ネットワーク運用管理視点による隠蔽通信路の分類

櫨山 寛章 † 室田 朋樹 ‡ 加藤 朗 ††

奈良先端科学技術大学院大学 † 東京大学 ‡ 慶應義塾大学 ††

要 旨

隠蔽通信路とは、プロトコル設計や標準規格、システムメカニズム上で意図されていないネットワーク上の通信チャネルや情報伝達手法である。既存の隠蔽通信路の分類は情報の個別の隠蔽手法に着目した分類が多く、ネットワーク運用の場面で隠蔽通信路対策を統合的に施す際に扱いにくい分類となっている。そこで、ネットワーク運用において隠蔽通信路を他のネットワーク攻撃と同列に扱えるようにする隠蔽通信路の分類の作成を本稿では試みる。ネットワーク監視に対する回避攻撃手法とみなした場合の分類と隠蔽通信路を通信モデルによる分類との 2 種類の分類を本稿では提案する。

A Taxonomy of Network Covert Channels from the View of Network Operation

Hiroaki HAZEYAMA† Tomoki MUROTA‡ Akira Kato ††

Nara Institute of Science and Technology†, The University of Tokyo‡, Keio University††

Abstract

Network covert channels are communication channels or information transfer methods in networks which are not intended for information transfer in protocol designs, protocol standards or system mechanisms. Proposed taxonomies on network covert channels have categorized network covert channels by specific covert techniques, however, such taxonomies are difficult to be applied into network operation. In this paper, we try to create new taxonomies of network covet channels to handle network covert channels as well as other network security attacks. We propose two taxonomies of network covert channels; one is a taxonomy which considers network covert channels as evasion techniques against audits, the other is a taxonomy according to communication models of covert and overt channels.

1 はじめに

インターネットは今日社会インフラとして広く活用されており、我々の日々の生活のみならず、企業や政府などでも機密性の高い重大なデータが日常的にインターネットを介して交換されている。そのため、ネットワークを介した情報漏洩はセキュリティ上の問題の一つとなっている。情報漏洩の手段の一つとして、TCP/IP やイーサネットなどのネットワークプロトコルにおいて、規格や実装上で情報伝達の手段として意図されていないネットワークプロトコルの利用方法により情報を隠蔽し伝達する通信路が知られている。このネットワーク上の隠蔽された通信路は一般にネットワークコバートチャネル (network covert channels) と呼ばれる [1]。以降、本稿ではネットワークコバートチャネルを隠蔽通信

路と呼称する。

隠蔽通信路構築手法および対策手法の分類は数多く行われている [1–5]。しかしながら、個別の構築手法に対する対策手法の研究自体は数多くあるが、産業界で扱える包括的な隠蔽通信路対策手法は未だ存在しない [5]。また、隠蔽通信路構築手法と対策手法に関する包括的な分類も現状存在していない [5]。

この現状に対し、ネットワーク運用の場面で扱える隠蔽通信路構築手法に関する包括的な分類を行う第一歩として、我々は先行研究 [6] にて隠蔽通信路を構成する分類指標の洗い出しを行った。先行研究 [6] で洗い出した分類指標は詳細な要素まで洗い出しているため非常に扱いにくいが、分類指標を洗い出していく過程で包括的な分類を行うための知見がいくつか得られた。そこで、本稿では、先行研究 [6] で洗い出した分類指標と知見を元に、包括的な隠蔽通信路の分類表の作成を試みる。本稿でのアプローチは、1) ネットワーク監視に対する一般的な回避攻撃として捉えた場合の隠蔽通信路の分類、2) 詳細な通信モデル分析による隠蔽通信路の分類、以上 2 つの側面から隠蔽通信路を分類する。

2　隠蔽通信路に関する既存の分類と通信モデル

隠蔽通信路 (covert channel) は Lampson により OS での設計上意図していない権限委譲を利用した通信チャネルとして 1973 年に定義され [2]、以後様々な研究者によってネットワーク上での隠蔽通信路と対策手法の検討が行われている [1–5]。2.1 節では、文献 [5] を元に、本稿で用いる語彙の定義と基本的な隠蔽通信路に関する通信モデルの説明を行う。

2.1　基本的な用語の定義

以下に、文献 [5] を踏まえた、隠蔽通信路に関する基本的な語彙の定義と通信モデルを説明する。

2.1.1　隠蔽通信路の基本構成

隠蔽通信路 **(Covert Channel)** とは、ネットワークプロトコルを用いた情報の隠蔽、もしくは、隠蔽情報を伝達する通信路を指す。本稿では、情報が技術的に隠蔽されているか否かは問わない。一方、公然通信路 **(Overt Channel)** とは、システムメカニズムによって公認されている情報伝達する通信路を指し、一般的には隠蔽通信路の埋め込み先となる通信路を指す [7]。隠蔽情報 **(Covert Information)** は隠蔽通信路によって伝達される情報を指し、Hidden Information, Covert Message, Covert Data と呼称する場合もある。

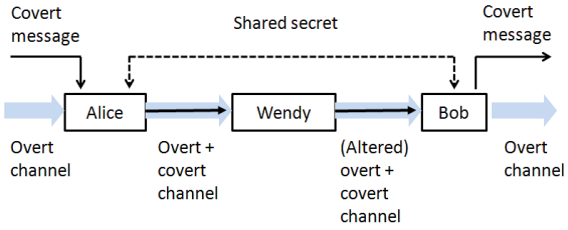

図 1: 基本的な隠蔽通信路モデルその 1

隠蔽情報送信ノード **(Covert Sender)** は隠蔽通信路の送信元ノードまたは隠蔽情報の送信ノードを指し、隠蔽情報受信ノード **(Covert Receiver)** は隠蔽通信路の宛先ノードまたは隠蔽情報の受信ノードを指す。公然情報送信ノード **(Overt Sender)** は公然通信路の送信元ノードまたは公然情報の送信ノードを指す。公然情報受信ノード **(Overt Receiver)** は公然通信路の宛先ノードまたは公然情報の受信ノードを指す。隠蔽情報送信ノードと隠蔽情報受信ノードの間で共有されている秘密情報は共有秘密情報 **(Shared Secret)** と呼ばれ、共有秘密情報には隠蔽情報埋め込み手法や隠蔽情報抽出方法、符号化・復号化アルゴリズム、暗号化アルゴリズム、共有鍵などが該当する。

中間ノード **(Intermediate Node)** はネットワークトポロジ上、公然通信路の中間に位置するノードを指す。中間ノードは公然通信路のメッセージを転送し、場合によっては公然通信路のメッセージに対して何らかの変化を加える。悪意ある中間ノード **(Middleman)** は隠蔽情報送信ノードである中間ノード、または隠蔽情報受信ノードである中間ノードを指す。一方、結託中間ノード **(Collude Intermediate Node, Colluder)** は隠蔽情報送信ノードまたは隠蔽情報受信ノードではないが、共有秘密情報を共有し、隠蔽通信路に対して何らかの操作を行う中間ノードを指す。文献 [5] では記述されていないが、本稿では悪意ある中間ノードと区別するため結託中間ノードを定義する。

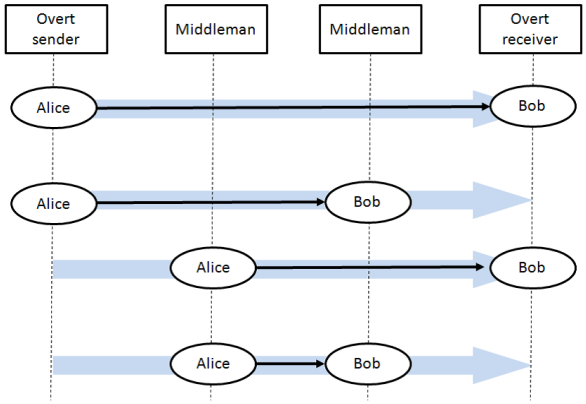

図 2: 基本的な隠蔽通信路モデルその 2

図 1 は文献 [5] で示されている基本的な隠蔽通信路のモデルである。図 1 は Alice が隠蔽情報送信ノード、Bob が隠蔽情報受信ノードであり、Wendy が中間ノードである。Alice と Bob の間では共有秘密情報があらかじめ共有されている。

Alice は自身が構築する、もしくは転送する公然通信路のメッセージに隠蔽情報を挿入し、Wendy に公然通信路のメッセージを転送する。中間ノードである Wendy は公然通信路のメッセージを Bob に転送する。場合によっては、Wendy は公然通信路のメッセージに何らかの変化を加える場合もある。隠蔽情報が含まれた公然通信路のメッセージを受信した Bob は共有秘密情報を用いて隠蔽情報を抽出する。Bob が中間ノードであり、公然通信路のメッセージを他のノードに転送する際、Bob は隠蔽情報を削除して転送する場合もあれば、隠蔽情報を含んだまま転送する場合もある。隠蔽情報を削除するか否かは隠蔽通信路構築手法によって変わる。

図 2 は、文献 [5] で示されている、隠蔽情報送信ノード Alice と隠蔽情報受信ノード Bob のネットワーク上の位置関係を表した図である。Alice と Bob が公然通信路の端点に位置する場合はそれぞれ公然情報送信ノード (Overt Sender)、公然情報受信ノード (Overt Receiver) となる。Alice または Bob がネットワーク機器など公然通信路の中間ノードの場合は悪意のある中間ノード (Middleman) となる。

2.1.2　隠蔽通信路の類型

文献 [5] によると、隠蔽通信路はストレージチャネルとタイミングチャネルに大別される。ストレージチャネル **(Storage Channel)** は、送受信者で交換されるメッセージ中に直接メッセージを書き込む貯蔵型隠蔽通信路を指す。隠蔽情報は、IP ヘッダや TCP ヘッダへの埋め込みなど公然通信路のメッセージに対して直接読み書きされる場合や、カプセル化などを用いて別のプロトコルとして認識させることによる隠蔽する場合、暗号や変調を用いて間接的に読み書きされる場合もある。また、特に技術的な隠蔽は行わずに、ネットワーク運用管理者の死角を突いて隠蔽するような隠蔽通信路も存在する。

一方、タイミングチャネル **(Timing Channel)** は隠蔽情報送信ノードから時間変調をかけた信号を公然通信路に埋め込む時間変調型隠蔽通信を指す。埋め込む対象としては、メッセージの到着間隔や CPU の使用率など様々なものがある。

また、文献 [4] では、複数のストレージチャネルやタイミングチャネルを組み合わせて周波数変調として用いる周波数チャネル **(Frequency Channel)** や HTTP など特定のプロトコルを用いるプロトコルチャネル **(Protocol Channel)** を定義しているが、ともにストレージチャネルとタイミングチャネルの派生もしくは応用とみなすことができる。具体的な隠蔽情報の埋め込み方法や抽出方法の説明は文献 [4,5] で整理されているため、本稿では 3 節で簡単に触れる程度にする。

2.2　本稿での狙い

本稿では、文献 [4,5] で整理されている個別の隠蔽通信路構築手法をネットワーク運用の立場から包括的な隠蔽通信路対策を施す際の指針となる隠蔽通信路の分類を作成することを目指す。ネットワーク運用管理の立場から考えると、特徴の似通った隠蔽通信路はファイヤウォールや侵入検知システム等で一括して対策したいと考えるのが常である。我々の先行研究 [6] では、個々の隠蔽通信路を特徴づける分類指標の洗い出しを行うため、既知の隠蔽通信路構築手法や隠蔽通信路構築に応用される可能性のある脆弱性や攻撃手法を解析した。その結果、以下の 4 つの知見を得た。

知見 **1)** 情報隠蔽手法はネットワーク監視に対する回避攻撃と捉える事ができる。よって、隠蔽通信路をネットワーク監視に対する回避攻撃の一つとして捉え直すことで、隠蔽通信路を他の回避攻撃と同等に扱え、攻撃手法として包括的に分類できる。作

成された分類表に基づき、運用管理者が隠蔽通信路対策に関する管理ネットワーク内の死角を把握できるようになることが期待できる。

知見 **2)** 隠蔽通信路の通信モデルは、いくつかの類型に細分化できる。よって、通信モデルを詳細に分析することにより、通信モデルの型により隠蔽通信路を包括的に分類できる。ネットワーク間の連携が必要か否かなど、対策手法の見極めが作成された分類表により容易に実施できることが期待できる。

知見 **3)** ネットワークの運用管理形態や信頼モデルの設定によって、隠蔽通信路構築コストおよび隠蔽通信路対策手法の設置コストが変わる。そのため、ネットワークの運用管理形態に沿って脅威モデルを設定することで、隠蔽通信路を構築するための攻撃および隠蔽通信路を用いた情報漏洩を実施する攻撃者側のコストと、隠蔽通信路対策を施すネットワーク運用者側のコストを比較分析し、隠蔽通信路の脅威レベルを設定できる可能性がある。設定した脅威レベルは、運用管理者が隠蔽通信路対策手法を管理ネットワーク内に適用すべきかどうかの指針として利用されることが期待できる。

知見 **4)** 隠蔽通信路構築手法、隠蔽通信路対策手法のどちらも、ラベル、要素、属性の組み合わせによるオブジェクトとして表現できる。そのため、CVSS (Common Vulnerability Scoring System) [8] のように機械的に脅威レベルを判定できるようになることが期待できる。

以降、本稿では知見 1、知見 2 に従って隠蔽通信路の分類を行う。3 節では、知見 1 を元に隠蔽通信路の構築手法をネットワーク監視に対する回避攻撃の手法として捉えて分類を試みる。知見 2 に基づく分類に関しては、4 節にて通信モデルの類型による隠蔽通信路構築手法の分類を試みる。また、分類においては文献 [5,6] で紹介されている既知の隠蔽通信路構築手法を対象として実施したが、ページ数の関係から既知の隠蔽通信路構築手法の一部を例として挙げる。以降それぞれの分類に関して説明する。

3 ネットワーク監視に対する回避攻撃手法としての分類

本節では、隠蔽通信路構築手法をネットワーク監視に対する回避攻撃として捉えた分類を行う。表 1 は我々が分類した、ネットワーク監視に対する回避攻撃として捉えた隠蔽通信路の分類表である。ネットワーク監視に対する回避攻撃は大別して隠蔽、撹乱、死角の 3 種類である。本節では、文献 [5] で取り上げられている隠蔽通信路構築手法や先行研究 [6] で検討した隠蔽通信路構築手法を隠蔽型回避攻撃、撹乱型回避攻撃、死角型回避攻撃として分類する。

ここで、それぞれの回避攻撃手法は組み合わせて利用できることや、単一の隠蔽通信路構築手法が複数の分類指標に分類される可能性があることをあらかじめ明記しておく。また、表 1 には、既知の隠蔽通信路構築手法を例として挙げてある。

3.1 隠蔽型回避攻撃

隠蔽 **(concealment)** は監視技術で隠蔽通信路の検知や隠蔽情報の解読ができないように技術的に情報を隠蔽する事による、ネットワーク監視への回避攻撃手法である。一般的に隠蔽通信路の主目的が「情報を隠蔽して伝達すること」であるため全ての隠蔽通信路は隠蔽型回避攻撃に該当する。後述の撹乱型回避攻撃や死角型回避攻撃と区別する場合は「情報の隠蔽のみを行う隠蔽通信路」だけが隠蔽型回避攻撃に該当すると本稿では定義する。

隠蔽型回避攻撃に該当する隠蔽通信路構築手法としては、プロトコルヘッダへの埋め込みによるストレージチャネル [9]、変調を用いたストレージチャネル [9] およびタイミングチャネル [10]、ステガノグラフィ [11]、暗号化を用いた隠蔽通信路構築手法 [4] などが挙げられる。

3.2 撹乱型回避攻撃

撹乱 **(disturbance)** は隠蔽情報送信ノードおよび隠蔽情報受信ノードの特定を技術的に困難にすることによる、ネットワーク監視への回避攻撃手法である。撹乱型回避攻撃を用いた隠蔽通信路構築手法や、副次的に撹乱が発生する隠蔽通信路構築手法が撹乱型回避攻撃に該当する。

撹乱型回避攻撃に分類される隠蔽通信路構築手法には、結託中間ノードによって宛先アドレス、利用プロトコル、メッセージ、データフォーマットなどに変換を加える変換型、ICMP トンネルなどカプセル化技術を用いたカプセル化型 [12]、送信元アドレス詐称を利用した詐称型 [9]、経路ハイジャック [13] などを用いた乗っ取り型、DNS Tunneling [14] な

表 1: ネットワーク監視に対する回避攻撃手法としての隠蔽通信路の分類表

分類			例
ネットワーク監視に対する回避攻撃	隠蔽	ヘッダへの埋め込み	[9]
		変調	[9,10]
		ステガノグラフィ	[11]
		暗号化	[4]
	撹乱	変換	
		カプセル化	[12]
		詐称	[9]
		乗っ取り	[13]
		結託中間サーバ	[14]
		制御信号	[15]
		チャネル消去	[16]
		ジャミング	[17]
	死角	技術上の死角	
		運用上の死角	[18,19]
		法令上の死角	

どの結託中間サーバ型、ボットネット の Command and Control (C&C) メッセージ [15] など制御信号型、キャッシュとして残った隠蔽情報を消去するチャネル消去型 [16]、ダミーパケットによるフレーム衝突 [17] などのジャミング型が含まれる。

3.3 死角型回避攻撃

死角 **(dead angle)** は、技術上、運用上、法令上の制約から監視対象の死角となっている情報伝達手法を用いた、ネットワーク監視への回避攻撃手法である。死角型回避攻撃は技術上の死角型、運用上の死角型、法令上の死角型の 3 つに分類できる。

死角型回避攻撃は、管理対象のネットワークにおける死角を分析し、死角を解消することにより対策できる。しかしながら、ネットワークを構成する全ての機器やユーザの行動、管理者のミスなど分析項目が多いため、分析そのものが困難である事が多く、問題を緩和するために例外を設置すると、その例外が死角となることもある。また、死角を解消できる手法が金銭面や他の運用上、法律上の問題で実現不可能な場合もあり、対策が非常に難しい。

技術上の死角型となる隠蔽通信路としては、高画質ビデオストリーム転送や隠蔽情報の暗号化や暗号化プロトコルへの埋め込みを用いた隠蔽通信路など、ワイヤーレートでの検証が技術上困難なプロトコルが通常監視対象から外されやすいことを利用した隠蔽通信路構築手法がある。

運用上の死角型となる隠蔽通信路としては、上記のような技術上監視が困難なプロトコルや暗号化プロトコルが運用上監視対象から外されやすいことや、イントラネットのルータやファイヤウォールなどのセキュリティ製品が監視対象から外されやすいことを用いた隠蔽通信路構築手法がある [18,19]。また、運用者の技術不足や管理ミスからアクセス制御を施していないルータやサーバなどの中間ノードが乗っ取られ、隠蔽通信路を構築される場合も運用上の死角をついた回避攻撃と言える。

法令上の死角型となる隠蔽通信路としては、通信の秘密やプライバシ保護に対する法令が強い国においてパケットへの検閲 (deep packet inspection) が困難であることや国際法の整備の不備をついて、法制度の違う国外サーバを経由し追跡されにくい形式を採った隠蔽通信路などが考えられる。

4 通信モデルの分析による分類

次に、ネットワーク運用管理視点から対策手法を設置する個所を検討する際の指針とするために、通信モデルの詳細分析による隠蔽通信路の分類を行

う。先行研究 [6] で検討した分類指標を元に再検討したところ、網羅性を示す上での最初の分岐となる指標として指標 **1)** 隠蔽通信路と公然通信路の対称性、隠蔽通信路を構築するノードの役割や振る舞いに関する指標として指標 **2)** ノードのネットワーク上の位置、指標 **3**）送信ノードおよび受信ノードの数、指標 **4)** 結託中間ノードの振る舞い、具体的な隠蔽通信路構築手法への細分化の指標として指標 **5)** 隠蔽情報の転送手法、指標 **6**）隠蔽度合い、指標 **7**）具体的な情報隠蔽手法の 7 つの指標で大まかに特徴づけが行えることが分かった。表 2 は、指標 1 による特徴づけを第 1 階層とし、指標 2、指標 3、指標 4 による特徴づけを第 2 階層とし、指標 5、指標 6、指標 7 での特徴づけを第 3 階層として表わした場合の通信モデルによる隠蔽通信路の分類表になる。

ここで、周波数チャネルのように 1 対多や多対多通信を用いた隠蔽通信路は、基本的にはいくつかの隠蔽通信路の重ね合わせであり、細かく分割すると 1 対 1 通信もしくは 1 対多通信に集約できる、表 2 には細分化の例としては記載しない。

4.1 対称型隠蔽通信路 (SC)

隠蔽通信路は、隠蔽通信路と公然通信路がコインの裏表のように対称である対称型隠蔽通信路と、隠蔽通信路と公然通信路それぞれの送受信ノードの組が異なる非対称型隠蔽通信路に大別できる。

対称型隠蔽通信路は隠蔽通信路と公然通信路の送受信ノードの組が同一であり、公然通信路と隠蔽通信路の配送経路が全く同一である隠蔽通信路である。ここで、対称型隠蔽通信路を SC 型 (Symmetric Covert channel type) 隠蔽通信路と以降では記載する。SC 型隠蔽通信路では、隠蔽通信路と公然通信路の送受信ノードのネットワーク上の位置と結託中間ノードの介在の有無で強く特徴づけが行える。ネットワーク運用の観点から SC 型隠蔽通信路を細分化すると、エンドホスト間で構築される隠蔽通信路であるエンドホスト間対称型隠蔽通信路 (以降、SC-E 型と記載) とネットワーク機器を交えたネットワーク機器端点対称型隠蔽通信路 (以降、SC-N 型と記載) に分割できる。

SC-E 型隠蔽通信路はエッジネットワークの監視のみで対応できる。一方、SC-N 型隠蔽通信路はネットワーク機器に対する監視も行わなければならないため対策が難しくなるという特徴を持つ。しかしながら、送受信ノードの組や通信経路に変化が加わらないため、単純なパケット解析や異常検知で隠蔽通信路を特定できる可能性が高い。

4.1.1 エンドホスト間対称型隠蔽通信路 (SC-E)

SC-E 型隠蔽通信路は隠蔽通信路および公然通信路の送受信ノードが同一のエンドホストとなる隠蔽通信路である。SC-E 型は、単一の TCP/UDP 通信などを用いたエンドホスト間でのデータ転送である **SC-E-EE** 型と、DNS の再帰要求など複数の TCP/UDP 通信などで行われるリダイレクタを介した転送 **SC-E-RD** 型 の 2 種類に細分化できる。

4.1.2 ネットワーク機器端点対称型隠蔽通信路 (SC-N)

SC-N 型隠蔽通信路は隠蔽通信路および公然通信路の端点ノードにネットワーク機器が含まれる、対称型隠蔽通信路である。SC-N 型をさらに細分化すると、ネットワーク機器とエンドホスト間のデータ転送である **SC-N-NE** 型、ネットワーク機器間のデータ転送である **SC-N-NN** 型、SC-N-NE 型にリダイレクタが介在する **SC-N-RNE** 型および SC-N-NN 型にリダイレクタが介在する **SC-N-RNN** 型の 4 種類となる。

4.2 非対称型隠蔽通信路 (AC)

非対称型隠蔽通信路 (Asymmetric Covert channel type、以降 AC 型と記載) はその名の通り、SC 型隠蔽通信路の補集合に相当する隠蔽通信路である。AC 型隠蔽通信路では隠蔽通信路と公然通信路の送受信ノードの組が異なる可能性があり、公然通信路と隠蔽通信路の配送経路が異なる可能性がある。また、結託中間ノードが加わる場合が多いため、隠蔽通信路の存在を確認できても、その端点である隠蔽情報送信ノードおよび隠蔽情報受信ノードの特定が困難になる可能性が高い隠蔽通信路である。SC 型隠蔽通信路とは異なり、AC 型隠蔽通信路では隠蔽通信路と公然通信路を合成・分離する手法により強く特徴づけが行えるため、本稿では、非対称型隠蔽通信路の細分化における型名を合成・分離する手法により命名した。

4.2.1 傍受型 (AC-IC)

傍受型隠蔽通信路 (以降 AC-IC 型と記載) は公然情報送信ノードと隠蔽情報送信ノードは同一であると想定し、悪意のある中間ノード (Middleman) において傍受手法 (Interception) 利用し隠蔽情報を受信する隠蔽通信路である。AC-IC 型は、ルータでの tcpdump や物理的なワイヤータップによる傍受を用いた受信による隠蔽通信路である **AC-IC-TAP** 型、ウェブプロキシでの隠蔽情報の取得などプロキシによる傍受を用いた隠蔽情報の受信による隠蔽通信路である **AC-IC-PROXY** 型に細分化できる。

4.2.2 混入型 (AC-IJ)

混入型隠蔽通信路 (以降 AC-IJ 型と記載) は、悪意ある中間ノード (Middleman) が隠蔽情報送信ノードとなるか、結託中間者ノードによって、隠蔽情報受信者が受信している任意の公然通信路に隠蔽情報を埋め込む隠蔽通信路である。

AC-IJ 型は、悪意ある中間ノードによる隠蔽情報の混入による隠蔽通信路のタイプである **AC-IJ-IJ** 型、悪意ある中間ノードまたは結託中間ノードによる隠蔽情報の追記を用いた隠蔽通信路のタイプである **AC-IJ-AP** 型、最初の隠蔽情報の混入が隠蔽情報送信ノードではなく結託中間ノードとなる **AC-IJ-CI** 型、および AC-IJ-CI 型に他の結託中間ノードによる隠蔽情報の追記を交えた **AC-IJ-CA** 型に細分化できる。AC-IJ-IJ 型の例としては、ルータでの IPv4 ヘッダの IPID フィールドへの埋め込みを利用した隠蔽通信路 [22] がある。AC-IJ-AP 型の例としてはマーキング型 IP トレースバック方式 [23] を利用した隠蔽通信路を想定すればよい。AC-IJ-CI 型、AC-IJ-CA 型の例は特に報告されていない。

4.2.3 抽出削除型 (AC-EX)

AC-IJ 型とは反対に、悪意ある中間ノード (Middleman) が隠蔽情報受信ノードとなり、隠蔽情報送信者が公然通信路に埋め込んだ隠蔽情報を隠蔽情報受信ノードで抽出し削除するタイプの隠蔽通信路である。AC-EX 型の実装方法としてはルータ、プロキシなどネットワークノードによる抽出と削除が考えられるが、具体的な隠蔽通信路としての報告は筆者らが確認したところでは特になかったため、他の例とは異なり細分化は行わない。

4.2.4 中間者間通信型 (AC-MM)

中間者間通信型隠蔽通信路 (以降 AC-MM と記載) は、AC-IJ 型と AC-EX 型を組み合わせた、悪意ある中間ノードである隠蔽情報送信ノードにより公然通信路へ隠蔽情報を埋め込み、悪意ある中間ノードである隠蔽情報受信ノードにより隠蔽情報を公然通信路から抽出・削除する隠蔽通信路である。つまり、AC-MM 型隠蔽通信路は公然通信路の端点ノードと隠蔽通信路の端点ノードが異なることになる。また、AC-MM 型隠蔽通信路の配送経路は寄生した公然通信路の配送経路に含まれることになる。

AC-MM 型は、悪意ある中間ノード間の隠蔽情報の混入と抽出・削除である **AC-MM-MM** 型、結託中間ノードによる隠蔽情報の追記を含めた 悪意ある中間ノード間の隠蔽情報の混入と抽出・削除である **AC-MM-AP** 型 に細分化できる。AC-MM-MM 型の例は SSH の Message Authentication Code への埋め込みと削除を用いた中間者間隠蔽通信路 [19] を想定すればよい。AC-MM-AP 型は Gong らの AS 内マーキング型 IP トレースバック方式 [24] を悪用した隠蔽通信路を想定すればよい。

4.2.5 分岐 (AC-SP)

分岐型隠蔽通信路 (以降 AC-SP 型と記載) は公然情報送信ノードと隠蔽情報送信ノードは同一であると想定し、何らかの方法によって隠蔽通信路が含まれた公然通信路ごと分岐させるか、隠蔽情報を公然通信路から抽出して分岐させる隠蔽通信路である。AC-SP 型では隠蔽情報受信ノードと公然情報受信ノードが異なるものと定義する。ブロードキャストやマルチキャストなど複数配送先による分岐が生じていても隠蔽情報受信ノードと公然情報受信ノードが同一であれば SC 型であると本稿では定義する。

AC-SP 型は、複数配送先フレーム・パケットを用いた公然通信路による分岐を用いた隠蔽通信路である **AC-SP-MA** 型、複数配送先メッセージを用いた公然通信路による分岐を用いた隠蔽通信路である **AC-SP-MM** 型、結託中間ノードによる公然通信路の複製を用いた分岐を用いた隠蔽通信路である **AC-SP-CC** 型、結託中間ノードによるフローサンプリングを用いた隠蔽情報の分岐を用いた隠蔽通信

路である **AC-SP-FS** 型、結託中間ノードでの傍受を用いた隠蔽情報の収集と分岐を用いた隠蔽通信路である **AC-SP-IC** 型、結託中間ノードでの隠蔽情報の貯蓄と隠蔽情報受信ノードによる回収を行う隠蔽通信路である **AC-SP-SF** 型に細分化できる。

AC-SP-MA 型の例は IP ブロードキャストや IP マルチキャストを用いた隠蔽通信路を想定すればよく、AC-SP-MM 型の例はメーリングリストを用いた隠蔽通信路を想定すればよい。AC-SP-CC 型の例はプロキシや P2P ネットワークでのメッセージ複製を想定すればよい。AC-SP-FS 型の例は、sFlow や NetFlow などのフローサンプリングに含まれるフィールドに情報を埋め込んだ隠蔽通信路を隠蔽情報送信ノードは構築することになる。AC-SP-IC 型は lawful interception 機能の悪用 [25] を想定すればよい。AC-SP-SF 型はステガノグラフィを用いた隠蔽情報を結託サーバで抽出して、後日隠蔽情報受信ノードがダウンロードで回収するという情報漏洩手法を想定すればよい。

4.2.6 混入分岐複合型 (AC-CO)

混入分岐複合型隠蔽通信路 (以降 AC-CO と記載) は、悪意ある中間ノードである隠蔽情報送信ノードが任意の公然通信路に隠蔽情報を埋め込み、結託中間ノードで分岐または抽出・消去を行って、任意の隠蔽情報受信ノードに隠蔽情報を配送する隠蔽通信路である。AC-CO 型隠蔽通信路は公然通信路の端点ノードと隠蔽通信路の端点ノードが異なることになる。また、AC-CO 型隠蔽通信路の配送経路は寄生した公然通信路の配送経路とは異なる。

AC-CO 型は、悪意ある中間ノードによる複数配送先フレーム・パケットへの混入による分岐を用いた隠蔽通信路である **AC-CO-MA** 型、悪意ある中間ノードによる複数配送先メッセージへの混入による分岐を利用した隠蔽通信路である **AC-CO-MM** 型、悪意ある中間ノードによる混入と結託中間ノードによる複製による分岐を用いた隠蔽通信路である **AC-CO-CC** 型、悪意ある中間ノードによる混入と結託中間ノードによる抽出・削除・再配送による分岐を行う隠蔽通信路である **AC-CO-EX** 型、結託中間ノードによる混入と結託中間ノードによる抽出・削除・再配送による分岐が発生する **AC-CO-DB** 型 に細分化できる。

AC-CO-MA 型の例はルータでの IP ブロードキャスト、IP マルチキャストアドレスを持ったパケットへの埋め込みによる隠蔽通信路を想定すればよい。AC-CO-MM 型の例はメールサーバによるメーリングリストへの埋め込みを用いた隠蔽通信路を想定すればよい。AC-CO-CC 型の例は悪意ある中間ノードで任意のパケットに埋め込み、結託中間ノードでブロードキャストアドレスに変更して配送するなどの隠蔽通信路を想定すればよい。AC-CO-EX 型の例は悪意ある中間ノードで任意のパケットに埋め込みを行う AC-SP-SF 型隠蔽通信路を想定すればよい。

4.2.7 ハイジャック型 (AC-HJ)

ハイジャック型隠蔽通信路 (以降 AC-HJ と記載) は、公然通信路の中に隠蔽するのではなく、アドレスハイジャックや経路ハイジャックなどを用いて、公然通信路の送受信ノードの組になりすまし、隠蔽情報送受信ノード間でデータをやり取りする隠蔽通信路である。AC-HJ 型は隠蔽通信路を検知した際に隠蔽情報送受信ノードの特定が困難となる特徴を持つため、ネットワーク運用管理上対策が難しい隠蔽通信路である。

AC-HJ 型は、スパムメールなどによく用いられる経路ハイジャックを用いたなりすましである **AC-HJ-RH** 型、送信元アドレス詐称などアドレスハイジャックを用いたなりすましである **AC-HJ-AH** 型に細分化できる。

4.2.8 配送経路分岐型 (AC-DP)

実用上、非常に考えにくいケースではあるが、形式的には結託中間ノード間で隠蔽情報と公然情報を分離し、別の経路で配送して、再び結託中間ノード間で合成して隠蔽情報受信ノードに配送する配送経路分岐型 (以降、AC-DP と記載) が考えられる。

5 考察とまとめ

本稿では、文献 [5] で課題として指摘されていた、隠蔽通信路に関する包括的な分類を作成するため、ネットワーク運用管理の視点から 2 種類のアプローチによって分類を試みた。具体的には、ネットワーク運用管理における対策の難易度も考察しながら、3 節で、一般的なネットワーク監視に対する回避攻

撃と同等に扱うことを目的とした隠蔽通信路の分類を実施し、4 節にて包括的な対策手法の検討の際の指針とすることを目的に通信モデルによる隠蔽通信路の分類を実施した。

分類における網羅性に関しては、3 節でのネットワーク監視に対する回避攻撃の分類に当てはめているので回避攻撃の分類の網羅性に依存している。一方、4 節での通信モデルによる分類に関しては、第一階層の分岐で排他的な分類を示しているため網羅性は確保しており、細分化に関しては第 2 階層、第 3 階層で隠蔽通信路として認識された際に追加するか、型名の組み換えを行えばよい構造となっている。

今後の課題として、本稿で作成した隠蔽通信路構築手法の分類と同じように隠蔽通信路対策手法の包括的な分類を行い、様々なネットワーク運用のシナリオにおける隠蔽通信路構築と隠蔽通信路対策の間のコスト比較を行い、脅威の大きさの分析を行う。

謝辞

本研究は、独立行政法人情報通信研究機構 (NICT) による委託研究「通信プロトコルとその実装の安全性評価に関する研究開発」の一部である。

参考文献

[1] C. G. Girling. Covert channels in lan's. *IEEE Transactions on Software Engineering*, Vol. 13, pp. 292–296, Feb. 1987.

[2] B. W. Lampson. A note on the confinement problem. *Communication of the ACM*, Vol. 16, No. 10, pp. 613–615, Oct. 1973.

[3] T. G. Handel et. al. Hiding Data in the OSI Network Model. In *Proceedings of IH 1996*, pp. 23–38, 1996.

[4] S. J. Murdoch et. al. Embedding Covert Channels into TCP/IP. In *Proceedings of IH 2005*, June 2005.

[5] S. Zander et. al. A Survey of Covert Channels and Countermeasures in Computer Network Protocols. *IEEE Communications Surveys and Tutorials*, Vol. 9, pp. 44–57, Oct. 2007.

[6] 室田朋樹ら. インターネットにおける隠蔽通信路の可能性とその検証についての一考察. 電子情報通信学会技術研究報告, ICSS2010, Vol. 110, No. 475, pp. 23–28, 2011 年 3 月.

[7] R. A. Kemmerer. A Practical Approach to Identifying Storage and Timing Channels. In *Proceedings of IEEE Symposium on Security and Privacy (SAP 1982)*, Apr. 1982.

[8] Common Vulnerability Scoring System (CVSS-SIG). `http://www.first.org/cvss/`.

[9] N. B. Lucena et. al. Covert Channels in IPv6. In *Proceedings of PET 2005*, pp. 147–166, May 2005.

[10] S. J. Murdoch. Hot or Not: Revealing Hidden Services by Their Clock Skew. In *Proceedings of ACM CCS 2006*, pp. 27–36, Nov. 2006.

[11] L. Bowyer. Firewall Bypass via Protocol Steganography, Sept. 2002. `http://www.networkpenetration.com/protocol_steg.html`.

[12] D. Stødle. Ping Tunnel. `http://www.cs.uit.no/~daniels/PingTunnel/`.

[13] T. Mizuguchi. Inter-Domain Routing Security - Route Hijacking -, Mar. 2007. APRITCOT 2007 Presentation.

[14] D. Kaminsky. Ip-over-dns using ozyman, 2004. `http://www.doxpara.com/`.

[15] P. Bächer et. al. Know your Enemy: Tracking Botnets, Aug. 2008. Technical Report `http://www.honeynet.org/papers/bots`.

[16] Y. Ohara and A. Kato. Consideration on OSPF LSDB Monitoring, Jul. 2011. individual draft.

[17] T. M. Dogu et. al. Covert Information Transmission through the Use of Standard Collision Resolution Algorithms. In *Proceedings of IH 1999*, pp. 419–433, Sept. 1999.

[18] D. Kundur et. al. Practical Internet Steganography: Data Hiding in IP. In *Proceedings of TWSIS 2003*, Apr. 2003.

[19] N. Lucena et. al. Syntax and Semantics-Preserving Application-Layer Protocol Steganography. In *Proceedings of IH2004*, May 2004.

[20] A. Dyatlov et. al. Exploitation of Data Streams Authorized by a Network Access Control System for Arbitrary Data Transfers: Tunneling and Covert Channels over the HTTP Protocol, Jan. 2005. Technical report.

[21] M. Bauer. New Covert Channels in HTTP: Adding Unwitting Web Browsers to Anonymity Sets. In *Proceedings of PES 2003*, pp. 72–78, Oct. 2003.

[22] E. Cauich et. al. Data Hiding in Identification and Offset IP Fields. In *Proceedings of ISSADS 2005*, pp. 118–125, Jan. 2005.

[23] S. Savage et. al. Networksupport for IP traceback. In *Proceedings of ACM SIGCOMM 2000*, pp. 295–306, Aug. 2000.

[24] C. Gong et. al. Toward a practical packet marking approach for ip traceback. *International Journal of Network Security*, Vol. 8, No. 3, pp. 271–281, 2009.

[25] T. Cross. Unauthorized Internet Wiretapping: Exploiting lawful intercept. In *Black Hat USA 2010*, July 2010.

表 2: 通信モデルによる隠蔽通信路の分類

	分類			例
	対称性	ノードの役割、振る舞い	データ転送手法、隠蔽度合い、隠蔽手法	
公然通信路と隠蔽通信路の関係	対称型 (SC)	エンドホスト間対称型 (SC-E)	エンドホスト間のデータ転送 (SC-E-EE)	[20]
			リダイレクタを介した転送 (SC-E-RD)	[21]
		ネットワーク機器端点対称型 (SC-N)	ネットワーク機器とエンドホスト間のデータ転送 (SC-N-NE)	
			ネットワーク機器間のデータ転送 (SC-N-NN)	
			リダイレクタを介したネットワーク機器とエンドホスト間の転送 (SC-N-RNE)	
			リダイレクタを介したネットワーク機器間の転送 (SC-N-RNN)	
	非対称型 (AC)	傍受型 (AC-IC)	タップ (AC-IC-TAP)	
			プロキシ (AC-IC-PROXY)	
		混入型 (AC-IJ)	悪意ある中間者による混入 (AC-IJ-IJ)	[22]
			悪意ある中間者による混入と追記 (AC-IJ-AP)	[23]
			結託中間ノードによる混入 (AC-IJ-CI)	
			結託中間ノードによる混入と追記 (AC-IJ-CA)	
		抽出削除型 (AC-EX)		
		中間者間通信型 (AC-MM)	中間者間通信 (AC-MM-MM)	[19]
			追記を含めた中間者間通信 (AC-MM-AP)	[24]
		分岐型 (AC-SP)	複数配送フレーム・パケットによる分岐 (AC-SP-MA)	
			複数配送メッセージによる分岐 (AC-SP-MM)	
			結託中間ノードによる複製 (AC-SP-SS)	
			フローサンプリング (AC-SP-FS)	
			タップ (AC-SP-TAP)	[25]
			結託中間ノードへの貯蓄と回収 (AC-SP-SF)	
		混入分岐複合型 (AC-CO)	複数配送先フレーム・パケットへの混入 (AC-CO-MA)	
			複数配送先メッセージへの混入 (AC-CO-MS)	
			結託中間ノードによる分岐 (AC-CO-CC)	
			結託中間ノードによる抽出・削除・再配送 (AC-CO-EX)	
			結託中間ノードによる混入と抽出・削除・再配送 (AC-CO-DB)	
		ハイジャック型 (AC-HJ)	経路ハイジャックによる隠蔽 (AC-HJ-RH)	
			アドレスハイジャックによる隠蔽 (AC-HJ-AH)	
		配送分岐型 (AC-DF)		