世界の暗号標準化活動:
AESの活動について

（株）東芝　研究開発センター
川村 信一

世界の暗号標準化活動

- AES（97~2001）
  - 米国NIST、2000年10月選定終了。FIPS出版待
    NIST=National Institute of Standards and Technology
- CRYPTREC(2000~　)
  - 日本、電子政府での利用に耐える方式の評価
- NESSIE（2000~　）
  - 欧州域内の利用を目指した評価選定Pj
- ISO（1999~　）
  - 国際規格の制定…暗号アルゴリズムにも着手

AESのねらいと背景

- DES方式に代わる共通鍵ブロック暗号アルゴリズムをFIPSとして制定

  FIPS=Federal Information Processing Standards
- DES仕様（64ビットブロック/56ビット鍵暗号）の寿命　→当面トリプルDESで対応
- 今後20-30年利用可能な安全性・処理効率の高い新方式
  - ブロック長：128ビット、鍵長：128／192／256ビット
  - トリプルDESよりも安全で高速
  - ロイアリティフリー

AES選定スケジュール

- 97/01　AES選定構想発表
- 97/04 公聴会
- 97/09-98/06 方式公募
- AES1（98/08）、同2（99/03）、同3（00/04）
- 00/10 RijndaelをAES候補に選定
- 01/02E-5E　FIPSドラフト公表とコメント募集
- 01/06以降　FIPS発行

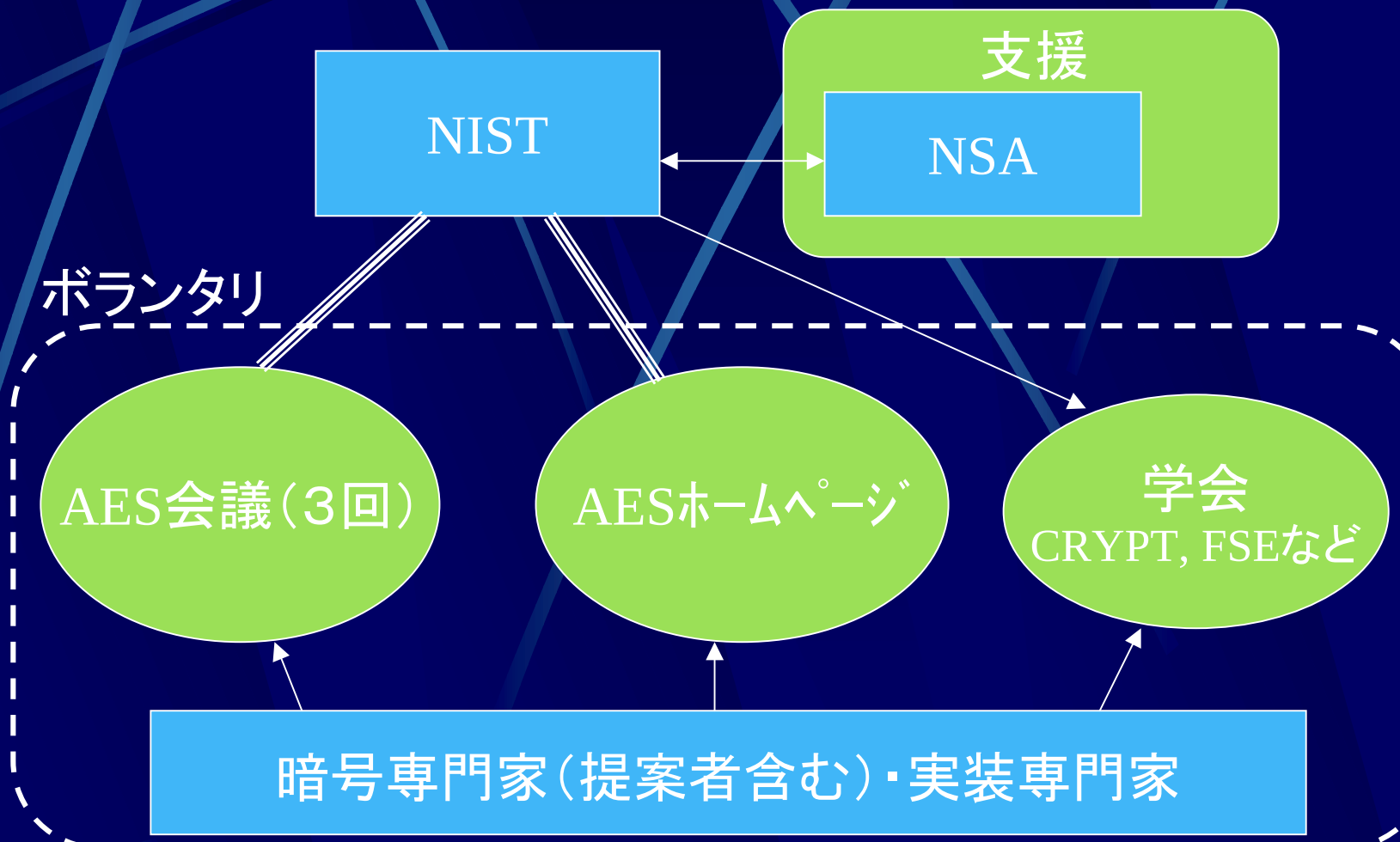
現在

候補絞り込み

- 第1段階：　書類審査
  - 21方式　→　15方式
- 第2段階：　ラウンド1（約1年）
  - 15方式　→　5方式（ファイナリスト）

    MARS、RC6、Rijndael、Serpent、Twofish
- 第3段階：　ラウンド2（約1年）
  - 5方式　→　1方式（ウィナー）

評価体制

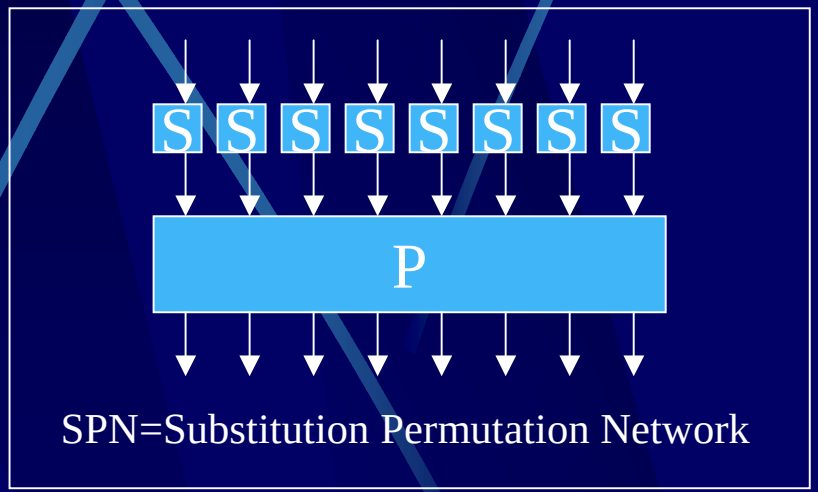

支援
NIST
NSA
ボランタリ
AES会議（3回）
AESホームページ
学会
CRYPT, FSEなど
暗号専門家（提案者含む）・実装専門家

評価項目

- 安全性
  - 各種の攻撃への耐性の評価
- 実装性
  - 各種CPUでのSW（C,Java,…）実装性
    - 32ビット、8ビット、64ビット
    - 処理速度、プログラム／ワークサイズ
  - HW実装性
    - ゲート規模、処理速度

Rijndaelの特色

- SPN構造
  - 差分･線形攻撃耐性
  - 処理の並列度が高い



- 処理単位は8ビット
  - S-Boxだけでなく P層も
  - 8ビット~64ビットまで幅広いプラットフォーム上で高速

AES選定プロセスの特色

- ゴールの明示
  - 公募時に方針とゴールが明確に示されたこと
- 透明性
  - 評価プロセスをできる限りあらゆる人に見える形にしたこと
- 一貫性
  - 既定の方針を全くたがえなかったこと
- 公正さ
  - 方式が公正な判断の下に選ばれたと信じられること

むすび

- AES候補としてRijndaelが選定され、FIPS出版待ち
- AES選定プロセスに対する専門家の評価は高い
- DES同様に世界に普及するのか、今後が注目される