

“<sup>じょう ほう</sup>情報セキュリティ<sup>こうぎ</sup>講座” No.4  
(児童向き)

<sup>こわ</sup>怖い “ボットネット”



警察庁 情報通信局 情報技術解析課 作成

ビット先生

「コン太くん、“**ボット**”には<sup>かんせん</sup>感染していない？」

コン太

「えっ、“**ロボット**”のことですか？」

ビット先生

「う～ん、もともとは“**ロボット**”から生まれた<sup>ことば</sup>言葉みたいなんだけど、“**ロボット**”じゃないんだよ。

「じゃあ、“**ボットネット**”っていうのも知らない？」

コン太

「エ？ それ何ですか？ 先生！ 教えて下さい。」



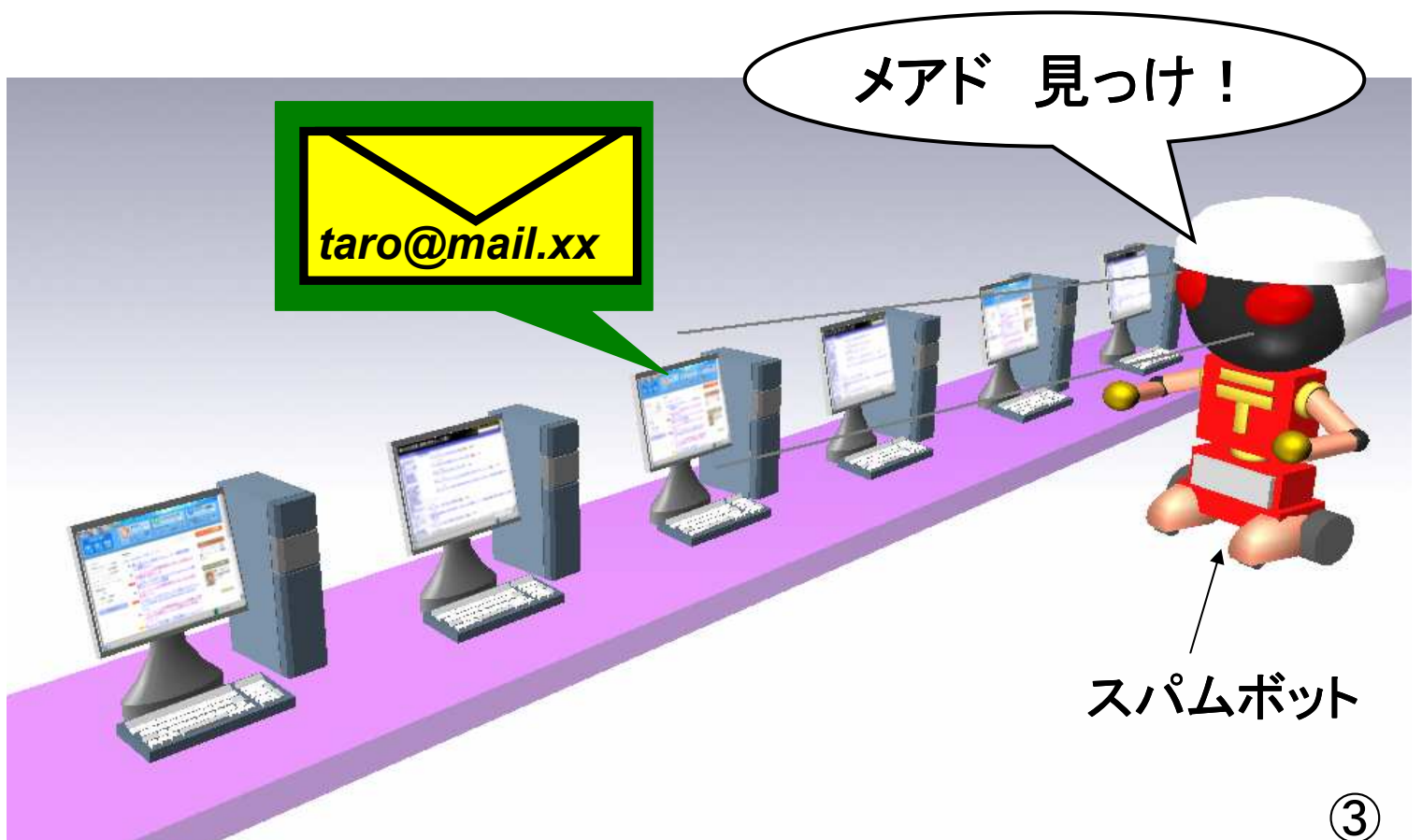
「インターネットを利用する場合に利用される“ロボット”という用語は、“プログラム”のことを指すんだよ。

例えば、“迷惑メール(スパム)”を送付するためにメールのアドレスを調べるプログラムは“アドレス収集ロボット”とか“スパムボット”とも呼ばれているんだ。」

「じゃあ、“ボット”や“ロボット”というのはみんな“悪いプログラム”なんですか？」

「必ずしも悪いとは限らないんだ。

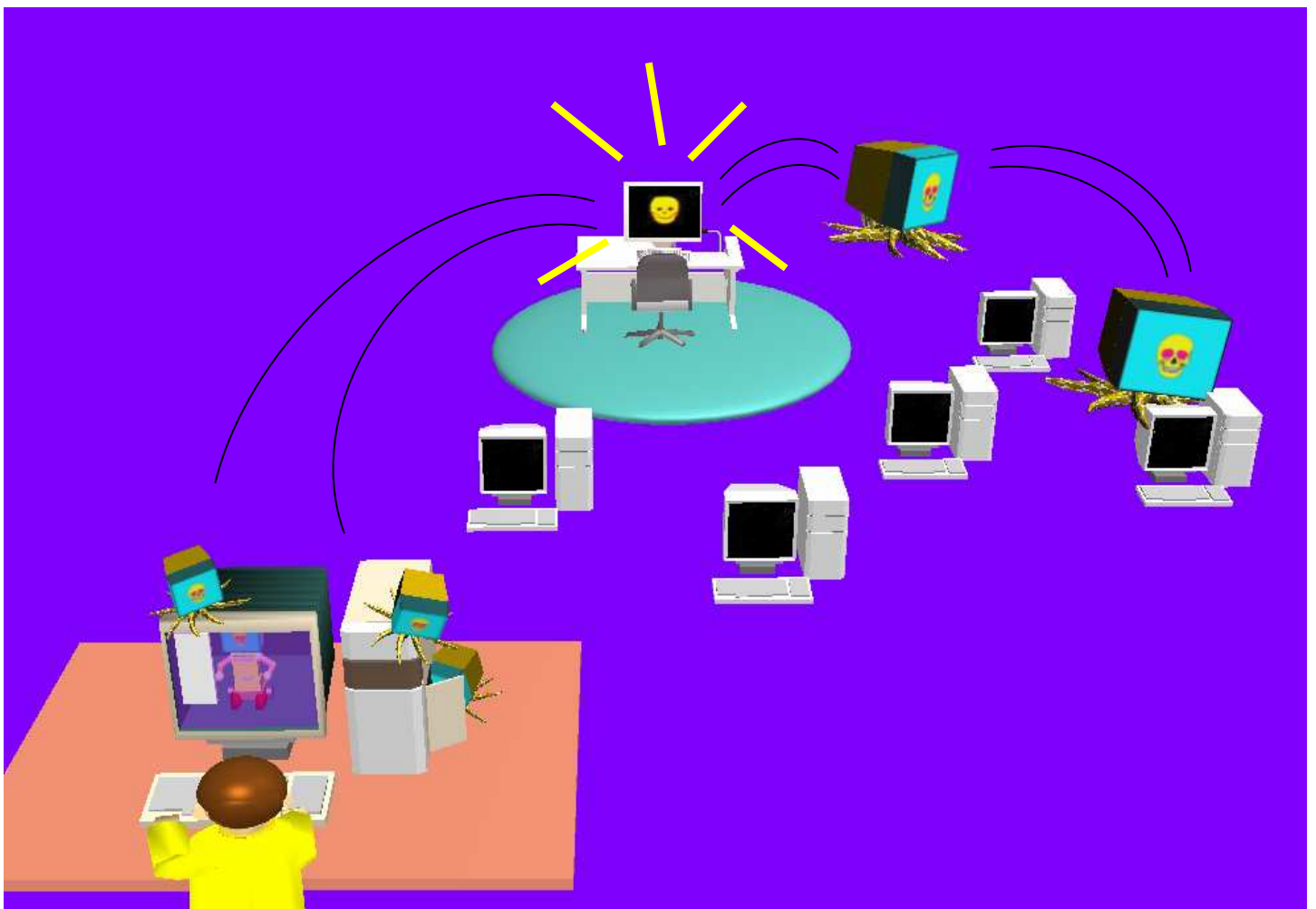
単にホームページ上の情報を集めるだけのプログラムなら“自動収集ロボット”と呼ばれていて、検索サイト等でも利用しているんだよ。」



「まず、“<sup>こわ</sup>ボット”が<sup>かんせん</sup>怖いのは、多くの場合、<sup>かんせん</sup>感染したことに気がつかない、ということかな。

もちろん、コンピュータ・ウイルスやワームも同じなんだけど、“<sup>かんせん</sup>ボット”は、<sup>かんせん</sup>感染を<sup>かくだい</sup>拡大するための<sup>しよくしゆ</sup>“触手”みたいなものを<sup>そな</sup>数多く備えている場合が多いんだよ。

コンピュータの<sup>じゃくてん</sup>弱点を<sup>つ</sup>突いて、知らない間にそのパソコンを乗っ取ってしまうことだってあるんだ。」



「乗っ取られると どうなるんですか？」

「本来の正当なユーザではない者から 指令を受けて、  
他のコンピュータを一斉に攻撃したり 感染を拡大さ  
せる“ボット”になってしまうんだよ。

このような状態になることを“ボット化”、あるいは  
“ゾンビ化”といい、その“ボット”の集団は“ボットネット”  
と呼ばれるんだ。

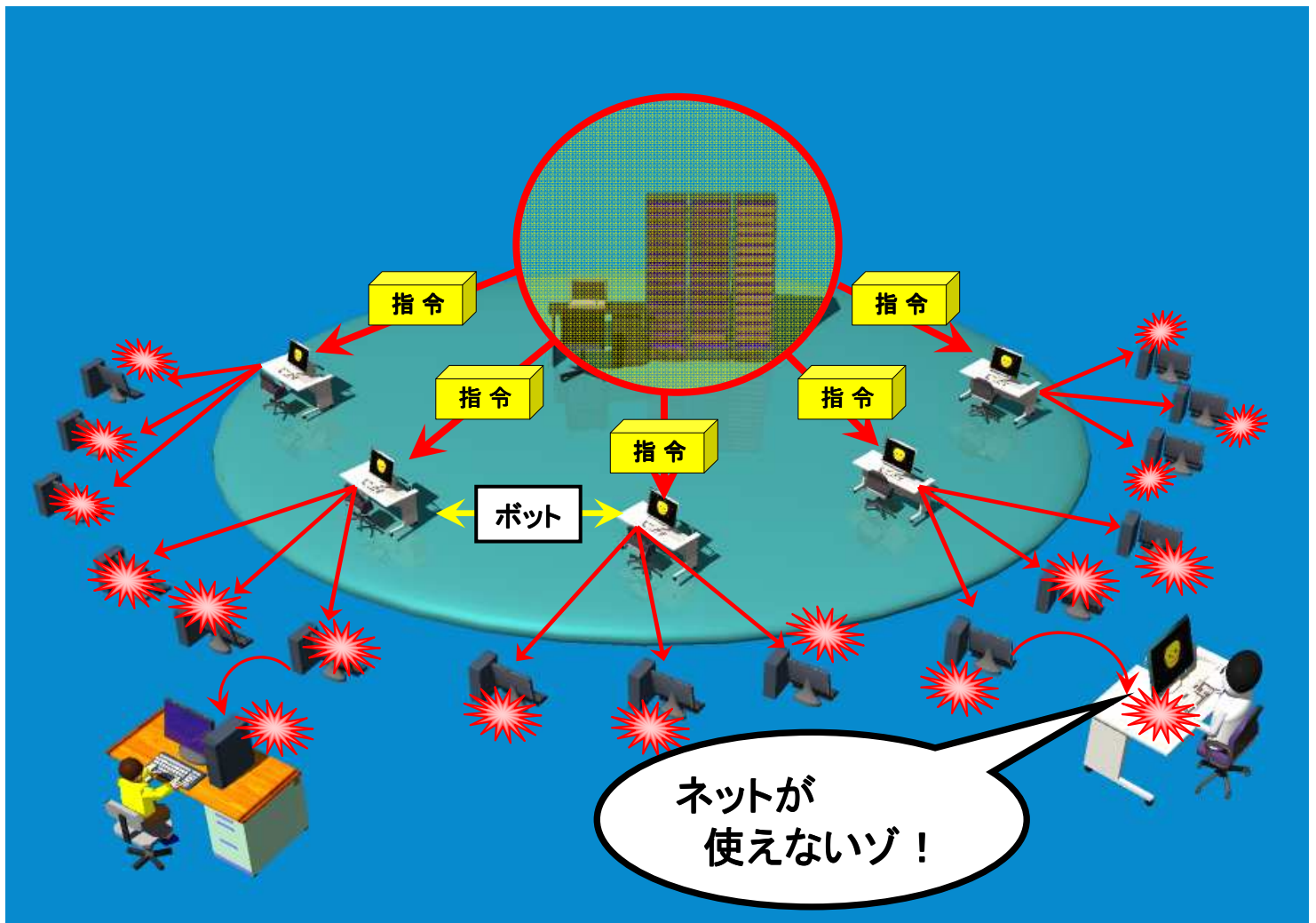
まるで、軍隊のように 命令する者の意のままにあや  
つられることから、“ゾンビ・アーミー”と呼ばれることも  
あるんだよ。」



「“**ボット**”は“**指令**”を受け取ると、その“**指令**”に忠実ちゆうじつに従って、**攻撃**を行うんだ。  
したが こうげき

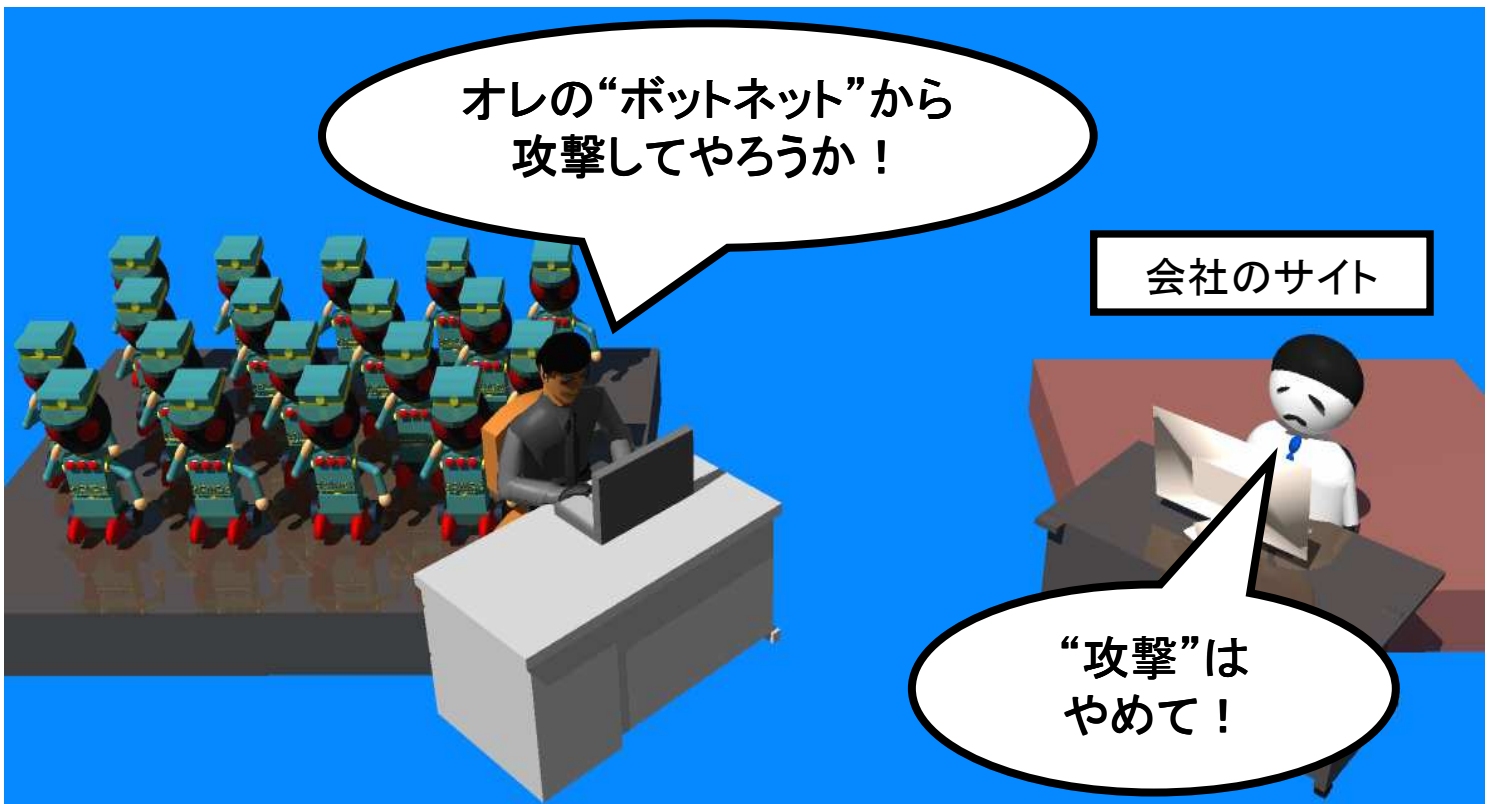
特に、数千、数万の“**ボット**”で構成される“**ボット**  
**ネット**”の場合には、一斉に他のコンピュータを**攻撃**  
すれば、サーバのみならず、インターネット自体の  
機能を麻痺させるような“**サービス妨害攻撃** (DoS、  
または**ドス攻撃**)”を行うことも可能なんだ。  
こうせい いっせい こうげき ぼうがい こうげき かのう

悪いやつが使えば、“**サイバーテロ**”だって起こせてしまうんだよ。」



「国内でも数十万台もの“<sup>そんざい</sup>ボット”が存在していると言われているんだけど、海外では、何百万台ものコンピュータが“<sup>かんせん</sup>ボット”に感染しているらしい。

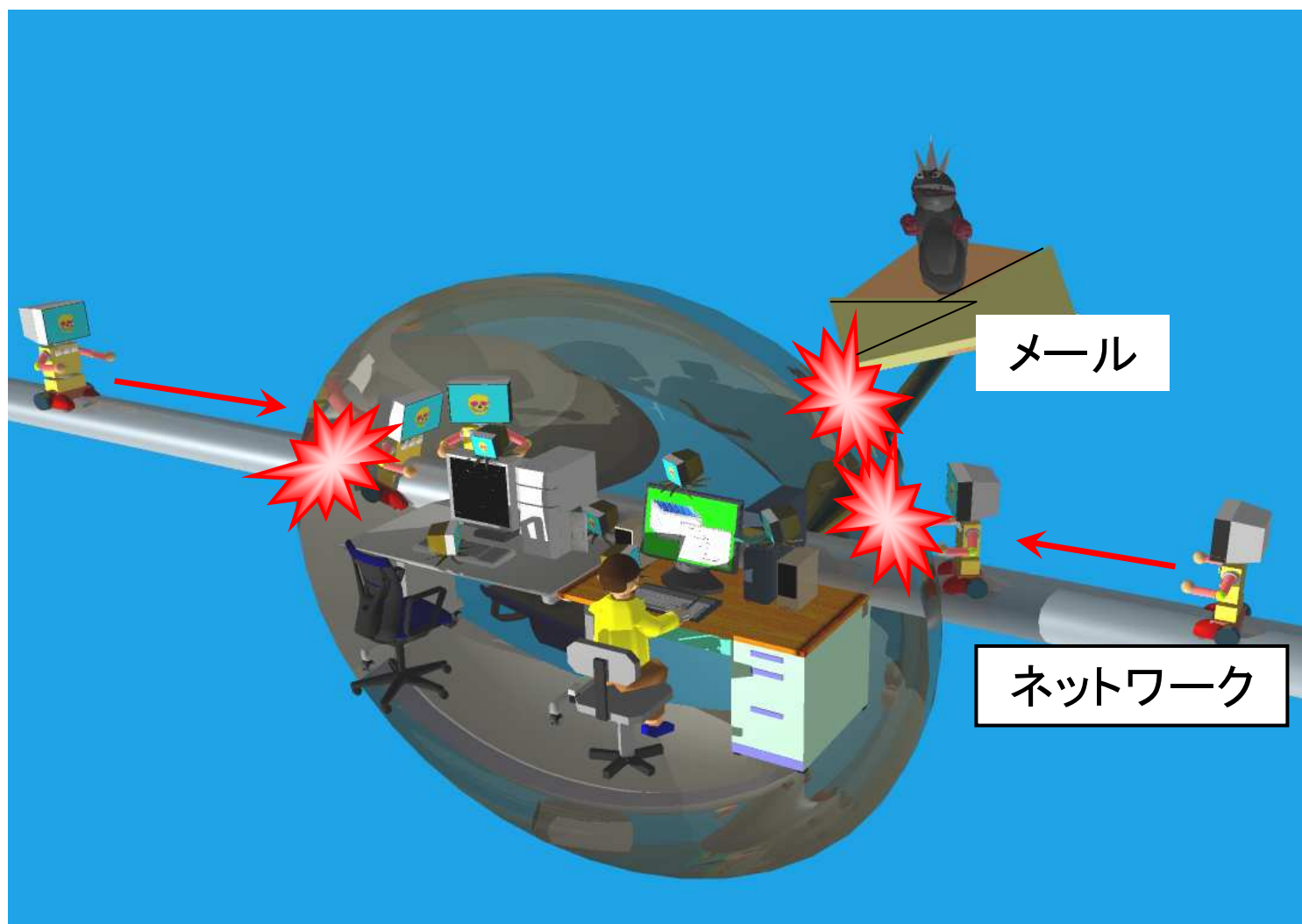
それに、<sup>じっさい</sup>実際に“ボットネット”を使って<sup>こうげき</sup>攻撃を行うだけでなく、会社などに対して「<sup>こうげき</sup>攻撃するぞ！」と<sup>きょうはく</sup>言って脅迫する、という事件も発生しているんだよ。」



「“ボット”には <sup>かんせん</sup> どのように感染するのですか？」

「“ボット”もウイルスやワームと同様、メールに添付 <sup>てんぷ</sup> されていたり、ネットワークを <sup>けいゆ</sup> 経由して <sup>かんせん</sup> 感染が <sup>かく</sup> 拡大 <sup>だい</sup> するんだよ。

だから、常に <sup>つね</sup> セキュリティを <sup>じやくてん</sup> チェックして、弱点が 無いようにコンピュータをガードしておくことが必要 なんだよ。」

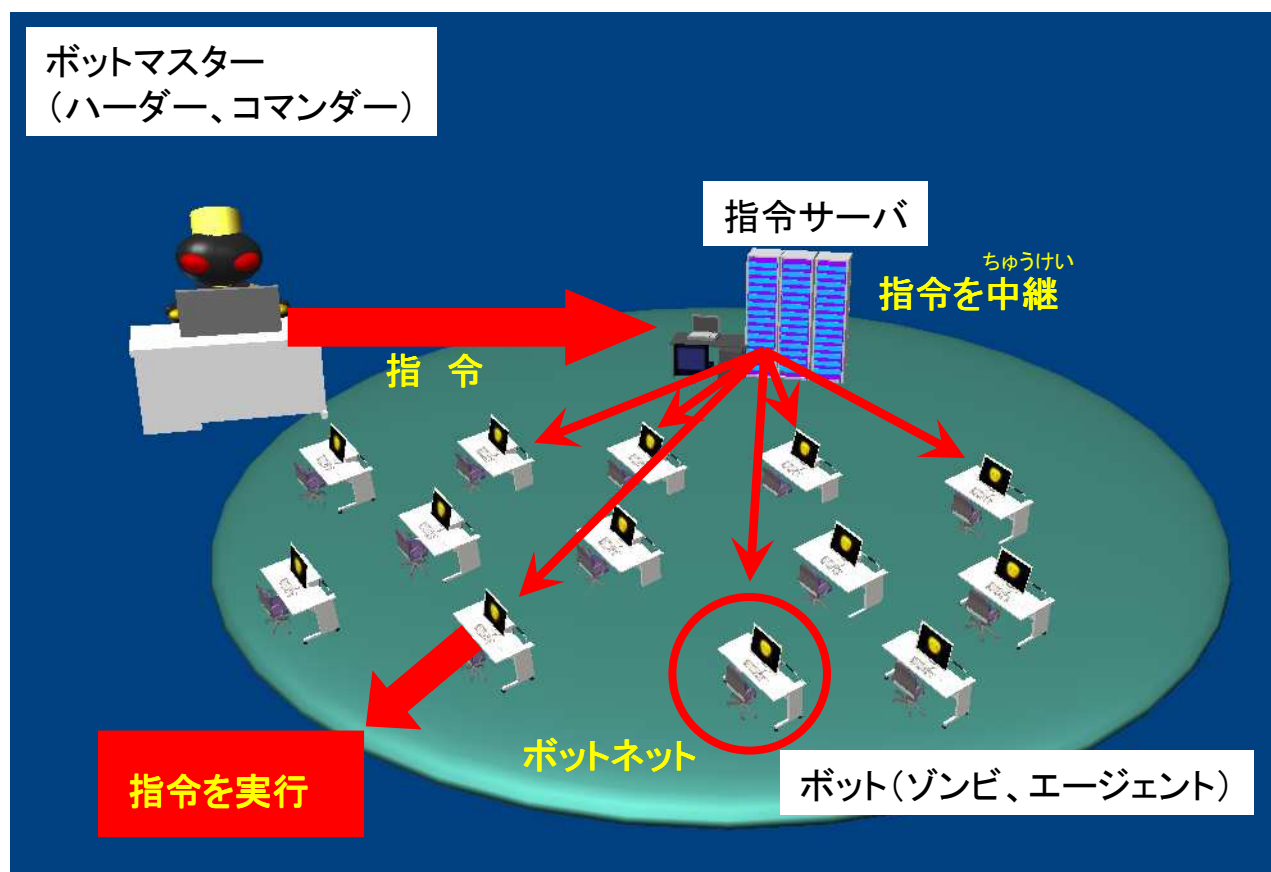


「“<sup>こうせい</sup>ボットネット”の構成はどうなっているんですか？」

「<sup>じっさい</sup>実際の<sup>こうげき</sup>攻撃等を<sup>しじ</sup>指示する“<sup>しじ</sup>ボットマスター”と多くの  
“<sup>こうせい</sup>ボット”で“<sup>こうせい</sup>ボットネット”は構成されている。

<sup>いっせい</sup>一斉に活動を開始させるのに便利なので、<sup>しじ</sup>指令  
を<sup>ちゅうけい</sup>中継するために“<sup>けいゆ</sup>指令サーバ”を経由して<sup>しじ</sup>指示  
を<sup>でんたつ</sup>伝達することも多いんだよ。

“<sup>こうせい</sup>ボット”は“<sup>ゾンビ</sup>ゾンビ”とか“<sup>エージェント</sup>エージェント”と呼ば  
れることもあるんだよ。」

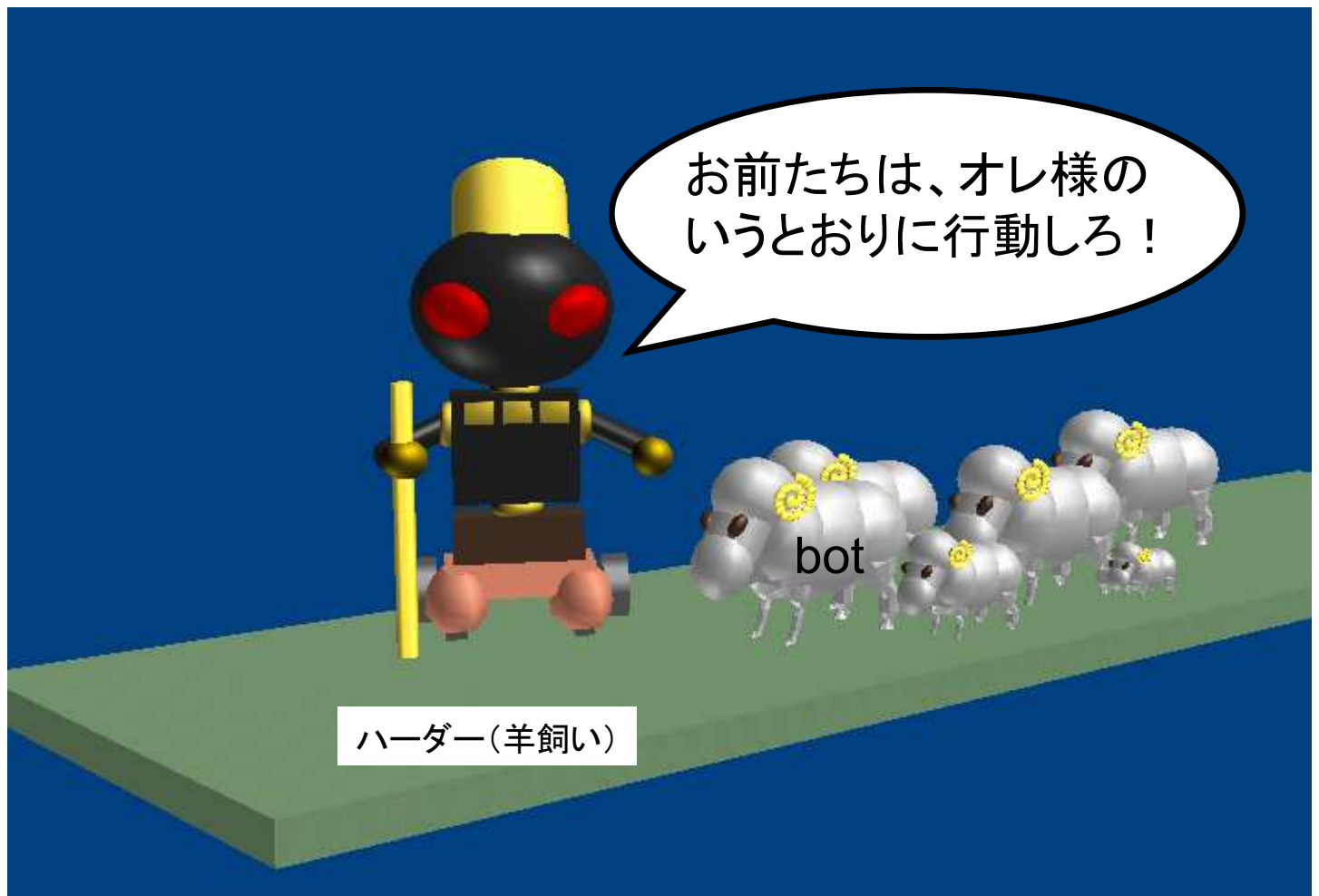


「“ボットマスター”は“ハーダー”とか“コマンダー(指  
令官)”とも呼ばれるんだよ。

ひつじか

“ハーダー”というのは、もともとは“羊飼ひつじかい”という  
意味で、“ボット”に感かん染せんしたパソコンを自在じざいに操あやつる、  
という意味がこめられているんじゃないかな。」

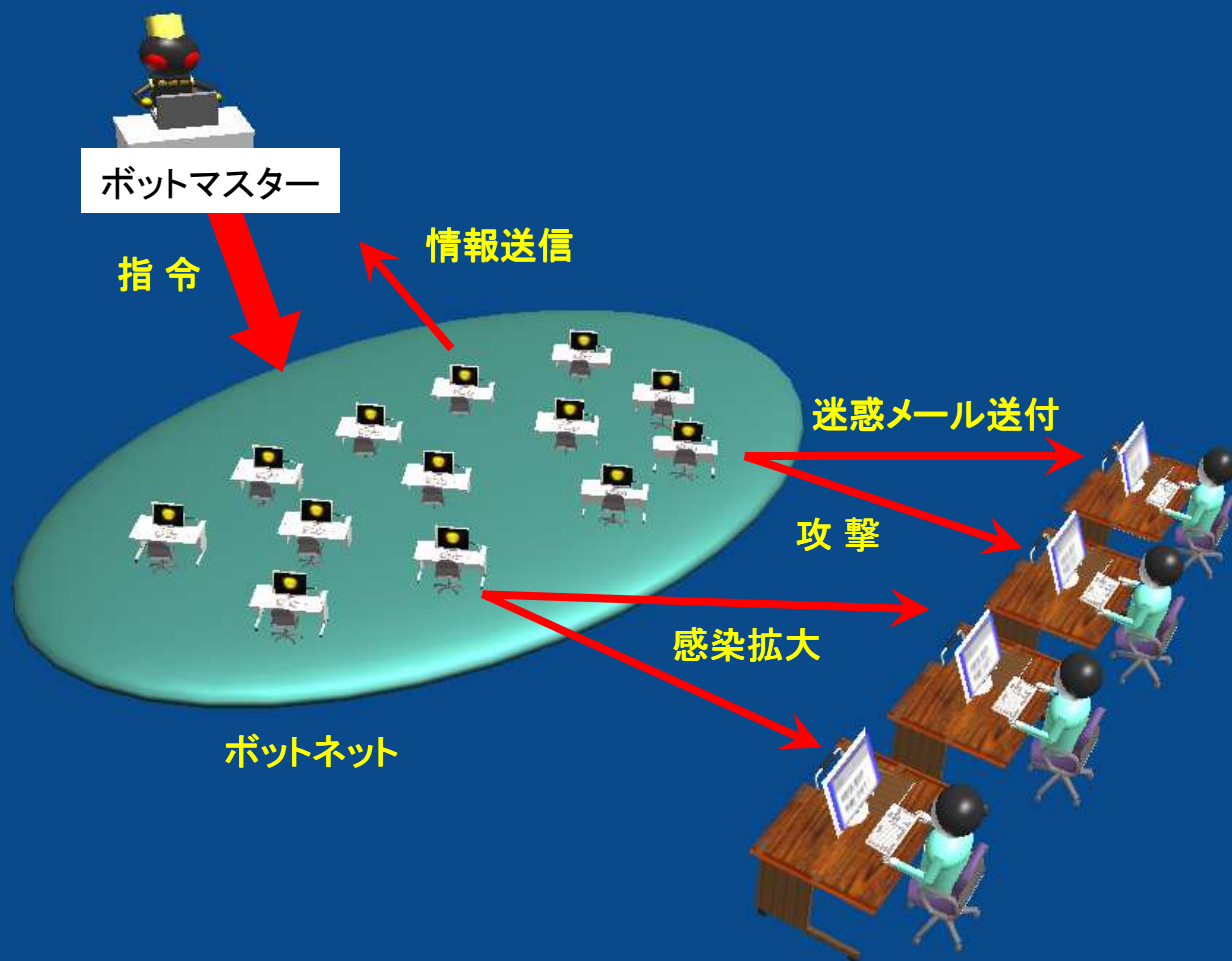
「自在じざいに操あやつる”ってどういうことなんですか？」



「特定の対象に対する攻撃を指示したり、“ボット”の感染を拡大させる、という命令を出すこともできるんだよ。

“攻撃”を指示するだけでなく、迷惑メールの送付を指示したり、コンピュータを使っている人がキーボードから入力した情報等を収集して送信させたりすることもできるんだよ。」

「でも、先生！ それって “ウイルス” や “スパイウェア” と同じじゃないですか？」



かん せん

「“ウイルス”の場合には、感染した直後から、あるいはあらかじめ決められたタイミングや条件を満足した場合に行動を開始するんだけど、“ボット”の場合には、“ボットマスター”が命令するまで待っている、というところが違うんだよ。」

時間がきたので  
データもらって  
いこまーす。

ウイルス

データ

ヤレ！

ボット  
マスター

命令されたんで  
データもらって  
いくよ。

ボット

データ

「先生、“ボットネット”の活動状況は <sup>かんし</sup>きちんと監視できるんですか？」

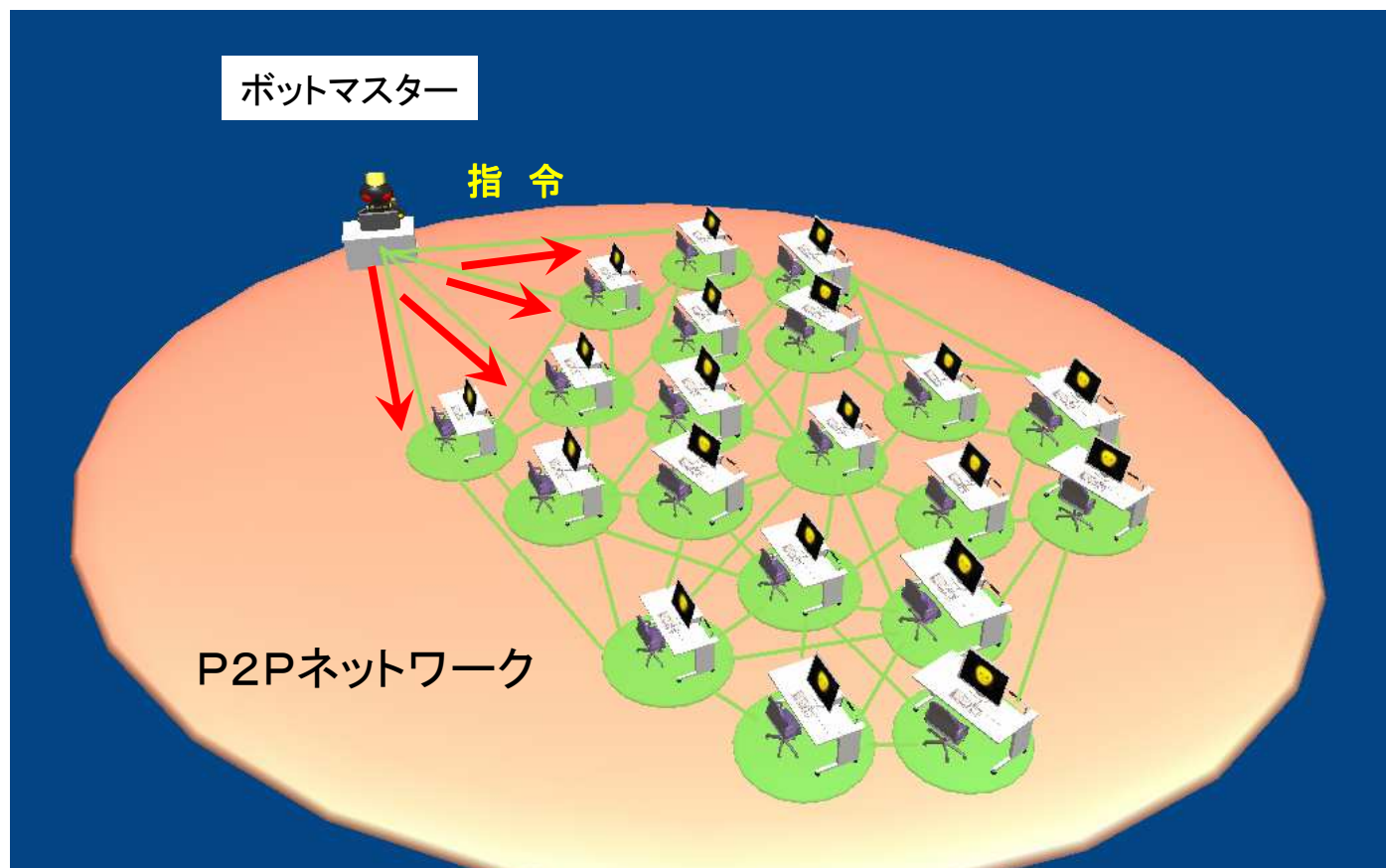
「う～ん。“ボット”に感染しているコンピュータ <sup>みわ</sup>を見分けることはなかなか <sup>むずか</sup>難しいんだよ。

<sup>けいさつちょう</sup>警察庁のサイバーフォースセンターでも2005年から <sup>かんし</sup>監視しているんだけど、他のコンピュータを <sup>むさべつ</sup>無差別に <sup>こうげき</sup>“攻撃”したりする <sup>のぞ</sup>ような場合を除いては、<sup>ぜんよう</sup>全容を <sup>はあく</sup>把握 <sup>むずか</sup>することは難しいんだよ。」



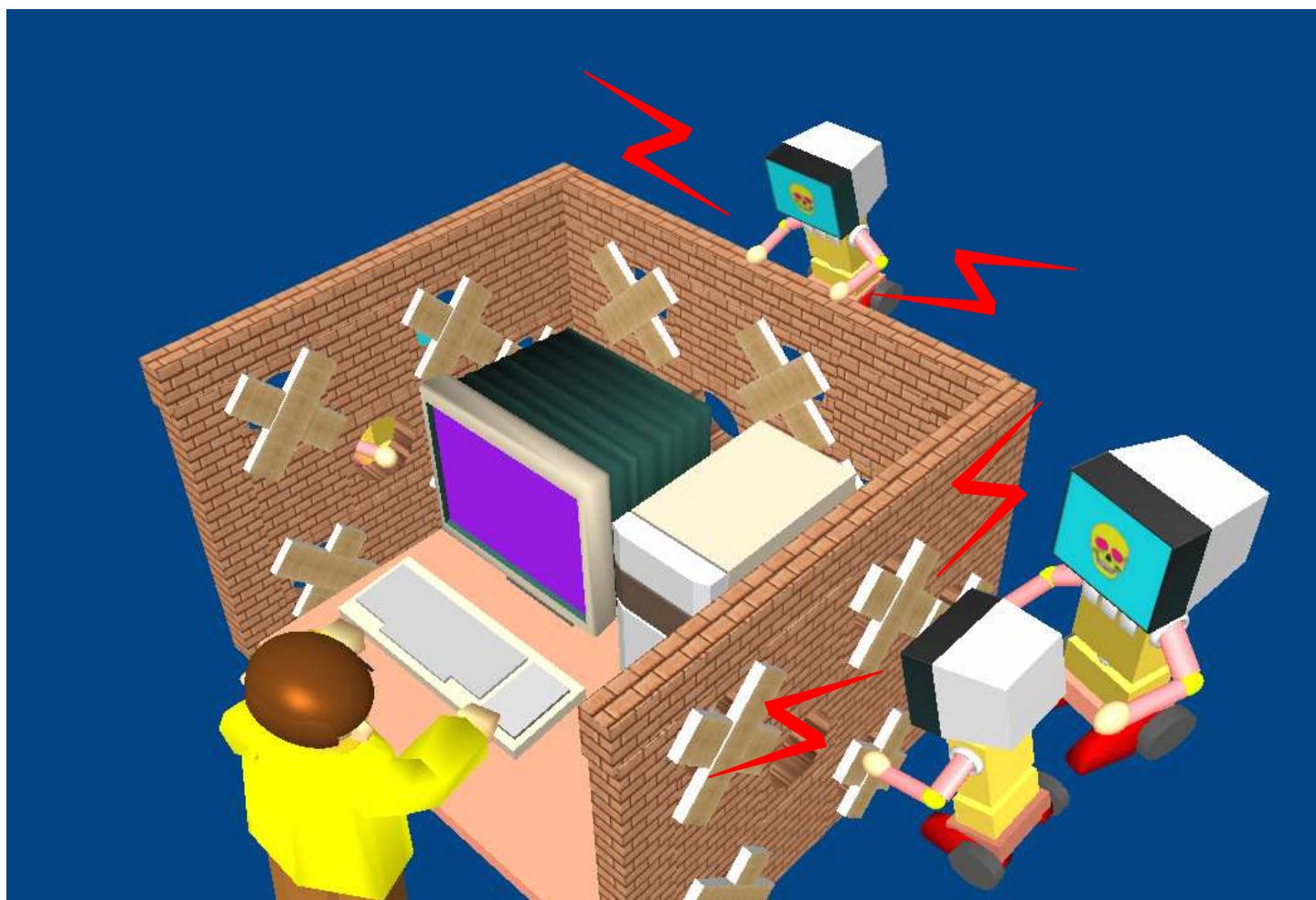
「今までは、“指令サーバ”として“チャット”等で利用するサーバを利用することが多かったんだけど、最近<sup>さいきん</sup>は監視<sup>かんし</sup>の目<sup>の</sup>を逃<sup>のが</sup>れるためにインスタント・メッセージやファイル共有ソフト等で利用するP2Pネットワークを利用したり ホームページを見るのと同じような通信手法で指令を伝える“ボットネット”も登場<sup>とうじょう</sup>し、正確<sup>せいかく</sup>な活動<sup>じつたい</sup>実態<sup>じつたい</sup>の把握<sup>はあく</sup>はできていないんだ。」

「じゃあ、まずは感染<sup>かんせん</sup>を防<sup>ふせ</sup>がなくてはいけませんね。  
先生！ どのようなことに注意すればいいんですか？」



「“ボット”に感染しないためには、ウイルスやスパイ  
ウェア対策と同じで、きちんと対策ソフトを導入し その  
定義ファイルもきちんと更新する等の作業を継続して  
実施することが不可欠なんだよ。

また、他のコンピュータを感染させたり攻撃する場合  
には、特定のポートを利用することが多いので、ファイ  
アウォール機能等を確実に動作させて これらの動作  
を阻止することが重要なんだ。」



「先生、“**ボットネット**”は<sup>おそ</sup>恐ろしいけど、<sup>かんせん</sup>感染しないように気をつけ、  
そして<sup>かんせん</sup>感染した場合には<sup>ただ</sup>直ちに<sup>くじよ</sup>駆除することにより、被害の拡大  
をくい止めることが可能なんです。」

「そうだよ。ひとりひとりの心がけと地道な<sup>じみち</sup>努力が<sup>どりよく</sup>あれば、  
“**ボットネット**”を<sup>こんぜつ</sup>根絶することは 決して<sup>むり</sup>無理じゃないん  
だよ。」

おわり

文と絵 はむろえいたろう

@police

<http://www.cyberpolice.go.jp/>



この資料は、非商用に限り 印刷又は配布して活用することが可能です。

ただし、資料の部分的な抜粋や利用はおやめ下さい。