本資料について

- 本資料は下記論文を基にして作成されたものです。文書の内容の正確さは保障できないため、正確な知識を求める方は原文を参照してください。

- 著者：竹森敬祐、力武健次、三宅優、中尾康二
- 論文名：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
- 出展：情報処理学会論文誌 Vol.4 No.8
- 発表日：2003年8月

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

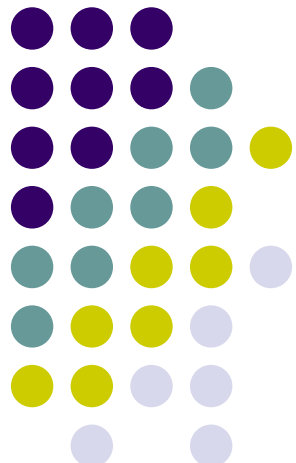
名城大学理工学部　渡邊研究室

竹尾大輔 ※0

竹森敬祐 ※1　力武健次 ※1

三宅　優 ※1　中尾康二 ※1

※0 編集･発表者　※1 KDDI研究所



1．はじめに

ネットワークシステムにセキュリティホール

ファイアウォール

- 通過を許可された通信により引き起こされる攻撃

防御システム

防げない
検知できない

攻撃手法の把握が必要

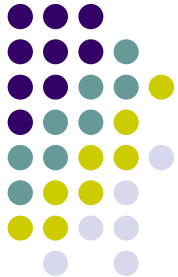
IDS

- シグネチャ情報を持たない未知の攻撃
- サイト独自のアプリケーションに対する攻撃

Honeypot

- 侵入手法、ツール、侵入者の意図の分析
- 脆弱性を持ったおとりのシステム

Internet Trap



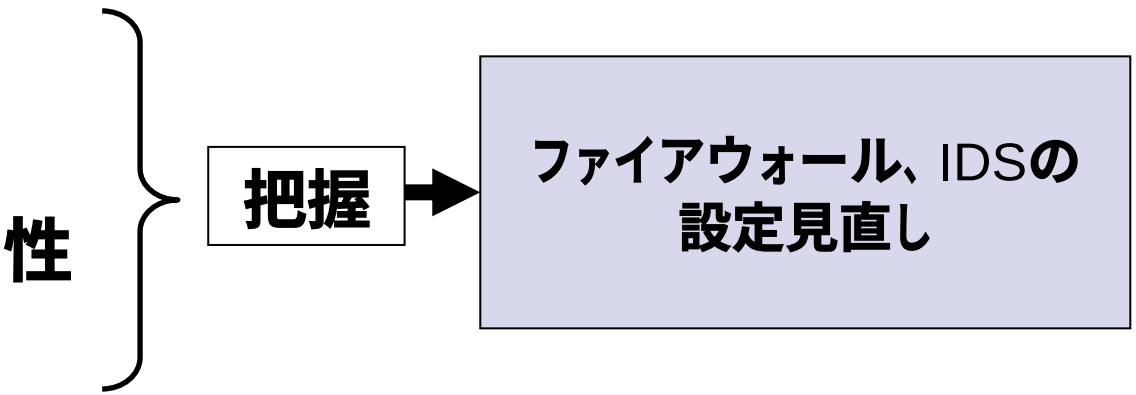
- 正規システムからおとりシステムへ強制切替え
  - トラヒック監視→疑わしいアクセスを検知→切替え
- 利点
  - Honeypotで達成できる機能を実現している
  - 正規システムを防御できる
  - 犯罪の誘発につながらない
- 問題点
  - 切替えはTCPコネクションの開始時のみ
    - 疑わしいコネクションが継続→正規システムへの攻撃
  - 行動ログの改竄、消去

提案

- ITS（Intrusion Trap System）
  - 継続中のコネクションでもおとりへ切替え
  - 正規システムを守りつつ情報収集が可能
- 2つの設計手法を提案
  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
- 2.のITSモデルに注目
  - FTP・HTTPに適用時の切替え機能の設計・実装
  - 処理性能に関する測定
    - 本来のサービスに与える影響の抑制、迅速な切替え

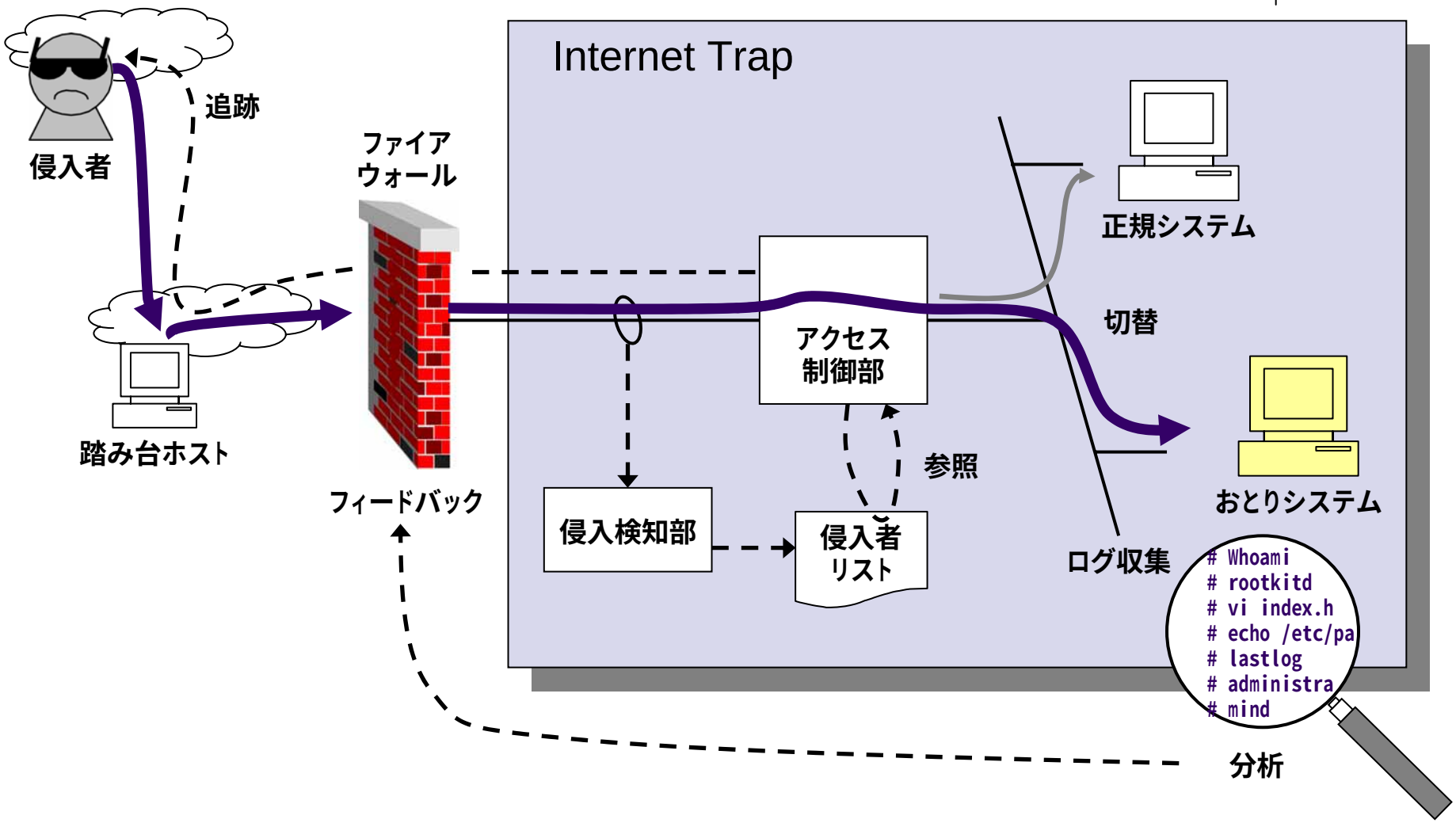
2．既存システムの概要と問題点
既存のInternet Trapの概要

- 正規の利用者＋侵入者にもサービスを提供
  - 侵入者にはおとりシステムからサービスが提供される
- 侵入者の行動ログを分析
  - 侵入手法
  - 利用ツール
  - サイト上の脆弱性
  - 侵入目的



- 追跡のための時間稼ぎが可能

既存のInternet Trapの構成



問題点

- コネクションの開始時点で切替え
  - 不正なコネクションが継続→正規システムへ攻撃
    - おとりシステムへ強制切替・・・シーケンス処理の不整合
    - 切断して再接続を促す・・・通信シナリオの矛盾

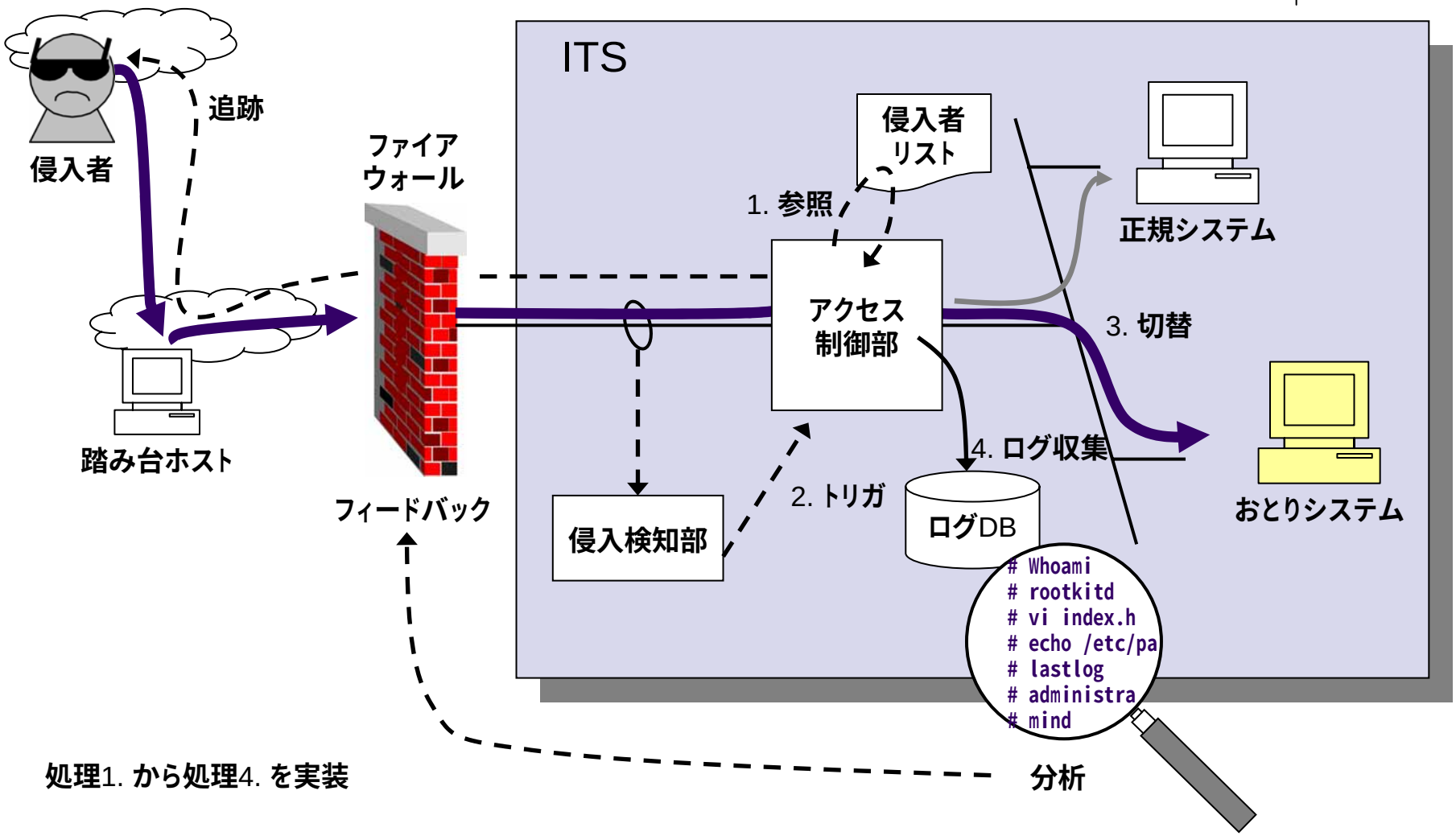
      通信シナリオの矛盾
      - ログイン処理、ディレクトリ間移動、ファイル生成・変更・削除、…
        →おとりシステムに反映されていない

    - 切替え機構の発覚→情報収集を円滑に行えない
- ログはおとりシステム上で収集
  - 管理者権限奪取→ログの改竄・削除
    - 収集した情報が信頼できない

必要とされる機能

- TCPコネクションを継続したままの切替え
- 切替え前後の通信シナリオの継続性を保つ
- 迅速な切替え処理
- おとりシステム以外でのログ収集

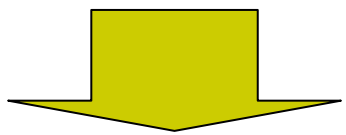
3．提案システムの概要
提案するITSの構成



処理1. から処理4. を実装

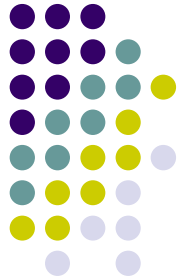
ITSの概要

- ITSの目的
  1. 正規システムの安全確保
  2. 収集した行動ログの活用
- 継続的なサービスによる期待
  - 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



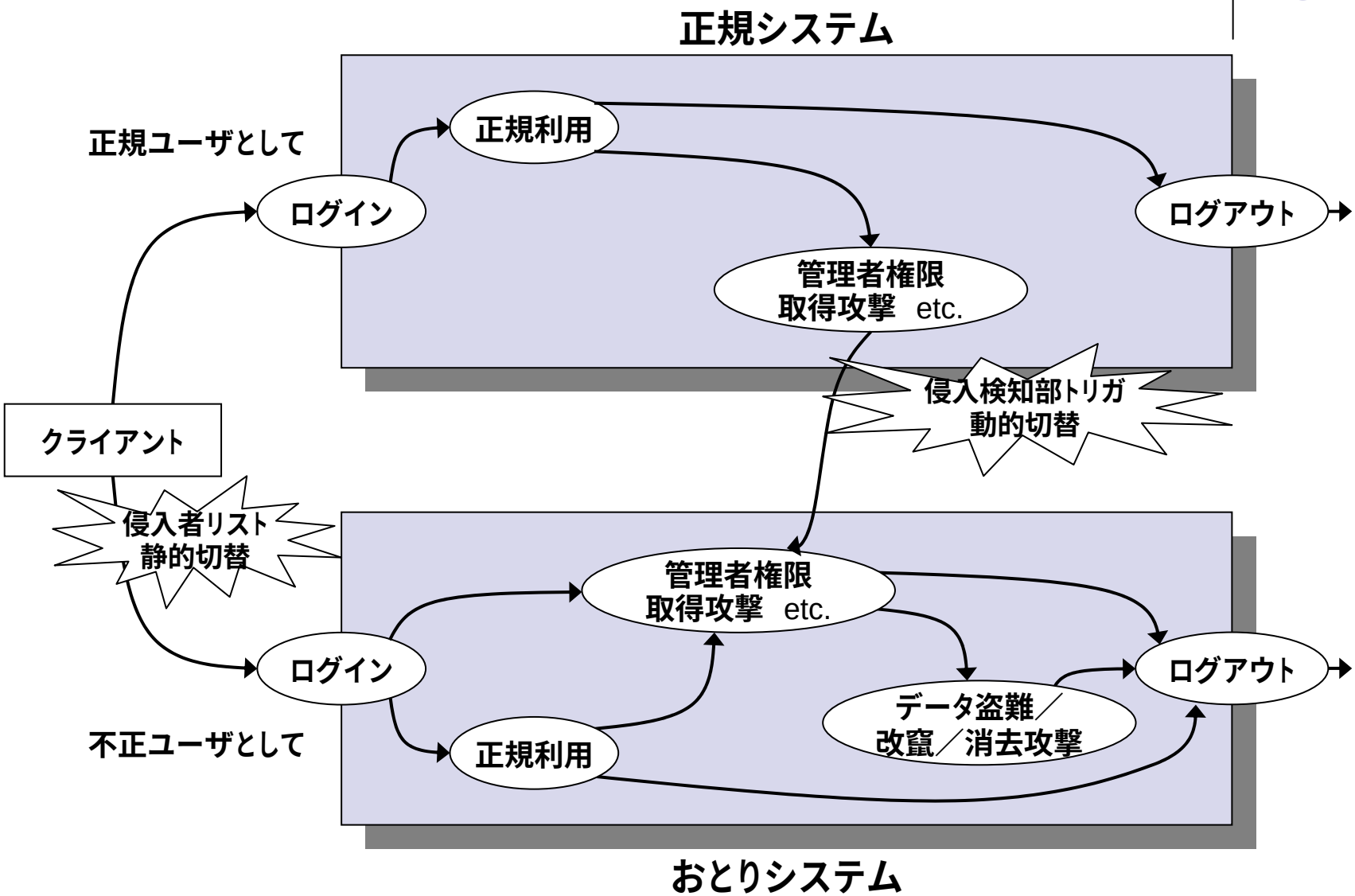
- 切替え後に逃げられても、それまでのログ収集が可能

4．切替え手法
静的切替えと動的切替え



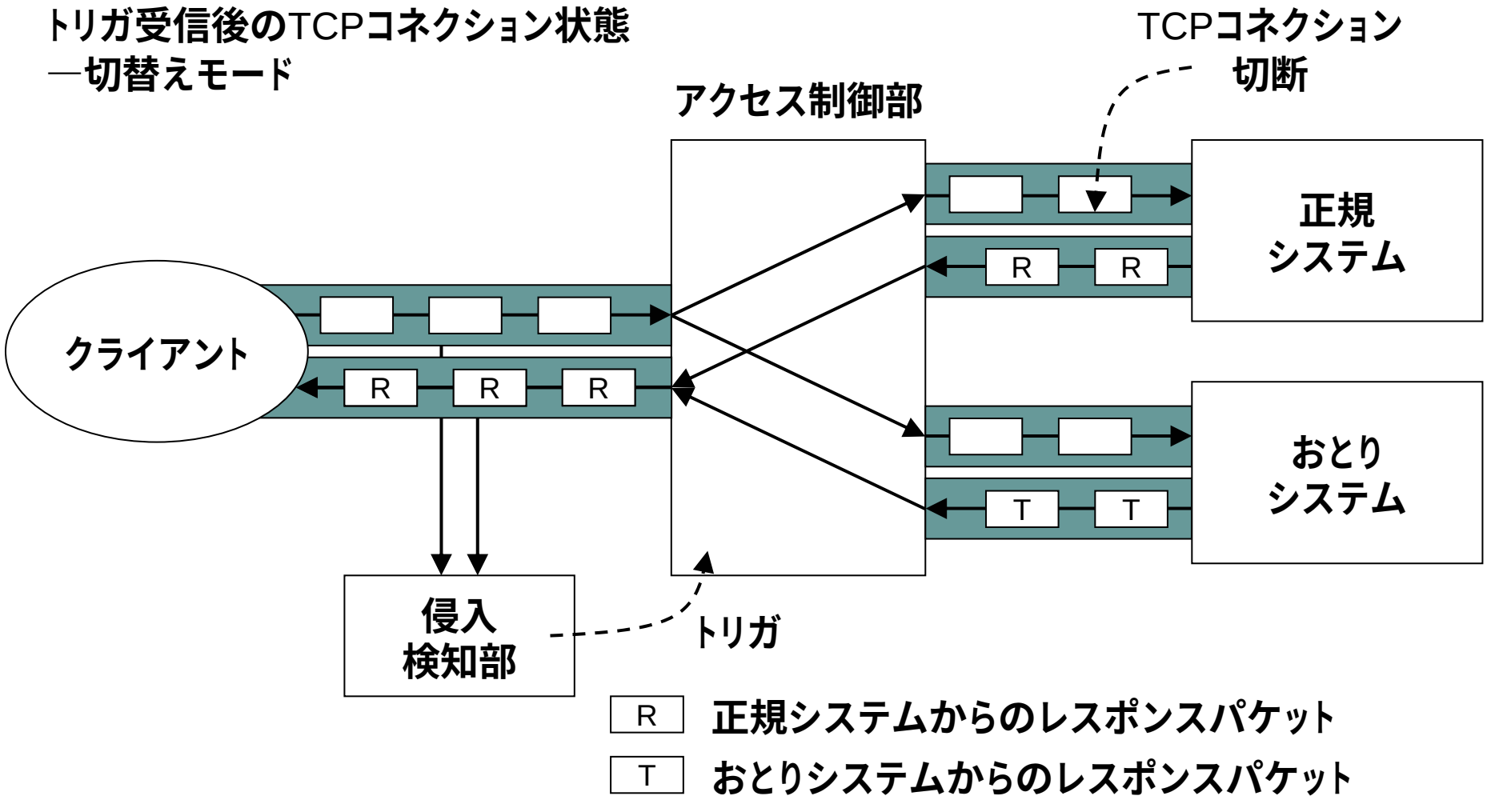
- 静的切替え
  - TCPコネクションの開始時点で切り替え
  - 既存Internet Trapの切替え手法
- 動的切替え
  - 継続中のTCPコネクションを切り替え
    - 通信シナリオの継続性
    - 切替処理の迅速性

切替えの様子

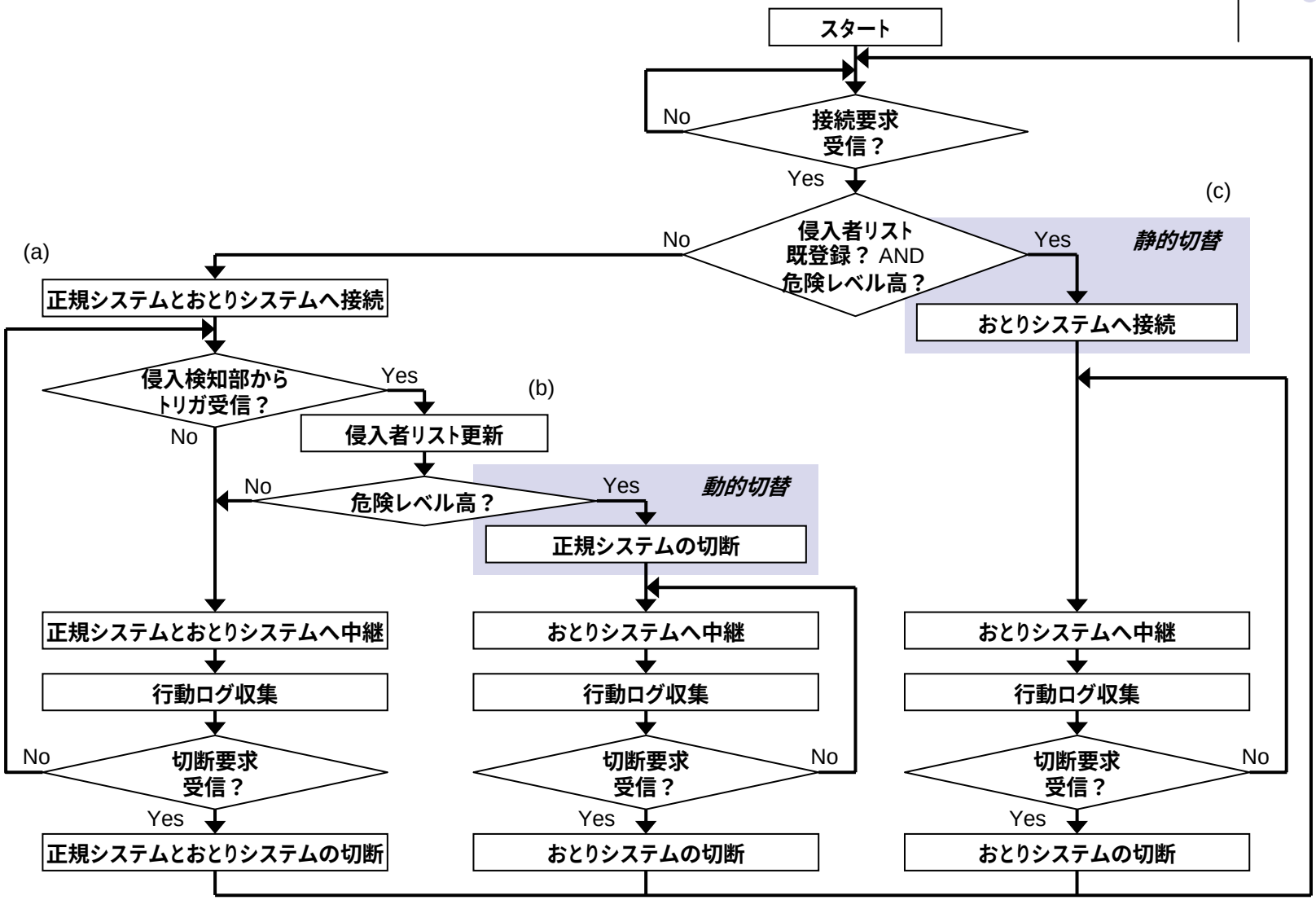

正規システム
正規ユーザとして
正規利用
ログイン
ログアウト
管理者権限
取得攻撃　etc.
侵入検知部トリガ
動的切替
クライアント
侵入者リスト
静的切替
管理者権限
取得攻撃　etc.
ログイン
ログアウト
データ盗難／
改竄／消去攻撃
不正ユーザとして
正規利用
おとりシステム

動的切替えの詳細

トリガ受信後のTCPコネクション状態
—切替えモード



アクセス制御部の処理フロー



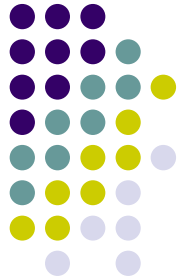
通信シナリオの継続性における課題

- 状態を完全に一致させることは不可能

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が目標

- 排除しきれない状態の不整合
  - プロセス･メモリの不整合
  - ファイルの不整合
  - IPアドレスの不整合
  - 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

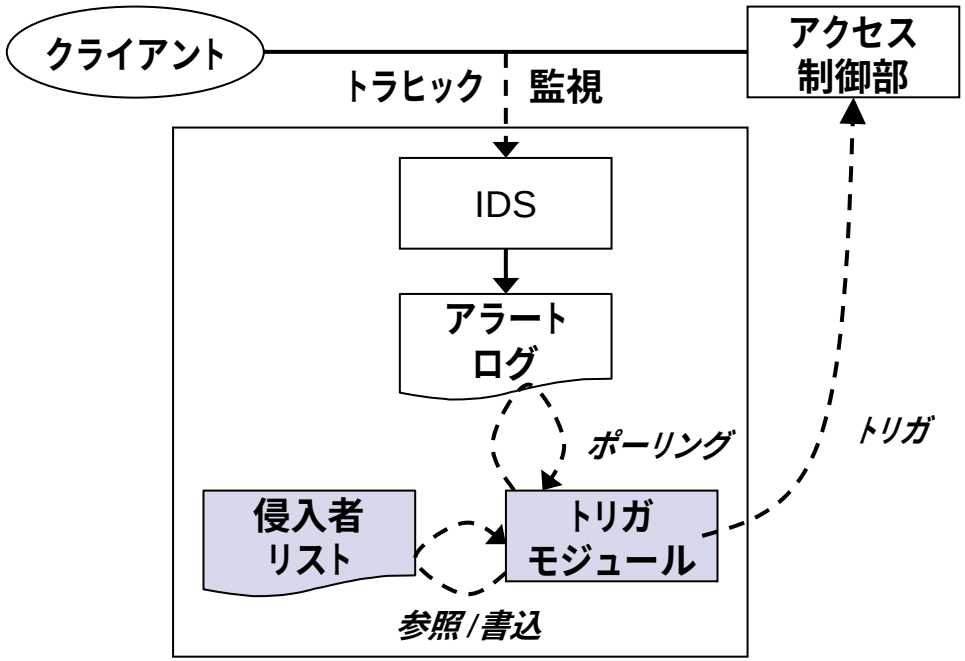
5．構成機器の設計



- 例：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
  - 各モジュールの具体的な設計
    - 侵入検知部
    - アクセス制御部
    - 正規サーバとおとりサーバ
    - 周辺機器

侵入検知部

侵入検知部の設計

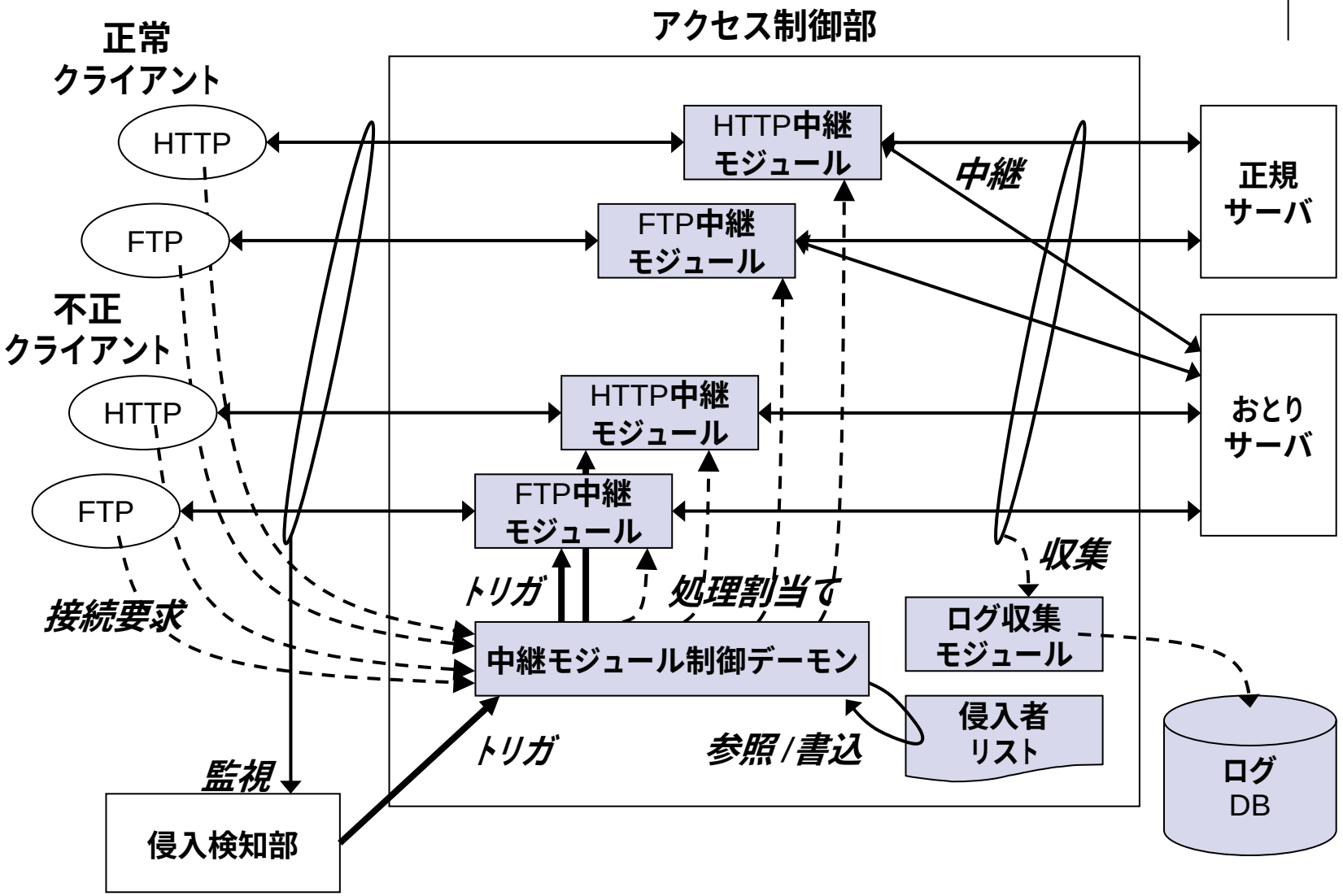


侵入検知部

侵入者リスト

侵入者 IPアドレス	最大危険		初回危険	
	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
・・・	・・・	・・・	・・・	・・・

アクセス制御部


正常
クライアント
HTTP
FTP
不正
クライアント
HTTP
FTP
接続要求
アクセス制御部
HTTP中継
モジュール
FTP中継
モジュール
HTTP中継
モジュール
FTP中継
モジュール
中継
正規
サーバ
おとり
サーバ
収集
トリガ
処理割当て
ログ収集
モジュール
中継モジュール制御デーモン
侵入者
リスト
ログ
DB
監視
トリガ
参照/書込
侵入検知部

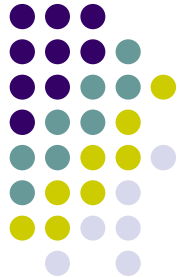
正規サーバとおとりサーバ

- 正規サーバ
  - そのまま利用可能
- おとりサーバ
  - 正規サーバと同じデータ、サービス、セキュリティ対策
  - 重要なデータやユーザ情報はおとり
- おとりシステム上のファイルが改竄されたら
  - 改竄時の行動ログ分析
  - 両システムのセキュリティ対策
  - 改竄前の状態に戻す

周辺機器

- ITSが踏み台に利用されてはならない
  - ファイアウォールなどでフィルタリング
    - 外部への接続要求を拒否

6．性能評価
評価環境

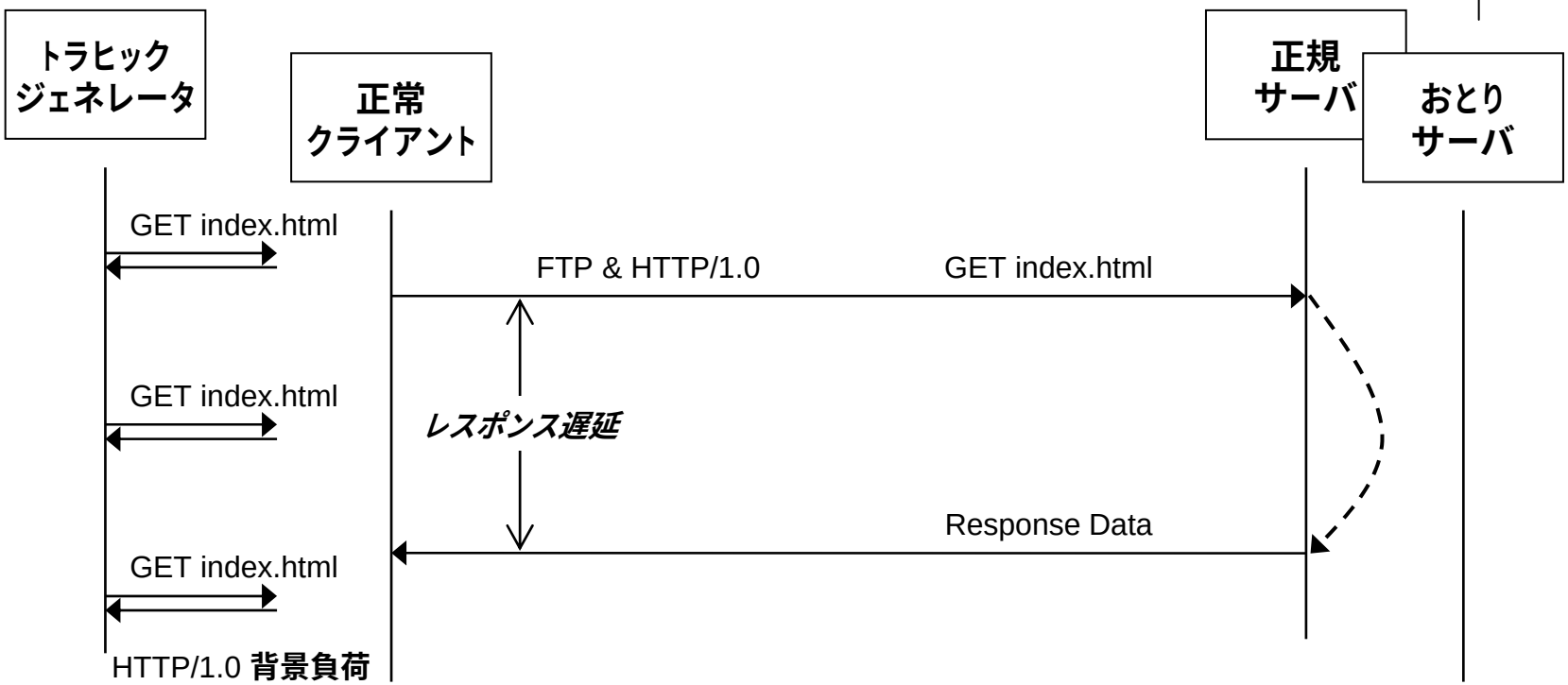


- ハードウェアスペック

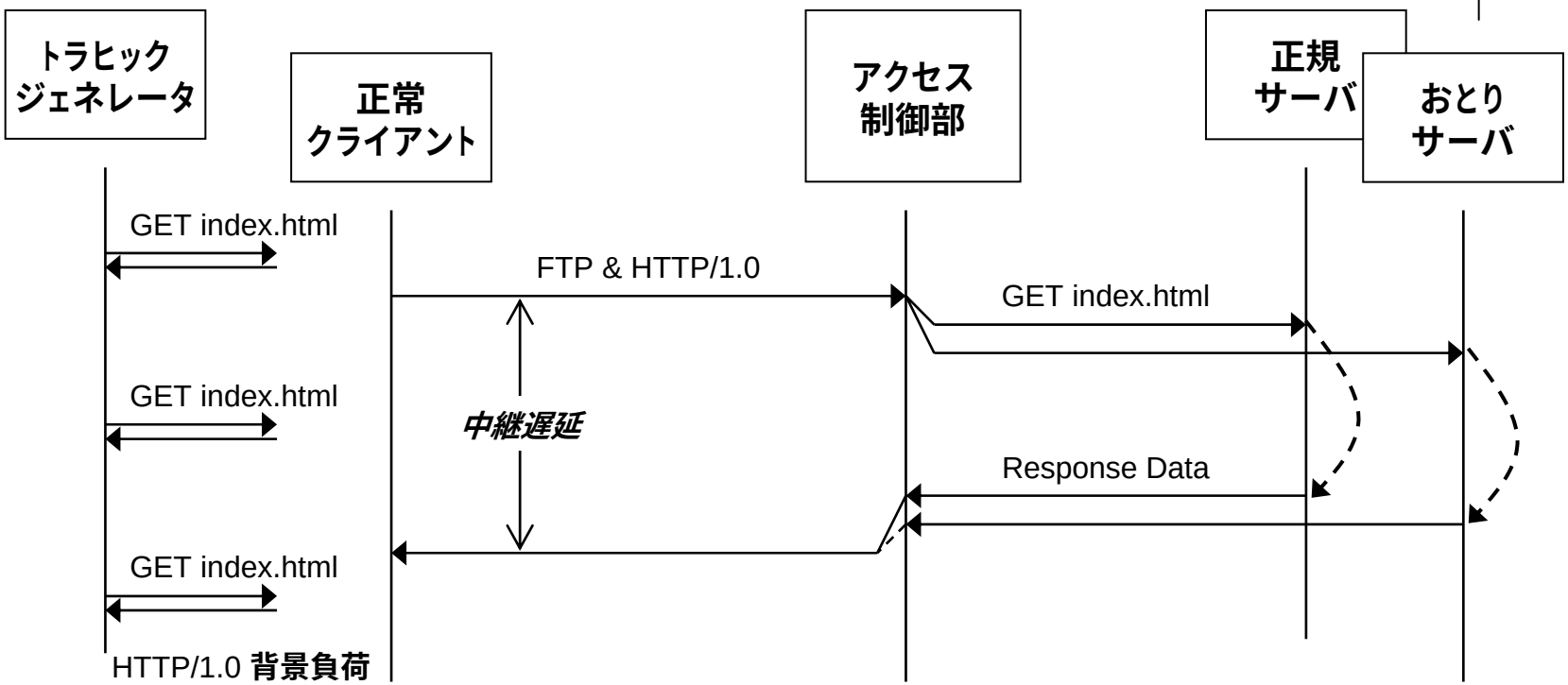
モジュール	CPU	メモリ
正常＆不正クライアント	PentiumIII 1GHz×1	256MByte
侵入検知部	PentiumIII 1GHz×1	256MByte
アクセス制御部	PentiumIII 1.13GHz×2	256MByte
正規＆おとりサーバ	PentiumIII 1GHz×1	256MByte

- 各機器は100Base-TXのLANで接続
- 一定間隔でHTTP/1.0-GETの背景負荷
  - 取得するindex.htmlのファイルサイズは2.9KByte

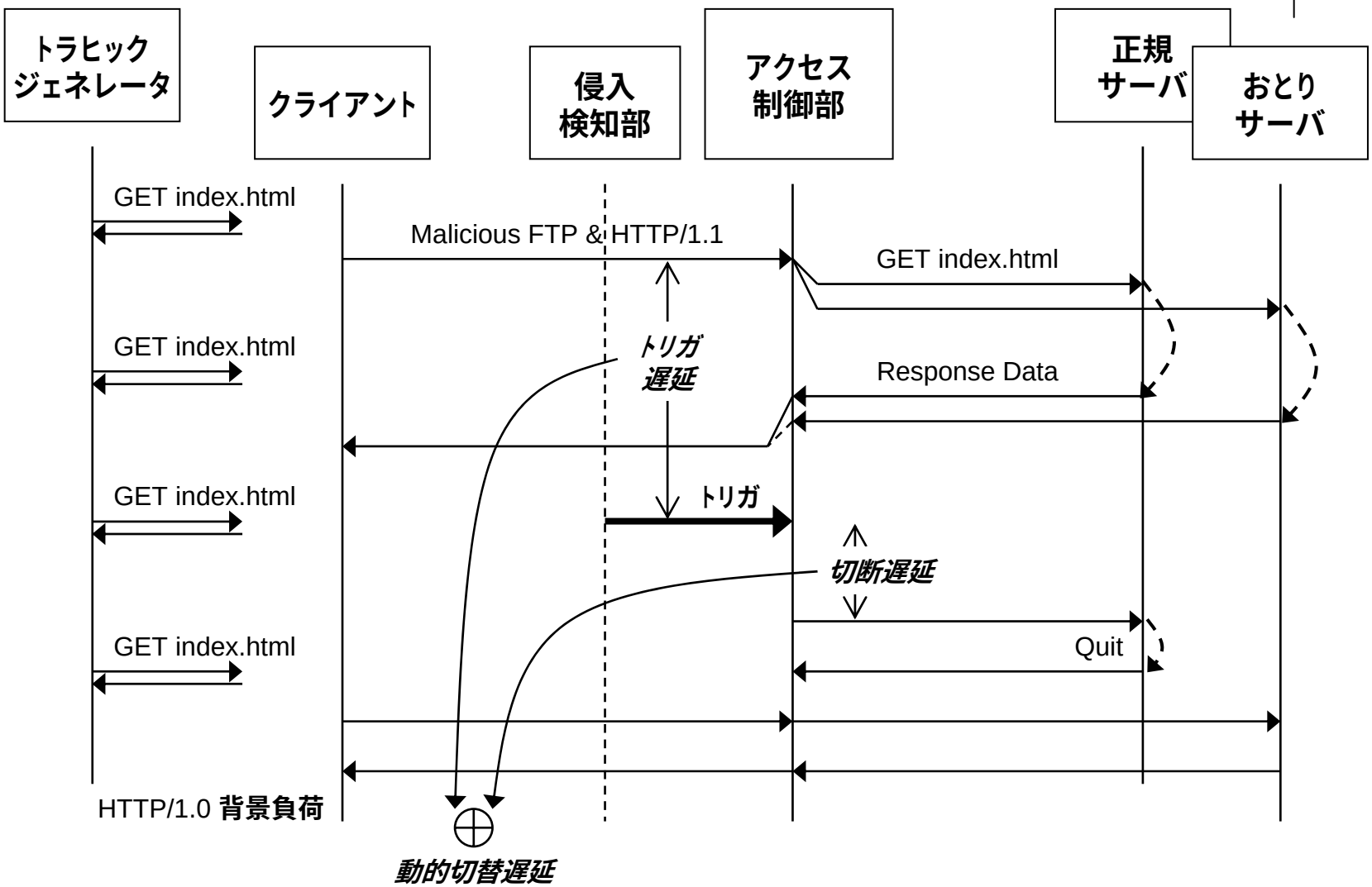
直結時のサーバレスポンス遅延



ITSによる中継時のサーバレスポンス遅延



ITSによる動的切替遅延



ITS適用時のサービスに与える影響に関する評価結果

- **直結時とITS適用時のFTP/HTTP遅延**

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	2.3 msec	2.3 msec
	中継	3.5 msec	3.5 msec
HTTP/1.0	直結	1.7 msec	1.5 msec
	中継	81.2 msec	86.4 msec

- **FTPサービスについて**
  - **測定できないほど影響は小さい**
- **HTTP/1.0サービスについて**
  - **ネットワーク経由利用のHTTPへの影響は小さい**

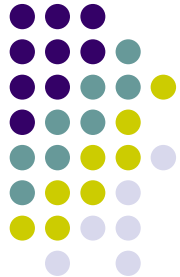
動的切替え速度に関する評価結果

- ITSにおけるFTP/HTTP動的切替遅延

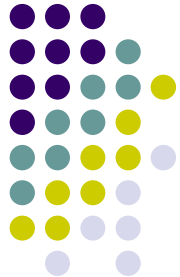
クライアント側 プロトコル	遅延種別	HTTP/1.0 none	背景負荷 50 GETs/sec
FTP	トリガ	154.5 msec	186.3 msec
	切断	3.1 msec	5.3 msec
	動的切替	157.6 msec	192.6 msec
HTTP/1.1	トリガ	102.3 msec	135.3 msec
	切断	6.0 msec	11.6 msec
	動的切替	108.3 msec	146.9 msec

- FTPとHTTP/1.1の両サービスについて
  - 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る

7．おわりに



- 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
  - 切替えはTCPコネクション開始時点と継続中に可能
  - 通信シナリオ継続により侵入者に気付かれない
- FTP・HTTPサービスでの構成機器を設計
- 実装および中継遅延・動的切替遅延を測定
  - 本来のサービスに与える影響は小さく、切替えは十分迅速であることを確認



おわり

用語説明

- **ポーリング**
  - **通信機器やソフトウェアが複数で連携動作する際に、送信（あるいは処理）要求がないか、一つ一つの相手に聞いて回る方式。ソフトウェアの場合は、プログラム内部のメインルーチンが、個々の手続きを順に呼び出して応答がないかチェックし、応答があれば何らかの処理を行なう。**
    （IT**用語辞典** e-Words：http://e-words.jp/）

原文参考文献

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).

原文著者・共著者情報

竹森　敬祐（情報処理学会正会員）

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（情報処理学会正会員）

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（情報処理学会正会員）

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研究所コンピュータ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（情報処理学会正会員）

1979年早稲田大学教育学部数学科卒業。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。

編集・発表者情報

竹尾　大輔（渡邊研究室 B4）

2000年三重県立桑名高等学校普通科卒業。現在、名城大学理工学部情報科学科在学中。インターネットセキュリティの研究に従事。2002年度情報科学科プログラミングコンテスト特別賞受賞。ソフトウェア同好会部員。情報処理学会学生会員。

このプレゼンテーションは、渡邊研究室の輪講用として、竹森他著「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」（情報処理学会論文誌、Vol.4 No.8、2003年8月）を基に、竹尾大輔が製作したものです。