網路營運商之路由安全相互協議規範(MANRS)

Mutually Agreed Norms for Routing Security (MANRS)

中文版

（本文為 https://www.manrs.org/isps/ 之翻譯，
於 2019 年 9 月，由 TWNIC 提供此翻譯中文版供參考。）

概述

在動機面，安全通常都是一個困難推動的領域。全球網際網路基礎設施的資訊安全，無論 DNS 或路由，都會帶來額外的挑戰：資安措施的效果常是取決於眾多其他各方的協調行動。

綜觀網際網路的歷史，各方參與者之間的合作以及分擔平順運作之責任，一直是支撐網際網路驚人成長與成功，以及其安全與韌性(resilience)的兩大支柱。技術解決方案為不可或缺的要素，但是僅有技術仍不足夠，為了能明顯改善此領域，需要在集體責任文化方面進行更大幅的改變。

本文之目的在於取得此合作精神，並針對解決全球網際網路路由系統的資訊安全及韌性等問題，為網路營運商提供指引。另一個重要的目標是記錄行業領導者在解決此類問題方面的承諾，且隨著更多支持者的加入，應可擴大其影響。

目標

1. 藉由展示不斷成長之支持者群體的承諾，喚起意識及鼓勵採取行動
2. 針對網際網路全球路由系統的韌性及資訊安全，促進集體責任的文化
3. 展示業界以集體合作之精神，解決網際網路全球路由系統之韌性及資訊安全問題的能力
4. 為 ISP 提供工作架構，以深入瞭解和協助解決與網際網路全球路由系統韌性及資訊安全有關的問題

範圍

在改善網域間路由系統之資訊安全及韌性方面，有許多不同的建議，且有部分建議似乎有些矛盾，其關鍵決定通常是源自於瞭解對特定網路最重要或最適當的面向，同時考慮該網路的大小及資源、外部連線數量、擁有的客戶與最終使用者、員工數量，以及專業知識等。

下列預期及進階行動(Expected and Advanced Actions)強調一系列對於全球路由系統之整體資安與韌性，以及網路營運商本身極具有價值的建議。主要解決三種問題：

- 與錯誤路由資訊有關的問題，
- 與偽造來源 IP 位址流量有關的問題，以及
- 與網路營運商之間的協調及合作有關之問題。

預期行動定義了基本的「方案」－一套應明確由支持此 MANRS 文件之營運商執行的建議。此方案非詳盡無遺，且預期有許多網路營運商已開始或計畫於未來實施更有效的措施及控制。本文件稍後提到的進階行動，為此基本方案的進一步延伸。

我們意識到一項事實，亦即任何特定之行動都不是所述問題的全面性解決方案。但是，如果大量支持者中的每一位都踏出一小步，則可能會大幅改善全球網際網路路由系統的韌性。因此，行動的選擇係以小量增加的個別成本與潛在共同利益之間的平衡，做為評估基礎。

定義

為了闡述預期及進階行動的具體內容，即必須明確定義許多用語，以說明其於網際網路行業中的一般用途。

- **基礎設施(Infrastructure)**－營運商的內部網路，必須能在網際網路上存取。
- **最終使用者(End User)**－在營運商路由及管理網域內的網路。
- **對等網路(Peer Network)**－與您相應之基礎設施及客戶網路交換流量的外部網路。
- **中轉網路(Transit Network)**－發送與您的基礎設施及客戶網路有關的流量，但是，一般是從該處接收來自網際網路之流量的外部網路。
- **客戶網路(Customer Network)**－營運商提供中轉服務的外部網路。
- **單一定址(Single Homed)**－網路之間或連接一個最終使用者與基礎設施的單一、簡單連結，且代表流量可在網路內或網路之間流動的單一路徑。
- **多重定址(Multi Homed)**－網路之間（甚至多個網路間）或連接一個最終使用者與基礎設施之間的多重路徑，且可在基礎設施及網際網路上建立多個路徑，以使流量可以來回移動。

原則

1. 組織（ISP／網路營運商）意識到全球路由系統相互依存的本質，以及其本身在促進安全和具有韌性之網際網路中的角色。
2. 組織將與路由資訊安全及韌性有關之最佳實務，整合至其內部與本行動一致的網路管理程序中。
3. 組織致力於透過符合行動之同行及其他 ISP 協調合作，防止、偵測及減緩路由事件。
4. 組織鼓勵其客戶及同行採取這些原則及行動。

預期行動

1. 防止傳播錯誤的路由資訊。

- 網路營運商定義了明確的路由政策，並已建置一個系統，確保其本身及其客戶發布至相鄰之網路上，具有前綴與 AS 路徑粒度之通知的正確性。
- 網路營運商能與相鄰之網路通訊，以指出哪些是正確的通知。
- 網路營運商負責檢查其客戶之通知的正確性，特別是客戶是否合法持有其通知的 ASN 及位址空間。

討論：

最重要的是透過使用***顯示***的前綴層級過濾器或同等機制，保障內送路由廣告，特別是來自客戶的此等廣告。其次，可使用 AS 路徑過濾器，要求客戶網路表明係屬於該客戶下游的自治系統(ASes, Autonomous Systems)，或採用封鎖 ASes 客戶通知的 AS 路徑過濾器，由具有免費關係的供應商防範部分路由「洩漏」類型。僅透過 AS 路徑過濾器過濾客戶的 BGP 通知，***不足以***防範系統層級的災難性路由問題。

參考文件：

- 「網際網路服務供應商資安服務及程序建議(Recommended Internet Service Provider Security Services and Procedures)」，Section Network Infrastructure, http://www.rfc-editor.org/bcp/bcp46.txt
- 「BGP 操作及安全(BGP operations and security)」，https://datatracker.ietf.org/doc/rfc7454/
- 邊界閘道協定安全，NIST 特刊 SP 800-54 (Border Gateway Protocol Security, NIST: Special Publication SP 800-54)，http://csrc.nist.gov/publications/nistpubs/800-54/SP800-54.pdf

- 「大型網際網路服務供應商(ISP) IP 網路基礎設施作業安全要求(Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure)」，http://tools.ietf.org/html/rfc3871
- 「RPSL 使用實務(Using RPSL in Practice)」，http://tools.ietf.org/html/rfc2650
- 「以 RIPE 資料庫做為網際網路路由暫存器(Using the RIPE Database as an Internet Routing Registry)」，https://labs.ripe.net/Members/denis/using-the-ripe-database-as-an-internet-routing-registry
- BGP 安全實佳實務，FCC CSRIC III WG4 最終報告(BGP Security Best Practices, FCC CSRIC III WG4 Final Report)，http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf

2. 防止偽造來源 IP 位址的流量。

- 網路營運商建置了一個至少能為單一定址的袖珍客戶網路、本身之最終使用者，以及基礎設施進行來源位址認證的系統。網路營運商開始實施防偽造過濾，以阻止具有錯誤來源 IP 位址的封包進入及離開網路。

討論：

解決此問題的常見方式與軟體特性有關，例如在纜線數據機網路上的 SAV（來源位址認證），或在路由器網路上的嚴格 uRPF（單播逆向路徑轉發）認證。這些方法皆可在路由及拓撲相對較不具動態之情況下，減輕管理的負擔。另一個方式為使用內送前綴過濾器資訊，建立一個僅允許具有來源 IP 位址之封包的封包過濾器，使網路可以合法宣傳其可達性。

參考文件：

- 「網路入口過濾：防禦使用偽造 IP 來源位址的阻斷服務攻擊(Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing)」，http://tools.ietf.org/html/bcp38
- 「多重定址網路之入口過濾(Ingress Filtering for Multihomed Networks)」，http://tools.ietf.org/html/bcp84
- 「鞏固邊緣安全(Securing the Edge)」，http://www.icann.org/committees/security/sac004.txt
- RIPE 防偽造工作小組(RIPE Anti-Spoofing Task Force HOW-TO)，http://www.ripe.net/ripe/docs/ripe-431

- BGP 安全實佳實務，FCC CSRIC III WG4 最終報告(BGP Security Best Practices, FCC CSRIC III WG4 Final Report)，http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf

3. 促進網路營運商之間的全球運作溝通及協調。

- 網路營運商留存可全球存取之最新的聯絡資訊。

討論：

留存此等資訊的常見位置，包括 PeeringDB、RIRs 的 whois 資料庫，以及 RADB 和 RIPE 等大型 IRR。網路營運商應至少在上述之一的資料庫中登錄和全天候聯絡資訊，且應包括營運商針對 AS 的 NOC、所有網區及網域名稱的最新聯絡人資訊。鼓勵營運商在 IRR 中記錄其網路路由政策，同時歡迎記錄額外的資訊，例如在其 PeeringDB 紀錄中之適當欄位內的窺鏡 URL (looking glass URL)。

參考文件：

- 「RPSL 使用實務(Using RPSL in Practice)」， http://tools.ietf.org/html/rfc2650
- Peering DB, https://www.peeringdb.com
- RADB, http://www.radb.net/

進階行動

4. 促成全球規模的路由資訊認證。

- 網路營運商具有可向外部各方宣傳的路由政策、ASN 及前綴等公開文件紀錄。

討論：

為了促成全球規模的其他網路路由資訊認證，有必要提供可向外部各方宣傳的路由政策、ASN 及前綴等資訊。

使政策可公開取得的方式之一，是在任何一個由 RADB 鏡像的網際網路路由暫存器(IRR)（例如 RIPE、ARIN、RADB）中，利用 RPSL 進行記錄。於此情況下，營運商必項登錄與維護至少一個（或多個）可供自動工具使用，含有向外部各方宣傳之 ASN 列表的「如設定(as-set)」IRR 物件，以產生前綴過濾器。營運商同時必須維護其於 IRR 內的資訊，以確保為最新資訊。

另一種促成全球規模認證之更安全的措施，是透過 RPKI 系統。營運商可向分配該前綴的 RIR 取得本身之前綴的 RPKI 證書，並公開及維護與其發布之前綴對應的 ROA。

營運商亦必須鼓勵其客戶網路營運商採取此方式，以協助其他網路在全球規模上認證通知。

參考文件：

- 「RPSL 使用實務(Using RPSL in Practice)」，http://tools.ietf.org/html/rfc2650
- 「以 RIPE 資料庫做為網際網路路由暫存器(Using the RIPE Database as an Internet Routing Registry)」，https://labs.ripe.net/Members/denis/using-the-ripe-database-as-an-internet-routing-registry
- 「以資源公鑰基礎設施(RPKI)為基礎的來源認證作業(Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI))」，http://www.rfc-editor.org/bcp/bcp185.txt