# 応募状況説明

CRYPTREC事務局

CRYPTREC
Cryptography Research and Evaluation Committees

# 公募の目的 (公募要項P.4 第5.1節抜粋)

・策定から5年以上が経過し、解析・攻撃技術の高度化及び暗号技術の開発が進展している

・安全性評価のみならず危殆化及び移行対策を含めた適切な暗号選択の支援への要望

・導入コスト、相互運用性、普及度合いなどの評価観点の必要性の指摘

・リストの改訂に必要な技術の追加

CRYPTREC
Cryptography Research and Evaluation Committees

# 応募暗号に関する留意事項(公募要項P.2 第2.2節抜粋)

- 2010年9月までに査読付き国際学会に採択されていること
- 第三者が全ての機能を実装可能となる情報が開示されていること
- 国内外での評価が可能であること
- 評価に際しては、知的財産の利用が無償で行えること
- 電子政府リスト策定後3年以内に調達可能なこと

CRYPTREC
Cryptography Research and Evaluation Committees

# 本日の説明対象技術カテゴリ

・共通鍵暗号（128bitブロック暗号）

・エンティティ認証

CRYPTREC
Cryptography Research and Evaluation Committees

# 128bitブロック暗号

・128bit/192vit/256bitの鍵サイズ

・暗号は守秘目的以外にも利用されるので、いわゆる暗号文単独攻撃以外の既知平文攻撃、(適応的)選択平文・暗号文攻撃、関連鍵攻撃、選択IV攻撃等、攻撃者 にとって非常に都合のよい環境での耐性も評価を行う。

・差分攻撃法や線形攻撃法等の既知の一般的な攻撃法に対する耐性を評価します。また、応募暗号に特化した攻撃法や、ヒューリスティックな安全性の根拠も評価の対象とすることもある。

・鍵に対する全数探索よりも効果的な攻撃手法が発見されていないこと

・サイドチャネル攻撃に対する安全性も加味(新設)

・現リスト暗号よりも安全性/実装性で優位であること(新設)

CRYPTREC
Cryptography Research and Evaluation Committees

# 128bitブロック暗号応募状況及び評価対象

応募技術　2件

- CLEFIA　　ソニー株式会社
- HyRAL　　株式会社ローレルインテリジェントシステムズ

現リスト技術　5件

- AES　　事務局提案
- Camellia　　日本電信電話株式会社
- CIPHERUNICORN-A　日本電気株式会社
- Hierocrypt-3　　株式会社東芝
- SC2000　　富士通株式会社

CRYPTREC
Cryptography Research and Evaluation Committees

# 現リスト暗号 AES

・SPN型のブロック暗号

・ブロック長、鍵長：128ビット、192ビット、256ビット

・米国連邦政府標準暗号（FIPS 197）、ISO標準（18033-3）、IETF RFC 3268, 3394などに含まれる

・現状の安全性解析状況
  ・192ビット・256ビット鍵に対し、フルラウンドの関連鍵攻撃(Asiacrypt 2009)
  ・関連鍵攻撃以外では、全鍵サイズでフルラウンド攻撃に至らず
    128ビット鍵　10段中7段　collision attack(3rd AES conf),partial sum (FSE 2003)
    192ビット鍵　12段中8段　partial sum (FSE 2003)
    256ビット鍵　14段中8段　partial sum (FSE 2003)

CRYPTREC
Cryptography Research and Evaluation Committees

# 現リスト暗号 Camellia

・Feistel型のブロック暗号

・ブロック長：128ビット
・鍵長：128ビット、192ビット、256ビット

・ISO標準（18033-3）、IETF RFCなどに含まれる

・安全性と実装のバランスに優れたアルゴリズムであり、特にハードウエア実装（ゲート数あたりの処理速度とゲート数）において優位な点がある。

・現状の安全性解析状況
・全鍵サイズでフルラウンド攻撃は存在しない
　128ビット鍵　18段中12段 (FL関数無し)　不能差分攻撃(SAC 2009)
　192ビット鍵　24段中13段 (FL関数無し)　不能差分攻撃(CT-RSA 2008)
　256ビット鍵　24段中14段 (FL関数無し)　不能差分攻撃(CT-RSA 2008)

CRYPTREC
Cryptography Research and Evaluation Committees

# 現リスト暗号 CIPHERUNICORN-A

・Feistel型のブロック暗号

・ブロック長：128ビット
・鍵長：128ビット、192ビット、256ビット

・ラウンド関数での拡大鍵探索を困難にするために、複雑なラウンド関数を設計。ラウンド関数における初等統計評価においてデータ撹拌における偏りはないと主張。

・前回の評価においては、ラウンド関数の評価は困難であったが、複数の評価者が近似された異なるラウンド関数により安全性を評価。

・現状の安全性解析状況
・縮小モデルに対する具体的攻撃は存在しない

CRYPTREC
Cryptography Research and Evaluation Committees

# 現リスト暗号 Hierocrypt-3

・（入れ子型）SPN型のブロック暗号

・ブロック長：128ビット
・鍵長：128ビット、192ビット、256ビット

・ICカードやミドルウエアでの暗号化の高速性を重視した設計。

・現状の安全性解析状況
・全鍵サイズでフルラウンド攻撃は存在しない
　128ビット鍵　6段中3段　SQUARE攻撃(FSE 2001)
　192ビット鍵　7段中3.5段　SQUARE攻撃(FSE 2001)
　256ビット鍵　8段中3.5段　SQUARE攻撃(FSE 2001)

CRYPTREC
Cryptography Research and Evaluation Committees

# 現リスト暗号 SC2000

・FeistelとSPNの重ね合わせによるブロック暗号

・ブロック長：128ビット
・鍵長：128ビット、192ビット、256ビット

・Bitsliceによる高速実装や、非線形演算処理においてCPUの1次キャッシュに応じた高速実装が可能。

・現状の安全性解析状況
・全鍵サイズでフルラウンド攻撃は存在しない
　128ビット鍵　19段中13段　差分解読／線形解読(2nd NESSIE Workshop)

# エンティティ認証(新設)

・電子政府推奨暗号リストに掲載された共通鍵暗号、公開鍵暗号、ハッシュ関数、メッセージ認証コードの組み合わせによって実現されるエンティティ認証、あるいは、安全性を計算量的な困難さに帰着できるエンティティ認証

・安全性を脅かす状態としては、なりすましの 成功、セッションの取り換え等を想定

・電子政府推奨暗号リストに掲載されている、あるいは 応募中の共通鍵暗号、公開鍵暗号、ハッシュ関数、メッセージ認証コードのみを利 用している場合には、暗号プリミティブを理想的に安全なものとする

・その他の暗号プリミティブを用いる場合には、暗号プリミティブを理 想化せずに安全性の検証を実施

・提案者はプロトコルの安全性を示す情報を提出し、本公 募における安全性評価では、これらの正当性を検証

CRYPTREC
Cryptography Research and Evaluation Committees

# エンティティ認証応募状況及び評価対象

応募技術

・無限ワンタイムパスワード認証方式(Infinite One-Time Password）　　日本ユニシス株式会社

事務局選出技術

・ISO/IEC 9798-2（共通鍵暗号を用いたプロトコル）

・ISO/IEC 9798-3（電子署名を用いたプロトコル）

・ISO/IEC 9798-4（検査関数（MAC）を用いたプロトコル）