Aerie: WWWのための完全分散型匿名プロキシ
Aerie: Fully distributed anonymyzing proxy for WWW

阿部洋丈 † 加藤和彦 †,‡
Hirotake Abe † and Kazuhiko Kato †,‡

† 筑波大学 † University of Tsukuba
‡ 科学技術振興機構 ‡ Japan Science and Technology Corporation

habe@osss.is.tsukuba.ac.jp

WWW サーバとクライアントが直接通信を行うと，クライアントの持つ IP アドレスがサーバに判明する．IP アドレスは，インターネット中から一意に計算機を特定するための識別子である．そのため，クライアントの IP アドレスがサーバに判明すると，計算機を特定することが容易になり，プライバシーの漏洩に繋がることが懸念される．本展示では，我々が開発した，WWW 利用時におけるプライバシの侵害を防ぐための分散システム *Aerie* のデモンストレーションを行う．Aerie では，システムに参加しているノード同士が協調して互いに通信を肩代わりし合い，WWW サーバに対して送信者の匿名性を実現する．Aerie は完全分散型の Peer-to-Peer システムであり，中央のサーバ無しに動作する．Aerie は，システム内における高速なノード間通信のために Chord [1] を用いる．

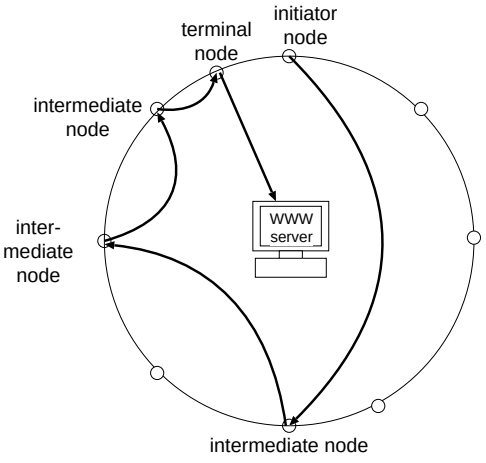

図 1: Aerie の動作

図 は，Aerie のノードによってリクエストが中継される様子を表している．説明のため，最初にリクエストを送信するノードを **開始ノード (initiator node)**，他のノードからのリクエストをさらに他へ転送するノードを**中間ノード (intermediate node)**，サーバにリクエストを送信するノードを**終端ノード (terminal node)** と呼ぶ．

Aerie においては，開始ノードは始めに終端ノードをランダムに選択する．開始ノードは，直接ノードを選択する代わりに，ランダムなキーを発生させ，そのキーが写像されるノードを終端ノードとして間接的に選択する．

Aerie において，中間ノードの選択は，終端ノードの場合と同様のランダムな選択によってではなく，Chord のアルゴリズムよる探索過程を利用して決定される．そうすることによって，終端ノードを探索する手続きと，中間ノードの選択，およびそれらを経由させながらリクエストを送信する手続きが同時に実行され，少ないメッセージのやりとりで一連の手続きが実行可能である．

いくつかの中間ノードによる中継を経て，リクエストが終端ノードに到達すると，終端ノードはサーバに接続してリクエストを送信する．サーバとの通信に成功してデータが得られると，終端ノードは自分にリクエストを送信してきた中間ノードにそのデータを送信する．中間ノードは，中継先のノードにリクエストを送信した後もその接続を維持しているので，その接続を経由してデータを送信することができる．このようにして，リクエストが中継された経路を逆に辿って，開始ノードにデータが返される．

参考文献

[1] Ion Stoica, Robert Morris, David Karger, Frans Kaashoek, and Hari Balakrishnan. Chord: A Scalable Peer-To-Peer Lookup Service for Internet Applications. In *Proceedings of the 2001 ACM SIGCOMM Conference*, pp. 149–160, 2001.