「暗号/情報セキュリティ」

三菱電機株式会社
情報技術総合研究所
情報セキュリティ技術部
山岸　篤弘
atsuhiro@iss.isl.melco.co.jp

2002-10-21

目次

- 情報セキュリティおよび暗号技術の現況
  - 情報セキュリティ技術と暗号技術
  - 暗号技術とは何か
  - 情報セキュリティシステムと標準化
  - 暗号技術の現状と課題
- 三菱電機における研究開発

暗号技術に関する研究開発での方針決定のケーススタディー

- 暗号技術に関する基礎技術開発での場合
- 独自暗号技術の普及に向けて
- 情報セキュリティシステムの構築の為に

情報セキュリティおよび暗号技術の現況

情報セキュリティ技術と暗号技術

PKI: (Public Key Infrastructure)

古典暗号から現代暗号へ

- 古典暗号の世界
  - 暗号の歴史は人類の歴史と同じ長さ
  - 軍事外交目的の非公開技術
  - 参加者限定の1対1通信を前提
  - 文字の置換を中心とする変換処理
  - 安全性評価は文字の出現頻度の統計学
- 現代暗号の世界
  - 本格的に開かれた研究は1970年代から
  - プライバシー保護という動機付け
  - 不特定多数が参加するネットワーク指向
  - ディジタル信号の変換処理
  - 計算量理論との融合

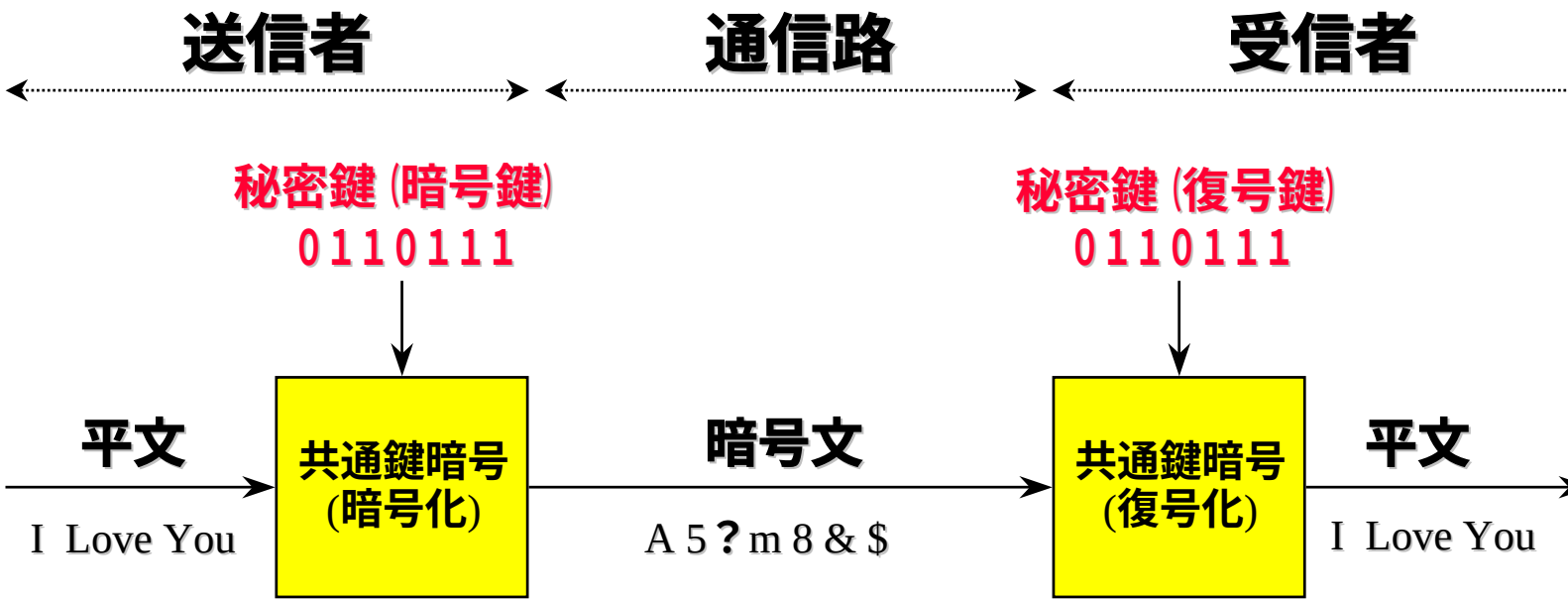
現代暗号のコンセプト

- 非公開技術から公開技術への転換
  - 1976年　米国政府標準暗号DESの制定と仕様公開
  - 1978年　公開鍵暗号の発明⇒ﾈｯﾄﾜｰｸ暗号の実現
- 暗号方式の公開が定着へ
  - 第三者の安全性検証による信頼性向上
  - 暗号の健全利用の促進
- 電子社会の見えざるインフラに
  - ディジタル情報保護のために不可欠な道具
  - キーワードは「Privacy」と「Money」

暗号方式の分類

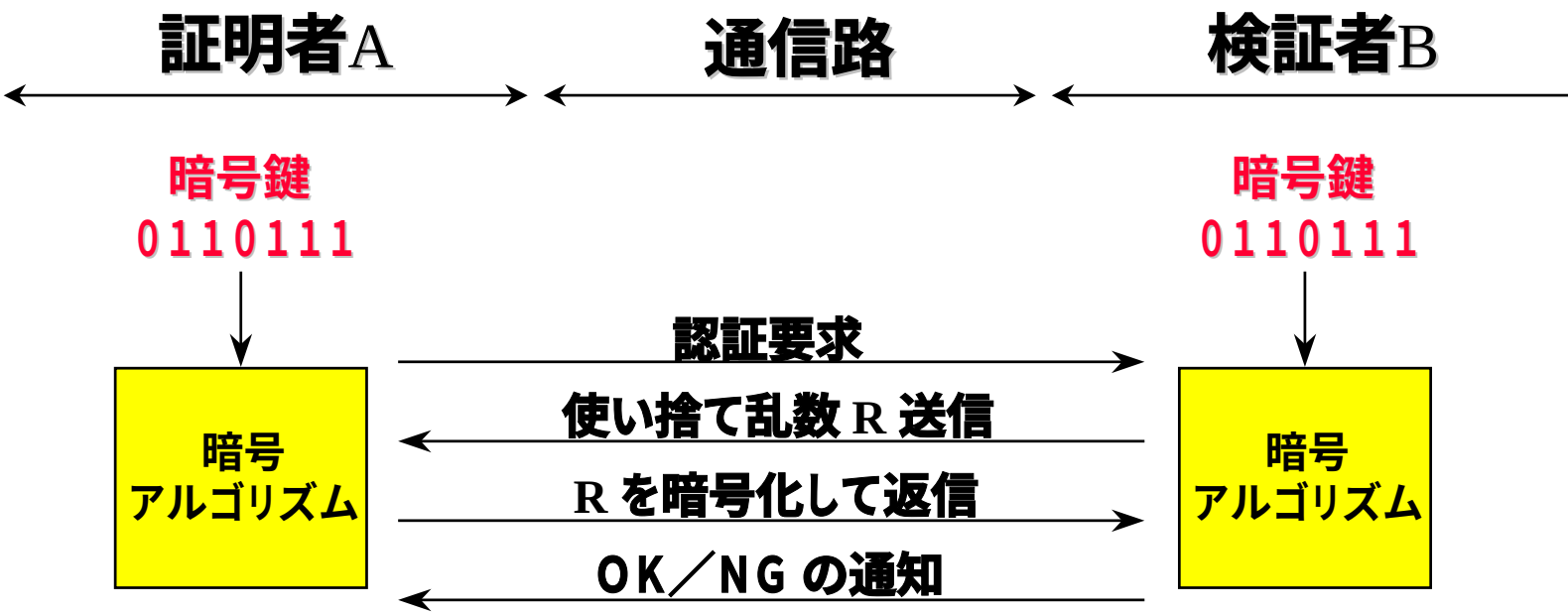
- **共通鍵暗号 (秘密鍵暗号，対称鍵暗号)**
  - **送信者と受信者が共通の鍵をもつ**
  - **小型･高速であることにその存在価値**
  - **(例)** DES, RIJNDAEL, MISTY, KASUMI
- **公開鍵暗号 (非対称鍵暗号)**
  - **暗号化の鍵と復号の鍵が異なる特殊な仕掛けが必要**
  - **ディジタル署名や鍵配送など応用が豊富、但し低速**
  - **(例)** RSA, DSA, **楕円暗号**

共通鍵暗号の原理



- 暗号化の鍵と復号の鍵が同じ (これを秘密鍵と呼ぶ)
- 秘密鍵は事前に何らかの方法で共有しておく必要がある

共通鍵暗号によるユーザ認証



- パスワード (暗号鍵) を通信路に流すことなく認証が可能
- A が乱数を生成して B に暗号化させることにより、相互認証も可能となる

代表的な共通鍵暗号（1）

DES (Data Encryption Standard)

- 米国政府（商務省）が共通鍵暗号の公募
- ＩＢＭが応募したものがＤＥＳの原形
- ＮＳＡ（National Security Agency）が評価および改良
- １９７６年ＦＩＰＳ（連邦政府情報処理標準）として成立
- １９８１年ＡＮＳＩに採用
- ＩＳＯでの標準化は米国自身が拒否
- デファクト共通鍵暗号として世界中で利用
- 計算機の進歩の結果 DES はもはや安全ではない
- 現在 Triple-DES が急速に浸透中
- NIST は新暗号の標準化を目指す ⇒ AES

代表的な共通鍵暗号（2）

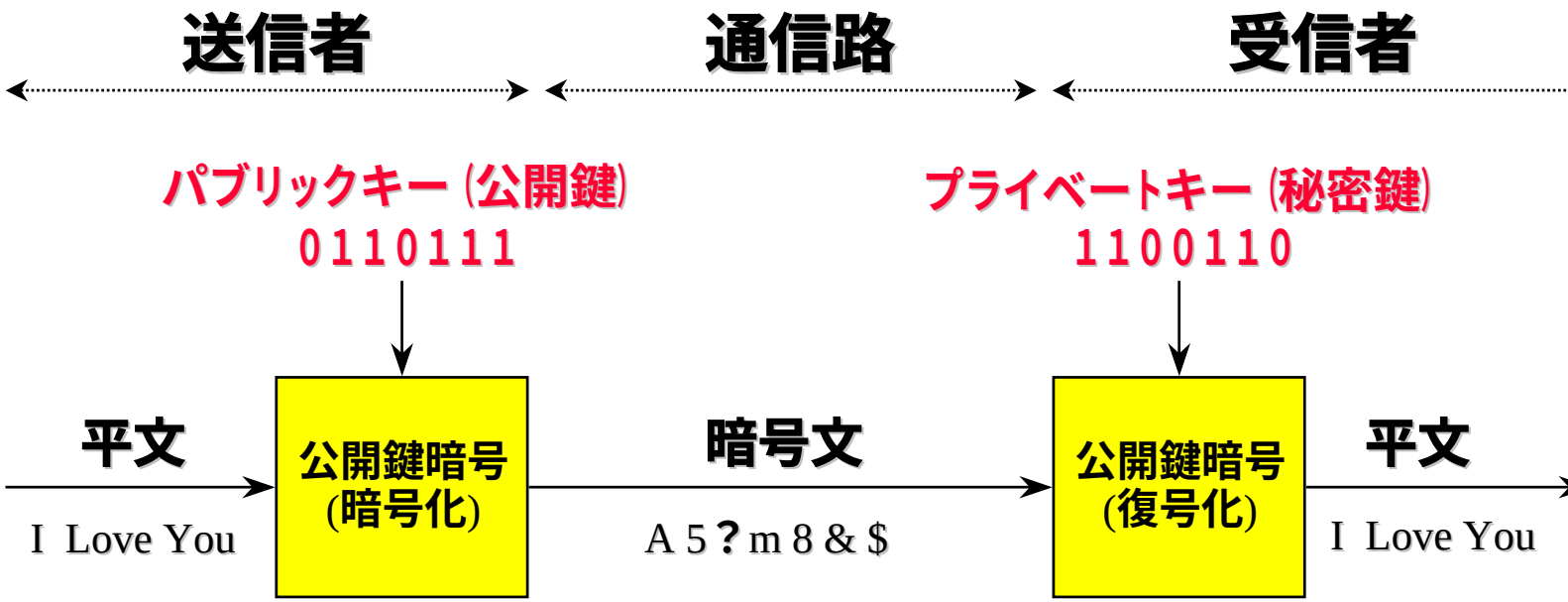
AES (Advanced Encryption Standard)

- DES の後継共通鍵暗号を選定する米国のプロジェクト
- NIST（商務省の組織）が主催する公募によって選定
- 選定されたアルゴリズムは FIPS に登録
- １９９７年１月AESプロジェクト開始
- 世界各国から１５個の暗号方式が提案された
- 第１次選考で５本に絞られた（１９９９年８月）
  米国提案３本、欧州提案２本
- 最終選考で選ばれたのはベルギー製のRIJNDAEL
- AES の Official Home Page
  http://csrc.ncsl.nist.gov/encryption/aes/aes_home.htm

AES のインパクトと今後

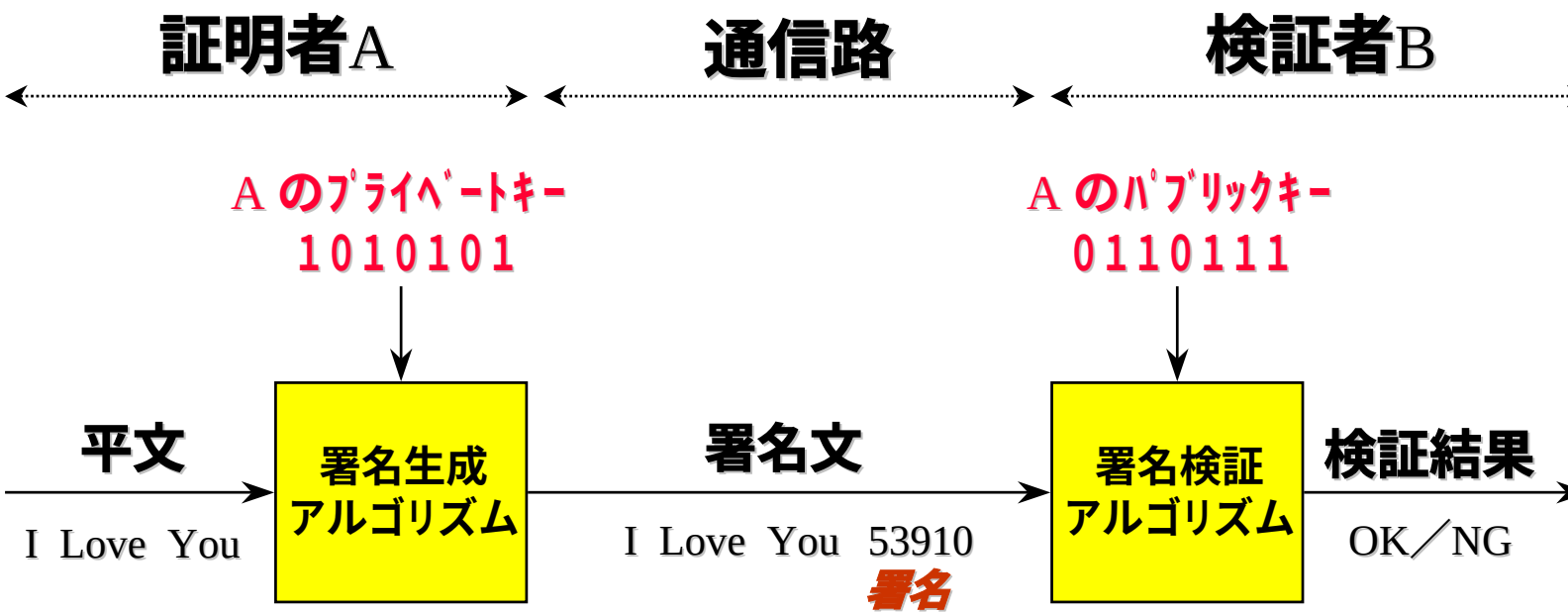
- 欧州の候補がAESに選定された
  - 政治的には意外，技術的には当然
- 将来世界のデファクト標準共通鍵暗号に
  - アメリカ政府公認，ライセンスフリー
- Triple-DES との住み分けは？
  - AES の本格的な普及は3～5年後
- 日本標準暗号は必要か
  - 必要との認識が多数　ただし決定機関なし
- Target Specific Cipher は生き残る

公開鍵暗号の原理



- 暗号化鍵と復号鍵が異なっている（各人がペアで用いる）
- 暗号化鍵の方は公開しても安全性が保たれる

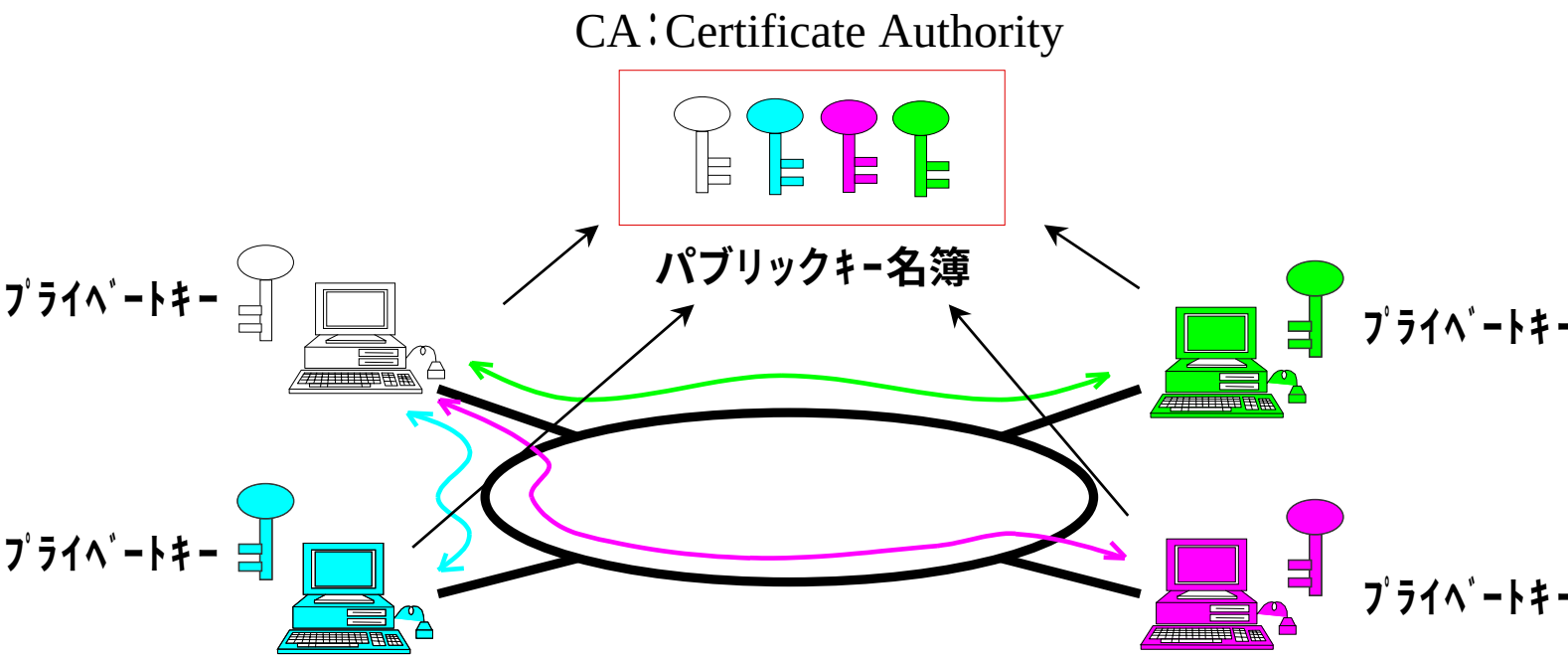
ディジタル署名（電子署名）



- 署名を生成できるのは Private Key を持っている A だけ
- だれもが A の署名の正当性を確認することができる
- ネットワーク暗号における最も重要な機能

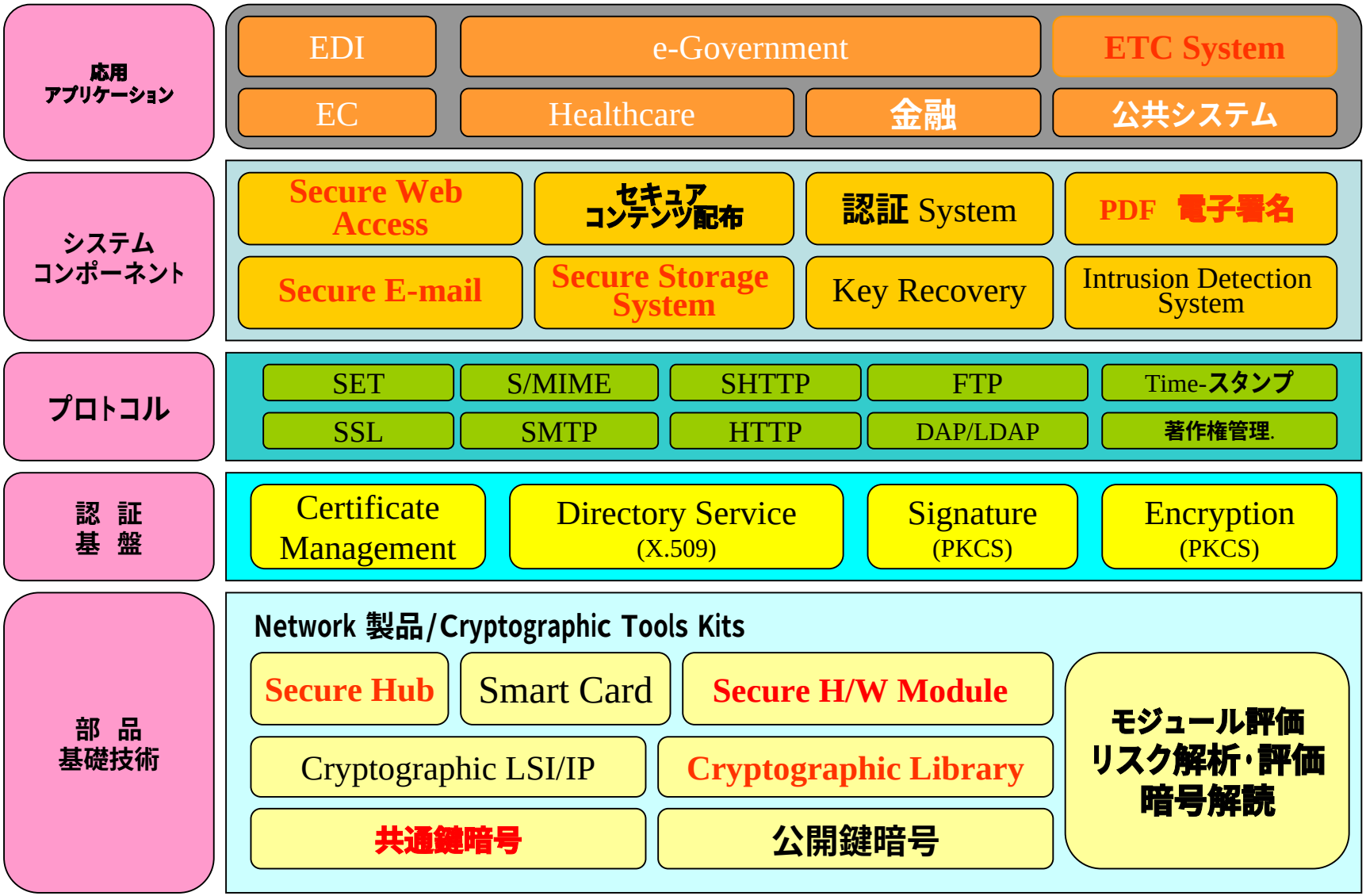
ｵｰﾌﾟﾝﾈｯﾄﾜｰｸでの暗号ﾓﾃﾞﾙ

PKI (Public Key Infrastructure)



- 各ユーザーは自分のﾌﾟﾗｲﾍﾞｰﾄｷｰだけを管理すればよい
- 送信相手のﾊﾟﾌﾞﾘｯｸｷｰはＣＡの名簿を参照して得る
- ﾒｯｾｰｼﾞは共通鍵暗号で暗号化し、その鍵を公開鍵暗号で暗号化

情報セキュリティの階層



暗号技術関連の標準化

- ISO/IEC JTC1 SC27
  - IS9979：**暗号の登録制→破綻** (13/24)
  - NW18033：**新たな標準化を検討中**
- IETF：Internet**での標準化**
  - **強度評価なし**
- CRYPTREC：**電子政府での標準暗号**
- NESSIE：**欧州の標準暗号**

業界標準（1）

- FIPS（**米国政府調達標準**）
  - FIPS 46-2：DES
  - FIPS 74：Guidelines for using DES
  - FIPS 81：DES modes of operation
  - FIPS 102: Guidelines for certification & accrediation
  - FIPS 112: Password usage
  - FIPS 113：Data authentication (CBC-MAC)
  - FIPS 140-1：Cryptomodule security requirements
  - FIPS 171：Key management using X9.17
  - FIPS 180-1：Secure Hash Standard (SHA-1)

業界標準（2）

- FIPS（米国政府調達標準）－続
  - FIPS 181：Automated Password Generator
  - FIPS 185：Key Escrow (Clipper & Skipjack)
  - FIPS 186：Digital Signature Standard (DSS)
  - FIPS 188: Standard Security Labels for Info Transfer
  - FIPS 190-191: Guidelines for Authentication & Analyzing LAN
  - FIPS 196：Entity Authentication

業界標準（3）

- PKCS (Public-Key Cryptography Standards)
  RSA Laboratories **から発行された仕様で、各種アルゴリズムをベースとしたセキュリティ技術の利用を標準化するという試みで、関連のデータをＡＳＮ．１等の抽象構文で定義したものである。**

(1)PKCS #1: RSA Encryption Standard
(2) PKCS #3: Diffie-Hellman Key Agreement Standard
(3) PKCS #5: Password-Based Encryption Standard
(4) PKCS #6: Extended-Certificate Syntax Standard
(5) PKCS #7: Cryptographic Message Syntax Standard
(6) PKCS #8: Private-Key Information Syntax Standard
(7) PKCS #9: Selected Attribute Types
(8) PKCS #10: Certification Request Syntax Standard
(9) PKCS #11: Cryptographic Token Interface Standard
(10) PKCS #12: Personal Information Exchange Syntax Standard
(11) PKCS #13: Elliptic Curve Cryptography Standard

URL http://www.rsa.com/rsalabs/pubs/PKCS/

業界標準（4）

- IETF（インターネット標準）
  - RFC 1319-21：MD2, MD4, MD5
  - RFC 1421-24：PEM
  - RFC 1508, 2025, 2078：GSS-APIRFC 1510: Kerberos V5 Network Authentication
  - RFC 1828：Keyed MD5
  - RFC 1848：Security Multiparts for MIME(S/MIME)
  - RFC 1938：One-time Password System
  - RFC 1968-69：PPP Encryption
  - RFC 1991, 2015：PGP
  - RFC 2401, 2408-9, 2412：IPSEC

業界標準（5）

- ISO
  - X.509
    X.500シリーズ（ディレクトリ）の中で認証書の形式を規定した標準
  - CC(Common Criteria)
    セキュリティ評価基準を規定した標準
    rating：11クラスの機能要件、10クラスの保証要件に基づいた8つの保証レベル（EAL 0～7）からなるクライテリア

業界標準（6）

- X.509
  ITU－T（国際電気通信連合電気通信標準化部門）のX.509勧告で定められた公開鍵認証書の形式
- **記載事項**
  - X.509のバージョン番号
  - 認証証のシリアル番号
  - 署名アルゴリズムID
  - 発行者（認証機関）名
  - 証明証の有効期限
  - ユーザ名
  - 公開鍵情報（アルゴリズム種別、パラメータ）
  - 発行者ID
  - ユーザID
  - 拡張領域

Edition	ISO Document No.	ITU-T Document No.
Edition 1 (88)	ISO/IEC 9594-8 : 1990	CCITT Recommendation X.509 (1988)
Edition 2 (93)	ISO/IEC 9594-8 : 1995	ITU-T Recommendation X.509 (1993)
Edition 3 (97)	ISO/IEC 9594-8 : 1997	ITU-T Recommendation X.509 (1997)
Edition 4 (Planning)	ISO/IEC 9594-8 : 200x?	ITU-T Recommendation X.509 (200x?)

ISO9979 暗号登録制度

- ISOにおいてDES の標準化失敗をうけて成立
- どんな暗号アルゴリズムも登録可能
- アルゴリズムを公開する必要もない
- 国内での登録申請は IPA が実施
- 安全性などの保証は一切ない
- 登録番号を交付されることにﾋﾞｼﾞﾈｽ上意義
- 最近、再度標準化を行う方向で進んでいる

ISO 登録暗号一覧（2000年12月）

B-CRYPT	BT(UK)	1992
IDEA	Ascom(CH)	1993
LUC	LUC(NZ)	1994
DES	NCS(US)	1994
CDMF	IBM(US)	1994
Skipjack	NSA(US)	1994
RC4	RSADSI(US)	1994
RC2	RSADSI(US)	1994
MULTI2	Hitachi(JP)	1994
FEAL	NTT(JP)	1994
BARAS	ETSI(FR)	1995
SXAL/MBAL	Laurel Intelligent Systems (JP)	1995
MISTY1	Mitsubishi Electric(JP)	199
ENCRiP	NEC(JP)	199
ACR	SAGEM(FR)	199
FWZ1	Check Point Software(IL)	199
SPEAM1	Matsushita (JP)	199
ELCURVE	Hitachi (JP)	199
CIPHERUNICORN-E	NEC(JP)	199
M8	Hitachi (JP)	199
GCC	International Information Science Institute (JP)	200
TRIPLO	Toshiba (JP)	200
FSAngo	Fuji Soft ABC (JP)	200

ISO/IEC JTC1/SC27暗号標準化

ISO/IEC WD 18033-1/-2/-3/-4 Encryption Algorithms

- ９９年末に再び暗号の標準化に方向転換
- 公開されたアルゴリズムに限定
- 各国の国内委員会に候補提案を要請
- 共通鍵暗号とともに公開鍵暗号も標準化の対象
- 早ければ２００３年に標準化される可能性
- ＩＳＯは国（地域）が一票を投じて決定する

NESSIE プロジェクト (1/3)

- 欧州委員会が行なう欧州暗号標準化計画
  New European Schemes for Signatures, Integrity, and Encryption
- ２００２年末までの３年間のプロジェクト
- ＡＥＳと同じく公募を行なったのち選考する
- 専門家からなるボードメンバーが中心になる
- 選考方法などの詳細は現時点では未定
- ボードメンバーも有力な投稿者
- http://cryptonessie.org/

NESSIE プロジェクト (2/3)

- **NESSIEの計画**

2000年1月	NESSIEプロジェクト開始
2000年3月	公募要項公開
2000年9月	公募締め切り
2000年11月13,14日	第1回 NESSIE会議(ベルギー
2001年9月12,13日	第2回 NESSIE会議 (イギリス)
2001年10月	第1次選考
2002年10月	第3回 NESSIE会議
2002年12月	最終選考

NESSIE 応募暗号一覧

公開鍵 (守秘)	ACE	IBM	共通鍵 (ストリーム)	BMGL	Hastard 他	Leviathan	Cisco
	ECIES	Certicom		LILI-128	Dawson 他	SOBER-t16	Qualcomm
	EPOC-1-2-3	NTT		SNOW	Johansson他	SOBER-t32	Qualcomm
	PSEC-1-2-3	NTT	共通鍵 (64ビットブロック)	CS-Cipher	CS Communication & Systems		
	RSA-OAEP	RSA		Khazad	Baretto, Rijmen		
公開鍵 (認証)	GPS	France Telecom		MISTY1	三菱電機	Nimbus	Machado
公開鍵 (署名)	ACE	IBM		Hierocrypt-L1	東芝	IDEA	Mediacrypt
	ECDSA	Certicom	共通鍵 (128ビットブロック)	Anibus		Baretto, Rijmen	
	ESIGN	NTT		Caemellia		NTT, 三菱電機	
	FLASH	BULL CP8		Grand Cru		Borst	
	QUARTZ	BULL CP8		Noekeon		Daemen 他	
	SFLASH	BULL CP8		Q		McBride	
	RSA-PSS	RSA		SC2000		富士通	
ハッシュ関数	Whirlpool	Baretto,Rijmen		Hierocrypt-3		東芝	
メッセージ認証	Two-Track-MAC	Boer, Rompay	共通鍵 (160ビット)	SHACAL		Gemplus	
	UMAC	Rogaway 他	共通鍵 (複数ビット)	RC6	RSA	NUSH	LAN Crypto
				SAFER++	Cylink		

NESSIE 第1次選考結果

公開鍵(守秘)	ACE (*)	IBM	共通鍵(ストリーム)	BMGL	Hastard 他		
	ECIES	Certicom				SOBER-t16	Qualcomm
	EPOC-2 (*)	NTT		SNOW	Johansson他	SOBER-t32	Qualcomm
	PSEC-2 (*)	NTT	共通鍵(64ビットブロック)				
	RSA-OAEP (*)	RSA		Khazad	Baretto, Rijmen		
公開鍵(認証)	GPS	France Telecom		MISTY1	三菱電機		
公開鍵(署名)						IDEA	Mediacrypt
	ECDSA	Certicom	共通鍵(128ビットブロック)				
	ESIGN (*)	NTT		Caemellia		NTT, 三菱電機	
	QUARTZ	BULL CP8					
	SFLASH	BULL CP8					
	RSA-PSS	RSA					
ハッシュ関数	Whirlpool	Baretto,Rijmen					
メッセージ認証	Two-Track-MAC	Boer, Rompay	共通鍵(160ビット)	SHACAL		Gemplus	
	UMAC	Rogaway 他	共通鍵(複数ビット)	RC6	RSA		
(*) はアルゴリズムの若干の変更があったもの				SAFER++	Cylink		

NESSIE プロジェクト (3/3)

- **NESSIEの最終目標は産学の「コンセンサス」**
  - ISO 等の標準化活動へのはたらきかけ
- **選考方法や選定アルゴリズム数は未定**
  - 必ずしも1つに絞り込むことが目標ではない
- **IPR (Intellectual Property Rights) Jungle**
  - NESSIE は応募アルゴリズムの IPR に対する強制力をもたない
- **選考結果は大きな影響力をもつ可能性**
  - 幅広い対象、超一流の主催者グループ、Industrial board との協調

国内における暗号標準化活動 暗号技術評価委員会 (1/3)

- CRYPTREC（Cryptography Research and Evaluation Committee）
- 2003年度の電子政府のセキュリティ基盤
- 暗号アルゴリズムを公募し選定する
- 専門的観点から評価しリストアップする
- 各省庁が暗号を利用する際の参考とする
- 2000年度は IPA の事業として実施
  (http://www.ipa.go.jp/security/)

国内における暗号標準化活動
暗号技術評価委員会 (2/3)

2000年度活動内容

暗号アルゴリズムの募集

共通鍵暗号、公開鍵暗号、ハッシュ関数、乱数生成法等

第1次スクリーニング評価

CRYPTREC 委員による書面審査

第2次詳細評価

内外の研究者に安全性･性能評価を委託

最終報告書作成･公開

http://www.ipa.go.jp/security/enc/CRYPTREC

国内における暗号標準化活動
暗号技術評価委員会 (3/3)

2001年度活動内容

総務省（TAO），経済産業省（IPA）の共同開催

暗号アルゴリズムの募集と評価

昨年度すでに評価したものについては、継続した詳細評価を
実施するか、「監視対象」として登録

その他のアクティビティ

SSL**プロトコルの評価、電子政府暗号の要件調査**

最終報告書作成･公開

http://www.ipa.go.jp/security/enc/CRYPTREC

2001年度評価対象暗号一覧

公開鍵（署名）	ESIGN	NTT
	RSA PKCS#1 1.5	ー
	RSA-PSS	RSALAB
	DSA	ー
	ECDSA	ー
	ECDSA in SEC1	富士通/Certicom
公開鍵（守秘）	OK-ECDSA(*)	日立製作所
	EPOC-2	NTT
	HIME-R (*)	日立製作所
	RSA-OAEP	RSALAB
	ECIES in SEC1	富士通/Certicom
	NTRU (*)	NTT
公開鍵（鍵共有）	*DH*	ー
	ECDH in SEC1	富士通/Certicom
	OK-ECDH (*)	日立製作所
	PSEC-KEM (*)	NTT

共通鍵（ストリーム）	MULTI-S01	日立製作所
	MUGI (*)	日立製作所
共通鍵（64ビットブロック）	CIPHERUNICORN-E	日本電気
	Hierocrypt-L1	東芝
	MISTY1	三菱電機
	TripleDES	ー
共通鍵（128ビットブロック）	*Camellia*	NTT/三菱電機
	CIPHERUNICORN-A	日本電気
	RC6	東芝
	SC2000	RSALAB
	Rijndael	富士通
	AES	ー
ハッシュ関数	SHA-256,384,512	ー
	RIPEMD-160	ー
	SHA-1	ー
擬似乱数生成法	*PRNG based on SHA1*	ー

斜字体は「監視状態の暗号」、(*) はスクリーニング対象
その他は詳細評価対象

わが国の現状と課題（1）

- CRYPTRECの意義
  - 暗号技術の中立的評価
  - ユーザ（政府）自身による評価
- 現状
  - 2003年3月までに、推奨暗号（リスト)の完成
- 暗号技術評価の継続
  - 組織・体制づくりの整備が必要
  - 予算処置：「継続は力なり」

わが国の現状と課題（2）

- 公的情報セキュリティ技術評価機関への第一歩
- 暗号モジュール評価
  - 2002年10月：国際標準の提案
  - 暗号モジュール評価制度の検討着手
- 暗号プロトコルの安全性評価
- 情報セキュリティ評価基準等との整合
  - IS 15408、IS 17799、etc

ケーススタディ

三菱電機おける暗号技術開発

三菱電機での暗号技術研究の歴史

1985年～1990年 情報電子研究所　メディア部　情セG

- 黎明期（技術蓄積、文献研究中心、技術的には試行錯誤）

1990年～1995年 情報システム研究所　メディア部　情セG

- 基礎技術研究段階（ゼロ知識証明，線形解読法，DESの解読実験，等）

1995年 情報技術総合研究所 情報セキュリティ技術開発センター

- 基礎技術から製品展開（アプリケーションの模索）へ
  - （MISTY，PowerMISTY，Japan-Netシステム，暗号LSI, DVD-ROM著作権方式等）

1996年～ 情報技術総合研究所　情報セキュリティ技術部

- 実用化段階
  - 基礎技術開発：楕円暗号，暗号強度評価，KASUMI, Camellia, 量子暗号
  - 製品対応開発：ETCSAM, SMTK（認証ﾗｲﾌﾞﾗﾘ），CryptoSign，TRUSTWEB, CERTMANAGER(企業向け認証ｻｰﾊﾞ)侵入検知システム,電子カルテ,PDF署名,TurboMISTY他

基礎技術の蓄積と研究方針の確立

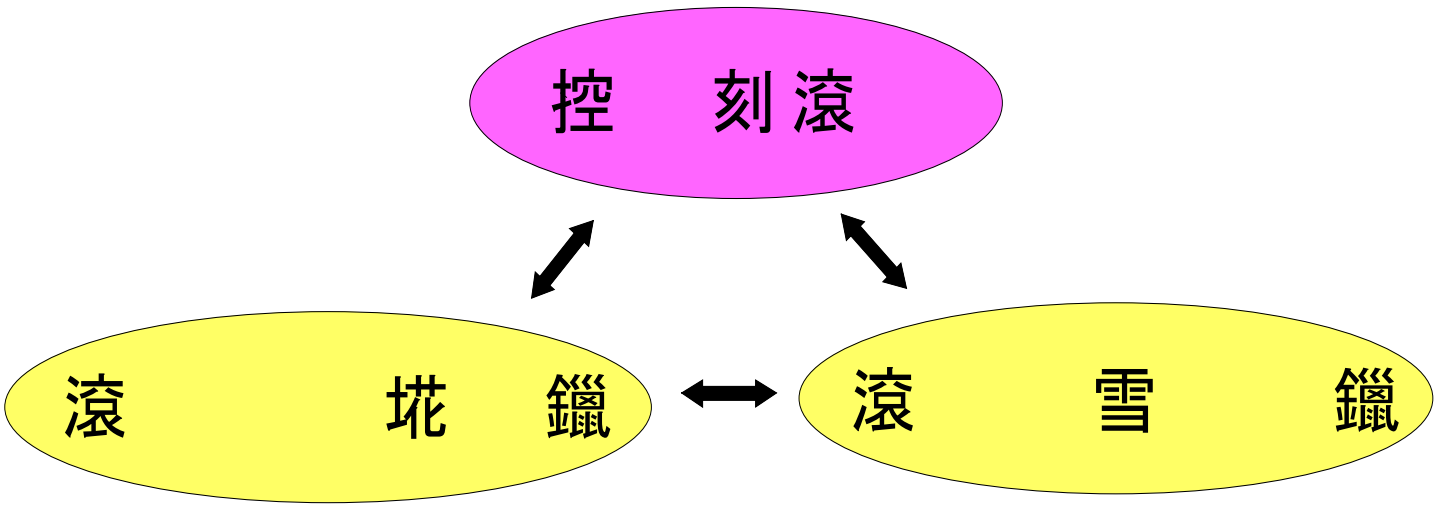
- 研究開発の発端
  - 興味本位，他者追従
  - アンダーグラウンド
  - 試行錯誤
- 研究方針の確立期
  - 独自コンセプトを目指して
  - “強い暗号”とは？

新規参入のための方針は？

応用用途
と
基礎技術

暗号技術と評価技術

“強い暗号”



“暗号強度評価指標”　　“暗号解読法”

暗号技術と評価技術

- 新規(独自)暗号技術“売り”は何か
  - 安全性
    - どうして「安全」なのか？
  - 強度評価＝解読の手間
- “線形解読法”の発見
  - DESが解けた!

新規技術(MISTY)の普及に向けて

- 「強い暗号」の開発
  - MISTYの公表
  - 「証明可能安全性」を持つ暗号
- 事業化への壁
  - 「アルゴリズム」≠「金」
  - 手軽に使える環境整備
    - 暗号LSI、暗号ライブラリー
  - 自社開発か、共同開発か

普及方策は？

電子政府に向けた法制度整備

施行・成立した法律・制度	平成6年10月　施行	●行政手続法施行
	平成10年7月　施行	●帳簿書類の電子データ保存制度 （電子計算機を使用して作成する国税関係帳簿書類の保存等の特例に関する法律）
	平成11年5月　成立	●情報公開法（行政機関の保有する情報の公開に関する法律）
	平成11年6月成立	●著作権法の改正
	平成11年8月　成立	●改正住民基本台帳法（住民基本台帳法の一部を改正する法律）
		●通信傍受法（犯罪捜査のための通信傍受に関する法律）
		●不正アクセス防止法（不正アクセス行為の禁止等に関する法律）
	平成12年10月　施行	●商業登記制度の電子化 （電気通信回線による登記情報の提供に関する法律案）
	平成12年11月　成立	●IT基本法（高度情報通信ネットワーク社会形成基本法）
	平成13年4月　施行	●電子署名・認証法（電子署名及び認証業務に関する法律）
今後予定される法律・制度		●確定申告（申告手続きの電子化等に関する法律） ●電子公証（電子公証制度に関する法律） ●個人情報・プライバシー保護法　他

自治体チャンネルVOL.17(99/12)より引用（出典：三菱総合研究所）＋最近動向

「高度情報通信ネットワーク社会形成基本法」（IT基本法）

平成12年11月29日成立、平成13年1月6日施行

内容：・高度情報通信ネットワークの拡充、コンテンツの充実、情報活用能力の習得の一体的推進
・電子商取引の推進
・電子政府、電子自治体の推進
・ネットワークの安全性及び信頼性の確保、個人情報保護
・研究開発の推進、国際的な協調及び貢献

狙い：IT革命に的確に対応し、高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に推進

効果：・全国民がITの成果を享受
・経済構造改革の推進
・活力ある地域社会の実現
・適切な官民の役割分担
・情報格差の是正
・雇用等の課題への対応

［備考］
① 政府が講じるべき施策（目標・達成期限）を定めた重点計画を策定
② 高度情報通信ネットワーク社会推進戦略本部を内閣に設置

公的機関の動向

情報セキュリティ分野の標準化作業と公的機関（政府・自治体等）公益企業（通信・金融・医療・電力・ガス・化学・物流等）へのISMS導入作業がグローバルに進められている

日本政府：
政府機関のホームページ改ざん事件を機に、「情報セキュリティポリシに関するガイドライン（BS7799を参考）」「重要インフラのサイバテロ対策に係る特別行動計画」を展開

金融庁：
金融検査マニュアルにセキュリティ確立について明記
参考：http://www.fsa.go.jp/

財団法人金融情報システムセンター（FISC）：
「金融機関等におけるセキュリティポリシー策定のための手順書（BS7799,ISO/IEC15408を参考）」を発行(平成11年1月)

管理系

技術系

＊ISO/IEC15408
情報技術セキュリティ評価基準

（暗号アルゴリズム標準化）

＊FIPS140-2（暗号製品）

汎用
＊BS7799
ISO/IEC17799
ISO/TR13335GMITS
＊JIPDEC ISMS制度

事業継続計画
WD18044
DRI

個人情報保護
＊JIS Q 15001

金融
ISO/TR13569
FISC

認証局
RFC2527
ECOMｶﾞｲﾄﾞﾗｲﾝ

個人情報保護
EU指令

電子署名法

製品/システム　マネジメントシステム　法制度

＊認定制度有り

情報セキュリティシステムの構築

- 利用環境（部品）はそろえた
- 応用用途の模索
  - 客先訪問
    - 「セキュリティ機能」は必要か
    - 「守る」対象は？
    - システムの運用と管理＝コスト
  - 複数からの選択
    - 選ぶ基準は、「暗号技術」？！

どうやって
売り込むか

研究者が楽になる
にはどうするか

伝道師