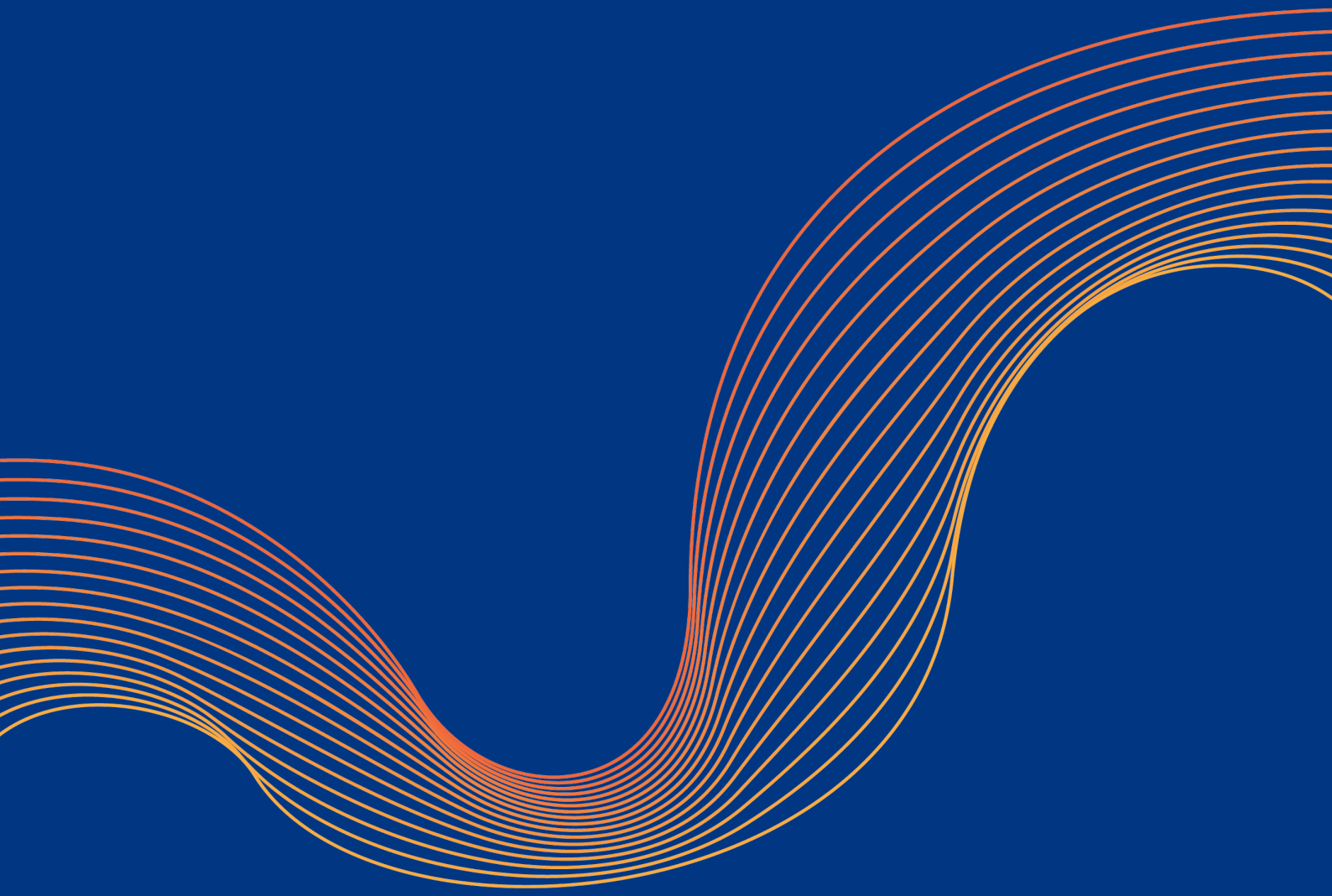
白皮書

Cloudflare 網路如何維護資料隱私



+ 886 8 0185 7030 | enterprise@cloudflare.com | www.cloudflare.com/zh-tw/

目錄

介紹

Cloudflare 的網路和業務最終都建立於客戶信任的基礎之上。為尋求不斷贏得和維護這種信任，我們不僅建立了隱私權至上的原則和程序，來指導我們管理系統上的客戶和最終使用者資料，而且將隱私權融入於我們的產品和服務中。為此，我們持續增強系統安全性，加密靜態和傳輸中資料，並允許我們的客戶自行決定如何檢查世界各地的流量。

本文詳細介紹了當資料通過我們的網路傳輸時，以及當我們分析網路中的中繼資料 (Metadata) 時，Cloudflare 如何使用安全措施來保護隱私權。

第 1 部分說明了資料如何周遊於我們的全球資料中心邊緣網路，以及我們如何在該網路中運用加密手段以保證隱私權。

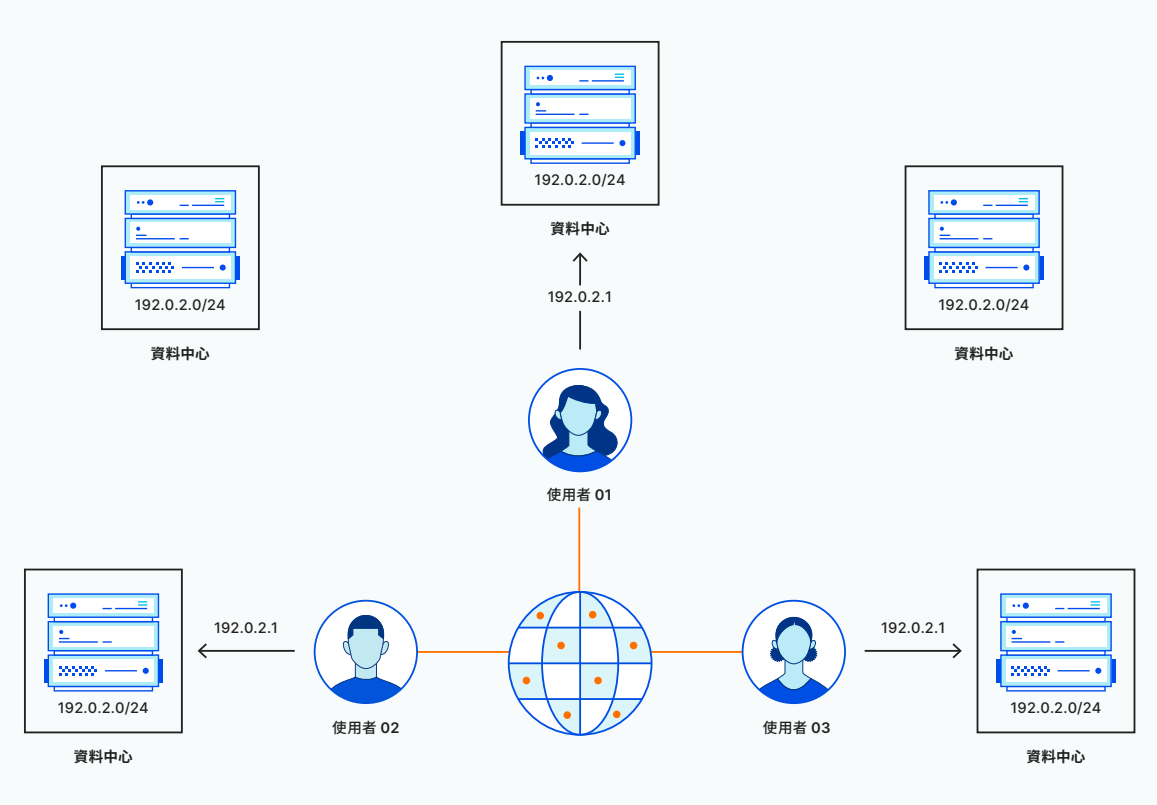
第 2 部分說明了我們如何使用加密來保護我們從該邊緣網路中收集的中繼資料 (Metadata)。

第 3 部分討論了我們如何保護加密金鑰，以使外界無法破解加密。

第 1 部分：如何在 CLOUDFLARE 網路上傳輸資料

Cloudflare 網路所包含的資料中心遍布 100 多個國家/地區的 200 多個城市。為了確保復原能力和更高的效能，Cloudflare 網路被建構成 Anycast 網路，這意味著每個地點都會公告所有 Cloudflare IP 位址。由於這種建構方式，使用者一旦針對 Cloudflare 網路上的某網站或應用程式提出請求，總是會被導向至距離他們最近的資料中心。

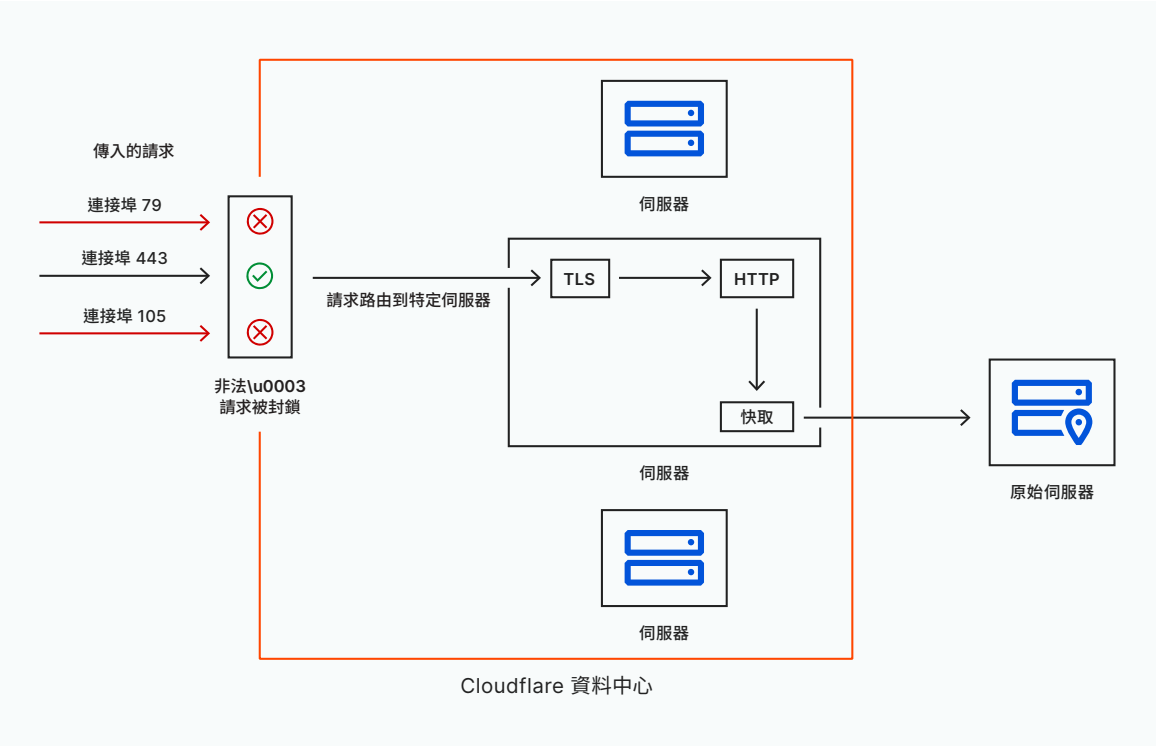
舉例而言，德國科隆的 Katerina 載入了一個位於 Cloudflare 網路上的網站。她對該網站的請求傳送到了位於德國杜塞爾多夫的 Cloudflare 資料中心，該資料中心距離她只有 45 公里左右。現在假設 Katerina 第二天驅車前往德國法蘭克福，並載入同一個網站：由於法蘭克福的 Cloudflare 資料中心公告的 IP 位址與杜塞爾多夫的資料中心相同，因此 Katerina 的請求現在被導向到法蘭克福的資料中心。



第 1 部分：如何在 CLOUDFLARE 網路上傳輸資料

像 Katerina 這樣的使用者將其裝置連線到任一 Cloudflare 資料中心後，將按如下方式處理請求：

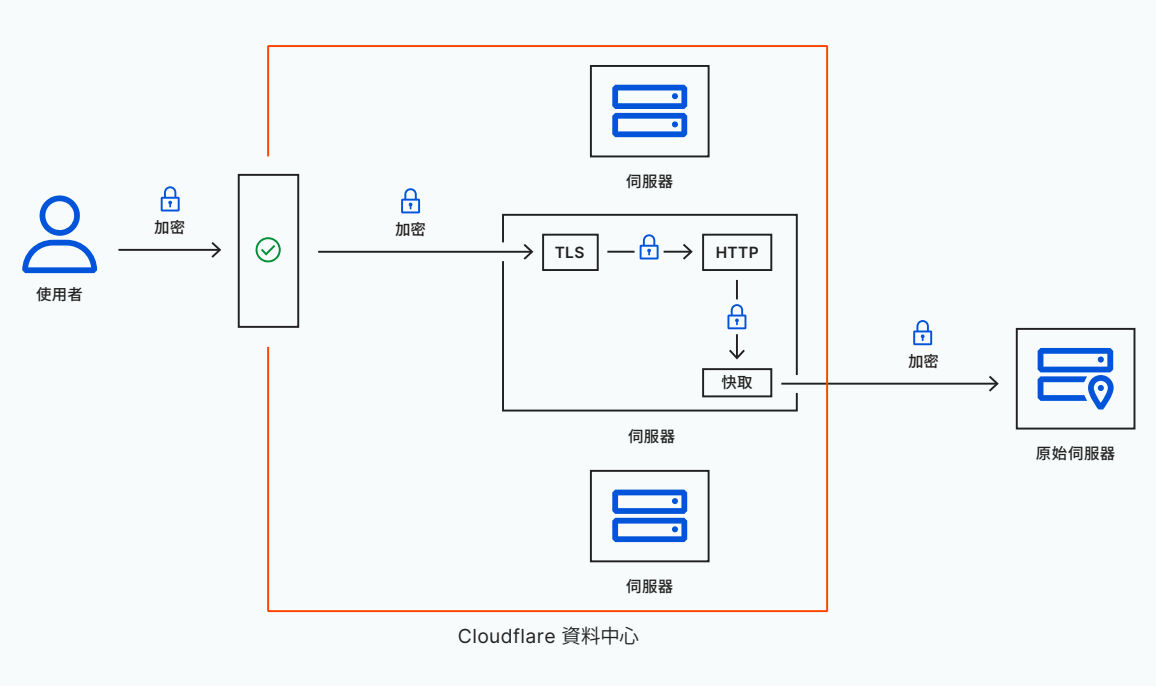
- 某些類型的資料請求若可用於網路攻擊，則會根據位址資訊立即刪除。
- 接下來，使用客戶所請求的業務邏輯（頁面規則、防火牆規則、限速等）對該請求進行檢查。這可以偵測和預防各種類型的網路攻擊和惡意流量，包括第 7 層 DDoS 攻擊、自動機器人流量、憑證填充和 SQL 資料隱碼攻擊等等。
- 隨後，將請求傳遞到快取。如果快取可以在請求中填入被快取的內容副本，它就會這樣做；如果不可以，它會透過網際網路，將請求轉寄到客戶的原始伺服器。如果客戶啟用了加密，Cloudflare 伺服器與原始伺服器之間的流量就會經過加密。
- 如果回應來自客戶的原始伺服器，則任何靜態內容都會快取到加密磁碟上。然後，回應就會在網際網路中透過該鏈結回到使用者處。



第 1 部分：如何在 CLOUDFLARE 網路上傳輸資料

HTTP 請求的隱私權

根據客戶指示，Cloudflare 會對在最終使用者與任何 Cloudflare 資料中心之間傳輸的所有資料強制使用 TLS 加密。無論中間第三方是提供傳輸服務的中間網路，還是惡意攻擊者，都無法查看加密資料，這確保了資料的隱密和安全。



資料中心內的流量、資料中心之間的流量以及 Cloudflare 網路與客戶源站之間的流量，同樣亦會經過加密。此外，Cloudflare 資料中心內的所有請求和回應都會在記憶體中得到處理；除了被快取的靜態內容外，任何內容都不會寫入磁碟，並且所有快取磁碟都已加密。

如何使用 Cloudflare Regional Services 傳輸資料

許多 Cloudflare 客戶紛紛表示，他們願意對資料的處理地點和方式進行精細控制。

憑藉 Cloudflare Regional Services，Cloudflare 客戶能夠指定他們希望的資料檢查地點。對於已啟用 Regional Services 的客戶，Cloudflare 網路會以上述相同方式處理請求，但一個重要的區別在於：只有當這些請求到達指定地區內的網路中心時，才會檢查請求的網路安全風險，並且對請求進行快取。

最終使用者的請求仍會傳送到距離最近的資料中心（距離以網路躍點數衡量）。如果資料中心位於指定地區之外，則該請求會先轉寄到指定地區內的資料中心，然後再套用業務邏輯。Regional Services 客戶會獲得專用 IP 位址以啟用此特定於地區的處理，同時仍享有全球 DDoS 保護的優勢。

第 2 部分：資料收集和隱私權

Cloudflare 從邊緣收集哪些資料？

Cloudflare 的業務從不立足於追蹤使用者或販賣廣告，我們力求最大限度減少對個人資料的收集。Cloudflare 從我們的全球資料中心邊緣網路收集中繼資料 (Metadata)，以保持網路平穩運轉並最佳化我們的服務，這些中繼資料 (Metadata) 主要屬於技術性質；中繼資料 (Metadata) 包含的個人資料極其有限，通常以 IP 位址的形式存在。收集到的資料將傳送到位於美國的核心資料中心進行處理。

Cloudflare 收集的中繼資料 (Metadata) 分為三大類：

1. **系統指標和偵錯資料**
2. **Cloudflare 資料中心產品收集的資料**
3. **用於運轉 Cloudflare 網路的 HTTP 請求中繼資料 (Metadata)**

下文將詳細介紹每一類中繼資料 (Metadata)。

1. 系統指標和偵錯資料

Cloudflare 收集並處理與伺服器和網路效能相關的各種指標，例如特定資料中心每分鐘收到的請求數，或資料中心之間的往返時間 (RTT)。這些指標被收集起來作為彙整的統計資料，脫離了上下文背景。這些彙整的統計資料不包含個人資料，將傳送至我們的核心資料中心進行處理。從邊緣傳送至核心的所有資料皆在傳輸過程中使用 TLS 加密。

Cloudflare 還從運轉於邊緣網路上的所有軟體中收集偵錯資訊，用於日常維護。

所有這些資料僅在必要限度內收集，目的是為了保持 Cloudflare 網路和 Cloudflare 服務的正常運轉。除了在傳輸過程中使用 TLS 加密之外，所有這些資料還在我們的核心資料中心內透過硬碟加密進行靜態加密。

2. Cloudflare 資料分析產品

Cloudflare 為客戶提供資料產品，使他們能夠瞭解 Cloudflare 的服務以及如何更有效地使用 Cloudflare。我們的資料產品亦有助於客戶更好地保護自己的原始伺服器、設定我們的服務，並瞭解自身業務和系統的特性。

我們所有的資料產品都衍生自與運轉於邊緣資料中心的軟體有關的中繼資料 (Metadata)。例如，就 HTTP 請求而言，Cloudflare 納入了 URL、有關 Cloudflare 功能使用情況的資訊、時間資訊、快取資訊以及指定 HTTP 請求和回應標頭。同樣，Cloudflare 還收集與 DNS 請求、TCP 流、Access 登入、串流視訊觀看以及我們所有產品有關的中繼資料 (Metadata)。我們還提供隱私權至上的網頁分析服務，讓客戶深入瞭解使用者如何瀏覽他們的網站。

在客戶啟用的情況下，Cloudflare Logs 會向客戶提供有關每個事件的詳細資訊。這些在傳輸過程中加密的資料會從邊緣網路傳送回核心，然後推送給客戶。客戶可以選擇將加密的記錄資料儲存在核心中長達 7 天時間。

Analytics 和 Logs 都能對往返於邊緣網路以及往返於客戶的資料進行傳輸中加密。

第 2 部分：資料收集和隱私權

3. Cloudflare 使用的隨機採樣的 HTTP 流量資料

Cloudflare 儲存透過我們網路提供的所有 HTTP 流量的簡單隨機樣本。這些資料經過匿名處理，無法用於在不同的網際網路設備之間追蹤個別使用者。Cloudflare 無法將任何一個 IP 位址與任何一個自然人聯繫起來。收集的所有樣本資料都會透過加密連線進行傳輸、使用安全影碟加密進行儲存，並保留有限的一段時間（不超過 12 個月）。我們使用樣本資料來診斷惡意活動、幫助調查客戶事件，並提高我們安全產品的整體效果。在我們整個網路中採樣的資料會不斷累積智慧，讓每一位 Cloudflare 客戶都受益良多。

第 3 部分：我們對加密金鑰的保護

加密是我們各項技術措施的基礎，用於保護流經我們網路的客戶內容及中繼資料 (Metadata) 的隱私權。沒有第三方能夠破解我們網路上的加密。這對於隱私權具有至關重要的影響：只要加密金鑰是安全的，則受該加密保護的內容就會是隱秘的。

作為一家安全公司，Cloudflare 將保護加密金鑰視為首要目標。為了確保加密金鑰的安全，Cloudflare 建立了嚴格的物理安全標準和存取控制系統。正如 Cloudflare 透明度報告中所述，我們還許下了一個長期的公開承諾：如果任何政府試圖存取我們或我們客戶的加密或認證金鑰，我們都會竭力反抗。

鑑於加密金鑰的保密與保護具有極其重要的作用，我們認為不僅要建置強大的存取控制系統，還要確保我們的客戶可以自由選擇對自己的加密金鑰進行精細控制。如果客戶希望在資料中心這一精細度層級上限制儲存金鑰的地理區域，建議使用 Geo Key Manager。如果客戶希望在內部保管他們的私密金鑰，同時繼續使用我們的 SSL 服務，建議使用 Keyless SSL。

結論

Cloudflare 的使命是幫助建設更美好的網際網路。我們堅信，保護資料隱私權是實現該使命的重要前提。我們將延續十餘年來的努力，繼續銳意創新，確保我們的客戶乃至整個網際網路的隱私和安全。

CLOUDFLARE

白皮書