Building Secure e-Government & Cryptography

通産省機械情報産業局情報セキュリティ政策室
Office of IT Security Policy, MITI, Japan

情報セキュリティ政策（3つのアプローチ）
(Three approaches for Secure Cyber Space)

1　セキュアな基盤構築（Building Secure Infrastructure）

- 技術開発（Development of Protection Techniques）
- 制度・規制（Institutions/Regulations）
- マネジメント・ガイドライン(Guidelines/Management)
- 人材開発(Management/Human Resources)

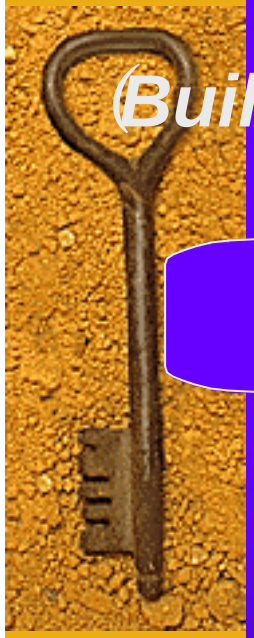
2　実施支援(Application/Implementation)

- 政策的支援(Gov. Assistance)
- 情報分析・提供(Info. Analysis/Sharing)
- 普及・啓発(Awareness/Education/Training)
- ベストプラクティス(Best Practices)

3　調和／互換性(Harmonization/Interoperability)

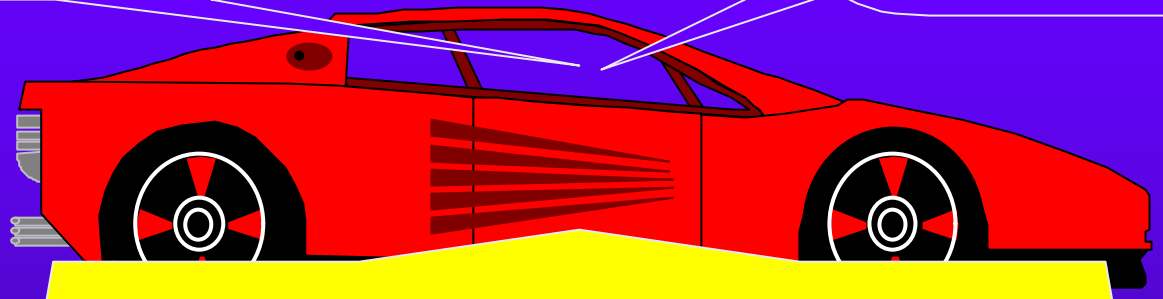
- キャッチアップ（Catch up)
- 標準化(Standardization)
- 国際協力(Int'l Cooperation)

技術・製品に関する信頼の確立
（Building Confidence on Technologies & Products）



セキュリティ管理
【Management】

人材
【Personnel】



技術&製品：Technologies & Products

技術／製品の客観評価による信頼の確立
【Building Confidence by IT Products Evaluation】
ex. ISO/IEC15408, FIPS140-1/2, NIST/AES

セキュアな電子政府の構築
(Building Secure e-Government)

1　技術開発(Development of Technologies)

不正アクセス・ウィルス対策、侵入検知システム、暗号技術・認証等々

(Anti- Hacking/Virus, IDS, Encryption/Authentication etc.)

2　実装(Application)

-セキュリティ水準の高い製品の利用

Use of Evaluated IT Products : ISO/IEC15408, FIPS140-1,2

- 暗号アルゴリズム評価（暗号技術評価委員会：座長東大今井教授)

Cryptrec, Chaired by Prof. Imai, University of Tokyo

- 政府の利用方針(Government-Wide Use Policy)

3　セキュリティ管理(Security Management)

- 情報セキュリティポリシーガイドライン

The Guidelines for IT Security Policy Development for Gov.

ベスト・プラクティス(Best Practices)

暗号政策と今後の課題
(Crypto Policy & Challenges)

1　OECD暗号政策ガイドライン（1997年）
OECD Guidelines for Cryptography Policy (1997)

2　暗号の民生利用の促進と開発の推進
Promotion of the Use of Crypto & Development of Related Technologies

3　暗号評価の推進（技術革新、電子署名、暗号モジュール）
Promotion of Crypto Evaluation (Tech. Innovation, D/S, Crypto Module)

4　互換性、標準化と技術的中立性
Interoperability, Standardization & Technical Neutrality