



---

# 網頁應用程式防火牆 方案簡介

數位通國際

---

# 網站安全事件頻傳

## 網站安全攸關企業的營運、資料、交易及形象

yahoo! 97.2K 人追蹤 ☆追蹤

### 期交所：凱基期貨網頁版交易平台 26日疑遭駭客攻擊

2021年11月27日 · 1分鐘 (閱讀時間)

又傳駭客入侵！國內證券商日前傳出駭客入侵網路下單資安事件後，台灣期貨交易所今天也表示，昨天（26日）下午5時37分接獲凱基期貨的資安事件通報，該公司網頁版交易平台疑似遭駭客攻擊，凱基期貨已立即封鎖駭客攻碼，且近期憑證申請採人工加強驗證等措

自由財經 財經政策 Strategy 影音專區 video 國際財經 International 證券產業 Securities 房產資訊 Estate

首頁 > 財經政策

### 7家證券期貨商遭「撞庫攻擊」 金管會祭3大措施

2021/12/15 07:40

LINE

### 駭客入侵《菱傳媒》 襲擊後台、資料庫刪光所有新聞

新頭殼newtalk | 魏寶燭 綜合報導  
發布 2021.12.06 | 20:35

TBS 新聞網 64.4K 人追蹤 ☆追蹤

### 逾20家四五星飯店遭殃！全台最大票券商遭駭客竊個資

28 林啟獻 徐國衛  
2021年11月26日 · 3分鐘 (閱讀時間)

中央通訊社

### Apache Log4j爆嚴重漏洞 Steam、iCloud等恐淪駭客攻擊目標

2021/12/11 16:25 ( 12/12 14:41 更新 )

# 進行網站安全防護的困難



原廠本身漏洞  
無法自行修改



運行中的架構  
調整不易



系統老舊無法  
修正漏洞



資安威脅手法  
日益複雜

# WAF對網站安全防護的效益



原廠本身漏洞  
無法自行修改



運行中的架構  
調整不易



系統老舊無法  
修正漏洞



資安威脅手法  
日益複雜

WAF  
功能

可針對原廠漏洞問題  
提供暫時性的防護措施

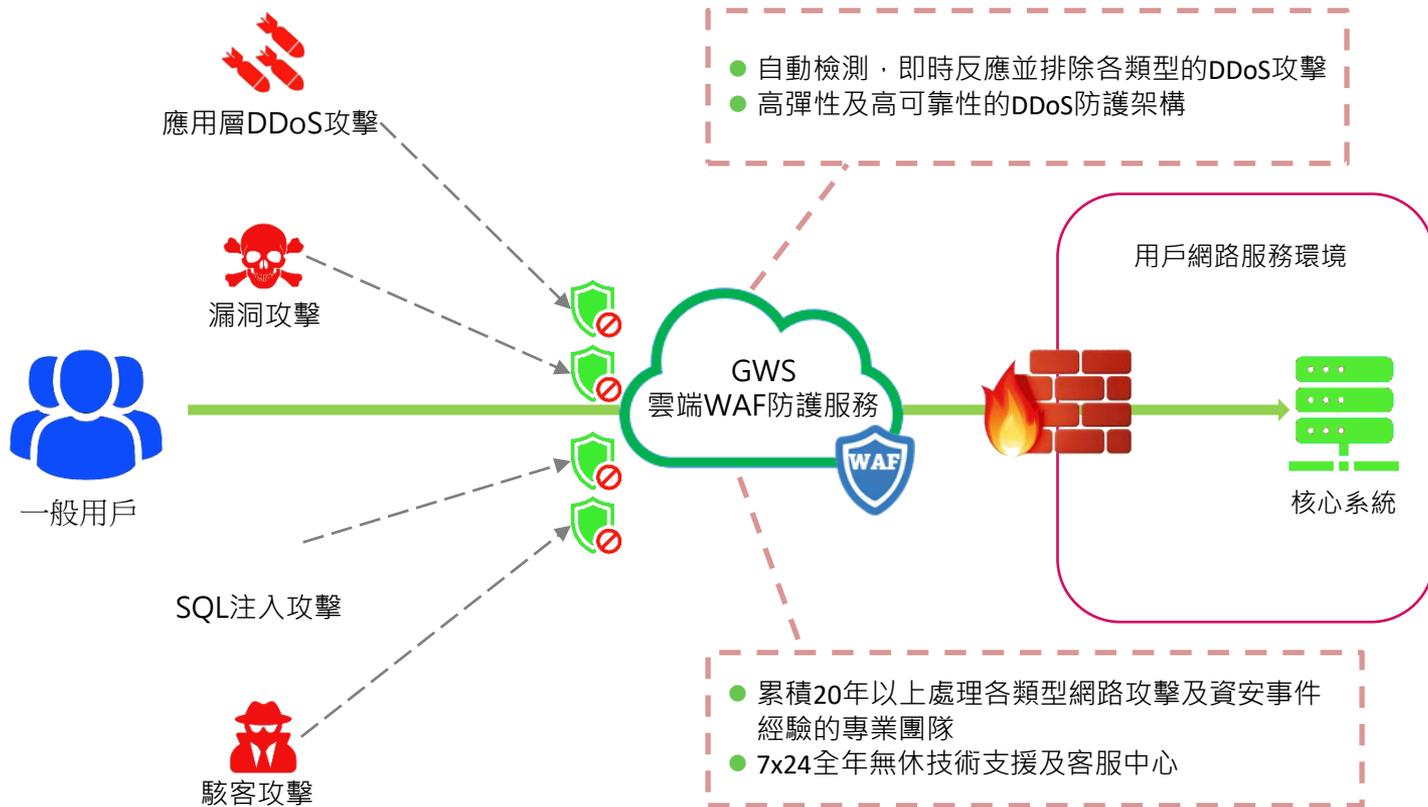
可針對現有漏洞問題  
設定專屬的防護規則

透過機器學習與行為分  
析，防護未知攻擊

達到保護企業資產  
避免損失的目標



# GWS 雲端WAF防護服務



# 實際案例介紹\_Log4j

The screenshot shows the iThome website's navigation bar with categories like 新聞, 產品&技術, 專題, AI, Cloud, DevOps, 資安, 研討會, 社群, 零信任資安講堂, and a search icon. Below the navigation bar, there are three main sections: 揭曉 2022 數位轉型的資安關鍵, 投稿分享SRE心法與建議, and 2022 iThome臺灣雲端大會 徵稿啟動!. The main content area features a news article with the headline "可俘虜數十億臺系統與設備! 超級資安漏洞風暴正在席捲全球". The article text states: "Log4j的運用遍及世界各地與多種產業, 若不及時修補高風險資安漏洞Log4Shell, 等將如入無人之境, 深入企業網路環境與多種IT系統胡作非為". A search bar with the text "即刻探索" is visible on the right side of the article preview.

2021年12月網路上揭漏十年最危險的資安漏洞之一。這個名為「Log4j」(或Log4Shell) 的開放原始碼軟體漏洞，因為 Log4j被使用於Java語言、網站伺服器及網路應用的紀錄方案, 因此它的影響遍及各種企業廣泛採用的應用程式和服務，包括：蘋果iCloud、微軟Azure、Amazon、Google等，以及Oracle、IBM、Red Hat、Vmware、Cisco、Splunk 等等.....

## 實際運用介紹\_ Log4j防護

針對特徵碼進行防護，將以下幾項特徵加入WAF防護規則中，可緩解Log4j造成的影響

- Log4j 標頭
- Log4j 主體
- Log4j 網址





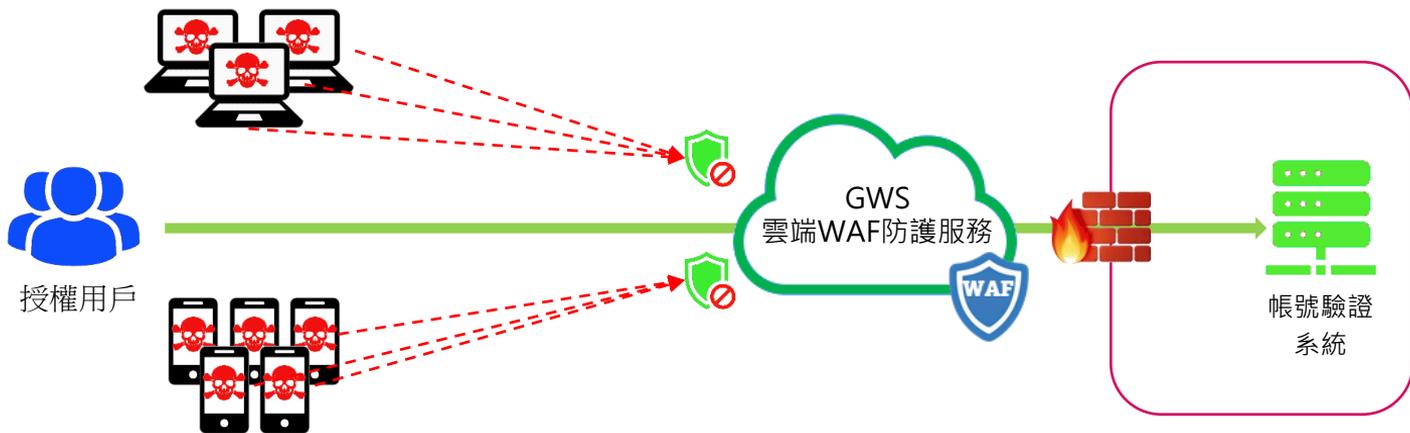
駭客使用撞庫攻擊行為模式如下:

- 1.透過不法方式取得外洩之帳密個資
- 2.使用自動化程式針對特定網站進行帳密驗站(撞庫攻擊)
- 3.透過撞庫取得可驗證成功之帳號及個資
- 4.使用成功驗證之帳號個資，登入應用系統，進行不法利益行為及破壞

## 實際運用介紹\_撞庫攻擊

針對行為進行防護

- 對單一帳號透過多個不同IP嘗試登入
- 對單一IP使用多個帳號進行嘗試登入
- 利用機器學習方式精準辨識自動化及爬蟲行為，防止駭客進行帳號驗證動作



# Thank You



0800-880-668



cs@easpnet.com



www.easpnet.com

 eASPNet

The logo for eASPNet, featuring a stylized circular icon to the left of the text "eASPNet". The background of the entire slide is a grayscale photograph of a city skyline with several skyscrapers. A vibrant, multi-colored diagonal line (with shades of blue, purple, red, and green) runs from the bottom-left towards the top-right, crossing the blue box and the logo.