VeriSign®
A SYMANTEC
AFFILIATED COMPANY

モバイルとPKI（公開鍵基盤）

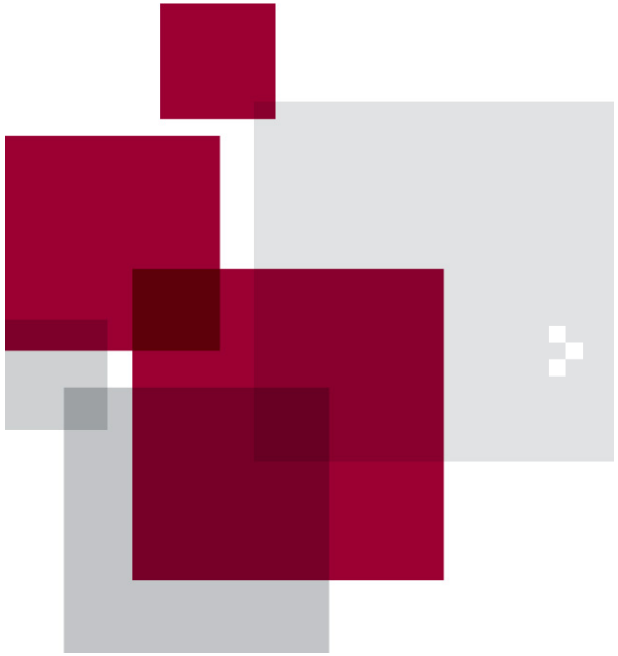
New Devices meet with Old Technologies

日本ベリサイン株式会社

2012年1月18日

アジェンダ

- はじめに
  - 日本ベリサイン株式会社のご紹介
- PKIってなに？
  - 信頼されている古い技術
- モバイルでPKI？
  - 新しいデバイスにおけるPKIの実装状況



はじめに

Do you know VeriSign ?

ベリサインといえば...

ノートンに生まれ変わる”信頼の証”

「ベリサインシール」は2012年4月に「ノートンセキュアドシール」に自動的に切り替わります。

- 2010年8月に日本ベリサインは米国シマンテックグループの一員になりました。
- その一環としてブランドが融合します。
- 新しいシールは、親しまれたチェックマークサークル、形状、”powered by VeriSign”の文言を含み、ベリサインのブランド価値を維持継続したまま、消費者認知度の高いノートンブランドを融合したものです。
- 1日6.5億回表示されている、「信頼の証」としての実績はそのまま引き継がれます。

日本ベリサインが提供するセキュリティソリューション

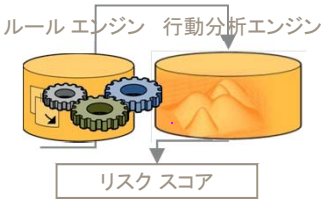
公開鍵基盤

強固な認証、暗号化、
電子署名が可能な
電子証明書の発行

Validation & ID Protection

複数種類のクレデンシャルを
選択可能な共有クラウドベース
の二要素認証ソリューション

オンライン詐欺検出サービス



リスクベースの認証、
及びソフトウェアベース
の詐欺検出

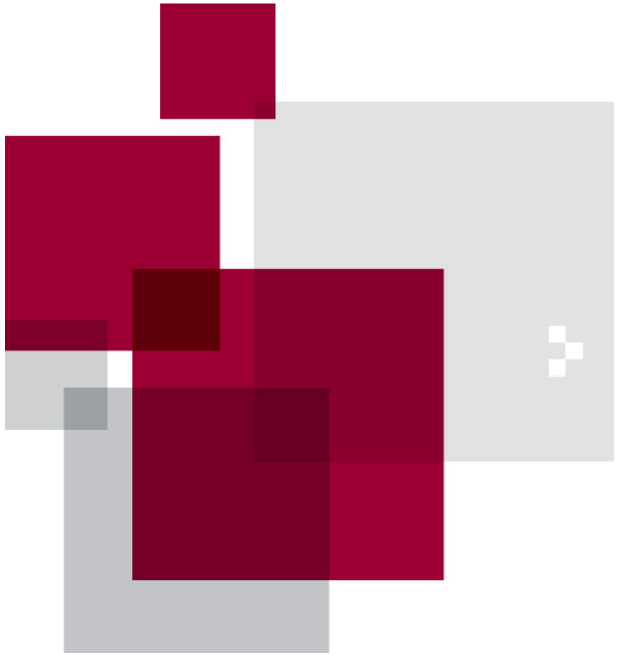
政府機関

電子商取引

企業

金融サービス

※米国VeriSignは、米国Symantecとは別事業を行う組織として存続しています。



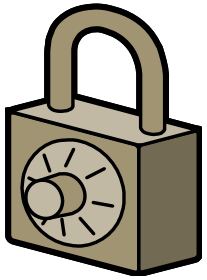
PKIってなに？

The Old Technologies

暗号の歴史小話(1/3)

奪う者と守る者との攻防の歴史

- 略奪者から財産を守る歴史
  - (残念ながら)人類は他人のモノを奪う生き物である
  - 自分の財産(家族、家畜、食糧、貨幣等)を守るためには？
    - 仲間を増やす
    - 武器をもつ
    - 柵や城壁をつくる
    - 扉や箱に錠前をかけて『鍵』で管理する



- 余談
  - ちなみに、財産の所有という概念がなかったら？
    - 人類の文明はここまで発展しなかったかも
  - あるいは、奪われる恐れがなかったら？
    - 江戸時代の日本の治安はよかった、らしい

暗号の歴史小話(2/3)

情報を伝えるという文明の発達

- 第三者から伝達情報を守る歴史
  - 価値のある情報の登場
    - 当事者間で有用な情報は、第三者にも有用である可能性が高い
  - 当事者間の有用な情報を安全に共有するためには？
    - 直接会って話す
    - 封をした書簡を信頼できる仲間に託す
    - 第三者が容易に解読できない情報に変換する⇒「暗号化」

暗号の歴史小話(3/3)

暗号化と解読の繰り返し

- 古典暗号
  - 換字式暗号
    - シーザー暗号
    - シャーロックホームズ「踊る人形」

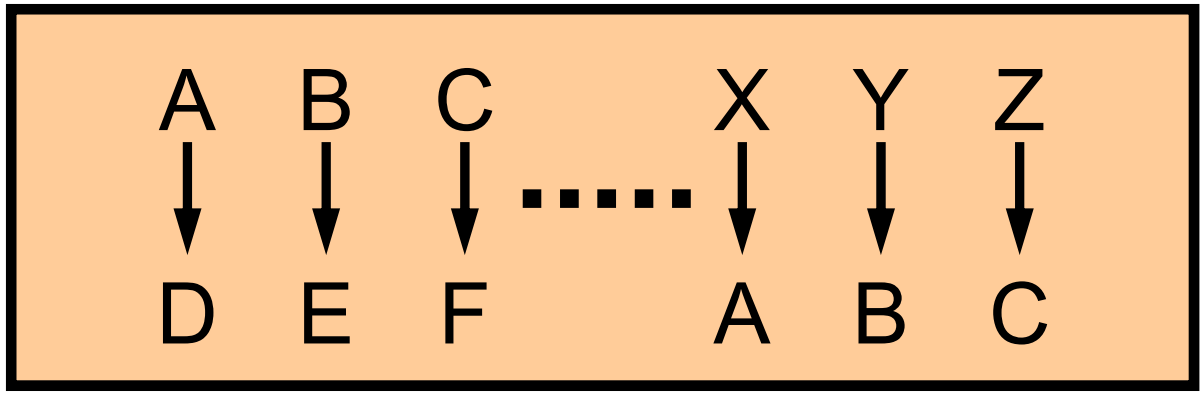
- 近代暗号
  - 機械式暗号
    - エニグマ暗号機
    - パープル暗号機(九七式欧文印字機)
- 現代暗号
  - 共通鍵暗号方式
    - ブロック暗号
  - 公開鍵暗号方式
    - RSA暗号

出展: Wikipedia – 暗号理論、換字式暗号

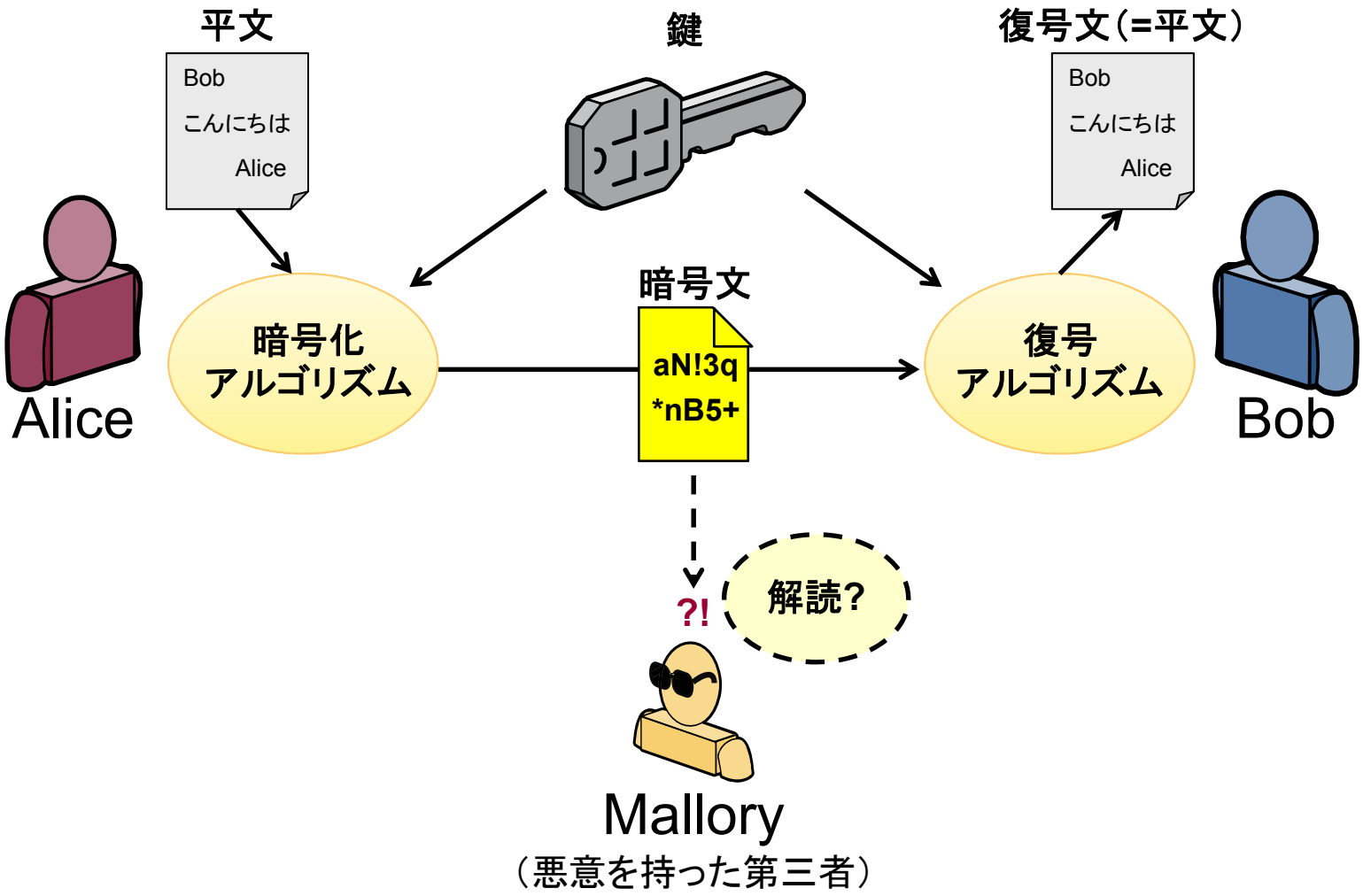
暗号技術とは

- 暗号技術とは
  - 文書やデータを、意図しない第三者に理解不能な状態に変換する技術
  - 当事者には有用な文書やデータを暗号化することで、当事者以外にはその有用性を失わせることを期待するもの

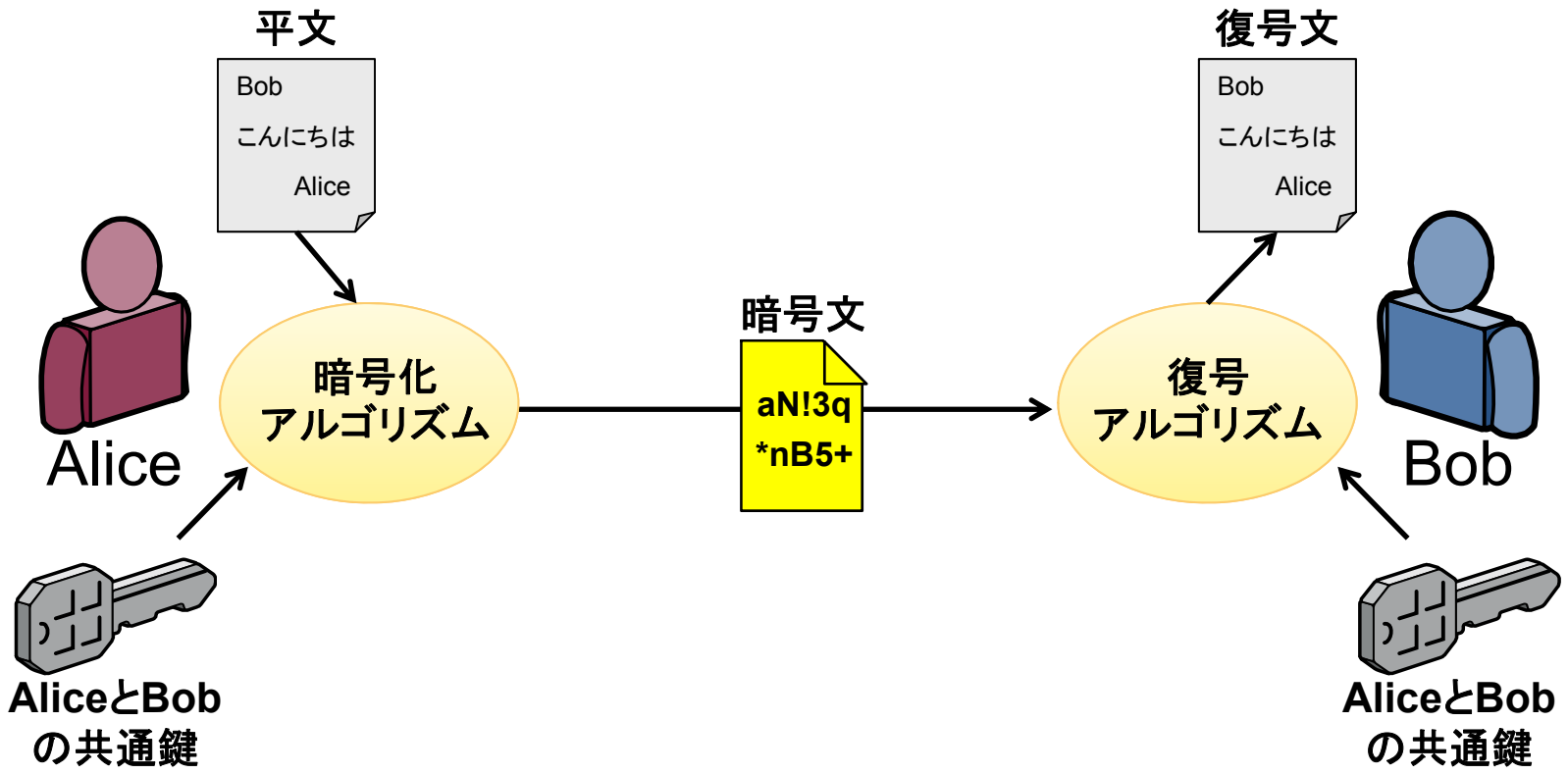
- シーザー暗号
  - 単純なシフト暗号（換字式暗号）
    - 知人に宛てた手紙を託す使者を信頼できなかった時に利用したといわれる



暗号技術の概念図と基本用語

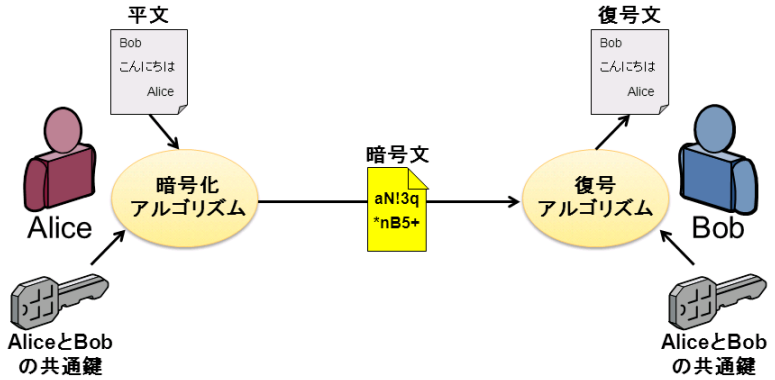


共通鍵暗号方式

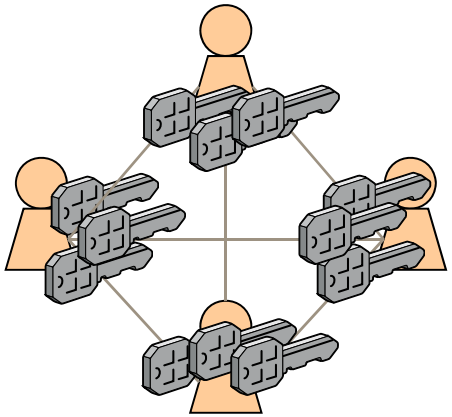

平文
Bob
こんにちは
Alice
暗号化
アルゴリズム
Alice
AliceとBob
の共通鍵
暗号文
aN!3q
*nB5+
復号文
Bob
こんにちは
Alice
復号
アルゴリズム
Bob
AliceとBob
の共通鍵

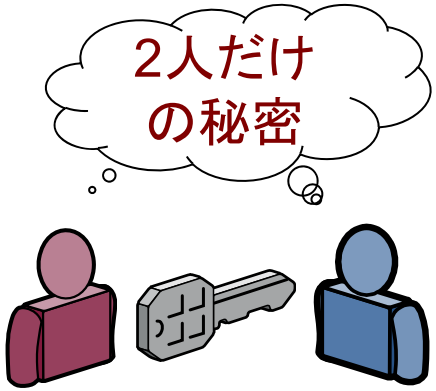
共通鍵暗号方式の特徴

- 特徴
  - 暗号化と復号を同一の鍵を用いて行う

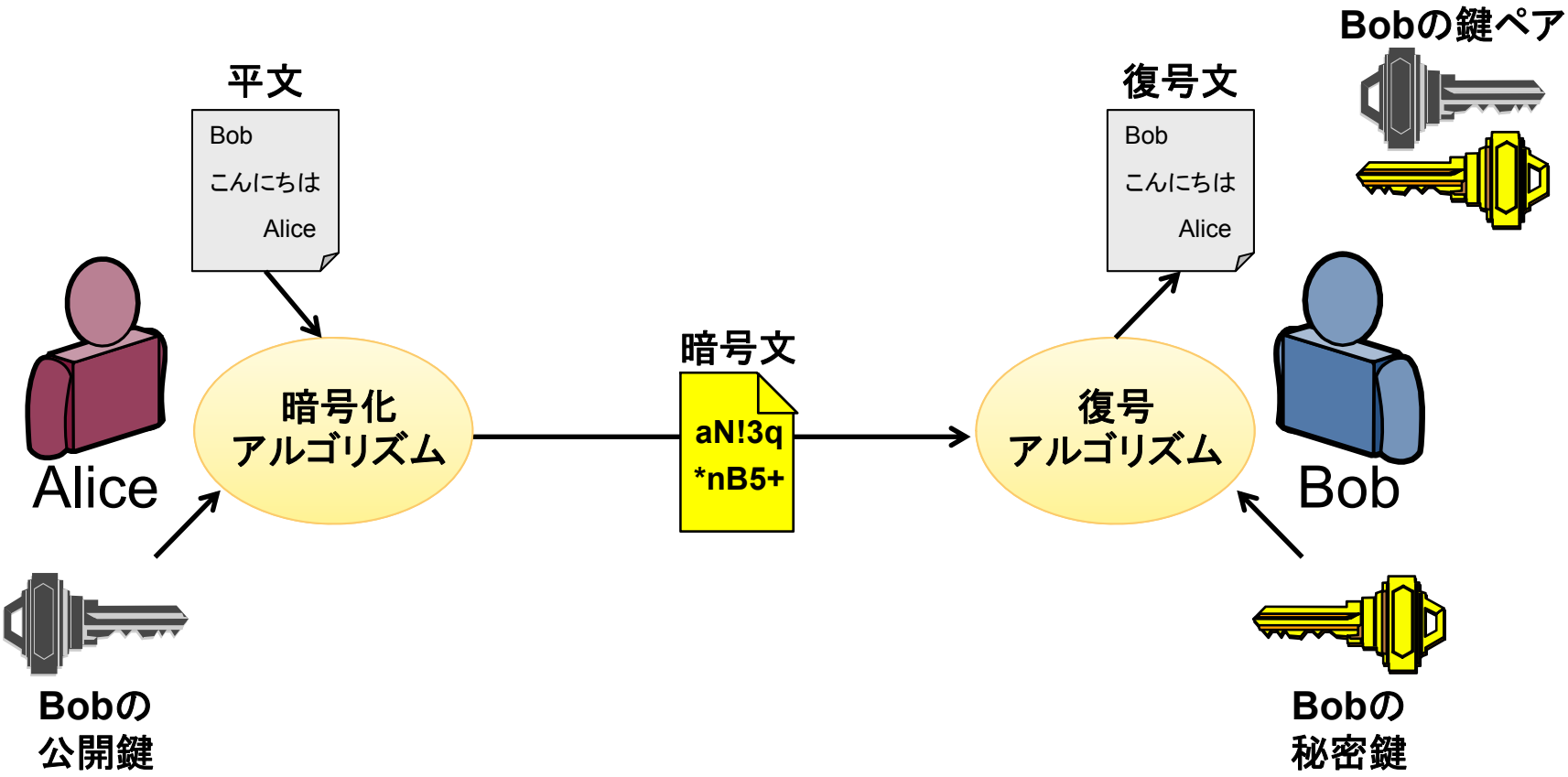


- 長所
  - 実装が容易であり、計算処理が速い
- 短所
  - 当事者間で共通鍵を安全に配布することが難しい
  - 当事者が増えることで管理すべき共通鍵の総数が膨大になる(=n*(n−1)/2)

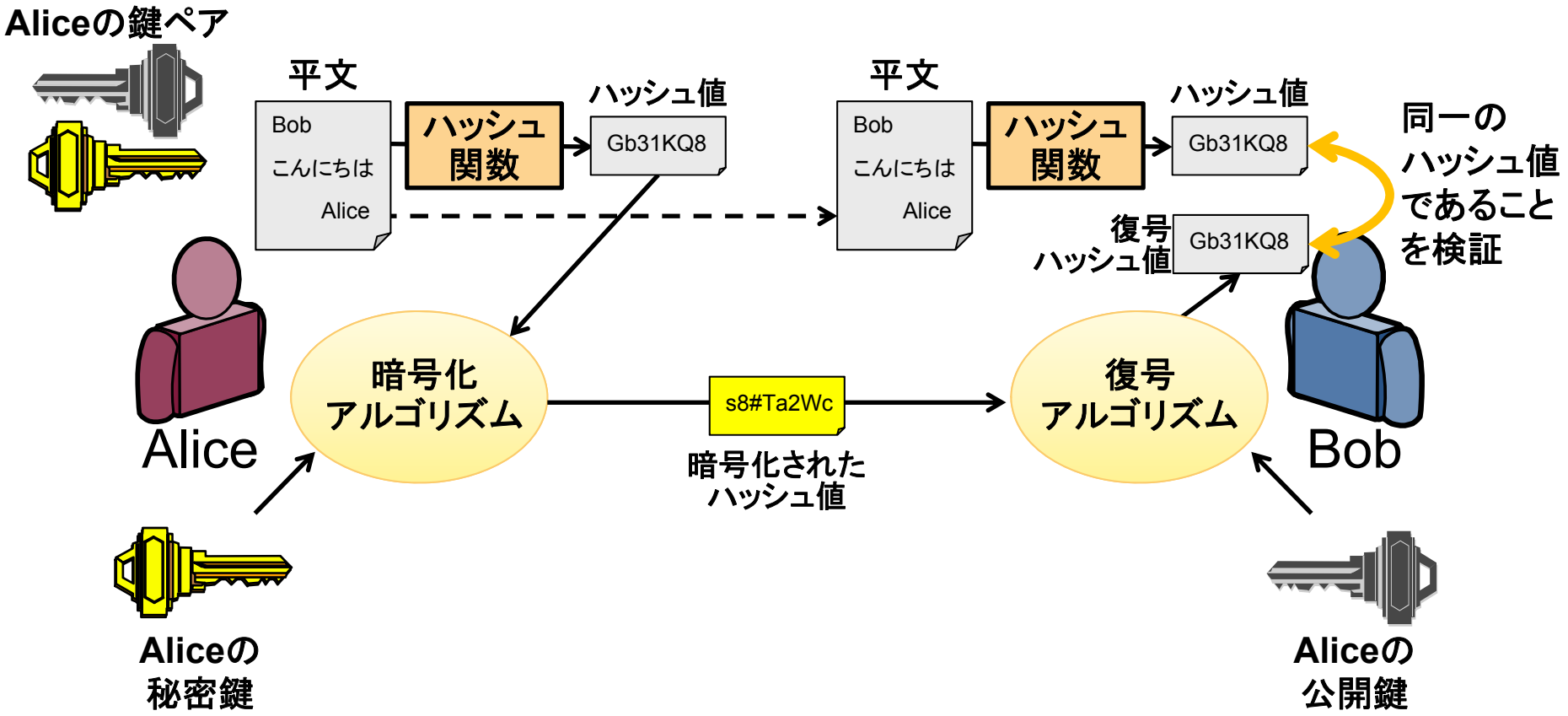




公開鍵暗号方式

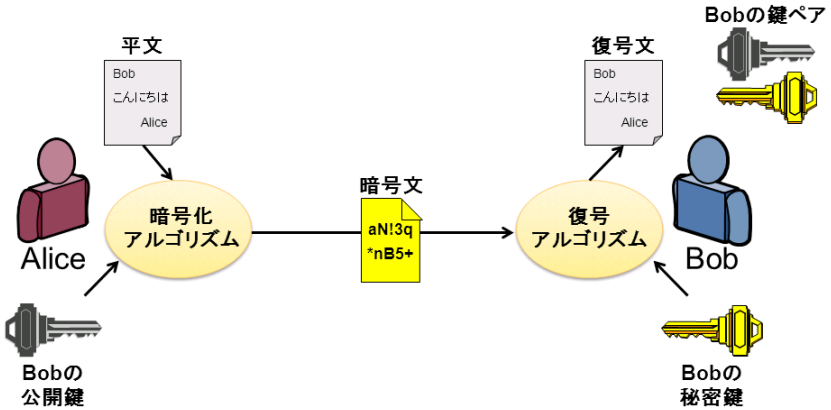

Bobの鍵ペア
平文
Bob
こんにちは
Alice
復号文
Bob
こんにちは
Alice
暗号文
aN!3q
*nB5+
暗号化
アルゴリズム
復号
アルゴリズム
Alice
Bob
Bobの
公開鍵
Bobの
秘密鍵

公開鍵暗号方式（応用：電子署名の場合）

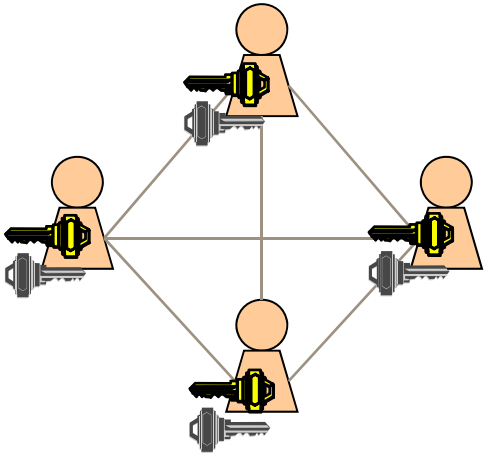


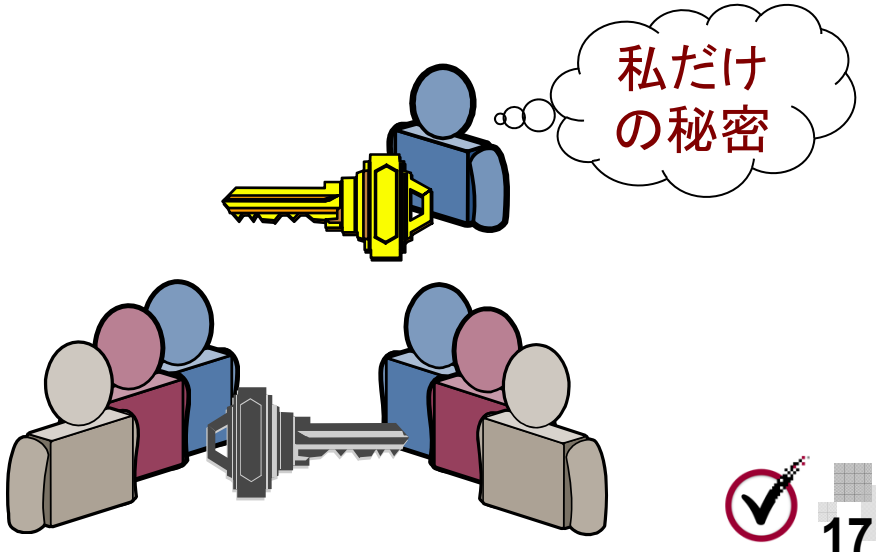
公開鍵暗号方式の特徴

- 特徴
  - 暗号化と復号を異なる鍵を用いて行う



- 長所
  - 公開鍵を公開して配布することができる
  - 共通鍵暗号方式に比べ、鍵の管理総数を減らせる(=2n)
- 短所
  - 計算速度時間が長い





公開鍵暗号方式登場までの経緯とその応用

- 安全な鍵交換方法の探求
  - Diffie-Hellman鍵交換方式の発表（1976年）
    - Bailey Whitfield DiffieとMartin Edward Hellman
    - 離散対数問題の難解性を根拠とした安全な共通鍵交換を実現したアルゴリズム

- 実用的なアルゴリズムの開発
  - RSA暗号の発表（1978年）
    - Ronald Linn RivestとAdi ShamirとLeonard Max Adleman
    - 素因数分解問題の難解性を根拠としたアルゴリズム
    - 公開鍵暗号方式の手法として現在でも広く利用されている

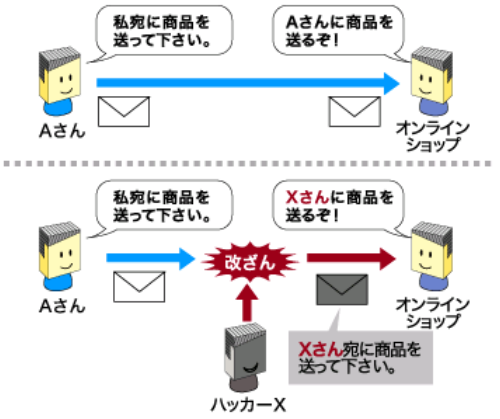
インターネットの普及

- インターネットとは
  - 世界中のネットワークが相互につながったパブリックネットワーク
  - 1990年のCERN（欧州原子核研究機構）によるHTML、HTTP、WWWの開発と、1995年のWindows 95の登場によって爆発的に普及

- インターネットの課題（4大脅威）
  - なりすまし
    - 通信相手を特定できない
  - 盗聴
    - 通信経路の途中で情報を盗み見られる
  - 改ざん
    - 通信経路の途中で情報を書き換えられる
  - 否認
    - 通信の結果を事後に否定する

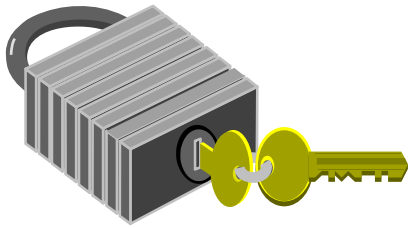
▪（なりすましの例）

▪（盗聴と改ざんの例）



課題への一般的な対応

- 一般的なセキュリティ対策
  - IDとパスワードを用いた認証
  - 共通鍵暗号方式による経路暗号



- これらの問題点
  - インターネットの脅威に対して、部分的にしか対応できない。

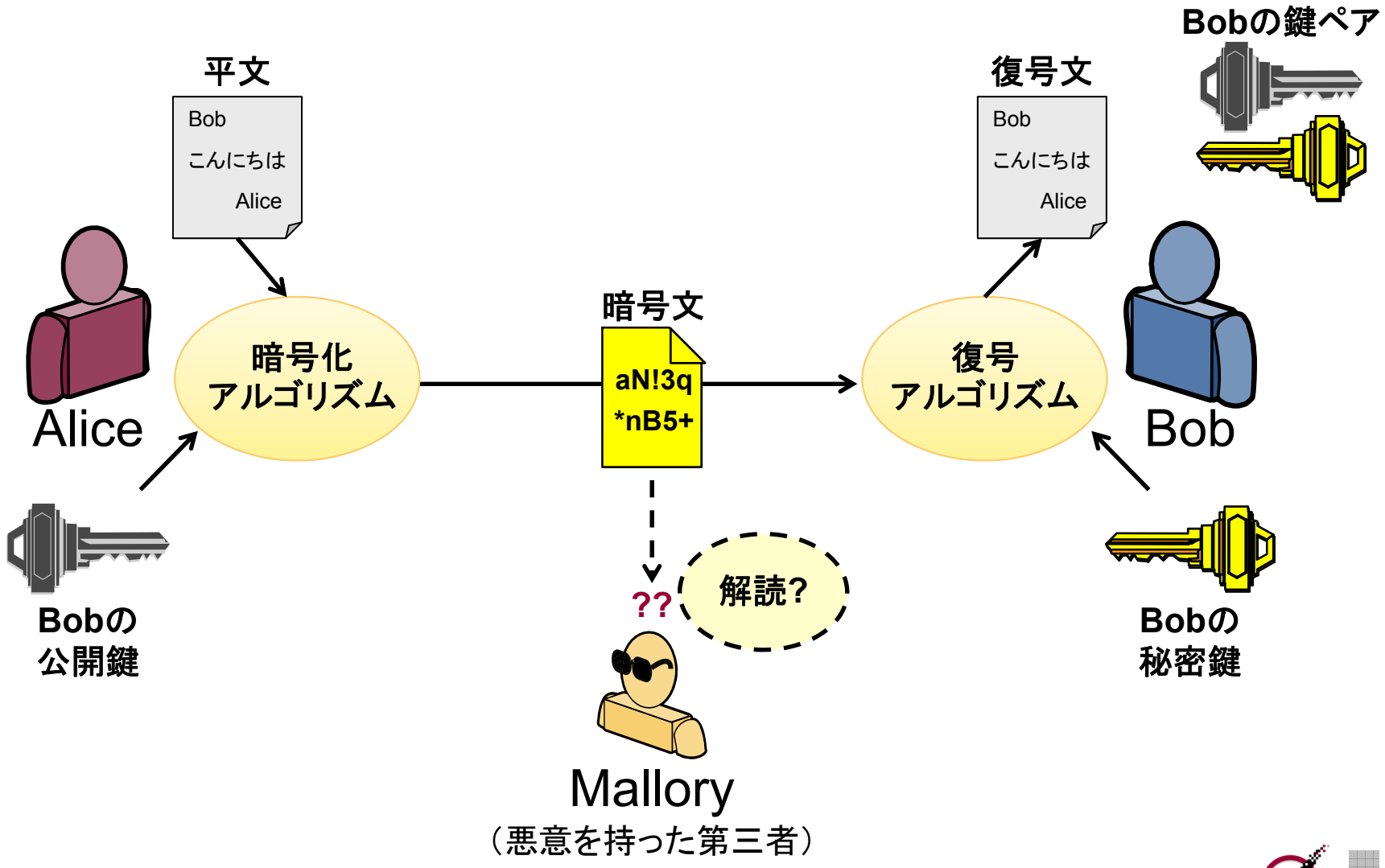
	なりすまし	盗聴	改ざん	否認
単純な認証	✓	×	×	×
共通鍵暗号方式	✓	✓	×	×

公開鍵暗号方式による課題の克服

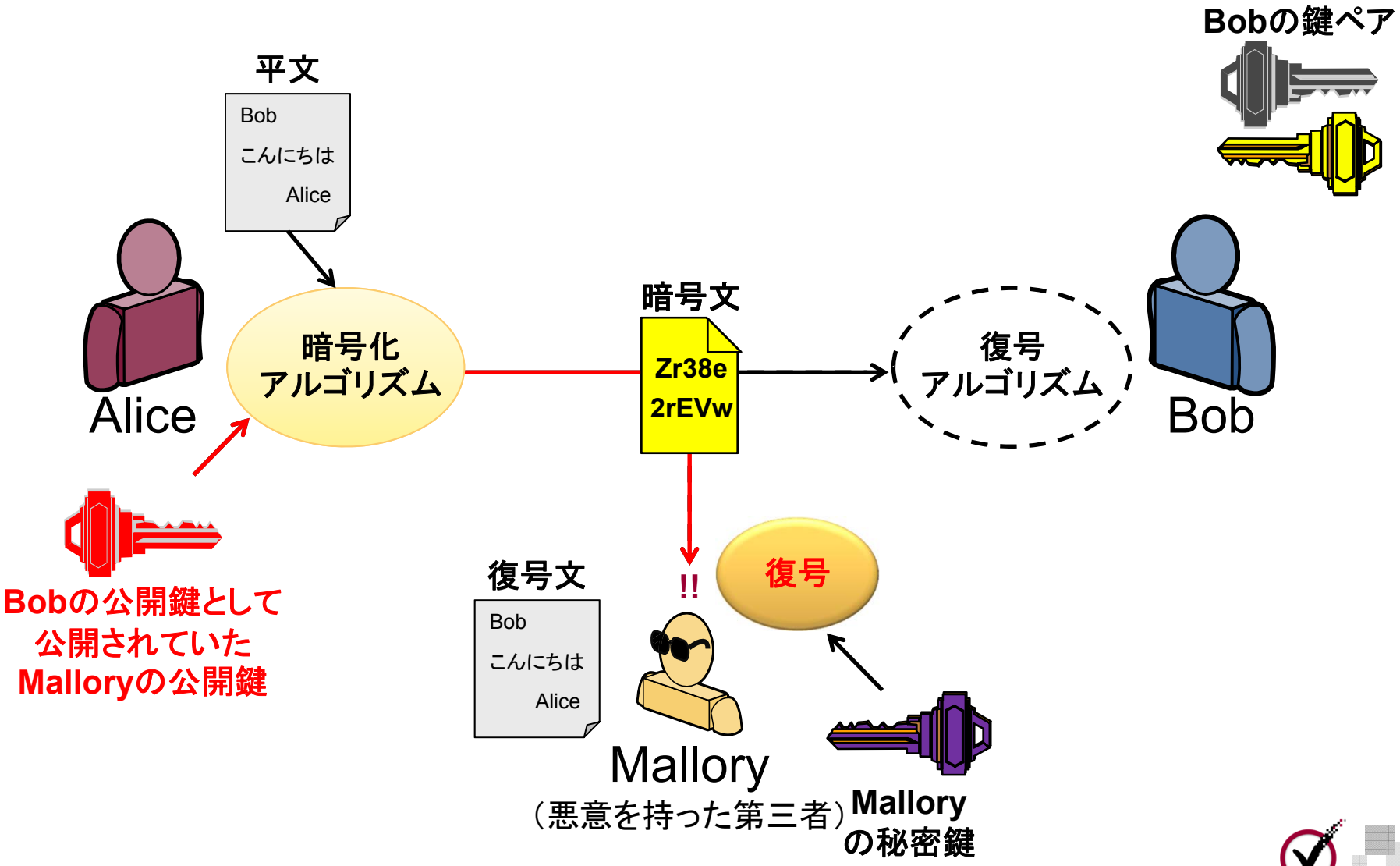
- 公開鍵暗号方式で実現できること
  - 公開鍵を用いた暗号化
    - 盗聴防止
  - 秘密鍵を用いた電子署名
    - なりすまし防止
    - 改ざん防止
    - 否認防止

	なりすまし	盗聴	改ざん	否認
単純な認証	✓	×	×	×
共通鍵暗号方式	✓	✓	×	×
公開鍵暗号方式	✓	✓	✓	✓

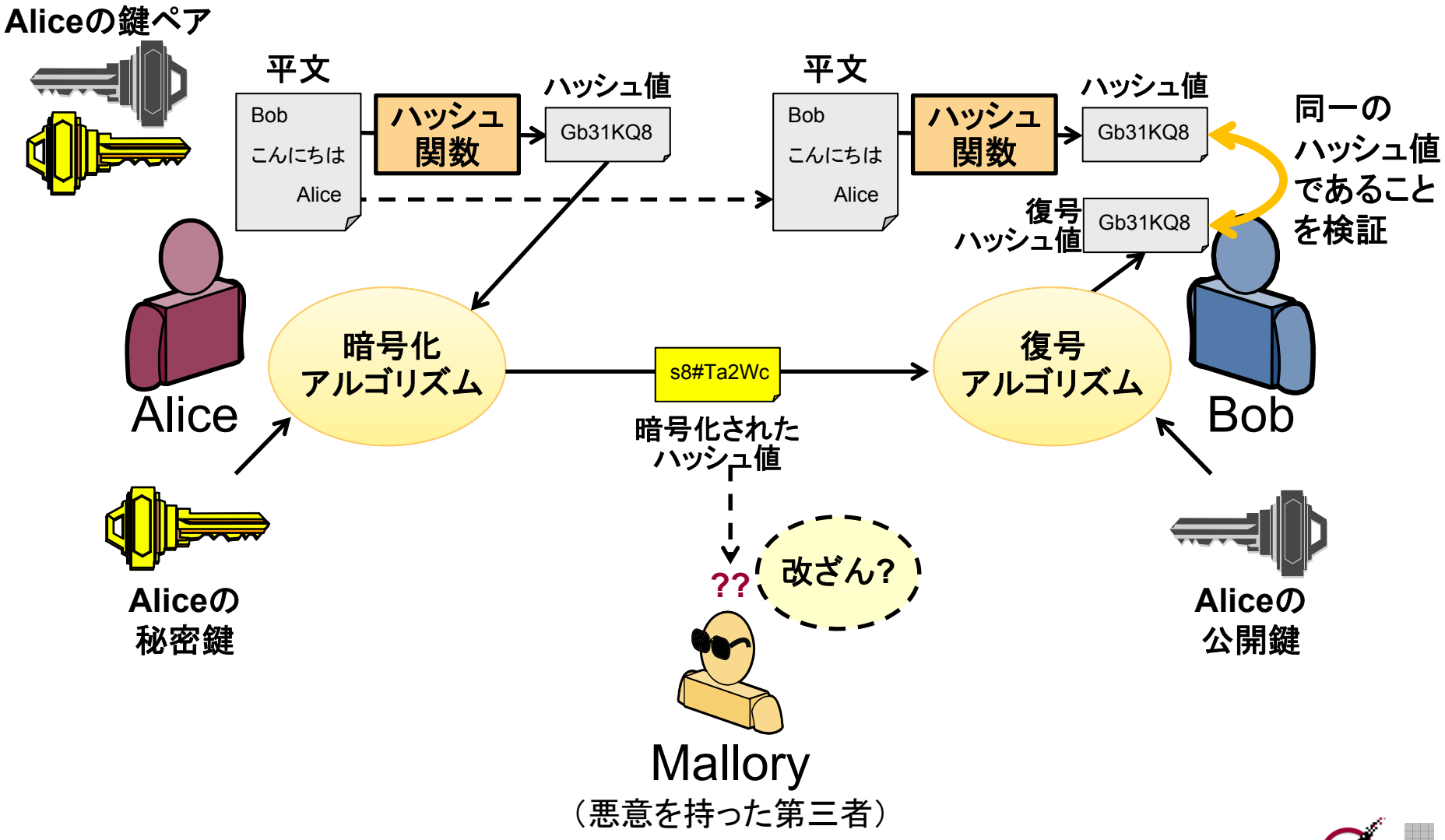
公開鍵暗号方式の問題点



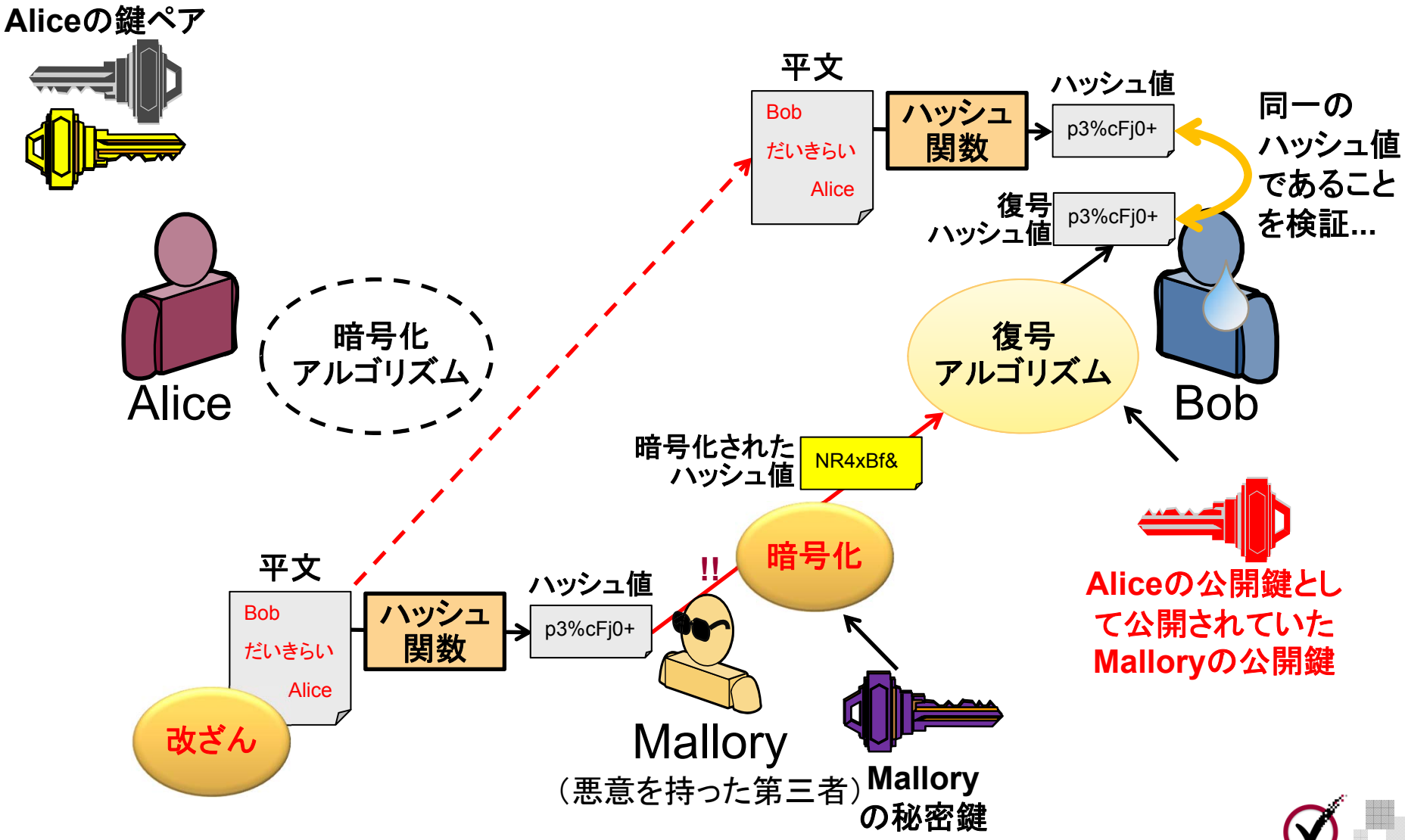
公開鍵暗号方式の問題点（暗号化の場合）



公開鍵暗号方式の問題点（電子署名の場合）



公開鍵暗号方式の問題点(電子署名の場合)



なにが問題なのか

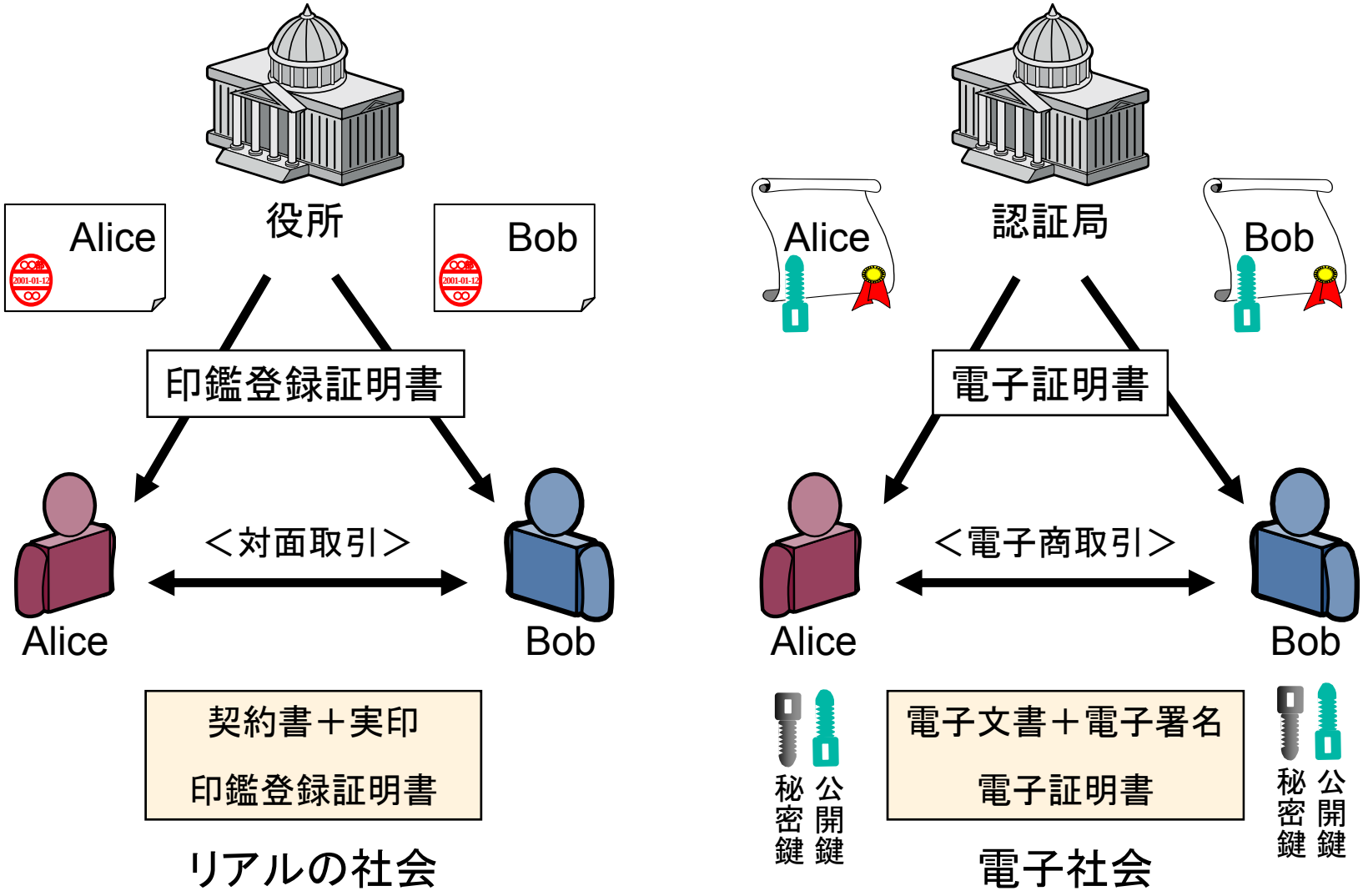
- 公開鍵暗号方式についておさらい
  - AliceからBobへ電子署名
    - Aliceは自身の秘密鍵で電子署名を作成、BobはAliceの公開鍵で検証
  - AliceからBobへ暗号化
    - AliceはBobの公開鍵で暗号化、Bobは自身の秘密鍵で検証（復号）
- 公開鍵暗号方式の運用に求められるもの
  - 電子署名
    - 受信者は、署名データの送信者の『正しい公開鍵』を必要とする。
  - 暗号化
    - 送信者は、暗号データの受信者の『正しい公開鍵』を必要とする。

公開鍵の所有者を証明できる仕組みが必要

PKI：公開鍵基盤

- PKI
  - Public Key Infrastructureの略
  - 公開鍵の所有者を証明するための仕組み
  - 『認証局（Certificate Authority）』と『電子証明書（Digital Certificate）』で構成
- 基本的な考え方
  - 市役所と印鑑登録証明書
    - 信頼できる市役所が印鑑登録証明書を発行するもの
      ⇒　信頼できる認証局が電子証明書を発行する
    - 印鑑登録証明書は印影とその所有者を結びつける
      ⇒　電子証明書は公開鍵と鍵の所有者を結びつける
    - 市役所から印鑑登録証明書を取得すると、相手の正しい印影を確認できる
      ⇒　認証局から電子証明書を取得すると、相手の正しい公開鍵を取得できる

役所と認証局の類似点


役所
Alice
Bob
印鑑登録証明書
＜対面取引＞
Alice
Bob
契約書＋実印
印鑑登録証明書
リアルの社会
認証局
Alice
Bob
電子証明書
＜電子商取引＞
Alice
Bob
秘密鍵
公開鍵
電子文書＋電子署名
電子証明書
秘密鍵
公開鍵
電子社会

PKIの標準技術

- X.509
  - 国際電気通信連合（ITU-T）が策定した通信技術標準
- RFC5280
  - IETF（Internet Engineering Task Force）が策定したインターネット標準
- 電子証明書のプロファイル

X.509 バージョン番号	・・	X.509 のバージョン
電子証明書のシリアル番号	・・	電子証明書ごとのユニークな番号
署名方法（アルゴリズム名）	・・	電子証明書の署名方法
発行者（認証局）の名前	・・	電子証明書を発行した機関名（認証局）
有効期間	・・	この電子証明書の有効期間
発行先（所有者）の名前	・・	登録された公開鍵の所有者の名前
 発行先（所有者）の公開鍵	・・	登録された所有者の公開鍵
拡張（X.509 Ver3 のオプション）	・・	X.509 の拡張フィールド
発行者（認証局）による署名	・・	上記全項目に対して一括して施した電子署名

電子証明書の役割

- 印鑑登録証明書の役割
  - 印影が捺印されている、ということの意味
    - 『Aliceの印影』がある書類は、Aliceが作成（捺印）したものであることを証明する
- 電子証明書の役割
  - 電子署名されている、ということの意味
    - 『Aliceの電子証明書（に含まれる公開鍵）』で検証できる電子署名付きデータは、Aliceが作成（電子署名）したものであることを証明する
  - 暗号化されている、ということの意味
    - 『Aliceの電子証明書（に含まれる公開鍵）』で暗号化するデータは、Aliceしか解読（復号）することができないことを担保する

しかし、その電子証明書は本物？

電子証明書の証明

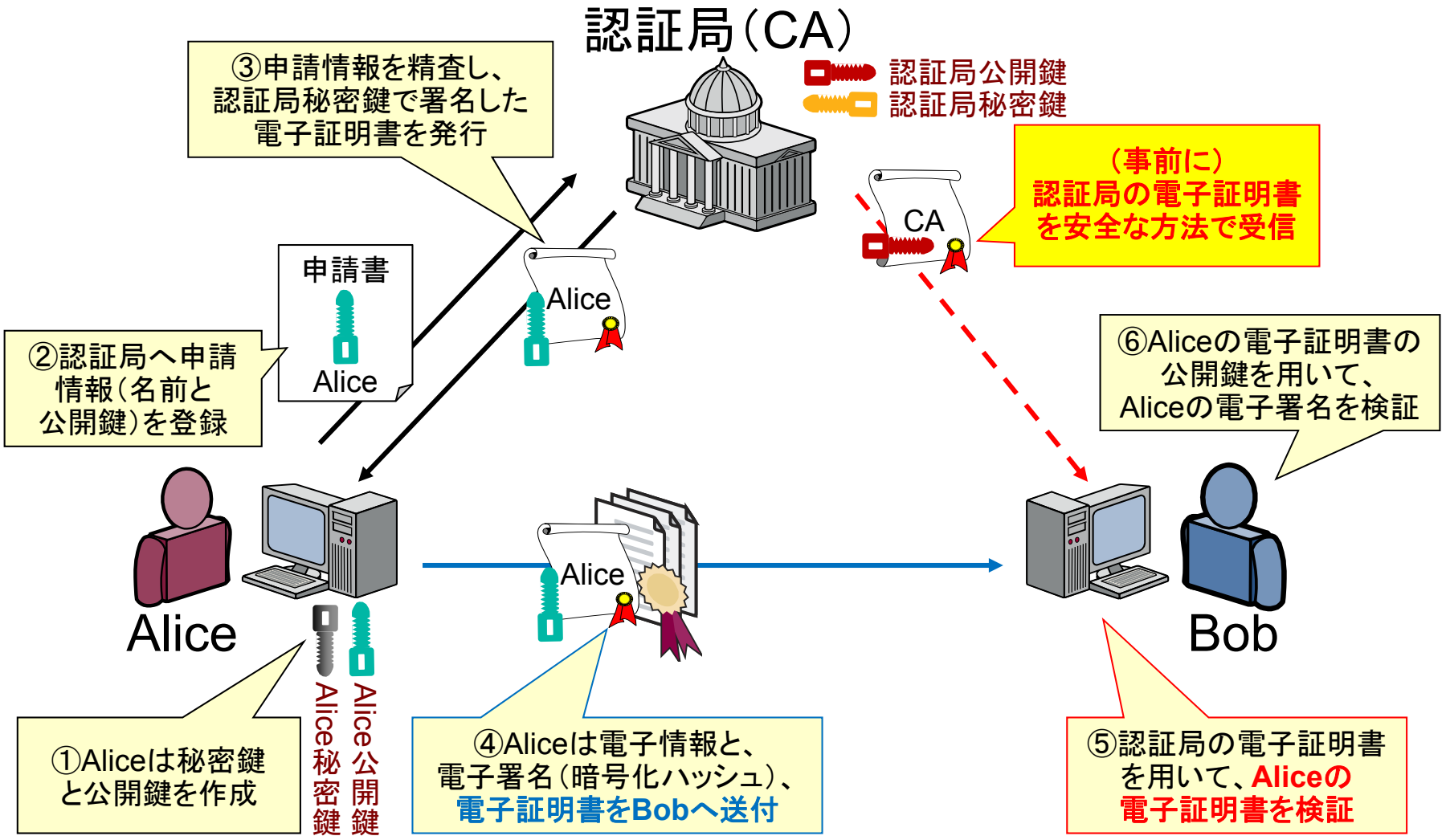
- 印鑑登録証明書の証明
  - 印鑑登録証明書には、『役所長（市長等）の記名』とその『押印』
    - 印鑑登録証明書が本物かどうか、役所長の印影をみて判断する。
- 電子証明書の証明
  - 電子証明書には、『認証局の名称』と『認証局による電子署名』が付与
    - 電子証明書が本物かどうか、電子署名を検証して判断する。

X.509 バージョン番号	・・	X.509 のバージョン
電子証明書のシリアル番号	・・	電子証明書ごとのユニークな番号
署名方法（アルゴリズム名）	・・	電子証明書の署名方法
発行者（認証局）の名前	・・	電子証明書を発行した機関名（認証局）
有効期間	・・	この電子証明書の有効期間
発行先（所有者）の名前	・・	登録された公開鍵の所有者の名前
 発行先（所有者）の公開鍵	・・	登録された所有者の公開鍵
拡張（X.509 Ver3 のオプション）	・・	X.509 の拡張フィールド
発行者（認証局）による署名	・・	上記全項目に対して一括して施した電子署名

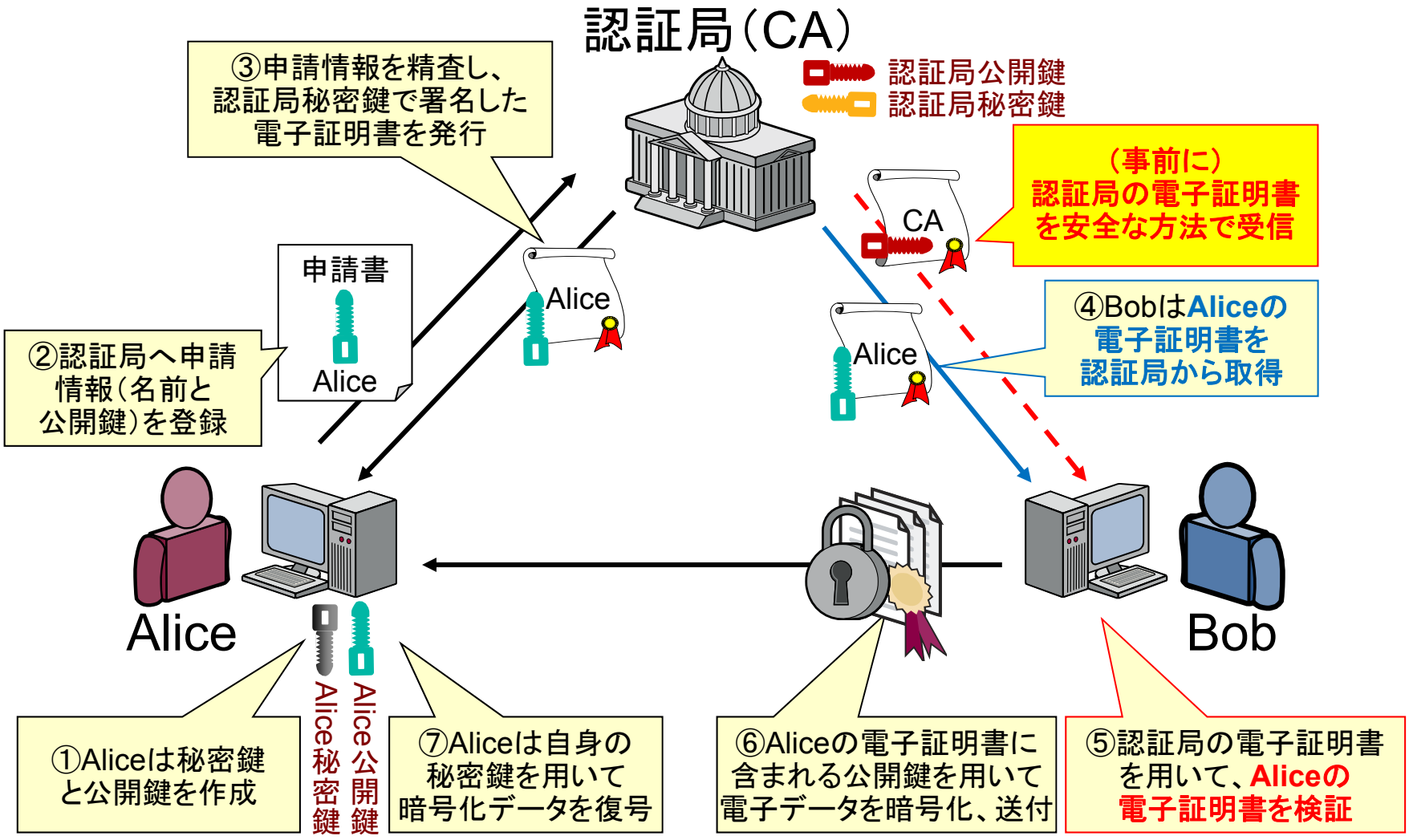
電子証明書の電子署名を検証

- 電子署名の検証に必要なものは
  - 署名者の公開鍵
    - （認証局で発行された）電子証明書に電子署名を付与したのは認証局
    - 検証には認証局の公開鍵が必要
    - 公開鍵とその鍵の所有者を結びつけるものは電子証明書
  - 『認証局の電子証明書』を入手する必要がある

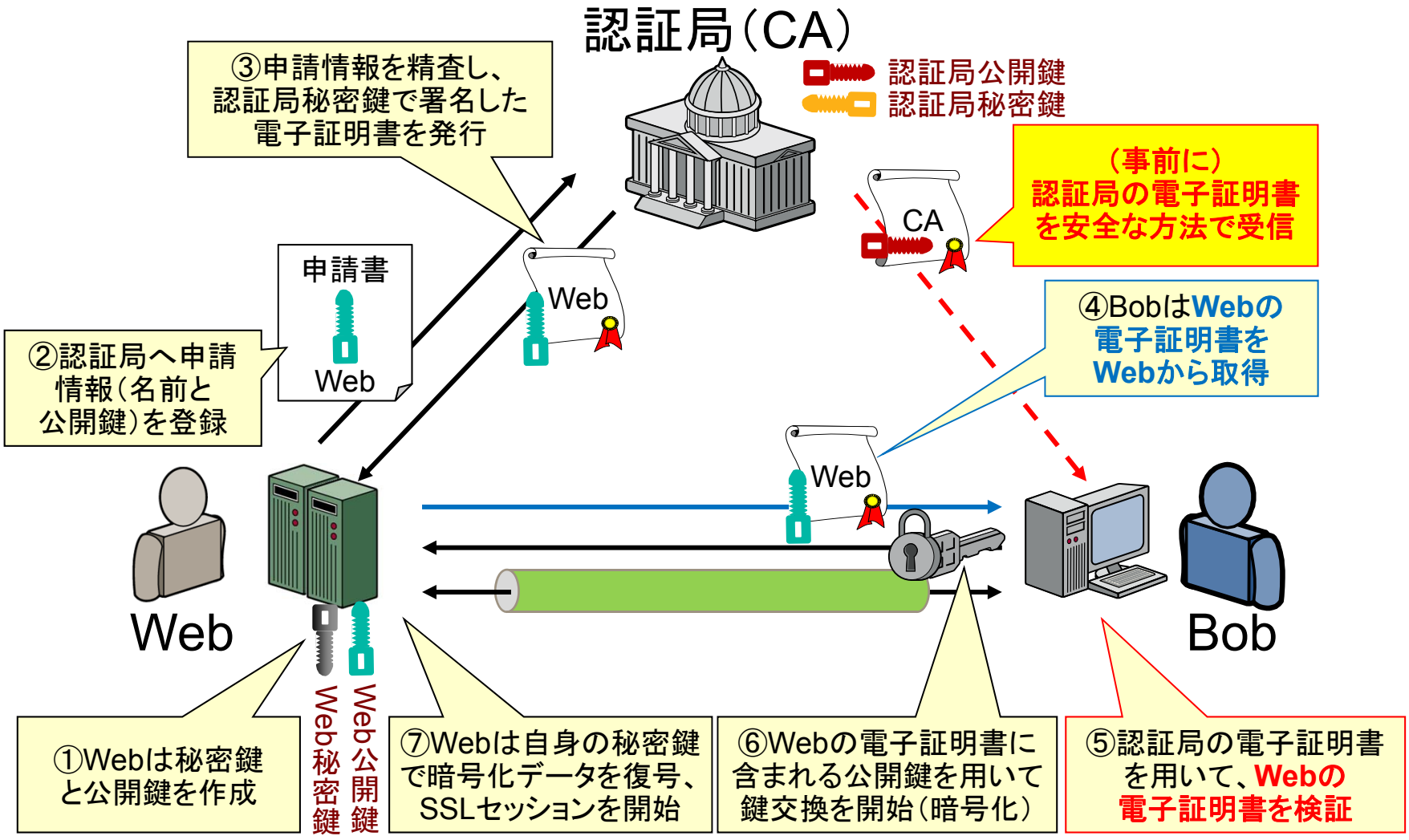
PKIの概念図（S/MIME署名：Alice→Bob）



PKIの概念図（S/MIME暗号化：Bob→Alice）

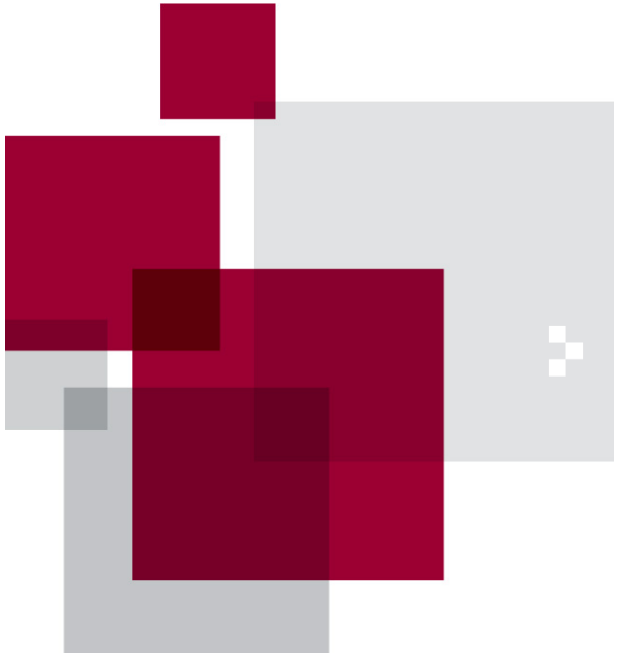


PKIの概念図（SSLセッション構築）



PKI：電子証明書と認証局（まとめ）

- PKIを構成する主なもの
  - 電子証明書
    - 電子証明書は、公開鍵とその所有者の結びつきを証明する
  - 認証局
    - 電子証明書発行要求の申請を精査し、電子証明書を発行する
- PKIを安全に保つための条件
  - （電子証明書を利用する）ユーザ
    - 自身の秘密鍵を安全に管理する
  - （電子証明書を発行する）認証局
    - 申請の精査を厳格に行う
    - 自身の証明書（認証局証明書）を適切に配布し、その秘密鍵を安全に管理する
- 余談
  - オレオレ証明書、DigiNotarの事件
  - 「小悪魔女子大生のサーバエンジニア日記」



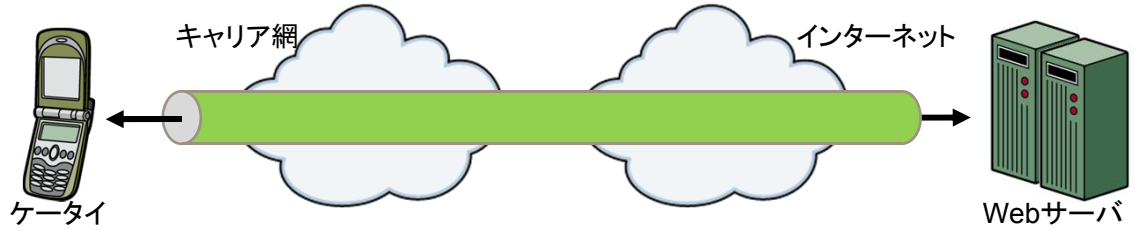
モバイルでPKI？

The New Devices

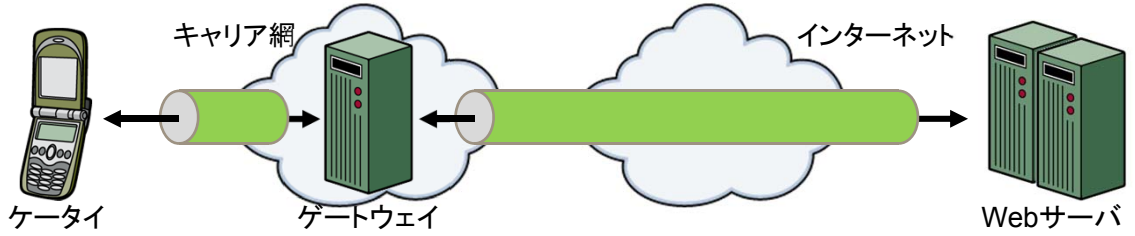
フィーチャーフォンとPKI（1/2）

iモードなどのインターネット接続サービスから

- 各キャリアのインターネット接続サービス（1999年）
  - iモード、EZweb、J-スカイ
    - 信頼された認証局証明書のプリインストール
    - SSLを用いた暗号化通信（HTTPS）の実現（サーバ認証）
- 余談
  - S社のSSLゲートウェイ（2011年6月末に廃止）
    - SSL通信は、端末-Webサーバ間が直接接続することが前提だが…



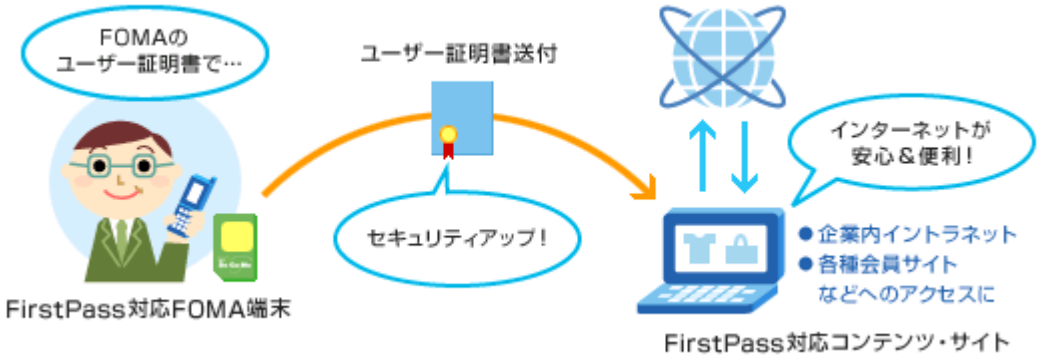
    - キャリア網のなかのゲートウェイで一度暗号が復号されていた



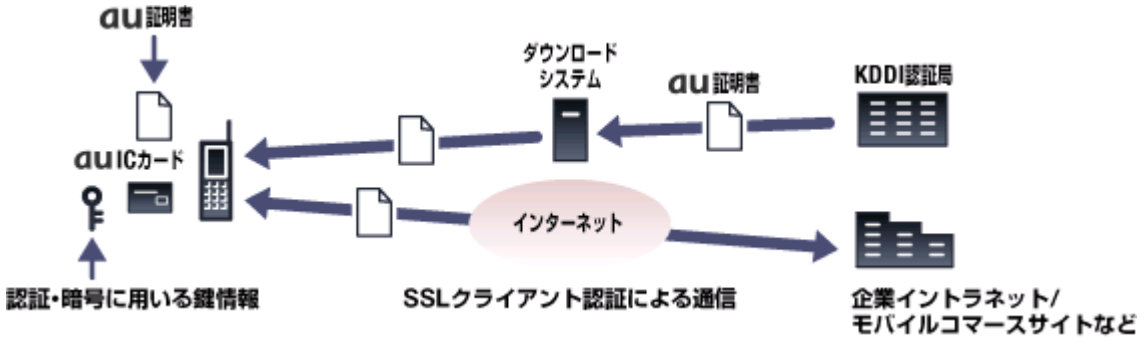
フィーチャーフォンとPKI（2/2）

ケータイ向けユーザ電子証明書

- （最強な）電子証明書　：『SIMに証明書を格納』
  - NTTドコモ：FirstPass



  - au（KDDI）：Security Pass（au証明書）

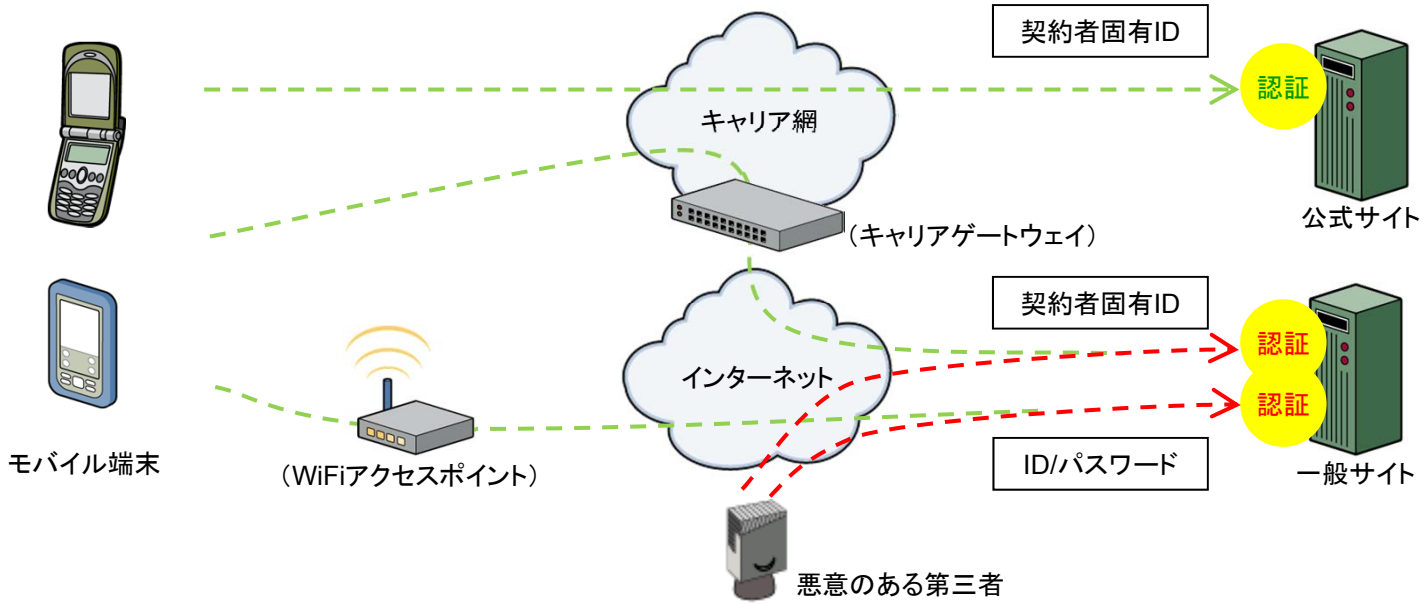


出展: http://www.nttdocomo.co.jp/service/safety/firstpass/
http://www.kddi.com/business/security_pass/

モバイル端末からの認証方式の考察(1/2)

従来の認証手法

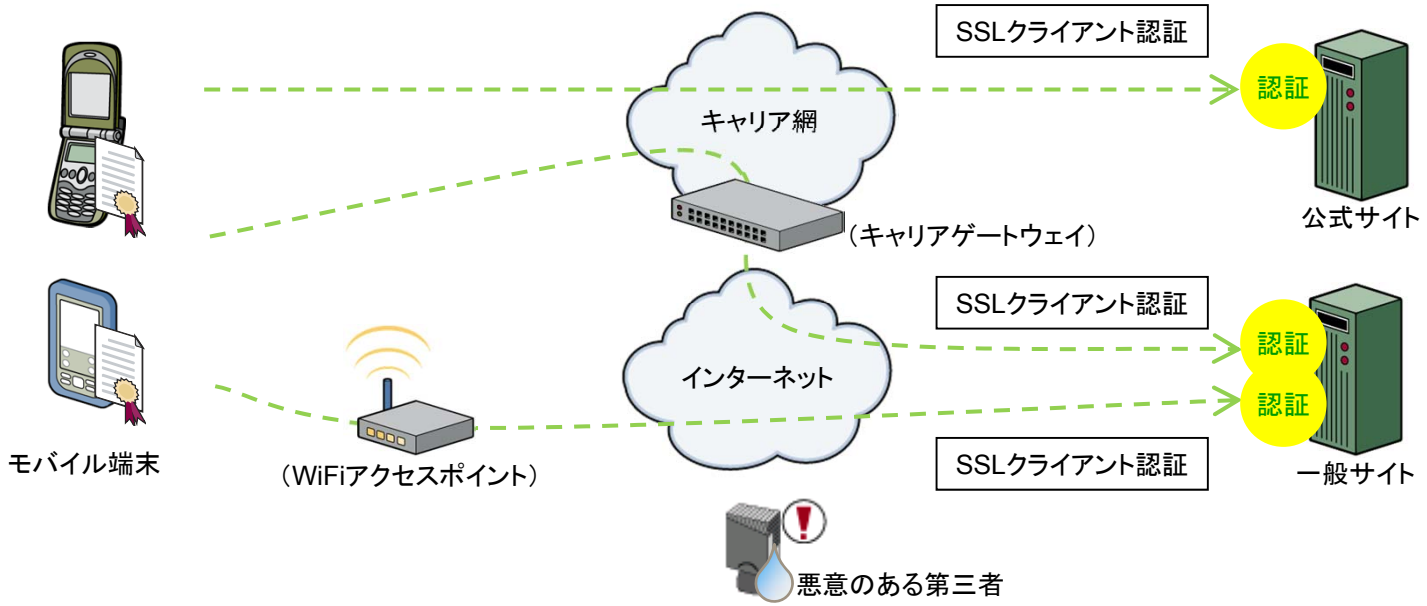
- 契約者固有ID
  - 主に公式サイトで利用された手法
- ID/パスワード
  - PC等でも広く利用されている汎用的な手法、だが…
    - キーボードがあるPCと違い、モバイル端末では一般的に入力が煩わしい



モバイル端末からの認証方式の考察(2/2)

モバイル端末こそ

- SSLクライアント認証
  - 簡易な操作性
  - 複雑なパスワードの記憶をユーザに求めない
  - なりすましは現実的に不可能
  - SIMのコピーが不可である限り、証明書のコピーも不可



突然ですが、実習です（※通信が発生します）

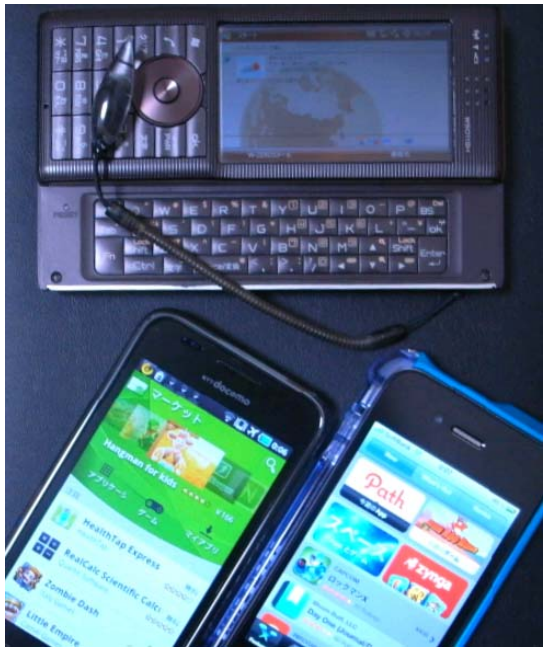
ケータイ向け電子証明書を取得して、SSLクライアント認証を試してみましょう！

- フィーチャーフォン限定
  - FirstPassの取得（NTTドコモ）
    - 取得：「iモードメニュー」 →「ユーザ証明書操作」
    - 取得後の確認：「各種設定」→「アプリケーション通信設定」→「証明書」
  - Security Passの取得（KDDI）
    - 取得：http://au-spdl.kddi.jp/spdl/reception →「au証明書ダウンロード」
      （ http://bit.ly/xkPXeP ）
    - 取得後の確認：「プライバシー/制限」→「証明書設定」→「証明書表示」
  - ソフトバンク
    - キャリア公式の証明書サービスがありません…。
  - SSLクライアント認証を試してみる！
    - https://client-auth.verisign.co.jp/
      （ http://bit.ly/ye80dJ ）

次はスマートフォン

その前に

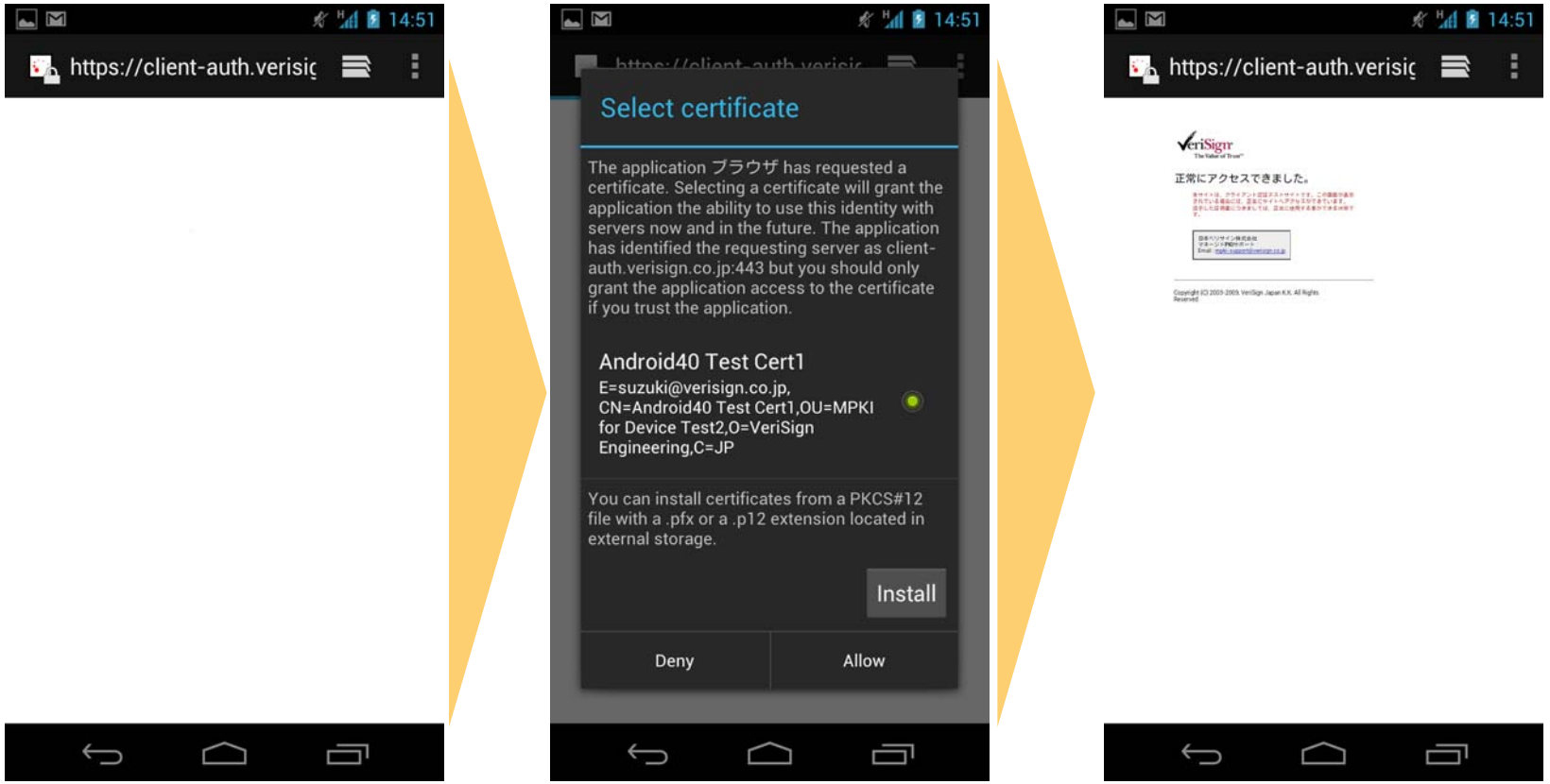
- 携帯電話の区分
  - ベーシックフォン、フィーチャーフォン、スマートフォン
- スマートフォンってなに？
  - PDA（携帯情報端末）から発展した、常時通信可能な小型PC
    - 劇的に端末の性能が向上、PC並みの機能をもち、かつ、常時接続が可能
  - OSメーカ主導の製品
    - 通信キャリアの差別化が困難
  - Jail Breakのリスク
    - 標準OSの挙動を示さない端末



Google Android OSとPKI

PKIの実装が遅かった

- Android OS4
  - Android OS 4からSSLクライアント認証を標準実装



Apple iOSとPKI

標準的なPKI用途の機能の実装をほぼ完了

- iOS5
  - iOS5からS/MIMEを標準実装

スマートフォンとPKI

サーバ認証はあたり前、クライアントサイドのPKI機能実装比較

- 実装の途上

	SSLクライアント認証	IPsec-VPN	EAP-TLS	S/MIME
Android2.2	×	×	✓	×
Android3.0	×	×	✓	×
Android4.0	✓	✓	✓	×
iOS4	✓	✓	✓	×
iOS5	✓	✓	✓	✓
Windows Mobile 6.1	✓	✓	✓	×
Windows Phone 7.5	✓	×	×	×

※本情報は、日本ベリサインによる独自調査結果（2011年12月現在）で、内容を保証するものではありません。仕様の詳細は各メーカにお問い合わせください。
資料に記載のある会社名、製品名等は、それぞれの会社の商号、登録商標または商品名称です。

- しかし、どのOSも
  - FirstPassやSecurity Passとの決定的で最大の違い
    ⇒ 『SIMに証明書を格納できない』（＝OSのセキュア領域に格納）
  - SIMはキャリアの所有物。今後に期待…

最後にスマートフォンの実習です（※通信が発生します）

テスト証明書をダウンロードし、SSLクライアント認証を試してみましょう！

- スマートフォン限定
  - ※注意事項※
    - Android OSは、証明書操作UIが十分に整っていません
  - テスト証明書の取得
    - PKCS#12形式のファイルをダウンロードします
      （ http://bit.ly/zAuWkD → 「デモ用テスト証明書のダウンロード」）
  - SSLクライアント認証を試してみる！
    - https://client-auth.verisign.co.jp/
      （ http://bit.ly/ye80dJ ）

- 会場のiOS5ユーザに限り
  - S/MIME用証明書を差し上げます
    - S/MIMEはメールアドレスを必要とします
    - 詳しくはセミナー終了後にご案内します

(※広告)Managed PKI for Device

現状の課題を補完するサービス

デバイス向け電子証明書の発行をクラウドモデルで提供

- 容易に電子証明書を取得
  - サーバを経由してほとんどのスマートフォンが対応している形式の証明書を発行
  - 管理者やエンドユーザに大掛かりなソフトウェア導入等の手間が不要
- さまざまなプラットフォームに対応
  - Webブラウザ向けと組み込み機器向けの2つのインターフェイスを用意
  - さまざまなプラットフォームに対応
- 安価な初期投資コスト
  - 鍵生成サーバとCA(IAとRAを組み合わせた認証局)はベリサインがホスティング

Q&A

質疑応答

Thank You

ありがとうございました