IIJ DNS フィルタリング定期レポート

2023 年 1 月～2023 年 3 月

2023 年 4 月 28 日

株式会社インターネットイニシアティブ

目次

1. DNS フィルタリングによるマルウェア対策について

インターネットは電気や水道のような社会インフラになりつつあり、IoT の浸透などにより接続機器が増えトラフィック量も大幅に増加しています。その一方で、既存のアンチウイルスなどの対策が難しいルータや監視カメラなどの IoT 機器の脆弱性を悪用した大規模な DDoS 攻撃の事件も増えてきています。また、ユーザの情報搾取するようなマルウェアも数多く確認されており悪意ある行為も増加傾向にあります。

この様な背景を受けて、総務省による「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」を通じて、DNS による C&C サーバ[1]の遮断など、電気通信事業者におけるサイバー攻撃への適正な対処に関して整理がされました。また、2018 年には、電気通信事業者同士で情報共有、マルウェア感染機器の遮断やマルウェア感染の恐れのある機器に対する注意喚起を促進するために、電気通信事業法及び国立研究開発法人情報通信研究機構（NICT）法が改正されました。

IIJ は、2016 年よりセキュリティのビッグデータ解析である情報分析基盤を構築し、マルウェア感染などの悪性通信の抑止に向けて独自対策を開始しています。これは、お客様から同意を取得の上、ご契約頂いているお客様ログの多角的な分析を行い、悪性通信の遮断に向けたレピュテーションデータ[2]の生成を行っております。今回の DNS フィルタリングによるマルウェア対策の取り組みは、接続サービスなどでご利用頂いている DNS サーバに C&C サーバへの名前解決要求があった際、レピュテーションデータと当該の通信先が合致した場合に、悪性通信を遮断するものです。また、今回の取り組みでは、ご利用頂く際の DNS 及び関連する通信のログに関しても、レピュテーションデータの品質向上と生成を目的とした分析、お客様サポート及びフィルタリング実施状況報告を目的とした統計情報作成に利用致します。

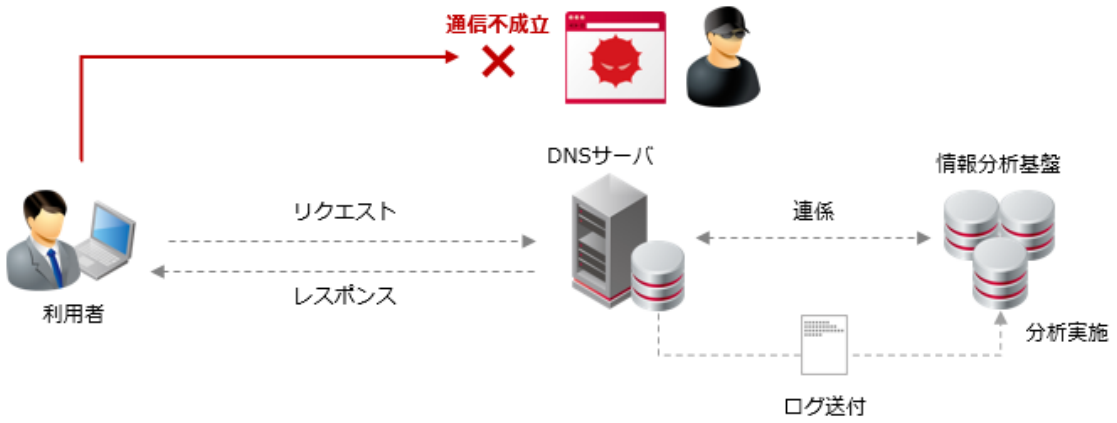
---

[1] Command & Control サーバの略で、マルウェアが感染した機器に対して、指令や制御を行うサーバ

[2] IIJ が生成する C&C サーバの宛先の情報

2. DNS フィルタリング概要

IIJ が行うマルウェア対策のための DNS フィルタリングはマルウェアに対して動作指令を中継するサーバ(C&C)サーバを対象としています。
マルウェアが攻撃者から指令を受け取るために、マルウェアはあらかじめ指定された C&C サーバとの間で通信を行います。C&C サーバとの通信の際には、マルウェアは C&C サーバのホスト名(FQDN)を DNS サーバに問い合わせ、IP アドレスを特定します。
DNS フィルタリングでは、IIJ が運用する DNS サーバがマルウェアからの問い合わせに偽の応答を返すことにより、C&C サーバとの通信を阻害します。



IIJ の DNS サーバは、問い合わせ FQDN がフィルタリング対象に該当した場合、IIJ が用意する特定のサーバの IP アドレスを応答します。
また、一覧の通信にかかるログは、IIJ の情報分析基盤に連携し、マルウェア活動状況の分析、お客様サポート、統計情報作成に利用いたします。

DNS フィルタリングが適用される IIJ サービスの一覧を表 1 に示します。
ここに示したサービスをご利用中の場合でも、所定の手続きでオプトアウト(フィルタリング不同意の意思表示)を行われた場合は、フィルタリングの適用対象外となります。

表 1. DNS フィルタリング適用範囲（2023 年 1 月 1 日～2023 年 3 月 31 日）

法人向けサービス

- インターネット接続サービス
- IIJ データセンター接続サービス
- IIJ インターネットアクセスサービス
- IIJ Omnibus サービス
- IIJ GIO インフラストラクチャーP2
- IIJ GIO コンポーネントサービス
- IIJ FiberAccess/F サービス
- IIJ FiberAccess/U サービス
- IIJ FiberAccess/Q サービス
- IIJ FiberAccess/C サービス
- IIJ DSL/F サービス
- IIJ ISDN/F サービス
- IIJ 接続アカウント管理サービス/タイプ A
- IIJ 接続アカウント管理サービス/タイプ E
- LaIT ひかりコネクト
- IIJ IPv6 FiberAccess/F サービス タイプ PPPoE
- IIJ モバイルサービス/タイプ D
- IIJ モバイルサービス/タイプ D 定額プランライト
- IIJ モバイルサービス/タイプ DS
- IIJ モバイルサービス/タイプ K
- IIJ モバイルサービス/タイプ I
- IIJ モバイル MVNO プラットフォームサービス
- IIJ モバイル M2M アクセスサービス
- IIJ マルチプロダクトコントローラサービス モバイルアクセスオプション

個人向けサービス

- IIJmio モバイルサービス
- IIJmio モバイルプラスサービス
- IIJmio eSIM サービス
- IIJmio IoT サービス
- IIJmio プリペイドパック
- Japan Travel SIM
- Japan Travel SIM for Unlocked Phone
- IIJmio ひかり
- IIJmio FiberAccess/NF
- IIJmio FiberAccess/DF
- IIJmio FiberAccess/SF
- IIJmio FiberAccess/DC
- IIJmio DSL/DF
- IIJmio DSL/SF

3. 本レポートについて

本レポートの対象とする期間は、以下の通りです。

2023 年 1 月 1 日 ～ 2023 年 3 月 31 日

4. DNS フィルタリング対象マルウェア

期間中に DNS フィルタリングの対象としたマルウェアを示します。(表 2)

フィルタリング対象とするマルウェアについては以下の手順で判断を行っています。

- 弊社の観測および協力機関から情報を入手
- 入手した情報を元に検体（マルウェア）を取得
- 弊社セキュリティアナリストが検体を解析し、その挙動、および通信先を確認
- 以下の条件に合致するマルウェアについてフィルタリング対象と判定
  - マルウェアの挙動がインターネットやお客様に被害をもたらすこと
  - 弊社の観測により現にそのマルウェアが活動していることを確認できたこと

弊社の観測によりマルウェアの活動が収束したことが確認できた場合、フィルタリング対象から除外いたします。

図 1

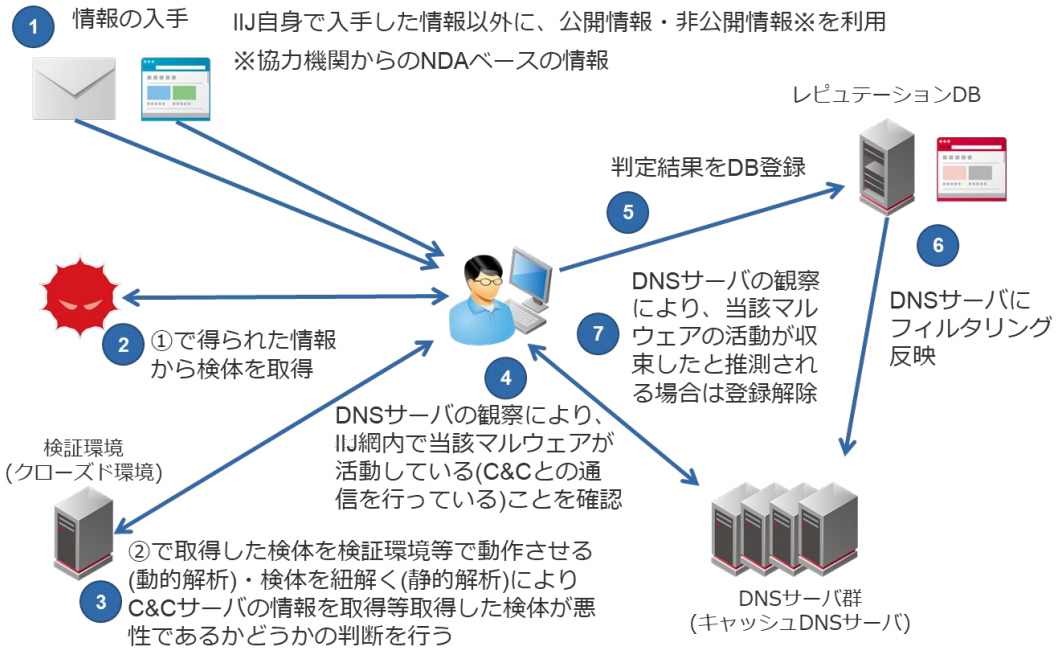


表 2 フィルタリング対象のマルウェア

識別子	FQDN 数	挙動	フィルタリング開始日	フィルタリング終了日
IIJ-20190701-0003	1	感染端末からの情報窃取・送信	2019/07/01	
IIJ-20190709-0001	1	バックドアの設置	2019/07/09	
IIJ-20190920-0001	1	感染端末からの情報窃取・送信	2019/09/20	
IIJ-20200114-0001	3	感染端末からの情報窃取・送信	2020/01/14	
IIJ-20200221-0001	1	感染端末からの情報窃取・送信	2020/02/21	
IIJ-20200311-0001	2	感染端末からの情報窃取・送信	2020/03/10	
IIJ-20200515-0001	1	感染端末からの情報窃取・送信	2020/05/15	
IIJ-20200515-0002	2	感染端末からの情報窃取・送信	2020/05/15	
IIJ-20210317-0001	3	感染端末からの情報窃取・送信	2021/03/17	
IIJ-20210602-0001	1	感染端末からの情報窃取・送信	2021/06/02	
IIJ-20210623-0001	1	感染端末からの情報窃取・送信	2021/06/23	
IIJ-20210903-0001	2	感染端末からの情報窃取・送信	2021/09/06	
IIJ-20210930-0001	1	感染端末からの情報窃取・送信	2021/09/30	
IIJ-20211006-0001	1	感染端末からの情報窃取・送信	2021/10/08	
IIJ-20211108-0001	1	感染端末からの情報窃取・送信	2021/11/09	
IIJ-20211108-0002	1	感染端末からの情報窃取・送信	2021/11/09	
IIJ-20211108-0003	1	感染端末からの情報窃取・送信	2021/11/09	
IIJ-20211129-0001	1	感染端末からの情報窃取・送信	2021/11/30	
IIJ-20211129-0002	1	感染端末からの情報窃取・送信	2021/11/30	
IIJ-20211202-0001	1	感染端末からの情報窃取・送信	2021/12/02	
IIJ-20220306-0001	3	大量通信(DDoS)	2022/03/06	
IIJ-20220328-0001	1	感染端末からの情報窃取・送信	2022/03/28	
IIJ-20220401-0001	2	感染端末からの情報窃取・送信	2022/04/01	
IIJ-20220412-0001	3	感染端末からの情報窃取・送信	2022/04/12	
IIJ-20220512-0001	2	感染端末からの情報窃取・送信	2022/05/12	
IIJ-20220704-0001	1	感染端末からの情報窃取・送信	2022/07/04	
IIJ-20220727-0001	2	感染端末からの情報窃取・送信	2022/07/27	

IIJ-20220825-0001	1	感染端末からの情報窃取・送信	2022/08/25	
IIJ-20220922-0001	2	感染端末からの情報窃取・送信	2022/09/22	
IIJ-20221004-0001	1	感染端末からの情報窃取・送信	2022/10/04	
IIJ-20221216-0001	2	感染端末からの情報窃取・送信	2022/12/16	
IIJ-20221227-0001	1	感染端末からの情報窃取・送信	2022/12/27	
IIJ-20230302-0001	1	感染端末からの情報窃取・送信	2023/03/02	
IIJ-20230303-0001	1	感染端末からの情報窃取・送信	2023/03/03	

凡例

- 識別名 … 当該マルウェアを識別するための名称です。公知の名称がないマルウェアの場合、弊社が独自に与えた識別名を記載します。
- 対象 FQDN の数 … 当該マルウェアの C&C サーバと特定され、フィルタ対象となった FQDN の数です。当該マルウェアが利用するすべての C&C サーバを網羅していないことがあります。
- 挙動 … 当該マルウェアをフィルタ対象とする判断に至った挙動です。当該マルウェアのすべての挙動を網羅しているものではありません。
- フィルタイリング開始日・終了日 … フィルタリングを開始した日、または、マルウェアの活動が収束したと判断し、フィルタリング対象から除外した日です。

5. DNS フィルタリング適用状況

期間中に影響を受けた DNS クエリの割合を示します。(表 3)

影響を受けたクエリの割合は以下の手順で算出しています

- フィルタ対象 DNS クエリ数 / 全 DNS クエリ数 = 影響を受けたクエリの割合
- フィルタ対象 DNS クエリ数 … フィルタ対象の FQDN を問い合わせた DNS クエリ数
- 全 DNS クエリ数 …IIJ の DNS サーバが処理した DNS の全クエリ数（オプトアウト分を除く）

表 3. DNS フィルタリングの適用状況

対象期間	影響を受けたクエリの割合
2023 年 1 月	0.000558551203614%
2023 年 2 月	0.000625722144112%
2023 年 3 月	0.001101286830301%

6. 期間中の DNS フィルタリングの運用状況について

IIJ では 2023 年 1 月から 3 月にかけて、協力機関から提供された情報、および IIJ が運用するインフラからご契約者のご承諾の元に取得した情報をもとにマルウェアの活動状況を調査し、検体の入手、分析を行いました。期間中に 2 件（IIJ-20230302-0001、IIJ20230303-0001）のマルウェアについて新たにフィルタリング対象として登録しています。

前回と同様に 2020 年 3 月から IIJ 網内で活動していると推測されるマルウェアについて、関連する FQDN へのクエリは継続して発生しておりました。また、2021 年 11 月に登録したマルウェアの宛先通信が 2023 年 2 月以降急増しており、該当マルウェアの再活動の兆しがあるものと考えています。これらの FQDN へのクエリは対象期間中に継続的に観測され、当該マルウェアは活動の兆しがあるものと考えています。

IIJ では今後も引き続きマルウェアの分析を行い、必要最小限の範囲でフィルタリングを実施いたします。

7.　お問い合わせ先

本レポートについてのお問い合わせは以下の窓口までご連絡ください。

IIJ DNS フィルタリングお問い合わせ窓口
E-Mail: request-security@iij.ad.jp
受付時間：9:30-17:30（土・日・祝日を除く）
（※）原則メールでの対応とさせていただきます。

IIJ DNS フィルタリング定期レポートは以下の URL に掲載いたします。
https://www.iij.ad.jp/sec-statement/

尚、DNS フィルタリングのオプトアウト(不同意の意思表示)を希望される場合は、ご契約中サービスよりご案内する手続きをお取り下さい。

・IIJ サービス全般：IIJ サービスオンライン　トップページ 「関連リンク　DNS フィルタリング」
・IIJ GIO コンポーネントサービス：IIJ GIO サポート Web 「お知らせ」
・LaIT：LaIT サポートセンター