

韓国サイバーテロ、中央管理サーバが悪意のあるコードを配布か

[管理人]

Tweet



2013年3月20日 20:01 | [コメント\(49\)](#)

登録タグ: [サイバーテロ](#) [セキュリティ](#) [脆弱性](#)

[記事をクリップ](#)

韓国のニュースサイト「イ・デイリー」は20日、韓国で発生した大規模なサイバーテロの原因について、不具合修正やセキュリティ更新を行う「パッチ管理サーバ」を介して悪意のあるコードが流布された可能性があると報じている。

このサイバーテロは、韓国放送局大手「KBS」「MBC」、ニュース専門チャンネル「YTN」や新韓銀行などの銀行2行、保険会社2社のコンピュータネットワークが狙われ、麻痺した問題。

この問題を追跡している官・民・軍のサイバー脅威合同対応チームは同日、悪意のあるコードを簡易解析した結果、パッチの更新管理サーバを経由して流布されたとの見解を示している。悪意のあるコードは、コンピュータのブート領域を破壊する非常に悪質性の高いもの。現在も詳細な分析を進めており、原因の究明を急いでいる。

サイバー脅威合同対応チームは、北朝鮮が地下核実験を行った直後である先月12日に「サイバー危機評価会議」を開き、警戒レベルを5段階中、下から2段階の「関心」に引き上げたばかり。ハッキングやDDoS攻撃に備えていたとされているが、（推定段階であるものの）今回はパッチサーバを経由して狙われた可能性がある。