Intrusion Trap Systemにおける安全で有効なログ収集のための動的切替え機能の実装

竹森敬祐[†] 力武健次[†]
三宅優[†] 中尾康二[†]

侵入者をおとりシステムへ強制的に切り替えてその行動の監視を行い，攻撃手法の分析や追跡をするプラットホームとして Internet Trap が注目されている．しかし，継続中の TCP コネクションを切り替えることができないために，正規システムを攻撃されかねないという問題がある．本論文では，侵入検知システム（IDS：Intrusion Detection System）を利用して，不審な挙動を知らせるトリガをきっかけに，TCP コネクションの開始時点のみならず継続中の TCP コネクションについても，正規システムからおとりシステムへと迅速に切り替える手法を提案する．以後，正規システムの安全を確保しつつ侵入者の行動ログを収集する本切替え機能を持つシステムを Intrusion Trap System（ITS）と呼ぶこととする．ITS は，正規システムとおとりシステムの通信状態の同期を図っておくことで，切替え時の通信シナリオを継続させることができ，自然な切替え動作は有効なログ収集を可能にする．本切替え機能は，TCP コネクションで提供される様々なアプリケーションサービスに適用できるが，本論文では FTP ならびに HTTP サービスへ適用したときの実装および評価を行い，侵入者に気付かれないレベルの高速な切替えを実現していることを確認する．

Implementation of Dynamic Diversion Mechanisms for Secure and Effective Logging on Intrusion Trap System

Keisuke Takemori,[†] Kenji Rikitake,[†] Yutaka Miyake[†] and Koji Nakao[†]

Internet Trap has been known as a notable platform to find out characteristics and an origin of intruders by recording the suspicious activities. However, it cannot divert a suspicious TCP connection to a trap system after the detection of suspiciousness even in the middle of TCP connections. Therefore, it may not be a perfect solution to protect a real system against malicious activities. In this paper, we propose advanced diversion mechanisms which can divert the suspicious TCP connections from a real to a trap system by using a trigger of Intrusion Detection System (IDS). The system is called Intrusion Trap System (ITS), which has the mechanisms for protecting a real system. Furthermore, the mechanisms provide synchronous connection flow management between connections with a real and a trap system so as for effective Logging. The diversion mechanisms are a general concept which is applicable to various types of application service. We implement ITS which applied for FTP and HTTP services, and evaluate performance of latency. As a result, ITS achieves high performance, we recognize that intruders hardly notice the existence of our system.

1. はじめに

ネットワークシステムを構成する機器には，日々セキュリティホールが報告されており，これらを狙った侵入者による攻撃やインターネットワーム[1]による攻撃など，侵入に対する脅威が拡大している[2]．一般的な防御システムとして，ファイアウォールや IDS[3)~6)]などがあるが，ファイアウォールの場合，通過を許可された通信により引き起こされる攻撃を防げないことや，IDS の場合，シグネチャ情報を持たない未知の攻撃やサイト独自のアプリケーションに対する攻撃を検知することができないという課題が存在する．

これら日々多様化する攻撃手法の把握は，セキュリティ確保の面で重要である．近年，侵入手法やツールさらには侵入者の意図などを分析するためのプラットホームとして，脆弱性を持つおとりのシステムを利用した Honeypot[5),6)] と呼ばれる手法が注目を集めている．本手法を適用した Honeynet Project[7)] では，インターネット上の各所におとりのシステムを設置して

† KDDI 研究所
KDDI R&D Laboratories Inc.

監視を行い，一般にみられる攻撃手法の分析を進めている．しかしながら，おびき寄せることを前提としたHoneypotは，サービスを提供しているシステム自体を防御するものではないため，IPアドレスをランダムに選択して攻撃してくる侵入者やインターネットワームから本来のシステムを守ることができない．また，おとりを用いることでおびき寄せによる犯罪の誘発に関する危惧など，その適用性について議論がやまない．

これに対して，IDSでトラヒックを監視しておき，疑わしい行為が検知されたIPアドレスからのアクセス先を，正規システムからおとりシステムへ強制的に切り替えるInternet Trap[5),8)~10)]が提案されている．これは，Honeypotで達成できる機能に加え，正規システムを防御できる点や，犯罪の予兆が検知されたアクセスを対象に切り替えるため，犯罪の誘発につながらない点で有効である．また，おとりとして正規システム上の重要なデータ以外のデータや各種設定情報をミラーリングしたシステムを用意することで，サイト独自のアプリケーションに対する攻撃についても収集できるプラットホームとなる．しかし，これまで提案，開発されてきたInternet Trap[8)~10)]の切替えはTCPコネクションの開始時点のみに行われるため，疑わしい行為が検知されたTCPコネクションが継続される限り，正規システムに攻撃が加えられる恐れがある．また，侵入者の行動ログをおとりシステム上で収集するため，これを改竄，消去されかねない問題も残っている．

そこで著者らは，TCPコネクションの開始時点のみならず継続中のTCPコネクションについても，IDSからの不審な挙動を知らせるトリガをきっかけにただちにおとりへと切り替えることで，正規システムを守りつつ情報収集を行えるITSについて，

(1) 1つのホスト上に正規領域とおとり領域を設ける手法，
(2) 正規ホストと独立した外部おとりホストを設ける手法，

の2つの設計手法を提案してきた[11)]．これら2つのITSは，継続中のTCPコネクションを切り替えるときに通信シナリオに矛盾が生じないように，正規領域（正規ホスト）とおとり領域（おとりホスト）の通信状態の同期を図る機能を設けており，機能面から継続的なサービスを提供するTCPコネクション管理を行っている．本論文では，正規ホストをそのまま利用できる(2)のITSモデルに注目し，FTPとHTTPサービスに適用するときの切替え機能の設計および実装を行う．そして処理性能に関する測定を行い，本切替え機能を適用した場合でも本来のサービスに与える影響を小さく抑えることができ，切替えも迅速に行われることを確認する．ITSは，TCPコネクションで提供される様々なアプリケーションサービスに適用できるため，サイト上で侵入者の行動を分析するためのプラットホームとして広く利用されることが期待される．

以降，2章では既存のInternet Trapの概要とその問題点について述べ，ITSに必要とされる機能をまとめる．3章でITSの全体構成を示して，本論文で実装する諸機能の位置付けを説明する．4章において中心的な役割を果たす切替え機能について説明し，5章でFTPとHTTPサービスに適用する場合のITSを構成する各モジュールの設計を行う．6章で処理性能に関する評価を行い，そして最後に7章でまとめる．

2. 既存システムの概要と問題点

2.1 既存の Internet Trap の概要

Internet Trapは，正規の利用者のみならず侵入者にもサービスを提供するシステムである．ただし侵入者に対しては正規システムに見せかけたおとりシステムからサービスが提供される．このサービス中に収集された侵入者の行動ログを分析することで，システムへの侵入手法や利用ツール，サイト上の脆弱性，侵入目的などを把握でき，ファイアウォールやIDS，その他の機器の設定を見直すことができるようになる．また，おとりシステムに接続させることで，追跡のための時間稼ぎが可能になる．

図1に，既存のInternet Trap[8)~10)]のシステム構成を示す．Internet Trapは，侵入検知部，侵入者リスト，アクセス制御部，正規システム，おとりシステムの5つのモジュールから構成される．アクセス制御部は，クライアントからアクセス要求を受け取ると，侵入検知部からの報告が記録されている侵入者リストを参照し，もし記録があればそのアクセス先をおとりシステムへと切り替える．このときの侵入者からの攻撃は，おとりシステムへ加えられるため，正規システムは守られる．

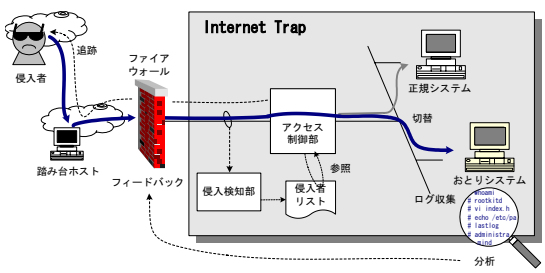

図1 既存の Internet Trap の構成
Fig. 1 Configuration of current Internet Trap.

2.2 問 題 点

既存の Internet Trap は，TCP コネクションの開始時点で切替えを行っており，不正が検知された後の TCP コネクションから切り替えられる．もし，不正の検知された TCP コネクションが継続されれば，正規システムに接続されたままになり攻撃を受けてしまう可能性がある．既存の Internet Trap では，クライアントからの TCP コネクションはアクセス制御部を経由して，正規システムで終端されている．このため，通信中の TCP コネクションを継続したまま正規システムからおとりシステムへと切り替えることは，TCP のシーケンス処理上の不整合が発生するため，不可能である．

既存の Internet Trap で継続中の TCP コネクションからの攻撃を防ぐには，TCP コネクションをいったん切断して再接続を促すことになり，このとき侵入者に逃げられてしまうことも考えられる．たとえ再接続に来たとしても，切替えまでに行われた正規システムへの行為を，おとりシステムへ反映させる機能はなく，切替え時の通信シナリオに矛盾が生じる．

ここで通信シナリオの矛盾とは，TCP コネクションにより提供されるサービスを例に説明すると，正規システムへの TCP コネクション上で行ったログイン処理やディレクトリ間の移動，ファイルの生成，変更，削除などの作業の結果が，おとりシステムに反映されていないことである．このように既存の Internet Trap では，TCP コネクションを切断したり通信シナリオに矛盾が生じたりすることで，侵入者に切替え機構の存在に気付かれてしまう可能性が高く，情報収集を円滑に行うことができない．

その他，侵入者のログはおとりシステム上で収集されるため，侵入者がおとりシステムの管理者権限の取得に成功してログの改竄や削除を行った場合，収集した情報が信頼できないものになる．

2.3 必要とされる機能

正規システムを保護しながら情報収集を円滑に行うためには，不正が検知されると TCP コネクションの途中であっても TCP コネクションを継続したままおとりシステムへと切り替える機能が必要である．このとき，切替え前後で通信シナリオの継続性を保つ機能も必要になる．また，一連の切替え処理は迅速に行われなければならない．その他，行動ログはおとりシステム以外でも収集すべきである．

3. 提案システムの概要

図 2 に，TCP コネクションの動的切替機能を持った ITS のシステム構成を示す．

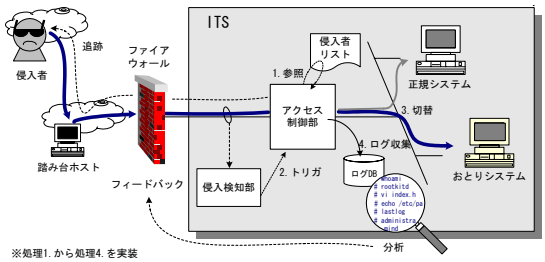

図 2 提案する ITS の構成
Fig. 2 Configuration of proposed ITS.

ITS の目的は，
目的 1. 正規システムの安全確保
目的 2. 収集した行動ログの活用
であり，本論文では，目的 1. の安全確保と，目的 2. の前段階となる有効なログ収集を達成するために，侵入者の TCP コネクションを開始時点のみならず継続中にも，おとりシステムへと切り替える手法として，図 2 の処理 1. から処理 4. までの機能を提案・実装する．

ここで有効なログを収集するためには，切替え前後において侵入者に継続的なサービスを提供することが重要である．継続的なサービスは，

- 攻撃中のログを収集できること
- 多くの侵入者をおとりシステムにつなぎ止めること

などが期待され，注意深い侵入者に切替え後のある時点で逃げられてしまった場合でも，それまでの行動ログを収集できるようになる．

ITS は，既存の Internet Trap が持つ各処理部と正規・おとりシステムに加え，おとりシステム上のログへの攻撃対策としてアクセス制御部に侵入者の通信記録を管理するログ DB を設置する．以後の章において，切替え機能と各処理部の詳細を説明する．

4. 切替え手法

4.1 静的切替えと動的切替え

本論文で提案する ITS は，侵入者の TCP コネクションを正規システムからおとりシステムへと切り替える手法として，静的切替えと動的切替えの 2 つの機能を持つ．静的切替えは，TCP コネクションの開始時点で切り替える手法であり，既存の Internet Trap が持つ唯一の切替え手法である．動的切替えは，侵入検知部で不審な挙動が検知されるとただちに継続中の TCP コネクションを切り替える手法である．このとき切替えには，通信シナリオの継続性とその処理の迅

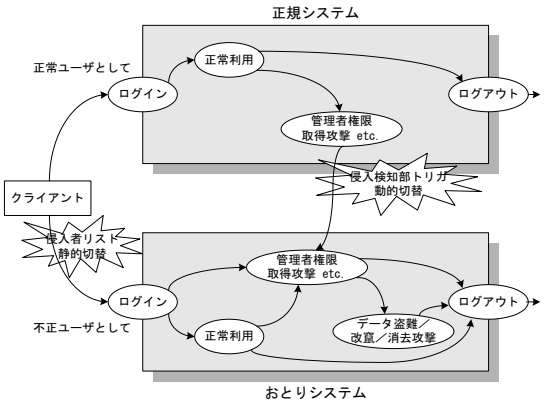

図 3 静的切替えと動的切替え
Fig. 3 Static diversion and dynamic diversion.

速性が要求される．

図 3 に，TCP コネクションにより提供されるサービスを例に切替えの様子を示す．

過去に不審な挙動が検知されていないユーザが接続しにきた場合，正規システムへログインする．その後，正常利用していた途中で管理者権限の取得攻撃などを試みた場合，侵入検知部がそれを検知してトリガを発行し，おとりシステムへと強制的に切り替える．切替え時には，正規システムとおとりシステム間の通信シナリオの同期を図っておくことで，ログイン処理や作業ディレクトリの移動などの処理は必要ない．このため，多くの侵入者は切り替えられたことに気付くことなく，データの盗難，改竄，消去など，おとりシステム上で様々な攻撃へと発展していく．

過去に不審な挙動のみられたクライアントの場合は，ログイン時点からおとりシステムへ切り替える．

初めの 1 つ目のパケットから未知の攻撃を仕掛けてくる侵入者については，提案する ITS は正規システムを守ることができない．しかし，手動による侵入者やインターネットワームの多くは，事前にターゲットホストを探すことが多く，IP スイープや Port スキャンなどの予兆が検知されるため，静的切替えが可能になる．

UDP プロトコルについては，TCP におけるコネクションの概念がないため，静的切替えのみ適用される．

4.2 動的切替えの詳細

切替えはアクセス制御部が主体となって行う．クライアントとアクセス制御部，アクセス制御部と正規システム，アクセス制御部とおとりシステムは，3 つの別々の TCP コネクションが張られており，アクセス制御部はアプリケーションレベルのデータ中継のみを行っている．正規システムからおとりシステムへと切り替えるときには，クライアントとアクセス制御部間の TCP コネクションは継続されたままであり，アクセス制御部と正規システム間の TCP シーケンス番号と，アクセス制御部とおとりシステム間の TCP シーケンス番号の違いを気にすることなく切替えを行うことができる．

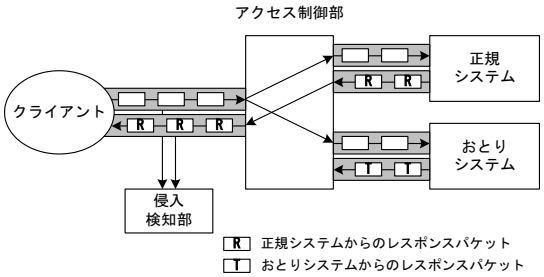

図 4 トリガ受信前の TCP コネクション状態—非切替えモード
Fig. 4 TCP connections before receiving a trigger — non-intrusive mode.

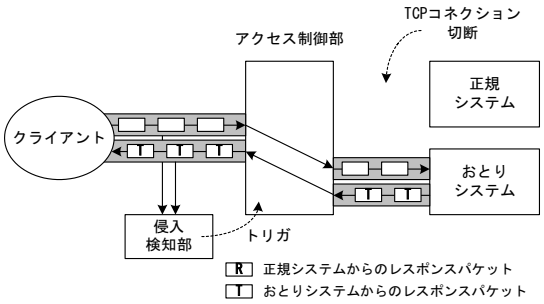

図 5 トリガ受信後の TCP コネクション状態—切替えモード
Fig. 5 TCP connections after receiving a trigger — intrusive mode.

図 4 に，動的切替え前の TCP コネクションの様子を示す．アクセス制御部は，クライアントからのリクエストパケットを正規システムとおとりシステムの両方へ同時に中継する．ただしクライアントへの応答は，両方のサーバからレスポンスパケットを受信するタイミングで，正規サーバから受信したものをクライアントへ返信する．これにより，正規システムとおとりシステム間の通信シナリオの同期を図っている．

図 5 に，侵入検知部において不審な挙動を検知してトリガが発行されたときの TCP コネクションの様子を示す．アクセス制御部が危険を知らせるトリガを受け取ると，ただちに正規システムとの TCP コネクションを切断する．以後のクライアントとの通信はおとりシステムとの間で行われる．このように，アクセス制御部とおとりシステム間の TCP コネクションをあらかじめ起動して正規システムと同じ通信を行っておくことで，切替え時の通信シナリオの継続性を保つ

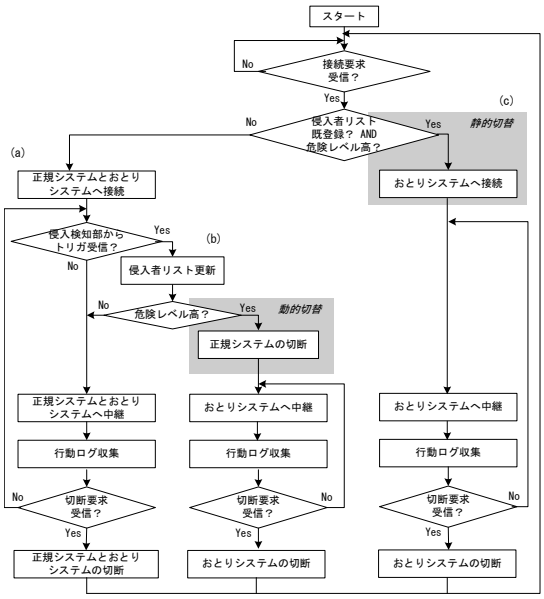

図 6 アクセス制御部の処理フロー
Fig. 6 Process flow on Access Controller.

ことができるとともに，切替えを迅速に行うことができる．

4.3 アクセス制御部の処理フロー

侵入者リストによる静的切替えと侵入検知部からのトリガによる動的切替えを行うアクセス制御部の処理フローを**図 6** に示す．アクセス制御部の処理は，クライアントの性質により大きく 3 つに分けられる．

(a) クライアントがつねに正常なアクセスを行う場合

アクセス制御部は，クライアントから接続要求を受信すると，まず侵入者リストを確認する．ここで過去に不審な行為がないかもしくはあらかじめ設定されている危険レベルよりも低いことが判明すると，TCP コネクションを正規システムとおとりシステムの両方へ確立し，行動ログを収集する．

(b) クライアントが通信中に不正を行った場合

(a) の状態で，通信中に侵入検知部からトリガを受け取ると，トリガ情報を基に侵入者リストを更新する．そして，トリガの危険レベルを確認して，あらかじめ設定されている危険レベルよりも高い場合には，正規システムとの TCP コネクションを切断する．以後の TCP コネクションはおとりシステムとのみ確立され，行動ログを収集する．

(c) あらかじめクライアントが侵入者リストに登録されている場合

もし通信の開始時点で侵入者リストに IP アドレスが記録されていて，かつあらかじめ設定されている危険レベルよりも高い場合には，TCP コネクションをおとりシステムとのみ確立し，行動ログを収集する．

アクセス制御部は，上記 3 つのケースのすべてにおいて TCP コネクションの切断要求を受け取ると，クライアントとそれぞれのシステム間の TCP コネクションを終了する．

4.4 通信シナリオの継続性における課題

ITS の切替え機能は，正規システムの安全を確保しつつ，できる限り多くの侵入者をできる限り長い時間，おとりシステムにつなぎ止めることで，有効な行動ログを収集することを目的としている．そのためにも，正規システムとおとりシステムの双方が提供するサービスに違いが出ないように，切替え前後において正規システムとおとりシステムの状態を可能な限り一致させている．このことは，悪意のないクライアントが誤検知によりおとりサーバに切り替えられた場合でも，サービスを受けることを可能にしている．

しかし，両システムの状態を完全に一致させることは不可能である．ここでは，本論文でのシステム状態の整合性は，切替え前後において再ログインやディレクトリの移動が不要なことなど，継続的なサービス提供を可能にするレベルの整合性までを目標とし，プロセス制御やファイル管理などの非決定的要素により，排除しきれない状態の不整合については今後の課題として以下に列挙しておく．

4.4.1 プロセス・メモリの不整合

初期状態において，おとりシステムの OS やファイルを正規システムと同じものを用意していた場合でも，プロセス ID，メモリ使用状況において差異が生じる．ここで，本切替え機能を telnet サービスに適用した場合，注意深い侵入者が，正規システムからおとりシステムへと切り替えられる前後において ps コマンドなどを用いることで，システム状態の不整合に気付く可能性がある．

4.4.2 ファイルの不整合

一時的に生成されるファイルの名前には乱数的な要素があるため，正規システムとおとりシステムでこれらのファイル名の同期を図ることはできず，ファイル状態の不整合に気付く可能性がある．

4.4.3 IP アドレスの不整合

正規システムとおとりシステムには，アクセス制御部と通信を行うために別々の IP アドレスが付与されている．ここで，本切替え機能を telnet サービスに適用した場合，注意深い侵入者が，正規システムからおとりシステムへと切り替えられる前後において ifconfig

コマンドを用いることで，IP アドレスの不整合に気付く可能性がある．

4.4.4 アクセス元 IP アドレスの違いによる改竄ファイルの不整合

ある IP アドレスからアクセスしてくる侵入者が，おとりシステムへと切り替えられておとりシステム内のファイルを改竄した後に，確認のために別の IP アドレスからアクセスしてきた場合，ファイルの不整合に気付くことになる．

5. 構成機器の設計

動的切替えは，各種 TCP コネクションにより提供されるサービスに適用できる切替え機能である．ここでは ISP が提供している代表的なサービスとして，複数のユーザが Web サーバ上のコンテンツを FTP でメインテナンスするシステムを例として，各モジュールの具体的な設計について述べる．

5.1 侵入検知部

侵入検知部は**図 7** に示すように，IDS，IDS が出力するアラートログ，侵入者リスト，トリガモジュールから構成される．

IDS として Snort[3] を利用した場合，Snort のアラートログには侵入者の IP アドレス，検知日時，攻撃名，危険レベルなどが記録される．**表 1** に侵入者リストを示す．これは，トリガ発行の制御に利用するものであり，検知された IP アドレス，その IP アドレスが初めて検知されたときの危険レベルと日時，その IP アドレスにおける過去最高危険レベルと検知日時を記録する．危険レベルについては，利用する IDS により異なるため，あらかじめ IDS が出力する危険レベルと侵入者リストへ記録する危険レベルの対応表を作っておく．

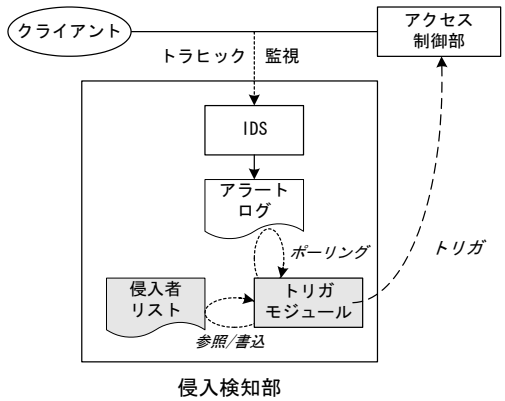

図 7 侵入検知部の設計
Fig. 7 Design of Intrusion Detector.

表 1 侵入者リスト
Table 1 Intruder list.

侵入者	最大危険		初回危険	
IPアドレス	レベル	検知日時	レベル	検知日時
192.168.0.10	中	2002.11.17-10:23:43	中	2002.11.17-10:23:43
192.168.2.23	高	2002.11.20-01:34:52	中	2002.11.18-10:51:38
192.168.10.20	低	2002.11.21-04:45:01	低	2002.11.21-04:45:01
192.168.32.8	中	2002.11.21-13:45:01	低	2002.11.21-12:57:29
…	…	…	…	…

侵入検知部は，クライアントとアクセス制御部の間でトラヒックを監視しており，IDS が攻撃を検知すると，アラートログへ各種情報を出力する．トリガモジュールは，アラートログをポーリング監視しており，新たなログが出力された場合には，その IP アドレスが以前に記録されていないか，もしくは，危険レベルが以前に検知されたレベルよりも高いかについて，侵入者リストに問い合わせる．初めての IP アドレス，もしくはより高い危険レベルの IP アドレスの場合には，アクセス制御システムへトリガを発行するとともに，侵入者リストを更新する．トリガの内容は，IP アドレス，危険レベル，検知日時であり，アクセス制御部の侵入者リストを更新するための差分データとなる．

5.2 アクセス制御部

アクセス制御部は，クライアントとサーバ間に設置する．**図 8** に，FTP ならびに HTTP サービスを中継するアクセス制御部の構成を示す．アクセス制御部は，中継モジュール制御デーモン，FTP ならびに HTTP 中継モジュール，侵入検知部のものと同じフォーマットを持つ侵入者リスト，ログ収集モジュールから構成される．

中継モジュール制御デーモンは，クライアントからの接続要求を一括して受け付ける．ここで，クライアントからの接続要求が FTP の場合には FTP 中継モジュールに，HTTP の場合には HTTP 中継モジュー

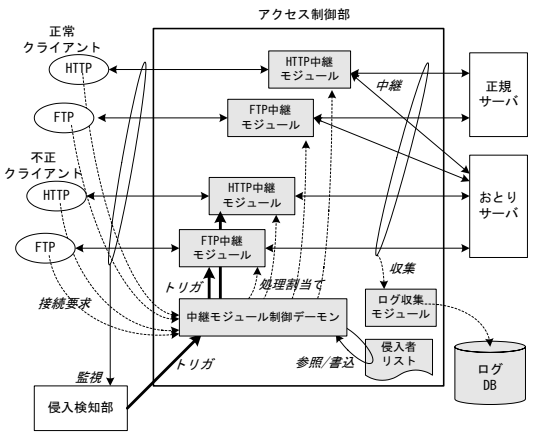

図 8 アクセス制御部の設計
Fig. 8 Design of Access Controller.

ルに，それぞれ正常もしくは不正クライアントとしての中継処理の指示を行う．FTP もしくは HTTP 中継モジュールは，各プロトコルを理解して制御を行うプロキシとして実現する．ここで，クライアントからの接続要求を迅速に処理するために，各中継モジュールは中継モジュール制御デーモンのスレッドとして，あらかじめ起動しておく．たとえば FTP の場合，クライアントから同時に接続される数は少ないと見積もって 10 程度を，HTTP の場合，ある程度接続が集中することを見積もって 100 程度を起動しておく．

中継モジュール制御デーモンから各中継モジュールへの処理の割当てやトリガ指示は，共有メモリを通じて行う．この通信用の共有メモリとして，FTP 中継モジュール制御用と HTTP 中継モジュール制御用をそれぞれ用意して，各中継モジュールであるスレッドを制御する．

アクセス制御部では，おとりサーバ上のログが攻撃された場合に備えて，各クライアントの通信ログを外部のログ DB へと記録する．ここで対象とするログは，不正なクライアントのみならず，正常なクライアントと判定されていたものについても収集する．これは，正常なクライアントと判定されていた場合でも，TCP コネクションの途中で切り替えられたときの切替え前後の挙動を分析するためである．

5.3 正規サーバとおとりサーバ

正規サーバはそのまま利用できる．おとりサーバは，正規サーバと同じデータ，サービス，セキュリティ対策を施す．ただし，重要なデータやユーザ情報については，おとりのものを用意する．ここで，4.4.4 項のおとりシステム上のファイルが改竄された場合には，正規システムにも同様な問題があるため，ただちに改竄されたときの行動ログの分析を行い，両システムのセキュリティ対策を図る．そして，次に誘導される侵入者にファイルの不整合を気付かれる前に，改竄前の状態に戻す必要がある．

5.4 周 辺 機 器

ITS が外部システムへ攻撃するような踏み台に利用されてはならない．このため，外部への接続要求を拒否するように，ファイアウォールなどの機器でフィルタリングを行うようにする．

6. 性 能 評 価

ここでは ITS のシステムへの適用性に関して，処理性能面から評価を行う．具体的には，ITS を適用したときの本来のサービスに与える影響と，不審な挙動が検知されたときの動的切替速度について評価，考察を行う．

表 2 ハードウェアスペック
Table 2 Hardware spec.

モジュール	CPU	メモリ
正常&不正クライアント	PentiumIII 1GHz ×1	256MByte
侵入検知部	PentiumIII 1GHz ×1	256MByte
アクセス制御部	PentiumIII 1.13GHz×2	256MByte
正規&おとりサーバ	PentiumIII 1GHz ×1	256MByte

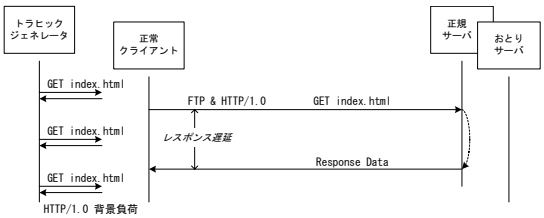

図 9 直結時のサーバレスポンス遅延
Fig. 9 Response latency of direct connection.

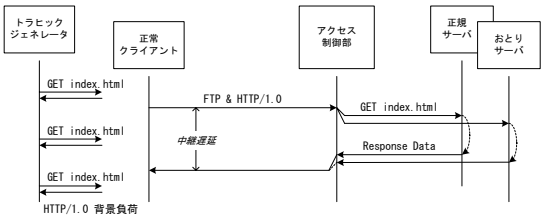

図 10 ITS による中継時のサーバレスポンス遅延
Fig. 10 Response latency on ITS.

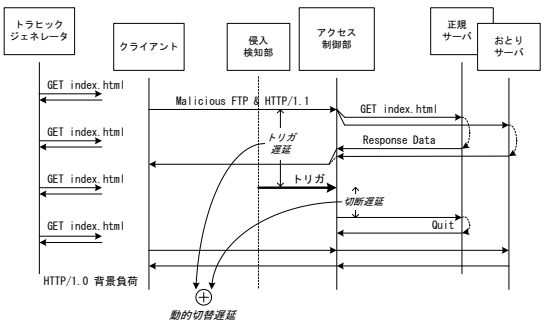

図 11 ITS による動的切替遅延
Fig. 11 Dynamic diversion latency on ITS.

6.1 評 価 環 境

評価に使用した機器のハードウェアスペックを**表 2** に示す．また，測定項目について，**図 9**，**図 10**，**図 11** に示す．

各機器は，100Base-TX の LAN で接続されている．ハードウェアのトラフィックジェネレータを使用して，サーバに対して一定間隔で HTTP/1.0-GET の背景負荷を与えた．このとき取得する index.html ファイルの

表 3 ITS 適用時と未適用時の FTP/HTTP 遅延
Table 3 FTP/HTTP latency comparison with and without ITS.

クライアント側		HTTP/1.0 背景負荷	
プロトコル	遅延種別	none	50 GETs/sec
FTP	直結（図9）	2.3 msec	2.3 msec
	中継（図10）	3.5 msec	3.5 msec
HTTP/1.0	直結（図9）	1.7 msec	1.5 msec
	中継（図10）	81.2 msec	86.4 msec

サイズは，2.9 KByte である．応答時間の測定は，ネットワーク上のパケット時間をモニタすることで行っており，5 回の測定の平均値を求めた．

性能測定は，次の 3 つの遅延について行った．

- 直結時のサーバレスポンス遅延（図 9）
  クライアントとサーバを直接接続したときの，FTP ならびに HTTP サービスのレスポンス遅延を測定する．レスポンス遅延は，クライアントがファイルの取得要求パケットを送信してから，クライアント側へレスポンスパケットが返信されるまでの時間を測定している．
- ITS による中継時のサーバレスポンス遅延（図 10）
  ITS を設置したときの，FTP ならびに HTTP サービスの中継遅延を測定する．中継遅延は，クライアントがファイルの取得要求パケットを送信してから，クライアント側へレスポンスパケットが返信されるまでの時間を測定している．
- ITS による動的切替遅延（図 11）
  ITS による，FTP ならびに HTTP サービスにおける継続中の TCP コネクションの動的切替遅延を測定する．動的切替遅延は，クライアントが不審パケットを送信してから侵入検知部がトリガを発行するまでのトリガ遅延と，アクセス制御部がトリガを受信してから正規サーバへ TCP コネクションの切断要求を送信するまでの切断遅延の合計時間を測定することで求めている．

6.2 ITS 適用時のサービスに与える影響に関する評価結果

表 3 に，直結時の FTP ならびに HTTP サービスと ITS 適用時の FTP ならびに HTTP サービスのレスポンス遅延を示す．測定は，背景負荷がないときと HTTP/1.0 による 50 GETs/sec の状況で実施した．

FTP サービスについては，背景負荷のないときと HTTP/1.0 の背景負荷を与えたときの両状況において，ITS 適用時のレスポンス遅延は直結時のレスポンス遅延と同じ結果となっており，FTP 本来のサービスへ与える影響は測定できないほど，小さなものであることが判明した．これは，背景負荷が HTTP/1.0 であるために，5.2 節で説明した中継モジュール制御デーモンと FTP 中継モジュール間の通信用共有メモリにおいて，FTP 中継モジュール間のメモリ参照の競合が発生しないためである．また，TCP コネクションが確立された後のコマンド中継は，TCP コネクション開始時点で行われる侵入者リストの確認処理が省かれるために処理時間が小さくなっている．

HTTP/1.0 サービスについては，負荷のないときと与えたときの両状況において，約 80 msec ほどの遅延が発生している．これは，HTTP/1.0 プロトコルの TCP コネクション制御が原因となっている．HTTP/1.0 では，ファイル取得要求ごとに新たに TCP コネクションを確立する．これにより，アクセス制御部は TCP コネクションが確立されるごとに，侵入者リストを参照して要求元 IP アドレスが正常クライアントからのものなのか不正クライアントからのものなのかを判断して，中継モジュールにその旨を割り当てるというオーバヘッドが発生している．また，背景負荷が HTTP/1.0 であるために，複数の HTTP 中継モジュールが動作中となり，中継モジュール制御デーモンと HTTP 中継モジュール間の通信用共有メモリにおいて競合が発生してしまうことも原因となる．しかしながら，ITS 適用時の HTTP/1.0 の中継遅延は 100 msec より小さく，ネットワークを経由して利用される HTTP サービスへの影響は小さいといえる．

表 3 の FTP サービスの結果を基に HTTP/1.1 サービスにおける遅延について推定してみると，HTTP/1.1 では TCP コネクションを継続したままファイル取得要求を送信できるため，FTP と同じくファイル取得要求時に侵入者リストの確認処理が省かれる．よって，中継処理は FTP サービスのときと同じくらい高速に行われることになる．逆に，HTTP/1.0 サービスの結果を基に FTP サービスおけるログイン処理遅延についても推定してみると，ログイン処理の際には新たに TCP コネクションが確立されるため HTTP/1.0 プロトコルの場合と同様なオーバヘッドによる遅延が生じることになる．

6.3 動的切替え速度に関する評価結果

表 4 に，ITS 適用時の FTP ならびに HTTP サービスにおいて，正常クライアントが不審なパケットを送信してからアクセス制御部へトリガが送信されるまでの遅延，アクセス制御部がトリガを受信してから正規サーバへ切断要求を送信するまでの遅延，これら 2 つの遅延を合計した動的切替え遅延を示す．測定は，背景負荷がないときと HTTP/1.0 による 50 GETs/sec の状況で実施した．

表 4 ITS における FTP/HTTP 動的切替遅延
Table 4 FTP/HTTP dynamic diversion latency on ITS.

クライアント側		HTTP/1.0	背景負荷
プロトコル	遅延種別	none	50 GETs/sec
FTP	トリガ	154.5 msec	186.3 msec
	切断	3.1 msec	5.3 msec
（図11）	動的切替	157.6 msec	192.6 msec
HTTP/1.1	トリガ	102.3 msec	135.3 msec
	切断	6.0 msec	11.6 msec
（図11）	動的切替	108.3 msec	146.9 msec

FTP サービスについては，負荷のないときと与えたときの両条件において，侵入検知部が不審なパケットを検知してからトリガを送信するまでのトリガ遅延が 150 から 200 msec 程度となっている．これは，IDS が不審パケットを検知してからアラートファイルに書き出すまでの遅延が大きなためである．アクセス制御部がトリガを受信してから正規サーバへの TCP コネクションを切断するまでの切断遅延は数 msec となっていた．これらトリガ遅延と切断遅延の合計となる動的切替遅延は，200 msec 以下であり，手動でコマンドを送信する侵入者に対しては十分高速に切り替わっていることが分かる．

HTTP/1.1 サービスについても，負荷のないときと与えたときの両条件において，トリガ遅延が 100 から 140 msec 程度に，切断遅延が 10 msec 程度に，その合計の動的遅延遅延は 100 から 150 msec になっていた．HTTP/1.1 サービスについても，手動でコマンドを送信する侵入者に対しては十分高速に切り替えられていることが分かる．

7. おわりに

本論文では，不審な挙動の TCP コネクションを強制的に正規システムからおとりシステムへ切り替えることで，正規システムを保護しながら侵入者の行動ログを収集する ITS の切替え機能を提案した．切替えは，TCP コネクションの開始時点のみでなく継続中の TCP コネクションについても可能であり，また正規システムとおとりシステムの通信状態の同期を図っておくことで切替え時の通信のシナリオを継続できるため，侵入者に気付かれることのない手法となっている．提案した手法について，FTP ならびに HTTP サービスに適用する場合の各構成機器の設計を行った．これに従い実装を行い，コマンドの中継遅延ならびに TCP コネクションの動的切替え遅延について測定した．その結果，ITS を適用しても本来のサービスに与える影響を小さく抑えることができ，かつ切替えについても手動で攻撃してくる侵入者に対しては十分迅速に行えることを確認した．

参 考 文 献

1) 新種ウィルス「W32/Nimda」に関する情報，情報処理振興事業協会．http://www.ipa.go.jp/security/topics/newvirus/nimda.html
2) コンピュータ緊急対応センタ（JPCERT/CC）．http://www.jpcert.or.jp/
3) Snort. http://www.snort.org/
4) Proctor, P.E.: *Practical Intrusion Detection Handbook*, Prentice Hall, NJ (2001).
5) Amoroso, E.: *Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps and response, Intrusion*, Net Books, Sparta, NJ (1999).
6) 武田圭史，磯崎　宏：ネットワーク侵入検知，ソフトバンクパブリッシング (2000).
7) Honeynet Project, http://project.honeynet.org/project.html
8) 宮川明子，稲田　徹，後沢　忍：不正侵入者を外部ネットワークに設置したおとりサーバへ誘導するセキュリティシステムの検討，情報処理学会コンピュータセキュリティ研究会，CSEC, pp.225–230 (2001).
9) Decoy Server Solution, http://www.atsweb.it/Images/Documenti/TOP_DS_Decoy%20Server%20Solution.pdf, Top Layer Networks Product.
10) Man Trap. http://enterprisesecurity.symantec.com/products/products.cfm?ProductID＝157, Symantec Product.
11) 竹森敬祐，田中俊昭，中尾康二：不正侵入者に探知されない通信セッションのおとりサーバへの引継ぎ方式の検討，情報処理学会第 61 回全国大会，4F-3 (2000).
12) 竹森敬祐，田中俊昭，清本晋作，中尾康二：不正侵入者に探知されることなくおとりのデータ領域へと誘導するおとりシステムの実装評価，情報処理学会コンピュータセキュリティ研究会，CSEC, pp.79–84 (2001).
13) 竹森敬祐，力武健次，清本晋作，田中俊昭，中尾康二：Intrusion Trap System の設計および実装，情報処理学会第 63 回全国大会，2G-1 (2001).
14) 竹森敬祐，力武健次，田中俊昭，清本晋作，中尾康二：Intrusion Trap System の実装および評価，情報処理学会，コンピュータセキュリティシンポジウム 2001，pp.415–420 (2001).

(平成 14 年 12 月 2 日受付)
(平成 15 年 6 月 3 日採録)

竹森 敬祐（正会員）

1994 年慶應義塾大学理工学部電気工学科卒業．1996 年同大学大学院修士課程修了．現在，（株）KDDI 研究所コンピュータセキュリティグループに勤務．慶應義塾大学大学院理工学研究科開放環境科学専攻博士課程在学中．トラヒック理論，インターネットセキュリティの研究に従事．2002 年度電子情報通信学会学術奨励賞受賞．電子情報通信学会会員．

力武 健次（正会員）

1988 年東京大学計数工学科卒業．1990 年同大学大学院修士課程修了．現在，（株）KDDI 研究所コンピュータセキュリティグループに勤務．大阪大学大学院情報科学研究科マルチメディア工学専攻博士課程在学中．2001 年 3 月より技術士（情報工学部門）．DNS，インターネットセキュリティ，テレワークの研究に従事．著書に「プロフェッショナルインターネット」（1998 年，オーム社）ほか．第 63 回情報処理学会全国大会大会優秀賞受賞．ACM，日本テレワーク学会，Internet Society 各会員．

三宅 優（正会員）

1988 年慶應義塾大学理工学部電気工学科卒業．1990 年同大学大学院修士課程修了．現在，（株）KDDI 研究所ネットワークセキュリティグループに勤務．高速通信プロトコルの実装，インターネットアクセス，インターネットセキュリティの研究に従事．1989 年度電気・電子情報学術振興財団猪瀬学術奨励賞，1995 年度情報処理学会学術奨励賞受賞．電子情報通信学会会員．

中尾 康二（正会員）

1979 年早稲田大学教育学部数学科卒業．現在，（株）KDDI 研究所ネットワークセキュリティグループおよび KDDI（株）情報セキュリティ室に勤務．早稲田大学，電気通信大学の非常勤講師を兼務．ネットワーク技術，セキュリティ技術の研究に従事．1987 年度情報処理学会研究賞受賞．電子情報通信学会会員．