様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ６ 月　 ８ 日現在

機関番号：１４４０１
研究種目：基盤研究(C)（一般）
研究期間：2019～2022
課題番号：１９Ｋ１１９４３

研究課題名（和文）ＩＰｖ６アドレス範囲割当及び組織内動的経路制御への利用者区別可能な認証機構の導入

研究課題名（英文）Introduction of User Distinguishable Authentication Mechanism to Address Assignment and Site Internal Dynamic Routing of IPv6

研究代表者
大平　健司（OHIRA, Kenji）

大阪大学・情報推進本部・准教授

研究者番号：４０５１５３２６

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：本研究課題では、動的経路制御機構に関し、OSPFv3経路広告情報に、RFC 8362で規定されるE-Router LSAを用いて、署名情報を格納する拡張を行い、この署名情報を検証する機構についても実装した。また、動的アドレス割当管理機構に関し、サブスクライバセッション管理の概念を導入することが、SLAACにより割り当てられたアドレスの追跡可能性向上に有効であることを確認した。

研究成果の学術的意義や社会的意義
学術機関のネットワークは管理不十分となっていることが多く、学術機関が関連する情報セキュリティインシデントが相当数ある。本研究課題は、学術機関の持つ特性を考慮に入れつつ、主にインシデント発生時の原因端末追跡可能性を向上させるものである。これにより、学術機関における情報セキュリティレベルの向上が期待される。

研究成果の概要（英文）：In this research, on the subject of dynamic routing mechanism, we have extended OSPFv3 routing information to store digital signature with E-Router LSA defined in RFC 8362 and have implemented a signature verification mechanism. On the subject of dynamic address assignment mechanism, we have confirmed that introducing subscriber session management is effective to improve traceability of addresses assigned with SLAAC.

研究分野：情報ネットワーク

キーワード：IPv6　経路制御　アドレス動的割当　正統性検証

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

大学は対外的には一つの組織であるが、その歴史的経緯の中で特に学問の自由や部局の自治への考慮が求められており、その結果、基幹ネットワークを管理する全学としてのネットワーク管理者（以下、全学ネットワーク管理者と呼ぶ）だけでなく、接続する各サブネットワークに対し、それぞれ管理者（以下、サブネットワーク管理者と呼ぶ）を指定し分散管理していることが多い。また、大学では端末をキャンパスネットワークに接続する際に、一般的に不正アクセス対策や情報の機密性の保持といった一定の接続基準を設けているが、端末の接続についての基準の具体化は各サブネットワーク管理者に委ねられることが多い。

法令や学内規則等に反する行為がキャンパスネットワークを通じて行われた場合、その行為者を特定ししかるべき措置をとる必要がある。各種ライセンス違反事案や不正アクセス関連事案などに関連して外部から大学に対して照会がある場合、その照会内容には IP アドレスの情報が含まれる。この照会に対し全学ネットワーク管理者が学内に対して調査を行う場合は当該 IP アドレスの情報を用いてサブネットワーク管理者を特定して問合せを行い、照会を受けたサブネットワーク管理者は…と調査が進められることとなる。

一方で、学生にラップトップコンピュータ等の BYOD（Bring Your Own Device: 自己所有機器の持ち込み）を推奨する大学が増えているが、これらの端末に対しては、そのソフトウェアライセンス管理状況やセキュリティ対策の実施状況について、各サブネットワーク管理者の目も十分行き届かない形でキャンパスネットワークに接続されるケースも少なからず見受けられる。その結果、大学としての管理責任が問われかねない情報セキュリティインシデントに発展するケースすら現実のものとなってしまっている。

２．研究の目的

上述した背景から、

外部からは一塊りのものとみなされるが、内部的には 3 階層以上の分散管理されたサブネットワークから構成される、組織の IP ネットワークにおいて、追跡・検証可能性が失われない動的アドレス割当管理機構や動的経路制御機構にはどのような性質が求められるか

という問いに対する解を得ることを本研究の目的とした。

対象組織の IP ネットワークに接続される機器に対して割り当てられる IP アドレスが個々の機器の実際の利用者ないし管理責任者と強く対応付ける必要があることは論を俟たないが、本研究の対象とする組織・構成員及び IP ネットワークについては、1) サブネットワーク構成を決定する要因となりうる、組織内の部署やプロジェクトの構成は、時間経過に対して大きく変更される可能性が高い、2) 組織構成員は複数の部署やプロジェクトに所属する可能性が高い、3) 組織構成員の保持管理する端末は複数である可能性が高く、それらは出自も機能性能も多様である可能性が高い、4) サブネットワーク管理者については、必ずしも IP ネットワークに関する専門知識を一定以上有すると期待できるとは限らない、という特性を持つ。これらの特性も考慮したうえで、誰がどの範囲の対応関係を管理するかについて設計する必要がある。

また、正しい対応付けの得られない IP アドレスは組織ネットワーク内でルーティングされないようにするため、IP アドレス割当管理と経路制御の間で連携・連動することが求められる。この対応付けや連携・連動を行なうための具体的な設計・試験実装・評価検討を行うことが本研究の二つ目の目的である。

３．研究の方法

外部からの検証可能性を考えたとき、IPv4 で多用されている NAT がサブネットワーク内で使用される状況は不都合なものと捉えられる。組織ネットワークをすべて収容できる大きさのアドレス空間を確保することを考えたとき、1) 組織ネットワーク全体を単一の NAT の内部に収容する、2) IPv6 を使用する、の選択肢があり得る。本研究では後者について検討を進める。

IPv6 において代表的なサイト内動的経路制御方式として OSPFv3 が挙げられる。これをサイト内動的経路制御方式の具体的な実装のベースとして想定し、広告される経路情報に電子署名を付加し受け取ったルータで署名検証を行う拡張を施すことによりプレフィクス（アドレス範囲）の追跡可能性向上を図る。これにより、例えば A 部局に割り当てたはずの範囲のアドレスが B 部局から広告されているというような状況を防止する。

IPv6 においてアドレス割当の代表的な方式として DHCPv6 と SLAAC が挙げられる。この両者を比較すると DHCPv6 による方が管理は容易なように考えられるが、Android OS において利用できないことが大きな問題である。SLAAC は単純に用いたのではアドレスを割り当てた端末の管理が難しい問題がある。そのため、末端の端末にとっては SLAAC によりアドレス割当を受けたように見せつつ、割り当てを受けた者の追跡が可能な管理方法を探索する。

４．研究成果

動的経路制御機構において、OSPFv3 経路広告情報に、RFC 8362 で規定される E-Router LSA

(Extended Router LSA)を用いて、署名情報を格納する拡張を行った。また、この署名情報を検証する機構についても実装した。これらの実装を用いることで、各ルータは予め認められた範囲のプレフィクスしか広告できない（広告しても有効な経路情報として受理されない）状況を実現できた。

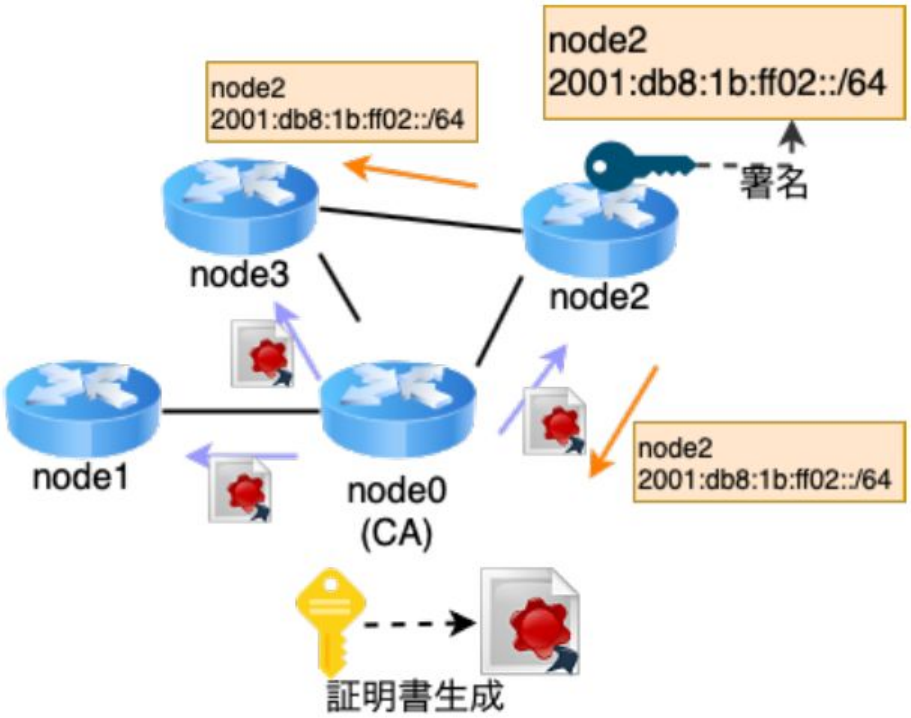

図 1：OSPFv3 拡張の概要図

動的アドレス割当管理機構において、サブスクライバセッション管理の概念を導入することが、SLAAC により割り当てられたアドレスの追跡可能性向上に有効であることを確認した。この方式により、アドレス被配付側は単純な SLAAC と何ら変わりない手順でアドレス配付を受けられる一方、アドレス配付側ではセッションの概念を持ち、セッション毎に論理インタフェースが生成される。セッションに関連付けられた IP アドレス範囲からのパケットのみが上記論理インタフェースに着信する。どのセッションにも関連づかない IP アドレス範囲からのパケットは物理インタフェースには着信するが単純なフィルタにより転送しないようにできる。

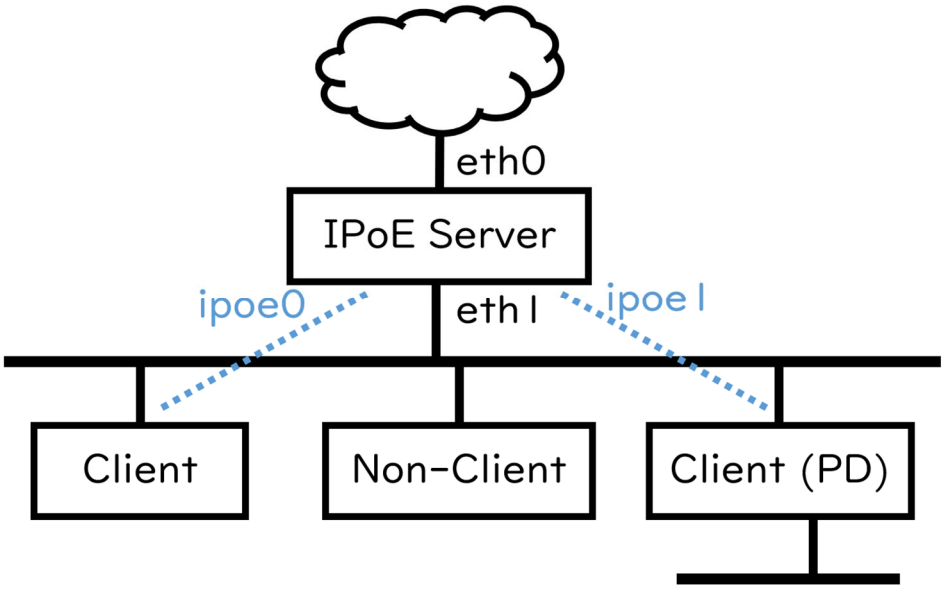

図 2：サブスクライバセッションの概要図

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　0件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 大平健司	４．巻 IEICE-121
２．論文標題 キャンパスネットワークにおけるIPoEを用いたIPアドレス割当管理の検討	５．発行年 2022年
３．雑誌名 信学技報	６．最初と最後の頁 75 78
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Takahiro Oriishi, Kenji Matsuura, Kenji Ohira	４．巻 9
２．論文標題 PKI-enabled OSPFv3 for Reliable IP Traceback	５．発行年 2019年
３．雑誌名 Bulletin of Networking, Computing, Systems, and Software	６．最初と最後の頁 7 11
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 居石峻寛，松浦健二，大平健司	４．巻 IEICE-119
２．論文標題 プレフィクスの送信元を保証するためのPKIを用いたOSPFv3拡張	５．発行年 2020年
３．雑誌名 信学技報	６．最初と最後の頁 175 180
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計3件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 大平健司
２．発表標題 キャンパスネットワークにおけるIPoEを用いたIPアドレス割当管理の検討
３．学会等名 電子情報通信学会インターネットアーキテクチャ研究会
４．発表年 2022年

１．発表者名 Takahiro Oriishi, Kenji Matsuura, Kenji Ohira
２．発表標題 PKI-enabled OSPFv3 for Reliable IP Traceback
３．学会等名 The 10th International Workshop on Networking, Computing, Systems, and Software（国際学会）
４．発表年 2019年

１．発表者名 居石峻寛，松浦健二，大平健司
２．発表標題 プレフィクスの送信元を保証するためのPKIを用いたOSPFv3拡張
３．学会等名 電子情報学会インターネットアーキテクチャ研究会
４．発表年 2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関