電子メール技術動向とシステム構築

- IMAP, PGP, S/MIME -

（株）オレンジソフト
渡部直明
kitarou@orangesoft.co.jp

（株）電通国際情報サービス
デジタルキャンパス
熊谷誠治
kuma@isid.co.jp

Orangesoft

iSiD

Agenda

- 耐障害性の高いメールサーバーの構築
- メールシステムの安定運用
- 安全なメールシステムとは
- モバイル環境での電子メール
- VPNとワンタイムパスワード
- POPとIMAP
- 暗号メールの基本
- PGPとS/MIME
- 暗号メール運用上の問題点

Orangesoft

メールサーバの運用

Orangesoft

メールはビジネスインフラ

- これまでは…
  - 「電話が止まると仕事にならない」
    - » 重要なビジネス・インフラだった
- 今は…
  - 「メールが止まると仕事にならない」
    - » メールがビジネス・インフラに成長した
- あなたの会社のメール・システムは大丈夫 ？
  - トラブル発生時に何時間以内に回復しますか ？
  - どのようなトラブルを想定していますか ？
  - 利用者はどのようなことに気をつけるべきですか ？

トラブルが起こるとどうなる ？

- トラブルの内容によって状況は変わる
  - これまでは電話屋さんが直してくれた
    - » 停止時間はせいぜい2時間程度 ？
- 電子メールのトラブルの場合は ？
  - 社内に担当窓口はあるのか ？
  - 発信したメールは消えるのか ？
  - 着信しているはずのメールは消えるのか ？
  - 相手とどのように連絡を取ればいいのか ？
  - いつ直るのか ？
- 実質的な損害は ？
  - 機会的損失を含めると莫大に

トラブルはいつ復旧しますか？

- 利用者にとっては最重要課題
  - 「わかりません」や「そのうちに」は許されない
  - これによってとりあえずの仕事の進め方が変わる
- 手順が明確でないと判断できない
  - 事故はいつも突発的
  - めったに起こらないからすぐに対応策を忘れる
  - 対応手順書を作ろう
- システム設計時に検討が必要
  - 目標復旧時間に合わせてシステムを設計する
  - もちろん運用システムも含めての検討が重要
  - Non-Stop、2時間、12時間、24時間、運任せ

Orangesoft

どのように復旧しますか ？

- トラブル発見
  - ユーザに任せる ？
- トラブル内容特定
  - 状況から本当のトラブルを見極める
- トラブル原因究明
  - トラブルの様子から原因を探す
- トラブル原因排除
  - 原因を排除する
- トラブル復旧
  - 関連する影響を調べて、問題点をすべて直す

Orangesoft

トラブルを避けるために

- トラブルによる影響を抑えるには準備が必要
  - 準備がないと対応が遅れる
  - 重要性がなければ準備は不要
- トラブルの原因の例
  - 停電
  - ハードウェアの故障
  - ソフトウェアのバグ
  - 設定・操作ミス
- 対応策を考えている企業は少ない
  - トラブルが起こるまで重要性を認識できない
  - トラブルが起こってから気づくのでは手遅れ

Orangesoft

目標復旧時間を決めてますか ？

- トラブルによって復旧時間は違う
  - ハードウェアトラブル → 修理 + リストア
  - 停電 → 停電復旧時間 + [ハードウェアトラブル]
  - 設定ミス → リストア
  - インターネット接続 → プロバイダ次第
- 復旧時間の想定によってコストが違う
  - 冗長性の高いシステムはコストも高い
  - 万全な体制は金がかかる
    - » 24時間オンサイトメンテナンス契約
    - » 要員を配置すれば人件費がかさむ
- 金イトの世界

Orangesoft

iSiD

停電

- 工事や検査に伴う停電
  - 事前に分かっているので準備可能
  - 休日にすれば影響は少ない
  - 期間が分かっている
  - 事前にシステムを停止 … 復帰時に立ち上がらない
- 事故による停電
  - 突然襲ってくる
  - 機器の故障やデータの破損につながることも
  - 回復時間が分からない
- 事故停電は避けられない
  - UPSで守る

Orangesoft

ハードウェアの故障

- 機械は必ず壊れる
  - 故障時の修理手順の明確化
    - » 自分たちで直すのか、メンテナンス屋を呼ぶのか
    - » メンテナンス屋の連絡先
  - 保守契約に入っているのか
    - » 保守時間帯と修理時間
    - » そもそも、保守契約が用意されているのか
- データの破損を防ぐ
  - データのバックアップ
    - » 連続してデータが増えるメールには不向き
  - ディスクの二重化
    - » 1台がクラッシュしてもデータは壊れない

ソフトウェアのバグ

- ソフトウェアにはバグはつきもの
  - しかし、そのことが許されるわけではない
  - バグの少ないソフトウェアを使うことが重要
- フリーウェアは避けるべきか ？
  - 実績のない製品よりも安全
  - 製品であってもサポートが完璧なんてありえない
  - 品質はベータ以下でも製品として売られることも
- 大メーカなら大丈夫か ？
  - たくさんの人がだまされ続けているケースも
  - それでいいわけができればひとつの選択肢

設定ミス・操作ミス

- 人がやることだからミスは起こる
  - しかし、許されることではない
  - 状況によっては非常に大きな影響も
  - 慣れない人が特に危ない
  - 慣れた人でも危ない
- しくみとしてミスを防ぐ
  - 誤操作の影響が致命的な損害にならないように
  - 設定のチェックとテストの体制づくり
- それでも事故はなくならない
  - ファイルの消去、メールのループ、配送遅延など
  - ミスの多い担当者を再教育

トラブル対応マニュアル

- トラブル発生時の連絡先
  - トラブルの受付体制と関係者との連絡方法
  - メンテナンス会社の連絡電話番号
- トラブル検出のしくみ
  - 第一報はユーザから届くことが多い
    - 「メールが送れない」、「メールが届かない」
  - ユーザが検知できないトラブルもある
    - 管理者が検出しないとトラブルが続く
  - 検出するしくみが重要に
- 過去のトラブルをデータ・ベースに
  - 同じトラブルでは時間をとられない

Orangesoft

耐障害性の高いメールサーバ

- 予備マシンや部品を用意する
  - 故障すればマシンを交換
  - 故障した部品を交換
- システムを二重化する
  - ミラー・ディスク、RAID5
  - ホット・スタンバイ
  - フェイル・オーバー
- 停まらないコンピュータを用意する
  - 銀行システムなどで使われている
  - 非常に高価
  - サーバが停まらないだけでは運用は続けられない

Orangesoft

メールシステムの安定運用

- 壊れにくい機器と安定したOS
  - 世の中には1か月連続運転できないようなOSもある
    - » 負荷が高まれば早くトラブルが出る
- 迅速なメンテナンスの受けられる機器
  - “普通の” PCのオンサイト契約じゃだめ
- 集中メールシステム(サーバが1台)
  - 集中方式にすれば停まるときはすべて停まる
  - 分散方式は利用者が構成を意識する必要あり
  - 離れた場所のサーバは対応が遅れる
  - 機器が増えればトラブルも増える

Orangesoft

SPAMメール問題

- SPAM(スパム)とはハムの缶詰
  - 勝手に送られてくる電子メールの広告を意味
  - うるさい
- 捨てるだけだが読むのにもコストがかかる
  - これまでのダイレクトメールは発信者のコストが大
  - ダイレクト電子メールは読む側のコストが大
- 悪質なものと単なる無知と
  - 「1000万人に広告を送ってあげます」
  - そのような業者に広告を依頼しないことが一番
- 中継に使われることも

サーバのチューニング

- 同じ機器でも設定次第でパワーを発揮できない
  - ボトルネックを探すことが重要
    - » CPU、ネットワーク、メモリ、ディスクアクセスなど
    - » ボトルネックを順々に解消していく → 努力が重要
  - 「タコ」な設定はマシンの能力を殺す
- 利用方針に合わせた設定が必要
  - 受け取られなかったメールの戻し方
  - 受発信ログの残し方
- 「これ」という解決策はない
  - システムに合わせて調整する
  - 経験がものをいう

Orangesoft

安全なメールシステムとは

- 届いてなんぼのシステム
  - 届かないメールをメールとは呼ばない
- いつもちゃんと動いている
  - たびたび停まると安心して使えない
- メールがなくならない
  - あたりまえ
- メールが届いていないことを教えてくれる
  - 6時間送れないのなら教えてほしい
- 不正なメールを送らない
  - メール・ループをよく起こすシステムもある
- よく考えてシステムを選ぼう

HTML, Riched Text

- メールの表現力をアップする
  - 強調文字、色文字、アンダーライン、フォント
  - 絵、音、動画で伝える
- これらの機能を売り物にするツールも登場
  - マルティメディアメール
  - MIME(Multmedia Intenet Mail Extension)を利用
  - NetscapeもOutLookも対応
- こんなメールが必要なのか ？
  - 読めないメーラもある
  - トラフィックが増える
  - 知らず知らずに送っていませんか ？

Orangesoft

モバイル環境での電子メール

Orangesoft

iSiD

モバイル環境での電子メール

- メールが重要な通信手段なら...
  - いつでも読み書きできなければならない
  - どこででも読み書きできなければならない
- 移動中や移動先ではEthernetは使えない
  - 接続方法が問題
  - 無線電話(携帯、PHS)、公衆電話、ホテルの電話
- 無線は高くて遅い
  - PHSでさえ29.2kbps
- 有線も高くて遅い
  - ISDNでさえ最高128kbps
- どうすりゃいいの ？

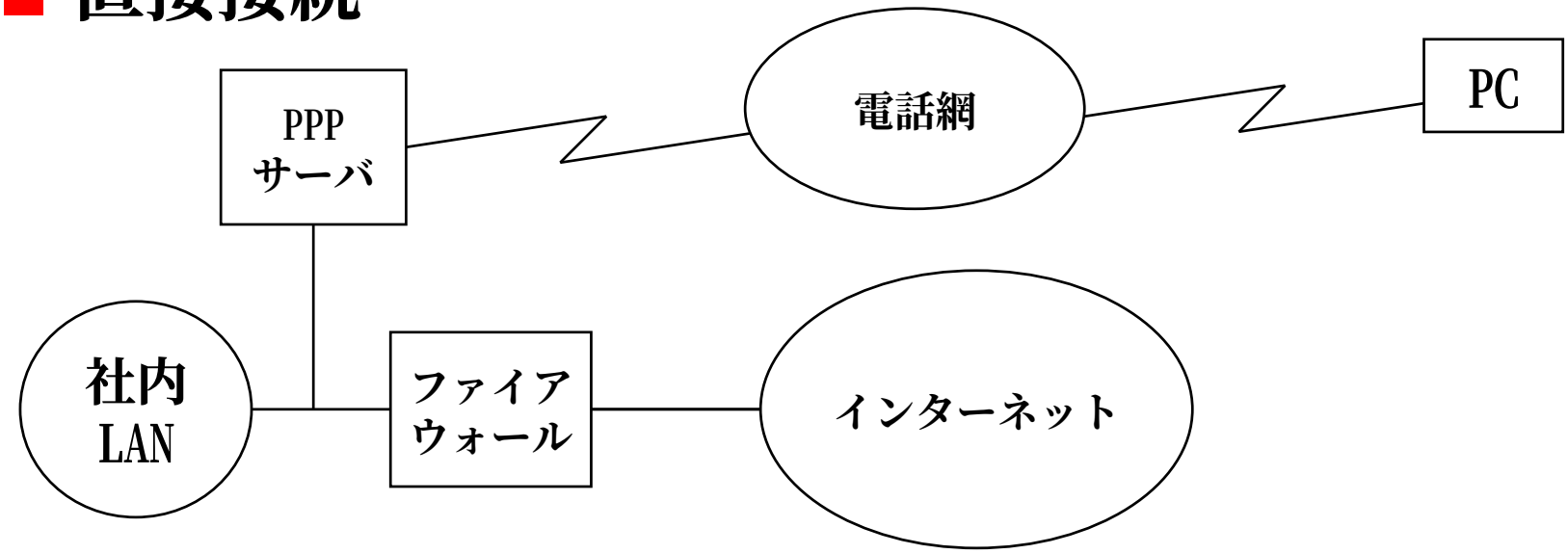
Orangesoft

モバイルでの接続方法

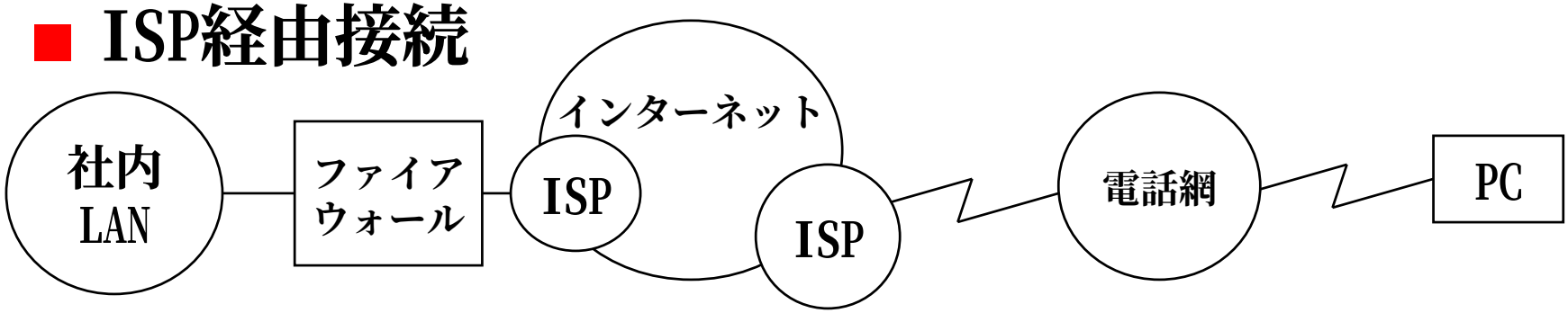
- インターネット経由で接続
  - インターネットは盗聴される
    - » パスワードが盗まれる
    - » メール自体を読まれてしまう
  - やっぱりインターネット経由は危ない
- 社内ネットワークにダイアルアップ接続
  - PPPサーバを社内に設置
  - 出張先からは長距離電話や国際電話…非常に高価
  - 社員が接続できればクラッカーも接続できる
- セキュリティをどうしようか ？

外部からの接続例

■ 直接接続



■ ISP経由接続



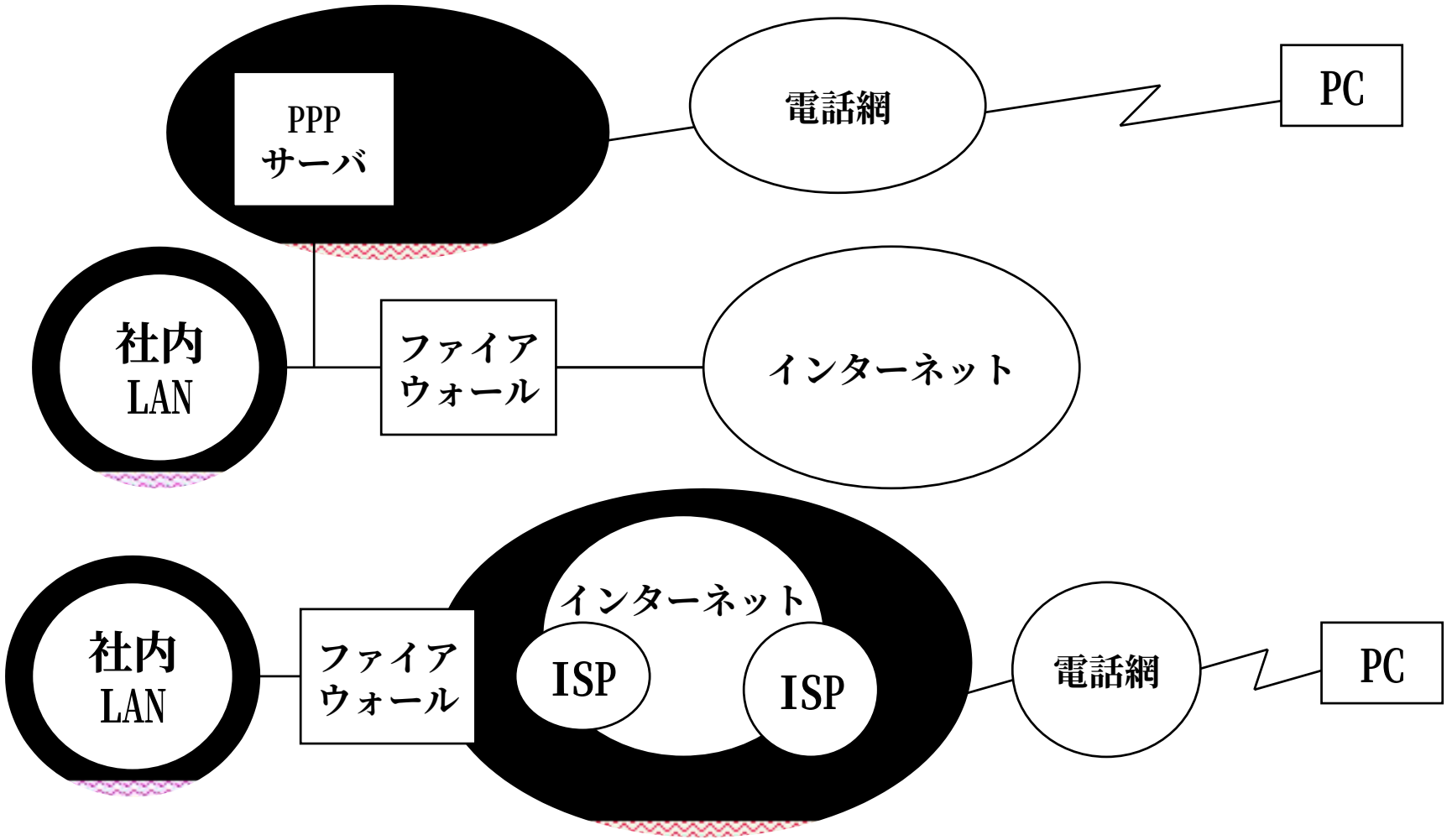
Orangesoft

[redacted]

安全にネットワーク接続したい

- 安全とは
  - 侵入されない → 接続パスワードを守る
  - なりすまされない → 接続パスワードを守る
  - 盗み読みされない → 通信路の暗号化
- パスワードだけの接続は危ない
  - 玄関にダイアル錠をつけておくようなもの
    - » 何度かトライすれば「偶然」入れる
    - » 鍵を開けるところを盗み見する
  - これではセキュリティを確保できない
- インターネットは盗聴されている
  - メールが流れれば中身を読まれる
  - パスワードを送ればパスワードが盗まれる

ここが危ない



Orangesoft

外部からの接続は許さない？

- セキュリティを考えると外部接続は許せない？
  - そう考える組織もある
- 物理的に相手を認証する
  - コールバック
  - 発信者番号通知
- パスワードを使い捨てる
  - ワンタイムパスワード
  - ワンタイムパッド
- セキュリティを捨てる
  - 安全よりもコストや使いやすさを優先
  - 何が起こってもしかたがない
  - まともな組織はこんなことを許さない

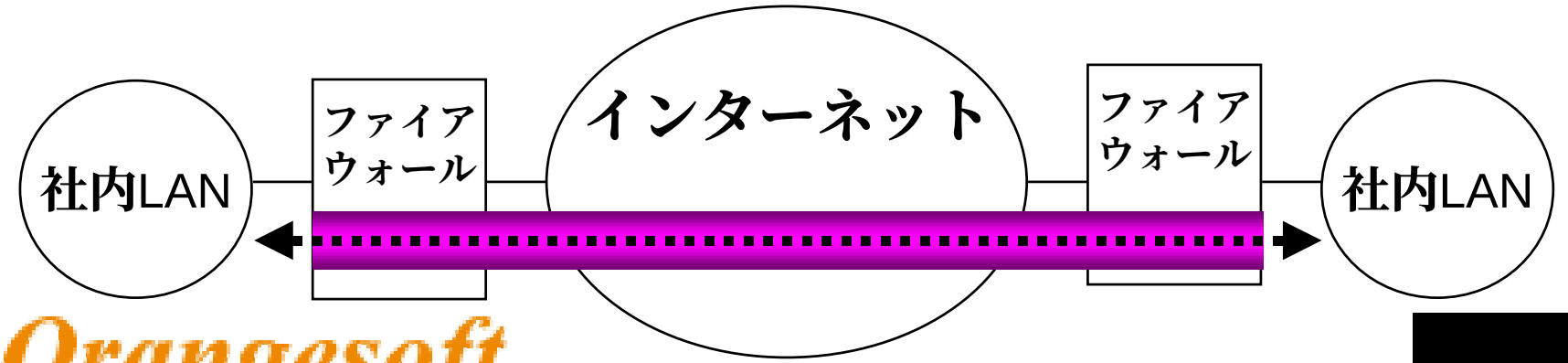
Orangesoft

安全にネットワーク接続する

- 接続が安全なだけでは不十分
  - 経路によっては盗聴対策が必須
  - インターネットを経由すると盗聴が大問題
- 通信路を暗号化する
  - VPN (Virtual Private Network)
  - SSL (Secure Sockets Layer)
  - SSH (Secure SHell)
- 安全につないで安全に使う
  - 接続時の安全確保と接続中の安全確保
  - 両方考えないといけない

VPN

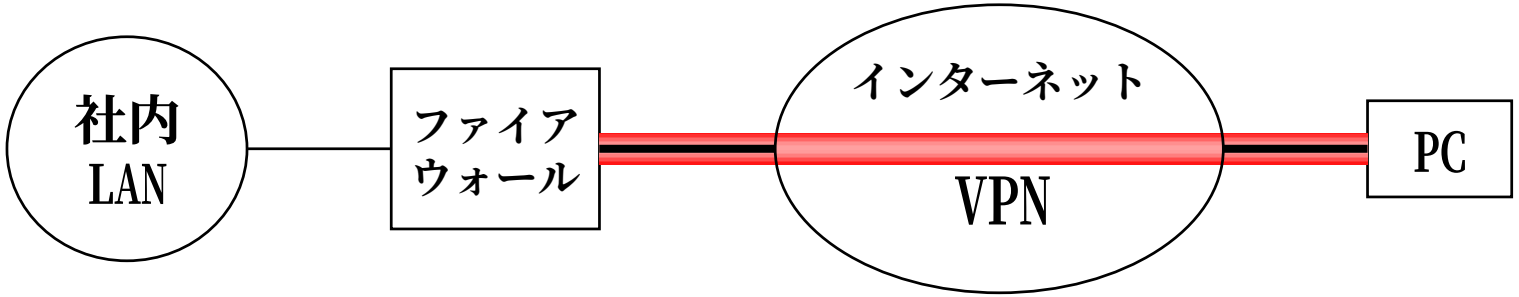
- Virtual Private Network
  - インターネットを専用線のように使う
  - インターネット内を暗号化して通す
- 特徴
  - ネットワークの信頼性はあくまでもインターネット
  - ネットワークの価格もインターネット
  - インターネット接続部のセキュリティ確保が問題



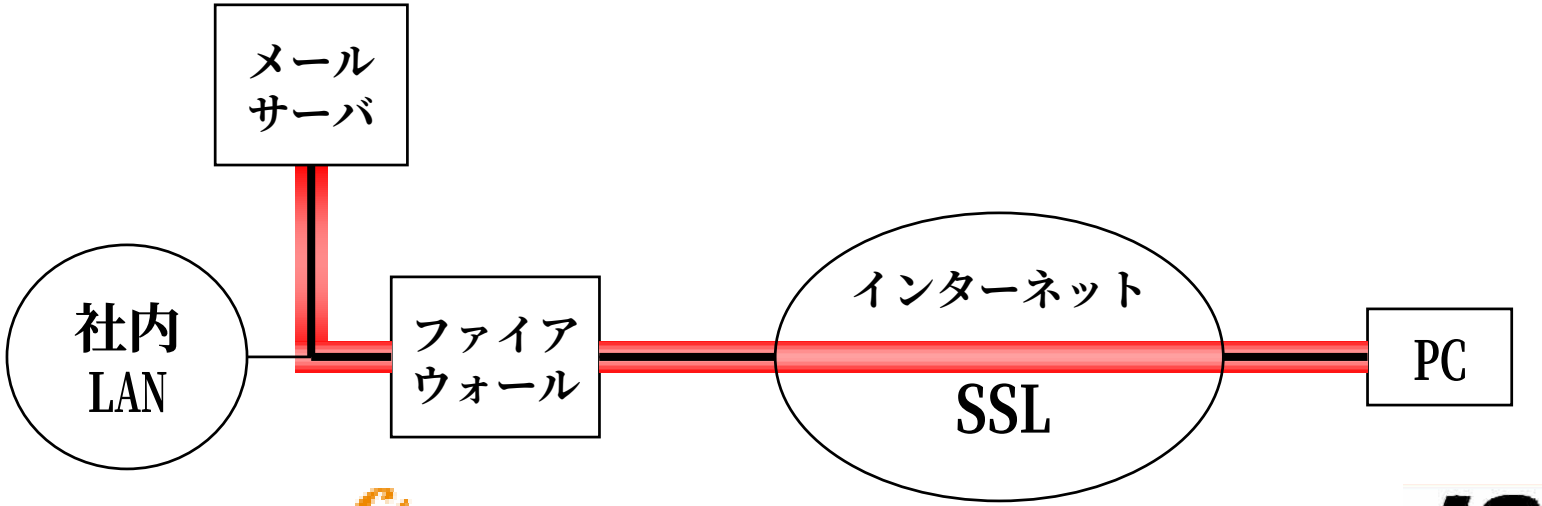
Orangesoft

通信路を暗号化する

- VPN(Virtual Private Network)



- SSL(Secure Sockets Layer)



Orangesoft

iSiD

具体的な接続方法

- 日本国内なら
  - 自宅の電話(直接接続、ISP経由)
  - ISDN公衆電話(直接接続、ISP経由)
  - 携帯電話、PHS(直接接続、ISP経由)
  - ホテルの部屋の電話(直接接続、ISP経由)
- 海外から
  - 国際電話(直接接続、ISP経由接続)
    - » 空港のラウンジ、ホテルの部屋、飛行機のなか
  - 市内電話(ISP経由)
    - » 空港のラウンジ、ホテルの部屋、飛行機のなか
  - 携帯電話

ISDN公衆電話

- 最近はどこにでもある
  - モデムでもISDNでも使える
  - ISDNを使えば安定して通信が行える
  - 速度も64Kまたは128Kも可能
- 認証が問題
  - 発信者番号通知を使った認証が行えない
  - コールバックも行えない
- 落ち着いて使えない
  - 受話器ももたずに電話ボックスにいると…
  - 後ろに並ばれると…

Orangesoft

ホテルの部屋の電話

- 米国ではモジュラコンセントが用意されている
  - 日本ではまだまだ少ない
  - 電話機を外してケーブルをつなぐ
  - いなかにいくとモジュラじゃない !!
- 認証が問題
  - 発信者番号通知を使った認証が行えない
  - コールバックもできない
- 国によってモジュラコンセントの形が違う
  - いろんな形が販売されている
  - しかし、うまくいくとは限らない

Orangesoft

携帯電話

- ほとんどどこでもつながる
- 新幹線の中でも大丈夫
  - 接続は安定しないので長時間の通信には不向き
  - 切れる場所を把握しておくことが重要
    - » トンネル、長い橋、山のなか
- 通信速度が遅い
  - 9600bsp
  - デジタル通信だと安心 ？
- 発信者番号通知を利用した認証が可能

PHS

- 都市部では大体使える
  - 携帯電話の使えない所でも使える
    - » 地下鉄やビルの中
- 移動中の通信には不向き
- 通信速度は少し速い
  - 32K(29.2k)
- バッテリが長持ち
  - しかし、大事なときになくなる
  - バッテリ交換が面倒
- 発信者番号通知を利用した認証が可能

Orangesoft

メーラを考える

Orangesoft

モバイル時代のクライアント

- 多彩なクライアントが登場
  - PDA、サブノートPC、ノートPC、携帯電話、CE
- 機能が違う
  - 入力装置、表示装置、記憶装置
- 用途に合わせてクライアントを選ぶ
  - メール、メモ、住所録、電話帳、Web、FAX
- 使い分けの例
  - PalmPilot　　スケジュール、カレンダー
  - サブノートPC　メール、Web、プレゼンテーション
  - 携帯電話　　電話帳、ライト、時計
  - メモ帳　　メモ

Orangesoft

リモート環境からメールを使う

- POP(Post Office Protocol)が主流
  - サーバにログインしてメールを使う人は少ない
- 社内でもPOP、モバイルでもPOP
  - POPはメールはPCに取り込む
    - » 複数のPCで扱うのは難しい
  - サーバに残したまま取り込むこともできるが...
    - » あとの整理が大変
- 最近IMAP4に注目が集まる
  - Internet Mail Access Protocol Version 4

モバイル環境に求められる機能

- 利用者の使い方で要求は変化する
  - いつも外出している人
  - ときどき外出する人
  - ほとんどオフィスにいる人
- オフィス環境←→モバイル環境の移行が簡単
  - どちらでも同じようにメールを読みたい
- 端末が軽量でバッテリで長時間使える
  - 重いと持ち歩きたくなくなる
- 読みたいメールだけをダウンロード
  - Subjectを見て判断
  - 添付ファイルは必要なものだけ

Orangesoft

多くの人はPCを使う

- Windowsが主流
  - 95から98へ ？
  - 多くのアプリケーションがそろっている
  - ダイアルアップ接続も簡単
- メーラ
  - 多くのメーラが存在
    - » フリーなものから1万円以上するものまで多彩
  - 「まぬけ」なメーラも多いので要注意
    - » 例えば…
- アクセス方法はもっぱらPOP3かIMAP4
  - 簡単でわかりやすい

Orangesoft

POP3

- Post Office Protocol Ver.3
- 一般に広く普及している
- プロトコルが簡単
  - サーバ側で複雑な管理はできない
- メールサーバは一時的なメールのスプール
- メールの管理は全てクライアント側
  - 複数の端末の利用には不便
  - サーバにメールを残したままのユーザも多いのでは?
- メールのバックアップは各自の問題
- クライアントが壊れたときの復旧方法は?

POP3のコマンド

POP3(RFC1939)	
STAT	メールボックスのメール数とサイズの所得
LIST	ここのメールのサイズの所得
RETR	指定したメールの取出し
DELE	指定したメールの削除
NOOP	何もしない
RSET	操作の取消し
QUIT	接続の終了
TOP	指定したメッセージのヘッダと本文を指定した行数所得する
UIDL	ここのメールのサーバ内でのIDを所得する
USER	ユーザ認証時のユーザ名の送信
PASS	ユーザ認証
APOP	で暗号化されたユーザ認証

POP3でのメールの取得

```
+OK POP3 beer.orangesoft.co.jp v5.49 server ready
USER kitarou
+OK User name accepted, password please
PASS nazonazo
+OK Mailbox open, 1230 messages
RTET 1
+OK 3360 octets

メール本文

.
DELE 1230
+OK Message deleted
QUIT
+OK Sayonara
```

Orangesoft

IMAP4

- Internet Mail Access Protocol Ver.4
- 採用しているベンダが増加中
  - サーバ製品
    - » SunMicrosystems, Netscape, Microsoft, Lotus, NEC
  - クライアント製品
    - » Netscape, OutlookExpress, Eudora, WeMail, Winbiff
- メールの管理はサーバ側
  - 未読/既読の管理
  - フォルダの管理
  - メールの保存は基本的にサーバ側
- 各自のメールのバックアップはサーバで

Orangesoft

IMAP4(cont'd)

- 複数の端末から同じようにメールが読める
  - 自席のデスクトップと外出先のノートPC
- 多彩なメール取得手段
- クライアントの実装次第
  - ヘッダ(From:, Subject等)を指定して取得できる
  - MIMEのパート単位の取得
- 必要なメールだけダウンロード
  - Subjectをみて選べる
  - メモリが少ないマシンでも使える
    - » PDAやインターネットTVなど

IMAP4rev1のコマンド

IMAP4(RFC2060)	
CAPABILITY	サーバのIMAP4のバージョンや認証機能等のサーバの機能の所得
NOOP	何もしない
LOGOUT	接続の終了
AUTHENTICATE	LOGIN以外の認証方式によるユーザ認証
LOGIN	サーバへのLOGIN
SELECT	メールボックスの選択(メールボックスのオープン)
EXAMINE	読み込み専用でメールボックスを選択(メールボックスのオープン)
CREATE	メールボックスの作成
DELETE	メールボックスの削除
RENAME	メールボックスのリネーム
SUBSCRIBE	ニュースグループの購読
UNSUBSCRIBE	ニュースグループの購読中止
LIST	メールボックスリストの所得
LSUB	指定したニュースグループの階層のリストの所得
STATUS	指定したメールボックスのメール数とUIDの所得
APPEND	指定したメールボックスへのメッセージの書き込み
CHECK	SELECTしたメールボックスの新着チェック
CLOSE	SELECTしたメールボックスのクローズ
EXPUNGE	DELETEフラグがセットされたメッセージの削除
SEARCH	メッセージの検索
FETCH	メッセージ、フラグ等の取出し
STORE	メッセージへのフラグのセット
COPY	メッセージのコピー
UID	UIDを指定してコマンドの実行

IMAP4でのメールの取得(1)

```
* OK beer.orangesoft.co.jp IMAP4rev1 v11.241 server ready
A1 LOGIN kitarou nazonazo
A1 OK LOGIN completed
A2 SELECT INBOX
* 1229 EXISTS
* 10 RECENT

 省略

A2 OK [READ-WRITE] SELECT completed
A3 FETCH 1235 BODYSTRUCTURE
* 1235 FETCH (BODYSTRUCTURE (("TEXT" "PLAIN" ("CHARSET" "iso-2022-jp") NIL NIL "
7BIT" 113 10 NIL NIL NIL)("APPLICATION" "X-PKCS7-SIGNATURE" ("NAME" "smime.p7s")
 NIL NIL "BASE64" 3630 NIL ("ATTACHMENT" ("FILENAME" "smime.p7s")) NIL) "SIGNED"
 ("PROTOCOL" "application/x-pkcs7-signature" "MICALG" "rsa-sha1" "BOUNDARY" "---
------911557871-23039209") NIL NIL))
* 1236 EXISTS
* 2 RECENT
A3 OK FETCH completed
```

Orangesoft

IMAP4でのメールの取得(2)

```
A4 FETCH 1235 BODY[HEADER.FIELDS (DATE FROM SUBJECT)]
* 1235 FETCH (BODY[HEADER.FIELDS ("DATE" "FROM" "SUBJECT")] {144}
Subject: =?ISO-2022-JP?B?GyRCJDMkcyRLJEEkTxsoQg==?=
From: Watanabe Naoaki <kitarou@orangesoft.co.jp>
Date: Fri, 20 Nov 1998 19:31:12 +0900

)
* 1240 EXISTS
* 6 RECENT
A4 OK FETCH completed
A4 FETCH 1235 BODY[1]
* 1235 FETCH (BODY[1] {113}
 これは、テストです。

 省略
)
* 1241 EXISTS
* 7 RECENT
A4 OK FETCH completed
```

Orangesoft

それぞれのメリット

- POP3
  - 接続すれば全てのメールがクライアントに届く
  - 全部が自分のマシンで管理できる
- IMAP4
  - 必要なメールを自分で選択してダウンロードできる
  - 通信時間が見積もれる
  - 自分のマシンが壊れてもメールは安心
  - 過去のメールも参照できる
  - ネットワークのトラフィックの軽減

それぞれのデメリット

- POP3
  - 通信時間がわからない
    - » どれだけメールがあるか事前にわからない
  - 自分のPCが壊れると保存してあるメールが消滅
    - » バックアップは自分の責任
  - 別のマシンに保存してあるメールは読み出せない
- IMAP4
  - サーバにそれなりのディスクが必要
  - サーバソフトの選択に注意が必要
    - » サーバのバグやクライアントとの互換性
  - サーバ側でバックアップが必要
  - サーバが停まると過去のメールも読めない

IMAP4は膨大な資源が必要 ？

- 一人当り1日50通、1通のサイズ平均50KBとして
  - 10人で1日500通の場合
    - » 500通*10Kとして5000K/日*365日で約1.82GB
  - 1,000人で1日50,000通での運用
    - » 50,000通*10Kとして500MB/日 * 365日で約182.5GB
  - kumaが保存しているメールは300M(毎日増えている)
    - » kumaが1000人いると300G !!
- メールをサーバ側で検索すると
  - メールサーバに負荷がかかる
  - みんなが検索すると巨大な負荷に
- (SPARC167MHz*2,1G,400G)/1000人という例も

Orangesoft

今後の主流はIMAP4か ？

- ハードウェアは安くなる
  - どんどん買い足せばいい !?
    - » 安くなっても機器が増えれば管理工数が増える
  - 300Gのディスクをどのようにバックアップするの ？
- IMAP4対応のサーバ製品は増えてきている
  - 検索機能等の高速化がサーバ製品の勝負どころ
  - 管理のしやすさも重要
- IMAP4対応のメーラも増えてきている
  - サーバとメーラの互換性は大丈夫 ？
- IMAP4でもPOP3と同じような使い方もできる
  - クライアントに依存する

Orangesoft

IMAP4サーバの選び方

- カタログや比較表の ○ の数はあてにならない
  - 陥りやすい過ち
  - 本当に必要なのは安定性
- 価格にだまされてはいけない
  - 高価だからいいとは限らない
    - » フリーだからいいとも限らない
- 操作画面の日本語化にだまされてはいけない
  - 本当の日本語化はサーバのSEARCH機能など
- どれだけのクライアントと接続実績があるか
  - クライアントのバージョンも重要
    - » バージョンが上がるとコマンドの使い方が変わることも

Orangesoft

暗号電子メール

Orangesoft

iSiD

電子メールの弱点

- インターネットは盗聴可能
  - 電子メールも盗聴(盗み読み)される危険がある
  - 重要な内容は送れない
- 受け取った電子メールは本物 ？
  - 相手を確認する手段がない
  - こちらが本物であることも証明できない ？
  - 内容を書き換えても分からない
- そこでS/MIMEが登場
  - Secure/Multipurpose Internet Mail Extensions
  - 電文を暗号化し目的の相手以外には読めないように
  - 電子署名で発信人を特定し改ざんを発見

暗号メールは必要なのか

- インターネットは盗聴されているのか ？
  - 盗聴は行われている(社内LANはもっと深刻)
  - 盗聴されたかどうかを確認する手段はない
  - あなたのメールは盗聴されても大丈夫か ？
- メールを暗号化して送っている人は ？
  - あまり見かけない :-(
  - 適当なツールがない
  - いちいち暗号化するのが面倒
  - 相手も暗号化メーラを使っている必要がある
- PGPとS/MIME
  - 一部のメーラがサポートを始めた

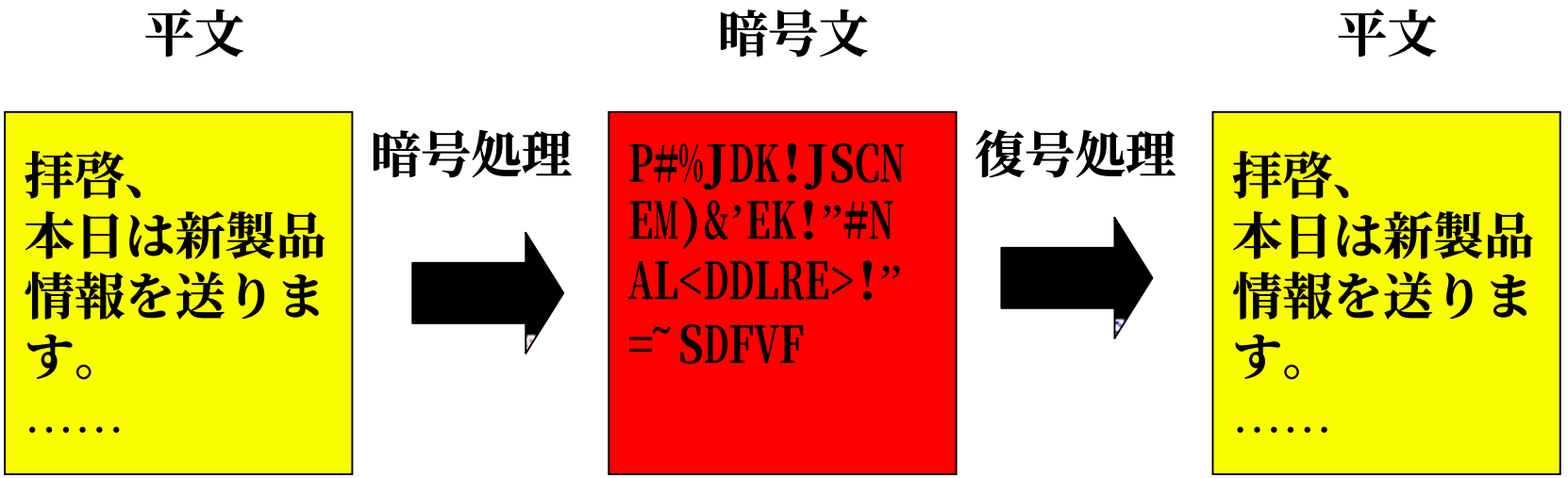
Orangesoft

暗号メールの基本

- なぜ、電子メールに暗号が必要か
  - 理由は明確
  - 暗号で解決できるのか ？
- Firewallでは守れないのか?
  - 電子メールはFirewallを通過してやってくる
  - SMTP、POP、IMAP4はFirewallを通過して通信する
- 暗号化すれば安全か
  - 暗号は破られないのか ？
- 自分が出したメールでないことを証明する
  - 他人が自分のアドレスを勝手に使用

Orangesoft

暗号を使うと…


平文
暗号文
平文
拝啓、
本日は新製品
情報を送りま
す。
……
暗号処理
P#%JDK!JSCN
EM)&'EK!"#N
AL<DDLRE>!"
=~SDFVF
復号処理
拝啓、
本日は新製品
情報を送りま
す。
……

重要な暗号技術

- 暗号の利用方法
  - インターネットは相手が見えない — 認証
  - インターネットはほかから丸見え — 暗号
  - インターネットには悪人もいる — 改ざん発見
- すべて暗号技術で解決できる(はず)
  - 米国の技術が中心
  - 公開鍵暗号方式(RSA、Diffie-Hellman)
  - 共有鍵暗号方式(DES、RC-2、RC-4)
  - メッセージ・ダイジェスト(MD5、SHA-1)
- 応用範囲の広い暗号技術
  - 携帯電話、スマートカード、認証など

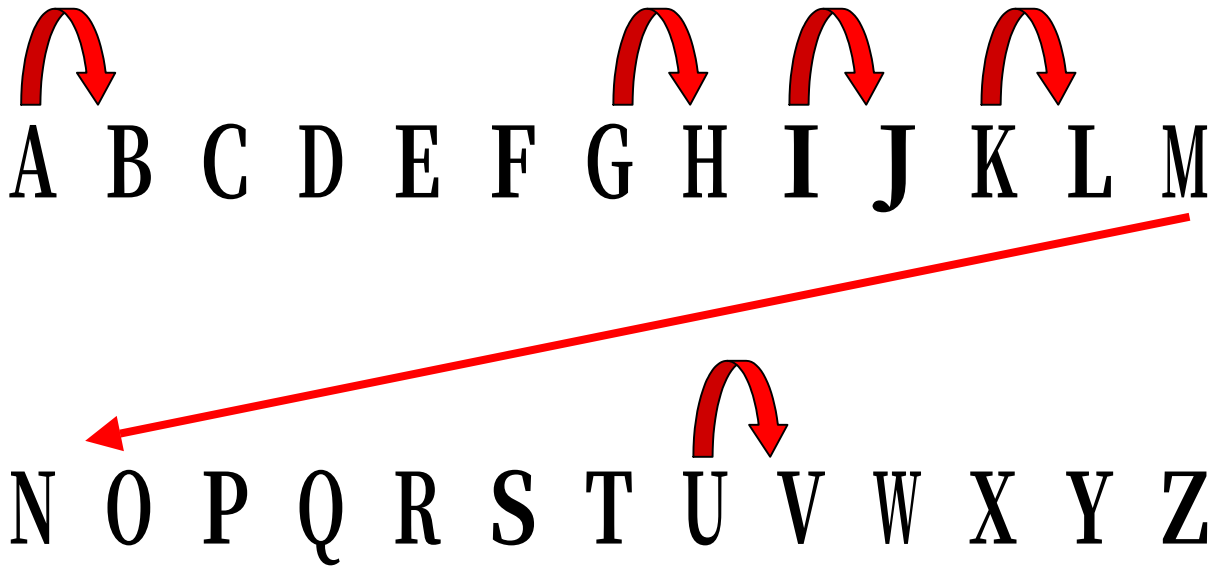
重要な暗号技術(cont'd)

- 暗号は強度が問題
  - 強度が弱いと簡単に解読できる
  - 強い暗号には米国が輸出規制
- 公開鍵暗号方式
  - 公開鍵(Public Key)と秘密鍵(Private Key)のペア
  - 公開鍵をみんなに公開、秘密鍵は誰にも教えない
  - 公開鍵で暗号化 → 秘密鍵でのみ復号可能
  - 秘密鍵で暗号化 → 公開鍵でのみ復号可能
- 認証局
  - 公開鍵が本物であることを証明する組織
  - 現在は民間企業が運営

輸出規制問題

- アメリカの輸出規制
  - 暗号は軍事物資
  - 輸入して使用することに関して制限はない
  - 用途などによって鍵長の制限がある
    - » DES 56bit,RC2 40bit などなど
- 日本の輸出規制
  - 輸入して使用することに関して制限はない
  - 暗号製品の輸出は個別審査
    - » 明確な規定がない ？
    - » 審査を避けたい通産省 ？
  - テロ・麻薬取引などに利用されると困る
  - 国外持ち出しには許可が必要という話も ？

アルファベット表を使う暗号



K → L、U → V、M → N、A → B
G → H、A → B、I → J

Orangesoft

アルファベットを置き換えると

平文（くまがいです）

KUMAGAIDESU

暗号処理

アルファベット表で
5文字右の文字

PZRFLFNIJXZ

暗号文

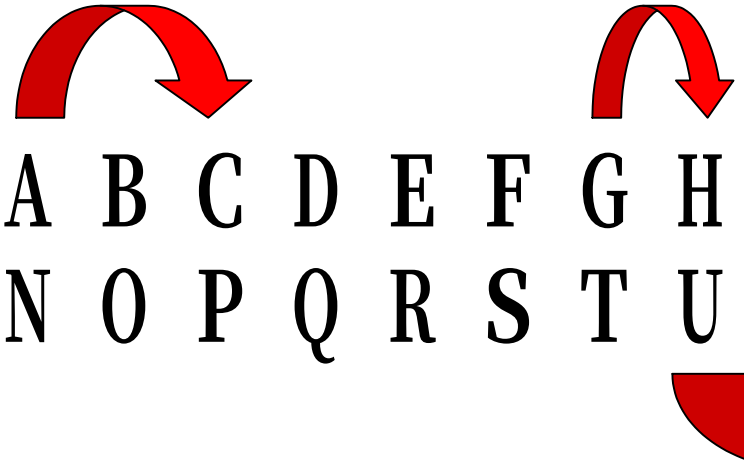
復号処理

アルファベット表で
5文字左の文字

平文（くまがいです）

KUMAGAIDESU

アルファベット表 + 乱数表



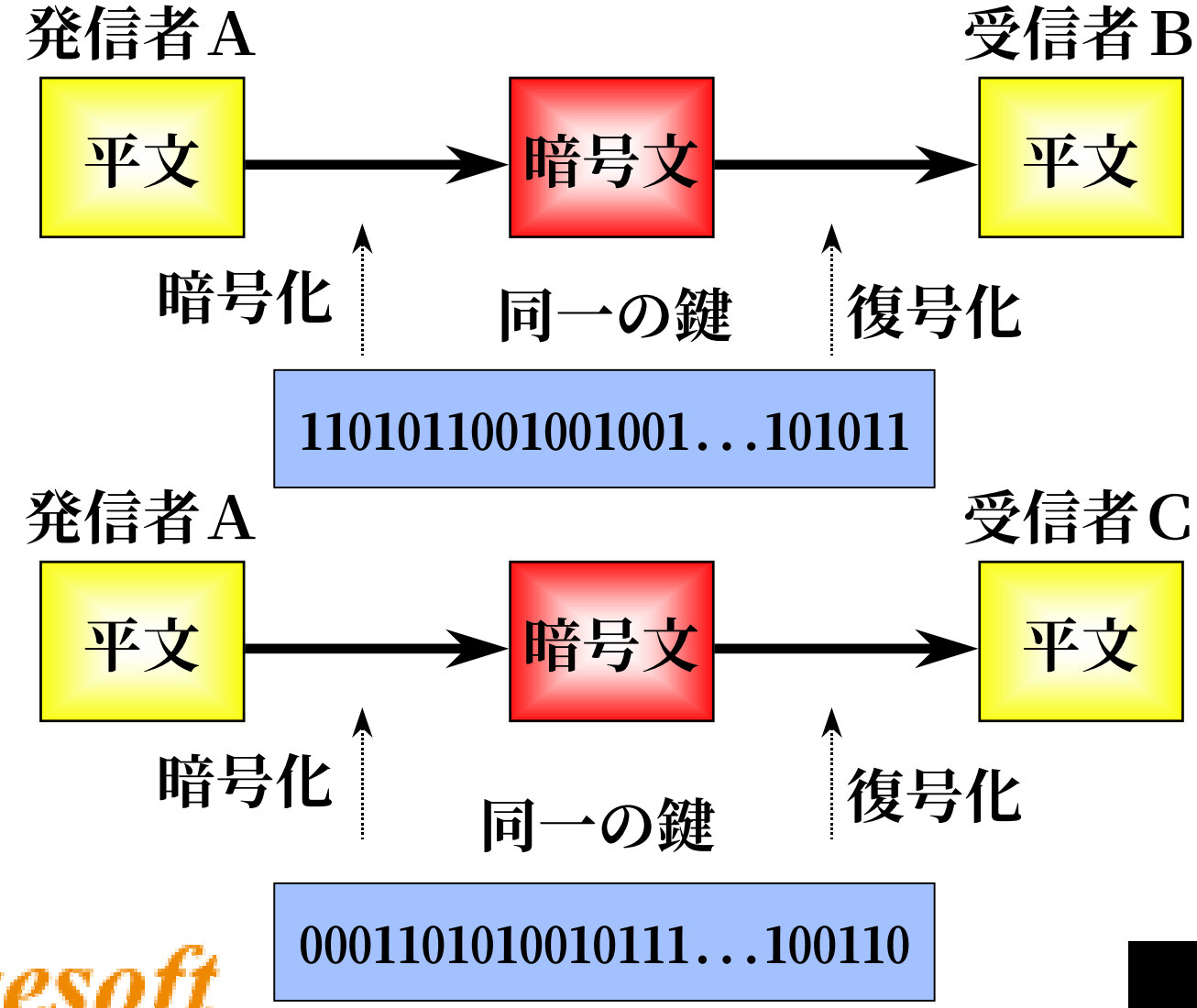
平文	K	U	M	A	G	A	I	D	E	S	U
乱数	0	3	5	2	1	0	8	6	4	2	0
暗号文	K	X	R	C	H	A	Q	J	I	U	U

Orangesoft

共有鍵暗号方式

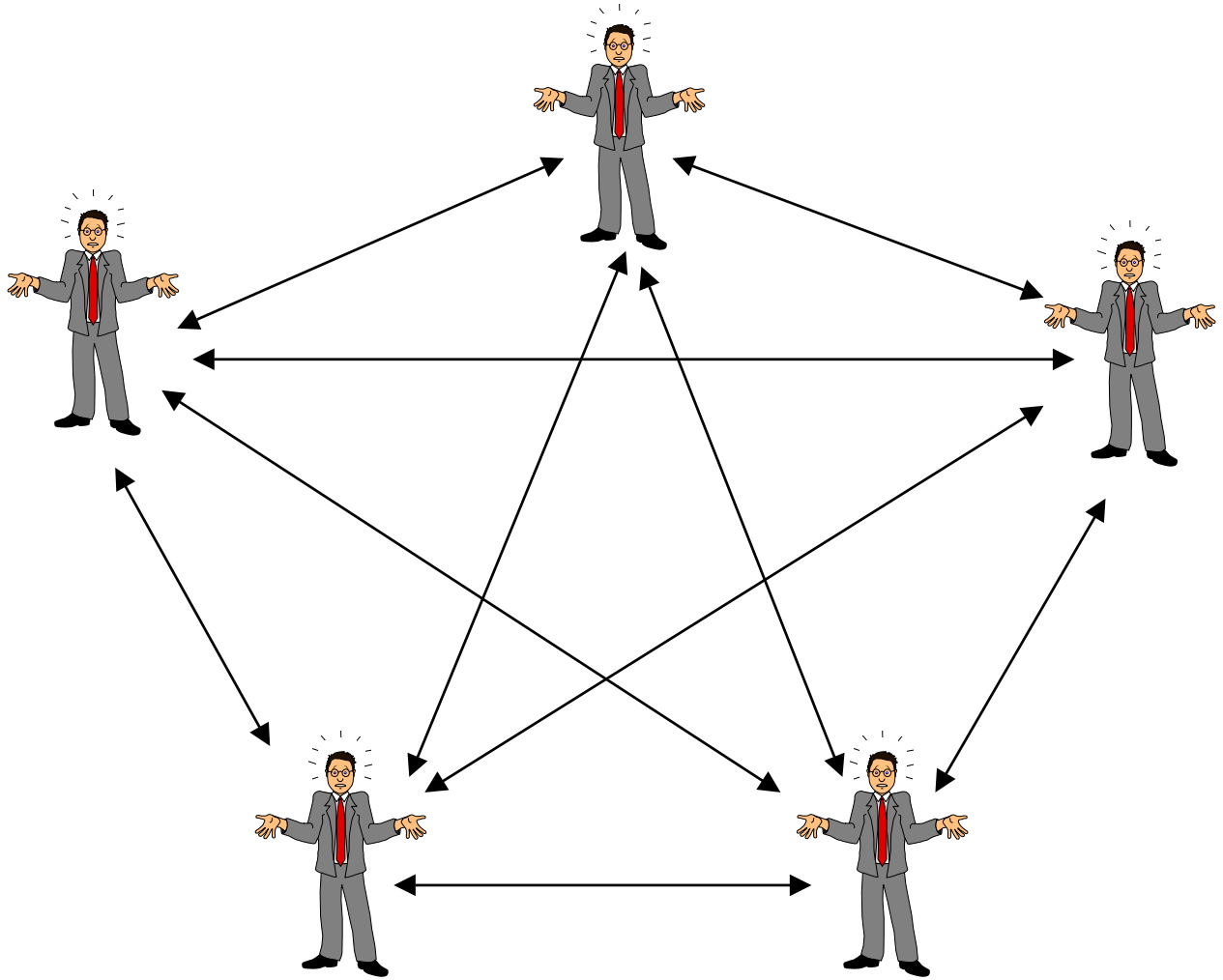
- 送信者と受信者は暗号、復号に同じ鍵を使う
  - 同じ鍵を共有するから「共有鍵暗号」
- 送信者と受信者の間での鍵の受け渡しが問題
  - 定期的に鍵は交換したい
    - » 通信ごとに変える方が安全
  - 安全な鍵交換の方法
    - » メールで送ると盗聴される
    - » 鍵が盗まれては意味がない
  - 複数人に鍵を配布するのが面倒
    - » 相手ごとに違う鍵が必要
- 処理速度は速い

共有鍵暗号は同一の鍵を使う



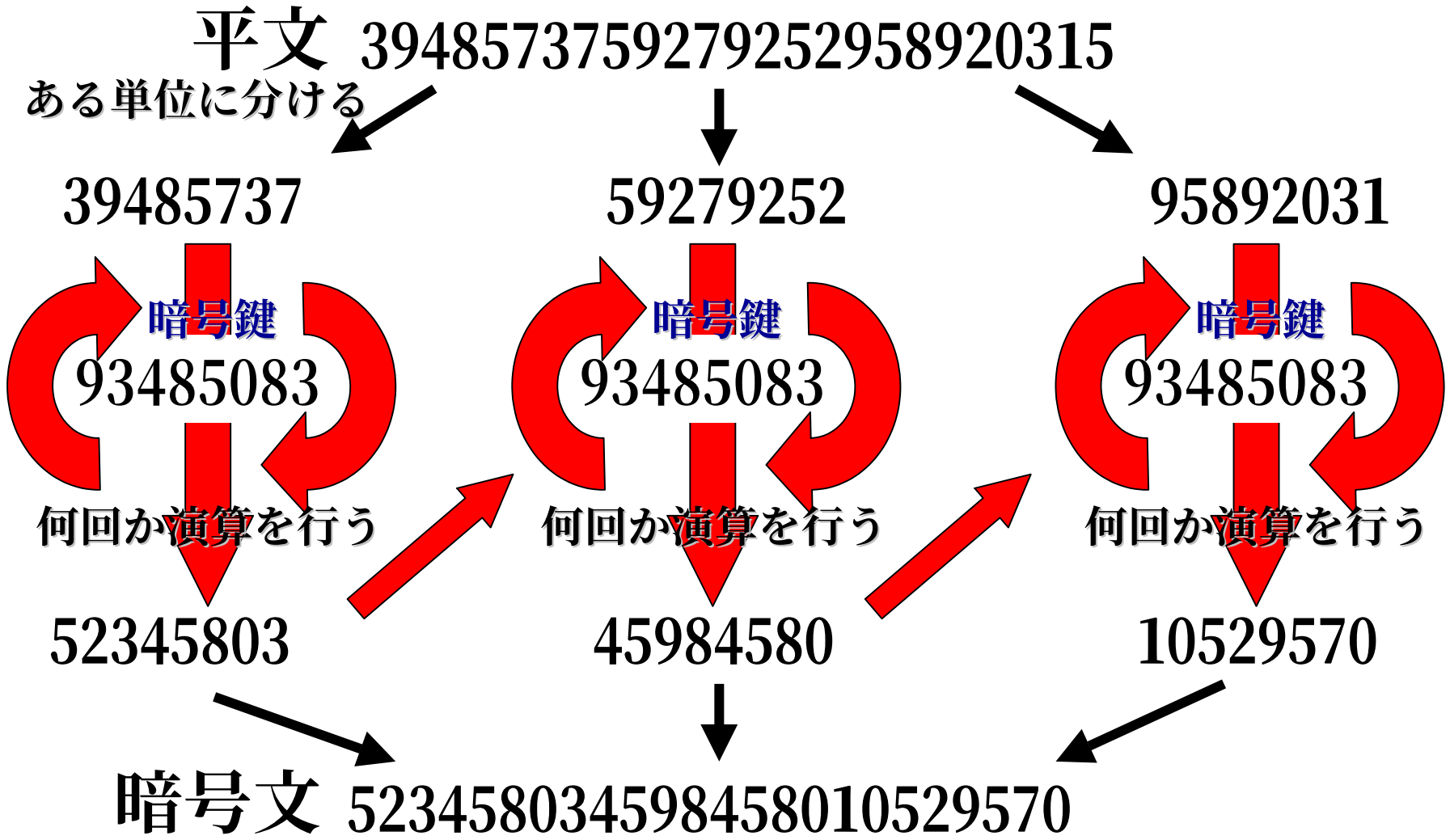
Orangesoft

4人の相手と共有鍵を使う



Orangesoft

暗号処理の例



Orangesoft

[redacted]

暗号鍵の長さと鍵の組み合わせ

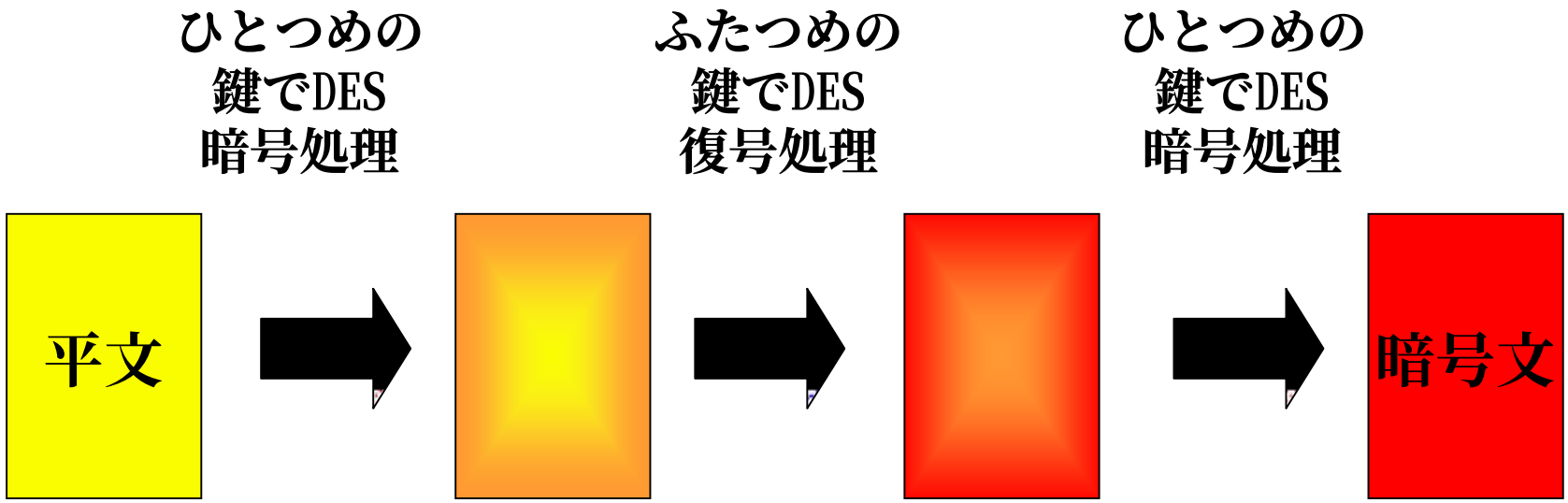
40ビット	1,099,511,627,776
56ビット	72,057,594,037,930,000
64ビット	18,446,744,073,710,000,000
128ビット	340,282,366,920,900,000,000,000,000,000,000,000,000

(有効数字13桁)

Orangesoft

iSiD

Triple DESの暗号化手順



ふたつの秘密暗号鍵で合計で3回のDES暗号化処理を行う

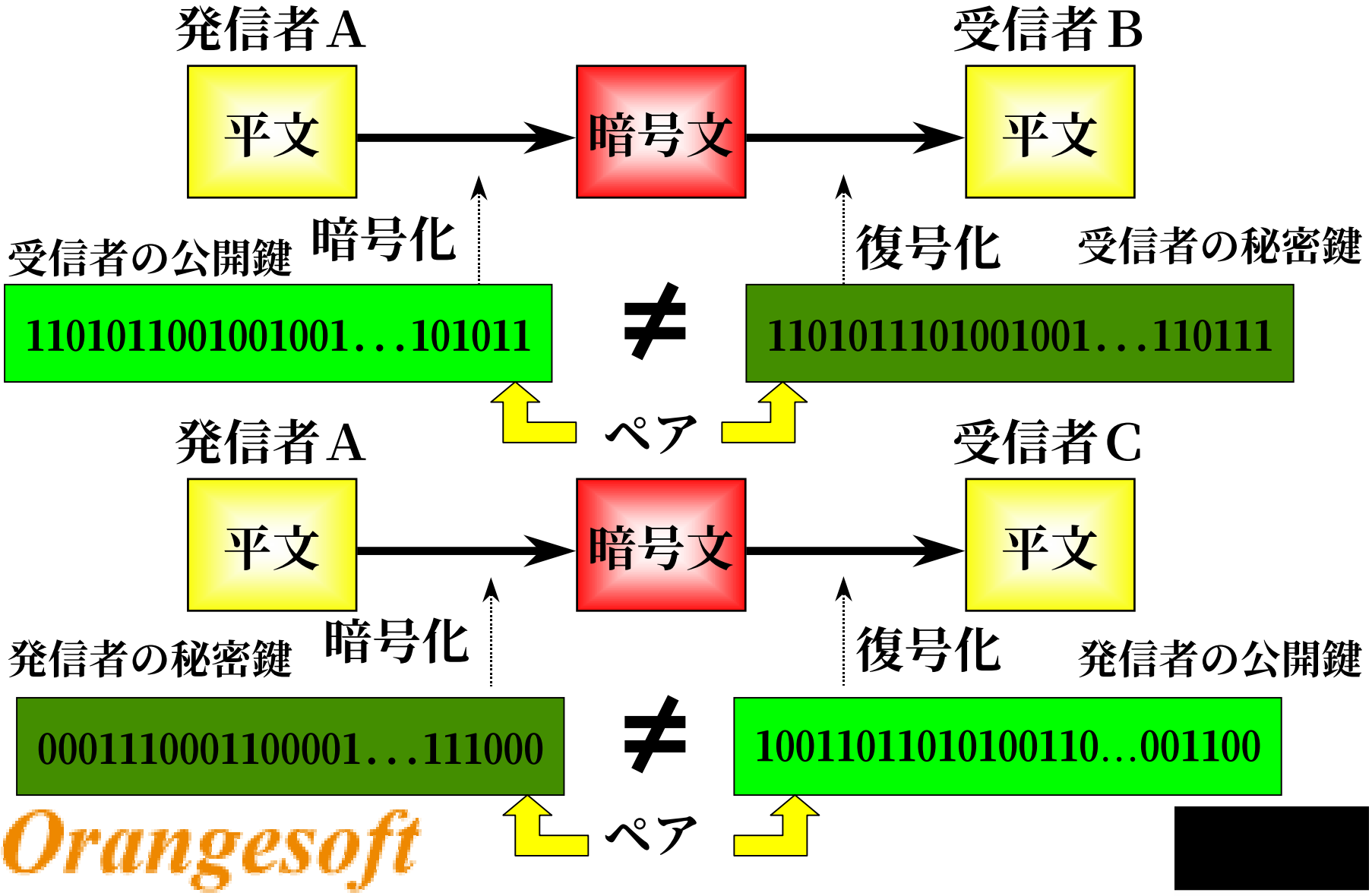
Orangesoft

公開鍵暗号方式

- 暗号化鍵と復号化鍵が異なる
  - ふたつの鍵がペアになっている
  - 片方を公開(公開鍵)し、片方を秘密(秘密鍵)に
- 公開鍵から秘密鍵を求めるのが困難
  - 復号化鍵(公開鍵)は誰にでも配布できる
  - 公開鍵を安全(確実)に相手に渡す
    - » 公開鍵のすり替えに注意
- 処理速度は遅い
  - メッセージ全体の暗号には不向き
  - 共有鍵暗号の鍵を暗号化する

Orangesoft

公開鍵暗号方式はペア鍵を使う



Orangesoft

暗号の強度

- 共有鍵暗号方式
  - ４０ｂｉｔ　ｖｓ　１２８ｂｉｔ
  - 鍵の組合わせ
    - » 10^{12}　ｖｓ　10^{38}
  - 解読時間（1995年に100万ドルのコンピュータで）
    - » ３３分　ｖｓ　10^{22}年
- 公開鍵暗号方式
  - ５１２ｂｉｔ　ｖｓ　１０２４ｂｉｔ
  - ｂｉｔ数と桁数
    - » １５４桁　ｖｓ　３０８桁
  - 素因数分解に要するコスト(1995年現在)
    - » 10^{7}ドル　ｖｓ　10^{15}ドル

Certification Authority

- 認証機構
  - 認証を業務とする組織
  - 公的機関が存在を保証
- 他人を信用するためには…
  - 市役所で印鑑証明をもらう(個人)
  - 法務局で印鑑証明をもらう(法人)
  - 信用できる誰かに保証人になってもらう
  - 誰も信用しない
- ところで…
  - 誰が誰に何を認証するのか ？
  - インターネットの世界でどうする ？

Orangesoft

どのような認証があるのか

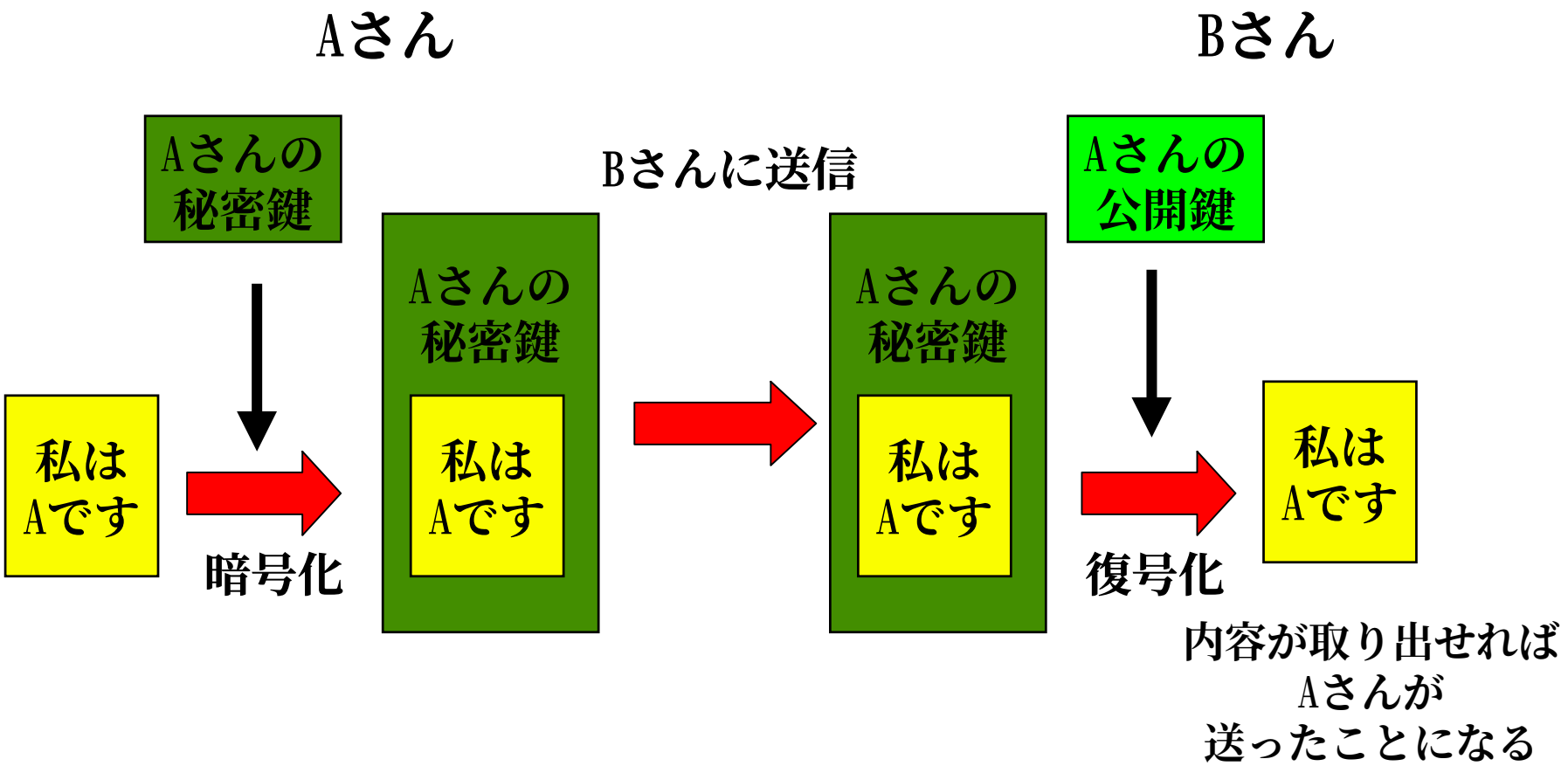
- クレジットカード
  - 個人ではなくカードそのものを認証
  - カード会社が保証
- 個人・企業
  - 私設の認証機関(たとえばVeriSign)
  - 認証してくれるだけでそれ以上でも以下でもない
  - 私設の機関をどこまで信じるのか
- どのような形が望ましいのか
  - やはり公的機関
    - » 市役所や法務局
  - 私設を使うなら範囲も限られる

暗号化メールと個人認証

- 暗号化メールには本人確認が必須
  - 誰が証明してくれるのか
    - » 特定の企業、地方自治体、ボランティア組織
  - その証明書は何を証明できるのか
- CA(Certification Authority)
  - 証明書発行機関
  - メーラごとに証明書が必要 ？
- 公開鍵暗号方式を使う
  - メールの暗号鍵を相手の公開鍵で暗号化
  - みずからの個人鍵でメールに署名

Orangesoft

電子署名の使い方



Orangesoft

盗聴

- 盗聴はどこででも起こる
  - インターネット上での盗聴
  - 社内LANでの盗聴
  - PC上のファイル
- 電文を暗号化すればよい
  - 送った相手は復号化する
  - 暗号鍵の受け渡しが必要

なりすまし

- 他人の名前を使用する
  - Fromは自由に設定できる
  - 悪意を持ってメールを出す
- 他人のアドレスをFromに設定してメールを出す
  - 受取った人は確認の手段がない
  - SMTPには認証がない
- 本当に自分が出した証明が必要
  - 全てのメールに電子署名を行う
  - やばいメールには署名しない :-)
    - » こんなのありですか ?

改ざん

- 電子メールの内容を変更する
  - そんなことができるんですか ？
  - できます !!
- どこで変更されるか ？
  - メールを出したときのSMTPサーバ
    - » 誰が管理してるかわからない
  - 経由するSMTPサーバ
    - » 不正にメールを横取りされる場合もある
  - 自社のメールサーバ
    - » 管理者の権限は絶大
  - 取込んだ後の自分のパソコン

Orangesoft

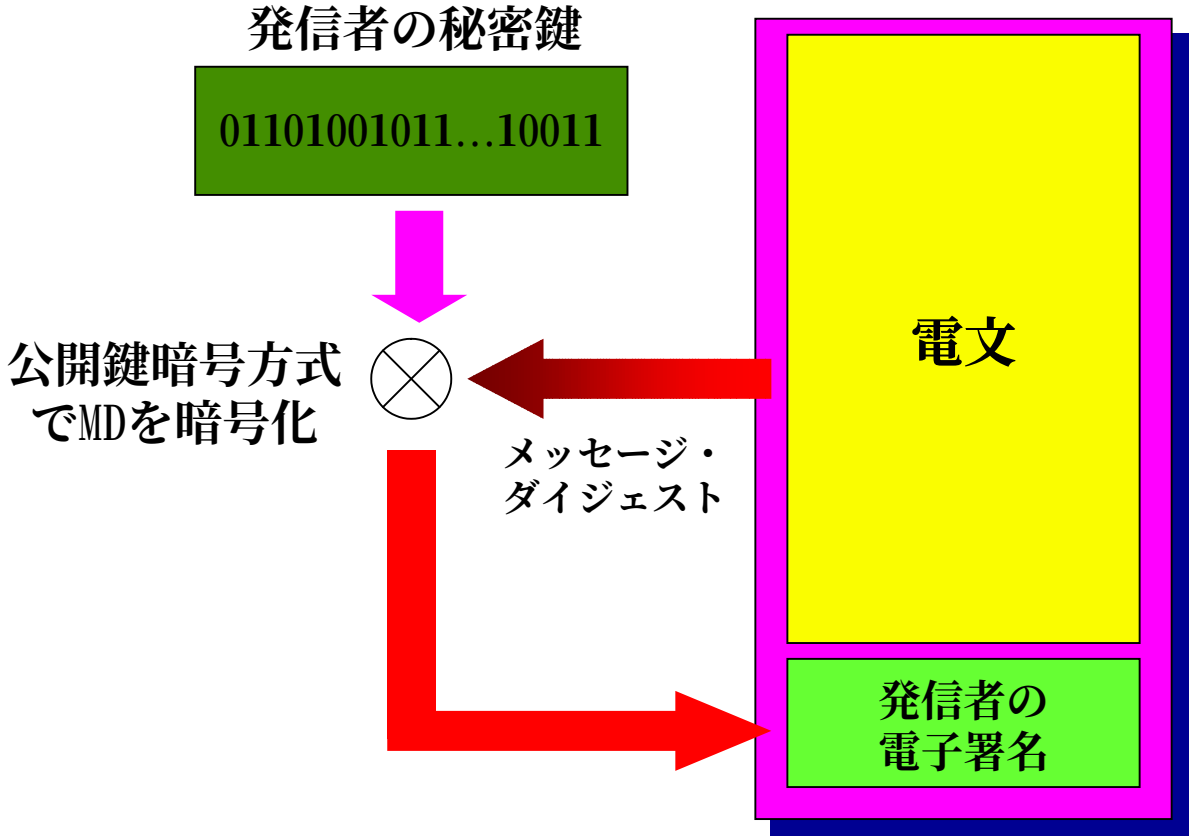
ユーザ認証

- わたしは「くまがい」です
- わたしは「きたろう」ではありません
- 何を根拠に信頼するのか？
  - 免許証
  - パスポート
  - 指紋
- 本物であることを知るしくみが重要
  - 信頼のおける人に保証してもらう
  - 信頼のおける組織に保証してもらう
  - 印籠を持っていることを確認する

暗号メールで使用される暗号

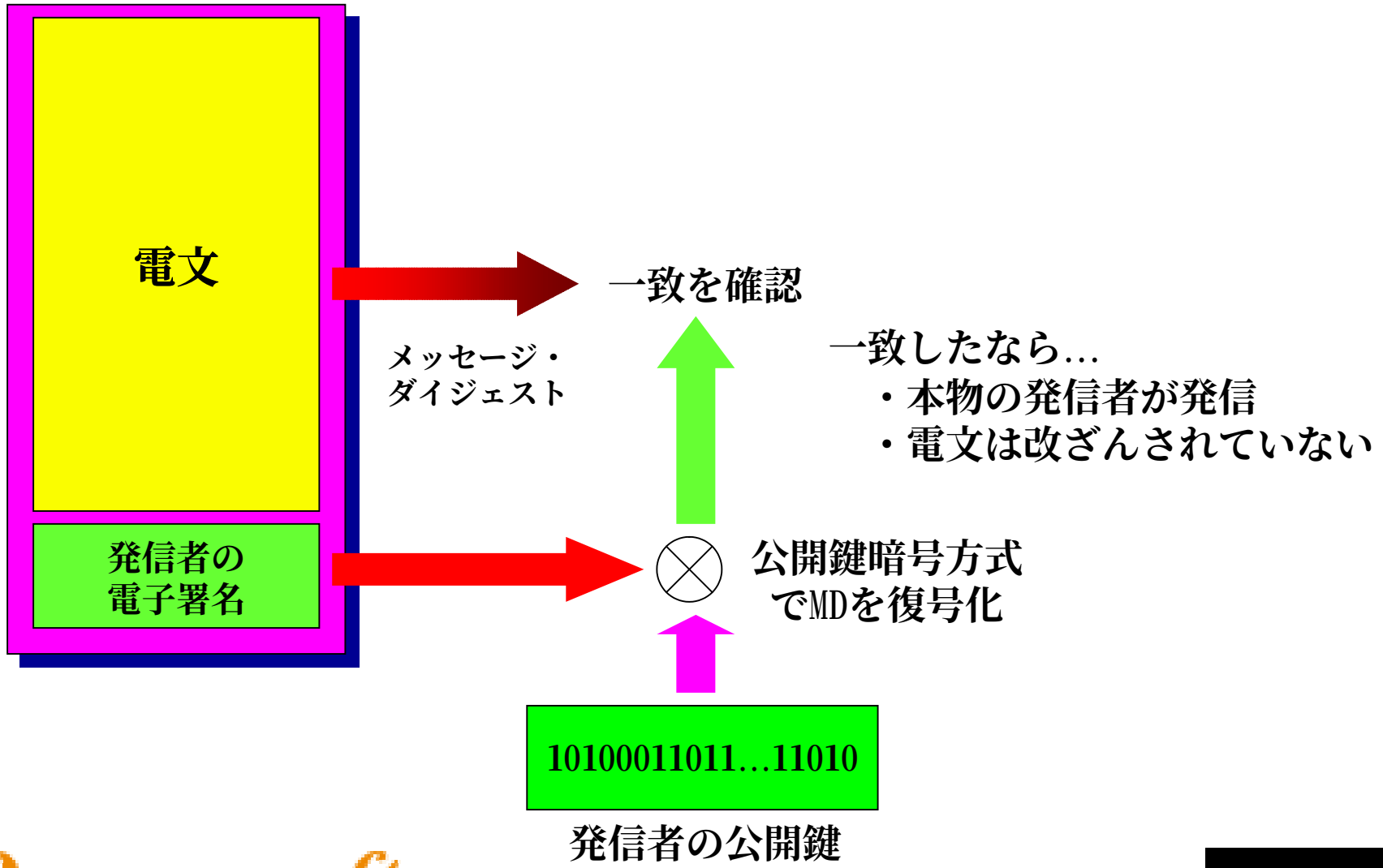
- 共通鍵でメッセージを暗号化
  - 共有鍵暗号方式
    - » DES,3DES,ISEA,RC2,MISTY,FEAL,CAST
- 公開鍵暗号方式で共通鍵を暗号化
  - 公開鍵暗号方式
    - » RSA,Diffie-Hellman,ElGamal
- ハッシュ関数
  - メッセージダイジェストを作成する
  - SHA-1,MD5

電子署名で改ざんを防ぐ



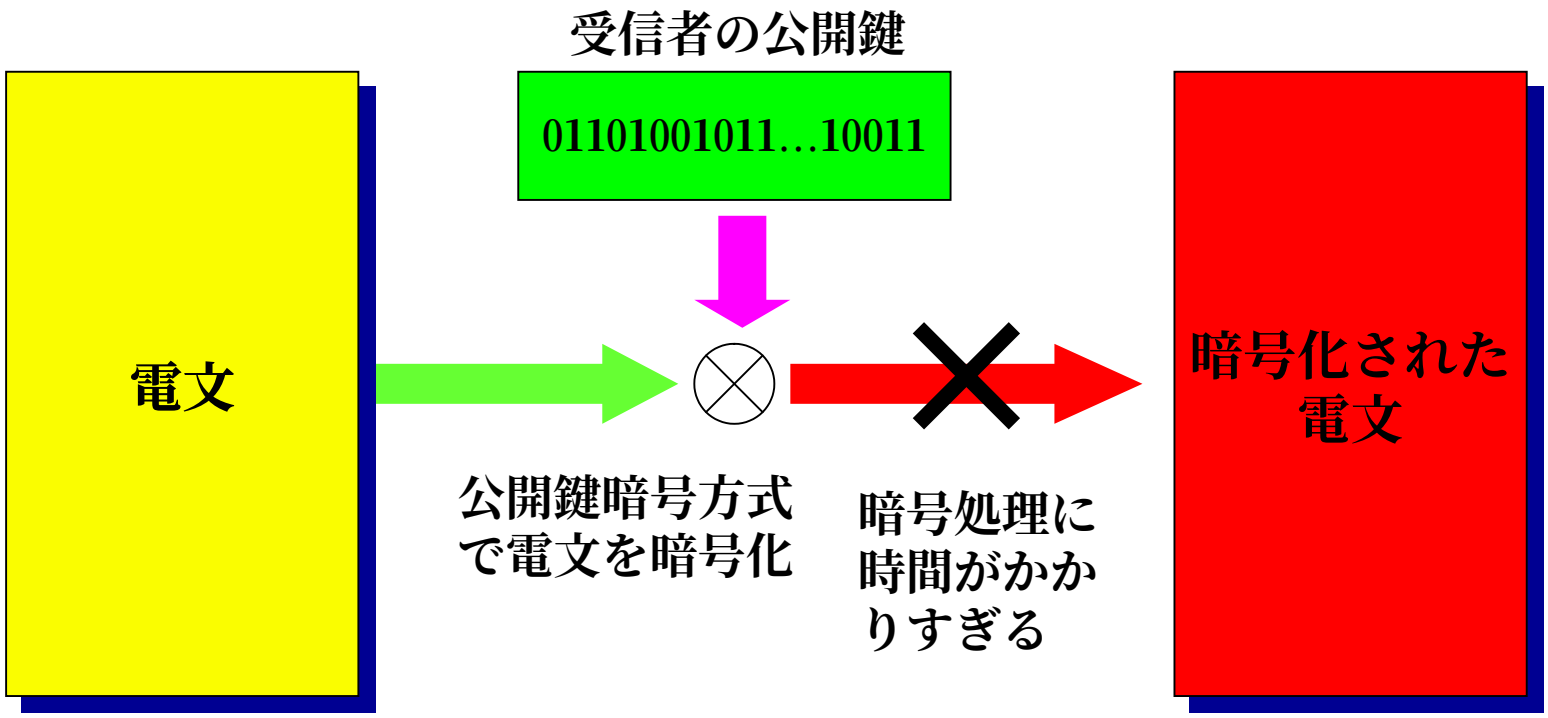
Orangesoft

電子署名で改ざんを確認する



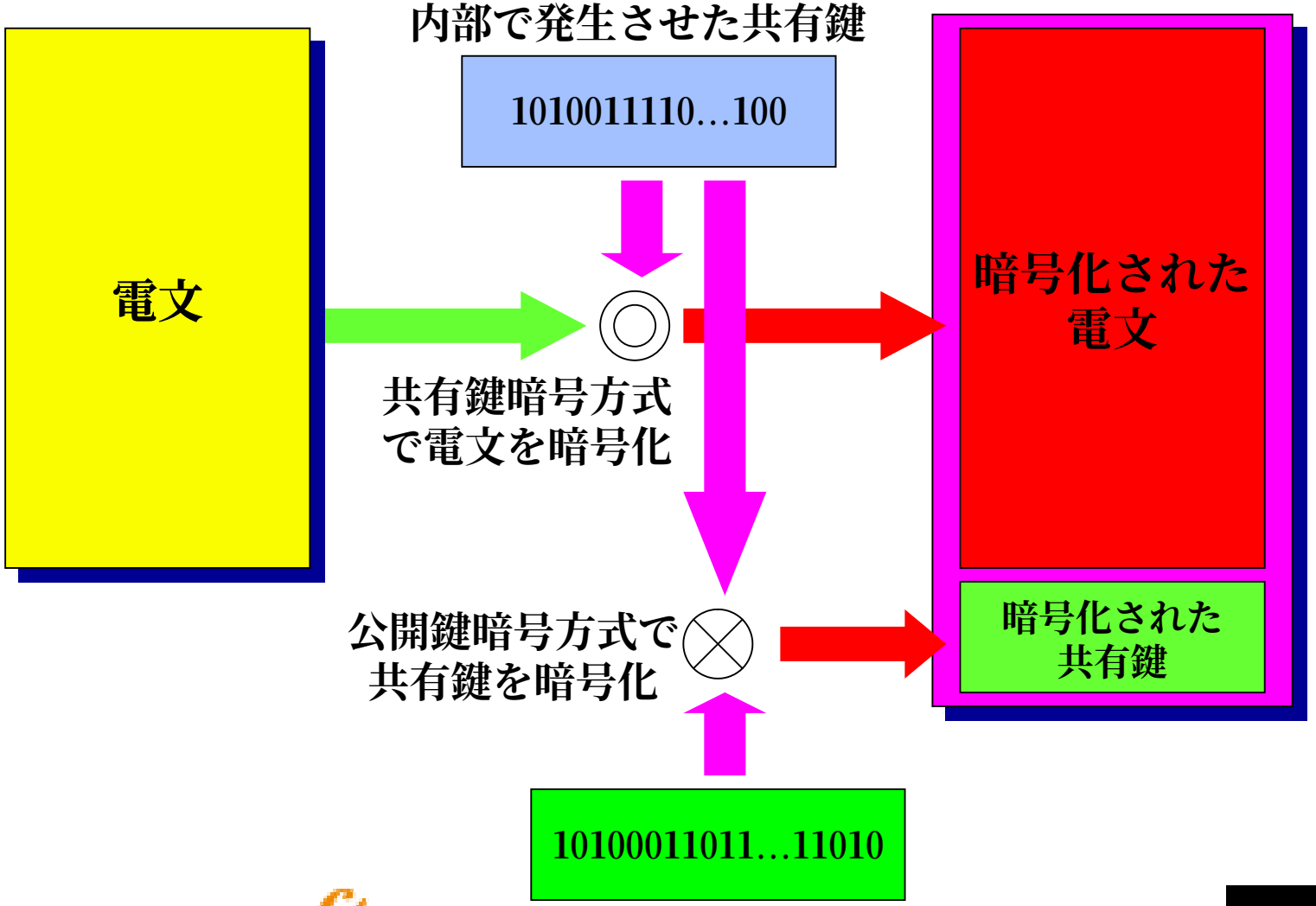
Orangesoft

電文の暗号化に公開鍵暗号方式は不向き



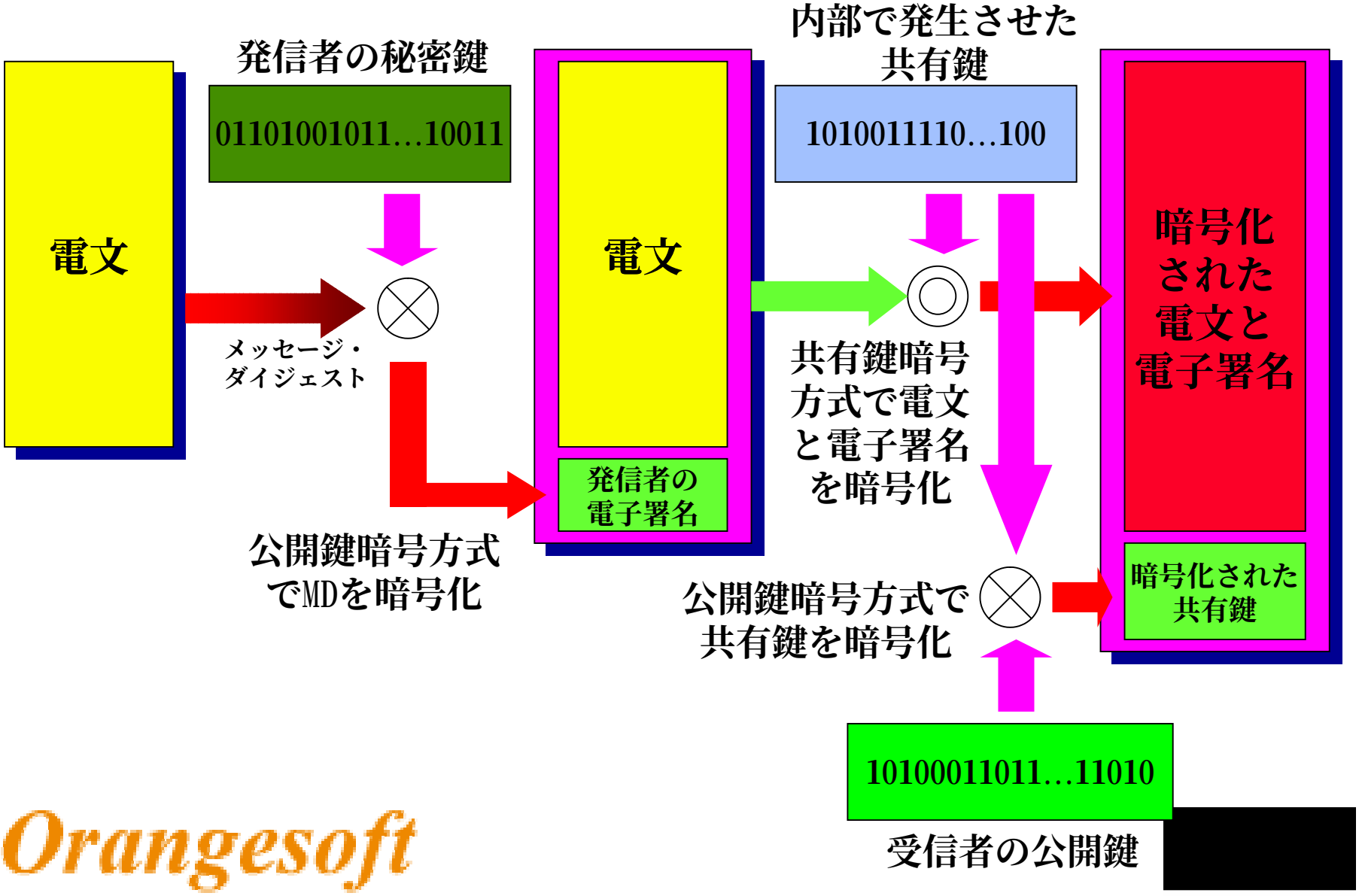
Orangesoft

共有鍵を受信者の公開鍵で暗号化



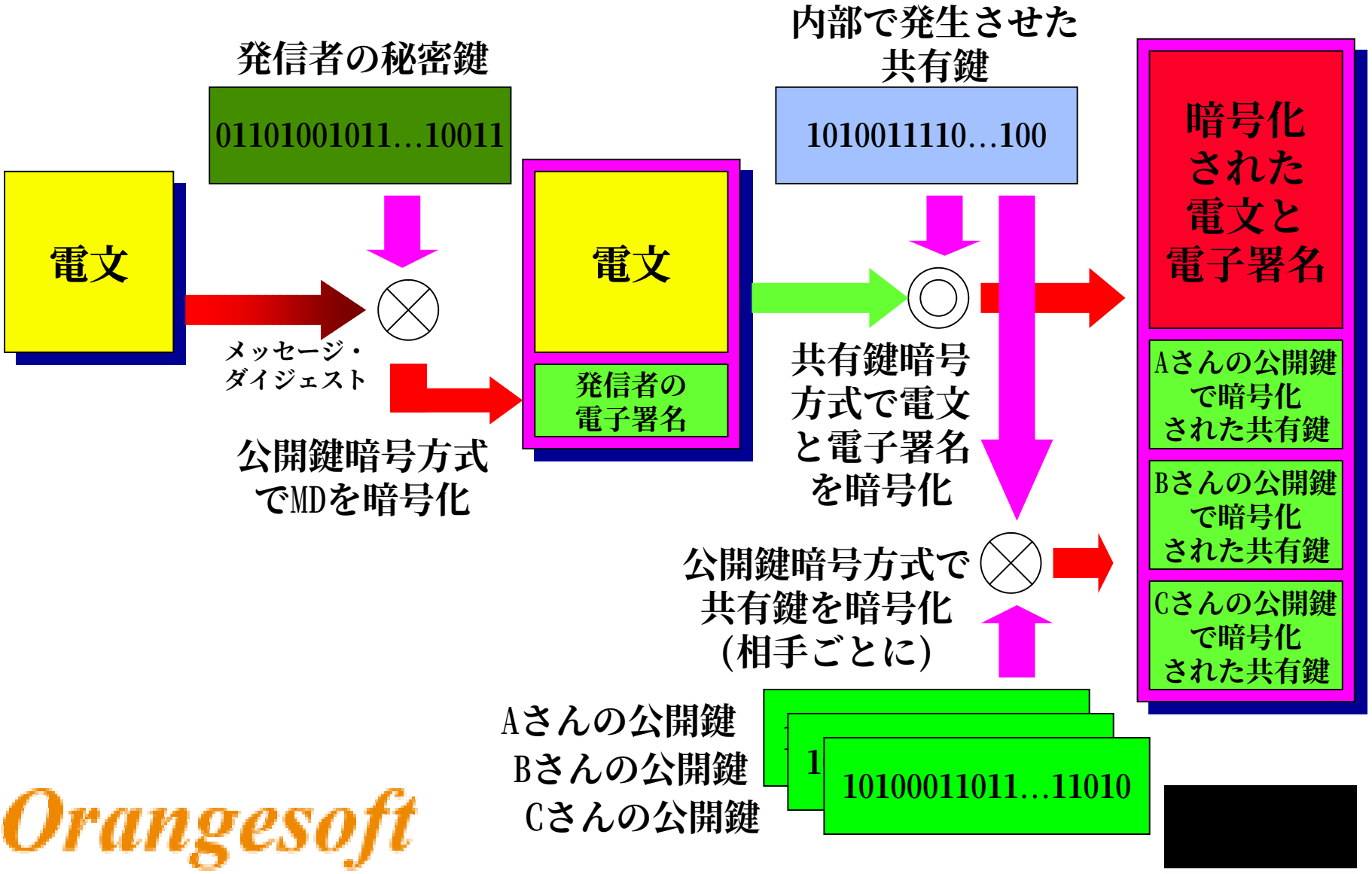
Orangesoft

電子署名と暗号の組み合わせ



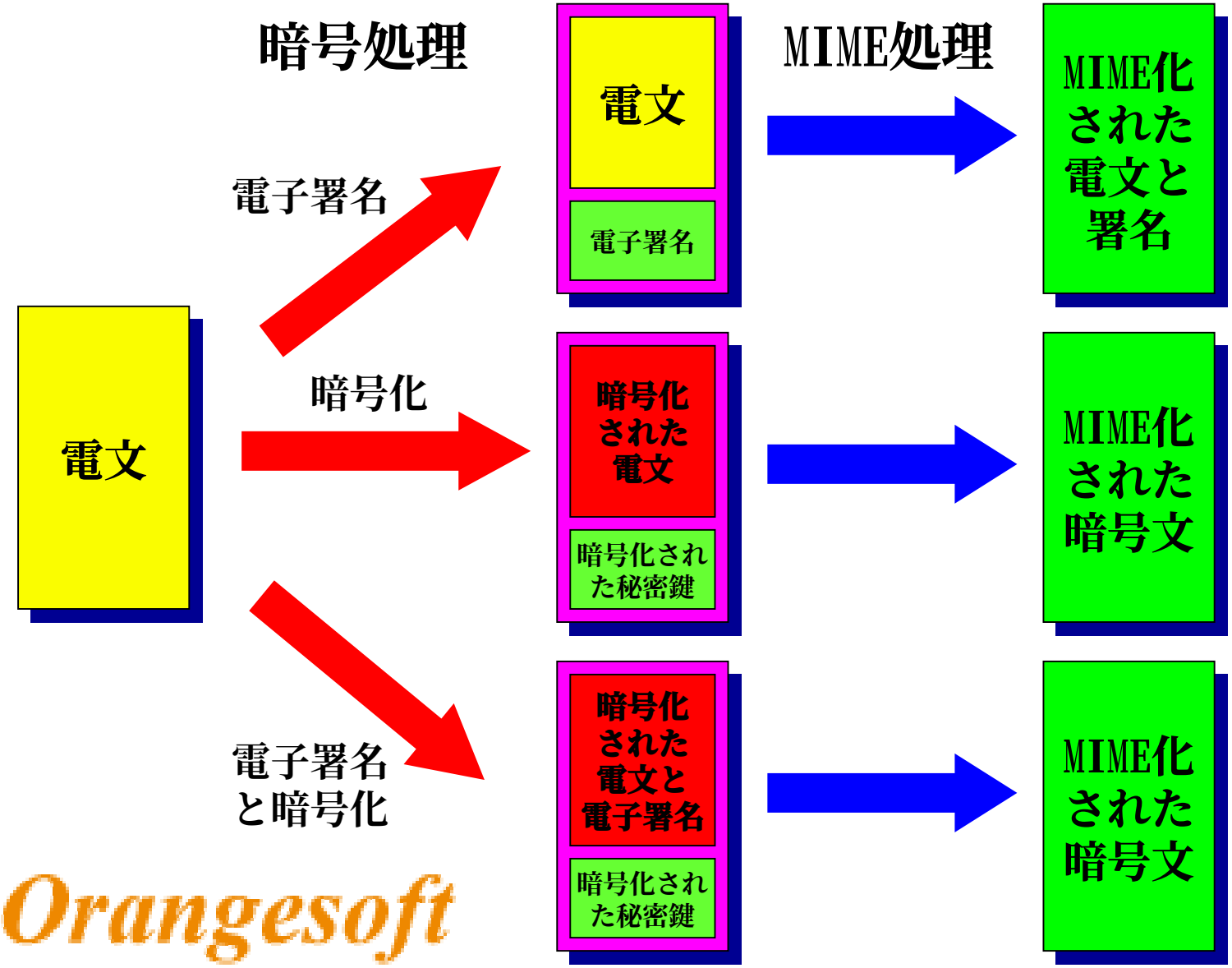
Orangesoft

複数の相手に暗号メールを同報



Orangesoft

暗号文をMIME化して送る



Orangesoft

クリア署名されたメールの実体

```
Subject: =?ISO-2022-JP?B?GyRCJDMkbCRPJUYlOSVIGyhK?=
From: Watanabe Naoaki <kitarou@orangesoft.co.jp>
X-Mailer: Winbiff [Version 2.10 beta5]
Date: Thu, 28 May 1998 16:56:04 +0900
Mime-Version: 1.0
Content-Type: multipart/signed;
    protocol="application/x-pkcs7-signature";
    micalg=rsa-sha1; Boundary="---------896342156-727845"

This is a multi-part message in MIME format.

----------896342156-727845
Content-Type:text/plain; charset=iso-2022-jp
Content-Transfer-Encoding:7bit

 金額は 10円です。

----------896342156-727845
Content-Type: application/x-pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
```

Orangesoft

電子署名+暗号化されたメール

```
To: kitarou@orangesoft.co.jp
Subject: Crypt
From: Watanabe Naoaki <kitarou@orangesoft.co.jp>
Message-Id: <199811202201.FAI36687.ULSVBJP@orangesoft.co.jp>
X-Mailer: Winbiff [Version 2.20 beta1]
Date: Fri, 20 Nov 1998 22:02:19 +0900
Mime-Version: 1.0
Content-Type: application/x-pkcs7-mime; name="smime.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7m"

MIAGCSqGSIb3DQEHA6CAMIACAQAxgDCCARcCAQAwgcAwgasxCzAJBgNVBAYTAkpQ
MRwwGgYDVQQKExNWZXJpU2lnbiBKYXBhbiBLLksuMTQwMgYDVQQLEytWZXJpU2ln
biBDbGFzcyAxIENBIC0gSW5kaXZpZHVhbCBTdWJzY3JpYmVyMUgwRgYDVQQLEz93
```

Orangesoft

メールに証明書を添付

```
To: kitarou@orangesoft.co.jp
Subject: Public key
From: Watanabe Naoaki <kitarou@orangesoft.co.jp>
X-Mailer: Winbiff [Version 2.20 beta1]
Date: Fri, 20 Nov 1998 22:03:23 +0900
Mime-Version: 1.0
Content-Type: MultiPart/Mixed;Boundary="---------911567003-32172559"

----------911567003-32172559
Content-Type: text/plain; charset=iso-2022-jp

 証明書を添付します。


----------911567003-32172559
Content-Type: application/x-pkcs7-mime; smime-type=certs-only; name=smime.p7c
Content-Transfer-Encoding: Base64
Content-Disposition: attachment; filename=smime.p7c

MIAGCSqGSIb3DQEHAqCAMIACAQExADCABgkqhkiG9w0BBwEAAKCAMIIFTTCCBLagAwIBAgIQ
Qcv0fTyx0ybYG2kqwf57eDANBgkqhkiG9w0BAQQFADCBqzELMAkGA1UEBhMCSlAxHDAaBgNV
BAoTE1ZlcmlTaWduIEphcGFuIEsuSy4xNDAyBgNVBAsTK1ZlcmlTaWduIENsYXNzIDEgQ0Eg
```

Orangesoft

電子署名時の漢字コード

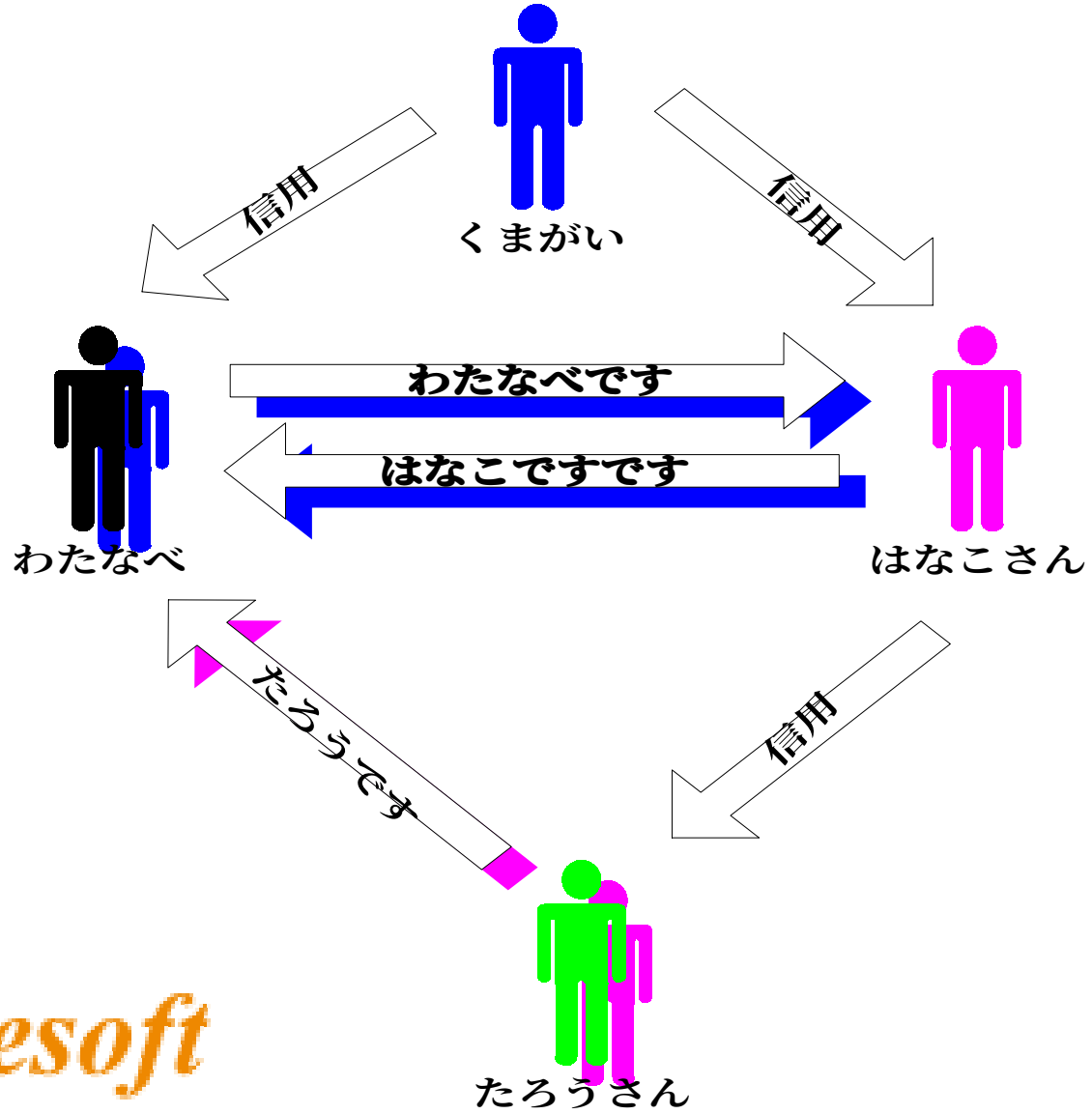
- クリアテキスト署名
  - 内容は誰でも読める
  - しかし署名の確認が必要
- 配送途中で漢字コードを変更されると...
  - 当然、メッセージダイジェストが変化する
    - » 署名の検証ができない
  - 漢字コードのしくみを理解できないメーカも
    - » Content-Type: text/plain; charset=iso-2022-jp
      メッセージに対してShift_JisでMDをつけないで !!
    - » 受信側はiso-2022-jpでMDを作成し署名を検証する
      - ■ 署名の検証ができない

PGPとS/MIME

- PGP
  - 公開鍵に対する認証はお互いが信用に基づく
  - 信頼の輪
    - » 信用できる証明者
  - PGP2.6.3i
  - PGP5.5
- S/MIME
  - 公開鍵に信頼できる機関による認証が行われる
    - » 認証局による証明書の発行
  - Netscape Communicator,OutlookExpress,Winbiff等々

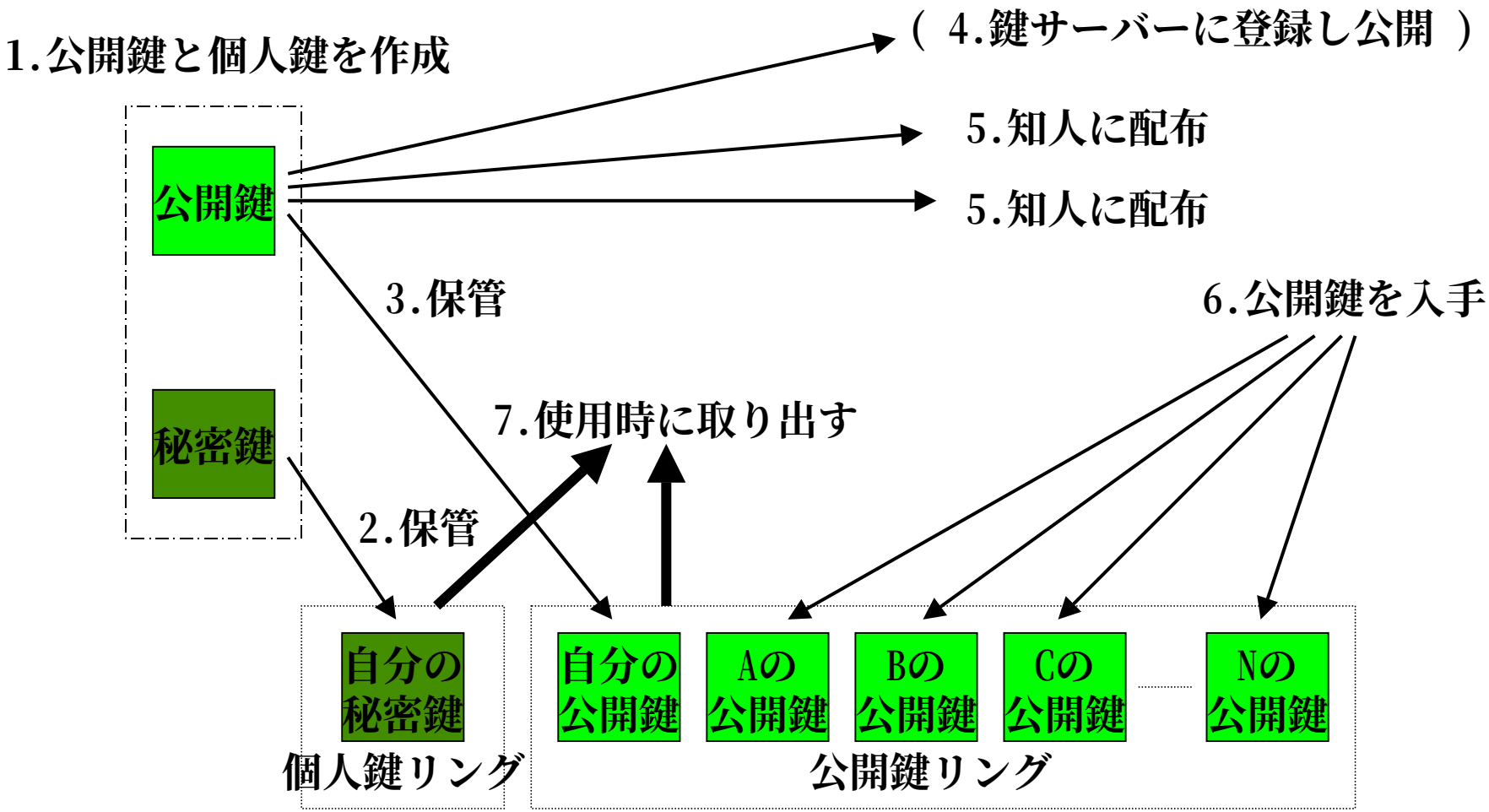
Orangesoft

信頼の輪(web of trust)



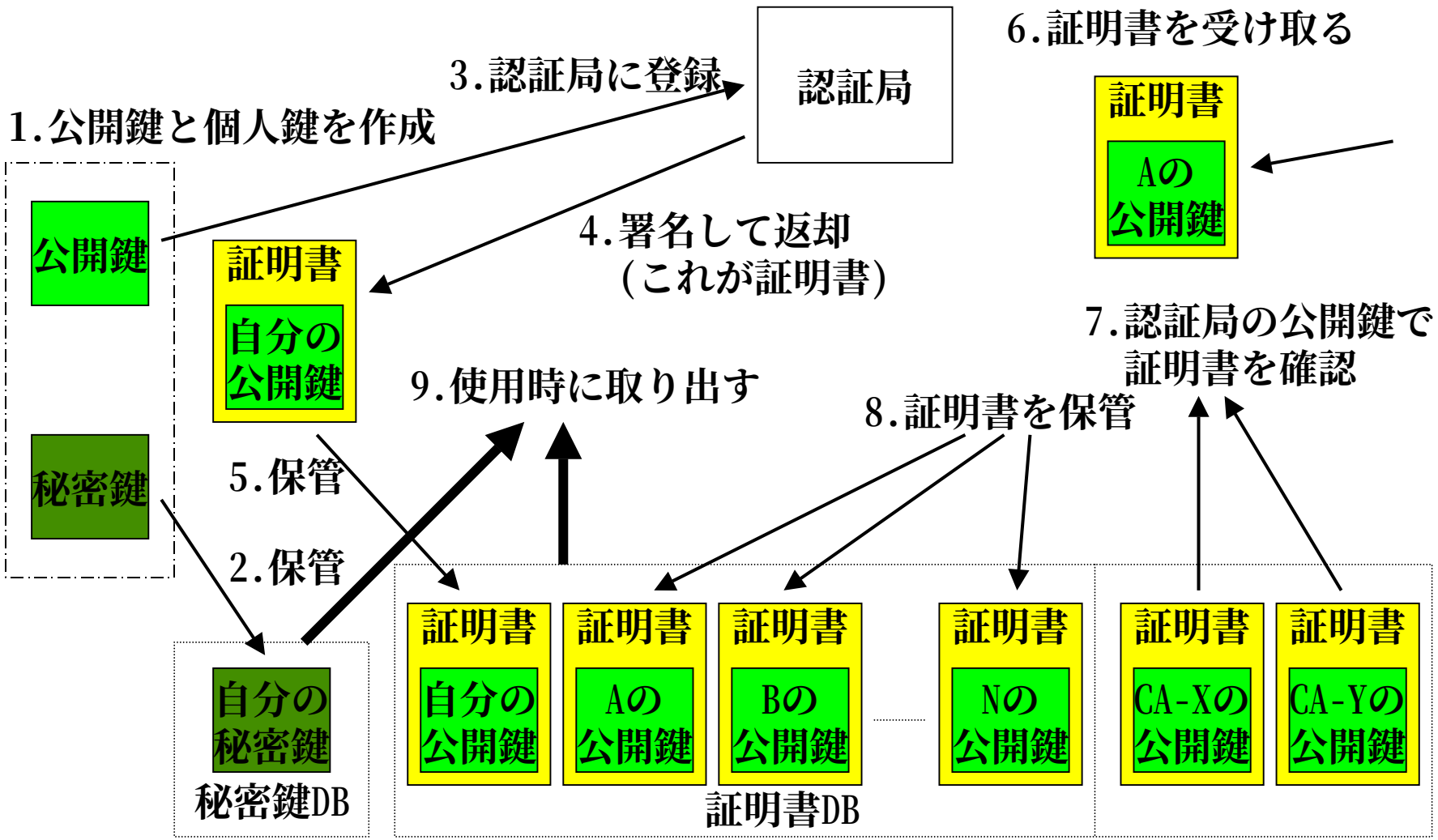
Orangesoft

PGPにおける鍵の管理



Orangesoft

S/MIMEにおける鍵の管理



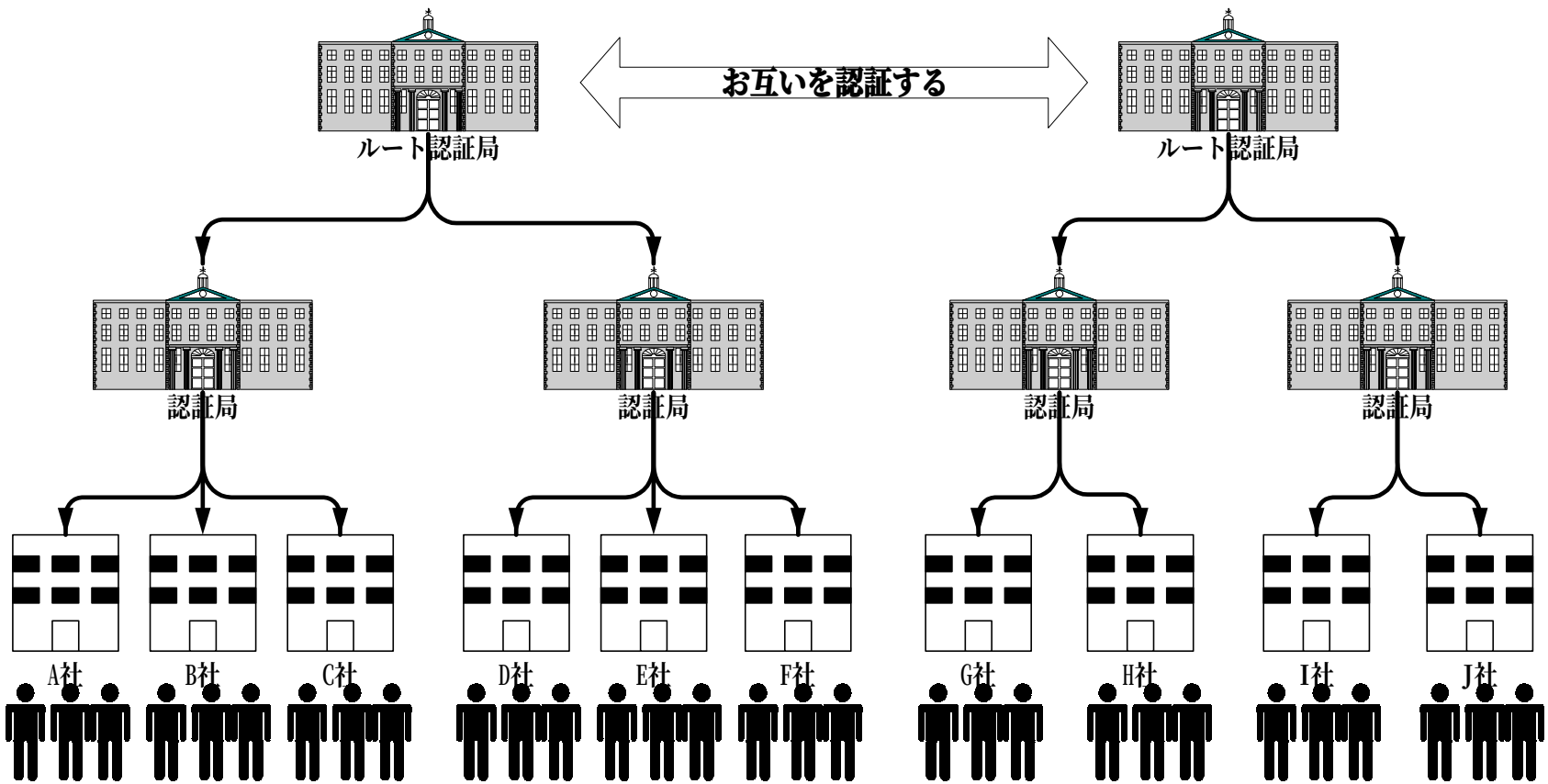
Orangesoft

認証局

- 証明書発行機関
  - 公開鍵が正しいことを証明書
    - » 印鑑証明書
- 商用サービス
  - 日本ベリサイン などなど
- プライベート認証局
  - 自社で運営する認証局
  - 誰の権限で証明書を発行するか ？
  - 他の認証局に認証を受けるのか ？
- 認証局の秘密鍵管理が重要
  - 盗まれると大問題に

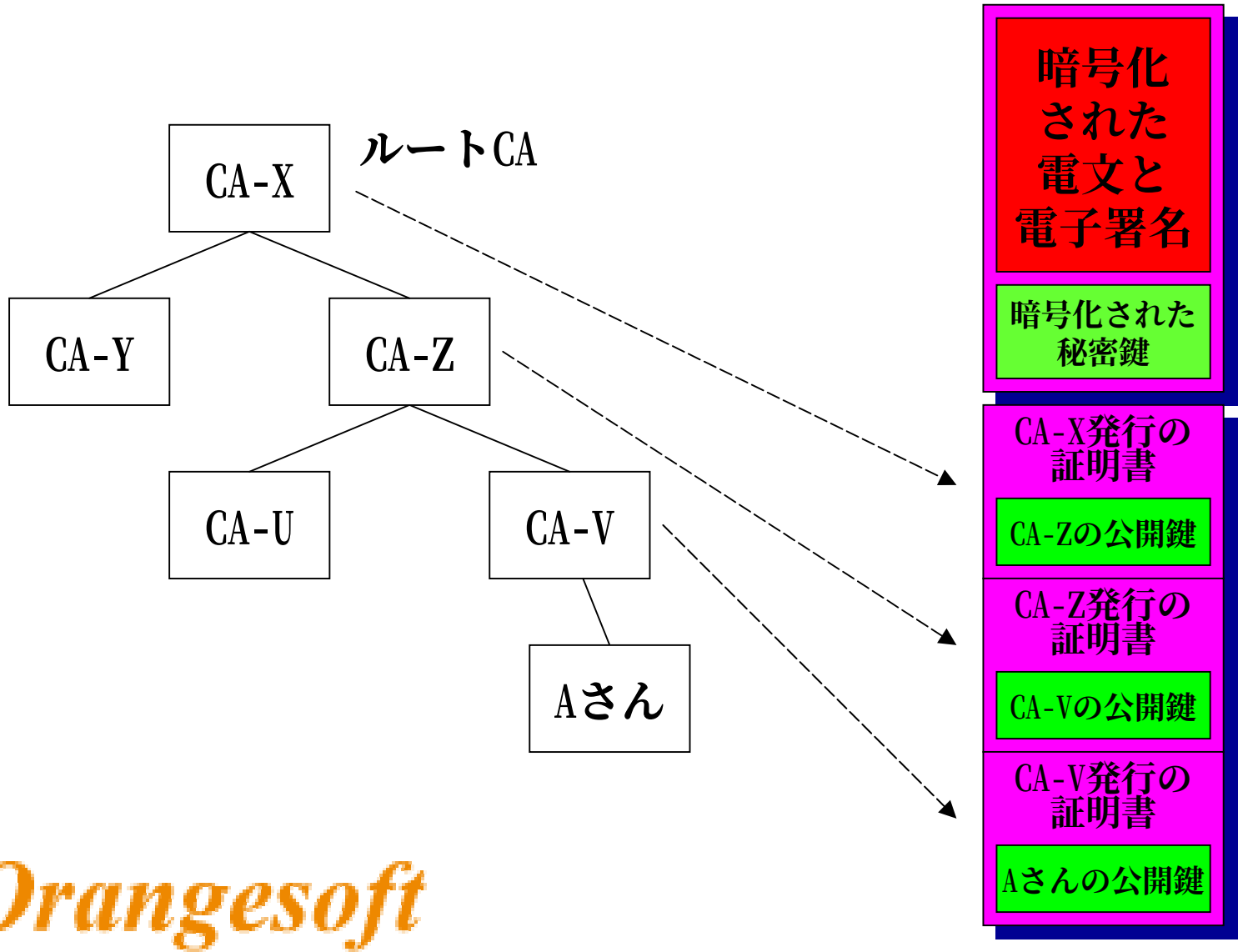
Orangesoft

認証局による認証



Orangesoft

上位認証局の証明書を添付



Orangesoft

暗号メール運用上の問題点

- 使おうとすると簡単ではない
  - 使えるメーラが少ない
  - メーラがこなれていない
  - 互換性に疑問が残る
- 証明書が高くつく
  - 商用認証局は高すぎる
  - 自社で認証局を開設しても運用が必要
- その他の問題点
  - LDAP
  - CRL
  - メーリングリスト

Orangesoft

認証局の選び方

- どの認証局に任せるのか
  - 商用サービス局
  - ボランティア局、試験局（無料 ?)
  - 自社(プライベート局)
- ルートCAが...
  - ブラウザやメーラに登録されていないとつらい
  - 利用者が登録する手もあるが...
- 自社で構築するにも適当なツールがない
  - ライブラリを組み合わせて開発
  - 市販ツールに運用を合わせる
- コストが大きな問題に

証明書のレベル

- 確実な認証にはコストがかかる
  - 簡単な認証でいい場合もある
  - 完璧な認証を求める場合もある
- 完璧さとコストを秤にかけて複数のレベルを
  - クラス１　メールアドレスが正しい(誰かに届く)
  - クラス２　第三者機関を通して個人情報を確認
  - クラス３　戸籍謄本など公的書類で確認
  - クラス４　所属組織も含めて調査し確認
- レベルによって発行料金が違う
  - 1,500円/年 ～ 数千円/年
  - ちょっと高すぎないか !!

Orangesoft

証明書の発行

- 証明書(公開鍵)の有効期限
  - 長すぎると内容が変わったときの処理が面倒
  - 短すぎるとたびたび発行しなければならない
- 証明書の内容
  - 部署名まで含めると部署が変わると変更が必要
    - » 実際は変更でなく、無効にして再発行
- 証明書(公開鍵)の配布方法
  - FDに書き込み、メールに添付
  - Webで公開、LDAPで公開
- CRL(無効証明書)のメンテナンス

鍵の生成

- クライアントで秘密鍵、公開鍵のペアを生成
  - 認証局に証明書発行依頼を行う
  - 秘密鍵の管理をどするか ？
  - 誰でもできる操作なのか ？
  - パスフレーズはユーザが自分で考える
- サーバで秘密鍵、公開鍵のペアを生成
  - 全員分を一気に生成 or 個別に生成
  - ICカードやFDで鍵を配布する
  - サーバ側で秘密鍵の管理もできる
  - パスフレーズの受け渡しも必要

鍵ペアの管理

- 秘密鍵の紛失
  - なくすやつは必ずいる
  - パスフレーズを忘れるやつも必ずいる
  - 誰かに秘密鍵を預けておこう
- 退職などによる証明書の失効時の処理
  - 暗号化されたメールが読めなくなってしまう
    - » 業務上のメールは読めないと困る
    - » 企業秘密を送っていないだろうか
  - 企業側で管理しよう
- 誰が秘密鍵を管理するか
  - 本人はもちろんだけど…

Orangesoft

キーリカバリとキーエスクロウ

- キーリカバリ
  - 共有鍵、秘密鍵がなくても復号可能
  - 安全性とプライバシーは ？
  - しかし、どうしても復号したい場合もあるのでは ？
- キーエスクロウ(鍵寄託)
  - 第三者に復号可能な鍵を預ける
    - » 部分的な預託もありうる
    - » 使うときのルールが重要
  - 会社等では必要 ？
    - » 社員が退職した時
    - » 鍵を紛失してしまった
    - » 検閲

Orangesoft

LDAPとは

- Lightweight Directory Access Protocol
  - X.500から無駄な機能を取り除いて簡素化した
- インターネット上のアドレス帳
  - bigfoot,YahooPepleSerach等
- 電子メールアドレスの検索
  - もちろん証明書やCRLの検索にも
  - Webで公開すると組織構成がばれる
- 登録される情報
  - 氏名、メールアドレス、証明書、公開鍵、電話番号
  - 証明書、公開鍵の有効、無効

Orangesoft

CRLとは

- Certification Revocation List
  - 無効になった証明書の一覧表
- クレジットカードのブラックリストと同じ
  - 証明書を受け取ったたびに確認しなければならない
  - どうやってリストを配布するか
  - 公開していいとは限らない
- 退職者はCRLに載る
  - 証明書が無効になるから
  - 公開すると問題にならないか

メーリングリストの運営

- メールを暗号化してみんなに送る
  - 誰の鍵で暗号化するのか ？
  - 送信時に全員の公開鍵で個別に暗号化する ？
    - » 発信者にとっては大きな負荷
  - メーリングリスト用の秘密鍵を全員に配布
    - » メンバーが変ったときにどうするか
- 暗号化メーリングリストサーバが必要 ？
  - 参加者の公開鍵をメーリングリストサーバに登録
  - 利用者はサーバの公開鍵で暗号化してサーバへ送る
  - サーバは自分の秘密鍵で復号化
  - サーバでメンバー個々の公開鍵で暗号化して配送

オレンジソフト

- 業務内容
  - メールソフト Winbiffの開発、販売
  - S/MIME用アドイン S/Goma
  - PGP 5.5.3ij用 Goma2(Free)
  - PGP2.6.3iフロントエンド Goma(Free)
  - システム・インテグレーション
  - セキュリティに関するコンサルティング
- 問合わせ等
  - URL=http://www.orangesoft.co.jp/
  - E-Mail: info@orangesoft.co.jp

Orangesoft

(株)電通国際情報サービス

- Information Services International-Dentsu,ltd.
  - URL=http://www.isid.co.jp/
  - 設立　　1975年 12月 11日
  - 資本金　5億820万円
  - 売上高　414億4700万円（1998年３月期）
  - 従業員数 826名（1998年4月1日現在）
  - 営業拠点
    - » 東京、大阪、名古屋、ニューヨーク、ロンドン、香港、シンガポール、ブラッセル
- 事業内容
  - 国際ネットワーク(特別第二種通信事業者)
  - システム・インテグレーション、ソフトウェア開発
  - CAD/CAM/CAEソフトウェア販売　など

Orangesoft