#11 Security, 暗号、認証局

Yutaka Yasuda

セキュリティ問題

- システムの安全性
  - いかにして確保するか
- 二つの安全性
  - 通信上の安全性
  - 内部処理システムの安全性
- 両者を分けて考えよ

システムの安全性

- 二つの安全性
- 内部の処理システムの安全性
  - 記録されるデータを第三者に渡さない
  - システムを止めない
- 通信の安全性
  - 流れるデータを第三者に見せない
  - 通信が切れない
  - 通信している相手の真正性
- 技術的には両者は別のもの

内部処理システムの安全性

- まずはハードウェア確保
  - 耐震性、耐火性
  - バックアップ、冗長性
  - 入室管理、なりすまし（いわゆる社会工学）
- それでも起きる
  - 社員による内部犯行もある

ポイント

- 社内の人間による内部システムの不正利用は以前からある
  - なくならないし、問題ではあるが今回はとりあげない。（そもそもコンピュータを使わないシステムでの不正と本質的に同じ）
- このクラスでは
  - ネットワーク越しの不正利用に注目

内部処理システムの安全性

- システム不正侵入
  - 昨今は「不正アクセス」と呼ばれる事が多い
  - システムの不備をついて意図せぬ処理をさせる
- インターネット接続システムが増えた
  - 不用意にバグをさらしているシステムも増えた
  - 大学なども多く侵入されている
  - 今は個人宅が危ない

システム不正侵入

- 対策
  - オープンネットにつながない？
  - ソフトウェアの不備はなくならない
- 技術武装しかない
  - 現在のシステムの脆弱性はどこから？
- セキュリティ関連ビジネスの台頭
  - 企業が多く乗り出しつつある

通信の原理

- 通信とは
  - システム間のデータ受け渡し方法の一つ
  - データ化ルールを送受信者間で共有
- 通信の安全性とは
  - 通信路（線路）を流れるデータの内容（情報）を第三者に渡さない（漏らさない）
  - オープンネットでは困難
  - 例： Web でクレジットカード番号を入力

傍受

- 通信の傍受は技術的には多くの場合可能
  - 傍受そのものは犯罪ではない場合が多い
    例：国内の無線、但し暗号化された無線通信を解読することは違法となった。
- デジタル情報である限り複製が可能
- 複製してもオリジナルに改変を与えない
- 傍受を検知・防御することが困難

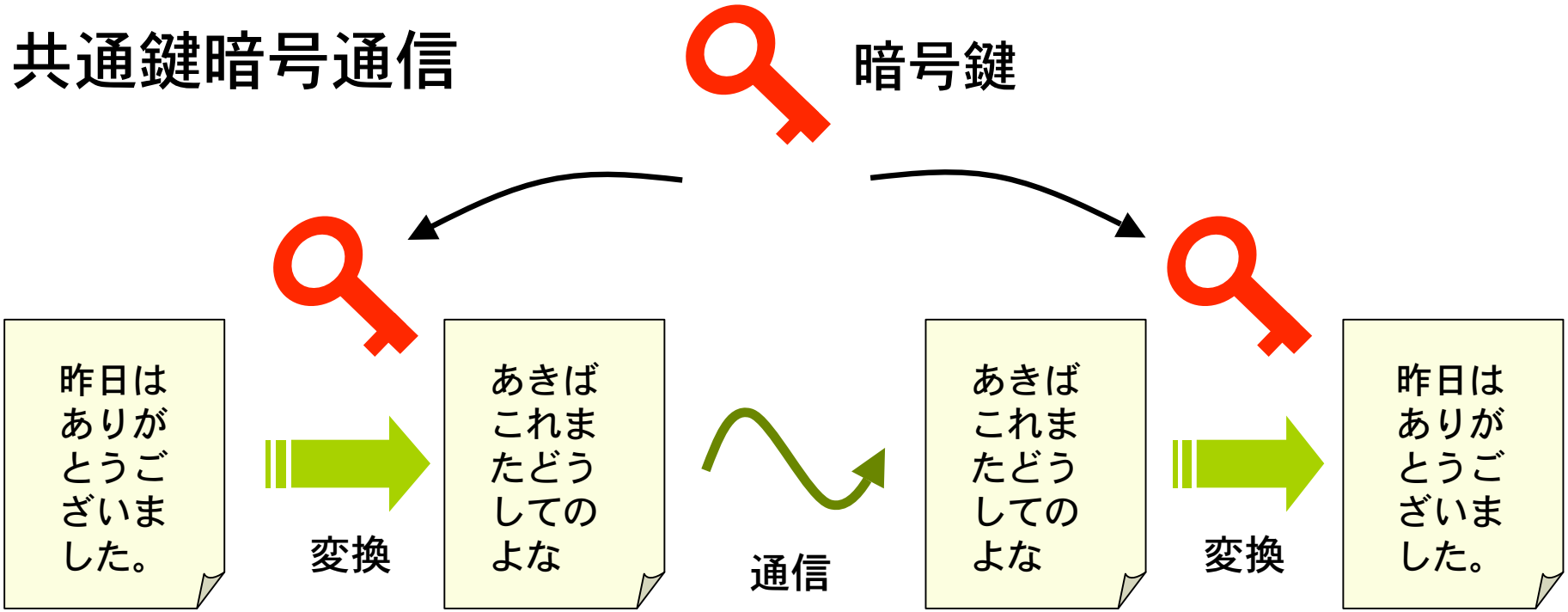
暗号

- では暗号化で対策
  - 傍受されても中身が判らないようにする
- 暗号
  - 当事者以外に復号できなくする
  - 復号ルール（の一部）を秘密にする
    （「鍵」と呼ばれる場合もある）

暗号

- 通信に関わる脅威
  - 秘密情報の取得だけではない
  - なりすましや改竄など
- 現時点では暗号技術の応用で対応
  - 公開鍵暗号技術
  - 誰もが公開鍵で暗号化でき、彼だけが秘密鍵で解読できる
  - 彼だけが秘密鍵で暗号化でき、誰もが公開鍵で検証(復号)できる
  - 英語表現では Public key, Private key

共通鍵暗号通信

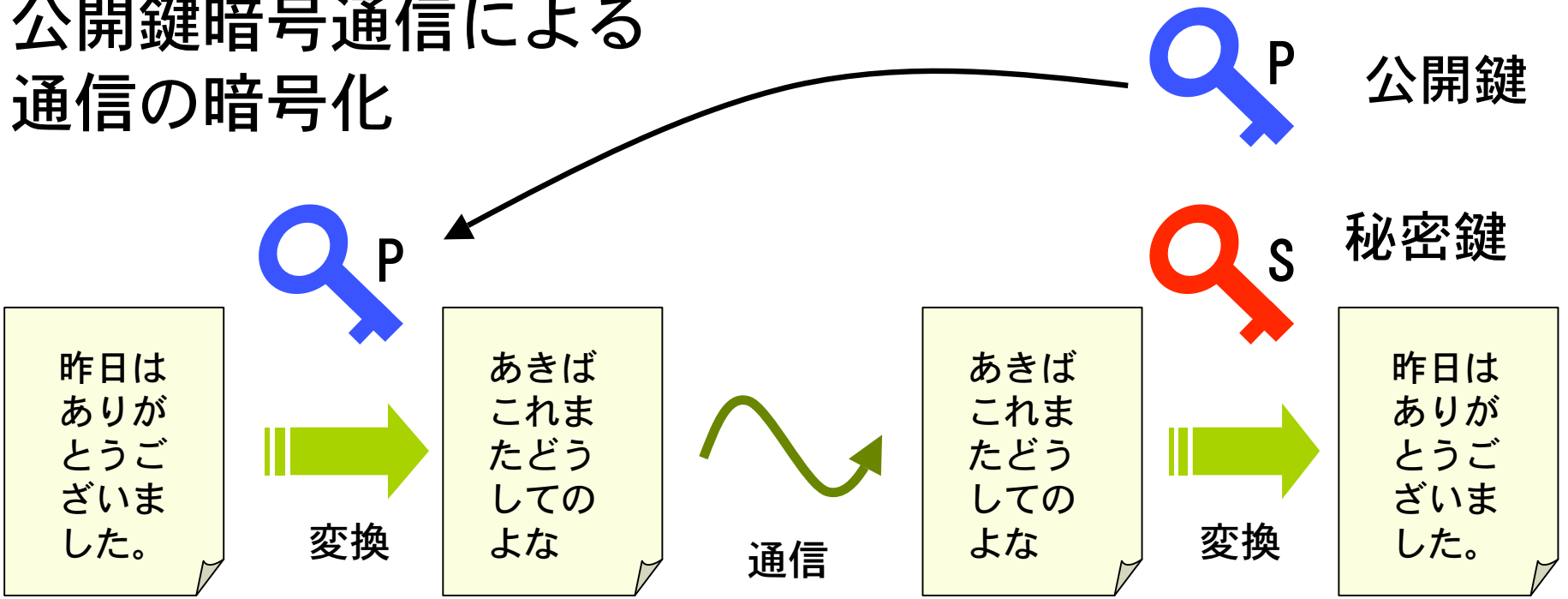


内容を相手だけに解けるように暗号化して相手に送る場合：

1. 両者は信頼できる経路であらかじめ鍵を交換
2. 暗号化し、送る
3. 相手は同一の鍵またはそこから計算できる解読鍵で読む

欠点：インターネットのような場ではあらかじめ鍵を安全に交換するようなことができない

公開鍵暗号通信による通信の暗号化

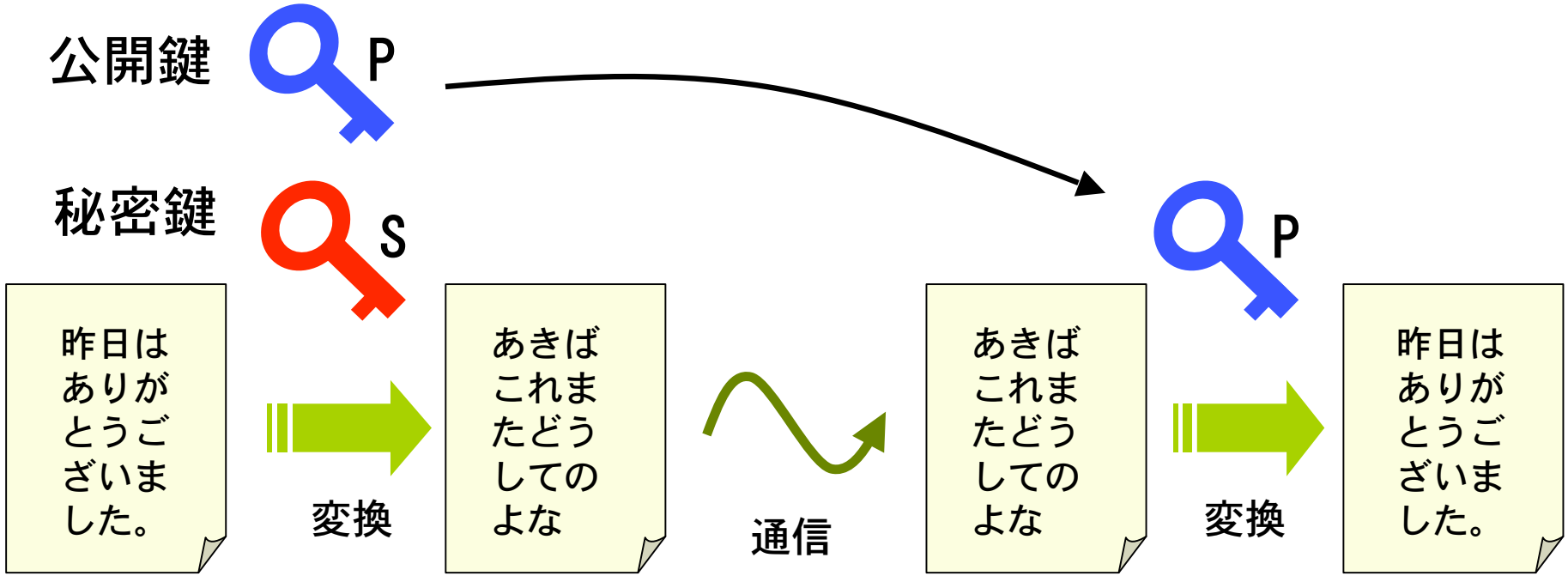


内容を読者だけに解けるように暗号化して相手に送る場合：

1. 読者から暗号化のための鍵を受け取る（公開鍵）
2. 公開鍵で暗号化し、送る
3. 相手は公開鍵に対応した秘密鍵で解読する。

必要になった時点で公開鍵を貰えば良い。
（秘密にする必要がないので取得手段が自由）

公開鍵暗号通信による電子署名（改ざん、本人確認）



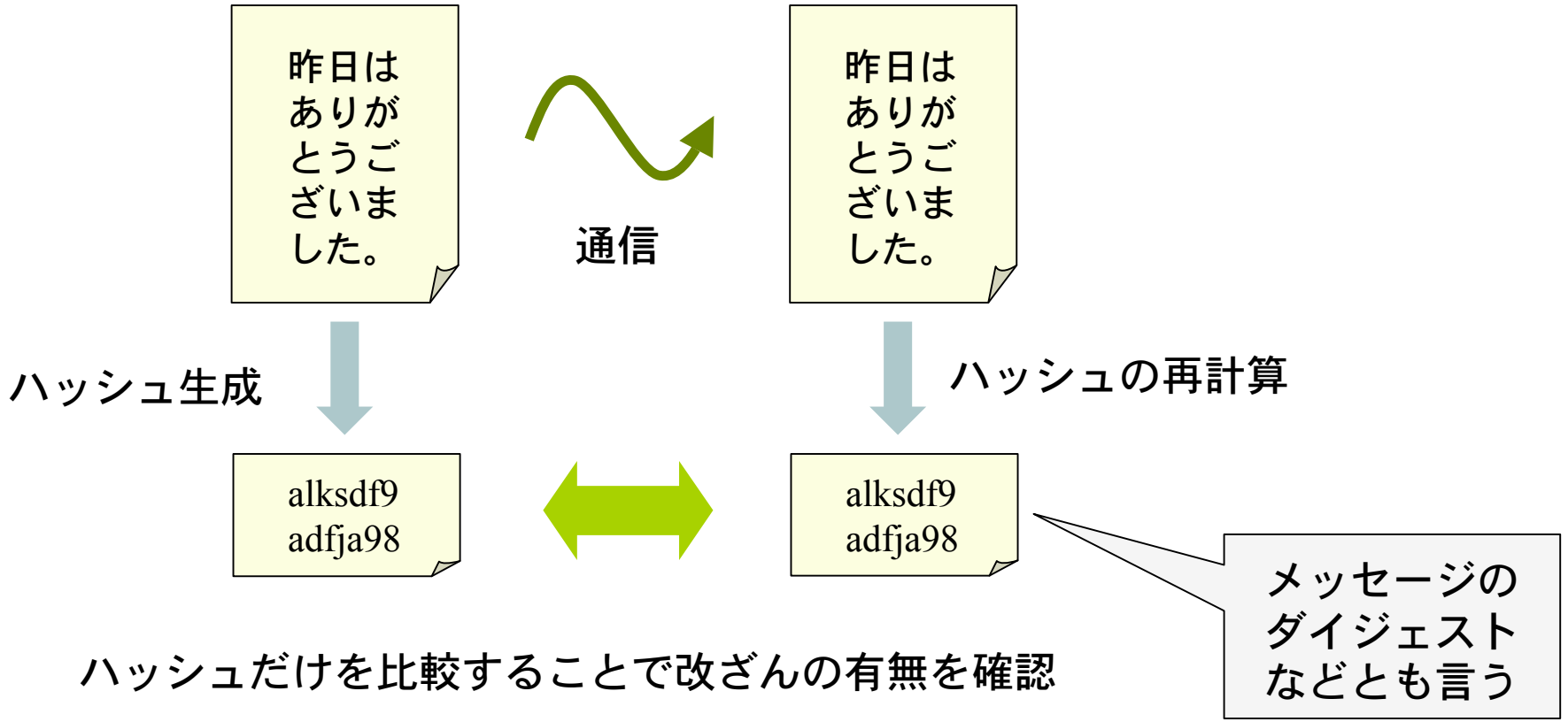
内容は公開だが発信者の確認ができる（なりすまし防止）

1. 読者は「信頼できる経路で」あらかじめ公開鍵を保持
2. 送信者は秘密鍵を用いて文書を暗号化し、送る（公開する）
3. 読者は公開鍵で復号し、復号できることで送信者が公開鍵の持ち主であることを確認する

ハッシュ（ダイジェスト）

- Hash
  - あるデータから一定の長さの数値を出力
  - MD5, SHA-1
- 特徴
  - 元データが一バイトでも変わったらハッシュ値が大きく変わる
  - 同じハッシュ値を持つ、別の元データを推測することが困難（一方向性）
- 改ざんチェックに用いられる
  - ただし時間付きの安全性

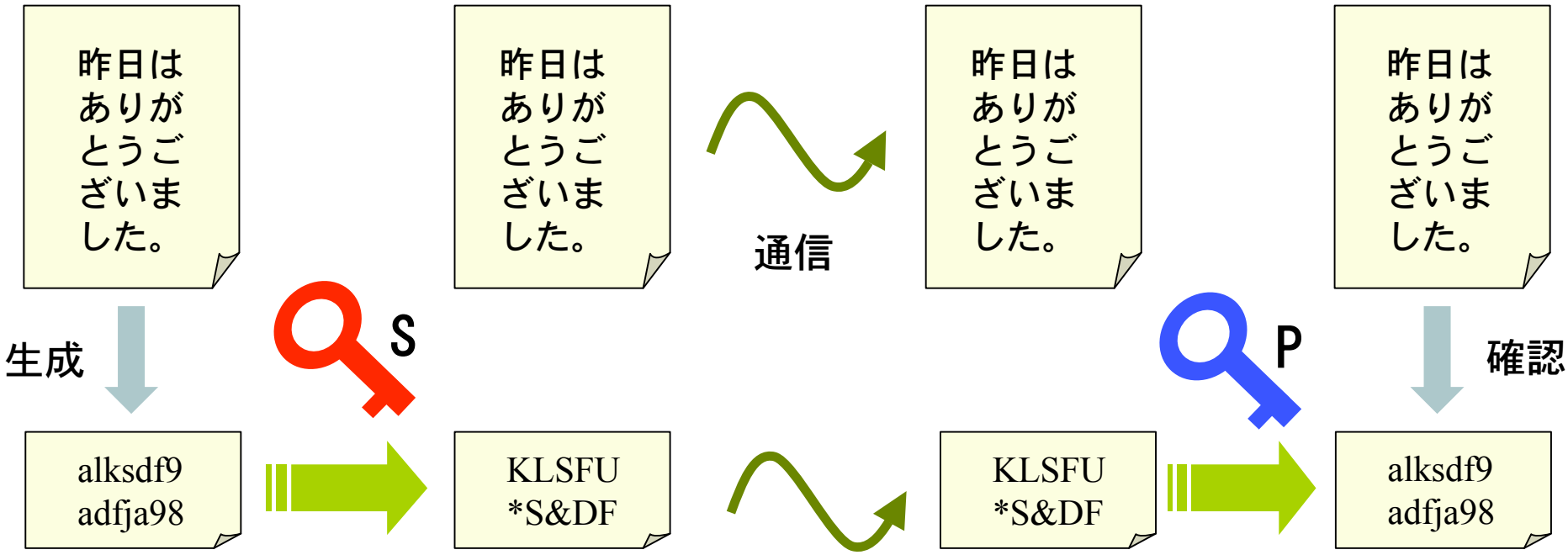
ハッシュによる改ざん確認



ハッシュだけを比較することで改ざんの有無を確認

当然ながらハッシュ値はデータとは別の経路で安全に送る必要がある

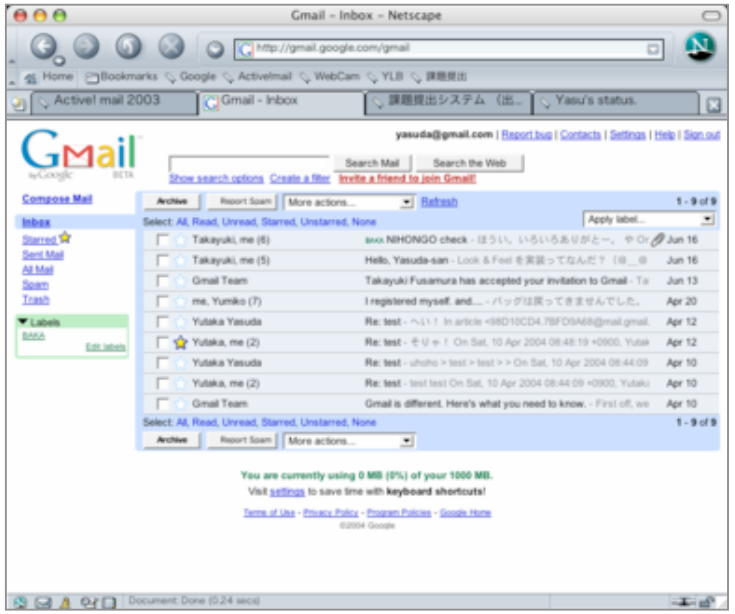
公開鍵暗号通信による
電子署名（改ざん、本人確認）

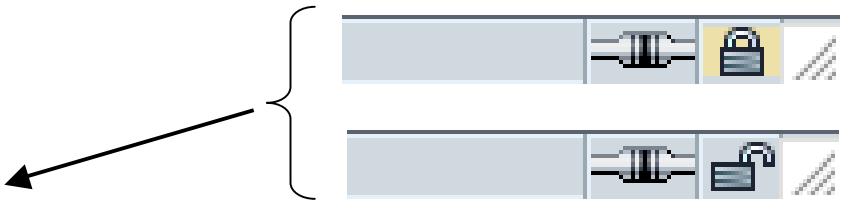


全文は平文でも可。ダイジェストは暗号化して送る。
このときダイジェストが署名として機能する＝電子署名

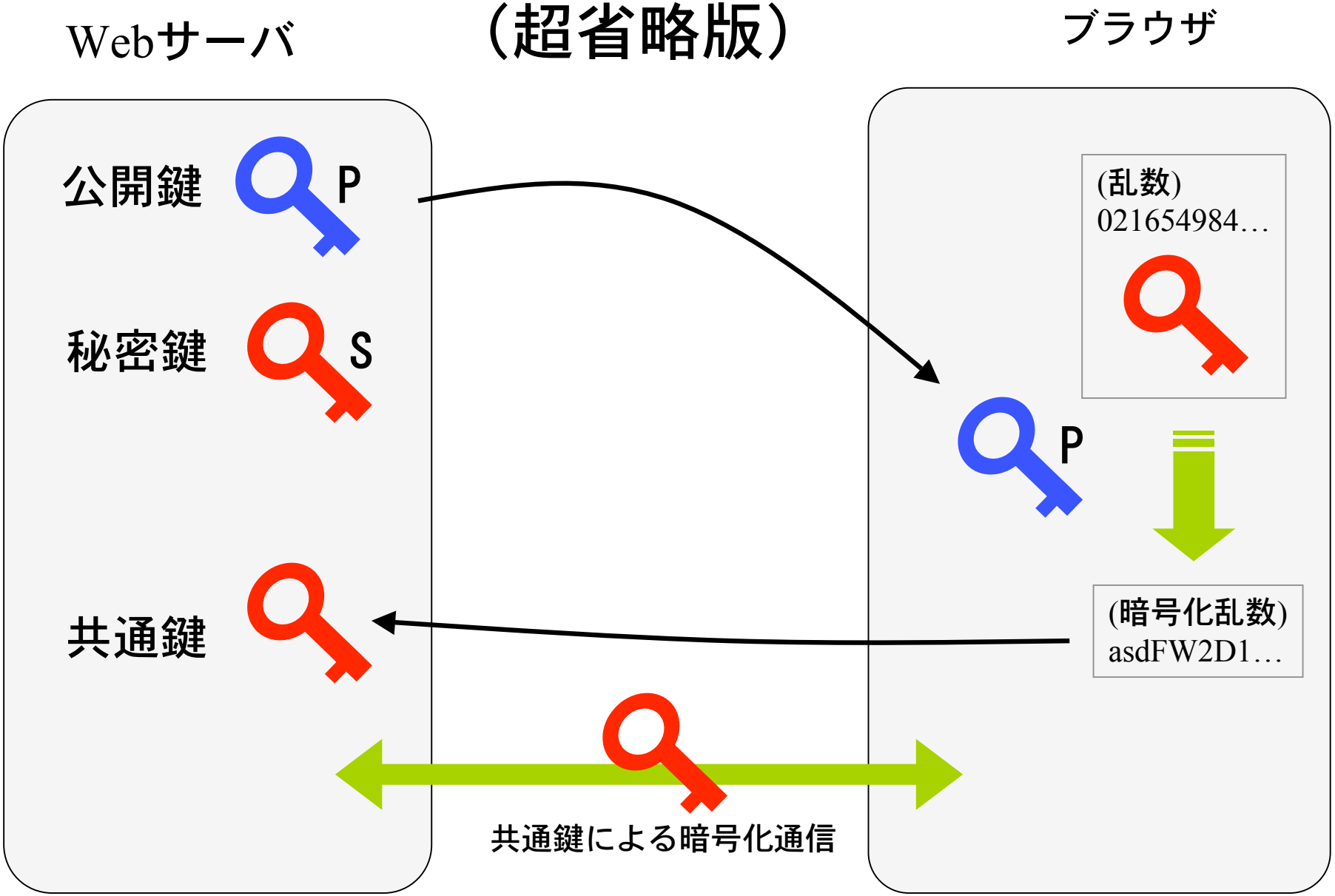
SSL：暗号通信の例

- SSL：ほとんどの Web 取引で利用
  - クレジットカード番号の暗号化など
- 実現手法
  - 公開鍵暗号技術を利用





SSLによる暗号化手順（超省略版）



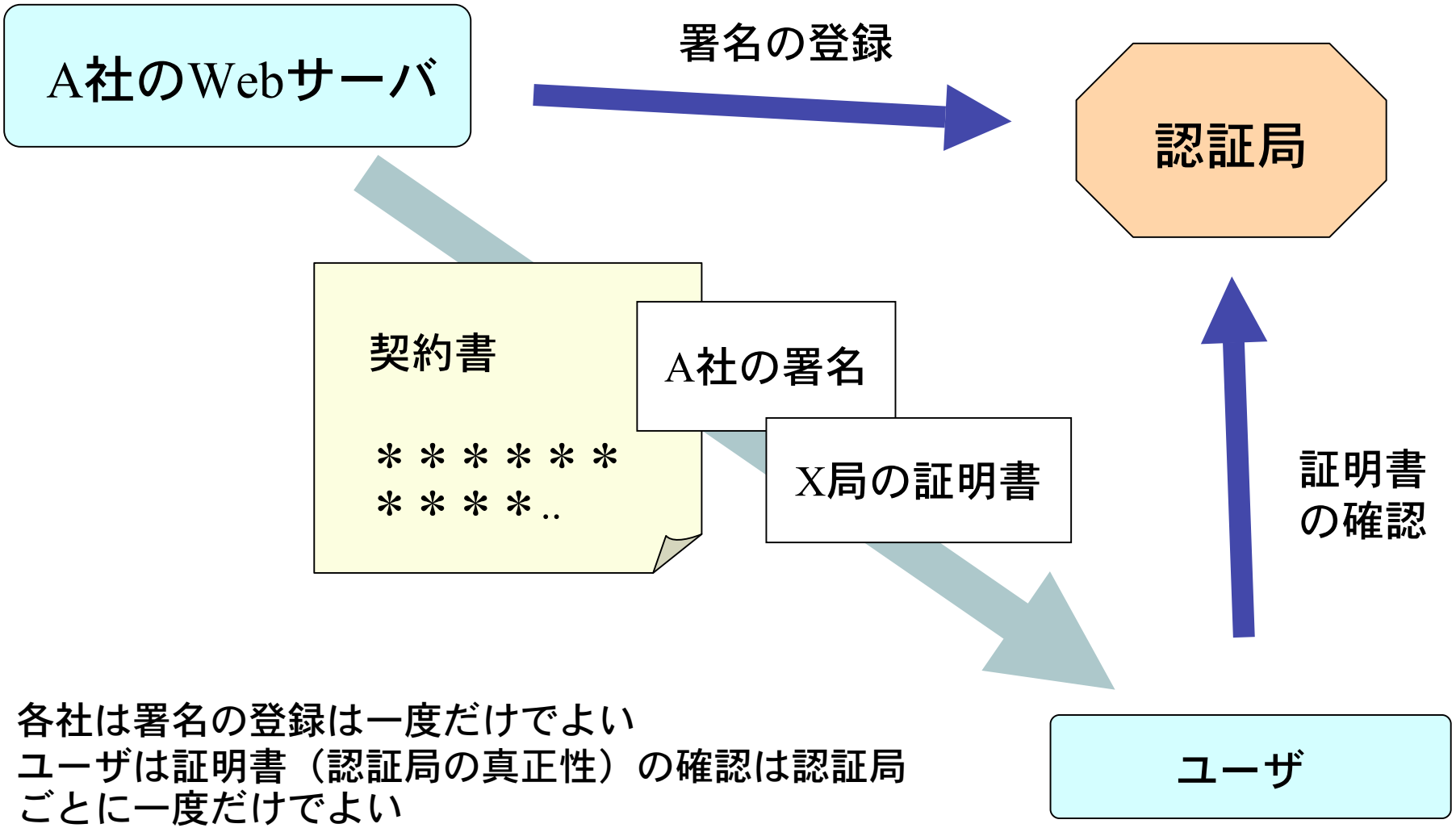
認証：本人確認

- 公開鍵を貰う
  - 相手は本当に自分が通信対象と思っている相手に間違いないか？
  - 「あらかじめ安全な経路で公開鍵を貰う」？
  - 電子商取引では通用しない
  - 本人確認の手段が必要

CA, 認証局

- 認証局 Certification Authority
  - 公開鍵の真正性を裏書きするものが必要
  - 公開鍵に対する証明書とは？
  - 信頼できる第三者の署名で良いだろう
- 認証局は信頼できる第三者機関であるべき
- 認証局ビジネス
  - 本人確認を実世界の手続きを経て行う
  - Verisign 等多数存在する

文書と署名・証明書のながれ



各社は署名の登録は一度だけでよい
ユーザは証明書（認証局の真正性）の確認は認証局ごとに一度だけでよい

CA, 認証局

- 認証局の証明書はどうやって信用する？
  - 印鑑証明と同じ。何が信用の根元か？
  - ユーザの承認に他ならない
- しかしそんな警告を俺は見たことがない！
  - CAの情報が最初からブラウザに登録されている
  - Verisign が利益の源泉としている価値はどこに？

暗号についてまとめ

- 利用例
  - SSL : ほとんどの Web 取引で利用
  - 電子署名 (電子署名・認証法 2001.4.1 施行)
  - 電子政府
  - 認証局ビジネス
- 問題点
  - 数学的強さと計算量問題「期限付きの鍵」
  - ICカードで処理できる鍵＝弱い鍵
  - 最初の承認をどこで取るか
- それでも普及は間違いない

安全性

- 安全性とは何か？
- 総合的なリスクコントロールが重要
- 道路にセキュリティシステムはない
- ネットや技術は個人や企業を対等な立場に
  - 問題もまた対等に、個人に突きつけられる