

Academic Research Directions of Information Security

(学問としての情報セキュリティの研究の方向性)

--- An Administrative Perspective ---

Kanta MATSUURA
(University of Tokyo)

Contents



- What

- A layered understanding.

- Who

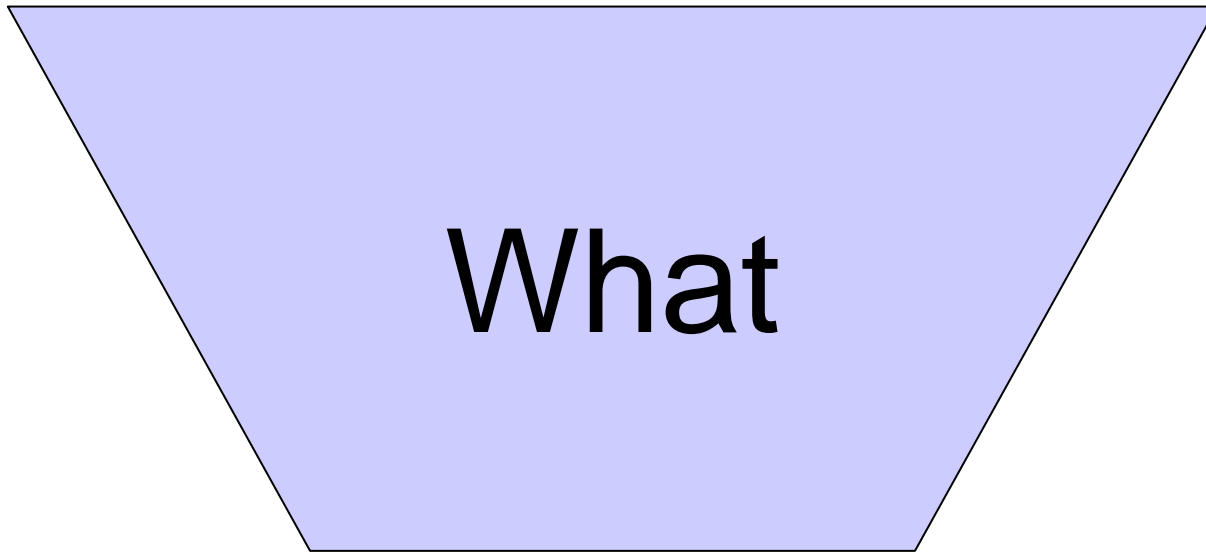
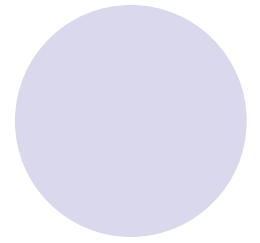
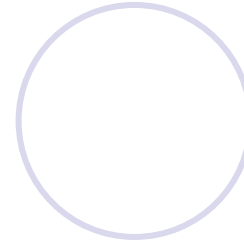
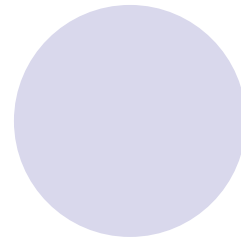
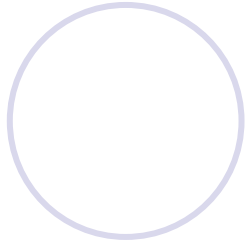
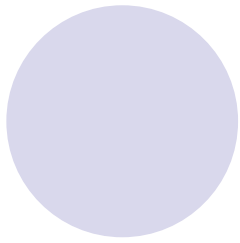
- Different research communities.

- Different sectors.

- How

- Research network.

- Conclusions

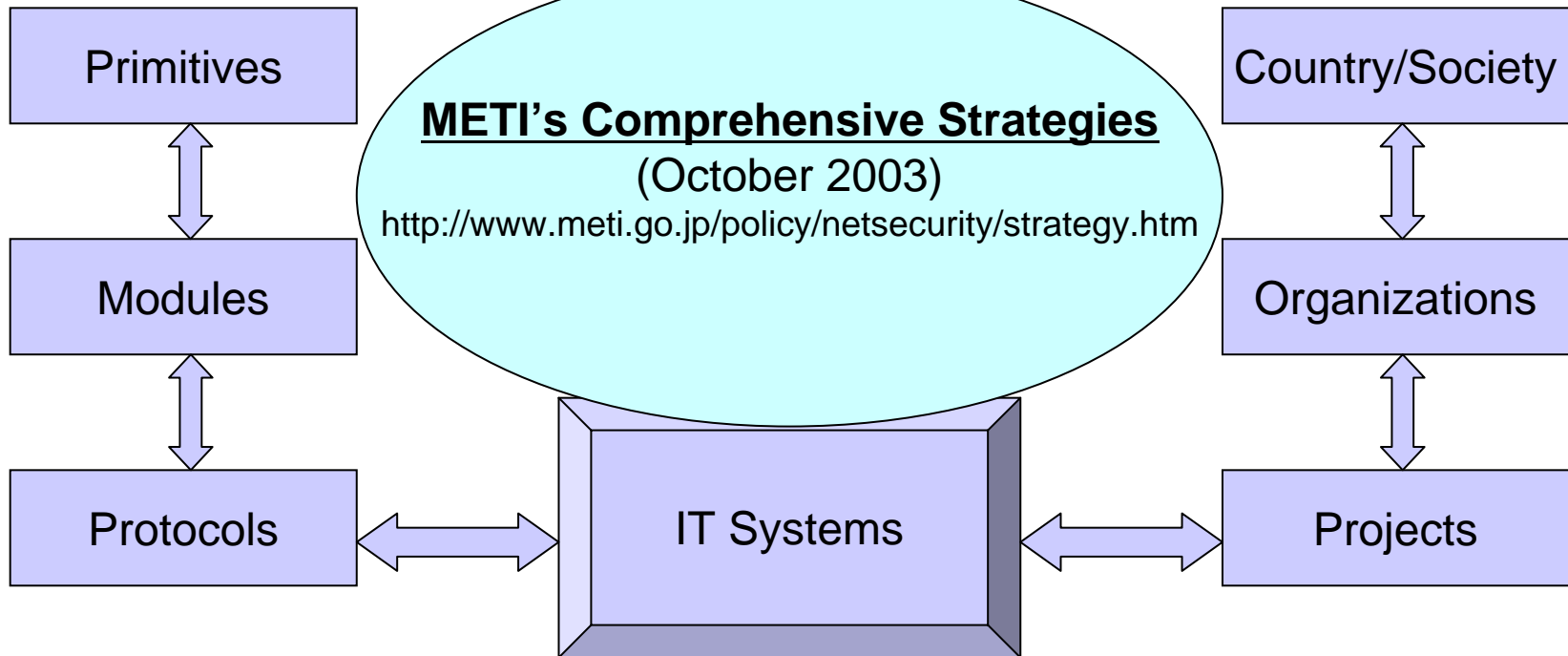


A layered understanding

● Technologies

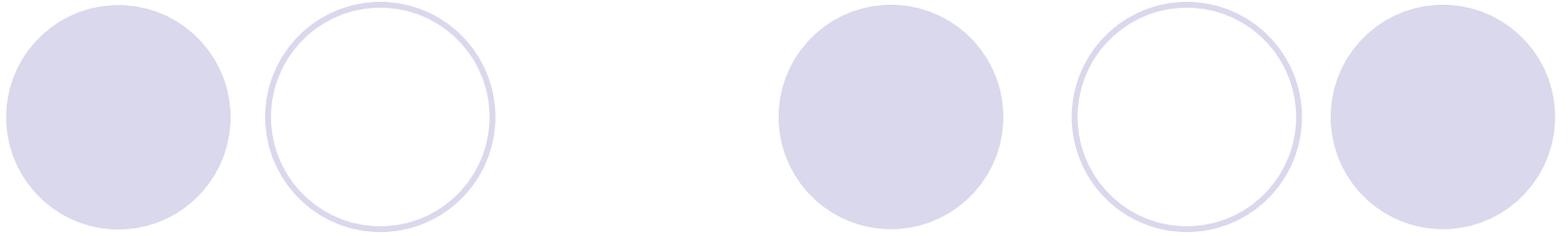
● Management

CRYPTREC



Academic approaches should (could)

- Place more emphasis on
 - Long-term issues (e.g. information-theoretically secure technologies, quantum cryptography, multiple-period financial models),
 - Multi-disciplinary issues (e.g. real-world attacks, deployment problems, comprehensive evaluation)
- With keeping the basic principles:
 - Things must be open.
 - Cares must be taken for education.



Different research communities

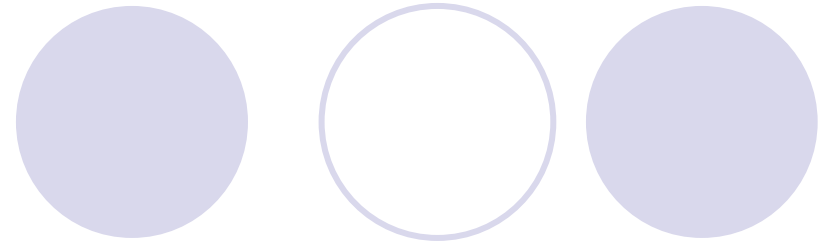
- Problems due to a wrong sense of evaluation:
 - Biometrics security breaches.
 - DRM by “security through obscurity”.
 - Implementation blunders: Change particular algorithms/protocols/platforms, and still keep the same assumptions/models without efforts for finding particular attacks (even if well-known in different communities).
 - Deployment problems.

Toward improvements

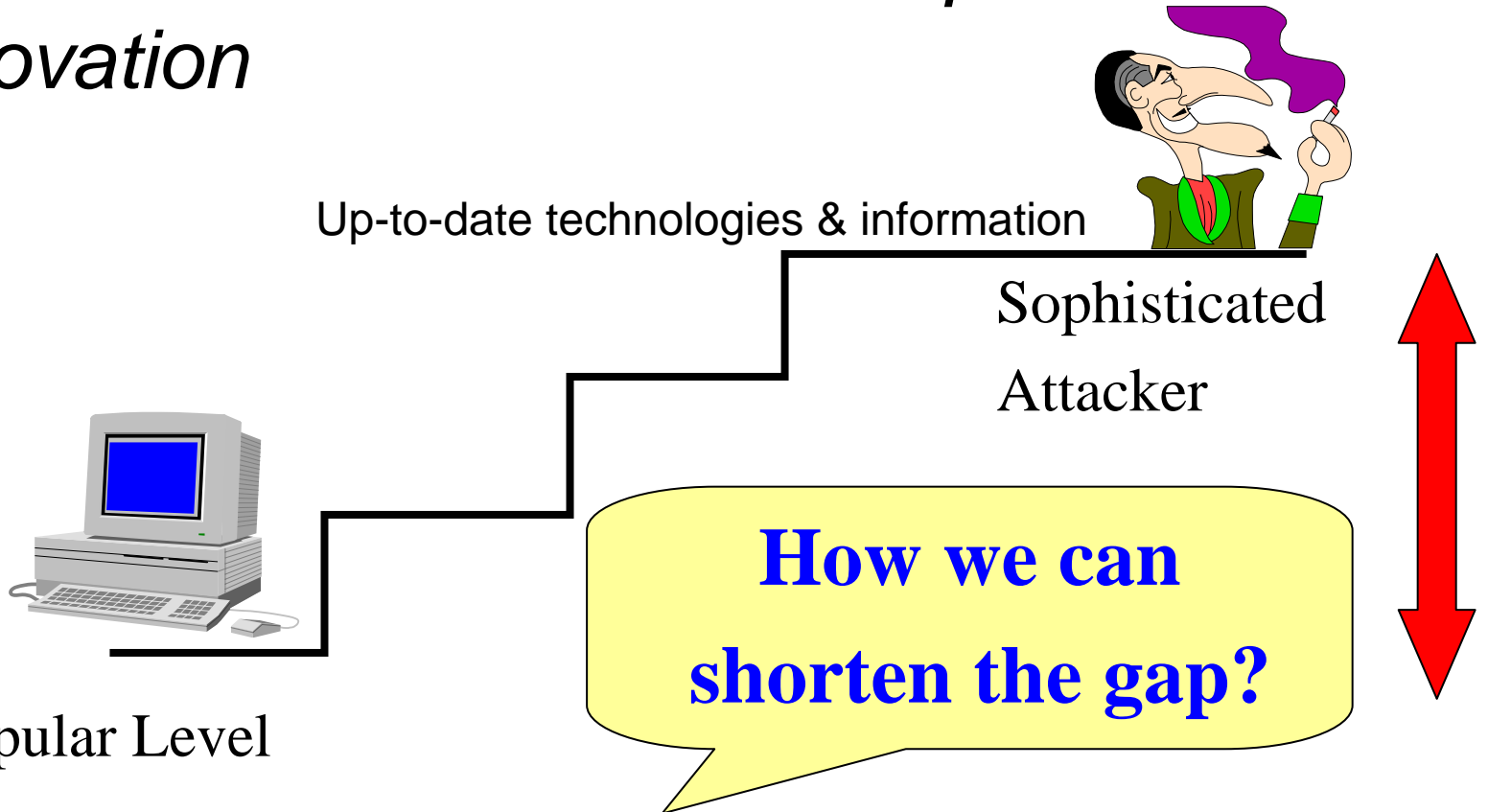


- New conferences with the involvement of major players in different communities (e.g. security and economics/finance, privacy protection and metrics).
- Joint projects among different communities (e.g. MEXT Grant-in-Aid Scientific Research on Priority Area "Informatics").

Different sectors



- Inter-sector collaboration *for quicker innovation*

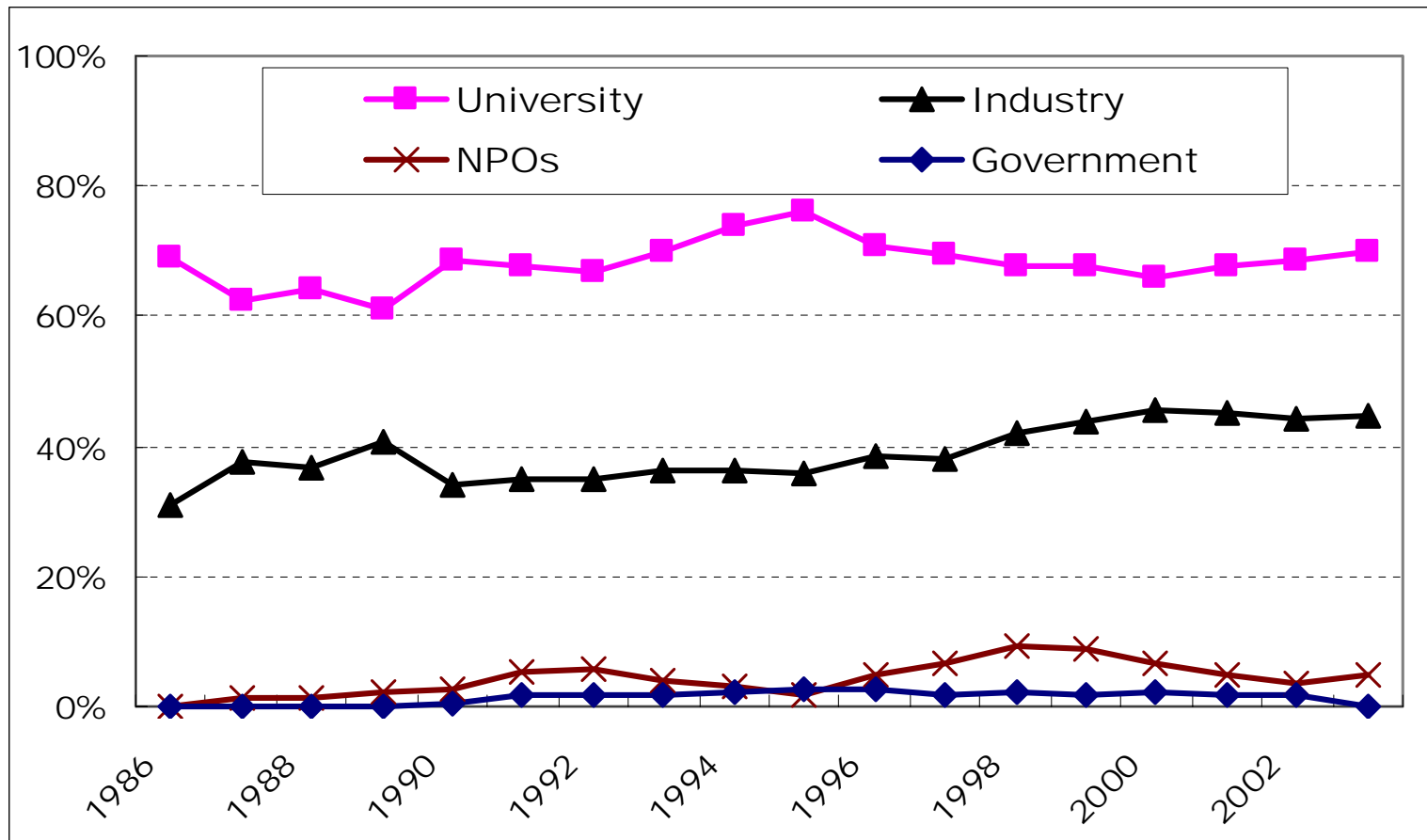


Findings by a bibliometric analysis

- Co-authorship in SCIS (Symposium on Cryptography and Information Security)
 - Founded in 1984 and held annually
 - A large number of research papers
 - Addressing information security from various angles (not only cryptography)
 - Quality of published material is semi-automatically controlled (by pressure)
 - In Japan, domestic academic societies are very active and domestic conferences are important (even musts)

Share of papers

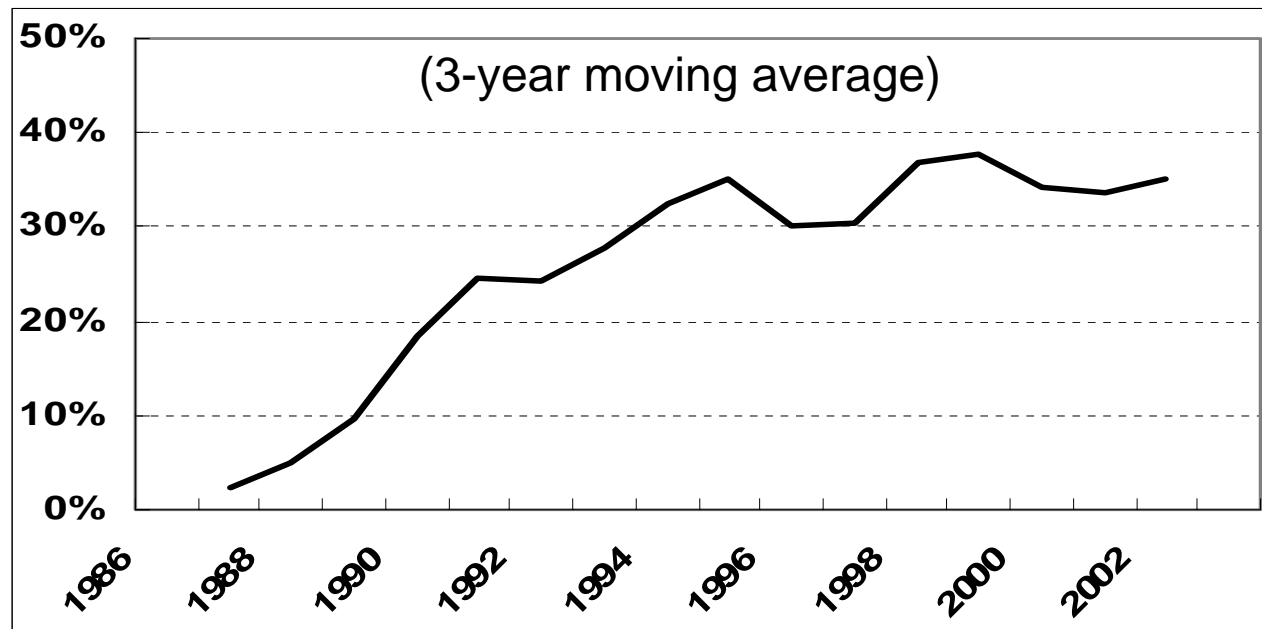
● No significant change



Share of cross-sector coauthored papers among industry-involved papers

- References: 54% in the electrical field (1995)
78% in the machinery field (1995)
- Remained steady at 30-40% in SCIS (1994-2003)

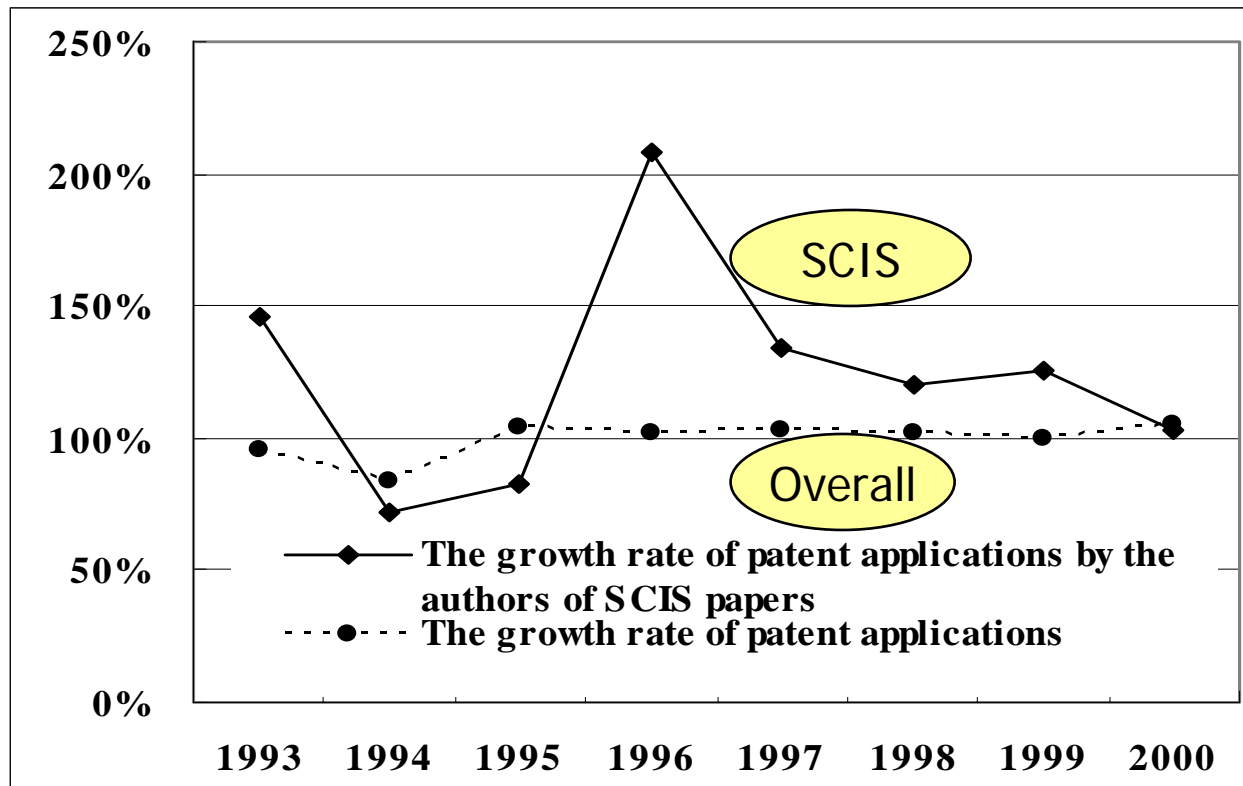
Lower level compared to the other fields



Cf.: If among all papers, saturated around 20%.

However, maybe working better than we are afraid...

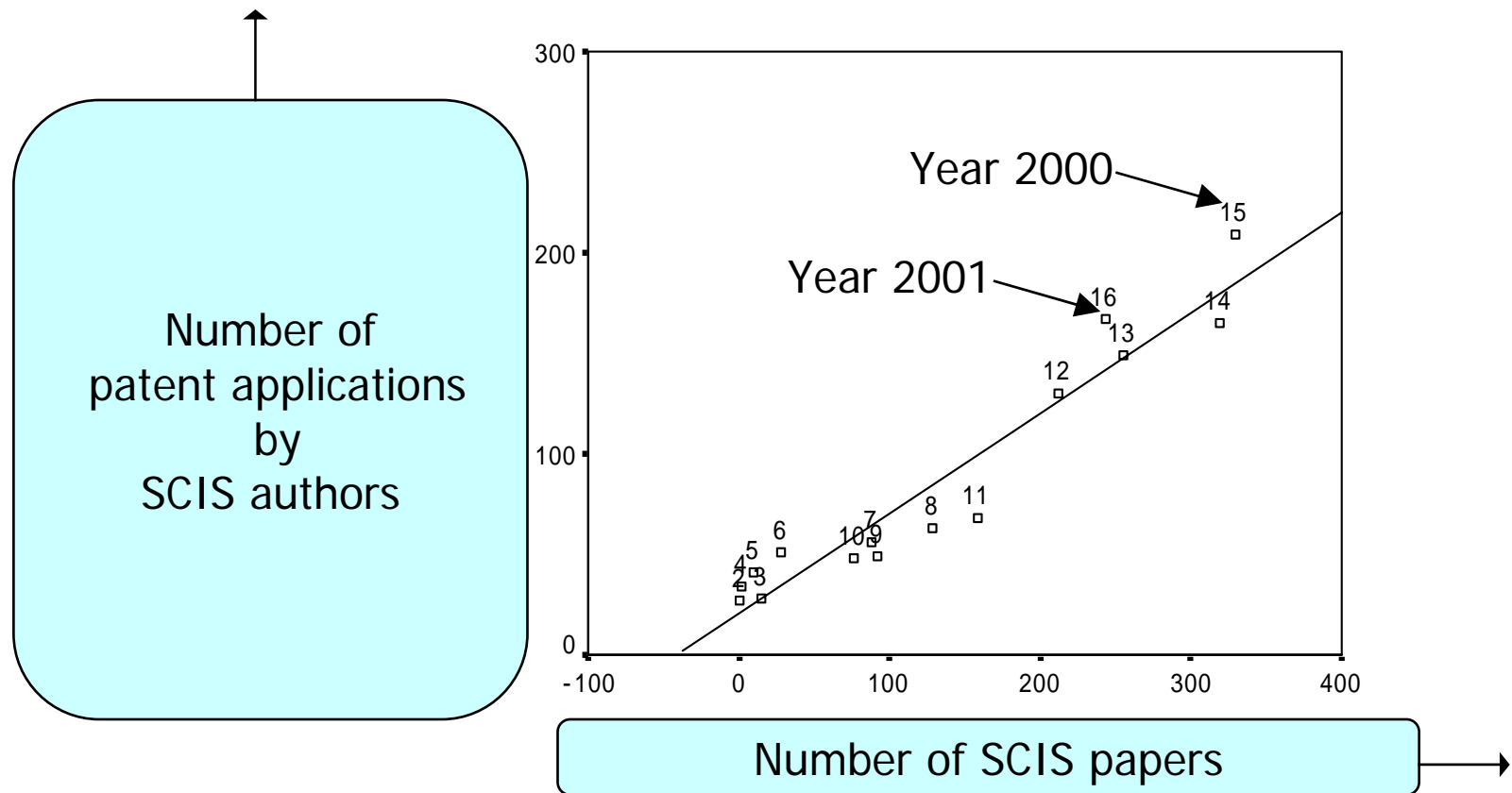
- Upward trend in patenting

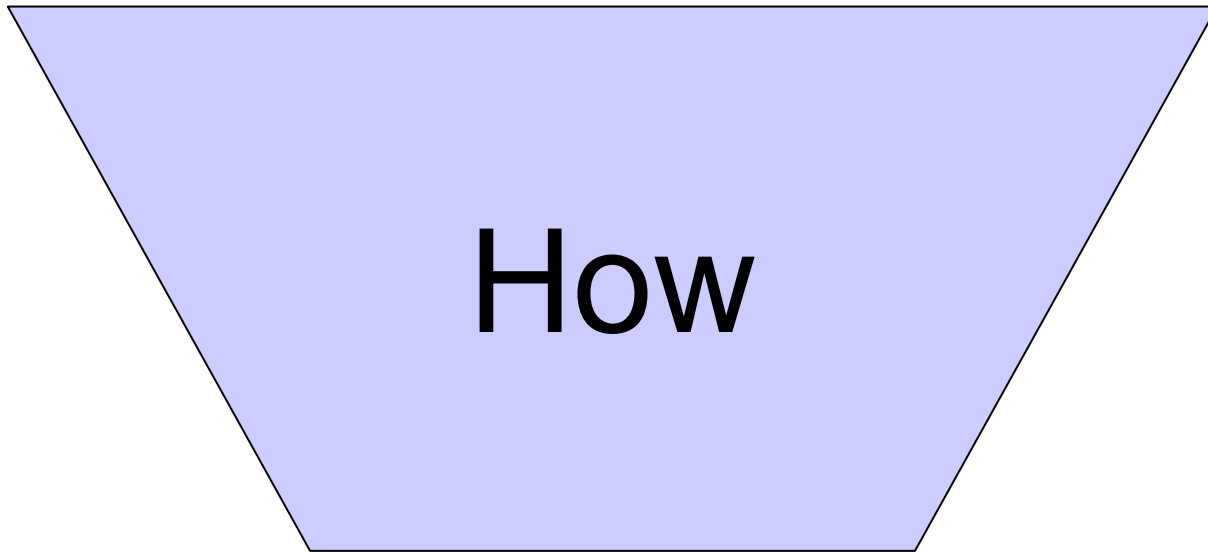


Scatter plot of the number of papers and the number of patent applications

● Clear correlation

(Each plot: Each year)





Average number of coauthors when we eliminate particular types of SCIS authors

- Results for the top 80 authors

| After elimination of | Average # of coauthors |
|--|------------------------|
| Authors who worked in industry sector only | 4.8 |
| Authors who worked in university sector only | 4.7 |
| Authors who worked in multiple sectors | 4.2 |

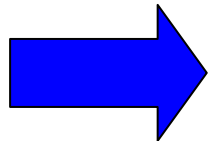
Importance of personnel issues for collaboration



Conclusions

“Open” is a key word

- Research targets are getting deeper and wider across discipline borders but we must bear in mind that the basics remain important.
- Evaluation must be reliable and shared.
- Research network is important.



for academic systematization
in the context of social responsibility