電子政府推奨暗号リストについて

2009年2月18日

暗号技術検討会座長
暗号技術評価委員会委員長
今井秀樹(中央大学)

1

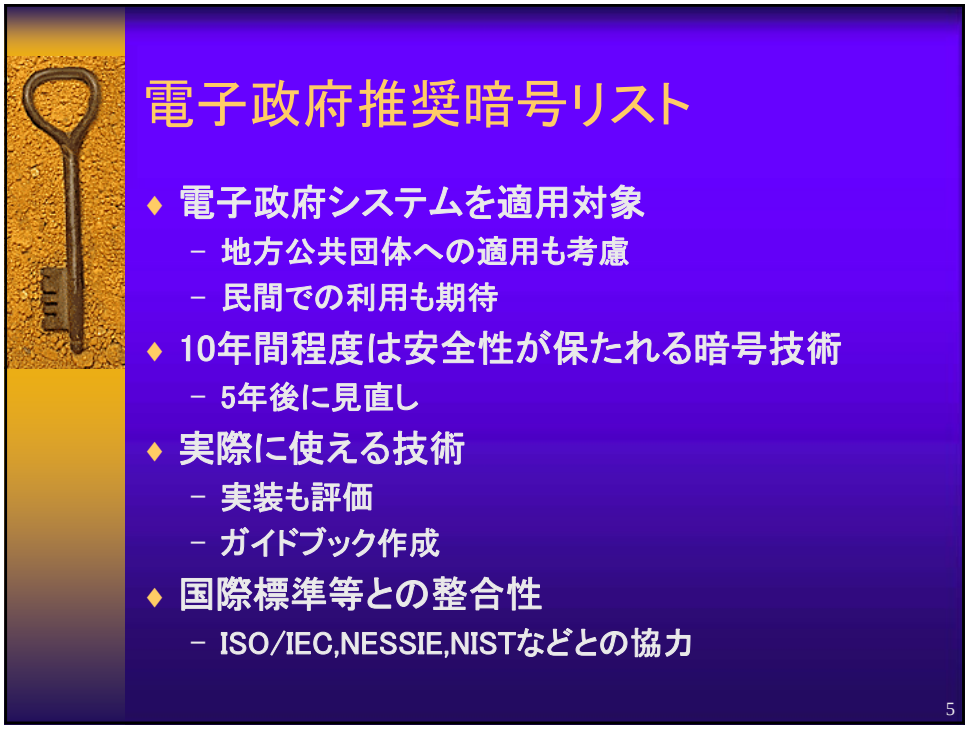
電子政府推奨暗号リストの母体 CRYPTREC

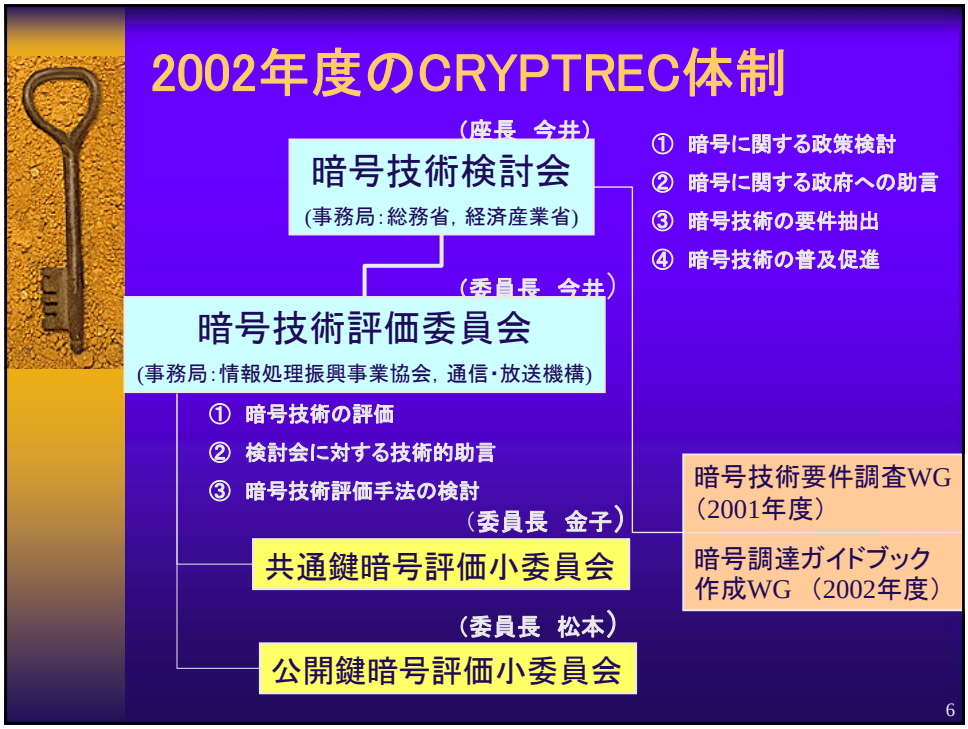
- Cryptography Research and Evaluation Committees（暗号技術検討会，暗号技術評価委員会等）の略．しかし，その後，プロジェクト名としても使われる．
- 電子政府推奨暗号リストを策定したプロジェクト
- 現在は電子政府推奨暗号の安全性等の監視，暗号モジュールの評価基準等を検討

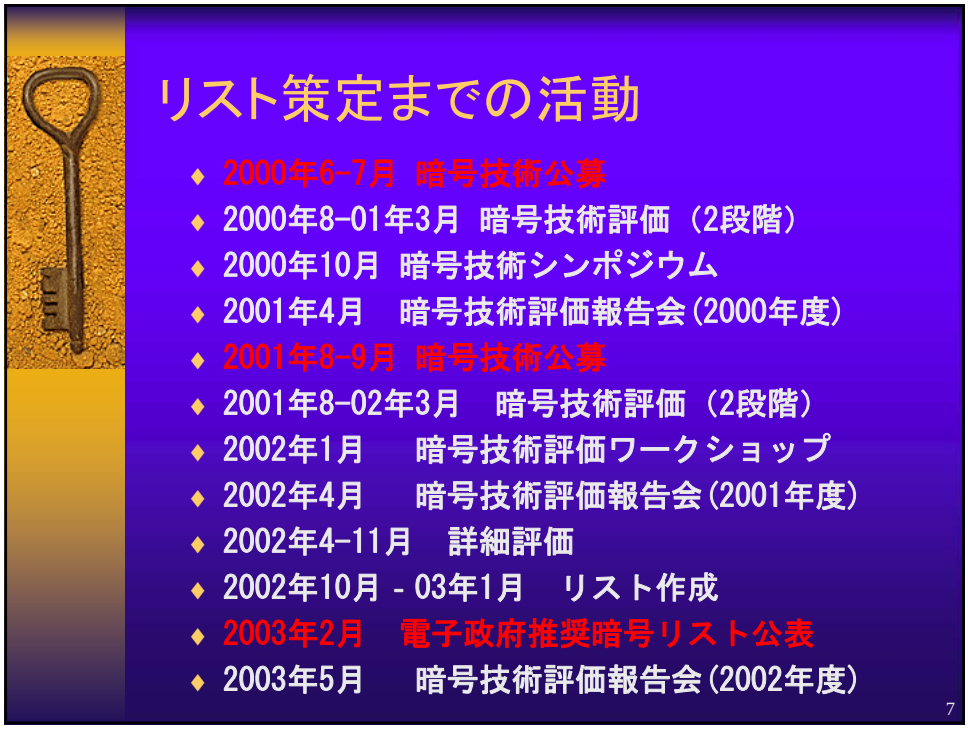
2


CRYPTREC活動の背景
♦ 電子政府の基盤構築へ
– 1990年代後半：行政の情報化推進
– 1999年：ミレニアムプロジェクト
· 2003年までに電子政府の基盤構築
– 2000年以降：IT基本法，e-Japan戦略など
♦ 情報セキュリティの重要性の認識
– 2000年省庁のホームページ改ざん事件
– 2001年以降：IT戦略本部e-Japan重点計画など
· 高度情報通信ネットワークの安全性・信頼性の確保
♦ 情報セキュリティの基盤としての暗号
– 暗号の政府調達基準の不在
– 暗号は電子政府の安全性の基盤
3

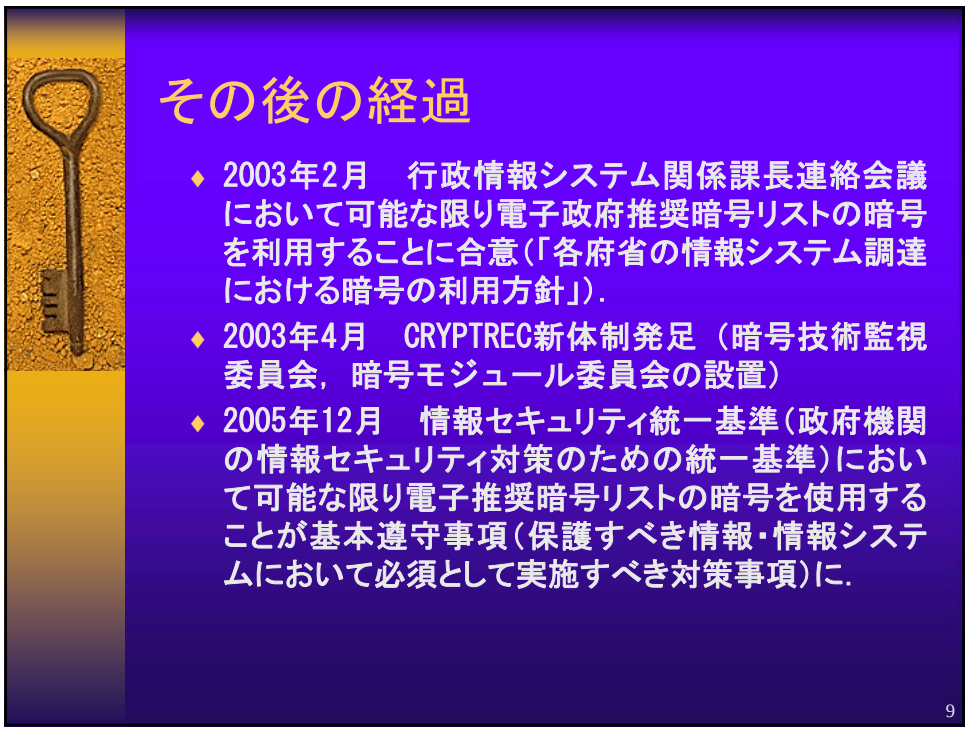

CRYPTRECの目的
♦ 電子政府に利用可能な暗号技術を提示
– 電子政府システムに適用可能な暗号技術を公募
– 応募暗号技術および事務局提案暗号技術を技術的・専門的見地から評価
– 安全性，実装性等の特徴を分析・整理したリスト（電子政府推奨暗号リスト）を作成
♦ 暗号技術標準化へ貢献
♦ 暗号技術に対する信頼感醸成
– 活動の公平性・透明性を確保
4


電子政府推奨暗号リスト
♦ 電子政府システムを適用対象
– 地方公共団体への適用も考慮
– 民間での利用も期待
♦ 10年間程度は安全性が保たれる暗号技術
– 5年後に見直し
♦ 実際に使える技術
– 実装も評価
– ガイドブック作成
♦ 国際標準等との整合性
– ISO/IEC,NESSIE,NISTなどとの協力
5

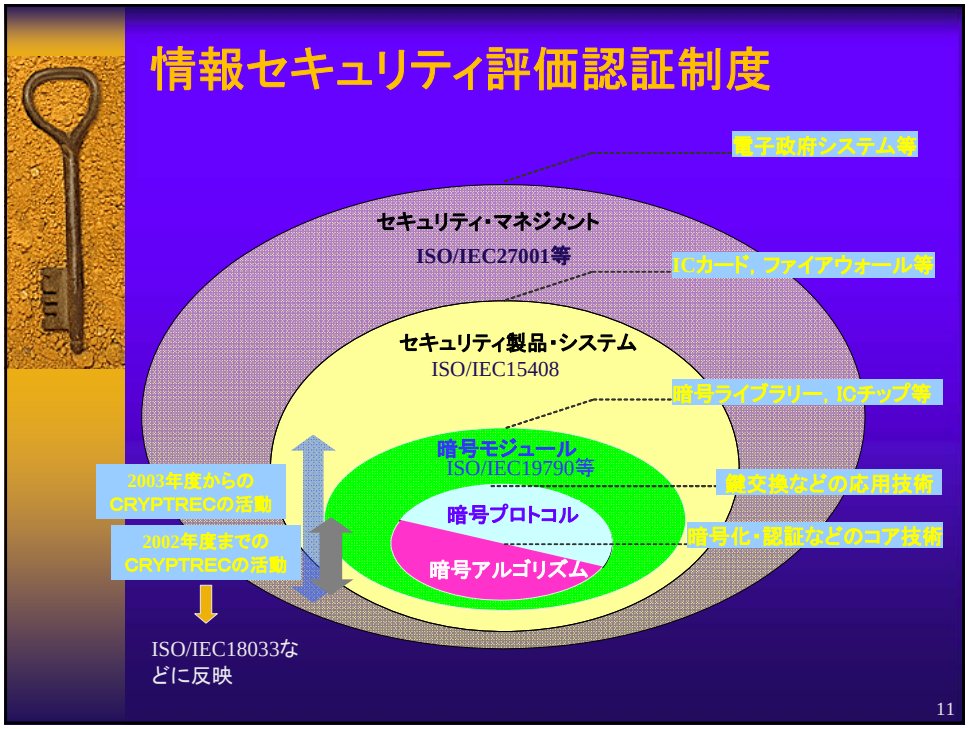

2002年度のCRYPTREC体制
（座長　今井）
暗号技術検討会
(事務局:総務省，経済産業省)
① 暗号に関する政策検討
② 暗号に関する政府への助言
③ 暗号技術の要件抽出
④ 暗号技術の普及促進
（委員長　今井）
暗号技術評価委員会
(事務局:情報処理振興事業協会，通信・放送機構)
① 暗号技術の評価
② 検討会に対する技術的助言
③ 暗号技術評価手法の検討
（委員長　金子）
共通鍵暗号評価小委員会
（委員長　松本）
公開鍵暗号評価小委員会
暗号技術要件調査WG
（2001年度）
暗号調達ガイドブック
作成WG （2002年度）
6

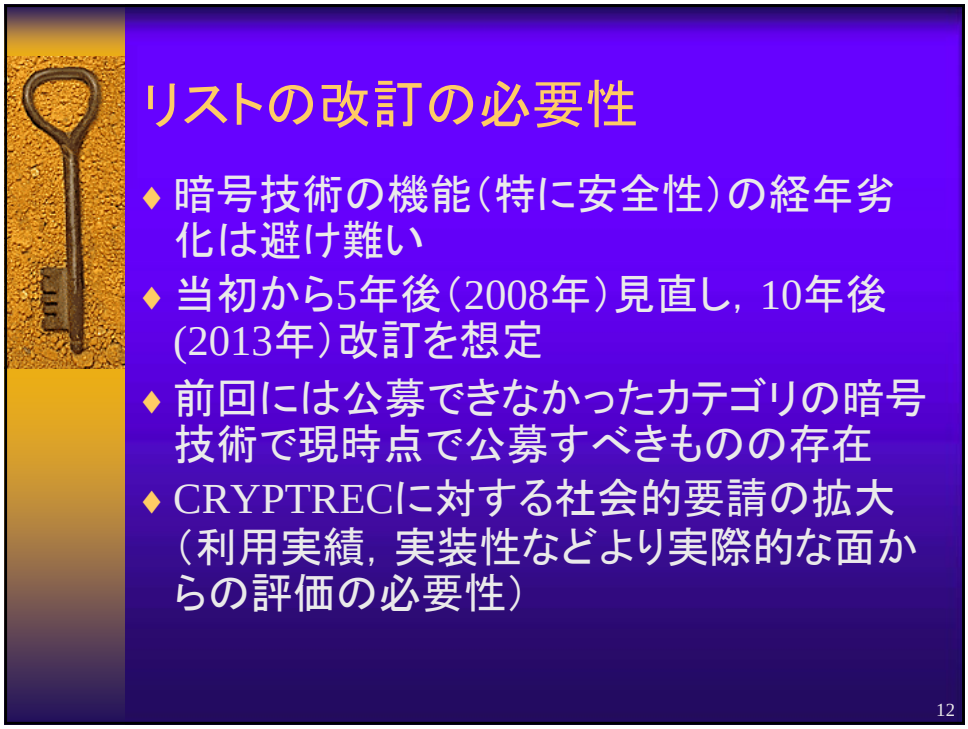

リスト策定までの活動
♦ 2000年6-7月 暗号技術公募
♦ 2000年8-01年3月 暗号技術評価 (2段階)
♦ 2000年10月 暗号技術シンポジウム
♦ 2001年4月 暗号技術評価報告会(2000年度)
♦ 2001年8-9月 暗号技術公募
♦ 2001年8-02年3月 暗号技術評価 (2段階)
♦ 2002年1月 暗号技術評価ワークショップ
♦ 2002年4月 暗号技術評価報告会(2001年度)
♦ 2002年4-11月 詳細評価
♦ 2002年10月 - 03年1月 リスト作成
♦ 2003年2月 電子政府推奨暗号リスト公表
♦ 2003年5月 暗号技術評価報告会(2002年度)
7

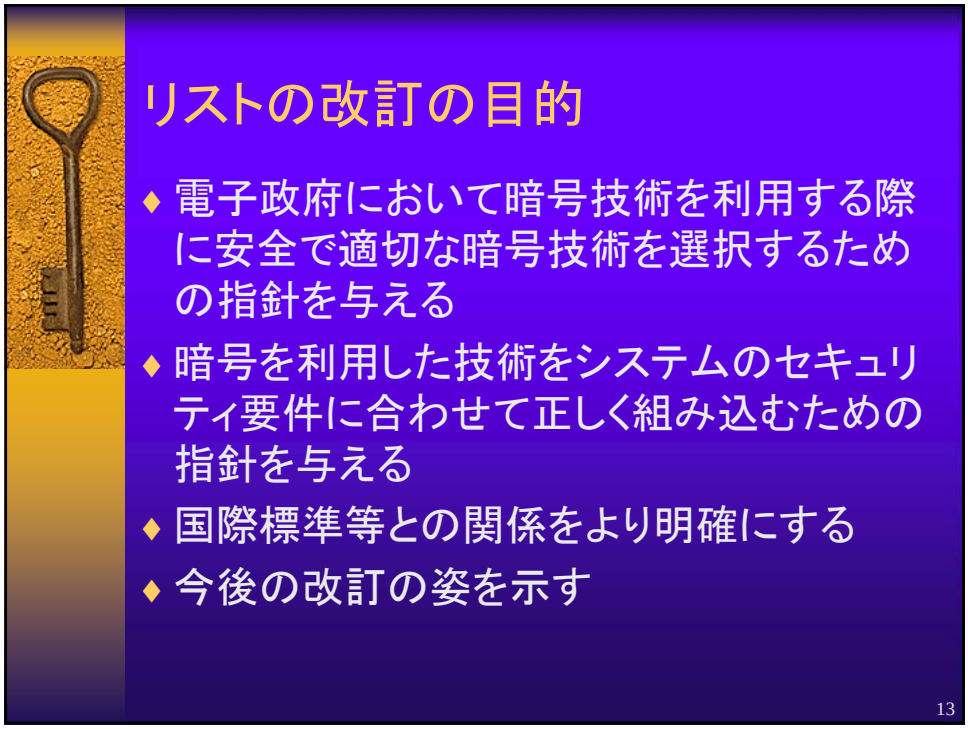

電子政府推奨暗号リスト作成のための
暗号評価の概要
公開鍵暗号
共通鍵暗号
守秘
署名
鍵共有
認証
64bitブロック暗号
128bitブロック暗号
ストリーム暗号
ハッシュ関数
擬似乱数生成系
その他
計
応募総数 9 10 8 1 4 9 9 0 9 2 61
評価総数 10 15 9 1 6 11 10 6 15 2 85
最終結果 2 4 3 0 4 5 3 5 3* 0 29
＊は例示
8

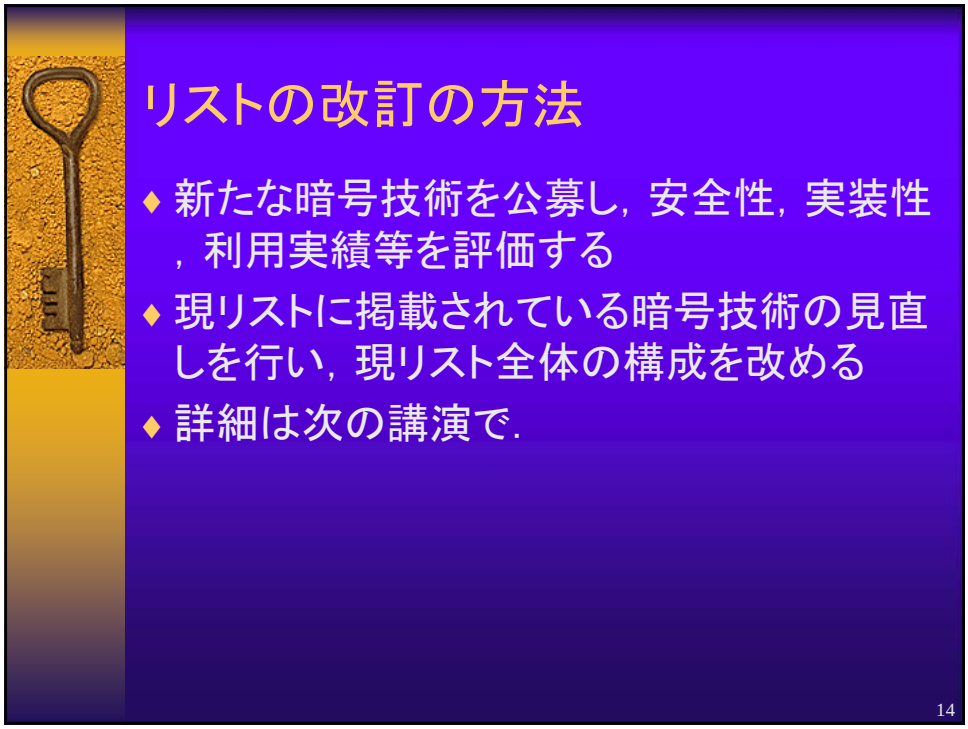

その後の経過
♦ 2003年2月　行政情報システム関係課長連絡会議において可能な限り電子政府推奨暗号リストの暗号を利用することに合意(「各府省の情報システム調達における暗号の利用方針」).
♦ 2003年4月　CRYPTREC新体制発足（暗号技術監視委員会，暗号モジュール委員会の設置）
♦ 2005年12月　情報セキュリティ統一基準(政府機関の情報セキュリティ対策のための統一基準)において可能な限り電子推奨暗号リストの暗号を使用することが基本遵守事項(保護すべき情報・情報システムにおいて必須として実施すべき対策事項)に.
9


現在のCRYPTREC体制
（座長　今井）
暗号技術検討会
(事務局:総務省，経済産業省)
（委員長　今井）
（委員長　松本）
暗号技術監視委員会
(事務局:NICT，IPA)
暗号モジュール委員会
(事務局:IPA，NICT)
（1）電子政府推奨暗号の監視
（2）暗号アルゴリズム等を主な対象とする 調査・検討
（3）電子政府推奨暗号リストの改訂に関する調査・検討
（1）暗号モジュール評価基準及び試験基準の作成
（2）暗号実装関連技術を主な対象とする調査・検討
IDベースWG
リストガイドWG
電力解析実験WG
10


情報セキュリティ評価認証制度
電子政府システム等
セキュリティ・マネジメント
ISO/IEC27001等
ICカード，ファイアウォール等
セキュリティ製品・システム
ISO/IEC15408
暗号ライブラリー，ICチップ等
暗号モジュール
ISO/IEC19790等
暗号プロトコル
暗号アルゴリズム
電子署名などの応用技術
暗号化・認証などのコア技術
2003年度からの
CRYPTRECの活動
2002年度までの
CRYPTRECの活動
ISO/IEC18033など
に反映
11


リストの改訂の必要性
♦ 暗号技術の機能（特に安全性）の経年劣化は避け難い
♦ 当初から5年後（2008年）見直し，10年後(2013年）改訂を想定
♦ 前回には公募できなかったカテゴリの暗号技術で現時点で公募すべきものの存在
♦ CRYPTRECに対する社会的要請の拡大（利用実績，実装性などより実際的な面からの評価の必要性）
12


リストの改訂の目的
電子政府において暗号技術を利用する際に安全で適切な暗号技術を選択するための指針を与える
暗号を利用した技術をシステムのセキュリティ要件に合わせて正しく組み込むための指針を与える
国際標準等との関係をより明確にする
今後の改訂の姿を示す
13


リストの改訂の方法
新たな暗号技術を公募し，安全性，実装性，利用実績等を評価する
現リストに掲載されている暗号技術の見直しを行い，現リスト全体の構成を改める
詳細は次の講演で.
14


むすび
現リストは多くの第一線の暗号研究者の献身的な努力があり，初めて策定できた.
今回の改訂も暗号関連の多くの方々にご協力を頂くことになる.
何卒よろしくお願いいたします.
質問，ご意見はCRYPTREC事務局に.
ホームページ：http://www.cryptrec.go.jp/
15