2020 年 8 月 28 日

サービス＆セキュリティ株式会社 e-Gate センター

# Windows DNS サーバーの脆弱性（CVE-2020-1350 について）

## 1. 概要

DNS（Domain Name System）はインターネット上のホスト名やメールアドレスに使われるドメイン名と IP アドレスの対応を管理するシステムであり、インターネットを利用する上でなくてはならない存在です。この必要不可欠な DNS サーバーの 1 つである Windows DNS サーバーに対する脆弱性（CVE-2020-1350）を修正する更新プログラムが、Microsoft の 2020 年 7 月度の定例アップデートにおいて公開されました。脆弱性の対象は DNS サーバーとして動作している Windows Server であり、脆弱性の深刻度を示す共通脆弱性評価システム CVSS が 10 と最も高い危険度であると評価されています。

そこで今回修正された Windows DNS サーバーの脆弱性とその影響で起こり得る DNS レコードの改ざんについてご紹介いたします。

## 2. 今回の Windows DNS サーバーの脆弱性の詳細と想定される攻撃

7 月度のアップデートの対象である Windows DNS サーバーの脆弱性は RCE（リモートコード実行）の脆弱性です。脆弱な DNS サーバーに細工した DNS クエリを送信することでバッファオーバーフローが起き、攻撃者は任意のコード実行ができます。任意のコード実行により情報の窃取や改ざん、マルウェア感染などを引き起こすことができるため RCE の脆弱性は高い危険性を持ちます。これに加えて、攻撃者が脆弱な DNS サーバーを当脆弱性により乗っ取り、マルウェアを自動で拡散するなどのさらなる攻撃活動に悪用することで、複数のサーバーでのマルウェア感染が起こり得ます。このため、CVSS は最高危険度の 10 と評価されています。

外部から直接 DNS クエリを受信しない内部ネットワークの DNS サーバーでも攻撃を受ける危険があります。攻撃者はメールなどで細工した URL を送り、受信者に URL を開かせることで Internet Explorer や Microsoft Edge などのブラウザを経由し攻撃することが可能です。Windows の DNS はドメインコントローラーやファイルサーバーと同一サーバー上に併設されることが多く、内部ネットワークのそのようなサーバーが攻撃を受けると任意のコード実行により重要な情報を窃取される可能性があります。

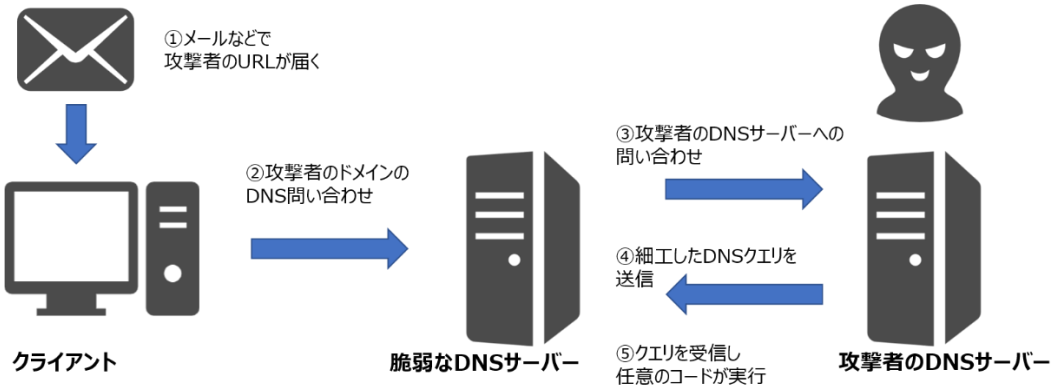


**図 1 内部ネットワークの Windows DNS サーバーへの攻撃手法**

影響を受けるシステムは DNS サーバーとして動作している Windows Server のすべてのバージョンです。前述のとおり重要な情報の窃取の危険があるため、速やかな対策が必要です。また改ざんによる被害も大きく、次項にてその影響をご説明いたします。

## 3. 脆弱性の悪用で起こり得る DNS レコードの改ざんとその影響について

一般的に任意のコード実行が行われた場合、情報の窃取や改ざんといった被害が考えられます。DNS サーバーへの任意のコード実行の攻撃が起きた場合では、ドメイン名と IP アドレスや別のドメイン名を紐づける DNS レコードの改ざんが行われる可能性があります。攻撃の一例としては、ドメイン名と IP アドレスを紐づけているレコードを改ざんすることで、利用者を攻撃者のサイトに誘導することができます。ドメイン名は変わらないため利用者は正規の web サイトにアクセスしていると思い、そこで入力されたパスワードなどの個人情報が攻撃者によって窃取されます。

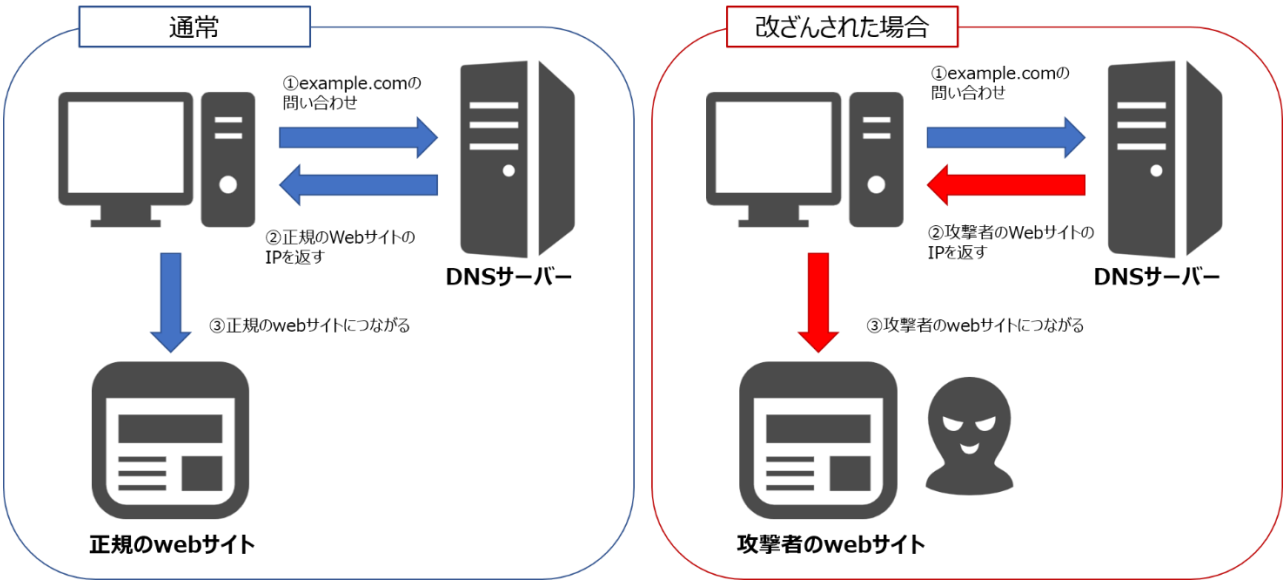


**図 2　DNS レコードの改ざん例**

今回のような脆弱性の悪用による DNS レコードの改ざんは現時点では確認されていませんが、これまでに DNS レコードの改ざんによる被害は複数報告されています。2019 年には米国国土安全保障省のサイバーセキュリティ・インフラストラクチャセキュリティ庁が米国内で行政機関のドメインの DNS 設定が改ざんされる被害が多発していることから緊急の対策を指示しました。改ざんは DNS サーバーの管理権限を不正に取得されたことで発生し、下記の表 1 のような特定の DNS レコードの改ざんが行われました。ドメイン名と IP アドレスの対応を改ざんすることによって、フィッシングサイトへ誘導する、送信先を変えてメールを盗み取るといった被害が起こり得ます。今年に入ってからでは国内で管理アカウントの不正入手によって名前解決を行うサーバーを定義する NS レコードが改ざんされる事件が起こっています。攻撃者の DNS サーバーで名前解決が行われることで、正規の IP アドレスではなく攻撃者の IP アドレスへの通信となってしまい、利用者の個人情報が窃取される被害が発生しています。

表 1 DNS レコードの改ざんの種類

| DNSレコード | 受ける被害 |
|---|---|
| Aレコード(Address) | 本来とは別のwebサイトが表示される |
| MXレコード(Mail Exchanger) | メールが盗み取られる |
| NSレコード(Name Server) | 名前解決が悪意あるDNSサーバーで行われる |

今回のような脆弱性の悪用によっては、DNS サーバーのみならずその利用者にも情報窃取の被害が及びます。DNS サーバーへの攻撃影響は利用者視点では気づくことが難しいため DNS サーバーの管理者側での対策が求められます。

## 4. 対策

**【Windows DNS サーバーの脆弱性に対しての対策】**

**・最新のアップデートを適用**

脆弱性を修正するセキュリティ更新プログラムが Microsoft より公開されています。Windows DNS サーバーへの速やかなアップデートが推奨されます。

**・Microsoft の推奨する回避策を適用**

バッファオーバーフローを引き起こさないように受信できるパケットのサイズを制限します。参考情報の「KB4569509: DNS サーバーの脆弱性に関するガイダンス CVE-2020-1350」をご参照ください。ただし、回避策を適用する場合、パケットのサイズが制限されることにより一部の名前解決ができなくなる可能性があります。

**【DNS レコードの改ざんに対しての対策】**

**・監視ツールを用いての DNS レコードの監視**

監視ツールを用いての DNS サーバーのログの監視によって DNS レコードの改ざんを検知できます。

**・DNS 設定変更には多要素認証やアクセス制限を行う**

多要素認証やアクセス制限によって管理権限への不正アクセスのリスクを低減できます。

## 5. 参考情報

**・Microsoft**

CVE-2020-1350 | Windows DNS サーバーのリモートでコードが実行される脆弱性
https://portal.msrc.microsoft.com/ja-JP/security-guidance/advisory/CVE-2020-1350

KB4569509: DNS サーバーの脆弱性に関するガイダンス CVE-2020-1350
https://support.microsoft.com/ja-jp/help/4569509/windows-dns-server-remote-code-execution-vulnerability

**・株式会社日本レジストリサービス（JPRS）**

米国国土安全保障省による DNS 設定の改ざんに関する緊急指令の公開について
https://jprs.jp/tech/security/2019-01-28-cisa-emergency-directive.html

## 6. e-Gate の監視サービスについて

e-Gate のセキュリティ機器運用監視サービスでは、24 時間 365 日、リアルタイムでセキュリティログの有人監視を行っております。サイバー攻撃への対策としてセキュリティ機器を導入する場合、それらの機器の運用監視を行い、通信が攻撃かどうかの分析、判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが重要です。e-Gate のセキュリティ監視サービスをご活用いただきますと、迅速なセキュリティインシデント対応が可能となります。

また、e-Gate の脆弱性診断サービスでは、お客様のシステムにて潜在する脆弱性を診断し、検出されたリスクへの対策をご提案させていただいております。

監視サービスや脆弱性診断サービスをご活用いただきますと、セキュリティインシデントの発生を予防、また発生時にも迅速な対処が可能なため、対策コストや被害を抑えることができます。

■総合セキュリティサービス「e-Gate」

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた「IT 運用のノウハウ」と最新のメソッドで構築した「次世代 SOC“e-Gate センター”」。この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”サービスです。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】

https://www.ssk-kan.co.jp/e-gate/



**«お問合せ先»**
サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp