身体はhttpsを求める

nashikです

最近やっているゲーム

AC6、ピクミン4、原神、タルコフ

ロボットをぐりぐり動かすのたのしいですね

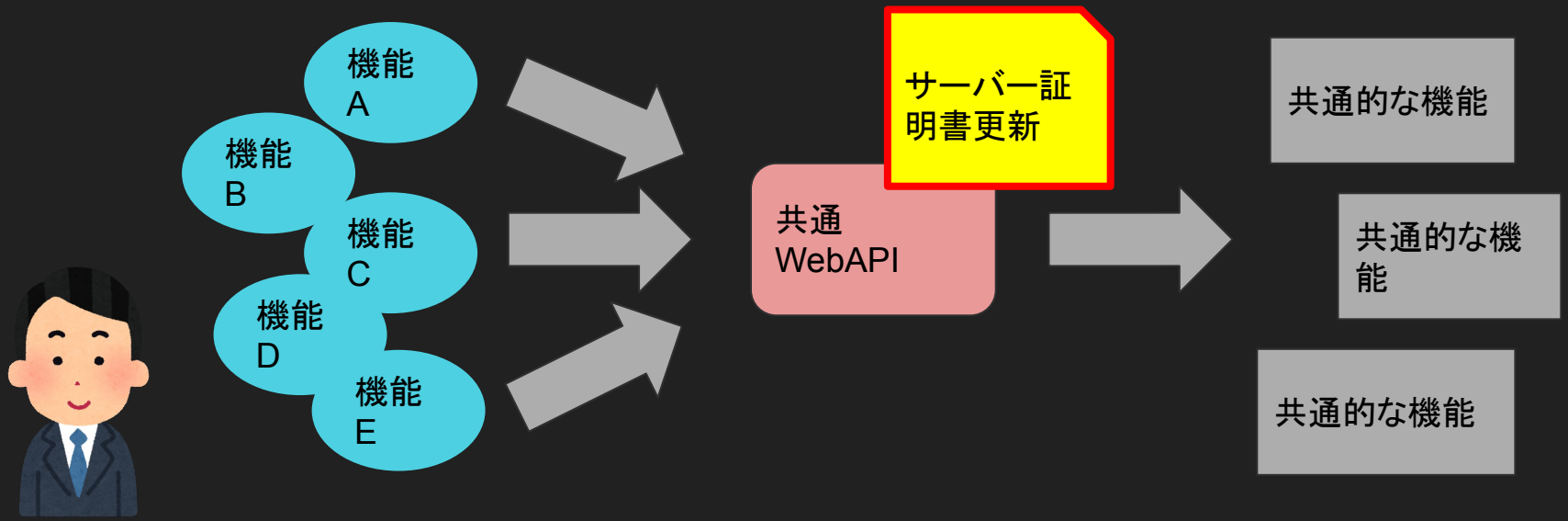
勉強会の話（たぶん20minくらい）

サーバー証明書の更新をしたら、Webサーバーに通信できなくなりました

その内容と、背景を勉強したものを発表します

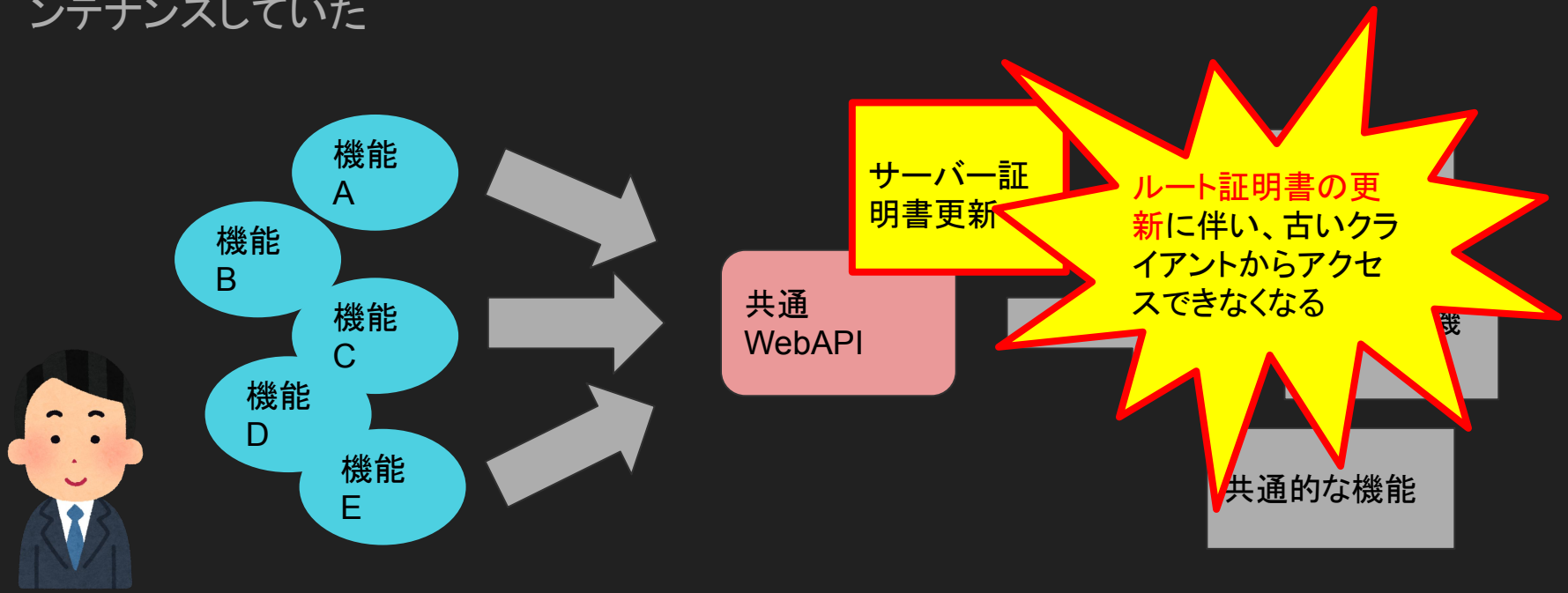
裏で何が起きていたか？

障害発生時、いろんな機能で利用している共通WebAPIで、サーバー証明書更新のメンテナンスしていた



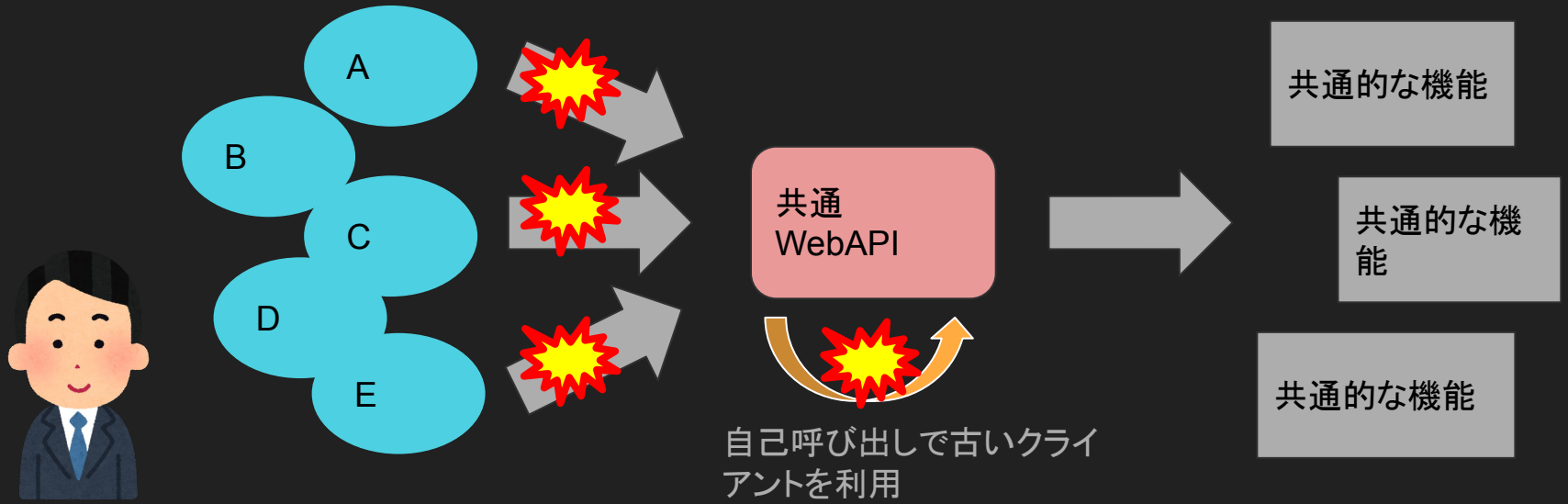
裏で何が起きていたか？

障害発生時、いろんな機能で利用している共通管理用APIで、サーバー証明書更新のメンテナンスしていた



裏で何が起きていたか？

障害発生時、いろんな機能で利用している共通WebAPIで、サーバー証明書更新のメンテナンスしていた



教訓

・サーバー証明書の更新しつつ、ルート証明書の更新について認識しようね

・古いクライアントをつかうのやめようね

おしまい

.....

なにが悪かったか、ピンときました？私はピンとこなかった

そもそも、「証明書」について知識が浅くて具体的になにが悪くて何を対策すれば再発しないのか、もやっとした

勉強しなおし

SSL/TLSについてざっくり学ぼう

目次

・httpとhttpsの違いについて

・SSLとTLSについて

・tcpにおける、ssl/tlsについて

・サーバー証明書、CA中間証明書、ルート証明書

・参考）オレオレ証明書って？

・サーバー証明書の認証局と証明書有効期限について

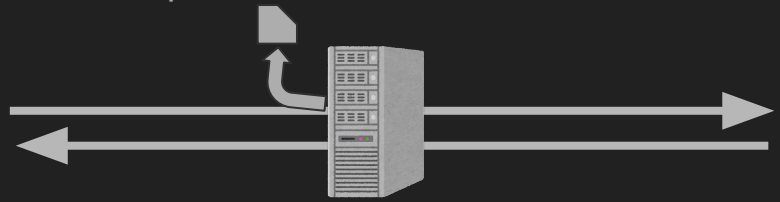
・linux内のルート証明書

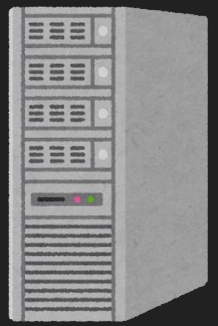
・これを踏まえて障害について見てみる

httpとhttpsについて（証明書の前提）

HTTP: HTTPはデータを平文で転送

HTTPS: HTTPSはSSL（Secure Sockets Layer）またはTLS（Transport Layer Security）プロトコルを使用してデータを暗号化して転送





SSLとTLSについて（証明書の前提）

どちらもhttpsを実現するためのプロトコル。

SSL（Secure Sockets Layer）

　1.0,2.0,3.0のバージョンがある。SSL3.0から後述のTLSが派生した。もはや古いので使ってはいけない。

TLS（Transport Layer Security）

　1.0, 1.1, 1.2, 1.3のバージョンがある。1.0, 1.1は古め。1.2, 1.3の仕様が推奨される。

tcpにおける、ssl/tlsについて（証明書の前提）

ClientHello

暗号化スイートのリスト送ったりする

暗号化スイートのリスト送ったりする

ServerHello

Server Certificate

Key Exchange

Hello Done

Client Key Exchange

Change Cipher Spec

Handshake Finished

tcpdumpで読むと実感できて面白い

細かい仕様をテキストメモに。

サーバー証明書、CA中間証明書、ルート証明書

SSL/TLSにて使われる証明書は3段階。

ルート証明書

中間CA証明書

サーバー証明書

サーバー証明書、CA中間証明書、ルート証明書

クライアントに入っている。
5,10,20年とか長いスパンで有効

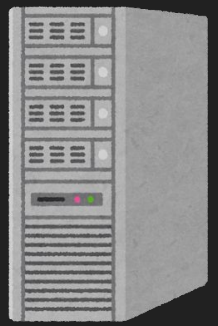
ルート証明書
（クライアント利用者が管理）

CA中間証明書

中間CA証明書で認証されている。

Webサーバーに配置する。サイバートラストとかから買って配置する。Lets Encryptとかは無料。半年とか1年とかで更新する

サーバー証明書
（サーバー管理者が管理）



サーバー証明書、CA中間証明書、ルート証明書

CA中間証明書

サーバー管理者、利用者はあんまり意識しなくてよさそう

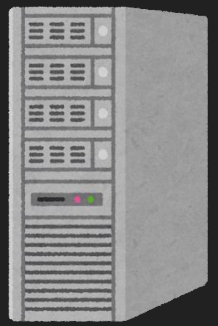
ドメインごとに、有効期限を気にして更新しようね

更新とかしたことないよ？

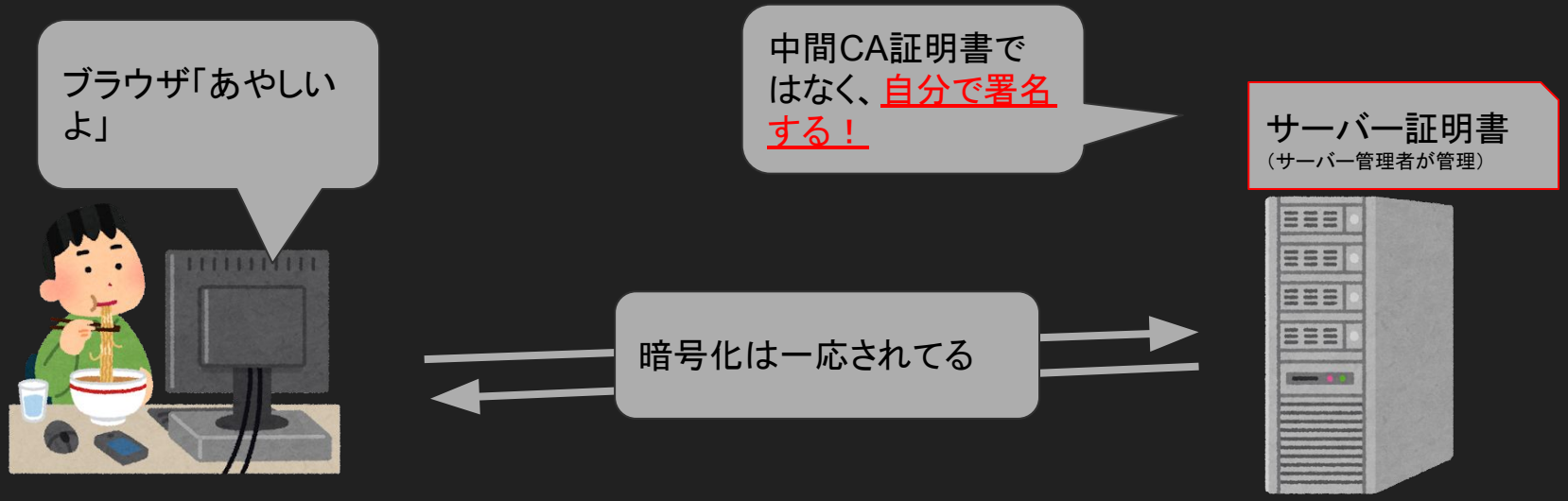
ルート証明書
（クライアント利用者が管理）

windows updateとかで勝手にやってんよ

サーバー証明書
（サーバー管理者が管理）



（参考）オレオレ証明書って？



サーバー証明書の認証局と証明書有効期限について

SSL/TLS サーバー証明書を発行してくれる認証局はいろいろある

・Symantec →一番有名らしい

・GlobalSign

・cybertrust →ニフクラでも提供

・GeoTrust

・Let’s Encrypt →無料！でもすぐ有効期限が切れるイメージ

昔は長期間（3～5年等）の証明書が変えたが、近年、セキュリティの観点から、1年程度の有効期限になっているよう。

サーバー管理者は、1年程度で証明書を入れ替えるように気をつけましょう

https://college.globalsign.com/blog/ssl90days_230411/
https://knowledge.digicert.com/ja/jp/solution/SO22917.html

linux内のルート証明書

・CentOS系の例

・基本的にopensslというソフトウェアが入っており、opensslがルート証明書を管理している（※要出典）

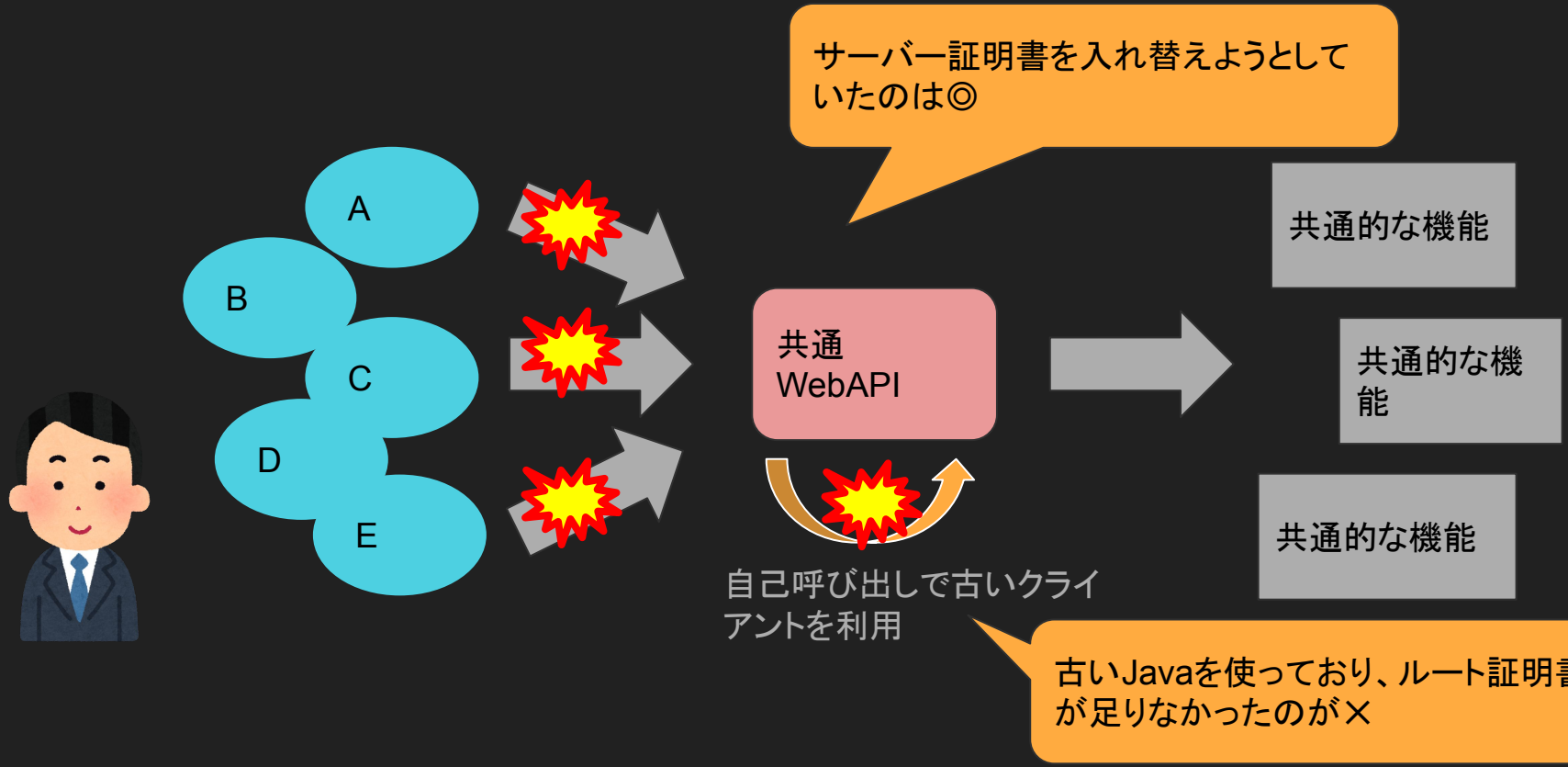
    ・ `/etc/pki/ca-trust/extracted/openssl`

・各種ソフトウェアは、httpsの通信をする際にopensslを使ってhttpsするイメージ

・ただし、Javaやruby等、プログラミング言語？は個別にルート証明書を持っている様子（※要出典）

    ・`./jre/lib/security/cacerts`

ここまでを踏まえて障害について見る



サーバー証明書の更新だけでなく、ルート証明書を意識して、クライアントの更新をちゃんとしましょう