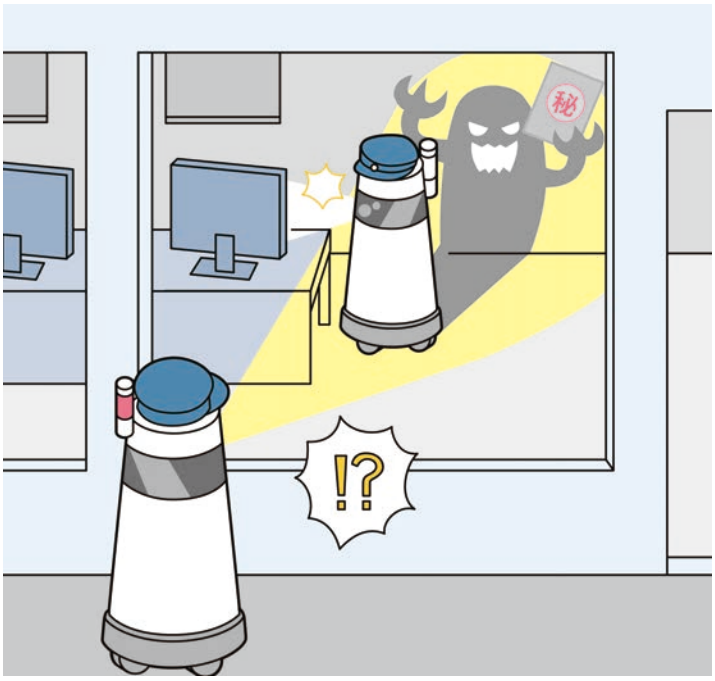
S-E01 Verification of AI's identity by its profile

IOWN Evolution

Enable a use of changing AI with confidence by verifying its identity

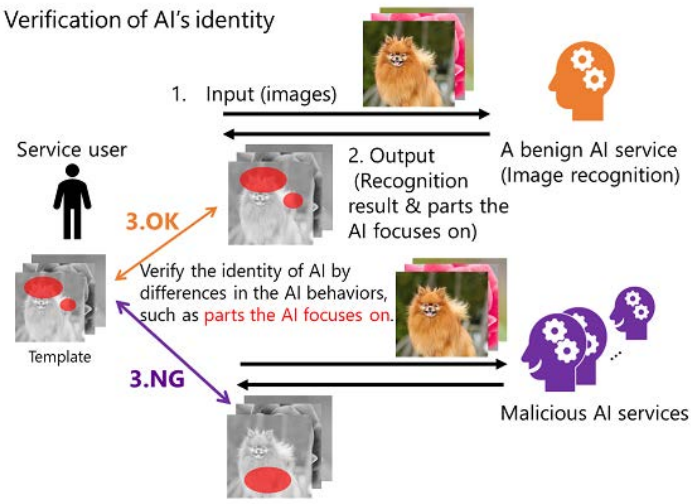


Background

In the near future, widespread AI may change into an unintended AI due to unexpected changes or the intervention of attackers, or AI impersonation may occur due to unauthorized copy and harm users. Therefore, users themselves must be able to verify the identity of the AI.

Summary

We started research and development on technologies to detect changes of AI caused by attacks or impersonation of AI, based on the behavior of the AI, and to determine whether the AI remains the AI we have used even if it changes through daily learning.



Feature 1

Proposed a new method to verify the identity of AI by focusing on where AI focuses on input data and the output results of processing input data

Feature 2

Determine if an AI has lost its identity by looking at the impact of an attack

Future benefits

By identifying inappropriate AI, such as AI impersonation, you can use AI with confidence. In this way, we will promote the business use of AI and aim for co-prosperity between people and AI.

Collaboration partners

National University Corporation Shizuoka University

Exhibiting Company

NIPPON TELEGRAPH AND TELEPHONE CORPORATION

Contact

rdforum-exhibition@ml.ntt.com