セキュリティへの脅威1
―インターネットの特異性と攻撃の分類―

野口　拓
Taku NOGUCHI

仮想空間

- インターネットでトラブルが多いのは、それが仮想空間だから？
  - 物理的な「相手」は存在している
  - 交流が物理的ではなく、コンピュータ上のデータを通して行われる
- 仮想空間への不安の本質
  - 安全性を確保する法律や仕組みがまだ十分に整備されていない
  - cf. 車が比較的安全に道を走行できるのは、免許・道路交通法・罰則などの安全制度が整っているから

トラブル：trouble

データ：data

匿名性

- インターネットでは、相手が特定できない？
  - IPアドレスを使って照会可能
  - 会員制サイトの個人情報は、外部に公開されることはないが、サイト運営側は把握している
- 匿名性：法律の保護の下で、サイト運営側に委ねられている
- SNSの投稿から素性を明かされることもある
- ビッグデータ時代に誰がどのように匿名化を保証するのかは大きな課題

アドレス：address

サイト：Website

ビッグデータ：big-data

開放性（openness）

- インターネットは規格が公開されており、誰でも利用できる
  - 誰でもそれらを利用して新しい技術を開発し、便利な社会を作り上げることができる
  - 犯罪者もそれを利用できる
    - 通信途中でIPパケットを抜き取り、中身を覗く
    - 第三者のPCを遠隔操作し、迷惑メールを送信したりウイルスをばらまく

パケット：packet

メール：e-mail

ウイルス：virus

無料(フリー)の文化

フリー：Free

- インターネットでは様々なサービスが「無料」
  - QQやgmailなどの電子メール
  - 動画配信
  - 地図

サービス：service

- 無料サービスで人々を集め、そこから情報を収集し有料ビジネスへ活かすモデル

ビジネス：business

  - cookieとIPアドレス、検索キーワードの内容などから「匿名の統計情報」を収集

キーワード：keyword

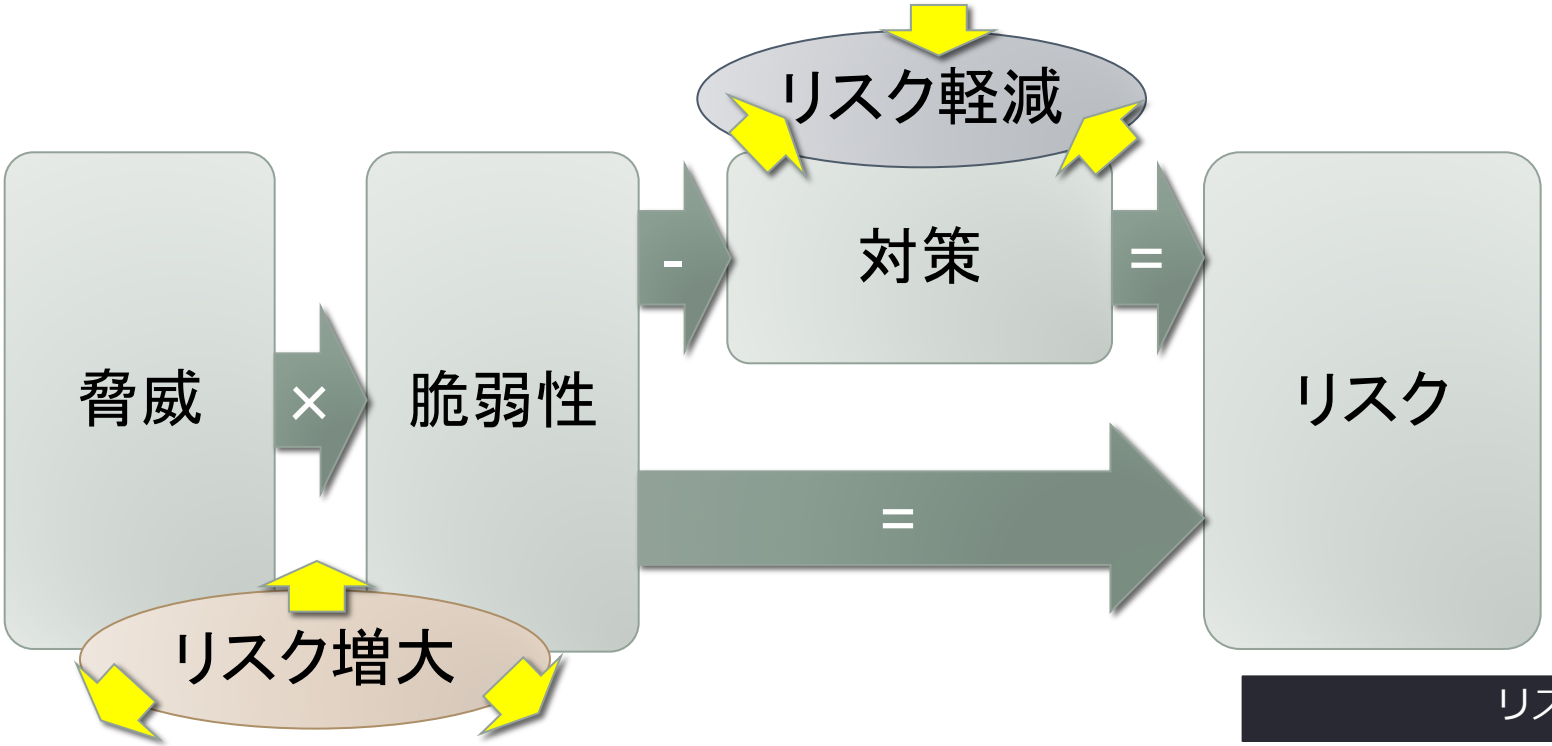
  - アカウントでログインした場合は、例えばメールアドレスとそれらが紐づけられる

アカウント：account

ログイン：login

セキュリティと脅威・脆弱性・リスク

- 脅威：　外部からの攻撃
- 脆弱性：弱点
- 対策：　弱点回避策
- リスク：損失の可能性



リスク：risk

リスクの評価

- 考えておくべき指標
  - 事象(脅威)が生じる確率　Prob
    - 例:不正アクセスの成功確率
  - 事象が生じた場合の影響の大きさ　M
    - 例:復旧に要するマンパワー

マンパワー:manpower, human-resources

- リスク評価の指標:Prob×M

影響の現れ方のレベル

レベル：level

- 情報システムへの影響
  - 情報システムを正常に運用できなくなる
- 業務への影響
  - 情報システムが正常に運用できないことにより、企業などの業務へ大きな影響を及ぼす
- 国民生活への影響
  - 銀行・鉄道などのオンラインシステムの停止などにより、国民生活へも大きな影響を及ぼす

オンライン：online

  - サイバーテロ

サイバーテロ：cyber terrorism

攻撃者

- 部外者
  - 愉快犯
  - 産業スパイ
  - テロリスト

スパイ：spy

テロリスト：terrorist

- 部内者
  - 従業員やアルバイトなどによる内部犯罪

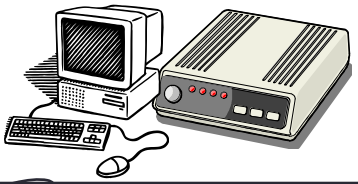
アルバイト：part-time worker

古くからの脅威

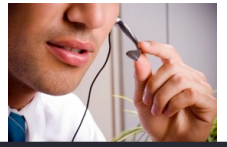
- スパイ
  - 秘密書類を盗む，会話を盗聴する
- 電波（無線）による情報通信
  - 誰でも聞ける
- War Dialing
  - パスワードアタック
- ソーシャルアタック
  - 巧みなやりとりでパスワードを聞き出す
- 攻撃のためにコンピュータを使えるようになってくる
- インターネットの普及がクラッカーの活躍の場を広げる
  - いわゆるセキュリティホールを攻撃しての侵入が一般化

スパイ：spy

暗号



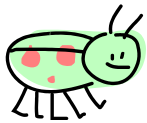
パスワードアタック：password attacking



ソーシャルアタック：social engineering

クラッカー：cracker

セキュリティホール：security hole

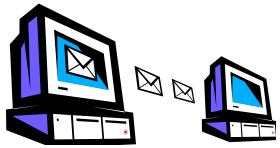


攻撃目的とその変化

- 従来　・・・　成功を誇示するもの
  - 悪いんだけれども，まだいたずらの延長線上とも言える
  - Web改ざんのインパクト
  - コンピュータウィルスの感染規模や感染速度，インパクト

インパクト：impact

ボットネット：botnet



- 最近　・・・　営利目的
  - 明らかに犯罪
  - SPAM業者にボットネットを貸し出す
  - 特定組織から情報を盗む目的の攻撃
  - Antinnyウィルスなど重要な情報を流出させた　・・・　悪意が大

攻撃対象とその変化

- 従来　・・・　不特定多数・目立つサイト
  - 自己顕示欲を満たすためなので
- 最近　・・・　特定の目標を狙った攻撃が増加（標的型攻撃）
  - 内部文書を装ったもの
    - 2006年 日本でも政府を対象としたウィルスメールが
  - 派手なWeb改ざん，あからさまなウィルスの発症はなく，「静かな攻撃」

- 一方で
  - 踏み台に使用するためのサイトへの攻撃が増加
    - 管理が行き届いていないサイト
    - ドライブ・バイ・ダウンロード
  - メールの添付ファイルではなく，URLをクリックさせるタイプ
    - メールサーバ等によるウィルスチェックを避ける
  - OSやサーバの脆弱性から，アプリケーションの脆弱性へ
    - 攻撃が簡単で対応が遅い．DBへのアクセスやコンテンツへのアクセスが簡単

ドライブバイダウンロード：drive-by download

メールサーバ：mail server

アプリケーション：application　アクセス：access　コンテンツ：contents

攻撃手法とその変化: 心理的手法

- ソーシャルアタック (social engineering)

- フィッシング (phishing)
  - 会員の期限切れ，新サービスへの移行などを餌に
  - 本物を装った偽サイトへ誘導し，パスワード等を取得する
- ワンクリック詐欺 (single-click fraud)
  - クリックしただけで入会等したことにされ，料金が請求される(?)
- スパムによるアクセス誘導 (spam)
  - フィッシングやワンクリック詐欺の入り口の一つとして

- 一般ユーザ，(user)
  とりわけIT知識の少ない人をどう守っていくのか・・・

組織内部の脅威

- 内部者の悪意・不注意・怠慢　・・・　もっと重大な脅威
  - 職務上の権限，
    システム管理上の権限が強い内部者は致命的
    - 暗号化，アクセス制御などをすりぬける
- といって・・・
  - 性悪説での対応は　・・・　信頼関係崩壊と対立の可能性
  - 管理する側の都合だけでは　・・・　効率低下の可能性

攻撃方法

- 直接的攻撃
  - 攻撃者が（通信路を通じて）直接コンピュータに侵入し、ファイルなどへの攻撃を行う
  - 不正アクセス
    - パスワードを盗むなどして、他人になりすまして侵入
    - 脆弱性を利用して侵入
- 間接的攻撃
  - 不正なソフトウェア（マルウェア）をコンピュータに送り込んで、ファイルなどへの攻撃を行う

マルウェア：malware

脆弱性

- 脆弱性は，弱点の有無・度合いを示す指標
- 脆弱性が含まれる対象
  - ハード，またはハードと一体で動作するファームウェア
  - ソフトウェア：市販のパッケージソフト，独自開発ソフト
  - 両者が組み合わされたシステム

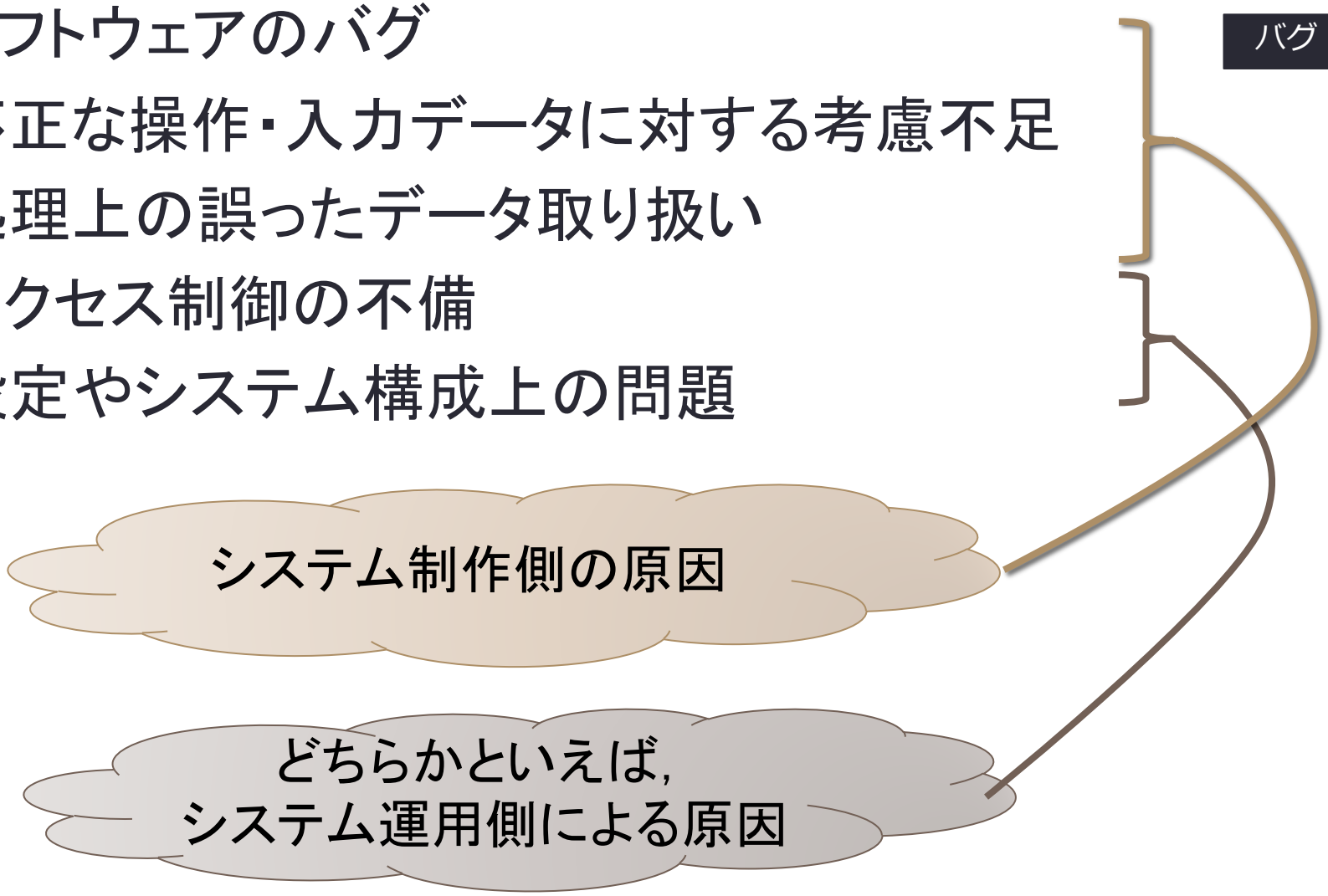
ファームウェア：firmware

- 脆弱性によって生じる問題
  - システム機能やデータへの不正アクセス（読み・変更・破壊）
  - 意図しない情報の暴露
  - 不正プログラムの実行
  - システム制御権の奪取，利用権限の昇格
  - 踏み台ホストになってしまう

ホスト：host

脆弱性が発生する原因

- ソフトウェアのバグ
- 不正な操作・入力データに対する考慮不足
- 処理上の誤ったデータ取り扱い
- アクセス制御の不備
- 設定やシステム構成上の問題



バッファオーバフロー

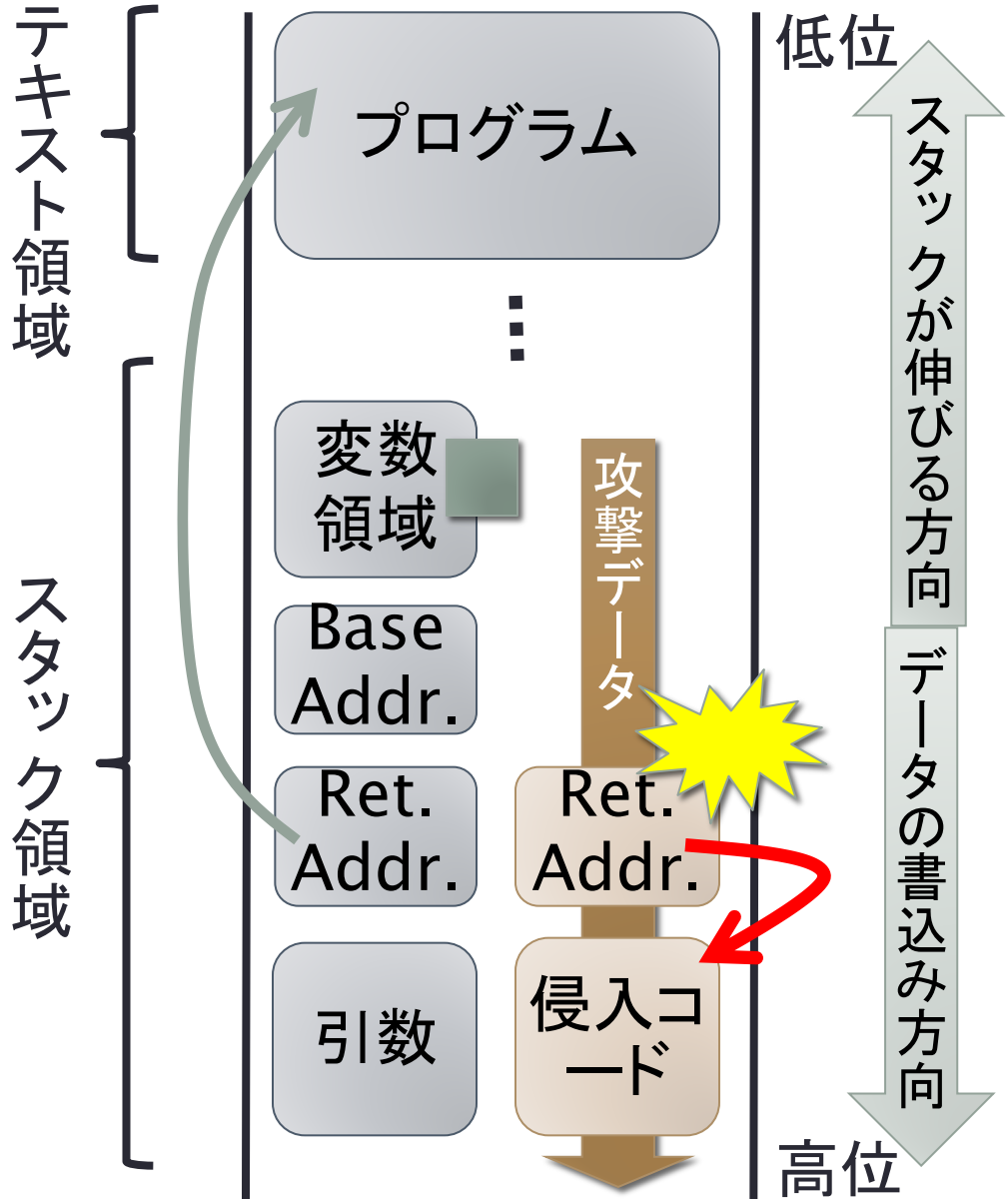
```
func()
{
        char s[512];

        scanf("%s", s);
}

main()
{
        func(a, b, c);

        other(x);
}
```

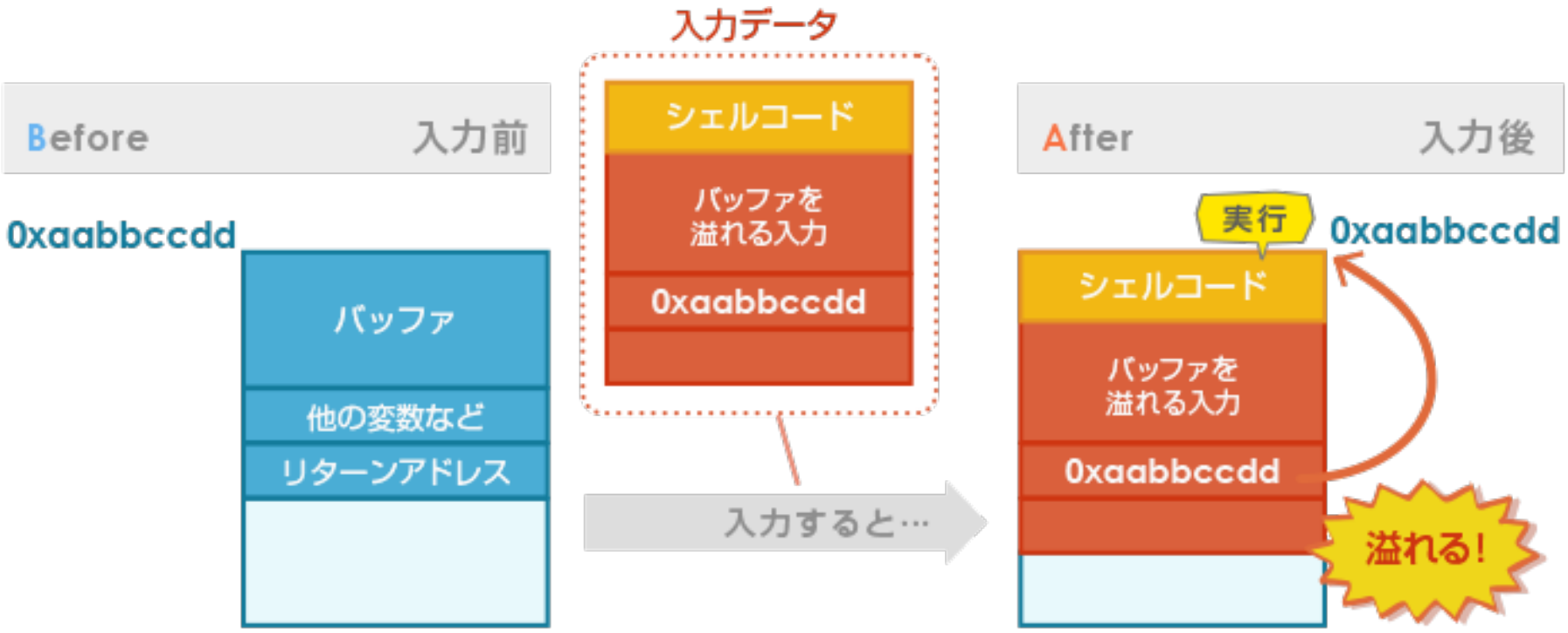
これが，リモートから実されれば・・・

テキスト：text

リモート：remote

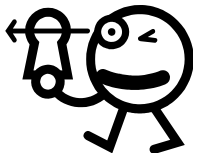
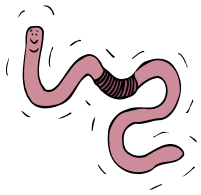
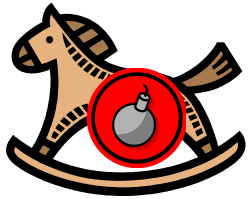
スタック：stack



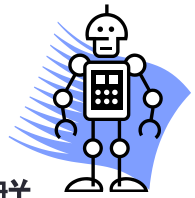

Before
入力前
0xaabbccdd
バッファ
他の変数など
リターンアドレス
入力データ
シェルコード
バッファを
溢れる入力
0xaabbccdd
入力すると…
After
入力後
実行
0xaabbccdd
シェルコード
バッファを
溢れる入力
0xaabbccdd
溢れる!

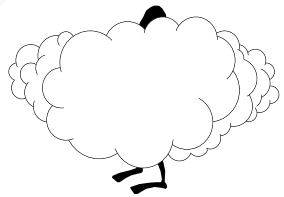
間接的攻撃：マルウェア

- マルウェア（Malware: Malicious Software）
  - Virus
  - Worm
  - Spyware
  - Trojan horse

- Malwareは，
  ファイアウォール内のコンピュータへの侵入が目的
  - 電子メール，Webなど，ファイアウォールに止められない方法
- 高度な手法も
  - bot: ネットワーク経由でコントロール
  - rootkit: 感染・侵入を隠すためのプログラム群
  - covert channel: 監視システムから隠す(他の通信に紛れる)





ファイヤウォール：firewall

マルウェアの配布形態

- Web
  - 最近はこれが流行
  - Webサイトを見ると，XSSやSQLインジェクションなどにより不正なコード(javascript, PDF, …)をダウンロードさせられる
  - ブラウザ・プラグインの脆弱性をつかれることも
- USBフラッシュメモリなどのリムーバブルメディア
  - 差し込まれると自動実行機能
- メール
  - それらしく偽装し，
    URLをクリックさせたり，添付ファイルを開かせようとする
  - 添付ファイルは，必ずしも実行ファイルだけでなくPDF, DOCも

XSS：cross site scripting

SQLインジェクション：SQL-injection

ブラウザ：browser

プラグイン：plugin

フラッシュメモリ：flash memory

リムーバブルメディア：removable media

マルウェアの挙動

- 破壊活動
  - ファイル削除，無駄データのランダムな書き込み
- パスワード・アカウント収集
  - キー入力などを盗みクレジットカード番号，パスワードを盗む
  - オンラインゲームの情報を盗むものも多い
- DoS攻撃
- スパム送信
- バックドア作成
  - 特定のTCPポートで待ち受け，コマンド入力を受け付けるなど

ランダム：random

クレジットカード：credit card

オンラインゲーム：online game

DoS：denial of service

スパム：spam-mail

バックドア：backdoor

マルウェアの挙動

- ネットワーク設定の変更
  - DNSキャッシュポイズニングと同等の効果が.
  - /etc/hosts, \windows\system32\drivers\etc\hosts
  - /etc/resolv.conf

ネットワーク：network

キャッシュポイズニング：cache poisoning

- 偵察行為
  - 感染したコンピュータが接続されたネットワークについて，
    どんなコンピュータが居るか，ファイル共有の状況を調べる
- セキュリティ更新プログラムのインストール
  - マルウェアに感染したコンピュータに他のマルウェアが感染しないように，
    更新プログラムを追加する

マルウェア例

- Morris worm (1988)
  - インターネットの10%(6000台)が感染
  - 自己増殖機能を有していた
- Melissa virus (1999)
  - MS word 97,98,2000のマクロ機能を使ったファイル
  - メールで添付ファイルとして送られてくる
    開くととOutlookに登録された50アドレスへさらに転送
  - メールサーバなどにも負荷が
- Love Letter virus (2000)
  - タイトル「I LOVE YOU」，本文「添付のラブレターを見てね」
- Code Red (2001)
  - MS IIS
  - 感染活動によるトラフィックの生成，ネットワーク機器の再起動
    Web改ざん，特定サイトへのDoS攻撃

マクロ：macro

トラフィック：traffic

マルウェア例

- Code Red II (2002)
  - レジストリの書き換え＆バックドアの設置
- Nimda (2001)
  - MS IIS, ネットワーク共有など複数の感染ルート
- Slammer (2003)
  - MS SQLサーバ
  - 感染速度が速い！10分で感染可能なサーバの90%へ
  - 過大なトラフィックを生成．韓国ではネットワークが麻痺するほど
- Blaster (2003)
  - MS Windows ・・・ かなり多くの数が対象
  - 管理者権限を奪われ，windowsupdate.comへのDoS

レジストリ：registry

清掃費の振込のご連絡を頂きありがとうございました。
清掃支払関係の担当にお伝えいたします。

また、OICでの学会が開催されることになりましたら
お力添えになれるよう参りたいと思いますので
ご連絡ください。

今後ともどうぞ宜しくお願い致します。

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝
株式会社クレオテック
OICキャンパス業務部 OICキャンパス業務課
下川　由佳
〒567-8570 大阪府茨木市岩倉町2-150
ＴＥＬ：072-665-2020（内線 513-2037）
ＦＡＸ：072-665-2039（内線 513-2039）
E-mail：oic-cam03@creotech.co.jp
＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

Osako FUTURE PLAZA
Re: RE: 【貸出備品】　2/27　国際会議Mobicase2018
宛先: 松村耕平

Unable to show this message

Click here to show full message

SMTP message delayed: GPLj - Date: 08/20/2018 1:21:12（ritsumei）