FORTINET™

REAL TIME NETWORK PROTECTION

ゲートウェイウイルス対策の マルチベンダー化のご提案

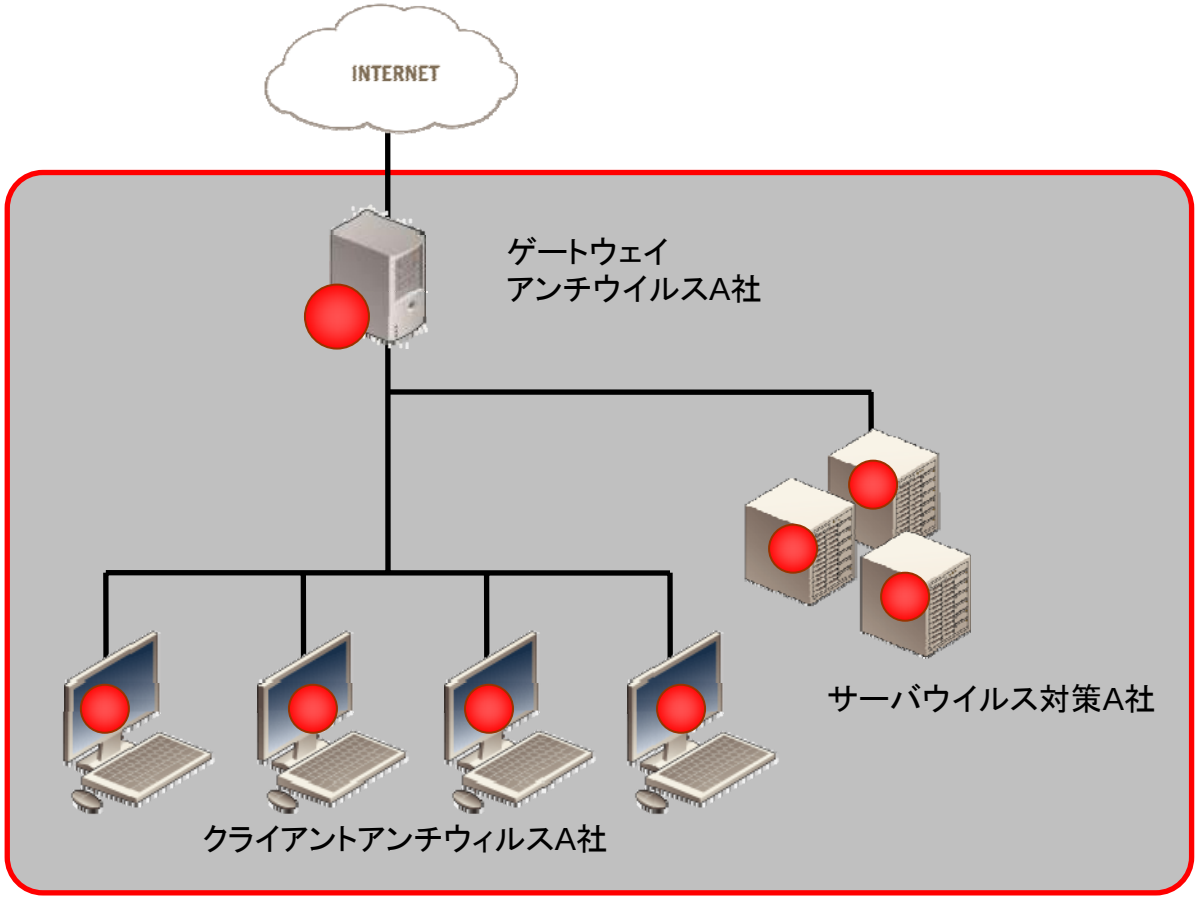
フォーティネットジャパン株式会社

インターネット経由のウイルスは驚異的なスピードで侵入

メールからの侵入	一台の感染マシンから数千通から数万通のウイルスメールを送信する場合も・・・
脆弱性を利用した侵入	Webサーバからクライアントまでユーザの操作無しで感染、中にはWebを見るだけで感染する場合も・・・
感染マシンからの攻撃	感染マシンが攻撃の踏み台に・・・

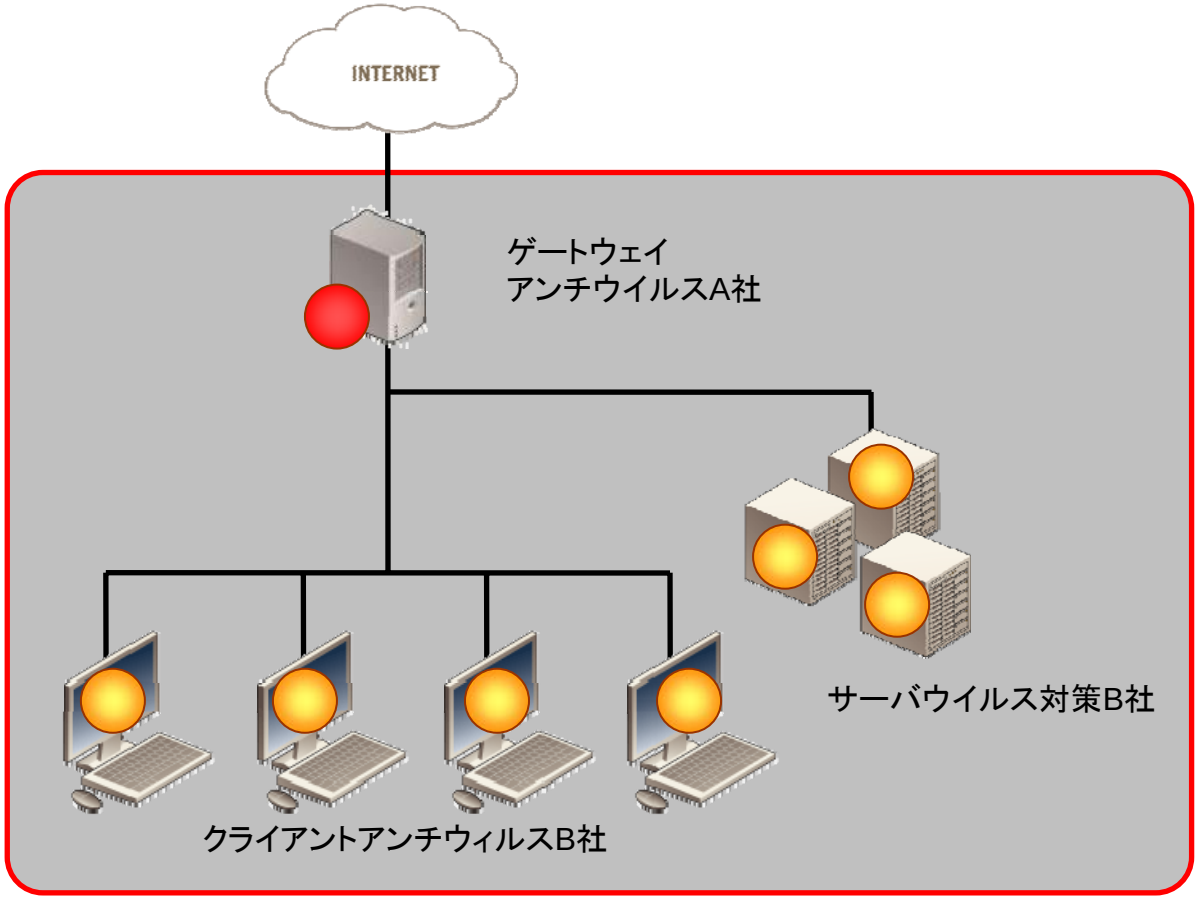
インターネットからの進入はスピードが速く、
発生から数十分で侵入の場合も

Case1:ウイルス対策一社依存型の危険性



A社のパターンファイルが遅れた場合、
その間ウイルスは侵入可能

Case2:クライアントとゲートウェイアを マルチベンダーポリシーにて構築



一社依存ではないが
クライアントの配信は時間がかかる

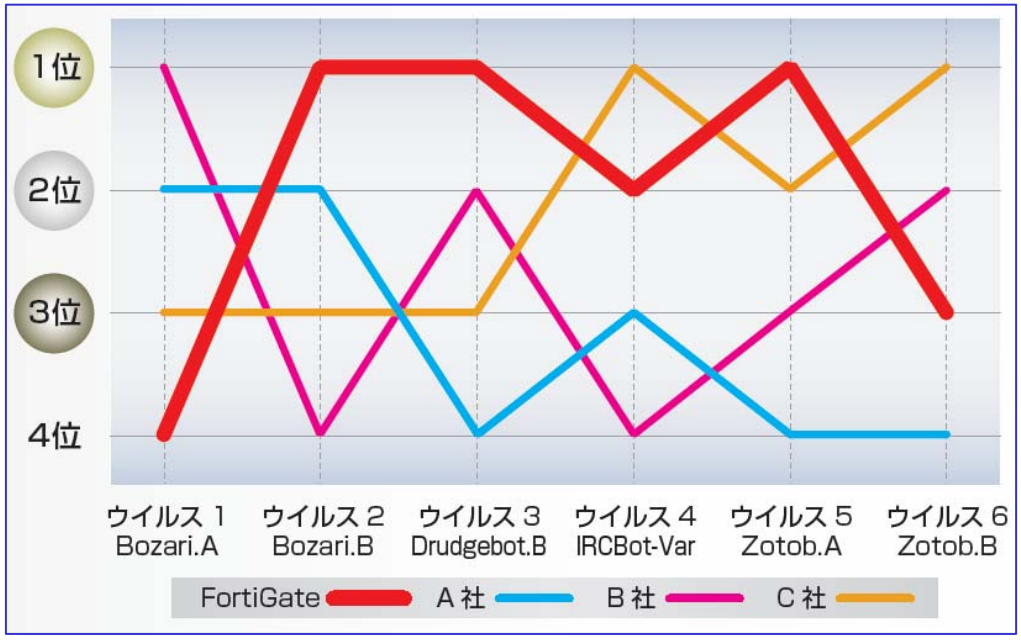
ベンダー毎に意外と差がある パターンファイルの配信スピード

パターンファイルの作成から配信まで

検体入手 → 解析 → パターンファイル作成 → テスト → 配信

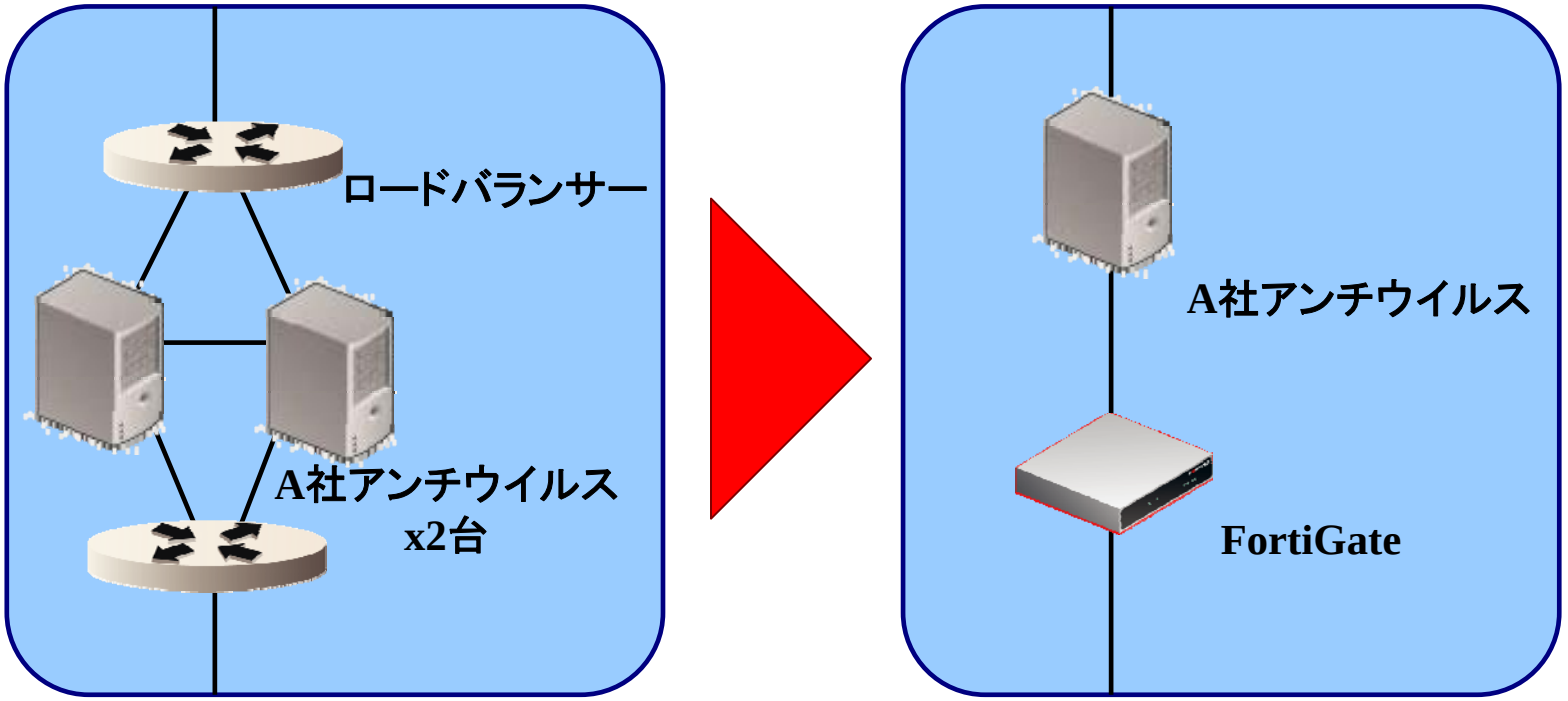
パターンファイルの更新の早さの比較

2005年8月発表のMS05-039の脆弱性を利用する6種類のウイルスに対して、更新した時間が早かったベンダー順にグラフ化したもの。



※グラフは、ドイツの第三者機関「AV-Test.org」による調査データを元に作成。（調査月：2005年8月）

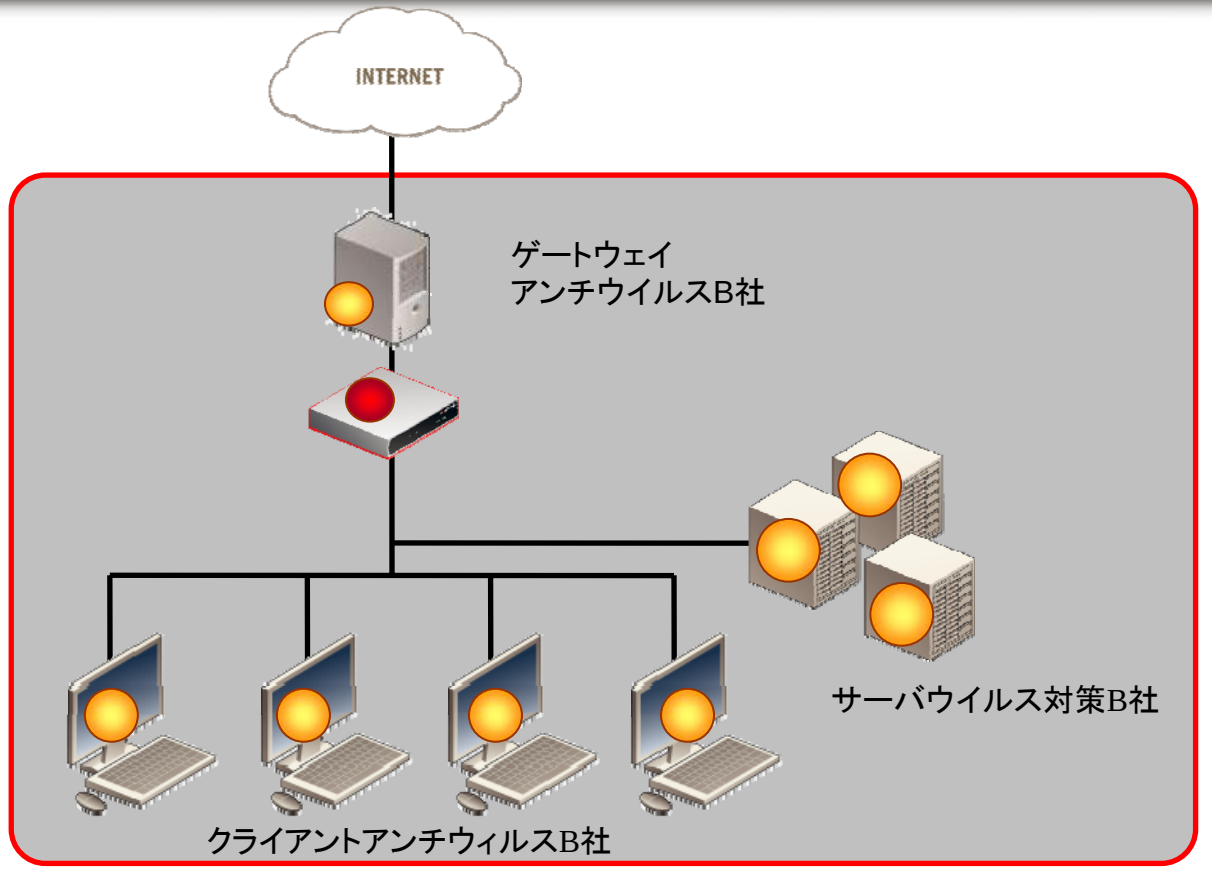
ゲートウェイウイルス対策
マルチベンダー化のご提案



いつ発生するかわからない故障に備え、
ハードウェアを二重化。

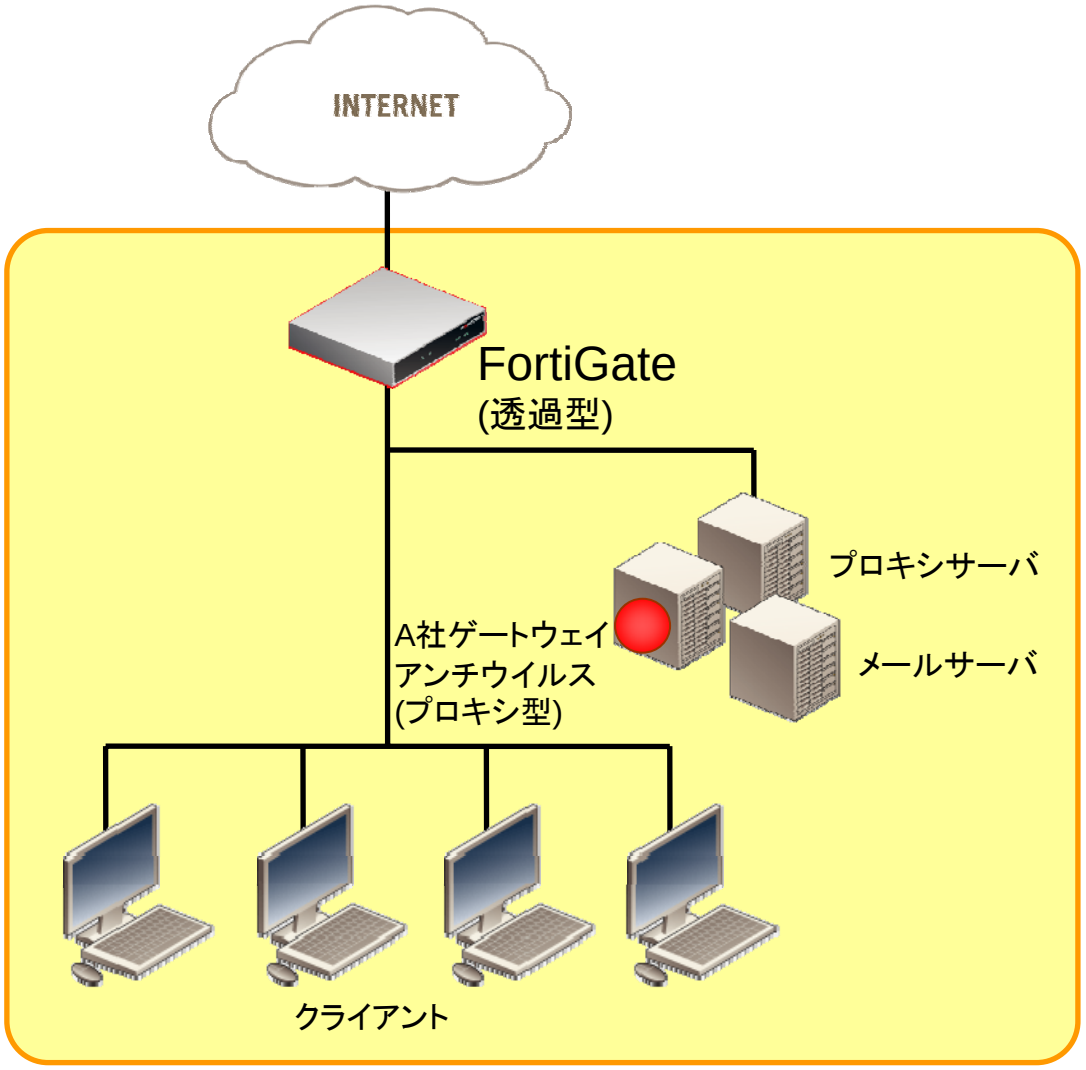
月に約100の新種とその中でも月に2～3の
アラート級のウイルスの為にアンチウイルスを
マルチベンダーで二重化。

事例:大手印刷会社



管理面を考慮しアンチウイルスベンダー1社に依存していたが、
パターンファイル遅延時の危険性を実感し
ゲートウェイアンチウイルスをマルチベンダー化

ウイルス対策二重化の構成例




FORTINET
REAL TIME NETWORK PROTECTION
ありがとうございました。
Mydoom
Bagle
Alcaul
SDBot
RBot
Annil
Evaman
M/Opey