講義資料（第一部）

セキュリティTIPSうすしお味
不正アクセス対応 RDP編

～実践的なインシデント対応と調査技術活用の一例～

2019年9月28日

仙台CTF推進プロジェクト

目次

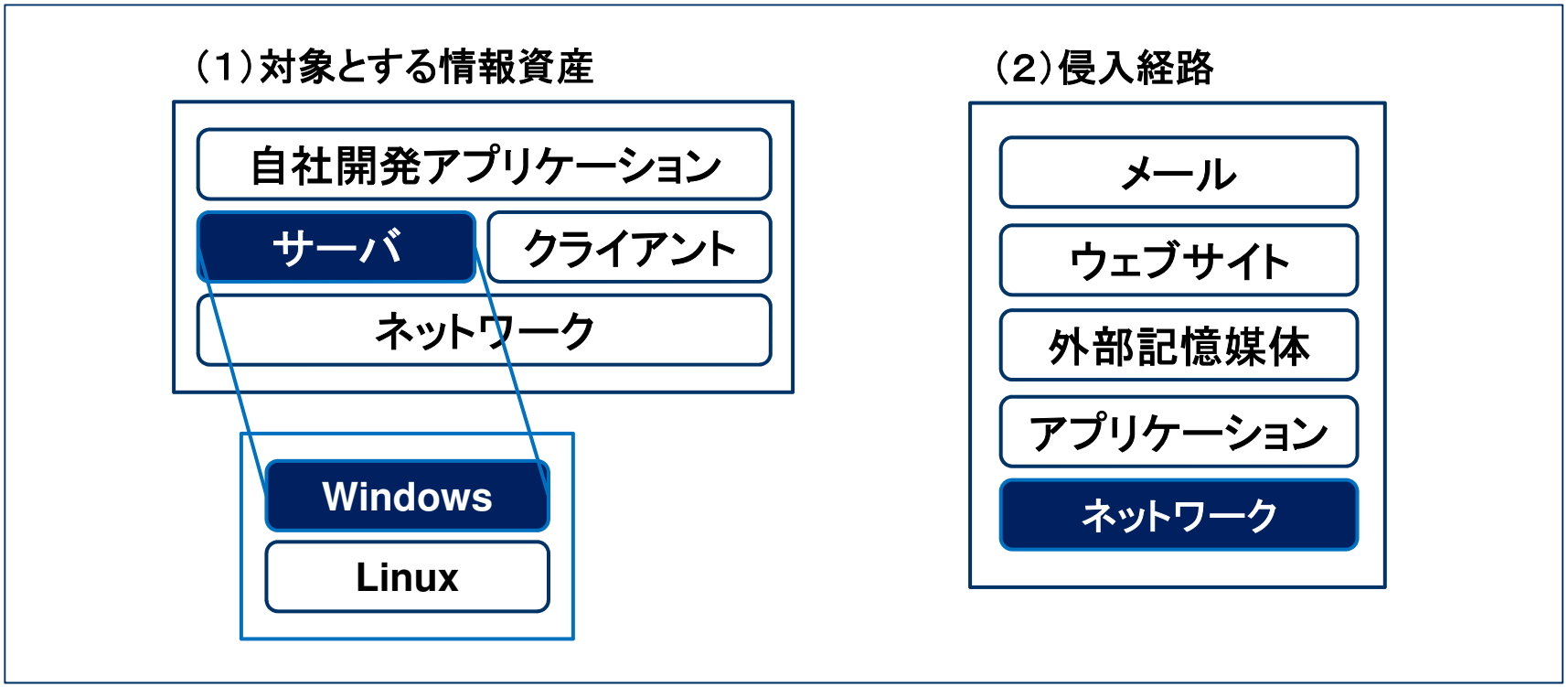
講師自己紹介

名前	戸羽　秀人（とば　ひでと）
職業	会社員
趣味	・ドライブ ・温泉

本講座の対象範囲

- 本講座では、自組織の公開サーバが外部から侵入された場合の調査・対応手法について、学習します。

◆本講座の対象範囲



本講座の学習目標とねらい

学習目標

① 不正通信を調査し、被害を受けたサーバを推測できる。

② Windowsサーバのイベントログを調査し、いつ・どこから・どのように攻撃されたかを推測できる。

③ マルウェアの静的解析（リバースエンジニアリング）を行い、マルウェアの動作を推測できる。

ねらい

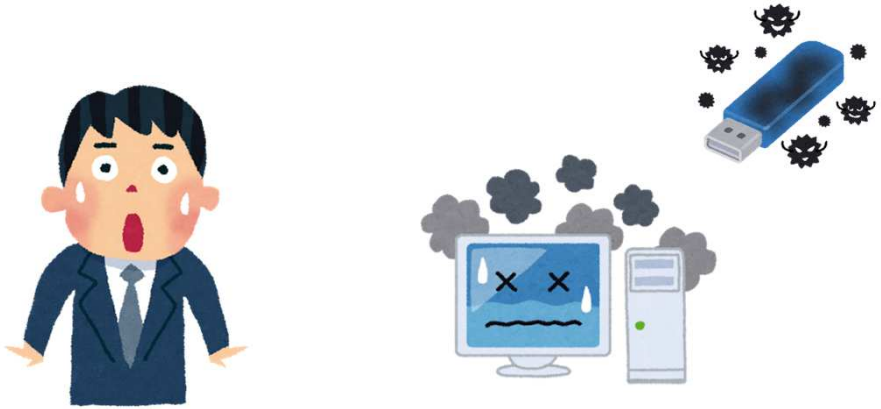
ツールを活用したインシデント対応を体験

↓

面白そう・使ってみようかな、勉強してみようかな

舞台設定

- あなたは、架空の企業「株式会社仙台シーテーエフ」に入社したばかりの新米情報セキュリティ担当者です。
- 先輩と2人で業務を進めていましたが、先輩が怪我で入院してしまったため、社内の情報セキュリティに関するさまざまな問題に一人で対処することになりました。



本講座の進行に関するお願い事項

- 本講座は盛りだくさんの内容となっていることから、時間の都合上、要点を絞って説明します。説明を割愛したスライドについては、後日、各自で資料をご参照ください。

- また、実習時間も短めとなっており、時間内に全ての実習が終わらないこともあるかと思いますが、実習終了時間になったら講義を再開させていただきます。

- 講義資料、実習資料ともに、皆様が持ち帰り復習できるよう準備しておりますので、ご理解・ご協力くださいますようお願いいたします。

第1章. インシデント対応の基本手順

この章では、インシデント対応をどのような手順で行えば良いのか、全体的な流れと考え方について学習します。

講義

インシデント対応とは

- 情報セキュリティ分野における「インシデント」とは、不正アクセス、マルウェア感染、情報流出事故など、情報セキュリティを脅かす事象のことです。
- インシデン対応とは、インシデントが発生した際に、被害を最小限に抑止するための「事後対応」のことを指します。

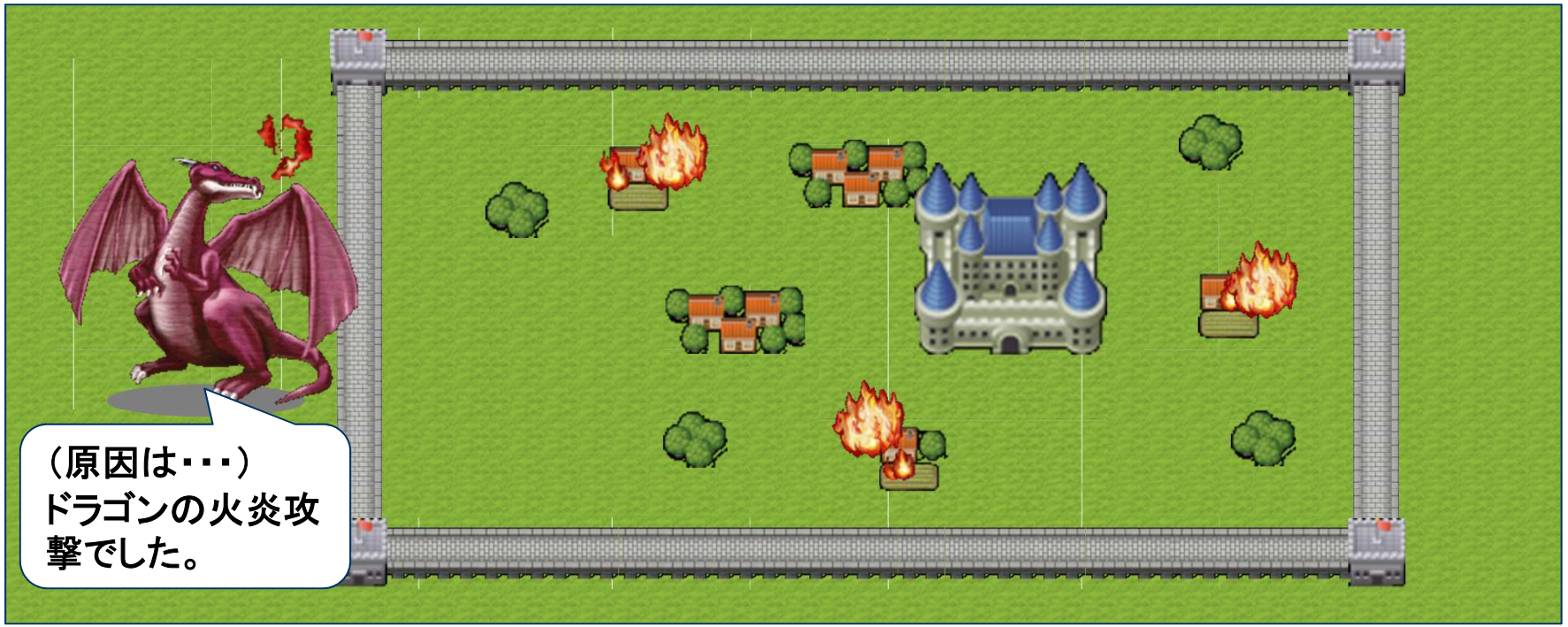
- 防御策の実施に加えて、万が一インシデントが発生した場合に備え、迅速的確に対応できる体制を整備しておくことが大切です。

（補足）ISO/IEC 27001では、インシデントは、「望まない、又は予期しない一連の情報セキュリティ事象であって、事業運営や情報セキュリティを脅かす可能性が高いもの」と定義されています。

インシデント対応のイメージ（1）

- 城壁の中で爆発が発生しました。あなたは警備隊の隊長です。さて、どうしますか？

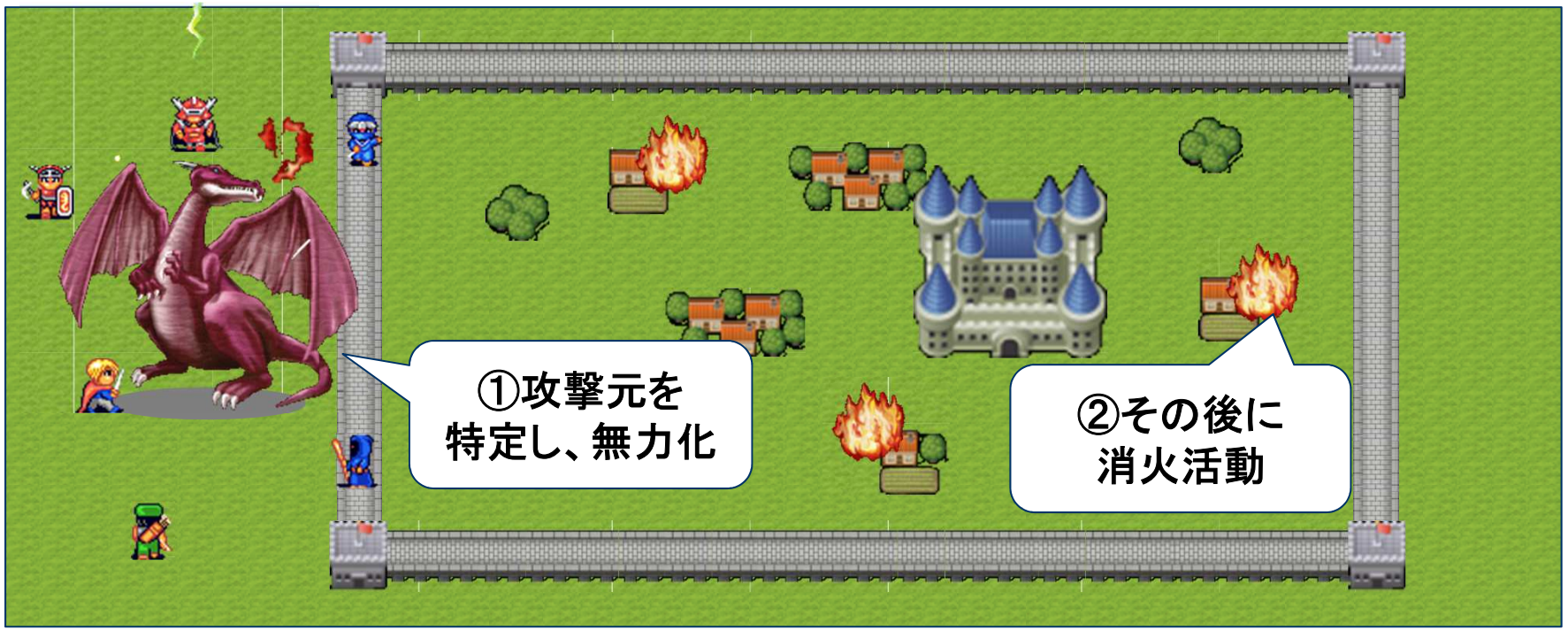
消火 ➡ 新たな爆発 ➡ 消火 ➡ 新たな爆発！
原因が不明なまま闇雲に対処しても、イタチゴッコになる可能性がある。



インシデント対応のイメージ（2）

- 現在進行形で被害が拡大している場合は、最初に攻撃元を無力化します。
- それから復旧（消火）活動、および事後処理を行います。

状況を正しく把握できれば、対応は意外とシンプル

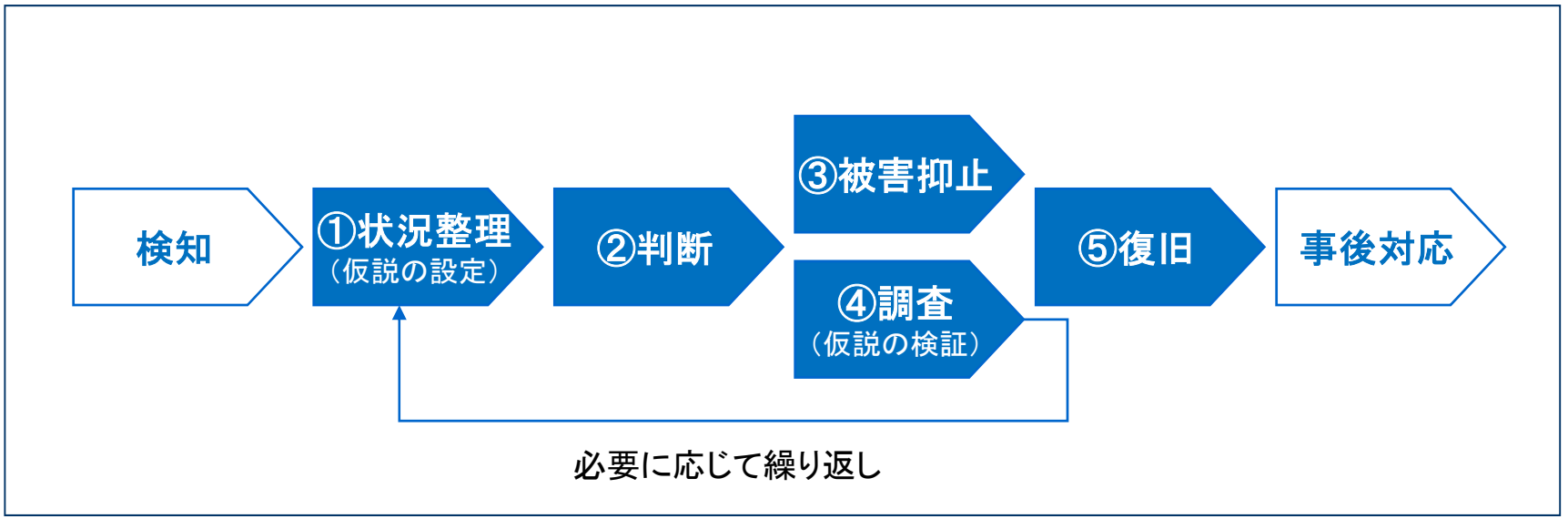


講義

インシデント対応の基本手順

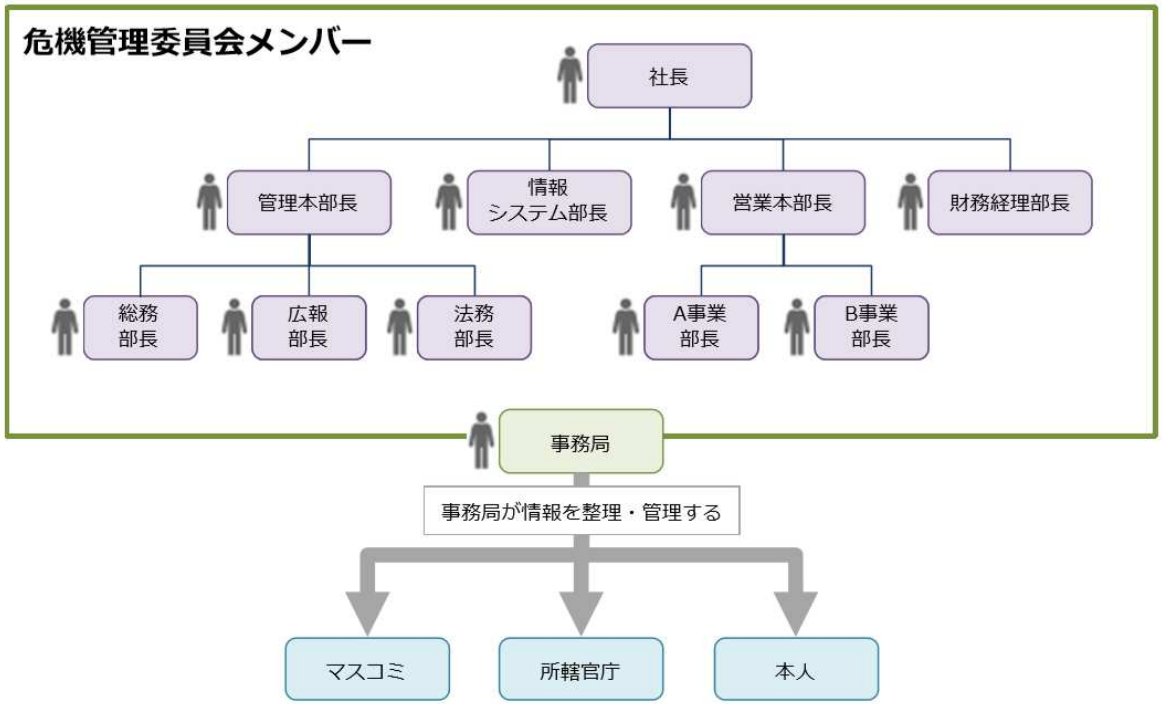
- **インシデント対応では、次の①～④の手順を繰り返し、⑤復旧を目指します。**
  - ① 事実と推測を整理し、発生している事象とリスクの「仮説」を設定する。
  - ② リスクの大きさと、対応にかかる労力などを考慮し、対応方針を判断する。
  - ③ 被害抑止のため、仮説で想定したリスクの対策を講じる。
  - ④ 判断に必要な情報が不足している場合は、調査を実施し、仮説の検証を行う。
  - ⑤ 同様の攻撃を受けないよう応急処置を施した上で、復旧作業を実施し、事態を収束させる。

◆ インシデント対応の基本手順



インシデント対応における留意事項

- 適切なインシデント対応を行わず、組織の信頼低下につながった事案が多くあります。
- インシデント対応は、組織の危機管理対応です。IT部門だけでなく、各部門が連携して対応しなければなりません。上司への報連相、ビジネスへの影響を踏まえた対応策の検討を心掛けましょう。
- 特に、現場で調査をしていると全体が見えなくなります。調査者と管理者（指揮者）を明確に分けて対応しましょう。



出典：丸山満彦「個人情報が流出 有事のときの危機管理 第 2 回 情報漏えいに備えた社内体制の整備」22, ITmedia, 2005/03/03

第2章. いきなり体験！インシデント対応

この章では、実際のインシデントを想定した対応を体験していただきます。インシデント対応のTIPSを紹介し、TIPSを活用する演習を実施していただきます。

ストーリー

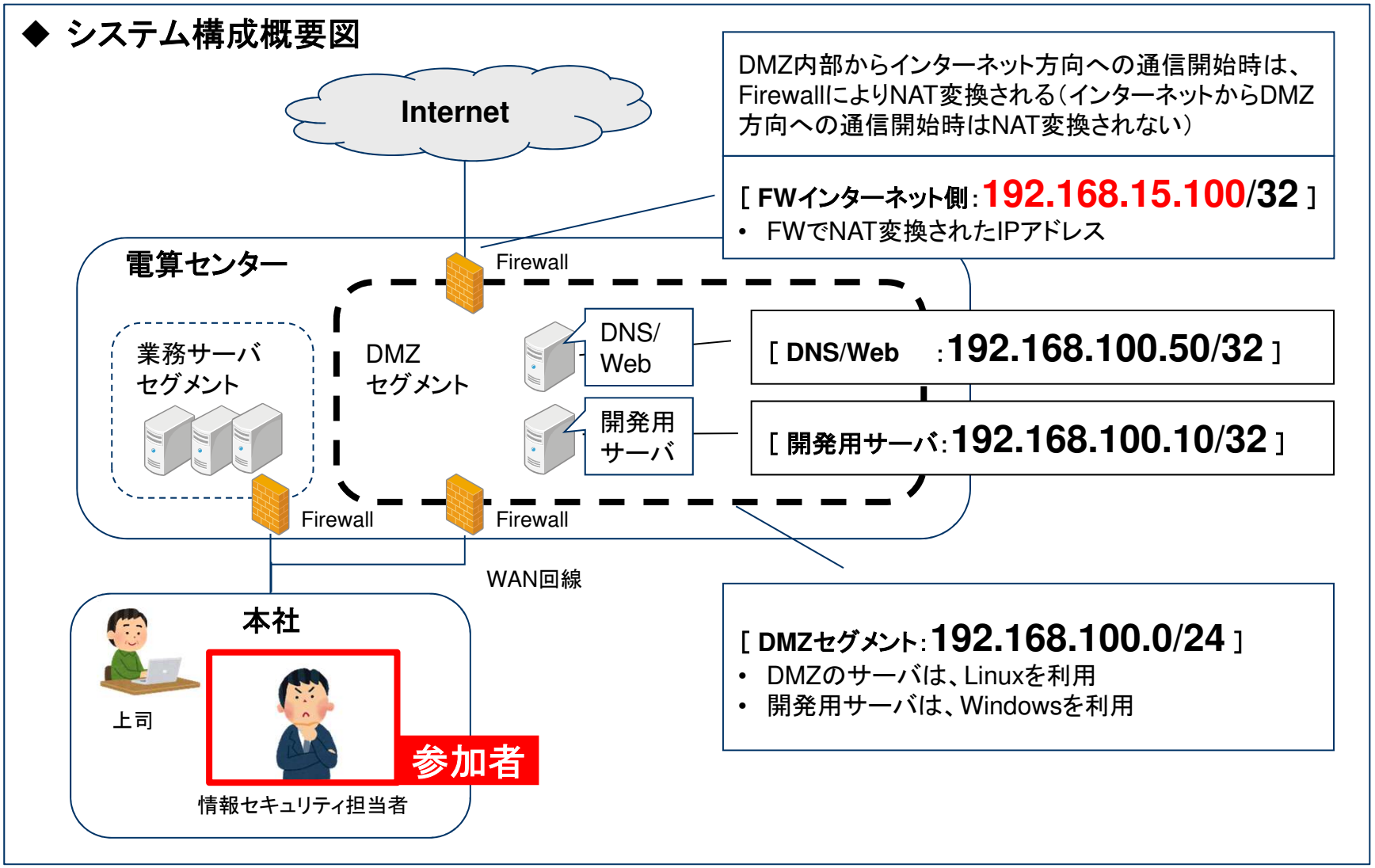
本日のインシデント

- とある休日の夜、あなたが自宅でSNSを閲覧していたところ、「うちのサーバが192.168.15.100から大量のRDPアクセス受けてる。仙台シーテーエフのIPみたいだけど乗っ取られているのか？とりあえずファイアウォールで遮断しておこう。」と投稿されていることを発見しました。
- 「192.168.15.100」は、DMZのインターネット側ファイアウォールのIPアドレスです。さて、どうしますか？

ストーリー

「株式会社仙台シーテーエフ」のシステム構成

◆ システム構成概要図



DMZ内部からインターネット方向への通信開始時は、FirewallによりNAT変換される（インターネットからDMZ方向への通信開始時はNAT変換されない）

[FWインターネット側：192.168.15.100/32]
- FWでNAT変換されたIPアドレス

[DNS/Web　：192.168.100.50/32]

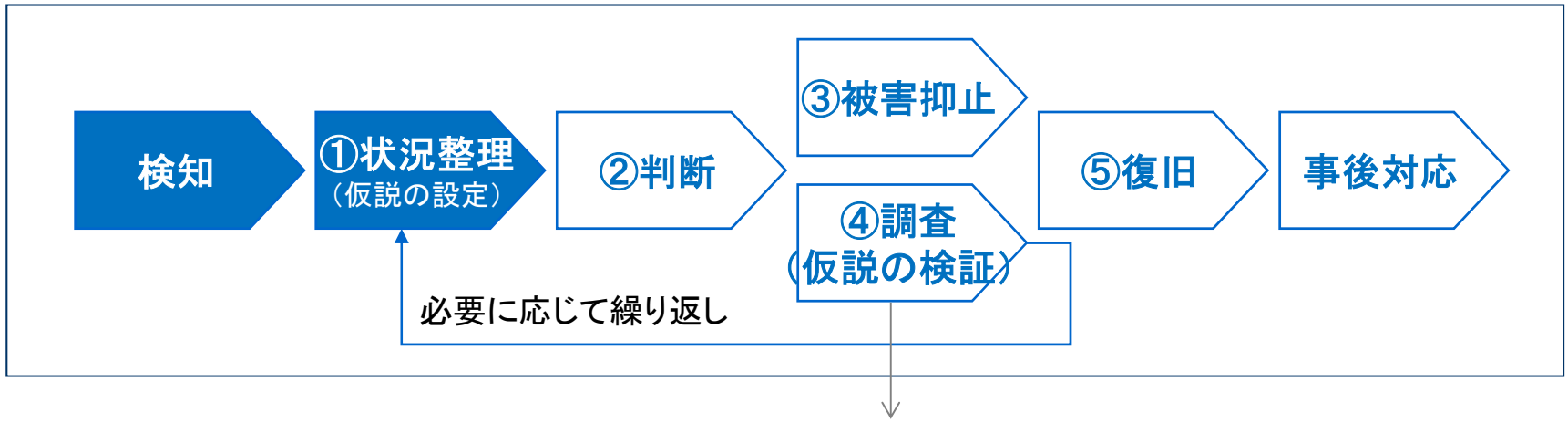
[開発用サーバ：192.168.100.10/32]

[DMZセグメント：192.168.100.0/24]
- DMZのサーバは、Linuxを利用
- 開発用サーバは、Windowsを利用

ストーリー

状況整理1

- システム構成などを踏まえ、冷静に状況を想定します。
- イタズラ投稿の可能性はないか？
  → イタズラの可能性はありますが
  実際のIPアドレスと合致しており、イタズラと断定できる根拠がないです。
- 投稿者はなぜIPアドレスから会社を特定できたのか？
  → IPアドレスを逆引きすれば、会社名が分かります。
- ただ、RDPを有効にしている自社DMZのサーバは無いはずだが・・・
- （休日だけれど・・・） 調査が必要

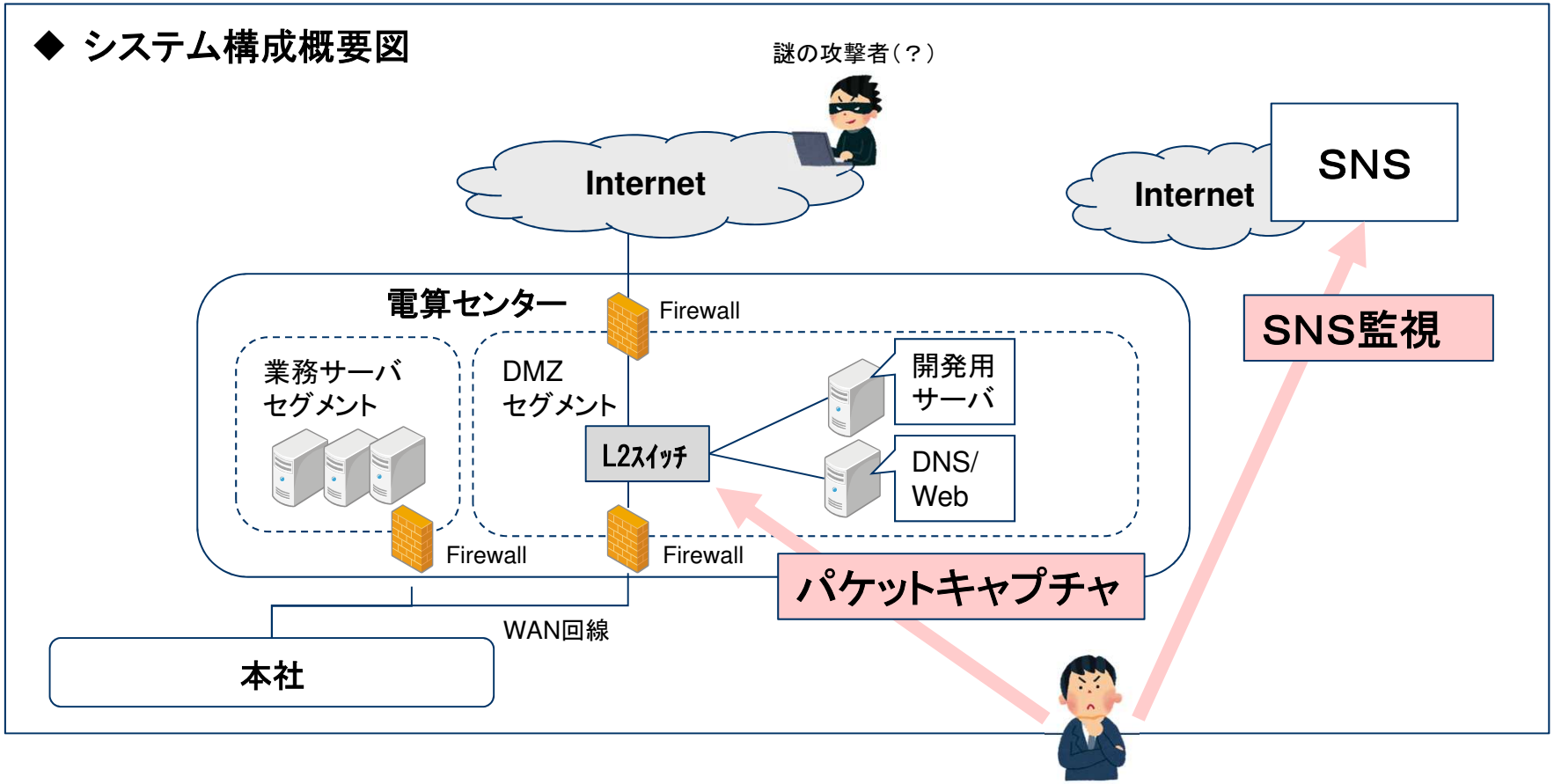


TIPS-1 実習1 パケット解析

ストーリー

判断1

- 調査が必要と判断しました。上司に電話で報告・相談のうえ出社し調査開始しました。
- 調査方法として①パケットキャプチャ、②サーバ個別点検がありますが、サーバ台数が多いため①を選択しました。また、調査と並行してSNSの監視を実施します。



講義

（補足）RDP

RDP【Remote Desktop Protocol】

RDPとは、サーバコンピュータの画面をネットワークを通じて別のコンピュータ（クライアント）に転送して表示・操作するリモートデスクトップあるいは仮想デスクトップで、サーバとクライアントの通信に用いられる通信プロトコル（通信規約）の一つ。Microsoft社が開発したもので、Windowsのリモートデスクトップ（Remote Desktop Service）などで利用されている。

サーバ側で展開される画面情報をクライアント側に転送したり、クライアント側で利用者がキーボードやマウスなどを操作した情報をサーバ側に転送したりする際のデータ形式やデータ伝送手順を定めている。

RDPのサーバやクライアントは同社のWindowsやWindows Serverに標準で同梱されているため、特にソフトウェアの導入や設定などを行わなくてもすぐにリモートデスクトップを利用することができる。RDPの仕様は公開されており、同社以外が開発・公開したRDPサーバやRDPクライアントなどもあり、Windows以外の環境で動作するものもある。

【出展】IT用語辞典 e-Words http://e-words.jp/w/RDP.html

Windowsが利用するRDPデフォルトの待ち受けポート番号は「3389」番

TIPS-1 パケット解析

ネットワーク上を流れるデータを取得し、どのような通信が行われているかを調査する方法を学習します。

パケットキャプチャ

- 本番環境におけるパケットキャプチャは、サーバ上で取得する場合とネットワーク上で取得する場合があります。
- サーバ上で取得
  - 障害対応の場合はサーバで取得することが多いですが、インシデント対応の場合は攻撃を受けたサーバは証拠保全のため操作できません。ネットワーク上で取得することになります。
- ネットワーク上で取得
  - 回線速度が速く（数Gbps～数百Gbps）、通信量が多い場合、パケットを取りこぼす可能性が高いため、専用機器を利用することを推奨します。
  - 専用機器の利用が難しいためツールを利用し、長時間キャプチャする場合は、CUIで動作するツールを利用することを推奨します。
    - GUIのツール例：Wireshark
    - CUIのツール例：dcpdump(Linux)、netsh(windows)、tsharkとdumpcap(WiresharkのCUI版)
- 今回のように、簡易的な調査を行う場合は、ネットワークスイッチにミラーポートを設定し、Wiresharkをインストールしたノートパソコンを接続して、キャプチャするのが一番簡単な方法ですし、実際にそのように対応するケースも多いです。

Wiresharkとは

- Wiresharkとは
  - ネットワークプロトコルアナライザ

- Wiresharkの主な機能
  - パケットロギング、プロトコルアナライズ、表示フィルタ、統計

- Wiresharkの特徴
  - 独自プロトコルもLua言語でプラグインを記述可能
  - Caine Linuxにディフォルトでインストール済み ※Windows版も有

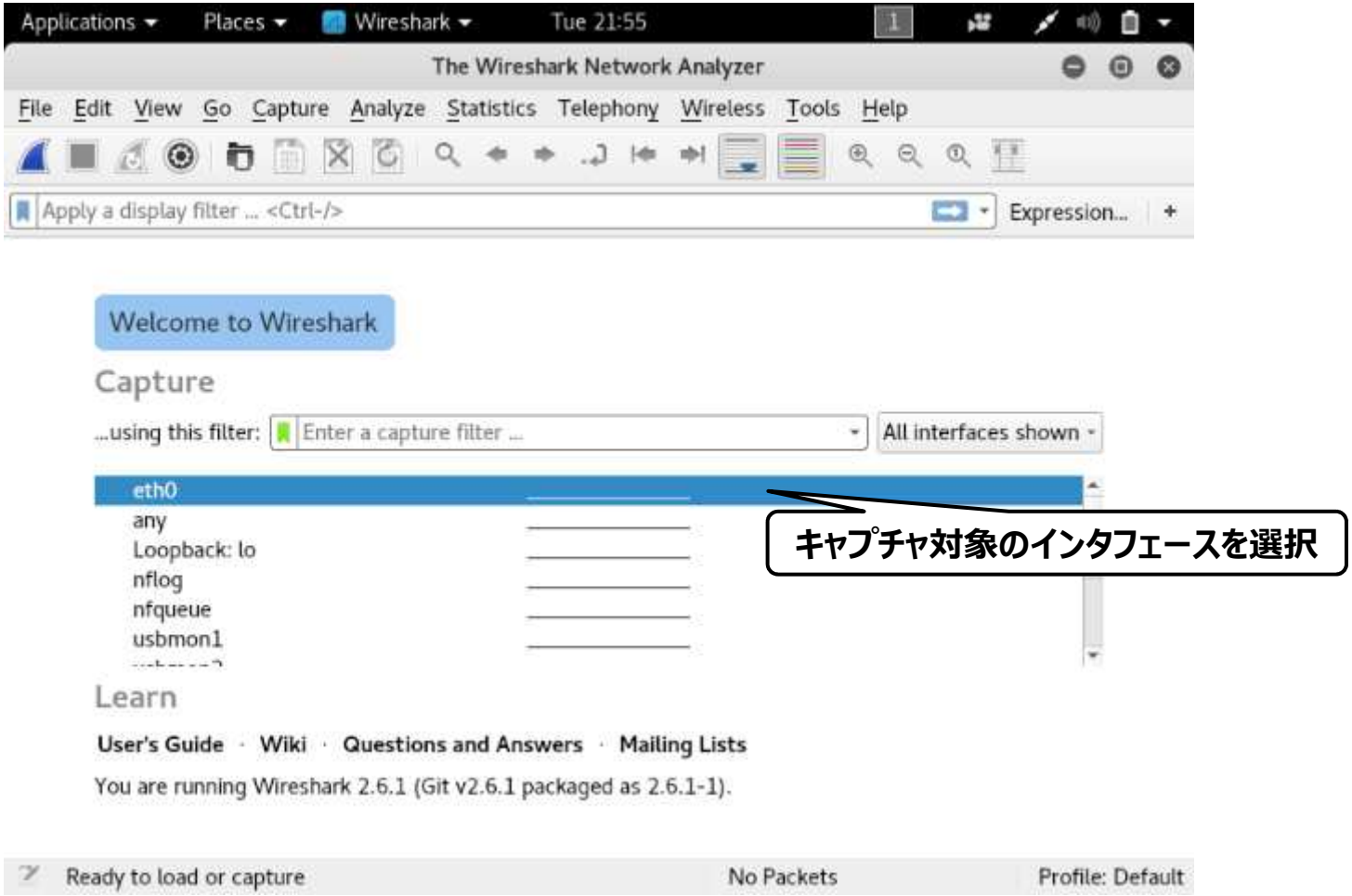
https://www.Wireshark.org/

Wiresharkの使い方 ー 起動

- 左下メニューボタン（赤丸）「Forensics Tools」->「Network forensics」->「Wireshark」で起動します。

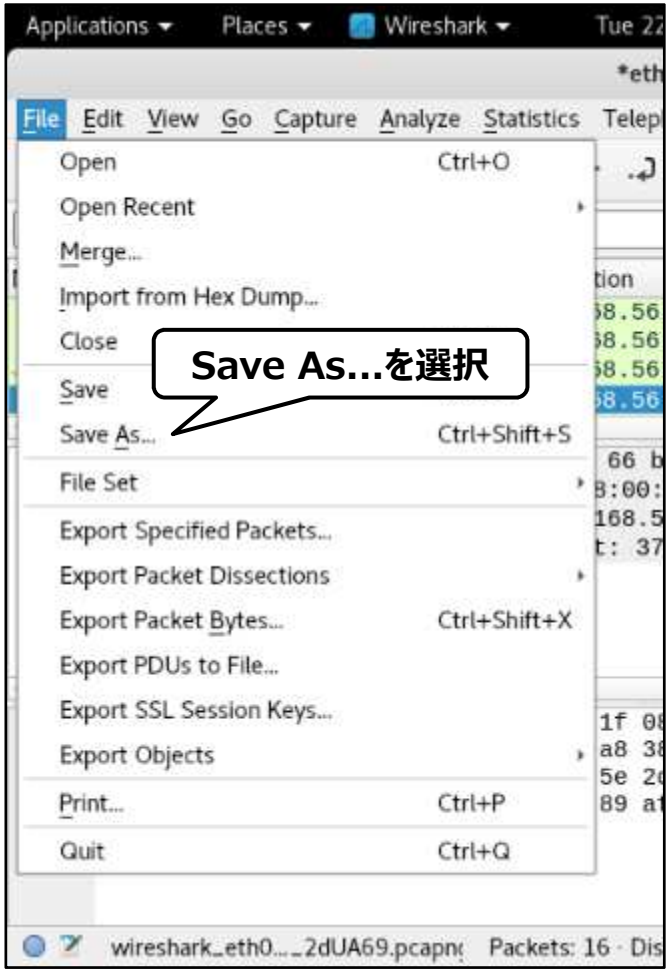
Wiresharkの使い方 － キャプチャ開始

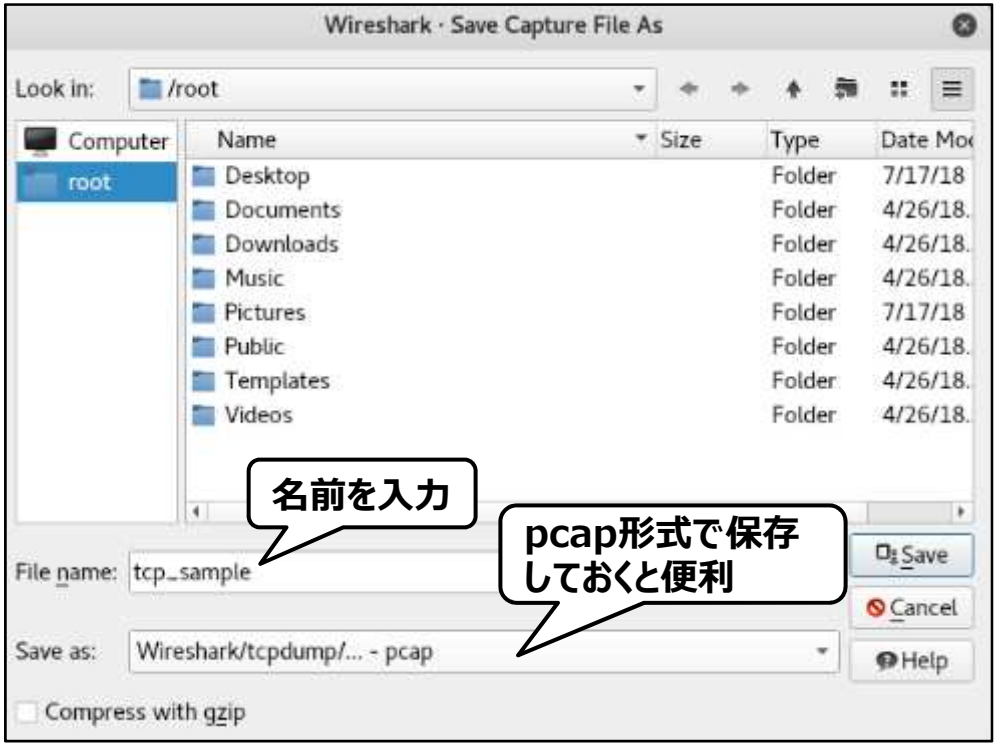
- キャプチャ対象のインタフェースを選択して、キャプチャを開始します。



Wiresharkの使い方 － キャプチャファイルの保存

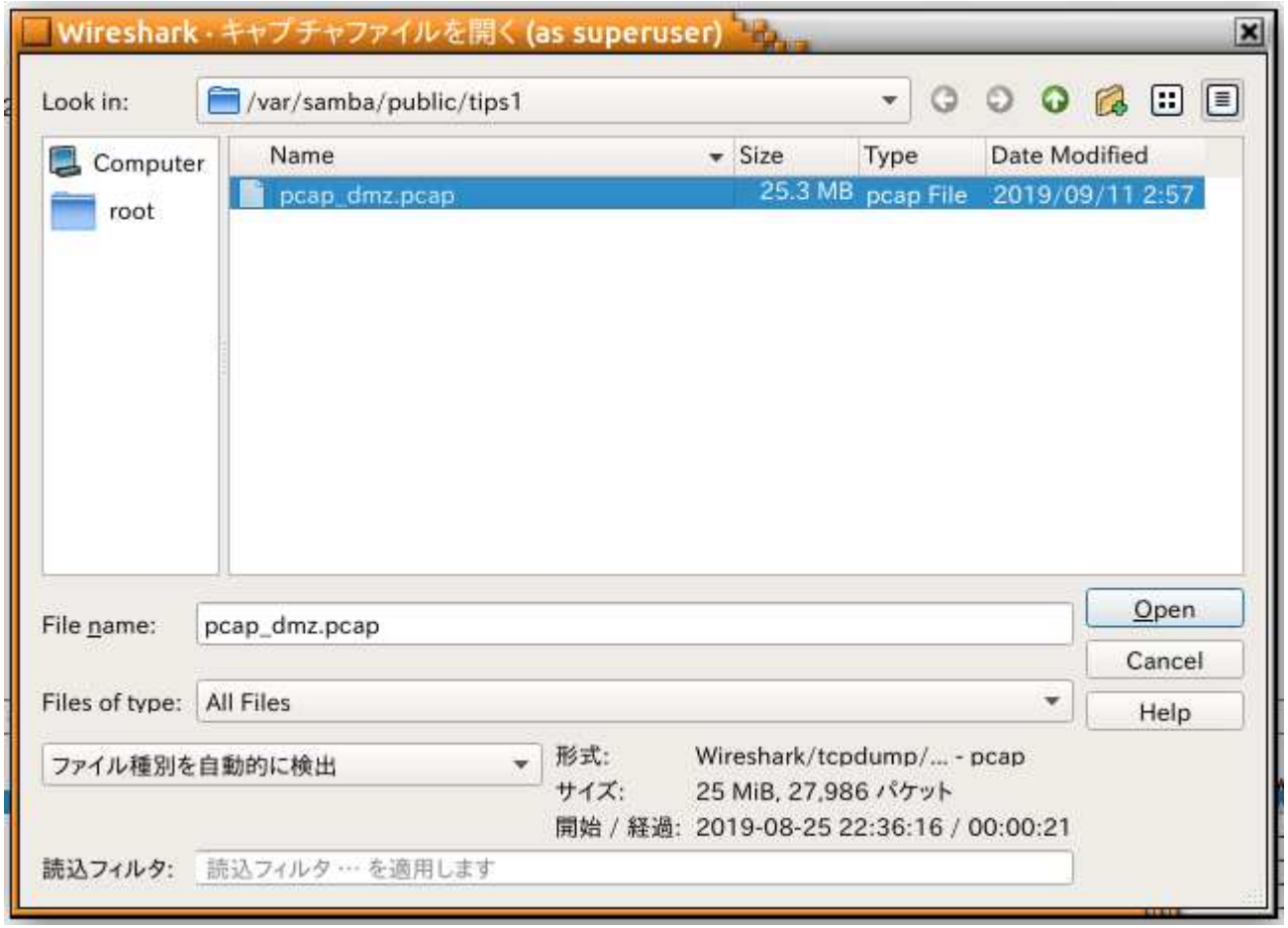
- メニューバー「File」->「Save As...」を選択し、キャプチャしたファイルを保存します。





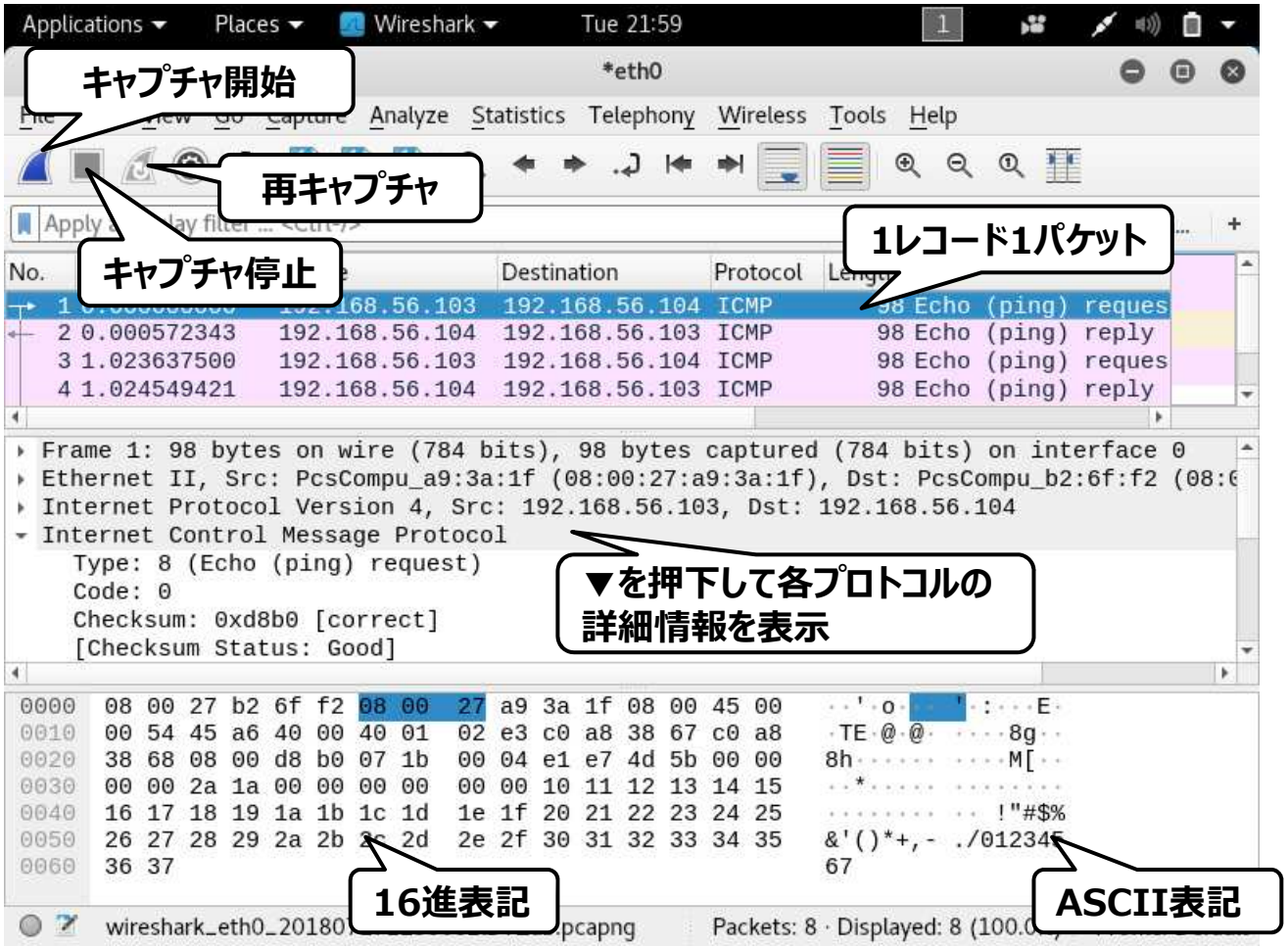
Wiresharkの使い方 － pcapファイルを開く

- メニューバー「ファイル」->「開く」を選択し、ファイル選択画面からキャプチャしたファイル（拡張子 pcap）を選択し、「Open」ボタンを押します。



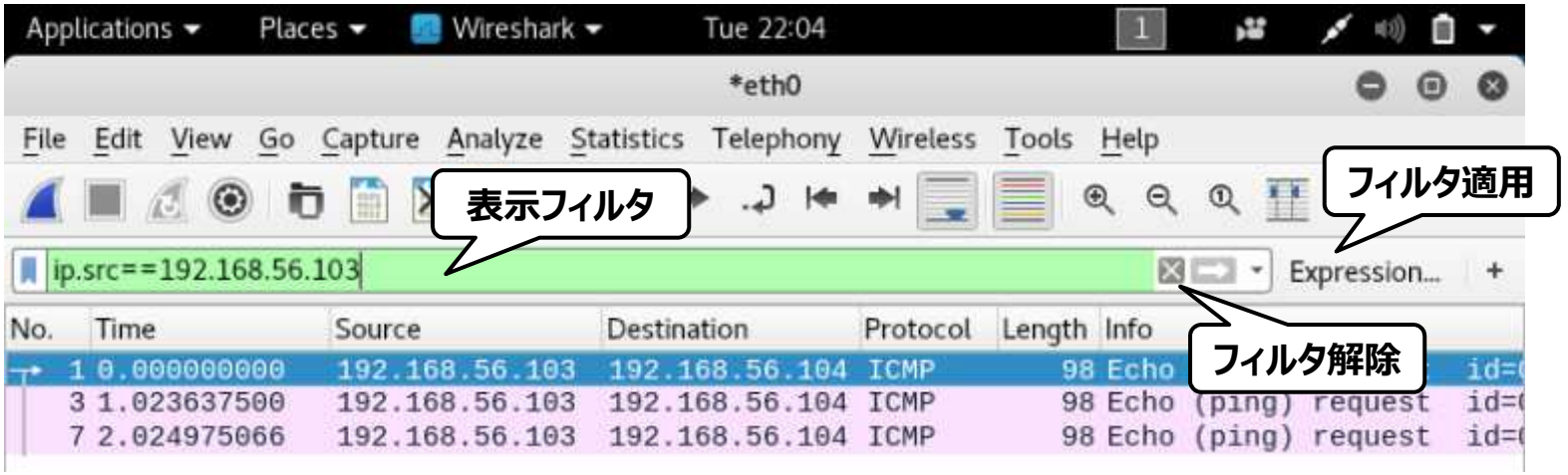
Wiresharkの使い方 － 基本操作と画面の見方

- キャプチャ画面では、任意のパケットの詳細情報を確認することができます。



Wiresharkの使い方 － 表示フィルタ

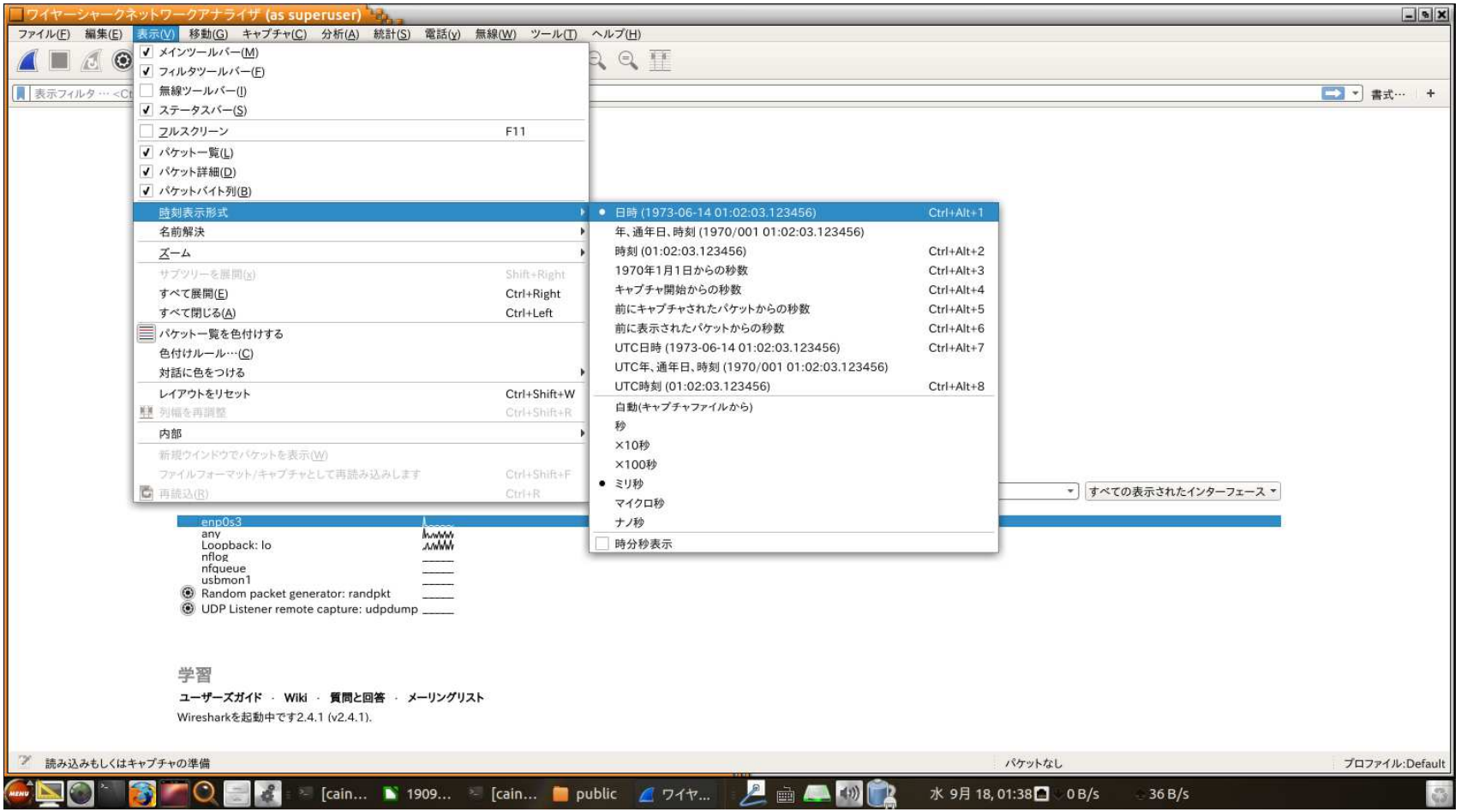
- 表示フィルタを用いて、特定のパケットのみを表示させることができます。構文が正しいと「緑」、間違っていると「赤」の背景色になります。「=」が2つ必要な点に注意してください。



フィルタ	概要	例
eth.src eth.dst	対象の送信元／宛先MACアドレスを含むパケットのみ表示	eth.src==08:00:27:46:d9:2a
ip.src ip.dst	対象の送信元／宛先IPアドレスを含むパケットのみ表示	ip.src==192.168.1.1 ip.dst==192.168.1.2
icmp	ICMPプロトコルのみを表示	icmp
!= (条件)	条件以外を表示。「!」は否定の意。	ip.src!=192.168.1.1

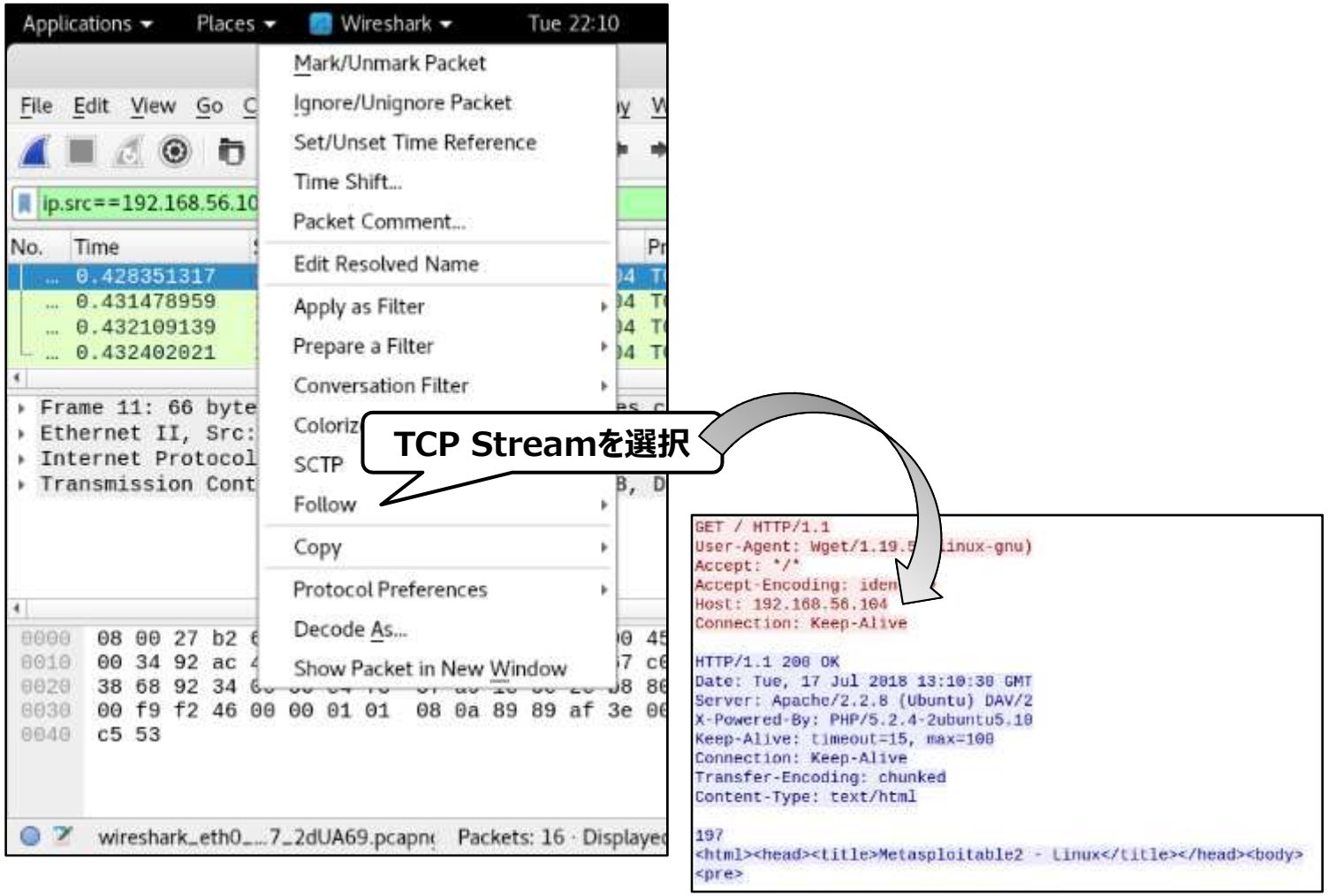
Wiresharkの使い方 － Time

- デフォルト設定では「Time」列は最初のパケットからの経過時間が表示されます。メニューバー「表示」->「時刻表示形式」->「日時」を選択することで、パケットを取得した時間が表示されます。



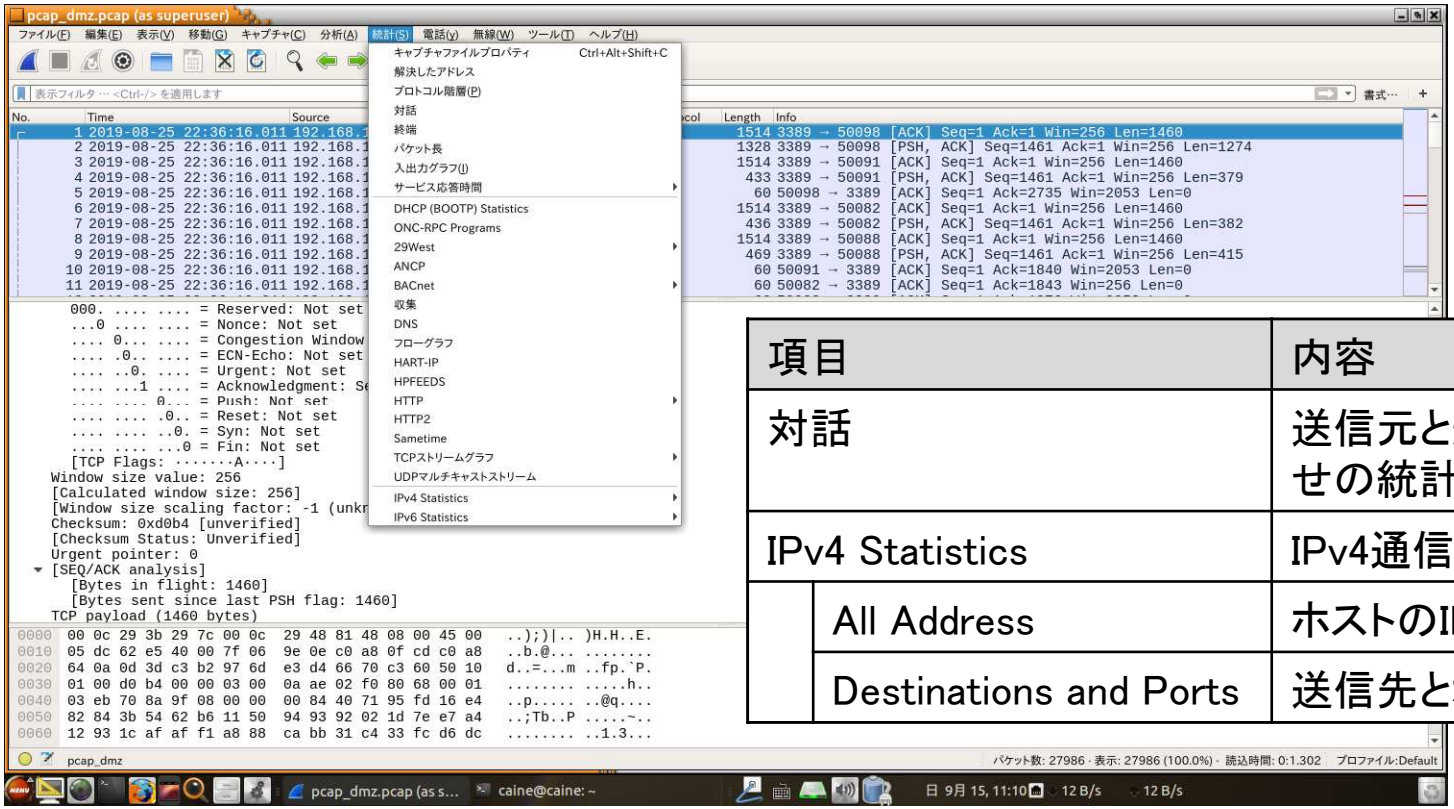
Wiresharkの使い方 － TCP Stream

- TCPパケット上で右クリックし、「Follow」->「TCP Stream」を選択し、TCPストリームが可視化できます。



Wiresharkの統計情報

- Wiresharkは、さまざまな統計情報を取得できます。
- メニューバー「統計」を選択すると、メニューが表示されます。



項目		内容
対話		送信元と送信先の組み合わせの統計情報
IPv4 Statistics		IPv4通信の統計情報
	All Address	ホストのIPアドレス一覧
	Destinations and Ports	送信先とポート番号一覧

- 個々のパケットだけを見ていてはわからないことがあります。統計情報から「あたり」をつけることが重要です。普段の状況（ベースライン）を把握していれば、異常（アノマリ）を検出しやすくなります。

実　習　1　パケット解析

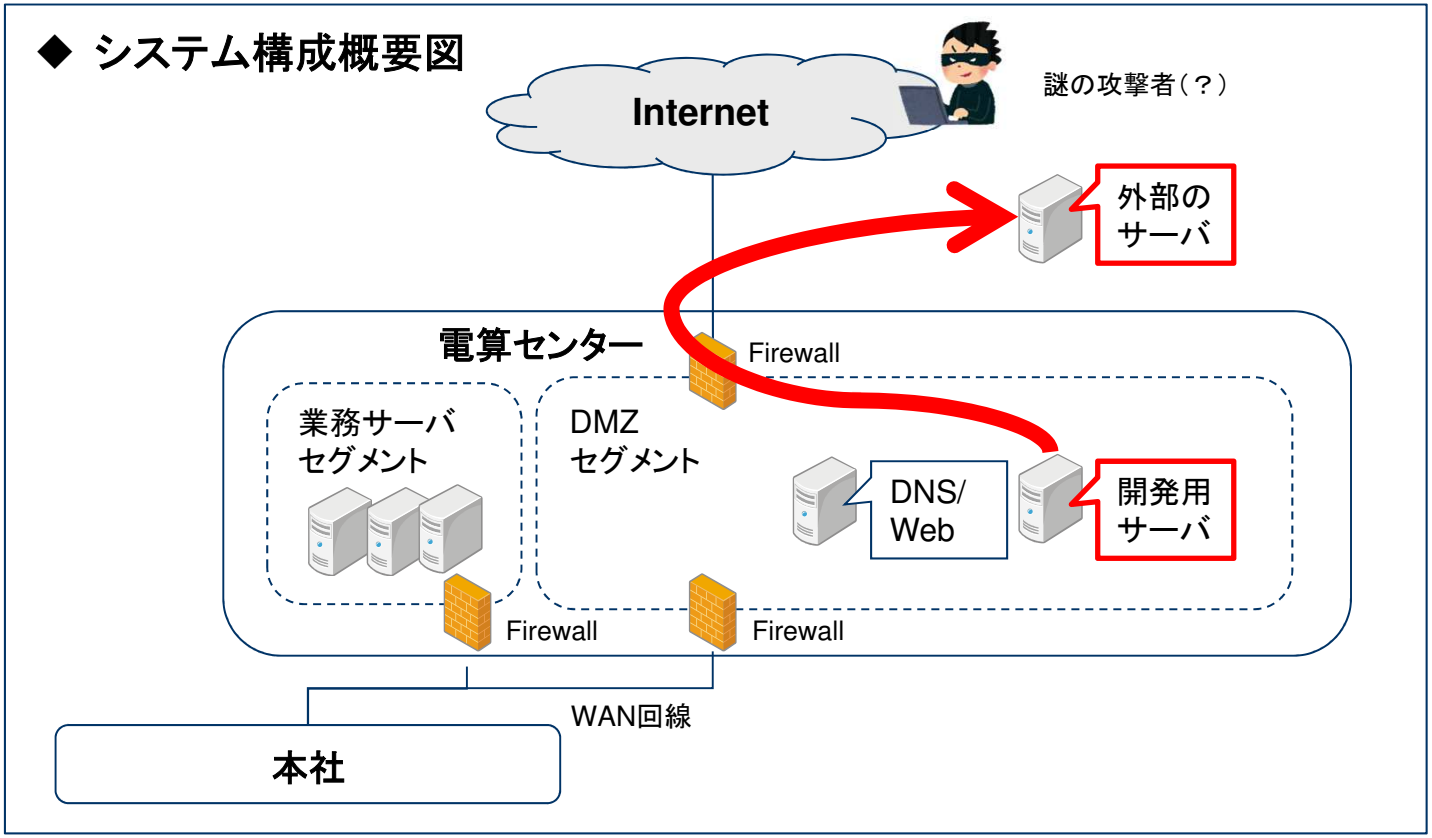
- 「別紙.TIPS-1 実習資料」を参照し、DMZのネットワークを流れる通信の記録から、外部に攻撃しているサーバを特定してください。

実習時間
20分間

ストーリー

不審通信発信元の特定

- 不審通信発信元は、事業部門がDMZに設置した開発用サーバ
- インシデントの可能性が高いと判断し、危機管理体制を立ち上げ



ストーリー

開発用サーバの隔離

- 事業部門に連絡したうえで、開発用サーバのLANケーブルを抜線
- 緊急時において、休日夜間における主管部門との連絡ルートは確保されているか、システム運用個所が切り離しできる権限があるか、を事前に定めることが重要

ストーリー

状況整理

- 事業部門の担当者が出社するまで待機
- その間に、開発用サーバがセキュリティ侵害された原因を推測（他サーバは現時点では不審通信なし）
- 事業部門担当者に聞き取り調査を実施（侵害の原因になりそうなものを確認）

・リモートアクセス系サービスの利用状況とパスワード強度は？
・セキュリティパッチ適用状況は？
・ネットワークの待ち受けポートとサービスは？

ストーリー

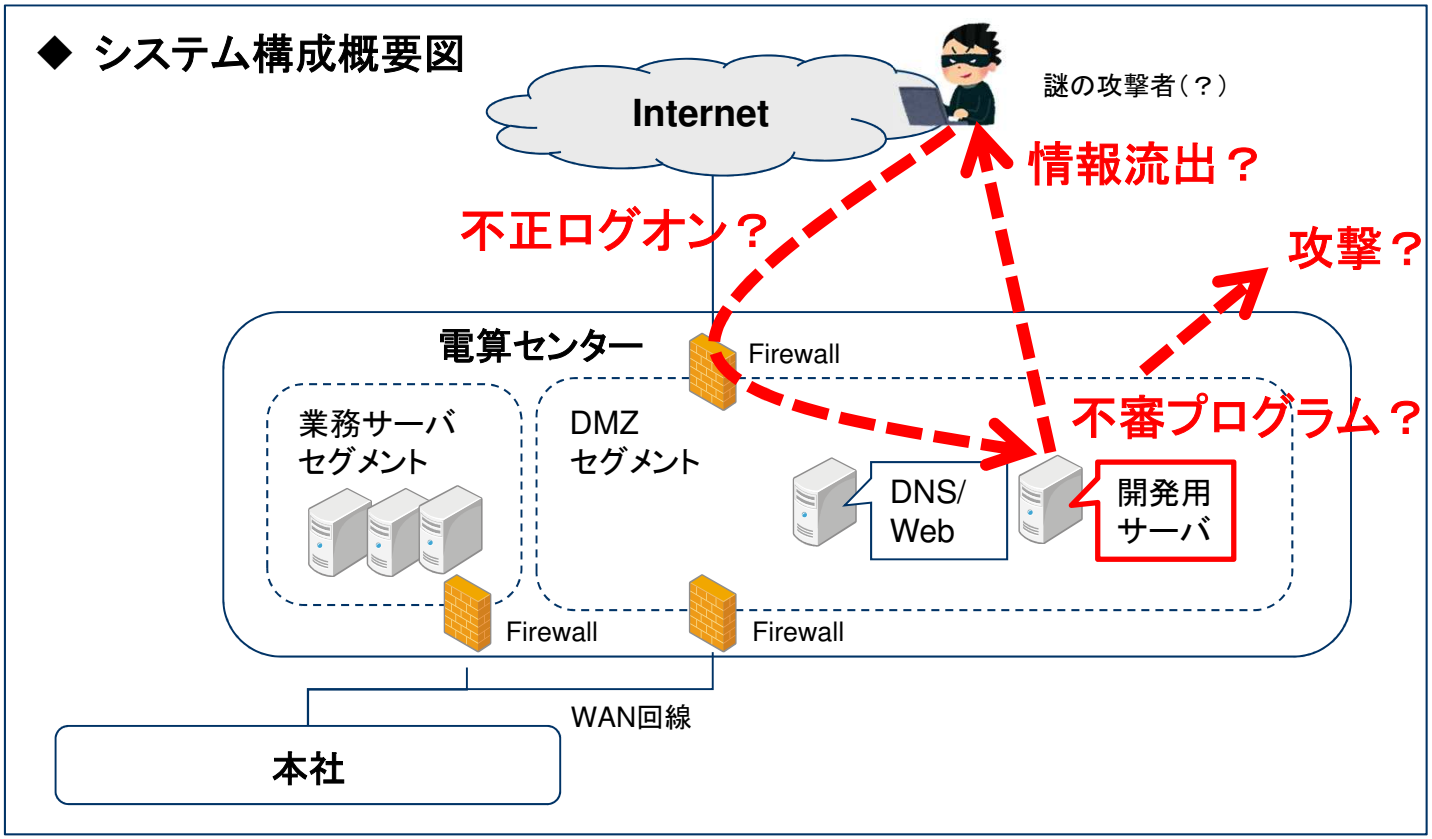
事業部門への聞き取り調査

- 事業部門の担当者が出社。聞き取り調査の結果、以下が判明。
- 開発作業が遅れており、本日（日曜日）も出社していたが予定作業が終わらなかったため、自宅で作業を継続しようと考え、インターネットからのRDP接続を有効にし、帰宅後に22時前頃に接続して作業を行った。管理者アカウント（Administrator）の**パスワードは容易に推測可能なもの**を設定していた。
- 開発用サーバは、セットアップ直後にアップデートしており最新状態となっていた。また、RDP以外にはネットワークから接続可能なサービスは有効化していなかった。
- 開発用サーバにはテスト用に本番データ（**顧客の個人情報**）**を格納**していた。

ストーリー

状況整理（仮説の設定）2

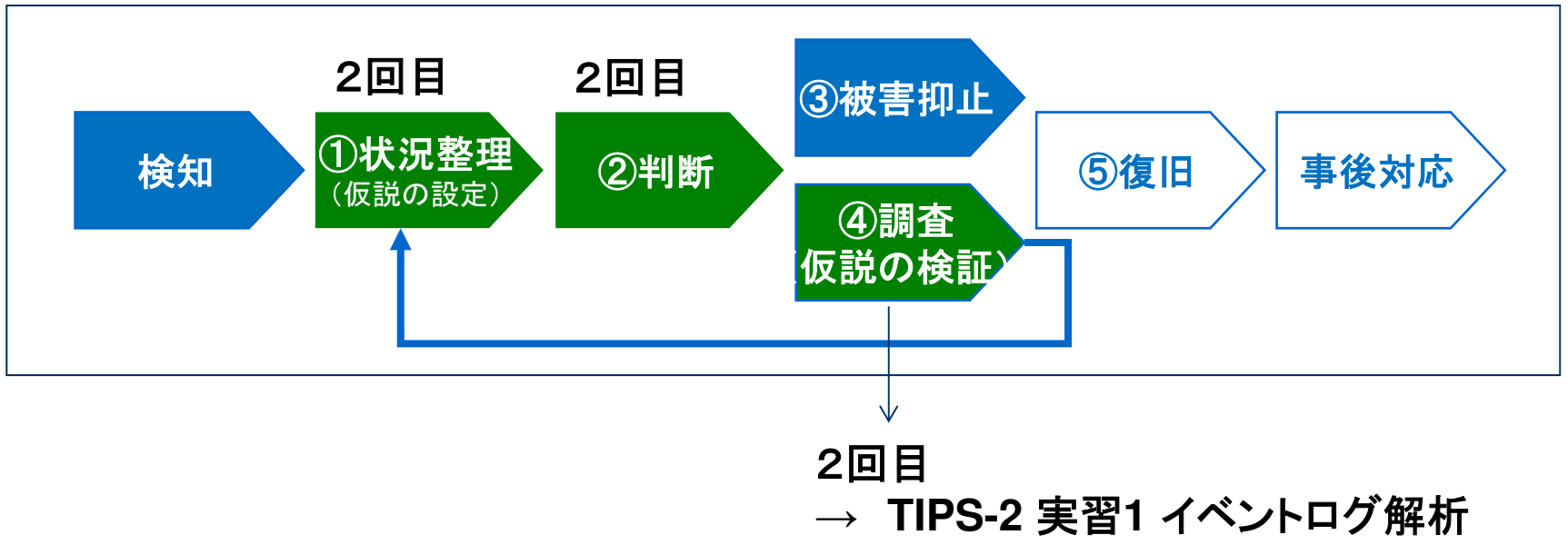
- 聞き取り調査の状況からRDP経由で不正ログインされた可能性が高い。なお、開発用サーバ以外のサーバ（情報システム部門管理）のID/パスワードは別管理でありシステム的な連携も無く、セキュリティパッチも適用されているため侵害された可能性は低い。
- また、第三者へのRDP攻撃に利用される不審プログラムも実行されたと思われる。
- 格納されていた本番データの情報流出も懸念される。



ストーリー

判断2

- 開発用サーバの証拠保全を実施し、セキュリティ侵害の原因を特定

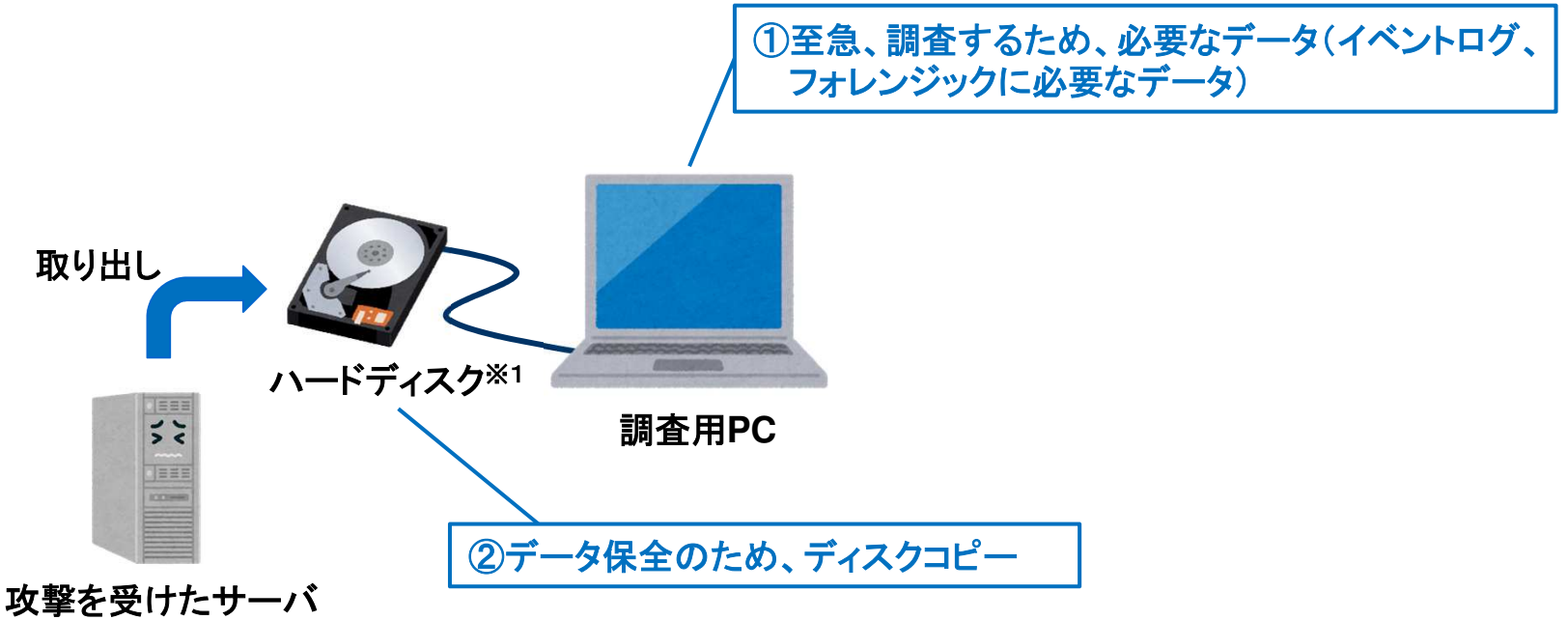


ストーリー

証拠保全

- 状況に応じて証拠保全の方法を使い分ける。
  - ディスクコピー
  - 必要なデータのみ抽出
- 今回はディスクを抜き出して必要なデータのみ保全したうえで、ディスクコピーを作成することとした。

◆フォレンジック調査の方針



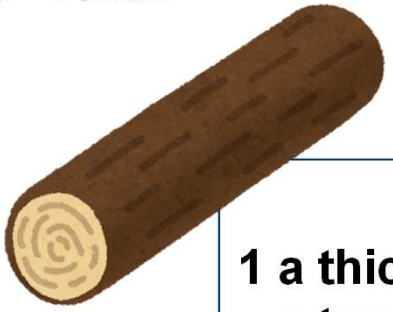
TIPS-2 イベントログ解析

ログを解析するためには、ログの意味を理解する必要があります。また、実際のインシデント対応では、ログ解析に十分な時間を確保できないことが多いです。効率的・効果的にログ分析する手法について学習します。

講義

ログとは？

- ログはコンピュータの動作記録です。
- 「log」の語源



1 a thick piece of wood that has fallen or been cut from a tree
2 (also logbook) the official written record of a ship's or an aircraft's journey

【出展】Oxford wordpower dictionary

  - 船の速度でノット（英:knot 日:結び目）が使われるのは、木片に長い紐を括り付け、紐に一定間隔で結び目をつけ、流れ出た結び目の数を船の速度としたことに由来します。この木片が丸太（log）であり、船の計測が航 海日誌（logbook）へと結びついたとされています。

セキュリティログ分析の流れ

- ①ログの取集と蓄積
  - 一元管理
- ②怪しいログを見つける
  - 基本的には、大量のログから攻撃に関係する記録を絞り込みます。
  - 攻撃に関係のない正常なログも記録されていることから、普段見慣れていないと難しいです。また、ログの意味が分からないと理解できません。
  - 全体のログから正常なものを取り除いたり、全体をあるキーでソートして出現回数の低いものに着目します。
  - 常時監視するためには、見つける手順をロジック化したり、文字列としてパターン化して自動化します。
- ③分析し、確証を得る
  - 怪しいログが見つかったとしても、それが本当に攻撃かは断定できません。
  - 成功したか否かまではわかりません → アプリが動作しているサーバのログを分析します。
  - ツールによる単純な攻撃であればある程度自動的に判断できますが、少し複雑な攻撃になると自動化が難しくなります。
  - 攻撃者の行動について仮説を構築しながら、ログを分析していくことになります。ツールはこれらの分析を支援してくれますが、絞り込んでいけるかどうかは分析者の技量に大きく依存します。

講義

ログ分析のTIPS（1）

- コンピュータが動くとログが蓄積されます。ただし、デフォルト設定で必要なログが記録されるとは限らないことに注意が必要です。インシデントが起きる前に実際のログを利用した訓練を行い、取得しているログの項目や保存期間が十分か確認しましょう。

- 不正ログインに対する分析の視点の例を示します。

分析の視点	内容
いつ（When）	日時、時間帯（日中なのか、夜間なのか。） ※時刻の正確さが重要です。NTP等で時刻同期しましょう。時刻がずれていると、ログの突合に苦労します。
誰が（Who）	ログオンID（管理者、利用者）
どこから（Where）	接続元IPアドレス（許可しているIPアドレスか。海外か。）
何を用いて（How）	ログオン手段（実習2はRDP）
どうなった（What）	処理結果。ログオン失敗、成功。

ログ分析のTIPS（2）

- 特に大容量のログを扱う場合、（できれば）高スペックなマシンで行います。
- 初めは軽いツールで絞り込みます。最初から高機能なツールに大容量のログを読み込ませると時間がかかります。動作の軽いツールで絞り込み、ログサイズを小さくします。

- ログ分析で重要になるのがツールです。多くの場合、ログは大容量になるので、ExcelやWindows上のフリーソフトなどでは処理能力の面から力不足になることが多いです。なお、昨今はアプリケーションの能力（Excel等含む）の大幅な向上により、問題ないことも多くなりました。
- Windows標準のログ参照ツール（イベントビューア）は、機能不足です。効率的に行うためには別の手法を推奨します。

  ①ツール等を利用して、イベントログを抽出。本勉強会では、Evtx Explorer/EvtxECmd（※1）を利用します。

  ※1　Eric Zimmerman's tools
  https://ericzimmerman.github.io/

  ②抽出したログを、ログ分析ツールや表計算ソフトで調査

講義

Windowsイベントログ

- **Windowsのログオン、ログオフに関するイベントIDは次のとおりです。事前にログの意味を知ることで、迅速・効率的に分析ができます。**

分類	イベントID	概要	概要
Logon/Logoff	**4624**	Successful logon	ログオン成功
Logon/Logoff	**4625**	Failed logon	ログオン失敗
Logon/Logoff	**4634**	An account was logged off	ログオフ
Logon/Logoff	**4647**	User initiated logoff	ログオフ
Privilege Use	**4672**	Administrative logon	特権ログオン

分類	備考
Logon/Logoff	・「Logon Type」の数値でログオンの種類がわかる。 2：対話型ログオン **3：ネットワーク経由** 5：Windowsサービス ・「Logon Id」で、ログオンとログオフのイベントを関連付けられる。
Privilege Use	・「Logon Id」で、ログオンとログオフのイベントを関連付けられる。

- **（参考資料）Windows で出力されるセキュリティ イベントの一覧情報について**
  https://blogs.technet.microsoft.com/jpntsblog/2017/02/27/security-event/

実　習　１　イベントログ解析

- 「別紙.TIPS-2 実習資料」を参照し、開発用サーバのイベントログを調査し、攻撃内容を推測してください。

実習時間
20分間

まとめ（TIPS1、TIPS2）

仮説を立て、調査し、事実を確認します。さらに仮説を立て、調査（繰り返し）します。

事前の準備が大切です。（普段の状態を知る、連絡体制を確立する、非常時のルール・権限を決める、ログの調査方法を定める）

Wiresharkの機能を活用することで、ネットワーク上に流れるデータの取得および分析ができます。

ログの意味を事前に把握することで、迅速・効率的に分析できます。インシデント対応は限られた時間での勝負になります。