2013 年 6 月 10 日

国際ロータリー第 2830 地区

WEBサイト不正改ざんの概要及びサーバー復旧のご報告

2012-13 年度 第 2830 地区ガバナー 松本康子
同サイト管理者

5 月 31 日未明、第 2830 地区及び県内各クラブが使用（用途：WEB サイト公開等）しているレンタルサーバー＜rotary-aomori.org＞に何者かが不正に侵入し、データの改ざん（不正プログラムの混入）を行ったことが判明しました。

この結果、検索サービス最大手のGoogleに「不正なプログラムを用いている違法サイト」と判断され、2003 年以降の第 2830 地区及び県内各クラブのWEBサイトの全てがGoogleの検索結果からは閲覧できない状態となりました。また、その悪意ある第三者により、短期間ながら当地区及び県内各クラブの WEB サイトがコンピュータウィルスの拡散に利用された可能性があります。

つきましては、WEB 運営担当者は勿論のこと、過去に当地区もしくはいずれかの県内クラブの WEB サイトを閲覧した方は、**早急にご使用のパソコンにセキュリティ対策ソフトを導入し、感染の確認並びに駆除を行って下さい**。加えて、パソコン内のあらゆるソフトウェアを最新の状態にアップデートし、脆弱性を最小限に抑えることも重要です。

一方で、当地区及び県内各クラブの WEB サイトの閲覧履歴が無い場合でも、セキュリティ対策を施していないパソコンでネット接続をされている場合は、既に他のサイトで感染している可能性が多分にあります。一部報道にありましたように、現在、当地区同様の WEB サイト不正改ざんの被害が国内で急増しており、それに伴いインターネット閲覧時の危険性は急激に高まっております。会員の皆様には例外なく、セキュリティ対策の実施を強く推奨致します。

今回の被害状況、対応の経緯、原因等を以下に記します。

被害状況

◆不正アクセス対象＝23 団体　◆「改ざん＋感染」データ件数＝（842 件）

※（ ）内は団体ごとの被害データ件数

第 2830 地区：2003 年度（186）/2004（30）/2005（82）/2007（5）/2008（55）/2009（16）/2010（32）/2011（10）/2012（28）/2013（20）

五所川原RC（30）/五所川原中央（142）/八戸北（59）/弘前（35）/弘前西（4）/金木（6）/七戸（4）/東北（6）/十和田東（7）/鶴田（2）/六ヶ所（8）

2005 年度ガバナーエレクト事務所（54）/青少年育成委員会（21）

原　　因

特定は困難ですが、被害状況などから総合的に判断するに、ロータリー関係者の過失による情報漏洩が原因と思われます。

この際の関係者とは、第 2830 地区がサーバーを開設した 2003 年以降、当地区及び県内各クラブの WEB サイトの制作、更新、運営に携わった方々のことです。今回のデータ改ざんは非合法な行為であり、不正なアクセスではありますが、そのアクセスには正規のIDとパスワードが用いられた可能性が高いです。つまり、ある関係者のパソコンがウィルス等に感染し、サーバーへアクセスする際に使用する「FTP情報（サーバー名、ID、パスワード）」が漏洩、奪取されたものと思われます。

加えて、ひとつのサーバーに複数の WEB サイトのデータを格納し、10 年間もの長期に渡り不特定多数の方が同一のパスワードを用いてきた運営手法も被害拡大の一因になったと推測されます。

発生から解決までの対応経緯

① 5 月 31 日以降、Googleの検索結果において、当地区のWEBサイトが違法であると表示される
② 調査した結果、サーバー内のデータに不正な改ざんの痕跡を確認
② 侵入者を排除すべく、サーバーに関連するパスワードを全て（全 53 アカウント）変更
③ サーバー内に格納されている全てのファイル（550 フォルダ/8,277 ファイル）を見直し、
感染ファイル、改ざんされたプログラムを特定
④ 感染ファイルを駆除、改ざんされたプログラムを修正した後、再度サーバーへアップロード
⑤ サーバー内のデータを正常にした旨Googleに報告し再審査を申請、
違法サイトの認定を取り消すよう要求
⑥ 6 月 9 日正午、Googleの再審査が完了し、「健全なサイト」に評価が改められた

現在、データ復旧を完了し、サーバー内のデータは正常に稼働しております。不正アクセスへの対策も講じました。以上、会員の皆様にご報告申し上げます。

― 各クラブのWEB運営担当者様へ ―

- 上述のように、ＷＥＢサイトの制作・更新にお使いのＦＴＰパスワードを勝手ながら変更させていただきました。新しいパスワードを別紙にてご案内いたしますので、今後の作業にはそちらをご使用ください。

- 可能な限りファイルの修復を致しましたが、一部、隔離もままならず削除することでしか対応できない感染ファイルがございました。事態は急を要しており、修復不可能なファイルはさらなる事態悪化の要因ともなりかねないと判断し、サーバー内より抹消しました。何卒ご了承ください。

- 被害状況の詳細として、不正改ざん並びに感染の被害にあったファイルリストを別途公開致します。それをご確認の上、必要があればサイトを再構築してください。

- 当方ではセキュリティ上問題のあるファイルのみ修正を施しました。従って、セキュリティ上問題はなくとも、不正アクセスによる影響が残存している可能性があります。

- 今回の件とは関連がなく、以前より正常に機能していなかったと思しきサイトも散見されました。各クラブのＷＥＢ運営担当者様ご自身で、ブラウザでの閲覧に支障が無いことを確認し、ディレクトリ内のデータも一度精査して下されば幸いです。

- 一部クラブで、サイト上で公開しないファイルを大量にＷＥＢサーバーへ格納し、ファイルサーバー（保管庫）として使用しているケースがあるようです。レンタルサーバーはガバナー事務所をはじめ県内各クラブで共用しており、その容量にも上限があります。データサイズの縮小にご協力下さい。また同様の理由から、同一ファイルを複数のフォルダに重複して格納するのもお控えください。

- ファイル名のルールを守って下さい。サーバー内に格納するファイル名は英数字と許可された一部の記号で構成されなければなりません。漢字、ひらがな、カタカナ等はサーバー内では認識されず、閲覧に不具合が生じるばかりか、サーバー内のメンテナンス性が著しく損なわれます。

- 同一のフォルダ階層において、ファイル名の重複は禁止されています。早々に解決してくださることが望ましいです。

情報セキュリティ徹底のお願い

新たに配布したパスワードが再度漏洩したり、サーバーアクセス時に再度ウィルスが混入したりしてしまっては元の木阿弥です。情報管理に無頓着な関係者が１人でもいれば、明日にでも今回と同様の事態が再発してしまいます。新しいパスワードを用いてサーバーへアクセスする前に、ご自身のパソコンのウィルス感染を疑ってください。ＷＥＢサイトの制作・更新作業には十分なセキュリティ対策を施した端末を使用し、安全なネットワーク環境下でサーバーとの通信を行って下さいますよう深くお願い申し上げます。