資料標記化：遮蔽資料的新方法

用標記化技術來取代敏感資料，為企業提供了眾多安全性與符合規範上的優勢。

文／ Yash Mehta　譯／曾祥信

企業需要健全的資料安全策略，將使用的資料匿名化，並預防潛在的資料安全漏洞。資料標記化（data tokenization）是一種新的資料安全策略，它意謂著企業可在完全符合資料規範的條件下，有效率且安全地運用手上的資料。資料標記化已發展成為中小企業間受歡迎的方法，讓他們在提升信用卡與電子商務交易安全性的同時，還能降低在符合產業標準與政府法規上所需要的成本和複雜度。

標記化（tokenization）指的是，將敏感資料與獨一無二的識別符號進行交換的過程，它能維持所有資料當中必要的資訊，同時不讓安全曝露於風險之中。標記化會以和資料相同的格式，產生完全隨機的字元，用來取代真實資料內容。

有效運用資料標記化

標記化用獨特的識別資料來遮蔽或取代敏感資料，並同時保留所有必要的資訊。這種對等且獨特的取代資料，就稱為標記（token）。標記化是一種非破壞式的資料遮蔽形式，透過獨特的取代資料，即標記，可還原出原始的資料。透過資料標記化來實現資料加密的主要方法有兩種：

- Vault-based 標記化。
- Vault-less 標記化。

第一種方法利用「標記保險庫（token vault）」作為敏感資料值的字典，將資料值對映到標記值（token value），而標記值則會用來取代資料庫當中的原始資料值。如此一來，應用程式或使用者在存取字典當中的原始資料值時，會取得對應的標記值，並可用它來還原出原始資料值。標記值是用來將關聯的標記對應到原始資訊的唯一管道。

第二種資料標記化方法沒有牽涉到保險庫的概念。在 vault-less 標記化當中，保護隱私資料的標記，是透過演算法來儲存，而非安全資料庫。只要標記可還原，原始的敏感資訊通常就不會存在保險庫之中。

為了幫助讀者更容易理解，以下是一個利用標記保險庫來實現標記化的實例情境。

客戶提供他們的信用卡卡號以進行任何交易。在傳統交易裡，信用卡號碼會被傳送到支付系統，接著被儲存在商家的內部系統裡，以供日後再次使用。現在，讓我們看看在實現資料標記化之後，這種交易會如何進行。

當客戶提供信用卡號碼以進行任何交易時，信用卡號碼會被傳送到標記系統或是保險庫，而不是支付系統。

標記系統或保險庫會以隨機產生的字母和數字組合，也就是標記，來取代客戶的敏感資訊，即信用卡號碼。

接著，當標記產生出來後，標記會以安全的形式，傳送到商家的零售點電子轉帳系統（POS terminal）和支付系統，以成功地完成交易。

有了資料標記化技術，企業就能透過無線網路安全無虞地傳輸資料。不過，為了有效實現資

料標記化，企業還必須使用支付閘道系統（payment gateway）以安全地儲存敏感資料。支付閘道系統可以安全地儲存並產生交易所需的信用卡資訊。

為什麼需要資料標記化？

對企業而言，目標是保護企業系統內任何敏感的付款或個人資訊，並將這類資料儲存在安全的環境裡。資料標記化能用難以解讀的標記來取代每個資料集合，協助企業達到這項目標。

以下是資料標記化攸關企業的五項理由：

如果浪費是你面臨的問題，那麼精實正是你的解藥。

1. 減少資料外洩及罰款的風險

資料標記化能幫助保護企業免於資料竊盜所造成的負面財務影響，在任何類型的資料外洩事件中，都能保護用戶個人資料。

安全漏洞事件通常會直接導致企業的營收下降，因為客戶往往會選擇轉向更妥善保護其支付資訊的其他競爭對手。

在資料外洩後，企業也可能因被起訴而蒙受損失。例如，在一連串的網路安全漏洞事件（包括誤導用戶的端點對端點加密技術）之後，Zoom 不得不建立一個 8,500 萬美元的基金，來支付美國使用者的現金索賠。此外，不遵守多項支付和安全標準，也可能導致鉅額的商業罰款和處罰。例如，不遵守 PCI（支付卡產業資料安全標準）會導致信用卡公司每個月向企業罰款 5,000 至 100,000 美元。

2. 建立客戶信任

標記化能幫助公司與其客戶建立信任。標記化可確保資料的格式正確並以安全方式傳輸，進而維護客戶和企業線上交易的安全性。這項技術能大幅強化資料安全性，讓網路攻擊和支付詐欺行為難以獲取客戶的敏感資料。

3. 符合產業規範

標記化能協助企業遵守產業規範，例如，任何接受現金卡和信用卡的企業，皆必須遵守或符合支付卡產業資料安全標準（Payment Card Industry Data Security Standard，PCI DSS）。標記化技術，符合支付卡產業資料安全標準當中，對於「遮蔽敏感持卡人資訊與安全地管理其儲存和刪除」的要求條件。因此，標記化不只提供了與支付卡相關敏感資料的安全防護，同時也降低了與符合規範相關的成本支出。

4. 促進訂閱式購買

結帳過程中更快速且更優質的顧客體驗，能夠有效提升「訂閱式購買（subscription-based purchase）」的機會。更快速的結帳流程，需要客戶以安全的方式儲存他們的支付資訊。標記化能以不敏感的標記來保護這類金融資料，像是信用卡資訊。在駭客面前，標記值永遠都是難以解讀及破解的資料，為經常性支付創造出一個安全的環境。有些主要的行動支付閘道系統，例如 Google Pay 和 Apple Pay，已經在運用資料標記化帶來的優勢，從而創造無縫且更加安全的用戶體驗。同時，安全保證也有助於企業說服更多用戶註冊。

5. 確保安全的資料共享

企業經常將敏感資料用在其他業務用途，例如行銷指標、分析或報告。實現了資料標記化，企業就能將儲存敏感資料的位置減少到最低數量，並確保標記資料可供執行資料分析或其他商業流程的使用者和應用程式存取。透過確保「單一使用者，只能存取特定任務所需的特定資料」，標記化技術可用來實現「最少權限（least-privileged）」的存取流程。因此，標記化過程維護了原始敏感資料的安全性。

總結

任何組織的合乎規範責任，多少會與其系統的規模成比例 - 系統中有越多應用程式用到敏感資料，就越有必要重新思考或更新其合乎資料規範的檢查標準。基於這個原因，使用標記化平台變得越來越普遍。標記化平台能幫助企業保護敏感資訊，同時確保企業符合安全規範。

用標記化技術來取代敏感資料，提供了諸多安全性與符合規範的優勢。降低安全風險和審計範圍這兩項優勢，可降低企業符合規範的成本，並減輕管理資料的負擔。