応用情報技術者試験

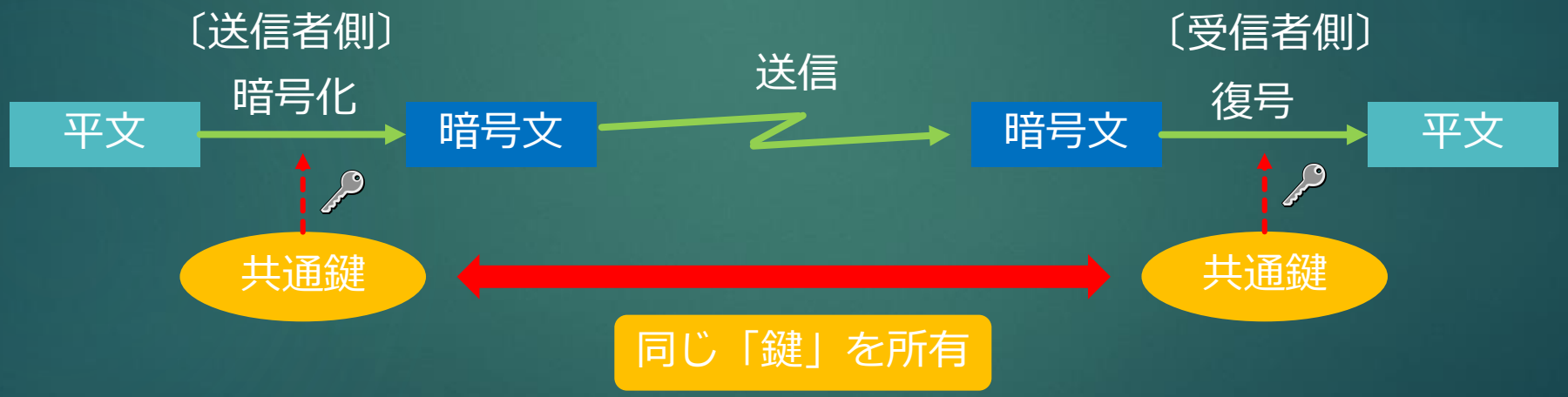
第8章　セキュリティ

1. 暗号技術
共通鍵暗号方式

- **暗号化**と**復号**に同じ鍵（**共通鍵**、**対称鍵**）を用いる暗号方式のことを、**共通鍵暗号方式**という。共通鍵は送信者と受信者で共有し、これを用いた演算を**平文**や**暗号文**に施すことで暗号化・複合を行う。

平文

暗号化されていないデータ



共通鍵方式の特徴

- 共通鍵暗号方式には次の特徴がある。

・暗号化や復号に要する処理時間が短い
→大量データの暗号化・復号に有利

・利用者が多くなるほど鍵の種類が増え管理が煩雑になる
→n人の利用者が相互に通信：**$n(n-1)/2$種類**の鍵が必要

代表的な共通鍵暗号方式

DES	米国の旧国家暗号規格。56ビットの共通鍵に用いるブロック暗号
AES	DESの後継規格
RC	SSLやWEPなどで広く使われているストリーム暗号
Kcipher-2	九州大学とKDDIが共同開発したストリーム暗号

ブロック暗号

データを固定長のブロック単位で暗号化する方式

ストリーム暗号

データをビット単位あるいはバイト単位に逐次暗号化する方式

公開鍵暗号方式

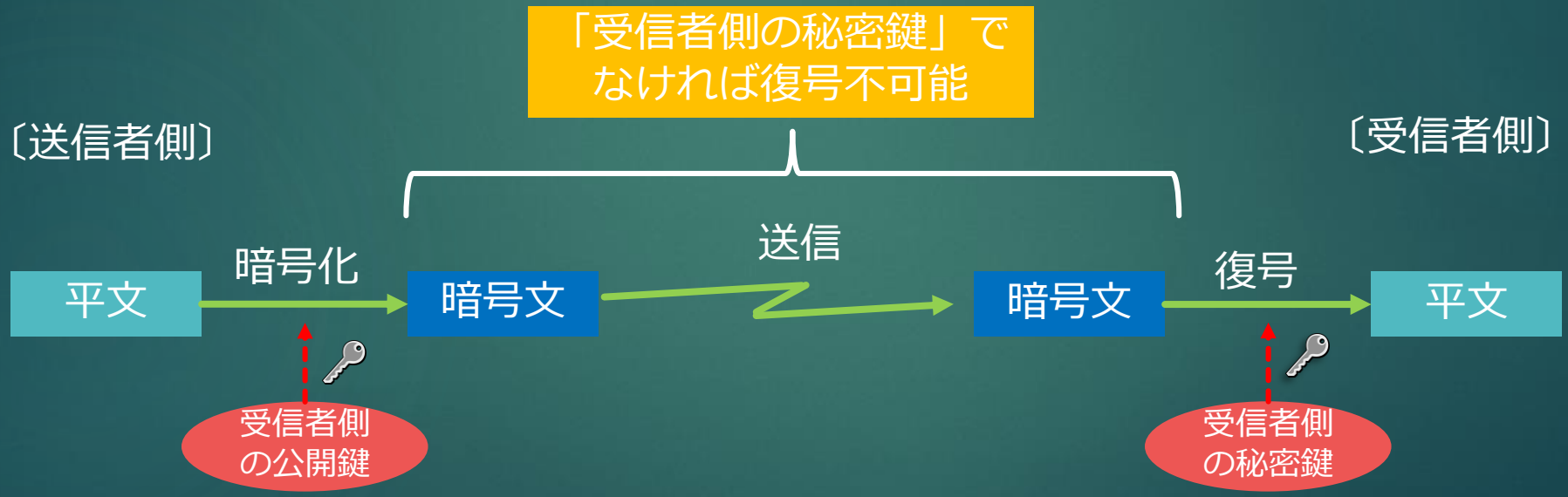
- **公開鍵暗号方式**は、暗号化と復号に対となる二つの鍵（**鍵ペア**）を利用する方式である。鍵ペアは次の特徴をもつ。

・一方で暗号化したデータは、対となる鍵でのみ復号できる。
・一方の鍵から、もう一方の鍵を推測できない

- 利用者は、一方の鍵を**秘密鍵**(Private Key)として他者に知られないように厳重に管理し、もう一方を**公開鍵**(Public Key)として公開する。

公開鍵暗号方式

- 公開鍵方式で暗号化通信を行うためには、平文を受信者の公開鍵で暗号化する。これを復号できるのは、受信者のみが持つ受信者の秘密鍵であるため、第三者による盗聴を防ぐことができる。



公開鍵暗号方式の特徴

- 公開鍵暗号方式には次の特徴がある。

・秘密鍵は本人が保有し、公開鍵のみ配送する

→秘密鍵は漏洩しないので安全な鍵配送が実現

・共通鍵暗号方式に比べ、鍵の種類が少ない

→n人の利用者が相互に通信：**$2n$種類**の鍵

→不特定多数が同じサイトに送信：**2種類**の鍵

・暗号化や復号に要する処理時間が長い

鍵の少なさによる管理の容易さが、公開鍵暗号方式の大きな利点である。相互通信が必要な環境に利用者が一人加わるとき、増える鍵は利用者の鍵ペア（2種類）のみなので、結果として、**n人の相互通信環境で必要になる鍵は$2n$種類**に収まる。

代表的な公開鍵暗号方式

RSA	実用的な公開鍵暗号方式として最初に公開された方式。開発者の三人の頭文字をとってRSAと命名された。大きな数の素因数分解の困難性を利用している。
楕円曲線暗号	楕円曲線上の離散対数問題が困難であることを利用した暗号方式
ElGamal暗号	位数が大きな群の離散対数問題が困難であることを利用した暗号方式

セッション鍵方式

- 公開鍵方式を用いながらも、暗号化と復号に一時的な共通鍵である**セッション鍵**を利用する方式を、**セッション鍵方式**とよぶ。公開鍵方式の安全さと共通鍵方式の高速性を組み合わせた方式で、次の流れで処理を行う。

[1] 送信者が使い捨ての共通鍵（セッション鍵）を生成する

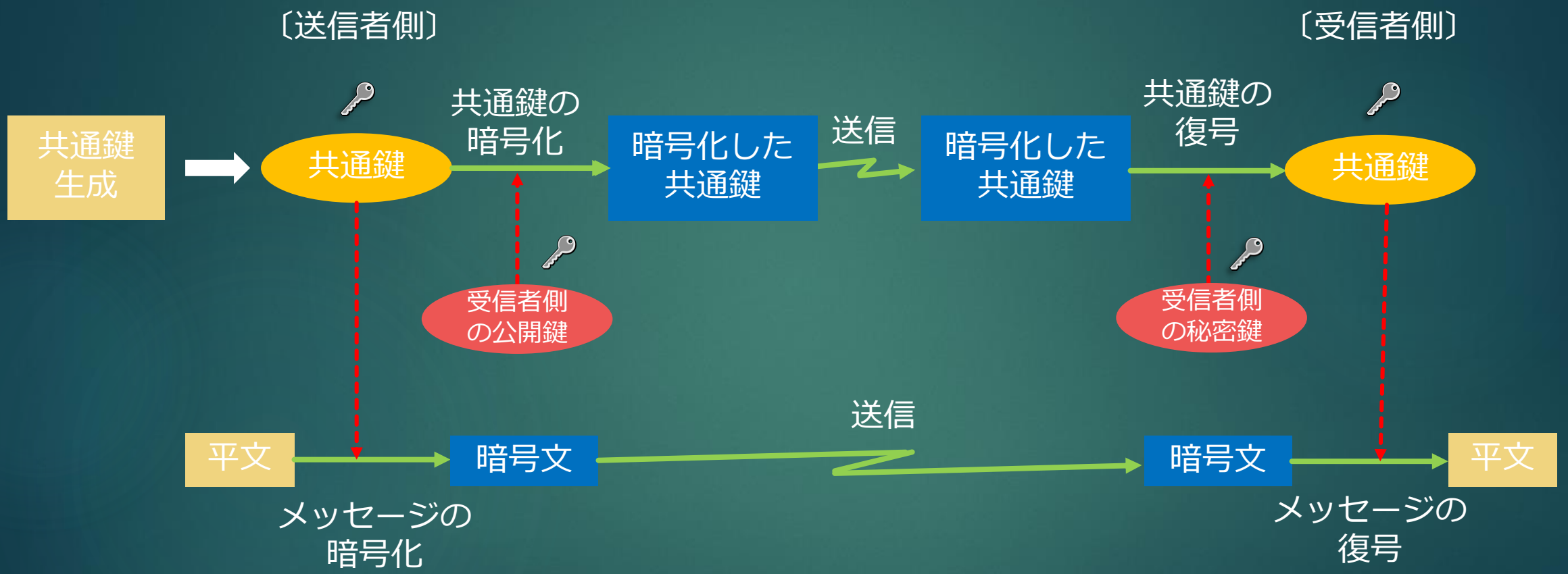
[2] セッション鍵を受信者の公開鍵で暗号化して送信する

[3] 受信したセッション鍵を受信者の秘密鍵で復号する

[4] セッション鍵を用いて暗号化通信を行う

[5] 通信が終了したら、双方でセッション鍵を破棄する。

セッション鍵方式



※セッション鍵（共通鍵）は通信終了時に破棄される

2. 認証
ユーザ認証

- **ユーザ認証**は、正当な利用者であることを確かめる技術である。ユーザIDとパスワードを用いる伝統的な方式から、ICカードやUSBキーを用いるもの、試問や静脈パターン、虹彩（アイリス）を用いる**バイオメトリクス認証**まで数多くの方式の方式がある。

- USBキー

USBキーは、USBインタフェースを備えたセキュリティ機器で、これを抜くとパソコンがロックされ、差すと解除される。長いパスワードを忘れたり、メモに残すなどの危険を防止することができる。同種の機器で、USB機器にICチップを内蔵し、セキュリティ処理を実行できるものを**USBトークン**とよぶ。

チャレンジ/レスポンス方式

- チャレンジ/レスポンス方式は、パスワードそのものを送るのではなく、パスワードを所有することを証明する方式である。サーバによるクライアント認証は、次の手順で行う。

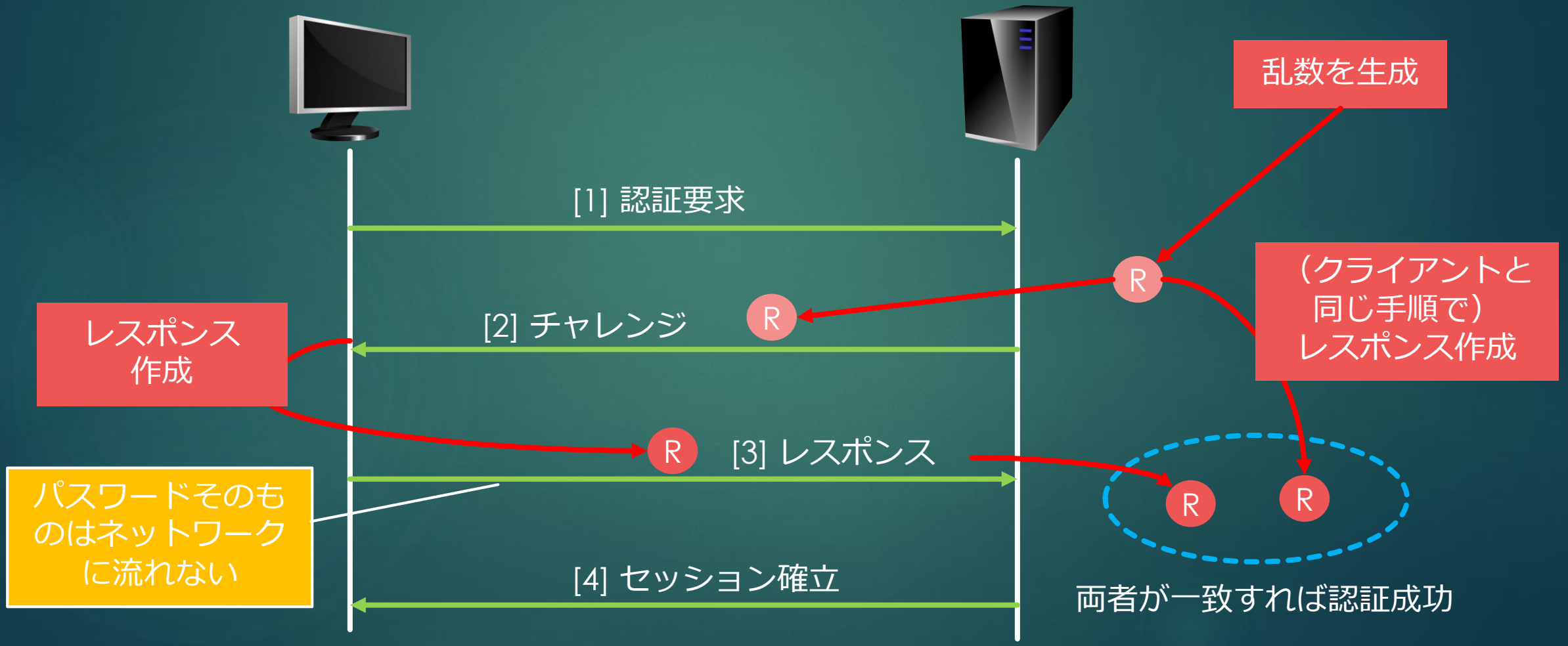
[1] クライアントが認証サーバに対して認証を要求する

[2] 認証サーバは乱数をもとにチャレンジ（要求文字列）を生成し、クライアントに送信する

[3] クライアントはチャレンジとパスワードなどからレスポンス（応答文字列）を生成し、認証サーバに送信する

[4] 認証サーバは受信したレスポンスと、自身で生成したレスポンスを比較する。両者が一致すれば認証を成功させ、セッションを確立する。

チャレンジ/レスポンス方式



チャレンジ/レスポンス方式

- チャレンジ/レスポンス方式を用いた認証方式を**CHAP**とよぶ。この方式は**パスワードそのものはネットワークに流さない**ため、パスワードの漏洩を防止できる。またチャレンジとレスポンスが毎回異なるため、**リプレイ攻撃**も防止できる。

- **リプレイ攻撃**

暗号化されたパスワードを盗み出し、そのまま再利用することで他者に成りすます攻撃のこと

認証サーバ / その他

- 認証サーバ

ユーザ認証は**アクセスサーバ**で行われる。そのため、複数のアクセスサーバを利用する際には、アクセスサーバごとにユーザ情報を登録しなければならず、運用が複雑になる。これを避けるため、アクセスサーバとは別にユーザ認証に関する情報を一括管理する**認証サーバ**を設け、これにユーザ情報を一元化する。認証サーバを用いた代表的な認証プロトコルにRADIUSがある。

- その他

これらの他にも、使い捨てのパスワードを用いる**ワンタイムパスワード方式**、一度の認証で複数のサーバを利用できる**シングルサイオン(SSO)**などの技術もある。

ディジタル署名

- **ディジタル署名**は、データの正当性を保証するために付与される暗号化された情報であり、データの**送信者を証明**し、データが**改ざんされていないことを保証**する。ディジタル署名は現実世界の署名と同様の効力を持つことが、**電子署名法**（電子署名及び認証業務に関する法律）により定められている。

ディジタル署名

[1] 送信者は、送信データをハッシュしてメッセージダイジェストを生成する（ダイジェスト1とする）

[2] 送信者は、送信者の秘密鍵を用いてダイジェスト1を暗号化してディジタル署名を生成する

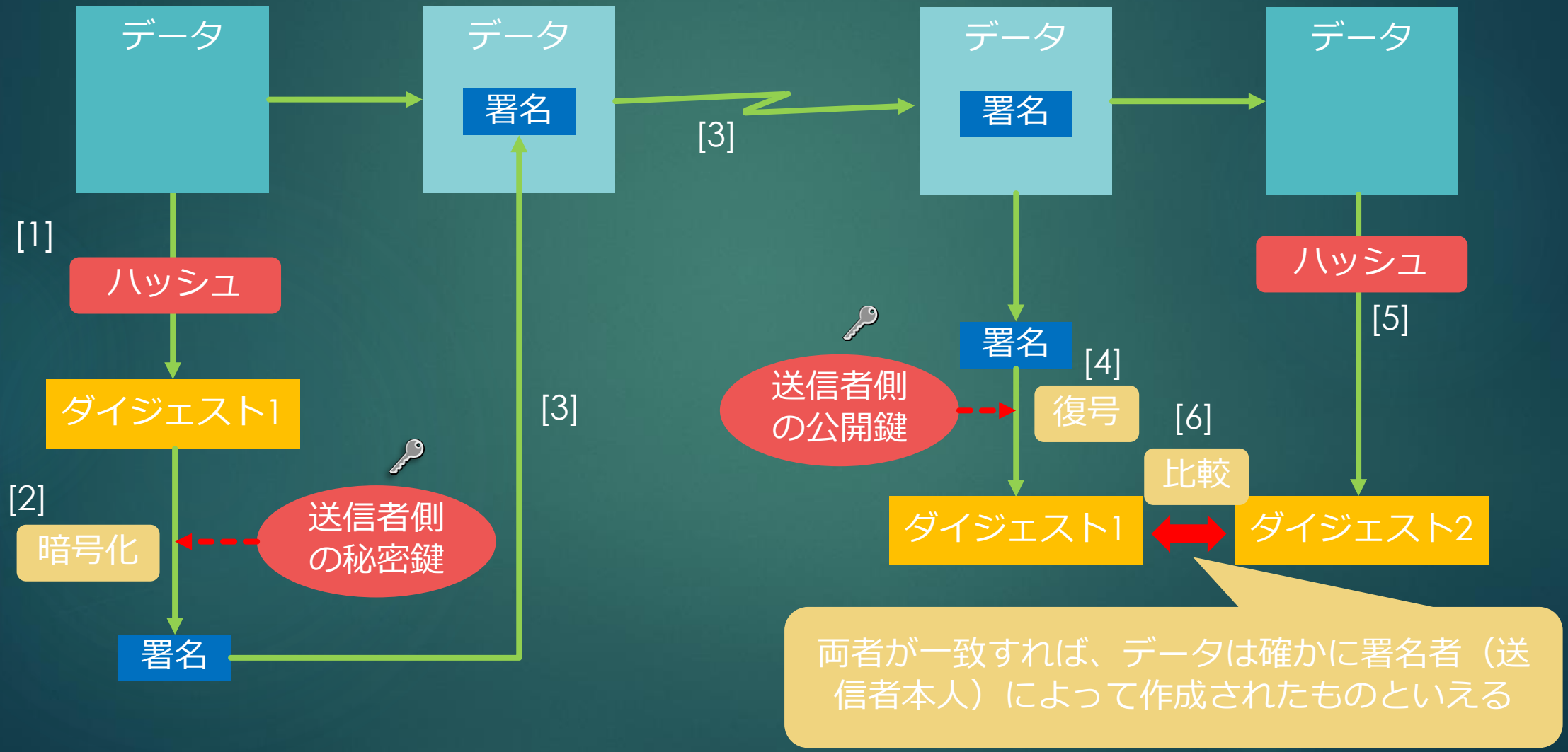
[3] 署名をデータにふかして受信者に送る

[4] 受信者は、データに付加されたディジタル署名を送信者の公開鍵を用いて復号し、元のダイジェスト1を得る

[5] 受信者は、受信したデータからメッセージダイジェスト（ダイジェスト2とする）を生成する

[6] ダイジェスト1とダイジェスト2が一致すれば、データを受け取る

ディジタル署名


データ
データ
署名
[3]
データ
署名
データ
[1]
ハッシュ
ダイジェスト1
[2]
暗号化
送信者側
の秘密鍵
署名
[3]
送信者側
の公開鍵
署名
[4]
復号
[6]
比較
ハッシュ
[5]
ダイジェスト1
ダイジェスト2
両者が一致すれば、データは確かに署名者（送信者本人）によって作成されたものといえる

ハッシュ関数の性質

- ハッシュ関数は、データから数値を得る関数で、コンピュータの様々な分野で用いられる。ディジタル署名で用いるハッシュ関数には、次の性質が求められる。

①ハッシュ値から元データを復元することが困難であること（一方向性）

②同じハッシュ値をもつ異なるデータを生成することが困難であること（衝突困難性）

①は**署名から元データが漏洩しない**ことを保証し、②は**ハッシュ値が等しい場合は、元データも等しい**（＝改ざんを受けていない）ことを保証するものである。

ディジタル署名の効果

- ディジタル署名が正しい（ダイジェスト1, 2が一致した）ことが確認できれば、次の2点が確認できたことになる。

①**データは改ざんを受けていないこと**（改ざん検知）

②**データは送信者本人により作成されたこと**（否認防止）

①はハッシュ関数の性質から導かれることである。

②はディジタル署名が送信者の公開鍵で正しく復号できたことから導かれることである。送信者の公開鍵で復号できたということは、その暗号化には送信者の秘密鍵が用いられたことになる。送信者の秘密鍵は送信者の秘密鍵は送信者本人のみが保有する鍵で、それを用いることができるのは本人以外ありえないからである。

時刻認証

- **時刻認証**は、**タイムスタンプ局**(TSA)とよばれる第三者機関が**タイムスタンプ（時刻印）**を発行することにより、その時刻に文書が存在し、改ざんされていないことを証明する方式である。
- ディジタル署名を併用すれば、次のような証明を行うことができる。

・タイムスタンプを発行済みの文書に署名

→文書はその時刻以降に署名された

・署名済みの文書にタイムスタンプを発行

→文書はその時刻以前に署名されている

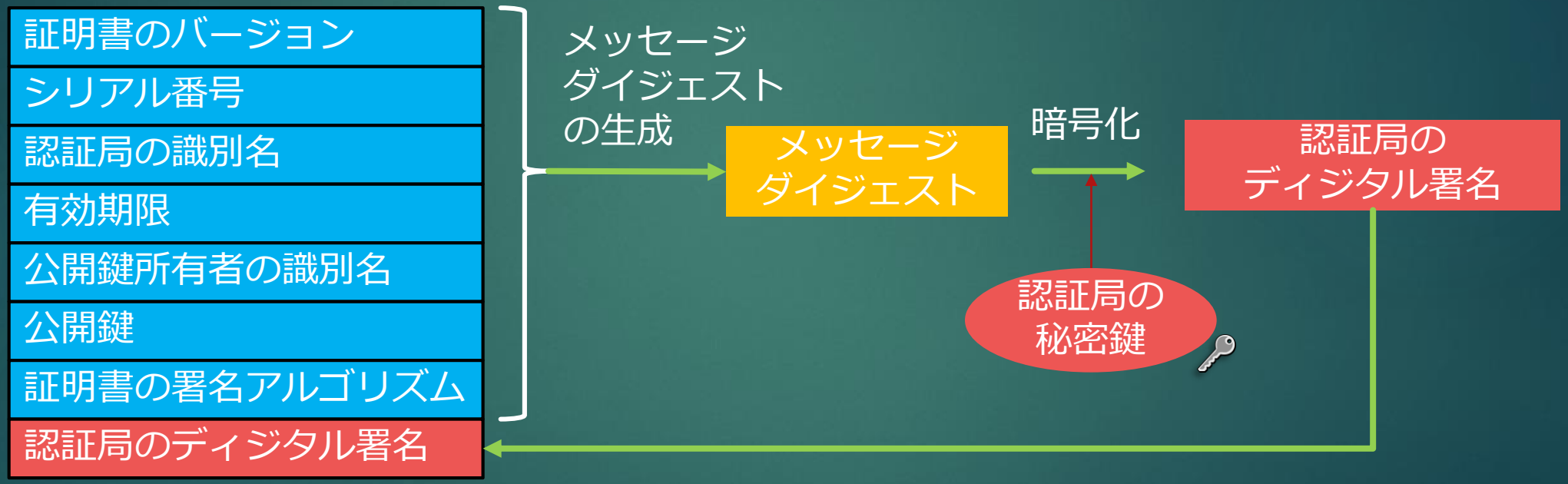
3. PKI（公開鍵基盤）
認証局(CA：Certificate Authority)

- 公開鍵が正しく本人のものであることは、その結びつきを信頼できる第三者が保証されなければならない。そのような**信頼できる第三者機関**を**認証局(CA)**とよぶ。

- 認証局は本人情報を確認の上、本人の公開鍵に保証を与えた証明書（**ディジタル証明書**）を発行する。利用者は証明書から「認証局が認めた公開鍵」を取得して利用することになる。

ディジタル証明書

- 証明書の規格には、ITU-Tが定めた**X.509**がある。



ディジタル証明書

- 署名所のフィールドには「公開鍵」に加えて「**認証局のディジタル署名**」が含まれている。証明書を取得した利用者は、最初に認証局の署名を確認し、これが確認できれば、公開鍵は「証明書に記載された所有者本人のもの」となる。

CRL

- 公開鍵の漏洩や誤発行など、何らかの理由によって有効期限内に証明書が失効することがある。そのような証明書のシリアル番号は、**失効リスト(CRL**：Certificate Revocation List)に加えられ、認証局から定期的に配布される。

- 証明書の利用にあたっては、署名や有効期限だけではなく、**証明書がCRLに含まれていないかどうか**も確かめる必要がある。

PKIにおける認証

- PKIでは、受け取った証明書を検証し、それが確かにCAによって発行されたものであれば、証明書に含まれる公開鍵を正当なものとして認める。証明書の発行から証明書の検証までは次のようになる。

〔証明書の発行〕

[1] Xは、自身を証明する情報を添えて、CA（認証局）に対して証明書の発行を申請する

[2] CAはXに対して証明書を発行する。この時点ではXは証明書の所有者となる。

PKIにおける認証

〔証明書の検証〕

[3] Xと通信を行う利用者Yは、通信に先立ちXの証明書を入手する

[4] Yは以下の手順で証明書を検証する

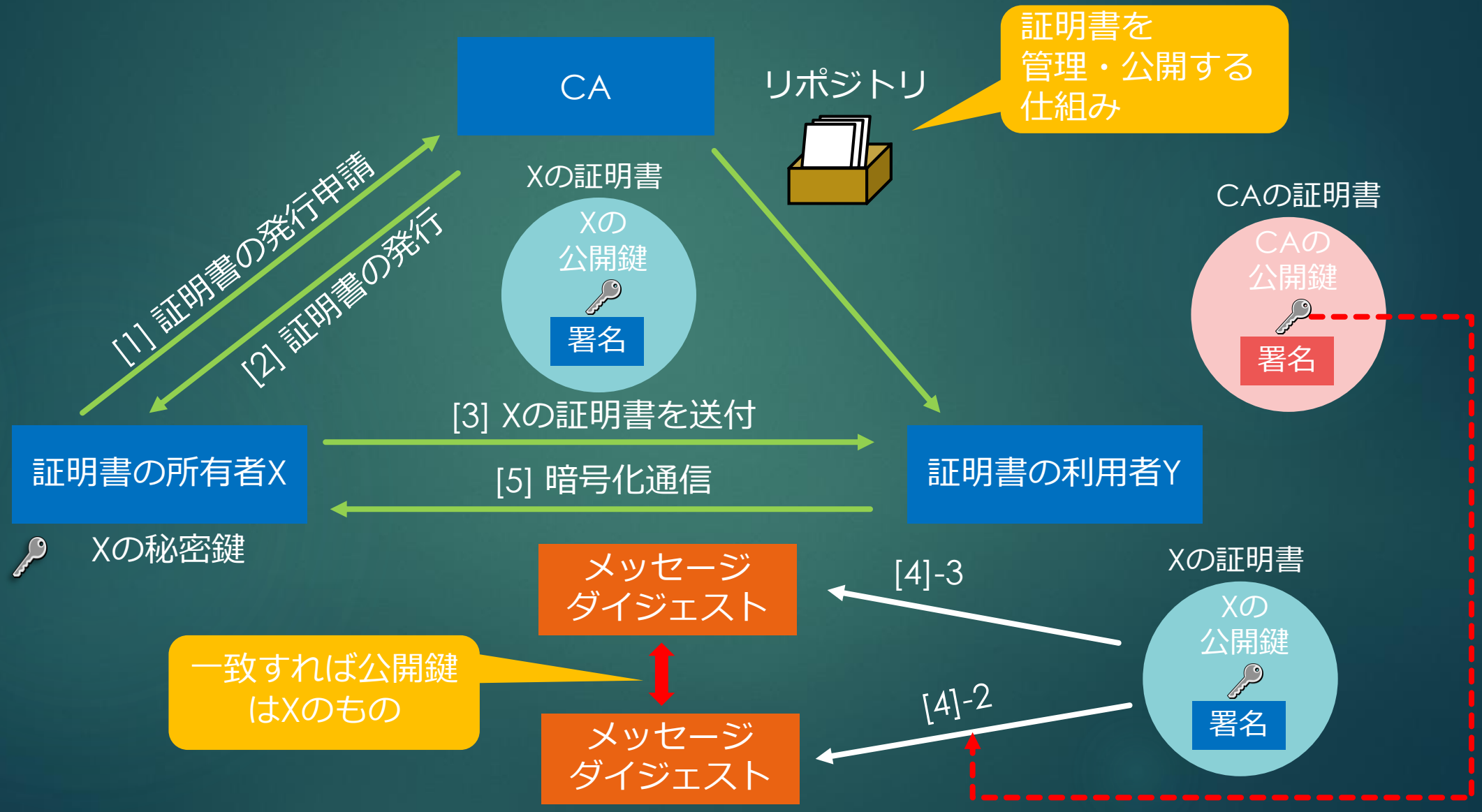
[4-1] Xの証明書を発行したCA（認証局）について、「そのCAの証明書」を入手する

[4-2] CAの証明書に含まれる「CAの公開鍵」を用いて、Xの証明書の署名を復号し、メッセージダイジェストを得る

[4-3] Xの証明書からメッセージダイジェストを生成し、上で得たメッセージダイジェストと一致するかを検証する。一致すれば、証明書に含まれる公開鍵が所有者Xのものであることが証明できる。

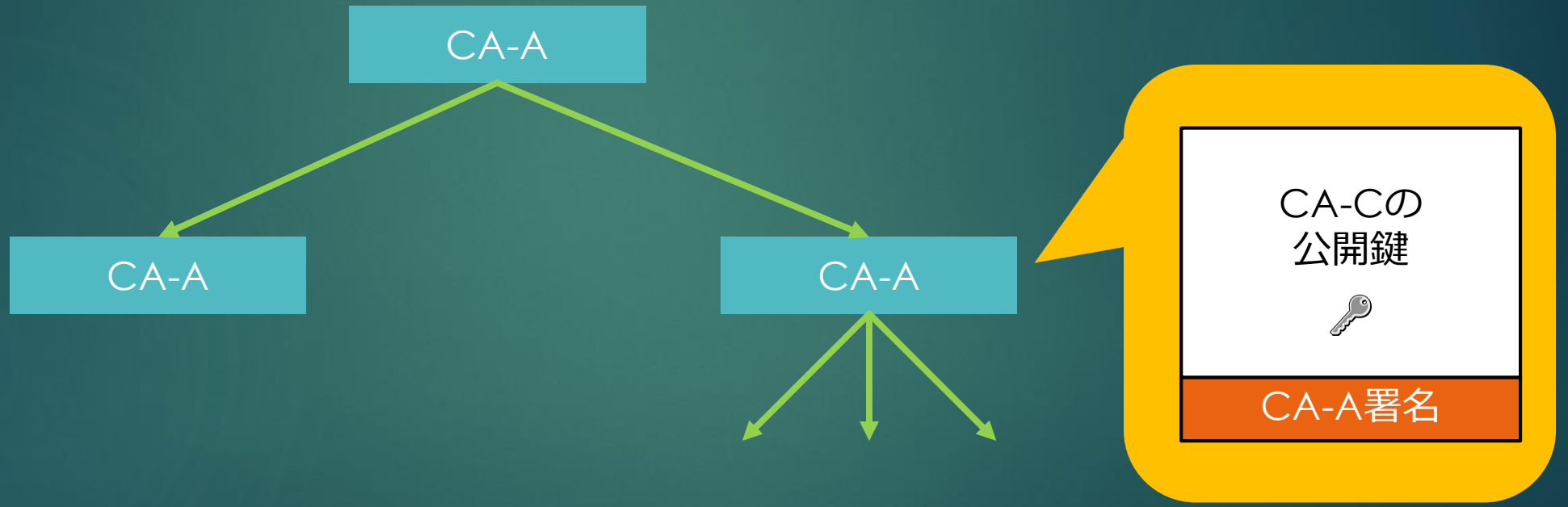
[5] Yは、証明書から取得したXの公開鍵を用いて、暗号化通信を行う。

PKIにおける認証


CA
リポジトリ
証明書を
管理・公開する
仕組み
Xの証明書
Xの
公開鍵
署名
CAの証明書
CAの
公開鍵
署名
[1] 証明書の発行申請
[2] 証明書の発行
[3] Xの証明書を送付
[5] 暗号化通信
証明書の所有者X
証明書の利用者Y
Xの秘密鍵
メッセージ
ダイジェスト
[4]-3
Xの証明書
Xの
公開鍵
署名
一致すれば公開鍵
はXのもの
[4]-2
メッセージ
ダイジェスト

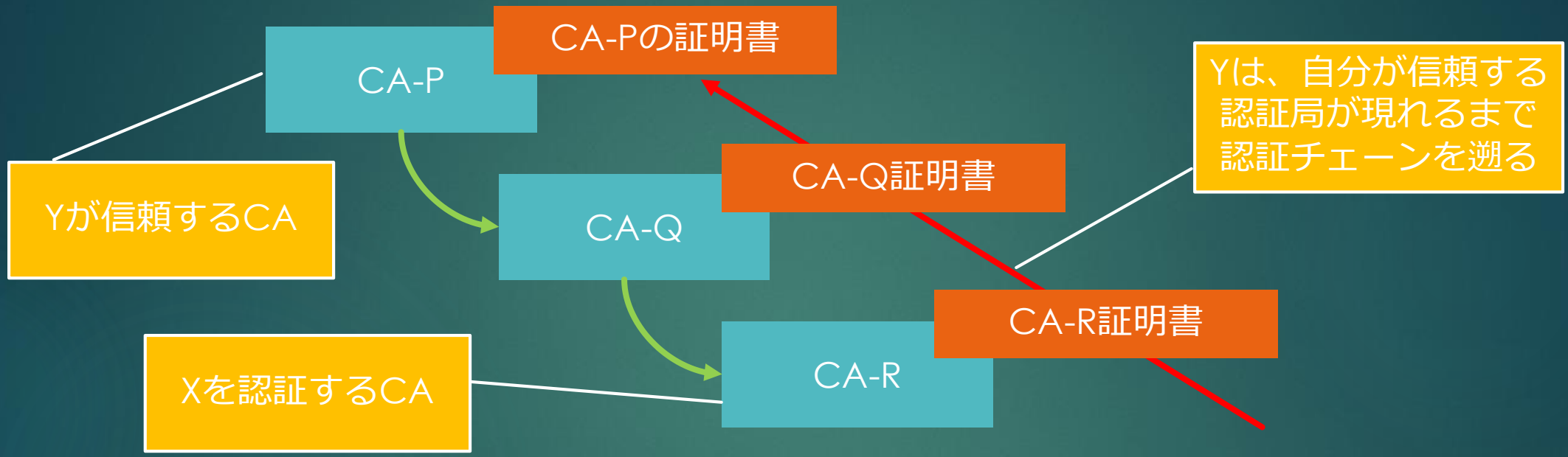
認証局の階層

- 認証局(CA)は、上位（大手）のCAが下位のCAを認証するような階層構造をとる。上位のCAに認証された証として、下位の認証局は「上位のCAが署名したディジタル署名」をもっている。
- CAの階層



- ある利用者の公開鍵を認証するCAを、他のすべての利用者が信頼しているとは限らない

認証局の階層



- Xを認証するCAはCA-Rであり、YはCA-Pを信頼しているものとする。受信者Yは、送信者Xを認証するCA-Rを信頼していない。このときYは、CA-Rから認証局の階層を遡る。具体的にCA-Rの証明書からCA-Qの識別名を取得して、CA-Qの証明書を取り寄せる。さらにCA-Qの証明書からCA-Pの識別名を取得する、という処理を繰り返す。その過程で、Yが信頼する認証局(CA-P)が現れた場合は「受信者Xの公開鍵は、自分(Y)が信頼する認証局(CA-P)により間接的に認証されている」と結論付け、Xを信頼する。

認証局の階層

- 階層構造の根に位置する認証局は、自分自身を証明する**ルート証明書**を発行している。利用者は**自分が信頼する認証局のルート証明書をあらかじめインストールしておく**ことで、間接認証を可能にしておく。なお、多くのOSやブラウザには、主要な認証局のルート証明書があらかじめインストールされている。

- **ルート証明書**

認証局が自身の正当性を証明するために、自ら署名したディジタル証明書

4. 脅威と対策
不正とアクセスの脅威と対策

ソーシャル エンジニアリング	上司を装って電話をかける、パスワードの入力をのぞき見するなど、**人間の心理的な隙を乗じる攻撃**の総称。警察や銀行員を装ってキャッシュカードの暗証番号を聞き出すような詐欺も、ソーシャルエンジニアリングの一種
キーロガー	キーボードから入力されたストロークを記録する仕組み。これとデータ送信機能を組み合わせ、入力情報の盗難に悪用されることもある
バックドア	正規の手続きを踏まずに利用できる**不正なアクセス経路**。侵入者が次回の侵入に備えて意図的に作りこむことが多い。バックドアをつくり侵入の痕跡を消去する、ルートキット(rootkit)とよばれるツール群もある 【対処例】ログの分析など

不正アクセスの脅威と対策

フットプリンティング	攻撃対処の弱点を発見するために、攻撃者が行う事前調査および偵察行為
ブルートフォース攻撃	総当たり攻撃。パスワードや暗証番号に対して、可能性のあるすべての組合せを試す。桁の少ない単純なパスワードは、ブルートフォース攻撃に耐えられない恐れがある。 【対処例】単純なパスワードを使用しない
パスワードリスト攻撃	すでに流出したパスワードを再利用してログインを試みる攻撃 【対処例】同じパスワードを使い回さない
SQLインジェクション	不正なSQLを含む悪意の入力データを与え、データベースに対する不正な問い合わせを実行させる攻撃 【対処例】バインド機構の利用、サニタイジング、WAF

SQLインジェクション

```
SELECT *
   FROM member
   WHERE name = ' ? '
```

社員情報確認ウィンドウ

社員名を入力して
表示ボタンを押してください

太田学'OR'X'='X

表示

```
SELECT *
   FROM member
   WHERE name = '太田学' OR 'X' = 'X'
```

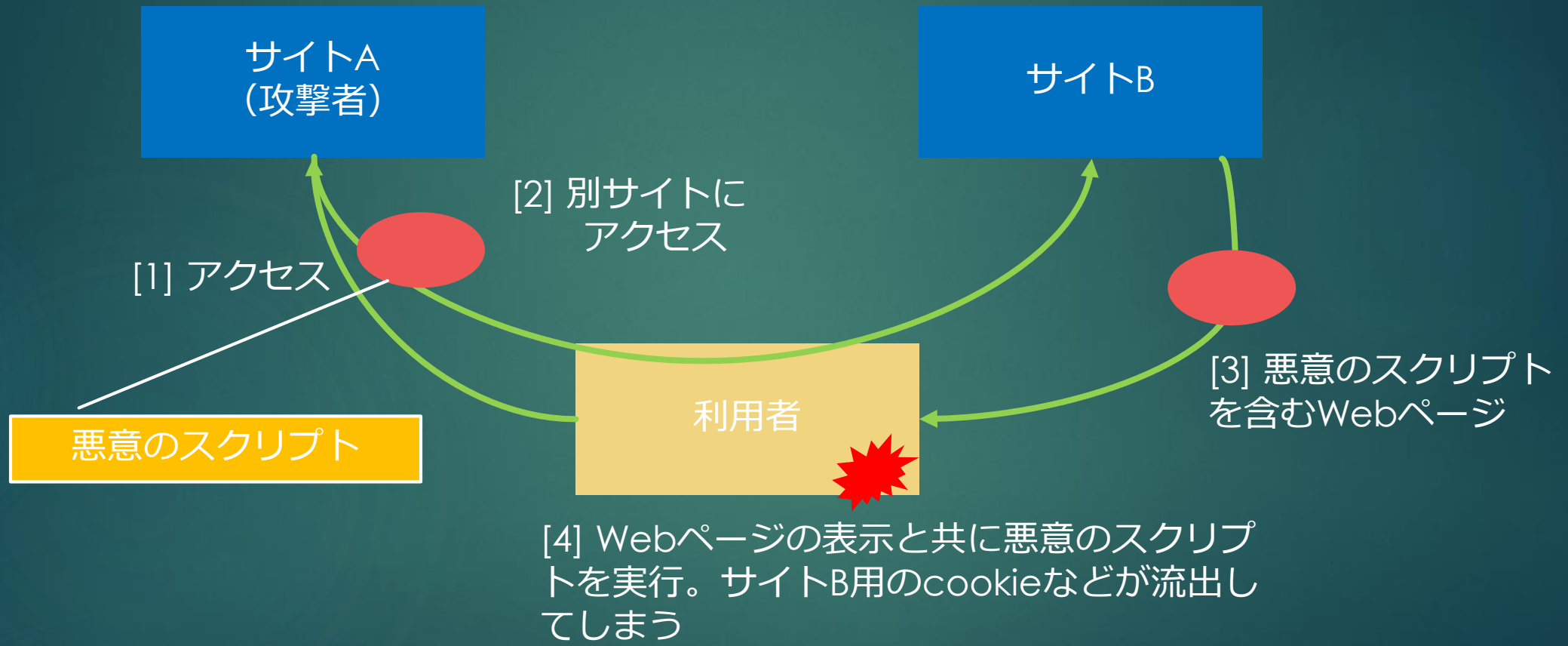
意図しないSQL文の実行
'X'='X'は常に成立するので、
member表の全行を表示する

SQL文を含む
不正な入力が行われる

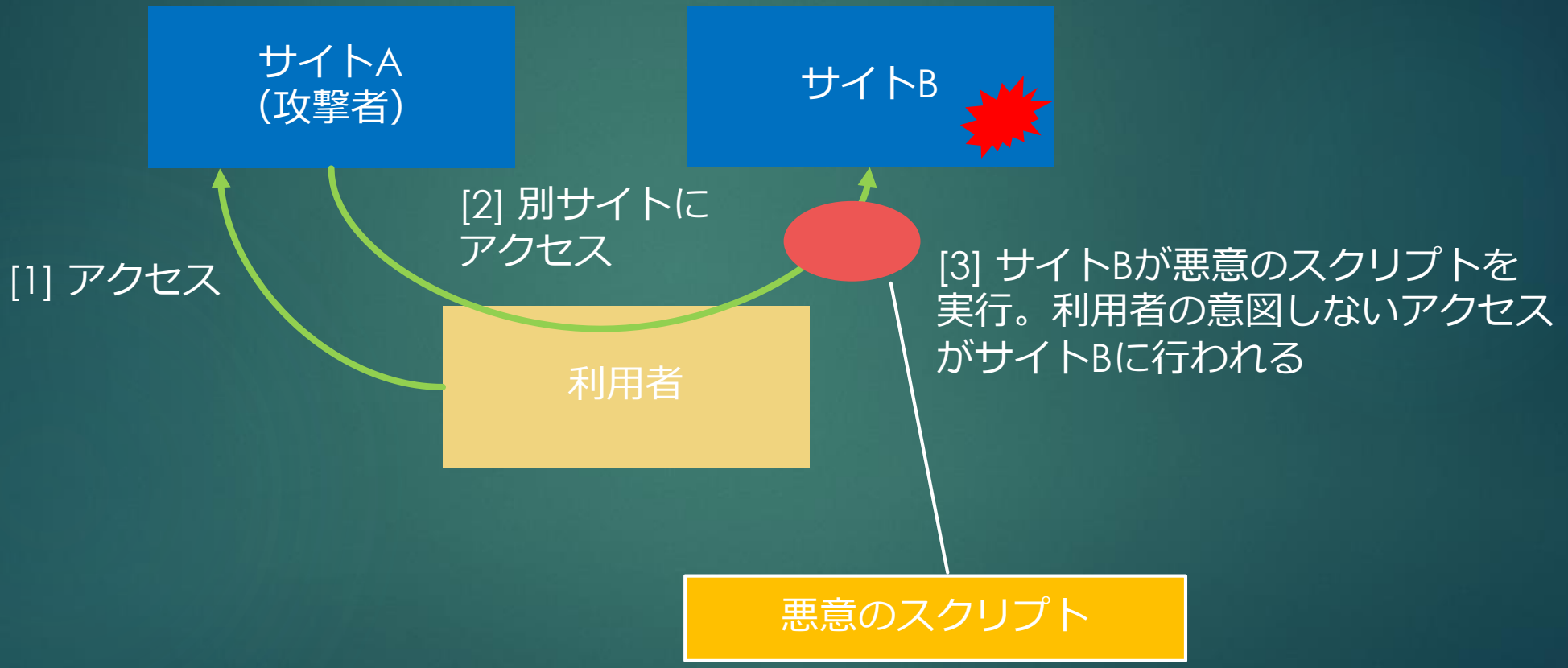
不正アクセスの脅威と対策

コマンドインジェクション	**不正なOSコマンドを含む悪意の入力データ**を与え、これを実行させる攻撃 【対処例】シェルを起動できる機能を使わない、サニタイジング
クロスサイトスクリプティング(XSS)	攻撃者から送り込まれた悪意のスクリプトを、**別サイトのアクセス時に実行させる**攻撃 【対処例】サニタイジング
クロスサイトリクエストフォージェリ(CSRF)	攻撃者が用意したサイトから不正なHTTPリクエストを送信することで、別サイトに対して利用者の意思ではない操作を行わせる攻撃。サイトをまたがって不正なスクリプトを実行する点でXSSと似ているが、XSSは不正な処理がクライアント側で実行されるのに対し、CSRFはサーバ側（サイト側）で不正な処理が実行される。 【対処例】パスワードの再入力、CAPTCHA

クロスサイトスクリプティング



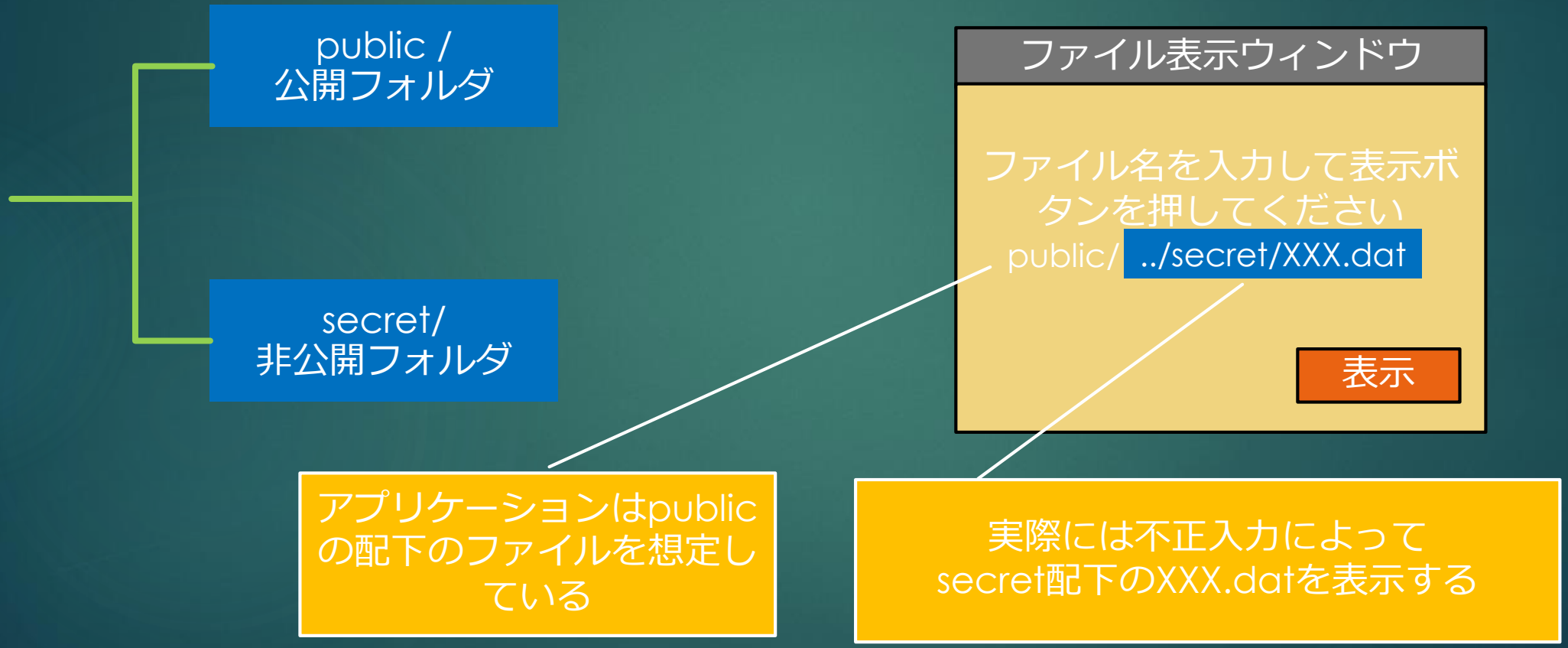
クロスサイトリクエストフォージェリ



不正アクセスの脅威と対策

ゼロディ攻撃	脆弱性が明らかになった直後に攻撃を開始すること。脆弱性の公表とセキュリティパッチの提供とのタイムラグに乗じて、対策が行われる前に脆弱性を攻撃する
ディレクトリトラバーサル攻撃	パス付きのファイル名の入力を想定していないプログラムに対し、パスを含むファイル名を直接指定することで、本来は許されていないファイルに不正にアクセスする攻撃 【対処例】ファイルパスを指定しない（パスの削除）
Dos攻撃	サーバなどを標的にアクセスを大量に発生させ、サービスが提供できない状態に追い込む攻撃
フィッシング	電子メールなどで不正なURLを送り付け、偽のWebサイトに誘導し、機密情報の搾取や詐欺行為を行う攻撃

ディレクトリトラバーサル



不正アクセスの脅威と対策

IPスプーンフィング	攻撃者のコンピュータのIPアドレスを、別に用意した偽のIPアドレスに付け替えて偽装する手口
セッションハイジャック	セッションIDの予測や盗聴などを通じて他者のセッションを横取りし、そのセッション上で不正な操作を行う攻撃 【対処例】予測困難なセッションIDを用いる
DNSキャッシュポイズニング	不正なドメイン情報を含むパケットを、DNSの応答を偽ってDNSサーバに送り込んでキャッシュさせる。これをもとに、利用者を悪意のサイトに誘導する攻撃

不正アクセスへの対策

- 不正アクセス全般

WAF(Web Application Firewall)は、**Webアプリケーションに対するアクセスを監視し**、不正なアクセスを遮断するファイアウォールである。WAFのもつサニタイジング機能は、SQLインジェクションやコマンドインジェクション、クロスサイトスクリプティングなどで入力された不正コマンドを無力化するので、WAFの設置は不正アクセス全般に対して極めて有効である。

- クロスサイトリクエストフォージェリ対策、セッションハイジャック

これらの対策には、HTTPリクエストを発したのが人間（利用者本人）仮想ではないかを識別することが求められる。重要なイベントごとに**パスワードの入力を求めたり、CAPTCHA**を適切に利用するとよい。

不正アクセスへの対策

- 非公開サービスへのアクセス遮断

公開していないサービスへのアクセスを遮断するためには、パケットフィルタリング型の**ファイアウォール**をインターネットと内部ネットワークの接点に設置する。

- その他

セキュリティ機能を常に最新に保つこと、怪しいサイトには近づかないことなどは、原則的な対処といえる。URLフィルタリングなどの利用が有効である。また無線LAN環境で、**WPA2**などによる暗号化や、アクセスポイントの存在を隠す**SSIDステルス**などの利用も有効である。

不正アクセスへの対策

- 不正アクセスへの究明

万一不正アクセスを含むコンピュータ犯罪が発生した場合には、ログを分析して不正アクセスの足跡を追跡し、証拠データを解析して原因を追究する。これらの技術を、**ディジタル鑑識（ディジタルフォレンジックス）**と総称する。

不正アクセスへの対策

サニタイジング	入力データに含まれるHTMLタグやプログラム、SQL文などを無害化すること
CAPTCHA	機械では判別しにくいゆがんだ文字の画像を表示し、目視で読み取らせて入力させる仕組み
URLフィルタリング	閲覧させたくないWebページにアクセスできないようにする仕組み。閲覧を禁止するWebページをブラックリストに、許可するWebページをホワイトリストに登録し、これらに基づいてアクセスを制御する

コンピュータウイルスの脅威と対策

- コンピュータに被害を与えるプログラムのうち、

自己伝染機能、潜伏機能、発病機能

をもつものを**コンピュータウイルス**という。ただし、広義には、利用者に被害を与えるような不正プログラムをコンピュータウイルスということもある。また、悪意をもって作成された、利用者の意図しない動作をする不正なプログラムを総称して**マルウェア**ともいう。

マルウェアの種類と特徴

種類	特徴
ファイル感染型ウイルス	実行可能ファイルに感染するタイプのウイルス。ウイルスプログラム単体では動作せず、既存の実行可能ファイルに追記または上書きする形で感染し、感染したファイルの実行に伴い、起動する
ブートセクタ型ウイルス	フロッピーディスクのブートセクタなど、システムを起動するために必要な領域に感染するウイルス。ハードディスクに感染するものもある
マクロウイルス	ワープロや表計算といったアプリケーションのマクロ機能を利用し、データファイル経由で感染するため、実行されるプラットフォームには依存しない
ワーム	単体での動作が可能であり、システム上で自信を複製し、自己増殖する機能をもつ不正プログラム。現在では、OSやアプリケーションの脆弱性を利用してネットワークを介して増殖を繰り返すものが多い
トロイの木馬	単体での動作が可能であり、有用なプログラム（ユーティリティやゲームなど）を装って実行されるのを待つ不正プログラム
スパイウェア	ユーザの行動履歴や個人情報を収集するプログラム。有用なプログラムの一機能として含まれる場合もあり、利用許諾にて個人情報の収集を明示している場合は、不正プログラムとはみなされない場合もある

コンピュータウイルスの脅威と対策

- マルウェアは大きな社会問題になることも多く、2008年に猛威をふるったUSBワームはその一つといえる。**USBワーム**は自動実行の仕組みをUSBメモリ内に作成し、USBメモリ経由で感染を広げた。また、マルウェアがオンラインバンキングの通信を乗っ取り、振込先を改ざんする**Man-in-the-Browser**とよばれる攻撃も報告されている。

コンピュータウイルスの脅威と対策

- 対策

ウイルスを含むマルウェアの対策として

・出所の不明なファイルを不用意に開かない

・安易にプログラムをダウンロードしない

・怪しいWebサイトを閲覧しない

・OSやアプリケーションを最新の状態に保つ

・電子メールに添付されたファイルは慎重に扱う

・**ウイルス対策ソフト（ワクチンソフト）**を利用する

といった対策が効果的である。

コンピュータウイルスの脅威と対策

- ウイルス対策ソフトは、ウイルスの特徴的な部分を定義した**パターンファイル（シグネチャファイル、ウイルス定義ファイル）**と検査対象のファイル（またはプログラム）を比較する「パターンマッチング」によってウイルスを検出するものが多く、最新のウイルスに対処するために、

  ・パターンファイルを常に最新に保つ

  ことが非常に重要である。

ウイルス検出手法

インテグリティチェック法	ディジタル署名などの認証技術を適用する
コンペア法	安全に保管されている原本と比較する
チェックサム法	プログラム（実行ファイル）のサイズに変化がないか監視する
パターンマッチング法	ウイルスに特徴的な部分をパターンとして記録しておき、検査ファイルと照合する
ビヘイビア法	ウイルスによって引き起こされる動作パターンを監視する

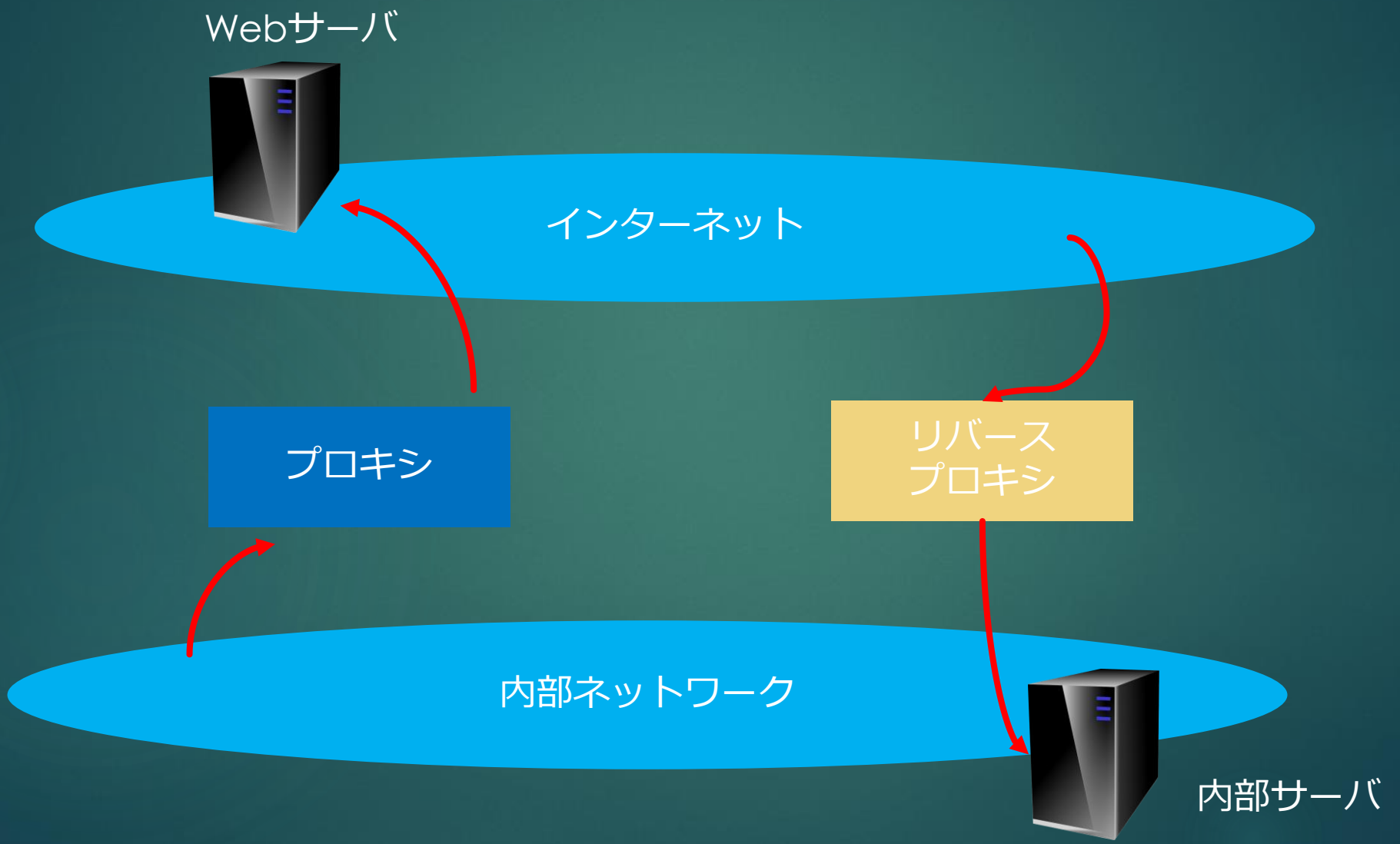
検疫ネットワーク

- ウイルスに対する安全性を高めるため、**検疫ネットワーク**を構築する方法もある。検疫ネットワークはウイルスの検査や利用者の認証を行う検査用のネットワークで、社内ネットワークからは独立している。クライアントはまず検疫ネットワークに接続し、認証やウイルスチェックを済ませた後、社内ネットワークに接続するという方法をとる。

その他

- ハードウェアやソフトウェアは、内部構造やデータを解析しにくくする、すなわち**耐タンパ性**を高める工夫が必要である。例えば、プログラムそのものを暗号化しておけば、逆アセンブルによる解析を防ぐことができる。盗聴やデータの不正利用に対しては、データの不可視化で対処することができる。データの不可視化には、暗号化の他にもデータ自体の存在を隠す方法（ステガノグラフィ、後述）がある。暗号化には各種のセキュリティプロトコルを使用する。
- **インターネットとの直接のアクセスを避ける**ため、プロキシやリバースプロキシを設置する。**プロキシ**はインターネット上のWebサーバへのアクセスを代理するサーバである。**リバースプロキシ**は内部サーバの代理として、インターネットからの要求を受け付けるサーバで、これを設置すればインターネットからの直接アクセスを防止できる。**ペネトレーションテスト**を実施して、不正に侵入できないかどうかを確認することも大切である。

プロキシ / リバースプロキシ



ステガノグラフィ

- データを暗号化するのではなく、データの存在を隠してしまうという方法を**ステガノグラフィ**という。例えば、音声や画像データの中で人間に検知できない部分を使ってメッセージを埋め込めば、画像や音声の送信に隠れてメッセージを送信することができる。画像に著作権データを埋め込む**電子透かし**はステガノグラフィの一種である。

セキュリティプロトコル

- 暗号化や認証機能を提供するプロトコルをセキュリティプロトコルと総称する
- セキュリティプロトコル

名称	用途	概要
SSL(Secure Socket Layer)	TCP通信全般	TCPを拡張して認証や暗号化の機能を提供する
IPsec	IP通信全般	IPパケットレベルで認証や暗号化の機能を提供する
HTTPS (HTTP over SSL/TLS)	主にHTTP	下位層にSSLを用いることで、HTTP通信に認証や暗号化の機能をもせたプロトコル
SET(Secure Electronic Transaction)	クレジット掲載	クレジット決済を安全に行うためのプロトコル
PGP (Pretty Good Privacy)	電子メール	電子メールの暗号化や電子署名の機能を提供する。公開鍵は第三者ユーザが保証する（信用の輪）

セキュリティプロトコル

名称	用途	概要
S/MIME (Secure/Multipurpose Internet Mail Extensions	電子メール	電子メールの暗号化や電子署名の機能を提供する。公開鍵は認証局が保証する
SMTP-AUTH	電子メール	利用者認証を行い、成功した場合のみ電子メールを受け付ける
SPF (Sender Policy Framework)	電子メール	IPアドレスをもとに、正しい送信者かどうかを判断する
SSH(Secure SHell)	リモートコンピュータの利用	リモーロコンピュータへのログインや操作を安全に行う
OCSP (Online Certificate Status Protocol)	ディジタル証明書	証明書が失効しているかどうかを確認する

セキュリティプロトコル

- SSLは最も広く用いられているセキュリティプロトコルで、これをハードウェア的に実装する機器（**SSLアクセラレータ**）もある。SSLやIPsecなどを用いてインターネット上に構築した仮想的な専用ネットワークを**VPN(virtual Private Network)**とよぶ。

5. 情報セキュリティマネジメント
情報セキュリティとは

- JIS Q 27001は情報セキュリティを「情報の機密性、完全性及び可用性を維持すること」と定義している。これらの特性は、その頭文字をとって情報セキュリティのCIAともよぶ。

機密性(Confidentiality)	認可されていない個人、エンティティまたはプロセスに対して、情報を使用不可または非公開にする特性
完全性(Integrity)	資産の正確さおよび完全さを保護する特性
可用性(Availability)	認可されたエンティティが要求したときに、アクセスおよび使用が可能である特性

情報セキュリティとは

- これに加え「さらに真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めてもよい」と定義を拡張している。

真正性(Authenticity)	ある主体または資源が、主張通りであることを確実にする特性
責任追跡性(Accountability)	あるエンティティの動作が、その動作から動作主のエンティティまで一意に追跡できることを確実にする特性
否認防止(Non-Repudiation)	ある活動または事象が起きたことを、後になって否認されないように証明する能力
信頼性(Reliability)	意図した動作及び結果に一致する特性

情報セキュリティとは

- 情報セキュリティインシデント

情報セキュリティインシデントは、コンピュータの誤操作や情報資産の管理ミス、パスワードの漏洩など、**情報セキュリティを脅かす出来事**をいう。

- 脅威

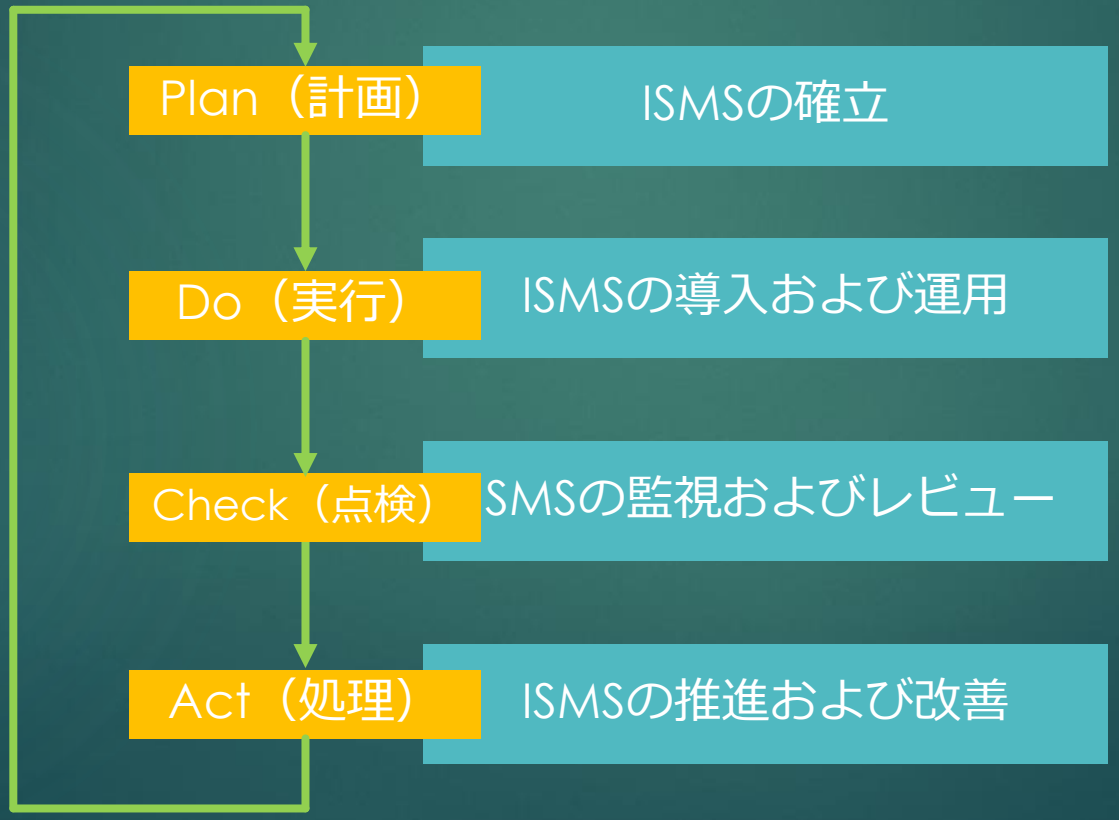
脅威は、システムまたは組織に損害を与える可能性がある**インシデントの潜在的な原因**をいう。

- 脆弱性

脆弱性は、一つ以上の脅威がつけこむことができる、資産または資産グループがもつ弱点をいう。

情報セキュリティマネジメント

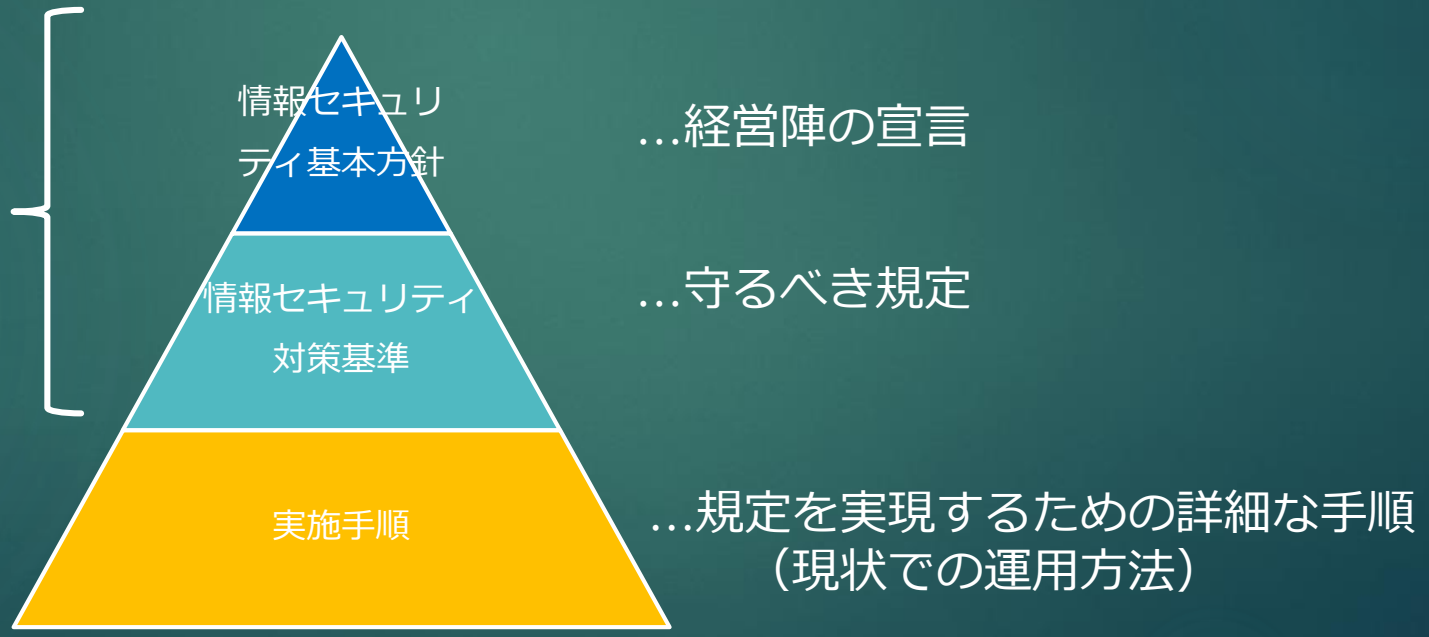
- 情報セキュリティを維持し、継続的に改善する一連の管理活動を**情報セキュリティマネジメント**といい、このための仕組みを**情報セキュリティマネジメントシステム(ISMS**：Information Security Management System)という。JIS Q 27001ではISMSにPDCAモデルを採用している。



継続的改善によって
情報セキュリティ水準の
向上を図る

情報セキュリティポリシ

- ISMSの確立時に作成される基本方針および対策基準を情報セキュリティポリシとよぶ。情報セキュリティポリシは、ISMSのプロセスを実施するうえでの核となる方針、基準である。多くの場合、情報セキュリティポリシは階層構造で考える。
- 2階層ポリシモデル



情報セキュリティポリシ

- 情報セキュリティ基本方針

基本方針には、情報セキュリティの目標および原則を指示する経営陣の意向、リスクマネジメントを含め管理目的・管理策を設定するための枠組み、情報セキュリティマネジメントにおける責任の定義といった、**組織が情報セキュリティに取り組むための基本的な方針**（何をどのような脅威から、なぜ保護するのか）が盛り込まれる。

- 情報セキュリティ基準

対策基準には、基本方針をどのように実現すればよいのかといった観点から、**遵守すべき行為や判断基準**などが盛り込まれる。

リスク分析

- ISMSの確立にあたっては、組織に影響与えるリスクを特定し、その分析および評価を行う。リスク分析の手法には、定性的リスク分析手法と定量的リスク分析手法がある。

定量的リスク分析手法	過去の被害件数や被害額をもとに、リスク値を「予想損失額×発生確率」などのように金額ベースで算出する
定性的リスク分析手法	リスク値を点数や段階などで評価する。例えば「資産価値（１～５）×脅威（１～３）×脆弱性（１～３）」でリスク値を算出するとき、リスク値は１～４５で評価される

リスク対応

- JIS Q 27001では、リスク対応を「リスクを変更させるための方策を選択及び実施するプロセス」と定義している。
- リスクを変更するための方策

方策	内容	例
リスク低減	適切な管理策（コントロール）を採用することにより、リスクが発生する可能性やリスクが発生した場合の影響度を低減する	セキュリティ技術の導入、入り口の施錠、スプリンクラの設置など
リスク回避	リスクと資産価値を比較した結果、コストに見合う利益が得られない場合など、資産ごと回避する	業務の廃止、資産の廃棄など
リスク移転	資産の運用やセキュリティ対策の委託、情報化保険など、リスクを他者に移転する	ハウジングサービスの利用、情報化保険の加入など
リスク受容	識別されており、受容可能なリスクを意識的、客観的に受容する。リスクが顕在化したときは、その損害を受け入れる	会社が損失額を負担するなど

インシデント対応

- インシデントが発生した場合、あらかじめ計画しておいた手順に沿って対策チームが対応する。このような**インシデント対応の専門チーム**を**CSIRT（シーサート）**とよぶ。
- 各企業のCSIRTを連係させるためのコーディネーションセンタが設置されることもある。日本では**JPCERT/CC**がその役割を果たしている

JPCERT/CCの役割（参考）

・インシデント報告の受付
・対応の支援
・発生状況の把握
・手口の分析
・再発防止策の検討や助言

情報セキュリティの規格

JIS Q 27001	情報セキュリティマネジメントシステムの**要求事項**。情報セキュリティマネジメントの導入・実践にあたって要求される事項をまとめた規格
JIS Q 27002	情報セキュリティマネジメントの**実践のための規範**。実践にあたっての手引きとなる規格
ISO/IEC 15408	情報技術を利用した製品やシステムのセキュリティ機能が、評価基準に適合するかを評価するための規格
JCMVP	暗号モジュール試験及び認証制度。暗号化や署名機能が正しく実装されており、暗号鍵やパスワードを適切に保護していることを試験、認証する制度
JISEC	ITセキュリティ評価および認証制度。IT関連製品のセキュリティ機能を、ISO/IEC 15408に基づいて評価、認証する制度