L-026

検疫ネットワークの分散ダウンロードについての研究

Research on distributed download in quarantine network

林碩† 黒石 光雄‡ 中里 秀則† 浦野 義頼†
Shuo Lin Mitsuo Kuroishi Hidenori Nakazato Yoshiyori Urano

† 早稲田大学大学院国際情報通信研究科
Graduate School of Global Information and Telecommunication Studies,. Waseda University

‡株式会社インターネットイニシアティブ
Internet Initiative Japan

1. はじめに

情報化社会ではセキュリティの問題は非常に深刻になっており、特に内部ネットワークへの持ち込み PC を基点としたコンピュータウィルスの拡大や、社内ネットワークの不正接続による機密情報の漏洩が問題とされている。これらの問題を防止及び解消するために隔離、検疫、治療、排除の機能をもつ検疫ネットワークが市場に出るようになった。検疫ネットワークではセキュリティホールを無くすために、ソフトウェアを最新の状態に維持する自動パッチの仕組みを備えている。しかし従来の検疫ネットワークではパッチサーバが一元的にパッチを保持し、各 PC へパッチを配布しているため、パッチサーバ側の負荷が問題となる。これを解決するためには、パッチのダウンロードを分散して行うという方法が考えられる[2]。

本稿では、DHCP 型検疫ネットワークにおける、パッチの分散ダウンロード手法について述べる。

2．従来手法とその問題点

2．1 DHCP型検疫ネットワークの概要

DHCP 方式とは、社内 PC の IP アドレスを DHCP で割り振り、検疫済み PC のネットワークを、未検疫 PC のネットワークを分ける方式である。

通常の DHCP の場合、1 つの LAN に 1 つのネットワーク IP アドレスを振り割る。しかし、DHCP 方式で検疫ネットワークを構築する場合、論理的に検疫ネットワークと業務ネットワークの 2 つのネットワークアドレスを使う。例えば、社内 LAN に接続した PC にはまず 192.168.0.0/16 の IP アドレスを割り振り、検疫ネットワークに接続し、検疫が無事済んだあとに 10.0.0.0/8 の業務ネットワークに属する IP アドレスを振りなおすことにより、セキュアでない PC の隔離を行う。

2．2現行システムの問題点

不合格端末は業務ネットワークに接続できないため、治療のためのパッチダウンロードのためには検疫ネットワークに接続されたパッチサーバ内ですべてパッチを保持しなければならない。この場合、以下三点の問題が発生する。

1．同時に複数端末が加入するときや新しいパッチが登録された場合、一斉にパッチサーバへのアクセスが発生するため、パッチサーバに大きな負荷がかかる。
2．検疫ネットワーク内で治療されている端末は業務ネットワークから隔離されているため、治療が済むまで、端末での業務が実行できない。
3．治療中の端末は論理的に業務ネットワークから隔離されているが、物理的には同じネットワーク中にあり、通信路を共有している。そのため、パッチダウンロードしている間は正常の業務の妨害になる可能性がある。

3． 提案手法

以上の問題を解決すべく、現行の DHCP 型検疫ネットワークにおいて P2P による並列処理の概念を導入し、Hub 毎に PC をグループに分け、グループ単位でパッチをダウンロードする手法を提案する。

3．1 PCをグループ分けする手法

一つの Hub に繋がる PC を一つのグループとする。一つのグループ中の PC はそれぞれサーバや PC グループ内の他の PC から、対象パッチファイル内の異なる block をダウンロードする。そして、グループ内の PC 間で互いの block を補完することにより、対象パッチファイルを再構成する。

P2P の概念を導入することによって、サーバへのアクセスを分散し、負担を減少することができる。また PC をグループ分けすることによって、グループ内におけるパッチファイル再構成のための通信はすべて Hub 以下のネットワークで行われ、Hub 以上のネットワークのトラフィックに影響しない。また、物理的にも論理的にも一番近いマシン間の最大通信速度（Hub と LAN ケーブルによる転送速度）を達成できる。本手法により、サーバに負担をかけず、かつ正常マシンの正常業務に影響を及ぼさないだけでなく、最小時間内の分散ダウンロードを実現することができる。[3]

3．2ダウンロードプロトコルの提案

検疫ネットワークでの分散ダウンロードの特徴としては、システムの中にパッチサーバを持ち、パッチダウンロード、インストールを完成した PC が速やかに業務ネットワークに戻ることである。また本稿提案のもう一つの目的はダウンロード効率を向上することであり、できるだけダウンロ

ードを管理するトラフィックを抑えたいと考えている。故に、本稿では BitTorrent[5]プロトコルのように、サーバを中心したダウンロード管理システムを採用しない。また Gnutella[4]プロトコルのような、ピュアな P2P システムを構築することが必要ないという状況である。

本稿では、上述した条件を考え、また 3.1 で述べたグループ分けがなされていることを仮定している。

3．2．1 メタデータについて

ダウンロードを実行する時に必要となるメタデータを以下のように定義する。

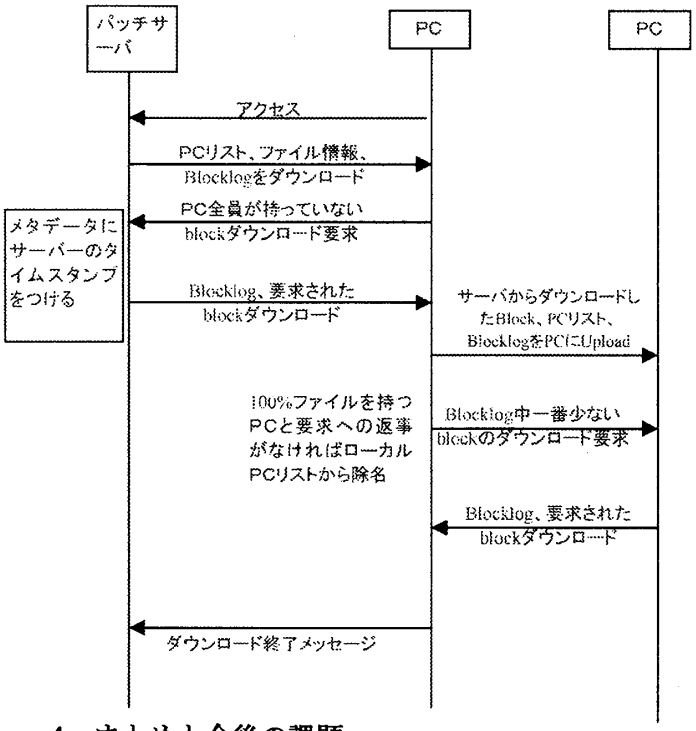
① PCID: グループ内の各 PC の IP アドレス、MAC アドレスを基に生成したグループ中のユニークな識別子。
② PC リスト: グループ内各 PC の PCID とサーバのアドレス、およびタイムスタンプからなる情報。
③ BlockID: 一つのパッチファイルを、ダウンロード単位である Block に分割する。その各 Block の識別子。
④ ファイル情報: ダウンロードするファイルのファイル名、大きさ、Block の情報と BlockID からなる情報 (BitTorrent における .torrent ファイル[5]のようなもの)
⑤ Blocklog: BlockID とその Block をダウンロード済みの PC の PCID、およびタイムスタンプからなる情報。

3．2．2 ダウンロードシーケンス

パッチファイルのダウンロードシーケンス（図１）は以下のようになる。

① PC はパッチサーバへアクセスし、PC リスト、ファイル情報、Blocklog をダウンロードする。
② Blocklog の中から、他の PC ダウンロードしていない Block をランダムに選び、パッチサーバへダウンロード要求をする。
③ パッチサーバから PC リスト、Blocklog、および Block 自体を一緒にダウンロードする。
④ ダウンロードした Block と PC リスト、Blocklog を PC リストから選択した他 PC にアップロードし、他 PC から Blocklog をダウンロードし、自身の Blocklog を更新する。
⑤ ステップ④を Blocklog 中のすべての未ダウンロード PC について繰り返す。
⑥ Blocklog からこの PC がもっておらず、かつ保持する PC が最も少ない Block を選び、該当 Block を持つ PC をランダムに選び、ダウンロード要求を送信する。
⑦ 要求された PC から Blocklog と Block をダウンロードする。
⑧ ステップ⑥からステップ⑦をダウンロードが完了するまで繰り返す。
⑨ ダウンロードを終了したあと、サーバへ終了メッセージを送信する。パッチをインストールし、検疫ネットワークから離脱する。

図1ダウンロードシーケンス



4．まとめと今後の課題

本稿では、DHCP 型の検疫ネットワークにおける、分散パッチダウンロードのためのグループ間の分散ダウンロードプロトコルを提案した。

これにより、パッチサーバへの一斉アクセスを防ぐことができると共に、各 PC がダウンロードする時間を短縮し、効率をよくすることができる。

今後の課題としては、プロトコルの検証実験、実装をすることとグループ間での分散ダウンロードの可能性についての検討である。

参考文献

[1] 許 京鵬, 黒石 光雄, 中里 秀則, 浦野 義頼, “検疫ネットワークにおける PPPoE を用いた端末管理の提案,” 信学技報, vol. 106, no. 577, NS2006-195, pp. 193-196, 2007 年 3 月.

[2] 許 京鵬, “検疫ネットワークにおける PPPoE を用いた端末管理の提案” 早稲田大学大学院国際情報通信研究科修士卒業論文, 2007

[3] 林 碩, 黒石 光雄, 中里 秀則, 浦野 義頼, “検疫ネットワークにおける、パッチ分散ダウンロードのための端末グループ分け手法”, IEICE 2007 年ソサイエティ大会発表する予定

[4]http://www9.limewire.com/developer/gnutella_protocol_0.4.pdf

[5]http://www.bittorrent.org/protocol.html