2011 年 12 月 5 日

FortiGate 販売代理店 各位

フォーティネットジャパン株式会社

FortiOSv3.0 向け IPS シグネチャ・アップデートによる CPU 負荷高騰障害の報告

拝啓　貴社益々ご清祥のこととお喜び申し上げます。平素は格別のご高配を賜り、厚くお礼申し上げます。 この度は弊社機器障害により、みなさまに大変なご迷惑をおかけしたことをお詫び申し上げます。
障害内容および対応につきまして下記のとおりご報告致します。

記

1. 障害対象機器

FortiOSVer3.0 が動作する FortiGate 全モデル
(IPS エンジン Ver1.129 を搭載する IPS シグネチャ・アップデート・サービス利用機器)

2.障害経緯

FortiOSVer3.0 を搭載した FortiGate にて FortiGuard IPS シグネチャー Ver3.115 へのアップデートを行った後､FortiGate 内の IPS エンジンによるシグネチャ更新処理が本体 CPU 負荷を高騰させ FortiGate を通過する通信に対し大幅な遅延障害を発生させました。
今回の障害は、次のような経緯で推移いたしました。

- **2011 年 12 月 1 日 AM5:00（日本時間）**
  IPS シグネチャ・パッケージ Ver3.115 を FDS（FortiGuard Distribution Service） を通じ提供開始しました。

- **2011 年 12 月 1 日 AM7:00（日本時間）**
  FortiOSVer3.0 をご利用中のユーザ様より IPS シグネチャ（Ver3.115）へのアップデート後に CPU 負荷高騰による通信遅延障害が発生しているとのご報告を複数いただきました。
  同時に弊社 FDS 運用部門にて IPS シグネチャ・アップデート後 FortiOS Ver3.0 を搭載した FortiGate の CPU 使用率が高騰したままになる事象を確認し FDS からの FortiOSVer3.0 向け IPS シグネチャ Ver3.115 の配布を停止しました。

- **2011 年 12 月 1 日 AM8:00（日本時間）**
  FortiGuard ラボの IPS シグネチャ開発部門での事象分析により、緊急対応として稼働実績のある IPS シグネチャを新規 IPS シグネチャ･パケージ Ver3.116 として再配布することを決定しました。その後、シグネチャ・アップデートの有効性、および動作の正常性確認を開始いたしました。

- **2011 年 12 月 1 日 AM9:00(日本時間)**
  FortiOSVer3.0 向け IPS シグネチャ Ver3.116 を緊急対応として FDS 経由にて配布開始しました。

フォーティネットジャパン株式会社
〒106-0032 東京都港区六本木 7-18-18　住友不動産六本木通ビル 8 階

1. 障害原因

今回の事象は、FortiOS Ver3.0 向けに提供をしているIPSエンジンVer1.129 における、シグネチャ更新処理の不具合が原因と判明いたしました。

IPSシグネチャ・アップデート処理ではFortiGate内のデータベースを更新する際、IPSエンジンによりFortiGate内のIPSシグネチャ・データベースと新規IPSシグネチャ・パッケージによる最適化処理を実行しています。 この、IPSエンジンによる最適化処理において新規IPSシグネチャ・パッケージとIPSシグネチャ・データベースの差分情報が特定の組み合わせになっていた場合、メモリー破壊を発生し、システム全体に対し過剰な負荷をかけ続けてしまう問題が内在していました。

IPSエンジンVer1.129 の過去2年間の稼働実績で同様の問題点が発見されておらず、IPSシグネチャ更新前のFortiGateの稼働状況よってIPSシグネチャ・データベースの状態が異なるため、シグネチャ・パッケージ配布前の検査において、CPU負荷高騰の事象を検出することができず、原因追究に時間を要してしまいました。

なお、FortiOSVer4.0以降は、最適化処理方式を変更したIPSエンジンを提供しているため同様の事象は発生していません。

2. 今後の対応

今回の障害に対する直接対応は次の項目です。

- 新規 IPS シグネチャ・パッケージと FortiGate 内のシグネチャ・データベースの特定の差分情報が契機になる問題であるため、IPS シグネチャ開発部門にて、新規 IPS シグネチャ・パッケージを作成する際、不具合発生を回避するパッケージ構成になるよう、作成手順を変更しました。

- IPS エンジン Ver1.129 に内在するデータベース更新処理の問題であるため、FortiOS3.0 向けの IPS エンジンのアップデートを検討中です。

この度は弊社サービスの不具合によりお客様に大変なご迷惑をおかけし、誠に申し訳ございません。
重ねてお詫び申し上げます。

以上

フォーティネットジャパン株式会社
〒106-0032 東京都港区六本木 7-18-18　住友不動産六本木通ビル 8 階