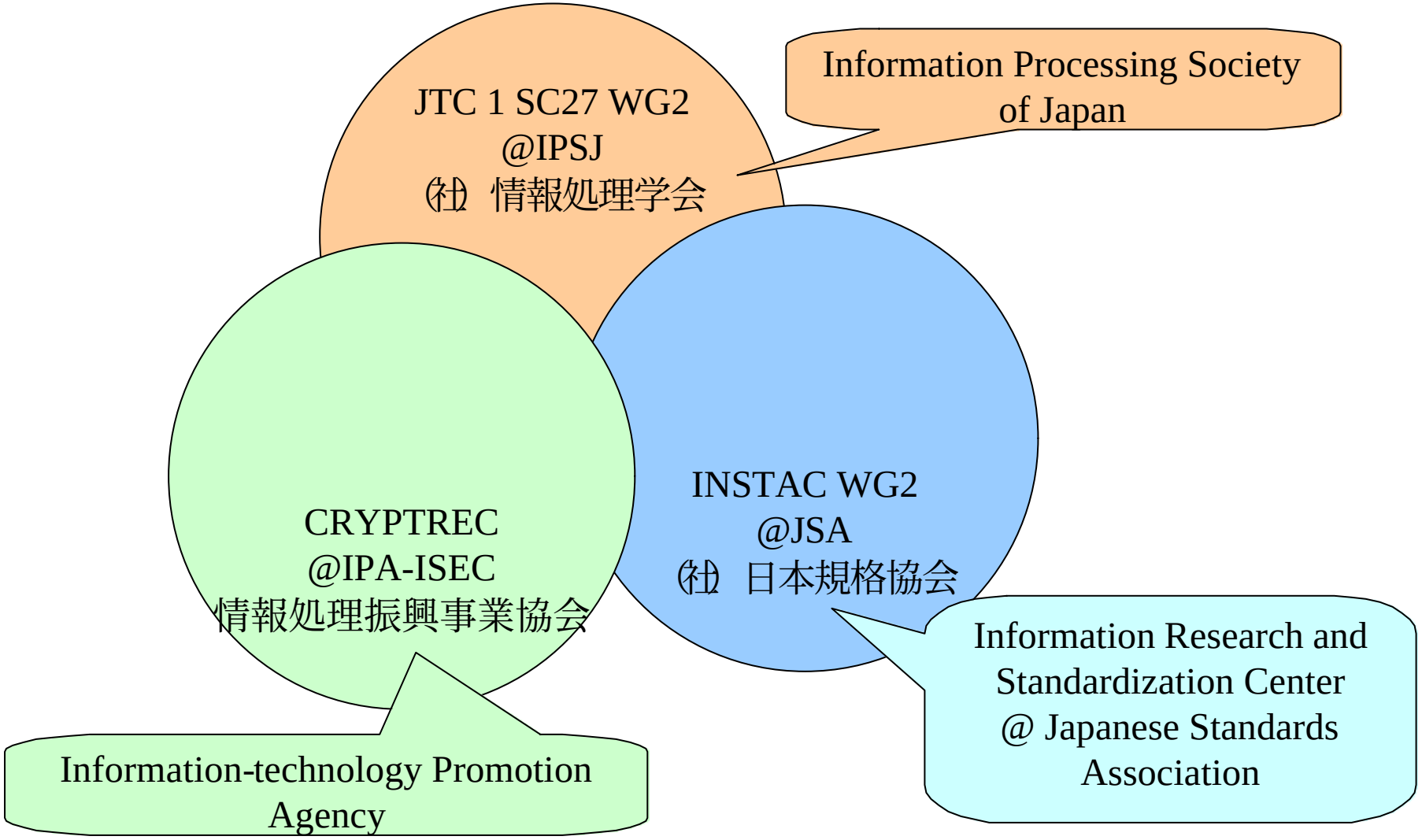
日本における暗号技術標準化関連活動

Standardization of Cryptographic technology in Japan

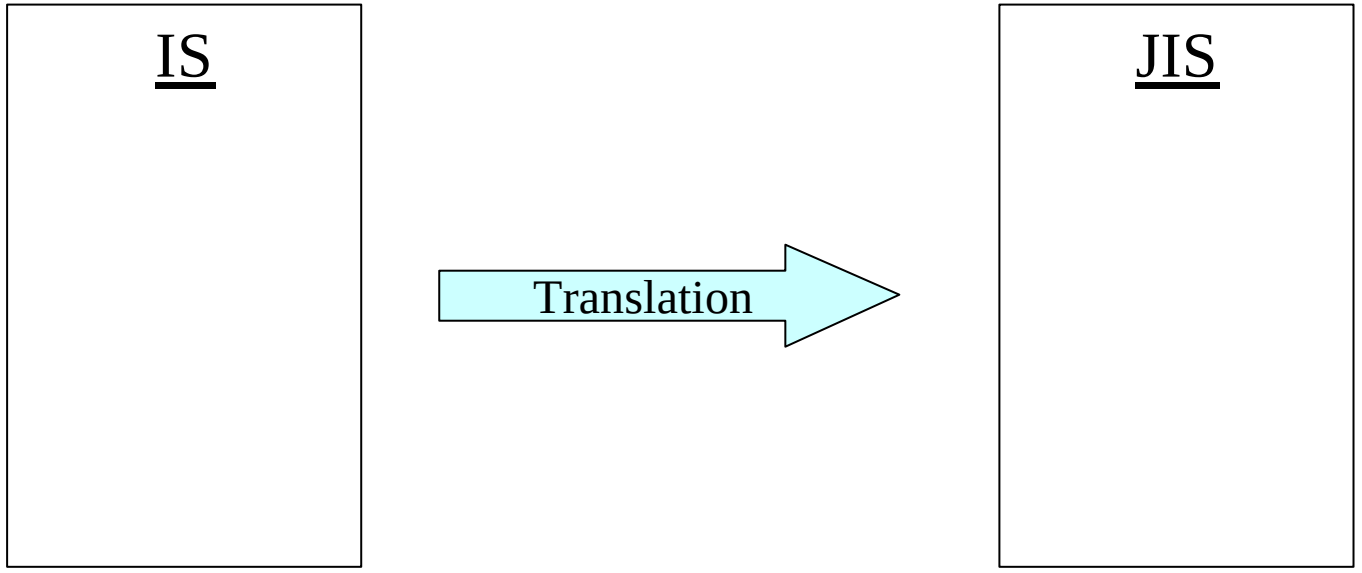
桜井　幸一

Koichi Sakurai

Organizations



INSTAC
(Information Research and Standardization Center)

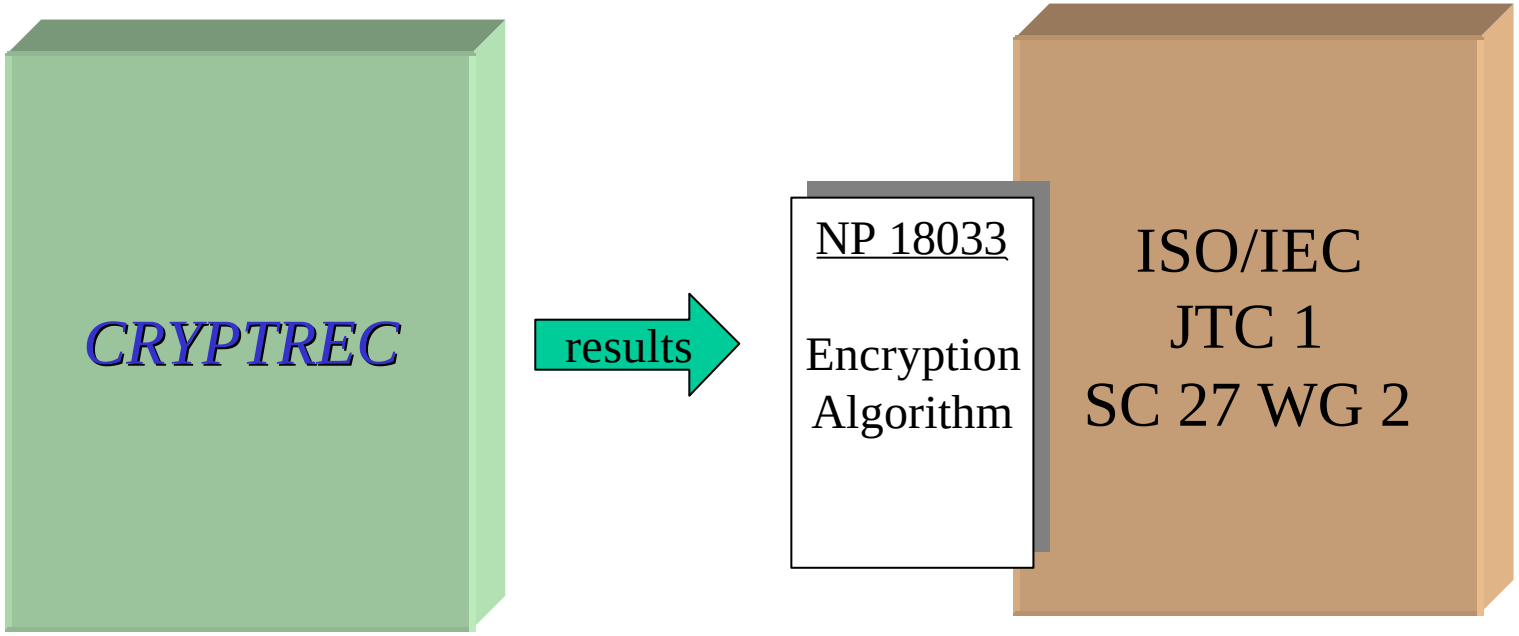


ISO/IEC JTC 1/SC 27

Origin:

OSI in ISO -> JIS

CRYPTREC & JTC 1 SC 27 WG 2



NP 18033-4: Encryption Algorithm
- Stream Cipher -

- SC 27 Tokyo Meeting WG 2 (Oct.18-19,2000)
- Framework (Cris Mitchell)
  - Part A: Key stream Generation Algorithm
    - A1. Using Block Ciphers
    - A2. Dedicated Algorithm
  - Part B: Modes of Key stream
    - B1. + Binary Additive
    - B2. New Model

N2656r2:
National Body contributions on NP 18033

- Expert contribution from HITACHI
- MULTI-SO1 (under CRYPTREC)
  - A new mode + PANAMA
- Call for Contribution
  - Meeting in OSLO (April, 2000)