DNS Day mini

- 大切なドメイン名を守る –

日本DNSオペレーターズグループ
株式会社インターネットイニシアティブ
其田　学

自己紹介

Manabu Sonoda
其田 学

所属

株式会社インターネットイニシアティブ
日本DNSオペレーターズグループ 幹事

経歴

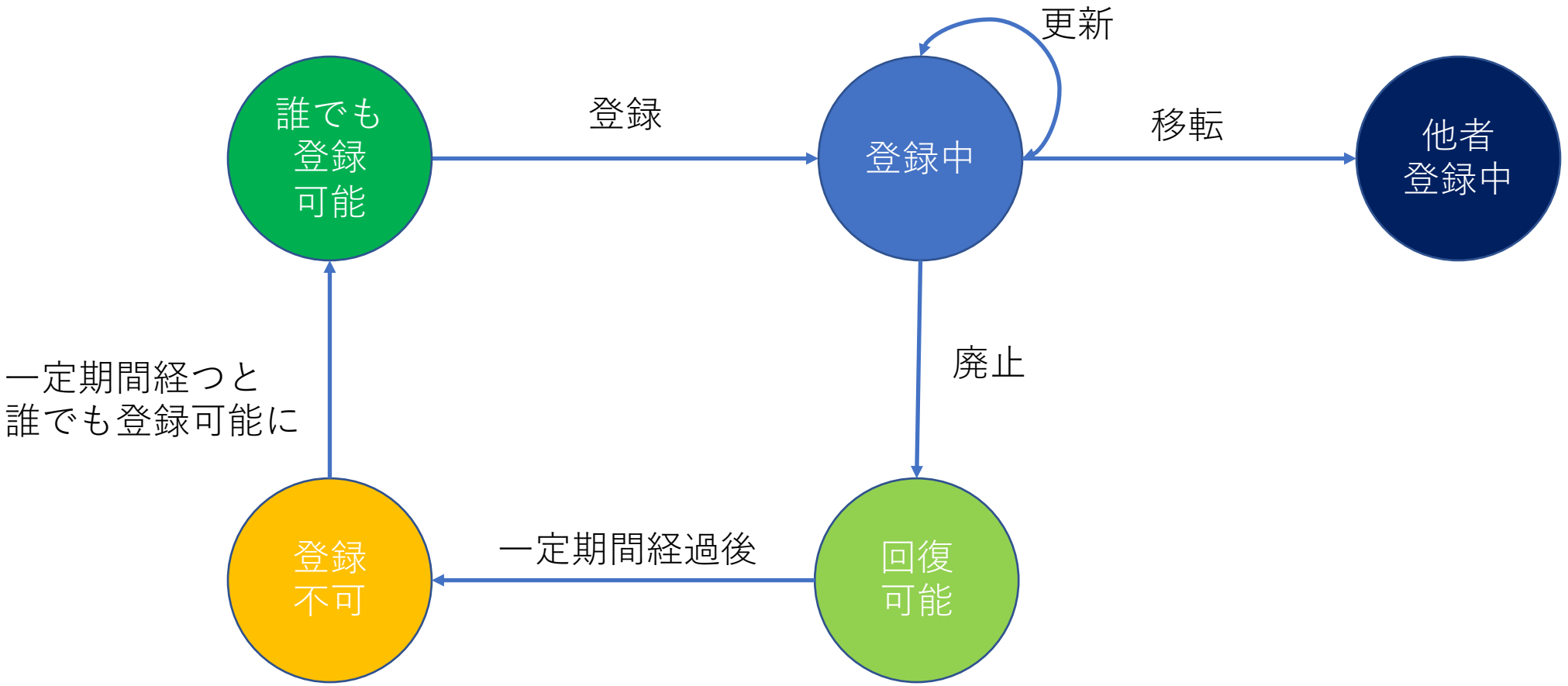
- 2008年 AS4704でL1-L8まで行うフルスタックエンジニア
- 2014年 IIJにて現職
  - IIJのお客様提供用のDNSサーバの設計、構築、運用
  - D.DNS.JPの構築、運用
  - コミュニティ活動、啓蒙活動などなど（イマココ）

本日のゴール

- ドメイン名に対する脅威がわかるようになる。
- 脅威、リスクについての緩和策がわかるようになる。

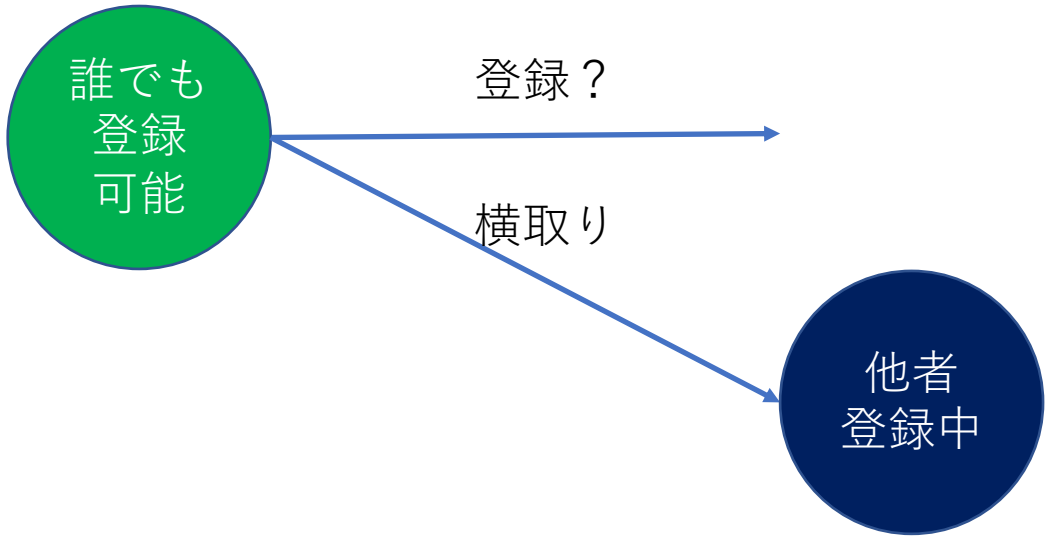
ドメイン名のライフサイクルから見る
ドメイン名に対する脅威、リスク

ドメイン名のライフサイクルの流れ



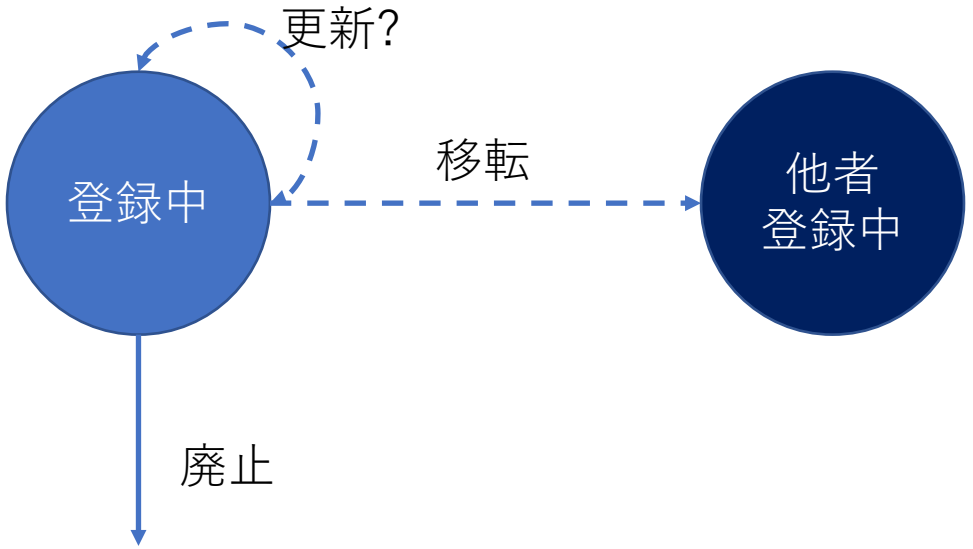
ライフサイクルの各状態のリスク

- 登録時のリスク
  - 悪質なレジストラが、ドメイン名を登録可能か確認した際に横取りしてしまう。（フロントランニング）



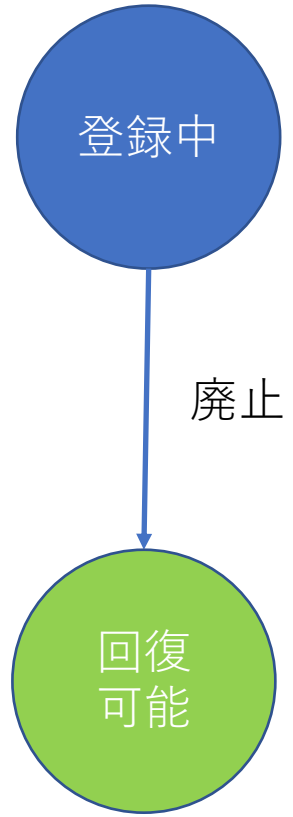
ライフサイクルの各状態のリスク

- 更新、登録中のリスク
  - 更新忘れによる意図しない廃止
  - 通知を見ていないなどによる、JPドメイン名の移転申請のリスク
  - 標的型攻撃などによる、登録中ドメイン名の管理権限奪取による登録者の意図しない移転



ライフサイクルの各状態のリスク

- 廃止のリスク
  - 廃止したつもりが、レジストラが削除しない
    - ドメインパーキング
    - そのあとはオークションに出されたり
  - ドメイン名は廃止されると人類の共有財産なので、誰でも登録可能になる[1]
  - 廃止ドメインを他者が登録することをドロップキャッチと呼び、ある程度使われているドメイン名であれば、ほぼドロップキャッチされる
    - 私の私的なプログラムを公開していたWEBサイトのドメイン名ですらドロップキャッチされました。



1 そのドメイン名を取る資格があれば。例えば汎用JPであれば日本に住所があれば

ドメイン名がドロップキャッチされると

もちろん普通の使われ方をする場合もありますが、
大抵はろくな使い方はされません。

- ましなパターン
  - アフィリエイトサイトに化ける
    - Amazonとかの広告
    - アダルト系や、風俗系のリーチサイトとか
  - 情報販売系のサイトに化ける
    - 例: 絶対儲かるDNSサーバマニュアル

- ダメなもの
  - 明らかに法に触れるコンテンツに化ける
    - 違法薬物系とか
    - オンラインカジノ系とか
  - 元のサイトのなりすましサイト

事例

IW2018 - DNSDAY ドメイン名ライフサイクルマネージメントより抜粋

産経ニュース　　閉じる

2016.11.15 11:07

市の旧ＨＰからカジノ誘導…偽観光サイト、第３者が取得悪用　愛媛・新居浜

愛媛県新居浜市の旧ホームページ（HP）のドメイン（インターネット上の住所）を使った偽の観光サイトが作成され、利用者がカジノのサイトに誘導されていることが15日、同市への取材で分かった。市が手放したドメインを第三者が取得、悪用したとみられ、市は注意を呼び掛けている。

悪用されたのは、市運輸観光課が今年3月まで運用していた観光サイトのドメインで「niihamakanko.com」。市の観光案内なども表示されるが、オンラインカジノの関連情報が表示され、誘導するようになっていた。

観光サイトを今年4月、市の公式ホームページに移設し、旧ドメインは手放していた。

運輸観光課の高橋利光課長によると、旧ドメインの保有には年間約2万8千円が必要。「仕組みに理解不足があった。旧ドメインも一定期間は保持するべきだった」と話している。

同課によると、15日現在で、被害や苦情は確認されていない。

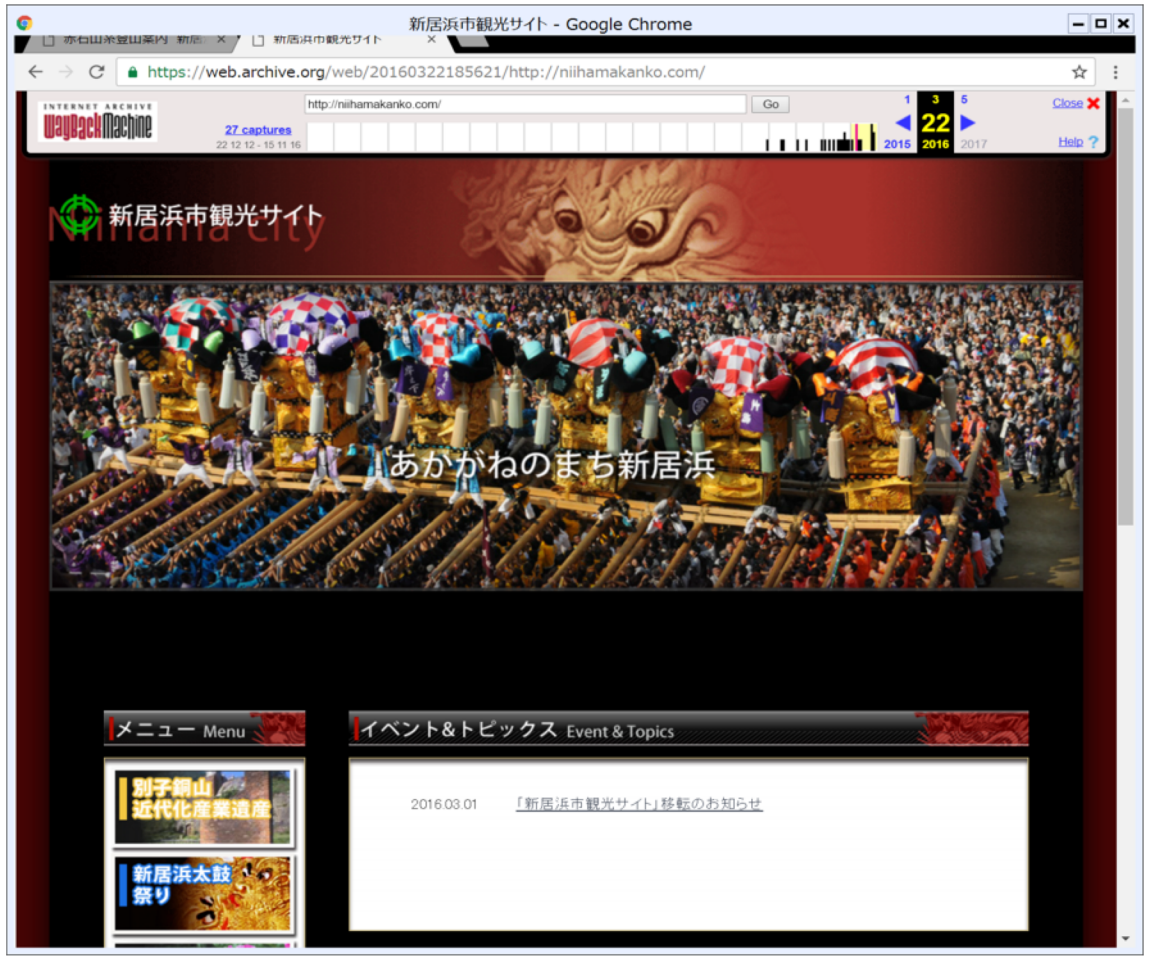
市は、愛媛県警に相談するとともに、今後の対応を検討している。

愛媛県新居浜市の旧ＨＰのドメインを使った偽の観光サイト。オンラインカジノの関連情報が表示される

http://www.sankei.com/west/news/161115/wst1611150034-n1.html

IW2018 - DNSDAY ドメイン名ライフサイクルマネージメントより抜粋

ケース1: niihamakanko.com

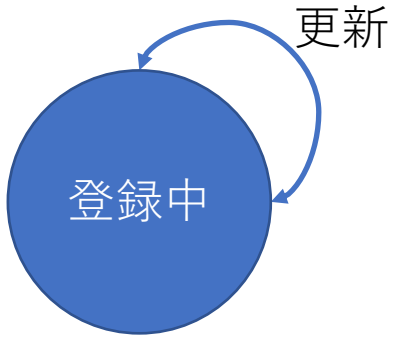


- コンテンツは乗っ取られているが、ドメイン名はドロップキャッチ
- 現時点（2018/11/16）ではレジストラで保持されている状態

対策

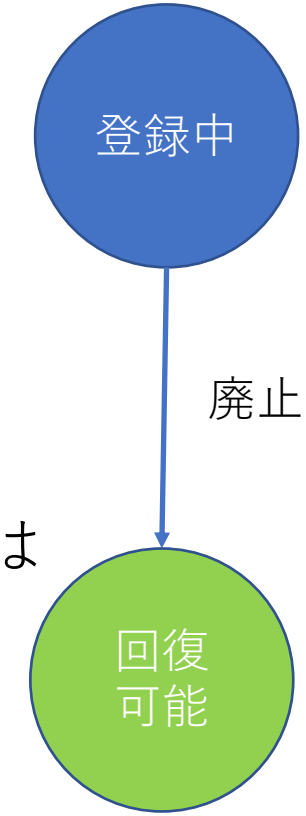
- ドメイン名の登録
  - 出来るだけ、組織のドメイン名のサブドメインを使いましょう
  - また、政府系機関はgo.jp, 地方自治体の場合はlg.jpという特別なドメイン名が使えます。これらは登録制限があるので、ドロップキャッチされません。(多分)
  - どうしても新規でドメイン名を登録したい場合
    - 基本的には、知財管理する部門などが承認しないと、ドメイン名を登録できない様にする（野良ドメイン名防止）
      - 基本的に廃止できない、永続的に維持費がかかることを覚悟いただく
      - 知財部署が知的財産の一部として管理するのが望ましい。
    - ドメイン名の名簿を作成し、ドメイン名毎の責任者を明確にする
    - １年に一回棚卸を行い、不要になったものは削除フェーズへ

対策



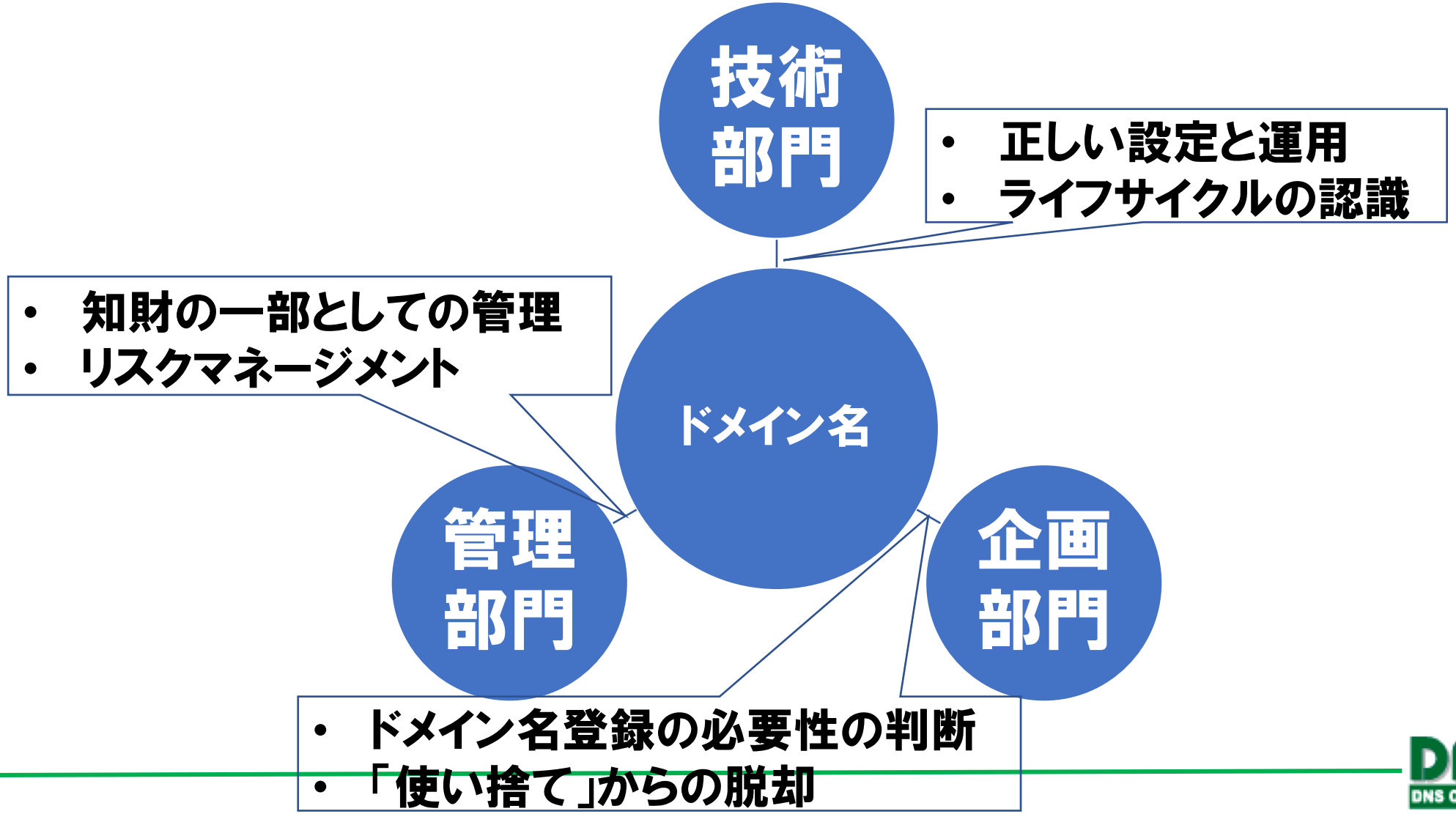
- ドメイン名の維持
  - ドメイン名の登録者情報は新しいものに更新する
  - １年～半年に1回は登録者情報を確認する。
  - JPドメイン名の意図しない移転が起こらないレジストラを選ぶ
  - レジストラは、なるべく多要素認証ができる事業者を選び、多要素認証を有効にする。（後述）
  - ロック機能がある事業者は機能を有効にする（後述）

対策



- ドメイン名の廃止
  - そのドメイン名がどういう風に使われていたかによりますが、一般のユーザが見るWEBページなどを運用してしまった場合は廃止することにはリスクが伴います。
  - それでもどーしても廃止する場合
    - ブランド毀損を覚悟して廃止しましょう。
    - 山梨医科大学の事例の場合、１２年後に同じドメイン名を登録され、風俗紹介サイトに化けたこともあります。
  - 年間数千円なので、黙って維持する方がいいです。

ドメイン名のライフサイクルマネージメント



ー大切なドメイン名を守るー
管理権限を守る

管理権限を守る

- ドメイン名登録者のできること
  - ネームサーバ申請
  - 登録者情報の変更申請
  - 他者への移転申請

- これらはレジストラのWEBサイトで行うことが一般的
  - サイト上のドメイン名登録者の管理権限のセキュリティが大変重要

なりすまし攻撃について

ドメイン名に対する攻撃 – なりすまし攻撃

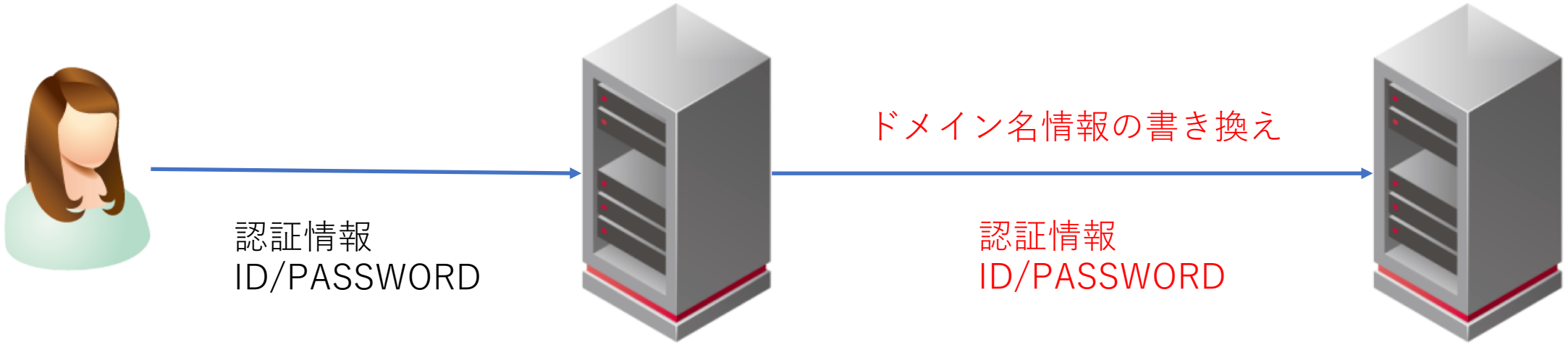
いつもお世話になっております。●●Jサポートセンターです。
お客様のご登録いただいておりますドメイン名 example.jpについて
登録者情報の更新をお願いしております。
更新していただけない場合、レジストリの規定に基づきドメイン名が利用停止になる恐れがございます。

ドメイン名情報の更新は下記URLより行えます。
https://●●j.jp/login

ご不明な点がございましたら、
●●Jサポートセンタにお問い合わせください。

なりすまし攻撃

- レジストラの管理画面になりすまして、
  ユーザIDやパスワードなどの認証要素を窃用
- 窃用した認証要素を使って悪さをする



なりすまし攻撃 – 被害

- WEBサイト側で何も対策していない場合、
  管理者でログインできるため、すべての行為が可能になります。

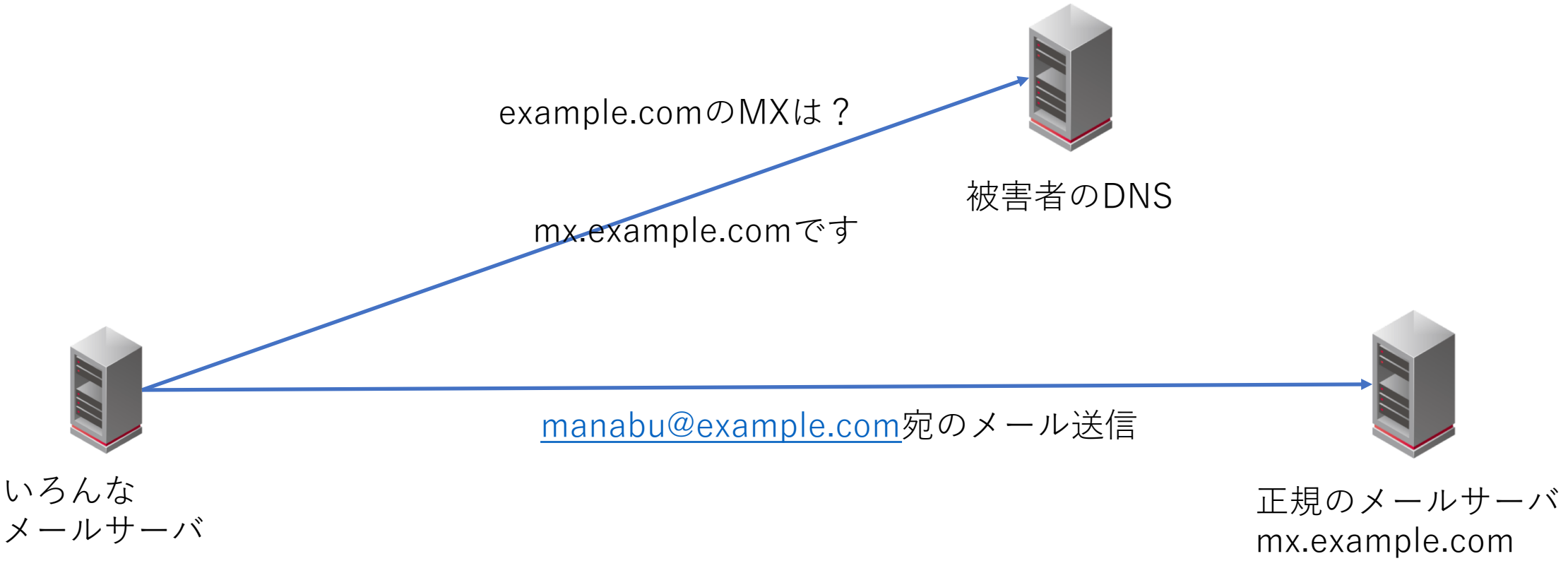
- その結果、以下の攻撃が可能になります。
  - ドメイン名の移管
  - ネームサーバを変更して、ゾーンを書き換えて行う中間者攻撃
  - TLS証明書の発行

ドメイン名の移管

- ドメイン名の登録が他者（攻撃者に渡ってしまいます）
- 自組織の管理権限がなくなります。

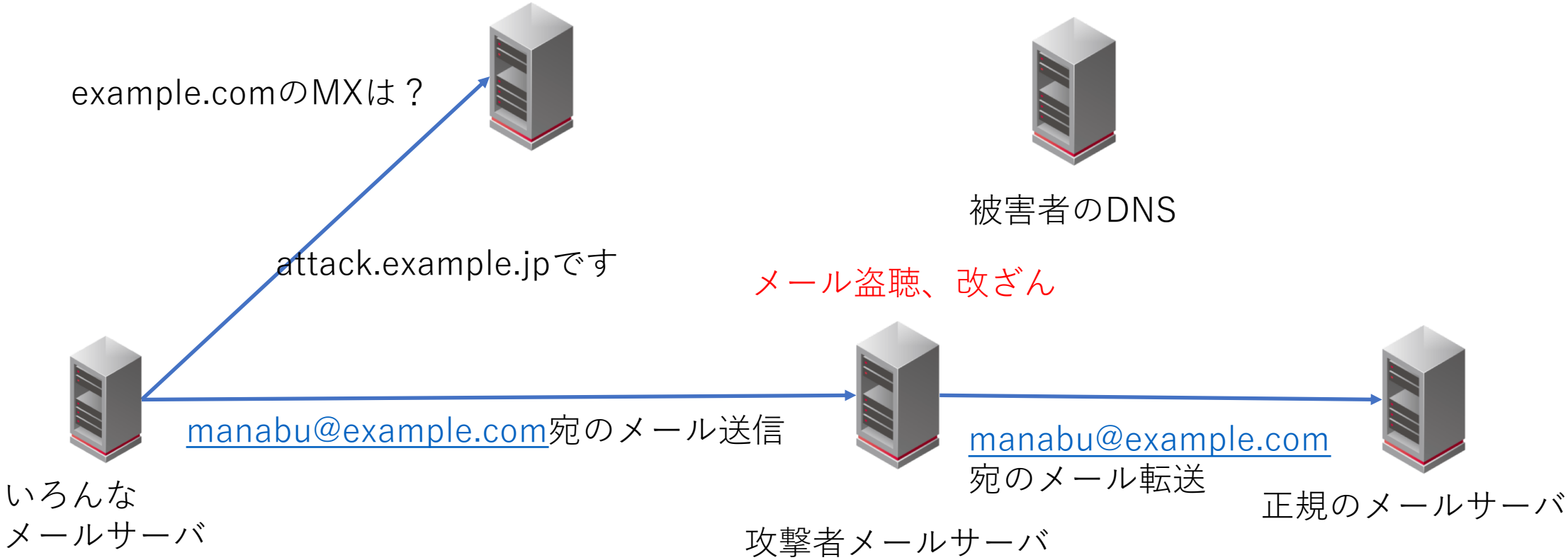
ネームサーバを変更して
ゾーンを書き換えて行う中間者攻撃

- メールの例



ネームサーバを変更して
ゾーンを書き換えて行う中間者攻撃

- 攻撃者のメールサーバ



TLS証明書の発行

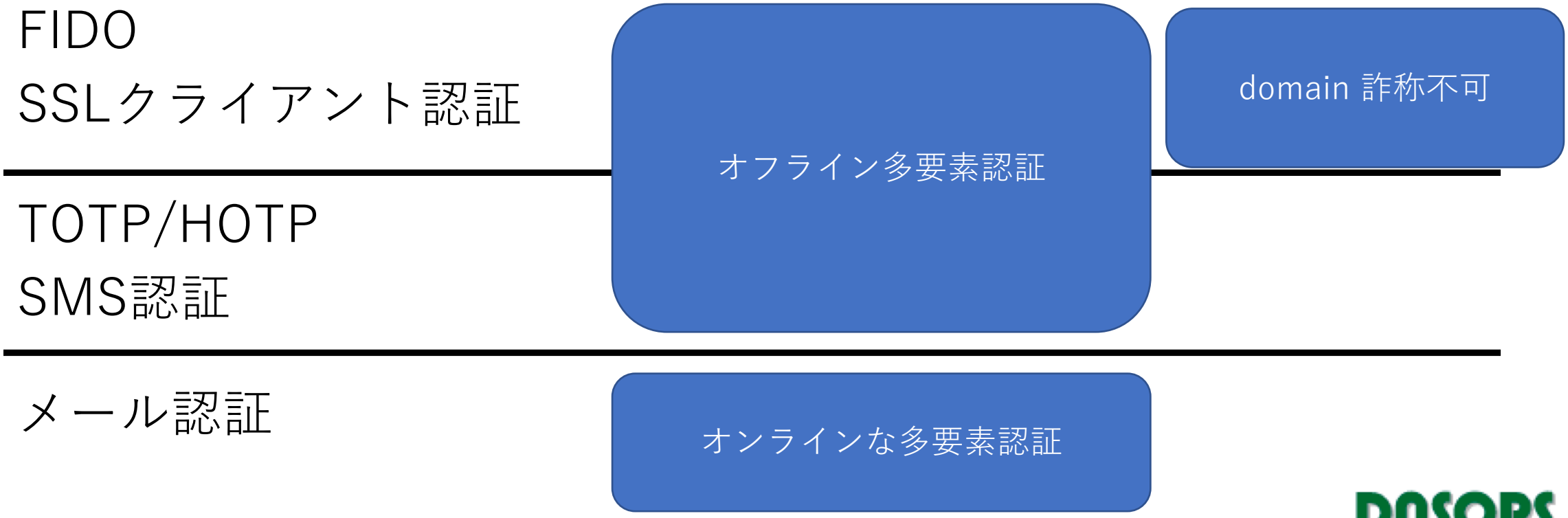
- ネームサーバの乗っ取りができると、ネームサーバを使ってドメイン認証型(DV)のTLS証明書が取得できます。
- また、登録者情報のメールアドレスを書き換えても、ドメイン認証型(DV)のTLS証明書が取得できます。
- 足がつく可能性が高いですが、EVやOV証明書に関しても、登録者情報を変更すれば取得可能です。

対策

管理画面の認証の強化

管理画面の認証の強化

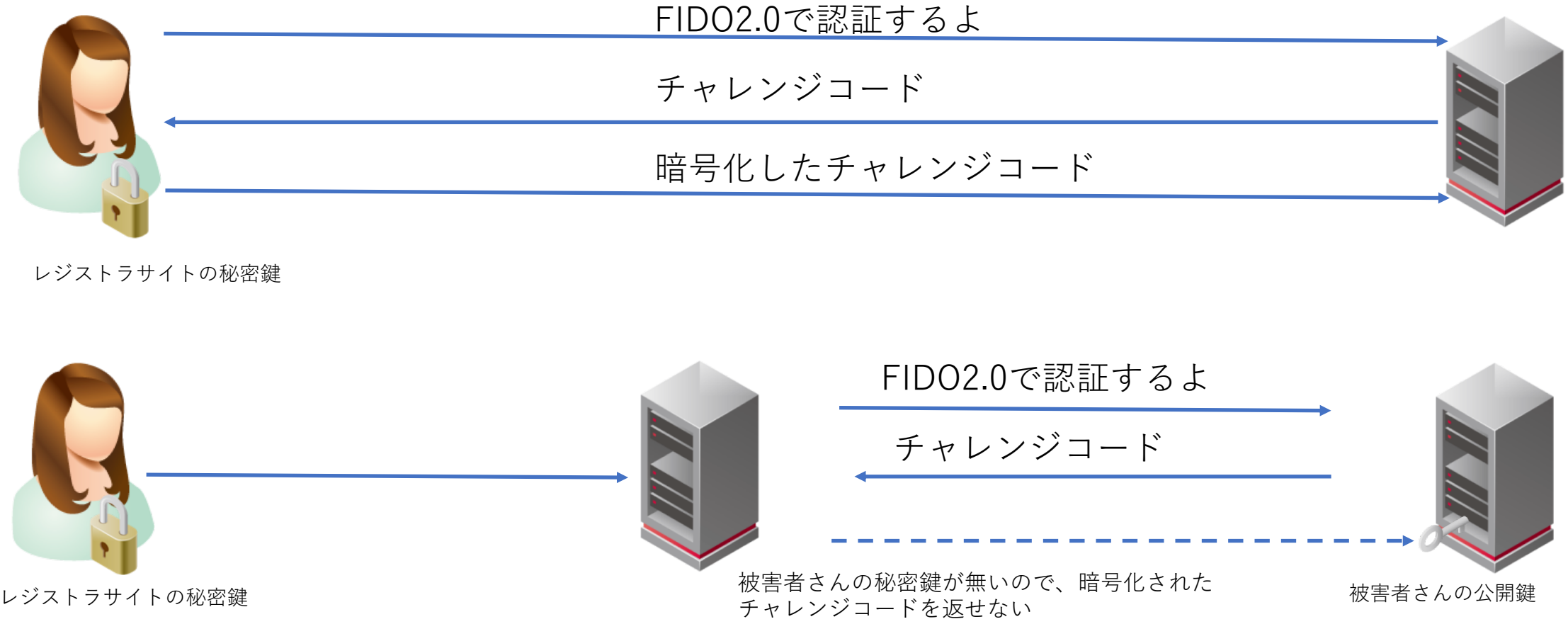
- ID、パスワードに加えて、他の要素でも認証する方法で、単純にIDとパスワードが漏れてもログインできない



管理画面の認証の強化- FIDO

- 公開伴暗号方式を使った今後の認証のスタンダード規格
- キーデバイス上にドメイン名毎に暗号化鍵、復号鍵を格納
- サーバに対して、復号鍵を登録
- 認証時は、サーバから送られてきたチャレンジを暗号化して送り返すことで認証します。
- ドメイン名毎に鍵が作られるため、元サイトに似せた名前の「なりすましサイト」に対して効果があります。

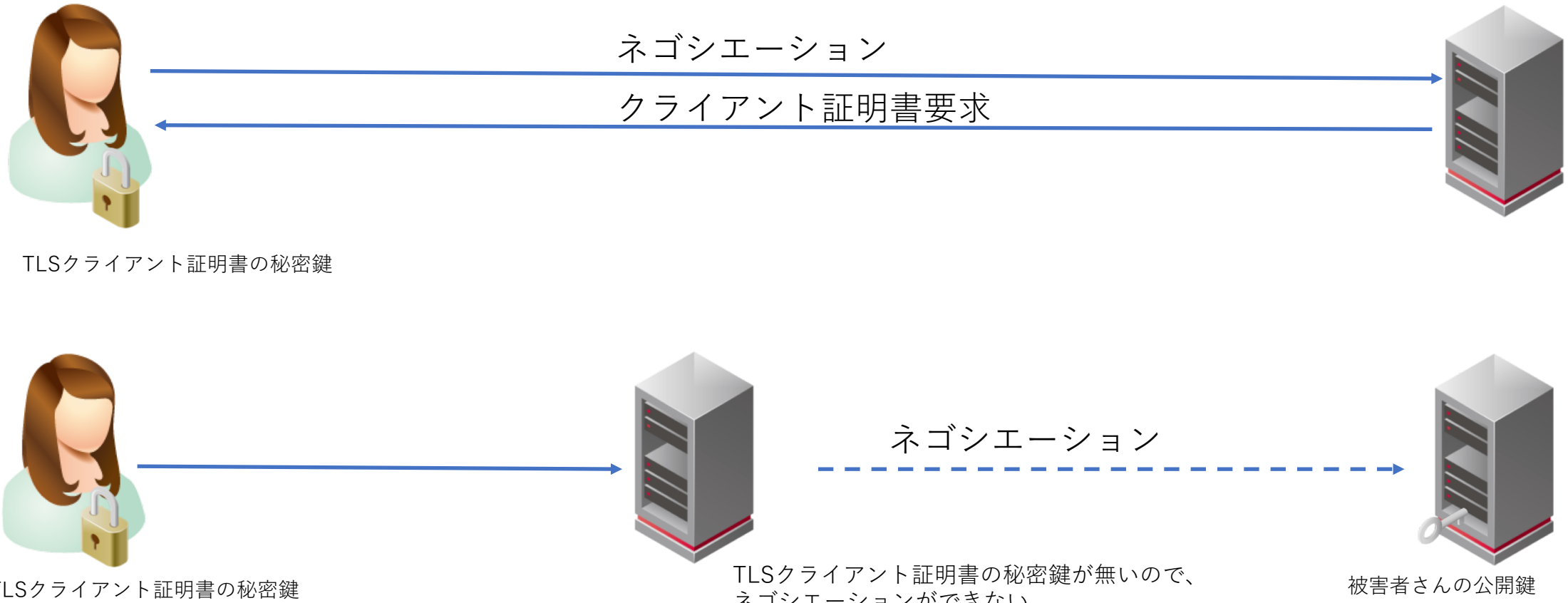
FIDO - なりすまし耐性



管理画面の認証の強化 – TLSクライアント証明書認証

- TLSクライアント証明書を用いて認証を行う。
- 日本だとJPNICとかJPRSの管理画面で使われてたりする
- 証明書のライフサイクル管理が大変面倒 （特に証明書を物理媒体でやり取りする場合）
- 秘密鍵がないとTLSセッションを張れないので、なりすましサイト経由で正規サイトをいじられることはない。
- マルウェア感染などで、端末に侵入された場合、秘密鍵が暗号化されていないと認証情報を奪われる可能性あり

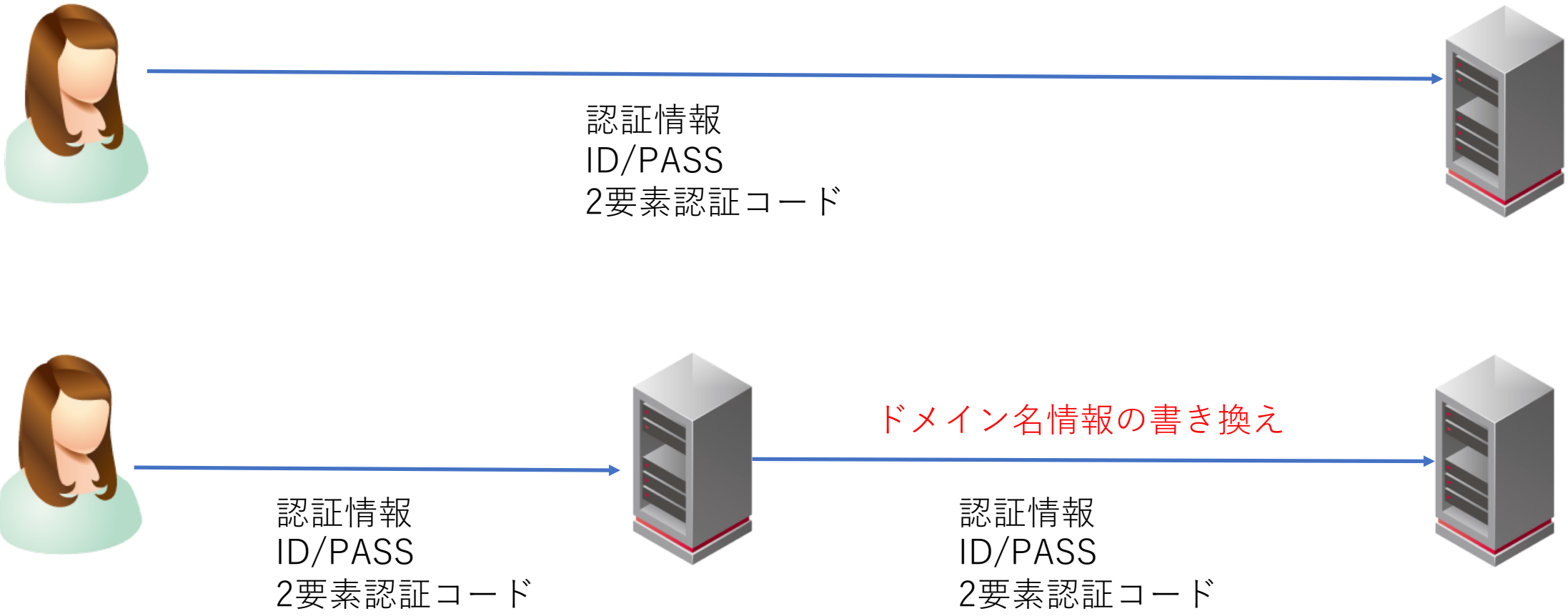
TLSクライアント証明書 - なりすまし耐性



管理画面の認証の強化 -TOTP/HOTP

- ワンタイムパスワードや、時間によって変わるパスコードを入力させるこ とで、認証する方式
- Google authenticatorとかIIJ SmartKeyとかのアプリケーションを使ったり、パスコード生成機を使ったりする。
- なりすましサイトのログイン

TOTP/HOTP - なりすまし耐性



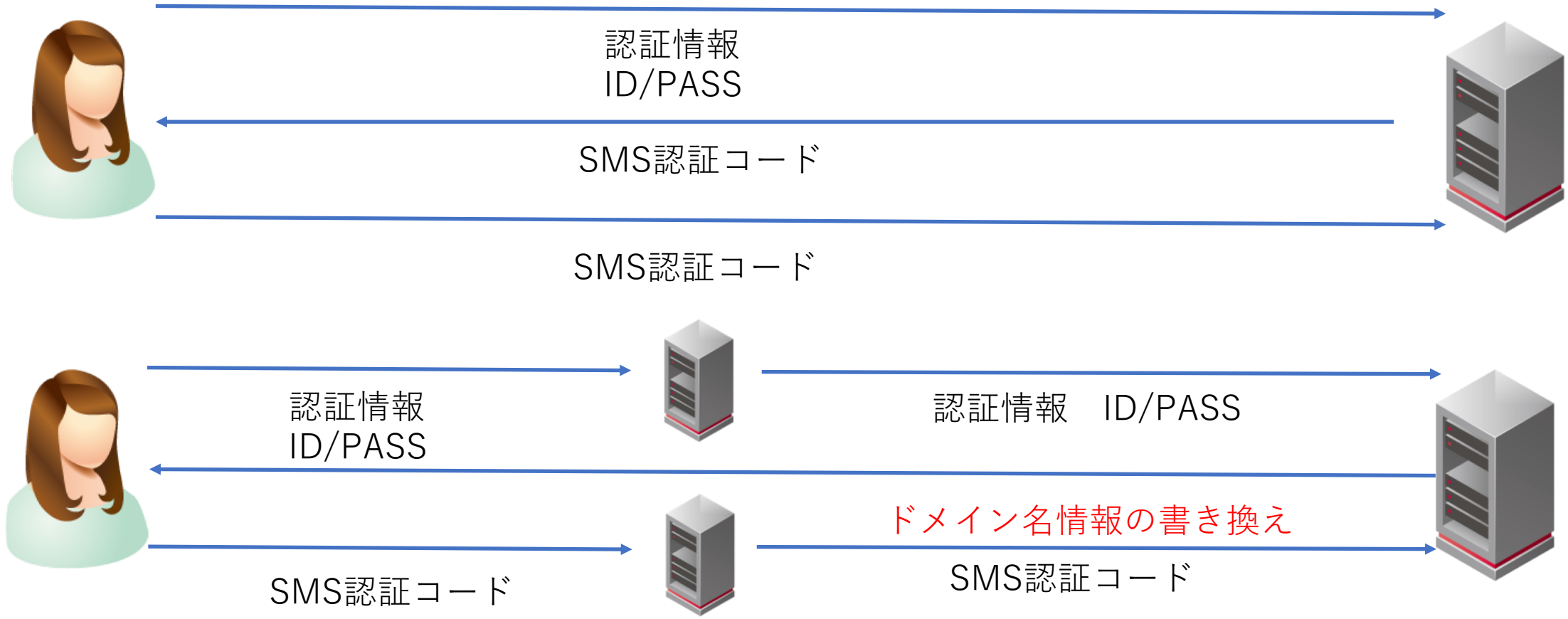
管理画面の認証の強化 –SMS認証

- ID,パスワードでのログイン成功時に、SMSでワンタイムパスワードを送信し、追加認証する方式

- 携帯電話を持っていないと認証が通らない
  - 海外ではオペレーターが不正にSMSメッセージ覗きみたいしてるようなのですが。。

- なりすましサイトには効果がない

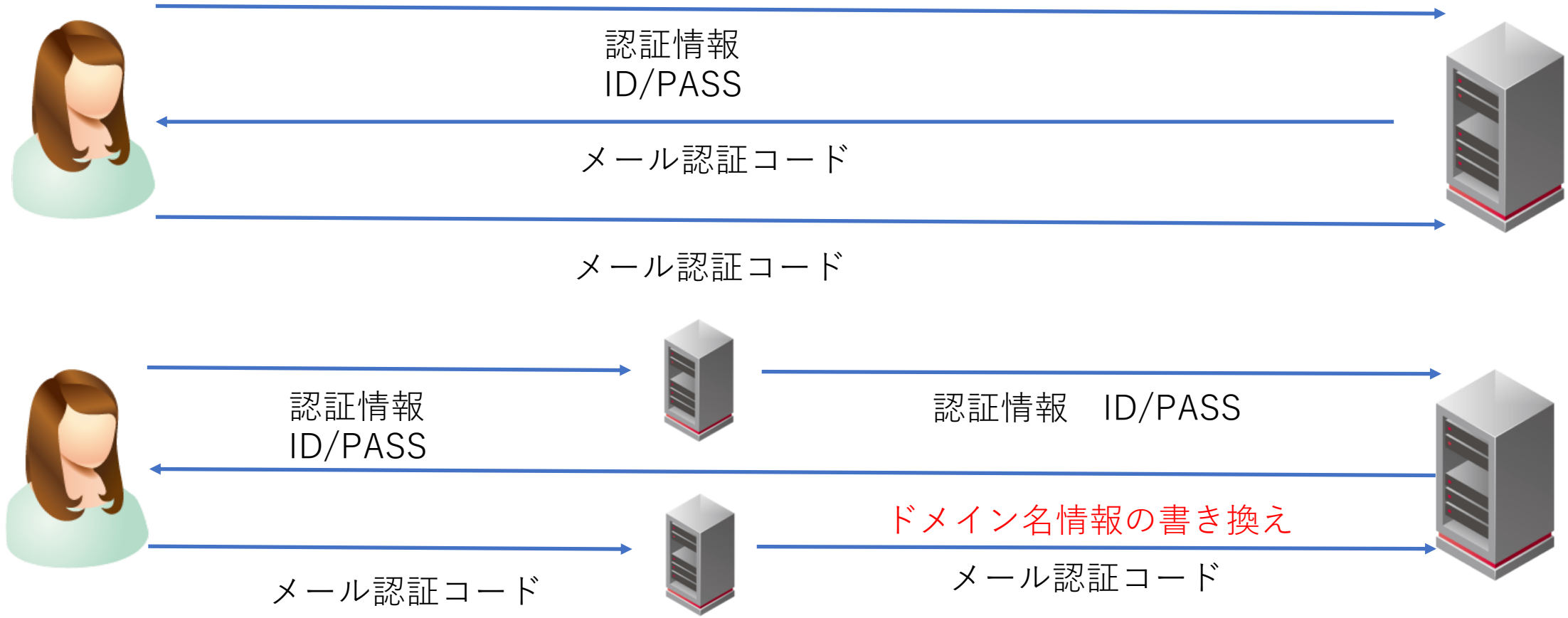
SMS認証 - なりすまし耐性



管理画面の認証の強化 - メール認証

- ID,パスワードでのログイン成功時に、メールでワンタイムパスワードを送 信し、追加認証する方式
- 無いよりはマシという感じ
- なりすましサイトには効果がない
- マルウェア感染などで、端末に侵入されたら、メールが盗めるかも。。

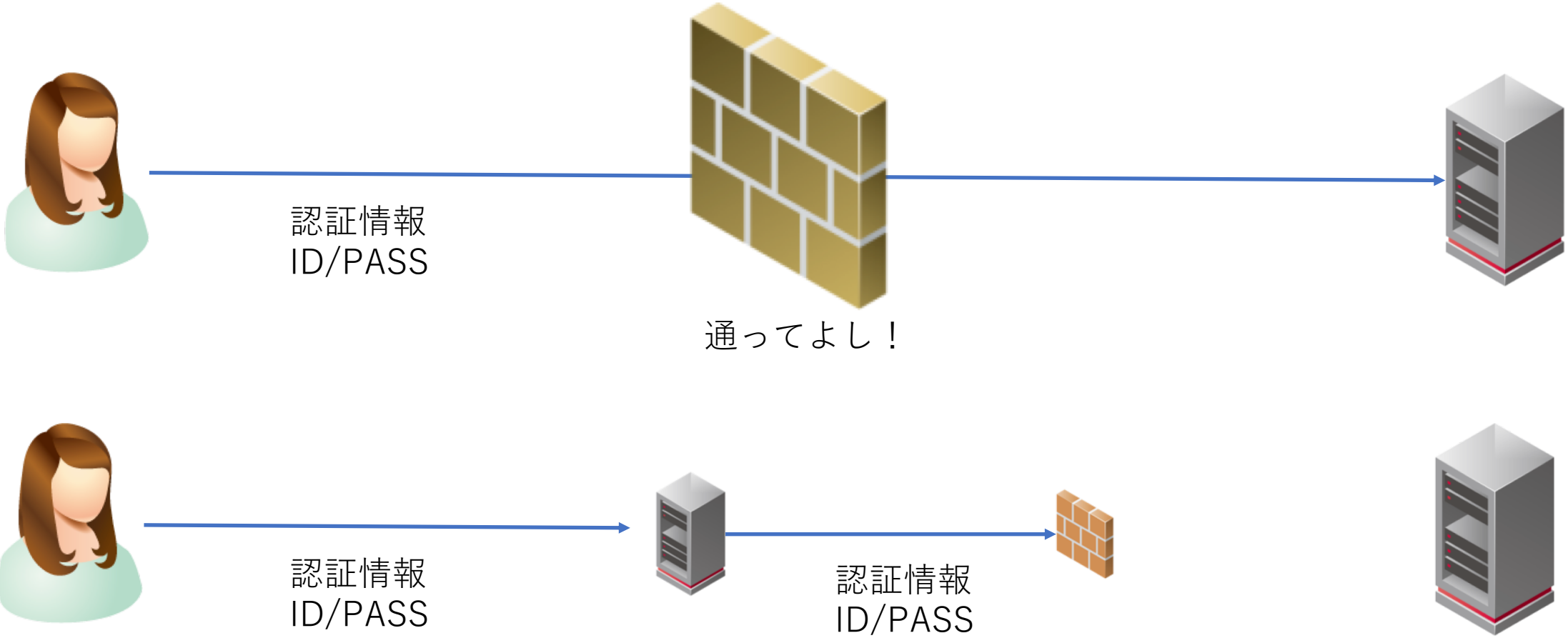
メール認証 - なりすまし耐性



管理画面の認証の強化 - ACL

- コントロールパネルにログインできるIPを制限することで、そのIP以外か らのなりすまし攻撃を防ぐことが可能
- なりすましサイトからのログインを防げる
- マルウェア感染などで、端末に侵入されたら効果はない

ACL- なりすまし耐性


認証情報
ID/PASS
通ってよし！
認証情報
ID/PASS
認証情報
ID/PASS
被害者
攻撃者のWEBサイト
正規のレジストラサイト

管理画面上での再認証

なりすまし攻撃の耐性がない認証でも、
重要な操作で再度認証することで、リスク低減できることがあります。

例
- ドメイン移転の申請後申請確認メールを送って、認証する。
- ネームサーバの変更時に再ログインさせる

ドメイン管理系の場合、ほぼ全ての申請が重要な操作なので、
なんらか対策が入っていることが望ましいです。

コントロールパネルへの認証への対策 -まとめ

事業者視点

- なりすまし対策まで行うならFIDO対応したい。
- 最低でもTOTP/HOTPぐらいは対応
- 再認証の実装

ユーザ視点

- ID,PASSWORD漏れはあり得るので、多要素認証は絶対欲しい
- TOTP/HOTPであれば、鍵のバックアップも簡単なので、
  最低でもTOTP/HOTPに対応していって欲しいところ。

対策

情報書き換えに対する対策

情報書き換えに対する対策

- 管理画面のロック
  - コントロールパネル上での情報変更をできなくする機能
    - 登録者情報やネームサーバ情報は滅多と変更しない
    - ロックしたままにしても特に問題ない
- レジストラロック
  - レジストラ側で、移転申請や、情報変更を拒否する機能
- レジストリロック
  - レジストリ側で、移転申請や、情報変更を拒否する機能

いっぱいロックあるんですが、問題は解除方法

ロック解除は難しい

- コントロールパネル上の認証情報だけでロック解除できるのはなんの意味もない。
  - 攻撃方法たくさんありましたよね。
  - 推奨されるロック解除方法は、ドメイン名や、ゾーン情報に依存しない情報での認証。
- コールバック認証
  - ただし連絡先の電話番号もロック対象であること。
- 書面による認証
  - 代表印あり、もしくは登録者の印鑑証明付きの押印がある書面による申請

ロック解除例 – レジストリロック

- ベリサイン（com ,net ,tv ,cc）
  - レジストラが登録者を認証しベリサインにロック解除申請を出す。
  - ベリサインは登録者にコールバックし、パスフレーズで認証して確認
  - つまりレジストリが本人確認している。ロック解除のリスクはどのレジストラでも同じ。

- JP（JPRS）
  - 指定事業者（レジストラ）が登録者を認証し、レジストラがJPRSに対して申請を出す。
  - JPRSはレジストラにコールバックして確認する。
  - つまりレジストラが本人確認しているので、ロック解除のリスクは各レジストラの実装次第。。
    - 信頼できるレジストラを選びましょう。

ロック解除例 – レジストリロック

- ベリサイン（com ,net ,tv ,cc）
  - レジストラが登録者を認証しベリサインにロック解除申請を出す。
  - ベリサインは登録者にコールバックし、パスフレーズで認証して確認
  - つまりレジストリが本人確認している。ロック解除のリスクはどのレジストラでも同じ。

- JP（JPRS）
  - 指定事業者（レジストラ）が登録者を認証し、レジストラがJPRSに対して申請を出す。
  - JPRSはレジストラにコールバックして確認する。
  - つまりレジストラが本人確認しているので、ロック解除のリスクは各レジストラの実装次第。。
    - 信頼できるレジストラを選びましょう。

まとめ

- ドロップキャッチされると、ブランドや組織イメージ毀損につながる可能性があります。
  - ドメイン名の登録はリスクと必要性を考えて慎重に
  - 基本的には一度登録したドメイン名は廃止できないと思ってください。
- 標的型攻撃など、なりすましサイトなどを使って、ドメイン名の管理権限の認証要素を奪う攻撃が頻発しています。
  - WEB申請可能な事業者の場合、多要素認証に対応しましょう
  - また、登録者もそういう事業者を選びましょう
  - レジストリロック、レジストラロックなどの機能がある場合は積極的に使っていきましょう。

ドメイン名のライフサイクルマネージメント

ご利用は計画的に