情報セキュリティ

第3回： 攻撃について

授業計画

① ガイダンス
② インターネット上の脅威について
③攻撃について
④ コンピュータウイルス（マルウェア）について
⑤ 小テスト，ネットワーク上の各種攻撃の紹介
⑥ 攻撃の技術
⑦ 情報・ネットワーク技術の基礎
⑧ ネットワークセキュリティに関する技術と方法
⑨ 暗号の基礎
⑩ 小テスト，セキュリティ技術と方法に対する確認
⑪ 対処法１（システムリスク）
⑫ 対処法２（ソーシャルリスク：SNS）
⑬ 対処法３（ソーシャルリスク：インターネット・スマホゲーム）
⑭ 対処法に関する小テスト
⑮ 全体のまとめ

本日の講義内容

1. 攻撃の分類
2. セキュリティリスクの外部要因と内部要因
3. 情報資産の価値とその評価方法
4. 攻撃への対策

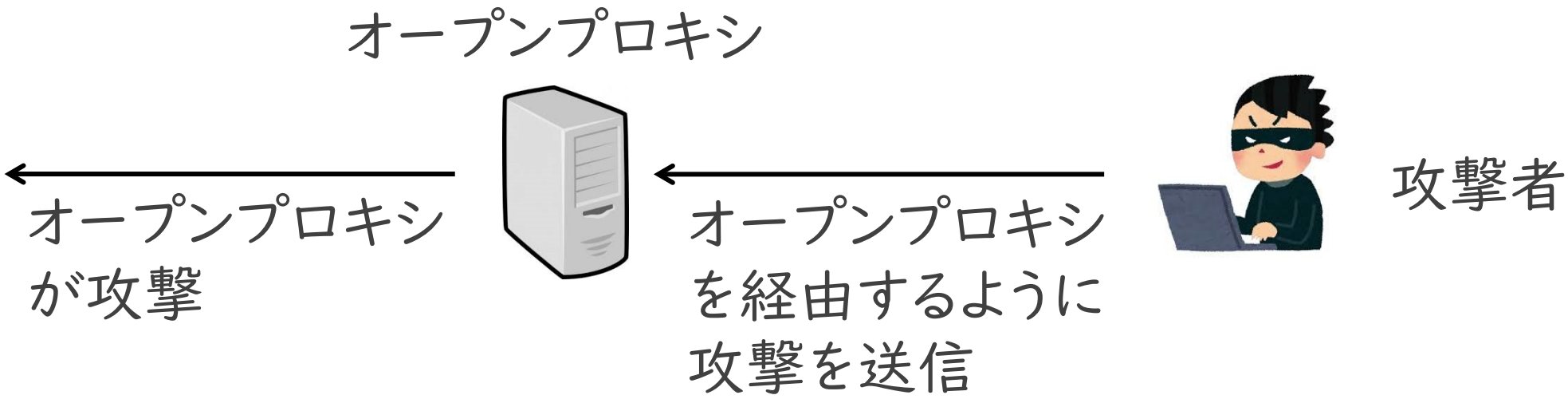
1. 攻撃の分類

1.1 サイバー攻撃の仕組み

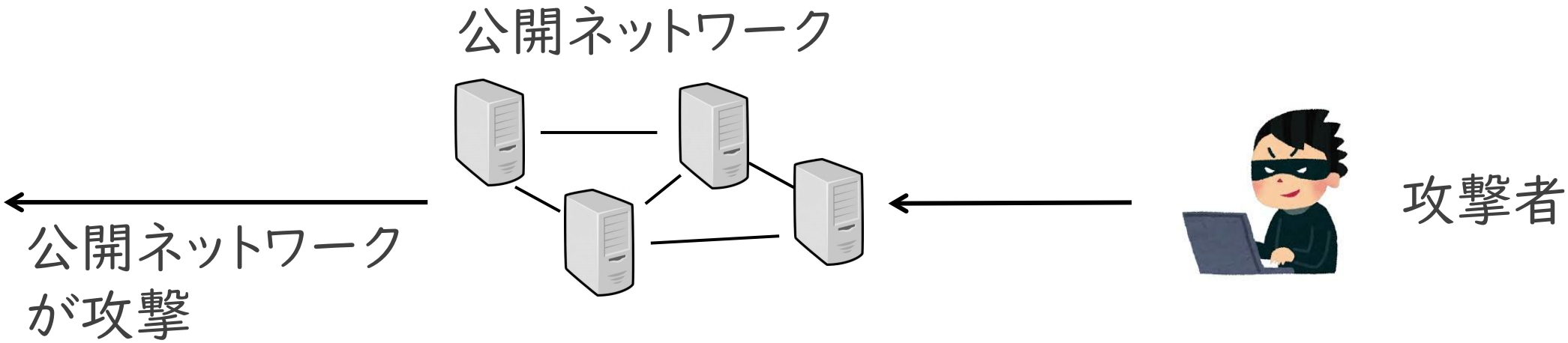
サイバー攻撃とは，情報端末やネットワークに侵入してデータの窃取や破壊を実施したり，システムを機能不全にしたりする行為です．

攻撃者は，自身の存在を隠ぺいしながら，他人のホストを経由して攻撃を実施します．

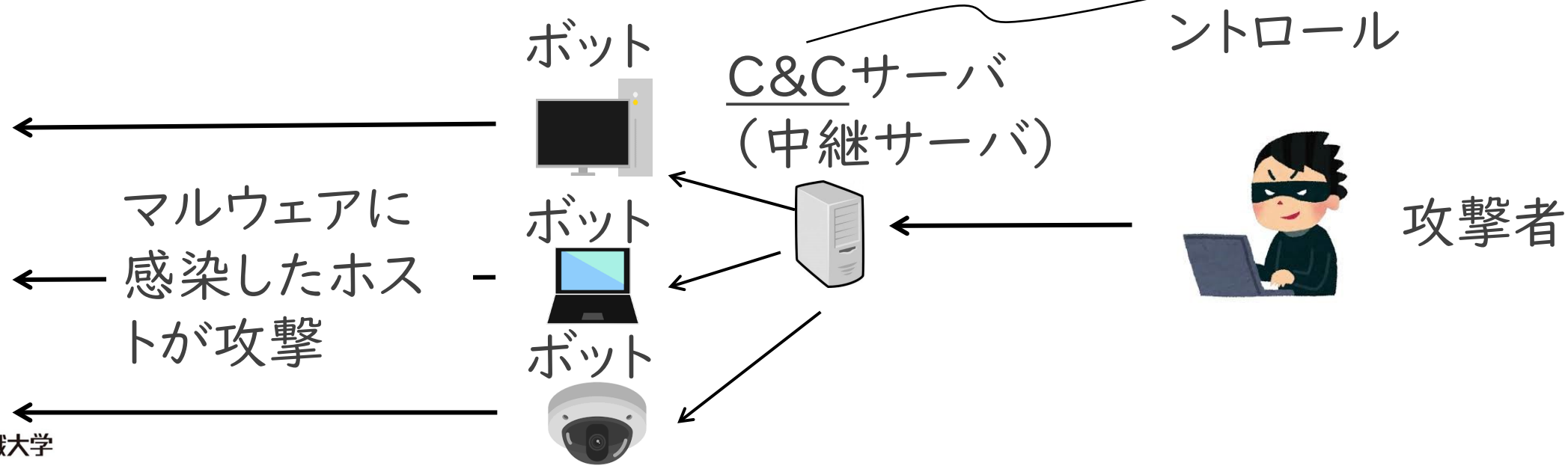
① オープンプロキシ（第三者が用意した代理アクセス用サーバ）を使う



② 一般公開されているネットワーク（例：Tor）を使う



③ 他人のホスト（ボットネット）を使う



1.2 攻撃の対象と仕掛け方による分類

- 攻撃対象が産業システムにも広がりました.
- 攻撃方法も高度化して特定組織を狙った標的型攻撃が行われるようになりました.
- 攻撃目的も国家によるサイバー攻撃, 犯罪者による金銭目的, ハクティビストによる主義主張の目的などに多様化しました.

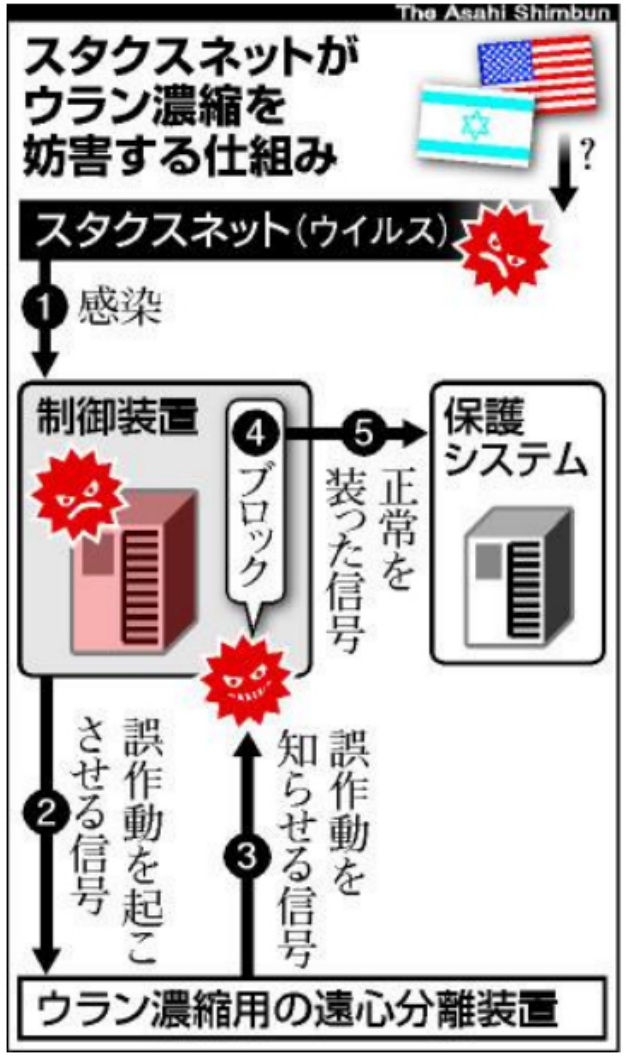
攻撃の対象	攻撃の仕掛け方	特徴
標的型	能動的	• 特定対象に対して直接攻撃する • 攻撃される側の行動は不要で, いつでも攻撃可能
	受動的	• 特定対象に対して直接攻撃する • 攻撃者は, 利用者が特定の行動をとるよう誘導する
非標的型	能動的	• 不特定多数の対象に対して攻撃する • 攻撃される側の行動は不要で, いつでも攻撃可能
	受動的	• 不特定多数の対象に対して攻撃する • 攻撃者は, 利用者が特定の行動をとるよう誘導する

1.3 攻撃の目的による分類

- 攻撃の目的は，自己満足・信念のみならず，経済的利益や信仰・国防まで含まれます．
- サイバー犯罪の産業化・組織化・分業化が行われています
- 国家が関与する攻撃も増えています（APT＝Advanced Persistent Threat）．

攻撃の目的		攻撃者
自己満足・信念	ハクティビスト	集団，個人
	ネット被害	集団，個人
	興味本位	個人
経済的利益	サイバー犯罪	組織，集団，個人
信仰・国防	国家危機管理	国家
	サイバーインテリジェンス	国家，組織
	サイバーテロ	組織，集団，個人

イラン核施設の妨害ウイルス イスラエルと米国が開発か



産業制御システムを乗っ取る新しいコンピューターウイルス「スタクスネット」が、国家が関与するサイバー攻撃の一環として開発された可能性が高まってきた。16日付の米紙ニューヨーク・タイムズは、イランのウラン濃縮を妨害する狙いで、イスラエルがスタクスネットの試験を行っていたと報じた。米国の核技術専門家らの証言などが根拠で、開発には米国も協力していたという。

（朝日新聞, 2011.01.16）

2. セキュリティリスクの外部要因と内部要因

2. 1　外部要因

（1）マルウェア（サイバー攻撃に使われる重要な「武器」）

ウイルス，スパイウェア，ボット，ランサムウェアなどの悪意のあるプログラムの総称．最近は，マルウェアが巧妙化・凶悪化し，感染の兆候が目に見えず，脅威が見えにくくなっている特徴があります．一般の利用者が感染に気付くことは困難になっています．情報の盗みだしやスパムメールの発信，DDoS攻撃の踏み台として使われたりしているのです．

国内マルウェア検出数上位（2023年9月）

順位	マルウェア名	割合	種別
1	DOC/Fraud	21.4%	詐欺サイトのリンクが埋め込まれたDOCファイル
2	JS/Adware.Agent	15.2%	アドウェア
3	HTML/Phishing.Agent	12.0%	メールに添付された不正なHTMLファイル
4	JS/Adware.TerraClicks	7.4%	アドウェア
5	JS/Adware.Sculinst	5.2%	アドウェア
6	JS/Agent	3.9%	不正なJavaScriptの汎用検出名
7	HTML/Fraud	2.6%	詐欺サイトのリンクが埋め込まれたHTMLファイル
8	Win32/Exploit.CVE-2017-11882	1.8%	脆弱性を悪用するマルウェア
9	JS/Adware.Subprop	1.3%	アドウェア
10	MSIL/TrojanDownloader.Agent	1.2%	ダウンローダー

（2）外部からの侵入（不正アクセス）

- 攻撃用ツール
  スニファ（sniffer）：ネットワーク盗聴
  ポートスキャン（port scan）：通信に使用するポートの状態調べ
  パスワードクラッキング（password cracking）：パスワード解析
  など
- 侵入行為の段取り
  事前調査 ⇒ 権限取得 ⇒ 不正実行 ⇒ 後処理

  パッケージされているマルウェアを各段階の攻撃ツールとして使います．感染後に，特定のWebサイトにアクセスし，別の不正プログラムをダウンロードし，不正実行機能をバージョンアップしていくということもあります．

（3）サーバへの攻撃（サービス妨害）

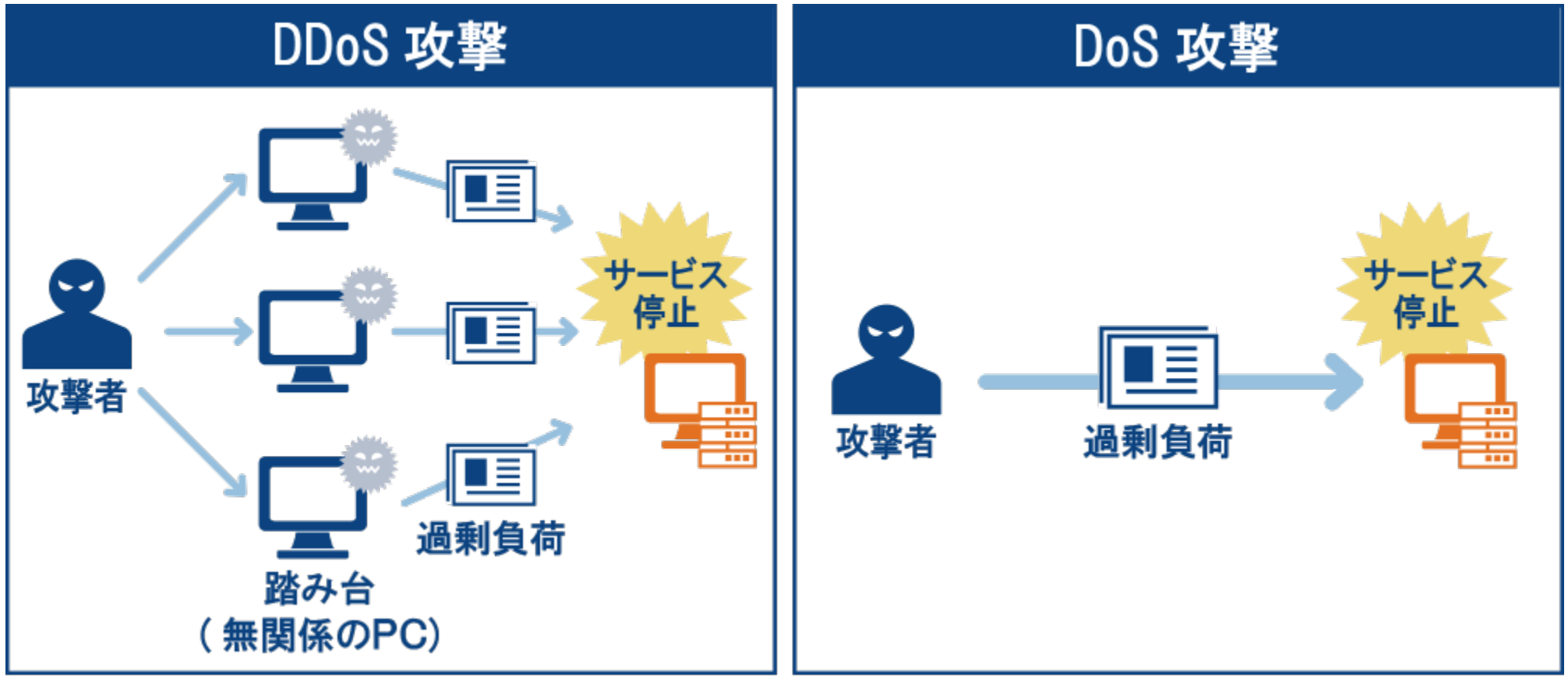
- Webサーバ
  ユーザのブラウザからのリクエストに応じてコンテンツを提供しています．サーバアドレスが公開されていますので，攻撃のターゲットとしてねらわれやすい．

- メールサーバ
  メールサービスが利用され，メールの集配を行います．サーバアドレスが入手できますので，攻撃を受けやすい．

- DDoS攻撃（Distributed DoS: 分散DoS攻撃）

  DoS攻撃：サーバに大量のデータを送って過大な負荷をかけ，サーバのパフォーマンスを極端に低下させたり，サーバを機能停止に追い込んだりする攻撃（Denial of Service）
  DDoS攻撃：世界中に散らばった非常に多くの端末からいっせいに仕掛ける攻撃のこと．以下のような手口が使われます．

  - ボットネットワーク
  - リフレクター攻撃（ルータやDNSサーバに偽装送信し，応答結果を標的組織に送りつける）
  - DNS水責め攻撃（標的組織のランダムなサブドメインへ問い合わせ，DNSサーバに負荷をかける）


DDoS 攻撃
攻撃者
サービス
停止
過剰負荷
踏み台
（無関係のPC）
DoS 攻撃
攻撃者
過剰負荷
サービス
停止

2.2 内部要因

（1）情報システム（コンピュータやソフトウェア）の脆弱性

脆弱性とは，セキュリティ上の弱点を指します．セキュリティホールとも呼びます．

- OSの脆弱性
  コンピュータにおいてはWindows，Linux，Mac OSなどが，スマートフォンにおいてはiOSやAndroidなどが利用されていますが，脆弱性が存在しています．基本的なソフトウェアであるため，脆弱性による影響が広範囲を及びます．
- ソフトウェア（アプリケーション）の脆弱性
  設計上の問題またはコーディング上の問題によって脆弱性が組み込まれました．例：Webブラウザ，メールソフト，動画再生プレーヤー，ファームウェア，ドライバーなど．

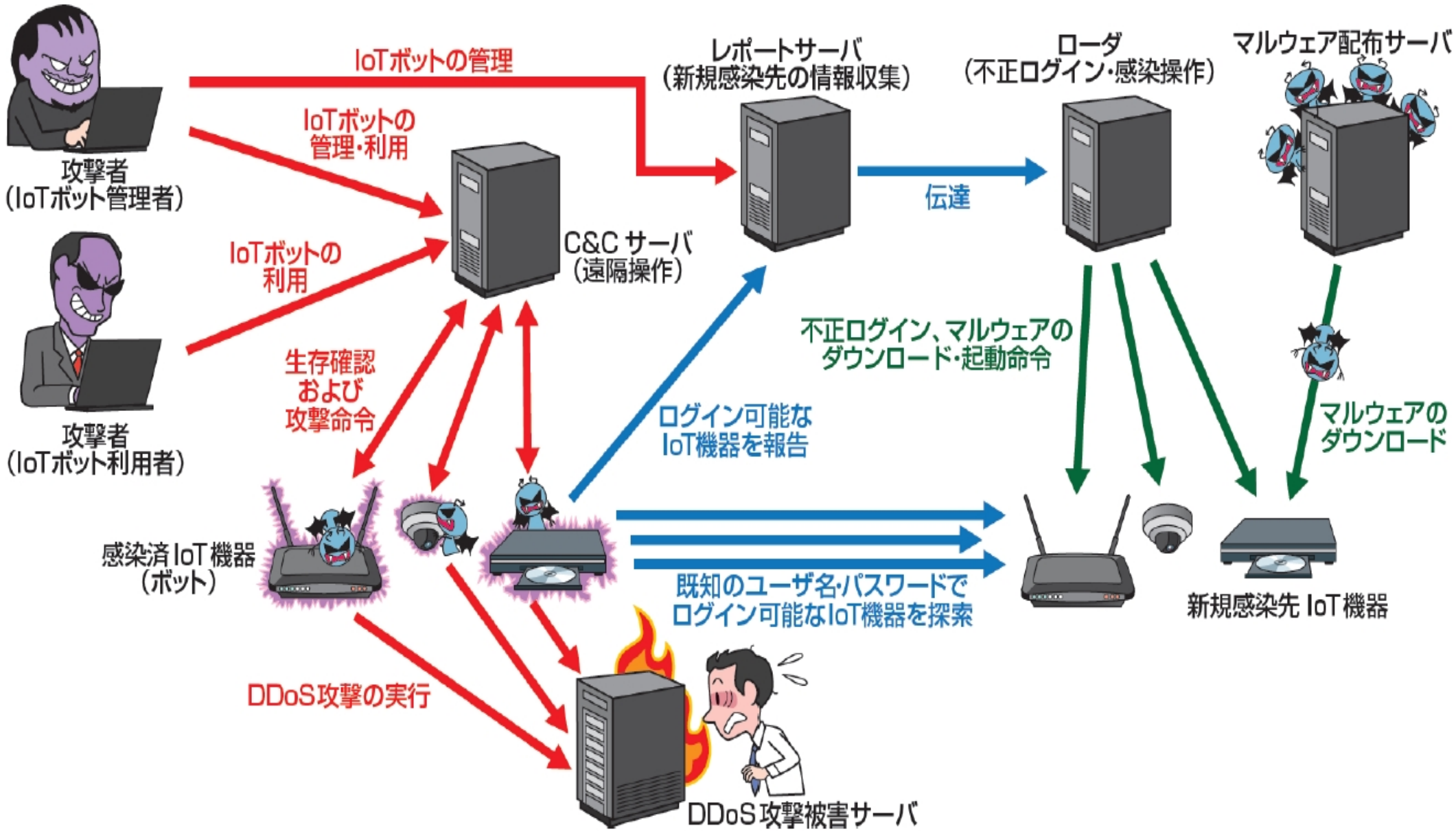
- サーバの脆弱性

  サーバ側で処理を行うのは，Webアプリケーションと呼ばれるプログラムで， PHP，JavaScript，ASP.netといった言語で作成されています．Webアプリケーションに脆弱性が含まれると，サーバ上の非公開ファイルを入手されたり，悪意のあるプログラムを実行されたりなどの被害を受ける．

- ルータやIoT機器の脆弱性

  2016年10月に，Miraiと呼ばれるウイルスが蔓延しました．このウイルスはおもにルータ製品やIoT機器の脆弱性を標的にしていました．DDoS攻撃の踏み台にされてしまいました．

Miraiの挙動： 感染 → ボットネット構築 → DDoS攻撃



（2）組織に内在する脆弱性

組織体制の不備，管理不足，意識欠如など

- 紛失・盗難
  情報の持ち出しルールの不順守や盗難への予防対策なし
- 誤公開，誤送信
  個人情報公開．機密のファイルを送るべきでない人に送ってしまいました．アクセス権限設定の誤り　など
- 内部犯行
  情報の無断持ち出し，第三者へ売却
  気のゆるみ，うっかりミス，管理不足による出来事

3. 情報資産の価値とその評価方法

- セキュリティリスク評価において，情報資産価値の評価は必須です．情報資産価値があるからこそリスクが生まれ，そこにセキュリティ対策が必要となります．
- 情報資産は以下に分けられます．
  ① 有形資産
  コンピュータ関連機器，社内文書など
  ② 無形資産
  ソフトウェア，データ，技術情報，プライバシー情報など
- 情報資産の価値の評価は，定性的評価（金額に換算不可な資産の評価）と定量的評価（金額に換算可能な資産の評価）に分類されます．

3.1 情報資産管理台帳

すべての情報を洗い出し，一覧表を作成します．機密性，完全性，可用性の3大要素に評価値をつけます．

情報資産管理台帳の例

情報資産管理台帳

業務分類	情報資産名称	備考	利用者範囲	管理部署	媒体・保存先	個人情報の種類			評価値			重要度	保存期限	登録日
						個人情報	要配慮個人情報	特定個人情報	機密性	完全性	可用性			
寄付管理	寄付者の個人情報	取得時、一時保存	寄付者・システム	情シス	社内サーバー	有			2	2	2	2		2020/1/26
寄付管理	寄付者の個人情報	取得時(クレジットカード申し込み)	寄付者・システム	経理	社外サーバー	有			2	2	2	2		2020/1/26
寄付管理	決済情報(クレジットカード)	取得時(クレジットカード申し込み)	寄付者・システム	経理	社外サーバー				1	2	2	2		2020/1/26
寄付管理	寄付者の個人情報	取得時・保管時	寄付者・システム	情シス	社内サーバー	有			2	2	2	2		2020/1/26
寄付管理	決済情報(銀行)	取得時	経理	経理	社外サーバー				1	2	2	2		2020/1/26
寄付管理	決済情報(銀行)	取得時(CSV)	経理	経理	事務所PC				1	2	2	2		2020/1/26
寄付管理	決済情報(銀行)	取得時・保管時	経理	経理	社内サーバー	有			2	2	2	2		2020/1/26

3.2 3大要素の評価値のつけ方

- 3段，4段または5段評価
- 右図のような評価値や評価基準テーブルを作成し，それに基づいて各情報資産に対してどれに当てはまるかを決め，その評価値をつけます．

評価値		評価基準	該当する情報の例
機密性 アクセスを許可された者だけが情報にアクセスできる	2	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている	●個人情報（個人情報保護法で定義） ●特定個人情報（マイナンバーを含む個人情報）
		守秘義務の対象や限定提供データ[12]として指定されている 漏えいすると取引先や顧客に大きな影響がある	●取引先から秘密として提供された情報 ●取引先の製品・サービスに関わる非公開情報
		自社の営業秘密として管理すべき（不正競争防止法による保護を受けるため） 漏えいすると自社に深刻な影響がある	●自社の独自技術・ノウハウ ●取引先リスト ●特許出願前の発明情報
	1	漏えいすると事業に大きな影響がある	●見積書、仕入価格など顧客（取引先）との商取引に関する情報
	0	漏えいしても事業にほとんど影響はない	●自社製品カタログ ●ホームページ掲載情報
完全性 情報や情報の処理方法が正確で完全である	2	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている	●個人情報（個人情報保護法で定義） ●特定個人情報（マイナンバーを含む個人情報）
		改ざんされると自社に深刻な影響または取引先や顧客に大きな影響がある	●取引先から処理を委託された会計情報 ●取引先の口座情報 ●顧客から製造を委託された設計図
	1	改ざんされると事業に大きな影響がある	●自社の会計情報 ●受発注・決済・契約情報 ●ホームページ掲載情報
	0	改ざんされても事業にほとんど影響はない	●廃版製品カタログデータ
可用性 許可された者が必要な時に情報資産にアクセスできる	2	利用できなくなると自社に深刻な影響または取引先や顧客に大きな影響がある	●顧客に提供しているEC サイト ●顧客に提供しているクラウドサービス
	1	利用できなくなると事業に大きな影響がある	●製品の設計図 ●商品・サービスに関するコンテンツ（インターネット向け事業の場合）
	0	利用できなくなっても事業にほとんど影響はない	●廃版製品カタログ

3.3 リスク値の算定（簡単な例）

ある情報資産に対して，特定攻撃（脅威）を受けるとして，この情報資産を保持する側に脆弱性があるため，その情報資産のリスク値を以下のように算出する．

リスク値 ＝ 機密性の評価値 × 被害発生可能性
＋ 完全性の評価値 × 被害発生可能性
＋ 可用性の評価値 × 被害発生可能性

ただし，被害発生可能性 ＝ 脅威レベル ÷ （4 － 脆弱性レベル）

[脆弱性レベル＝0～3とした場合]

3.4 不正行為と情報セキュリティ3大要素への影響

不正行為	内容	影響されるセキュリティ要素
盗聴	ネットワークを流れるデータや保存されいるデータの不正入手 例：パスワードの盗用，個人データ（メール，日記など）の盗み見，企業データの漏えい	機密性
改ざん	データの書き換え 例：Webページの改ざん，設定の書き換え	完全性
なりすまし	別の個人を装い，本人のふりをしたさまざまな行為 例：盗み出したID，パスワードで正当なユーザに見せかけて侵入，他人のクレジットカード番号によるショッピング	機密性

不正行為	内容	影響されるセキュリティ要素
破壊	データやプログラムの削除，ハードディスクの初期化など	可用性
コンピュータ不正使用	遠隔操作や自動起動など不正使用	機密性，完全性，可用性
不正プログラムの埋め込み	ユーザの知らない間に情報を入手して外部へ送信したり，ファイルを破壊したりするなどの不正プログラムの埋め込み	機密性，完全性，可用性
踏み台	不正アクセスの中継地点として他人のコンピュータを使用．所有者の意図に反し，本人の知らない間に攻撃に荷担させられます．例：DoSやDDoS攻撃に利用される．スパムメールの中継	機密性，完全性，可用性

4. 攻撃への対策

以下は対策の概要のみです．（詳細については今後の授業で紹介します）

外部からの攻撃	対策概要
マルウェア	アンチウイルス（隔離／無効化，遮断，実行回避）
外部からの侵入（不正アクセス）	ファイアウォール（IDS，認証強化）
サーバへの攻撃（サービス妨害）	ネットワークセキュリティ（不用ポートの閉鎖，脆弱性の解消，認証）
盗聴，偽造	暗号化

練習問題

1. DoS攻撃は，標的のサーバに大量のデータを送って過大な負荷をかけ，サーバのパフォーマンスを極端に低下させたり，サーバを機能停止に追い込んだりする攻撃です．DoS攻撃の対象，仕掛け方，目的はそれぞれどの種類に属するかを述べなさい．

2. 下記不正行為の特徴について簡単に述べなさい．

   盗聴　改ざん　なりすまし　破壊　踏み台