HIBUN

HITACHI
Inspire the Next

預防資料外洩解決方案

JP1/HIBUN Device Control

管制機密資料的路徑來防止資料外洩

如今，公司的 IT 資產使用範圍不僅限於辦公室內，也包括辦公室外。透過建置 JP1/HIBUN　系統，監管設備和網路，避免資料外洩。

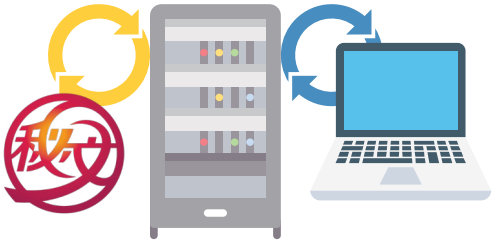
JP1/HIBUN Device Control 的資料外洩預防措施

控管資料存儲媒體

透過禁用各種可攜式存儲媒體（智慧型手機和 USB 等），防止未經授權的資料複製。

限制可連接的網路

JP1 禁止在不透過公司網路的情況下連接互聯網，例如使用智慧型手機共享網路。因此，這將迫使員工遵守 VPN 的使用規範。



從 WSUS* server 自動發佈 JP1/HIBUN 補丁

每當有 Windows 需要更新時，您不需要自行升級 JP1/HIBUN Server，因為 JP1/HIBUN Server 會透過 WSUS 伺服器自動向用戶端發佈補丁。
WSUS* : Windows Server Update Services

JP1/HIBUN Device Control 可以...

管制各種設備

JP1 可以透過管制 PC 或 PC 群組的可攜式媒體 (如智慧型手機、USB 或 SD 卡) 或是網路通訊方式 (如無線、有線網路和藍芽) 等方式來防止資料外洩。

透過 WSUS 無縫對接 WaaS*2

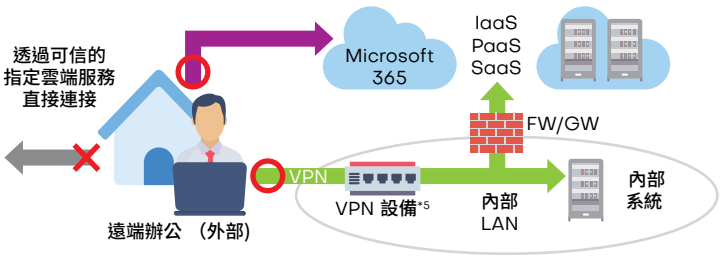
JP1/HIBUN 補丁被註冊到 WSUS Server 後，會被自動發佈到 JP1/HIBUN 用戶端，無需升級 JP1/HIBUN Server 或重新設計參數，因此可在 Window 10 中繼續使用 JP1/HIBUN。

可連接的網路限制或使用PC的場所

JP1 可以禁止未經管理者允許使用智慧型手機的網路共享方式連接到網路。JP1 也可以在未經授權的地方鎖定 PC 禁止其使用。*3

除了連接到特定雲端服務之外，強制使用 VPN

當 PC 在公司外使用時，JP1 可以強制使用者經由內部 VPN 伺服器，從而保持內網的高度安全。也允許客戶不經由VPN ，利用翻牆*4技術直接連到可靠的特殊雲端服務。



*1智慧型手機根據其作業系統、製造商、連接方法等被識別為各種設備。JP1/HIBUN 透過禁止使用所有這些設備來防止資料被複製。
*2 WaaS: Windows as a Service *3 透過使用 JP1/HIBUN Data Encryption 對PC數據進行加密，可以更可靠地保護重要資訊。 *4 這是一個無需通過防火牆、閘道器和VPN就可以直接進入互聯網或是雲端服務的系統。 *5 只有穿隧類型的 SSL-VPN 是目標。

Hitachi Asia Ltd.
7 Tampines Grande #08-01, Hitachi Square, Singapore 528736 • **Tel:** +65 6535 2100 • **Fax:** +65 6260 0717 • **Email:** jp1.info.px@hitachi.com

代理商
APES. 艾博斯科技 股份有限公司 APES Technology Co., Ltd.
高雄總公司: 高雄市苓雅區海邊路31號26樓之7・**Tel:** 07-3310858・**Fax:** 07-3314840・**Email:** marketing@apes.com.tw
台北辦公處: 台北市內湖區行善路48巷56號2樓之1・**Tel:** 02-25777669・**Fax:** 02-25773969