クレジット：
UTokyo Online Education Education コンピュータシステム概論 2018 小林克志

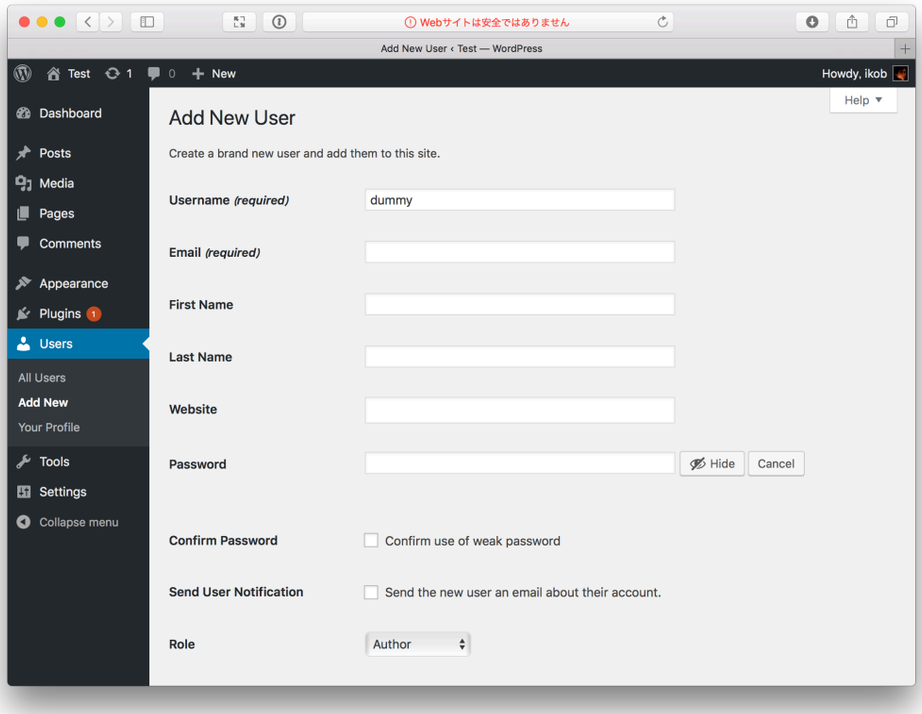
コンピュータシステム概論
第10回

小林克志

- 事務連絡
- 先週の課題、レビュー（振り返り）
- まくら
- SSL / TLS
- 公開鍵基盤 (PKI:Public Key Infrastructure)
- 演習: X509 証明書の表示
- 演習: SSL/TLS 対応 Web サーバ

課題 1 wordpress ユーザ追加とデータベース確認

- 前ページまでの演習で Wordpress データベースのユーザテーブルの内容を確認
- 以下の URL から Wordpress の管理画面にアクセス
  http://<自身が install した wordpress>/wp-admin
- Users-> Add New で近くの席の学生をユーザとして追加する。
  - Role は Author
  - **Send User Notification は OFF**
- Users-> Add New で近くの席の学生をユーザとして追加する。
- SQL コマンドでユーザが追加できていることを確認する。SQL コマンドの出力結果をレポートする。



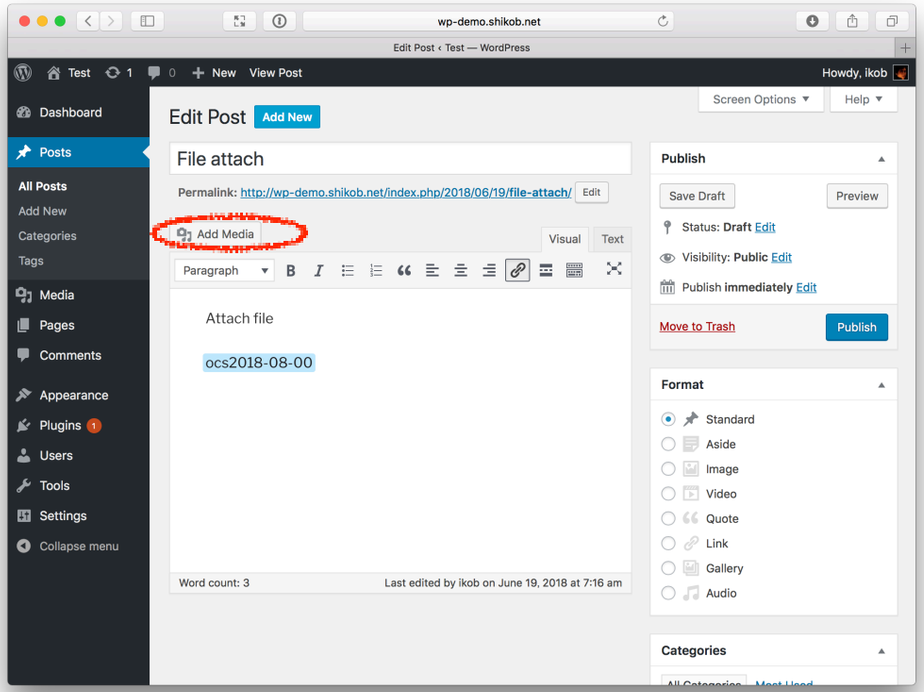
The WordPress software, GPLv2

課題 2 WordPress ファイルアップロードとデータベース確認

- chown で WordPress 関連ファイルの権限を変更する

```
$ cd /var/www
$ sudo chown -R apache.apache *
```

- +New をクリック、新規ページ作成画面に遷移する。
- 作成画面で Add Media をクリック
- 適当な画像 or PDF ファイルをアップロードする。
- ページに Insert するかどうか聞かれるので Insert し、ページを Publish する。
- SQL コマンドで wp_posts に新しいページ、アップロードされたファイルの URL(guid) が追加されていることを確認する。
- アップロードしたファイルの実体は別にある。WordPress サーバのどこに置かれるか？実態が別にあることの利点・欠点を考察せよ。



The WordPress software, GPLv2

著作権の都合により
ここに挿入されていた画像を削除しました

2018年6月27日　日本経済新聞電子版
「みずほ証券ネット取引停止、
丸1日たっても復旧せず」
https://www.nikkei.com/article/DGXMZO3228961
0X20C18A6000000/

著作権の都合により
ここに挿入されていた画像を削除しました

2018年6月27日　日本経済新聞電子版
「ネット振り込みに障害　りそなや新生など」
https://www.nikkei.com/article/DGXMZO3229115
0X20C18A6MM0000/

Mizuho Bank, Ltd.

新システムへの移行に関するご案内 | みずほ銀行

個人のお客さま　法人のお客さま　みずほ銀行について　ニュースリリース　採用情報　English　FAQ

MIZUHO みずほ銀行

商品・サービス　各種お手続き　キャンペーン プラン情報　ATM・店舗　金利・手数料

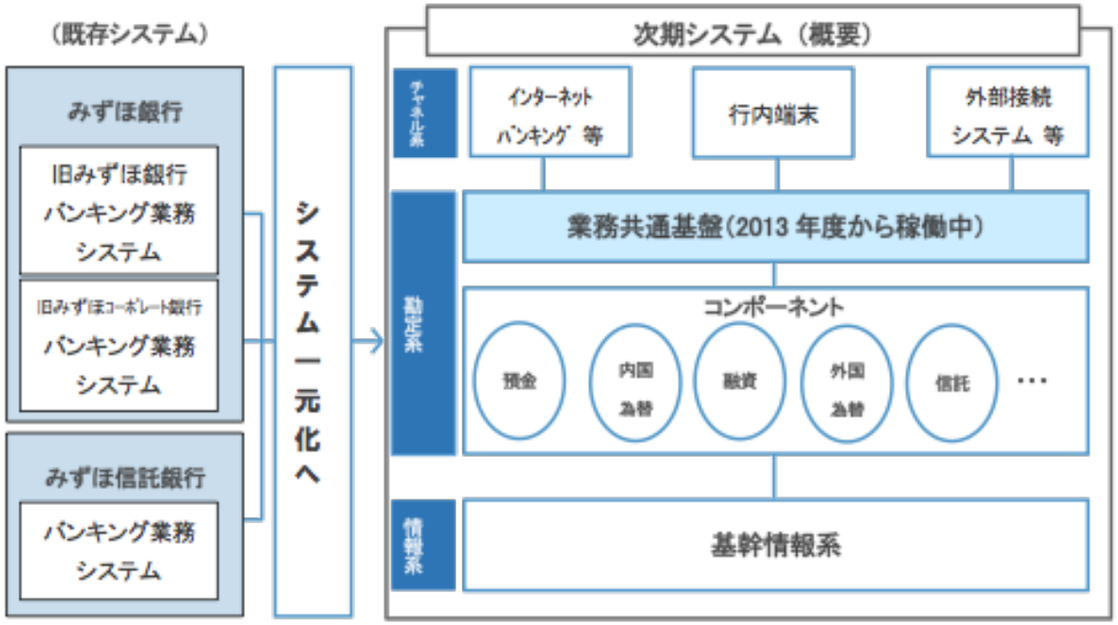
ホーム> 新システムへの移行に関するご案内

平素は格別のお引き立てを賜り、厚くお礼申しあげます。
新システムへの移行により、新サービスへの柔軟な対応や新規開発の期間短縮等を実現し、お客さまへのサービスや利便性の向上を一層進めてまいります。
今後も<みずほ>は、お客さまへのよりよいサービスの提供に社員一丸となって取り組んでまいります。
引き続きご支援ご愛顧を賜りますようお願い申しあげます。

みずほ銀行HP　新システムへの移行に関するご案内 ©2013 Mizuho Bank, Ltd.
https://www.mizuhobank.co.jp/transition/index.html?rt_bn=top_transition_bnr

（別紙 1）

＜次期システムへの移行（イメージ図）＞



＜次期システム移行による実現事項＞

- ■ 旧みずほ銀行/旧みずほコーポレート銀行/みずほ信託銀行の勘定系システム一元化
  - IT システムのスリム化・効率化
  - 障害対応力の向上
- ■ 業務・機能別にコンポーネント化
  - シンプルな構成による柔軟性向上
  - 新サービスへの柔軟な対応が可能に
  - 新規開発の期間短縮・コスト削減
- ■ 最先端の「次世代」勘定系システム
  - サービス提供基盤の強化
  - 事務処理スピードの向上

みずほ銀行HP 「次期勘定系 システムへの移行 」および「 移行に伴う オンラインサービスの臨時休止 」について（2018年2月15日付け）別紙1

https://www.mizuhobank.co.jp/transition/index.html?rt_bn=top_transition_bnr

ネットワークサービス に対する脅威

- ネットワーク
  - なりすまし
  - 盗聴
  - 改ざん
  - …
- 端末・サーバ
  - 侵入
  - マルウェア
    - 遠隔実行によるリソース搾取、情報奪取・破壊
  - …
- 複合
  - 分散サービス妨害 (Distributed Denials of Service (DoS))

SSL(Secure Socket Layer)
TLS(Transport Layer Security)

- 機能
  - デジタル署名によるサーバ認証
  - デジタル署名によるクライアント認証（あまり使われていない）
  - 暗号化による機密性
  - メッセージ認証コード（Message Authentication Code, MAC）による完全性
- 歴史
  - 1994：Netscape によって SSL 2.0
  - 1995 : Netscape によって SSL 3.0
  - 1999 : IETF によって TLS 1.0 RFC2246
  - 2018: IETF によって TLS 1.3

SSL / TLS（続き）

- 利用者・開発者・Web サービス提供者にとって使いやすく、一気に普及した
  - 利用者：SSL/TLS とルート証明書を組み込んだブラウザだけ用意すれば済む
  - プログラム開発者：ネットワーク・トランスポート層の中間に実装されるため既存プログラムの改修範囲が限定的で済む（wrapper を使えば改修すら不要）
  - Web サービス提供者：サーバ証明書を用意すれば済む
- 3つの技術を利用して、認証、機密性、完全性を実現
  - 公開鍵：
    - デジタル署名によるサーバ/クライアント認証
    - 共通鍵の交換
  - 共通鍵：
    - 通信を暗号化し機密性
  - MAC：
    - 衝突耐性の高いハッシュにより改ざん検出

ネットワークサービス に対する脅威

- ネットワーク
  - なりすまし
  - 盗聴
  - 改ざん
  - …
- 端末・サーバ
  - 侵入
  - マルウェア
    - 遠隔実行によるリソース搾取、情報奪取・破壊
  - …
- 複合
  - 分散サービス妨害 (Distributed Denials of Service (DoS))

公開鍵暗号
(Public Key Cryptography) (再掲)

- 送信者が暗号化・受信者が復号化にあたって別の鍵、それぞれ公開鍵・秘密鍵を利用する暗号化方式。以下の性質を利用して送受信者間で安全な通信がおこなえる。
  - 公開鍵は公開情報として配布しておけば暗号化はだれにでもおこなえる、
  - 秘密鍵は公開されていないので、復号化は持ち主にしかできない。
  - 以下の課題もあるが、公開鍵暗号の応用である程度解決できる:
    - だれでも暗号化できるので送信者を特定するには、デジタル署名が必要になる。**これを利用して認証をおこなうこともできる。**
    - 配布されている公開鍵の信頼性は別に担保する必要がある。e.g. PKI(Public Key Infrastructure)
- 暗号・復号化に同じ鍵を利用する共通鍵暗号では、送受信者が安全に鍵を共有することに普及の困難さがあった。公開鍵によってこの問題を回避することができる。

公開鍵による電子署名と認証

- 秘密鍵で生成した署名を、公開鍵で検証できることが必要
  - ざっくり言えば、
    - 署名 = 秘密鍵で平文（のハッシュ値）を復号化したもの
    - 検証 = 公開鍵で署名を暗号化、平文（のハッシュ値）と比較
- 送信者の認証方式は（送受信者が）オフライン・オンラインで手続き・安全性は異なる。
  - オフライン
    1.送信者が自分の秘密鍵で本文に署名
    2.送信者から受信者に本文＋署名を転送
    3.受信者は必要な時点で送信者の公開鍵で署名を検証
  - オンライン：
    1.受信者が送信者にチャレンジ（乱数）を送る
    2.送信者は自分の秘密鍵でチャレンジに署名
    3.送信者は受信者にチャレンジ＋署名を転送
    4.受信者は送信者の公開鍵で署名を検証

公開鍵基盤・PKI
(Public Key Infrastructure)

- 公開鍵を利用した電子署名によって問題を解決:
  - 未知の相手を信用できるか？
    - 信用の連鎖(Chain of Trust)
      - 信用できる既知のだれかに保証してもらう。
        - 有効期間前の失効手続きもセットで必要。
    - 初期(出荷)状態では既知はいないのでは？
      - 出荷物に信用できる既知の相手を埋め込む。
        - 信用点・トラストアンカー(Trust Anchor)
- ビジネスモデルとの親和性:
  - 信用点は保証行為の対価を利用者から得る
  - ベンダーは出荷物への埋め込み対価を信用点から得る
  - 情報システム全体として信頼性の向上

IETF Public-Key Infrastructure using X.509 (PKIX) RFC5280

- X.509 は X.500 ディレクトリ（サービス）仕様の一部として 1988 年に初版が公開された証明書形式である。X.509 は現在 IETF PKIX で利用されている。
- IETF PKIX の構成要素：
  - エンドエンティティ：end entity (EE)
    - 証明書利用者 or/and 証明書が対象とするユーザ端末
  - 認証局：Certification Authority (CA)
    - 証明書の発行、失効リストの管理
  - 登録局：Registration Authority (RA)
    - CA より役割の一部を委託される
  - 失効リスト発行者：CRL issuer
    - 失効リスト(Certification Revocation List)の発行・署名をおこなう
  - レポジトリ：repository
    - 証明書・失効リストの保管・配布

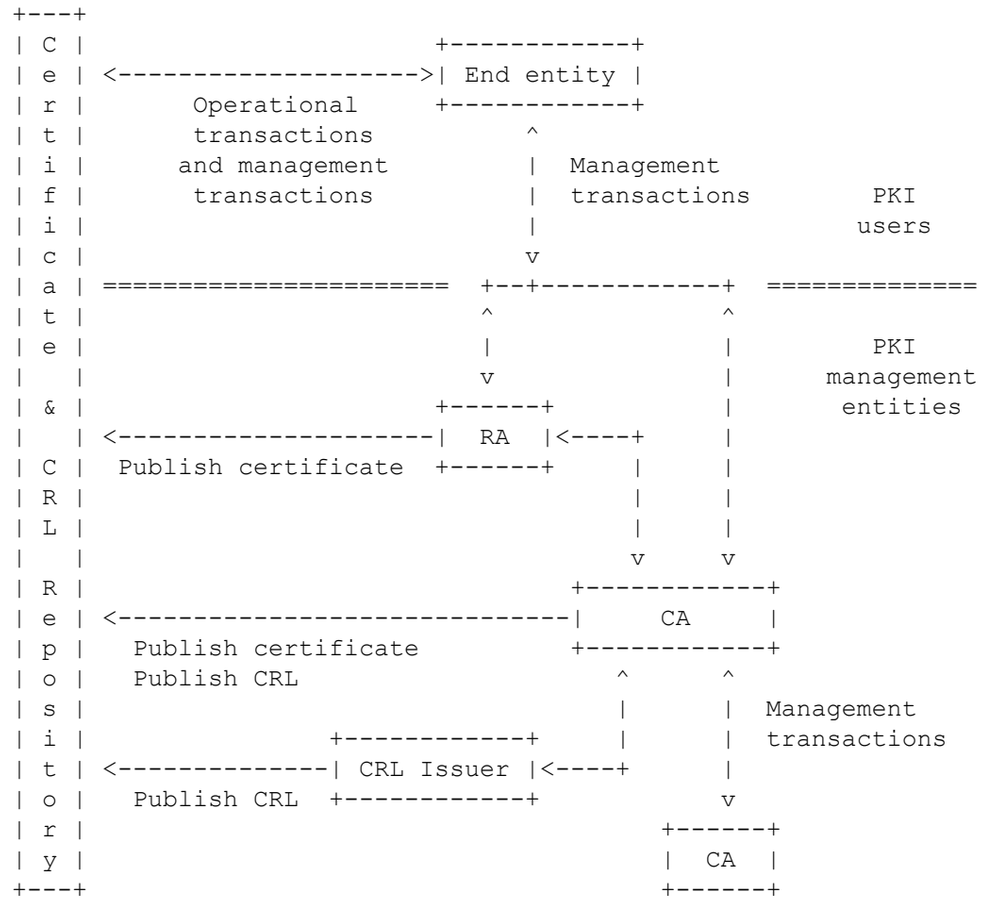


Figure 1. PKI Entities

IETF Public-Key Infrastructure using X.509 (PKIX) RFC5280, p.8 Figure 1. PKI Entities
https://datatracker.ietf.org/doc/rfc5280/?include_text=1

PKI サーバ証明書では
何を保証している / していないのか？

- 一般のサーバ証明書:
  - 単に鍵アイコンがブラウザで表示されるだけ。詐欺サイトも通常サイトと区別できない。
    - 今日では、ドメイン所有者であれば（ほぼ）無審査・無償で発行される。過去には発行審査コストが高時代もあったが、競争によって劇的に下がった
    - 盗聴・改ざん・なりすまし対策としての暗号化が目的で、発行先が信用できるかどうかはわからない。
- Extended Validation (EV)証明書:
  - サイトの悪意の有無を評価するものではない。
    - 発行元が発行先の審査を厳格（物理・法的実在性の確認）におこなう。
    - 対応ブラウザでは視覚的に EV 証明書とそれ以外を区別する。
      e.g., 緑色のアドレスバー

演習：X509 証明書を表示してみる(0/)

- 注意：
  - OpenSSL が必要になります。
  - AWS Educate Starter が使えない場合は自身のコンピュータか基盤センターの MacOS で試してください。

演習：X509 証明書を表示してみる（1/）

- 講義 Web の概要ページから、
「ocs.shikob.net 秘密鍵・証明書」
をダウンロード・展開する。
- ocs.shikob.net ディレクトリに移動する
- AWS のサーバ（Web ブラウザがインストールされていない）を利用する場合は、例えば、

  1.自身の PC にダウンロード

  2.scp コマンドで AWS サーバにコピーする。
  scp -r はディレクトリ以下を再帰的にコピーする。
  コピー先ホストの IP アドレス末尾にコロン記号を入れること（ホストではなくファイル名と認識されてしまうため）

```
$ scp -r ocs.shikob.net ec2-user@aa.bb.cc.dd:
```

演習：X509 証明書を表示してみる(2/)
RSA 秘密鍵

```
$ openssl rsa -in privkey1.pem -text
Private-Key: (2048 bit)
modulus:
ここに秘密鍵の情報が 16 進数で表示される
```

- 注意：秘密鍵は X509 形式ではない

演習：X509 証明書を表示してみる（3/）
サーバ証明書

- *.ocs.shikob.net の（ワイルドカード）サーバ証明書

```
$ openssl x509 -in cert1.pem -text      表示コマンド
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            03:d2:a6:30:af:7e:8d:63:11:0f:50:d6:82:fb:31:95:f1:23
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3        発行者
        Validity                                                            有効期間
            Not Before: Jun 23 14:57:21 2018 GMT
            Not After : Sep 21 14:57:21 2018 GMT
        Subject: CN=*.ocs.shikob.net                                        証明書が証明している事項
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment                         用途
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Subject Key Identifier:
                81:DE:83:7F:35:FA:9A:EA:2D:A5:90:F2:72:60:97:3D:59:AC:58:E2
            X509v3 Authority Key Identifier:
                keyid:A8:4A:6A:63:04:7D:DD:BA:E6:D1:39:B7:A6:45:65:EF:F3:A8:EC:A1

            Authority Information Access:
                OCSP - URI:http://ocsp.int-x3.letsencrypt.org               証明書の状態問い合わせ先
                CA Issuers - URI:http://cert.int-x3.letsencrypt.org/        発行者


            X509v3 Subject Alternative Name:
                DNS:*.ocs.shikob.net
            X509v3 Certificate Policies:
                Policy: 2.23.140.1.2.1
                Policy: 1.3.6.1.4.1.44947.1.1.1
                  CPS: http://cps.letsencrypt.org
                  User Notice:
                    Explicit Text: This Certificate may only be relied upon by Relying Parties and only in accordance with the Certificate Policy found at https://letsencrypt.org/repository/

            CT Precertificate SCTs:
                Signed Certificate Timestamp:
                    Version   : v1(0)
                    Log ID    :
                    Timestamp : Jun 23 15:57:21.351 2018 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
                Signed Certificate Timestamp:
                    Version   : v1(0)
                    Log ID    :
                    Timestamp : Jun 23 15:57:21.367 2018 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    Signature Algorithm: sha256WithRSAEncryption
         27:85:89:f4:9b:90:88:1a:67:4d:f4:aa:e5:0e:d3:c1:c9:c3:
```

演習：X509 証明書を表示してみる(4/)
認証局(CA)証明書

- Let's Encrypt 認証局(CA) に対する証明書

```
$ openssl x509 -in chain1.pem -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0a:01:41:42:00:00:01:53:85:73:6a:0b:85:ec:a7:08
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: O=Digital Signature Trust Co., CN=DST Root CA X3          発行者
        Validity
            Not Before: Mar 17 16:40:46 2016 GMT
            Not After : Mar 17 16:40:46 2021 GMT
        Subject: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3     証明事項
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign             用途
            Authority Information Access:
                OCSP - URI:http://isrg.trustid.ocsp.identrust.com
                CA Issuers - URI:http://apps.identrust.com/roots/dstrootcax3.p7c

            X509v3 Authority Key Identifier:
                keyid:C4:A7:B1:A4:7B:2C:71:FA:DB:E1:4B:90:75:FF:C4:15:60:85:89:10

            X509v3 Certificate Policies:
                Policy: 2.23.140.1.2.1
                Policy: 1.3.6.1.4.1.44947.1.1.1
                  CPS: http://cps.root-x1.letsencrypt.org

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://crl.identrust.com/DSTROOTCAX3CRL.crl

            X509v3 Subject Key Identifier:
                A8:4A:6A:63:04:7D:DD:BA:E6:D1:39:B7:A6:45:65:EF:F3:A8:EC:A1
    Signature Algorithm: sha256WithRSAEncryption
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

演習: SSL/TLS 対応 Web サーバ

- 秘密鍵・証明書をアップロードし、展開する。

```
> scp ocs.shikob.net.zip ec2-user@aa.bb.cc.dd:
Enter passphrase for key '/Users/ikob/.ssh/id_rsa':
ocs.shikob.net.zip
$ unzip ocs.shikob.net.zip
Archive:  ocs.shikob.net.zip
   creating: ocs.shikob.net/
  inflating: ocs.shikob.net/privkey1.pem
  inflating: ocs.shikob.net/fullchain1.pem
  inflating: ocs.shikob.net/cert1.pem
  inflating: ocs.shikob.net/chain1.pem
>
```

- サーバに ssh でログインし、mod24_ssl を導入する

```
$
$ sudo yum -y install mod24_ssl
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

$
```

演習: SSL/TLS 対応 Web サーバ

- 秘密鍵・証明書をコピーする

```
$ cd ocs.shikob.net
$ sudo cp privkey1.pem /etc/pki/tls/private/localhost.key
$ sudo cp cert1.pem /etc/pki/tls/certs/localhost.crt
```

- Apache HTTPD を再起動する

```
$
$ sudo service httpd restart
Stopping httpd:                            [  OK  ]
Starting httpd:                            [  OK  ]
$
```

- Web ブラウザで https://[登録した名前]/index.html にアクセスする。
  Wordpress の場合は設定が必要になる。
- ブラウザの「鍵」アイコンをクリックし、以下を確認する。
  - 証明書の内容
  - トラストチェイン
- 以下の操作で OS / ブラウザに root 証明書が組み込まれていることを確認する
  - MacOS: /Applications/Utilities/Keychain¥ Access.app
  - Windows10: コントロールパネル -> コンピュータの管理-> 証明書の管理
  - ブラウザによっては証明書管理をブラウザ自身がおこなっているものもある

課題：https://www.kantei.go.jp のサーバ証明書

- 表記サイトのサーバ証明書、ルート証明局からのトラストチェインについて説明せよ。
- 日本政府は公的個人認証サービス（JPKI）を運営、ルート証明局も稼働している。しかしながら、官邸の Web サイトではこの証明局は利用されていない。官邸が JPKI を利用しない理由を考察せよ。
- 講義 Web より回答すること。