ネットワーク社会に必要なセキュリティ技術

神奈川大学 工学部 電気工学科

木下宏揚

セミナーの内容

- □セキュリティ技術の必要性
- □暗号の基礎
- □アクセス制御
- □ファイアウォール
- □電子透かし

セキュリティ技術はなぜ必要か

- □インターネットの普及により、商取引をはじめ家電の制御など生活のあらゆる局面でネットワークを利用する機会の増加
- □クラッカーによるネットワークシステムへの不正侵入
- □個人情報の取り扱いに関連したプライバシー侵害
- □ネットワークによるマルチメディア情報の配信で問題となる著作権保護
- □ネットワークを前提としたグループウェア

セキュリティが脅かされる原因

- □物理的な情報破壊
  - ○災害、故障 対策、システムの二重化、分散
  - ○犯罪　対策、入室管理、利用者認証
- □不正な情報操作(情報セキュリティの研究分野)
  - ○不正アクセス 盗聴、偽造、改竄
  - ○不正コピー 再送
  - ○結託　秘密情報の交換
- □守るべき対象
  - ○伝送媒体(ネットワーク)
  - ○蓄積媒体(メモリ、ディスク、テープ)
  - ○処理媒体(CPU)

これからの高度情報通信

- □中央管理型
  - ○通信相手が役所、銀行、大企業など信用できる組織
  - ○騙される可能性は少ない
- □分散型
  - ○個人または小規模の組織同士の通信
  - ○騙される可能性が高い
  - ○安心して通信、取引できるメカニズムが必要

個人情報保護法案

□コンピュータなどに蓄積された個人情報の保護

□個人情報の定義

○個人情報保護法案第一条二　生存する個人に関して記録された情報で、当該情報に含まれる氏名、生年月日その他の記述、または個人別に付された番号、記号等により当該個人を識別できるものをいう。

□先進民主主義国で一般化しているプライバシーの概念

○自分に関する情報の流れをコントロールする権利

○本人が情報が正しいかどうか、チェックできる体制

不正アクセス行為の禁止などに関する法律

□第5条(アクセス管理者による防御措置)アクセス制御機能を特定電子計算機に付加したアクセス管理者は、当該アクセス制御機能に係る識別符号又はこれを当該アクセス制御機能により確認するために用いる符号の適正な管理に努めるとともに、常に当該アクセス制御機能のよう構成を検証し、必要があると認めるときは速やかにその機能の高度化その他当該特定電子計算機を不正アクセス行為から防御するため必要な措置を講じるよう努めるものとする。

情報セキュリティの研究分野

基盤技術
- □整数論
- □暗号理論
- □セキュリティモデル

応用技術
- □暗号
- □認証
- □アクセス制御技術(OS,TCP/IP,Database)
- □著作権制御
- □マルチパーティープロトコル
- □プライバシーの保護

暗号の歴史

換字式暗号(シーザー暗号)

- □アルファベットのならび順に1文字ずらす
- □IBM → HAL

転置式暗号

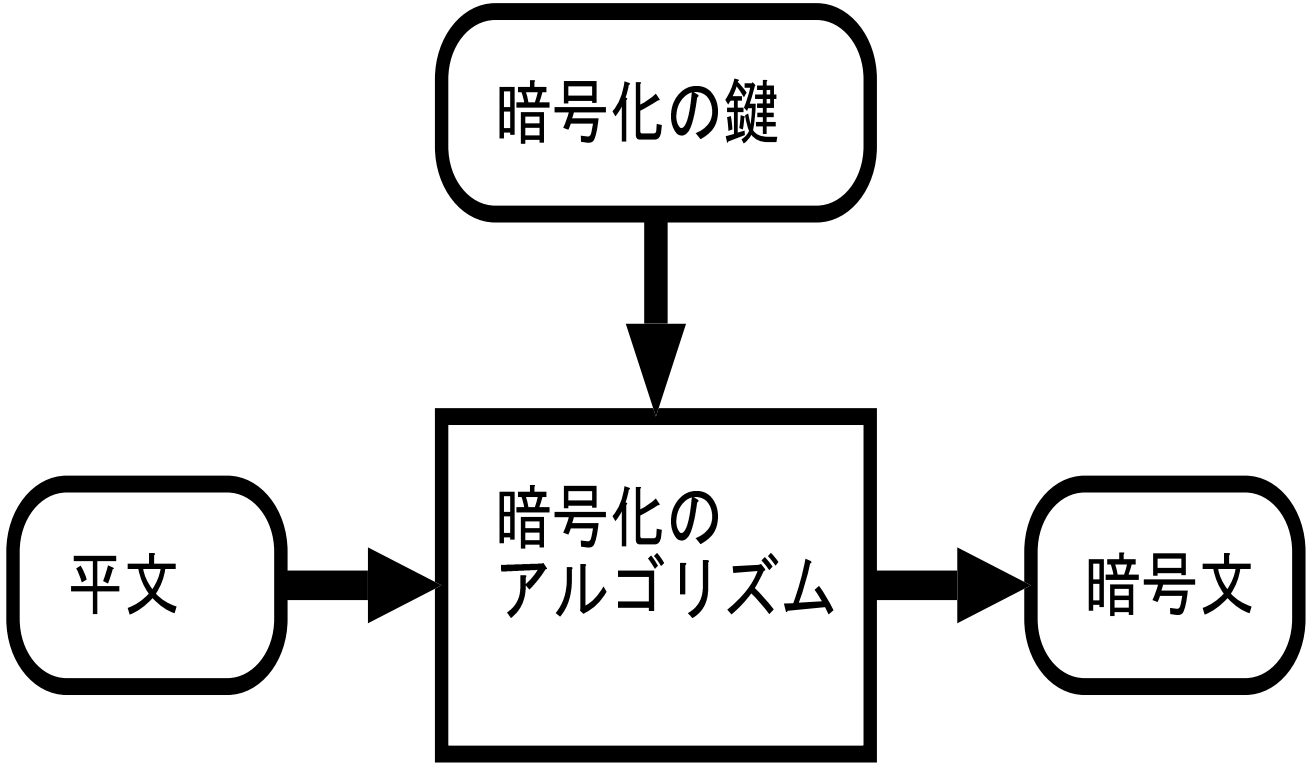
- □1番目の文字は3番目へ
- □2番目の文字は1番目へ
- □3番目の文字は2番目へ移動
- □IBM → BMI

アルゴリズムと鍵

□暗号システム

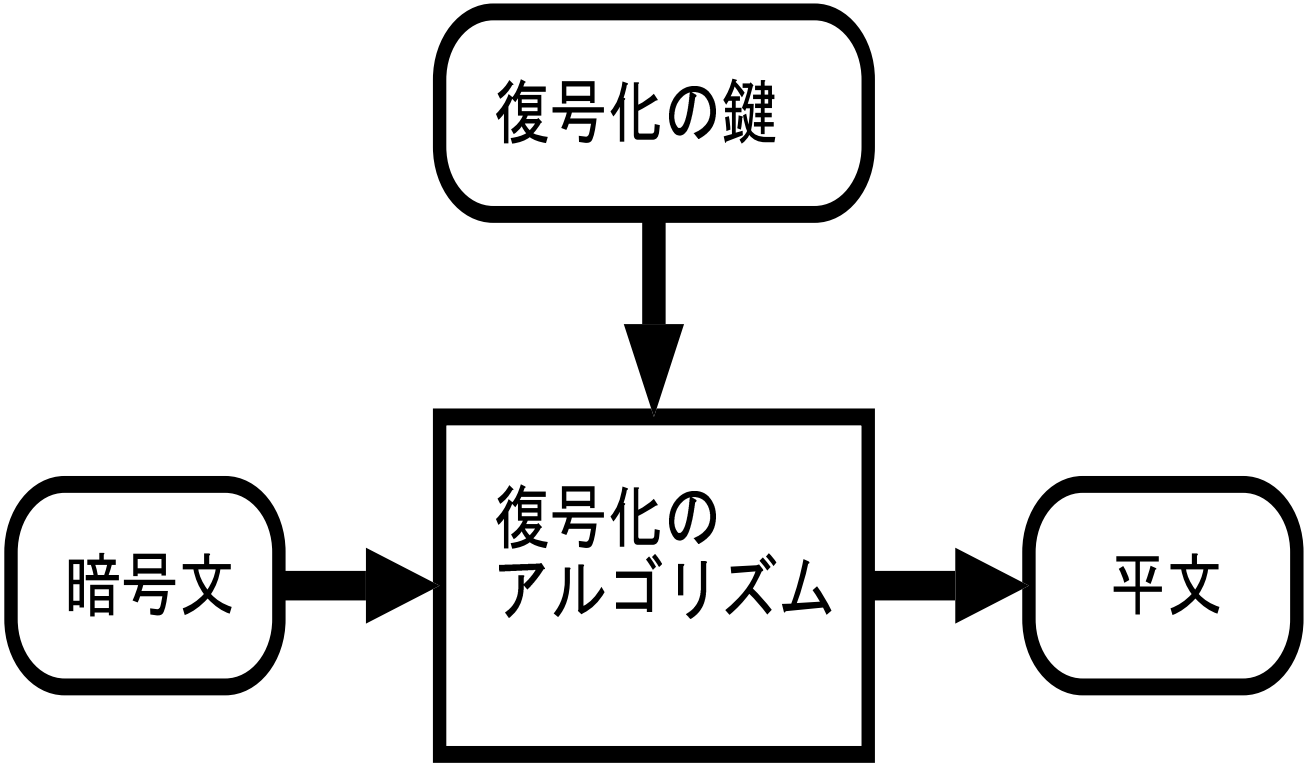
○アルゴリズム(暗号の掛け方、戻し方)

○鍵



暗号文を解読するには

□暗号文、アルゴリズム、鍵をすべて知っている必要がある
□どれかひとつでもわからなければ解読できない



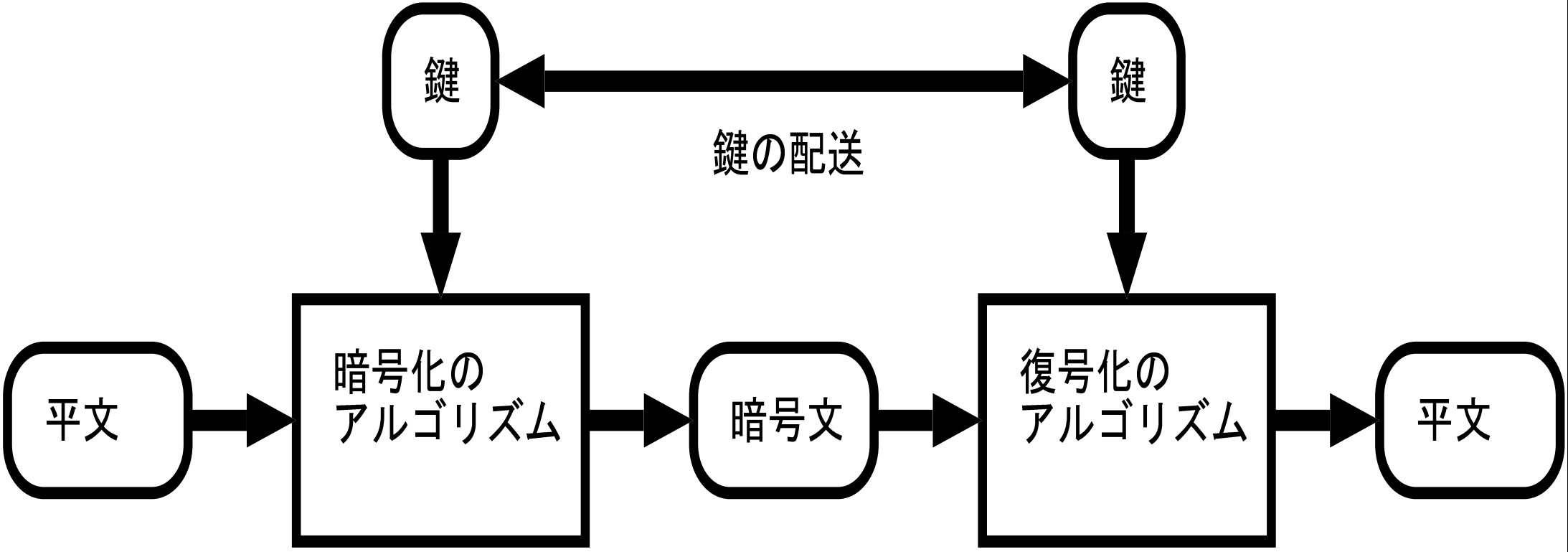
アルゴリズムは秘密にするべきか?

- □昔の暗号と軍事目的の暗号
  - ○限定されたグループ内で通信
  - ○アルゴリズムと鍵の両方が秘密
  - ○標準化が困難
- □これからの暗号
  - ○不特定多数が通信
  - ○アルゴリズムは公開
  - ○鍵は秘密
  - ○標準化が容易

慣用鍵暗号

- □慣用鍵暗号・共通鍵暗号・秘密鍵暗号・対象鍵暗号
- □暗号化する鍵と復号化する鍵は同じ鍵
- □送信者と受信者で同じ鍵を持っている必要がある
- □鍵は秘密に配送しなければならない
- □暗号化と復号化を比較的高速に行える
- □代表的な慣用鍵暗号
  - ○シーザー暗号
    - ▹アルゴリズムと鍵が秘密
  - ○DES暗号、FEAL暗号
    - ▹アルゴリズムは公開、鍵は秘密

慣用鍵暗号



慣用鍵暗号の例

アルファベットの符号化と排他的論理和

□アルファベット数字対応表

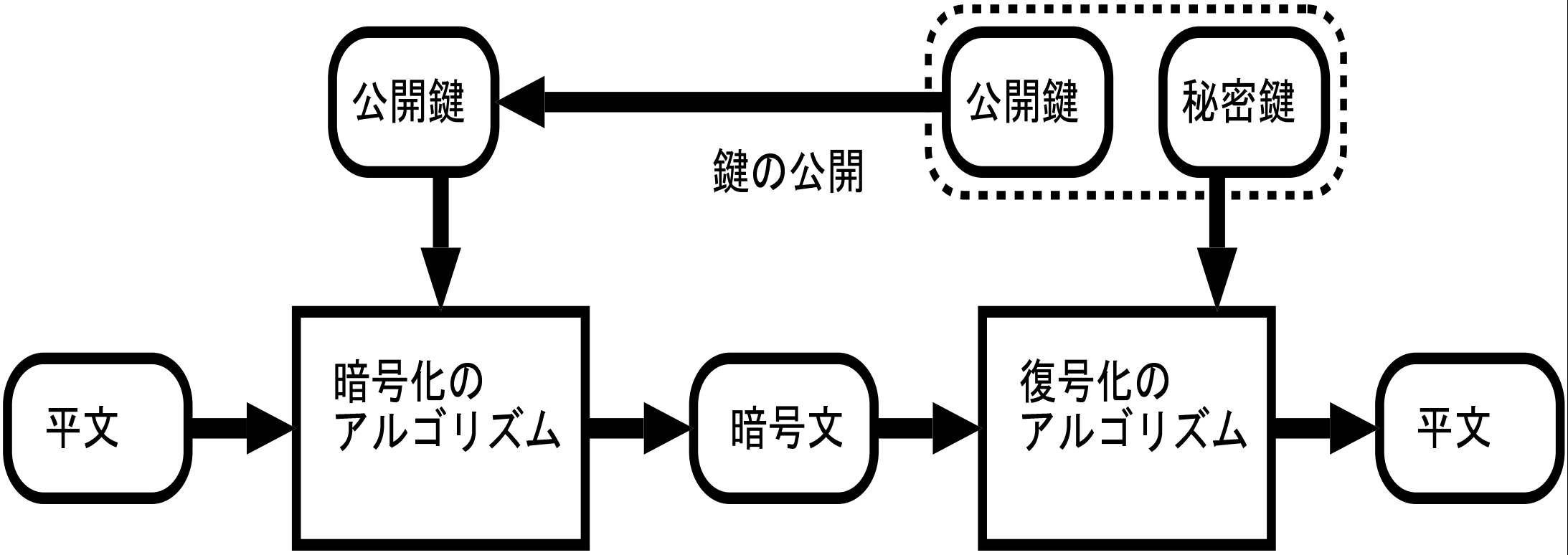
A 01 B 02 C 03 D 04 E 05 F 06 G 07 H 08 I 09
J 10 K 11 L 12 M 13 N 14 O 15 P 16 Q 17 R 18
S 19 T 20 U 21 V 22 W 23 X 24 Y 25 Z 26

□平文 KANAGAWA → 符号化 M=1101140107012301
□鍵 AJSBKTCL → 符号化 K=0110190211200312
□暗号化MとKの排他的論理和 C=10110D0316212013
□復号化CとKの排他的論理和

公開鍵暗号

- □暗号化する鍵(公開鍵)と復号化する鍵(秘密鍵)は別の鍵
- □アルゴリズムと暗号化する鍵は公開
- □復号化する鍵は秘密
- □送信者はアルゴリズムと公開鍵だけ知っていればよい
- □鍵を秘密に配送する必要がない
- □暗号化と復号化が多少遅い
- □代表的な公開鍵暗号
  - ○RSA暗号

公開鍵暗号



慣用鍵暗号と公開鍵暗号の鍵の数の違い

- □N人のなかで任意のふたりが暗号通信をするために必要な鍵の数
- □慣用鍵暗号の場合、${}_{N}C_{2}$個、1000人なら499500個
- □公開鍵の場合、N個、1000人でも1000個(公開鍵と秘密鍵のペアで1個)

鍵の配送

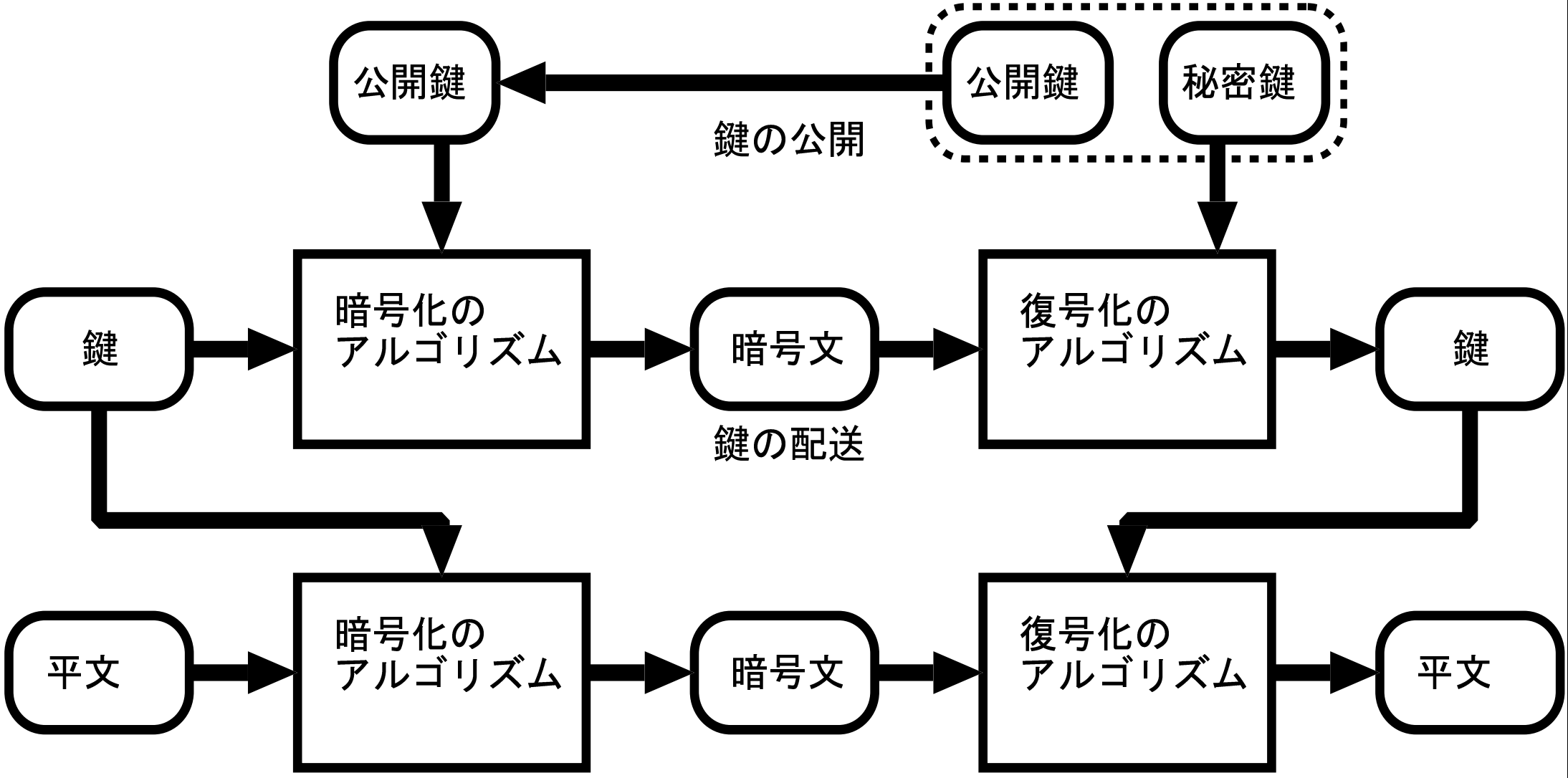
慣用鍵暗号の最大の弱点

- □郵便で送る
- □別の暗号で送る
- □スパイが直接相手に届ける

公開鍵暗号の最大の利点

- □電話で送る
- □電話帳に載せる
- □新聞広告に載せる

公開鍵暗号で慣用鍵暗号の鍵を配送する



公開鍵暗号の絡繰

□暗号化はアルゴリズムと公開鍵を知っていれば解くのがやさしい問題
□復号化はアルゴリズムと秘密鍵を知っていれば解くのがやさしい問題
□復号化はアルゴリズムと公開鍵しか知らないと解くのが難しい問題

□やさしい問題
  ○パソコンで数分で解ける
□難しい問題
  ○スーパーコンピュータ1億台でかかっても解くのに100億年

公開鍵暗号は本当に安全？

- □公開鍵を使って平文と暗号文の対応表を作る
  - ○春はあけぼの → ABE?&*@ab@
  - ○夏はよる → di(;?&*@aO
  - ○秋はゆうぐれ → lOKkeo3u
  - ○冬はつとめて → jkrh49fj
- □対応表の長さは膨大で原子1個で1ビット記憶するとしても宇宙中の原子使っても足りない
- □対応表ができたとしても長すぎて宇宙の寿命があるうちに検索できない
- □原理的には解けるけれども計算量的に安全

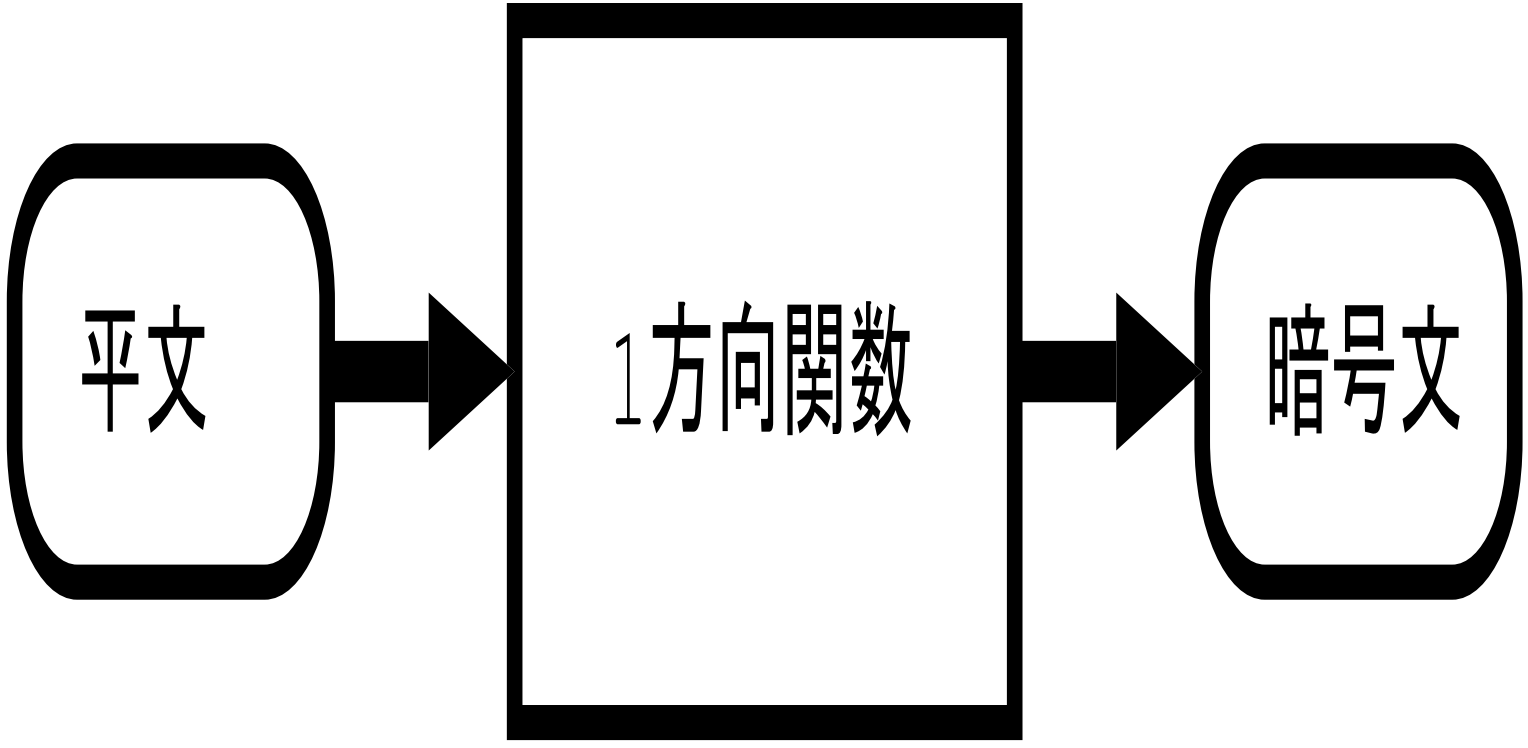
公開鍵暗号はどうやって作るか？

□1方向関数
- ○y=f(x)
- ○xからyを求めるのはやさしい問題
- ○yからxを求める(逆関数)のは難しい問題

□素因数分解
- ○2個の素数P,Qから合成数N(素数でない数)を求める計算 N=P×Q
- ○P,QからNを求めるのは優しい問題
- ○Nが200桁位になるとNからP,Qを求めるのは難しい問題

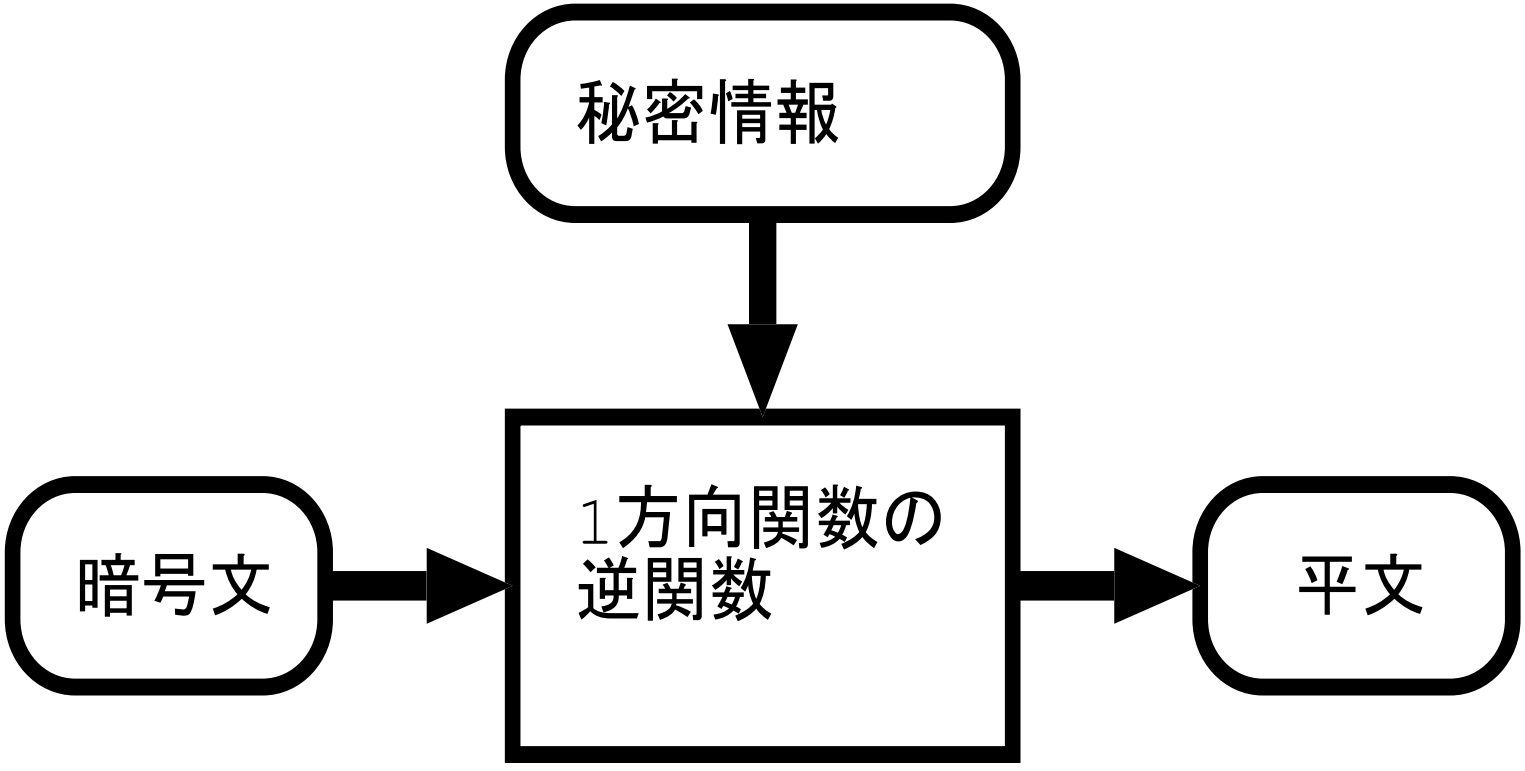
1方向関数による暗号化

□逆関数は求めることは難しい問題なのでだれも解読できない究極の暗号



落とし戸付1方向関数

□ある秘密情報を持っていると逆関数がやさしい問題になる
特別な1方向関数
□秘密情報を秘密鍵として使えば公開鍵暗号が作れる



RSA暗号

- 鍵の生成

  1. 50 桁程度の素数 p と q を選び $n = pq$ を計算する
  2. $\Phi(n) = (p-1)(q-1)$ と互いに素な整数 e を決める (gcd(e,(p-1)(q-1))=1)
  3. $ed \equiv 1 mod\ \Phi(n)$ を満たす d を求める
  4. n と e を公開、p と q、d を秘密にする

- 暗号化　$C \equiv M^e\ mod\ n$
- 復号化 $C^d = M^{ed} = M\ mod\ n$

RSA暗号

例

公開鍵：$n = 55, e = 7$

秘密鍵：$p = 5, q = 11,$

$\Phi(n) = (p-1)(q-1) = 40,$

$d = 23(7 \times 23 \; mod \; 40 = 1)$

平文：$M = 3$

暗号化 ： $C \equiv M^e \; mod \; n \quad 3^7 \equiv 42 \; mod \; 55$

復号化 ： $M \equiv C^d \; mod \; n \quad 42^{23} \equiv 3 \; mod \; 55$

暗号システムへの攻撃

攻撃者の知っている情報により難易度が変わる

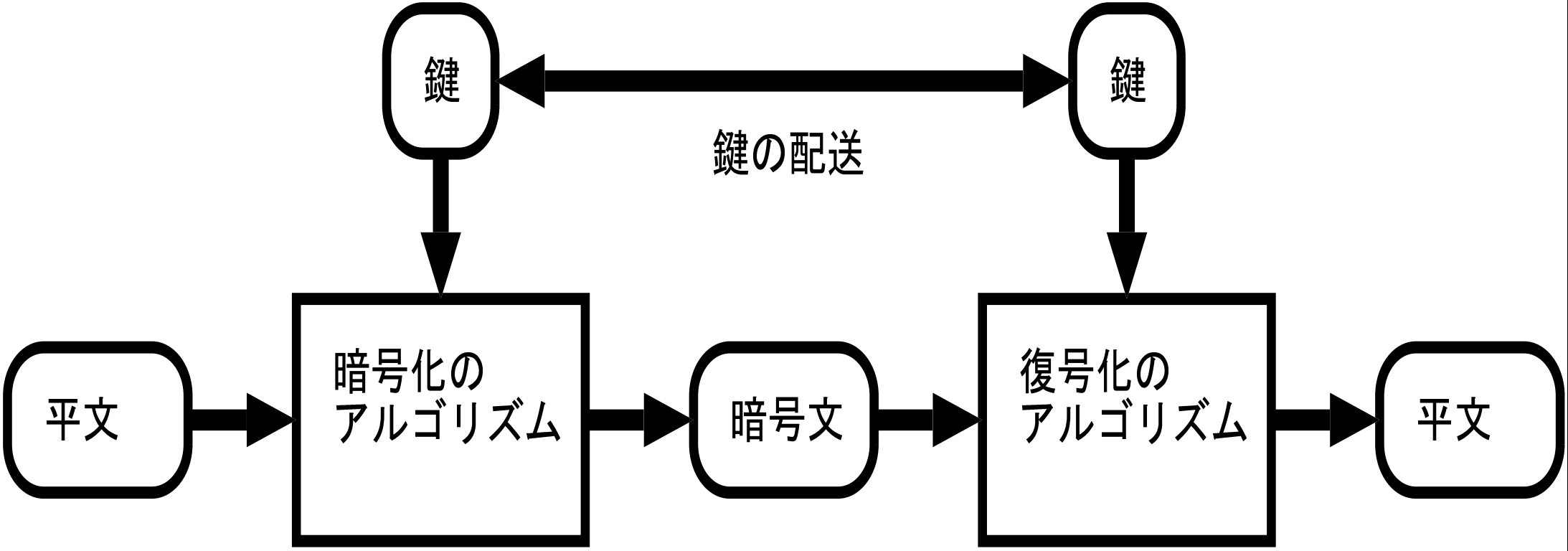
- □何も知らない場合
- □暗号文だけ知っている
- □暗号化方式のアルゴリズムを知っている
- □鍵を知っている
- □平文を知っている

署名と認証

署名　情報の発信元を保証する機能
認証　相手がだれであるか確認する方法
- □印鑑、自筆の署名
- □電子化は困難

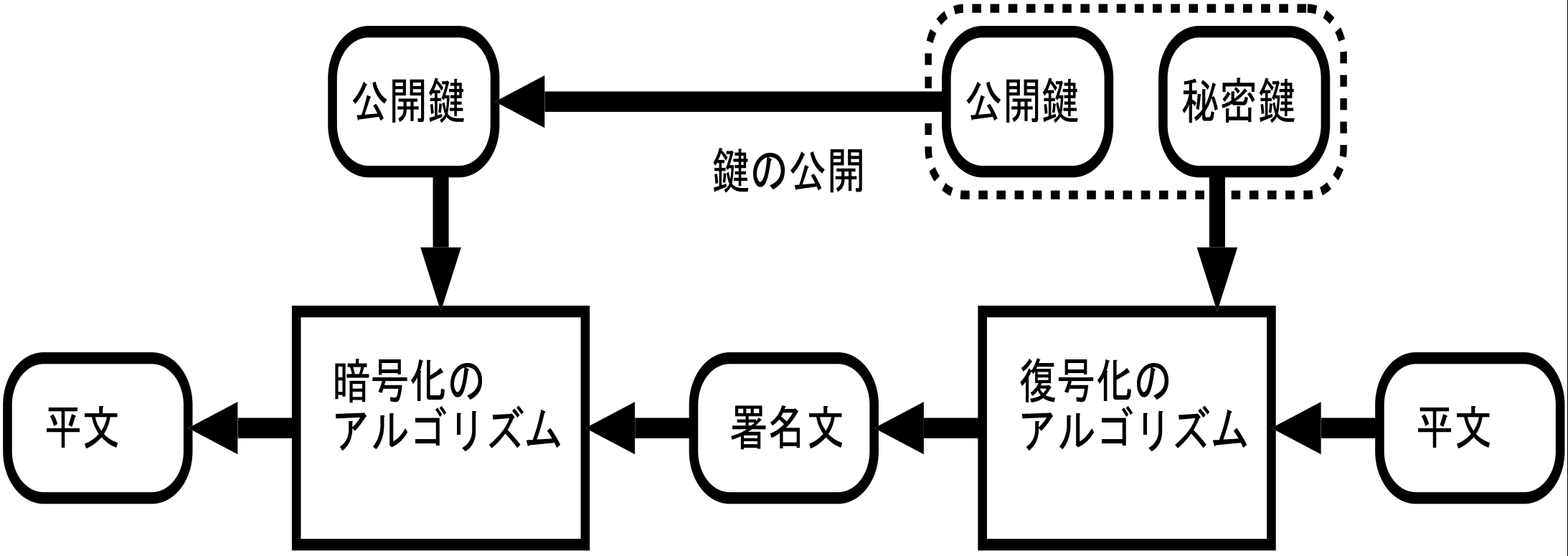
慣用鍵暗号とディジタル署名

鍵を持っているのはふたりだけだから相手から送られてきたメッセージだと確認可能
後でメッセージを送ったことを否定することを防止はできない
ふたり以外が署名を確認できない



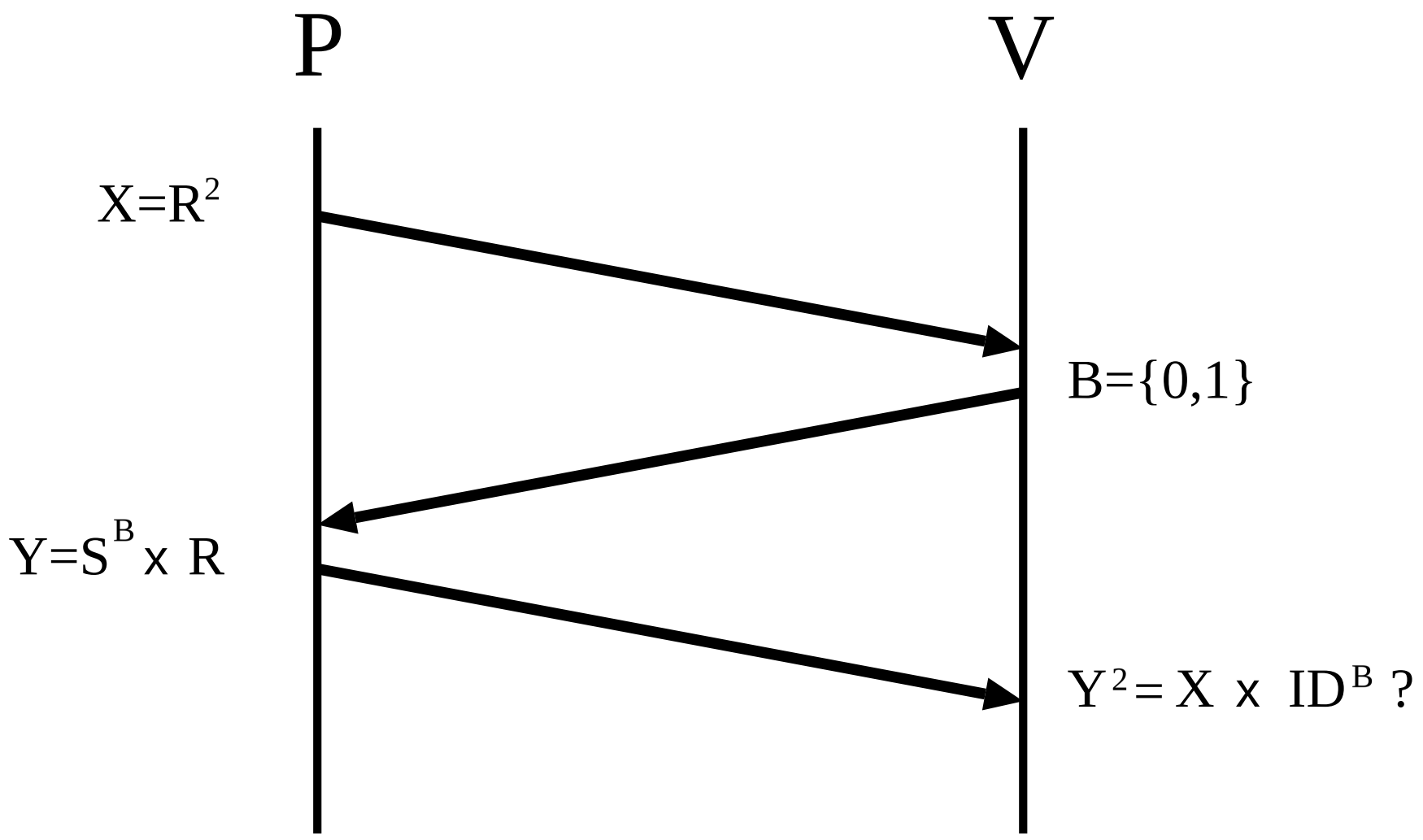
公開鍵暗号とディジタル署名

署名文を作れるのは秘密鍵を持っている人だけ
メッセージを送ったことを後で否定できない
だれでも署名文の署名を確認できる



零知識相互証明(Fiat-Shamir 法)

- ○知識などがあることをその知識を見せずに相手に納得させる
- ○認証などに応用

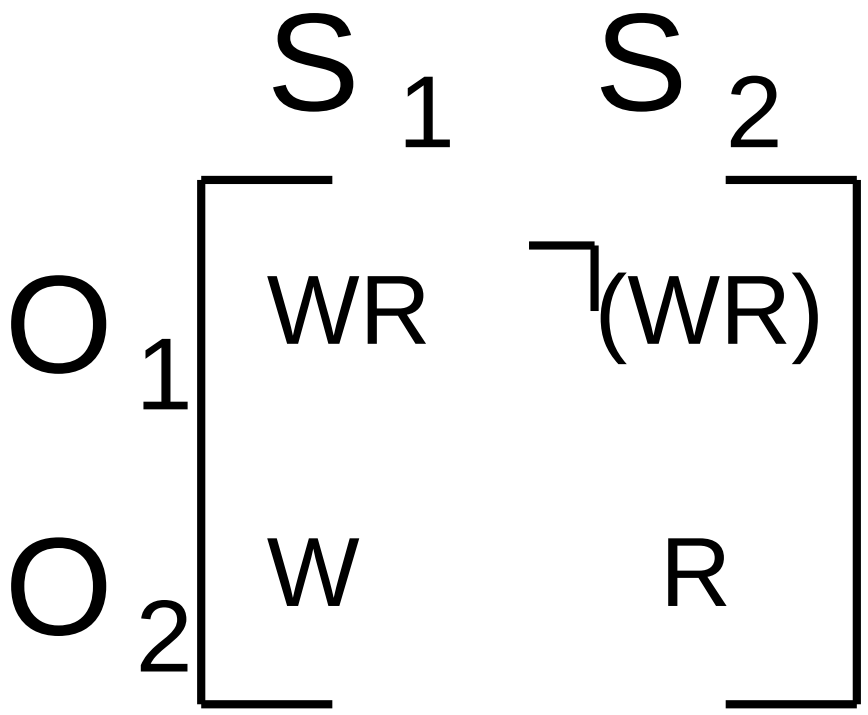


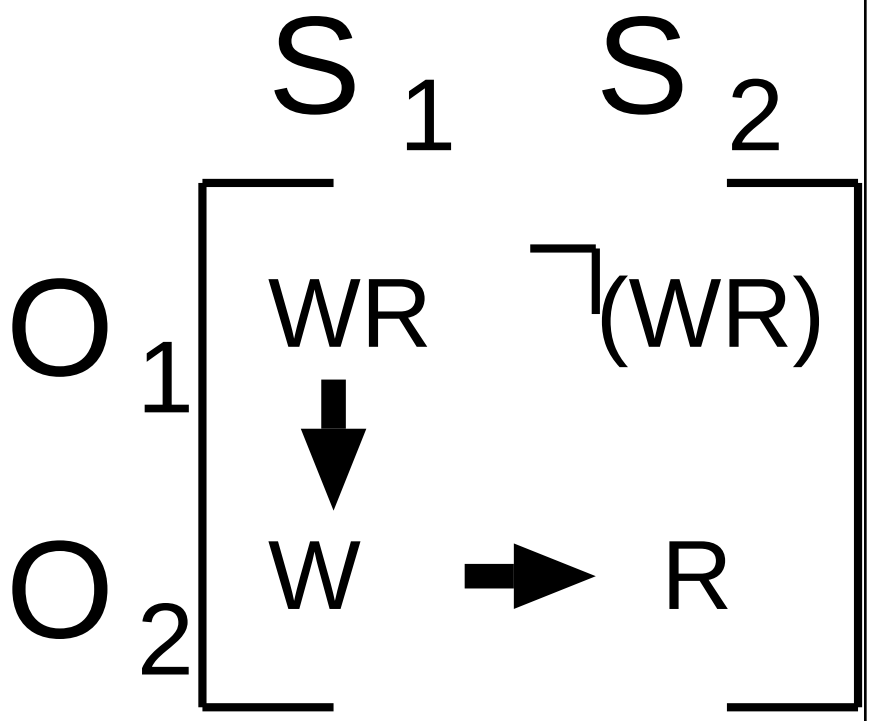
アクセス制御

- □情報収集者は様々な組織から情報を収集可能
  - ○病院、学校、市役所、銀行、保険会社
  - ○新聞社、雑誌社、不動産会社、警察
- □単独の情報源から収集した断片的情報から完全な情報を構築可能な場合がある
- □Covert Channel
- □Take Grant Model
  - ○アクセス権の取得・譲渡
- □Chinese Wall Model
  - ○競合・協調する組織間の情報の流れ
- □質問分割法
  - ○統計データベース

Covert Channel

- 主体S(ユーザやプログラムなど) 客体O(ファイルやデータなど)
- 読み出し権R 書き込み権 W





インターネットとセキュリティ

- □インターネットは軍関係や大学などの研究機関で発展してきたため，基本的には性善説の立場に立ち，悪いことは誰もしないという前提の下に発展してきた。
- □現在のインターネットのプロトコルIPv4では，セキュリティに関して考慮されていない。
- □現在のようにインターネットが商取引や決済に用いられ，不特定多数の人が利用するようになると犯罪や悪戯が横行するようになる。

Cracker と Hacker

- ネットワークやコンピュータに対して攻撃を行う人のことはクラッカー(cracker)と呼ぶ。
- ハッカー(hacker)は本来，プログラミングやコンピュータの優れた技術を持っている人に対して称賛の意味を込めて使用する言葉。
- RFC1392
  - cracker
    - A cracker is an individual who attempts to access computer systemswithout authorization. These individuals are often malicious, asopposed to hackers, and have many means at their disposal forbreaking into a system. See also: hacker, Computer EmergencyResponse Team, Trojan Horse, virus, worm.
  - hacker
    - A person who delights in having an intimate understanding of theinternal workings of a system, computers and computer networks inparticular. The term is often misused in a pejorative context,where "cracker" would be the correct term. See also: cracker.

インターネット上のセキュリティ上の問題

[不正侵入]

- □パスワードを盗聴
- □セキュリティホール(security hall)を突く
- □ホスト上のユーザの権限を手にいれる
- □特にルート(スーパーユーザ，特権ユーザ)の権限を手にいれることは致命的な結果を招く

インターネット上のセキュリティ上の問題

[データの盗聴]

- □盗聴はパスワード情報など他の不正を行うための情報収集に有効な手段となる
- □インターネットの盗聴は電話の盗聴よりも簡単に行うことができる
- □経路上のルータまたは経路上のネットワークのホストの管理者あるいはルートの権限を手にいれたクラッカーであれば，だれでも盗聴することができる
- □クラックしなくても廊下などに設置されたネットワーク機器にノートパソコンなどを直接接続を行っても良い
- □ファイルの内容を見る

インターネット上のセキュリティ上の問題

[データの改竄，消去]

□ファイルシステム上のデータ，あるいはネットワーク上を転送中のデータの内容を書き換えたり，消去する不正

[なりすまし]

□ユーザ名やホスト名，IPアドレスなどを偽る不正

□rコマンドなどはホスト名やユーザ名に基づいて認証を行うため、なりすましに弱い

[データ送出の否定]

□いったん送出した情報を後になって否定する不正であるオンラインショッピングでの注文を後になって注文していないと言うような場合

インターネット上のセキュリティ上の問題

[経路の追跡]

- □どのホスト間でどのような種類の通信が行われているかという情報の漏洩
- □この種の情報はプライバシーの侵害や商取引の障害になる場合がある

[著作権の侵害]

- □電子化された情報は簡単にコピーができるため，ソフトウェアや画像，音声などの情報を不正にコピーされる可能性がある

インターネット上のセキュリティ上の問題

[過負荷]

- □DoS攻撃 (DoS Denial of Service)
- □ホストで高負荷のプロセスを実行させる，大量のメールを送りつける(SPAM)といった特定のデーモンにサービスの要求を集中させる
- □直接メールを送りつけるのではなく足がつかないようにいくつかのメールサーバーを中継させる場合が多い
- □ネットワークに大量のパケットを送出する
- □ホストやネットワークの資源を故意に消費させ，通常のサービスを麻痺させる不正行為

[踏み台攻撃]

- □ある組織に対して侵入する際にまず別の組織に侵入して踏み台にする

コンピュータとインターネットのセキュリティ

- Virus
  - ソフトウェアに忍び込んで悪さをする
  - ソフトウェアに感染する
  - ソフトウェアからソフトウェアへ伝染する
  - UNIXなどプログラムが他のプログラムから保護されているオペレーティングシステムではほとんど感染しない
- Worm
  - 独立したプログラム
  - ネットワークを媒体として自己増殖する
  - ありふれたプログラムの振りをして発見を防ぐ
  - パソコンのOSでは発生しにくい
- トロイの木馬
  - プログラムに本来の目的以外の機能を密かに潜り込ませる
  - 増殖や感染はしない

これらの攻撃に対する対策の基本的な技術

- □情報自体を隠してしまう暗号技術
- □暗号技術に基づいた認証技術
- □情報に近づくことを防ぐアクセス制御技術
- □著作権を保護する電子透かし技術
- □不正が起きた際に犯人やその手口をを突き止める手掛かりとなるロギングの技術

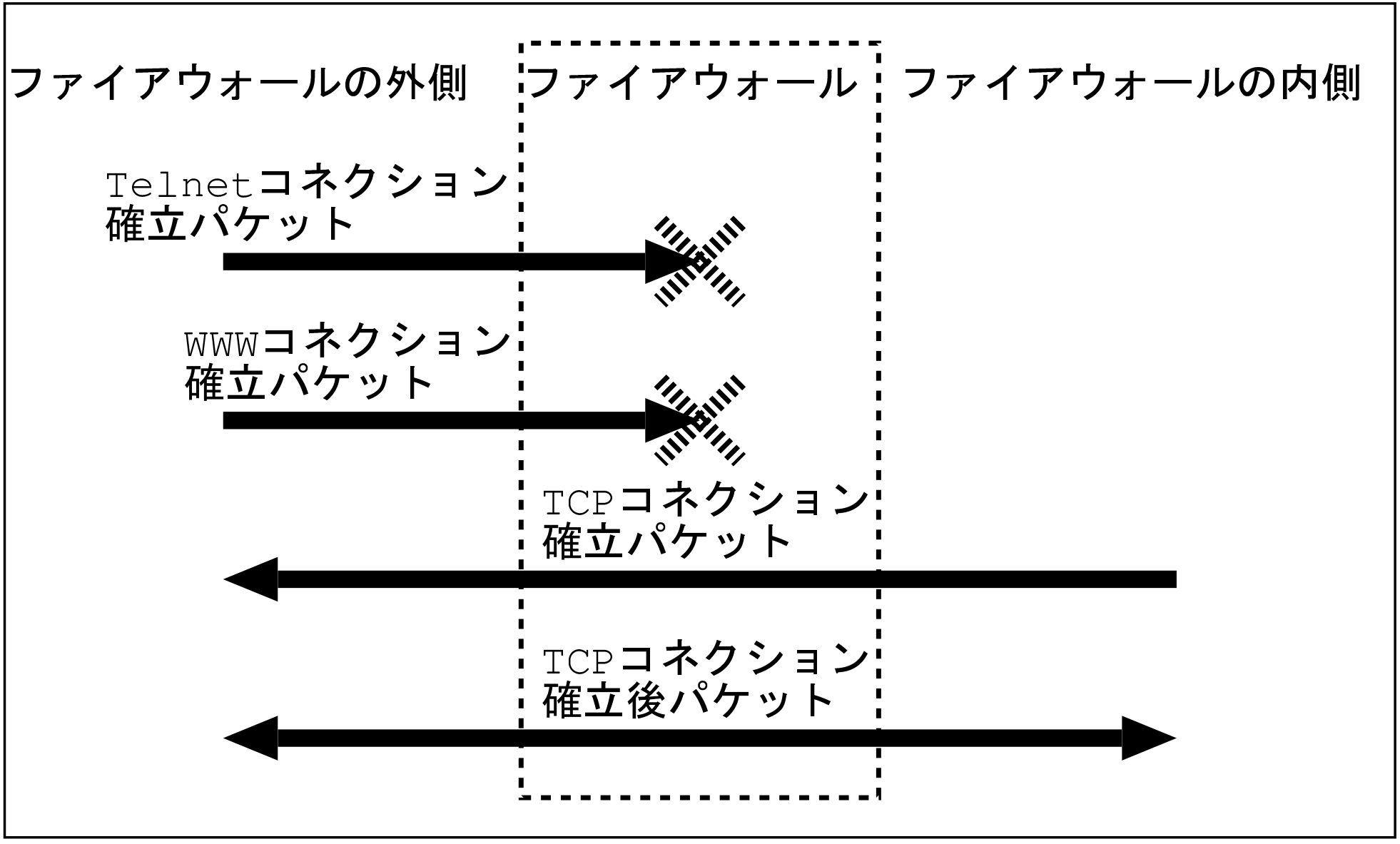
ファイアウォールの必要性

- □組織内の計算機を管理する場合，管理者は個々の計算機のセキュリティに常に気を遣う必要がある
- □例えれば，外の道路(ネットワーク)は泥棒だらけだから，1軒1軒きっちり戸締まりする必要があるような場合である
- □住宅街を城壁で囲んで門(ルータ)に警備員を24時間体制で配置すれば，個々の家の戸締まりはそれほど厳重でなくて済む。
- □ファイアウォールは大学の研究室や会社など一定の組織内のネットワークと外部のインターネットの接続点にセキュリティ対策のために設置されるルータである。
- □ファイアウォールを設置することによりセキュリティ対策を一元化でき，内部のネットワークの個々の計算機のセキュリティを緩くすることが可能となる。

ファイアウォールの種類

- □パケットフィルタリング(packet filtering)
  - ○ネットワークとネットワークを分離
  - ○カーネルレベルで転送
  - ○特定のプロトコルや宛先のパケットしか通過させない
- □プロキシーサーバ(proxy server)
  - ○インターネット上のサーバに代って内部のネットワークにサービスを提供する
  - ○デーモンが転送
  - ○内部のネットワークと外部のネットワーク間のパケットの転送を行う
- □ロギング(logging)
  - ○クラッカーの痕跡を残し犯人追求の手がかりに利用
- □NAT(network address translation)
  - ○IPアドレスの不足を解消するために組織内だけでの使用が認められているプライベートアドレスと外部のインターネットへの接続が許されるグローバルアドレスを変換する

パケットフィルタリング



○IP層での中継、特定のアドレス、プロトコルのみ転送

パケットフィルタリング

ルータの機能

- パケットの最終目的地をもとに複数のネットワークインタフェースの間でパケットを転送(forwarding)すること
- 通常パケットの転送はカーネルの機能

パケットフィルタリング

- 転送の際に特定のパケットのみを通過させる
- それ以外のパケットは転送を阻止することによって内部のネットワークを保護する。
- 通過させるかどうかの判断基準をルールリストと呼ぶ。

パケットフィルタリング

- □パケットのヘッダの情報を元にルールリストの先頭からマッチングを行う
- □マッチするルールがあると指定されたルールアクションが実行される
- □ルールアクションが適応されるのは最初にマッチしたルールのみで，マッチングはその時点で終了する。
- □ルールチェーン
- □ルールアクション
  - ○パケットを転送する。
  - ○パケットを廃棄する。
  - ○パケットの発信元にICMPメッセージを送り返す。

ルールリスト

プロトコル
- □通過させるパケットのプロトコルに応じてフィルタリングを行う
- □IP，UDP，TCP，ICMP
- □全てのパケットを対象とする場合はIPを指定
- □特定のプロトコルに対して指定したい場合はTCPなどを用いる

ソースIPアドレス，デスティネーションIPアドレス
- □発信元である送信者のIPアドレス
- □目的地である受信者のIPアドレス
- □ネットワークアドレス(ネットワークに接続している全てのホストを対象)
- □ホストのIPアドレス

ルールリスト

ソースポート番号，デスティネーションポート番号

- □TCP，UDPではアプリケーションのサービスの種類毎に用意されたアドレス
- □これをもとにどの上位レイヤとデータ転送を行ったら良いかを決定している
- □クラッカーはポートスキャンと呼ばれる手法ですべてのポート番号を探索し，サービスが行われているポート番号を見付だし，攻撃の足掛かりとすることが可能である。
- □特定のサービスを禁止する場合などに用いられる。

ネットワークインタフェース

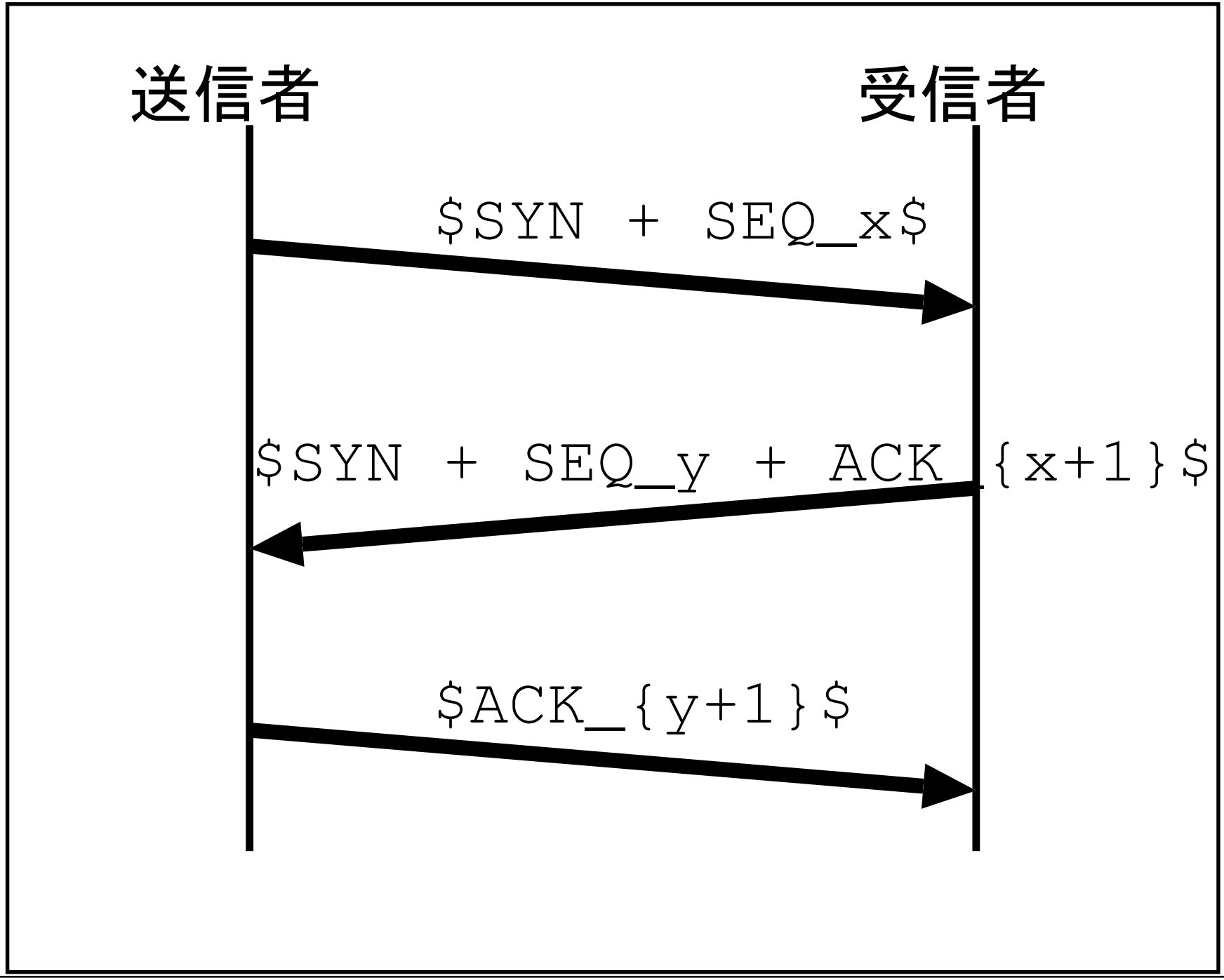
- □特定のネットワークインタフェースを通過するパケットを指定
- □インタフェース名とルータからみた入出力の方向を指定

ルールリスト

TCPのフラグ

- □UDPやICMPはコネクションレスな通信
  - ○ポート番号やIPアドレス，ネットワークインタフェースを用いたフィルタリングのみ
- □TCPはコネクション指向の通信
  - ○通信の様々な段階で異なるフラグがを手掛かりにした
  - ○フィルタリングが可能
- □コネクション確立時のパケット
  - ○SYNフラグ有り
  - ○ACKフラグ無し
  - ○コネクションの確立時に確立しようとする側から最初に送られてくるパケットに付けられるフラグ
- □コネクション確立後のパケット
  - ○ACKフラグまたはRSTフラグ有り
  - ○コネクションの確立後の通信のパケットに付けられるフラグ

TCPのコネクション確立



非対称的なフィルタリング

□組織内から外部のインターネット上のホームページをみることは可能

□外部から組織内のネットワーク上のホームページをみることはできない

deny tcp from any to 192.0.0.0/24 80 setup SYNのみ
allow tcp from any to any http established ACKあり
allow tcp from any http to any established ACKあり

□組織外から組織内へ転送されるコネクション確立のためのHTTPのパケットは阻止

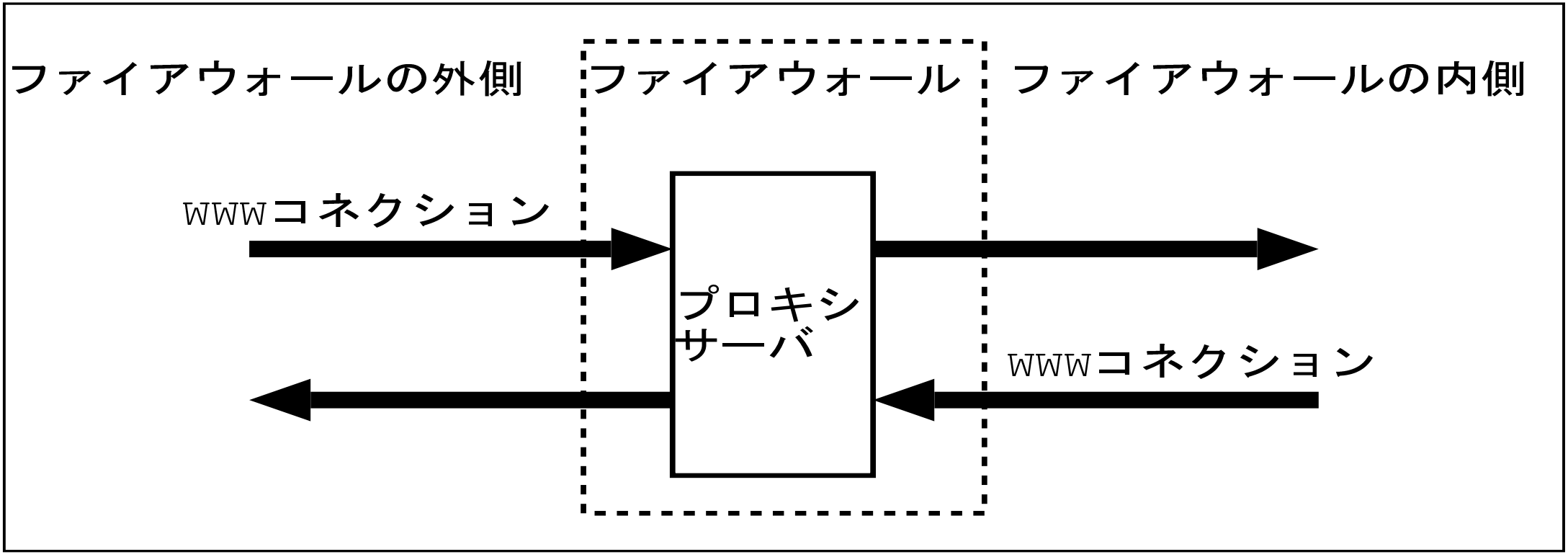
□コネクション確立後のHTTPパケットと組織内から組織外へ転送されるコネクション確立のHTTPパケットを通過

フィルタリングのポリシー

- デフォルトでは全てのパケットを阻止して，サービスに必要なパケットのみフィルタリングして通過させる方法
- デフォルトでは全てのパケットを通過させ，セキュリティ上必要なパケットのみ阻止する方法

プロキシサーバ

○アプリケーション層での中継、特定のアドレス、プロトコルのみ転送

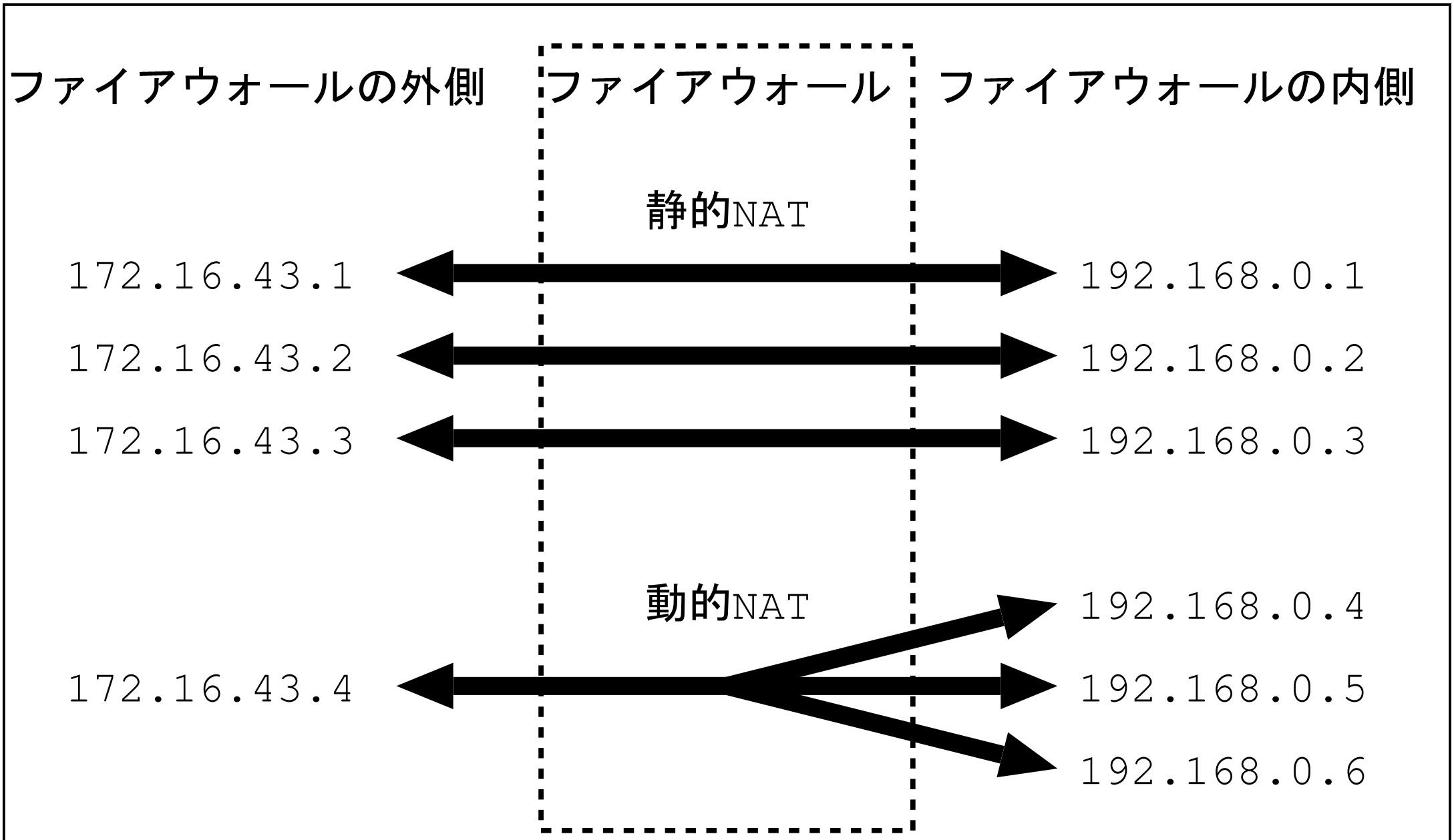


プロキシサーバー

- □パケットフィルタリング
  - ○カーネルのパケット転送機能により適切なパケットのみ通過
- □プロキシサーバ
  - ○カーネルのパケット転送を禁止
  - ○サービス毎のデーモンを置き換えることによりパケットを転送

- □WWWのプロキシサーバではクライアントがファイアウォール外のWWWサーバにアクセスする際，プロクキシサーバがクライアントに代ってWWWサーバからデータを取得し，それをクライアントに転送する。
- □一般にプロキシサーバは通常のホストより強固な認証手段を実装している。

NAT: Network Address Transration



NAT

- □セキュリティ問題とは直接関係ないファイアウォールの機能のひとつとして実装されることが多い
- □NATはIPv4のIPアドレス枯渇を解消するための一つの解決法である
- □NATではファイアウォールの内部のネットワークではプライベートアドレスを用い，必要に応じて外側のパブリックアドレスへの変換をおこなう。
- □アドレス変換の形態
  - ○静的NAT
    - ▹パブリックアドレスとプライベートアドレスを1対1の関係で固定的に変換する
    - ▹外部からアクセスする必要があるサーバなど
  - ○動的NAT
    - ▹複数のプライベートをひとつのパブリックアドレスに割り当てる
    - ▹外部から内部へのコネクションの確立はできない
    - ▹内部宛てのパケットで特定のポート番号宛てのものを特定のプライベートアドレスに変換することで解決する方法もある。

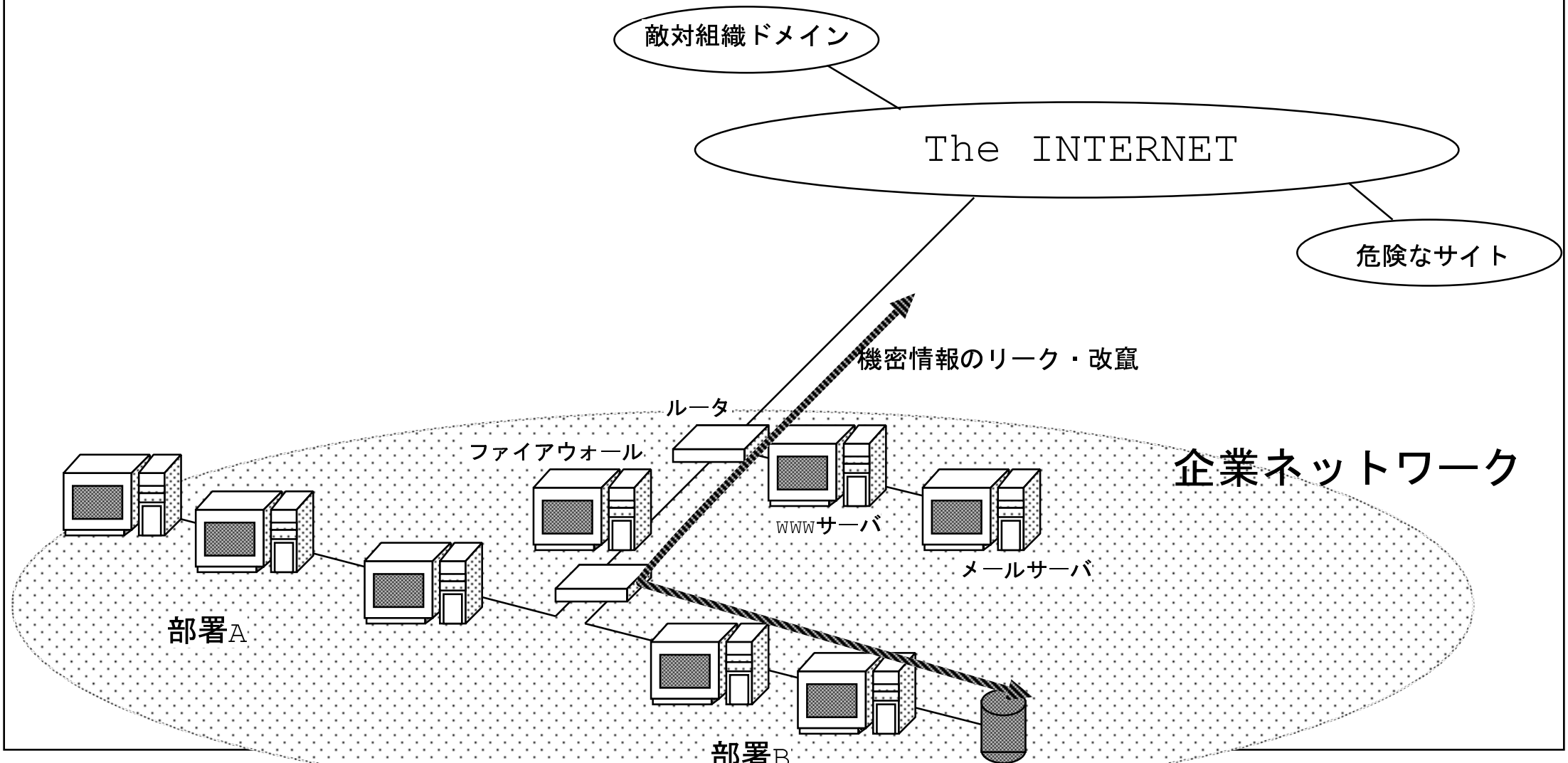
ロギング

- ファイアウォールはセキュリティの要であるからクラッカーからのアタックにさらされる可能性が高い。そこで万が一の不正侵入に備えてユーザの行動やパケットフィルタリングの結果などの記録をとることが必要となる。これをロギング(logging)という。
- ロギングは主にデーモンsyslogdにより行われる。
- 主な記録
  - ユーザのログイン時刻の記録,
  - ログインしているユーザのリスト,
  - ログイン，ログアウトの記録,
  - ユーザの実行したコマンドの記録,
  - プログラムのメッセージの記録などがある。

企業ネットワークの利用形態

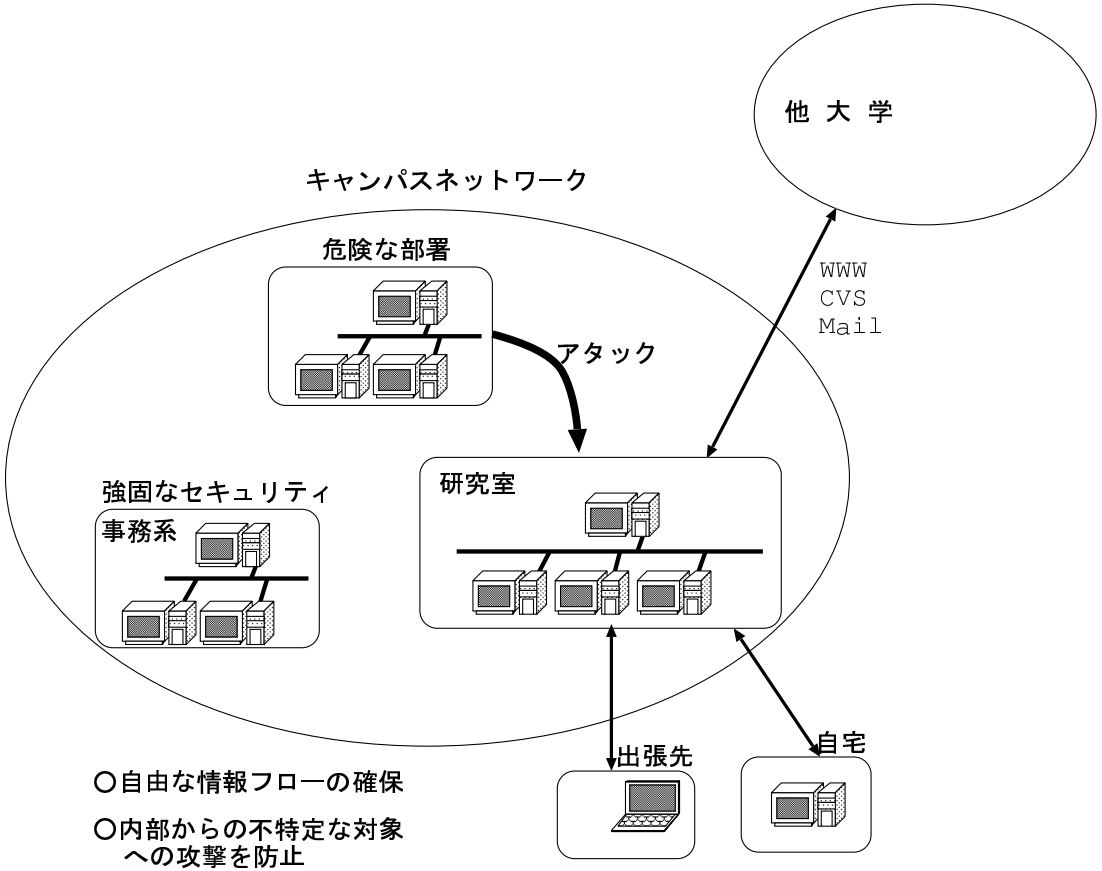
○機密情報／顧客の情報を外部からの攻撃から守るため.

- ▹危険と思われるサイトへのアクセスの禁止
- ▹社外サイトへのアクセスの監視
- ▹社員のメールの監視



キャンパスネットワークの利用形態

- ▹学外研究機関との共同研究
- ▹学外から研究室へのアクセス
- ▹事務系業務での利用
- ▹要求されるセキュリティレベルは様々
- ▹ユーザのモラルの問題
- ▹学外だけでなく学内からの攻撃
- ▹物理的なセキュリティの問題



ファイアウォールの管理のコストと安全性

- □プロキシサーバの場合
  - ○コスト：外部からアクセスできるマシンがなければ、主にプロキシサーバの管理だけである
  - ○安全性：主にプロキシサーバのセキュリティレベルに依存
- □パケットフィルタリングの場合
  - ○コスト：一般的に外部からアクセスできるマシンもあるため、管理するマシンの数が多くなる
  - ○安全性：プロキシーサーバ以外にも管理マシンが増えるためプロキシー型より安全性は減る

本人認証

間接的証拠としての所持品

- □水戸黄門の三葉葵の入った印篭
- □鍵、印鑑、顔写真のない証書
- □磁気記録カード
- □トークン式、暗証番号式、署名式
- □発信機能付き装身具

顔写真付き所持品

- □身分証明書、許可証、免許証

本人認証

固有の記憶情報
- □パスワード、暗証番号、生年月日の口証、
- □ディジタル署名、零知識相互証明

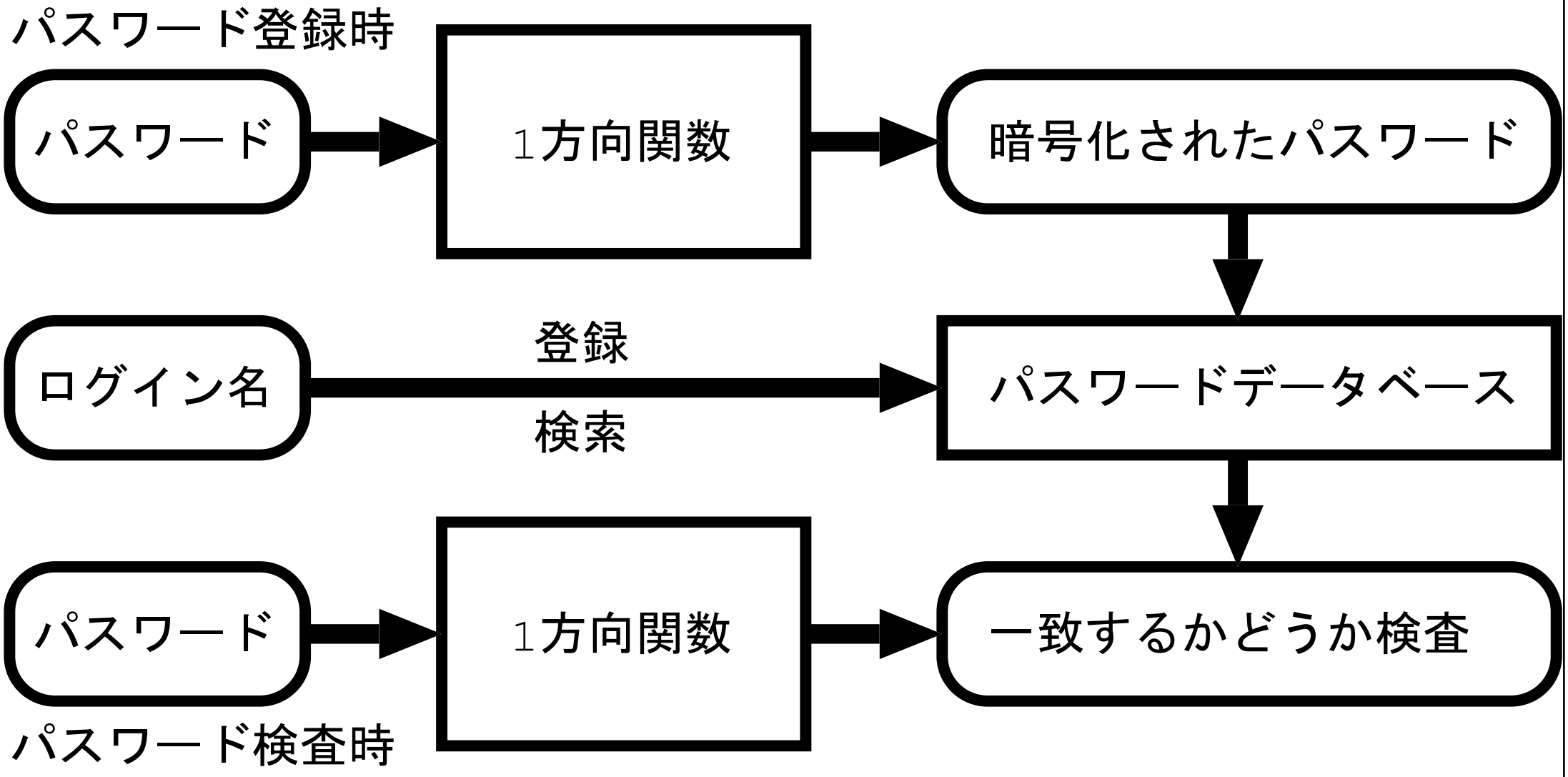
習慣化した動作による生成物
- □署名、筆跡

身体的属性
- □指紋、手形掌紋、顔
- □音声、声紋
- □歯形
- □網膜パターン
- □DNA鑑定

UNIXのアカウントとパスワード

- UNIXはマルチユーザのシステムであるから，ユーザが別のユーザやシステム重要なファイルに対するアクセスを制限し，ファイル内のデータの保護する仕組みが必要不可欠。
- ユーザは計算機を使用する際にユーザ名となるアカウントとパスワードを入力することによりログインを行う。
- パスワードの付け方
  - パスワードの取り扱いは極めて重要
  - ひとりの不注意が研究 室のシステムだけでなく、全学のシステムさらに他の機関のシステムまで危機 に陥れる危険がある
  - 踏み台攻撃

1方向関数によるパスワード暗号化



パスワードを決めるときの注意点

- □**6～8**文字の英数字、記号の組合せ
- □9文字以上でも構わないが無視される
- □数字だけはだめ
- □大文字、数字、記号を混ぜた方が強度が増す(例: tcp/IP)
- □ログイン名や個人情報、所属組織情報から類推されるものはだめ
- □できるだけランダムなもの
- □人名、地名、その他の単語など日本語、英語、仏語、独語の辞書に載っているような単語を単独で使ってはだめ(例: Kanagawa)
- □単語を逆さにしても効果はない(例: awaganak)
- □キーボードのならび順はだめ(例 asdfjkl;)
- □本に乗っているものやこの講義で出てきた例はだめ

パスワードの取り扱い注意

管理上の注意点

- □パスワードは暗記する
- □紙やファイルに書いたり、他人に（シス テム管理者も含む）教えてはいけない
- □年に数回はパスワードは変更した方が安全
- □他の組織と同じパスワードを使ってはいけない

良さそうな例

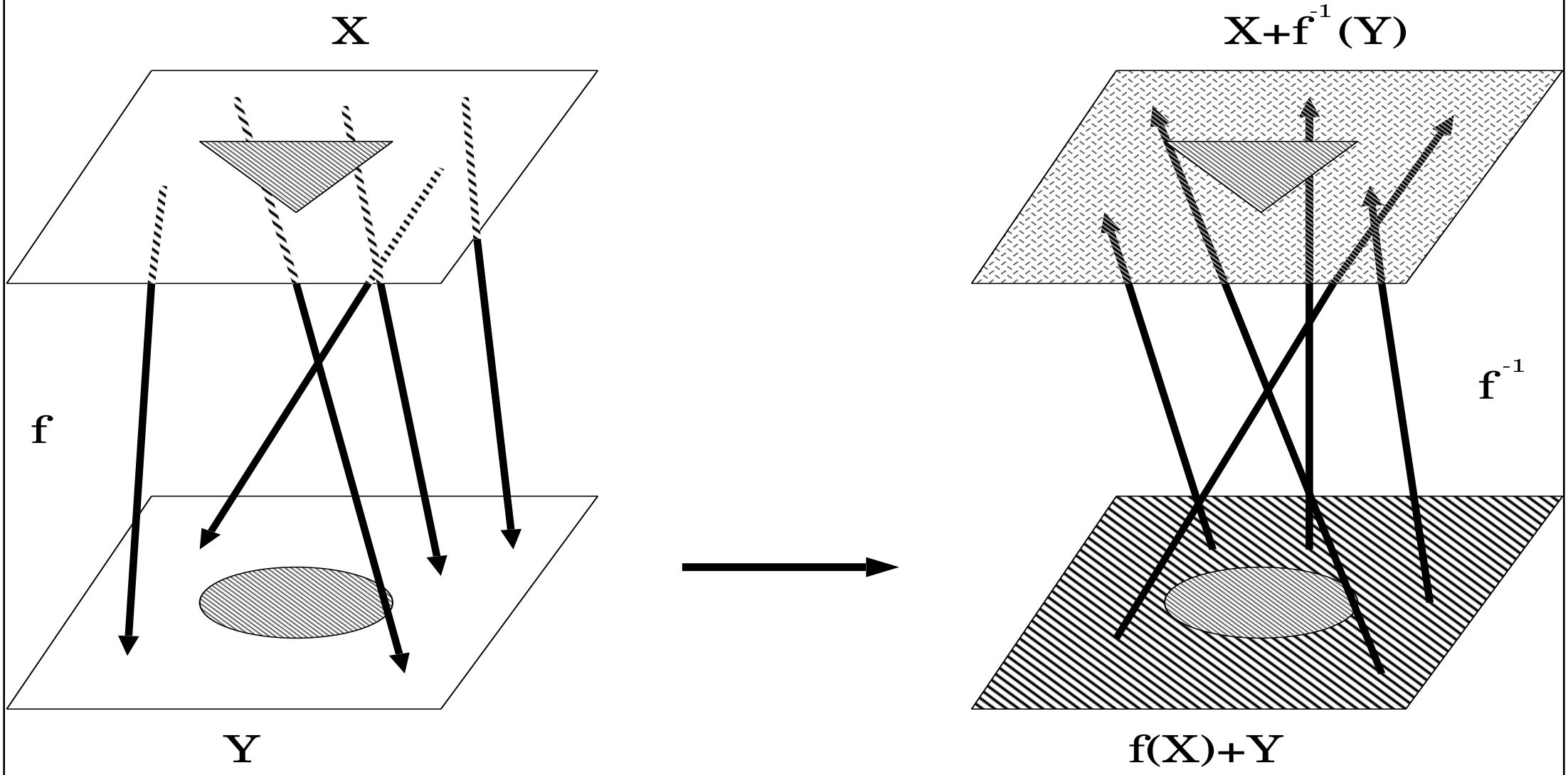
- □歌詞や標語の頭文字を並べる。「五月雨をあつめてはやし最上川」ならSaAHaMo
- □好きなタレントのイニシャルを並べる。鈴木一郎。鈴木次郎。鈴木三朗子。なら SiSjSs

画像情報の暗号化

- □画像情報はデータ量が多い
- □画像情報は冗長度が大きい
- □内容を判断するのは人間の視覚
- □なにをもって解読に成功したとするか
  - ○首脳会談のテレビ電話→誰が喋ってるかわかればいい
  - ○有料テレビ→ノイズのない画像が要求される
- □静止画、動画
- □評価基準
  - ○安全性、コスト、品質、処理速度

電子透かし

□画像や音声情報に視覚聴覚的にはほとんど影響が出ないように情報を埋め込む



電子透かしの必要性

- □画像通信の利用が広がるにつれて、データ通信のセキュリティと同じように画像情報の秘匿や著作権保護といった画像通信におけるセキュリティについても検討することが必要となる。
- □従来提案されている方法では、透かし情報を検査するエンティティに対して透かしが公開されてしまうため、偽造の可能性がある。
- □著作権保護のためには、効率的がよく安全なディジタル署名や、コンシールドイメージ（透かし情報の埋め込み）が不可欠である。
- □ディジタル画像はコピーが容易に行える
- □現在は著作者の情報が含まれていない
- □暗号化では画像の自由な流通を妨げる恐れがある

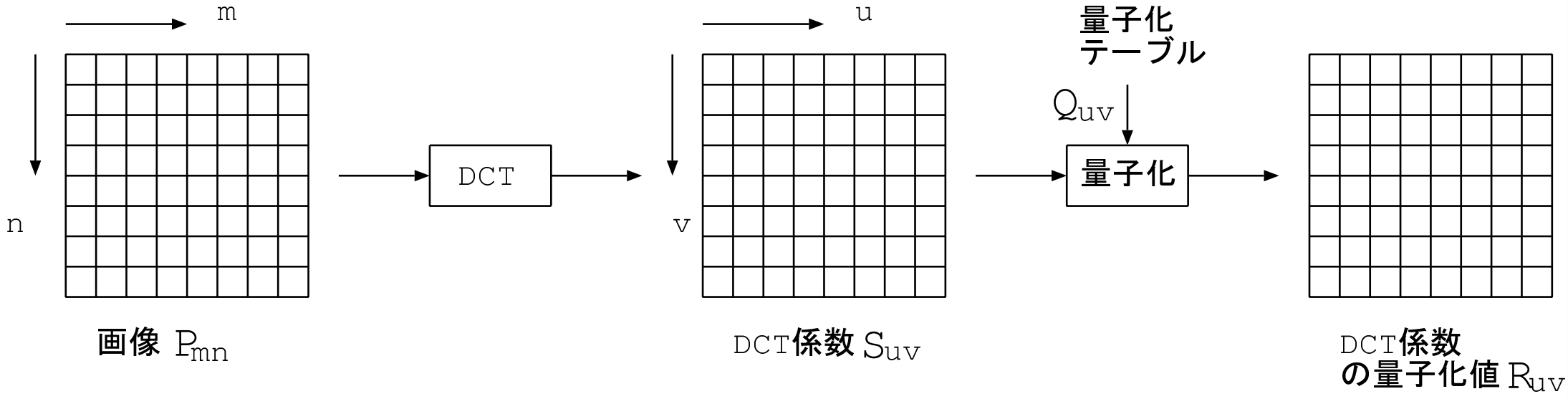
電子透かしに求められる条件

- □電子透かしは画像自身に埋め込まれること。画像全体にわたり分散配置することが望ましい
- □透かし情報は編集、圧縮、伝送などの各種変換処理に対し変質、消失しないこと
- □透かし情報の埋込みとその復元に必要な手続きは簡単で、処理時間は短いこと
- □透かし情報の消去、改ざんなどの攻撃を排除できること

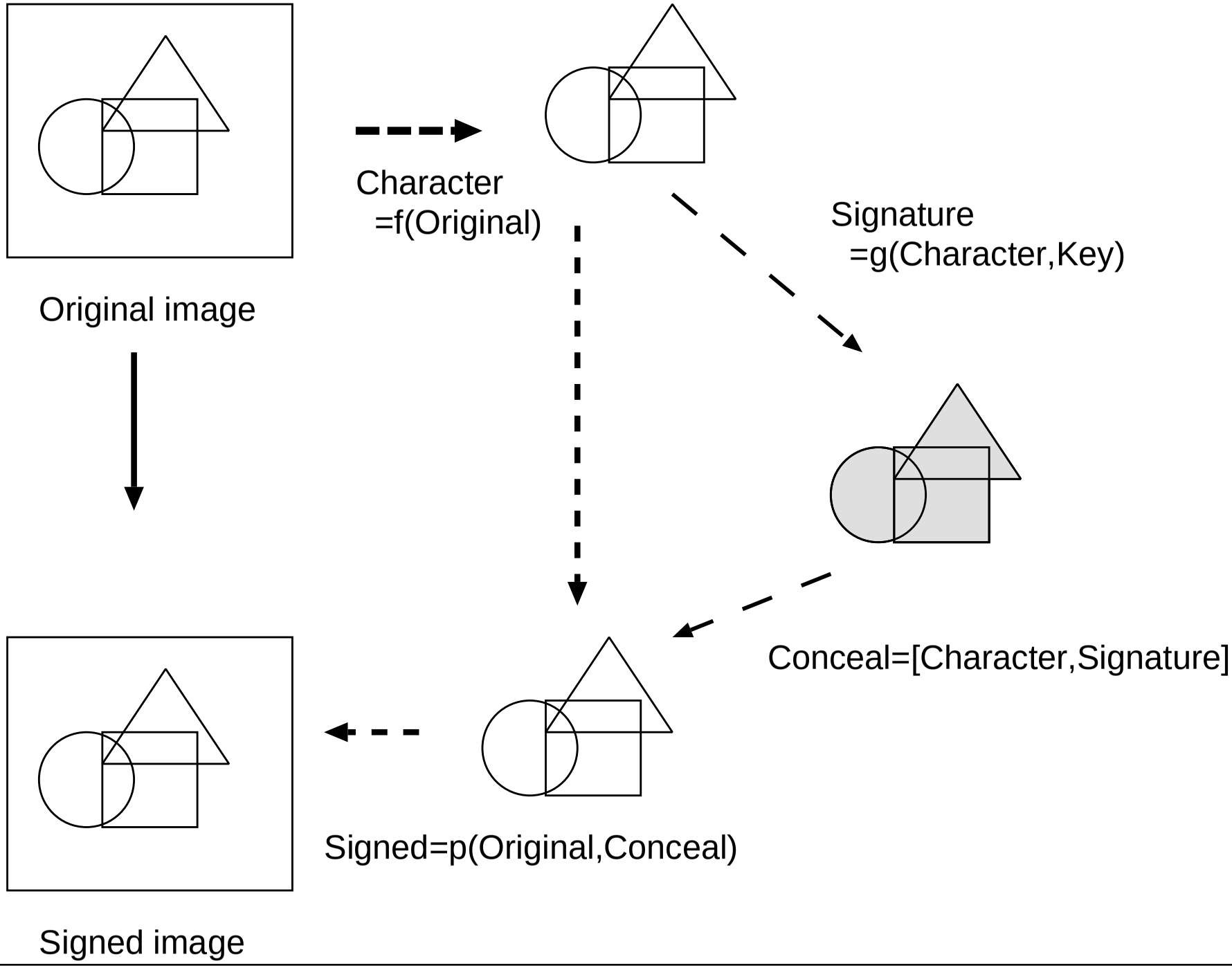
電子透かしの構成法

□空間領域の電子透かし
- ○画素値を直接操作する電子透かし
- ○透かし情報は、主に画素値の下位ビットに埋め込まれる。

□周波数領域の電子透かし
- ○離散コサイン変換など直行変換による電子透かし
- ○DCTはMPEG,JPEGに用いられる周波数変換であり、透かし情報はビット情報として各ブロックのDCT成分に数値制御で埋め込まれる



透かし情報作成


Character
=f(Original)
Signature
=g(Character,Key)
Original image
Conceal=[Character,Signature]
Signed=p(Original,Conceal)
Signed image

StirMark

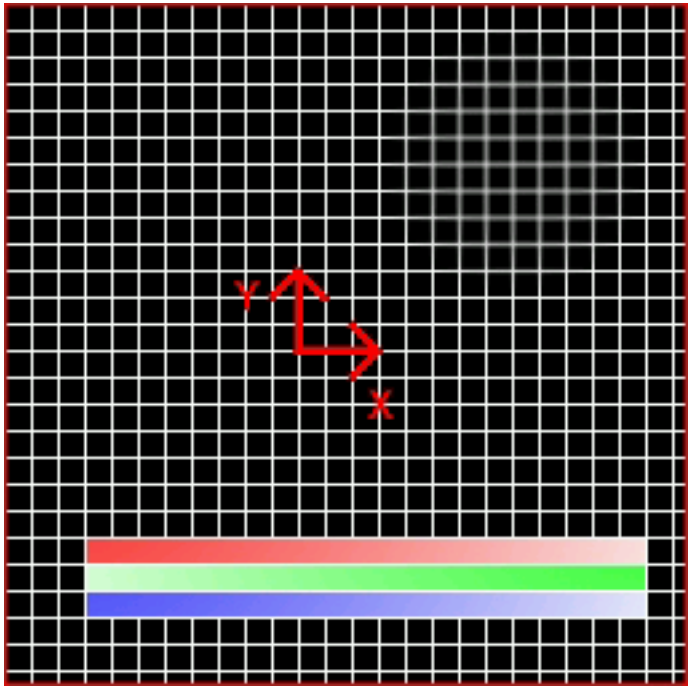
StirMarkとは

□透かし除去を目的としたプログラム

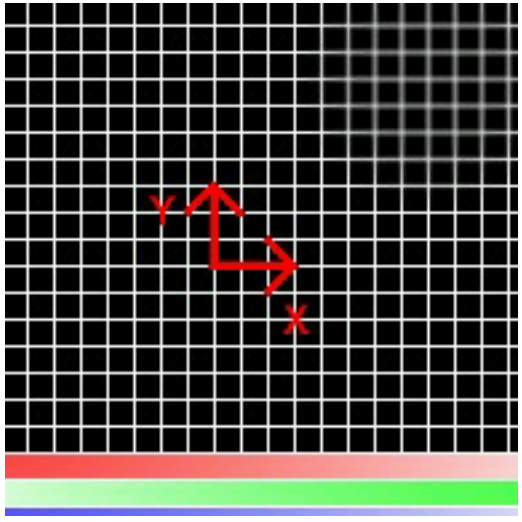
□透かし画像への予想される攻撃を想定

□電子透かしの耐性の指標となる

StirMark

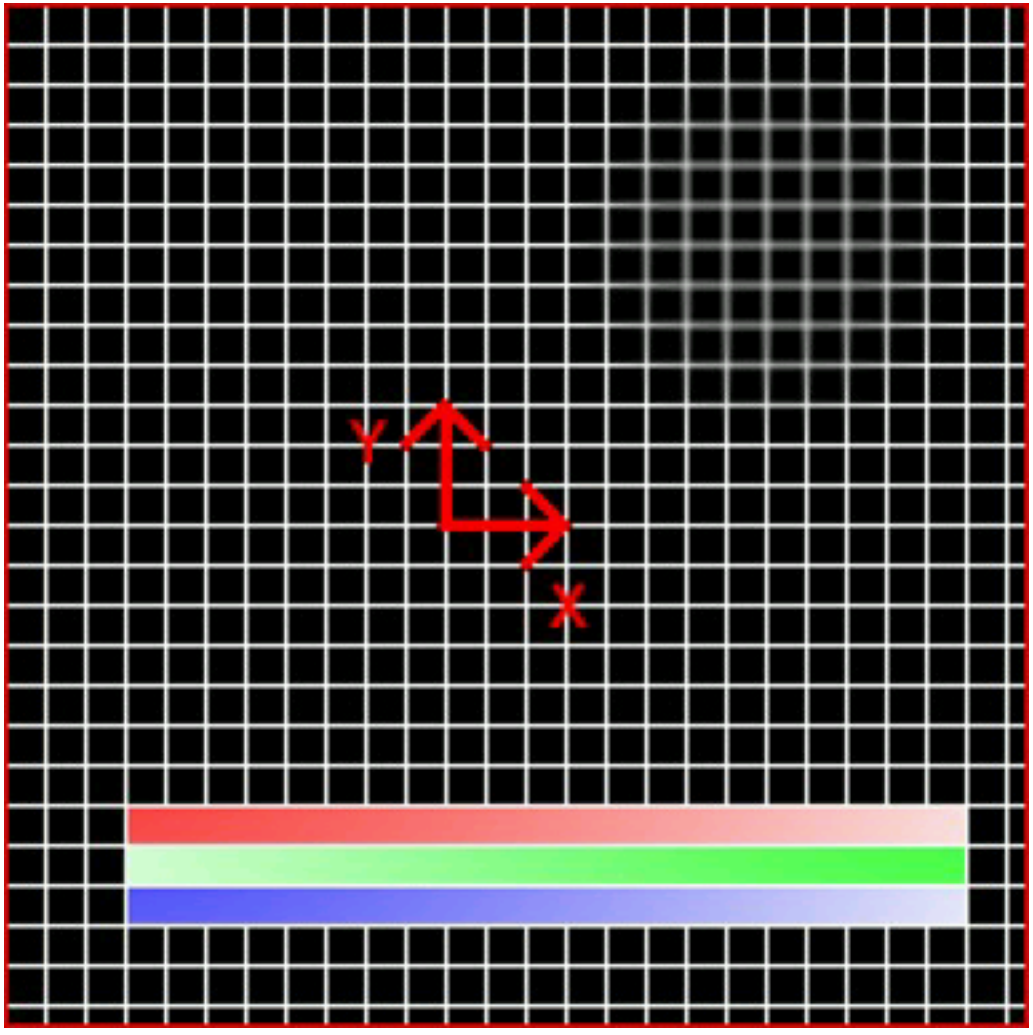


原画像(Image Size 256×256)



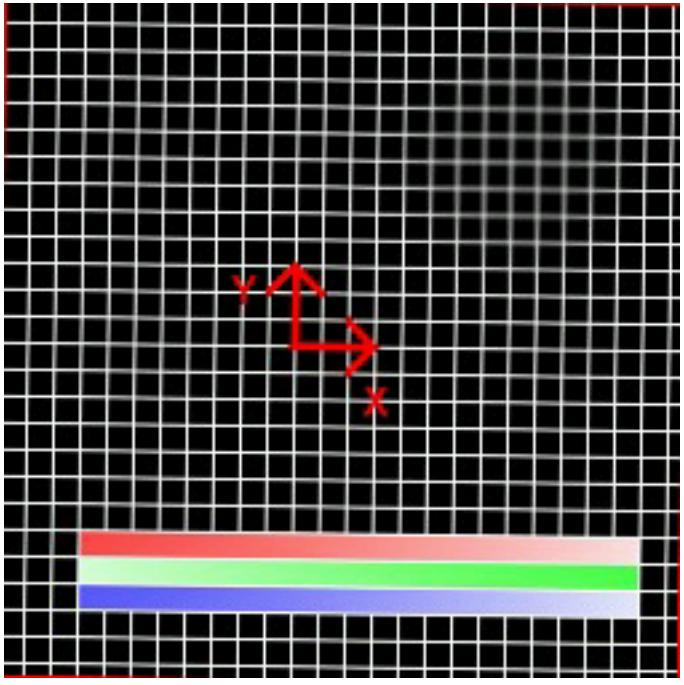
base - Cropping 25%

StirMark



base - Scaling 1.50 150%に拡大。出力画像は384×384

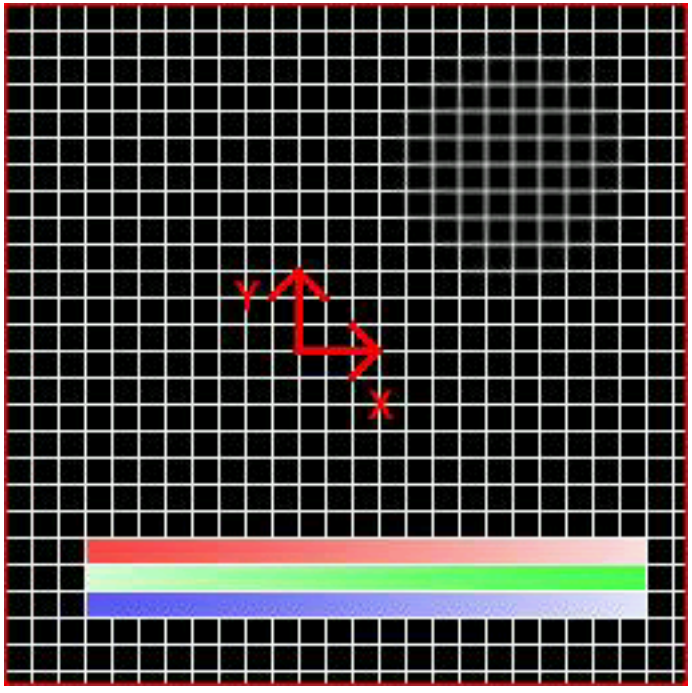
StirMark



base - Rotation 0.75 with cropping

（0.75度回転。出力画像は253×253）

StirMark



base - JPEG compression 70

（圧縮率70のJPEG圧縮。出力画像は256×256）

御質問・御問い合わせ

kino@cc.kanagawa-u.ac.jp

http://kinoshita.cc4-4.kanagawa-u.ac.jp