

報道関係者各位
(参考資料)

2013年11月18日
株式会社インターネットイニシアティブ

IIJ、インターネットの最新の技術動向・セキュリティ情報のレポート **「Internet Infrastructure Review」Vol.21 を発行**

株式会社インターネットイニシアティブ(IIJ、本社:東京都千代田区、代表取締役社長:勝 栄二郎、コード番号:3774 東証第一部)は、インターネットの基盤技術に関する最新動向や、セキュリティ情報を紹介する技術レポート「Internet Infrastructure Review (IIR)」の Vol.21 を本日発行いたしました。

今号では2013年7月から9月までの3ヵ月間に発生したインシデントと期間中に発生したセキュリティ関連の着目すべき事象について解説をしています。さらにオープンリゾルバ問題、SDN の最新動向と関連製品「OmniSphere」について取り上げます。

今号のトピックは以下のとおりです。

◆期間内のインシデント動向

- DNS Open Resolver の探査や、それを悪用した DDoS 攻撃を確認。
- 歴史的日付に関連したサイバー攻撃が予測されたが、被害は小規模に留まる。

◆インシデント対策の調査研究

- 「PlugX」は標的型攻撃に利用される RAT 型(Remote Administration Tool。インストールされたホストを遠隔から操作する。)のマルウェア。IIJ では解析を行い、PlugX の特徴に着目し、それに基づく検出手法と対策を提案。
- 特定の組織に対して継続して行われた標的型メール攻撃の実例と、実施された対応を紹介。
- P2P ネットワークと暗号技術を用いて、利用者の匿名性を確保しながら、商取引を可能にする仮想通貨「Bitcoin」について解説。

◆DNS オープンリゾルバ問題

- 外部からの不要なアクセスを制限していないキャッシュ DNS サーバ(オープンリゾルバ)が、大規模な DDoS 攻撃の踏み台として悪用されるケースが頻発している。
- オープンリゾルバ問題の有効な対策例は以下のとおり。
 - キャッシュ DNS サーバに適切なアクセス制限を設定。
 - ルータに詐称パケットの通過不許可を設定。

◆SDN と OmniSphere

- 株式会社ストラトスフィアの製品「OmniSphere」は、人事異動やレイアウト変更で発生するオフィスの有

線・無線 LAN 環境の再設定を自動化できる、SDN を活用したソリューション。

- OmniSphere は、スイッチ側はフリーで利用できる、OpenWrt や trema-edge などの実装を採用。
一方、コントローラ側には分散コンピューティング処理に適した Apache Zookeeper を採用。

以下のサイトで IIR の全文をご覧ください。

<http://www.ij.ad.jp/company/development/report/iir/index.html>

【IIR について】

「Internet Infrastructure Review」は、インターネットが抱える技術的課題についての認識を、関連する多くの機関やお客様と共有することで、インターネットが安心、安全な社会基盤として発展する一助となることを目指し、2008年10月より季刊で年4回発行している技術レポートです。IJ がインシデント観測の仕組みで収集した各種攻撃の傾向と対策に関する情報や、インターネットバックボーンの運用を通して蓄積した技術的知見を掲載しています。

報道関係お問い合わせ先

株式会社インターネットイニシアティブ 広報部 小河、村松

TEL: 03-5259-6310 FAX: 03-5259-6311

E-mail: press@ij.ad.jp URL: <http://www.ij.ad.jp/>