March 10, 2022

Proposal of security standard for secure computation providers

Digital Garage, Inc. (TYO:4819), NTT Corporation (TYO:9432), Ierae Security Inc, NEC Corporation (TYO:6701), today announced that we have proposed security standard in order to ensure that the security of secure computation is mutually understood by providers and users and that everyone can use secure computation properly.

Secure computation is a technology that allows data to be computed while the data is encrypted. There are multiple schemes and their security definitions in secure computation. It has been difficult for users of secure computation without specialized knowledge to understand the difference between them, and this has been an obstacle to choosing an appropriate scheme in a real-world application. Therefore, we have proposed a security standard that enables users to evaluate the security of multiple schemes in a unified manner. We believe that it will promote mutual understanding of secure computations between providers and users by having the providers explain the security of their schemes to users in accordance with the security standard, and as a result, the user can choose an appropriate method.

The four companies will continue to discuss and improve the safety standards in cooperation with companies and academic institutions that engage in the secure computation and will engage in activities that contribute to the realization of a society in which various data can be shared and used safely.