

量による攻撃(=DoS攻撃)とは、

DoS(Denial of Service)攻撃とは、サーバの脆弱性を突く攻撃とは違い、ターゲットに対して正常なアクセスを大量に送りつけることでサーバのリソースを消費させて、正規ユーザのアクセスを処理しきれない状態を発生させる攻撃のことです。

<DoS攻撃手法の主な例>

- ・大量のTCP接続要求を送りつける「synflood攻撃」
- ・Webサーバに対して更新ボタンを連打することで大量の接続要求を行う「F5攻撃」
- ・攻撃目的のサーバのNICに対してそのNICを送信元とする大量のTCP接続要求を行う「Land攻撃」

最近では、ボットネットを使ったDDoS攻撃も頻繁に発生しています。

有効な事前対策が無い！！

量による攻撃(DoS攻撃)は正常なアクセスとの見分けがつけにくい。例えば、「F5攻撃」は正常なアクセスを連続して大量に行うだけの攻撃であり、1アクセス単位では正規利用者のアクセスと全く同じである。

つまり、量による攻撃(DoS攻撃)に対しては、ファイアウォールによるアクセスコントロールやIPS/WAFによる不正アクセス遮断といった対策が有効ではない。(攻撃と判断できないため)

⇒ファイアウォールログからアクセス数に着目し、量の変化をリアルタイムに監視することで、早期発見を行うことが唯一有効な対策と言える。

解決案

- ・量による攻撃(DoS攻撃)により、レスポンス低下など業務に影響が出ることを懸念
- ・量を監視する仕組みが必要

- ・ファイアウォールログをリアルタイムに監視
- ・閾値評価によるアクセス数(量)の監視

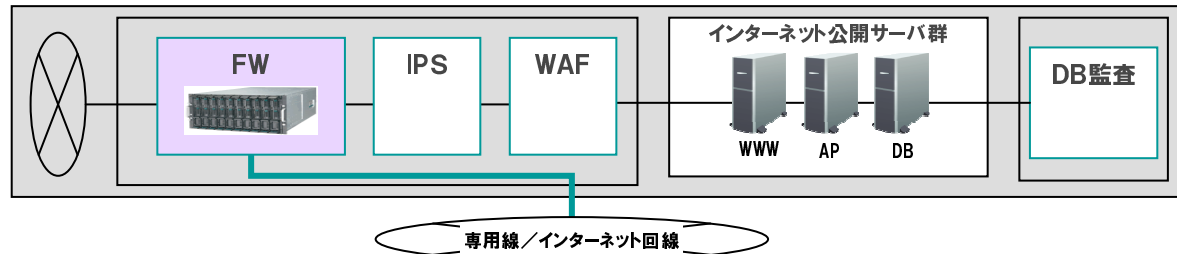
効果として・・・

- ・量による不正アクセスを早期発見
- ・アクセス数の状況を即時把握可能

FW監視サービス

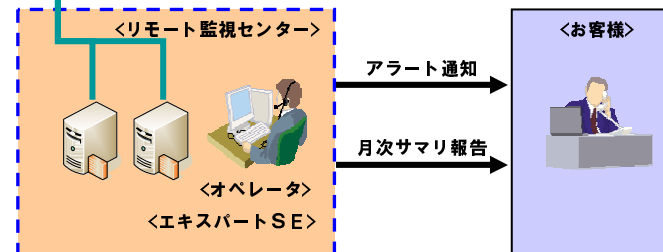
通常のFW設置運用に加え、リアルタイムでFWログをモニタリング

独自プログラム分析により、アクセスの集中傾向をいち早く検知します



<サービス内容>

- リアルタイム監視・通報
 - ⇒事前に設定した閾値によるアラート監視
 - ⇒アラート通報(第一報、サマリ解析結果の第二報)
- 定期報告
 - ⇒前月分ログのサマリ解析結果を報告書提出



【お問い合わせ先】 株式会社 富士通九州システムズ (FJQS)

東京オフィス 〒144-0035 東京都大田区南蒲田2-16-2 テクノポート三井生命ビル9F

Tel. 03-5703-7028 Fax. 03-5703-7050 (担当:セキュリティセンター)

大分事業所 〒870-8551 大分県大分市東春日町17-58 (ソフトパーク内)

Tel. 097-534-8119 Fax. 097-535-1064

2009. 6