関東地区大学理工系
就職研究会
40周年記念祝賀会
基調講演

実用化に近づいた量子情報技術

-量子エニグマ暗号と量子レーダーカメラ-

玉川大学・量子情報科学研究所
所長　廣田　修

平成２８年１１月２５日
アルカディア市ヶ谷

講演内容

１：概要

- 講演者の系図
- 量子情報科学とは？
- 量子情報科学研究所

２：サイバー攻撃と防御技術

３：全天候対応の量子レーダーカメラ

■ 講演者の系図

Norbert Wiener：確率過程、一般化フーリエ解析論
（サイバネテイクス創始）

池原止戈夫
素数定理
フーリエ解析
サイバネティクス理論

ＭＩＴ卒
東京工業大・理学部
数学科教授
東京工業大・名誉教授
東京電機大学・教授

多数の数学者を輩出

未松安晴
光通信　半導体レーザー
東京工業大・元学長
文化勲章受賞

廣田　修
量子情報科学の創設に寄与

臼田　毅
量子通信理論
愛知県立大学

N.Wiener国際会議（2016年7月、メルボルン）

Wiener国際会議運営委員会：

日本におけるWiener思想の継承をパネルで紹介

Wiener：ウイーナー過程論
一般化タウバー型定理

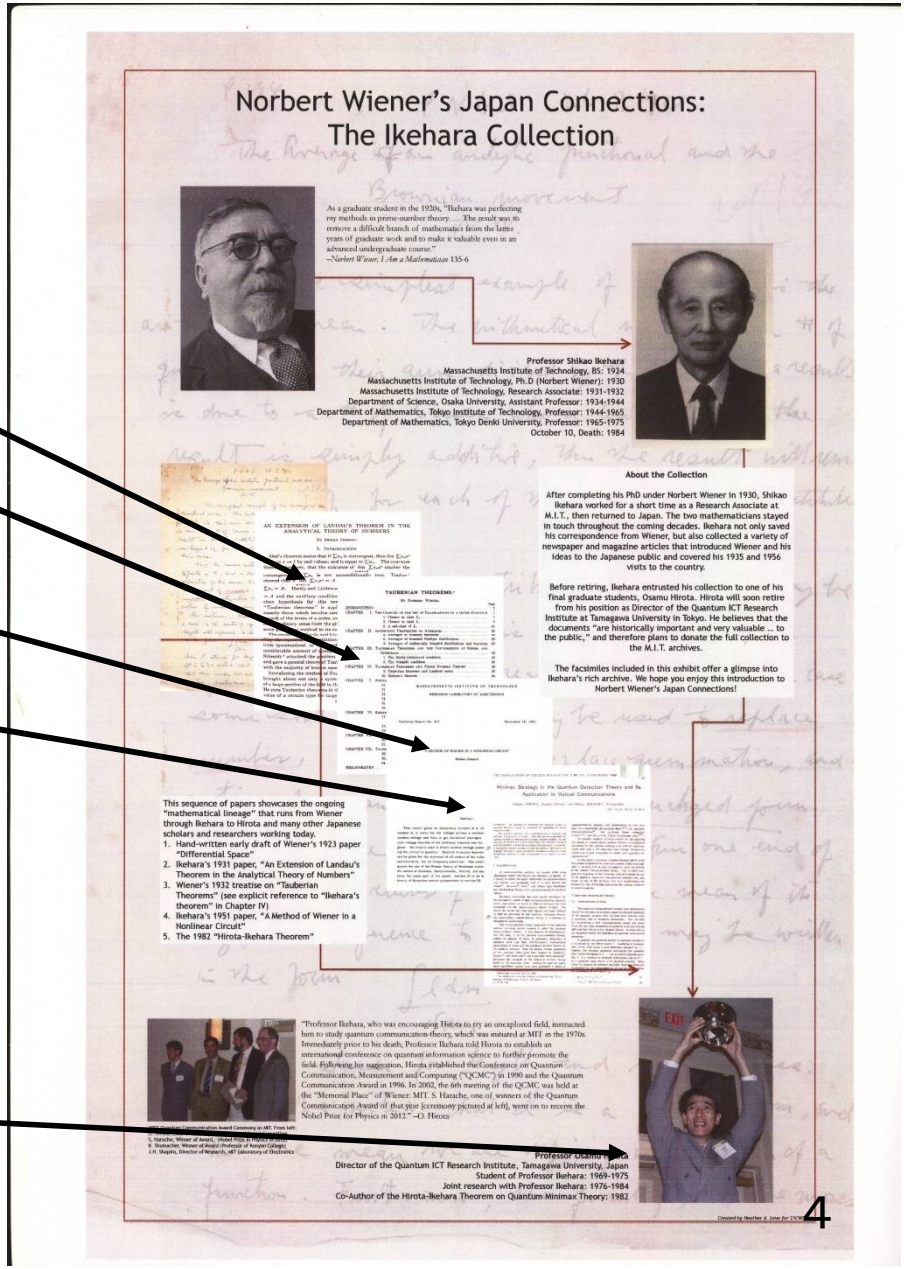
↓

池原-Wiener： 素数分布定理

↓

廣田・池原：量子ミニマックス定理

廣田：ＭＩＴからWiener思想を発展させる量子情報科学の国際会議の創設と運営に対する感謝の銀杯を拝受（2002年）



■ 量子情報科学とは？

◆ 従来の情報科学：

情報を運ぶ信号の物理は重要ではなく、
記号の世界のみで情報伝送、処理、計算原理を確立

- 通信理論、情報処理理論、計算理論の開発

N.Wiener
C.E.Shannon
J.von Neumann

- 電子回路等による実現技術の開発＝＞実用化

◆ 量子情報科学：

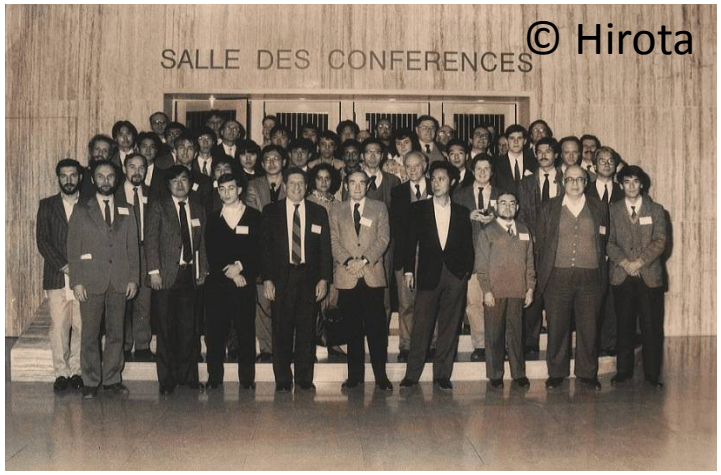
情報を運ぶ信号の物理現象を考慮した情報伝送、
処理、計算原理を確立

- 量子通信理論、量子情報処理理論、量子計算理論の開発
- 量子回路等による実現技術の開発＝＞実用化

日本発の量子情報の国際会議

- 廣田　修、1990年創設
  （２０年間組織委員長）

Quantum Communication, Measurement and Computing (QCM&C)



1990年　第一回会議（Paris,France）

３人のノーベル物理学賞

Claude Cohen-Tannoudji, 1997年
David Wineland,2012年
Serge Haroche, 2012年

- 今井　浩（東大）, 2001年創設

Asian Quantum Information Science (AQIS)

上記の２つの世界の評価：参考文献

C.H.Bennett, 大川賞受賞記念講演、大川情報通信基金2010年度　年次報告

量子通信理論の基礎研究

Shannon型量子通信理論の基礎研究

1960年～2000年

C.W.Helstrom
A.S.Holevo
H.P.Yuen
O.Hirota

A.S.Holevo,

応用研究

Y-00暗号,
量子エニグマ暗号など

A.S.Holevo, M.Sohma, O.Hirota,
PRA vol.59, no.3, pp.1820-1828, 1999.

A.S.Holevo, M.Sohma, O.Hirota,
Report on Mathematical Physics vol.46, no.3, pp.343-358, 2000

Wiener型量子通信理論の基礎研究

1970年～2010年

R.L.Stratonovich
V.P.Belavkin
O.Hirota

R.L.Stratonovich, V.P.Belavkin

応用研究

量子レーダーカメラ、
量子ジャイロ、
など

V.P.Belavkin, O.Hirota, R.Hudson,
Quantum Communication and Measurement, Plenum Press, 1995.

量子情報科学の応用の時代へ

-2000年～現在-

数理系基礎研究

実社会で要望される情報技術の開発

■ 量子情報科学研究所

小原芳明学長　創設

（ミッション：社会的課題に対する貢献）

[A]「サイバー攻撃に対する防御技術の研究開発」

二見史生　教授
加藤研太郎　教授
相馬正宜　教授

光回線からのインフラ破壊攻撃に対処する

超高速量子エニグマ暗号の開発

[B]「天候に影響を受けないカメラの研究開発」

政田元太　教授
村上　弾　助教
相馬正宜　教授

悪天候時の自動運転に対処する

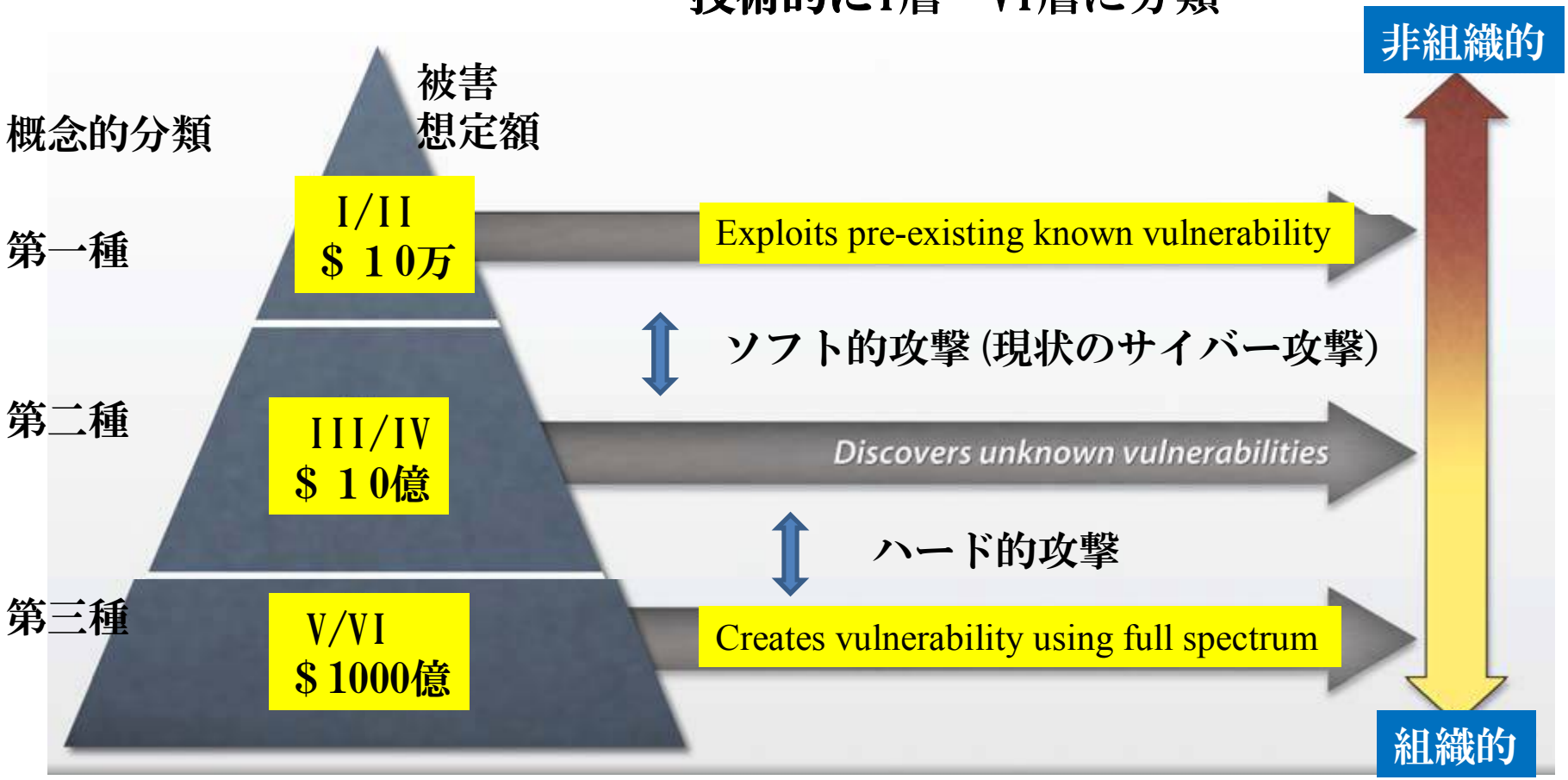
量子レーダーカメラの開発

2部

サイバー攻撃と防御技術

■ 米国防総省サイバー攻撃の分類

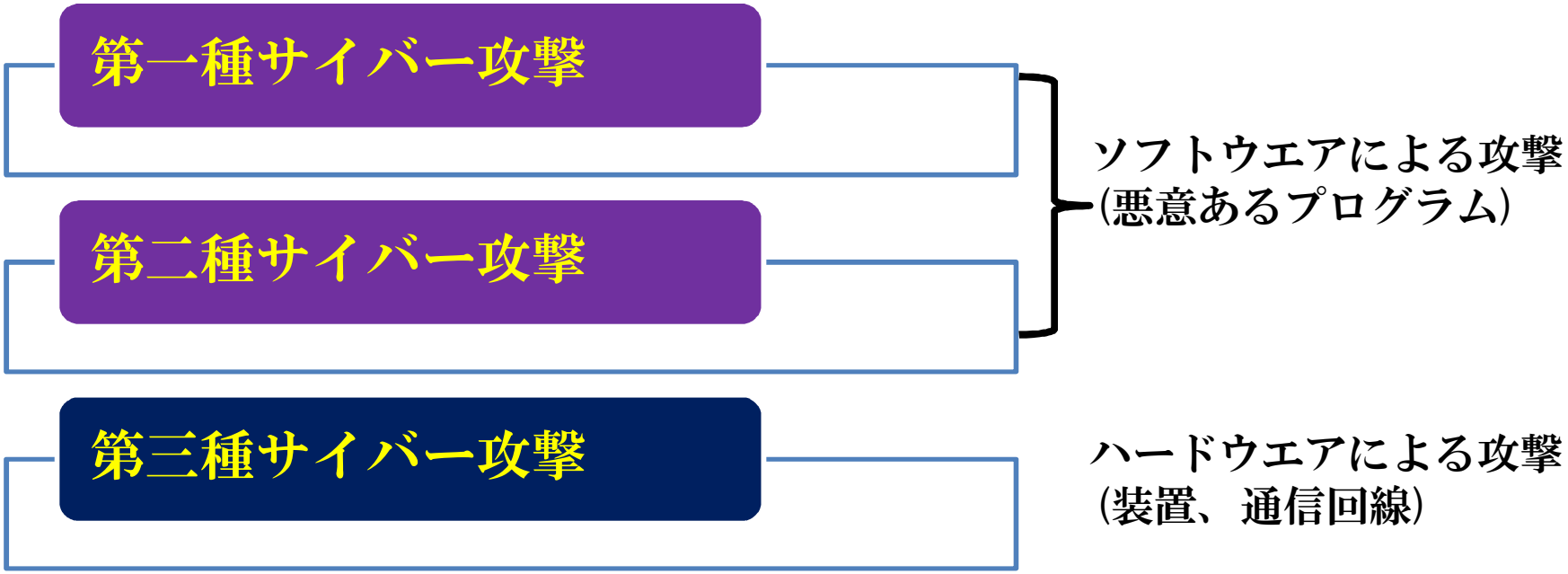
技術的にI層～VI層に分類



出典：米国 Defense science board, 2013
(Task force report)

■ サイバー攻撃

ソフトウエアの世界からハードウエアの世界へ



■ 第三種攻撃の実例報告

攻撃対象

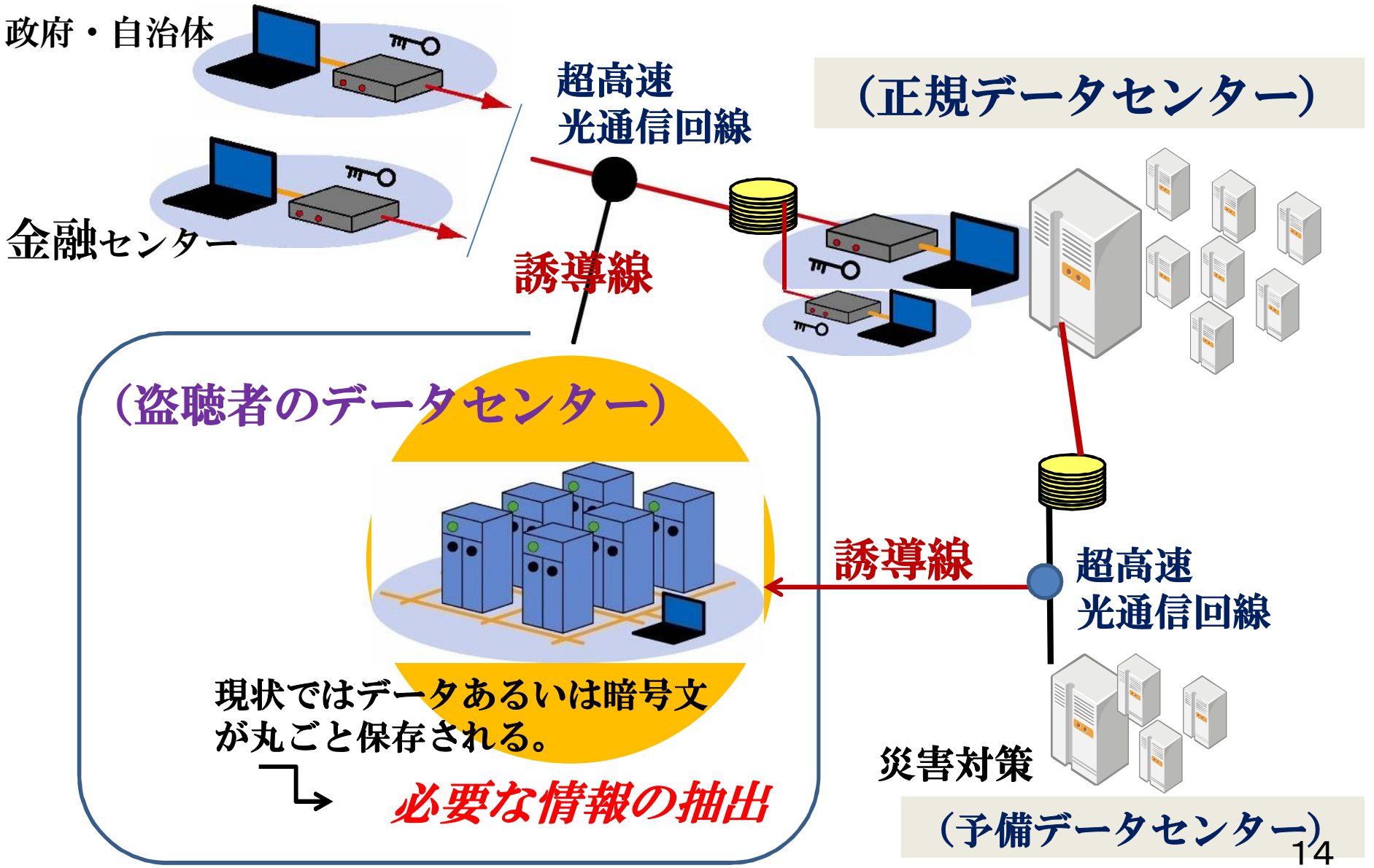
出典：DER SPIEGEL
No-28，７月８日、2013

◆陸上超高速光通信網
1 Gbit/sec～100 Gbit/sec

◆海底光ファイバーケーブル
100 Gbit/sec～1 Tbit/sec

１波長当たり、
1 Gbit/sec～10 Gbit/secの
光信号情報を保護する
暗号技術が必須となる

■ 攻撃の具体的手法 （通信インフラからのタッピング）



■ 課題解決の必須技術

➢ニーズ

超高速
光通信網の
安全性保証

◆1Gbit/sec～
100Gbit/sec

◆1000Km～
１万km

現状は無防備

➢現状技術の問題

数理暗号の
危殆性

➢解決策
(DARPA提唱)

超高速
物理暗号
の開発

世界中のデータセンター間
を結ぶ光通信網の保護技術

■ ２つの量子暗号

◆ BB-84型量子暗号　Shannon理論体系の範疇

単一光子通信で暗号用の鍵系列を安全に配送

特徴

- ➢ 配送された鍵系列（乱数）を用いてOne Time Padによって通信文を暗号化して通信する。
- ➢ 単一光子のため通信の速度がきわめて遅くなる

◆ Y-00型量子暗号　Shannon理論を超える

強力なレーザー信号の通信文を直接、
量子効果で暗号化する

特徴

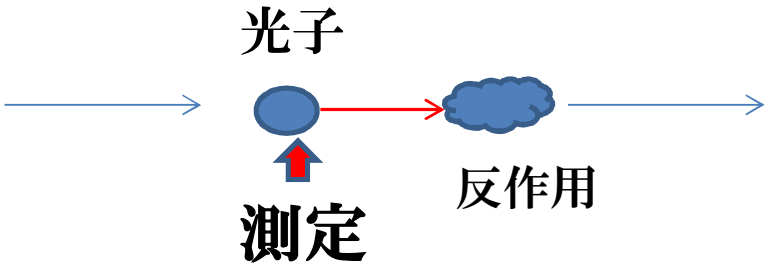
- ➢ 鍵の長さは256ビットでよい。
- ➢ 強力なレーザーのため超高速通信が可能

■ 量子暗号の２大原理

微視的量子効果
BB84型
（量子鍵配送＋One Time Pad)

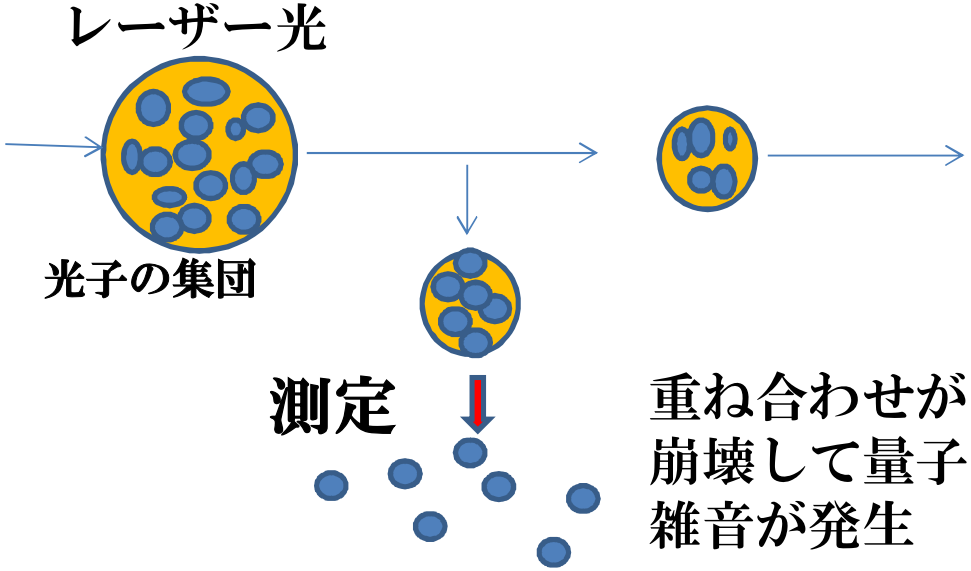
巨視的量子効果
Y-00型
（直接データ暗号化方式）

反作用の法則



反作用の大きさを評価して
安全性を保証する

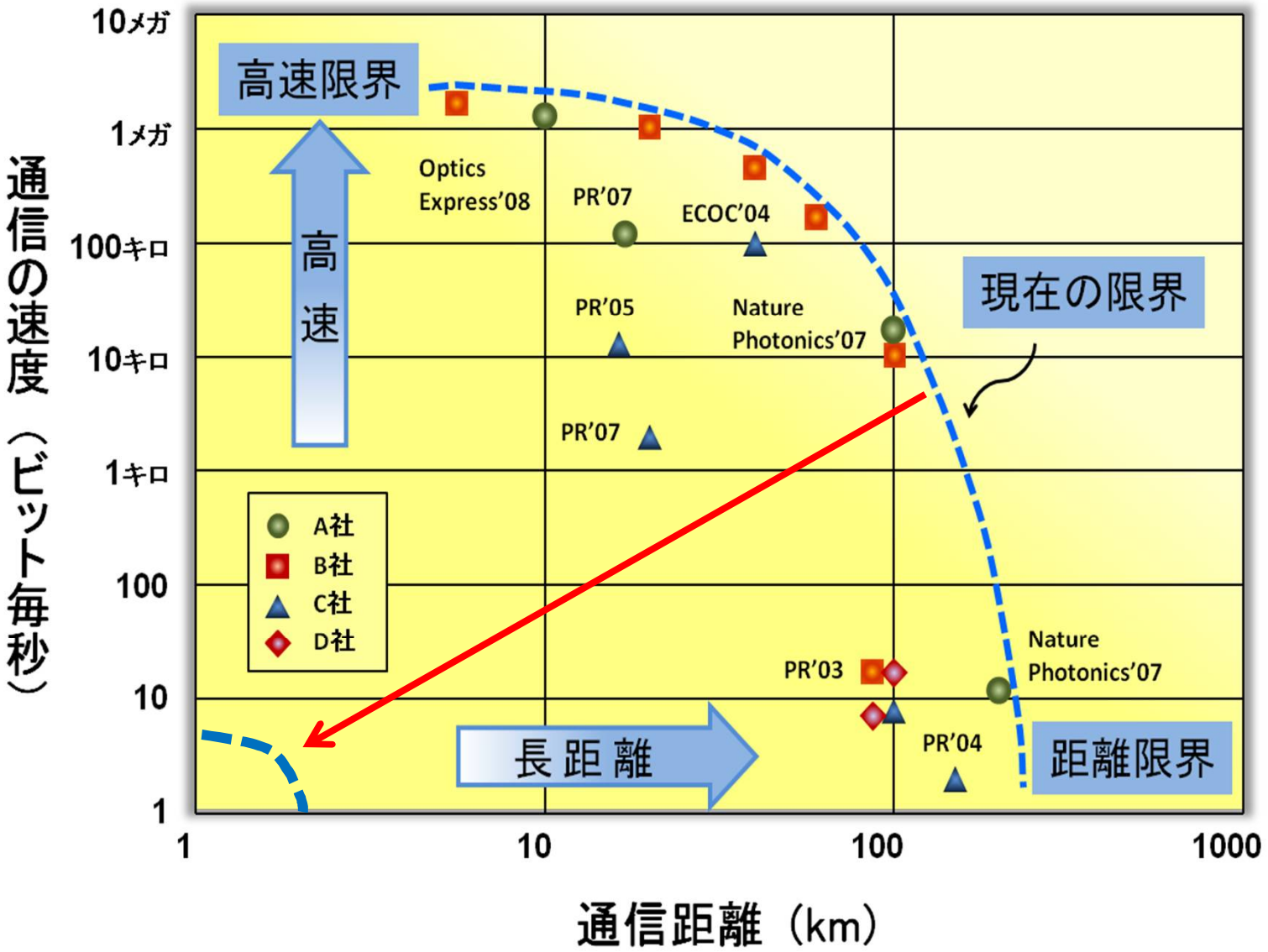
崩壊の法則



重ね合わせが
崩壊して量子
雑音が発生

量子雑音の量が安全性の強さになる

■ BB-84の速度と距離のトレードオフ
（商用化は？）



■ なぜY-00型量子暗号が必要か？

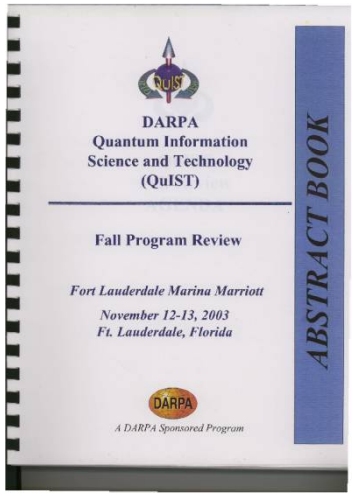
ハイゼンベルグの不確定性原理を応用するBB-84型の
量子暗号は通信性能（距離、情報量）が極端に低く、
さらに安全性は暗号学のShannonの限界まで。

通信速度： 100 Kbit/sec
通信距離： 数十 Km

ボルンの法則を応用するY-00型の量子暗号は通信性能
（距離、情報量）が高く、
さらに安全性は暗号学のShannonの限界を超える。

通信速度： 1 G～10 Gbit/sec
通信距離： 1000Km～1万Km

■ Y-00型量子暗号プロジェクトの経緯



米国防総省支援プログラム・シンポジューム：2003,Nov.
（フロリダ、関係者のみ）

理論検討・原理実験	玉川大特別参加

空軍研究所支援プログラム・シンポジューム：2008，Mar.
（Dayton空軍キャンプ、関係者のみ）

開発状況報告	玉川大招待講演

陸軍研究所ワークショップ（San Diego，公開）：2009,Aug.

開発状況報告	玉川大招待講演

■ 量子エニグマ暗号への進化

Y-00型量子暗号：量子雑音の効果が小さい

量子エニグマ暗号

数学的な暗号を量子現象（物理）で強化する暗号で
暗号学のShannon限界を完全に超越する暗号

O.Hirota and K.Kurosawa,（廣田・黒澤）
Quantum Information Processing, vol-6, no-2, pp81-91, 2007.

Y-00をさらに発展させた構造によって実現可能と
なるが、Y-00は第一世代となる。

■ 量子エニグマ暗号実用化へ

Northwestern大学 (Y-00型)
特徴：高速、長距離、高コスト
G.Borbosa, et al, Physical Review Letters, vol-90, 227901,2003

位相変調方式

連携

連携

強度変調方式

調整中

パルス位置変調方式

モデル装置開発中

玉川大学
日立情報通信エンジニアリング
(Y-00型)
特徴：超高速、長距離、低コスト

O.Hirota, M.Sohma, M.Fuse, K.Kato,
Physical Review A, vol-72, 22335,2005

MIT (量子ロッキング型)
特徴：低速、中距離、中コスト
S. Lloyd, Nature, to be submitted , 2013
arXiv:1307.0380v1[quant-ph], July 2013.

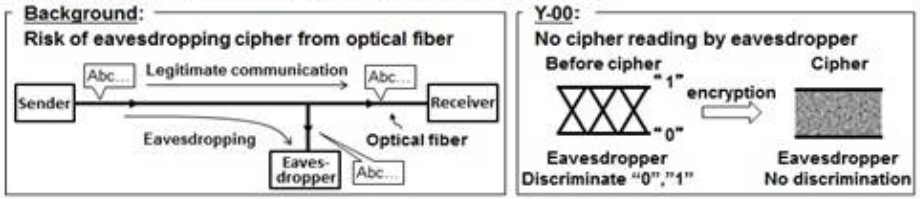
■ 世界最高性能を達成

二見史生　教授
東京大学工学部、大学院(博士)を経て
富士通入社、富士通研究所において
超高速光通信の研究に従事。博士（工学）
平成23年より現職

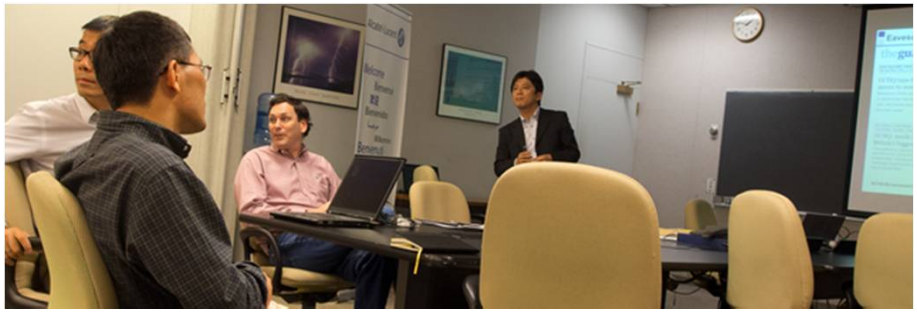
PHYS.ORG

The world's fastest Y-00 stream cipher transmission at 40 Gbit/sec over 120 km

March 6th, 2012 in Physics / Optics & Photonics



Fumio Futami at Tamagawa University, Quantum ICT Research Institute, announced the world first transmission of the stream cipher by Yuen 2000 protocol (Y-00) at the bit rate of 40 Gbit/sec over 120 km.



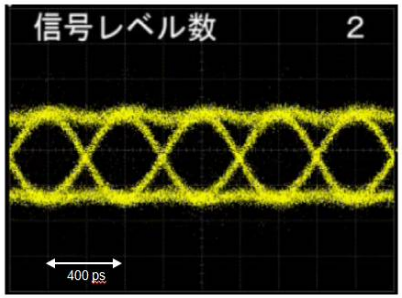
2012年

米国研究所での
招待討論会

2013年

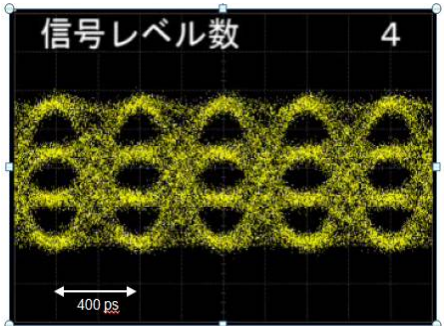
■ 量子エニグマ暗号の安全性保証

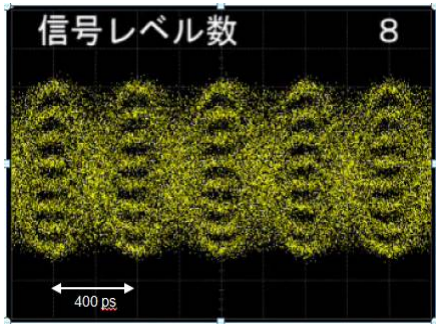
２値情報信号

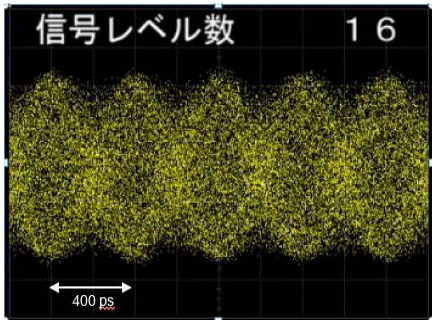


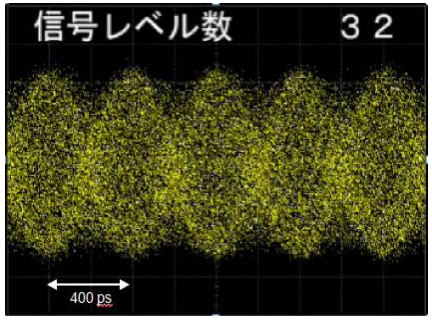
通信速度： 1 Gbit/sec
～40 Gbit/sec

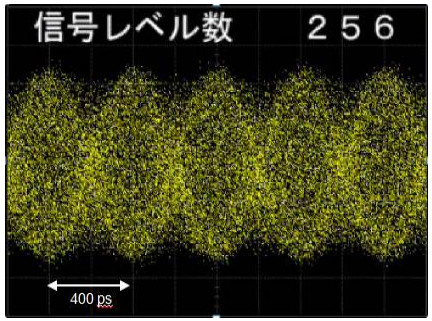
暗号化信号
（盗聴者の
受信信号）：
暗号化強度＝
信号レベル数

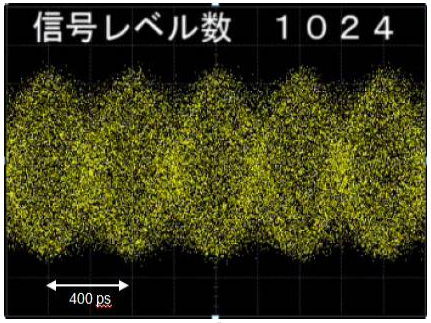


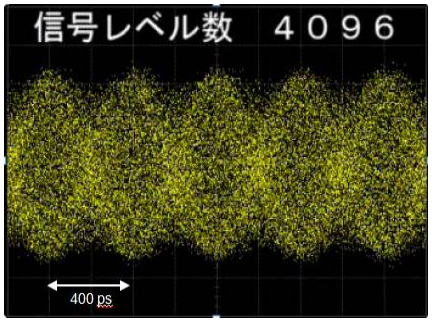






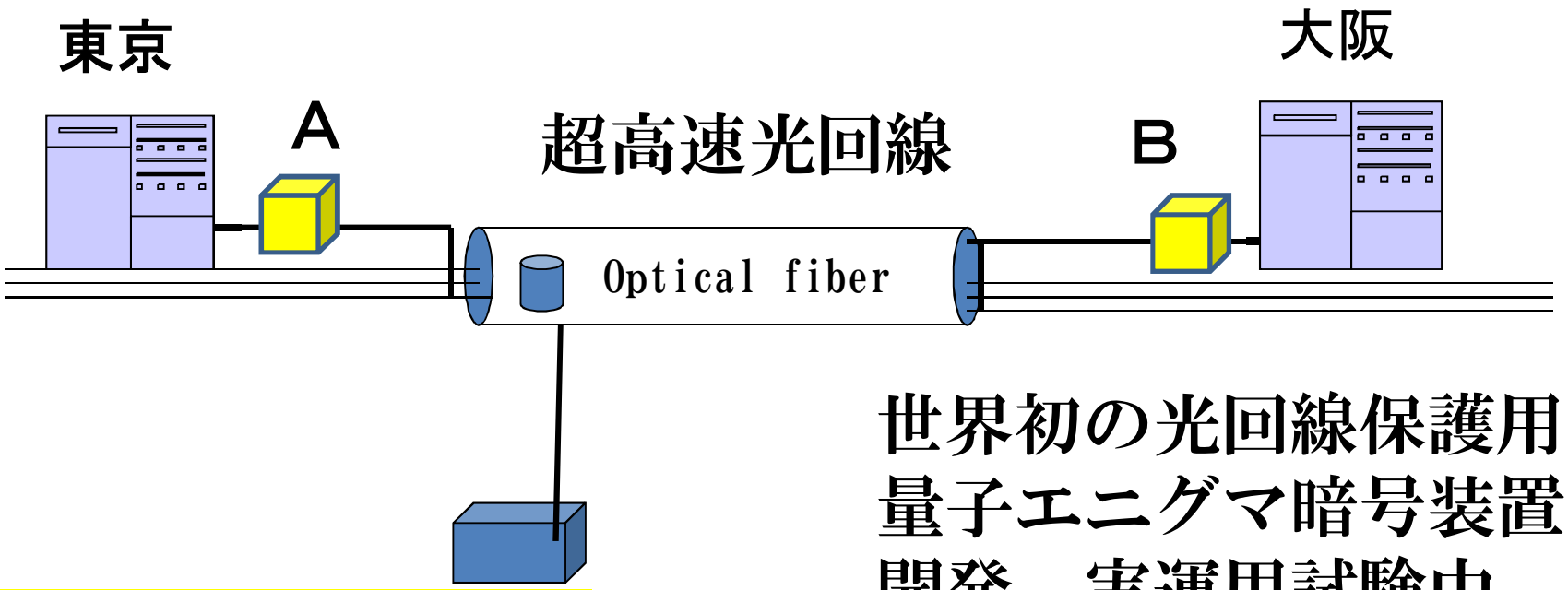






多値に分散された通信文や鍵情報が受信時の
量子雑音によって完全乱数に変換される

■ 量子エニグマ暗号（Y-00型）実装イメージ



光回線からの盗聴技術が急速に発達

防御

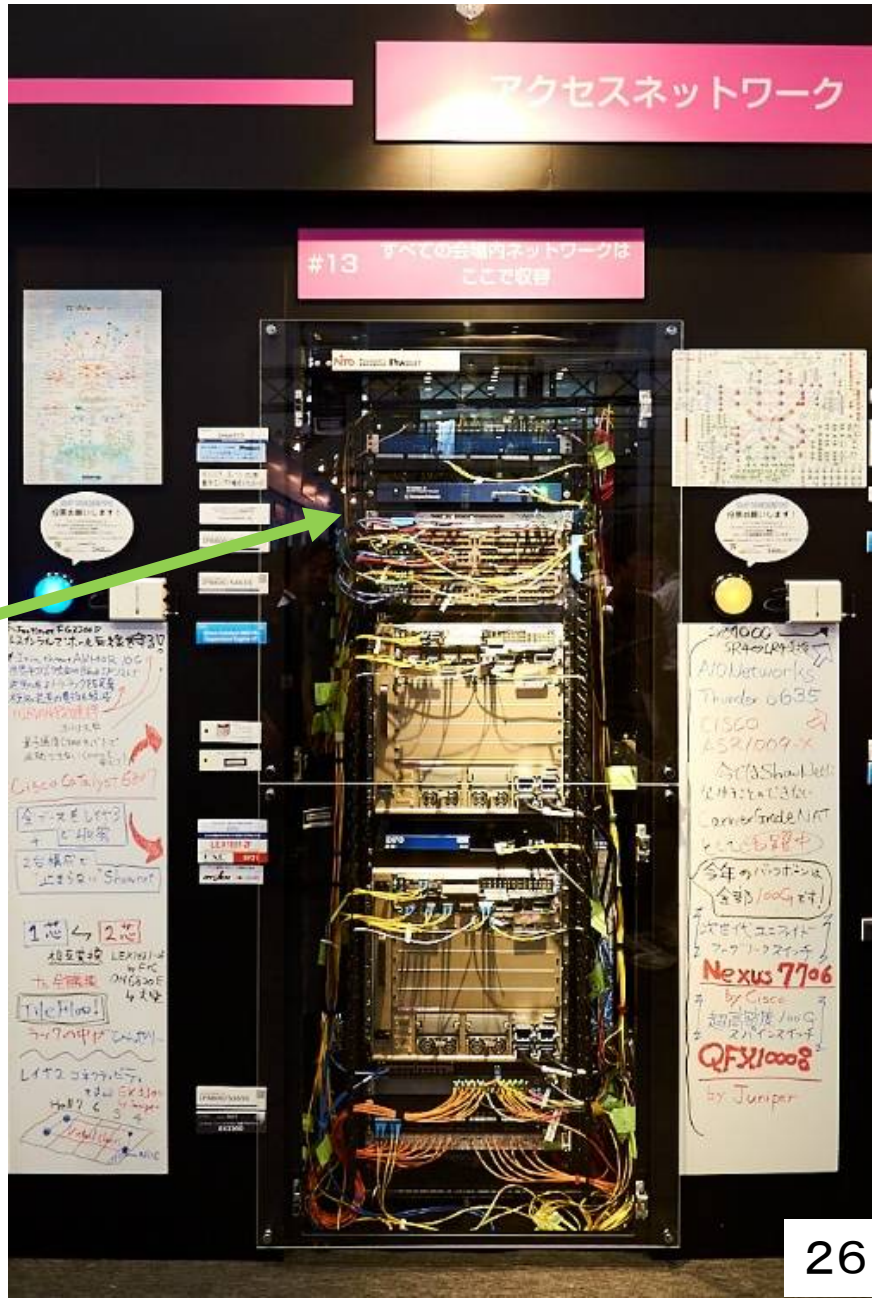
世界初の光回線保護用量子エニグマ暗号装置を開発、実運用試験中

ＡとＢに上記装置を設置するだけで情報の漏えい・改ざんを完全に阻止

Interop Tokyo 2016 アワード
ファイナリスト（幕張メッセ）

二見史生　教授
加藤研太郎　教授

量子エニグマ暗号トランシーバ
TU Cipher-0
1 Gbit/sec Ethernet対応機
（動態展示）

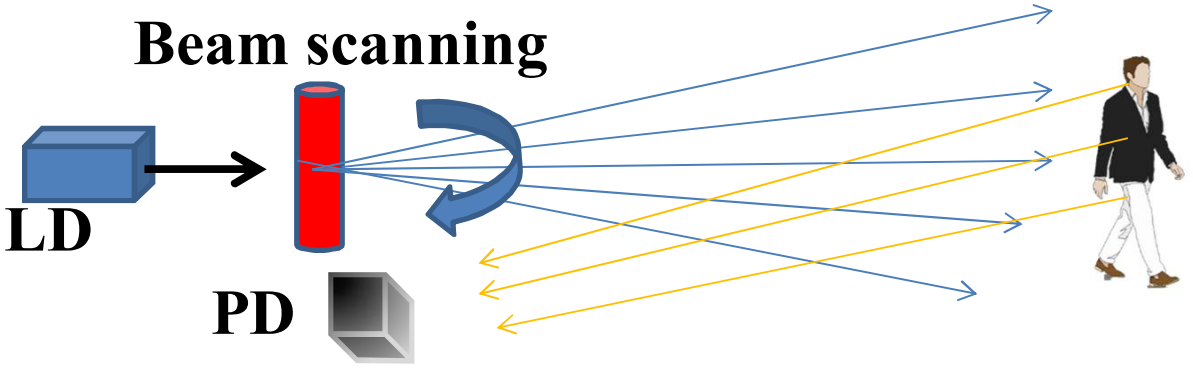


3部

全天候対応の量子レーダーカメラ

自動車用イメージセンサーの既存技術

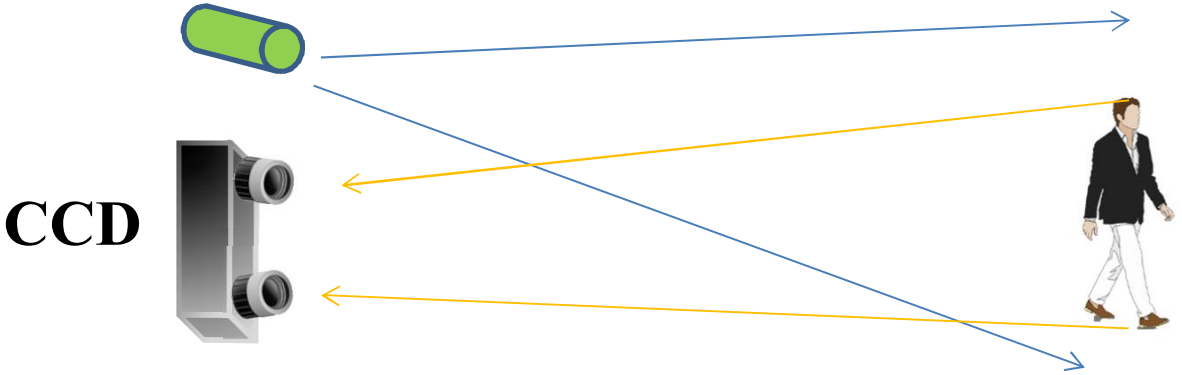
◆ **Lidar** (light detection and ranging system)



Low resolution
（低分解能）

◆ **Stereo Camera**

Head light (Halogen lamp, LED, et al)

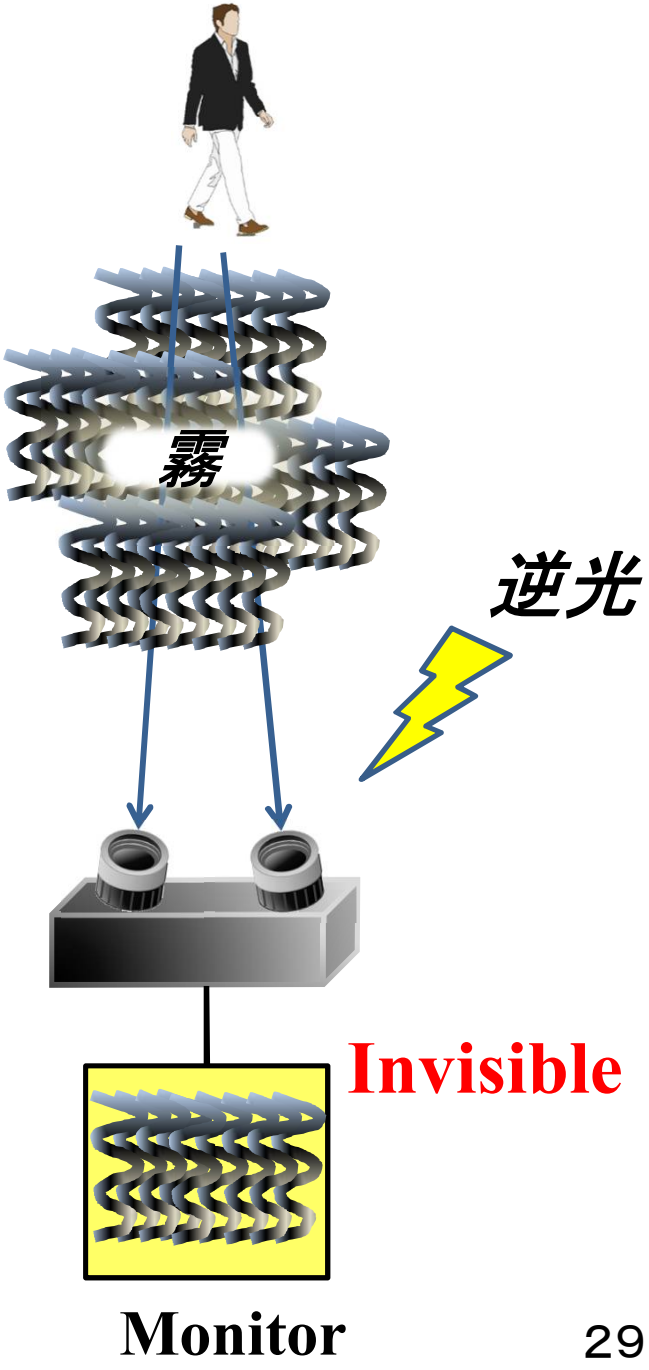


High resolution
（高分解能）

◆ステレオカメラの欠点

霧の中での自動運転の実験から
カメラでは歩行者の検出が難しい
ことが報告されている。

霧の中での自動運転
実験動画



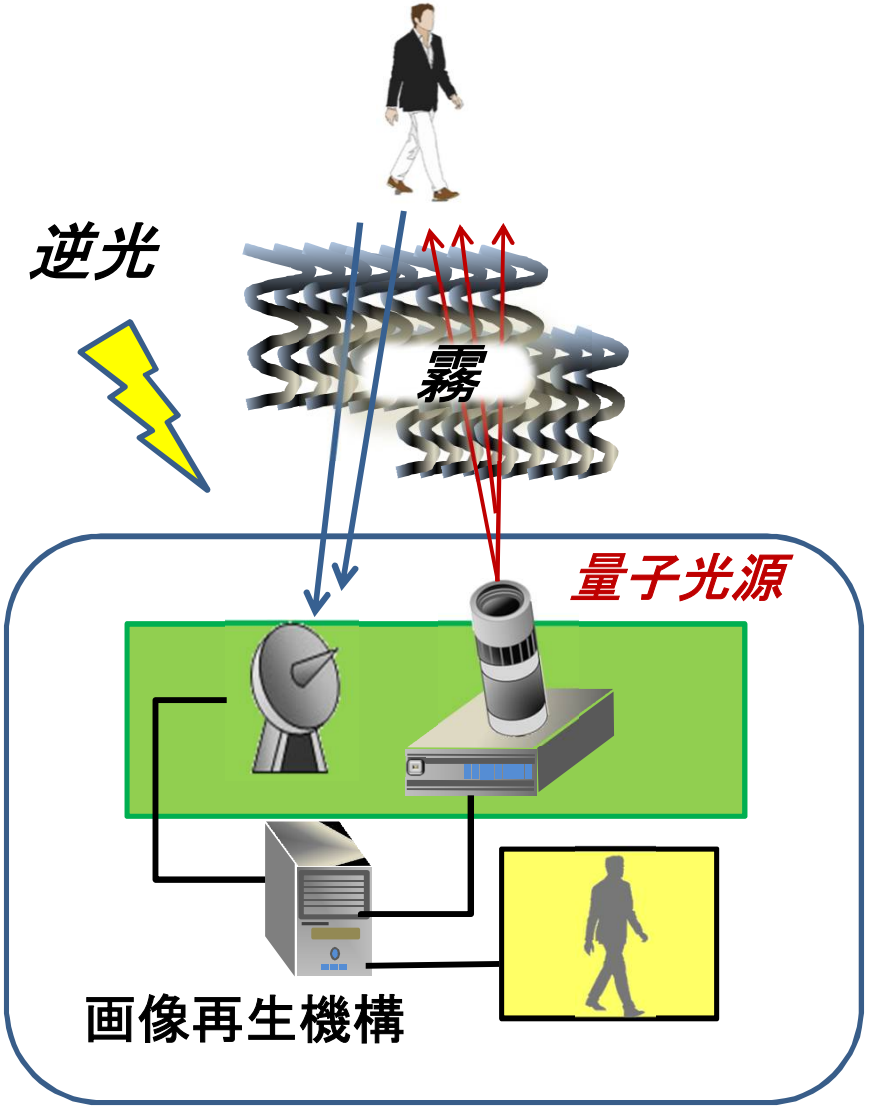
自動運転用量子レーダーカメラの開発

既存技術であるステレオ
カメラやレーダーでは
霧や逆光時に歩行者の
検知が困難

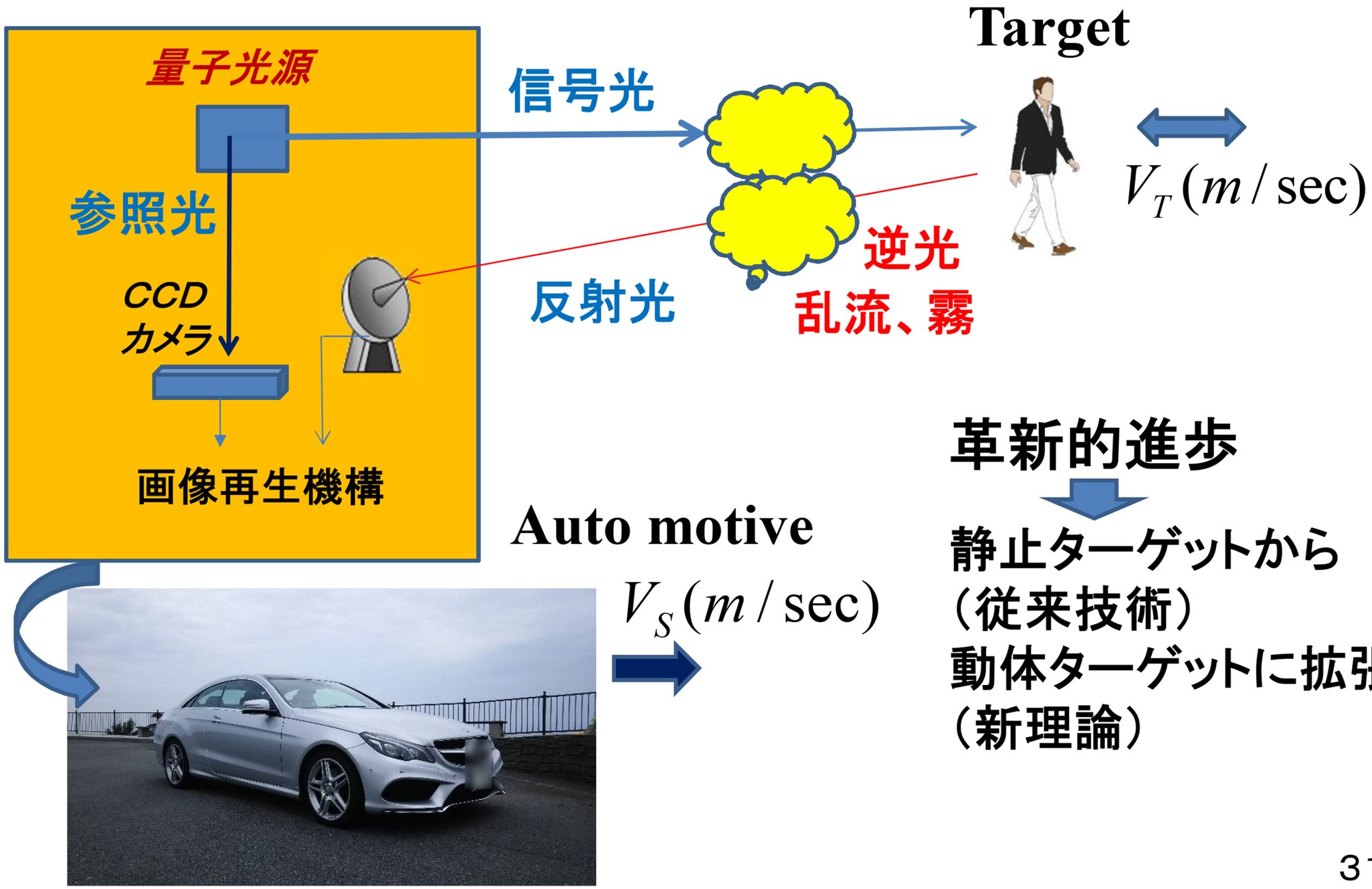
量子効果を応用して
如何なる悪天候時でも
歩行者などを捕捉する
量子レーダーカメラの
設計法を確立

モデル機作成に挑戦中

小糸製作所、日立製作所



■ 量子レーダーカメラの構成モデル



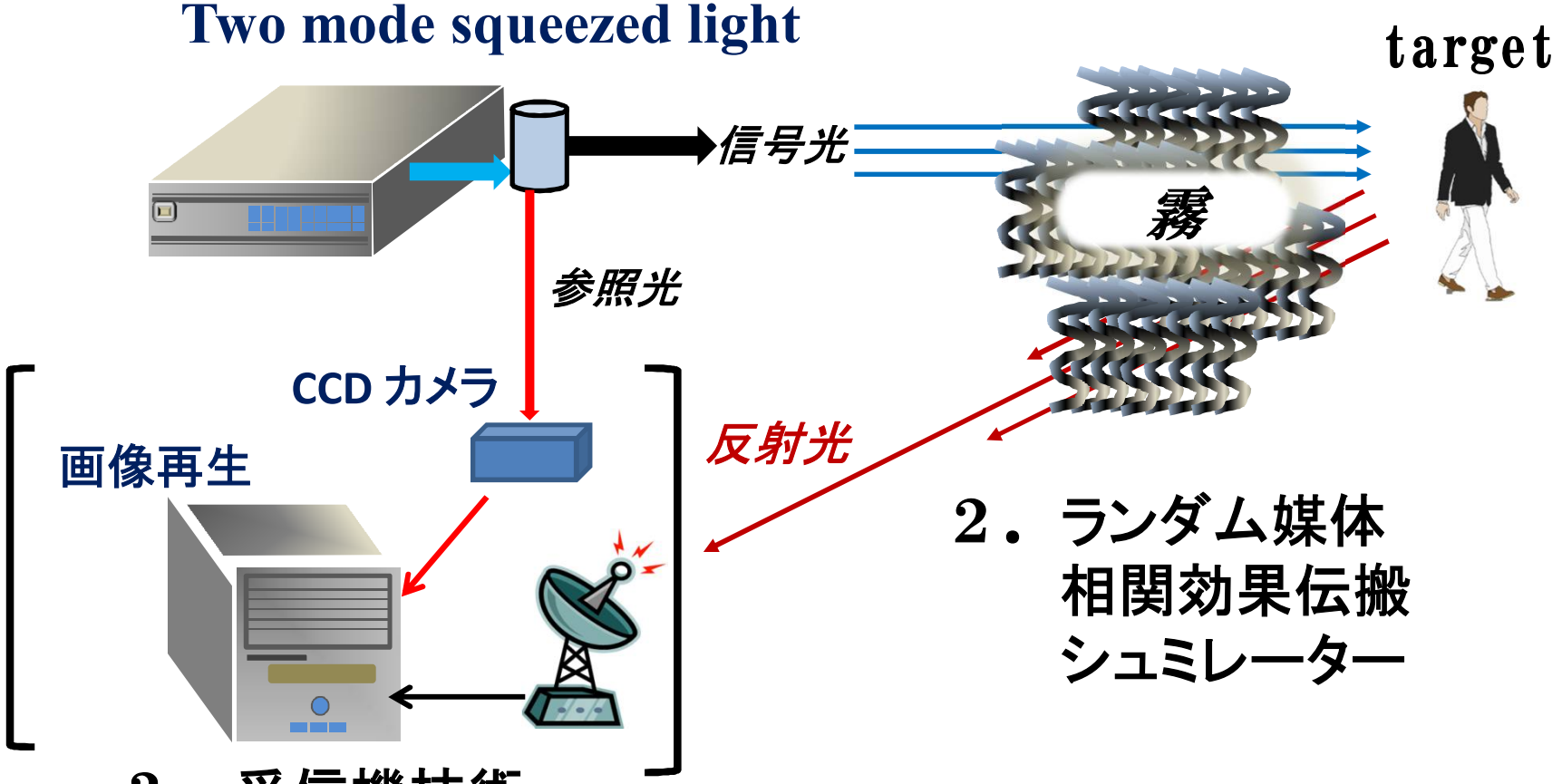
革新的進歩

静止ターゲットから
（従来技術）
動体ターゲットに拡張
（新理論）

■ 量子レーダーカメラの基盤技術

1．量子光源

Two mode squeezed light



2．ランダム媒体
相関効果伝搬
シュミレーター

3．受信機技術

Quantum Wiener Receiver

■ 出口と展開可能性

- 各種レーダー・人工知能との融合を経て、全天候対応の自動運転車の実現や超高感度監視カメラ実現に貢献

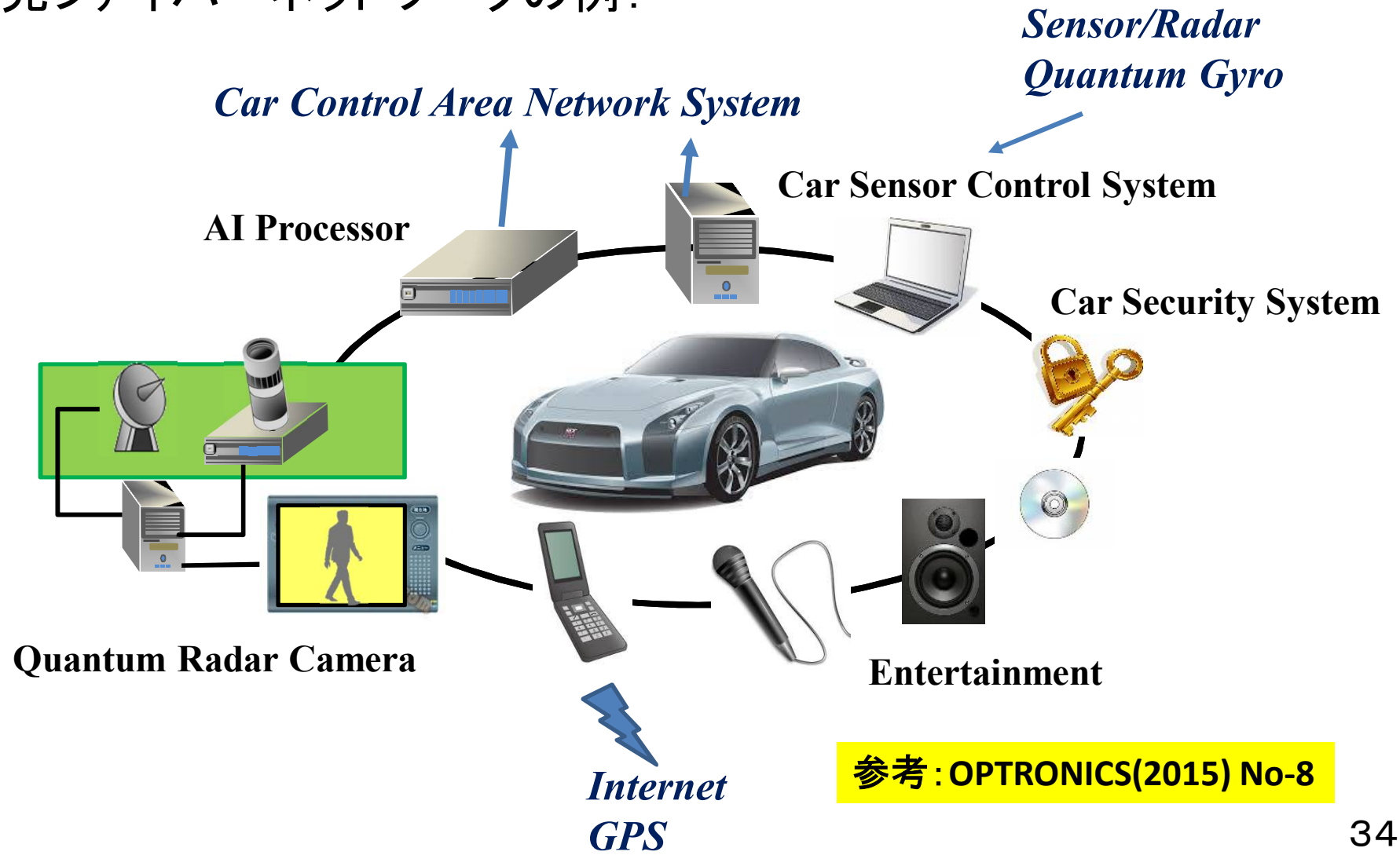
装着イメージ

2020年～2030年

- 日本の本技術を世界標準化
- 小型化と量産化：市場は1兆円規模
（日立製作所試算）

◆ 車内の高速ネットワークの開発と連携し,さらなる進化

1 *Gbit/sec*～10 *Gbit/sec*対応の車内インフラ用
光ファイバーネットワークの例:



参考:OPTRONICS(2015) No-8

むすび

今後も、量子情報科学の知見を戦略的に
社会に役立つ科学技術として提供できるよう
精進してまいります。

本日は、ご清聴いただき心より御礼申し上げます