

再配布禁止

情報科学概論 第4回

情報の伝達と通信

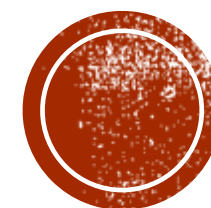
PART2

立教大学大学院 人工知能科学研究科

2023年5月8日

アンドラーデ ダニエル

andrade@rikkyo.ac.jp



本日の授業運用

■授業時間：

1. 「情報の伝達と通信」のPART 1 のおさらい
+ レポートの回答 (約10分)
2. 「情報の伝達と通信」のPART 2 (約50分)
3. 「計算の理論」 (約40分)

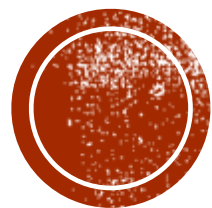


本日の授業運用

授業の運用：

- 「補足」のスライドは参考のために加えている。時間の都合で（あまり）説明しない予定。
- 出現している企業名はあくまでも例だけであり、企業への評価ではない。
- 授業中、ChatやSlackが見えない可能性がありますので、
キリのいいところで質問にまとめて答えます。
スライド上では「質問タイム」で表示します。
- 「質問タイム」ではChatや音声で質問をお願いします。
- 今回はBreakout Roomありません。
- 授業に関する意見・要望はお気軽にご連絡をお願いします。
(Slackや私のメールアドレス (andrade@rikkyo.ac.jp))に)





PART1のおさらい

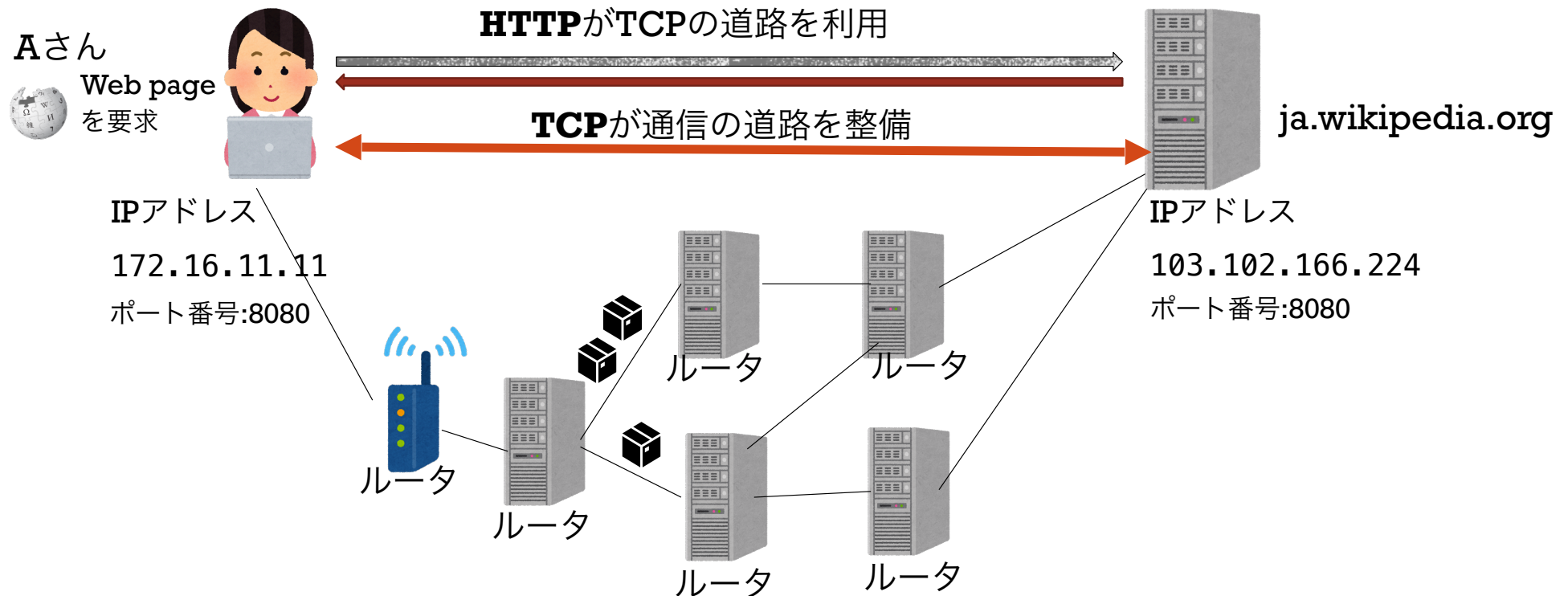
+

レポート課題の回答

インターネットにおける通信

PART1のおさらい

- インターネットに接続しているすべての機器には一意的なIPアドレスが割り当てられている。
- TCP/IPのProtocol群によって、仮想的な通信通路が整備され、Web pageのアクセスなどが可能になっている。



レポート課題

インターネットの仕込み

課題：

IPアドレスとMACアドレスの共通点と違いを思い出して、
それぞれの発行者を書いてください。



レポート課題

インターネットの仕組み

解答：

パソコンのWifi接続機のMACアドレスがその接続機のメーカーに発行された。

IPアドレスがWifiの接続されているルータ、またはそのルータの接続されているInternet Service Provider (ISP)に発行されている。

補足・おさらい：

MACアドレス： 一意的かつ変わりはない。

IPアドレス： 一意的だが、変りはある。



レポート課題

インターネットの仕組み

補足（２）：

テザリングや家のWifiでは「**Private IPアドレス**」がある。

実際には各ルータが「**192.168**」で始まる**Private IP**アドレスを発行し、インターネットで利用可能な**Public IP**アドレスに変更する。

今まで説明したIPアドレスは**Public IPアドレス**のことだった。

家のWifiルータを使った場合のIPアドレス

Private IP: 192.168.100.100 （重複可能性がある）

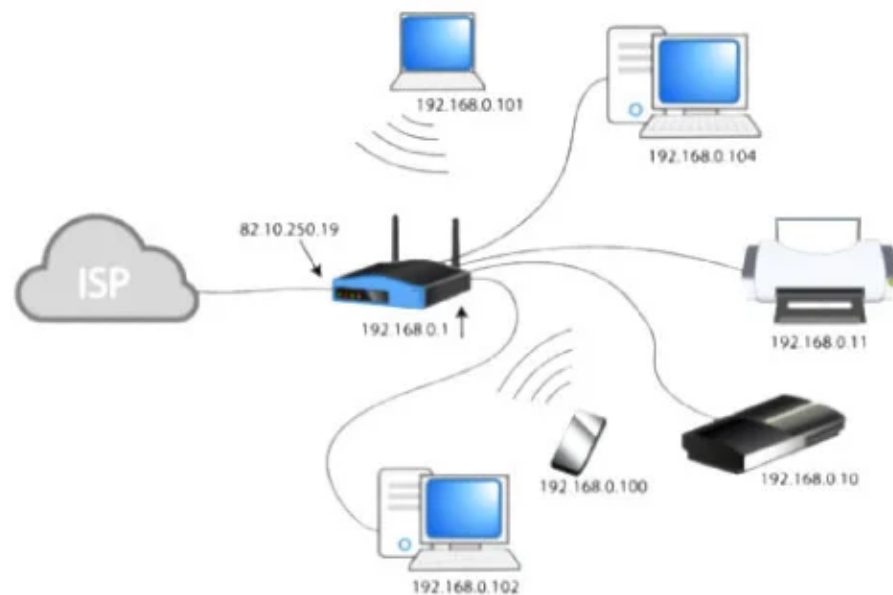
Public IP : 106.152.128.141 （一意的）

携帯テザリングを使った場合のIPアドレス

Private IP: 192.168.43.253

Public IP : 126.214.125.142

インターネットに接続するためには**Public IP**アドレスが必要
（**Private IP**アドレスはローカルしか利用されない。）



<https://whatismyipaddress.com/private-ip> より

レポート課題

インターネットの仕組み

補足（3）：

ほとんどの場合、**ISP**や組織に割り振られた(**Public**) IPアドレスは永久的ではなく、**DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol)で動的に決まる。

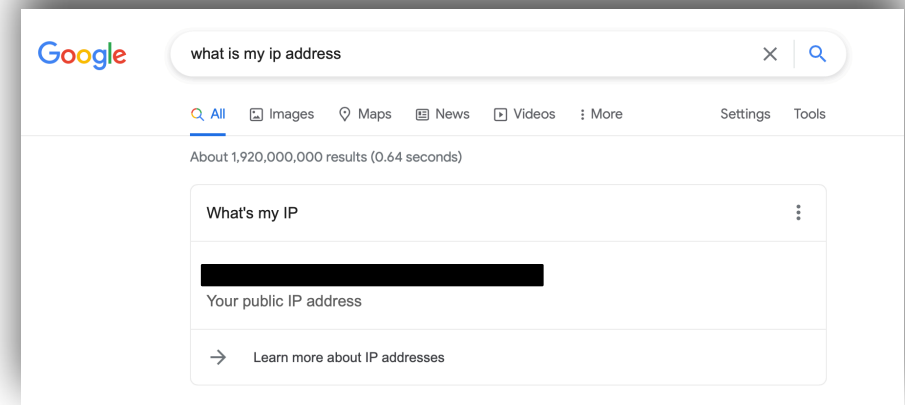
Public IPアドレスの調べ方：

googleの言語設定を「英語」にして、「what is my ip address」を検索してみてください。

(**Public**) のIPアドレスが表示されます。

今日と明日のIPアドレスは同じものですか。

(結果は**ISP**の方針によります。)



レポート課題

インターネットの仕込み

補足（4）：

「**ifconfig**」のコマンドで接続機器の**MAC**アドレスと**(Private) IP address**を調べることは可能。



通信におけるセキュリティ

PART1のおさらい

- 主な課題：
 - 秘密を守る： 盗聴による情報漏洩を防ぐ
 - 相手を認証する： なりすましからの防衛。
 - 元のデータを確実に受け取る： 改ざんを検知
- 対策方法： 暗号化と復号、 デジタル署名（今日のPART2）
- 暗号化の技術：
 - 共通鍵暗号： 同じパスワードで暗号化と復号
 - 公開鍵暗号： 次のページ



公開鍵暗号

PART1のおさらい

- 公開鍵暗号方式が**鍵のペア**を作成する。
 - 公開鍵 (public key) : 皆に知らせてよい。
 - 秘密鍵 (private key) : 秘密に保持する。
- 片方は暗号化のため、もう片方は復号のために利用される。応用によって役割が決まる。
- **公開鍵が分かったとしても、秘密鍵の推測が不可能。**
- 公開鍵で暗号化したデータは対応している秘密鍵でしか復元できない。
- よく利用されている公開鍵暗号方式：RSA, DSA
- 応用の例：**秘密文書の暗号化**
 - 秘密鍵：復号用
 - 公開鍵：暗号化用
 - AさんがRSAで鍵のペアを作成し、公開鍵を友達に渡す。友達がAさん宛にメールを送る際にはAさんの公開鍵を利用して、メールを暗号化する。効果：Aさんしか復号できない。他の友達も復号はできない。
- 他の応用例：**デジタル署名**（HTTPSやSSHで利用されている）



公開鍵暗号

PART1のおさらい

公開鍵暗号方式によって作成した鍵のペア：

錠



暗号化用の鍵

(例えば、公開鍵)

鍵



復号用の鍵

(例えば、秘密鍵)

暗号化



暗号化用の鍵

(例えば：公開鍵)

公開鍵暗号方式の
アルゴリズム



暗号化した文書

復号



復号用の鍵

(例えば：秘密鍵)

公開鍵暗号方式の
アルゴリズム



平文の文書



レポート課題の回答

公開鍵暗号

課題

AさんがBさんに自分の公開鍵をメールで送る。Bさんが受け取った公開鍵で社内の機密文書を暗号化する。どなたがその暗号化した文書を復号できる。

Aさん、Bさん、第三者のCさん？

解答の例：

Aさんだけ

Aさんが自分の秘密鍵で文書を復号できます。

回答が正解になるための仮定：

公開鍵はO、公開鍵Oと対応している秘密鍵はHとする。

(1) 秘密鍵HはAさんしか持っていない。

(2) Bさんが受け取った公開鍵O' がAさんの送信した公開鍵Oと同じ。



レポート課題の回答

公開鍵暗号

回答の補足：

上記のテキストではBさんが確実にAさんの公開鍵を受け取ったとは書いてありません。

次のスライドの可能性もあります。



レポート課題の回答

公開鍵暗号

1.



秘密文書



Bさん

Zさんの公開鍵を受け取った。



Zさんが通信を傍受し、Aさんの公開鍵を自分の公開鍵と置き換える。
(すり替え)

Man in the
Middle
Attack

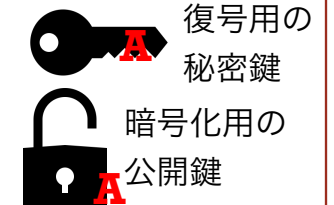


Aさん



復号用の
秘密鍵

暗号化用の
公開鍵



復号用の
秘密鍵

暗号化用の
公開鍵

2.



Bさん

暗号化した
秘密文書



通信を傍受し、
Bさんからの文書を自分の
秘密鍵で復号する。

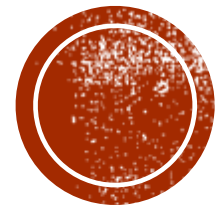


Aさん

Bさんが受け取った鍵はAさんのものだと思っているが、実際にはZさんの公開鍵で文書を暗号化してしまう。



質問タイム



情報の伝達と通信

本日の内容

通信におけるセキュリティ

- デジタル署名
- HTTPにおけるサイバー攻撃

参考文献： 第4章「情報の伝達と通信」 山口和紀, 情報第2版, 東京大学出版会(2017)



デジタル署名

デジタル署名によって、改ざんと成り済ましの防止が可能。

デジタル署名を実現するために以下の技術が利用される。

1. 公開鍵暗号

これから関数 g で暗号化を表す。つまり、データ x を暗号化したものは $g(x)$ で表す。Bさんの秘密鍵で暗号化したデータ x は $g_B(x)$ で表す。

2. 一方向ハッシュ関数 f

これから説明。

データ x にハッシュ関数を適応したものは $f(x)$ で表す。



デジタル署名の背景

一方方向ハッシュ関数 (CRYPTOGRAPHIC HASH FUNCTION)

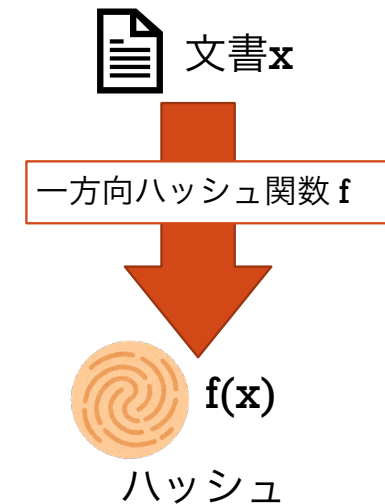
- 一方方向ハッシュ関数 f が入力 x を受けて、値 $f(x)$ を返す。
この場合、 $f(x)$ はハッシュと呼ぶ。
- 特徴：
 - 元の入力の推測ができない。
 - 入力が元の x でなければ、高い確率で出力されたハッシュも違う。
つまり、 $x \neq y \Rightarrow f(x) \neq f(y)$ 。
- 改ざんの防止に利用される。
- よく利用されているアルゴリズム：MD5, SHA-1。

$f(x)$ のサイズは元の x のサイズよりはるかに小さい。

つまり $\text{size}(f(x)) \ll \text{size}(x)$ 。

ハッシュ関数はセキュリティ分野以外でも広く利用されている。

例えば、pythonのset型（集合型）の実装に利用されている。

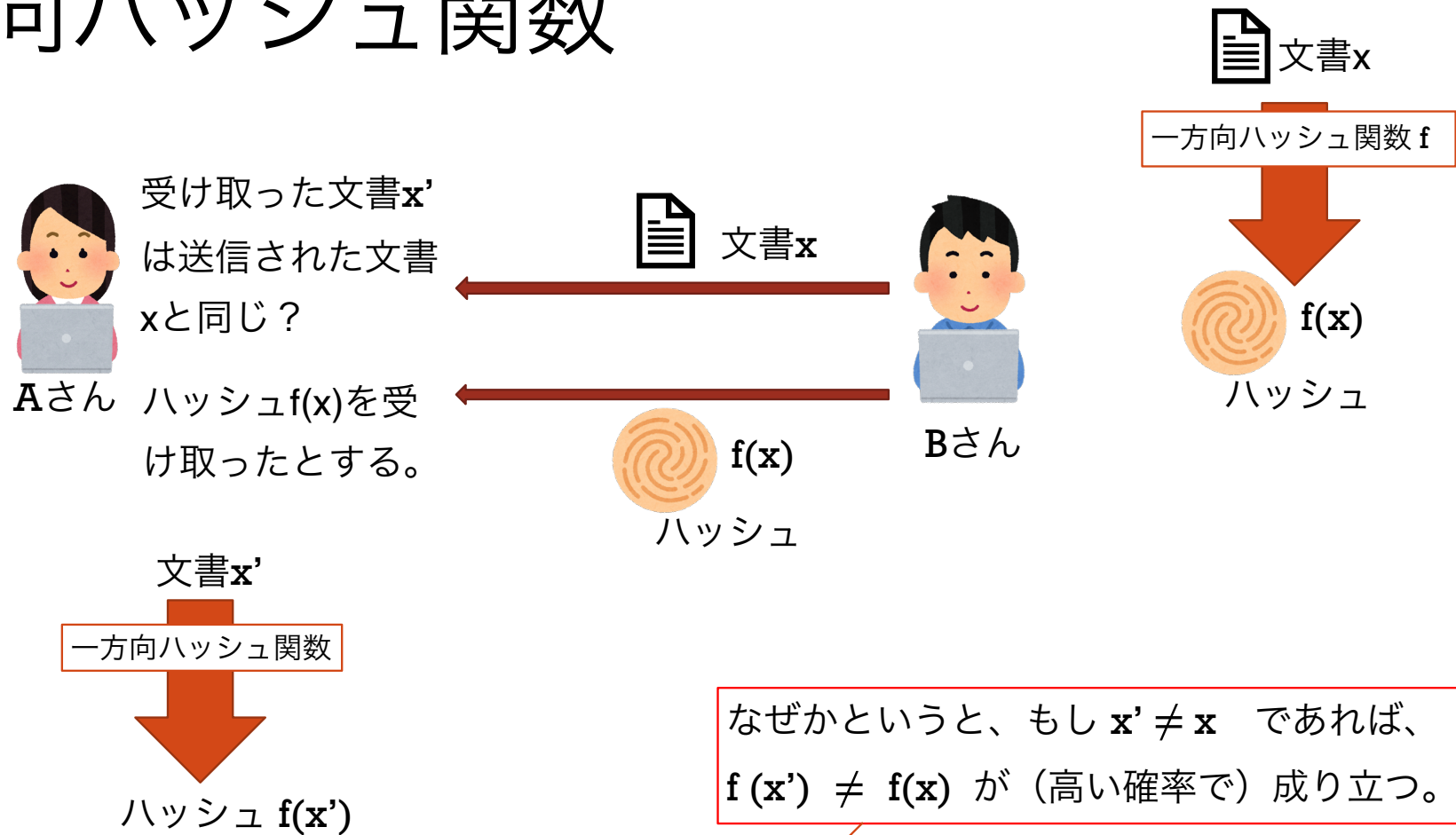


セキュリティ分野では $f(x)$ を
指紋(fingerprint)と呼ぶこ
とが多い。



一方向ハッシュ関数

改ざん防止の例



なぜかという、もし $x' \neq x$ であれば、 $f(x') \neq f(x)$ が（高い確率で）成り立つ。

$f(x') = f(x)$ かつ $f(x)$ が改ざんされなかったら、
受け取った文書 x' と送信された文書 x が一致している。



一方向ハッシュ関数

攻撃1

攻撃者が文書 x を編集する。

攻撃者Zが通信を盗聴して
文書 x を別の文書 x' に変更。



受け取った文書 x' は送信された文書 x と同じ？

ハッシュ $f(x)$ は確実に受け取ったとする。

Aさん

文書 x'

一方向ハッシュ関数 f

ハッシュ $f(x')$



Bさん

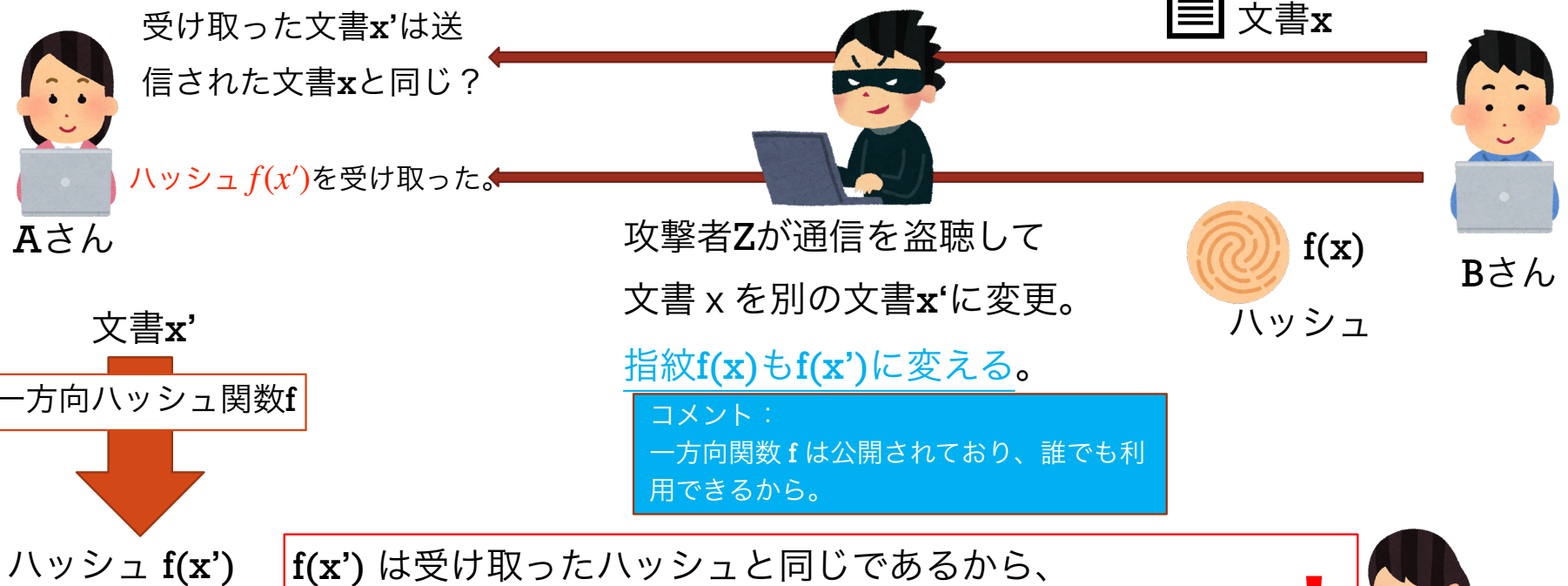
$f(x') \neq f(x)$ であるから、
受け取った文書 x' と送信された文書 x が一致しない。
⇒ 文書 x が改ざんされたことを検知できる。



一方向ハッシュ関数

攻撃2



攻撃者が文書 x を編集する。
ついでに新しい指紋も作成。



$f(x')$ は受け取ったハッシュと同じであるから、
受け取った文書 x' と送信された文書 x が一致していると思う。
⇒ 文書 x の改ざんは検知できない。



デジタル署名 (DIGITAL SIGNATURE)

- 秘密鍵：暗号化用  40pの応用の例と比べると、公開鍵と秘密鍵の役割が変わった。
- 公開鍵：復号用 
- 一方方向ハッシュ関数：文書の指紋を作成

Aさんが確実にBさんの公開鍵を所持しているとする。


Bさんの公開鍵



受け取った文書 x' は
送信された文書 x と同じ？

 文書 x



Bさん

  $g_B(f(x))$

文書 x'

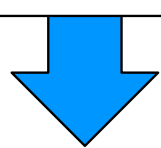
一方方向ハッシュ関数



ハッシュ h_1

$g_B(f(x))'$

Bさんの公開鍵



ハッシュ h_2


ハッシュ $h_1 =$ ハッシュ h_2 であれば


- 1.) ハッシュ h_1 はBさんの秘密鍵で暗号化された。
- 2.) 受け取った文書 x' と送信された文書 x が一致している。

文書 x

一方方向ハッシュ関数



 ハッシュ $f(x)$

Bさんの秘密鍵 



  $g_B(f(x))$

デジタル署名

デジタル
署名の作
成

なぜかという、ハッシュ h_1 とハッシュ h_2 が等価になるように、
文書 x とデジタル署名 $g_B(f(x))$ を両方も改ざんするのが困難だから。

デジタル署名 (DIGITAL SIGNATURE)

効果

秘密鍵はBさんしか持っていないとすると、
受け取った文書xはBさんによって作られたものと一致する。

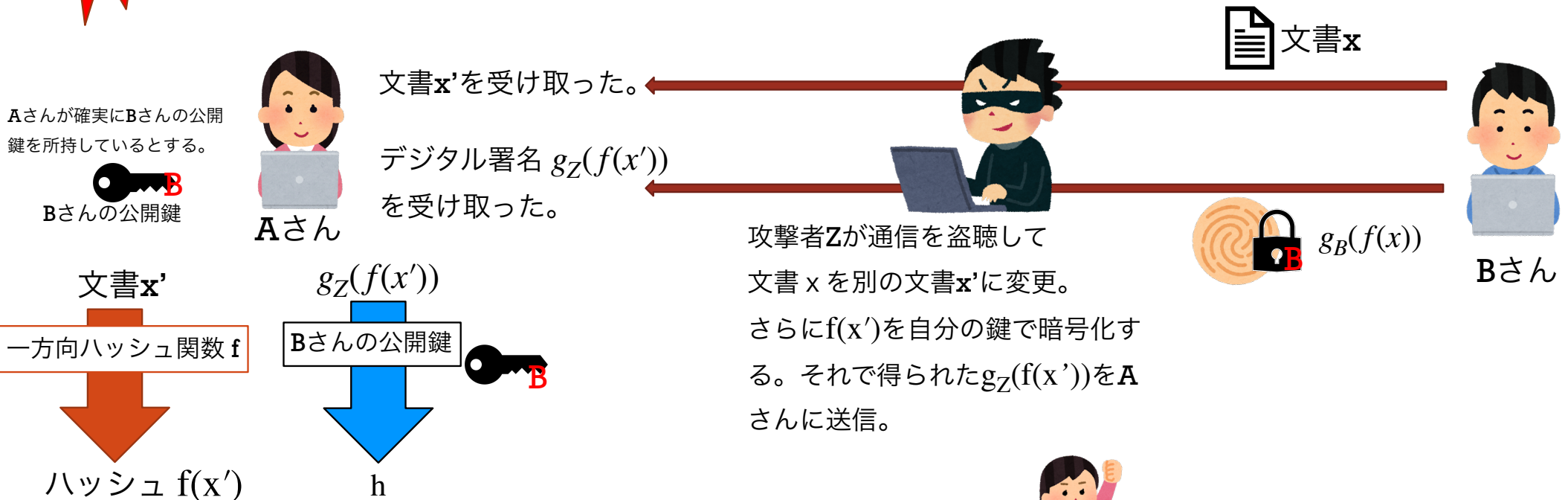
⇒ 成り済ましの防止 ∧ 改ざんの防止



デジタル署名 (DIGITAL SIGNATURE)

攻撃3

攻撃者が文書 x を編集する。
ついでに新しいデジタル署名も作成。

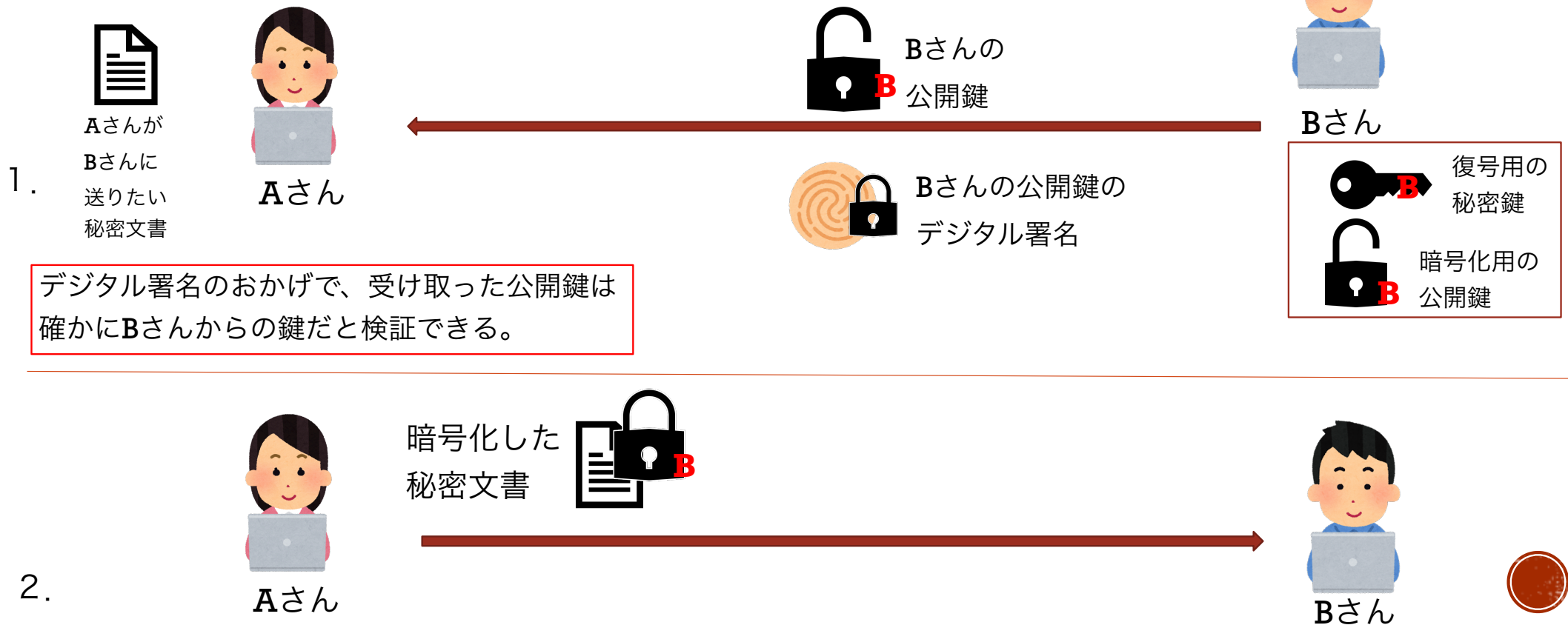


Bさんの公開鍵で復号したら、 $f(x') = h$ にはならない。
⇒ 文書 x や デジタル署名 $g_B(f(x))$ が改ざんされたことを検知できる。



デジタル署名 (DIGITAL SIGNATURE)

文書だけではなく、任意のデータをデジタル署名できる。
特に、暗号化用の公開鍵をデジタル署名することが多い。



Bさんの公開鍵への署名

問題：

- もしBさんが自分で署名したら、Aさんに署名の検証に必要な鍵も送信する必要がある。Man-in-the-Middle Attackのリスクが残る。

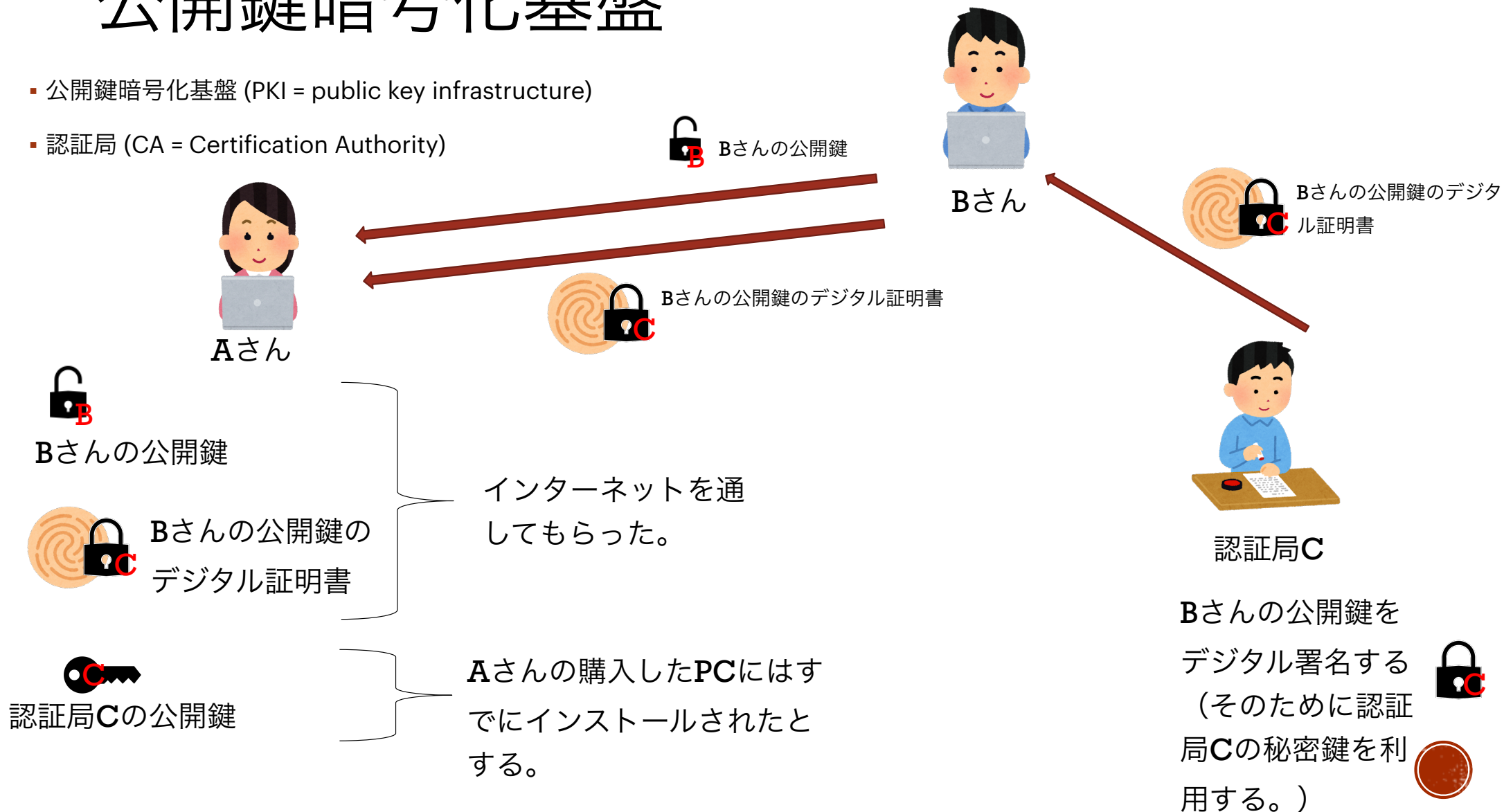
解決：

- Aさんが信頼している認証局Cの公開鍵を持っているとする。
(例えば、購入したPCにはすでにインストールされている。)
- 認証局CがBさんの公開情報（名前+Bさんの公開鍵）をデジタル署名する。
(つまり認証局Cが自分の秘密鍵を使って、Bさんの公開情報から作成したハッシュを暗号化する。)

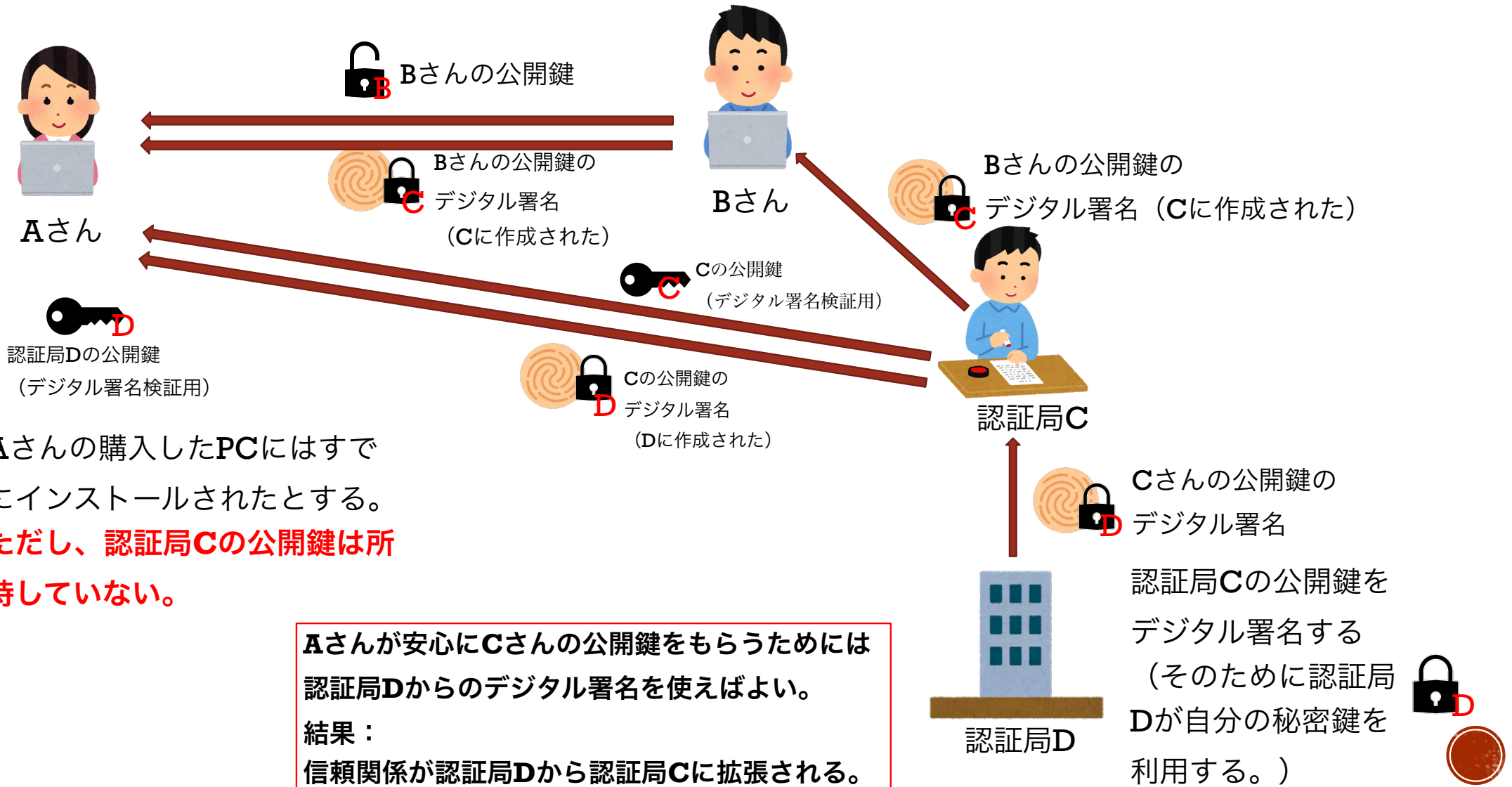


公開鍵暗号化基盤

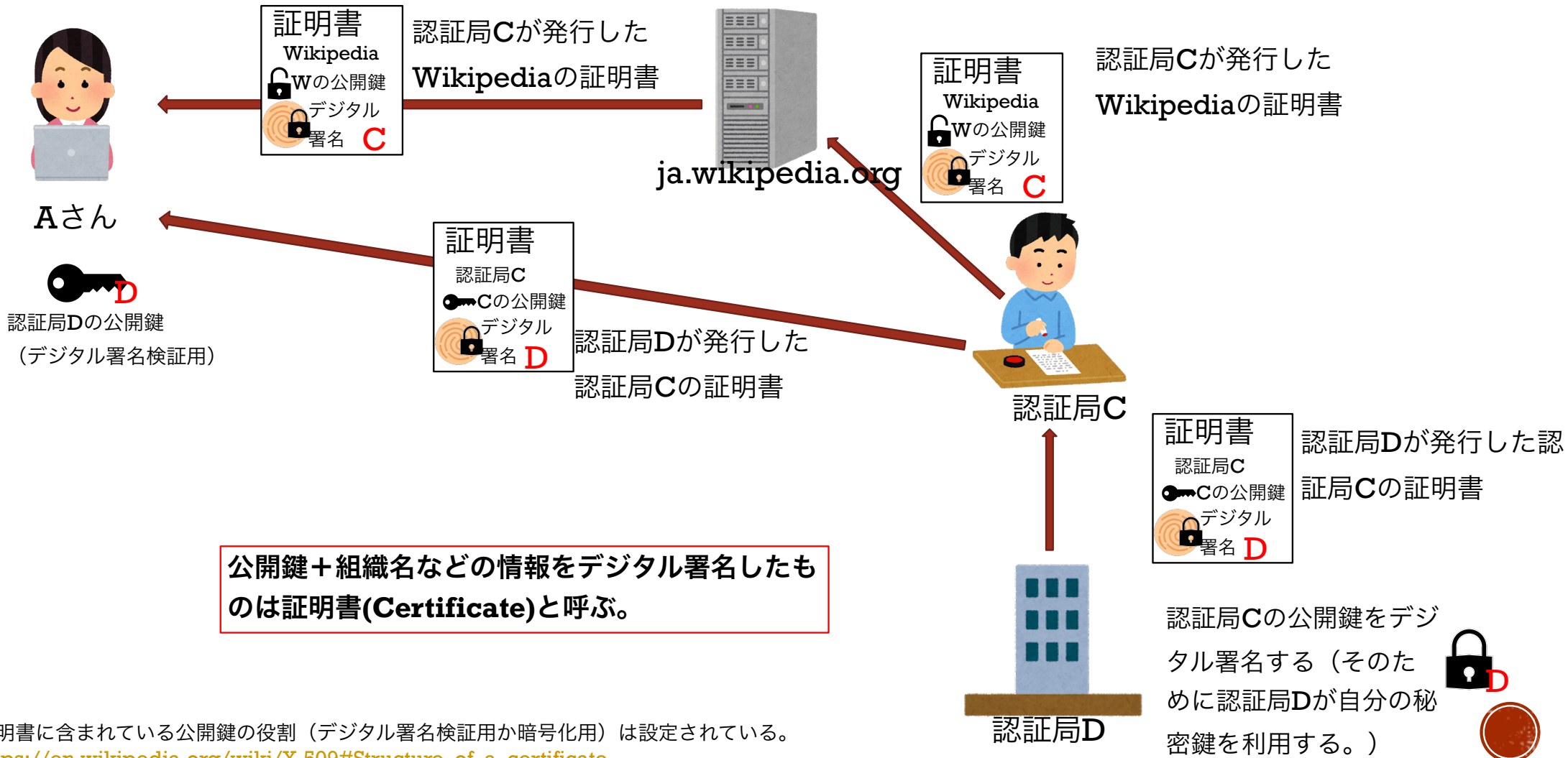
- 公開鍵暗号化基盤 (PKI = public key infrastructure)
- 認証局 (CA = Certification Authority)



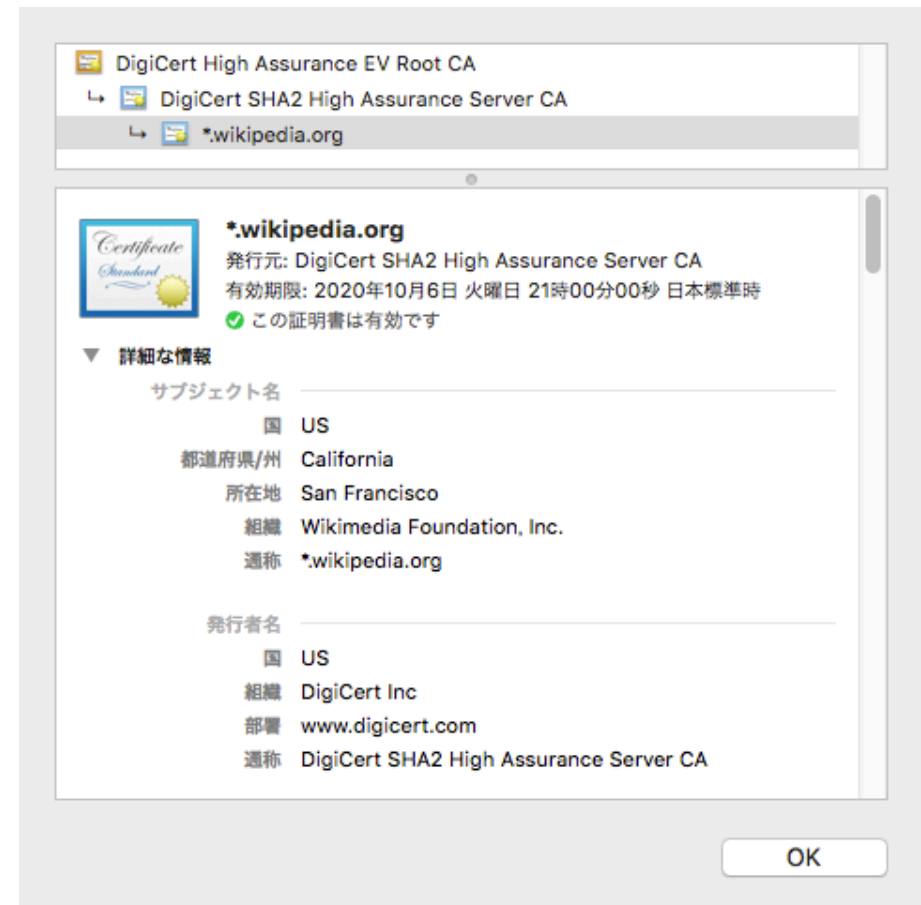
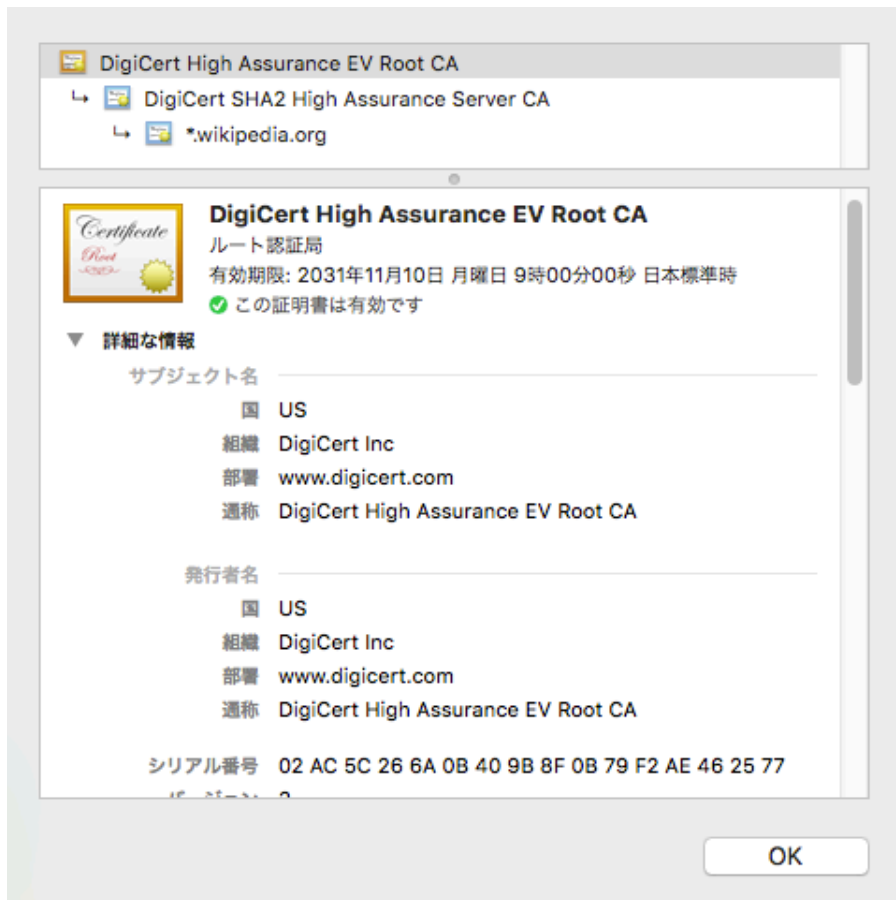
公開鍵暗号化基盤 — 信頼できる署名をさかのぼる



公開鍵暗号化基盤 — WEB BROWSERでの安全な通信を実現



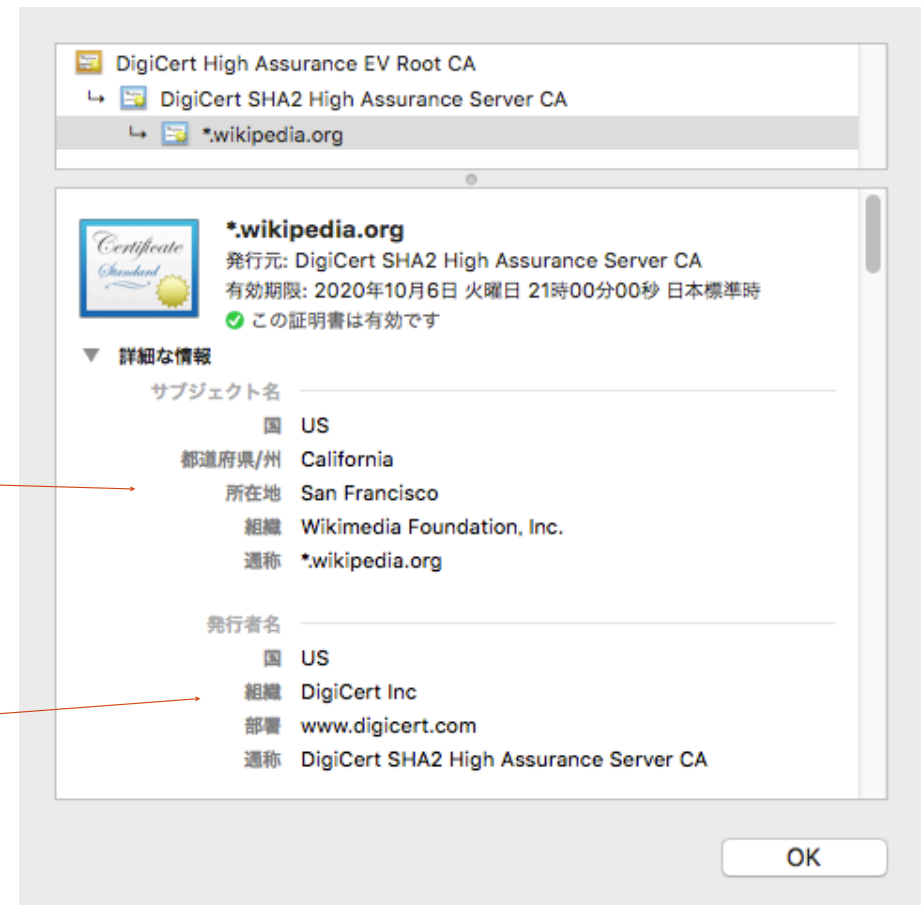
例：WIKIPEDIAの証明書を確認



例：WIKIPEDIAの証明書を確認

保証された内容

証明発行者（CA = Certificate Authority）の詳細



HTTPS (HYPERTEXT TRANSFER PROTOCOL SECURE)

- HTTPによって通信すると、情報が平文（ひらぶん）で通信されてしまう。
- HTTPSが認証と暗号化によって、通信した情報が第三者から読まれないようにしている。
- 通信の際にはHTTPSが暗号化とデジタル署名(*)を利用して以下の三つの攻撃から守ってくれる。
 - なりすまし
 - 盗聴
 - 改ざん
- 現在は多くのページがHTTPの代わりにHTTPSを利用している。

(*) TSL/SSLプロトコルで実現されている。



HTTPにおけるサイバー攻撃



Zさん

ハッカーがAさんのクレジットカードの情報を盗もうとする。
どのような方法が考えられる？



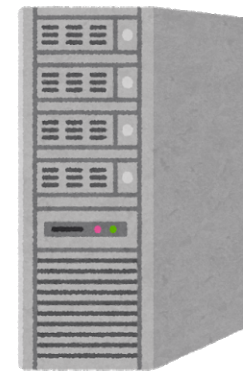
Aさん



Web page



クレジットカードの情報



www.amazon.com



盗聴



通過しているインターネットの
サーバからカード情報を盗聴。



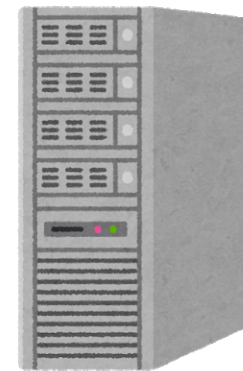
Aさん



Web page



クレジットカードの情報



www.amazon.com





盗聴



Zさんは暗号化している情報を
復号できない。

対策：

Amazonの公開鍵によ
ってカードの情報を暗
号化

- 公開鍵：暗号化用  Amazon
- 秘密鍵：復号用  Amazon



Aさん

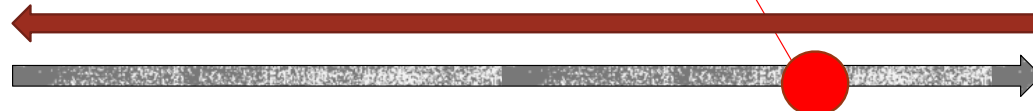


Web page



Amazon

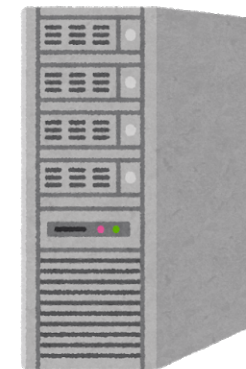
Amazonの公開鍵



Amazon

クレジットカードの情報

HTTPSで実現されている。



www.amazon.com



改ざん



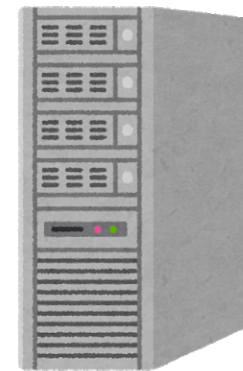
**Amazonの鍵をZさんの公開鍵
と置き換える。
=>Zさん暗号化されたカード
情報を復号できる。**



Aさん



クレジットカードの情報



www.amazon.com



改ざん



証明書の改ざんが難しい

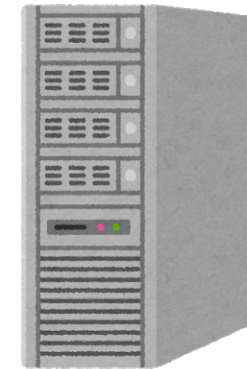
対策：
認証局(CA)によるデジタル署名



Aさん



Amazonの公開鍵が
含まれている証明書



www.amazon.com



Amazon

クレジットカードの情報

HTTPSで実現されている。

手元にあるCAの公開鍵
によって証明書を検証
(例えば、PCの初期時から保持)



なりすまし (PHISHING)

Amazonをなりすまして、クレジットカードカード情報を獲得しようとしている。



なりすまし (PHISHING)

対策：
CAの認証証
明書を確認

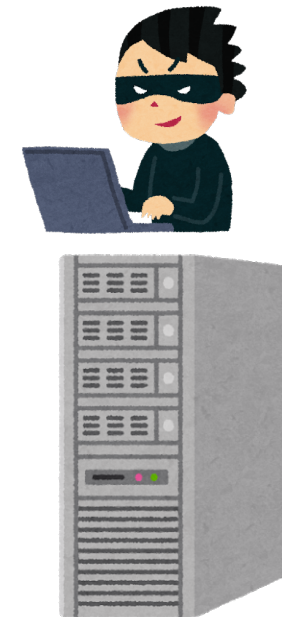
本当のAmazonのWeb
pageにそっくり



Web page



Zさんの公開鍵



CAの認証
証明書



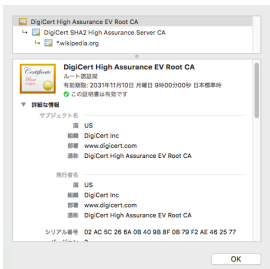
Aさん

怪しいからクレジットカード
の情報を送信しない。

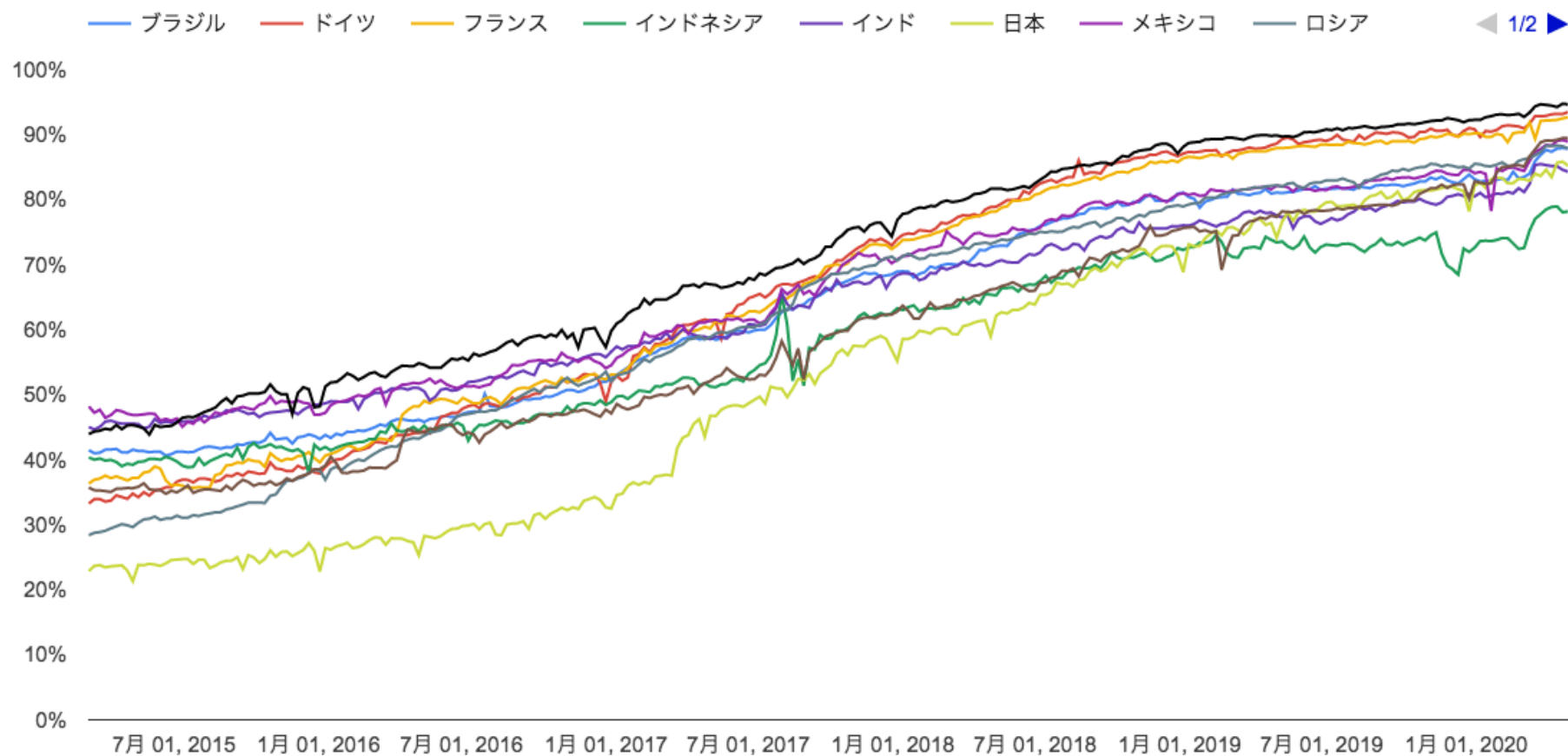


www.amaron.com (*)

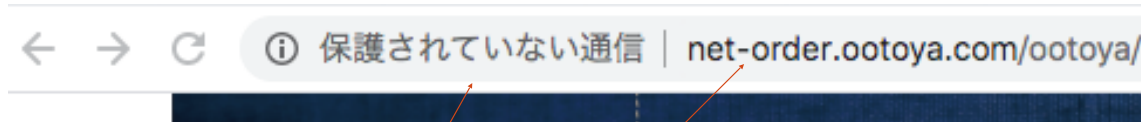
(*) わざとamazon.comに違い名称
今回はあくまでも例であり、
実際にamaron.comを運営している業者は不明。



WEB閲覧におけるHTTPSの利用割合



例：CHROMEでHTTPとHTTPSを区別する



HTTPのプロトコルが利用
されている場合



HTTPSのプロトコルが利
用されている場合



補足：通信以外のセキュリティ問題

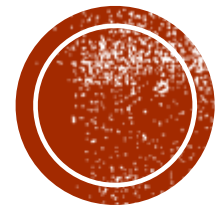
当たり前ですが、通信のセキュリティが保証されても、ClientやServerに保存したデータにおけるセキュリティのリスクがある。

対策の例：

- データの管理（暗号化した状態での保存、データへのアクセス権限の管理など）
- パスワードの管理
- Virus Softwareによって悪意のソフトウェアや侵入者を早期に発見。
- など



質問タイム



「情報の伝達と通信PART2」のまとめ

- 公開鍵暗号の主な応用は「秘密を守るための暗号」と「デジタル署名」
- 秘密を守るための暗号。
 - 公開鍵：暗号化用の鍵
 - 秘密鍵：復号用の鍵
- デジタル署名によって、なりすましや改ざんの防止が可能。
 - 公開鍵：復号用の鍵
 - 秘密鍵：暗号化用の鍵
- デジタル署名の重要な応用の一つはインターネットWeb siteの証明書
- 証明書の検証と暗号化用の公開鍵の受け取りがHTTPS (TSL/SSL) によって実現されている。



補足：暗号化とデジタル署名の詳細

分かりやすく概念レベルで説明するためにいくつかの詳細を割愛・簡易化した。

- 実際には公開鍵暗号の計算コストが高いため、共通鍵暗号と組み合わせることが多い。

例えば、秘密文書はパスワードをかけて共通鍵暗号で暗号化され、そのパスワードだけは公開鍵暗号方式で交換される。

- 「ssh-keygen -t rsa」で作成された公開鍵・秘密鍵の対がユーザ認証に利用される。（秘密文書の暗号化に直接に利用されない。）SSHに関する詳細は次のページにまとめている。



補足： SSH

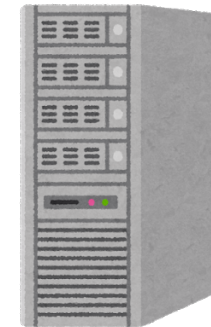
- Secure Shell (SSH) protocol とそれを利用可能にするプログラム (Linux/Mac: “ssh”)
- リモートサーバへのログインに広く利用されている。他の応用もある。
- 公開鍵暗号化方式が利用されている。
 - 公開鍵：暗号化専用の鍵
 - 秘密鍵：復号専用の鍵
- 2種類のログイン方法：
 - Password
 - ユーザが公開鍵を指定



Aさんが新しい深層学習アルゴリズムを開発して
GPUサーバで実行したい。

ローカルPCでSSH Clientがインストール済み
(Linux/Mac/Windows 10)

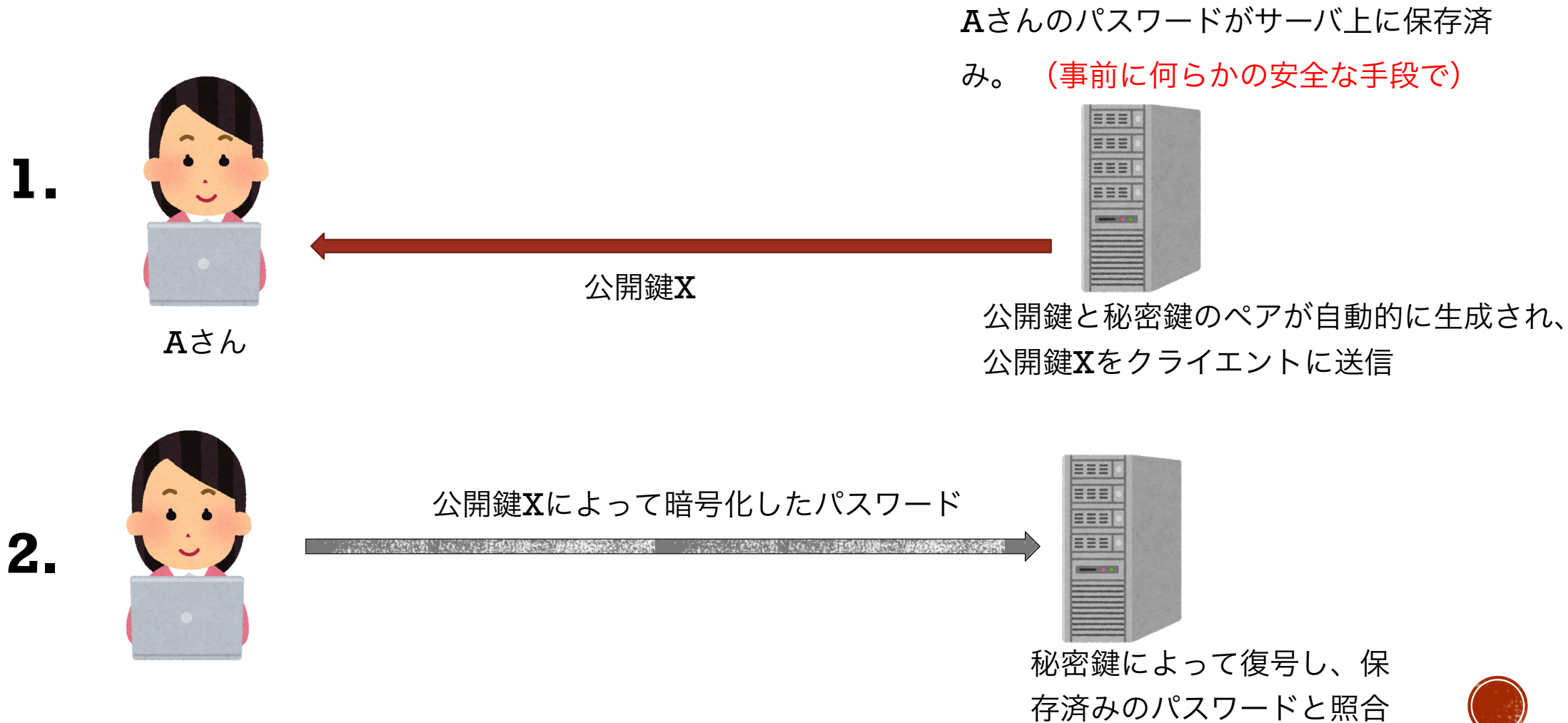
高性能の**GPU**サーバ



SSH Serverが稼働



補足：SSH PASSWORDによるユーザ認証



補足：SSH 公開鍵暗号によるユーザ認証

Aさんが公開と秘密鍵のペアを生成し、
公開鍵をサーバに保存した。

Aさんの公開鍵がサーバ上に保存済み。

事前に何らかの安全な手段で

(場所 ~/.ssh/authorized_keys)

1.



Aさんのログイン要求



2.



暗号化した文字列 $g_A(S)$



受け取った $g_A(S)$ を秘密鍵で復号し、
Sの指紋を求める。

2.1. ランダムな文字列Sを作成。

2.2. SをAさんの公開鍵によって
暗号化: $g_A(S)$



3.



Aさんが作ったSの指紋



その後、セッション鍵（自動的に作成したパスワード）を
使って、共通鍵暗号方式によって、データの交換を行う。

3. 受け取った指紋と $f(S)$ を照合。
等価であれば、Aさんのログイン
要求を受理。



レポートの課題 情報の伝達と通信PART2

1. デジタル署名と証明書に関する課題

www.amahon.com にアクセスして、証明書を確認してください。

(「www.amahon.com」から「www.amazon.com」に転送された場合は、
「www.amazon.com」の証明書を確認してください。または www.amahon.com にアクセスできない方は www.amazon.com に直接にアクセスしてください。)

1.1. Web pageは何企業に所属していますか。その証拠は何ですか。

1.2. Web browserを使ってwww.amahon.comにクレジットカード番号を送信してもよいですか。
送信しないほうがよい、または、送信してもよいと思う理由・仮説を書いてください。

(回答は50文字～200文字の範囲でお願いします。箇条書きでも結構です。)

