



情報法・政策 (第四回 :10月23日 )  
< 暗号 :情報社会のインフラ >

---

社会情報研究所  
助教授 田中 秀幸



# オープンネットワークで構築された情報社会

- 専用回線を用いたEDI(Electronic Data Interchange)とは異なり、インターネットは誰でもアクセス可能。
- インターネットでは、WEB状にデータが流通し、不特定のコンピュータ・システムが介在。第三者による関与の余地大。
- デジタル化された情報は、容易に改竄可能。

# オープンなネットワーク

(出典 :情報処理振興事業協会資料)





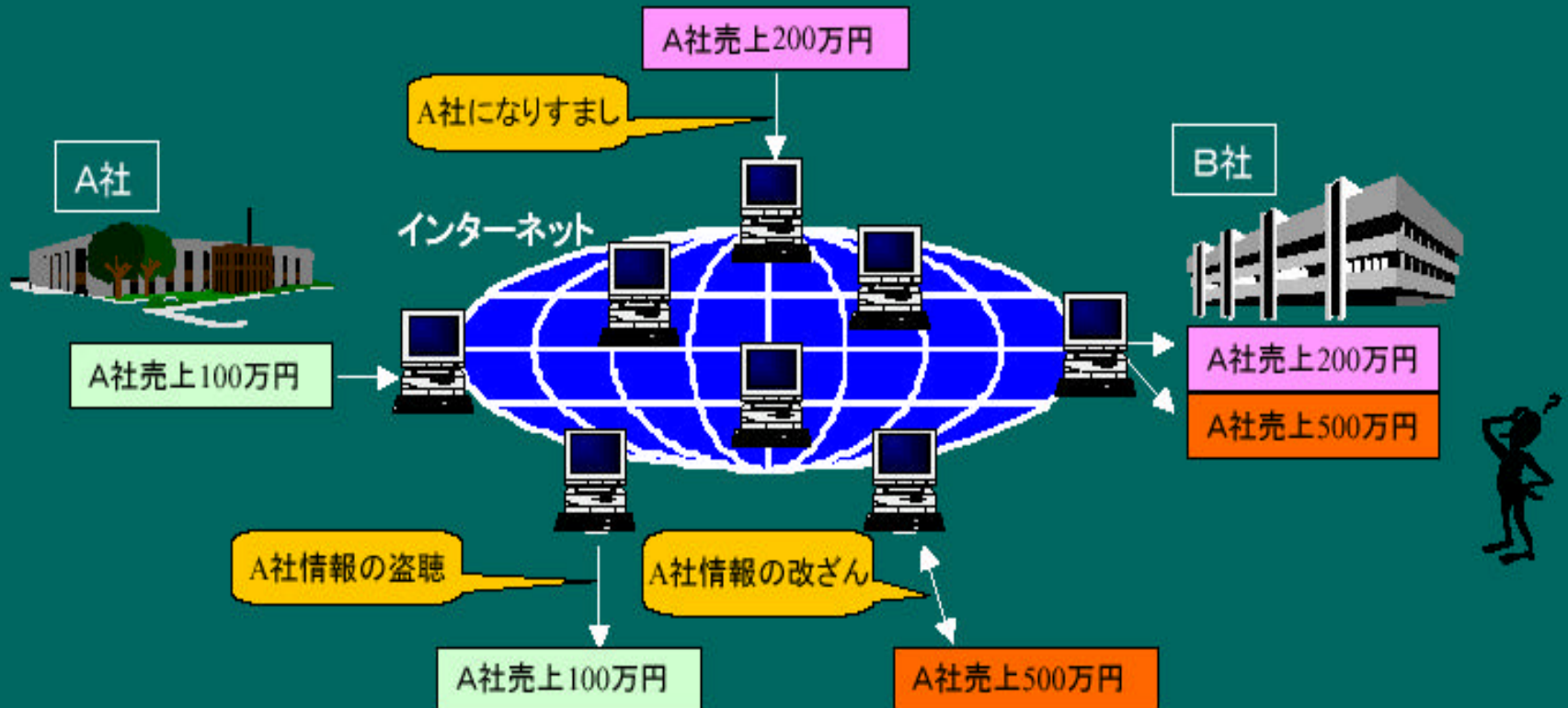
# デジタル社会のリスク (1)

---

- 情報の盗聴、漏洩、改竄
- なりすまし

# デジタル社会のリスク (2)

(出典 :情報処理振興事業協会資料)





# サーバー空間での暗号の役割

## 秘匿 (又は機密保持)

- 交換する情報や文書の中が第三者に漏れないようにする (盗聴防止)。

## 認証 (最近認識されてきた機能)

- 真を保証し、偽を防ぐ (辻井)。
- なりすまし、伝送否認、情報改竄などの情報通信ネットワーク上での不正行為やトラブルに対抗する手段。



# 暗号の利用例

---

電子商取引

電子マネー

携帯電話・PHS

ITS(Intelligent Transport System)

遠隔医療・電子カルテ

電子政府

などなど



# 暗号とは何か

---

**暗号**とは、一定の規則に従って文章 数などを他の表現に変えて、その規則を知らない人には元が何かをわからなくする技術。

**復号**とは、暗号文を元に戻すこと。

暗号化鍵とは、暗号化の規則。

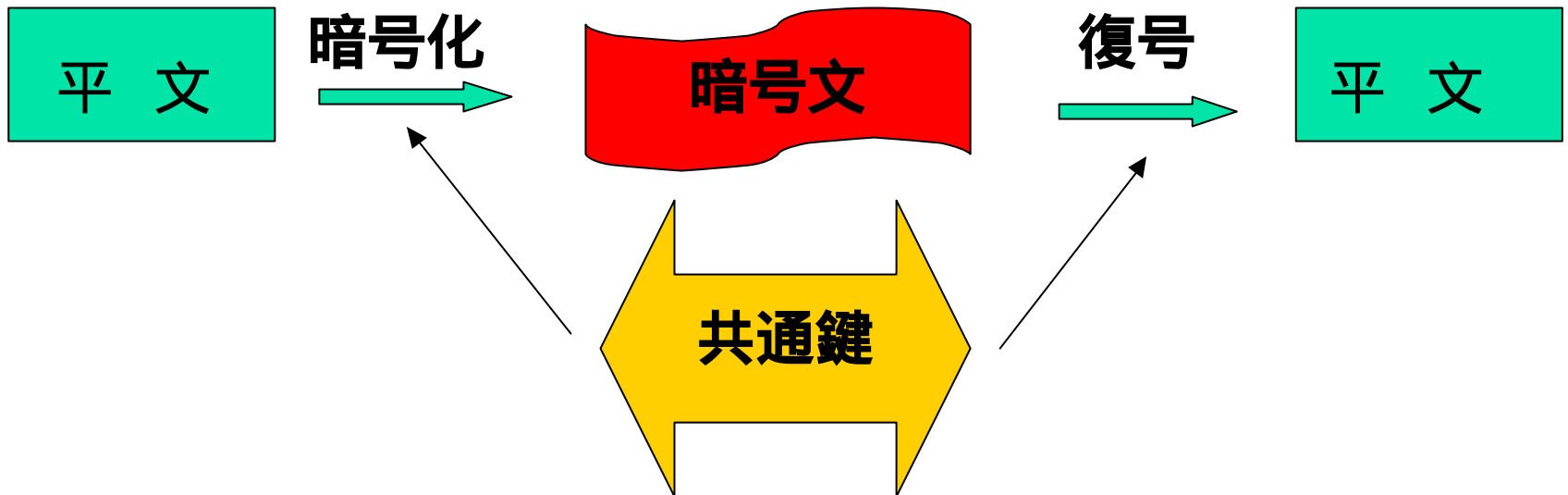
(例)

TODAI <=> UPEBJ

(アルファベットを一字ずらす)

# 暗号の種類 (共通鍵暗号)

暗号化と復号で同一の鍵を用いる。  
鍵を事前に共有する。





# 暗号の種類 (公開鍵) 1

---

- 公開鍵と秘密鍵 (個人鍵) がペア
- 公開鍵 : 不特定の相手に使用してもらうために公開。
  - 秘密鍵 : 自分だけが秘密に保管。



## 暗号の種類 (公開鍵) 2

---

暗号化

公開鍵を暗号鍵、秘密鍵を復号鍵

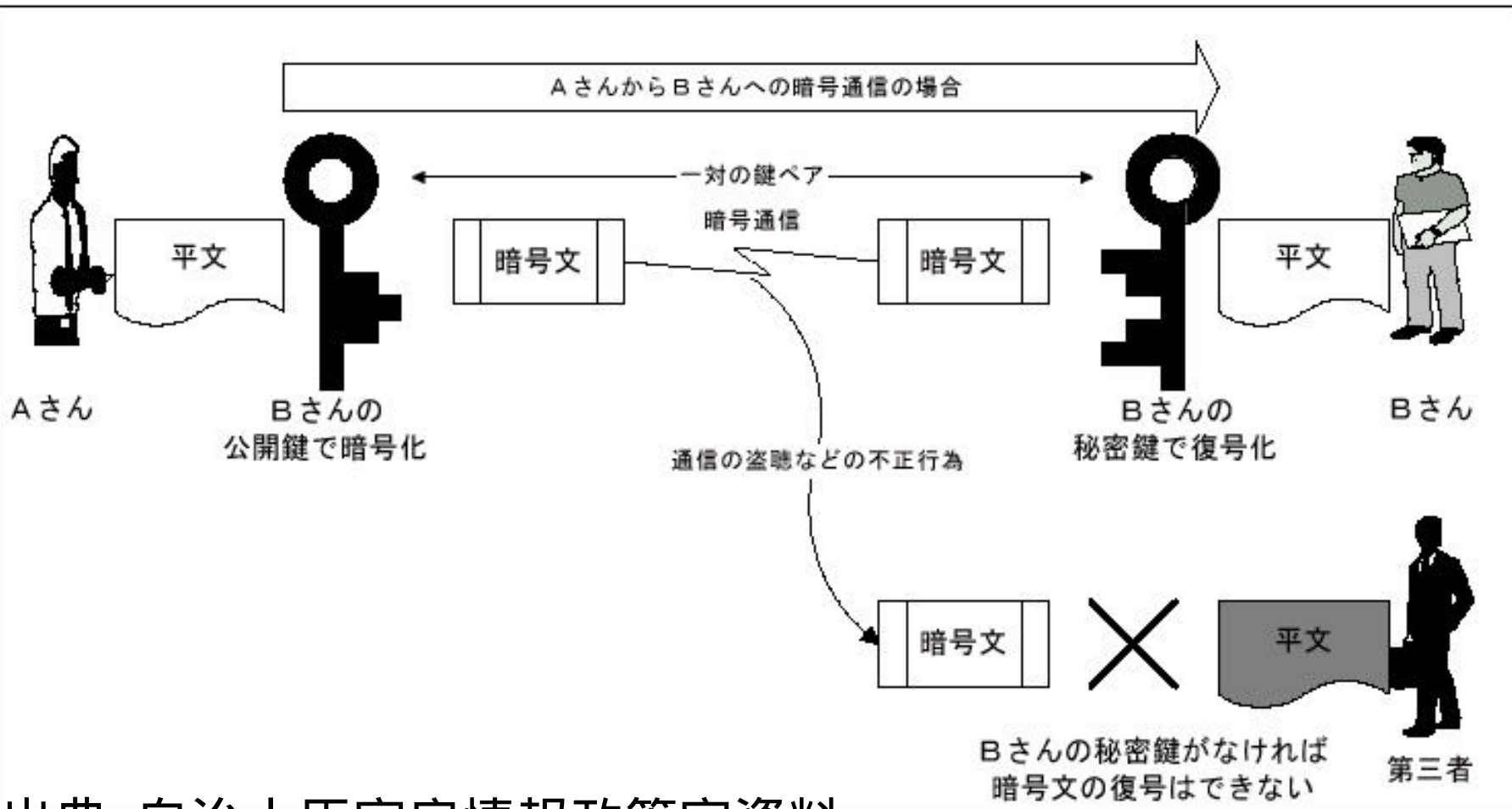
認証

秘密鍵を暗号鍵、公開鍵を復号鍵

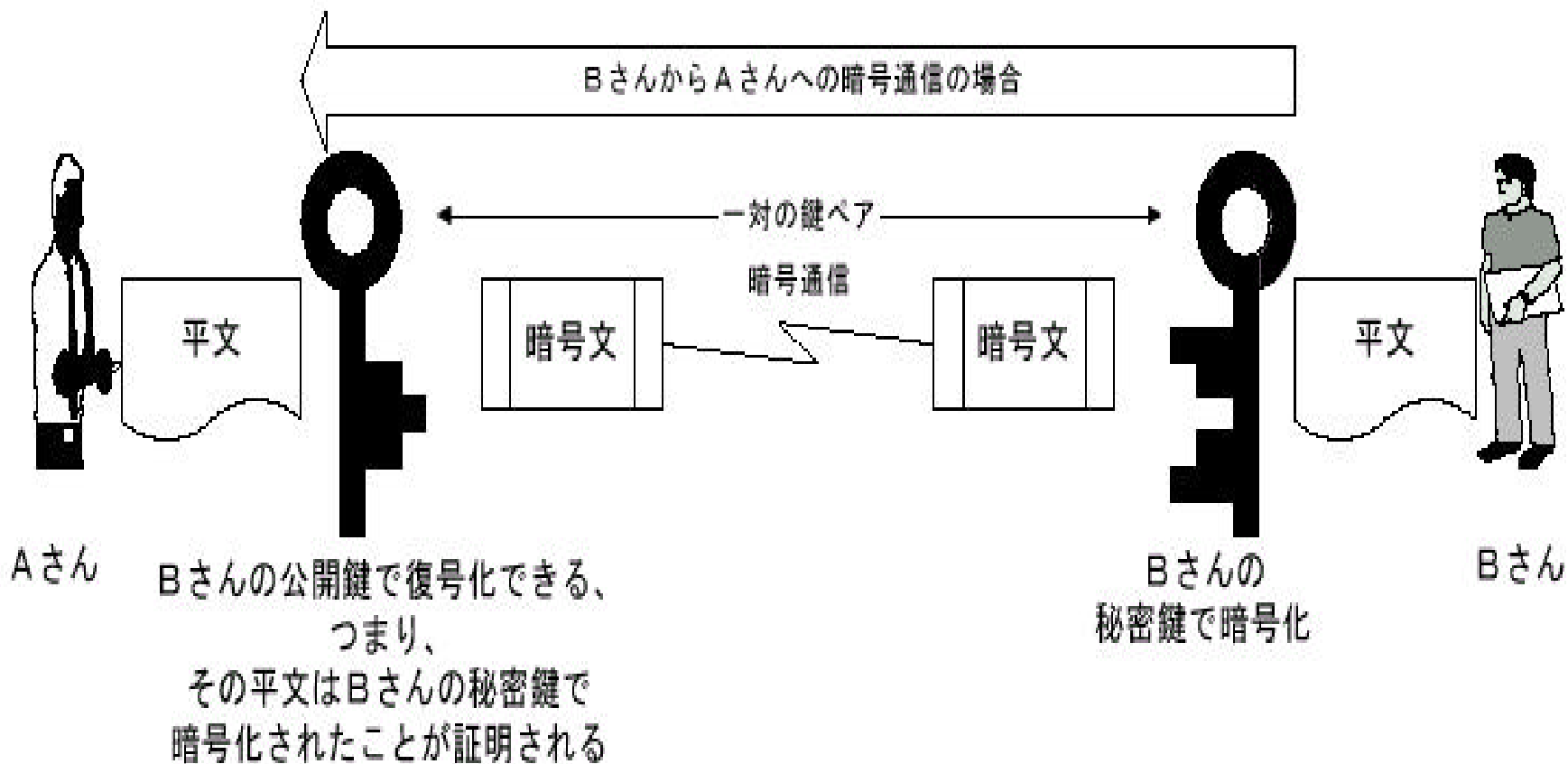
有名な公開鍵暗号

RSA (Rivest, Shamir, Adleman)

# 公開鍵による暗号化



# 公開鍵による認証





# 共通鍵暗号と公開鍵暗号の相違点 1

---

## -共通鍵暗号

通信相手毎に配布し、それぞれの鍵を管理（1対多の構築が困難。又はビッグ・ブラザーの存在が必要）

## -公開鍵暗号

鍵の配送を公然と行うなど管理が容易（1対多の構築が容易）

= > 公開鍵はインターネットの時代にふさわしい暗号方式



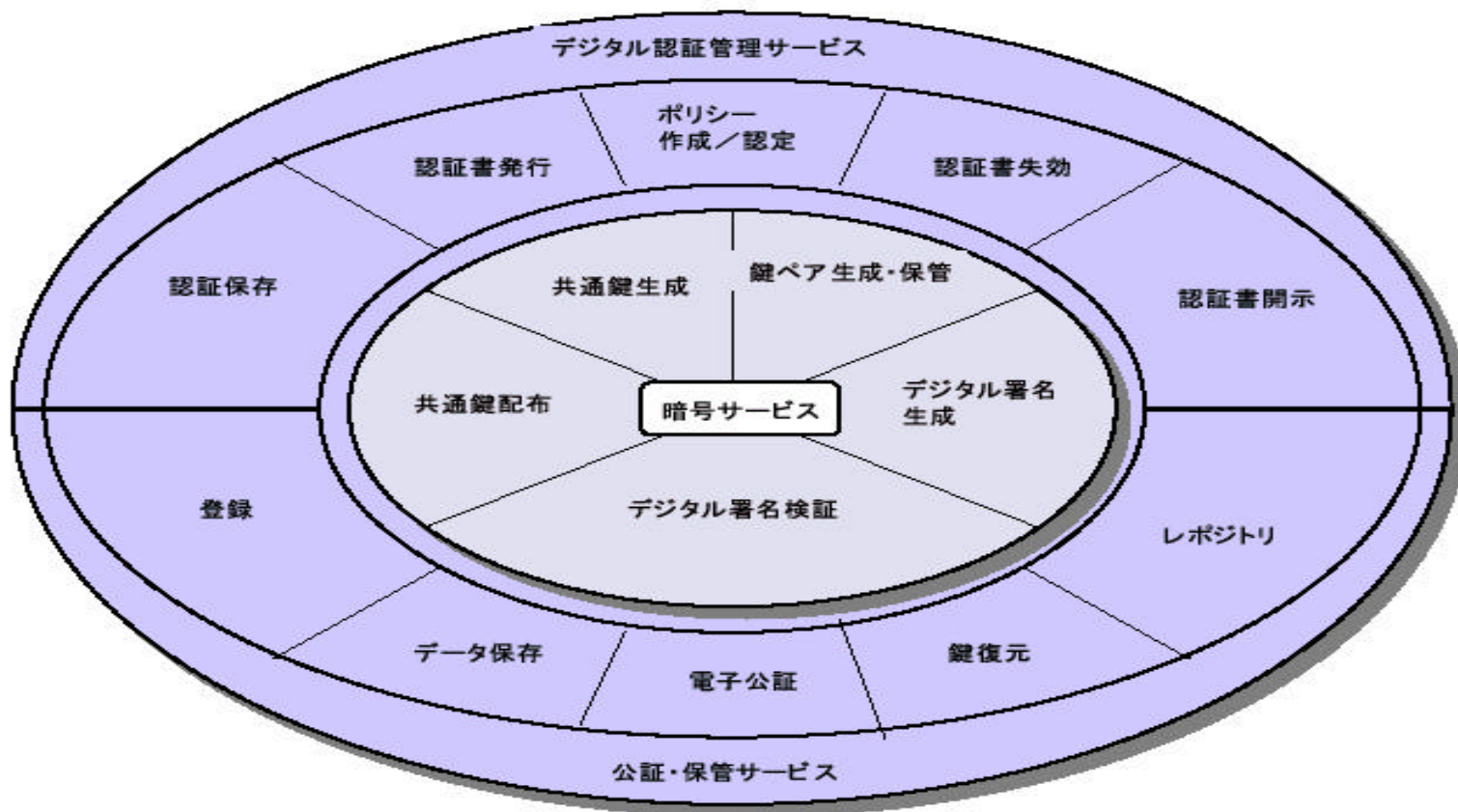
# 共通鍵暗号と公開鍵暗号の相違点 2

---

## 性能の相違

公開鍵暗号の方が、共通鍵暗号に比べて鍵長が長いいため、暗号・復号化の処理時間が長い。

# PKI公開鍵基盤,Public Key Infrastructure



公開鍵基盤の構成

認証局運用ガイドラインV1.0版平成10年3月  
電子商取引実証推進協議会認証局検討WG



# 暗号政策の体系

---

貿易管理

鍵寄託・回復

電子署名・認証制度

暗号技術の標準化

(辻井の整理による)



# 暗号の貿易管理政策 (ワッセナー・アレンジメント)

## WA 通常兵器を規制するレジーム

(1996年発足、ココムに代わるもの)

目的 : 国際の安全及び安全の維持

(注) 大量破壊兵器不拡散レジーム

NSG (原子力供給国グループ) 原子力関係

AG (オーストラリアグループ) 化学・生物兵器関係

MTCR : ミサイル関係



# 貿易管理関係の国内法制

---

根拠法

外国為替及び外国貿易法

規制の態様：

規制対象品目の輸出に当たっては、通商  
産業大臣の許可が必要

規制内容

ワッセナーアレンジメント等の国際合意に  
基づく



# 暗号の貿易管理の影響・問題

---

PHS (端末認証機能、秘話機能など)  
ブラウザ搭載パソコンの輸出  
米国の暗号貿易管理戦略  
インタangible・テクノロジー・トランスファー  
問題