

ご担当者の中で、ご閲覧ください。

皆様が気になる「お役立ち情報」をお届けします！

回 覧						
--------	--	--	--	--	--	--

# マルトヨ newsletter

2015  
2 月号

VOL.

046

## 編集担当者からひとこと

こんにちは、(株)マルトヨの佐藤です。年末年始の休暇を利用して、東北を旅して来ました。なかでも岩手県陸前高田市の「奇跡の一本松」は感慨深いものがありました。あの震災からもう4年経つのですね。お正月という事で売店にて豚汁が振舞われていたのですが、震災直後にこうして炊き出しが配られ、被災者が口にしていたかと思うと、自然とこみ上げてくるものがありました。瓦礫は殆ど撤去されていましたが、復興と言うには程遠い気がします。今の自分に何が出来るのか、色々な意味で考えさせられた旅でした。



編集担当：佐藤

## NEWS

### 01 3週間で50万件超の不正ログイン、「リスト型攻撃」が止まらない

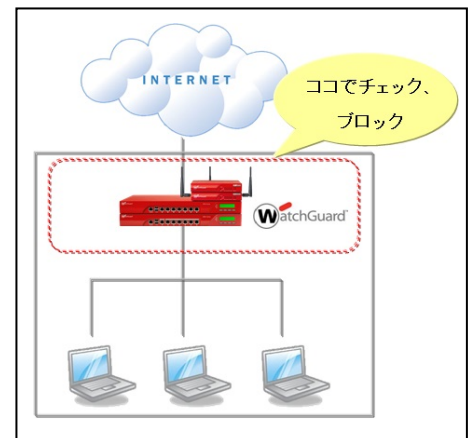
2014年6月以降、日本のネットサービスを狙った不正アクセス事件が相次いで発生しています(表)。攻撃の手口は「リスト型アカウントハッキング(リスト型攻撃)」である点が共通していることが挙げられます。

表●不正アクセスを受けた企業の例(2014年6月発表)

企業名	試行回数	不正ログイン数
LINE	非公表	303
ダウンゴ	約 335 万	約 29 万 5000
ミクシィ	約 450 万	約 26 万
サイバーエージェント	約 230 万	3 万 8280
はてな	約 160 万	2398

リスト型攻撃については、2014年10月号(VOL.42)で少し触れさせて頂きましたが、他人のID・パスワードでログインをして不正にポイントを使用したり、場合によっては不正送金を行い、本人の知らない間に被害にあっているというものです。昨年6月頃の3週間ほどで、ダウンゴ(ニコニコ動画)とミクシィに対するログイン試行回数は延べ800万件弱、そのうち実際にログインされた件数は合計50万を超え、VOL.42でもお伝えしたように「パスワードの使い回しをやめる」と

いった対策が必要です。しかしながら、90%近い人がパスワードを「使いまわしている」現状では、簡単に防げるものではありません。そこでひとつの方法として浮上するのが「Unified Threat Management(以下UTM)」です。これは簡単に言うと、インターネット上からの不正なアクセスに対し、パソコンに入ってくる前にゲートウェイでブロックをしようという物です。つまり、通常通りに使用していても気付かない間にアクセスされる脅威(ウイルス、不正アクセス、不正プログラム、迷惑メール)を事前に検知し社内への侵入を防ぐという事です。通常のウイルス対策ソフトとの大きな違いは、ウイルスがパソコンに侵入した時点で警告を出すのか、侵入する前段階で警告を出すのかという違いで、その差は非常に大きなものです。外部から持ち込まれる脅威(USBなど)への対策はウイルス対策ソフトに依存しますので、両方が必要という事になります。今後増加が予測される脅威(例えば情報漏洩)に対して企業としてコンプライアンスの要請が各方面からあろうかと想像されます。既に大企業だけの話ではなく中小零細企業が標的となっています。今から対策を施しましょう!



お客様の満足と喜びを  
私たちのよろこびとします!



発行:株式会社 マルトヨ

〒444-0008  
愛知県岡崎市洞町字宮ノ腰2-1

URL: <http://www.marutoyo.info>

マルトヨ

検索

TEL:0564-24-9138 FAX:0564-25-1391

