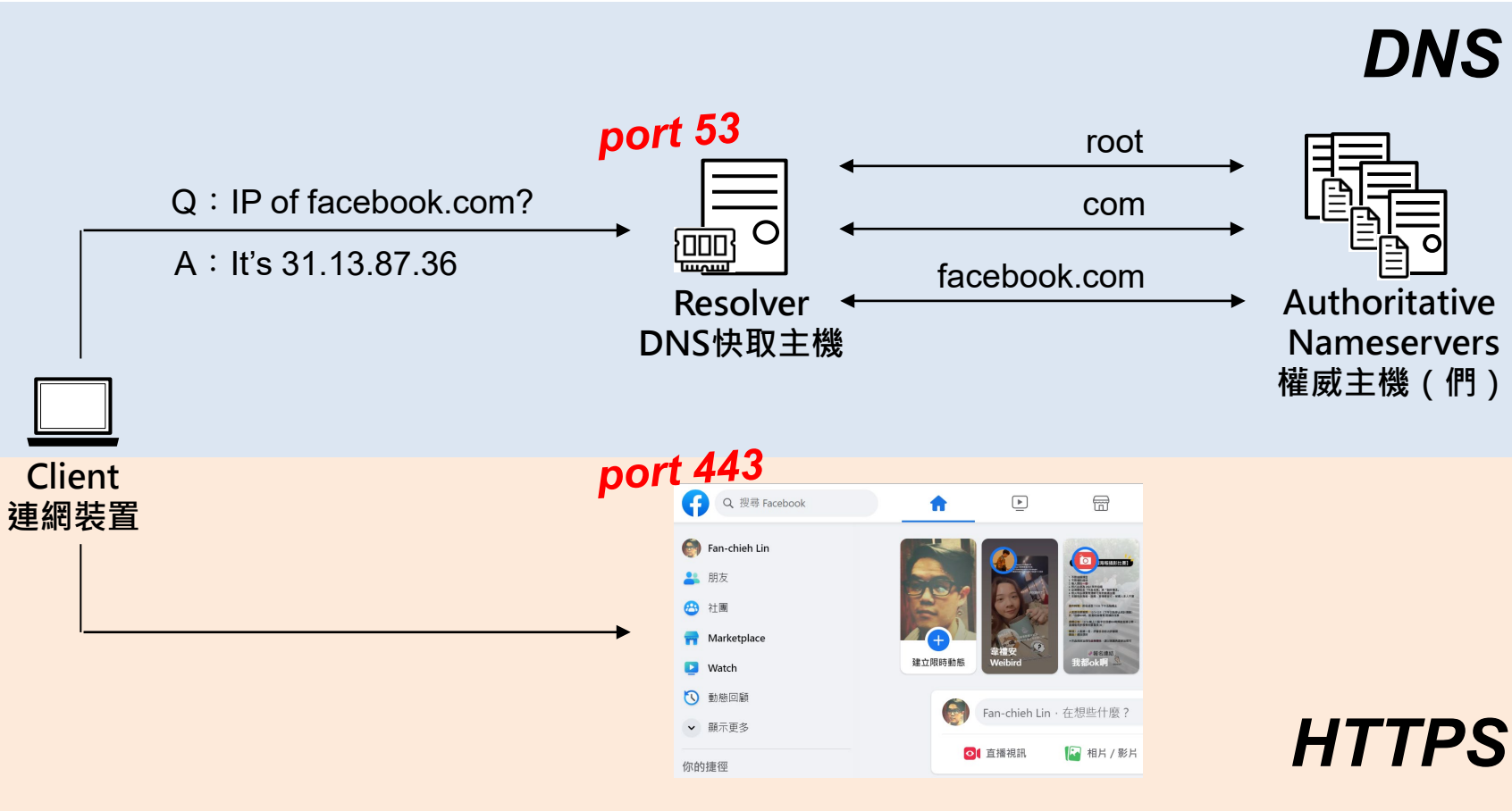
（以管理、發佈DNS紀錄）

worth

DNS的用途與原理

DNS可協助對應網域名稱與IP，為網際網路運作的關鍵環節

DNS主機可分為「resolver」「authoritative nameserver」兩類，用途與組態有別

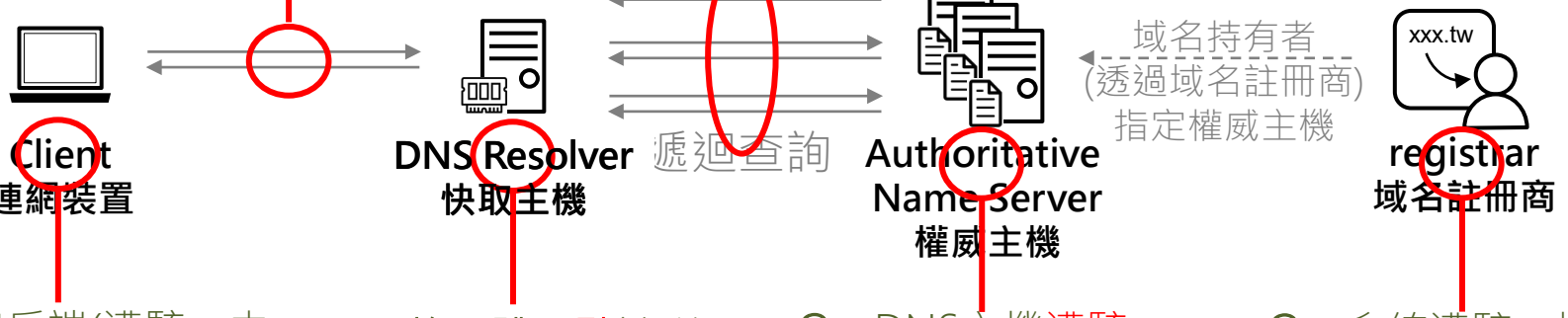


DNS的安全議題 (各環節的脆弱點)

（DNS封包以明碼傳輸、檢核不嚴謹等協定缺陷）

Q：傳輸過程中DNS封包被竊聽，導致privacy被侵害?

Q：傳輸過程中DNS封包被竄改，導致resolver快取到、client端收到錯誤答案? // “cache poisoning”



Client
連網裝置

DNS Resolver
快取主機

Authoritative Name Server
權威主機

registrar
域名註冊商

Q：客戶端(遭駭、中毒)，導致「預設DNS」被修改(改向惡意DNS查詢、被提供錯誤答案...)、或成為botnet參與DDoS攻擊?

Q：軟硬體弱點被利用導致服務中斷?

Q：遭受DDoS攻擊，因無法提供解析服務導致(大量)客戶無法上網?

Q：DNS主機遭駭、DNS紀錄遭竄改，導致提供錯誤IP?

Q：遭受DDoS攻擊，導致所管理之域名無法解析?

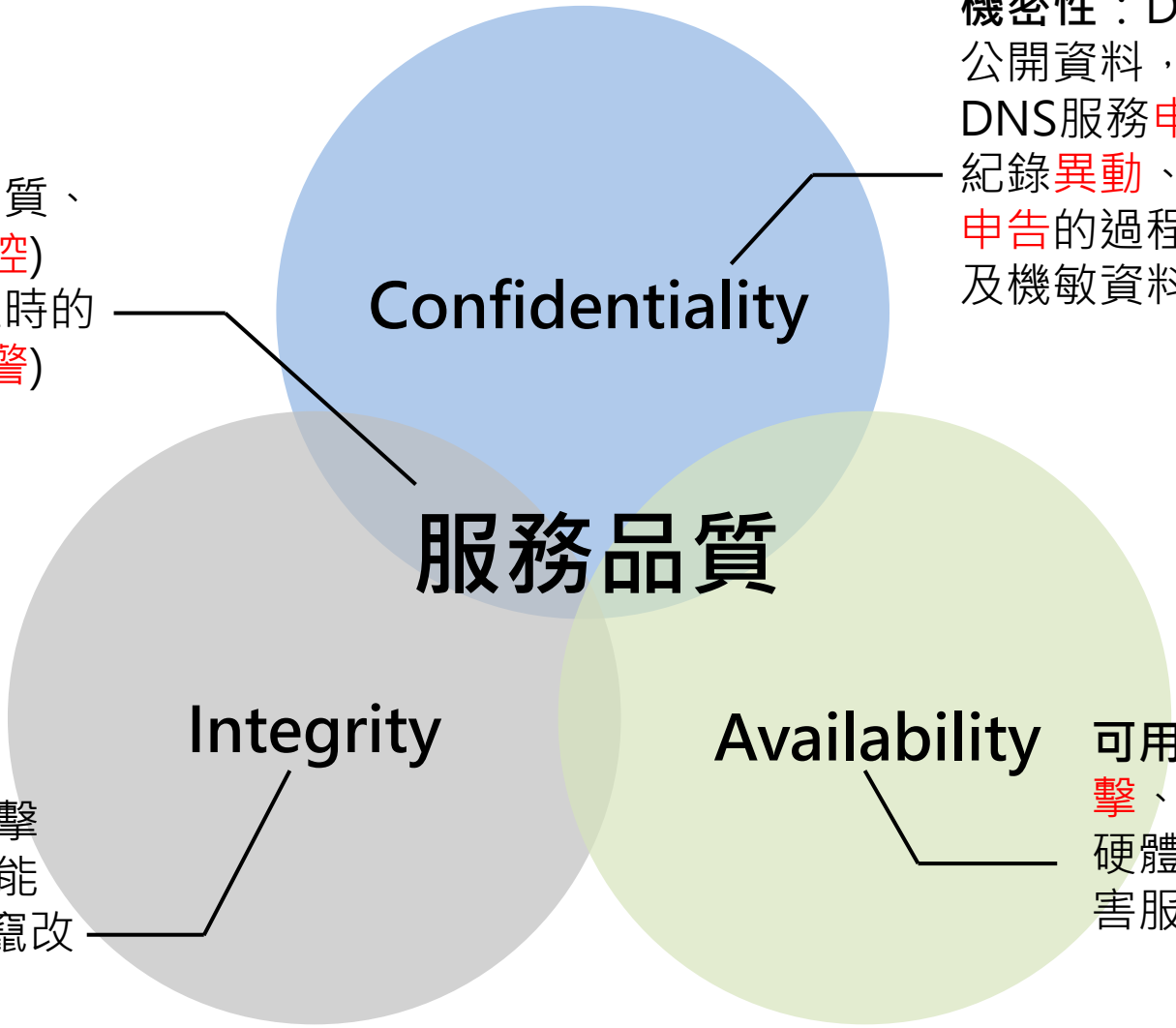
Q：系統遭駭、域名授權設定-NS紀錄遭竄改，導致網域名稱落入駭客手中?

中華電信 Chunghwa Telecom

此議程範疇 (挑選各位比較需要張羅的「權威主機」)

方向細節

DNS權威主機的安全需求 (以CIA triad觀點)



機密性：DNS紀錄是公開資料，但受理DNS服務申請、DNS紀錄異動、DNS相關申告的過程中可能涉及機敏資料

如何掌握服務品質、系統狀態？ (監控)
怎縮短異常發生時的反應時間？ (告警)

完整性：駭侵攻擊、快取汙染都可能使(DNS)資料被竄改

可用性：阻斷式攻擊、系統障礙、軟硬體弱點都可能危害服務的提供

服務品質

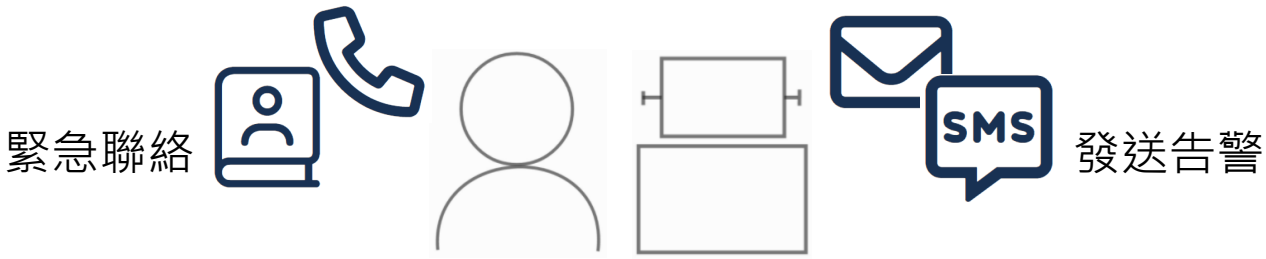
為充分掌握系統與服務狀態，採「使用者+管理者」兩種觀點進行多面向監測
一旦量化指標觸及門檻，將由監控系統與NOC人員進行告警與緊急聯絡

使用者觀點

- DNS解析失敗率監測
- DNS解析耗時監測

管理者觀點

- 訊務量監控
- 運算資源監控
- 軟硬體狀態監控
- 登入等操作監控



7*24

PS: icons引用自font awesome

可用性 透過系統與程序兩方面的作為強化

系統

提升量能
藉汰舊換新、架構優化
提供(至少)百萬級QPS
監看訊務成長情況規畫擴容

強化備援
HA架構、異地備援
(負載平衡；anycast)

建構縱深防禦
善用ISP優勢，結合骨幹網路

+HiNet DNS聯防
(RFC 7706)

程序

標準作業程序
妥善規劃弱點處理、系統變更，採用最佳實務
e.g. 關閉recursion等

演練
例行性

維持熟練度、驗證有效性

(包含備援切換、備份還原等類型並採用實兵演練的模式)

稽核
例行性

確認說寫做一致

中華電信 Chunghwa Telecom

PS: icons引用自font awesome

完整性

多管齊下，從網路、主機等層面進行主機駭侵、快取汙染之防治

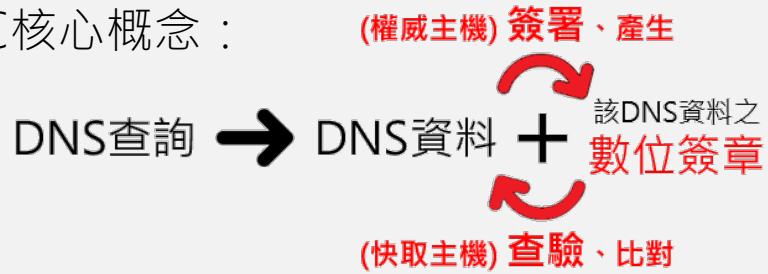
快取汙染防治

- HiNet DNS負載平衡架構與縱深防禦機制提高快取汙染的難度
- 採用領域最佳實務e.g.
  - ✓ 隱藏軟體版本、
  - ✓ 使用建議的軟體版本
  - ✓ 支援DNSSEC簽署

…

Resolver接受答案的條件：Port && Transaction ID

DNSSEC核心概念：



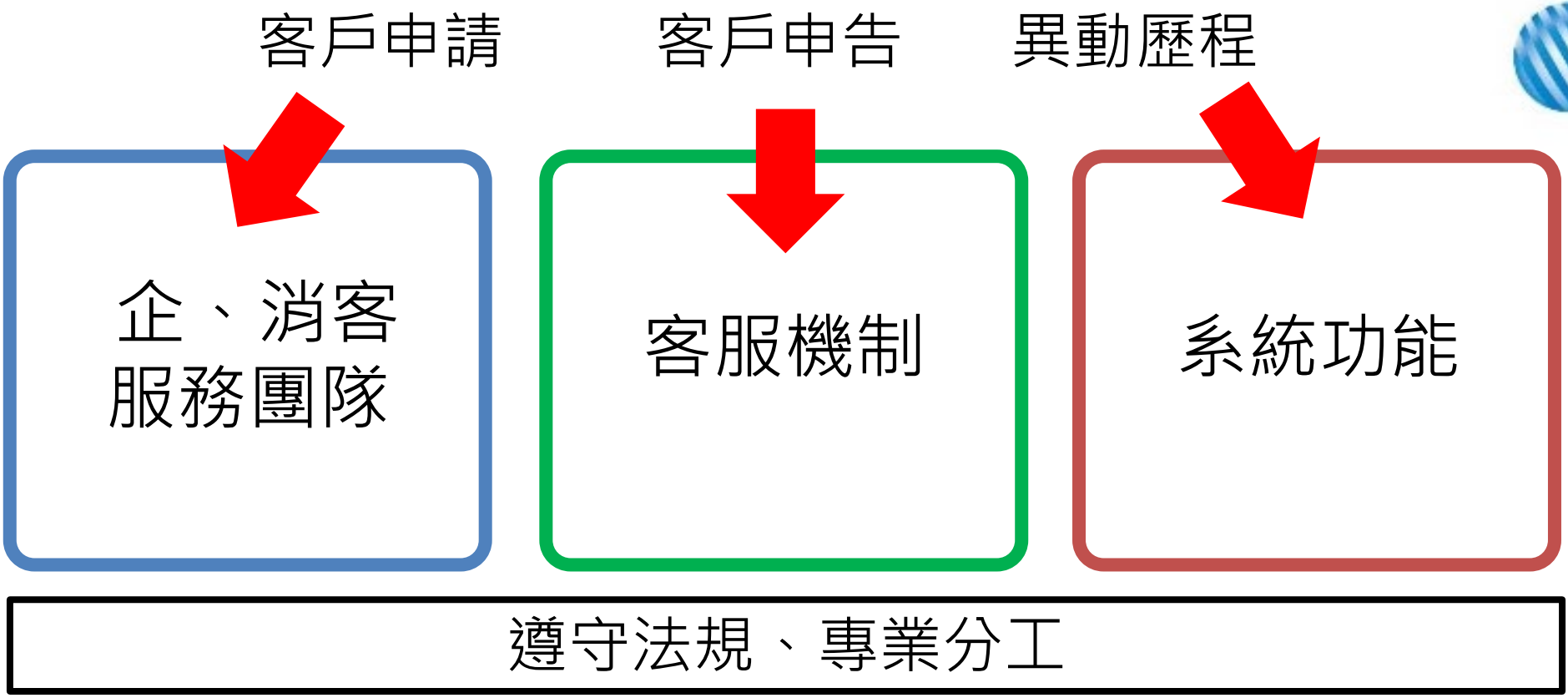
主機安全管理

- 服務與維運隔離(維運管道採OOB)
- 正向表列存取管控(只開放服務與維運所需+deny all)
- 帳號與權限管理
- 維運操作紀錄與告警
- 資料完整性監控(特定目錄的監控與告警等)
- 預備駭侵事件的緊急處理程序，與專業資安團隊保持聯繫

…

機密性

以遵守法規為前提進行專業分工，優化服務提供各環節的管理並減輕個別角色的負擔



key takeaways

- DNS領域知識
  - DNS的用途、原理、安全議題 (系統化盤點)
- 維運經驗分享
  - **專業分工，各司其職，持續優化**
    並維持跨組交流 (共享知識、資源、經驗)
  - **應用領域最佳實務、留意領域相關消息**
    e.g. 軟體升版防治快取汙染等、關閉不必要的功能降低負載 etc.
  - **盤點與善用資源、多管齊下**
    e.g. 縱深防禦 (、Pro DNS) etc.

DNS 經驗應用 → **其他情境/系統**

Q&A

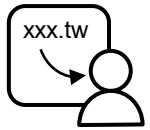
附錄

DNS關鍵角色與互動

Client
連網裝置

DNS Resolver
快取主機
(ISP / Public DNS)

Authoritative Name Server
權威主機



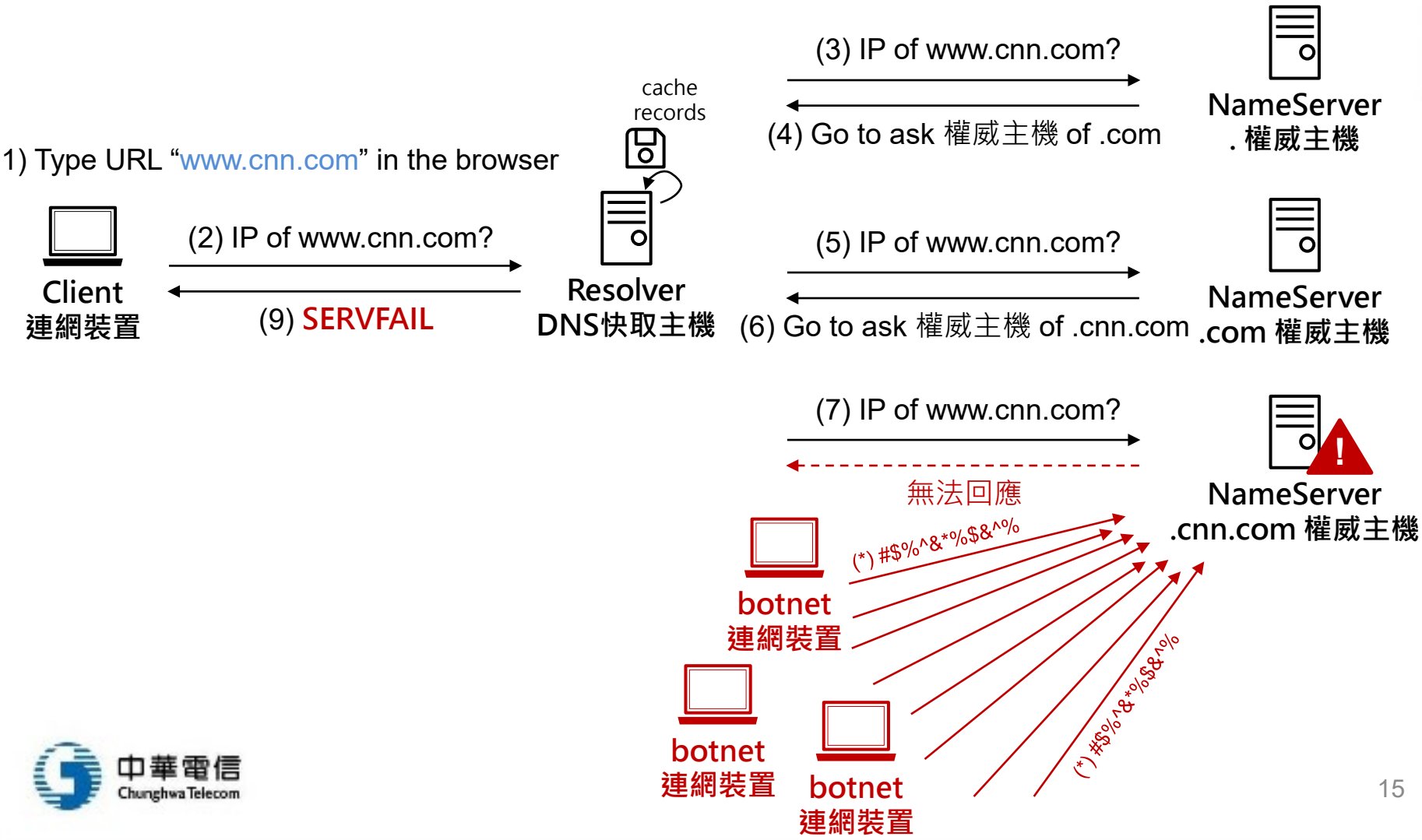
registrar
域名註冊商

1. **A公司**註冊網域名稱 (from域名註冊商)
2. **A公司**安排DNS主機管理&發佈DNS紀錄 (自建/代管 + 透過域名註冊商指定)
3. **Client終端**發出DNS查詢 (e.g.用瀏覽器存取A公司官網)
4. 終端的「**預設DNS**」受理查詢並進行解析
5. 各層**權威主機**提供相關DNS紀錄
6. 「**預設DNS**」快取並回覆解析結果
7. **Client終端**取得IP後與網頁主機建立連線

中華電信 Chunghwa Telecom

DNS DDoS

情境：標的為DNS權威主機



DNS DDoS (cont.)

情境：標的為DNS快取主機