# 2.11 DNS キャッシュポイズニング

## 2.11.1 DNS キャッシュポイズニングとは

**DNS キャッシュポイズニング**とは，DNS のキャッシュ機能を悪用して，ドメイン名を不正な IP アドレスに解決し，ブラウザを不正な Web ページなどに誘導する攻撃手法です。

DNS キャッシュポイズニングを理解する前提知識として，**キャッシュサーバ**と**コンテンツサーバ**を理解しておきましょう。

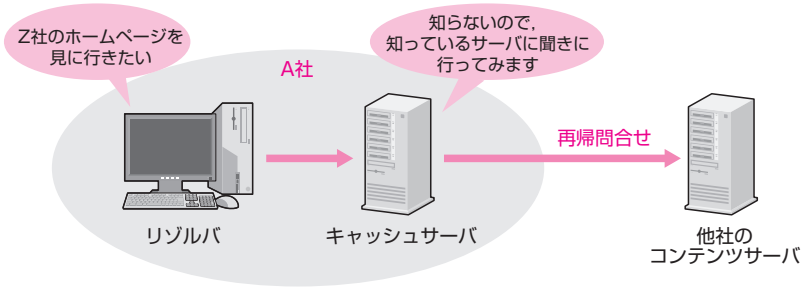
以前は 1 台のサーバでこの 2 つの機能を動作させていましたが，近年セキュリティの向上や運用性の向上を企図して，分けて構築することが増えてきました。

用語 **SEO ポイズニング**
××ポイズニングは他にもあって，過去試験では SEO ポイズニングが出題実績アリ。不必要なタグやリンクを大量に置くなどして，あるキーワードで検索したときの検索結果上位に不正サイトを載せ，利用者を誘導する。

### キャッシュサーバ

オリジナルの名前解決情報を持たない DNS サーバで，**リゾルバ**（DNS のクライアント）から問合せがあるとコンテンツサーバへ問合せ（**再帰問合せ**という）を行うものです。

コンテンツサーバから教えてもらった名前解決情報は，しばらくの間キャッシュ（蓄積）して，次の問合せに素早く答えられるようにしておきます。しばらくの間，と留保をつけているのは，オリジナルの情報が書き換わってしまったのに，リゾルバに古い情報を教え続けるのを防止するためです。




▲ 図 キャッシュサーバのしくみ

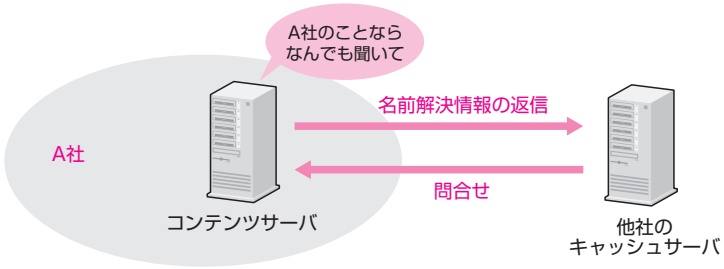
### コンテンツサーバ

名前解決情報のオリジナルを管理する DNS サーバです。キャッシュサーバからの問合せに答えます。オリジナルのデータを持っているので，権威サーバと呼ばれることもあります。





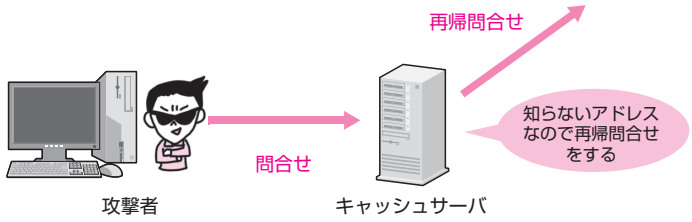





▲ 図 コンテンツサーバのしくみ

### DNS キャッシュポイズニングの手順

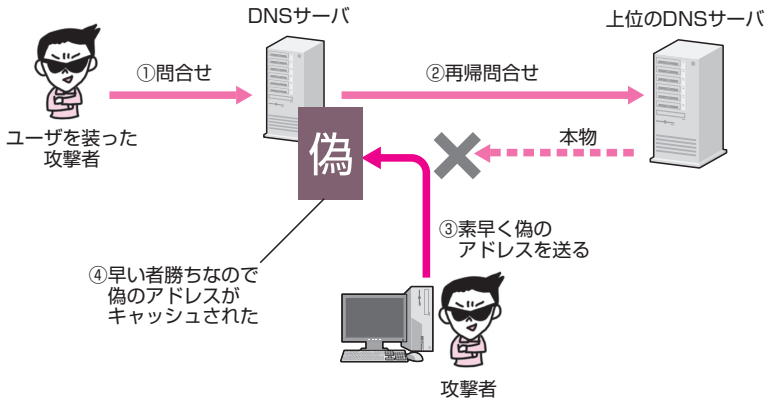
名前のとおり，DNS にキャッシュされた情報を汚染することで，DNS に偽の解決情報を登録させ，それを教えられたブラウザなどを任意の Web ページに誘導するわけですが，まず攻撃者自身が標的のキャッシュサーバに名前解決の問合せをします。そのキャッシュサーバは，情報がキャッシュされていない場合，上位の DNS サーバに再帰問合せをします。




用語 **ARP スプーフィング**
ARP 要求に対する応答が複数なされた場合，最も早くクライアントに届いた応答が登録される。この仕様を利用した攻撃手法で，偽の MAC アドレスを登録することで，意図しないノードと通信をするよう誘導するもの。

ところが，この問合せに対する返信については，トランザクション ID と呼ばれる簡単な ID 以外に真正性を確認する手段は設けられていません。この ID とポート番号さえ一致すれば，一番早く返ってきた返答をそのまま信頼します。通信プロトコル自体も UDP が使われており，パケットの偽装が簡単です。

つまり，攻撃者は正規の上位 DNS サーバが応答する前に，応答パケットを偽装して送りつけることで，標的のキャッシュサーバに偽の名前解決情報をキャッシュさせてしまえるのです。




▲図 DNS キャッシュポイズニングの流れ

## Kaminsky Attack

キャッシュポイズニング攻撃を効率的に行う方法です。例えば技術評論社を攻撃するなら，正規のドメイン gihyo.jp に対して，同じドメインで存在しない名前，uheuhe.gihyo.jp（uheuhe は架空のホスト名で，実在しない）を問い合わせます。キャッシュの TTL が長くても短くても，この FQDN の名前解決情報は存在しないため，キャッシュサーバは必ず再帰的問合せを行います。正当な応答が戻る前に偽の応答を行えば攻撃が成功するというものです。

参考 キャッシュの TTL を長くしておく手法もある。再帰的問合せがあまり発生しなくなるので，攻撃しにくくなる。しかし，攻撃が成功すると，偽情報が長くキャッシュされることになる。

## DNS キャッシュポイズニングへの対策

現時点で多くとられている対策は，キャッシュサーバが再帰問合せをする際の送信元ポート番号やトランザクション ID をランダムなものにして，攻撃者が偽装パケットを送りにくくする方法です。ただし，この方法は完全なものとはとてもいえず，あくまで「やりにくくなる」程度のものです。

また，こうした対策を実施する上で，DNS のベンダがパッチを当てて送信元ポート番号をランダム化するようにしても，古い設定で送信元ポート番号が固定になっているとパッチが有効に働かないなどの事例も報告されていて，混乱が続いています。

その他に，本試験の解答になりそうな解決策としては，DNS に問合せをしてよいクライアントを IP アドレスなどで限定すること，再帰的問合せと異なるトランザクション ID の通信や，コンテンツサーバからの返答数が問合せ数より多いことを検出するなどがあげられます。







根本的な解決策としては，DNS のプロトコル自体を改善した DNSSEC への移行を待たなければならないと思います。

## DNSSEC

DNSSEC（DNS Security Extensions）とは，旧来からある DNS のセキュリティ拡張方式です。規格自体は以前からありましたが，設定が難解で，つながらないなどのトラブルも多く，普及しなかったというのが実情です。

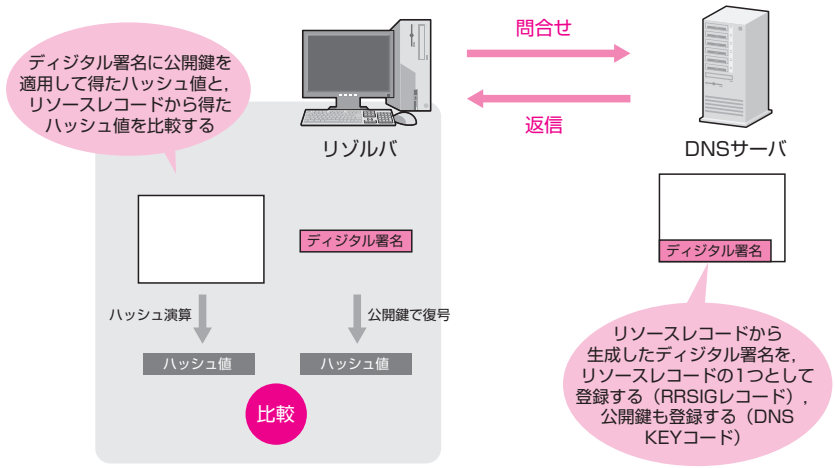
DNSSEC はサーバ，クライアントの双方が対応している必要があり，さらに DNS サーバ自身が多数の階層構造を持っていることも考慮すると，置き換えなければならないノード数は膨大です。普及を急速に進めるのは簡単ではありません。

しかし，DNS キャッシュポイズニングの多発により，近年注目を集めており，それにつれて出題も増加傾向にあります。DNSSEC を推進する団体の活動も目立ち始め，対応 DNS サーバも増えてきました。

参照 ディジタル署名 ➜ 第 4 章 4.9

参照 公開鍵暗号方式 ➜ 第 4 章 4.4

DNSSEC は DNS のリソースレコードのハッシュ値からディジタル署名を生成し，それ自身を RRSIG レコードとして登録します。情報を受け取った側は，RRSIG レコードを公開鍵で検証することで，送られてきたリソースレコードが正当なものであることを確認できます。




▲図 DNSSEC

# 5 パブリッククラウドサービス

**問題の概要**

パブリッククラウドがテーマとして設定されています。もちろん，クラウドについて知っておく必要はあるのですが，情報処理安全確保支援士試験の場合は，クラウドを構成する技術が詳細に問われることはありません。その運用方法（二要素認証など）であったり，事故が起きた場合の（クラウド特有の）対処方法・ポイントを問うのが主眼です。そこに注意して準備を進めてください。クラウドに限らず，出題対象の技術は日常生活でも使ってみると高い理解に結びつきます。

**キーワード**

なりすまし
モバイル端末管理
クッキー
ワンタイムパスワード
代替サービスへの移行

## パブリッククラウドサービスの安全な利用に関する次の記述を読んで，設問１～３に答えよ。

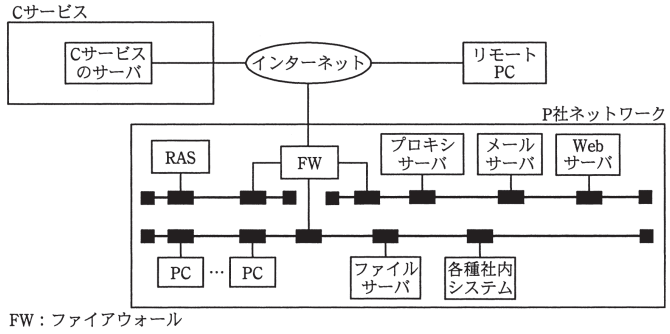
P社は，経営コンサルティングを行っている，従業員数60名の会社であり，オフィスは東京にある。P社には，オフィスに常勤している従業員と，主に客先や自宅で作業を行い，打合せのときだけオフィスに出社する従業員がいる。

社内にファイルサーバを設置して利用していたが，容量は十分であるものの検索の機能が不十分なことから，高機能のファイル共有サービス（以下，Cサービスという）を提供しているC社と契約し，Cサービスを利用し始めた。Cサービスは，ブラウザ経由でアクセスできるSaaS型パブリッククラウドのサービスである。P社は，Cサービスのサーバ内にP社専用の領域を確保して，使用履歴，作成者名，メモなどの情報を添えた上でプロジェクト資料を保管している。P社では，Cサービスを活用することで，検索を高速に行えるようになり，業務効率が格段に向上するものと見込んでいる。

客先や自宅で作業を行う従業員には，社外で利用するためのPC（以下，リモートPCという）を貸与しており，リモートPCをインターネットに接続できれば，リモートアクセスサーバ（RAS）経由で社内に接続し，社内システムにアクセスできる。客先や自宅からCサービスへのアクセスは，P社ネットワークを経由せずに直接行う。ネットワーク構成の概要を図1に示す。








FW：ファイアウォール

図1　ネットワーク構成の概要

〔Cサービスの認証の強化〕

Cサービスの契約と利用者管理については，総務部のX課長が管理責任者を務めている。Cサービスの採用については，Cサービスが停止するような事態が発生した場合の事業継続について具体的対策を1年以内にまとめることを条件に社長の了承を得ていた。

契約後に，“あるパブリッククラウドサービスから，パブリッククラウドサービス会社の管理が不十分であったのでパスワードが大量に漏えいし，保存されていたデータが漏えいした”との報道があった。漏えいがあったパブリッククラウドサービス会社はC社ではなかったが，報道を聞いたP社の社長は，Cサービスで保管している情報が漏えいして多大な損害が発生することを懸念し，X課長に，Cサービスを利用する際の認証の強化を検討するように指示した。X課長は，部下のQさんに，認証の強化策を調査するよう指示した。

Qさんはまず，Cサービスのセキュリティに関する機能を表1にまとめた。

表1　Cサービスのセキュリティに関する機能（抜粋）

| 番号 | 項目 | 機能 | 備考 |
|---|---|---|---|
| 1 | 利用領域へのアクセス制御 | 契約会社ごとに割り当てられた領域だけにアクセスできる。 | P 社が契約している領域は，200 G バイトである。 |
| 2 | 利用者管理 | 契約会社内の管理責任者が，C サービスの利用者管理機能を使って自社の利用者 ID を管理する。 | 管理責任者は，アクセス履歴も確認できる。 |
| 3 | 通信路暗号化 | 通信路は，サーバ認証による SSL で暗号化される。 | |
| 4 | 利用者認証 | Web 画面で入力された利用者 ID（会社が利用者に付与したメールアドレスを利用者 ID として使用）とパスワードを，C サービス内で照合し，利用者認証を行っている。認証情報は，利用者 ID とパスワードが必須である。<br>追加オプションとして，ログイン手続中に，利用者のメールアドレスに送信したワンタイムパスワードも入力する方式（以下，追加認証方式という）が用意されている。 | 全ての契約会社の利用者が，同じ URL の Web 画面からログインする。 |

Q さんは，利用者が個人所有の携帯電話メールアドレスを活用することも視野に入れて，追加認証方式の利用について検討した。検討結果を（1）～（3）に示す。

（1）業務上の支障の有無

次の理由から，業務上の支障はないと判断した。

・P 社では，P 社が契約した携帯電話を多くの従業員に貸与しており，個人所有を含めると全従業員が携帯電話を利用できる。

・携帯電話の故障，紛失などが年に数件発生しているが，個人所有の場合も含めて，携帯電話業者に依頼すれば速やかに同一電話番号かつ同一メールアドレスで利用が再開できる。

なお，P 社貸与の携帯電話は，盗難，紛失があった場合には必ず総務部に連絡することになっている。盗難届，紛失届を受けると総務部は，速やかに対応している。

（2）認証強度

他のパブリッククラウドサービスで利用者のパスワードが漏えいした事件を踏まえ，C サービスの利用者 ID とパスワードが漏えいした場合であってもなりすましが困難であるかどうかを評価することにした。

（3）追加認証方式の手順

Q さんは，追加認証方式について，次の手順案を作成した。

・C サービスの利用者 ID 登録手順案（図 2）

・C サービスの利用者 ID 変更手順案（図は省略）

・認証の手順案（図 3）







ヒント この携帯電話メールアドレスは誰のものか，そしてそれを確認する方法はあるのかを，考えてみよう。

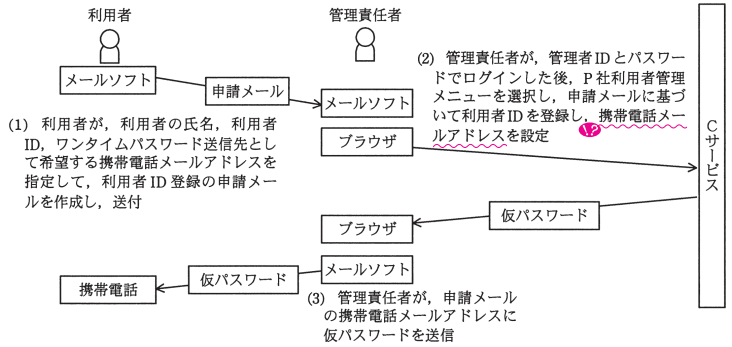
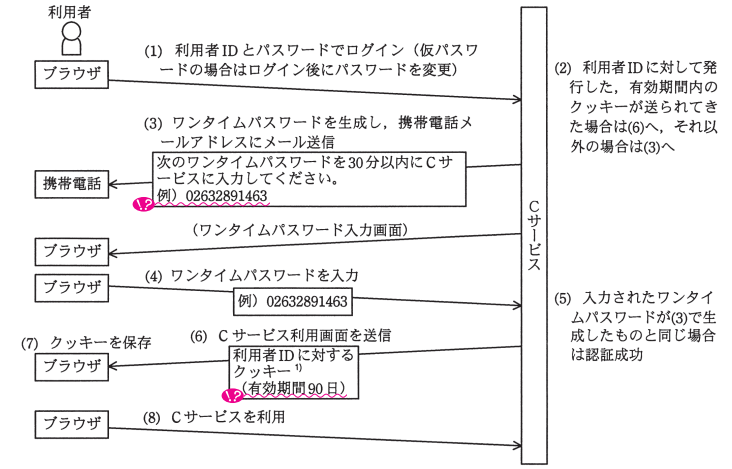



図2　Cサービスの利用者 ID 登録手順案（抜粋）

ヒント この手の数値は出題ポイント。通読しつつ，ざっとで良いので頭に入れておくようにしよう。

ヒント ここにも数値が出てきた。さっきとは単位が違う。




注 1)　(5)で認証が成功した場合だけ新たにクッキーが生成され，ブラウザに保存される。
同じ利用者 ID に対してさらに他のクッキーが生成された場合でも，このクッキーは 90 日間有効である。

注記　ログイン状態が 24 時間以上継続すると，自動的にログアウトされ，再度(1)から認証を行う。

図3　認証の手順案（抜粋）

Q さんが手順案を X 課長に提示したところ，“図 2 の手順では，①第三者が利用者になりすまして，仮パスワードを簡単に入手できてしまう”と指摘された。

さらに，“個人の携帯電話が盗まれ，かつ，利用者 ID とパスワードが推測されてしまったときに，②C サービスが不正使用され，しかも，それが長期間続くおそれがある”と指摘された。

Q さんは，それらの指摘に対応するため，手順を修正し，対策を追加した。

修正後，追加認証方式は，十分な認証強度をもっていると判断され，P 社では追加認証方式を採用することになった。

〔C サービスを利用できない場合の対応〕

Q さんは，C サービスが停止するような事態が発生した場合の具体的な対策を検討し，表 2 にまとめた。

表 2　C サービスが停止するような事態が発生した場合の具体的な対策

| 想定シナリオ | 求められる業務レベル | 事前準備として実施すること | 想定シナリオが現実化してから実施すること |
|---|---|---|---|
| C サービスのサーバが被災し，停止するが，2 週間後に元どおり再開する。 | 業務効率の低下は許容するが，C サービス停止の 24 時間後にはプロジェクト資料を使う業務を再開できる。 | a しておく。 | ファイルサーバを用いて，b する。ただし，C サービス復旧後は，C サービスの利用を再開する。 |
| C 社が，1 か月後に C サービスの提供を終了すると通知し，実際に 1 か月後にサービス終了となる。 | 業務効率を低下させることなく業務を継続できる。 | C サービスに代替可能なサービスを選定しておく。<br>C サービスからの c を確認しておく。 | 代替サービスと契約する。<br>代替サービスのセットアップ（ID 登録や設定）を行う。<br>C サービスのデータを代替サービスに移行する。<br>代替サービスの利用方法を従業員に周知する。 |

ヒント ファイルサーバの役割と言えば……。

表 2 の内容は承認され，P 社の事業継続計画に盛り込まれた。定期的に訓練が実施されることになり，その後，新しい手順で C サービスの利用が開始された。

**解答のポイント**

午後問題とはいうものの，午後Ⅰですと午前問題の延長で，知識問題のつもりで解いてしまう方もおられます。もちろん，それで解ける問題もあるのですが，午後Ⅱに比べて短めとはいえ長文のシナリオ問題です。きちんと文脈を把握しないと，解答できない問題が大多数です。

この問題は極めてオーソドックスな出題ですが，単にクッキーやなりすましを知っているだけでは解答できないように設計されています。慢心せず必ず問題文を（流し読みでいいので）1 度は通読してください。下線，空欄の前後は特に重要です。出題者は保身のために必ず問題文中に解答根拠を用意しています。単に正解を見つけるだけでなく，解答根拠も示す練習をしておくと，ぐっと合格率があがります。

**理解度チェック**

解答 → p.556

①なりすましって，何で防ぐ？

②P システムの認証手順は，どこに書いてありましたか？







**設問 1**

**本文中の下線①について，どのような方法で第三者が仮パスワードを入手することができるか。また，その対策としてどのように本人確認すればよいか。それぞれ 25 字以内で述べよ。**

## ■解説

**【方法】**

まず下線①をきちんと読み返しましょう。意外に，記憶に頼ったり，解答に必要ないと断じて読み返さずに考え始める方がいますが，大きな脆弱性を孕んだ行為です。下線①は［C サービスの認証の強化］パラグラフの，X 課長の指摘部分です。現実の上司は有能だったり，その正反対だったりと色々ですが，本試験に出てくる上司は十中八九有能なので，色眼鏡をかけずに素直に読むことが重要です。

> “図 2 の手順では，①第三者が利用者になりすまして，仮パスワードを簡単に入手できてしまう”と指摘された。

けっこう上から目線の指摘ですので，現実の業務では殺意を覚えるかもしれませんが，ここでは殺意ではなく解答を育てます。X 課長の指摘の論拠になっている図 2 を見てみましょう。

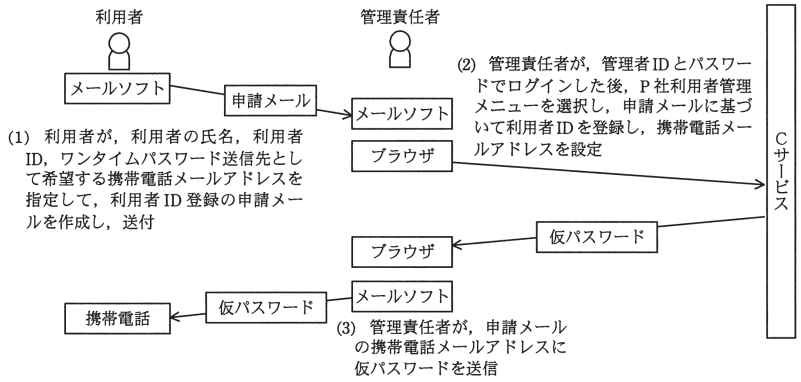



図 2　C サービスの利用者 ID 登録手順案（抜粋）

このプロセスでは，利用者が携帯電話のメールアドレスを指定した申請を行い，管理担当者がそのアドレスに対して仮パスワードを送信していることがわかります。

これはかなり牧歌的な手順です。だって，携帯電話メールアドレスを疑っていないのですから。申請メールに書くべき諸元（スペック）と，申請メールの送付先さえ知っていれば，誰でも申請メールを作成し，仮パスワードを入手することができてしま