勉強会タイトル:【実践編】顧客ビジネスを守るDNSセキュリティとアーキテクチャ設計

スライド1:タイトル

タイトル: 顧客ビジネスを守る DNSセキュリティとアーキテクチャ設計
サブタイトル: 攻撃メカニズムの理解と、堅牢な構成提案へのアプローチ
対象: インフラエンジニア / プリセールス
ゴール: セキュリティリスクを「ビジネスへの影響」として翻訳し、最適な構成を提案できるようになること。

スライド2:本日のアジェンダ

1. **DNS**の重要性**:** ビジネスインパクトとエンジニアの役割
2. 基礎と設計原則**:** 仕組みの可視化と「分離」の鉄則
3. 脅威と対策①**:** DNSアンプ攻撃(加害者リスク)
4. 脅威と対策②**:** キャッシュポイズニング(偽装リスク)
5. 脅威と対策③**:** DNSトンネリング(漏洩リスク)
6. アーキテクチャ**:** Hidden Master構成とクラウド活用

スライド3:はじめに - DNSは「サービスの心臓部」

【スライド上の要素】

- **DNS**の重要性**:** すべてのトラフィックの起点。
- 障害時のビジネスインパクト(金銭的損失)**:**
    - **EC**サイト**:**「1時間の停止で売上 ◯百万円の機会損失」
    - コールセンター**:**「Web閲覧不可による入電殺到 → オペレーション崩壊・顧客満足度低下」
    - 業務システム**:**「全社員が仕事できない時間の給与コスト」
- エンジニアのミッション**:**
    - 「名前解決ができる」は当たり前。**「攻撃に強く、停止しないインフラ」**を設計・提案すること。

【講師用トークスクリプト】
お疲れ様です。本日はDNSセキュリティについて、設計と提案の観点から話をします。
なぜ我々がDNSを守るのか? それは技術の問題ではなく「お金」の問題だからです。
例えば、年商規模の大きいECサイトなら、DNSが1時間止まるだけで数百万円が飛びます。コールセンターなら、Webが見れない顧客からの電話でパンクし、CS(顧客満足度)が地に落ちます。
我々の仕事は、DNSサーバーを構築することではなく、こうした**「ビジネス損失を防ぐアーキテクチャ」**を提供することです。

スライド4:【基礎復習】DNS通信の仕組み(キャッシュと権威)

【スライド上の要素】

- **【図解メモ: 左側に「社内ネットワーク枠」、右側に「インターネット枠」を描く】**
  - **社内枠:** Client PC → キャッシュ**DNS (Recursive Resolver)**
  - **境界線:** Firewall / Internet Boundary
  - **インターネット枠:** ルートDNS → TLD DNS(.com) → 権威**DNS (Authoritative Server)**
  - **矢印:** Clientからキャッシュへ、キャッシュから各権威へ順番に聞きに行くフロー。
- **2つの主役:**
  - ① キャッシュ**DNS (探索者): 社員が使う。社内に置くことが多い。**
  - ② 権威**DNS (管理者): 世界に見せる。社外（DMZ/クラウド）に置く。**

【講師用トークスクリプト】

セキュリティ設計の第一歩は「場所」の把握です。
この図を見てください。左側が「社内」、右側が「インターネット」です。
「キャッシュDNS」は社内の人間が外を見るためのもの。「権威DNS」は外の人間が自社を見るためのもの。
通信の流れる方向も、守るべき境界線も全く違います。ここを混同しないことが、後の「分離設計」の基礎になります。

スライド5：【基本設計】リスクを分離する（キャッシュと権威の分離）

【スライド上の要素】

- 鉄則: 「社内からのアクセス（キャッシュ）」と「外部への公開（権威）」はサーバーを分ける。
- リスク（同居の弊害）:
  - 内部PCへのマルウェア感染等でキャッシュ機能が高負荷になると、公開サービス（権威）も巻き添えでダウンする。
  - **アタックサーフェス（攻撃対象領域）**の拡大を防ぎ、**Blast Radius（爆風半径＝被害範囲）**を限定する。

【用語解説（脚注）】

- アタックサーフェス: 攻撃者が侵入や攻撃を試みることができる「接点」の広さ。
- **Blast Radius (ブラスト・ラディウス): 障害や攻撃が発生した際に、影響が及ぶ範囲の広さ。**

【講師用トークスクリプト】

設計の基本原則は「機能の分離」です。
なぜ分けるのか？ ここで覚えてほしい単語が**「Blast Radius（被害範囲）」**です。
もし同居させていると、社内PCがウイルス感染してキャッシュサーバーをダウンさせた時、全く関係ない「お客様向けのWebサイト（権威）」まで道連れで止まります。
被害を「社内だけ」に留めるために、サーバーを物理的・論理的に分ける。これがプロの設計です。

スライド6：脅威① DNSアンプ攻撃（DDoSの踏み台リスク）

【スライド上の要素】

- 攻撃のメカニズム: UDPの特性（ステートレス）と、応答サイズの差（増幅）を悪用。
  1. **Spoofing:** 攻撃者が送信元IPを「被害者」に偽装して問い合わせ。

2. **Amplification:** DNSサーバーは、被害者に対して巨大なパケットを送りつける。

- 対策:
  - オープンリゾルバ対策: 社外（インターネット）からの再帰問い合わせを拒否する（ACL設定）。
  - レートリミット **(RRL):** 異常な頻度の応答を制限する。

【顧客対話のポイント】
自社がダウンするだけでなく、他社への攻撃に加担してしまう**「サプライチェーンリスク」**として説明する。
【講師用トークスクリプト】
1つ目の脅威は「アンプ攻撃」です。これは自社のサーバーがDDoS攻撃の「増幅器」として悪用されるケースです。
顧客には「御社のサーバーが加害者になり、他社へ損害を与えるリスクがあります」と伝えてください。
技術的な対策としてはACLやRRLですが、ビジネス的には「加害者になって信用を失わないための保険」としての設定です。

スライド7：脅威② キャッシュポイズニング（フィッシング誘導）

【スライド上の要素】

- 攻撃のメカニズム: DNSキャッシュサーバーに「偽のIPアドレス」を注入する。
- 被害: 正規URLを入力しても偽サイトへ誘導され、ID/PASSが盗まれる。
- 対策:
  - ソースポートランダマイズ: 予測を困難にする（基本）。
  - **DNSSEC:** 電子署名を用いて、回答の正当性を検証する。
  - 【構成上の対策】: キャッシュサーバーをインターネットに直接晒さない（社内専用とし、外部からのアクセスを完全に遮断する）。

【用語解説（脚注）】

- **DNSSEC:** ドメイン情報の「正しさ」をデジタル署名で保証する拡張機能。改ざん検知が可能。

【講師用トークスクリプト】
2つ目は「ポイズニング」、偽の住所を覚え込ませる攻撃です。
DNSSECなどの技術的対策もありますが、「構成」で守ることも重要です。
スライド3の図を思い出してください。キャッシュDNSは「社内の人間」しか使いません。
なら、インターネット側からの通信をFirewallで全拒否してしまえば、攻撃者が毒を入れに来る経路自体を塞ぐことができます。

スライド8：脅威③ DNSトンネリング（情報の不正持ち出し）

【スライド上の要素】

- 攻撃のメカニズム: DNSプロトコルを「データの運搬経路」として悪用。C2サーバーとの通信路になる。
- リスク: Firewallをすり抜ける「セキュリティの抜け穴」。
- 対策: DNSログの監視・分析
  - 異常に長いサブドメイン名（例: SECRET-DATA-XYZ...123.attacker.com）
  - ランダムな文字列（意味不明な英数字の羅列）が頻出するドメイン

    - **TXT**レコードや特定ドメインへの高頻度クエリ
    - **SIEM**等での相関分析

【用語解説（脚注）】

- **C2 (Command & Control)** サーバー**:** 攻撃者がマルウェアに感染した端末へ命令を送ったり、データを盗んだりするための司令塔サーバー。
- **SIEM (**シーム**):** ログを一元管理し、複数のログを組み合わせて脅威を分析するシステム製品。

【講師用トークスクリプト】

3つ目は「情報漏洩」です。DNSを裏口（トンネル）にします。
これを見抜くには「ログ」を見るしかありません。
「意味のないランダムな長い文字列」や「異常な回数の問い合わせ」など、人間が見ても怪しいログを機械的に検知する必要があります。
ここで「SIEM（シーム）」などのログ分析基盤の提案につなげることができます。

スライド**9**：【推奨構成】**Hidden Master**（隠しマスター）による防御

【スライド上の要素】

- 構成コンセプト**:**
    - **Master (Origin):** ゾーン情報の「原本」を持つ。インターネットからの直接アクセスを遮断。
    - **Slave (Edge):** インターネットに公開し、クエリを処理する。
- メリット**:**
    - **Origin**の保護**:** 攻撃者がマスターサーバーを特定できないため、改ざんリスクが極小化される。
    - 復旧の迅速化**:** スレーブがダウンしても、マスターから再度展開すれば即座に復旧可能。

【講師用トークスクリプト】

堅牢なDNSアーキテクチャの基本、「Hidden Master（隠しマスター）」構成を紹介します。
データの原本を持つマスターサーバーを、インターネットから隔離（隠蔽）します。表側にはコピーを持ったスレーブサーバーだけを配置します。
こうすることで、アタックサーフェスを最小化し、万が一の攻撃時も原本データを守り抜くことができます。

スライド**10**：マネージド**DNS**（**Cloud**）活用の提案と注意点

【スライド上の要素】

- **Cloud (AWS Route53 / Google Cloud DNS)** のメリット**:**
    - **SLA（稼働率保証）**とDDoS対策基盤の利用。
    - 運用負荷（パッチ適用等）のオフロード。
- 考慮すべきリスク（バランス感覚）**:**
    - 単一障害点**:** クラウド事業者自体の大規模障害時に道連れになる。
    - ベンダーロックイン**:** 将来的な移行が難しくなる。

- 提案シナリオ:
    - 「可用性を最優先するなら、オンプレミスとクラウドのハイブリッド構成や、マルチクラウドDNSも検討しましょう」

【講師用トークスクリプト】
最後に、クラウドサービスの活用です。
クラウドに任せれば万事解決と思われがちですが、プロはリスクも伝えます。
「AWSのDNSが止まったらどうしますか？」という問いです。
単に丸投げするだけでなく、本当に止めてはいけないシステムなら、異なるクラウドを組み合わせる等の冗長化も視野に入れて提案してください。

スライド11：本日のまとめ（Key Takeaways）

【スライド上の要素】
- ビジネスを守る3つの視点:
    1. **Separation (分離):** キャッシュと権威を分け、被害の拡散（Blast Radius）を防ぐ。
    2. **Architecture (構成):** 設定だけでなく、Hidden Masterやクラウド活用で「堅牢な枠組み」を作る。
    3. **Business Logic (対話):** セキュリティ対策を「技術」ではなく「損害回避コスト」として説明する。
- **Next Action:**
    - 既存顧客のDNS構成を見直し、「分離」や「隠蔽」ができているかチェックする。
    - リスクが見つかれば、「御社のビジネスを守るため」という文脈で提案を行う。

【講師用トークスクリプト】
本日のまとめです。
DNSはただの「名前解決」ではなく、ビジネスを支える重要な土台です。
技術的な細かい設定も大切ですが、まずは**「分離する」「隠す」「リスクを翻訳する」**という3つの視点を持ち帰ってください。
明日からの現場で、単なる作業者ではなく、「お客様のビジネスを守るアーキテクト」として活躍されることを期待しています。

スライド12：QA

- 質疑応答
- 用語確認（Attack Surface, Blast Radius, SIEM, DNSSEC等）

【附録】本スライドの作成コンテキスト

※このセクションはスライド本編には含めず、企画・準備のための背景情報として参照してください。

1. 企画背景とターゲット

- 実施企業: CTCテクノロジー株式会社（インフラ構築・保守のプロフェッショナル集団）。
- ターゲット: 社内の若手・新人エンジニア。
    - DNSの専門家ではないが、基礎的なIT知識は有する層。
    - 「電話線」「シャッター」といった過度な子供向けメタファーは避け、実務に即した用語（

SLA、可用性など）での説明を希望。

- 実施目的:
  - DNSセキュリティのリテラシー向上。
  - 単なる知識習得に留まらず、**「顧客と対話し、リスクを説明し、構成を提案できる」**レベルへの引き上げ。

2. コンテンツの設計方針

- 脱・設定値偏重:
  - 設定ファイルの書き方よりも、「なぜその構成にするのか」というアーキテクチャ論（Hidden Master、クラウド活用など）を重視。
- ビジネスリスクへの翻訳:
  - 技術的な脅威（アンプ攻撃、ポイズニング）を、顧客視点のリスク（加害者になる、信用の失墜、サービス全断）に翻訳して伝える能力を育成する。
- 専門用語のバランス:
  - 「スプリットホライゾン」「nonce」などの過度に専門的な用語は避けつつ、「キャッシュ/権威の分離」「アタックサーフェス」といった現場で必須の概念は、平易な言葉（仕組みの図解など）で解説する。

3. 重点学習項目

1. 仕組みの理解: キャッシュ（探索）と権威（案内）の役割の違い。
2. リスクの理解: オープンリゾルバによるDDoS加担（加害者リスク）、トンネリングによる情報漏洩。
3. 設計への応用: リスクを回避するための分離設計、隠しマスター構成、クラウドへのオフロード提案。