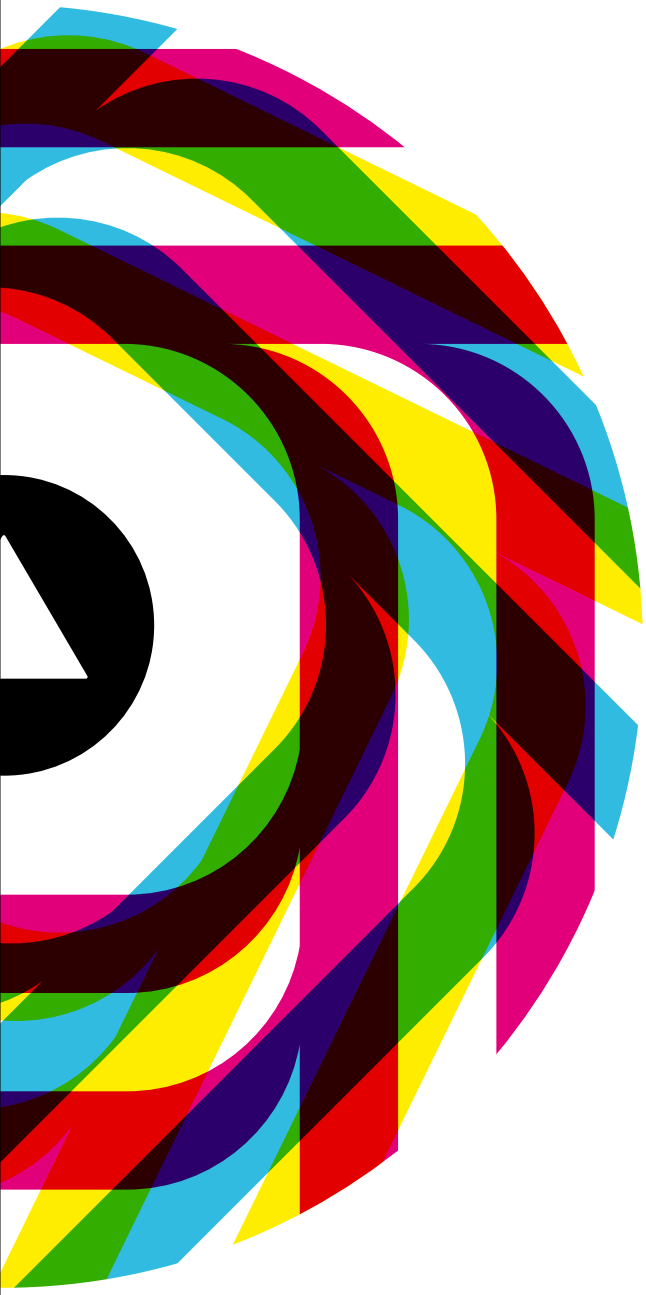


「贏」戰．個資法！

完整的IBM解決方案 協助企業贏在個資法之前

Part1：面對個資法衝擊，你必須先了解的12個關鍵問題

前言：個資法風暴來襲 …… 2

施行日期 個資法何時正式實施？ …… 3

準備時間 最快1年後面臨新法衝擊？ …… 3

規範對象 除了個人與企業，團體也受約束？ …… 3

個資定義 企業需要保護哪些個資？ …… 3

最低管轄數量 只要擁有1筆個資就得遵循新法？ …… 4

個人可行使權利 企業為滿足個人請求，勢必得改變流程？ …… 4

告知義務 個資蒐集或利用前須告知當事人？ …… 4

利用限制 利用個資須符合特定目的？ …… 5

有效同意 書面同意須用紙本，不能用電子文件？ …… 5

現有顧客資料 不是向顧客蒐集的個資，沒告知前無法使用？ …… 5

罰則 求償金額最高2億元，企業主最多5年刑責？ …… 6

企業舉證責任 企業必須自行舉證沒有違反個資法？ …… 6

IBM專家觀點 …… 7

Part2：IBM個資法錦囊妙計

個資法三大軸心 IBM推出完整解決方案 …… 10

錦囊妙計1 個資外洩風險評估處理與分析 …… 12

錦囊妙計2 強化資料運用與保護 …… 16

錦囊妙計3 建全節點資料存取及洩漏 …… 18

Part3：附錄

企業必知的個資法重點整理 最精簡扼要的個資法總整理 …… 20

個資法Q&A 29個問答集，掃除心中疑問 …… 22

個資法風暴來襲

今年4月27日立法院三讀通過了《個人資料保護法》（簡稱個資法），這個法案衝擊之大，遍及了臺灣123萬家企業和2,300萬民眾，無一倖免。

不論是一個人或一群人、中小企業或跨國企業、任何工作、任何活動，凡是需要蒐集、處理或利用到個人資訊的行為，包括紙本記錄和電腦資訊、甚至是隨手寫在便條紙上的聯絡資訊，若不留意，都有可能牴觸了個人資料保護法的規範。

對企業而言，個資法不僅會影響到未來企業蒐集顧客資料、利用個資行銷的作業方式，連企業現有的顧客資料都將受到影響，甚至在最嚴重的情況下，企業辛苦累積數十年的顧客名單將無法使用，企業可能面臨營運停擺的危機。

在新版個資法的規範下，一旦企業違法使用個資，顧客還能提出團體訴訟來求償，最高求償金額高達2億元。若因違法使用而對當事人產生損害時，老闆還得面臨五年以下的有期徒刑。這些都是個資法施行以後，企業立刻要面對的問題。

尤其是以往不受《電腦處理個人資料保護法》規範的企業，他們遭受的衝擊更大，例如，製造業者若無法符合新法規的要求，就不能使用往來廠商的聯絡資訊，這樣進一步就會影響到供應鏈系統的運作，生產線被迫停擺也是有可能的。

目前三讀通過的個資法只有基本條文，未來法務部還會擬定更詳細的施行細則，作為實際執行的參考依據。

這些細則更是直接影響企業處理個資的每一個決策，企業流程中有哪些個資需要保護？企業已經擁有的顧客資料要如何處理才能合法使用？如何降低告知當事人的費用？如何因應顧客要求刪除個資？等問題，甚至是法案何時實施，施行細則何時出爐，企業到底剩下多少時間可以準備？這些都是企業目前最關心的問題。

為此，我們特別採訪承辦個資法修法業務，也是推動施行細則草擬工作的法務部法律事務司科長黃荷婷，進一步了解個資法的實施時程和條文內容。

【本文係由「iThome電腦報週刊」雜誌授權刊載】

個人資料保護法案預估實施時程

1990年9月	法務部開始研擬電腦處理個人資料保護法
1992年6月	電腦處理個人資料保護法草案完成
1995年4月	法務部開始研擬施行細則
1995年7月12日	立法院三讀通過電腦處理個人資料保護法
1995年8月11日	總統公布電腦處理個人資料保護法
1995年8月13日	電腦處理個人資料保護法生效
1995年12月	電腦處理個人資料保護法施行細則草案呈行政院審議
1996年5月1日	電腦處理個人資料保護法施行細則發布施行
1997年~2010年3月	11次修法擴大非公務機關適用產業
2010年4月27日	立法院三讀通過個人資料保護法
2010年5月	總統公布個資法法案
2010年6月	●在北中南東部舉辦個資法公聽會，徵集各方對不確定法律概念的意見
	●總統公布後6～8個月，法務部完成個資法實施細則、特定目的與資料類型清單
	●細則草案報部後2～3個月 行政院審定施行細則
2011年5月	完成個資法施行細則作業流程
正式實施日	行政院公布施行細則，並指定法案正式實施日期
正式實施日+1年	法案施行一年內 企業完成舊有個資的告知作業

資料來源：法務部，iThome整理，2010年5月

施行日期 個資法何時正式實施？

就黃荷婷的估計，總統正式公布新法案後，法務部預估以6～8個月的時間訂定施行細則的草案，待草案呈報行政院後，行政院審核時間約需2～3個月，這些加起來，幾乎需要1年時間才能完成。目前法案已三讀通過，法務部立即展開擬定施行細則的相關作業。黃荷婷指出，施行細則將分成兩個部分進行。

第一部分，法務部在6月時開始舉辦，到臺灣北、中、南、東部舉辦公聽會，徵詢各界對法案中「不確定法律概念」的意見，這些概念包括了公共利益、公開場所、社交活動、家庭活動等。法務部會依據公聽會的意見，來訂定不確定法律概念的相關條文，再邀請專家學者組成工作小組，確認這些條文不會違反法律上應保障的利益，也不會侵犯司法權。

另一方面，法務部還會成立施行細則修法小組，由各部會派員參加，共同來訂定執行面的施行細則。遇到與地方事務有關的條文時，也會邀請相關的地方政府參加會議。施行細則還會包括特定目的清單和資料類型供企業選用。

準備時間 最快1年後面臨新法衝擊

透過多管齊下的作法，黃荷婷表示：「希望在總統公布後的1年內，完成個資法施行細則的作業流程，再由行政院決定施行日期。」倘若行政院比照《電腦處理個人資料保護法》施行細則的作法，在發布日時正式實施，以目前法務部的作業時程來看，行政院最快可以在1年後實施個資法，換句話說，企業最快1年後將面臨個資法的衝擊，因應時間從現在開始倒數大約只剩12個月。

規範對象 除了個人與企業，團體也受約束

更重要的是，新版個資法適用對象擴及各產業，不管是誰，1年後都需要面對個資法的衝擊。除了法人和自然人受個資法約束外，甚至包括各式各樣的團體都需要遵循個資法。黃荷婷解釋：「一般只要3人以上就可以稱為團體，或者是設有代表人的團體也是。」所以，舉凡任何個人、任何企業、任何形式規模的團體，哪怕是三五好友組成的私人讀書會，都在法條管轄範圍中。

個資定義 企業需要保護哪些個資？

新版個資法規範了企業必須保護的個人資料類型，包括了個人的姓名、出生年月日、身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動，以及其他可以直接或間接識別出個人的資料都屬於個資法的保護範圍。企業蒐集、處理和利用這些個資時，必須特別遵循個資法的規範。

不過，並非所有個人資料都可以識別出所對應的個人，這類無法識別的個資，就不屬於個資法的保護範圍。黃荷婷舉例說明，比如透過網路暱稱或網路代號不一定能識別出背後所代表的個人，或是部分數字模糊的身分證號也無法識別出對應的當事人。她進一步解釋：「如果有些類型的個人資料，一般人無法用一般方式查出對方是誰，這類資料就可以歸入無法識別的資料範圍，不受個資法的管轄。但是，如何判斷個人資料是否可以識別，未來將會由主管機關認定。在施行細則中也會盡量訂定出直接或間接識別的分辨標準。」

Part1：面對個資法衝擊，你必須先了解的12個關鍵問題

個資法不只衝擊企業，連老闆與員工都會受罰

新通過的《個人資料保護法》比過去法規更嚴厲，若違反個資法，不只企業面臨更高的罰則，連老闆和員工都會受罰，甚至要入獄服刑。

個資法新增加了團體訴訟求償的規定，受害當事人可集體向違反個資法的企業求償。每人每次可求償5佰～2萬元，相同原因產生的賠償金額合併計算，最高可以達到2億元，這個金額是舊有法規的10倍。

當企業違法使用個資造成當事人損失，除了賠償當事人以外，經手個資的員工也要面臨2年刑期或20萬元以下的罰金，若是故意違法利用個資來營利，刑期更是加重到5年以下有期徒刑，或併科罰金1百萬元。

平時，各行業的主管機關可以派員檢查企業是否符合個資法的規範，發現有違法情況，除了可以扣留違法使用的顧客資料外，主管機關還可以限期要求企業改善，若不改善則可以按次罰鍰，依違反情節不同，從2萬元到50萬元不等。如果企業老闆若沒有盡力避免違法情況發生，主管機關也會用同一額度罰鍰來處罰企業老闆。上至老闆、下至每一位員工，都必須清楚了解個資法的影響，才免於觸法的風險。

最低管轄數量 只要擁有1筆個資就得遵循新法

特別注意的是，臺灣個資法沒有最低資料筆數的限制，不像日本個資法只能管轄5千筆以上的資料。未來法案實施後，臺灣企業只要擁有1筆以上的顧客資料，企業就必須符合個資法的規範。而且也不只是儲存在企業伺服器中的數位資料需要守法，連書寫在任何紙本文件上的個人資料，不論形式或載體，企業所擁有的任何1筆個資都必須遵循個資法的規範。

個人可行使權利 企業為滿足個人請求，勢必得改變流程

在個資法中也明定了個人可以對自身資料可以行使的權利，包括了查詢、更正、要求停止蒐集、處理或利用，甚至是個人可以要求企業刪除等。企業為了滿足個人提出的請求，勢必得改變現有的個人資料作業流程。例如過去企業為了充分運用顧客資料，往往會盡可能保存，不會輕易刪除。

現在，企業必須回應顧客的請求，甚至得刪除資料庫中的顧客記錄。企業為了日後舉證確實執行顧客的請求，除了要記錄顧客提出的個資請求外，還得記錄執行請求的過程，各種與個資相關的作業流程都會受到影響，必須重新調整作法。不過，企業若是依據其他法律規定而蒐集或使用個資，例如財務資料依法必須保存7年，企業就有權拒絕使用者的刪除要求。「若有其他法律明文規定者，企業運用個資時，可不受個資法的限制。」黃荷婷說。

告知義務 個資蒐集或利用前須告知當事人

在使用行為的規範上，個資法從蒐集、處理和利用三大面向來要求個資法的合理使用範圍。當企業直接向顧客蒐集個人資料時，除了法定例外情況外，都必須盡到告知義務，企業必告知當事人，包括了蒐集目的、企業名稱、資料類別、資料利用期間、地區、方式、當事人權利，以及當事人不提供個資時，對其權益的影響等。如果企業委託第三方機構向顧客蒐集個資，委託機構所作所為視同企業，所以，企業利用這些委託機構蒐集的個資之前，也必須告知每一位當事人。

現今不少企業擁有的個人資料動輒數十萬、數百萬筆，若每一筆資料都需要告知當事人，多數企業擔心未來必須負擔龐大的告知費用。黃荷婷表示，法條中並未限制企業採取的告知方式。企業可以透過各種方式告知，電子郵件、簡訊、電話等方式，而且告知不需要對方回應，只要有記錄能事後舉證，證明企業確實有告知即可。除了告知方式不限外，「企業若曾對這些現有資料庫的顧客行銷，就不符合個資法第20條規定的首次行銷情況，企業不用再提供拒絕行銷的方式給顧客。」她補充。

利用限制 利用個資須符合特定目的

但是，黃荷婷也提醒，若是企業利用個資的目的，已經和當時蒐集的目的不同時，企業就必須符合蒐集要件的規定。除了不受限的情況下，個資法第5條規定，企業只能在特定目的範圍內，才能蒐集和使用個人資料。黃荷婷指出：「特定目的是個資法限制蒐集、限制利用的重要機制，也是主管機關監督管理的制度。」目前在《電腦處理個人資料保護法》中訂定了101項特定目的，黃荷婷表示，新法將由各產業主管機關和所屬產業共同提出需要的特定目的項目，再由法務部和主管機關共同公告。「最後訂定的特定目的數量不限，原則是讓每一個目的明確和清楚。企業可以同時告知多個目的，但不是全部的目的。」

有效同意 書面同意須用紙本，不能用電子文件

除了符合特定目的以外，企業蒐集或處理個資還要符合個資法第19條的蒐集要件。例如其中一個要件是企業必須取得顧客的書面同意，黃荷婷解釋：「法條中的書面同意是嚴格的紙本書面同意書的意思。不能使用電子文件或透過電子簽章的同意書，因為電子同意只符合同意的意思，但不是書面同意。」若不易取得書面同意，黃荷婷建議企業可以使用另外一項蒐集要件，也就是「契約或類似契約的關係」的要件。「這項要件不限形式，只要符合契約的法定規範，透過網頁同意按鈕的使用者條款也可以成立。」她說。

不過，企業從「一般可得來源，例如網際網路」蒐集來的個人資料，因為無法查證資料是否合法，個資法同樣將這類型為視為合法蒐集，但「企業若後來發現這些資料不合法，或者使用者要求企業禁用時，企業就必須刪除或停止使用。」黃荷婷說：「施行細則中會定義一般可得來源。」取得個人資料後，黃荷婷指出，只要企業利用資料的目的和當初蒐集資料的目的相同，企業就能在當初告知的特定目的範圍中利用。如果蒐集目的和使用目的不同時，企業必須重新取得當事人的書面同意，「即使是同一家公司裡的不同單位，只要目的不同，企業都要重新取得書面同意，除非符合其他例外條件，例如另有法律明文規定。」她說。

但對於個人自行公開的個資，或是其他合法公開的個人資料，企業就可以自行運用，不需要取得書面同意，也不用與當事人建立契約關係。但是，黃荷婷補充：「若是第三方公開的個人資料，企業必須確認這些公開資料的合法性後才能利用。」企業蒐集了個人資料後，如果是利用這些資料對新顧客進行第一次行銷時，還得提供顧客有拒絕行銷的方式。「即使已取得當事人同意，首次行銷時要提供拒絕行銷的機會，這是企業應盡的義務。」黃荷婷說。

現有顧客資料 不是向顧客蒐集的個資，沒告知前無法使用

個資法訂定了許多企業未來必須遵循的規定，但其中一條特別不同，個資法第54條特別溯及過往，規範了企業在法規實施前擁有的個人資料。企業如果是向當事人取得個資，而且使用上沒有超出當初告知的目的，就不用依據54條規定再次通知當事人。但企業若不是直接向當事人蒐集的個人資料，例如透過委託機構取得，企業必須在法案實施一年內告知當事人，在沒有告知當事人前，企業無法使用這些資料。

在個資法中也律定了企業其他告知義務，例如企業有維護個人資料正確性的義務，若資料有錯，企業必須告知曾經提供資料的對象，要求對方更新，例如子公司必須告知母公司資料有誤必須更新。若發生資料外洩事件，企業也要主動告知當事人。

罰則 求償金額最高2億元，企業主最多5年刑責

如果企業外洩個資，導致顧客遭受損害時，個資法也提供了權益受損顧客可以透過團體訴訟向企業求償。若無法估算損害金額時，每人每件可求償5佰～2萬元，相同原因造成的事件總求償金額最高2億元。蒙受損失的當事人若要進一步向違反個資法的企業求償，必須在違規事件發生後5年內向企業提出求償，而且當事人得知違規事件的消息後，必須在2年內提出求償，否則就會失去求償的權力。

企業若因違反個資造成他人損失時，相關人員也會面臨2年以下的有期徒刑、拘役或併科20萬元以下罰金。若是企業為了營利而違反個資法，相關人員刑期還會加重為5年以下有期徒刑、拘役或併科1百萬元罰金。

當事人也可以向各行業主管機關投訴企業違反個資法，主管機關會進一步派人稽查企業法規遵循的情形。若發現企業有違反個資法，限期改善無效後，主管機關會對企業處以行政罰鍰，依違法罰款從2萬～50萬元不等。若企業老闆不能證明自己盡力防止違法事情發生，也要接受同一額度的行政罰鍰。換句話說，企業被罰多少錢，老闆也會被罰多少錢。

企業舉證責任 企業必須自行舉證沒有違反個資法

在新版個資法中，企業必須證明自己確實符合法規要求。當企業進行各項遵循個資法的行動時，不論是各種告知義務、爭取當事人同意或回應個人請求等行為，都必須記錄，以作為未來事後舉證之用。黃荷婷表示：「個資法要求企業必須舉證說明自己沒有過失或故意違反法律。這可以讓企業更加重視隱私權和個人資料的保護。」

不過，在個資法大幅增加企業保護個資的義務以外，政府也同步規畫了協助企業的配套措施。針對個資法要求企業舉證的要求，經濟部商業司已經規畫了一個隱私權標章制度。這套隱私權標章制度提供了一套驗證機制，可以用來檢驗企業是否符合個資法的隱私權要求，符合者發放合格標章，而且驗證機構還會定期複查企業是否持續執行。驗證機構由各產業工會擔任，商業司則會另外訂定驗證機構的資格。黃荷婷說：「隱私權標章可以作為企業非故意或過失違反的舉證之一。」

新通過的個資法雖然只有56條，但是規範了所有人處理個人資料的方式，面對如此龐大的管轄範圍，黃荷婷坦言，個資法很難做到鉅細靡遺的要求，法務部會盡可能地透過施行細則完善各項個資規範。若實行細則還有不足，黃荷婷說：「考慮在施行細則中，授與各主管機關可以透過行政命令補充規範的權限，一來主管機關最了解產業實況，另一方面也能讓法規快速因應各種新科技衍生的個資問題。」未來，個資保護議題勢必成為企業必須長期關注的焦點，不但要了解個資法的法條和施行細則，還需要隨時掌握主管機關對於個資保護的最新要求。

(註1) 本12大關鍵問題係由「iThome/電週文化事業」授權刊載，原文刊載於「iThome電腦報週刊第451期」(http://www.ithome.com.tw/itadm/article.php?c=61306)。 轉載內容僅供一般訊息參考，IBM Taiwan在此並未提供任何個資法之法律意見或顧問諮詢；相關法規內容、解釋及適用，仍需請另諮詢法律專業人員之意見為準。

(註2) 個資法施行日期目前尚未經政府正式公告，「準備時間」仍需視政府相關法制作業時間為準。

(註3) 因違反個資法之行為態樣不一，仍請另諮詢法律專業人員可能之最高刑期。

IBM專家觀點：企業內個資洩漏的主要來源？

根據統計，個資洩漏事件，最主要可粗分為下列幾種事件來源：
- 筆記型電腦或個人電腦的遺失或被竊取
- 外部駭客攻陷Web應用程式或資料庫，抓取個資
- 惡意的高權限內部系統管理者或維護廠商
- 惡意的內部使用者

IBM軟體事業處 技術總監 林育震表示：「在這些管道中，75%是從伺服器所洩漏，尤其是存放大量個資的資料庫，成為駭客或惡意內部使用者鎖定的重要目標，其中惡意的內部使用者，不單只是離職員工，還有專門竊取資料的集團，派人故意應徵企業的資料管理員相關職務。對於這類惡意使用者，內部稽核與企業自行舉證能力便是十分重要的管理重點。」

Table 9. Detailed listing of compromised assets by percentage of breaches and records

Asset	Asset Group	% of Breaches	% of Records
POS system	Online Data	32%	6%
Database server	Online Data	30%	75%
Application server	Online Data	12%	19%
Web server	Online Data	10%	0.004%
File server	Online Data	8%	0.1%
Public kiosk server	Online Data	2%	0.4%
Authentication/ Directory server	Online Data	2%	0.1%
Backup tapes	Online Data	1%	0.04%
Documents	Online Data	1%	0.000%
Workstation	End-User System	8%	0.01%
Laptop	End-User System	4%	0.000%
PIN Entry Device	End-User System	2%	0.004%

Source: 2009 Data Breach Report from Verizon RISK Team

IBM專家觀點：除個人資料外，營業秘密亦是企業應考量的重點

IBM資訊科技服務事業處 資深架構師 饒康立表示：「由於每家企業都至少有雇員個資，所以遵循個資法、改變資料蒐集與使用的流程是必然的趨勢。個資洩漏之損失除實質貨幣付出外，亦含括無形商譽之影響，但是以整體企業觀點而言，企業營業秘密若是洩漏，將造成直接且立即性的營業損失，甚至傷害企業競爭力及市場優勢，所以在IBM對個資法的架構建議，將是一併納入個人資料與營業秘密的生命週期防護架構，一次完整做好防護，才是最節省成本的方式。」

行業別	營業秘密	個人資料
科技及製造業	製程流程與參數、設計資訊、未公開產品規格、軟體原始碼、營運及業務、財務、人事資訊	雇員個人資訊
金融行業	交易資訊、未公開營運資訊、業務、財務、人事資訊	雇員個人資訊、客戶個人資訊、信用卡或帳戶資訊
醫療行業	實驗數據、業務、財務、人事資訊	雇員個人資訊、病患個人資訊、病歷資訊、健康檢查資訊
教育行業	研究報告、業務、財務、人事資訊	教職員資訊、學生及家長個人資訊、學生學習紀錄
政府及軍事	軍事機密資訊、內部調查資料、未公開規劃、稅務資訊、情報資訊	國民、市民資訊、個人稅務及財務資訊
零售行業 網路及電視購物	交易資訊、未公開營運資訊、業務、財務、人事資訊	會員資訊、信用卡或帳戶資訊

IBM專家觀點：建構企業安全平臺 - 展現“無故意或過失責任”的免責

一般而言，企業面對個資法可採取的因應措施大致可分為兩大方向，包含「評估個資外洩的風險」及「建立符合需求的個人資料保護系統」。在評估個資外洩風險時，需瞭解個資外洩主要的可能管道：包含外部入侵、委外廠商洩漏、內控程序疏失，以及內部人員洩漏等，依照這些管道逐一建立防護措施。

而在建立符合規範的個人資料保護系統時，則要先了解個人資料處理的流程：

1.蒐集階段，要依法進行告知義務並取得書面同意。

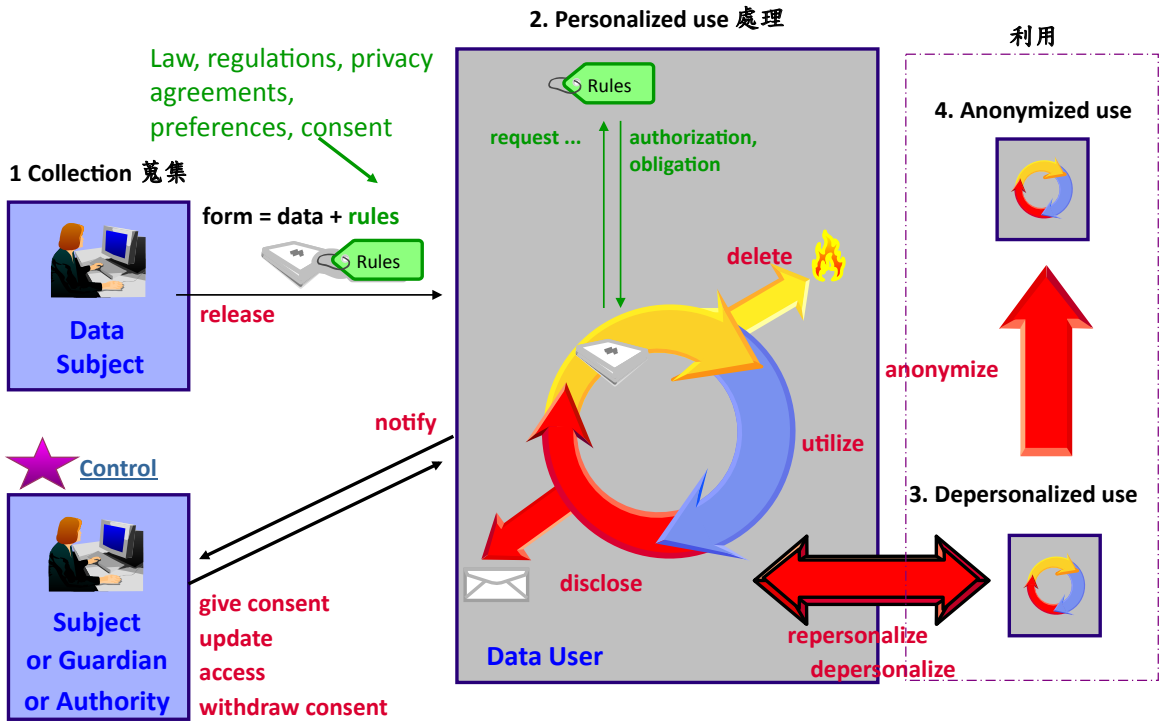
2.其次是保存，採取適當保護措施避免個人資料被竊取、竄改或毀損。

3.利用階段，客戶資料必須依蒐集時的特定目的範圍內才可使用（如果要在範圍外使用，必須另外取得書面同意）。

4.最後是銷毀，這也是最容易被企業忽略的階段，如果蒐集資料時的目的消失了，或期限屆滿，企業必須將資料完全銷毀。

個人資料/營業秘密之生命週期防護架構

IBM個人資料/營業祕密之生命週期防護架構，符合個資法蒐集、處理、利用銷毀三階段之完整規範：

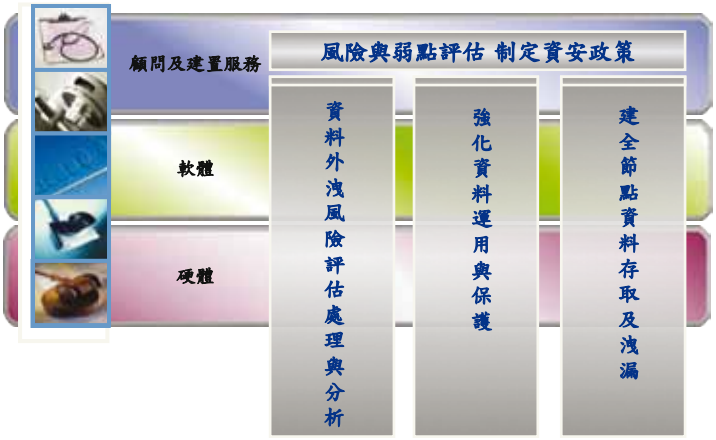


- 從「蒐集階段」運用適當的技術，保護隱私資料、避免外洩
- 在「處理階段」只有被授權之人員，系統才能處理/存取適當資料，本階段應全程受監控
- 在「後續利用階段」需去個人化才能做為測試、統計之運用

個資法三大軸心
IBM推出完整解決方案

新版個資法通過了，不但擴大適用範圍，涵蓋所有公民營企業，還加重刑責，讓企業原本視為寶貴資產的個資及相關資料，隨時可能翻轉成為引爆問題的負債！所以新法上路後，個資將會是企業的兩面刃，運用得當將是公司獲利的命脈，但是若未進行保護而外洩，將會危及企業的商譽及面臨鉅額的罰金。

因此，為迎戰個資法，IBM推出全方位資安解決方案，針對「資料外洩分析與處理」、「資料運用與保護」、「節點資料洩漏保管」等三大議題，從伺服器端、網路、乃至節點提供檢測分析與防禦，並搭配「風險與弱點評估制訂資安政策」顧問服務，協助企業盤點各環節，迎接嶄新的個資規範。



法規要求	個資軸心	IBM解決方案說明	IBM產品對應
個資法	· 風險與弱點評估制訂資安政策	· 個資文件與資料分類分析與保護政策的訂定 · 制定個人資料保護政策並進行隱私資料流分析	· 資訊分佈與系統風險評估顧問服務 · 資料運用與保護顧問服務
資料外洩需證明「無故意或過失責任」才能免責	· 資料外洩分析與處理	· 內部使用者行為稽核規劃與建置服務 · 資料庫稽核與防護系統規劃與建置服務 · 日誌集中管理及分析系統規劃與建置服務 · 身分辨認與授權管理規劃與建置服務	· 資料運用稽核建置服務 (Intellinx) · 資料運用稽核建置服務 & Guardium · 資料運用稽核建置服務 & Tivoli SIEM · 資料運用及保護建置服務 & Tivoli Identity Mgmt，Access Mgmt
應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏	· 資料運用與保護	· 入侵防禦弱點評估諮詢與設計服務 · 開發測試階段資料保護弱點評估諮詢與設計服務 · 網頁應用程式保護機制與開發規範暨安全性檢測服務 · 主動式入侵防禦及弱點保護系統規劃與建置服務 · XML/ WS防火牆規劃與建置服務	· 架構需求與規劃建置服務 & Tivoli ISS Enterprise Scanner · 架構需求與規劃建置服務& Optim · 架構需求與規劃建置服務 & Rational AppScan · 架構需求與規劃建置服務 & Tivoli ISS IDS/IPS · 架構需求與規劃建置服務 & WebSphere DataPower
	· 節點資料洩漏保管	· 端點設備資料外洩預防規劃與建置服務 · 資料加密規劃與建置服務 · 磁帶端點設備機加密與保管解決方案 · 雲端桌面資料保護解決方案	· 資料運用及保護建置服務 & Guardium · 資料運用及保護顧問服務 · IBM Tape Drive, Library · 桌面資料運用及保護建置服務 (Desktop Cloud)

錦囊妙計1 資料外洩風險評估處理與分析

做好資料外洩風險評估、處理與分析，是企業因應新版個資法的基礎措施。對此，IBM推出了兩大解決方案，協助您的企業杜絕資料外洩的風險：

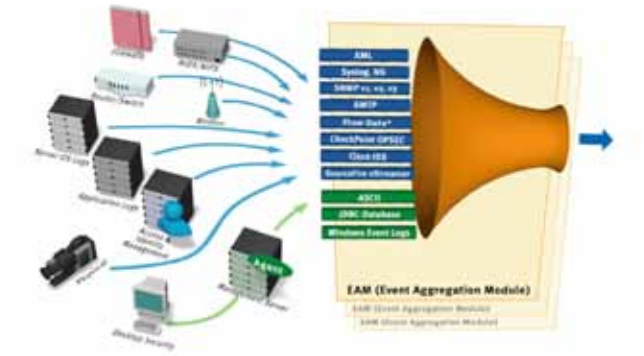
解決方案1 日誌集中管理及分析解決方案-完整提供端到端日誌管理

面對企業內部端到端日誌管理，您是否常常在思考下列的問題？

- 有沒有辦法從系統、應用程式、資料庫或網路層面的日誌進行追蹤？
- 是否有人對敏感資料進行了不當地使用或修改？（使用制度）
- 外包企業是否負責任地管理著系統和資料？（變化管理）
- 是否存在非法修改操作環境的情況？（變化管理）
- 如果有人新增使用者帳戶，我們能否收到警告？（帳戶管理）
- 是否定期記錄並審核系統管理員和系統操作人員的行為？
- 是否記錄下了所有的敏感資料存取活動-包括超級使用者／管理員和DBA的存取記錄？
- 是否對安全事故和可疑行為進行了分析和調查並採取了補救措施？
- 誰在未得到許可的情況下擅自終止了主要系統進程的運行？
- 管理員是否曾在系統中創建並批准創建特殊身份／特權？

針對上述問題，IBM推出「日誌集中管理及分析解決方案」能收集Desktop、Network Devices、Security Devices、Dainframe、OS...等的日誌，將安全事件關聯起來，產生各種合規報表，並隨時反映在儀表板上，隨時掌握各種狀況。

提供廣泛的安全事件及時收集



The IBM Tivoli SIEM Solution

即時反映資訊於儀表板上

解決方案2 資料庫稽核與防護解決方案-資料庫稽核

面對資料庫稽核與防護，您是否常常在思考下列的問題：

- 誰正在改變資料庫結構或刪除資料表?
- 何時有未授權的程式正在改變資料?
- DBAs或外包維護人員正在對資料庫作什麼事?
- 有多少未成功的系統登入發生?
- 誰正在擷取信用卡資料?
- 什麼資料正在被網路上的哪個節點所存取?
- 什麼資料正在被哪個應用程式所存取?
- 這些資料是如何被取得的?
- 這些日子來資料被取得的行為模式有哪些?
- 資料庫產生了什麼錯誤訊息?
- 敏感性物件的暴露風險是什麼?
- 何時有人發動了資料隱碼攻擊?

IBM的資料庫稽核與防護解決方案具備詳盡的稽核內容與安全項目，且能在不影響資料庫系統的效能之下找出是哪個終端使用者用什麼方式存取資料庫的什麼內容，並與解決方案1「端到端的日誌管理」互相結合提供完整訊息。

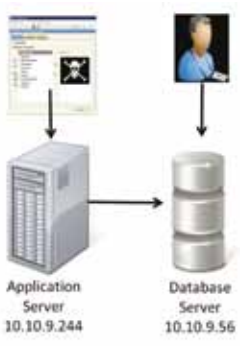
本解決方案特點：

- 非侵入性：Guardium可持續即時監控所有資料庫行動，但不需改變資料庫或應用程式配置，也幾乎不會影響效能表現。
- DBMS獨立性，支援多種資料庫及應用系統。
- 可達到細緻精密的策略與監控如：Who，what，when，how。
- 在評估階段找出資料庫弱點，在運行階段提供即時警示及阻絕。
- 可提供全面的活動監控：包含遠端及本機的存取。
- 職權分立：審核資料儲存於多個不同的實體或虛擬裝置中，內部人員或是駭客無法藉由篡改審核日誌資料來遮掩不法情事。這種作法不需仰賴原生的審核日誌（常駐於DBMS中），因此不需擔心被管理員輕易改動，便能確定職權分立。

此資料庫稽核解決方案亦可做到使用者行為分析，舉例來說：

案例1：

您知道組織內有哪些資料庫？有哪些使用者ID及應用系統ID被授權存取哪些資料庫？透過本方案您可以了解有哪些應用系統會存取哪些資料庫，而除了應用系統的ID外還有哪些人員的ID，所有訊息一目了然。



▲想了解更多？快撥0800-016-888按1查詢。

案例2：

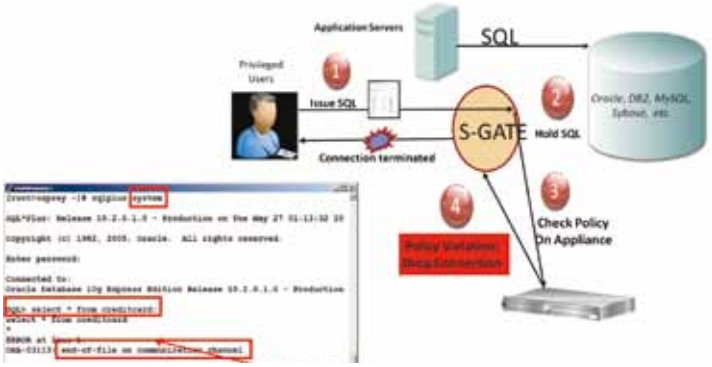
從下列分析報表中，清楚列出每位客服人員存取客戶資料的記錄，所有統計資料一目了然。但為什麼有客服人員能在一分鐘內處理99個客戶的資料？是否有資料外洩的嫌疑？但是當我們去稽核當事人做了甚麼事時，卻看到了不須要看的個資訊息。Guardium可以幫我們找出不適當的行為，也可以在稽核報表中保護隱私。

DB User Name	Sql	Records
STEVE	select * from ar.creditcard where i>? and i<?	4
HARRY	select * from ar.creditcard where i<?	4
JOE	select * from ar.creditcard where i<?	99

一般日誌管理並不會記錄資料庫的（讀取）行為，但這可能就是造成資料外洩的主因，透過IBM資料庫稽核解決方案（Guardium），讓資料庫使用狀況一目了然並可做使用者行為分析，避免資料庫（讀取）的稽核漏洞。

案例3：

透過本資料庫稽核與防護方案也能作及時阻斷：就算有授權的管理者在存取資料庫前，也必須先經過Guardium上制定的資安與隱私規則所核可，惡意的行為就會被拒絕。如此一來，也能確保資料庫管理者無資料外洩的嫌疑。

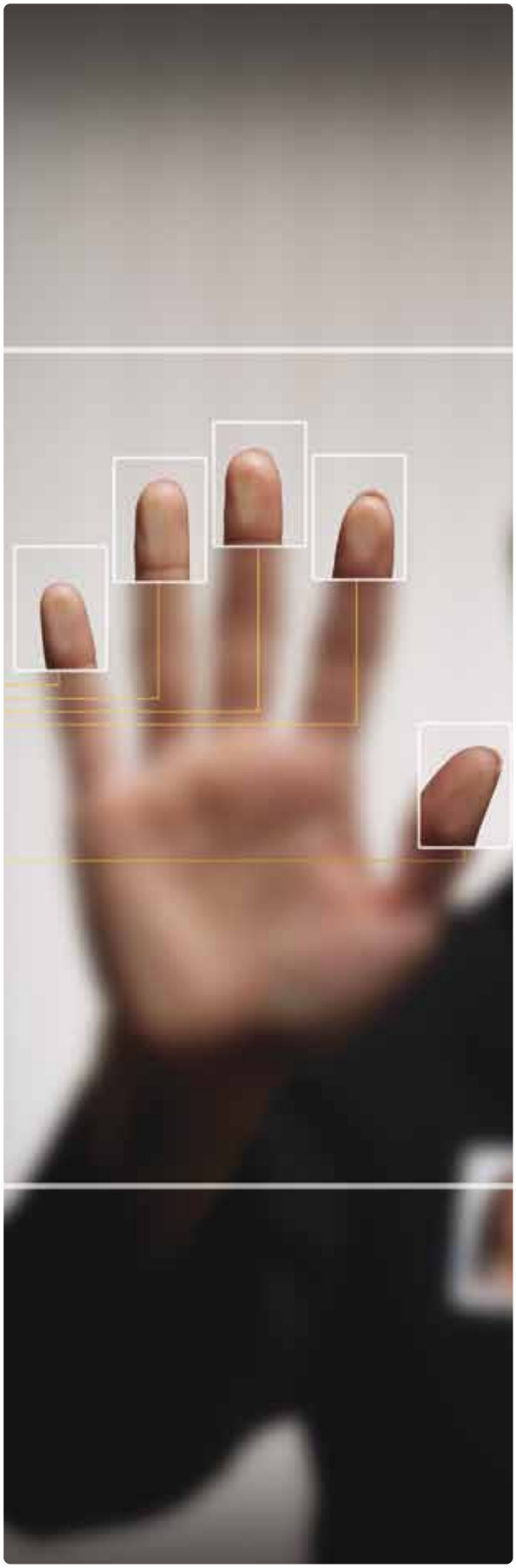


案例4：

有兩個應用系統的ID同時存取某資料庫，但從Guardium偵測出其中一個ID是在使用者工作站上執行，而非在正式的應用系統伺服器上，可懷疑是否有人假冒應用系統的ID來存取伺服器資料。

雖然是授權可以存取資料庫的應用系統ID，但是為什麼是由非此伺服器所在的IP發出的呢？趕緊發出警示通知吧！

Guardium也很容易用勾選的方式來設定要稽核的內容與項目。



▲想了解更多？快撥0800-016-888按1查詢。

錦囊妙計2 強化資料運用與保護

由於新版個資法加重企業保管個資的責任，IBM認為企業應採取更全面的資安防護機制、工具與政策保護資料安全。但是IT系統畢竟協助企業的工具，高階主管對於資安的共識、公司管理資料的流程、對員工進行管理政策的宣導，都必須全面性的規劃及考慮，所以在選擇系統之前，應先評估弱點與風險、建立制度，最後才是導入合適的IT系統。

IBM推出「資料運用與保護解決方案」，主要針對所涉及資料之蒐集、處理及利用等資料運用流程，提出網路資料傳輸入侵防護及資料外洩保管及相關流程整合解決方案。IBM並非僅提供產品，而是整體的解決方案，在顧問諮詢診斷的過程中，逐步改善企業管理流程、整體檢閱資料散佈情形、建立資料的資產管理機制、評估各項資料的外洩風險，並依據風險高低後，再運用「機制、工具或監控」等方式達到管理目標。

在強化與保護資料的「機制、工具或監控」方面，IBM已有許多成熟的方案可讓企業依需求選擇：

解決方案1 入侵防禦弱點評估諮詢與設計服務以及主動式入侵防禦及弱點保護系統規劃與建置服務：

IBM推出IBM ISS Proventia ESP（Enterprise Security Platform）企業安全平台，是綜合IBM4個關鍵環節+2類安全服務+1個統一安全管理平臺，可輕鬆實現前瞻動態威脅保護。」

IBM ISS Proventia ESP（Enterprise Security Platform）

傳統的入侵預防系統與防火牆技術已不足因應駭客攻擊，企業需以融合整合式網絡、伺服器保護技術，在IBM ISS網路安全防護方案的策略架構，結合網路入侵防禦設備及掃描工具、主機防護系統並整合稽核及中控系統功能，才能克服這些不斷演變的安全挑戰。

IBM ISS Proventia ESP（Enterprise Security Platform）企業安全平台，提供下列核心價值：

- 有效偵測已知、未知攻擊行為，發現攻擊立即阻擋
- 偵測 3,000+ 入侵攻擊
- 支援「 X-Force 虛擬補丁(Virtual Patch)」：使用者不必馬上更新系統的 Patch，即可在攻擊發生前完成防禦措施
- 「虛擬 IPS」功能：依客戶環境同時支援超過「1,500」組以上監控防護政策
- 高彈性佈署：線上模式、模擬模式、與監控模式
- 支援HA 與By Pass模組，保障客戶「服務」不中斷

資訊小百科：

IBM ISS X-Force®研發團隊，全球前瞻漏洞管理、威脅管理領域的領導者：

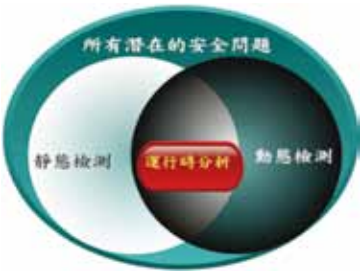
IBM ISS核心價值-Virtual Patch虛擬補丁：Virtual Patch為面臨最新漏洞威脅的企業提供了充分的時間緩衝，在系統和應用廠商就新漏洞提供補丁和更新之前，防止漏洞被利用，同時也可避免補丁與業務應用衝突的風險，確保企業的安全。

為什麼能夠實現前瞻性保護？（Proactive Protection）：由於IBM ISS首先發現的高危漏洞最多，同時，和系統廠商保持了雙贏的合作關係，所以有能力在漏洞被發現的第一時間提供針對漏洞本身的防護，而非提供針對攻擊的防護。因此，無論攻擊手法和利用程式如何變化，ISS提供針對高危漏洞的前瞻防護。

解決方案2 網頁應用程式保護機制與開發規範暨安全性檢測服務：

Rational AppScan為Web應用程式安全性檢測軟體的先驅，市佔率世界第一。協助您擁有全面的應用程式安全管理平台，能為軟體開發過程各階段增添應用掃描與安全診斷功能，提供下列核心價值：

- 是一套自動化弱點掃描工具，用來檢測Web應用系統的安全性，找出系統的資安漏洞，並一一提供詳盡的處理建議。
- 可簡化發現與修復Web應用系統安全性問題的工作，降低維護資訊安全的成本。
- 是當今唯一同時具備系統安全動態檢測（黑箱測試）和程式碼安全分析檢測（白箱測試）技術的公司。
- 黑箱測試工具由於直接模擬駭客的攻擊，是應用程式安全的基礎設施，應優先考慮。



資訊小百科：

黑箱測試：模擬各種駭客攻擊的手法，以無害的方式去使用運行中的Web應用系統，判斷系統是否存在各種安全性問題，並按照問題輕重緩急順序，提供可立即處理問題的建議做法。

白箱測試（Source Edition）：分析提供的原始碼，判斷系統是否存在各種安全性問題，指出有安全問題的原始碼位置，並按照問題的輕重緩急順序，提供可立即處理問題的建議做法

解決方案3 開發測試階段資料保護弱點評估諮詢與設計服務：

IBM Optim - Data Privacy對企業資料架構中隱私資料的控制點（Control Point），提供一個簡單、可擴展、易於整合的隱私資料保護解決方案；打造出可信賴的架構環境，讓企業能以充分反映資訊價值及保障用戶隱私的方式，安心地把資訊資產用於業務最佳化。

針對隱私資料保護 - IBM Optim提供了自動化的資料轉換、變形能力，能夠輕鬆地跨越多個資料庫將企業中涉及的各種個人資訊或保密資訊實施脫密、漂白處理，對不同資料格式亦提供不同遮蔽機制，能夠輕鬆地執行身份刪除（De-Identification）、去個人化（Depersonalize）、匿名化（Anonymize）及身份遮蔽（Masking）並同時保持資料完整性。不但幫助企業實現法規遵循，還能夠為測試或應用外包等作業提供無損企業利益的脫密資料版本，實現企業隱私資料的有效保護。

Optim 還可以提供各種各樣的資料遮罩技術，保護專用資訊的機密性。

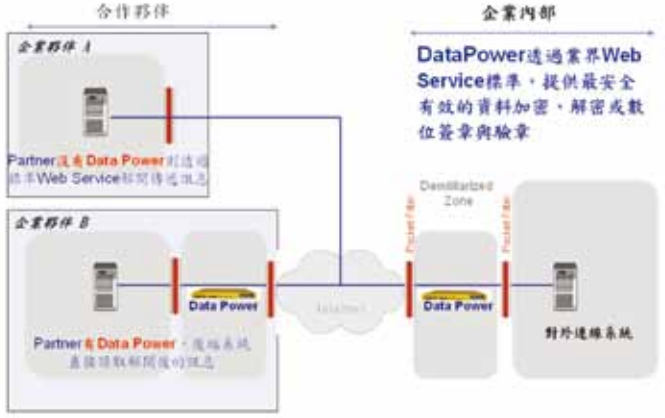
解決方案4 XML / WS防火牆規劃與建置服務：

在XML/Web Service應用中，WebSphere DataPower SOA Appliances可保護應用程式不受未經授權存取與惡意訊息的侵害，提供完整的安全資料交換機制。

Data Power SOA設備是業界第一個提供XML/WS 防火牆硬體解決方案的市場領導者，提供下列核心價值：

- Web服務安全支援與存取控制：支援SAML及WS-Security可控制內外部用戶端對 Web 服務應用程式的存取權並且能整合LDAP以達到授權認證之功能。
- XML Denial of Service（XDoS）保護：能防止惡意使用者及型態異常資料破壞企業的應用程式伺服器或營運。如Single-message XDoS與Multi-message XDoS惡意攻擊。
- XML訊息加密與解密Encryption/Decryption：可執行各種基本的XML加密、解密、數位簽章，即可將整個XML訊息或只將文件內某一個XML欄位加密/解密及簽章/驗證。
- XML/SOAP防火牆功能：支援過濾XML及SOAP資料流量，可防止惡意使用者及型態異常資料破壞企業的應用程式伺服器或營運。

IBM提供全面向，由顧問服務至產品導入之完整資料保護服務，由IBM資訊安全專家帶領整個專案之完善進行，並確保專案內由前期顧問服務與規劃至產品佈建之知識完整轉移，協助客戶掌握資安全貌與應變重點，有效抵禦個資法衝擊且完備資安防護。



▲想了解更多？快撥0800-016-888按1查詢。

錦囊妙計3 建全節點資料存取及洩漏

在強化資料運用及保護後，是否仍出現紀錄個資或重要營業秘密之資訊設備遺失、失竊、未完全清除等情況，甚至擔心外部維護廠商或內部員工取核心系統，難以保證個資或重要營業秘密不會由此途徑洩漏。

其實資料的流向是可以掌握的，從內部到外部、從外部到內部，以及內部間的傳遞，只要掌握住每一個節點資料，便可以建立資料加密、監控及導入管理機制。如此，企業便可以稽核使用者於節點上之資料使用行為、限制員工誤觸資料保護政策，並記錄重要個資或營運秘密的設備或移動媒體，在沒有經過適當的認證及授權前，他人無法讀取內部的資訊。

故為了健全節點資料存取，IBM提出三個節點資料保護技術的核心策略，可有效防制個資及營業機密洩漏。

策略1 利用雲端桌面技術，讓使用者無法直接觸碰資料

過去談論企業建立雲端技術的好處，通常是透過集中化、虛擬化的過程，減少實體設備的數量，進而節省電力、減少維護成本並透過自動化大幅提昇效率。但當採用雲端桌面進行桌面環境虛擬化並集中化，強制使用者端點不儲存機敏資料，僅允許螢幕影像傳輸而非實際資料檔案傳輸。此機制可直接避免機敏資料經由使用者惡意或無意的洩漏，亦能保護節點設備遺失時造成的機敏資料洩漏損失。而藉由集中控管的方式亦可統籌管理並強化使用者的桌面環境，減低資料漏失的風險。而雲端桌面技術於強化資料保護的同時，也提供了企業於管理面上的強化以及節能的好處。

策略2 於使用者設備進行機敏資料之使用稽核、政策管控、與加密保護

第二個策略，便是針對使用者端點的設備進行保護，除了個人電腦外，可移動的隨身碟、可燒錄的光碟，甚至每一顆硬碟都需要稽核、管控，並有加密保護措施，以降低設備遺失或是員工攜出這些可移動儲存裝置，所導致的資料外洩風險。

在此策略中，資料外洩防護（Data Loss Prevention , DLP）是十分重要的解決方案。DLP資料外洩防護是在2005年時所提出的概念，因為當時企業資料遺失風波不斷，而規劃出的資訊管理系統，初期以閘道器為主要架構進行閘道端機密資料掃描、過濾及攔截管理，目前防禦架構已經擴及文件政策、機密分級、行動裝置管理等資安項目，可追蹤控制對資料之存取行為，主動阻擋非授權行為，保留完整之資料使用過程。

所以隨著個人資料保護法即將通過，IBM已將個人資料提升為機密等級，進行監控、管理與防護，尤其是金融業、保險業、電子商務等握有大量個資的企業，或是針對內部人事系統進行員工資料保護。

策略3 於中心儲存媒體端進行資料加密，避免遺失或被竊取之風險

運用雲端技術並針對使用者設備進行防護後，也必須針對資料中心進行強化的管理，畢竟資料中心的儲存媒體，含硬碟與磁帶，仍為移動性媒體，可能在移動或儲存過程中遺失，或於廢棄時未完全將資料移除。

所以藉由IBM獨家的加密技術，於中心儲存媒體端進行資料加密，保護紀錄企業最核心個資或營運資訊的媒體，即使於運送或棄置時遺失或被竊取，仍可確保機敏資料不會被讀取。

IBM針對「資料外洩分析與處理」、「資料運用與保護」、「節點資料洩漏保管」所規劃的全方位資安解決方案，有利企業盤點資料流、保護資安弱點的各個環節，建立制度加上工具防禦，迎接嶄新的個資規範。

策略2圖說：

資料保護需求	雲端桌面保護機制	端點設備資料保護機制
可稽核節點上之資料使用行為	支援	強大
可限制節點上之資料保護政策違反行為	強大	強大
記錄或限制重要個資或營運秘密的設備或移動媒體的授權、認證、讀取等行為	強大	強大
適合對象	適合各種企業，尤其是主要位於LAN網路內之員工	適合各種企業，尤其是在外之主管與業務
不適合對象	長期在外之主管與業務	無
方案最重要風險	端點架構改變、如何滿足不同員工之資訊使用需求	於同一端點上佈建多個方案之衝突與管理問題
其他優點	強大的端點管理、節能	無

▲想了解更多？快撥0800-016-888按1查詢。

企業必知的個資法重點

個人資料保護法規範對象包括了公務機關、自然人、法人和其他團體。其中只有部分條文與企業有關，我們從這些條文中彙整出14項企業必知的個資法重點，這些都是企業因應個資法時必須了解的法條內容。

規範行為

蒐集、處理及利用個資。

個資定義

包括個人的姓名、出生年月日、身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動，以及其他可以直接或間接識別出個人的資料，不論紙本或數位形式，都屬於個資法的保護範圍。

個人權利

個人可向企業請求查詢、閱覽、提供複製副本、更正或補充、停止蒐集、停止處理或利用、請求刪除。個人請求後，企業需於時限內回覆。

規範對象

公務機關、自然人、企業法人、其他團體（3人以上即可視為團體）。代理蒐集機關則視同委託者。

主管機關

由目的事業主管機關管轄，而非事件發生地主管機關。多個主管機關或管轄者不明則透過協調聯繫機制決定。

告知責任

- 蒐集個資時應向當事人告知企業名稱、蒐集目的、資料類別、當事人權利、利用時間、地區、對象與方式、不告知的影響等。
- 使用目的改變時，企業應告知當事人。
- 非向當事人蒐集的現有顧客資料庫，必須在法案施行1年內告知。
- 個資異動後，應告知提供過個資的對象。
- 發生個資外洩情事後，應告知當事人。
- 告知形式不拘，有記錄可供事後舉證即可。

免告知情況

- 法律明文規定／依法執行公務。
- 告知將妨礙第三人重大利益。
- 當事人明知這些應告知內容。
- 當事人自行公開或其他合法公開內容。
- 無法告知當事人或法定代理人。
- 學術研究之必要，且無法識別之個資。
- 大眾傳播業為公共利益而蒐集。

可蒐集或處理的條件

必要條件：

- 應有特定目的，且只能在該目的範圍內利用。
- 不得蒐集醫療、基因、性生活與犯罪前科的個資。

多擇一條件：

- 法律明文規定。
- 與當事人有契約關係，契約形式不限，可用電子契約。
- 當事人自行公開或其他合法公開，企業需確認合法性。
- 當事人書面同意。
- 取自一般可得來源（如搜尋引擎）。
- 公共利益相關。
- 學術研究之必要，且無法識別之個資。

書面同意

意指紙本同意書，不能透過電子文件或電子簽章取得同意。

不適用個資法狀況

- 無法識別該個人的個資。
- 個人為了個人或家庭活動的蒐集、處理或利用。
- 公開場所或公開活動中的影片、圖像與聲音資料（未與其他個資結合）。

【本文係由「iThome電腦報週刊」雜誌授權刊載】

損害賠償

當事人可向違反個資法的企業求償，每人每次5佰～2萬元，相同原因合計最高求償金額2億元。

罰則

- 違法蒐集、處理或利用個資而產生損害時，處2年以下有期徒刑、拘役或併科20萬元以下罰金。
- 違法蒐集、處理或利用個資，意圖營利者處5年以下有期徒刑、拘役或併科100萬元以下罰金。

行政罰鍰

- 違反蒐集、處理與利用相關法規，限期未改善，每次可罰5～50萬元。
- 違反告知義務、維護義務、個人請求相關法規，限期未改善，每次可罰2～20萬元。
- 拒絕主管機關檢查者，每次可罰2～20萬元。
- 企業代表人未盡力防止發生上述違反事項，處相同額度之罰款。

企業現有個資（顧客與員工）處理原則

- 企業非直接向當事人蒐集的個人資料，必須在法案實施後一年內告知當事人，未告知前不能處理或利用。
- 現有行銷資料庫可視為非首次行銷的個資，不用提供拒絕行銷的管道。

【本文係由「iThome電腦報週刊」雜誌授權刊載】

個資法 Q&A

Q1.個資法什麼時候實施？

立法院於4月27日三讀通過個資法後，法務部會先用6～8個月完成施行細則，再呈報給行政院審核，審核時間約1～2個月。法務部預估在總統公布後1年內，完成施行細則的作業流程，再由行政院決定正式實施時間。

Q2.個資法管轄哪些行為？

個資法管轄個人資料的蒐集、處理和利用行為。

Q3.個資法保護哪些個人資料？

新版個資法規範了企業必須保護的個人資料類型，包括了個人的姓名、出生年月日、身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動，以及其他可以直接或間接識別出個人的資料都屬於個資法的保護範圍。

Q4.是不是只有5千筆以上的個資才會適用個資法？

不是，只要有1筆個資就會受到個資法規範。5千筆限制只是法案討論過程中，參考日本個資法的說法，後來未採納。

Q5.個資法是不是不管紙本上的個人資料？

不是，不論是電腦中的數位資料，或者是寫在紙張上的個人資料，全都適用個資法。

Q6.網路暱稱或Email屬於個資法規範的個人資料嗎？

由於網路暱稱不易識別出其代表的個人，所以，不會受到個資法規範。至於Email則有可能識別出個人，法務部會請主管機關NCC提供認定標準。

Q7.如果個人資料中部分內容模糊，例如身分證號中有4個數字模糊，是否還會受到個資法規範？

這類部分模糊的個人資料，由於一般人無法輕易識別，等同失去識別力，因此，這類資料就不適用個資法。但若和其他個資搭配後具有識別力，仍舊需要受到個資法規範。

Q8.是不是只有企業才需要遵守個資法？

不是，不論是自然人（也就是一般人），法人（企業）或其他團體都需要遵守個資法的規範。

Q9.其他團體如何定義？

任何3個人以上所組成的團體，或者團體可以有一位代表人或主席，就是一個團體。不論哪一種團體都要遵守個資法。換句話說，你和三五好友組成一個球隊，球隊所蒐集的個人保險資料、通訊資料，都要遵守個資法的規範。

Q10.在國外蒐集個資是否要遵守個資法？

不論在國內外，只要對中華民國的國民蒐集、處理或利用個資，都適用個資法。

Q11.個資法保障了哪些個人的個資權利？

每一個人對於他的個人資料可以請求閱覽或查詢、請求提供複製本、請求更正或補充、請求停止蒐集、停止處理或利用，最後還可以請求刪除。

Q12.企業是否可以拒絕個人提出的個資處理請求？

只有在三種情況下，企業可拒絕個人的請求，包括妨害國家重大利益、妨害公務機關執行法定職務、妨害蒐集機關或第三人重大利益時等。

Q13.企業必須多快回應個人提出的個資處理請求？

對於個人要求查詢、瀏覽或複製的請求，企業必須在15天內決定是否同意，若要拒絕得書面說明理由，最多可再延長15天。若是請求補充或更正，則可在30天內答覆，最多再延長30天。

Q14.若個人要求企業刪除個人資料，但另有法律規定要求企業保存，企業該如何處理？

若有其他法律規定，就可以拒絕個人的刪除請求。個資法規定，企業可依其他法律的規定或法定義務來蒐集、處理和利用個資。

Q15.個資法的主管機關為何？

每個行業的目的事業主管機關就是個資法主管機關，或者說，企業向哪個機關登記註冊，該機關就是個資法主管機關。若牽涉到多個主管機關或者主管機關不清楚時，則透過公務機關的協調聯繫機制決定如何共同執行或由誰主管監督，若無法決定則交由行政院決定。

Q16.企業可以任意自定蒐集或處理資料的目的嗎？

不行，法務部將會和各事業目的主管機關訂定新的特定目的項目，企業必須從中選擇其中一項或多項作為資料蒐集目的，就像是現行《電腦處理個人資料保護法》所訂定的101項特定目的。企業蒐集個資時不能踰越所選定的特定目的範圍，才能算是合法蒐集。

Q17.若有當事人投訴企業侵犯個資時，企業是否需要舉證，證明自己確實遵守個資法的規範？

是的，在個資法中規定由企業負擔舉證的責任，若有當事人投訴企業侵犯個資，企業必須證明自己盡到保護個人資料的義務，才能免責。

Q18.當事人合法公開在網路上的資料是否可以蒐集？

凡是當事人合法公開，或者是其他合法管道公開的資料，企業就能蒐集利用，但是企業必須確認這些資料來源的合法性。

Q19.個資法要求企業直接對當事人蒐集個資前，要先告知當事人，企業可以透過哪些方式告知？

告知形式不拘，電話通知、簡訊、電子郵件、書面通知等都可以，最重要的是，企業得保留記錄，事後才可以舉證已經盡到告知義務，通知方式則沒有限制。

Q20.直接對當事人蒐集個資時，有哪些情況不用告知？

對當事人蒐集個資時，下列情況就免告知，包括依法規定免告知、執行法定職務或法定義務時、告知時將妨礙公務、妨礙第三人重大利益，或者是當事人明確知道這些應告知的內容。最後一項例如當事人提供個資給仲介業者時，當事人已經知道房仲業者會將這些資料拿來建檔，作為提供房屋資訊的聯繫之用，此時房仲業者就不用再告知。

Q21.如果企業不是直接向當事人蒐集個資，仍舊需要告知當事人嗎？

即便不是向當事人蒐集個人資料，企業仍然要告知當事人，只有部分情況下才免告知。

Q22.什麼情況下企業取得個資時，不用告知當事人？

不用告知的情況例如法律規定免告知、執行法定職務或法定義務、告知將妨害第三人重大利益、當事人明知應告知內容、當事人自行公開、來自其他合法公開的個資、不能向當事人或法定代理人告知、為了公共利益或學術研究而資料經過處理無法識別個人時、或者是大眾傳播業者為了公共利益的蒐集時，這些情況就免告知當事人。

Q23.書面同意可以透過電子文件方式進行嗎？

不行，法條中的書面同意是指必須取得當事人的紙本同意書，透過電子文件或者是透過電子簽章取得的同意書，則不符合個資法的書面同意。

Q24.企業現有個人資料是否需要遵守個資法？

企業在個資法施行前蒐集的個人資料庫，若非由當事人提供，就必須在個資法實施後1年內告知當事人，讓對方知道企業擁有他的個人資料。告知後才能繼續利用他的個人資料。

Q25.企業對現有顧客行銷時，需要提供拒絕管道嗎？

由於企業現有的行銷資料庫已經不是首次行銷，所以，不用提供拒絕接受行銷的方式。

Q26.若發生個資損害時，當事人求償的時效多久？

當事人必須在事件發生5年內提出求償，或者當事人知道損害事件後，在2年內要提出，超過時間就不能再請求賠償。

Q27.發生個資損害時，賠償金額有多少？

若損害金額不易估算時，每人每一件可賠償5佰～2萬元，最高2億元賠償。涉及利益超過2億時，就按實際利益計算。

Q28.個資法會處罰企業老闆嗎？

企業違反個資法第46、47和48條的行政罰鍰時，如果老闆無法證明自己努力盡到防止義務，就會被處以相同額度的罰鍰。行政罰鍰從2萬～50萬元不等。

Q29.企業違反個資法時，老闆會被判刑嗎？

若企業違反個資法而導致顧客損失時，企業主必須面對最高2年以下的有期徒刑。若老闆為了營利而違反個資法時，刑期還會加重到最高5年以下有期徒刑。

【本文係由「iThome電腦報週刊」雜誌授權刊載】

台灣國際商業機器股份有限公司 台北市110松仁路7號3樓
IBM市場行銷處 0800-016-888按1 www.ibm.com/tw

© Copyright IBM Corporation 2010. 本公司保留所有版權。IBM and the IBM logo are registered trademarks of International Business Machines Corporation in the United States and / or other countries.

TW0AT01D