論文審査の要旨及び担当者

No.1

報告番号	甲　乙　第　　号	氏　名	William Carl Manning

論文審査担当者	主　査	政策・メディア研究科委兼環境情報学部教授　村井　純
	副　査	政策・メディア研究科委員長兼環境情報学部教授　徳田　英幸
	副　査	政策・メディア研究科委員兼環境情報学部准教授　バンミーター, ロドニー
	副　査	環境情報学部特別招聘教授　IIJ 技術研究所所長　長 健二朗
学力確認担当者：		

（論文審査の要旨）

William Carl Manning 君提出の学位請求論文は「Client Based Naming」と題し、8 章と付録からなる。

本研究では、インターネットのドメイン名システム(Domain Name System – DNS)における重大な制約からの解放に取り組んでいる。DNS は、問い合わせ/返答型のプロトコルを持つシステムで、インターネット上でパケットをやり取りするために、人の用いる名前(例: www.sfc.keio.ac.jp)から、インターネットプロトコルアドレス(例: 133.27.4.221) への変換を行うものである。DNS は、過去において最も成功した分散型名前解決システムと言えるが、最近活用が急激に増加しているモバイル型のクライアント、すなわち、接続性が不安定な端末への対応を念頭としたものではない。変化を旨とするインターネット、そして DNS 自身の変化によってもシステムの堅牢さは影響を受ける。一方、クライアントにとっては、サーバへの到達性への要求は高まるのみであり、新しい DNS の重要性は論を待たない。

本研究で提案される Client Based Naming (CBN) では、これらの問題に 3 種類の方法で対応するものである。すなわち、第三者によって運用されているサーバへの依存性を、DNS の名前木の根元にあたる「ルート」をクライアント自身が受け持つことによって緩和し、マルチキャストによりサーバ位置を発見し、暗号技術の適用により受け取る回答のうち正しいものを区別する。CBN は 3 つの点でのメリットを主張している。すなわち、(1) 第三者に運営されている DNS サービスからの独立、(2) 確実な名前解決を、厳しい、あるいは、正常に動作していることが疑われるような環境において実現、(3) 接続性によらない持続的な名前解決機能を提供、である。

本論文は、まず、第 1 章で、現在の DNS の問題について議論している。クライアントは、ネットワークへの接続性が、物理的な要因、例えば, WiFi ホットスポットのログインポータルのため、あるいは、悪意を持ったハッカーなどの攻撃等により不安定になることがある。このような場合であっても、名前解決は必要である。一方、DNS の「ルート」、あるいは、トップレベルのサービスは、4 種類の変化に同時に直面している: それらは、名前情報の正当性を暗号技術で証明するための DNSSEC の導入、名前の国際化(日本語などの英文字以外の文字の導入)、IPv6 への対応、そしてトップレベルドメイン(TLD)の数の急速な拡大である。これらの変化は、処理自体の複雑さを格段に増すとともに、ルートサーバ自身が受け取り返答すべき要求の通信量自体の増大も招いている。ある特定の、実際例によって、どのような問題が起き、クライアントに影響を及ぼしているのかが示されている。

論　文　審　査　の　要　旨

CBN は、全く新たな名前解決手法を設計し運用するのではなく、既存の DNS を改良することによって対応する。第 2 章では、この理由を示している。DNS の成功の源である、（特にキャッシュの利用による）強固なスケーラビリティと広範囲な活用の影響で、システムの入れ替えは大変困難と考えられる。さらに、DNS は継続的に機能を拡張されている。ピアツーピア方式や位置-ID(location-ID)分離による方式も議論されているが、インターネットにおいて別の目的にために用いられ、DNS を置き換えるのに適切なものではない。

第 3 章では、Client Based Naming の鍵となるアイディアを提示している。まず、IP エニイキャスト(単一の要求を複数のサービス可能なサーバに対して同時に届ける手法)が提案され、一時的な方策の一案として検証している。続けて、より完全な解法である、CBN 自身を提示している。CBN は基本的に 3 つの部分から構成されている: (1) DNS のルートをクライアント自身で受け持ち、クライアントは名前空間の他の部分の権威キャッシュとして働くようにする(Client Based Naming という名前は、ここからきている)。(2) ローカルネットワークにおけるサービス発見を IP マルチキャストを用いて行う。(3) サーバの身元と返答の内容を確認するために、暗号技術を用いる。 (1)により、クライアントはインターネットからの接続性が無い環境においても、クライアントは動作可能となる。これら 3 点の変更は、接続性が中途半端であったり、通信環境が半ば異常な状態であったり、あるいは、悪意を持った攻撃者が存在するような状況であっても、動作するように設計されている。

第 4 章では、ルートをクライアント側に移動した状態における影響について、分析的手法および実験により検討している。実際の環境において、クライアント側でキャッシングを行うことによる効果が示されている。小さめのキャッシュでもあっても的確に効果があることを見いだしている。悪意のある者によって引き起こされうる脆弱性が低いことを分析的に評価している。

第 5 章では、悪意のある者への対応についての分析が続く。悪意のある者を完全に分析することは不可能であるので、影響を減らすことに眼目が置かれている。ここでは、正規の名前サーバと詐称しようとしている名前サーバを区別するための基準を開発している。ネットワーク上の基準による判断を超える部分については、DNSSEC(暗号技術によるデータ完全性認証)が現実的な状況で使われた場合における評価としている。

第 6 章では、CBN の 3 種の利点（ (1) 第三者に運営されている DNS サービスからの独立、(2) 確実な名前解決を、厳しい、あるいは、正常に動作していることが疑われるような環境において実現、(3) 接続性によらず持続的に名前解決を提供） について評価している。モバイルノードにおけるシミュレーションを、OmNet++フレームワークを用いて行い、ノードの接続性が変わるのに伴うキャッシュの振る舞いについて調べている。CBN が、利点(1)および(3)を満たす場合において、効果があることが示されている。利点(2)については、第 4 章、第 5 章、第 7 章で議論されている。さらに、CBN の利用における、CPU、メモリ、ネットワーク利用におけるコストについて評価している。より単純なメカニズムと比較したとき、オーバヘッドの比率はかなり大きいものである一方、CBN を用いることのインパクトは、中程度の機能を持つモバイルノードで利用されることを仮定したとしても、絶対的な量としては依然小さいものであると言える。

論　文　審　査　の　要　旨

第 7 章では、CBN の実装に必要な、DNSSEC の暗号鍵の管理における未解決の問題点について示している。すなわち、鍵の長期間使われた後の失効や、何らかの問題により強制失効されたときの、モバイルノードのようなインターネットに間歇的に接続するようなノードの対処方法である。鍵交換(Key Rollover)という方式は、秘匿通信が始まった時代からさえあるが、「N 個の鍵のうちの M 個を用いる」方式により、どのサーバを信頼するかを判断し、さらに、DNS クエリ結果を信用するために必要な完全な署名の連鎖を再構築できる。

第 8 章で，議論をまとめている.

付録 A では、DNS の歴史と運用について、いかに HOSTS.TXT ファイルから DNS が発展していったのかを示す短いチュートリアルとなっている。

この接続性が間歇的であるモバイルクライアントにおける名前解決は、すでに実世界において影響を与えている。この研究自体は、実際には、DNS サーバを発見するための IP マルチキャスト活用という形で 2000 年頃に始まっている。このアプローチ自体は、例えば Apple によって標準機能の一部である “Bonjour” として採用され、本研究への明示的な引用と共に、既に 10 年間の実績がある。従って、この研究は、すでに世界に対して重大なインパクトをもたらしていると言える。

上記の成果と、それを記述した本論文を通して、著者の先端的な研究を行なうために必要な高度な研究能力、並びにその基礎となる豊かな学識、研究成果を社会貢献へ結びつける能力を有することを示したものといえる。よって、本委員会は、本論文の著者は、博士 (政策・メディア)の学位を受ける資格のあるものと認める。