จดหมายข่าวความปลอดภัยของข้อมูล

Vol2 Generative AI

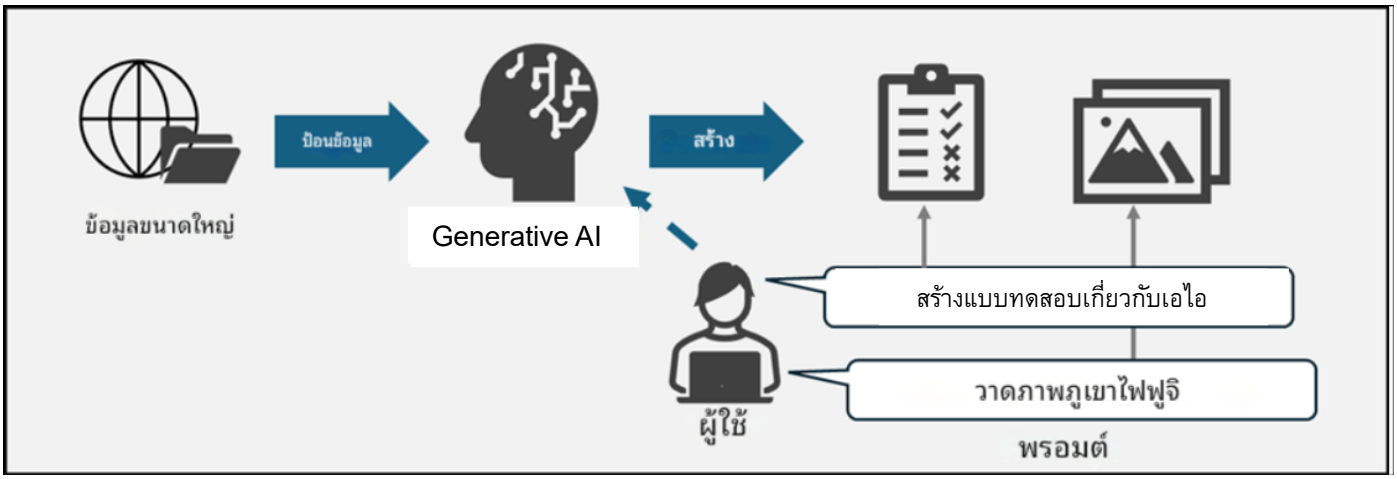
ปัญญาประดิษฐ์ที่ใช้การเรียนรู้เชิงลึก (Generative AI) คืออะไร?

Generative AI หมายถึง เทคโนโลยีที่สามารถสร้างเนื้อหาโดยอัตโนมัติ เช่น ข้อความ รูปภาพ และเสียง

กลไกการทำงานของ Generative AI อาศัยข้อมูลจำนวนมหาศาลที่ได้จากการเรียนรู้ของเครื่อง (Machine Learning) ในอดีต เพื่อนำมาสร้างเนื้อหาตามข้อมูลที่ผู้ใช้ป้อนเข้าไป

ประเภทหลักของ Generative AI ได้แก่ ปัญญาประดิษฐ์สำหรับสร้างข้อความ ปัญญาประดิษฐ์สำหรับสร้างภาพ และปัญญาประดิษฐ์สำหรับสร้างเสียง

กลไกการทำงานของ Generative AI



ความเสี่ยงจากการใช้ Generative AI

แม้ว่า Generative AI จะมีความสะดวกสบายในการใช้งาน แต่ก็มีความเสี่ยงบางประการเช่นกัน ที่นี่เราขอแนะนำความเสี่ยงที่พบได้บ่อย

การละเมิดทรัพย์สินทางปัญญา

มีความเสี่ยงที่เนื้อหาที่สร้างโดย AI อาจละเมิดลิขสิทธิ์หรือเครื่องหมายการค้าของผู้อื่น ตัวอย่างเช่น หากรูปภาพหรือข้อความที่สร้างขึ้นมีความคล้ายคลึงกับงานที่มีอยู่เดิมมาก อาจนำไปสู่ปัญหาทางกฎหมายได้ แม้ว่าบริการสร้างงานของ AI จะถูกระบุว่า "อนุญาตให้ใช้ในเชิงพาณิชย์" ก็ตาม แต่ก็ไม่ได้รับประกันว่าผลลัพธ์จะปราศจากการละเมิดสิทธิ์ของผู้อื่น

ปลอมลึก

อัลทำให้สามารถสร้างเสียงและวิดีโอปลอมที่มีความแม่นยำสูงจนแทบแยกไม่ออกว่าเป็นของจริง ส่งผลให้เกิดปัญหาต่างๆ เช่น การแพร่กระจายข้อมูลเท็จและการฉ้อโกงที่ทำลายชื่อเสียงของบุคคลหรือบริษัท

ความไม่แน่นอนด้านกฎระเบียบ

ปัจจุบัน กฎระเบียบของรัฐบาลและองค์กรต่างๆ ยังตามไม่ทันการพัฒนาและการใช้ AI เชิงกำเนิด หากมีความไม่แน่นอนใดๆ โปรดพิจารณาว่าสิ่งเหล่านั้นอาจส่งผลกระทบต่อความไว้วางใจของลูกค้าหรือนำไปสู่ปัญหาทางกฎหมายอย่างไร และต้องแน่ใจว่าได้รับการอนุมัติอย่างถูกต้องก่อนใช้งาน

มาตรการสำหรับผู้ใช้งานรายบุคคล

เพื่อให้สามารถใช้ Generative AI ได้อย่างปลอดภัย ผู้ใช้งานแต่ละคนควรคำนึงถึงประเด็นต่อไปนี้

- อย่าใส่ข้อมูลส่วนตัวหรือข้อมูลลับอื่นๆ ลงในระบบ Generative AI
- ตรวจสอบให้แน่ใจว่าเนื้อหาที่สร้างขึ้นจะไม่ละเมิดลิขสิทธิ์ เครื่องหมายการค้า สิทธิการออกแบบ หรือสิทธิในทรัพย์สินทางปัญญาอื่น ๆ ของผู้อื่น
- ควรตรวจสอบข้อมูลที่ได้รับจาก generative AI กับแหล่งข้อมูลที่เชื่อถือได้อื่นๆ เสมอ
- ตรวจสอบให้แน่ใจว่าเนื้อหาที่สร้างขึ้นไม่มีข้อมูลส่วนบุคคลที่เป็นเท็จ คำพูดที่หมิ่นประมาท หรือการแสดงออกที่เลือกปฏิบัติ

【ข้อมูลติดต่อสอบถาม】
ฝ่ายเลขานุการคณะกรรมการความปลอดภัยสารสนเทศ (กองเทคโนโลยีสารสนเทศ แผนกระบบสารสนเทศ ส่วนที่ 2)
อีเมล์ securitylearning@fanuc.co.jp

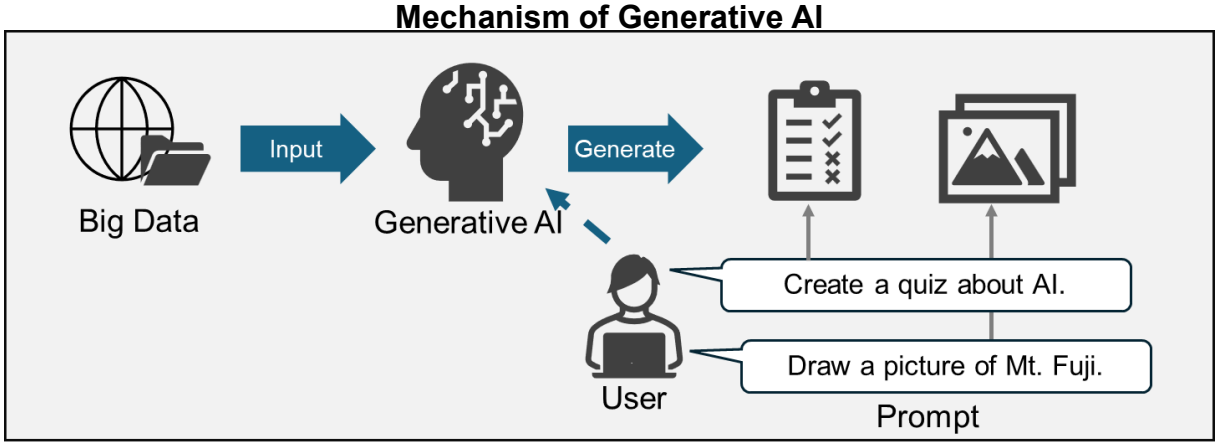
Information Security Newsletter

Vol2 Generative AI

What is Generative AI?

Generative AI refers to technology that automatically creates content such as text, images, and audio.
Its mechanism involves using vast amounts of data acquired through previous machine learning to generate content based on user input.
Major types of generative AI include text generation AI, image generation AI, and audio generation AI.

Mechanism of Generative AI

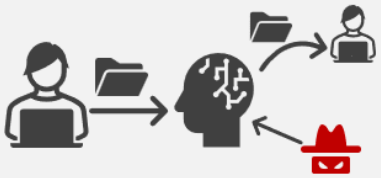


Risks of Using Generative AI

Generative AI is convenient, but it also comes with certain risks.
Here, we will introduce some of the most common ones.

Data breach

There is a risk that **data entered generative AI may be leaked externally**. Input data may be used for AI training and appear in responses to other users. Input data may also be stored in service providers' logs to prevent misuse. However, **if a malicious act occurs within the provider's organization** or **if an external attack is successful**, the information could be leaked.



Hallucination

Generative AI may sometimes **produce information that differs from facts**. This phenomenon is known as "hallucination." If the output contains misinformation or bias, trusting it could lead to incorrect decisions or actions.

Intellectual Property Infringement

There is a risk that content generated by AI may infringe on others' copyrights or trademark rights. For example, if a generated image or text closely resembles an existing work, it could lead to legal issues. Even if a generative AI service is labeled as "commercial use allowed," **it does not guarantee that the output will be free from infringement of others' rights**.

Deep fake

AI has made it possible to create fake audio and video with such high precision that they are indistinguishable from real ones. As a result, issues such as the spread of misinformation and fraud that damage the reputation of individuals or companies have emerged.

Regulatory uncertainty

Currently, **regulations by governments and organizations have not yet caught up** with the development and use of generative AI. "If there are any uncertainties, **consider how they may affect client trust or lead to legal issues**, and be sure to obtain proper approval before use.

Individual Measures

To use generative AI safely, each person should keep the following points in mind.

- **Do not enter personal or other highly confidential information into generative AI.**
- **Ensure that the generated content does not infringe on others' copyrights, trademarks, design rights, or other intellectual property rights.**
- **Always verify information provided by generative AI with other reliable sources.**
- **Ensure that the generated content does not contain false personal information, defamatory statements, or discriminatory expressions.**

【Inquiry】
Information Security Committee Secretariat
(IT Division information System Department Section 2)
securitylearning@fanuc.co.jp
