日米欧の暗号技術標準化・評価プロジェクトを終えて

― 実績と今後の展望 ―

NTT 情報流通プラットフォーム研究所
神田 雅透
kanda@isl.ntt.co.jp

暗号アルゴリズム標準化への流れ

1970年代　現代暗号の幕開け

1977年 米国政府標準暗号DES制定

1980年代　DES全盛期

暗号アルゴリズムは軍事用武器の一種

- 厳しい輸出規制
- ISO国際標準化見送り

1990年代　暗号アルゴリズムの氾濫期

- DESの安全性低下傾向が顕著
  DES Challenge III (1999): 22時間15分で鍵全数探索攻撃成功
- ネットワークセキュリティ・暗号への関心の高まり
- セキュリティ製品のアピール手段

2000年代　客観的評価による暗号標準化

- 日米欧での暗号技術標準化・評価プロジェクトの実施
- ISO/IEC国際標準暗号策定

暗号技術標準化・評価プロジェクト

- AESプロジェクト（米国：1997.1 – 2001.11）
  - Advanced Encryption Standard
  - 米国政府**標準**暗号を策定
- NESSIEプロジェクト（欧州：2000.1 – 2003.3）
  - New European Schemes for Signature, Integrity and Encryption
  - 欧州産業**推薦**暗号を選抜
- CRYPTRECプロジェクト（日本：2000.5 – 2003.3）
  - Cryptograpy Research & Evaluation Committees
  - 電子政府**推奨**暗号をリスト化
- ISO/IEC国際標準暗号（1999.12 – in progress）
  - 産業国際**標準**暗号を策定

各プロジェクトの概要

AESプロジェクトの概要

1997年1月　NISTはAESプロジェクトの開催を宣言

- DESに替わる**新米国政府標準暗号**AESを策定
  - センシティブ情報を取り扱う全連邦政府システムに対する強制利用対象暗号の一つ
  - 民間システムでは自発的な採用を推奨
  - 世界中から候補暗号を公募
  - 一般のユーザ、暗号研究者、産業界、標準化団体、政府関係者らの参加した開かれた選考プロセス
- **米国政府の施策**としてNISTの責任下で実施
  - NIST内部に「運営チーム」「技術検討チーム」を組織
  - NSAが技術的サポート
  - 法的根拠に基づくプロジェクト
    - 1987年コンピュータセキュリティ法
    - 1996年情報技術管理改革法
    - 大統領令13011号

AESプロジェクトの公募要綱

1997年9月　AES候補暗号の公募要綱を公開

〔仕様に関する事項〕

- ブロック長128ビット、鍵長128・192・256ビット
- 仕様が完全に公開
- Triple DESよりも安全かつ非常に効率性が改善
- 世界中でロイヤリティフリーで利用可能
- 設計方針や安全性自己評価を記した補助文書を提出
- 参照コードと最適化コードを提出

〔選定に関する事項〕

- 原則として、一つの公募暗号を選定
- 評価・選抜基準は、(1)安全性、(2)実装性能、(3)その他の特長、の順で考慮
- 2段階評価・選抜方式
- 1998年までに選定を終える必要はない

AESプロジェクトの推移

1997年 1月 AESプロジェクト開始を宣言
4月 AESワークショップ開催
9月 公募要綱公開
1998年 6月 公募締切

8月 第1回AES候補会議開催
12月 (FIPS46-2 DESの承認切れ)
1999年 3月 第2回AES候補会議開催 (ローマ)
4月 第1次評価コメント募集締切
8月 最終候補選抜・発表
2000年 4月 第3回AES候補会議開催
5月 第2次評価コメント募集締切
10月 Proposed AESとしてRijndaelを選定

2001年 2月 AESのFIPS化作業開始
11月 FIPS197 AES正式発効

公募要綱を議論

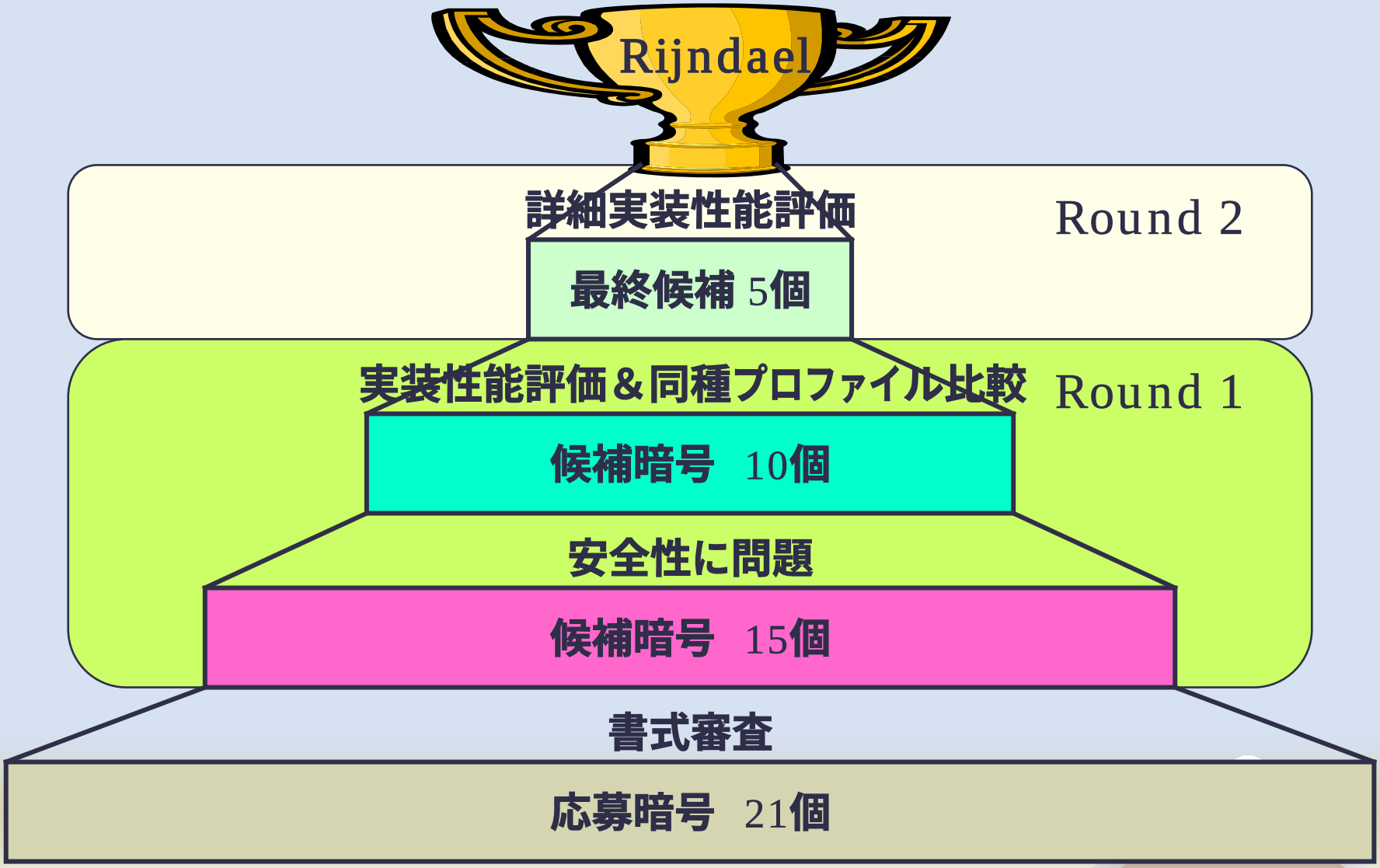
公募期間

Round 1

米国外で開催

Round 2

AESプロジェクトでの選定



NESSIEプロジェクトの概要

2000年1月　NESSIEプロジェクトの開催を宣言

- 安全かつ強力な**暗号技術推薦リスト**を選定
  - 暗号技術分野における**欧州産業界**の国際競争力強化および研究開発能力の優位性維持
  - 欧州産業界をはじめとする各種標準化への合意形成促進
  - AESプロジェクトへの**欧州の立場**からの寄与
  - 世界中から候補暗号を公募
  - 透明で開かれた選考プロセス
- EU傘下の欧州委員会策定の**第5次情報社会技術研究開発プロジェクトの一環**として実施
  - EUからは運営資金の拠出のみ
  - 欧州の大学に所属する暗号研究者中心の「技術運営チーム」と欧州のセキュリティ関連企業中心の「インダストリボード」を組織

NISSIEプロジェクトの公募要綱

2000年3月 NESSIE候補暗号の公募要綱を公開

- 基本的にはAESプロジェクトの公募要綱に準じる

〔AESプロジェクトと異なる主な事項〕

- 募集カテゴリ
  - ブロック暗号 (Normal-Legacy, Normal, High)
  - ストリーム暗号 (Normal, High)
  - メッセージ認証子 (Normal, High)
  - ハッシュ関数 (Normal, High)
  - 擬似乱数生成系 (Normal, High)
  - 公開鍵暗号
  - デジタル署名
  - 公開鍵認証方式
- 原則として各カテゴリ**二、三個**の暗号技術を選抜
- ロイヤリティフリーで利用できることが**望ましい**
- ICカードでの実装性能を重要視

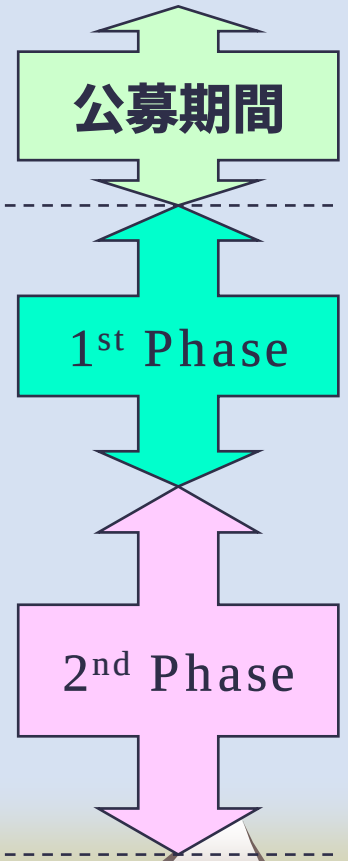
AESはこのカテゴリに該当

NESSIEプロジェクトの推移

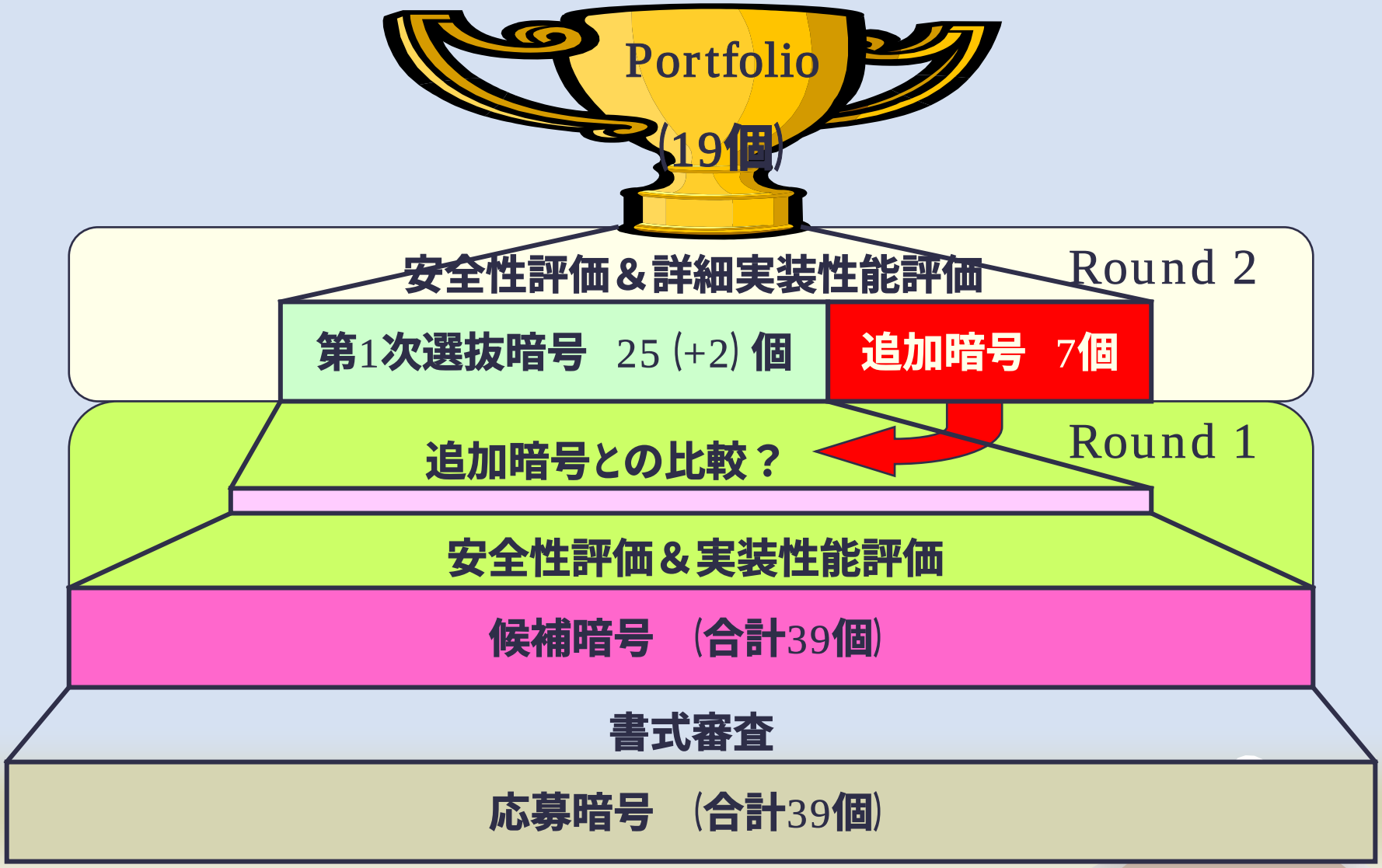
2000年　1月　NESSIEプロジェクト開始を宣言
　　1月　インダストリボード設立
　　3月　公募要綱公開
　　9月　公募締切

　　11月　第1回NESSIE会議開催
2001年　6月　(第1次評価予備審査)
　　9月　第2回NESSIE会議開催
　　9月　最終候補選抜・発表
2002年　2月　(第2次評価予備選定)
　　11月　第3回NESSIE会議開催
2003年　2月　第4回NESSIE会議開催
　　2月　NESSIE Portfolio発表

　　3月　NESSIEプロジェクト終了



NESSIEプロジェクトでの選定



NESSIEプロジェクトでの選抜

❒ NESSIE候補暗号数の変化

	応募数	第1次選抜		最終選抜
64ビットブロック暗号	6	3	—	1
128ビットブロック暗号	7	1	1 (AES)	2
256ビットブロック暗号	1	1		1
可変ブロック長暗号	3	2		0
ストリーム暗号	6	4	—	0
メッセージ認証子	2	2	2	4
ハッシュ関数	1	1		4
擬似乱数生成系	0	0		0
公開鍵暗号	5	5	1	3
デジタル署名	7	5	—	3
公開鍵認証方式	1	1	—	1

MISTY1

Camellia

PSEC-KEM

CRYPTRECプロジェクトの概要

2000年5月　CRYPTRECプロジェクトの開始

- 安全性・実装性等の**特徴を分析・整理**したリストを作成
  - 専門的知見及び客観的見地から**評価・調査**を実施
  - 暗号モジュール評価などの検討
  - 政府における**暗号利用指針作成への貢献**および実施環境の整備
  - 国産の暗号アルゴリズムの国際標準化への推進
  - 世界中から評価対象暗号を公募
  - 国内外の暗号研究者への**評価依頼**
- **旧通商産業省の一施策**として実施
  - ミレニアム・プロジェクトに基づいた旧通産省のアクションプラン
  - 日本有数の暗号研究者らによる委員と7省庁のオブザーバからなる「暗号技術評価委員会」を組織
    - 下部委員会として「共通鍵暗号評価小委員会」「公開鍵暗号評価小委員会」を設置

CRYPTRECプロジェクトの概要 (cont.)

2001年4月　一省庁施策から**政府施策**へ格上げ

- 電子政府システムに適用可能な暗号技術(推奨暗号技術)を**リストアップ**
  - 電子政府システムでの暗号技術調達の際に、**可能な限り、利用を推進**
  - 専門的知見及び客観的見地から評価・調査を実施
  - 世界中から評価対象暗号を公募
  - 電子署名・認証法、SSL/TLSプロトコルに対する評価
  - 国内外の暗号研究者への評価依頼
- **総務省・経済産業省主管の政府施策**として実施
  - IT基本法に基づく、e-Japan戦略、e-Japan重点計画の実施施策
  - 政策的課題を含めた評価・検討を行う「暗号技術検討会」を新設
  - 技術的評価は、「暗号技術評価委員会」「共通鍵暗号評価小委員会」「公開暗号評価小委員会」で継続実施

CRYPTRECプロジェクトの公募要綱

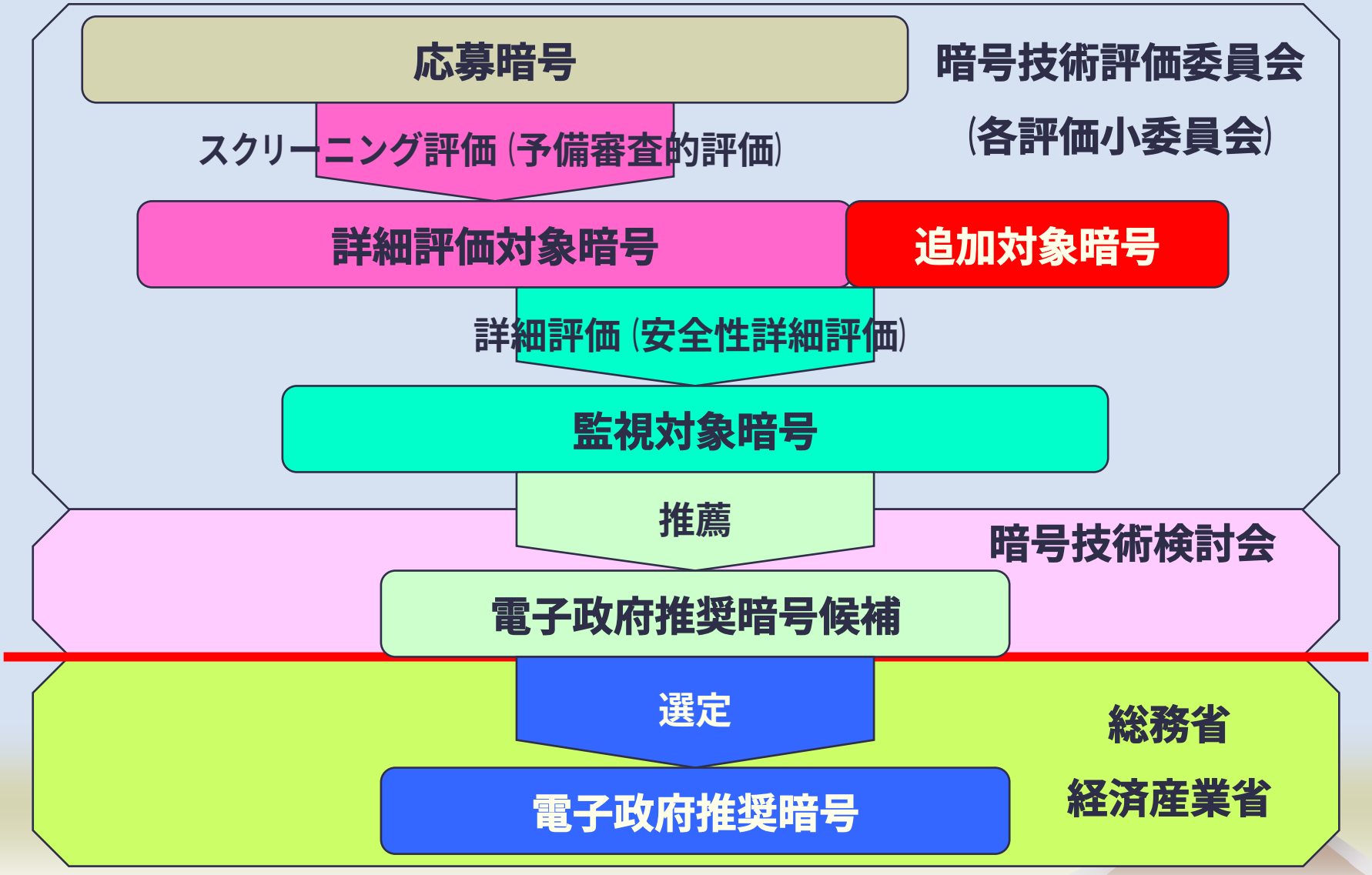
2000年6月、2001年8月　公募要綱を公開

- 基本的にはAESプロジェクトの公募要綱を参考

〔AESプロジェクトと異なる主な事項〕

- 募集カテゴリ
  - ブロック暗号（64ビットブロック暗号、128ビットブロック暗号）
  - ストリーム暗号
  - ハッシュ関数
  - 擬似乱数生成系
  - 公開鍵暗号技術（守秘、認証、署名、鍵共有）
- **非排他的かつ合理的条件**での特許許諾実施でよい
- 安全性・実装性能を評価・調査し、特徴をリストアップ
- 電子政府システムに**適用可能な暗号技術を推薦**
  - 各カテゴリ**原則複数**の暗号技術を電子政府推奨暗号候補として推薦
  - 電子政府推奨暗号を最終決定するのは総務省・経済産業省

CRYPTRECプロジェクトでの評価

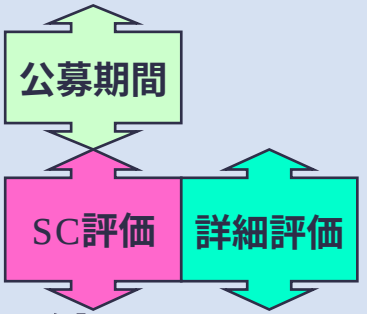


CRYPTRECプロジェクトの推移

2000年　5月　暗号技術評価委員会設置
　　6月　2000年度公募要綱公開
　　7月　2000年度公募締切

2001年　5月　暗号技術評価報告会（2000年度）開催

　　5月　暗号技術検討会設置
　　8月　2001年度公募要綱公開
　　9月　2001年度公募締切
　　10月　応募暗号説明会開催
2002年　1月　暗号技術評価ワークショップ開催
　　4月　暗号技術評価報告会（2001年度）開催



　　11月　電子政府推奨暗号リスト案公開
2003年　2月　電子政府推奨暗号リスト決定
　　5月　暗号技術評価報告会（2002年度）開催

各プロジェクトの比較総括

プロジェクトの比較総括 ー 意義

- 客観的評価を受けた暗号技術を使う原則を確立
  - OECD暗号政策ガイドライン8原則 (1997年)
    [原則4] 国際的なレベルに合致した技術的基準によって
    [原則3] 市場主導で開発された暗号のなかから
    [原則1] 信頼性の高い安全な暗号を
    [原則2] ユーザの責任で選択すべきである
  - 想定されている主なユーザ
    - AES: 米国政府機関 (+ 民間セクタ)
    - NESSIE: 欧州産業界 (+ 標準化団体)
    - CRYPTREC: 中央官庁 (+ 地方自治体)

どこまで
合意形成
をする？

民間セクタが想定ユーザとして事前に含まれているかが

プロジェクト運営方針に影響

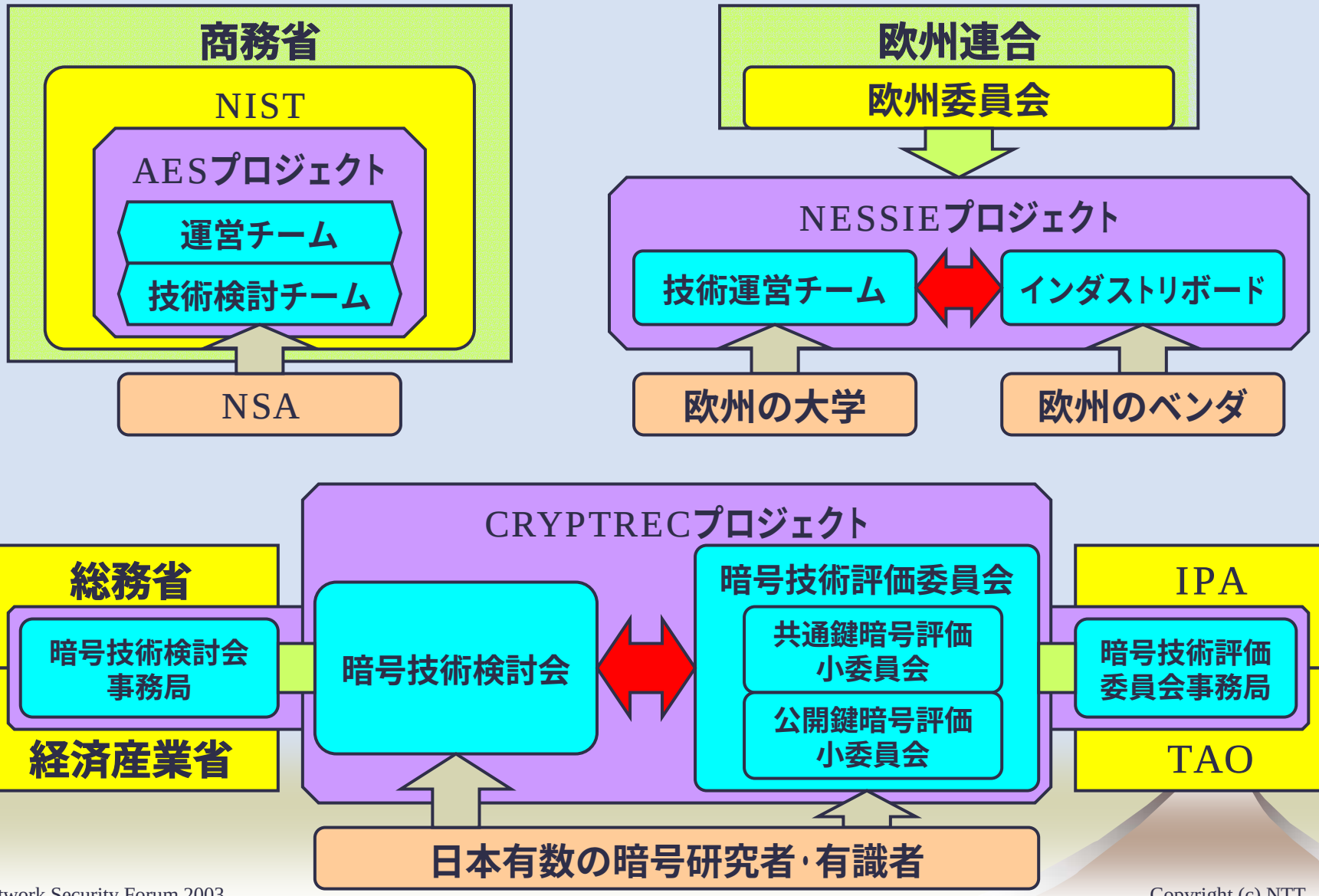
プロジェクトの比較総括 ー 運営上の違い

- 運営手法の違い
  - 透明で開かれた選考プロセス → AES, NESSIE
  - 内部評価による選考プロセス → CRYPTREC
- 選考方針の違い
  - 選抜方式 → AES, NESSIE
  - 足切り方式 → CRYPTREC
- 求める暗号技術像の違い
  - 今後20～30年間使える暗号 → AES, NESSIE
  - 調達可能な安全な暗号 → CRYPTREC

運営プロセスは基本的に

AES, NESSIE と CRYPTREC では異なる

プロジェクトの比較総括 ― 体制の違い



プロジェクトの比較総括 ー AES, NESSIE

- 透明で開かれた選考プロセス
  - 評価･選抜に用いる情報は**事前**に公開
    - 評価レポート、論文は投稿時公開が原則
  - **選考前の公開討論**が原則
    - ディスカッションフォーラムの設置
    - AES候補会議、NESSIE会議の開催
    - 暗号国際会議との協調
  - 計画日程よりも**参加者合意形成**を重視
  - 詳細な選定報告書
- 選抜方式による選定 = トーナメント方式の選定
  - 「一つ」、「二、三個」の極めて優れた暗号技術を選抜
  - 安全性と実装性能の両面からの評価
  - 相対比較で優位性がなければ落選 = **実装性能重視**
- 今後20〜30年使える暗号
  - 第1次評価コメントを反映した軽微な仕様変更を認める

事前合意形成
を重要視

プロジェクトの比較総括 – CRYPTREC

- 内部評価による選考プロセス
  - 評価・選定に用いた情報は**事後**に公開
    - 評価レポートも審議中は非公開
  - **選考後の結果報告**が原則
    - 暗号技術評価報告会開催
    - 一般公募型ワークショップは開催せず
  - 詳細な年度末報告書
- 足切り方式 = 選考基準クリア方式の選定
  - 一定水準以上の安全性を有する暗号技術を選定
  - 安全性と実装性能の両面からの評価
  - 安全性上の問題がなければ原則選定 = **安全性重視**
- 調達可能な安全な暗号
  - 評価中に仕様変更は認めない
  - 新規の暗号はあまり期待しない = 公募期間の短さ

プロジェクトの比較総括 ― まとめ

- AES, NESSIE
  - 安全性･実装性能の両面で優れた暗号技術を選抜
  - 審査結果以外の情報は評価期間中も原則オープン
  - 世界中の暗号研究者らを含めた事前の合意形成
  - 高い対外的訴求効果を獲得
  - 主催者の思惑とは違った結果になったかもしれない
- CRYPTREC
  - 電子政府で利用可能である安全な暗号技術を選定
  - 国内の有識者(暗号研究者)による評価判断
  - 説明責任を重視
  - 対外的訴求効果が弱くなったかもしれない
  - 評価データを含む全情報が評価期間中は委員会に集中

ISO/IEC国際標準暗号への影響

- 従来、暗号はISO/IEC国際標準暗号の対象外
  - 米国の反対でDESのISO国際標準化見送り
  - 暗号登録制度を制定 (ISO/IEC9979)
    ISO/IEC9979登録暗号 ≠ ISO/IEC国際標準暗号
- 1999年12月 ISO/IEC JTC1/SC27は方針転換
  - 2005年春目途にISO/IEC18033国際標準暗号策定
  - 客観的に評価された少数の安全な暗号アルゴリズム
    - 公開鍵暗号
    - 共通鍵暗号(64ビットブロック暗号、128ビットブロック暗号、ストリーム暗号)
- 暗号モジュール検証プログラム(CMVP)での利用承認暗号になる見込み
  - 2006年春目途にISO/IEC19790国際標準規格策定

選定暗号一覧 － 公開鍵暗号

	米国政府 標準暗号	NESSIE Portfolio	電子政府 推奨暗号	ISO/IEC 国際標準
署名	DSA RSA ECDSA	 RSA-PSS (1st) ECDSA (2nd) SFLASH (sp.)	DSA RSA-PSS RSASSA-PKCS1 ECDSA	ISO/IEC9796 ISO/IEC14888 ISO/IEC15946-2
守秘	なし	PSEC-KEM (1st) RSA-KEM (2nd) ACE-KEM (sp.)	 RSA-OAEP RSAES-PKCS1	ISO/IEC 18033-2
鍵共有	なし	なし	PSEC-KEM DH ECDH	ISO/IEC11770 ISO/IEC15946-3
認証	FIPS196	GPS	なし	ISO/IEC9798

選定暗号一覧 － 共通鍵暗号

	米国政府 標準暗号	NESSIE Portfolio	電子政府 推奨暗号	ISO/IEC 国際標準
64ビット ブロック 暗号	DES Triple DES	MISTY1	3-key Triple DES MISTY1 CIPHERUNICORN-E Hierocrypt-L1	ISO/IEC 18033-3
128ビット ブロック 暗号	AES	AES Camellia	AES Camellia CIPHERUNICORN-A Hierocrypt-3 SC2000	ISO/IEC 18033-3
256ビット ブロック 暗号	なし	SHACAL-2	なし	なし
ストリー ム暗号	なし	なし	MUGI MULTI-S01 128-bit RC4	ISO/IEC 18033-4

選定暗号一覧 － その他

	米国政府 標準暗号	NESSIE Portfolio	電子政府 推奨暗号	ISO/IEC 国際標準
ハッシュ関数	SHA-1 SHA-256 SHA-384 SHA-512	 SHA-256 SHA-384 SHA-512 Whirlpool	SHA-1 RIPEMD-160 SHA-256 SHA-384 SHA-512	ISO/IEC10118
メッセージ認証子	MAC HMAC	 HMAC UMAC TTMAC EMAC	なし	ISO/IEC9797
擬似乱数生成	FIPS 186-2	なし	FIPS 186-2 ANSI X9.42	なし

最後に

- 日米欧での暗号技術標準化・評価プロジェクト
  = 客観的に評価された暗号利用の推進を =
  - 世界中の暗号研究者らが長期間関与
  - 安全性評価や実装性能評価を客観的に実施
  - 日本では初めての公式な暗号技術の評価
  - ISO/IEC、IETFなどの標準化作業にも大きく影響
- プロジェクト運営上の違い
  = 事前合意形成重視 vs 説明責任重視 =
  - 詳細な報告書
  - 選定前の合意形成の重要性
  - 主催者、応募者、参加者における情報格差の解消
  - 対外的啓蒙効果

日米欧の暗号技術標準化・評価プロジェクトを終えて

― 実績と今後の展望 ―

NTT 情報流通プラットフォーム研究所
神田 雅透
kanda@isl.ntt.co.jp