國軍資訊備援中心規劃研究—以國軍某網路資料中心為例 Camera Ready
Study of the Model Plan for Military Backup Centers - Taking a military IDC Case

黃志泰 林佳穎

Gai-Tai Huang Chia-Ying Lin

德明財經科技大學 德明財經科技大學

資訊管理系 資訊管理系

副教授 碩士研究生

hgt@takming.edu.tw Carolin2351@gmail.com

摘 要

我國空軍分別於北、南、東區建立以雲端運算為服務概念建置網路資料中心(Internet Data Center，IDC)，同步提供各項應用服務給空軍各單位，達成應用服務集中控管之目的，並於各區建置分布一般行政作業區與機敏作業區，整體方案採用以雲端運算為基礎架構之虛擬化中央即控中端服務應用(Terminal Service)為主體，讓空軍各單位使用者於國軍廣域網路內自由存取及使用雲端服務，有效提升作環境及效率。

然而再好的資料中心也無法避免自然與人為的災害，尤其是國軍提供的服務中更包含了各項戰演訓系統，要如何在災難時候讓服務不中斷，有效減少資料落差(RPO)及加速服務啟動(RTO)，此時備援中心更為其備援系統的核心。

我國目前的備援模式僅利用檔案傳輸方式將備份檔案傳輸至另一 IDC 的儲存區域，若遇緊急情況再將資料傳回援 IDC 再於同機執行復原程序，這中間包含查修、找到問題、執行復原都是系統可能維持停止服務的時間，目前執行的演練科目也只是讓搶修時間盡量縮短，無法做到服務不中斷的程度。

本研究整理分析資訊中心的各種備援方法，並依我國空軍現行架構規劃一高可靠性及實用性的備援中心，先以比較分析法以分析各項資料中心備援模式與資料複製法，模式建立後再規劃出適用於空軍北部網路資料中心的備援中心。

目前異地備援機制分冷備援機制、溫備援機制、熱備援機制以及複合式備援機制，其中以複合式異地熱備援機制最適合本研究備援中心規畫需求，符合備援中心的設備及資料隨時處於待命的要求，並能即時運轉提供服務，當主要資料中心發生不預期的事件時，能夠立即接手並取代繼續運轉。

關鍵詞：網路資料中心、備援中心、備援模式。

Abstract

ROC Air Force establish Northern, Southern, Eastern Internet Data Center to provide cloud computing service to all Air Force units, to achieve the purpose of centralized management of application services, and to build the distribution of general administrative districts and smart work area work area, the overall program to adopt a cloud computing infrastructure, the virtual control center that is the end of the service application (Terminal Service) as the main body, so that Air Force users have free access within the military WAN and use cloud services, effective for the environment and enhance efficiency.

However, even the best data centers cannot avoid natural and man-made disasters, especially in the services provided services to the military .The point of how to make services are not interrupted when a disaster occur is to reduce Recovery Point Objective (RPO) and Recovery Time Objective (RTO), time of its backup center core aid system.

ROC military current backup mode is using only the backup file transfer to another IDC storage area. In case of when emergency occurred we could load data back and refine on the same machine. The repairing time includes finding the problem, perform system recovery. Our current implementations only to ensure repair time can be as short as possible.

This study analyzes the various backup methods finishing Information Centre, and according to our current Air Force architecture planning a high reliability and practicality backup center, first to the comparative analysis in order to analyze the data center backup mode with the data replication method, model is built after planning to apply to the Air Force in northern network data center backup center.

Contributing IT backup center, besides putting consideration on the information security issues, how to maintain the system service continues is what we want to achieve in this study.

第一章、序論

資訊備援只是資訊安全的一部分，但是當大家只顧著防毒、防駭客或是增加一堆資安設備時，備援卻是最常被忽略的一環。

本章主旨為針對研究動機、目的、範圍，及論文之流程架構，概略性的說明。

一、研究動機

一般企業異地備援的重要性及迫切性，在於資料一旦損毀，就沒有挽回的餘地，更何況是在軍中的各項戰演訓服務系統，只要停止福袋，帶來的影響就不只是損失金錢這麼簡單。

我國空軍分別於北、南、東區建立以雲端運算為服務概念建置網路資料中心(Internet Data Center，IDC)，同步提供各項應用服務給空軍各單位，達成應用服務集中控管之目的，並於各區建置分布一般行政作業區與機敏作業區，整體方案採用以雲端運算為基礎架構之虛擬化中央即控中端服務應用(Terminal Service) 為主體，讓空軍各單位使用者於國軍廣域網路內自由存取及使用雲端服務，有效提升作環境及效率。

然而再好的資料中心也無法避免自然與人為的災害，尤其是國軍提供的服務中更包含了各項戰演訓系統，要如何在災難時候讓服務不中斷，達成此時備援中心更為其備援系統的核心。

二、研究目的

現行空軍網路資料中心備分模式架構，以成立甲地IDC 為系統主機房，乙地 IDC 為備援主機房，正常情況下，由甲地提供資訊服務，當使用者連線後，經由甲地的網域名稱系統(Domain Name System，DNS)、各應用系統伺服器、資料庫伺服器，再將資料儲存於甲地的磁碟陣列中，再透過儲域網路路由器(SAN Router)，將光纖之網路協定轉換為 IP 網路協定，並將壓縮後的資料傳送至乙的的磁碟陣列中(架構如圖 1)。

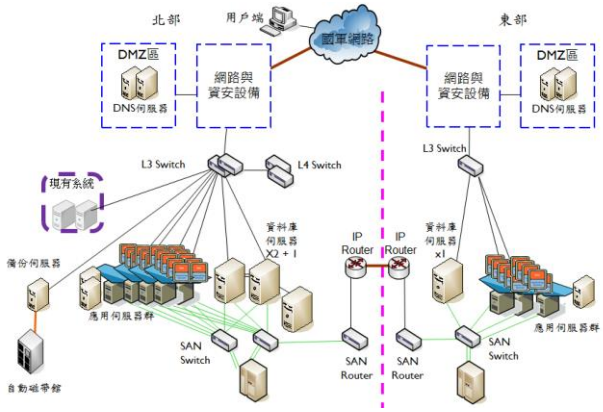

圖 1.現行空軍備援中心架構圖

當甲地 IDC 因故無法提供資訊服務時，及改由乙地 IDC 作業環境提供資訊服務，此時使用這連線時將經由乙地的 DNS、各應用系統伺服器、資料庫伺服器，將資料儲存於乙地的磁碟陣列中(轉換後資料流示意圖如圖 2)。

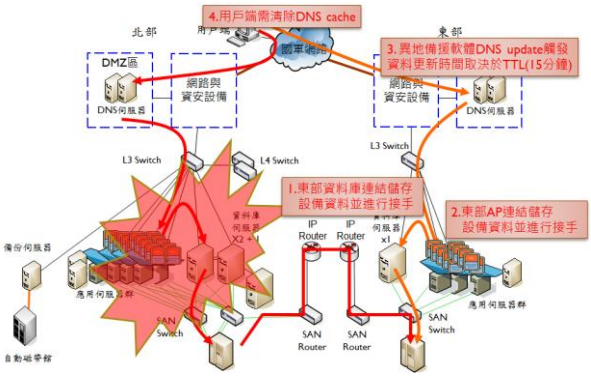

圖 2. 轉換後資料流示意圖

然經單位使用現行備援架構執行備援程序，發現以下問題:

1.異地備援地區雖依規定甲、乙兩地距離須 50 公里以上，但礙於網路品質及頻寬不足問題，加上資料量日益漸增，使得傳輸時間也日漸增加。

2.當資料進行備份時可能會占用系統效能，間接影響到用戶使用情況。

本研究主要目的為依現行架構規劃一高可靠性及實用性的備援規畫，先以比較分析法以分析各項資料中心備援模式與資料複製法，規劃出適用於空軍 IDC 架構的備援中心。

三、研究範圍

本論文研究範圍界定於我國空軍北部網路資料中心備援中心備援建置探討，並置重點於各項戰演訓系統備援模式以及資料複製模式規劃，其餘技術、軟硬體需求、人員管理及機房作業不在再本研究探討範圍內。

四、研究流程

本論文研究流程如圖 3。

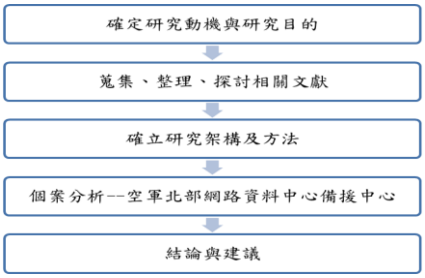

圖 3.研究流程

第二章、文獻回顧

就以備援機制設置地點而言，資訊中心備援機制可分為本地、異地以複合式備援等三種，本研究主要是針對異地備援模式做規劃。

本章主要分成三個部份，第一節將針對營運持續管理，第二節將異地備援，第三節介紹備援中心規畫模式

一、營運持續管理

營運持續(Business Counitinuous)就是災難發生時，能夠在最短時間內恢復系統運作，使各項服務不中斷，將損失降低至最小程度，陳俊賢(2006)認為營運持續為研析並降低人為或意外因素對重要業務可譴導致的威脅，使重要業務在系統發生事故、設備損壞時，仍可持續運作。尤其運用於軍中的系統，當重大災難生時，能夠確保各項服務不中斷，保持上級及各陣地正常的情報傳遞管道暢通。

1-1 衡量標準

為了要以結構化以及合乎常理的方式達到營運持續的目的，以下有 2 個必須考慮的衡量準則:

1. 系統恢復時間(Recovery Time Objective，RTO):
   為備援系統取代原有系統開始提供服務所需的時間。也就是災難發生、系統中服務後，一直到系統恢復運作的時間，也就是可容忍的系統中斷服務時間。
2. 資料回復點(Recovery Point Objective，RPO):
   為備援系統取代原有系統開始提供服務時，在資料上所能回復到的可用時間，也就是災難發生前最近一次資料備份資料或是資料可回復的最近時間點，也就是可容忍的資料損失程度(如圖 4)。

圖 4.RTO、RPO 示意圖

二、異地備援

所謂的災難復原（Disaster Recovery；DR），是針對企業資訊架構進行異地備援，也稱為異地備援系統。它是主系統外的另一套系統，當主系統中斷後，這套備用設備可以立刻接手，企業不需等待原有系統修復，只需將作業環境切換，即可持續正常的工作，讓業務不中斷（Business Continuity）的目標得以達成。其重點在於災難中盡速將系統復原，期望能降低災難對於運作中服務所造成的影響程度。一旦重要資料發生損毀，若無完善的備援機制，將馬上面臨群龍無首，上級命令無法正常下達的情況。更何況現在對於資訊的依賴日益漸劇，對於資訊的即時性更予重視，相對的異地備援更是能夠讓服務不中斷重要的一環。

2-1　異地備援七大等級

IBM（International Business Machine Company）公司本身為資訊大廠，也在災害備援議題上多所著墨，在其出版的「IBM Total Storage Solutions for Disaster Recovery」章節「Seven Tiers of Disaster Recovery」中提到七個資料異地備援的等級，這 7 個層級基本上可以區分為非在線系統、伺服器層次、儲存設備層次。層次由 0 到 7，依照這個定義下的分類，層級越高，備援完備性越高，系統回復時間越短，相對的層級越低，備援完整性越低，系統回復時間越長，圖 5 可以清楚表示各種災難備援方式，而本研究所探討的主要指是 Tier7 高度自動化的企業整合設計方式。

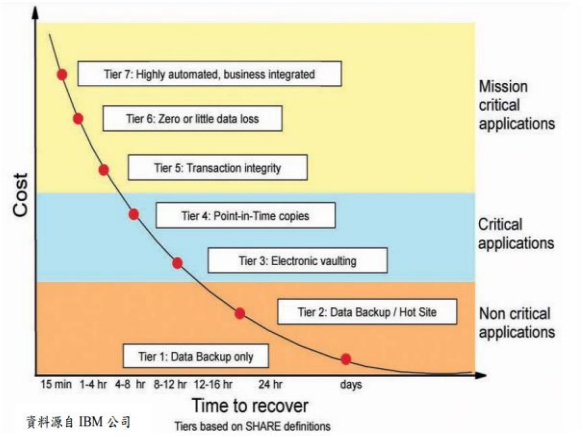

圖 5. 災難備援方式

將異地備援的 7 個等級做一比較表(表 1)，此表可清楚了解各備援等級的差異、備援模式以及資料回復方法。

表 1. 異地備援比較表

備援等級	等級敘述	資料更新/回復方式	主機狀態	RTO	RPO
Tier 0	資料為異地備份(No Off-Site Data)。僅執行本機備份未放置異地	本機備份	無備援主機(Cold Site)	未知	未知
Tier 1	磁帶異地備份(Data Backup with no Hot Site)。定期將資料儲存於磁帶中，並將磁帶運往異地儲存。	磁帶	無備援主機(Cold Site)	2-7天	2-24小時

Tier 2	有備援中心的磁帶備份(Data Backup with a Hot Site)，但備援中心平時不啟動。	磁帶	被動開機 (Warm Site)	1-3天	2-24小時
Tier 3	電信網路傳送備份資料(Electronic Vaulting)。	網路定時	被動開機 (Warm Site)	12-24小時	2-24小時
Tier 4	資料快照 (Point-in-Time Copies)，並以高速網路連結 IDC 與備援中心，資料已磁碟快照與高速網路執行備份。	網路區間異動更新	被動開機 (Warm Site)	12-24小時	5-30分鐘
Tier 5	多重交易系統整合 (Transaction Integrity)，兩中心可透過異動資料管理取得完整資料。	經網路傳輸，由應用程式執行備份及回復作業	主動式 (Hot Site)	1-12小時	5-10分鐘
Tier 6	遠端複製(Zero or Little Data Loss)，採用檔案系統或儲存設備的同步複製/鏡項功能複製資料，使兩中心資料可同時更新。	經網路傳輸，由應用程式執行備份及回復作業	主動式 (Hot Site)	1-4小時	5分鐘
Tier 7	遠端複製及自動化復原(Highly Automated, Business Integrated Solution)，針對電腦系加入 HA 機制，可由預備機立即接替主系統任務。	經網路傳輸，由應用程式執行備份及回復作業	主動式 (Hot Site, Fault Tolerence)	1小時內	5分鐘

2-2 異地備援運作模式

異地備援即是將資訊服務所需要運作的資料及設備分開兩地存放，被園地與資料待命，並可以即時運轉提供服務，以便當主中心設備發生問題時，另一地的備援設備可以上接替運轉，Friedl,WJ(1990)依復原時間要求將備援中心區分為 3 級:

1.冷備援中心(Cold Backup)：此類備援中心只包含高架地板、電力、線路、空調、防火設備。

2.溫備援中心(Warm Backup)：此類備援中心包含冷備援中心所有設備，另包含電腦、磁碟設備及磁帶設備，但頻日並不開機，只等主中心失能時才運作。

3.熱備援中心(Hot Backup)：此類備援中心包含住中心所有硬體設備，當主中心發生意外災害時，備援中心可理級取代。

IBM 於 2010 提出當企業完成雙中心建置，但仍對營運風險的容忍指數極低，則應於距離雙中心至少 100 公里外處，建置第三中心（或第四中心）於做為企業第二道防線，以確保機房資料的安全與完整，達成永續營運目標，如此，當大區域或大規模災變發生於同城雙中心無法運作時，此災難備援中心便能夠以最快速度接手(如圖 6)。

圖 6. IBM 建議兩地三中心規劃圖

第三章、研究方法

本研究以實驗方式作為驗證，採用實驗研究方法當中的「靜態組比較設計」，用以瞭解實驗組與對照組在實驗處理介入後是否產生不同的效果，藉以探討複合式異地熱備援機制架構是否具有高可用性。

一、實驗環境及軟硬體設備

本次以國軍公文系統資料備份作業作為實驗參考，並於甲地另一機房上至同規格硬體，建立磁碟陣列 HA 備援機制(如圖 7)，以原備份方式以及新備分方式各執行以周，並每日紀錄 RTO、RTO、級系統使用效能，觀察是否可有效提升備援機制。

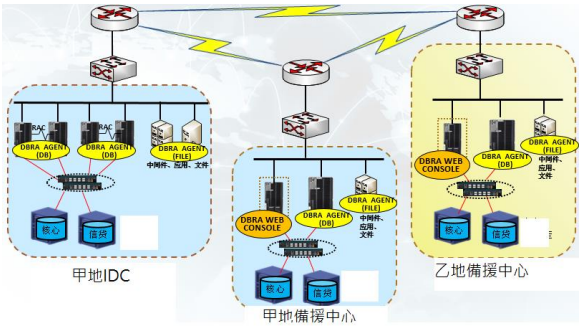

圖 7.實驗規劃圖

二、實驗研究假設

為實驗過程的假設，以利實驗的設計及進行，其研究假設共分為下列三項：

1.加入「複合式異地熱備援機制」有助於「系統完全復原所需時間」 (RTO)的縮短。

2.加入「複合式異地熱備援機制」有助於「系統需復原至過去的一個時間點」 (RPO)資料落差變小。

3.加入「複合式異地熱備援機制」有助於「備援切換程序」的減少。

三、資料處理

本研究直接針對有加入「複合式異地熱備援機制」(實驗組)與未加入「複合式異地熱備援機制」 (控制組)的測驗結果進行比較和分析，並注意實驗構面是否具有顯著差異。

四、實驗結果分析

經實驗結果分析，可以得知若執行複合式異地熱備援機制對於災難復原的高可用性確實有正面的影響，結論如下：

1. 加入「複合式異地熱備援機制」有助於「系統完全復原所需時間」 (RTO)的縮短。
2. 加入「複合式異地熱備援機制」有助於「系統需復原至過去的一個時間點」 (RPO)資料落差變小。
3. 加入「複合式異地熱備援機制」有助於「備援切換程序」的減少。
4. 加入「複合式異地熱備援機制」有助於降低系統負荷效能。

第四章、結論

國軍建置資訊備援中心，除了考量各項資訊安全問題外，如何維持各項戰演訓系統服務不中斷才是我們要達到的目標，本研究旨在規劃最合適的備援中心建置模式，提供未來建置國軍資訊備援中心的參考，保障資訊作業的完善。

參考文獻

[1]沈國輝。2009。雲端運算服務的應用在空軍資訊管理系統之初步研究。碩士論文。台北：國立臺灣科技大學資訊管理系。

[2]蕭火城。2014。國軍資訊管理導入「雲端運算」服務之風險評估分析。碩士論文。台北：國防大學資訊管理系。

[3]葉明宗。2012。銀行業資訊備援中心主機與模式規劃研究。碩士論文。彰化：國立彰化師範大學電機工程學系。

[4]姜俊成。2009。在儲域網路架構下異地備援之研究-以銀行業為例。碩士論文。台北：銘傳大學資訊管理學系碩士在職專班。

[5]許宏彬，異地備援及災害復原計劃 揭開異地備援九大架構，網路資訊雜誌，2002 年 5 月，119-121。

[6]金真芳。2005。金融機構異地備援中心建置模式之研究。碩士論文。台北：臺灣大學資訊管理學系。

[7]蔡登輝。2007。銀行資訊中心災害備援關鍵成功因素之研究。碩士論文。台北：世新大學資訊管理學研究所。

[8]王仁宏。2003。災害復原規劃之知識表達及推理法則研究。碩士論文。台北：國立中央大學資訊管理學系碩士在職專班。

[9]謝昆霖, & 呂易儒. 非營利單位資訊災難備援機制建置之研究.

[10]Baba, H., Watanabe, T., Nagaishi, M., & Matsumoto, H. (2014). Area Business Continuity Management, a New Opportunity for Building Economic Resilience.Procedia Economics and Finance, 18, 296-303.

[11]劉家誠。2012。 虛擬化環境之災難復原機制建置。 虎尾科技大學資訊管理研究所。

[12]蔡鎬宇。2014。金融信用卡服務系統異地備援決策因素之研究。碩士論文。台北：中國文化大學商學院資訊管理學系。

[13]陳俊賢。2006。BCP 企業永續運作計畫-災難復原計畫。來源網址: http://computer.ntsu.edu.tw/training/950714-1.pdf

[14] 數據中心解決方案-高可用技術白度書,華為3Com 技術有限公司,2003。

[15] Seven Tiers of Disaster Recovery,IBM Total Storage Solutions for Disaster Recovery,IBM，2004.

[16] 耿慧茹。2006。災難復原系統等級不同 對應備援等級亦大不同 。原文網址:http://www.digitimes.com.tw/tw/dt/n/shwnws.asp?id=0000036303_A2T7072SFN15RL827DJCG#ixzz3ppq8YG00。

[17] Friedl, W.J.,” The computer security framework,” IEEE 1990 International Carnahan Conference on Security Technology, 1990, 92 —99.