日本發布利用AI時的安全威脅、風險調查報告書，呼籲企業留意利用AI服務時可能造成資料外洩之風險

日本獨立行政法人情報處理推進機構於2024年7月4日發布利用AI時的安全威脅、風險調查報告書。

隨著生成式AI的登場，日常生活以及執行業務上，利用AI的機會逐漸增加。另一方面，濫用或誤用AI等行為，可能造成網路攻擊、意外事件與資料外洩事件的發生。然而，利用AI時可能的潛在威脅或風險，尚未有充分的對應與討論。

本調查將AI區分為分辨式AI與生成式AI兩種類型，並對任職於企業、組織中的職員實施問卷調查，以掌握企業、組織於利用兩種類型之AI時，對於資料外洩風險的實際考量，並彙整如下：

1、已導入AI服務或預計導入AI服務的受調查者中，有61%的受調查者認為利用分辨式AI時，可能會導致營業秘密等資料外洩。顯示企業、組織已意識到利用分辨式AI可能帶來的資料外洩風險。

2、已導入AI利用或預計導入AI利用的受調查者中，有57%的受調查者認為錯誤利用生成式AI，或誤將資料輸入生成式AI中，有導致資料外洩之可能性。顯示企業、組織已意識到利用生成式AI可能造成之資料外洩風險。

日本調查報告顯示，在已導入AI利用或預計導入AI利用的受調查者中，過半數的受調查者已意識到兩種類型的AI可能造成的資料外洩風險。已導入AI服務，或未來預計導入AI服務之我國企業，如欲強化AI資料的可追溯性、透明性及可驗證性，可參考資策會科法所創意智財中心所發布之重要數位資料治理暨管理制度規範；如欲避免使用AI時導致營業秘密資料外洩，則可參考資策會科法所創意智財中心所發布之營業秘密保護管理規範，以降低AI利用可能導致之營業秘密資料外洩風險。

本文同步刊登於TIPS網站（https://www.tips.org.tw）

相關連結

- IPAテクニカルウォッチ「AI利用時のセキュリティ脅威・リスク調査報告書」，独立行政法人情報処理推進機構
- AI利用時のセキュリティ脅威・リスク調査調査報告書，独立行政法人情報処理推進機構セキュリティセンター企画部調査グループ

你可能會想參加

→ 【2023科技法制變革論壇】AI生成時代所帶動的ChatGPT法制與產業新趨勢
→ 「跨域數位協作與管理」講座活動
→ 新創採購-政府新創應用分享會
→ 【線上場】113年「新創採購機制及鼓勵照護機構參與推動」說明會
→ 【北部場】113年「新創採購機制及鼓勵地方政府參與推動」說明會
→ 【南部場】113年「新創採購機制及鼓勵地方政府參與推動」說明會
→ 113年新創採購-照護機構獎勵說明會
→ 【南部場】113年「新創採購機制及鼓勵地方政府參與推動」說明會
→ 【北部場】113年「新創採購機制及鼓勵地方政府參與推動」說明會
→ 【中部場】113年「新創採購機制及鼓勵地方政府參與推動」說明會
→ 【臺北場】113年度新創採購-招標作業廠商說明會
→ 【臺中場】113年度新創採購-招標作業廠商說明會

→ 【高雄場】113年度新創採購-招標作業廠商說明會

王柏元
副法律研究員 編譯整理

上稿時間：2024年09月

資料來源：

IPAテクニカルウォッチ「AI利用時のセキュリティ脅威・リスク調査報告書」，独立行政法人情報処理推進機構，https://www.ipa.go.jp/security/reports/technicalwatch/20240704.html，最後瀏覽日：2024年8月3日。

AI利用時のセキュリティ脅威・リスク調査調査報告書，独立行政法人情報処理推進機構セキュリティセンター企画部調査グループ，https://www.ipa.go.jp/security/reports/technicalwatch/eid2eo00000022sn-att/report.pdf，最後瀏覽日：2024年8月3日。

文章標籤

人工智慧 資料管理 人工智慧風險管理

推薦文章