DNS Abuseと、DNS運用者がすべきこと
～ ドメイン名ハイジャックを知ることで、DNSをもっと安全に ～

2019年5月31日

Internet Week ショーケース in 仙台

株式会社日本レジストリサービス（JPRS）

森下 泰宏

本資料はInternet Week 2018 ランチセミナー資料のUpdate版です

講師自己紹介

- 森下 泰宏（もりした やすひろ）
  - 所属：JPRS 技術広報担当
  - 主な業務内容：ドメイン名・DNSに関する技術広報活動全般

＜略歴＞

1988年	独立系SIerに入社 1990年よりWIDE Projectメンバーとして、 日本のインターネット構築に創始期より参加。
1993年	学校法人東京理科大学情報処理センター着任 キャンパスネットワーク及び教育用システムの設計、 構築、運用を行う。
1998年	社団法人日本ネットワークインフォメーションセンター（JPNIC）着任 JPドメイン名登録システム及びJP DNSの管理運用に従事。
2001年	株式会社日本レジストリサービス（JPRS）に転籍 DNSに関する技術研究を中心に活動。
2007年	同社技術広報担当として、 DNSおよびドメイン名関連技術に関するプロモーション全般を中心に活動中（現職）。

JPRS著・監修「DNSがよくわかる教科書」

- 発売日：2018年11月22日（木）
- 著者：渡邉結衣、佐藤新太、藤原和典
- 監修者：森下泰宏
- 出版社：SBクリエイティブ株式会社
- 定価：本体2,280円+税
- ISBN：978-4-7973-9448-1
- A5版／332ページ

JPRSブースに見本誌があります！

本日の内容

1. DNS Abuseとドメイン名ハイジャックの基本
2. ドメイン名ハイジャックの主な事例
3. ドメイン名ハイジャックの分析
4. DNS運用者がすべきこと

1. DNS Abuseと
ドメイン名ハイジャックの基本

DNS Abuse／Domain Abuseとは
ドメイン名ハイジャックとは
DNS Abuseとドメイン名ハイジャックの関係
ドメイン名ハイジャックの標的と攻撃例

DNS Abuse／Domain Abuseとは

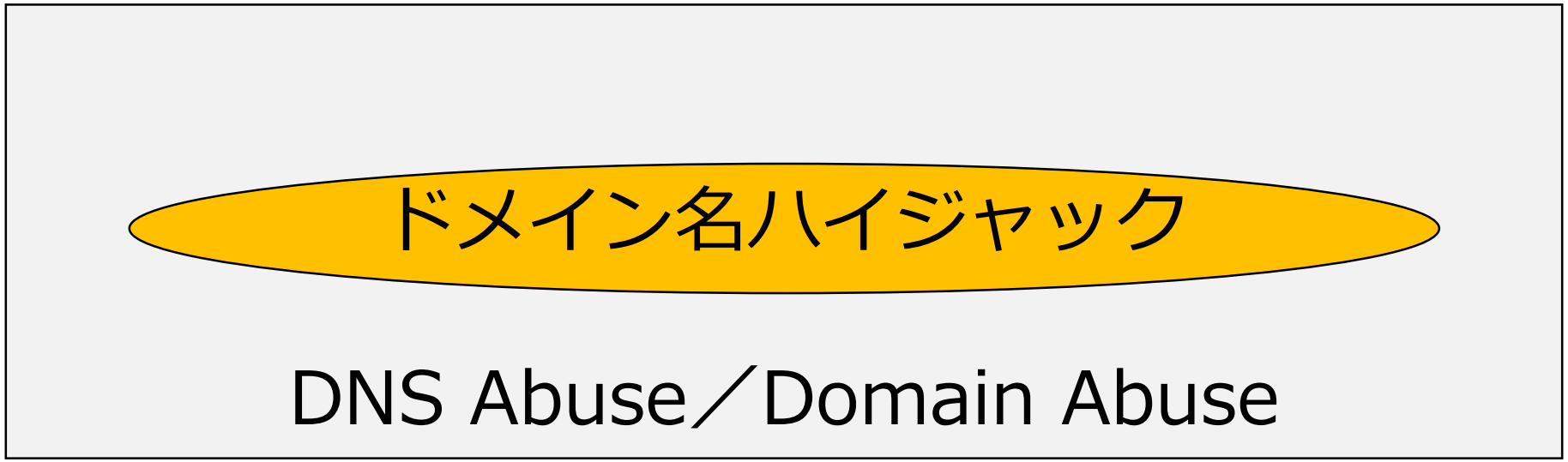
- Abuse ＝ **不正行為**
- DNS Abuse／Domain Abuse ＝
  ドメイン名の不正使用により実行される不正行為
  - DNS AbuseとDomain Abuseは、明確に使い分けられていない
  - 本資料では以降「DNS Abuse」を使用
- DNS Abuseによる不正行為の例
  - 偽造品・違法薬物の販売、フィッシングサイトの立ち上げ、マルウェアの注入・遠隔操作、機密情報の盗難など

ドメイン名ハイジャックとは

- ドメイン名の管理権限を持たない第三者が、
  不正な手段で他者のドメイン名を自身の支配下に置く行為
- さまざまな不正行為 ＝ Abuseにつながる
- DNS Abuseのための手段の一つ

DNS Abuseとドメイン名ハイジャックの関係

- ドメイン名ハイジャックは、DNS Abuseのための手段の一つ



以降では、ドメイン名ハイジャックにフォーカスを当てて解説

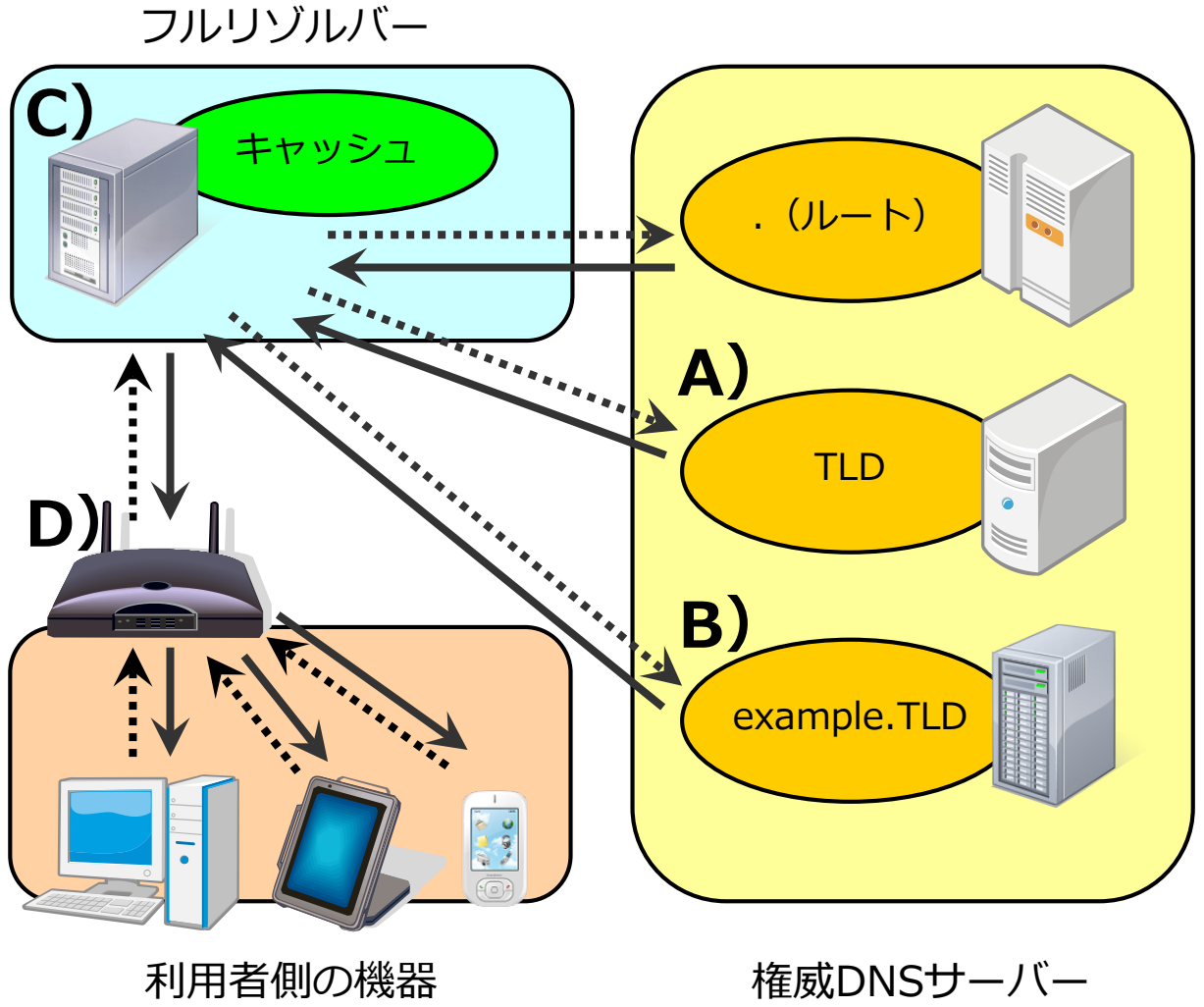
ドメイン名ハイジャックの標的と手法の例（DNSの構成要素・データに対する攻撃）

A) TLDの権威DNSサーバー
- ネームサーバー情報の不正変更
- ドメイン名の不正移転

B) 各組織の権威DNSサーバー
- 不正なデータを設定

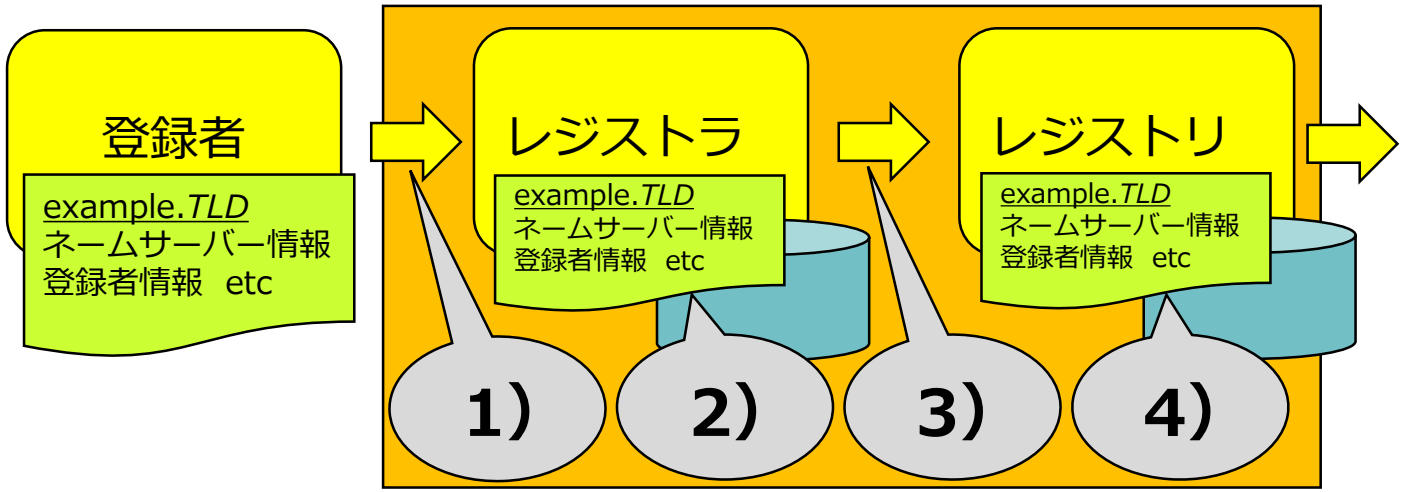
C) フルリゾルバー
（キャッシュDNSサーバー）
- キャッシュポイズニング

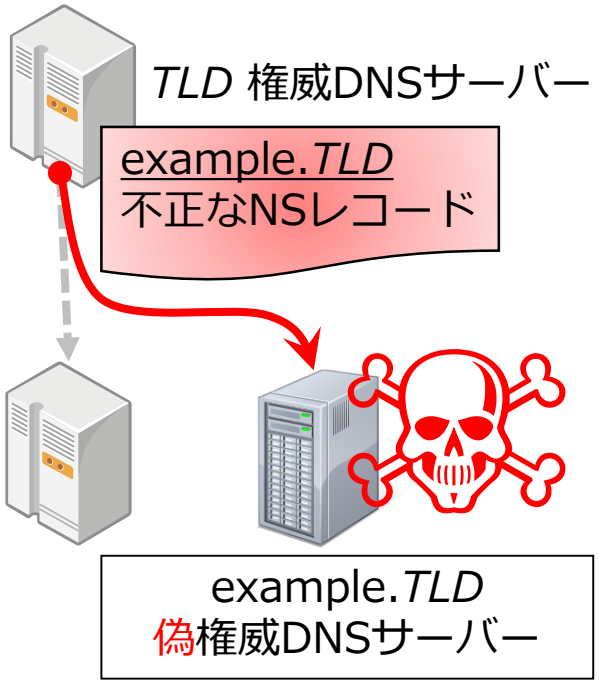
D) 利用者側の機器
- DNS関連設定の不正書き換え



ドメイン名ハイジャックの標的と手法の例（登録情報の不正書き換え）

- 登録情報の流れのどこかで、不正書き換えを実行



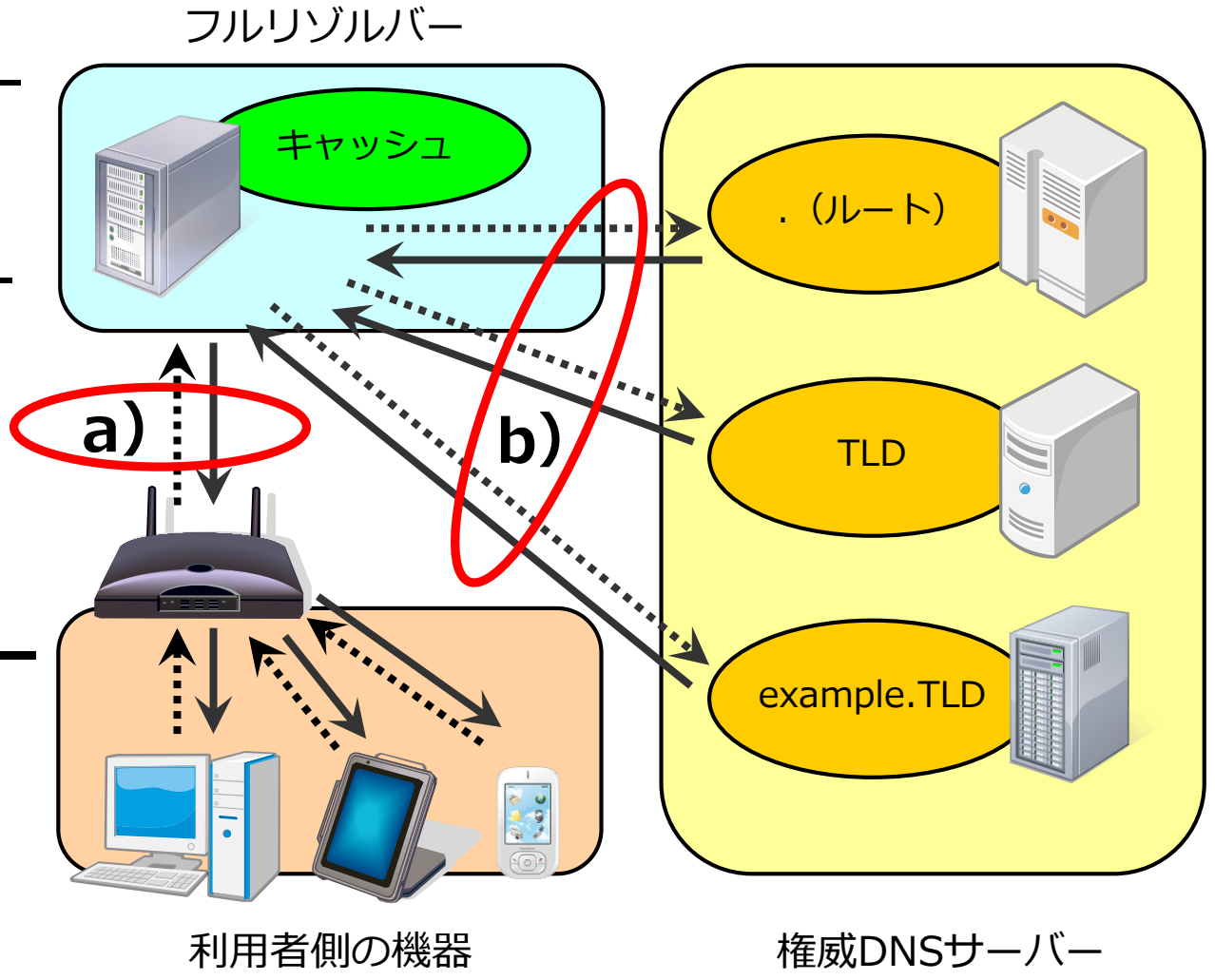


1）登録者になりすまして、レジストラのデータベースを書き換え
2）レジストラのシステムの脆弱性を突き、データベースを書き換え
3）レジストラになりすまして、レジストリのデータベースを書き換え
4）レジストリのシステムの脆弱性を突き、データベースを書き換え

（緊急）登録情報の不正書き換えによるドメイン名ハイジャックとその対策について
<https://jprs.jp/tech/security/2014-11-05-unauthorized-update-of-registration-information.html>

ドメイン名ハイジャックの標的と手法の例（構成要素間の通信に対する攻撃）

- 権威DNSサーバー・フルリゾルバーに対する**経路ハイジャック**
- 偽の経路情報を広告してネットワークトラフィックを乗っ取り、偽のサーバーに誘導する
  - **a）利用者⇔フルリゾルバー**
  - **b）フルリゾルバー⇔権威DNSサーバー**
- 意図的なものと、設定ミスによる経路情報の漏出がある
  - 状況のみからは判別しづらい



2. ドメイン名ハイジャックの主な事例

その後の攻撃トレンドとなった事例・
実際に被害が発生した最近の事例

本資料で紹介する事例

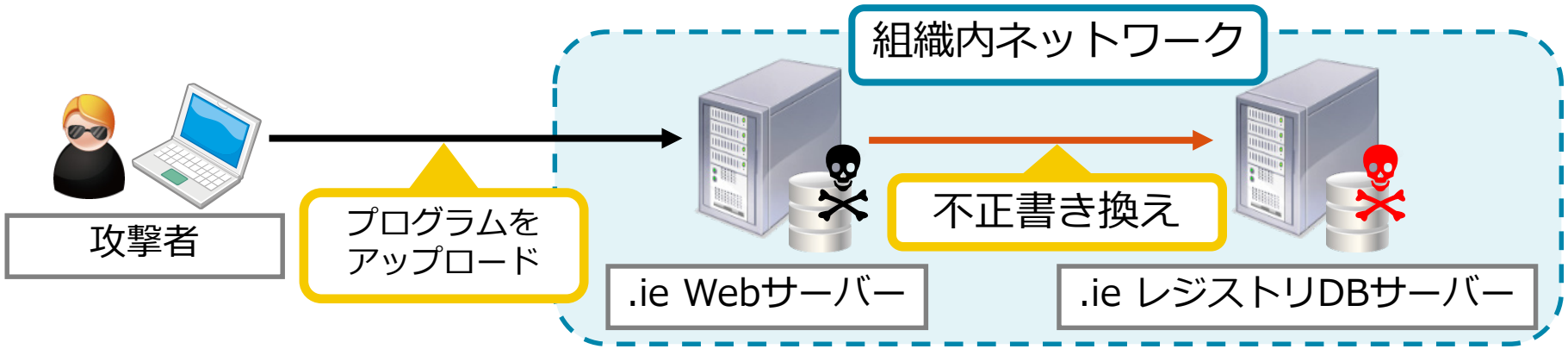
事例（年）	攻撃の**目的**	**標的**となったドメイン名	ドメイン名ハイジャックの**手法**	特記事項
事例①：IEDR（2012年）	**示威行為**	**google.ie、yahoo.ieなど**	**登録情報の不正書き換え**	以降、同様の示威行為が約2年にわたり流行
事例②：日経新聞・はてななど（2014年）	**閲覧者へのマルウェアの注入**	**nikkei.com、st-hatena.comなど**	**登録情報の不正書き換え**	日本国内における事例、攻撃の隠蔽を図った
事例③：Fox-IT（2017年）	**アカウント情報の不正入手**	**fox-it.com**	**登録情報の不正書き換え**	サーバー証明書の不正発行・不正使用にドメイン名ハイジャックを利用
事例④：Roaming Mantis（2018年）	**不正なアプリのインストール・アカウント情報の不正入手・仮想通貨のマイニングなど**	**security.apple.comなど**	**ホームルーターのDNS設定の不正書き換え**	A/AAAAが存在しないサブドメインを攻撃に使用
事例⑤：MyEtherWallet（2018年）	**仮想通貨の不正送金**	**myetherwallet.com**	**権威DNSサーバーに対する経路ハイジャック**	Google Public DNSに偽の情報がキャッシュされた

- 以降、攻撃の**目的・標的・手法**に注目する形で各事例を説明

事例①：IEDR（2012年）

- 目的：**示威行為**（Webブラウザーに「Hacked by ****」表示）
- 標的：**google.ie**、**yahoo.ie**など（IEDRは.ieのレジストリ）
- 手法：レジストリシステムに不正アクセスし、**登録情報を不正書き換え**
  - Webサーバーのコンテンツ管理に使っていた、CMSの脆弱性を利用（下図）
- 特記事項：この攻撃の後、**同様の示威行為が約2年にわたり流行**
  - 登録情報の不正書き換えによる示威行為

p.9のA
p.10の4



事例②：日経新聞・はてなど（2014年）

- 目的：**閲覧者へのマルウェアの注入**
- 標的：**nikkei.com**、**st-hatena.com**など
- 手法：レジストラ経由で**登録情報を不正書き換え**
  - 具体的な手法は不詳
- 特記事項：攻撃者が**不正書き換えの隠蔽**を図った
  - ネームサーバー情報の一部のみを書き換え
  - 1～2日程度で元の登録情報に切り戻し

p.9のA
p.10の1または2

事例③：Fox-IT（2017年）

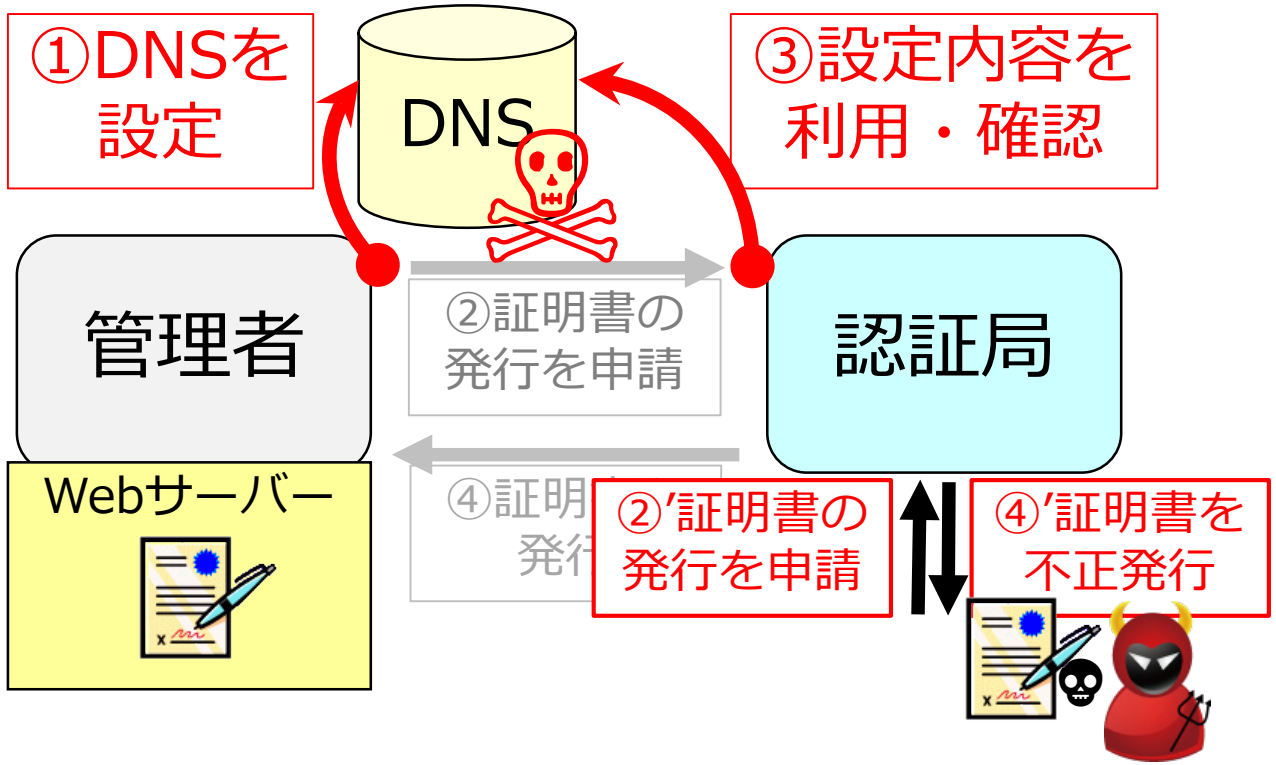
- 目的：**顧客のアカウント情報の不正入手**
- 標的：**fox-it.com**（Fox-ITはオランダのセキュリティ企業）
- 手法：登録者になりすまして、**登録情報を不正書き換え**
  - ログインID・パスワードをクラック
    - パスワードを長年変更しておらず、二要素認証などの認証強化は未提供・未使用
- 特記事項：**サーバー証明書の不正発行・不正使用**にドメイン名ハイジャックを利用
  - **HTTPSを攻撃**

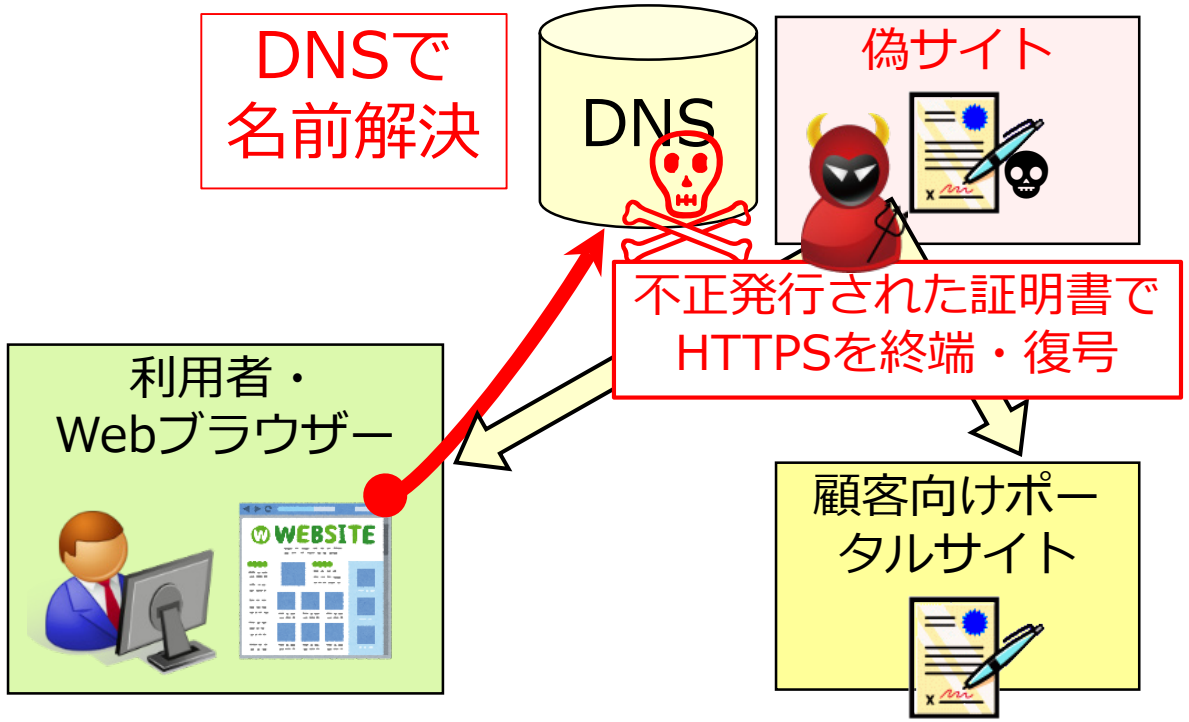
p.9のA
p.10の1

Fox-ITの攻撃で使われた手法

メール関連のDNS設定を変更し、メール認証を用いて**正規の方法でサーバー証明書を不正発行**

顧客向けポータルサイトのIPアドレスを変更して、**顧客のアクセスを偽サイトに誘導**、**HTTPSを終端・復号**後、正規のサイトに転送





事例④：Roaming Mantis（2018年）

- 目的：**Androidデバイスへの不正なアプリのインストール、iOSデバイス保有者のアカウント情報の不正入手、仮想通貨のマイニング**など
- 標的：**security.apple.com**など
- 手法：ホームルーターの**DNS設定の不正書き換え**
- 特記事項：**A/AAAAが存在しないドメイン名**を攻撃に使用
  - security.apple.comにはA/AAAAがなく、通常は直接アクセスしない
    - MXとTXT（SPF）は設定されている
  - **攻撃を見つけにくくする**ための手段の一つと考えられる

p.9のD

事例⑤：MyEtherWallet（2018年）

- 目的：**仮想通貨の不正送金**
- 標的：**myetherwallet.com**（仮想通貨ウォレットを提供）
- 手法：権威DNSサーバーに対する**経路ハイジャック**
  - 偽の経路情報を広告し、フルリゾルバーのアクセスを偽の権威DNSサーバーに誘導
- 特記事項：**Google Public DNS**に偽の情報がキャッシュ
  - パブリックDNSサービスやISPのフルリゾルバー経由で顧客を攻撃
  - **Webブラウザーの警告を無視して、先に進んだ顧客**が被害に

p.11のb

3. ドメイン名ハイジャックの分析

ドメイン名ハイジャックの変化
目的・標的・手法の変化
インターネットの運用形態・ユースケースの変化
変化から読み取れること

ドメイン名ハイジャックの変化

- インターネットそのものやそれを取り巻く状況の変化により、**ドメイン名ハイジャックの状況も変化**している
- 本パートでは、以下の二つに注目して分析
  - **ドメイン名ハイジャックの目的・標的・手法**の変化
  - **インターネットの運用形態・ユースケース**の変化

目的の変化

- ドメイン名ハイジャックの主な目的が、
  示威行為や主義・主張のアピールから、**実利の獲得**に
- 目的の例
  - マルウェアの注入（事例②）
    - 遠隔操作による計算機資源の不正使用が可能
  - アカウント情報の不正入手（事例③、④）
  - 仮想通貨の不正送金（事例⑤）

標的の変化

- 実利の獲得のため、著名企業やポータルサイトのドメイン名に加え、**それ以外のドメイン名**も標的に
- 標的の例
  - Webサイトに埋め込むスクリプトが使うドメイン名（事例②）
  - 顧客向けポータルサイトのドメイン名（事例③）
  - A/AAAAが存在しないドメイン名（事例④）
  - 仮想通貨の保持・取引に使うドメイン名（事例⑤）

手法の変化

- 基本的な手法は従来と同様
- 従来の手法に加え、
  目的・標的に対応した**新しい手法**や、**洗練された手法**も出現
- 新しい手法の例
  - 権威DNSサーバーに対する経路ハイジャック（事例⑤）
- 洗練された手法の例
  - ドメイン名ハイジャック以外の手法との組み合わせ
    （事例③、事例④）
  - 攻撃の隠蔽（事例②、事例③）

インターネットの運用形態・ユースケースの変化

- インターネットの**運用形態の変化やユースケースの変化**が、ドメイン名ハイジャックにも影響
  - 例：パブリックDNSサービスの普及
    - 利用者の集中
    - ISPに依存しないSingle Point of Failureの出現
  - 例：仮想通貨の取引や、フィンテックにおける利用
    - 仮想通貨取引サイトへの攻撃
    - マルウェアの注入による仮想通貨のマイニング、など

変化から読み取れること

- 目的・標的・手法の変化
  - 示威行為や主義主張のアピールから、実利の獲得に
  - より広範囲のドメイン名が標的に
  - 新しい手法・洗練された手法の出現
- インターネットの運用形態・ユースケースの変化
  - 新たな攻撃目標と、それを狙った攻撃の出現

単純なWebサイトのハイジャックが目的であった状況から、
実利の獲得のための手段の一つに変化

4. DNS運用者がすべきこと

対策の基本的な考え方
本パートで取り上げる対策とその概要
DNSをより安全にするために
おわりに：JPRSの情報発信

対策の基本的な考え方

- ドメイン名／DNS単体ではなく、**組織全体のリスクマネージメントの一環**として考え、対策する必要がある
- ドメイン名／DNSに関する対策としては、**何をどう守るか**に着目し、それぞれの対策を把握・導入することが重要
  - 何を：守る対象は？
    - 例：DNSの構成要素、DNSデータ、構成要素間の通信
  - どう守るか：その対策の効果は？
    - 例：ドメイン名ハイジャックの防止、ドメイン名ハイジャックの検知・対応

本パートで取り上げる対策

- 自組織で使っているドメイン名の状況把握
- 信頼できる事業者・サービスの利用・選択
- 事業者が提供するサービスの利用
- 監視サービスの導入・利用
- 経路ハイジャック対策

自組織で使っている ドメイン名の状況把握

- 個別の対策を実施するための**出発点**
  - 管理対象の正確な把握
- **ドメイン名のライフサイクルマネージメント**
  - 技術部門・管理部門・企画部門の連携が重要
  - 自組織で使うドメイン名・DNSの設計
    - どんなドメイン名をどんなサービスのために、どう使うか
    - 権威DNSサーバー名の選定も含まれる

次の「**DNS Day mini – 大切なドメイン名を守る –**」で、
ドメイン名のライフサイクルから見た脅威・リスクとその対策が解説されます

信頼できる事業者・サービスの利用・選択

- **マネージドDNSサービス**の利用
  - DNSサービスのメリットとデメリット、求められる機能などについて、以下の資料にまとめられている

> 権威DNSサーバ 脱自前運用のススメ
> <https://dnsops.jp/event/20180627/dns-summer-day-2018_simamura.pdf>

- **レジストリ・レジストラ・マネージドDNSサービス事業者**の選択
  - セキュリティを向上させるサービスを提供しているか
  - そのサービスを、自組織のドメイン名で利用可能か
  - 各種サービスについては、次ページを参照

事業者が提供するサービスの利用

- レジストリ・レジストラが提供する、**ロックサービス**の利用
  - レジストリロック・レジストラロック・ドメインロック
- 事業者のコントロールパネルに対する**アクセス制限**の利用
  - 登録情報や設定内容の意図しない変更の防止
- サービス利用における**認証**の強化
  - 二要素認証やクライアント証明書などの利用

次の「**DNS Day mini – 大切なドメイン名を守る –**」で、
管理権限を守るための認証強化とロックサービスの詳細が解説されます

登録情報の監視／監視サービスの利用

- ドメイン名ハイジャック対策の観点から監視すべき対象
  - レジストリの**Whois**の出力内容
  - レジストリの権威DNSサーバーの**NS/グルーレコード**の設定内容
  - 自組織の権威DNSサーバーの**A/AAAA/MXレコード**などの設定内容
- 確実な監視の実施
  - 自前での監視
  - 監視サービスの利用（項目の追加）

経路ハイジャック対策

- 以下、**AS運用者**における対策の例
  - RPKIの導入
  - 密なpeering
  - IRRへの正確な設定と、それに基づいたポリシーの設定
  - 経路情報の監視
  - 経路情報の細分化
    - MyEtherWalletの事件後、Amazon Route 53の経路が/24に
- 権威DNSサーバーの経路ハイジャックは、DNSSECで検知可能
  - DNSSEC検証エラーになる

DNSをより安全にするために

＜再掲＞ドメイン名／DNS単体ではなく、**組織全体のリスクマネージメントの一環**として考え、対策する必要がある

- それぞれの関係者・立場における、**地道で継続的な活動**
  - 各組織のドメイン名／DNSの運用・管理・企画担当者
  - DNSプロバイダー・パブリックDNSサービスの運用者
  - ドメイン名登録者・レジストラ・レジストリ、etc.
- 活動を継続可能にするための、**投資や体制作り**
  - 変化への対応（新たな目的・標的・手法）
  - よりよい対策の導入・実施

おわりに：JPRSの技術情報発信

- JPRS DNS関連技術情報
  <https://jprs.jp/tech/>
- JPRS トピックス & コラム
  <https://jprs.jp/related-info/guide/>
  – Internet Weekの展示ブースでも注入
- JPRS 公式SNSアカウント

- メールマガジン「FROM JPRS」
  <https://jprs.jp/mail/>
- JPRS サーバー証明書発行サービス
  <https://JPRSサーバー証明書.jp/>


@JPRS_official


JPRSofficial

JPRSでは今後も関連各位と協力しながら、
さまざまな形で情報発信を続けていきます

That’s it!