# 松浦研究室

## [暗号と情報セキュリティ]

生産技術研究所　情報・エレクトロニクス系部門
Department of Informatics and Electronics

情報理工学系研究科
電子情報学専攻

情報セキュリティ

http://kmlab.iis.u-tokyo.ac.jp/

- 侵入テスト
  - 脆弱性の悪用による攻撃を事前に防止するため、優れた技術を持つセキュリティエンジニアによる擬似的な攻撃を行う
  - 非常に有用だが、優れたエンジニアと、多量のコストを要求する

  →深層強化学習を用い、効率的な自動化の可能性を模索する。
- metasploit
  - 多数の攻撃用プログラムをまとめた侵入テスト用フレームワーク。
  - RPCサーバーを介してプログラム内からAPIとして呼び出すことができ、深層強化学習と協調を行うことが可能。

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.56.101   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:
<path>'
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

(上)metasploitの画面

(右)Deep exploitというオープンソースプログラムをもとにした、Metasploit自動化の概念図