


# SC27における 情報セキュリティ標準化の動向



2001 - 07 - 23

**SC27専門委員会委員長**

**苗村 憲司**

(慶應義塾大学 大学院 政策・メディア研究科)

# 1. 情報セキュリティの意義と目的

## 1.1 情報化社会の安全性

- 情報化社会の安全性は、情報システムに依存
- (狭義の)安全性(safety)=機械の故障、ソフトウェアのバグ等による誤動作、誤操作、自然災害等によって確率的に生じるリスクを最小化すること
- セキュリティ(security)=意図的・組織的な犯罪行為・不正行為、大規模災害等によって非確率的に生じるリスクを最小化すること

# 1. 情報セキュリティの意義と目的

## 1.2 情報セキュリティの目的

- 1) 当初の目的＝情報システムに対する脅威（犯罪行為、不正行為、災害等）への防御
- 脅威の例：
  - 盗聴 → プライバシーの侵害、企業/国家秘密の漏洩
  - 改竄 → 虚偽の情報が事実とみなされる
  - 破壊 → 企業/個人にとって重要な情報の紛失
  - 不正侵入、コンピュータウィルス → 上のすべての脅威を生じる可能性

# 1. 情報セキュリティの意義と目的

## 1.2 情報セキュリティの目的

- 2) 新たな目的＝情報システムの新しい応用分野  
(電子現金、電子商取引、電子申請、電子決裁、  
電子投票、著作権管理等)における信用の確保
- 信用を害する例：
  - なりすまし → 他者による偽の取引
  - 当事者の特定 → 取引内容のプライバシー侵害
  - 事後否認 → 取引の当事者が債務を逃れる
  - 確認手段の欠落 → 情報の信憑性の喪失

## 2. 情報セキュリティの基盤技術

- 暗号(cipher)→秘密保護/秘匿(confidentiality)
- 相手認証(entity authentication)→なりすましの検出
- デジタル署名(digital signature)→なりすましの検出、改竄の防止
- データ完全性(data integrity)→改竄の検出
- アクセス制御(access control)→不正侵入、コンピュータウィスルの防止

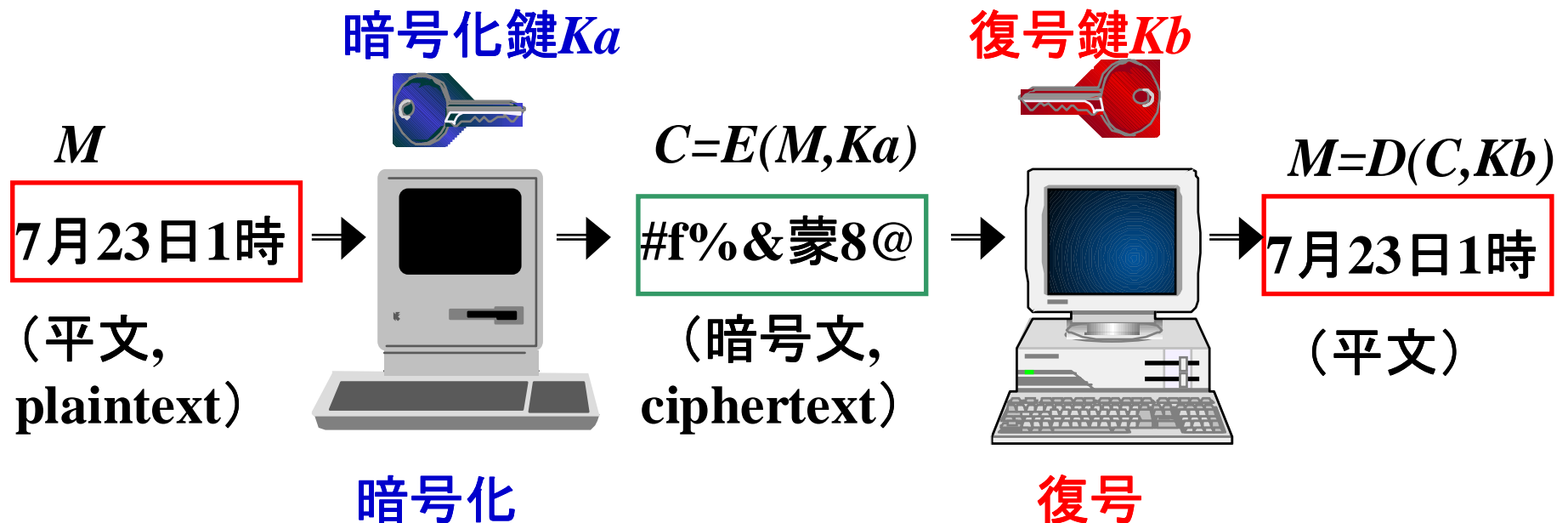
## 2. 情報セキュリティの基盤技術

- ファイアウォール(firewall)→不正侵入の防止
- 否認防止(non-repudiation)→公証(notarization)
- 電子透かし(watermark)→情報の流通経路検出
- 耐タンパー性(tamper-free)→秘匿、改竄防止
- ファイルの二重化(back-up)→破壊からの回復
- 監視(monitoring)・監査(audit trail)→脅威検出、原因追究

## 2. 情報セキュリティの基盤技術

### 2.1 暗号技術

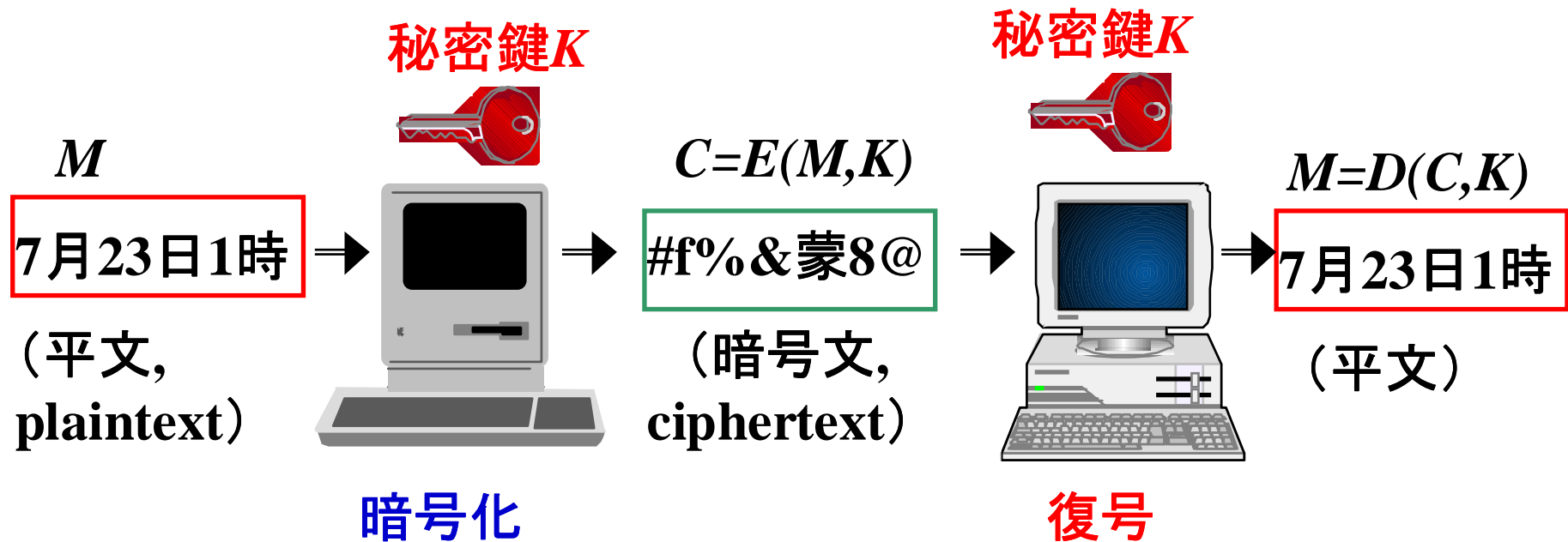
- 暗号化(encryption, encipherment)  
と復号(decryption, decipherment)



## 2. 情報セキュリティの基盤技術

### 2.1 暗号技術

#### ■ 対称暗号(共通鍵暗号、秘密鍵暗号)



## 2. 情報セキュリティの基盤技術

### 2.1 暗号技術

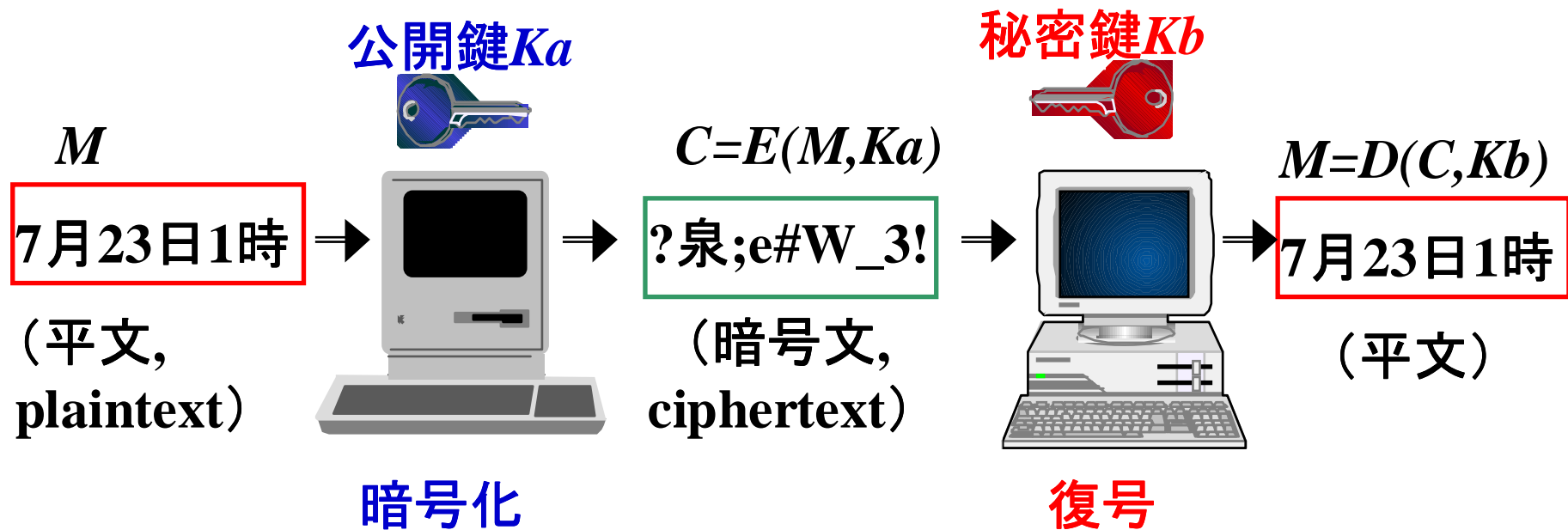
- 対称暗号（共通鍵暗号、秘密鍵暗号）
  - ブロック暗号
    - | 例：
      - | DES (Data Encryption Standard)、Triple DES
      - | IDEA、RC2、RC4、FEAL、MULTI2、MISTY1、
      - | Hierocrypt、Cipher-unicorn、Camellia、SC2000、
      - | AES (Advanced Encryption Standard) = Rijndael
  - ストリーム暗号
    - | 例：MULTI-S

# 2. 情報セキュリティの基盤技術

## 2.1 暗号技術

### ■ 非対称暗号(公開鍵暗号)

- $Ka$  から  $Kb$  を求めることは不可能であることが前提



## 2. 情報セキュリティの基盤技術

### 2.1 暗号技術

- 非対称暗号(公開鍵暗号)の例
  - 大きな整数の素因数分解の難しさに基づく方式
    - RSA (Rivest-Shamir-Adleman)、EPOC、HIME、ESIGN
  - 有限体上の離散対数問題の難しさに基づく方式
    - ElGamal、Diffie-Hellman、DSA
  - 楕円曲線上の離散対数問題の難しさに基づく方式
    - SEC1、PSEC、MY-ELLYTY ECMR

# 2. 情報セキュリティの基盤技術

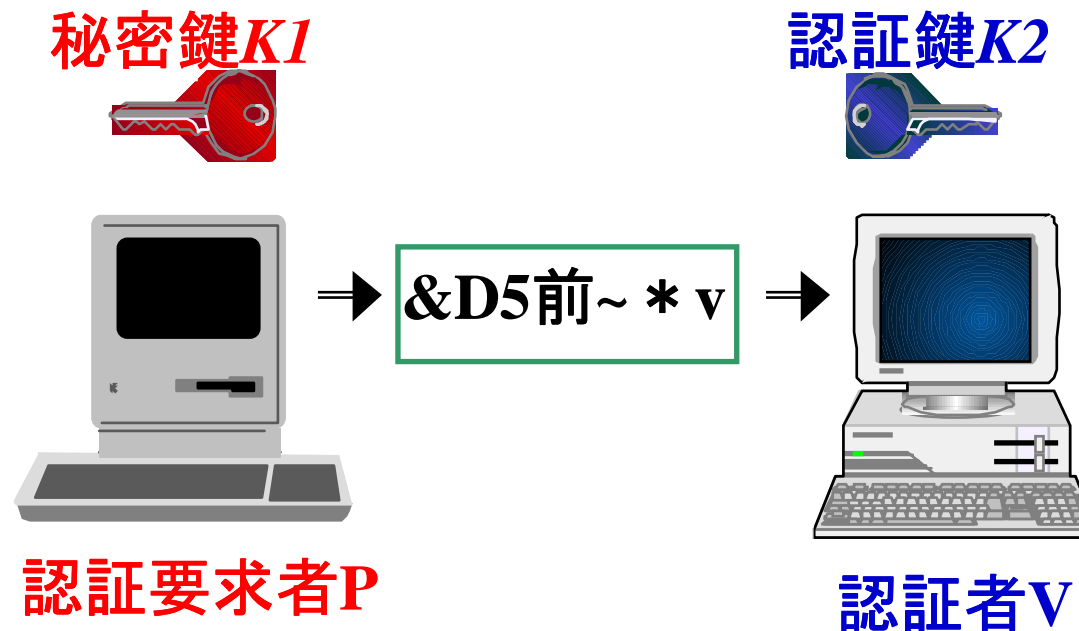
## 2.2 認証技術

- さまざまな認証 (authentication) 技術
- (1) エンティティ認証 (相手認証):  
なりすましができないことの検証
  - 個人認証
    - ┆ 本人のみが知っている情報を用いた認証
    - ┆ 本人のみが持っている物 (カード等) を用いた認証
    - ┆ 本人の身体的特徴 (指紋、声紋等) を用いた認証
  - 端末認証
- (2) メッセージ認証: 改竄がないことの検証

## 2. 情報セキュリティの基盤技術

### 2.2 認証技術

- 認証要求者 (prover) と認証者 (verifier)



## 2. 情報セキュリティの基盤技術

### 2.2 認証技術

- 対称暗号技術を利用して行う相手認証(原理):
- 要求者Pと認証者Vが秘密鍵Kを共有することにより、Vの相手がPであることを認証する
  - (1) PはVに認証を要求する
  - (2) Vは乱数rを生成してPに送る
  - (3) Pは  $E(r, K)$  をVに送る
  - (4) Vは  $D(E(r, K), K) = r$  を得て正当な相手であることを認証



## 2. 情報セキュリティの基盤技術

### 2.2 認証技術

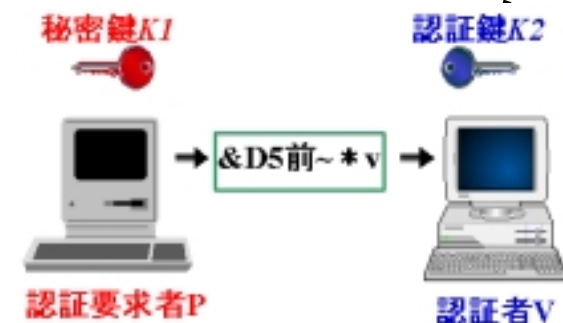
- 非対称暗号技術を利用して行う相手認証(原理):
- 要求者Pの真正の公開鍵 $K_p$ が公開され、秘密鍵 $K_s$ はPのみが所有することを前提として、Vの相手がPであることを認証する
  - (1) PはVに認証を要求する。
  - (2) Vは乱数 $r$ を生成して $E(r, K_p)$ をPに送る。
  - (3) Pは  $D(E(r, K_p), K_s)$  をVに送る。
  - (4) Vは受信した値が $r$ に一致することを確認して正当な相手であることを認証する。



# 2. 情報セキュリティの基盤技術

## 2.2 認証技術

- **メッセージ認証:**  
送信者Aと受信者Bが秘密鍵 $K_{ab}$ を共有することにより、Aの送ったメッセージMが改竄されずにBに届いたことを認証
- (1) AはMのダイジェスト $h(M)$ を計算し、メッセージ検証子 $E(h(M), K_{ab})$ をMに添付してBに送る
- (2) Bは受信したメッセージM'から $E(h(M'), K_{ab})$ を計算し、添付されたメッセージ検証子との一致を確認するより改竄がなかったことを認証



## 2. 情報セキュリティの基盤技術

### 2.2 認証技術

- デジタル署名（電子署名、電子捺印）：  
送信者Aの公開鍵Paが公開され、秘密鍵SaはAのみが所有することを前提として、Bの相手がAであること、並びに、Aの送ったメッセージMが改竄されずにBに届いたことを認証する
- (1) AはMのダイジェスト $h(M)$ を計算し、デジタル署名 $D(h(M), Sa)$ をMに添付してBに送る
- (2) Bは受信したメッセージM'とデジタル署名Cから $h(M')$ と $E(C, Pa)$ とを計算して一致を確認することにより、相手がAであること、および改竄がなかったことを認証する

## 2. 情報セキュリティの基盤技術

### 2.3 鍵配送技術

- 対称鍵暗号技術を利用して行う鍵配送 (Kerberos)
- 事前にA,Bは鍵配送センターSとの間でそれぞれ共有する秘密鍵 $K_{as}$ ,  $K_{bs}$  を入手しているものとする
- (1) AはSに通信当事者の名前(または番号)A,Bを送る
- (2) Sは Aに $E(T||K_{ab}||B, K_{as})$ ,  $E(T||K_{ab}||A, K_{bs})$  を送る。ここで、Tは時刻印
- (3) Aは  $E(T||K_{ab}||B, K_{as})$ を $K_{as}$ で復号してTと $K_{ab}$ を入手し、 $E(A||T, K_{ab})$ ,  $E(T||K_{ab}||A, K_{bs})$  をBに送る

## 2. 情報セキュリティの基盤技術

### 2.3 鍵配送技術

- 非対称鍵暗号技術を利用して行う鍵配送（認証機関CAを利用する方式）
- (1) Aは公開鍵 $P_a$ と秘密鍵 $S_a$ の対を生成し、 $P_a$ をCAに届ける。このときに、Aは何らかの身元証明を行う
- (2) CAはAの身元証明を確認し、デジタル署名 $D(h(P_a||A||\dots), S_{ca})$ をAに渡す
- (3) Aは $P_a||A||\dots$  と $D(h(P_a||A||\dots), S_{ca})$ をBに送る
- (4) Bは、デジタル署名を認証し、 $P_a$ を取り出す。次に共用鍵 $K_{ab}$ を生成し、 $E(K_{ab}, P_a)$ をAに送る
- (5) Aは $D(E(K_{ab}, P_a), S_a) = K_{ab}$ を得る

# 3. 情報セキュリティ技術の標準化動向

## 3.1 情報セキュリティ技術の標準化の必要性と問題点

- 1) 防衛的セキュリティ技術の標準化
- 必要性：一般の技術標準化と同様、例えば次2点
  - 量産による経済化（生産的機能ではないので特に安く）
  - 相互運用性（ネットワーク経由／ファイル共用等）
- 問題点：セキュリティ技術標準化に固有の問題点
  - 技術が公開されることにより、犯罪者に手の内を明かしてしまう
  - 技術が統一されることにより、それが破られたときは致命的状態になる

# 3. 情報セキュリティ技術の標準化動向

## 3.1 情報セキュリティ技術の標準化の必要性と問題点

- 2) 応用的セキュリティ技術の標準化
- 必要性: 一般の技術標準化の必要性に加え、
  - 新サービスの市場開拓には新技術開発を前提とする異業種協調が必要
- 問題点: 固有の問題点
  - 必要な標準の範囲が特に不明確 → de jure 標準化より de facto 標準化に適す

# 3. 情報セキュリティ技術の標準化動向

## 3.2 ISOにおける国際標準化の経緯

- 1) ISO/TC97における標準化(1987年以前)
  - SC16: Security Architecture (IS 7498-2), Security Framework (IS 10181)
  - SC20: 米国規格の暗号アルゴリズム(DES)のIS化を進めたが、米国の反対で中断
    - ┆ ⇒暗号アルゴリズムの登録制度(IS 9979)
- 2) ISO/IEC JTC1(1987年以降)
  - SC27: Security Techniques

## 3. 情報セキュリティ技術の標準化動向

### 3.3 国際標準化の枠組

- 情報システムのセキュリティの目的:  
OECD(1992年、情報システムのセキュリティのためのガイドライン)、JTC1/SC21等
  - (1) 利用可能性/可用性(Availability)
  - (2) 機密性/秘匿性(Confidentiality)
  - (3) 一貫性/完全性(Integrity)

# 3. 情報セキュリティ技術の標準化動向

## 3.3 国際標準化の枠組

- 新しい応用に対応するため、目的を拡大
- SC 27「ITセキュリティマネジメントガイドライン」(GMITS)第1部(TR 13335-1)では、上の3項目に加えて次の3項目を定義
  - (4) 釈明義務/責任追跡性(Accountability)
  - (5) 新憑性/真正性(Authenticity)
  - (6) 信頼性(Reliability)

# 3. 情報セキュリティ技術の標準化動向

## 3.3 国際標準化の枠組

- OECD 暗号政策ガイドライン (1997年3月)
  - 1. 暗号機能の信頼性
  - 2. 暗号機能の自由選択
  - 3. 市場の要求に基づく暗号機能の開発
  - 4. 暗号機能の標準
  - 5. プライバシーおよび個人情報の保護
  - 6. 法執行のためのアクセス
  - 7. 責務
  - 8. 国際協力

SC27の主な担当領域

IT Security

Availability

Confidentiality

Integrity

Reliability

Accountability

Authenticity

Cipher

Data Integrity

Digital Signature

Non-repudiation

Entity Authentication

Guidelines for Management of IT Security

Evaluation Criteria



# 3. 情報セキュリティ技術の標準化動向

## 3.4 ISO/IEC JTC1/SC27の活動状況

- SC27(幹事国:ドイツ)
  - WG1:情報セキュリティ要求条件と統合技術(主査:英)
    - ┆ 国内委員会主査:中尾 康二(KDDI研究所)
  - WG2:セキュリティ技術とメカニズム(主査:ベルギー)
    - ┆ 国内委員会主査:櫻井 幸一(九州大学)
  - WG3:セキュリティ評価基準(主査:スウェーデン)
    - ┆ 国内委員会主査:田渕 治樹(製品評価技術基盤機構)

# 3. 情報セキュリティ技術の標準化動向

## 3.4 ISO/IEC JTC1/SC27の活動状況

- (1) 暗号と鍵管理(WG2)
- ブロック暗号の利用法(modes of operation)  
(IS 8372, IS 10116)
- 暗号アルゴリズム
  - 一般: WD 18033-1
  - 非対称暗号: WD 18033-2
  - ブロック暗号: WD 18033-3
  - ストリーム暗号: WD 18033-4

# 3. 情報セキュリティ技術の標準化動向

## 3.4 ISO/IEC JTC1/SC27の活動状況

- (1) 暗号と鍵管理(WG2)
- 鍵管理
  - 枠組み(IS 11770-1)
  - 対称技術を用いるメカニズム(IS 11770-2)
  - 非対称技術を用いるメカニズム(IS 11770-3)
  - 楕円曲線型の暗号関連(FDIS 15946-1,3)

## 3. 情報セキュリティ技術の標準化動向

### 3.4 ISO/IEC JTC1/SC27の活動状況

- (2) 相手(エンティティ)認証(WG2)
  - 一般モデル(IS 9798-1)
  - 対称技術利用(IS 9798-2): Kerberos に相当
  - 非対称(デジタル署名)技術利用(IS 9798-3)
  - 暗号検査関数を用いる(IS 9798-4)
  - ゼロ知識証明を用いる(IS 9798-5)

# 3. 情報セキュリティ技術の標準化動向

## 3.4 ISO/IEC JTC1/SC27の活動状況

- (3) データ完全性とデジタル署名 (WG2)
- メッセージ認証符号 (message authentication code; MAC)
  - ブロック暗号を利用 (IS 9797-1)
  - ハッシュ関数を利用 (FDIS 9797-2)
- 非対称技術を用いるデジタル署名技術
  - メッセージ復元型 (IS 9796-2,3)
  - 付録型 (IS 14888-1,2,3)
- 楕円曲線型のデジタル署名 (FDIS 15946-2,4)

## 3. 情報セキュリティ技術の標準化動向

### 3.4 ISO/IEC JTC1/SC27の活動状況

- (4) 否認防止(non-repudiation) (WG2)
  - 通信/処理の後にそれに関する事実を否認するような嘘の主張を防止
  - 一般モデル(IS 13888-1)
  - 対称技術利用(IS 13888-2)
  - 非対称技術利用(IS 13888-3)

## 3. 情報セキュリティ技術の標準化動向

### 3.4 ISO/IEC JTC1/SC27の活動状況

- (5) 暗号・認証等で利用する部品的機能(WG2)
  - ハッシュ関数(IS 10118-1,2,3,4)
  - タイムスタンプ(FCD 18014-1,2,3)
  - 乱数生成(WD 18031)
  - 素数生成(WD 18032)

## 3. 情報セキュリティ技術の標準化動向

### 3.4 ISO/IEC JTC1/SC27の活動状況

- (6) 信頼された第三者機関サービス(WG1)
- Trusted Third Party (TTP) Services の利用と管理の指針(TR 14516)
  - 用途例: 相手認証、否認防止、鍵管理、デジタル署名等のための認証機関(CA)
- TTPのデジタル署名への応用(IS 15945)

# 3. 情報セキュリティ技術の標準化動向

## 3.4 ISO/IEC JTC1/SC27の活動状況

- (7) セキュリティ評価基準(WG3)
- 評価基準(Evaluation Criteria for IT Security)  
(IS 15408-1,2,3)
  - 情報システム/製品の調達にあたり、提供者の設計書、プログラム等を検査するための基準  
(機能要件、保証レベルEAL1～EAL7)
  - 北米・欧州政府の共通基準(Common Criteria)を基に作成(1998年10月、5カ国相互認証締結)

# 3. 情報セキュリティ技術の標準化動向

## 3.4 ISO/IEC JTC1/SC27の活動状況

- (7) セキュリティ評価基準(WG3)
- 保護プロファイル登録手続 (FCD 15292)
- 保護プロファイルとセキュリティ目標の指針(WD 15446)
- ITセキュリティ保証の枠組み(WD 15443-1,2,3)
- ITセキュリティ評価方法(NP 18045)

## 3. 情報セキュリティ技術の標準化動向

### 3.4 ISO/IEC JTC1/SC27の活動状況

- (8) 情報システムのセキュリティ管理(WG1)
- ITセキュリティマネジメントガイドライン(GMITS)  
(TR 13335-1,2,3,4,5)
  - 情報システムの運用にあたり、管理者が実施することが望ましい手段、方法のガイドライン
- 情報セキュリティ管理の実践規範 (IS 17799)
  - BS 7799 Part 1 の Fast Track による IS化

# 3. 情報セキュリティ技術の標準化動向

## 3.4 ISO/IEC JTC1/SC27の活動状況

- (8) 情報システムのセキュリティ管理(WG1)
- ITネットワークセキュリティ(WD 18028)
- セキュリティ情報オブジェクト(IS 15816)
- 侵入検出の枠組み(DTR 15947)
- 侵入検出システムの実装・運用・管理指針(WD 18043)
- セキュリティインシデンス管理(WD 18044)

# 3. 情報セキュリティ技術の標準化動向

## 3.5 当面の課題

- 暗号アルゴリズムのIS化対策
  - 電子政府用暗号技術評価(CRYPTREC)との整合
  - 暗号アルゴリズム登録制度(IS 9979)の運用の見直し
  - IEEE, NESSIE, IETF等との関連
  - 技術開発元と製品調達元との独立性
- IS 17799 の見直しへの対処
  - 国内条件と運用経験の仕様へのフィードバック
  - 認定制度への対処

## 4. 今後の課題

- 構造改革(全面的情報化) 情報セキュリティが重要
  - 電子政府システムのセキュリティ
  - 民間情報システムのセキュリティ
- 情報セキュリティの特性に応じた対策
  - 悪意の攻撃に対する防御策(性悪説に基づく対処が必要)
  - システム導入時の対策に加えて運用・管理の対策が重要
    - 悪意の攻撃を想定した防御のための管理手続きが必要
    - セキュリティ管理に関わる人材の育成が重要
- 日本としての情報セキュリティ政策の必要性