#11 Security, 暗号、認証局

Yutaka Yasuda, / 2003 spring term

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
- 技術的には両者は別のもの
  - むやみに危険と言ってみても何の役にも立たない
  - まずは理解することから

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

クラッカーが大手企業システムに侵入、セコムネットら10社から入札情報、社員個人情報が流出、情報を売買か？(1998)

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
  - 不正アクセス行為の禁止等に関する法律 2000年2月施行
- 一般に、
  - オープンネットに接続されたシステムの、
  - ソフトウェアの不備(バグ)を入り口として、
  - 相手のシステムに自分のやらせたい処理をさせる
- 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

7

システム不正侵入

- 原理的には
  - オープンネットにつながない事で止められる場合もあるが、、
  - 残念ながら、ソフトウェアの不備はなくならない
- 技術武装しかない
  - 防御、侵入検知など多方面で備える
  - いたちごっこになる
- それにしても現在のシステムは脆弱すぎ
  - オープンな文化で育った Unix / Internet の弱さ
- NRI など企業が多く乗り出しつつある

8

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
  - 電気や光の信号によって受け渡す
  - 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）
  - 閉鎖された通信路での対策は比較的簡単
  - インターネットのような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

9

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）
- 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
  - 複製されたことが判らない
  - 複製とオリジナルは完全に同一
    - つまり複製、オリジナルという概念そのものがない
- 傍受を防ぐことができない

10

暗号

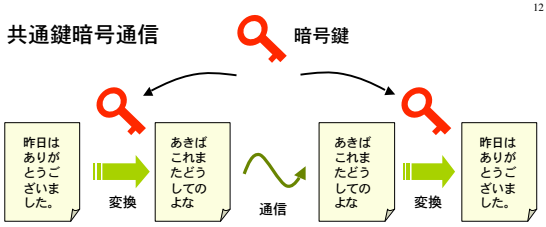
- では暗号化で対策
  - 傍受されても中身が判らないようにする
- 暗号
  - 通信では符号化するシステムと復号するシステムが異なる
  - 当事者以外に復号できなくする
  - 復号ルール（の一部）を秘密にする（「鍵」と呼ばれる場合もある）
  - データは読めるが、当事者以外には中身がわからない

11

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

12



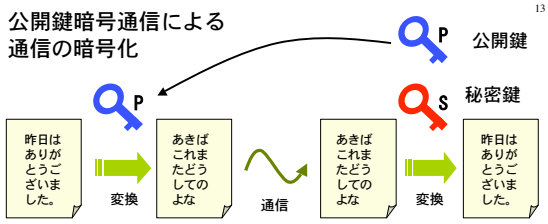
内容を相手だけに解けるように暗号化して相手に送る場合：

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

13

公開鍵暗号通信による通信の暗号化



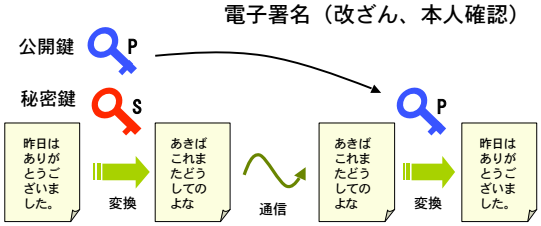
内容を読者だけに解けるように暗号化して相手に送る場合：

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）

14

公開鍵暗号通信による電子署名（改ざん、本人確認）

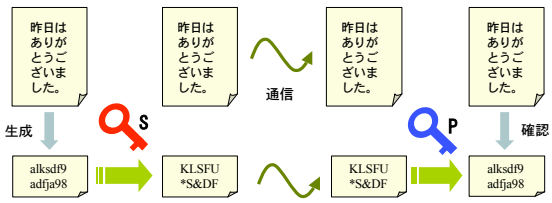


内容は公開だが発信者の確認ができる（なりすまし防止）

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

15

公開鍵暗号通信による電子署名（改ざん、本人確認）



実際には面倒くさいので全文ではなくダイジェストのみを署名として暗号化する（内容に秘匿性がないから）
ダイジェストは一方向性関数などで作る。MD5 etc...

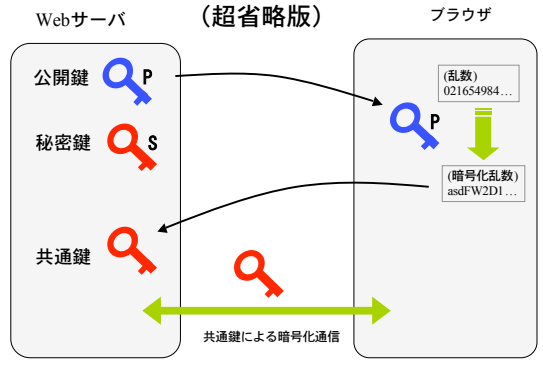
16

SSL：暗号通信の例

- SSL：ほとんどの Web 取引で利用
  - 通信経路の暗号化
- 実現手法
  - ブラウザ側でまず乱数を生成
  - サーバに接続し、サーバの公開鍵を得る
  - 乱数をサーバの公開鍵で暗号化
  - その乱数をタネに互いに共通鍵を共有
  - 実際の通信は共通鍵で行う
- 何故共通鍵？
  - 実は公開鍵暗号は計算量が大きい
  - 計算が膨大になることを利用して解読を防止している
  - 時限付きの暗号である

17

SSLによる暗号化手順（超省略版）



18

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えばよい」
    - Web で買う前に店舗に行って鍵を貰う？
    - 住民票申請をする前に窓口で鍵を貰う？
  - 電子商取引では通用しない
  - 本人確認の手段が必要

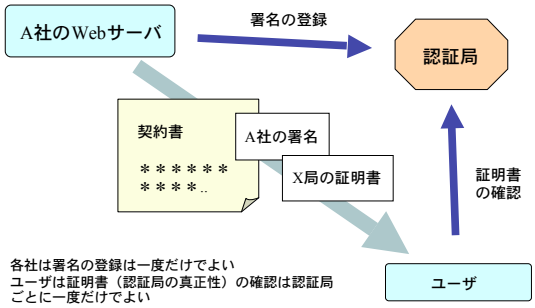
19

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
  - 印鑑証明書（印影＝申請者を保証）するのは役所
- 認証局ビジネス
  - 本人確認を実世界の手続きを経て行う
  - 証明書を売る（相手の身元情報に署名してあげる）
  - Verisign 等多数存在する

20

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

21

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
  - ユーザが一度認めた認証局はブラウザに登録され、その署名のある公開鍵は信用するようチェックが自動化されるに過ぎない
  - つまり最初の承認の裏書きはユーザに預けられている「この証明局を真生と認めますか？」
- しかしそんな警告を俺は見たことがない！
  - Verisign の情報が最初からブラウザに登録されているから
  - 自前証明書とVerisign証明書の価値の違いは？
  - Verisign が利益の源泉としている価値はどこに？

22

暗号

- 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）
- 問題点
  - 法規制の対象
  - 国によっては暗号は兵器と見なされる（た）
  - 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
- それでも普及は間違いない

23

安全性

- 安全性とは何か？
  - 道で撃たれないのはヨロイを着ているから？
- 総合的なリスクコントロールが重要
  - 法律・摘発・罰則・保険など （教育も重要）
  - 全て合わせてモータリゼーションを支える
  - コンピュータとネット化された社会でも同様
- 道路にセキュリティシステムはない
  - 現金輸送車はそれなりにガードされている
  - それは常識である（今は常識もない）
- 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