DNSのセキュリティ

DNSの運用に起因するセキュリティ問題

2014年11月20日

Internet Week 2014 チュートリアル

株式会社日本レジストリサービス（JPRS）

あはれん　よしたか

阿波連　良尚

目次

- セキュリティの3要素の紹介
- ケーススタディ: ソフトウェアの脆弱性
- ケーススタディ: 運用上の問題

セキュリティの3要素

- Confidentiality: 機密性
- Integrity: 完全性
- Availability: 可用性

DNSと機密性

- ゾーン情報は公開情報とみなされる
  - 機密性は求められない
- DNSパケットは平文で送受信される
- 脅威: リクエスト情報の漏洩
  - リクエストに関する情報（送信元IPアドレス、リクエストの名前・クラス・タイプ）を秘匿したい
  - IETFのdprive WGにて議論されている

DNSと完全性

- 完全性の保証がない
  - 完全性はDNSSECやTSIG等で提供される
- 脅威: キャッシュポイズニング
  - カミンスキー型攻撃
  - 第一フラグメント便乗攻撃
  - 委任インジェクション攻撃
- 脅威: 権威DNSサーバー間のゾーン情報の不一致
  - ゾーン転送の失敗
  - ゾーン転送経路での中間者攻撃

DNSと可用性

- DNSサービスには高い可用性が求められる
  - サービスが停止すると困る
- 脅威: DNSサービスの停止
  - サーバーへの多量リクエスト
  - DNSサーバーソフトウェアの脆弱性
  - ドメイン名の失効
  - オペレーションミス（DNSSEC関連など）

ケーススタディ

- ソフトウェアの脆弱性によるもの
- 運用上の理由によるもの

ケーススタディ
（ソフトウェアの脆弱性によるもの）

ケーススタディ（ソフトウェアの脆弱性によるもの）

- 実例
  - BIND 9: CVE-2013-2266（2013年3月）
  - NSD: CVE-2012-2978（2012年7月）
  - Unbound: CVE-2011-4528（2011年12月）
- 脆弱性への対処

BIND 9: CVE-2013-2266

- 細工したリクエストを送ることで、メモリを多量に消費させられる
  - 可用性に対する脅威: サーバープロセスの異常動作を引き起こしたり、停止に追い込むことが可能となる
- BIND 9のACLは効かない
  - ACL処理よりも前に問題のコードがある
- 対策はパッチの適用またはバージョンアップのみ

<http://jprs.jp/tech/security/2013-03-27-bind9-vuln-regexp.html>

BIND 9: CVE-2013-2266

- 正規表現をコンパイルするライブラリの問題を踏んだ
  - 特定のリソースレコードに含まれる正規表現の文法チェックを、コンパイルに成功するか否かで判断していた
- regcomp(3)のマニュアルに記載
  - 「バグ」節
  - `((((a{1,100}){1,100}){1,100}){1,100}){1,100}`

NSD: CVE-2012-2978

- 細工したリクエストを送ることで、プロセスを外部から異常終了させられる
  - 可用性に対する脅威
- 対策はパッチの適用またはバージョンアップのみ

<http://jprs.jp/tech/security/2012-07-20-nsd-vuln-remote-packet.html>

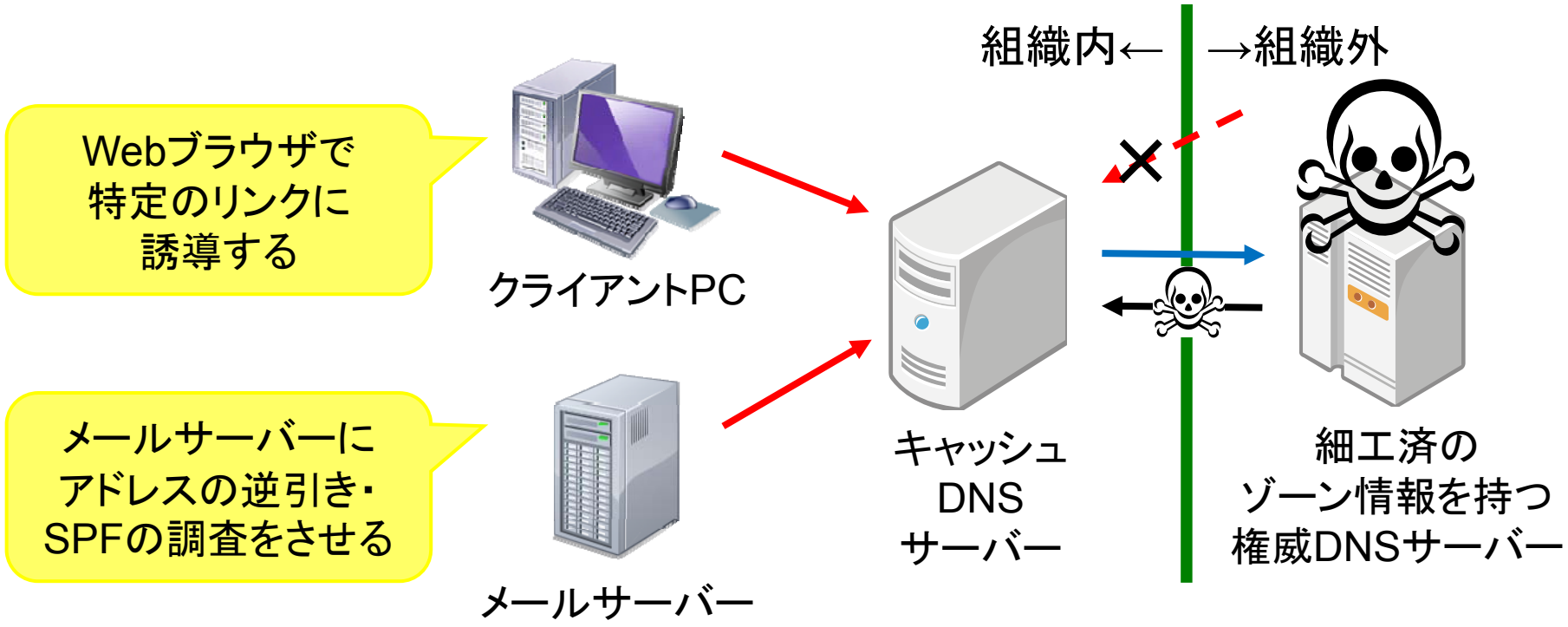
Unbound: CVE-2011-4528

- 細工したゾーンを処理させることで、プロセスを外部から異常終了させられる
  - 可用性に対する脅威
  - 細工したゾーンを公開する権威DNSサーバーを用意し、そのゾーンへのクエリを送信させることで攻撃できる
- 設定によって一時的に回避できるが、完全な解決策はパッチの適用またはバージョンアップのみ

<http://jprs.jp/tech/security/2011-12-20-unbound-vuln-multiple-redirection-signed-and-missing-nsec3.html>

アクセス元を制限していても注意が必要な例

- 組織外からDNSリクエストを送るよう仕向けることができる



脆弱性への対処

- 情報を集める
- 対策の要否を判断する
- 対策を適用する

情報を集める

- 各ベンダーのセキュリティアドバイザリ
  - 一次情報源として信頼できる
  - RSSやメーリングリストなど通知手段を利用する
- JPRSからの注意喚起
  - JANOGメーリングリスト・DNSOPSメーリングリストに注意喚起を配信している
  - Tech Webにも掲載 <http://jprs.jp/tech/>
- 各種CERT
  - JPCERT/CCのWebサイトやメーリングリスト <https://www.jpcert.or.jp/>

対策の要否を判断する

- 対策が必要か、どのくらい急ぎで対応する必要があるかを判断する
- セキュリティアドバイザリの内容や、CVSS Scoreを参考に判断する
  - 問題のある機能を利用しているか
  - すでに攻撃方法が公知になっているか

  など

対策を適用する

- 一時的な回避策（workaround）
  - 問題のある機能を設定で無効化するなどを行う
  - 存在しないこともある
  - ベンダーが公表していない（見つけていない）回避策を探すのは難しい
- 解決策（solution）
  - ほとんどの場合、開発元やベンダーから提供されたパッチの適用やバージョンアップを行うことになる

権威DNSサーバーの更新（例: JP DNSの場合）

- 変更履歴の確認
- 応答差異確認
- 性能確認
- サーバーソフトウェアのバージョンアップ

変更履歴の確認

- ChangeLog･CHANGESを確認する
- 応答内容に関わる箇所を主に確認する
- ソースコードの差分を確認する
  （diff -urコマンド）

応答差異確認

- JP DNSとして、あらかじめ考えられるパターンのクエリを網羅する
  - 社内で製作した評価ツールでパターンを生成する
- 新旧バージョンで応答内容を比較する
  - 社内で製作した評価ツールでテスト実施・比較する
  - 差異の詳細確認は人手で確認する

性能確認

- 応答性能
  - BIND 9付属のqueryperfコマンドにて、応答性能を計測する
  - JP DNSのクエリログを利用して、実環境のクエリを再現させる
  - 過去のクエリ数の傾向から決めた社内基準を満たすことを確認する
- ゾーン更新性能
  - JP DNSと同等のゾーン転送を受けるよう設定する
  - ゾーン更新にかかる時間が社内基準を満たすことを確認する

サーバーソフトウェアのバージョンアップ

- 権威DNSサーバー
  - 複数台あれば、1台が数秒程度止まっても全体としては問題なく動く
  - ルーティングやロードバランサーを利用して、サービスを止めずに行うことも可能となる
- キャッシュDNSサーバー
  - サービスの停止については権威DNSサーバーと同様である
  - 大規模なサービスでは、再起動後、サービスへの復帰前にいわゆる「キャッシュを暖める」ことも必要になる

ケーススタディ
（運用上の理由によるもの）

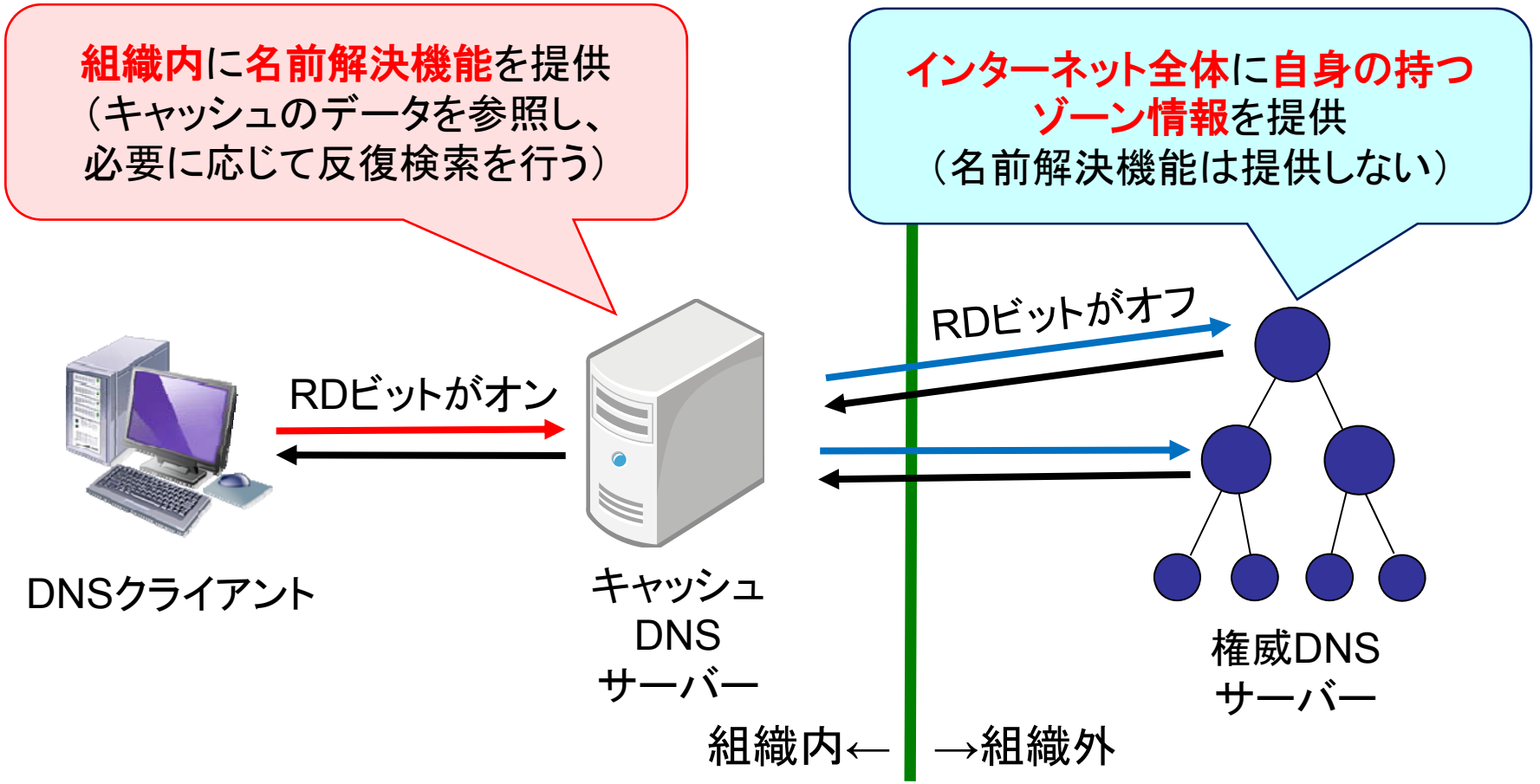
ケーススタディ（運用上の理由によるもの）

- DNSサーバーの設定によるもの
  - オープンリゾルバー
  - ソースポートランダマイゼーション
- ドメイン名の運用によるもの
  - ドメイン名の失効

オープンリゾルバー

- キャッシュDNSサーバーに対して、適切なアクセス制御がされていない状態を指す
  - 送信元を限定せず、RD（Recursion Desired）ビットがオンのリクエストに応じて、名前解決を行った結果を返してしまう
- 問題は2点
  - 可用性に対する脅威: DNS Amp攻撃の踏み台にされる恐れがある
  - 完全性に対する脅威:キャッシュポイズニング攻撃を受けやすくなる恐れがある

DNSサーバーの種類と役割



JPRS トピックス＆コラム DNSの安全性・安定性向上のためのキホン
<http://jprs.jp/related-info/guide/020.pdf>

適切な設定（権威DNSサーバー）

- RDビットがオンのリクエストに応じて、名前解決を行う必要はない
  - BCP 140の4章「Recommended Configuration」
    <https://tools.ietf.org/html/bcp140>
- キャッシュDNSサーバー機能を併せ持つDNSサーバーソフトウェア（BIND 9など）を利用している場合、設定が適切であることを確認する
  - 設定ガイド：オープンリゾルバー機能を停止するには【BIND編】

<http://jprs.jp/tech/notice/2013-04-18-fixing-bind-openresolver.html>

適切な設定（キャッシュDNSサーバー）

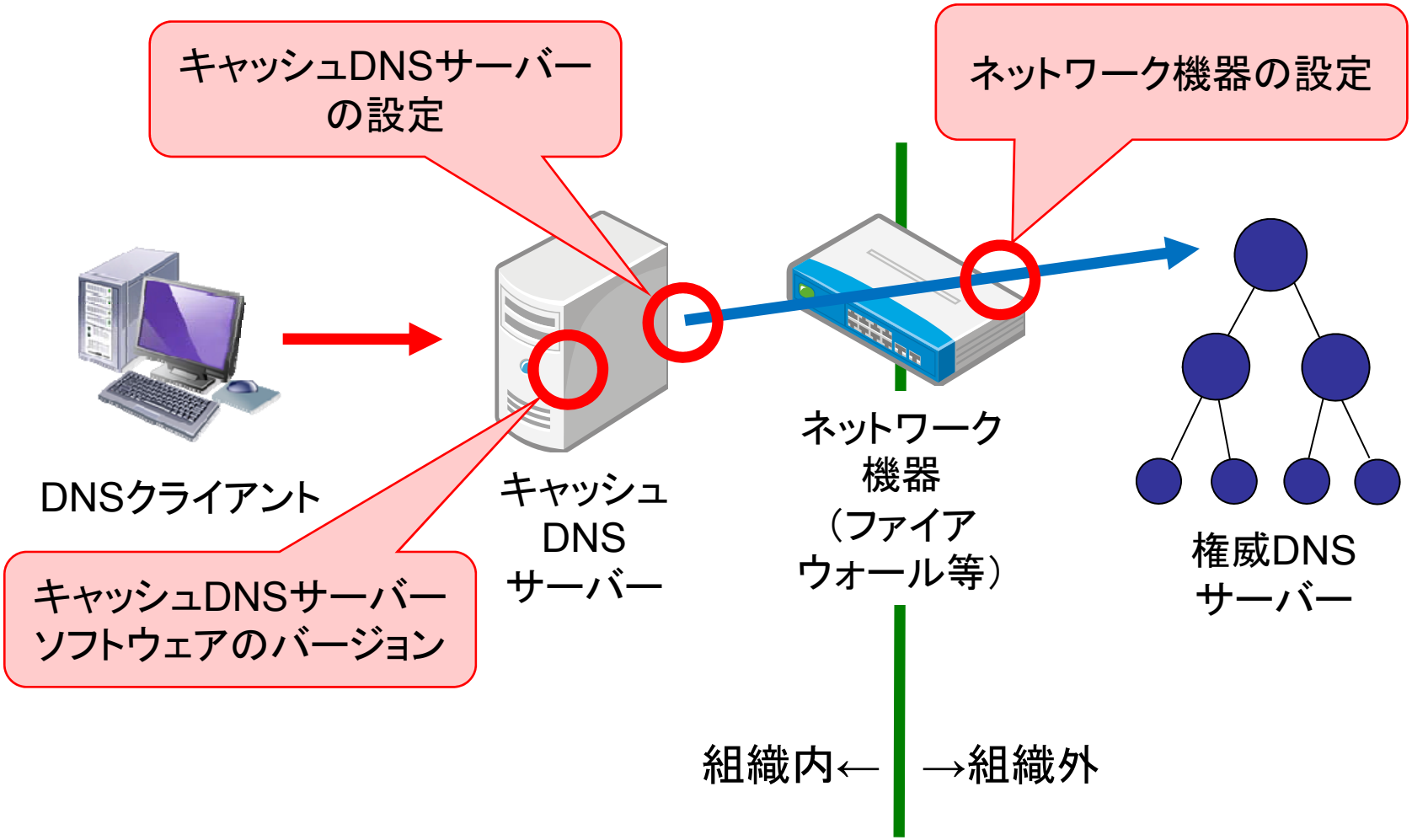
- サービス提供範囲を明確にする
  - 通常、自組織内のみをサービス提供範囲とする
  - Google Public DNSなどのパブリックDNSサービスは提供範囲を特定していないが、セキュリティ上問題を起こさないように設計・運用されている
- キャッシュDNSサーバーに、サービス提供範囲外からアクセスされないようなネットワーク設計・サーバーソフトウェアの設定が必要となる

ソースポートランダマイゼーション

- キャッシュDNSサーバーが反復検索を行う際、UDP送信元ポート番号をランダム化して、外部から推測されづらくすることを指す
- 未実施の場合、完全性に対する脅威となりうる
  - 偽の応答を注入される危険性がある
- DNS-OARCが提供しているテストで、ソースポートランダマイゼーションの実施状況を確認できる

  <https://www.dns-oarc.net/oarc/services/porttest>

確認するポイント



ドメイン名の失効

- Webサイトにアクセスすると、設定した覚えのないリンク集のようなWebサイトやレジストラのWebサイトなどが表示される
- Whois情報を確認すると、ネームサーバー情報が見覚えのないものに変更されている

ドメイン名の失効

- 利用しているドメイン名の登録更新手続きがされず、失効してしまった
  - ドメイン名が利用できない状態となり、可用性に対する脅威となる
- 影響期間はレジストラ（指定事業者）の対応によって変わる
  - ネームサーバー設定が解除された場合
  - ネームサーバーが別のサーバーに変更された場合

ネームサーバー設定が解除された場合

- ドメイン名の委任情報が削除された
- レジストリのDNSサーバーはNameError（NXDOMAIN、そのドメイン名は不在）を返す
  - NameErrorの場合、ネガティブキャッシュ（存在しないことを示すキャッシュ）として扱われる
  - ネガティブキャッシュのTTLは、レジストリのゾーンのSOAレコードに記述される

ネームサーバーが別のサーバーに変更された場合

- レジストラの用意したパーキング用のDNSサーバーなどに委任情報が変更された
- レジストリのDNSサーバーはReferral応答（委任先DNSサーバーの情報）を返す
  - 委任先DNSサーバーが正常な応答を返した場合、そのTTLの間だけキャッシュされる
  - 委任先DNSサーバーがRefused・ServFailを返した場合、レジストリのDNSサーバーが返したTTLの間だけキャッシュされる

ドメイン名を失効させないために

- ドメイン名の更新日と支払期日を確認する
- ドメイン名登録者情報としてレジストリやレジストラ・リセラーに登録したメールアドレスが有効である（メールを受け取れる）ことを確認する
  - 登録したドメイン名とは別のメールアドレス（ISPの提供するメールボックス等）を登録すると、そのドメイン名が失効した場合でも連絡を受け取れる

ドメイン名が失効した場合

- サービス停止に対する危機管理体制を構築する
- レジストラやリセラーに連絡し、復旧を依頼する
- サービス利用者に告知する
  - 他のドメイン名のWebサイト
  - ソーシャルメディア上の公式アカウント
- 失効に伴い変更されたNSレコードのキャッシュが消えるのを待つ

参考: CVSS Score

<http://nvd.nist.gov/cvss.cfm>

- 脆弱性を評価する指標の1つ
- Base Metrics: 何に対する脅威か
  - 機密性・完全性・可用性への影響の有無
- Temporal Metrics: 攻撃可能か
  - 実証コード公開の有無
  - 回避策・対応策の有無
- Environmental Metrics: 影響範囲は大きいか
  - 脆弱性による影響の大きさ
  - 脆弱性を利用して何ができるか

Q and A