

---

# 不正アクセスログの解析

東海大学電子情報学部コミュニケーション工学科

田口 元朗

指導教員

石井 啓之

# 研究目的

---

SSHサーバーアクセスログを観測し、不正アクセスの実態を調査することにより……

- どの国から攻撃を受けるのか？
- どういったIDで不正アクセスが来るのか？
- サーバーへの影響はどうか？

などの調査結果より、これらの危険への対応策は本当に十分なのか検討した。

# 調査方法

---

- 研究室サーバを使用

⇒Fedora core8, Celeron(R) CPU 2.53GHz,メモリ1GB

- Syslog

⇒各種のUNIXが備えるシステム・ログ出力機能

⇒システムメッセージをファイルに保存する仕組み

# ログ情報集計の流れ

---

- 研究室のSSHサーバーのログ情報を取得
- プログラムを用いてログ情報から不正アクセスを検出し、以下の項目を調査

国名

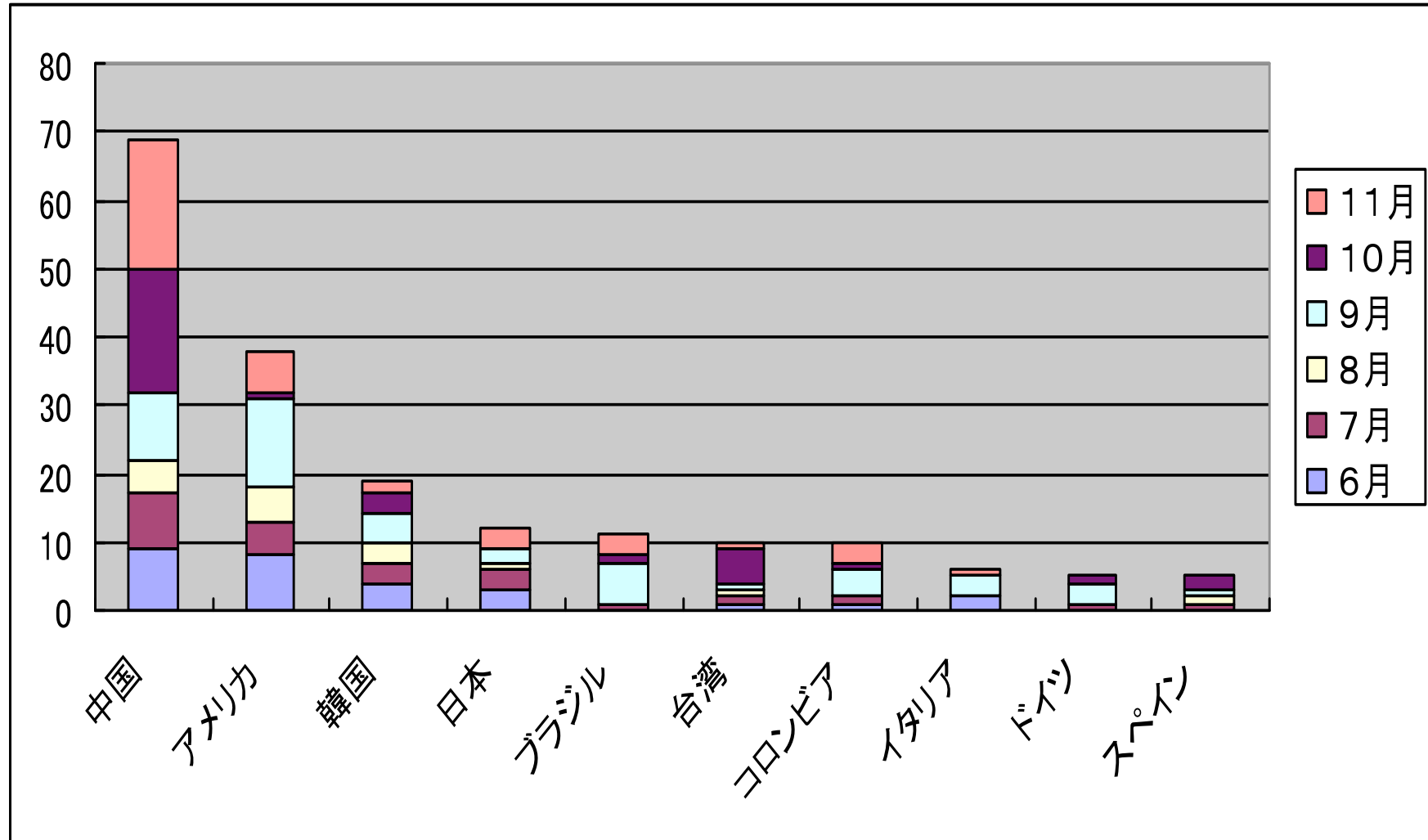
IPアドレス

月、日、曜日

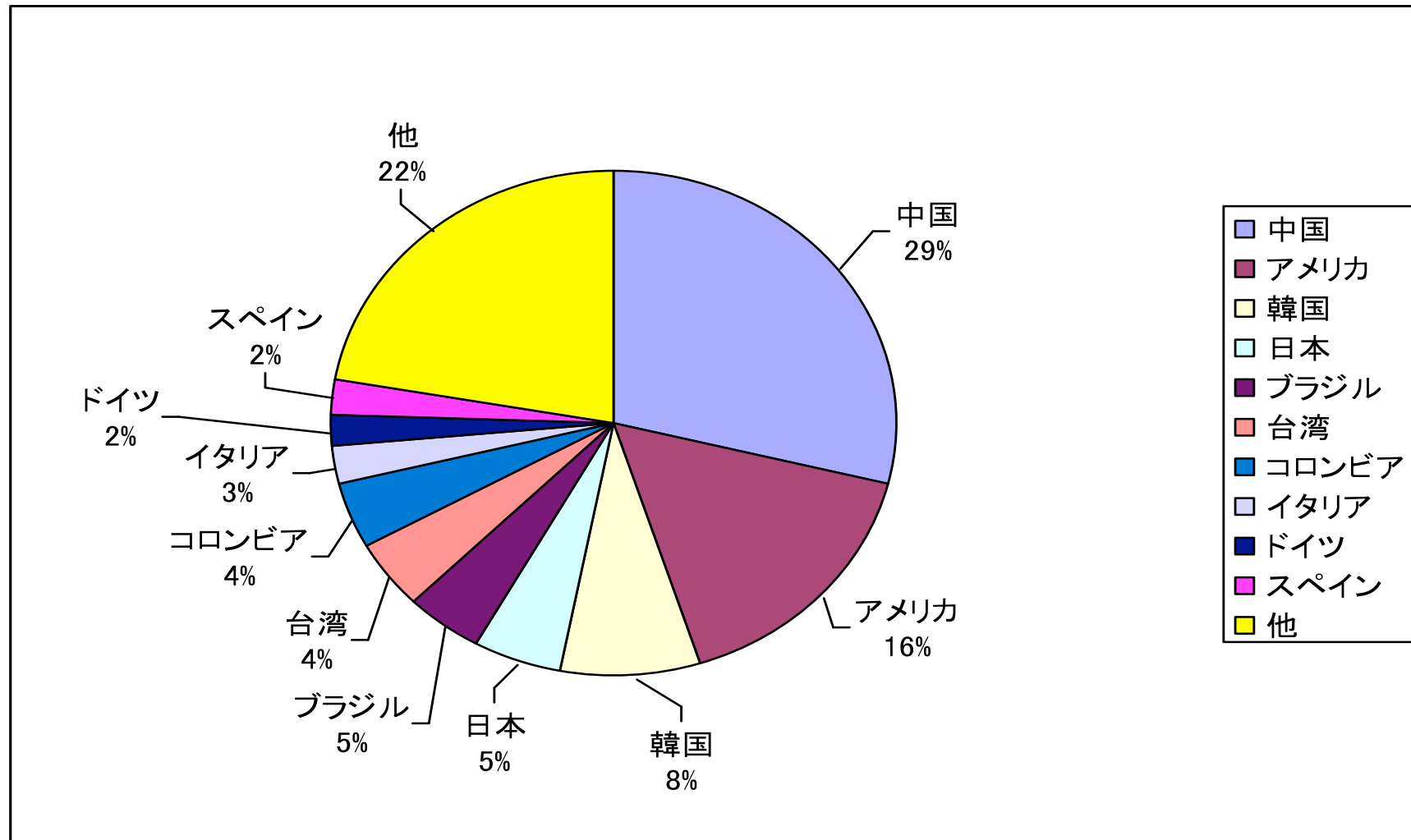
アクセス開始の現地時間

連続アクセス回数

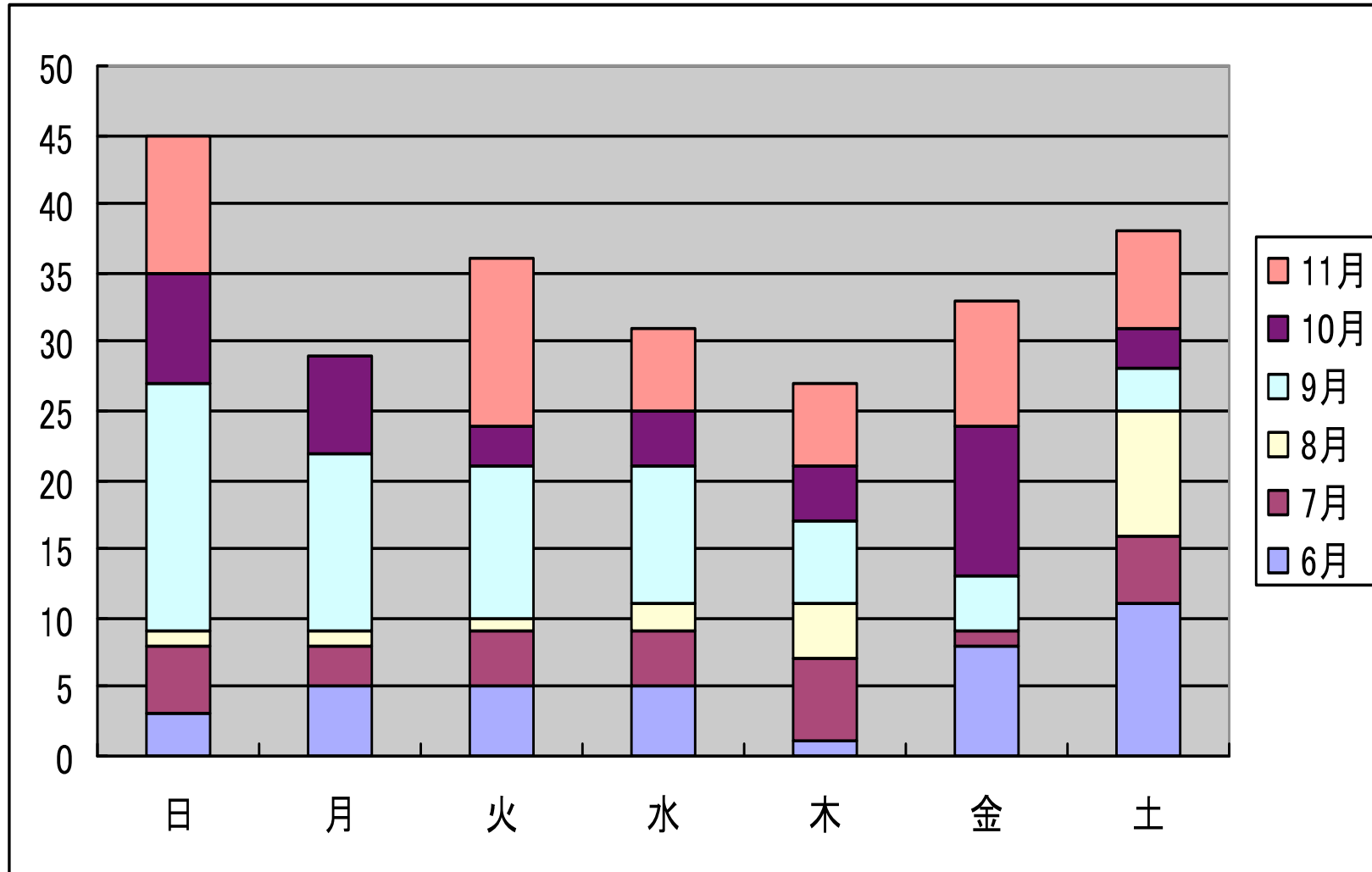
# 国別ホスト数



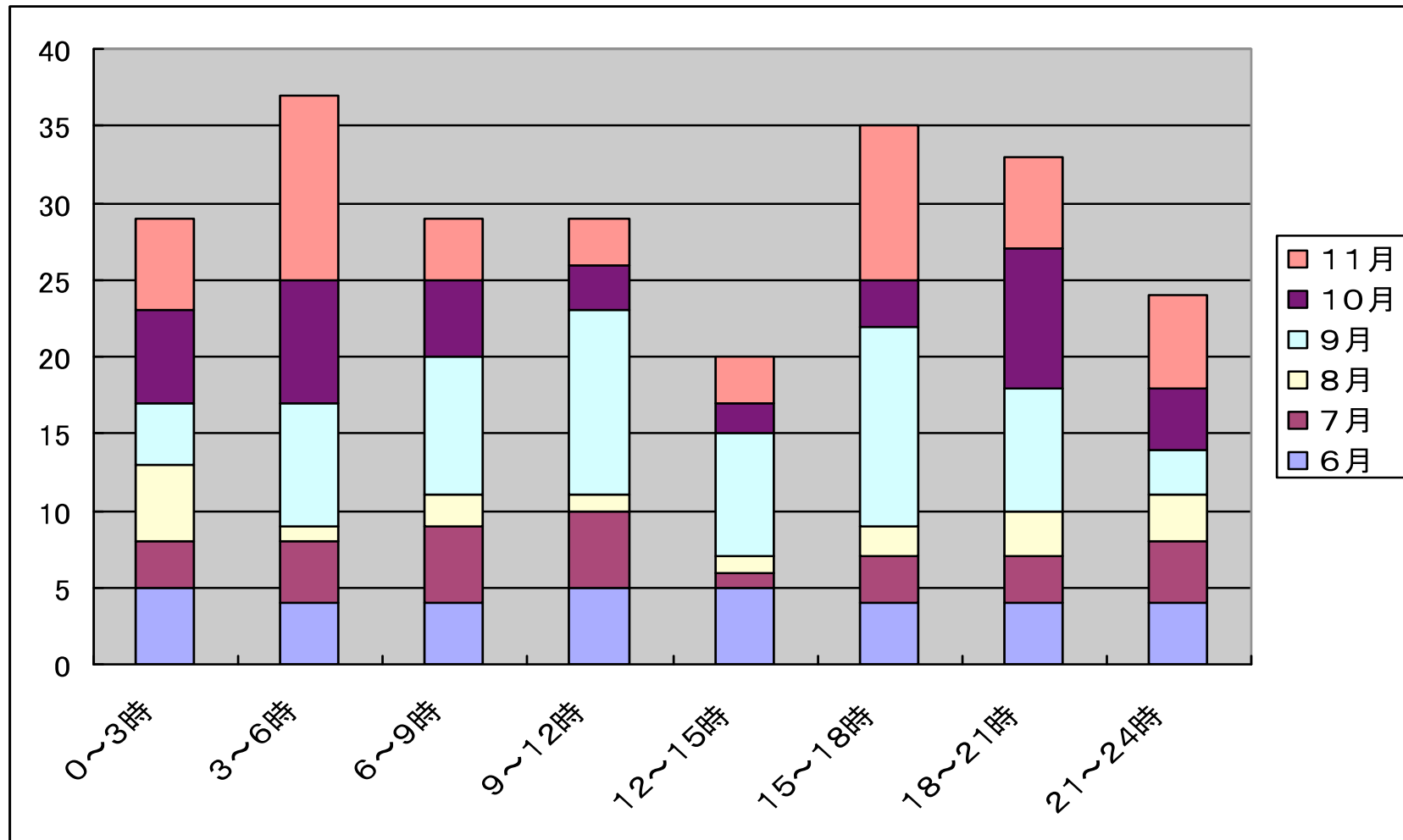
# 国別ホスト数



# 曜日別アクセス数



# 時間帯別アクセス数



# 不正アクセスの結果

---

## 6ヶ月分のホスト数及び不正アクセス数

総ホスト数            237

合計不正アクセス数    119280回

## 最高連続不正アクセス数

5503回

(約7時間)

# 使用頻度の高いuser名

---

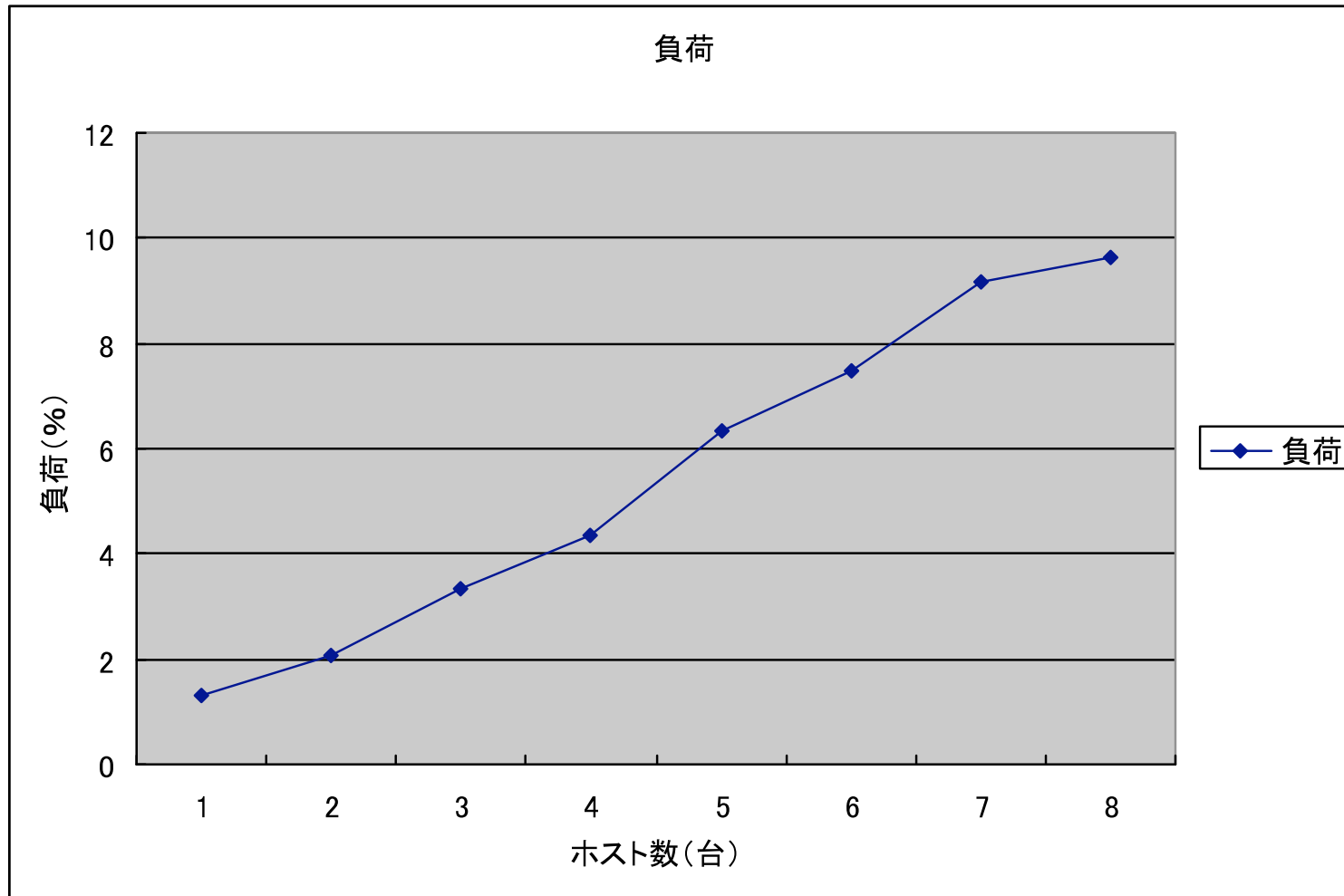
	Root	25744個
test(testuser,test○)		3402個
admin(adminmaster)		2090個
user(username)		1486個
web(webmaster,webtest)		1231個
guest(guest○,guestuser)		762個
oracle(oraclemaster)		623個
www(www-,www○)		416個

# サーバーの負荷計測

---

- サーバの負荷を測定
  - SSHによる不正アクセスが、システムにどのように影響を与えるか調査するため、わざとサーバに不正アクセスをし、計測してみた
- 実験方法
  - 擬似的にSSHで不正アクセスできるツールを使用
  - 研究室サーバーにアクセスし、15分間のload averageを計測
  - 上記の流れでホスト数を増やしていき、負荷を調べていく

# サーバーへの負荷



# 結果のまとめ

---

- 中国、アメリカからの攻撃が圧倒的に多い(全体の45%)
- プログラム制御のため、時間帯、曜日による攻撃の集中化はない
- 辞書攻撃が主流であり、簡単なUser名 (root,admin,testなど)は危険である

# 結論

---

- 使用頻度の高いuser名やパスワードは使用せず、管理を怠らない必要がある
- サーバーへの負荷を考え、規定の回数以上の連続不正アクセスを制限できるツール等を導入するべきである

# SSHサーバーのログ情報

- Jul 27 08:01:24 localhost sshd[6596]: Did not receive identification string from 143.107.128.103
- Jul 27 08:09:52 localhost sshd[6610]: Invalid user tracy from 143.107.128.103
- Jul 26 23:09:52 localhost sshd[6611]: input\_userauth\_request: invalid user tracy
- Jul 27 08:09:52 localhost sshd[6610]: pam\_unix(sshd:auth): check pass; user unknown
- Jul 27 08:09:52 localhost sshd[6610]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=rhost=143.107.128.103
- Jul 27 08:09:52 localhost sshd[6610]: pam\_succeed\_if(sshd:auth): error retrieving information about user tracy
- Jul 27 08:09:55 localhost sshd[6610]: Failed password for invalid user tracy from 143.107.128.103 port 52247 ssh2
- Jul 26 23:09:55 localhost sshd[6611]: Received disconnect from 143.107.128.103: 11: Bye Bye