第 8 章　経路制御におけるセキュリティの現状

内容

- 経路交換の問題点とその原因
- 経路情報保全に関する提案・活動等

8. 経路制御におけるセキュリティの現状

本章では、前章までの問題点などをふまえ、経路制御を行う上でのセキュリティの現状と実体について整理する。

最初に、経路交換を行にあたって、第１層や第2層で発生するセキュリティ上の問題点について整理する。その後、さらに上位層での問題点について整理し、最後に、経路情報保全に関する活動等についてまとめる。

8.1. 経路交換の問題点とその原因

経路交換を行う際には、データ伝送上 (第 1 層、第 2 層) の問題、セッションハイジャックや DoS (Denial of Services) の様なシステムの脆弱性を突いた攻撃、経路情報の信憑性の問題、そして経路情報の増大に関る問題等が上げられる。

本節では、これらの問題点について整理する。

8.1.1. データ伝送上の問題点

ここでは、通常、通信事業者がサービス行っているデータ伝送上の問題点のうち、主に第 1 層および第 2 層に関して述べる。

第 1 層／第 2 層の問題点としては、事故によるファイバ等の物理線の切断や通信機器障害により発生する通信障害、設備管理の不備等による第 3 者の故意による通信設備の破壊／不正アクセスによる不正情報の混入、盗聴等による情報の不正取得等がある。さらに通信上の情報が盗まれることで、より上位層への攻撃を容易にする可能性も増大する。

例えば、通信線は通常ビル内の 1 部屋(MDF 室と呼ぶ)に一度集められ管理／運営されることが多く、この集中管理部屋から各部屋へ再分配される。つまり、一度に数社の人間が MDF 室に入室する可能性がある。この時、さらに第 3 者が入室しても識別は困難である。この第 3 者が通信事設備に対して何らかの不正行為を行う可能性は排除できない。

もう一例としては、特定のエリアにおける Ethernet 環境下では仕様上、ある特殊なアドレスを送信先としてデータを送信すると、エリア内の全て機器はデータを受信して送信元に結果を送り返さなければならない。このとき送信元のアドレスが詐称されていたり、その応答が大量に発生し、応答トラフィックが増大した場合にエリア内での通信障害が起きたりする可能性が高く、さらには、どのような通信サービスを行っているかなどの基本的な情報が盗まれる可能性が大きくなる。

このような事象が発生する原因としては、データ伝送線やデータ伝送機器に対して保護が十分でない場合や、それら機器の管理が徹底されていない状況が考えられる。

データ伝送を行う上での物理的、運用上の様々なリスクを軽減するために ISO27001 等を利用する取り組みがなされている。この取り組みのなかでは、組織における資産の統一的、且つ、一定の基準を持った管理／運用ポリシが必要であり、その管理／運用ポリシを実行している事で、事故が起きたとしても迅速な対処が可能である。また、ポリシを持った運用を行っていることを対外的に示す事ができ、データ伝送提供者、利用者双方に利益につながる。

8.1.2. システムの脆弱性を突いた攻撃

ここでは、サービス・プロバイダの設備となるシステムの問題点として第 3 層から上位層に関して述べる。

第 3 層から上位層は、通信における付加価値サービスの提供を行うサービス・プロバイダや企業内で利用されるケースが多く見られる。現在は、インターネット・プロトコル(以降、IP)の利用が一般的である。IP の仕様は公開されており誰でも自由に参照／利用が可能である。しかし、自由であるが故に悪意のある攻撃者に弱点を突かれるケースもある。現時点では、攻撃によるリスクより利用者が受ける恩恵の方が大きいため、様々なリスク軽減措置を整えた上で IP が利用されている。

IP は、第 1／2 層の通信サービスを介して通信対象者同士が直接データ交換可能な仕組みを提供しているが、この時、通信相手の特定が問題になる。机の隣どうしで通信をする場合には通信機器も通信する人も見て確認できるが、遠距離になると難しい。特に、機器間の通信は設定が容易である IP アドレスを用いて行われるので、知らない間に通信相手が変わっていたと言うことが起こる可能性がある。通信相手が変わっているにもかかわらずそれを知る方法がないとすると、送信者は知らない間に秘密情報を送ってしまう場合があり、それに気づくのが遅れたり、最悪の場合気づかずにより大きい損害発生させたりする可能性がある。

また、IP を利用して通信を行うソフトウェアの弱点を突いて、悪意あるデータが送られた場合、IP を介して受け取ったソフトウェアが停止したり、ソフトウェアを介して重要な情報が盗まれたり、最初にあったソフトウェアが不正なソフトウェアに上書され他組織への攻撃に利用されたりする可能性がある。

最大の原因は、通信相手の特定を IP アドレスに頼っているのにも関わらず、その通信相手が本来の通信相手なのか詐称をしている第三者なのかの確認が困難であることである。

通信相手を確認する方法は様々な取り組みがなされており、利用方法により様々な方法が普及している。一例としては、IPsec を用いた接続先の認証や PKI を利用した接続先の検証などが挙げられる。これら仕組みは、接続先の検証のみではなく他の機能も含まれており適材適所で利用されており、様々な認証機能の仕組みが実現可能である。

8.1.3. 経路情報の信憑性の問題点

本節では、広域でかつ複数の組織が相互接続する環境で、IP 通信を行う場合に利用されている経路交換システム内で扱われる経路情報に関わる問題点に関して述べる。

事故／故意に関わらず、不正な経路情報が経路交換システムへ混入することにより、サービス提供者は提供サービスが正常に提供出来なかったり、サービス利用者が悪意あるサイトへ誘導され、さらに大きい被害に拡大したりする可能性がある。経路交換システムに関してはすでに本調査の前半にて既に述べられているが、経路交換システムで半自動的に受信した経路情報を経路交換システム自身で自動検証する枠組みは現時点では無い。

不正経路による偽サーバへの誘導を図 8-1 に示す。

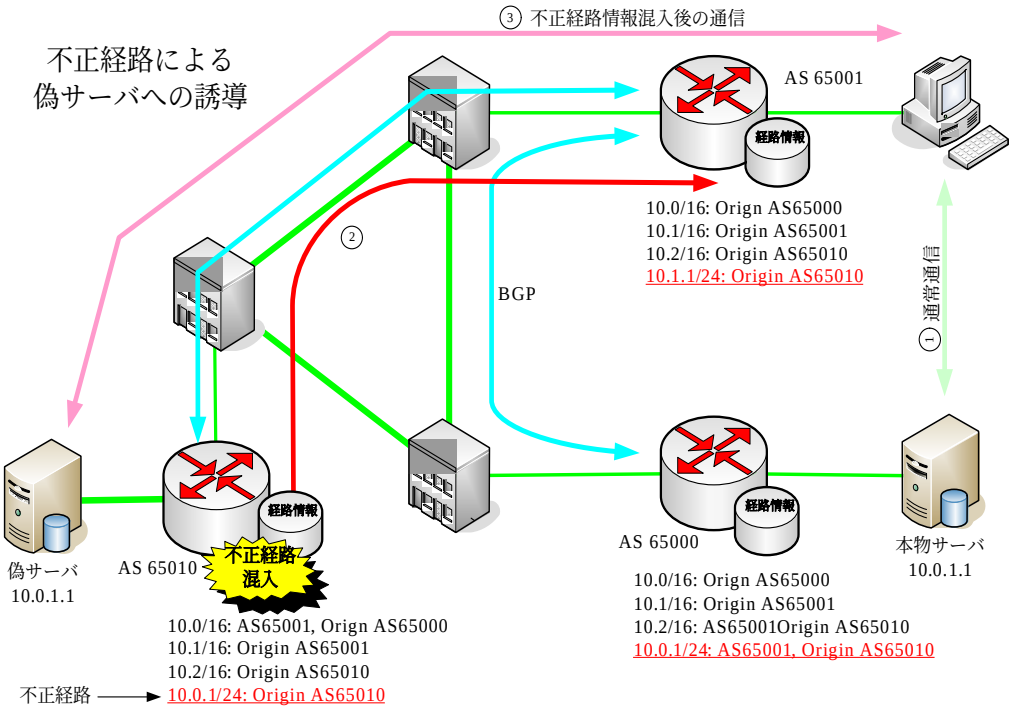

図 8-1　不正経路による偽サーバのへの誘導

しかしながら、不正経路の経路制御システムへの混入は現実問題として起きており、経路情報の保護の必要性が有る事は認識され様々な議論がなされている。このようななか、本調査では soBGP と S-BGP について次章にて述べる。

不正経路情報の排除に関する現実に行われている取り組みとしては、本調査で述べている IRR を利用する方法である。この方法では、IRR に登録されている情報を信用する事で経路制御機器に対して適切なフィルタを設定し、明らかに不正な経路を除外する。しかし、IRR を用いた「登録→フィルタ作成→機器」への設定にはある程度の時間が必要でありトラブルや緊急時の経路変更に対応するのは難しい側面もある。

BGP で現在行われている MD5 による保護は、隣接した機器間で交換される情報の信憑性は確認可能であるが、MD5 へ入力された情報に対する信憑性の有無に関して検証する物ではない。つまり、BGP-MD5 の目的は接続機器間における接続先の確認と通信情報の検証である。

8.1.4. 経路情報の増大に関わる問題

IP 接続組織が多くなるとともに経路情報も大きくなる。本節では、経路情報が大きくなったときにもたらされる問題点に関して述べる。

経路情報が多くなってくると、その情報を処理するための経路制御装置の CPU やメモリ等の容量拡大が必要になり、さらに経路情報に変動が生じたと時その変動を処理するために必要な時間が多く必要となる。また、データ伝送回線に占める経路交換に有する占有率が上がる等の問題がある。

原因は、経路制御機器の誤設定や IP を利用したビジネスの拡大等が考えられる。

経路情報の増大に関しては、現在ほぼ適切な時期に各ルータメーカーなどが CPU やメモリの増強等に対応した機器を発売するなどして対応が行われており、IPv4 の経路制御に関しては相当な対応がされている。しかしながら IPv4→IPv6 移行期や IPv6 普及期に入った時には、更なる経路数の増加が見込まれ、それに伴う更なる設備投資の必要性が考えられる。

8.2. 経路情報保全に関する提案･活動等

問題を解決するための技術や運用による一時対処的なものまで様々な領域で色々な活動が行われているが、IRR にみられる様な経路交換システムとは別のデータベースを利用する事で現行システムに対しての変更を限りなく少なくする取り組みと、soBGP や S-BGP にみられる様な経路交換システムに新たに機能を加えることで経路情報を守る方法と大きく 2 種類の方向性がある。IRR の取り組みに関しては、先に述べた。また、soBGP および S-BGP に関しては第 9 章にて記述する。