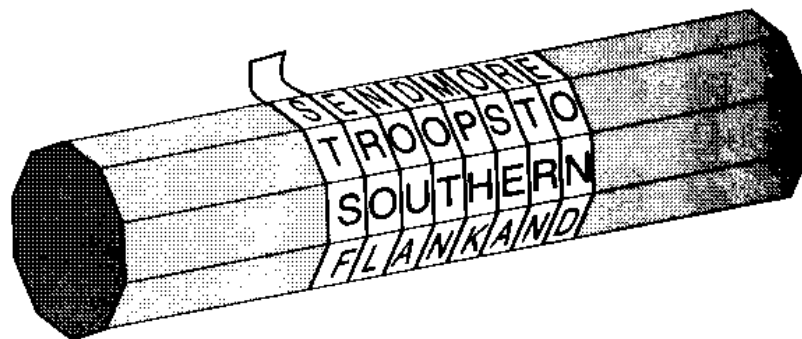


[暗号の歴史と現代暗号(3章)]

- 現代暗号の幕開け: DES暗号(1977)
- 現代暗号と歴史的暗号の違い
アルゴリズムは公開される
鍵を秘密にしておけば安全
- 共通鍵暗号と公開鍵暗号(1976)
- 共通鍵暗号の分類
ブロック暗号とストリーム暗号
- 共通鍵暗号の操作モード

[暗号の歴史(1)]

スキュタレー(Scytale)暗号(転置式暗号の一種)
紀元前5世紀頃、スパルタ



サイモン・シン、青木薫訳、暗号解読、新潮社
p.27 より引用

[暗号の歴史(2)]

シーザー暗号：アルファベットを決まった数だけずらす

ABCDEFGHIJKLMNOPQRSTUVWXYZ



暗号化

DEFGHIJKLMNOPQRSTUVWXYZABC

例： BOYS BE AMBITIOUS



ERBVEHDPELWLRXV

キョウキョウキョウキョウキョウキョウ

シャーロックホームズ：踊る人形

(単) 換字暗号

→文字の出現頻度を用いて簡単に解読することができる

[暗号の歴史(3)]

- ホモフォニック暗号
一つの文字に複数の文字を対応させる
ことで暗号化する
→文字の出現頻度を平均化する
- ホモフォニック暗号の解読
連接する文字の出現頻度を調べる
- ルイ14世(17世紀)の暗号など
2世紀の間、解読されなかった

[暗号の歴史(4)]

ビジネル暗号：文字ごとに変換方法を変える方法

鍵語： A B C D E F G H I J K L M N O ...

シフト量： 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 ...

例：

平文： MY FAVORITE SONG

鍵語： DO GDOGDOGD OGDO


暗号文： PM LDJU UWZH GUQU

→繰り返し現れる文字列から鍵語の長さを推定でき、
解読できる

符号化(encoding)と 暗号化(encryption)?

(広い意味では)符号化

DEVIL → † 8¶60

NEVER → 

あんごう → 11 03 25 *1 13

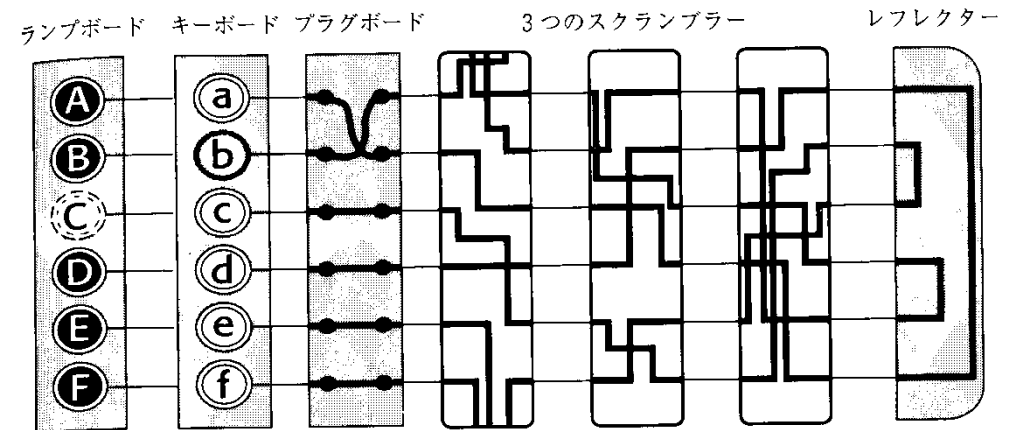
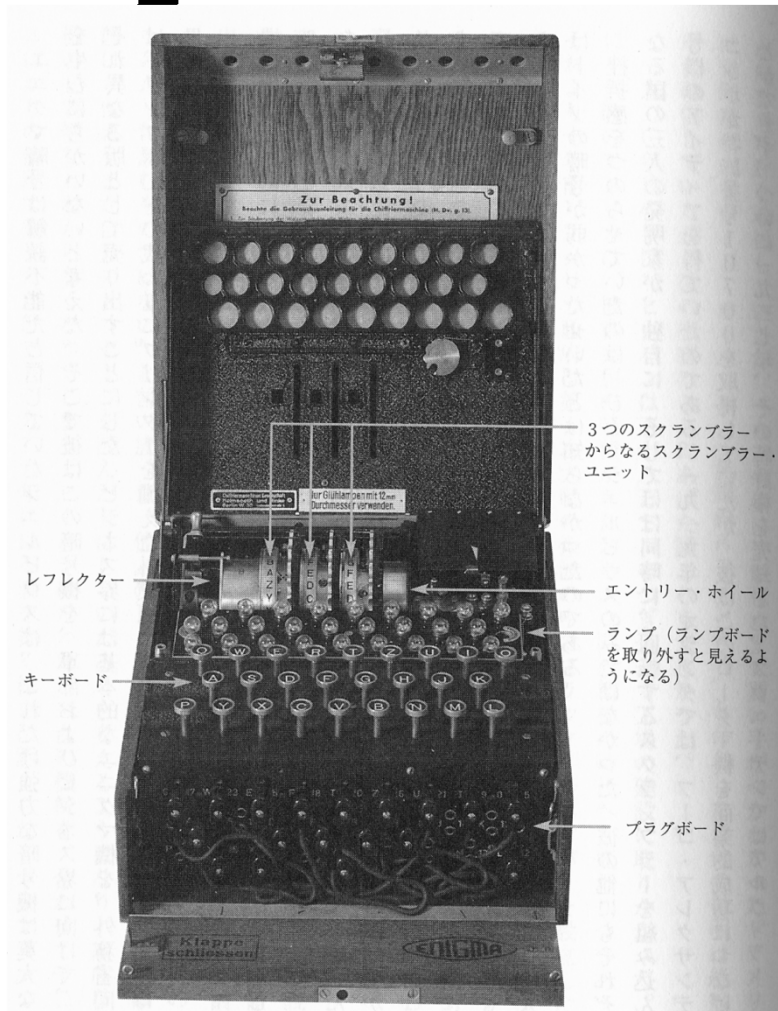
→ 符号化(変換方法が一定)

GOLD $\xrightarrow{\text{POE}}$ VCPS

\searrow_{DOYLE} JCJO

→ 暗号化(変換方法が鍵により変化)

[エニグマ暗号]



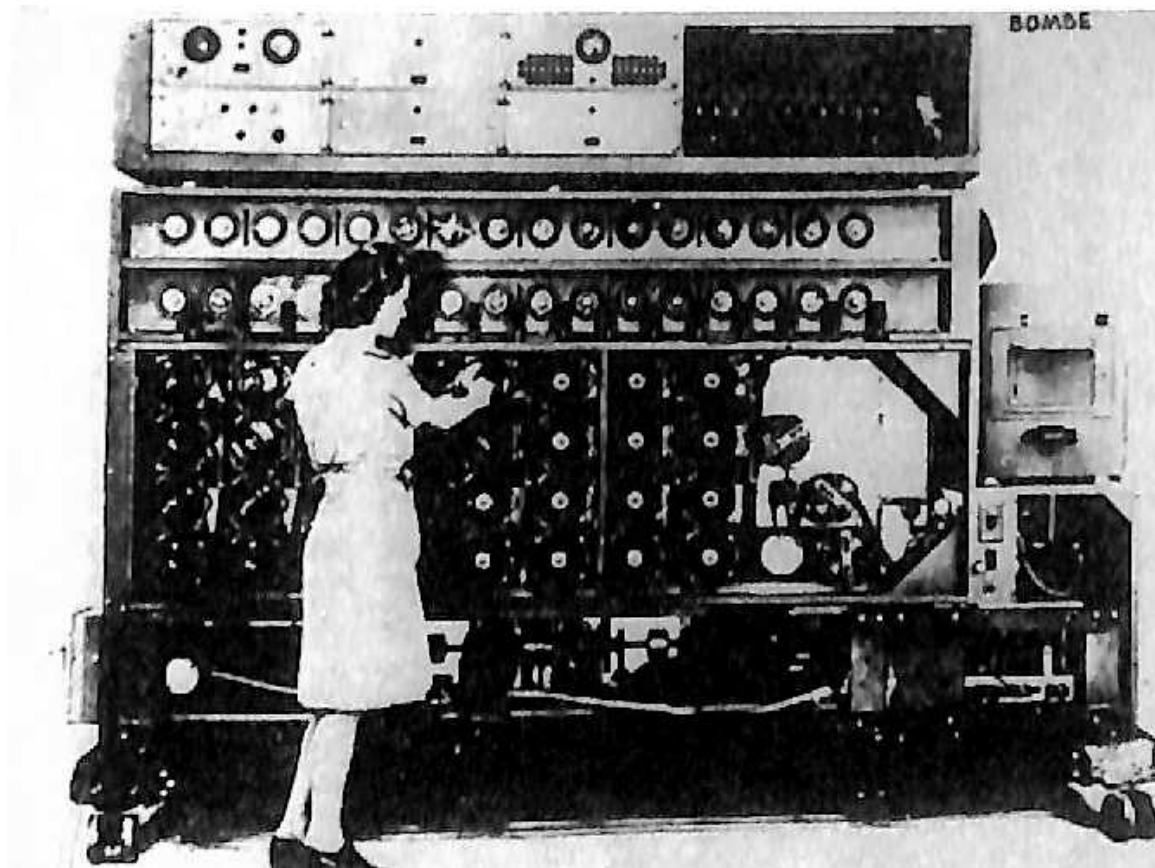
鍵の総数:

$$\begin{aligned} & 26 \times 26 \times 26 \quad (\text{スクランブラの向き}) \\ & \times 6 \quad (\text{スクランブラーの配置}) \\ & \times 26C_6 \quad (\text{プラグボードのつなぎ方}) \\ & = 10^{16} \quad (1京) \end{aligned}$$

鍵の総数が十分大きいことは必要だが十分ではない

サイモン・シン、青木薫訳、暗号解読、新潮社、p.188, p.193 より引用

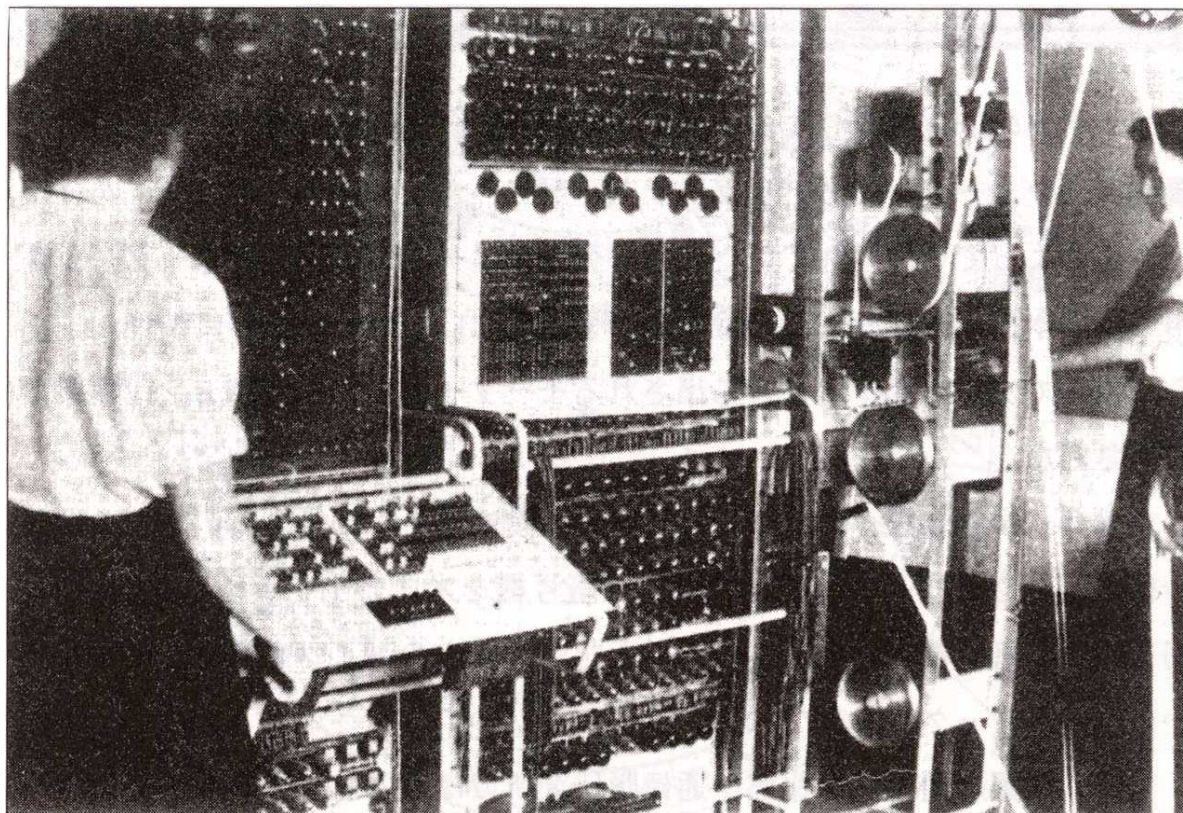
[暗号解読器(1)]



- Bombe(ボンブ): 1940年にイギリスのアラン・チューリング率いるエニグマ暗号解読チームが開発
- エニグマの解読とチューリングの生涯をテーマにした映画「イミテーション・ゲーム／エニグマと天才数学者の秘密」(2014)でも描かれている

サイモン・シン「暗号解読」, 2001(新潮社), p.244より引用

[暗号解読器(2)]



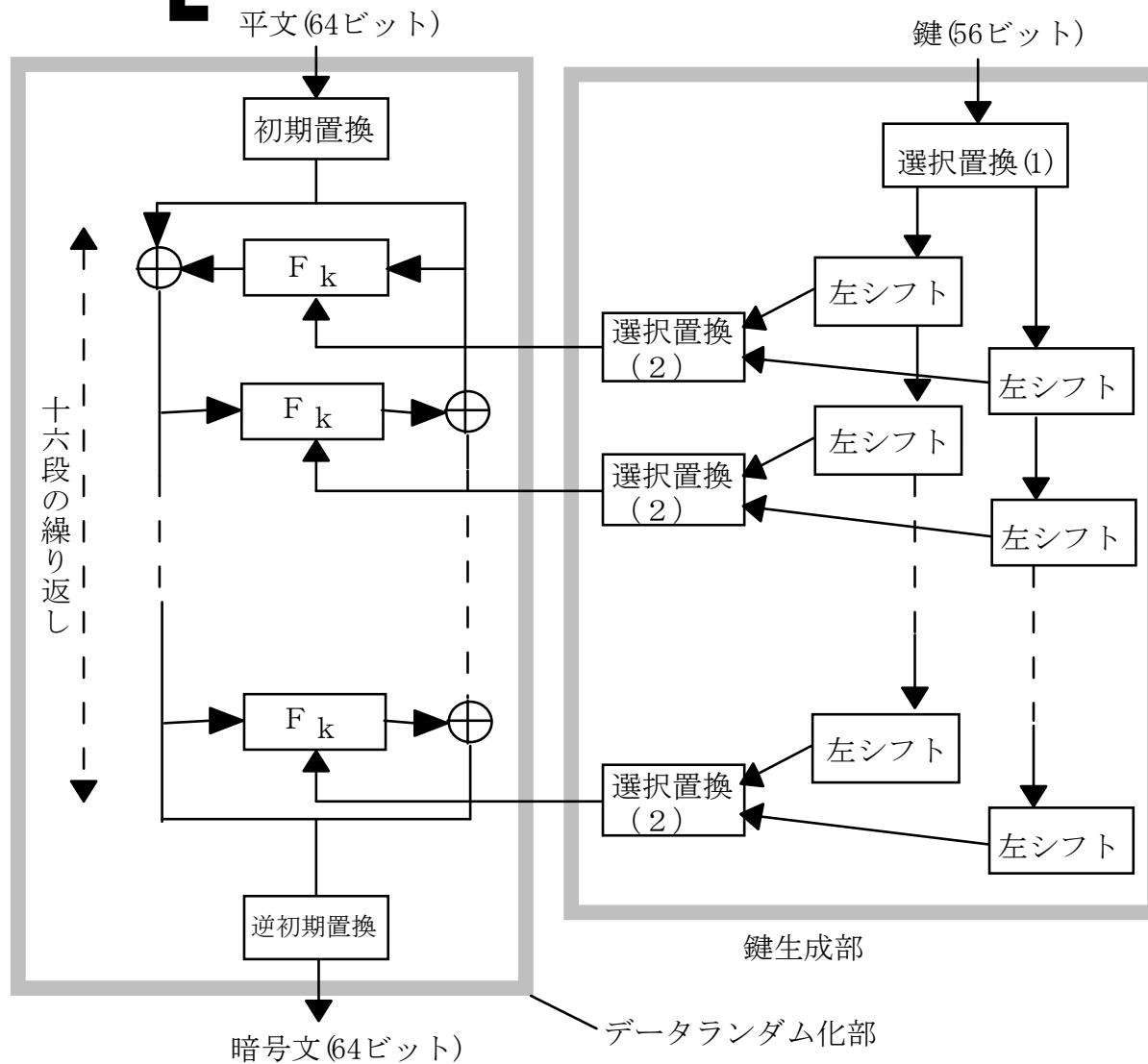
コロツサス(Mark II) 1944～

吹田智章著、暗号のすべてがわかる本、技術評論社、p.55より引用

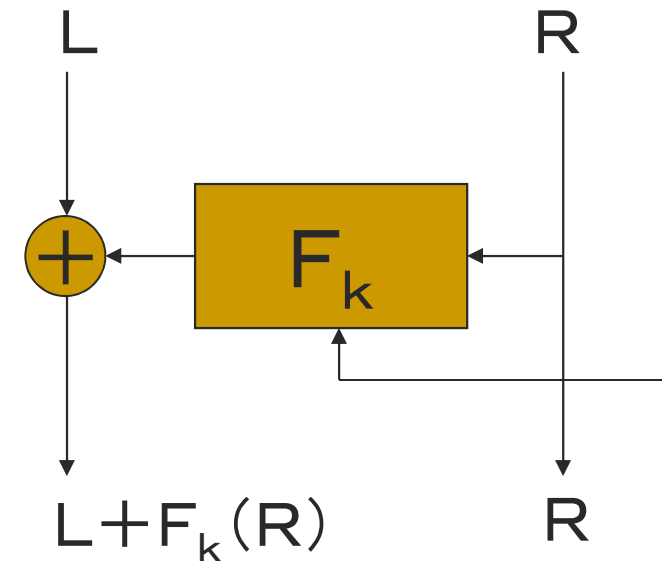
[共通鍵暗号]

- 共通鍵暗号(⇔公開鍵暗号)
 - ブロック暗号(ブロック単位で暗号化)
DES、AES、IDEAなど
 - ストリーム暗号(バイトまたはビット毎に暗号化)
同期式、非同期式
- 標準化(アルゴリズムの公開)が重要
 - 広範囲で利用できる
 - 安全性を第3者が評価、保証できる
 - 装置やソフトウェアが安価に実現できる

DES暗号(1976年)



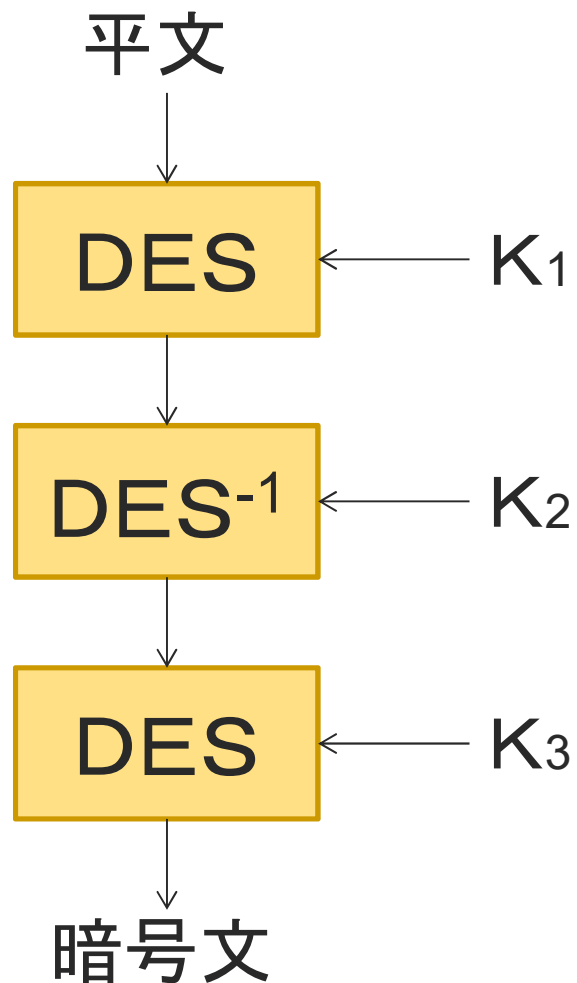
- 一般(ビジネス)用途
- 仕様(アルゴリズム)公開



DES暗号の基本ブロック

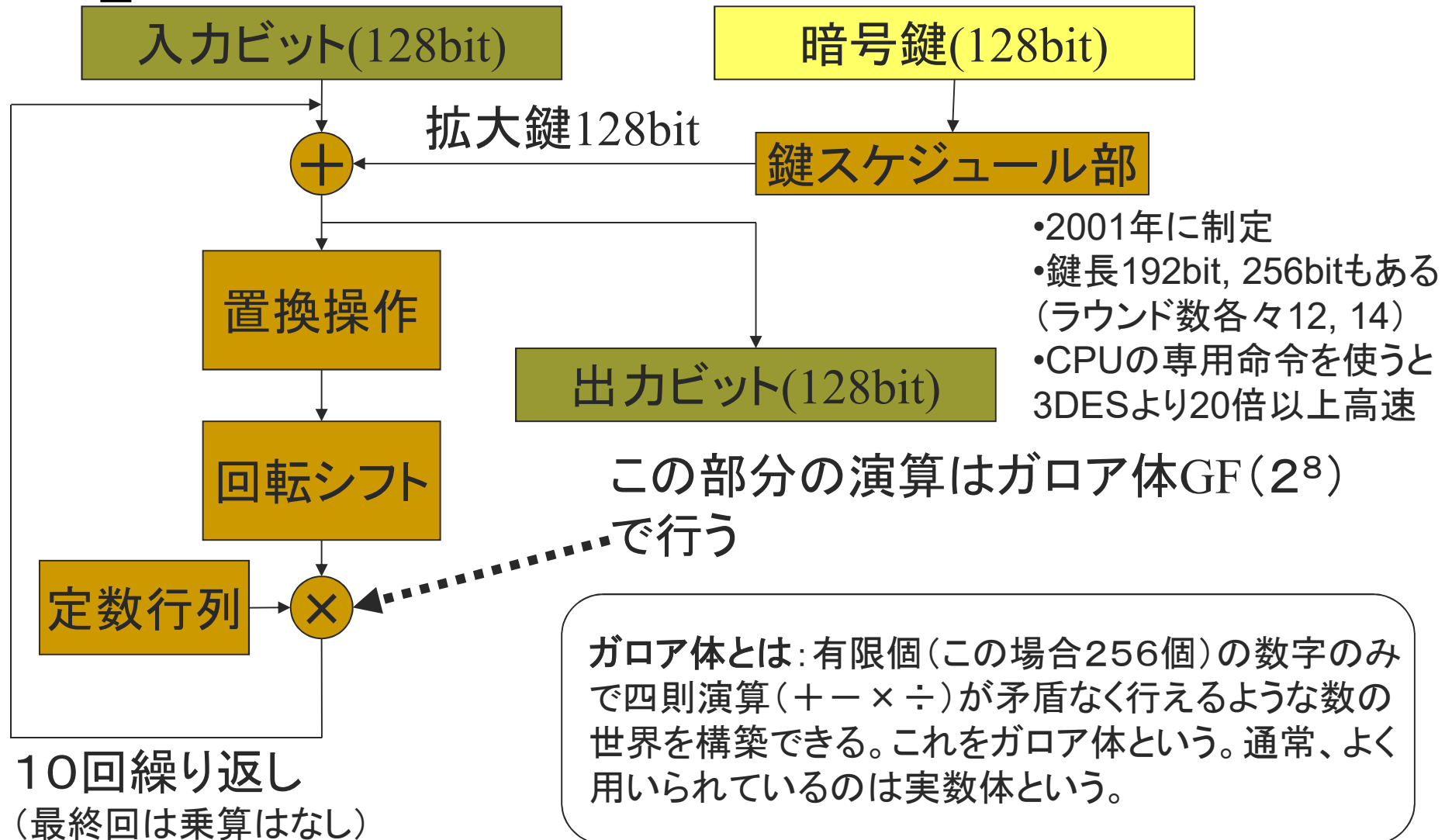
- 1994 線形解読法による解読 (松井)
- 1999年には1日以下で解読
- 現在はTripleDESとして利用

[Triple DES暗号]



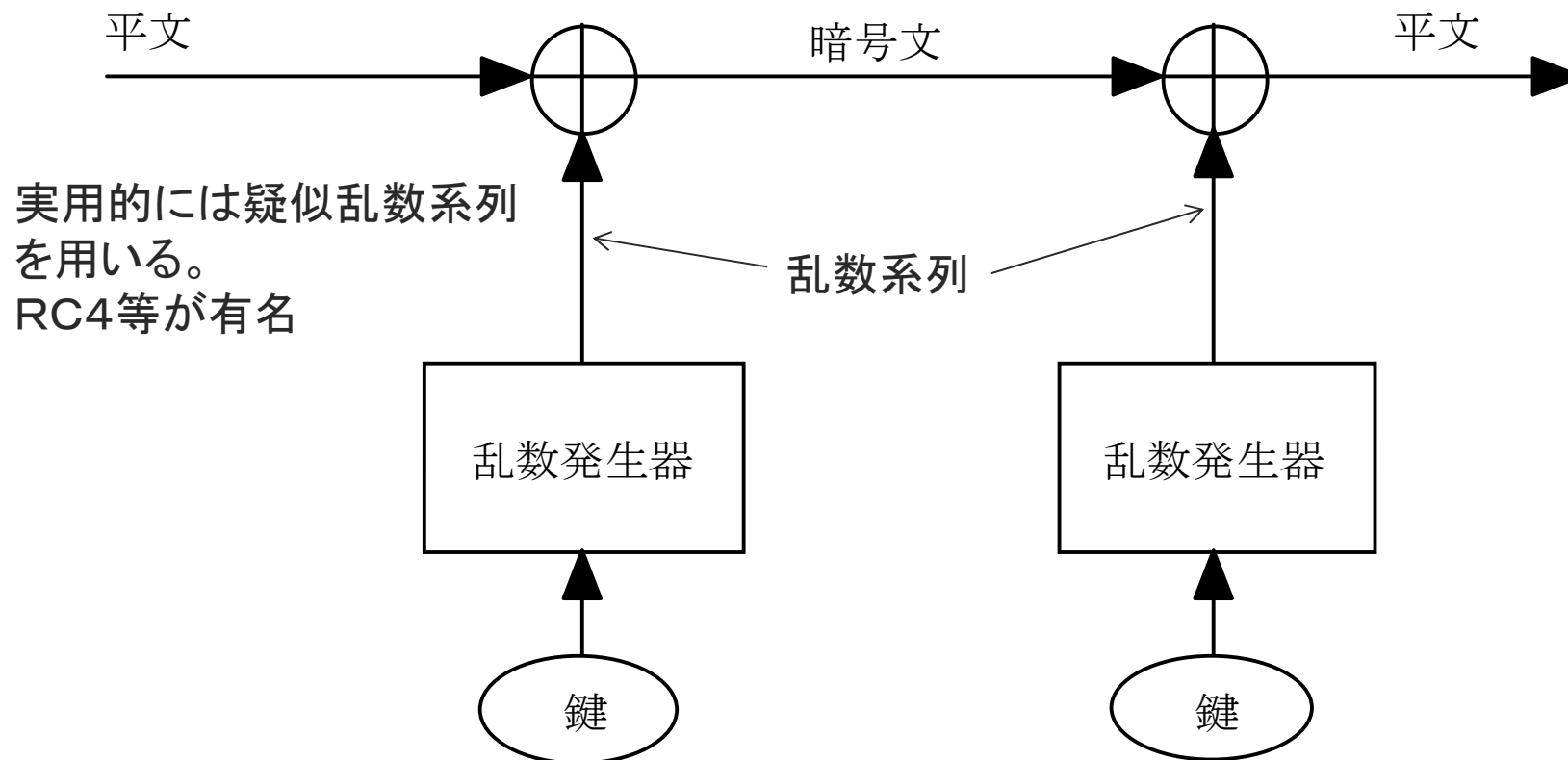
- ブロック長: 64ビット
(DESと同じ)
- 鍵長: 168ビット (= 56 × 3)
- 上位互換性: K₁=K₂=K₃とすればDESと等価になる
- 処理速度が遅い
(DESの3倍)

AES (Advanced Encryption Standard)



【ストリーム暗号とバーナム暗号】

平文系列に乱数系列を排他的論理和により加える。
乱数系列として完全な乱数（真性乱数）を一度限り使う場合は理論的に安全である（ワンタイムパッド）。



共通鍵暗号の操作モード

ECB(Electronic CodeBook)モード



- 同じ平文を暗号化すると同じ暗号文になるため通常用いられない
- 初期設定データや、鍵情報を暗号化するために用いることはある

[ECBモードの問題点]



原画像



暗号化画像(ECB)

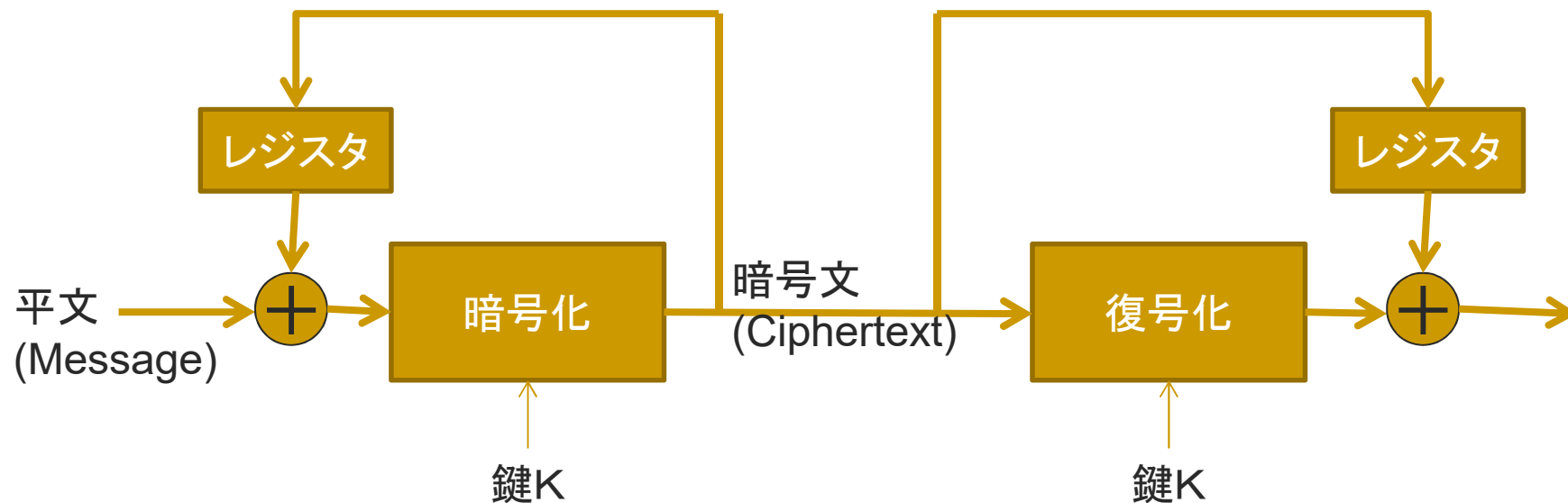


暗号化画像(ECB以外)

Cf. Wikipedia (<https://ja.wikipedia.org/wiki/暗号利用モード>)

共通鍵暗号の操作モード(2)

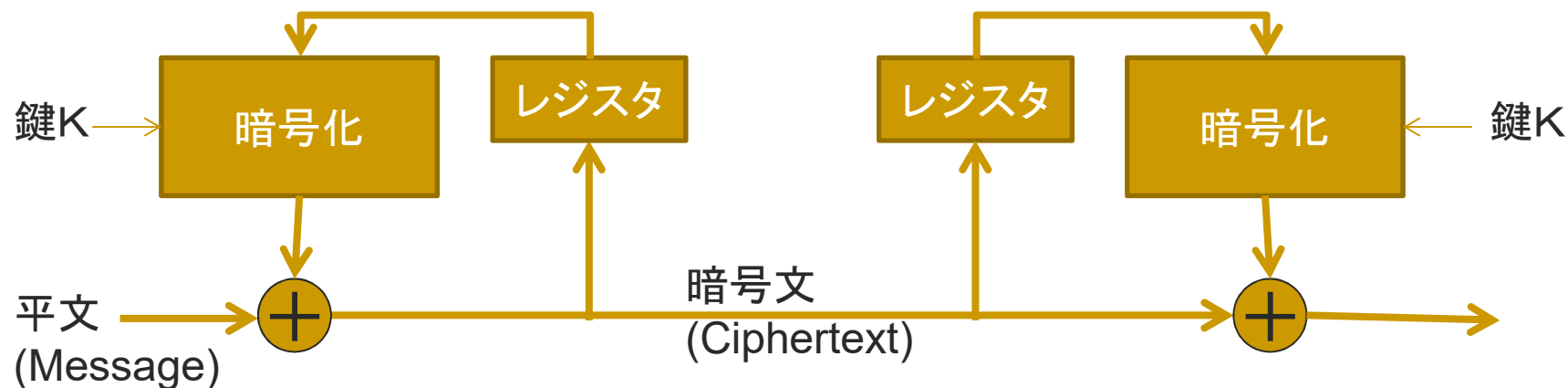
CBC(CipherBlock Chaining)モード



- レジスタにはあらかじめ初期値(IV)を入れておく
- 一般に同じ平文でも異なる暗号文になるので安全性が高まる
- 伝送路上のエラーが伝播してしまう

共通鍵暗号の操作モード(3)

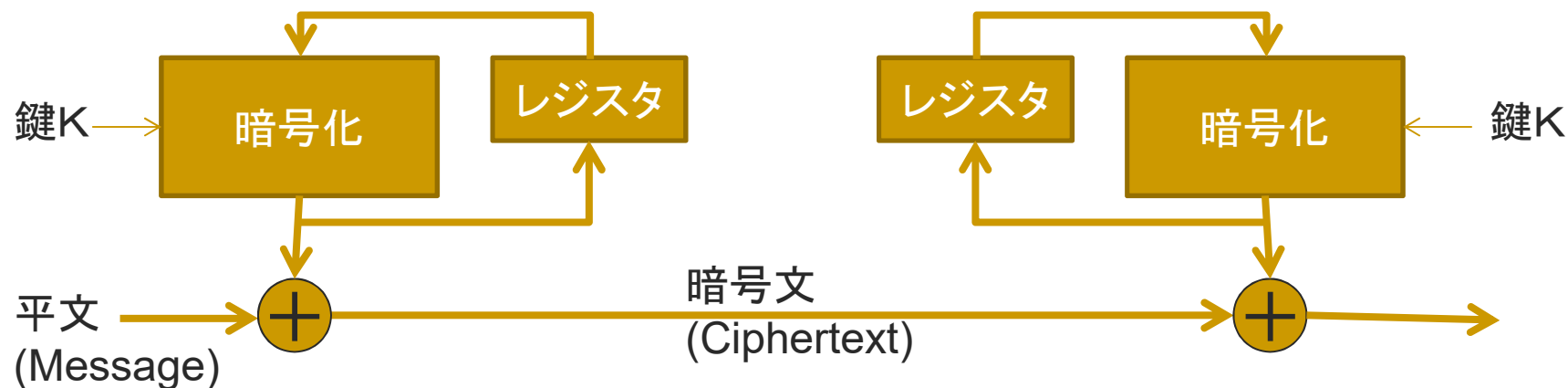
CFB(Cipher FeedBack)モード



- (暗号文に依存する) 乱数を用いたストリーム暗号と考えることができる
- 送信側も受信側も暗号化ブロックを用いる
- レジスタにはあらかじめ初期値 (IV) を入れておく
- 一般に同じ平文でも異なる暗号文になるので安全性が高まる
- 伝送路上のエラーが伝播してしまう

共通鍵暗号の操作モード(4)

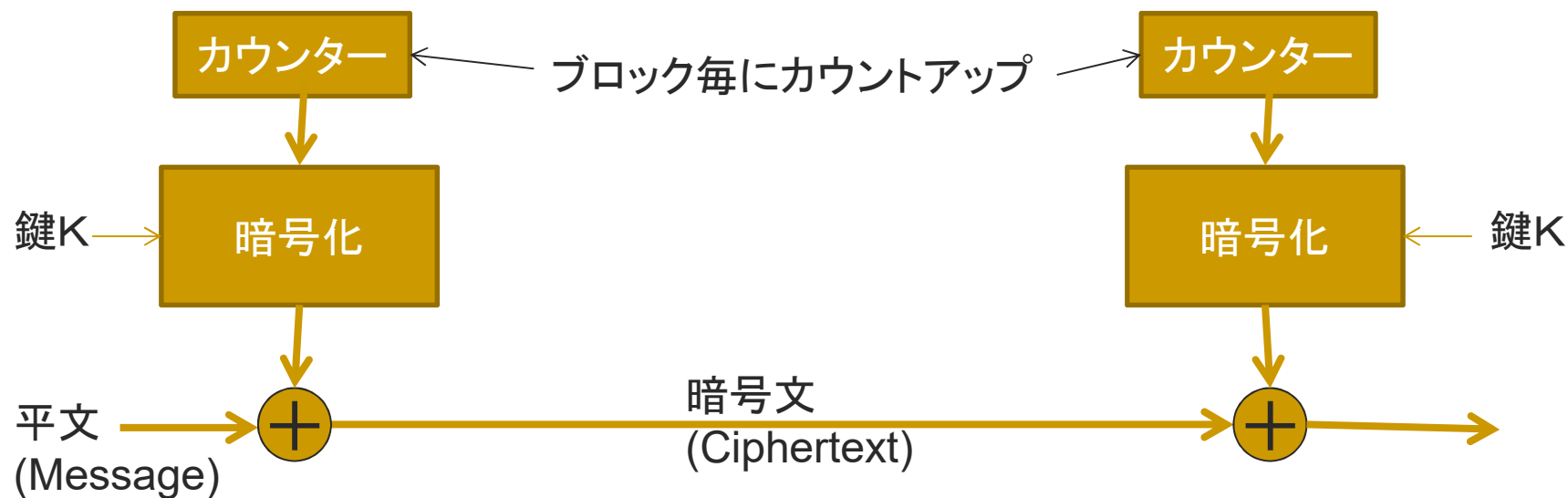
OFB(Output FeedBack)モード



- 暗号化ブロックによる乱数を用いたストリーム暗号と考えることができる
- 送信側も受信側も暗号化ブロックを用いる
- レジスタにはあらかじめ初期値 (IV) を入れておく
- 同じ平文でも異なる暗号文になるので安全性が高まる

共通鍵暗号の操作モード(5)

CTR(Counter)モード



- カウンター値を暗号化した値を加えるストリーム暗号と考えることができる
- 暗号化、復号化時に並列処理が可能(OFB等では並列処理できない)
- 送信側も受信側も暗号化ブロックを用いる
- 送受信者間で共通のカウンターの初期値(IV)を入れておく
- 同じ平文でも異なる暗号文になるので安全性が高まる

暗号解読(攻撃法)の分類

- 暗号文(単独)攻撃
暗号文のみ(選べない)入手可能
- 既知平文攻撃
対応する平文も入手可能
- 選択平文攻撃
任意に選んだ平文とそれに対応する暗号文
- 選択暗号文攻撃
任意に選んだ暗号文とそれに対応する平文
- 関連鍵攻撃
攻撃対象となる鍵と関連のある別の鍵について情報(平文暗号文ペア)が得られる場合

暗号攻撃法の種類

- 鍵全数探索法
鍵長 k (bit)に対し、 $2^{(k-1)}$ の計算量
- 差分攻撃法
1990年Biham, Shamirにより開発された選択平文攻撃法の一種。全数探索よりも少ない計算量で解読可能。
- 線形攻撃法
1993年に松井により開発された既知平文攻撃の一種。DESの解読に用いられた。
- サイドチャネル攻撃
暗号の実装方法の欠点を利用する攻撃法。暗号計算演算時の電力消費量の偏りを利用する方法など。