

資料2  
科学技術・学術審議会  
戦略的基礎研究部会  
数学イノベーション委員会  
(第25回) H28.1.20

# 数学イノベーションに必要な人材について

2016年 1月20日

顧問 堤 和彦

# 内 容

1. 三菱電機グループの概要
2. 三菱電機成長戦略の基本
3. 当社の数学科出身者の活躍先
4. 数学系出身者の開発本部内での活躍
5. 企業人から見て数学科学生が学生時代に学ぶべきこと

# 1.三菱電機グループの概要

設立 1921年1月15日  
従業員数 129,249人  
資本金 1,758億円 (2015年3月末現在)

## 情報通信システム



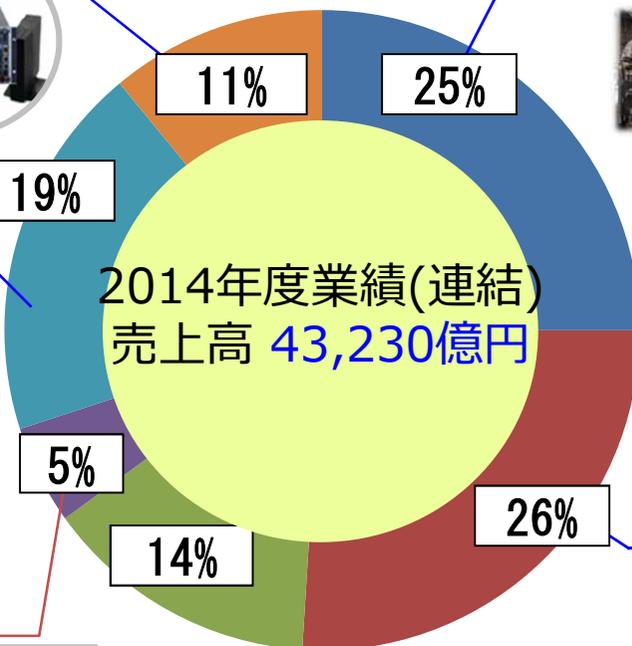
## 重電システム



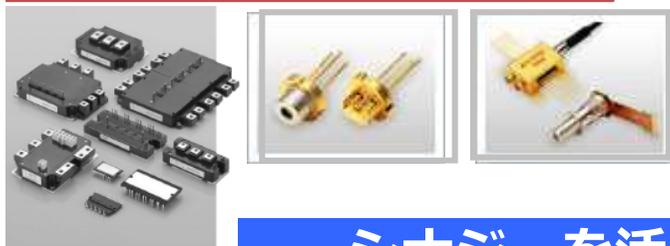
## 家庭電器



2014年度業績(連結)  
売上高 43,230億円



## 電子デバイス



## その他

2014年度のセグメント別  
売上高比率 (2015年4月)

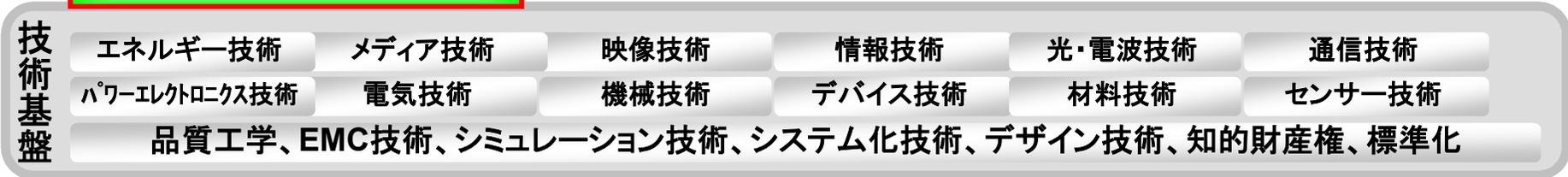
## 産業メカトロニクス



シナジーを活かした強い電機・電子事業の複合体

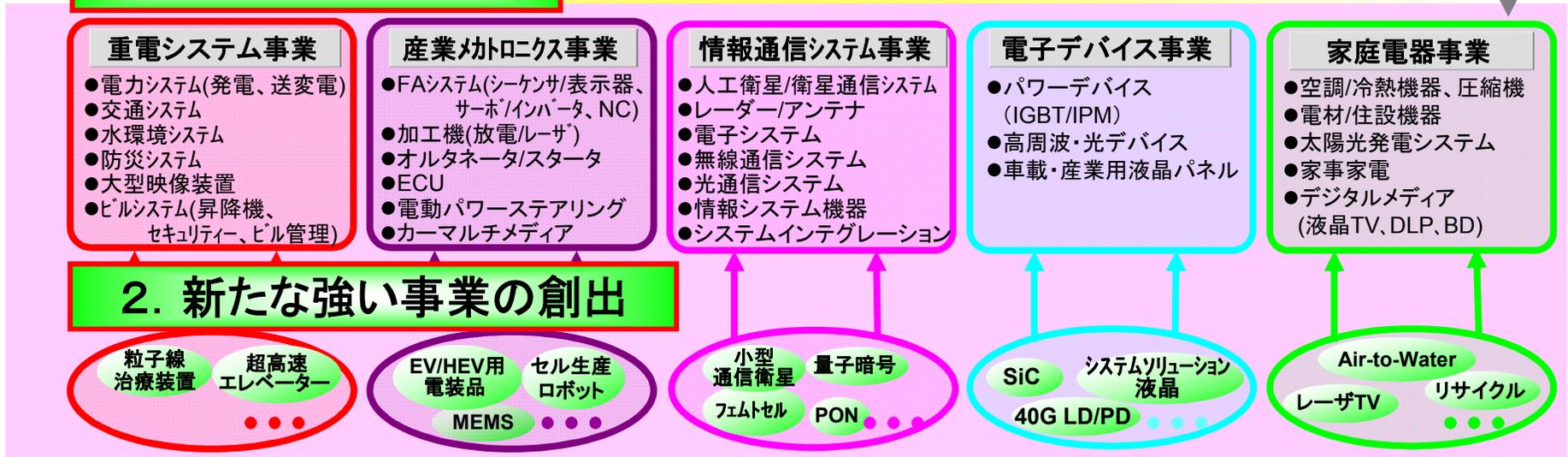
## 2. 三菱電機成長戦略の基本

### 3. 技術基盤の強化



### 1. 強い事業をより強く

技術シナジーによる製品競争力強化



### 2. 新たな強い事業の創出



製品シナジーによるソリューション事業創出

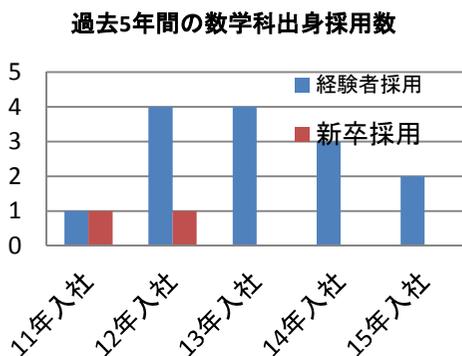


EMC: Electro-Magnetic Compatibility, NC: Numeric Controller, ECU: Engine Control Unit, DLP: Digital Light Processing, BD: Blu-ray Disc  
EV/HEV: Electric Vehicle/Hybrid Electric Vehicle, MEMS: Micro Electro Mechanical Systems, PON: Passive Optical Network, SiC: Silicon Carbide, LD/PD: Laser Diode/Photo Diode,

# 3. 当社の数学科出身者の活躍先

**取締役会**  
取締役会長  
指名委員会  
監査委員会  
報酬委員会

**執行役（会議）**  
執行役社長  
専務執行役  
常務執行役



## 4. 数学系出身者の開発本部内での活躍



- 1987年 三菱電機(株)入社 研究所に配属  
符号理論、暗号理論の研究開発に従事
- 1993年 新暗号解読手法「線形解読法」発表
- 1994年 米国標準暗号(当時)DESの世界初の解読  
実験に成功
- 1995年 ブロック暗号アルゴリズムMISTY発表
- 1999年 欧州にて第三代携帯電話W-CDMAの標準  
暗号設計に従事
- 2003年 第35回市村産業賞 本賞受賞  
平成14年度情報処理学会 業績賞受賞  
平成14年度電子情報通信学会 業績賞受賞
- 2004年 平成16年度発明協会 全国発明表彰  
恩賜発明賞受賞
- 2005年 情報セキュリティ技術部 部長
- 2006年 平成17年度情報処理学会 業績賞受賞  
第2回情報セキュリティ文化賞受賞
- 2008年 第53回前島賞受賞
- 2013年 この年より現職(松井暗号プロジェクトG)

### ■ 暗号に興味を持ったきっかけ

- 1990年に海外で暗号解読論文が発表、それまで解読困難と思われていたいくつかの暗号が解読できるということが示されていた。
- この結果が当時センセーショナルに伝えられたため、興味を持った。
- どんな難しい内容かと思って読んでみると当たり前の発想がそこに書いてあった。
- 当たり前のことをこつこつ積み上げてすごい高さまで到達していた。
- これに驚いて、方法論は簡単なのだから自分にも真似できるのではないかと、他の暗号の解読をやってみたところから暗号技術との関わりが始まった。

## 4. 数学系出身者の開発本部内での活躍

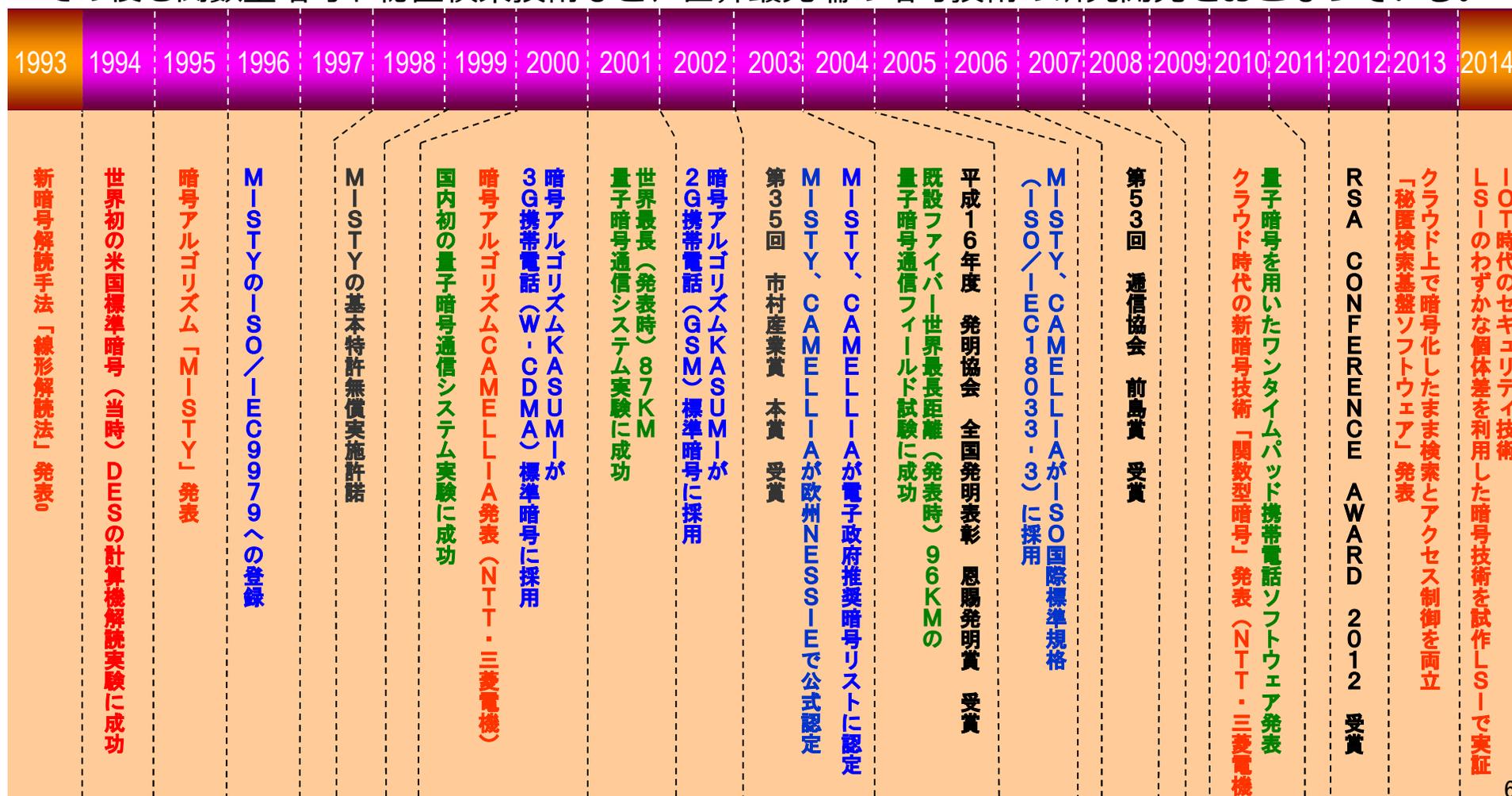
### 三菱電機の暗号技術 20年間の歩み

三菱電機の暗号技術は1993年「線形解読法」の発明にはじまった。

1995年発表の暗号アルゴリズム「MISTY」は2004年に全国発明表彰恩賜発明賞を受賞。

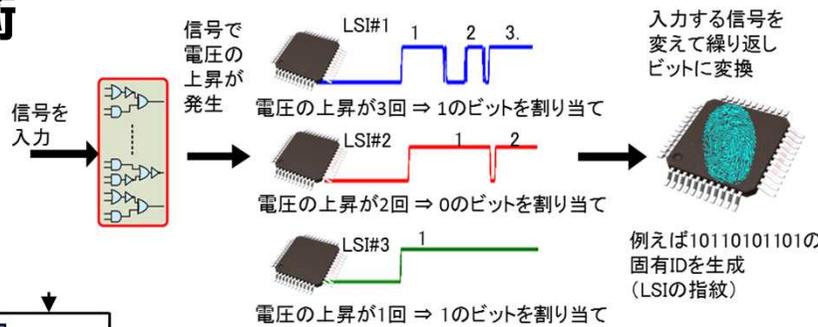
2005年にはISOの国際標準暗号となった。

その後も関数型暗号や秘匿検索技術など、世界最先端の暗号技術の研究開発をおこなっている。



# 4. 数学系出身者の開発本部内での活躍

## ■ 世界標準暗号技術



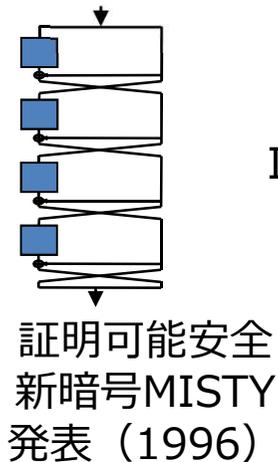
IoT時代に向けた  
セキュリティ技術 (2015)

**LSIの指紋 (PUF)**

**秘匿検索 (検索可能暗号)**

クラウドで機密情報を  
暗号化したまま検索 (2013)

MISTY  
ISO標準採用 (2005)  
**世界標準**



**MISTY暗号**

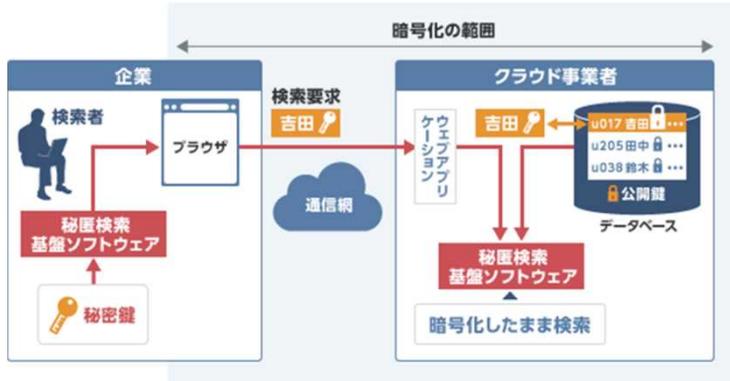


WCDMA携帯電話  
国際標準採用 (1999)  
GSM携帯電話  
国際標準採用 (2002)



米国標準 (当時) 暗号  
DESを世界で初めて  
解読に成功 (1994)

**線形解読法**



### 問1：数学科出身であったことや数学がバックグラウンドにあったことで入社後役に立った事は何か？

- ① 暗号の研究開発では、直接的に数学が役立つ。暗号の安全性を  
保証する技術は、数学の証明を行うことと同様であり、数学的な  
知識や思考法を身に付けて初めて正しく論証することが可能となる。
- ② 論理的にものを考える習慣が身に付いているため常識に囚われ  
ずもの事を進めることができた。
- ③ 数学的な基礎を有していたため、入社後に必要な通信や電気・  
電子工学の基礎を容易に習得できた。

### 問2：大学時代に数学以外で勉強しておいたら良かったことは何か？

- ① 「英語」 グローバル化に伴い英語は必須。
- ② 「物理」 物理現象を正しく捉えて、それを数式化して設計、開発につなげることが出来ると数学知識がより使える。
- ③ 電機メーカーに入社する前提であれば、電気・電子工学や計算機分野への応用的理論等。

### 問3：企業の立場から、今の数学科の学生が学生時代に学ぶべきことは何か？

- ① 「コミュニケーション」 数学は個人プレーの側面が大きいが、仕事はチームで行うことが多いため、サークル・ボランティア等で多様な価値観の人達との人付き合いの経験を積んでおくと良い。
- ② 「応用的な数学に触れる機会増」 様々な科学・技術の知識と数学の応用的な側面を勉強しておく入社後に役立つ。

