# サイバー攻撃の現状

2017年11月30日

株式会社東日本計算センター
伊藤　盛人

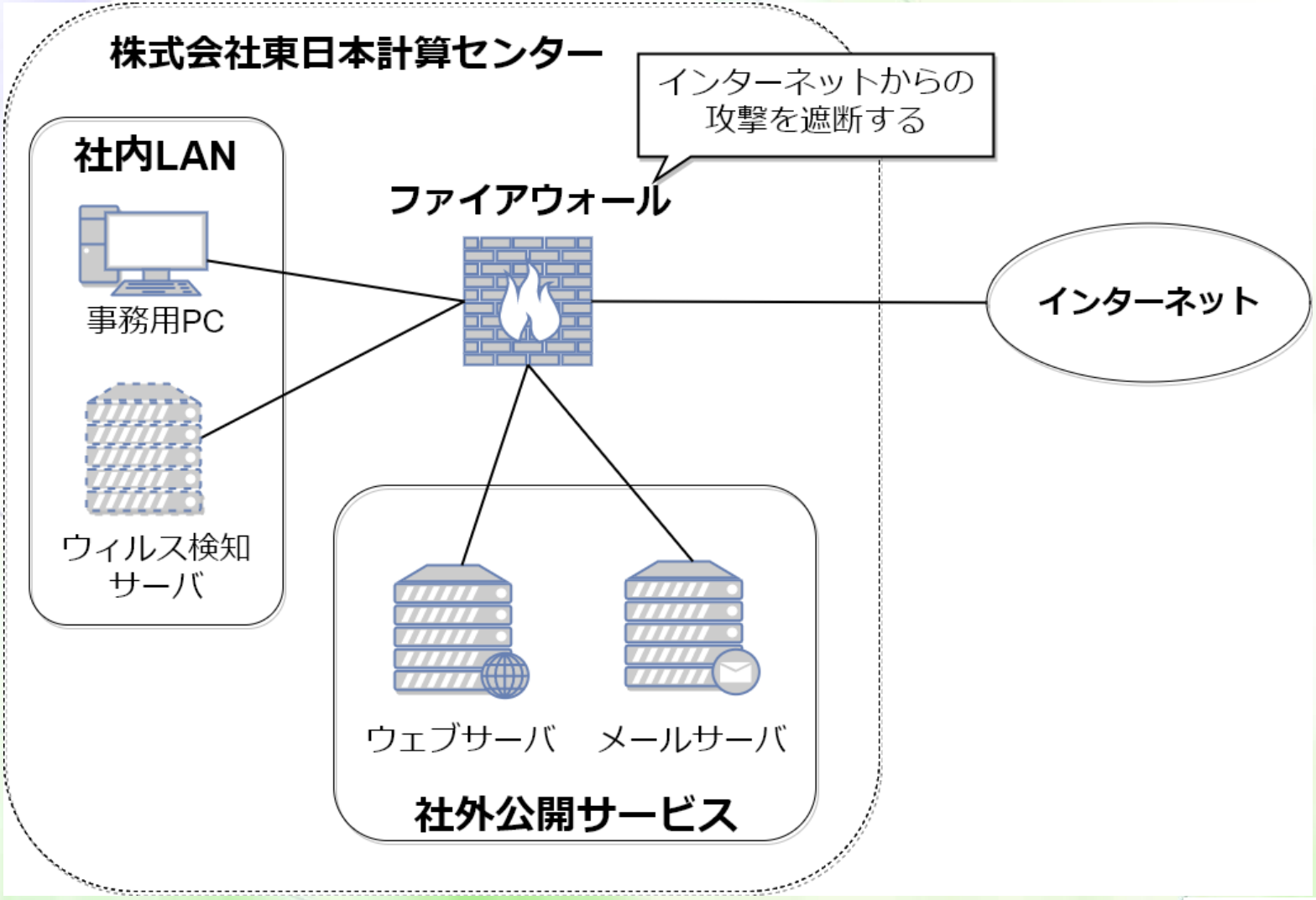
# 自己紹介

- ITインフラ技術者
  - 情報通信ネットワークの設計・構築・運用・保守
  - サーバコンピュータの設計・構築・運用・保守
  - 情報セキュリティ対策にも注力
- セキュリティ技術者
  - 情報処理安全確保支援士　登録番号003628号

# どのくらい攻撃されている？

- 全国規模の統計やニュースはよく見かける
- 大学などが公表する学内の統計情報もたまに見かける
- 中小企業の統計情報はほとんど見かけない
- いわき市の中小企業はどのくらい攻撃されてる？

# 情報通信ネットワークの構成

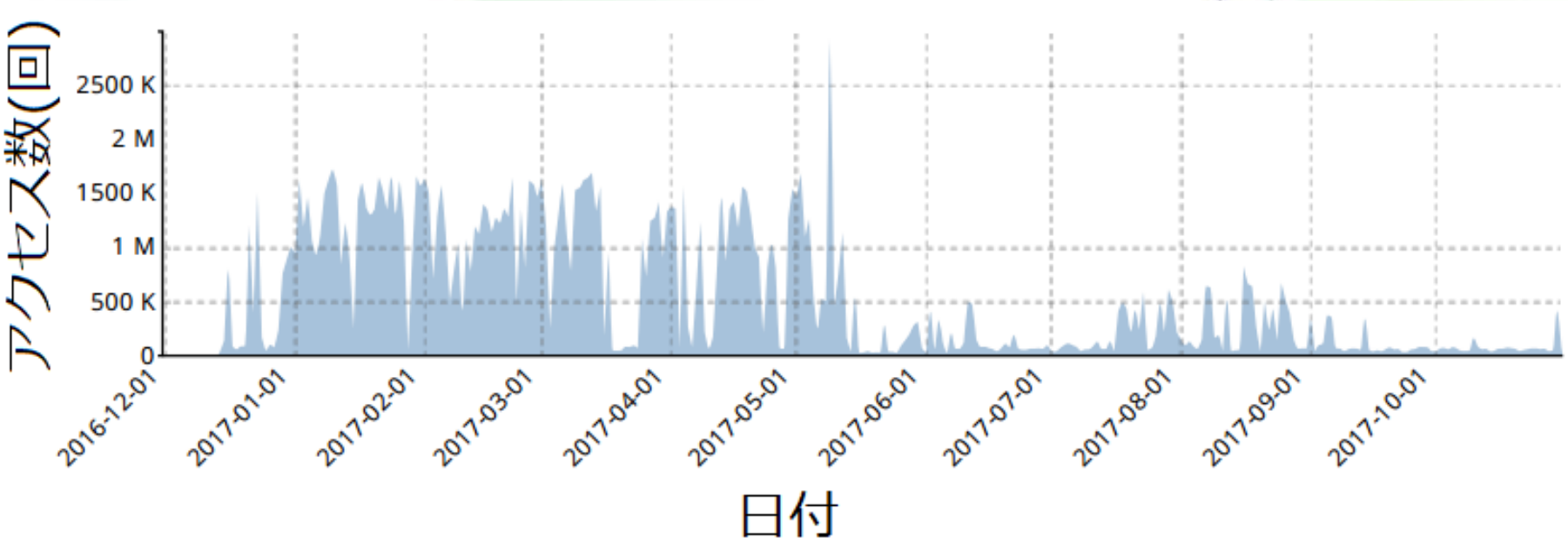


# インターネットからのアクセス数

５月下旬にサーバを１台撤去したためアクセスが減少

５月以前は100万回以上アクセスされる日も多かった

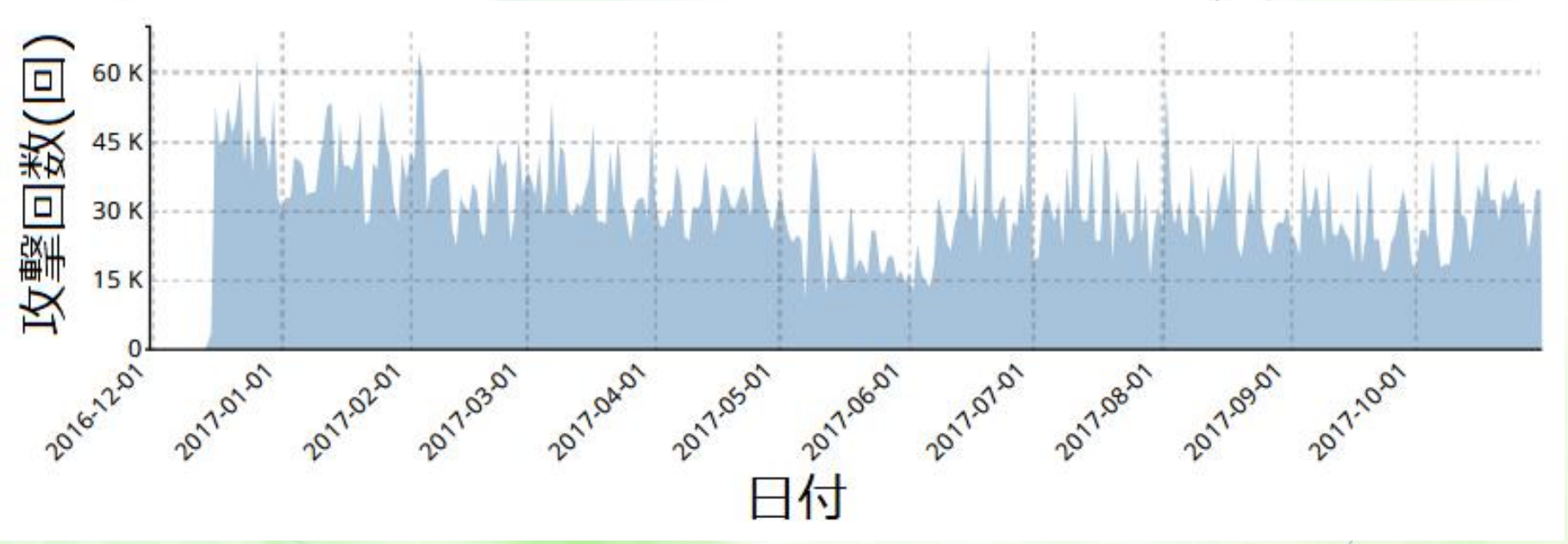
６月以降は多い日で50万回程度



# インターネットからの攻撃回数

１日当たりのアクセス数に関係なく、コンスタントに

１日 平均 ３万回程度の攻撃を受けている



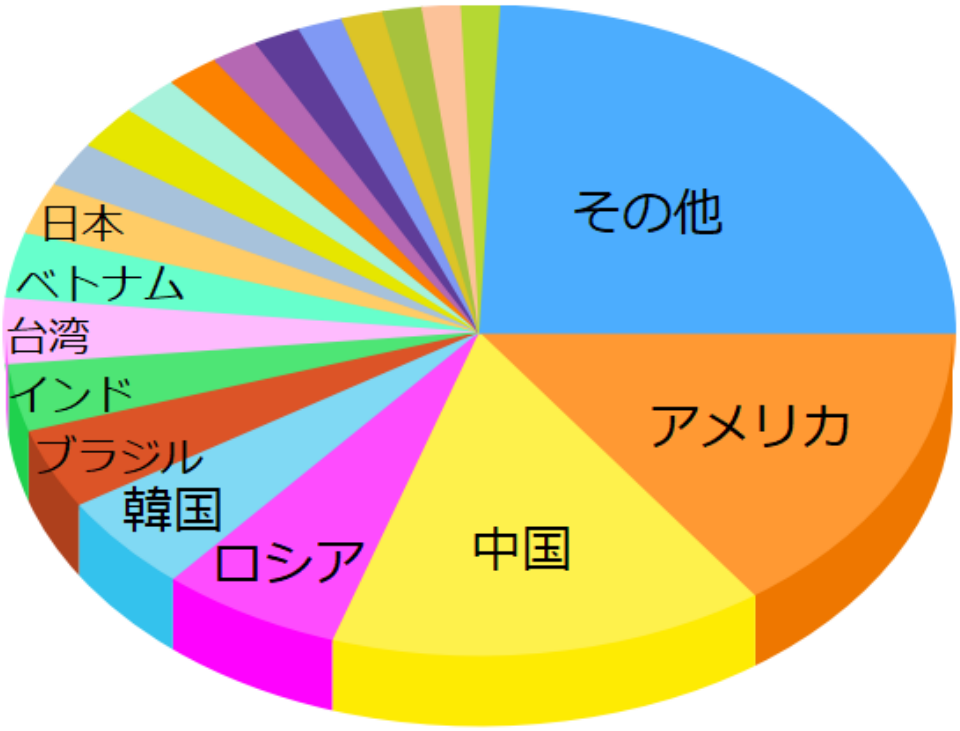
# 攻撃手法 TOP20

## メール配送システム、ウェブサービス、OS、ネットワークインフラへの攻撃

| 順位 | 攻撃名称 | 件数 | 攻撃対象 |
|---|---|---|---|
| 1 | Web.Server.Password.Files.Access | 1,881 | ウェブサービス |
| 2 | SSLv2.Openssl.Get.Shared.Ciphers.Overflow.Attempt | 1,297 | 暗号通信機能 |
| 3 | HTTP.URI.SQL.Injection | 1,101 | ウェブサービス |
| 4 | ZmEu.Vulnerability.Scanner | 1,037 | ウェブサービス |
| 5 | Web.Server.etc.passwd.Access | 888 | ウェブサービス |
| 6 | Muieblackcat.Scanner | 850 | ウェブサービス |
| 7 | Apache.Struts.Jakarta.Multipart.Parser.Code.Execution | 839 | ウェブサービス |
| 8 | udp_flood | 193 | ネットワーク過負荷 |
| 9 | MS.Office.RTF.File.OLE.autolink.Code.Execution | 190 | MS Office製品 |
| 10 | NetworkActiv.Web.Server.XSS | 178 | ウェブサービス |
| 11 | Apache.Camel.XSLT.Component.XXE | 163 | ウェブサービス |
| 12 | PHP.CGI.Argument.Injection | 132 | ウェブサービス |
| 13 | Zen.Cart.Local.File.Inclusion | 118 | ウェブサービス |
| 14 | Apache.Struts.2.DefaultActionMapper.Remote.Command.Execution | 97 | ウェブサービス |
| 15 | OpenSSL.Heartbleed.Attack | 69 | 暗号通信機能 |
| 16 | WordPress.Slider.Revolution.File.Inclusion | 50 | ウェブサービス |
| 17 | HTTP.URI.Script.XSS | 49 | ウェブサービス |
| 18 | PHP.Charts.Type.Parameter.Parsing.Code.Execution | 46 | ウェブサービス |
| 19 | Log1.CMS.WriteInfo.PHP.Code.Injection | 46 | ウェブサービス |
| 20 | Bash.Function.Definitions.Remote.Code.Execution | 45 | OS |

# 攻撃元 国別 TOP20

2016/12/15～2017/10/31




- 15.09% United States (1,541,206 )
- 14.94% China (1,526,536 )
- 6.18% Russian Federation (631,757 )
- 4.84% Korea, Republic of (494,093 )
- 4.01% Brazil (409,857 )
- 3.36% India (343,036 )
- 3.26% Taiwan (332,546 )
- 3.23% Vietnam (329,883 )
- 2.56% Japan (261,664 )
- 2.21% France (225,326 )
- 2.19% United Kingdom (223,409 )
- 1.96% Turkey (200,374 )
- 1.79% Netherlands (183,030 )
- 1.60% Argentina (163,677 )
- 1.60% Mexico (163,622 )
- 1.51% Germany (153,889 )
- 1.41% Ukraine (144,229 )
- 1.33% Sweden (135,883 )
- 1.32% Italy (134,939 )
- 1.32% Poland (134,597 )
- 24.30% Others (2,481,862 )

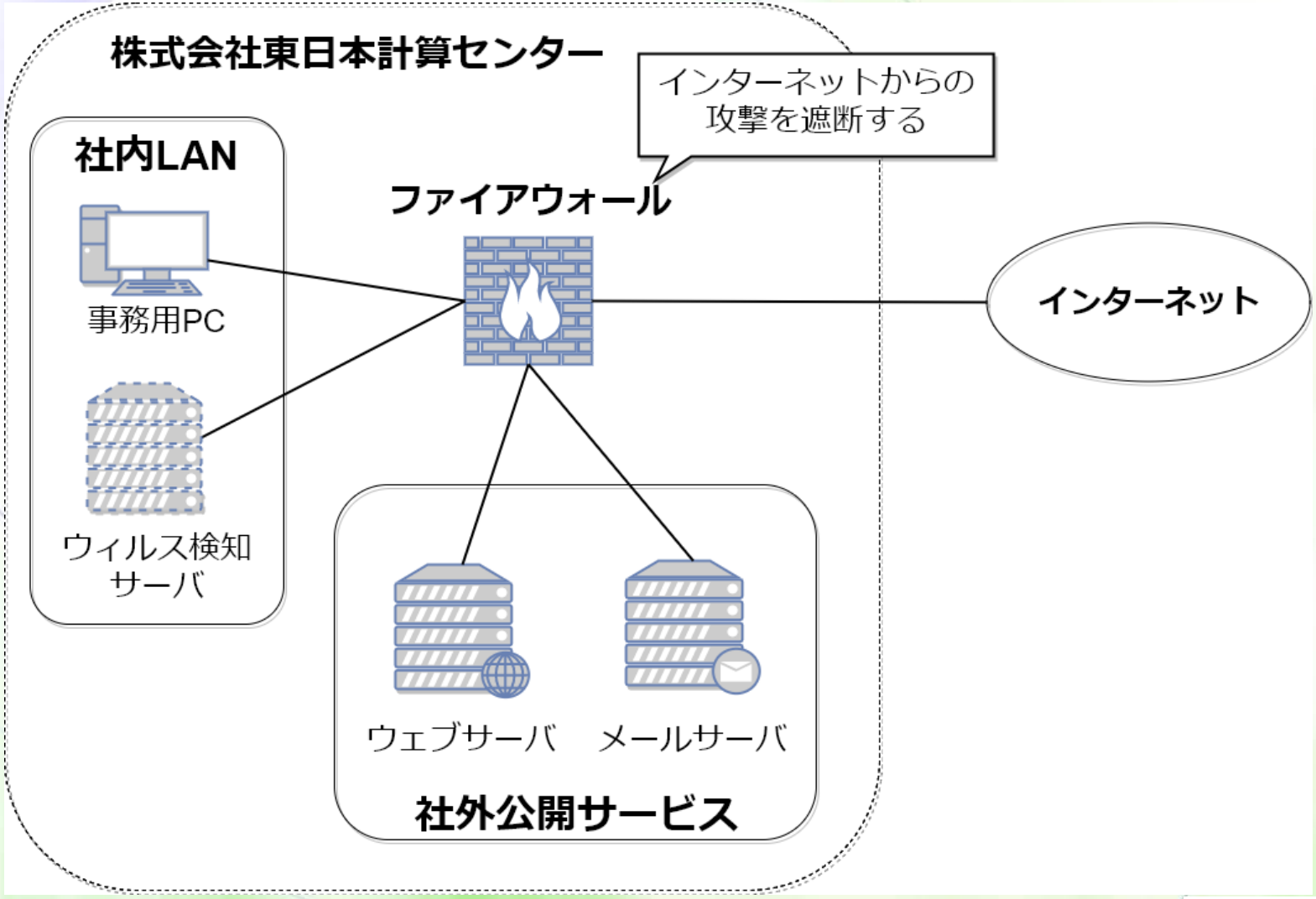
# 攻撃元が攻撃者なのか？

- 攻撃者が他人の機器を乗っ取る
  - 一般家庭のPC
  - 企業のPCやサーバコンピュータ
  - IoT機器
- 遠隔操作で、乗っ取った機器から攻撃を仕掛ける
- 機器の所有者は、自分の機器が攻撃に使用されていることに気付いていない

# ファイアウォールをすり抜ける？

- 正常な通信に紛れて、ファイアウォールをすり抜けてしまう！
- 攻撃の手口が年々巧妙化
- ファイアウォールをすり抜けた攻撃を、別の手法で検知する（多層防御）

# 情報通信ネットワークの構成

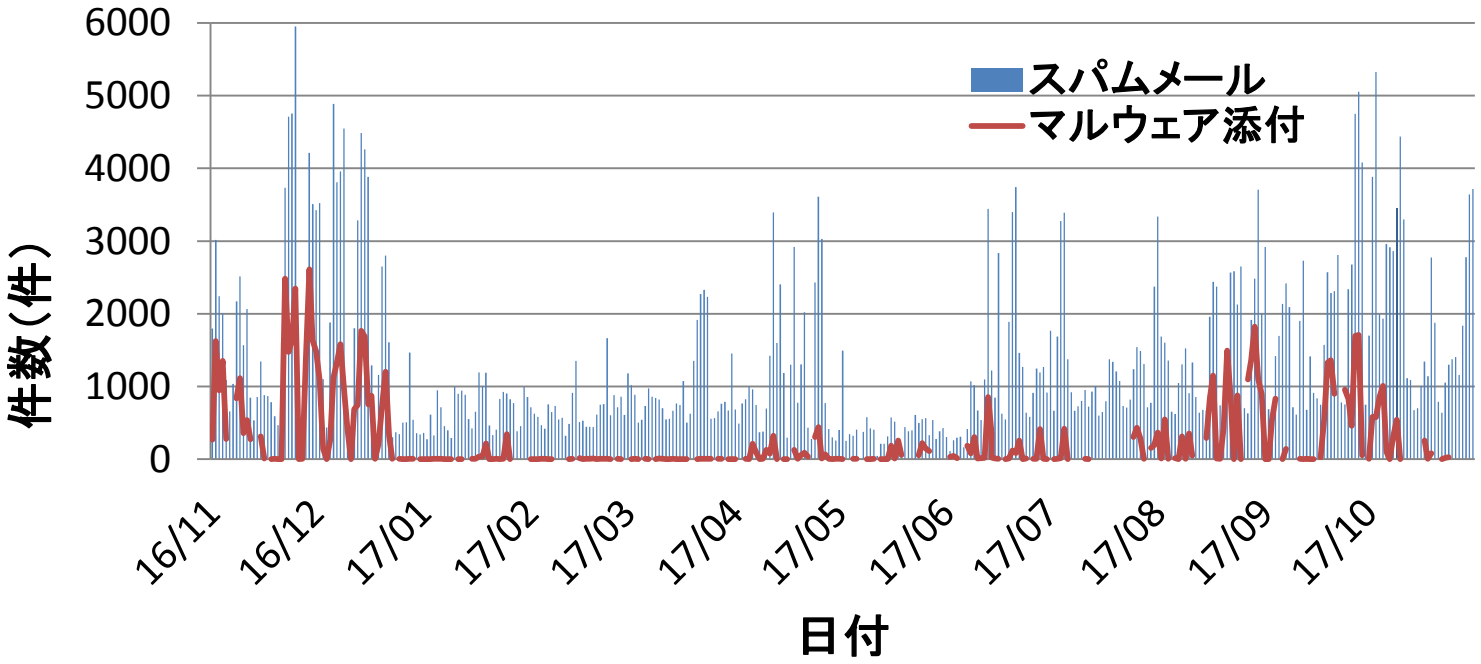


# スパムメールとマルウェア添付数

ファイアウォールで検知できたスパムメール

スパムメール　　483，511 件　中

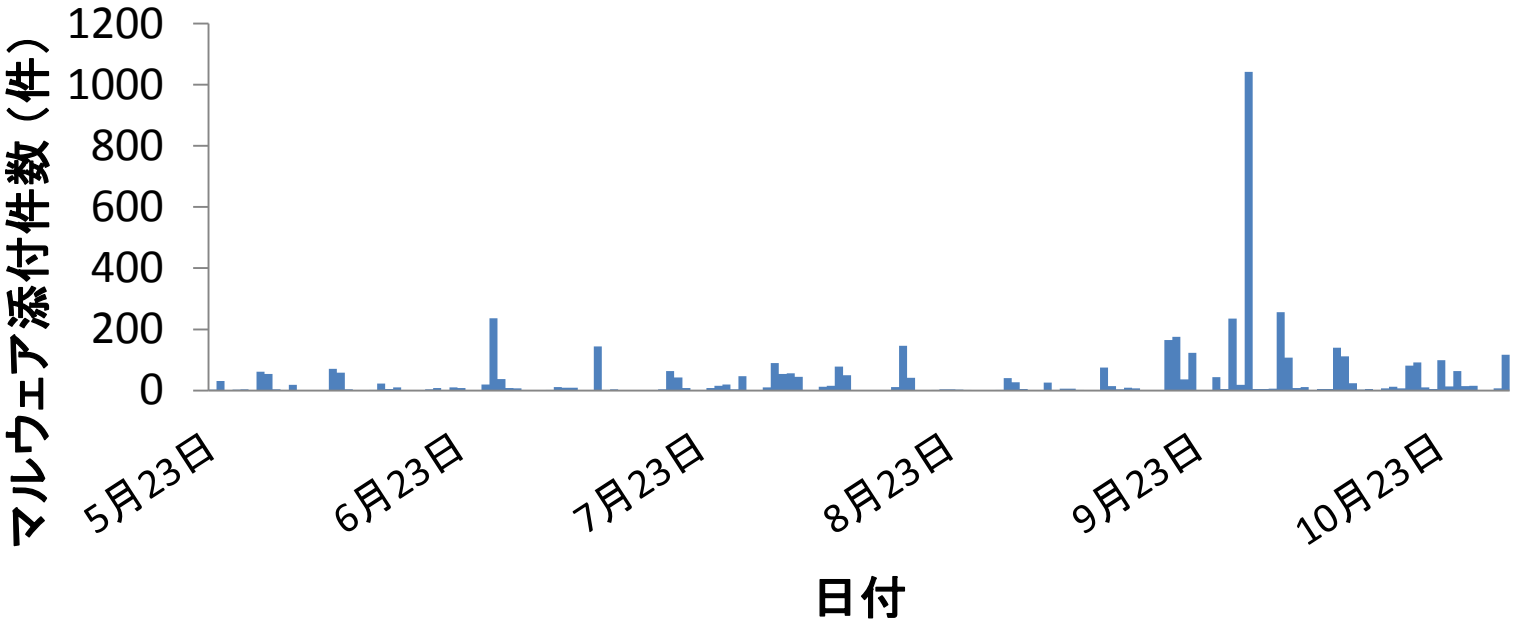
マルウェア添付　　77，355 件（16%）



# スパムメールとマルウェア添付数

ファイアウォールをすり抜けた

マルウェア添付メール　５，０１０ 件（２%）



# 最近のサイバー攻撃の傾向

- 社員自らの手で、マルウェアをダウンロードするように仕向ける（標的型攻撃など）
- 防火扉を外からこじ開けて侵入するよりも、中から開けてもらう方が楽（監視がゆるい）
  - 社内から社外への通信も監視しなければならない

# 最近のサイバー攻撃の傾向

- 目立たないようヒッソリと活動するものが主流
  - 侵入されてから、侵入に気付くまで平均100日かかる
  - 気付かれるまでの間に機密データを盗まれる
  - 社内にいるかのごとく、PCを遠隔操作できる

# 最近のサイバー攻撃の傾向

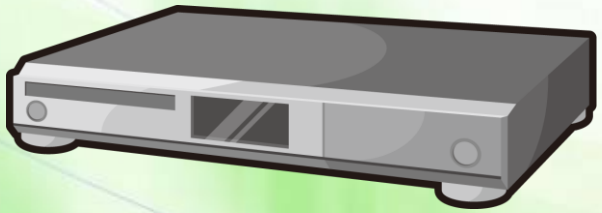
- ランサムウェアなどの短期決戦型も散発
  - ニュースで被害が知れ渡り、対策されるまでの間にできるだけ感染を広げたい
  - 重要なファイルを暗号化して解読できなくしまう
    - ファイルを元に戻して欲しければ金を払え」
    - 払っても元に戻してもらえる保証はない

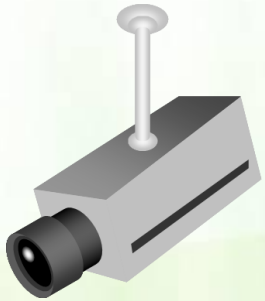
# 最近のサイバー攻撃の傾向

- システムを過負荷状態にして、サービスを提供できなくする攻撃
  - サービスが停止すると業務に影響する
  - オンラインショッピングサイトが停止したら売上に影響する
    - 「攻撃を止めて欲しければ金を払え」
    - 払っても止めてもらえる保証はない

# 最近のサイバー攻撃の傾向

- IoT機器を乗っ取って攻撃の踏み台に使用する
  - 2016年9月、Mirai による 過負荷攻撃でインターネット全体がマヒ
  - 防犯カメラ、ビデオレコーダー、ルータ、プリンタなど、約50万台が乗っ取られ、攻撃に使用された
  - 機器を乗っ取られた被害者が、一転して加害者となった





# 脆弱性が発見されるペース

１日３７件のペースで脆弱性が報告されている

２０１７年１ ～ ９月 に報告された脆弱性

１０，０７３件

IPA公開資料より

Windows、スマートフォン、会計ソフト、IoT機器など、様々な脆弱性が報告されている

# 情報セキュリティの3原則

- 機密性
  - 情報資産を正当な権利を持った人だけが使用できる状態にしておくこと
- 完全性
  - 情報資産が正当な権利を持たない人により変更されていないことを確実にしておくこと
- 可用性
  - 情報資産を必要なときに使用できること

# 情報セキュリティ対策

- 「攻撃を完全に防御することはできない」という前提に基づいて対策をしておく
- 情報セキュリティ体制を作り、運用ルールを策定しておく
- 脆弱性診断など、セキュリティ監査を行って、脆弱な部分をなくす努力を継続する
  - 各種セキュリティ対策製品の導入

# セキュリティ事故発生時の対応

- 被害の拡大を防止するのが最優先
  - LANケーブルを抜く、Wi－FiをOFFにする
- 証拠保全
  - ウィルス対策ソフトで駆除する前に証拠を保全
- 保全した証拠で被害状況を確認、原因を調査
- まずは専門家に相談する

# ICTシステム契約関連のトラブル

- セキュリティ事件・事故発生時に、システムの発注者と開発業者の間で裁判になることも
  - 個人情報が漏洩した際に、利用者への謝罪や賠償はどうする？
  - システム停止によって発生した機会損失の責任は？

損害賠償！

# ICTシステム契約関連のトラブル

- 発注者の重過失となりえるケース
  - 開発業者がセキュリティ対策の必要性を説明したにもかかわらず、発注者が対策を行わなかった場合
  - 契約書にセキュリティ要求事項が含まれていない場合

# ICTシステム契約関連のトラブル

- 開発業者の重過失となりえるケース
  - 開発業者が、発注者に対してセキュリティ対策の必要性を説明しなかった場合
  - 開発当時の技術水準に応じたセキュリティ対策を施さなかった場合

発注者は、開発者の専門的知見を信頼して
システムを発注している

# ICTシステム契約関連のトラブル

- 「結果の予見が容易、かつ、結果の回避も容易」であるにもかかわらず、セキュリティ対策を施さない場合は重過失となる
  - 提案依頼書にセキュリティ要求仕様を含める
  - セキュリティ対策費目を見積に含める

契約締結前に、発注者と開発者の間でセキュリティ対策についてきちんと話し合うことが重要

# ご清聴ありがとうございました