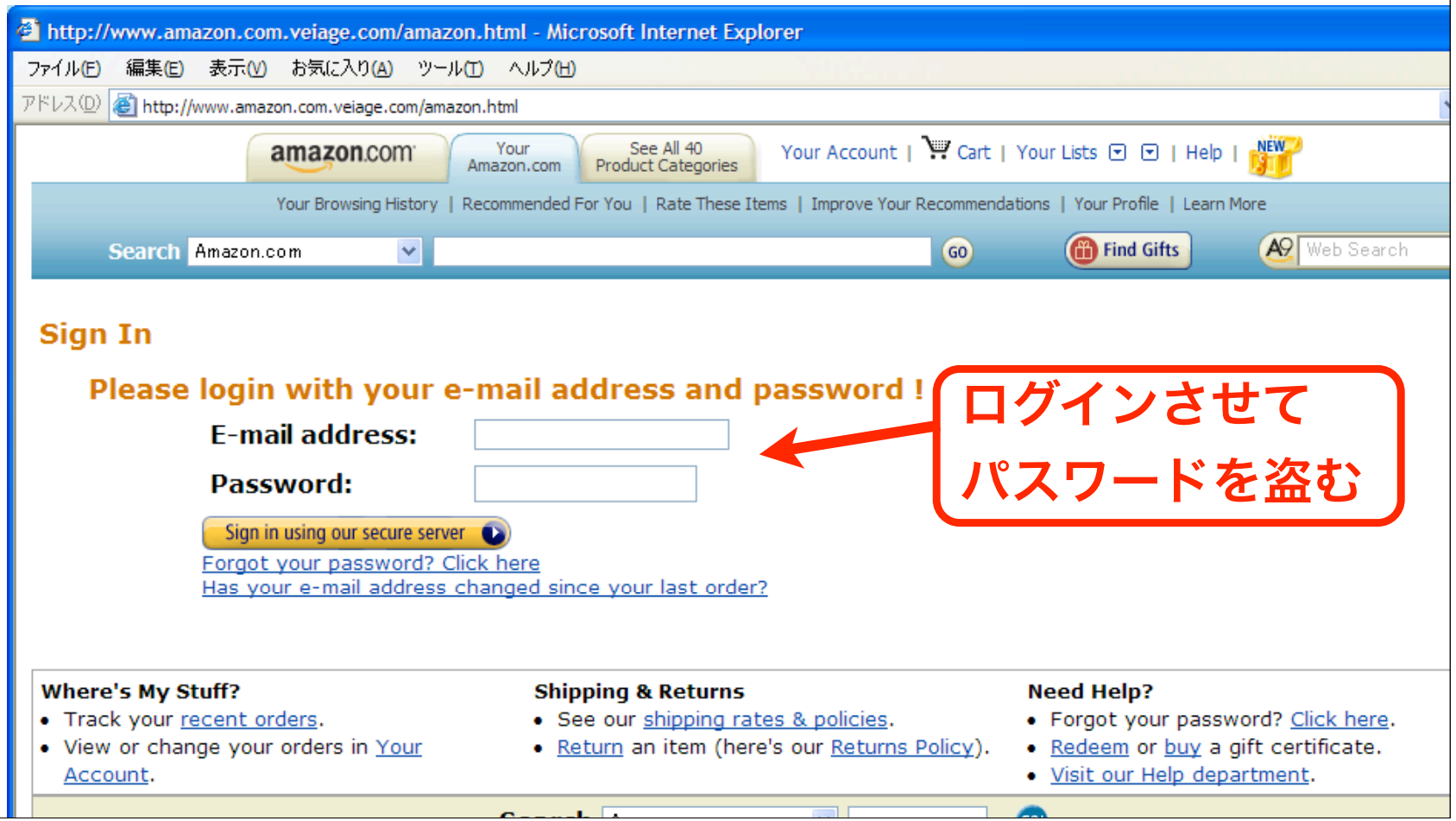
情報処理の概念

#9 Security, 暗号、 認証局

Yutaka Yasuda

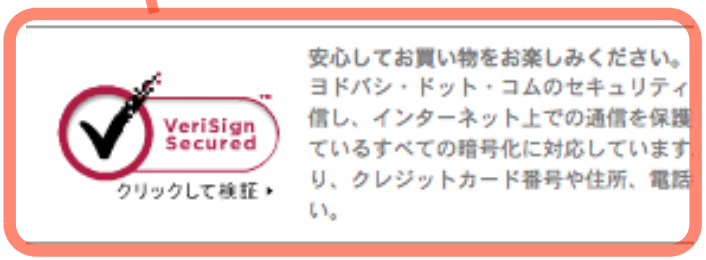
phishing フィッシング

例：amazon.com のなりすましサイト

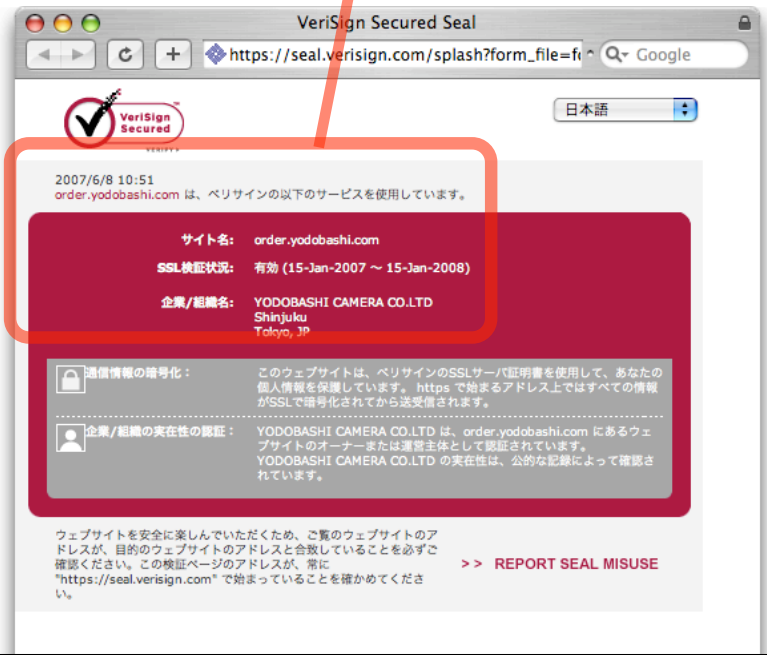



ショッピングカート
https://order.yodobashi.com/metis/order/shoppingcart/ShoppingCartInfoPost.do
www.yodobashi.com
これからご注文手続きを始めます
ショッピングカートの内容
次へ進む
ショッピングカートに戻る
Copyright (C) Yodobashi Camera Co.,Ltd. 1998-2007 All Rights Reserved.

VeriSign Secured
クリックして検証


VeriSign Secured
クリックして検証
安心してお買い物をお楽しみください。
ヨドバシ・ドット・コムのセキュリティ
信し、インターネット上での通信を保護
ているすべての暗号化に対応していま
り、クレジットカード番号や住所、電話
い。


2007/6/8 10:51
order.yodobashi.com は、ベリサインの以下のサービスを使用し
サイト名: order.yodobashi.com
SSL検証状況: 有効 (15-Jan-2007 ～ 15-J
企業/組織名: YODOBASHI CAMERA CO.L
Shinjuku
Tokyo, JP


VeriSign Secured Seal
https://seal.verisign.com/splash?form_file=f
日本語
2007/6/8 10:51
order.yodobashi.com は、ベリサインの以下のサービスを使用しています。
サイト名: order.yodobashi.com
SSL検証状況: 有効 (15-Jan-2007 ～ 15-Jan-2008)
企業/組織名: YODOBASHI CAMERA CO.LTD
Shinjuku
Tokyo, JP
通信情報の暗号化：
このウェブサイトは、ベリサインのSSLサーバ証明書を使用して、あなたの個人情報を保護しています。 https で始まるアドレス上ではすべての情報がSSLで暗号化されてから送受信されます。
企業/組織の実在性の認証：
YODOBASHI CAMERA CO.LTD は、order.yodobashi.com にあるウェブサイトのオーナーまたは運営主体として認証されています。
YODOBASHI CAMERA CO.LTD の実在性は、公的な記録によって確認されています。
ウェブサイトを安全に楽しんでいただくため、ご覧のウェブサイトのアドレスが、目的のウェブサイトのアドレスと合致していることを必ずご確認ください。この検証ページのアドレスが、常に "https://seal.verisign.com" で始まっていることを確かめてください。
>> REPORT SEAL MISUSE

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

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

ネットワーク越しの不正利用

- 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

  バグ・ウィルスに対する対策不充分

  大学なども多く侵入されている

  今は個人宅が危ない

ネットワーク越しの不正利用

- 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

- 技術武装あるのみ

  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

通信の安全性

- 互いのシステムは安全・では通信は安全か？

  通信の安全性とは

- 通信相手の真正性（なりすまし）

- 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

- 暗号化による対策

  傍受されても中身が判らない

- 暗号

  当事者以外に復号できない

  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

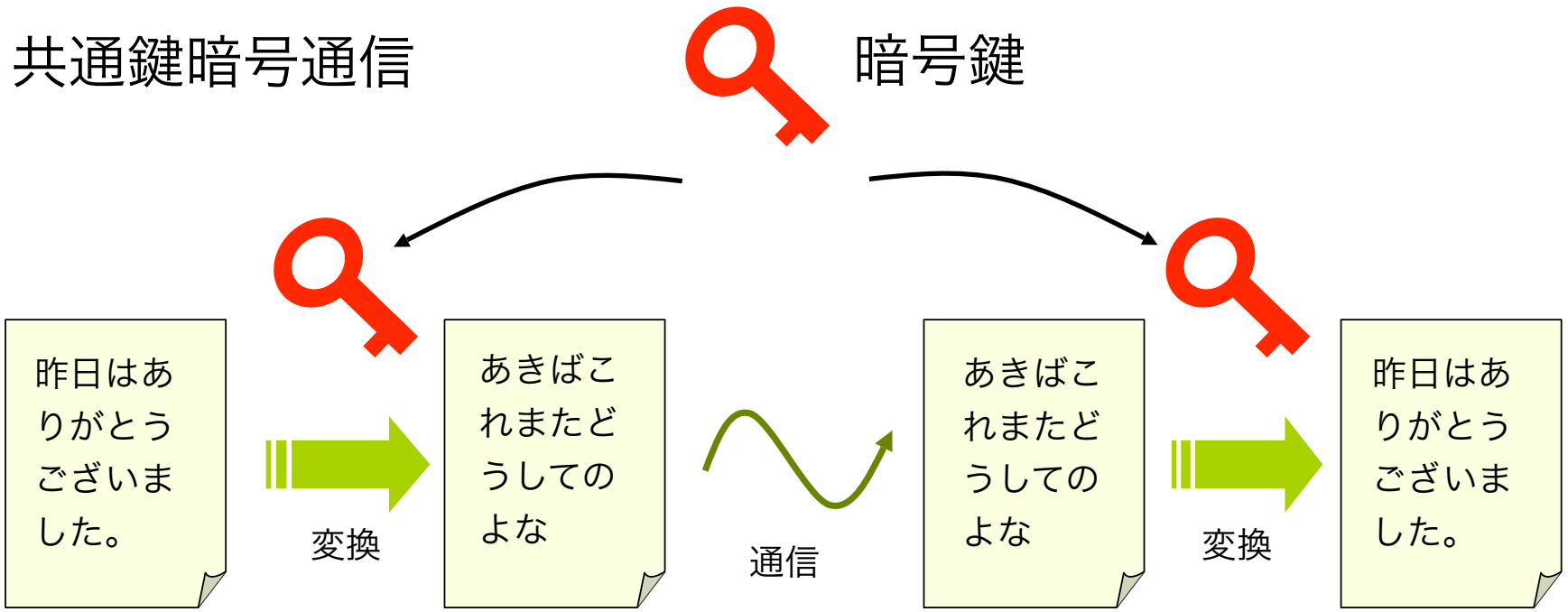
  傍受：秘密情報の取得だけではない

  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

共通鍵暗号通信

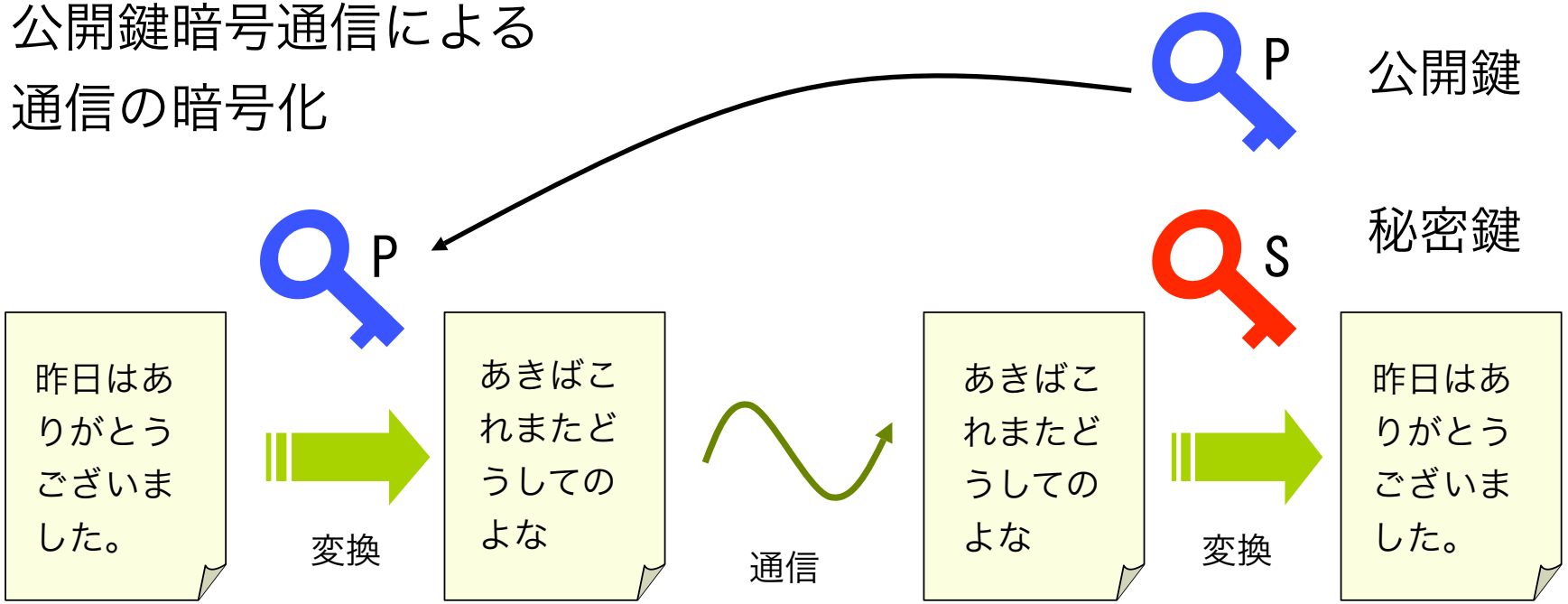


内容を相手だけに解けるように暗号化して相手に送る場合：

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

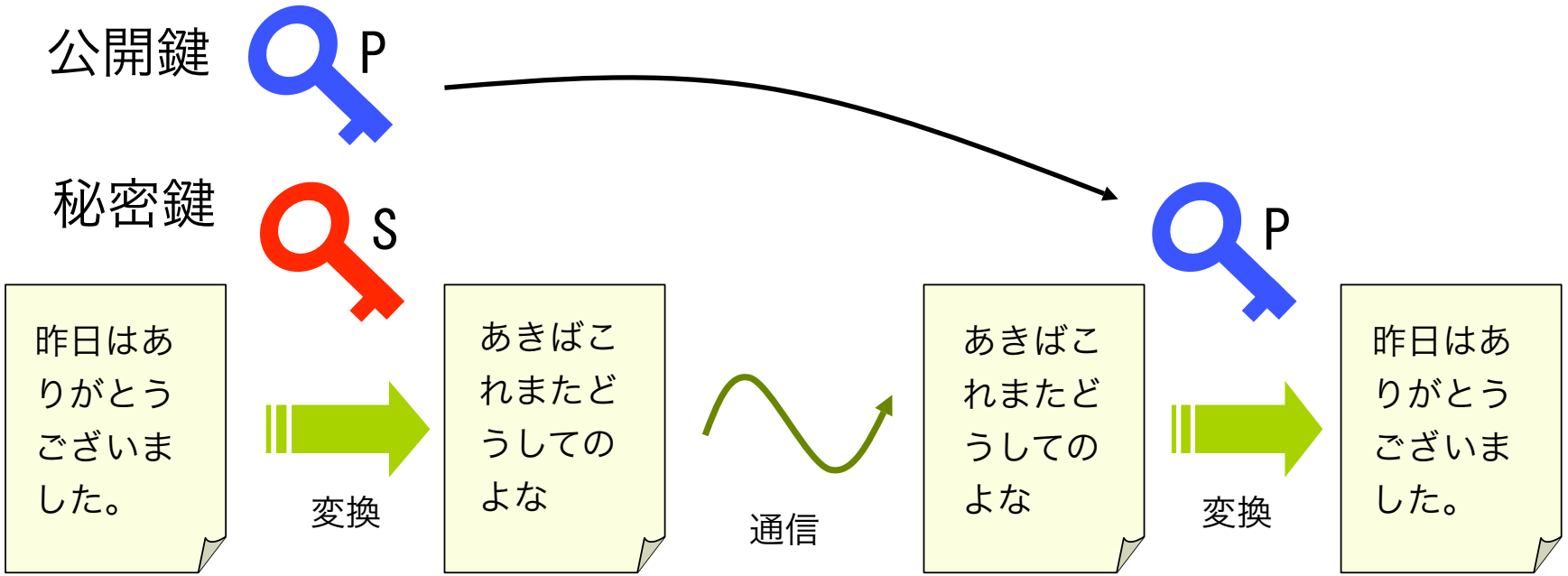


内容を読者だけに解けるように暗号化して相手に送る場合：

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する計算式

  MD5 (128bit), SHA-1 (160bit)

- 特徴

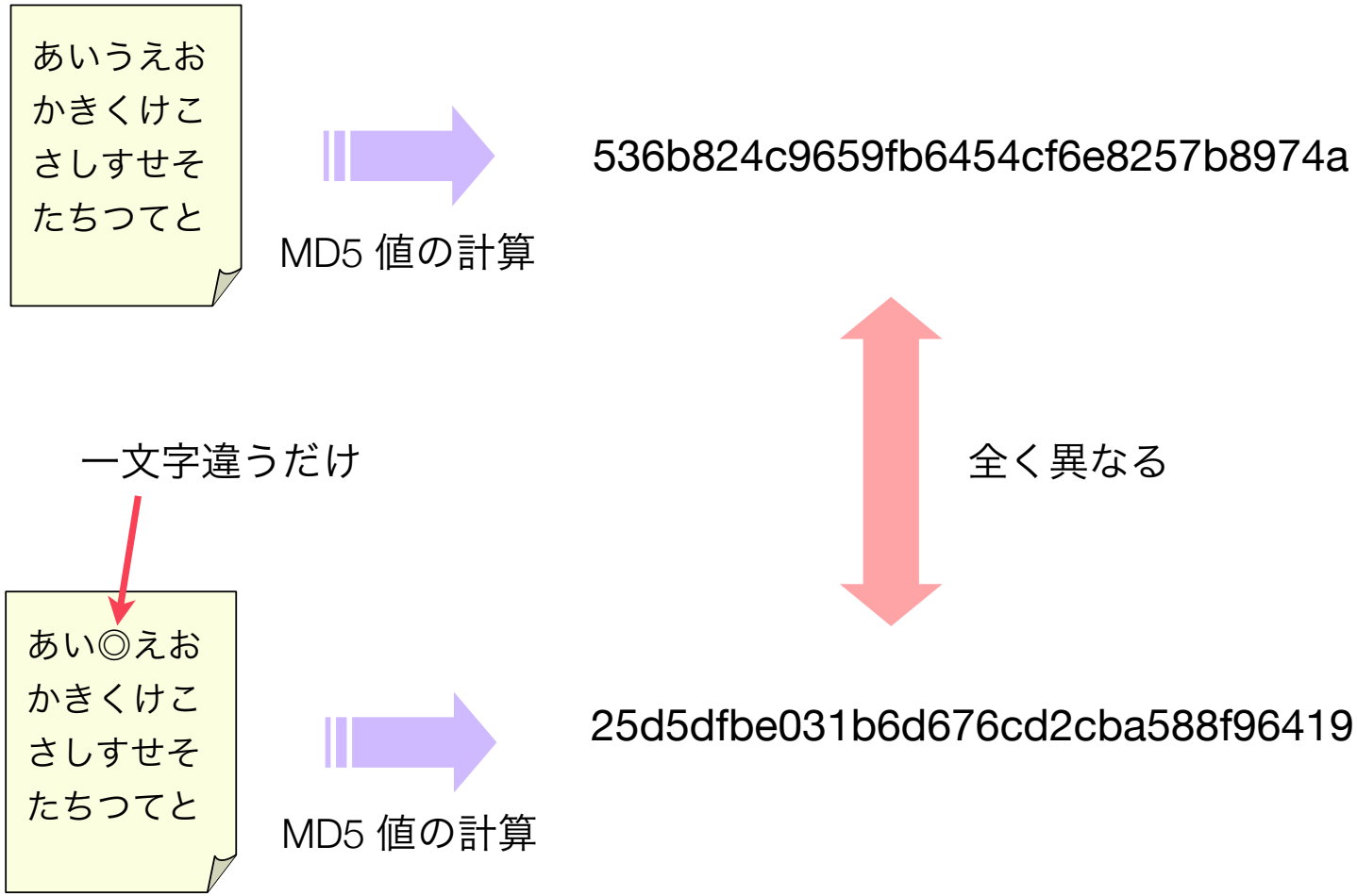
  元データが一バイトでも変わったらハッシュ値が大きく変わる

  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）

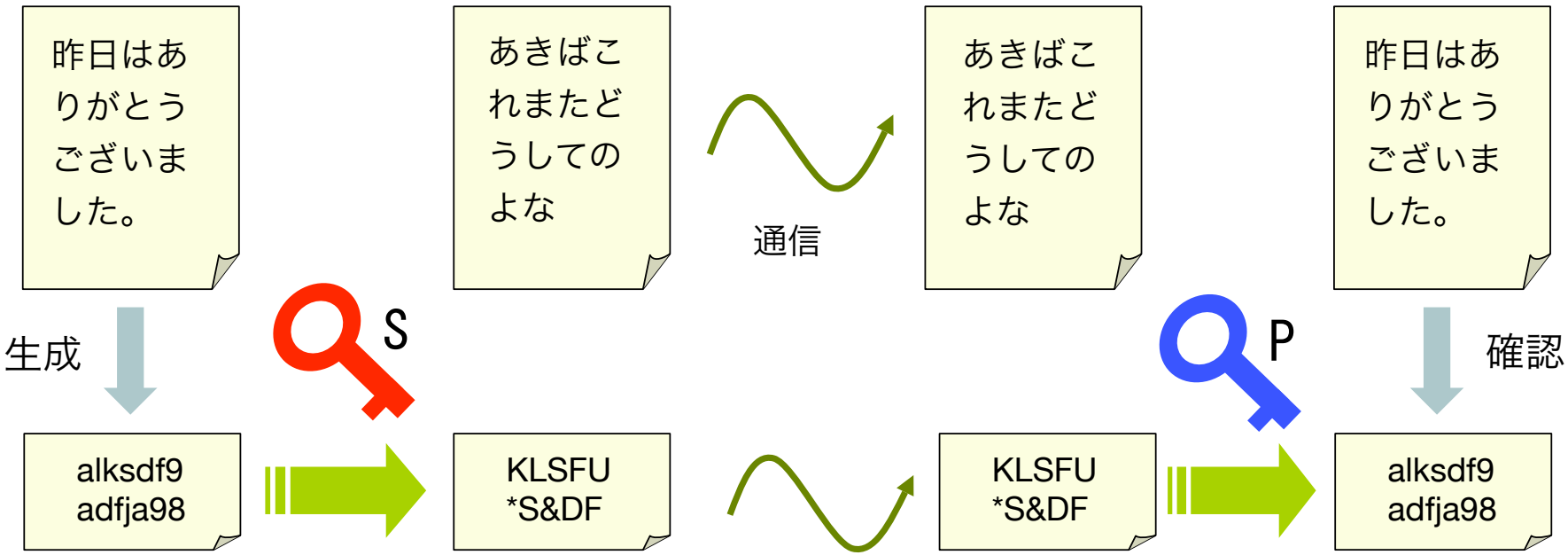
- 改ざんチェックに用いられる

  ただし時間付きの安全性

ハッシュ (例)


あいうえお
かきくけこ
さしすせそ
たちつてと
MD5 値の計算
536b824c9659fb6454cf6e8257b8974a
全く異なる
一文字違うだけ
あい◎えお
かきくけこ
さしすせそ
たちつてと
MD5 値の計算
25d5dfbe031b6d676cd2cba588f96419

ダイジェスト＋公開鍵暗号通信による電子署名（改ざん、本人確認）

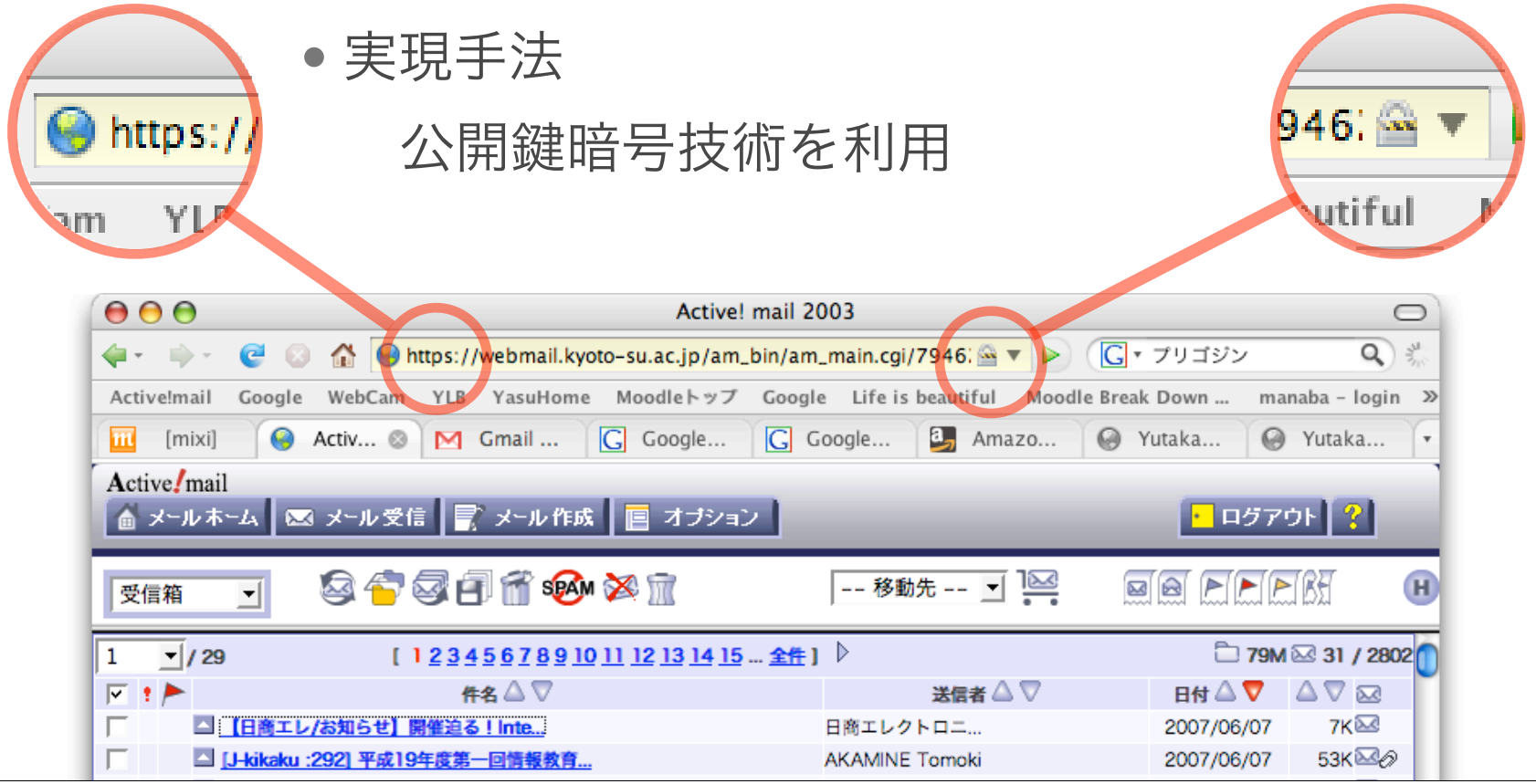


全文は平文でも可。ダイジェストは暗号化して送る。

このときダイジェストが署名として機能する＝電子署名

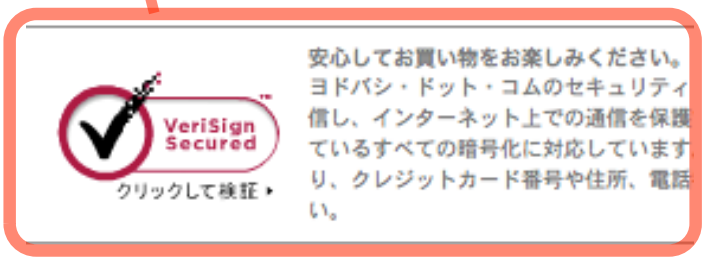
SSL：暗号通信の例

- 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

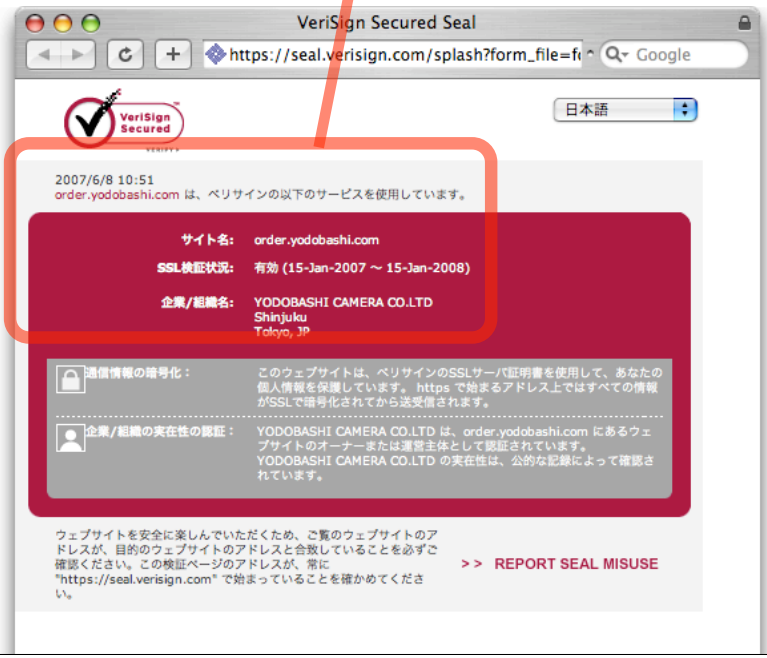


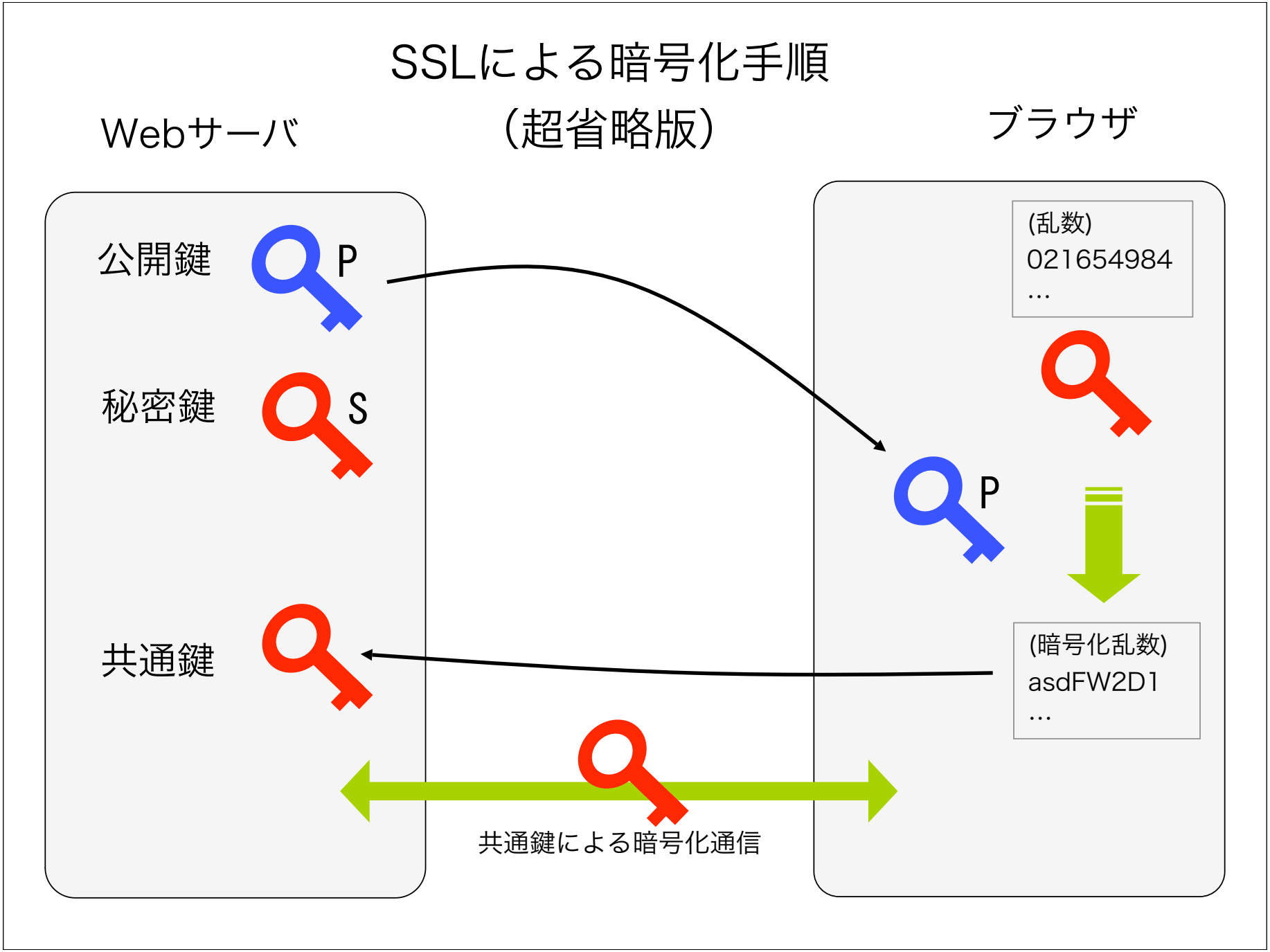

ショッピングカート
https://order.yodobashi.com/metis/order/shoppingcart/ShoppingCartInfoPost.do
www.yodobashi.com
これからご注文手続きを始めます
ショッピングカートの内容
次へ進む
ショッピングカートに戻る
Copyright (C) Yodobashi Camera Co.,Ltd. 1998-2007 All Rights Reserved.

VeriSign Secured
クリックして検証


VeriSign Secured
クリックして検証
安心してお買い物をお楽しみください。
ヨドバシ・ドット・コムのセキュリティ
信し、インターネット上での通信を保護
ているすべての暗号化に対応していま
り、クレジットカード番号や住所、電話
い。


2007/6/8 10:51
order.yodobashi.com は、ベリサインの以下のサービスを使用し
サイト名: order.yodobashi.com
SSL検証状況: 有効 (15-Jan-2007 ～ 15-J
企業/組織名: YODOBASHI CAMERA CO.L
Shinjuku
Tokyo, JP


VeriSign Secured Seal
https://seal.verisign.com/splash?form_file=f
日本語
2007/6/8 10:51
order.yodobashi.com は、ベリサインの以下のサービスを使用しています。
サイト名: order.yodobashi.com
SSL検証状況: 有効 (15-Jan-2007 ～ 15-Jan-2008)
企業/組織名: YODOBASHI CAMERA CO.LTD
Shinjuku
Tokyo, JP
通信情報の暗号化：
このウェブサイトは、ベリサインのSSLサーバ証明書を使用して、あなたの個人情報を保護しています。 https で始まるアドレス上ではすべての情報がSSLで暗号化されてから送受信されます。
企業/組織の実在性の認証：
YODOBASHI CAMERA CO.LTD は、order.yodobashi.com にあるウェブサイトのオーナーまたは運営主体として認証されています。
YODOBASHI CAMERA CO.LTD の実在性は、公的な記録によって確認されています。
ウェブサイトを安全に楽しんでいただくため、ご覧のウェブサイトのアドレスが、目的のウェブサイトのアドレスと合致していることを必ずご確認ください。この検証ページのアドレスが、常に "https://seal.verisign.com" で始まっていることを確かめてください。
>> REPORT SEAL MISUSE


SSLによる暗号化手順
（超省略版）
Webサーバ
ブラウザ
公開鍵
P
秘密鍵
S
共通鍵
(乱数)
021654984
…
P
(暗号化乱数)
asdFW2D1
…
共通鍵による暗号化通信

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」？

  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？

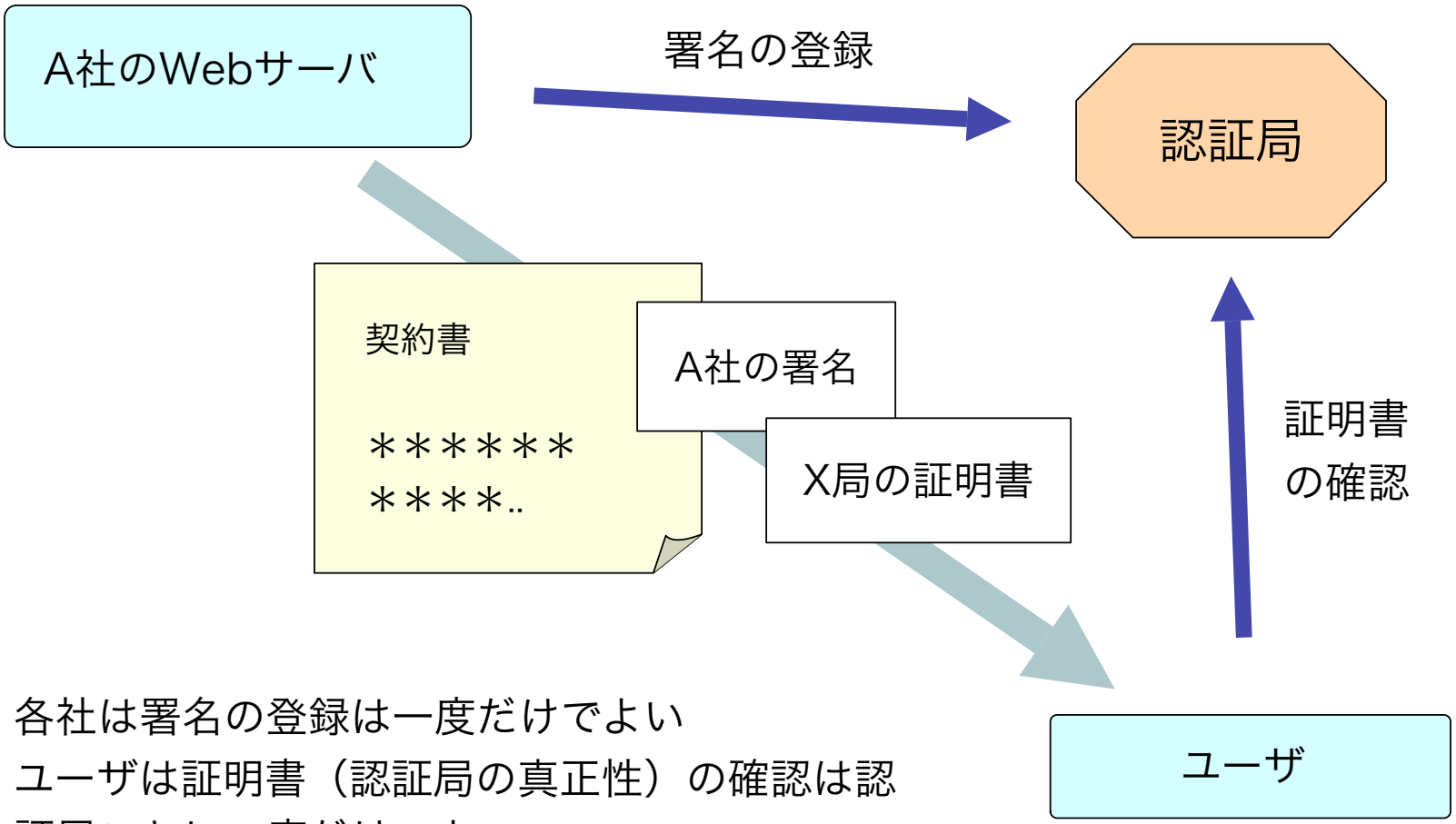
  信頼できる第三者の署名で良いだろう

- 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

  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

認証局の真正性

- 認証局の証明書はどうやって信用する？

  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